From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C)]sdoj.gov>
Sent: Wednesday, May 18, 2011 3:12 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: What do your schedules look like on June 9?

Do we have a telephone number for (b)(6),(b)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Wednesday, May 18, 2011 2:36 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(@cambridgepolice.org
Subject: RE: What do your schedules look like on June 9?

(b)(6),(b)(7)(C) called but said he was not officially representing (b)(6),(

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Wednesday, May 18, 2011 2:33 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) @cambridgepolice.org
Subject: RE: What do your schedules look like on June 9?

We're having grand jury scheduling problems and it may be important to have you on the 9th, if at all possible. I am having to move the witnesses scheduled for the 26th to the 9th, after which grand jury availability becomes uncertain.

Also, please send me the name and contact information for the attorney who said he was representing (b)(5), per EOUSA

From: (b)(6),(b)(7)(C) BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Wednesday, May 18, 2011 2:29 PM
To: (b)(6),(b) @cambridgepolice.org; Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: RE: What do your schedules look like on June 9?

I am on travel Rotation from May 24 to June 20 which means it is possible I could be sent on a trip. The Massachusetts Attorney's General Office, Cyber Crime Initiative has training on the 9th, it is not mandatory but I would like to attend if we could present on another day.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: Wednesday, May 18, 2011 1:57 PM
To: (b)(6),(b)(7)(C) @sdoj.gov (b)(6),(b)(7)(C) (BOS)
Subject: Re: What do your schedules look like on June 9?

I will be away from June 6 - 18, 2011.

From: Heymann, Stephen (USAMA) [redacted]@usdoj.gov>
To: [redacted](BOS) [redacted]usss.dhs.gov> [redacted]
Sent: Wed May 18 13:36:27 2011
Subject: What do your schedules look like on June 9?

(b)(3):Rule 6E

Per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, May 18, 2011 2:33 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) BOS); Extern (b)(6),(b) ambridgepolice.org
Subject: RE: What do your schedules look like on June 9?

We're having grand jury scheduling problems and it may be important to have you on the 9th, if at all possible. I am having to move the witnesses scheduled for the 26th to the 9th, after which grand jury availability becomes uncertain.

Also, please send me the name and contact information for the attorney who said he was representing (b)

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, May 18, 2011 2:29 PM
To: (b)(6),(b) cambridgepolice.org; Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) BOS)
Subject: RE: What do your schedules look like on June 9?

I am on travel Rotation from May 24 to June 20 which means it is possible I could be sent on a trip. The Massachusetts Attorney's General Office, Cyber Crime initiative has training on the 9th, it is not mandatory but I would like to attend if we could present on another day.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (b)(6),(b) (7)(C) [mailto cambridgepolice.org]
Sent: Wednesday, May 18, 2011 1:57 PM
To: (b)(6),(b)(7)(C) usdoj.gov'; (b)(6),(b)(7)(C) BOS)
Subject: Re: What do your schedules look like on June 9?

I will be away from June 6 - 18, 2011.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Wed May 18 13:36:27 2011
Subject: What do your schedules look like on June 9?

(b)(3):Rule 6E

steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, May 18, 2011 1:57 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) (BOS)
Subject: Re: What do your schedules look like on June 9?

I will be away from June 6 - 18, 2011.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) sss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Wed May 18 13:36:27 2011
Subject: What do your schedules look like on June 9?

(b)(3):Rule 6E

steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, May 18, 2011 1:36 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: What do your schedules look like on June 9?

(b)(3):Rule 6E

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, May 12, 2011 11:33 AM
To: (b)(6),(b)(7)(C) BOS); External-(b)(6), @cambridgepolice.org
Subject: Seizure Warrant Affidavit

Please let me know when you are final with the final version of the affidavit or any other changes that should be made. Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Thursday, May 12, 2011 10:44 AM
To: (b)(6),(b)(7)(C),Per USSS (BOS); External (b)(6), (b)(7)(C) @cambridgepolice.org
Subject: Concerning File Names

From: (b)(6),(b)(7)(C) [mailto: (b)(6),(b)(7)(C) @haka.org]
Sent: Wednesday, May 11, 2011 5:36 PM
To: Heymann, Stephen (USAMA)
Subject: FW: Could you check one thing in the morning for me?

Hi Steve,

Please see (b)(6), (b)(7) response below. As you can see, this is fairly complex!

Let me know if you need to discuss further with (b)(6),(b)(7)(C)
(b)(6), (b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Wednesday, May 11, 2011 4:59 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Could you check one thing in the morning for me?

Thanks (b)(6),(b)(7)(C)

(b)(5),(b)(6),(b)(7)(C)

per EOUSA

(b)(5),(b)(7)(C)

per EOUSA

Best,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, May 10, 2011 6:18 PM
To: (b)(6),(b)(7)(C)
Subject: Could you check one thing in the morning for me?

(b)(5)

per EOUSA

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, May 11, 2011 5:14 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: First Thing Thursday Morning

Please call and fill in (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, May 11, 2011 5:13 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Re: First Thing Thursday Morning

Interview with (b)(6),(b)(7)(C) complete

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(7)(C) cambridgepolice.org
Sent: Wed May 11 16:59:15 2011
Subject: First Thing Thursday Morning

<<Seizure Warrant Aff. Draft 5-11-10 updated.pdf>> This is an updated version of your proposed affidavit for the seizure warrant. First thing in the morning on Thursday (we want to get it before the judge as early in the day as possible):

(b)(6),(b)(7)(C)

Thanks you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, May 11, 2011 4:59 PM
To: (b)(6),(b)(7)(C),Per USS BOS)
Cc: External (b)(6),(b)(cambridgepolice.org
Subject: First Thing Thursday Morning
Attachments: Seizure Warrant Aff. Draft 5-11-10 updated.pdf

<<Seizure Warrant Aff. Draft 5-11-10 updated.pdf>> This is an updated version of your proposed affidavit for the seizure warrant. First thing in the morning on Thursday (we want to get it before the judge as early in the day as possible):

(b)(5),(b)(7)(C)

per EOUSA

Thanks you, Steve

From: (b)(6),(b)(7)(C) cert.org>
Sent: Wednesday, May 11, 2011 3:46 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C)
Subject: Re: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(5),(b)(6),(b)(7)(C)

Again, please let us know if you have any questions or you can reach us at (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Wed, 11 May 2011 14:19:23 -0400
To: (b)(6),(b)(7)(C) @cert.org>, (b)(6),(b)(7)(C) cert.org>
Subject: Fw: Potential Additional Paragraphs for the Seizure Warrant Affidavit

Feedback on this is also appreciated.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) Desk)
Mobile)
412-288-5226 (Fax)

From: (b)(6),(b)(7)(C) BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) usdoj.gov>
Cc: External (b)(6),(b) @cambridgepolice.org (b)(6),(b)(7)(C) cert.org> (b)(6),(b)(7)(C) (CID)
Sent: Tue May 10 15:25:25 2011
Subject: RE: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(5)

(b)(5)

(b)(5)

I emailed (b)(6), (b)(7)(and (b)(6), (b)(7)(to confirm this

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephan (USAMA) [mailto:(b)(6),(b)(7)(C) @doj.gov]
Sent: Tuesday, May 10, 2011 8:14 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: Potential Additional Paragraphs for the Seizure Warrant Affidavit

Please confirm the following today, contacting CERT and MIT as necessary. These are the facts, as I presently understand them. If any of them should be corrected or expanded, let me know.

(b)(5)

Per EOUSA

(b)(5)

Per EOUSA

Thank you, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cert.org>
Sent: Wednesday, May 11, 2011 3:34 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C)
Subject: Re: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(6),(b)(7)(C)

(b)(5)

Please let me know if this answers your questions. You can also reach us at (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) @usss.dhs.gov>
Date: Wed, 11 May 2011 14:18:26 -0400
To: (b)(6),(b)(7)(C) cert.org> (b)(6),(b)(7)(C) cart.org>
Subject: Fw: Potential Additional Paragraphs for the Seizure Warrant Affidavit

Gentlemen:

Could you take a look this request and provide some feedback.

(b)(6),(b)(7)(C)

Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (b)(6),(cert.org>
Cc: (CID)
Sent: Tue May 10 14:55:02 2011
Subject: FW: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(5)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, May 10, 2011 8:14 AM
To: (b)(6),(b)(7)(C) BOS)
Cc: (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(5)

(b)(5)

Thank you, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, May 11, 2011 10:02 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b) cambridgepolice.org
Subject: Draft Seizure Warrant Affidavit
Attachments: Seizure Warrant Affidavit 5-11-11 Draft.pdf

<<Seizure Warrant Affidavit 5-11-11 Draft.pdf>> (b)(6),

per EOUSA

Attached is the current draft of the affidavit in support of the seizure warrant. Please review it carefully, and let me know, any changes of any form that are necessary or appropriate.

(b)(5)

Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, May 10, 2011 4:55 PM
To: (b)(6),(b)(7)(C),Per USSS (BOS)
Subject: Sample .pdf

Please e-mail to me a sample .pdf from the pdf folder on the (b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) ambridgepolice.org>
Sent: Tuesday, May 10, 2011 2:18 PM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Subject: RE: Last Thing

(b)(6),(b)(7)(C)

Still waiting on information about other agencies.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, May 10, 2011 11:12 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C)
Subject: RE: Last Thing

(b)(6),(b)(7)(C)

RACE:
SEX:
DOB:
SSN:

(b)(6),(b)(7)(C)

and NCIC shows no criminal record for (b)(6), (b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, May 10, 2011 9:38 AM
To: (b)(6),(b)(7)(C),Per (BOS); External-(b)(6),(b)(7) cambridgepolice.org
Subject: Last Thing

(b)(5)

per EOUSA

Thanks again, Steve

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, May 10, 2011 2:09 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Last Thing

I've put a request in to get (b)(6), place of birth from another entity. Waiting on their reply. That will also include agency indices inquiry.

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, May 10, 2011 9:38 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: Last Thing

(b)(5),(b)(6),(b)(7)(C)

Per EOUSA

Thanks again, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, May 10, 2011 11:13 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Last Thing

Thank you

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, May 10, 2011 11:12 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(cambridgepolice.org
Subject: RE: Last Thing

(b)(6),(b)(7)(C)

RACE:
SEX:
DOB:
SSN:

(b)(6),(b)(7)(C)

and NCIC shows no criminal record for (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, May 10, 2011 9:38 AM (b)(6),(b)
To: (b)(6),(b)(7)(C) (BOS); External (7)(C),Per cambridgepolice.org
Subject: Last Thing

(b)(5) per EOUSA

Thanks again, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, May 10, 2011 9:38 AM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Last Thing

(b)(5)

per EOUSA

Thanks again, Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, May 10, 2011 9:07 AM
To: (b)(6),(b)(7)(C) (BOS); Extemal (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: (b)(6),(b)(7)(C)

And place of birth?

From: Heymann, Stephen (USAMA)
Sent: Tuesday, May 10, 2011 9:06 AM
To: (b)(6),(b)(7)(C),Per (BOS)'; (b)(6),(b)(7)(C)
Subject: (b)(6),(b)(7)(C)

What are (b)(6),(b)(7)(C) D.O.B. and Social Security number?

Thanks, Steve

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C)]usdoj.gov>
Sent: Tuesday, May 10, 2011 9:06 AM
To: [(b)(6),(b)(7)(C)] BOS); External [(b)(6),(b)(7)(C)]@cambridgepolice.org
Subject: [(b)(6),(b)(7)(C)]

What are [(b)(6),(b)(7)(C)] D.O.B. and Social Security number?

Thanks, Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, May 10, 2011 8:14 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(cambridgepolice.org
Subject: Potential Additional Paragraphs for the Seizure Warrant Affidavit

(b)(5)

per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, May 09, 2011 3:44 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please let me know when you get something from (b)(5) Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, May 05, 2011 5:16 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Twitter

please

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, May 05, 2011 5:16 PM
To: Heymann, Stephen (USAMA)
Subject: Re: Twitter

It says +0. But I am not sure if that means local or GMT. I can call and ask.

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu May 05 17:13:39 2011
Subject: RE: Twitter

(b)(3):Rule 6E

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, May 05, 2011 4:49 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Twitter

IP	DATE	TIME	PROVIDER
(b)(6),(b)(7)(C)	14-Feb-11	16:41	Comcast
	14-Feb-11	0:03	Amazon Web Services, Elastic Compute Cloud EC2
	13-Feb-11	4:59	Harvard University
	11-Feb-11	11:11	Harvard University
	11-Feb-11	12:09	T-Mobile
	9-Feb-11	14:54	T-Mobile
	6-Feb-11	14:22	T-Mobile
	4-Feb-11	22:51	T-Mobile
	4-Feb-11	10:51	T-Mobile
	29-Jan-11	0:52	T-Mobile
	28-Jan-11	19:10	Harvard University
	27-Jan-11	3:19	T-Mobile
	27-Jan-11	9:19	T-Mobile
	27-Jan-11	12:19	T-Mobile
	26-Jan-11	21:04	T-Mobile

(b)(6),(b)(7)(C)

19-Jan-11	4:41	Comcast
18-Jan-11	1:41	Comcast Business Communications
18-Jan-11	4:41	T-Mobile
18-Jan-11	19:41	T-Mobile
18-Jan-11	22:41	T-Mobile
17-Jan-11	1:20	T-Mobile
17-Jan-11	7:35	T-Mobile
16-Jan-11	21:05	Harvard University
16-Jan-11	1:20	T-Mobile
16-Jan-11	4:20	T-Mobile
13-Jan-11	0:30	T-Mobile
13-Jan-11	3:30	T-Mobile
13-Jan-11	12:46	T-Mobile
12-Jan-11	2:22	T-Mobile
12-Jan-11	22:33	T-Mobile
25-Dec-10	16:33	Comcast
25-Dec-10	21:52	T-Mobile
24-Dec-10	14:30	T-Mobile
24-Dec-10	20:30	T-Mobile
19-Dec-10	19:32	T-Mobile

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
Sent: Thursday, May 05, 2011 5:14 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Twitter

(b)(3):Rule 6E

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thursday, May 05, 2011 4:49 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: Twitter

IP	DATE		IDER
(b)(6),(b)(7)(C)	14-Feb-11		cast
	14-Feb-11		astic Compute Cloud EC2
		4:59	Harvard University
		11:11	Harvard University
		12:09	T-Mobile
		14:54	T-Mobile
		14:22	T-Mobile
		22:51	T-Mobile
		10:51	T-Mobile
		0:52	T-Mobile
		19:10	Harvard University
		3:19	T-Mobile
		9:19	T-Mobile
		12:19	T-Mobile
		21:04	T-Mobile
		4:41	Comcast
		1:41	Comcast Business Communications
		4:41	T-Mobile
		19:41	T-Mobile
		22:41	T-Mobile
		1:20	T-Mobile
		7:35	T-Mobile
		21:05	Harvard University
		1:20	T-Mobile
		4:20	T-Mobile
		0:30	T-Mobile
		3:30	T-Mobile
		12:46	T-Mobile
		2:22	T-Mobile
		22:33	T-Mobile
		16:33	Comcast

(b)(6),(b)(7)(C)

25-Dec-10	21:52	T-Mobile
24-Dec-10	14:30	T-Mobile
24-Dec-10	20:30	T-Mobile
19-Dec-10	19:32	T-Mobile

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, May 05, 2011 3:12 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Done

(b)(5),(b)(7)(C) per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, May 05, 2011 2:02 PM
To: Heymann, Stephen (USAMA)
Subject: Done

Done

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, May 05, 2011 1:53 PM
To: (b)(6),(b)(7)(C) BOS)
Subject:

(b)(5),(b)(7)(C) per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, May 05, 2011 1:53 PM
To: (b)(6),(b)(7)(C) (BOS)

(b)(5),(b)(7)(C)

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, May 03, 2011 3:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: CID/CERT: Feedback from MIT case

Mike,

per EOUSA

I do not know whether this is in your camp or theirs.

(b)(5)

Thanks, Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, May 03, 2011 3:06 PM
To: Heymann, Stephen (USAMA)
Subject: FW: CID/CERT: Feedback from MIT case

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cert.org]
Sent: Tuesday, May 03, 2011 3:05 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C)
Subject: Re: CID/CERT: Feedback from MIT case

(b)(6),(b)(7)(C)

We performed analysis of the Python scripts and bash history you requested and provided our analysis notes in late-March. We have not prepared any other reports as we were waiting for you and Stephen to determine if there was any additional analysis you wanted us to conduct.
If you would like we can prepare a more formal report of the analysis we conducted on the scripts and bash history, however we have not performed any additional analysis outside of those initial requests.

Please let us know how you would like us to proceed.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Tue, 3 May 2011 14:07:45 -0400
To: (b)(6),(b)(7)(C) usss.dhs.gov>, (b)(6),(b)(7)(C) cert.org>, (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) cert.org>
Subject: RE: CID/CERT: Feedback from MIT case

Was a report ever finalized for the Swartz exam?

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, March 16, 2011 1:30 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: CID/CERT: Feedback from MIT case

Sounds good.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5228 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (CID)
Sent: Wed Mar 16 13:28:51 2011
Subject: Fw: CID/CERT: Feedback from MIT case

No 6E letter is necessary

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C),Per (BOS)
Sent: Wed Mar 16 13:25:45 2011
Subject: RE: CID/CERT: Feedback from MIT case

(b)(3):Rule 6E,(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) uscg.dhs.gov]
Sent: Wednesday, March 16, 2011 1:13 PM
To: Heymann, Stephen (USAMA)
Subject: Fw: CID/CERT: Feedback from MIT case

Question from CERT

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 4:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: linode

Thx. Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, April 15, 2011 4:43 PM
To: Heymann, Stephen (USAMA)
Subject: linode

I just spoke with linode.com (609-593-7103) and they confirmed that www.aaronsw.com/weblog/theinfo is hosted on their server. (b)(5) (b)(5) I will send an updated letter.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 3:24 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C),Par cambridgepolice.org
Subject: Weblog

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 3:02 PM
To: (b)(6),(b)(7)(C) [BOS]; External-(b)(6),(b) cambridgepolice.org
Subject: Guerillaopenaccess.com

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 2:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Guerrilla Open Access Manifesto

Yes. Can you two give me a call. I will fill you in.

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, April 15, 2011 1:28 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Guerrilla Open Access Manifesto

Did the meeting occur today?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Friday, April 15, 2011 12:30 PM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(cambridgepolice.org
Subject: Guerrilla Open Access Manifesto

> ...*The Open Access Movement* has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.
> That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.
> "I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.
> Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.
> Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.
> But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.
> Large corporations, of course, are blinded by greed....
> There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.
> We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks....

http://www.earlham.edu/~peters/fos/2008/09/guerilla-oa.html

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 12:32 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: re: Guerilla Open Access

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, April 15, 2011 12:30 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Guerrilla Open Access Manifesto

...*The Open Access Movement* has fought valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

"I agree," many say, "but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there's nothing we can do to stop them." But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed....

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks....

http://www.earlham.edu/~peters/fos/2008/09/guerilla-oa.html

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Thursday, April 14, 2011 5:25 PM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov)
Cc: (b)(6),(b)(7)(C) BOS)
Subject: Updates of April 14, 2011 Swartz Investigation

Steve,

Item 1:

(b)(6),(b)(7)(C) reached out to me. The lease is up at the end of May 2011. Aaron asked to be a tenant at will, month to month, going forward. He told the landlord that he is probably starting a new job in September in New York and would probably move there in August.

Item 2:

I sat down with the fingerprint analyst today at CPD. I was reviewing the file, her notes, reports etc.

About a month ago I asked her to run (b)(6),(b)(7)(C) prints against prints recovered. I asked her about what she found and she said, "I can't eliminat (b)(6),(b)(7) I asked her to elaborate on this and she said she has a five point match on (b)(6),(b)(7) from the screen of the Acer.

In some prosecutorial regions, a five point match is sufficient, however, Cambridge Police / Massachusetts has a higher number then that.

With this in mind I had photos of the Acer, the fingerprint and (b)(6),(b)(7)(C) fingerprint card printed out in full glory.

(b)(5),(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, April 11, 2011 5:53 PM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: (b)(5),(b)(6),(b)(7)(C)

Per EOUSA

D.O.B.:

FBI I.D. No.:

Birthplace:

Address of Witness:

Alias(s):

SSN:

Thanks, Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Thursday, April 07, 2011 1:24 PM
To: (b)(6),(b)(7)(C) @usdoj.gov' (b)(6),(b)(7)(C) BOS)
Subject: R (b)(6),(b)(7)(C) Rescheduled

Rec'd,

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C), @usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Thu Apr 07 12:59:38 2011
Subject: (b)(6),(b)(7)(C Rescheduled

(b)(6),(b)(7)(C) 's proffer has been rescheduled to 12:30 on Wednesday the 13th, here. (i.e., tomorrow afternoon is off) (b) , enjoy the last of your paternity leave in peace. Call for details. Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, April 07, 2011 1:00 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6), (b)(7)(C) @cambridgepolice.org
Subject: (b)(6),(b)(7)(C) Rescheduled
Importance: High

(b)(6),(b)(7)(C)'s proffer has been rescheduled to 12:30 on Wednesday the 13th, here. (i.e., tomorrow afternoon is off (b)(6), enjoy the last of your paternity leave in peace. Call for details. Steve

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, April 06, 2011 7:18 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Response to Harvard Subpoena

Are you back in work?

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, April 05, 2011 5:38 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Response to Harvard Subpoena

Any returns I did not give you should be in the grey file cabinet to the right of my desk unless it came in after I left. I think I remember the harvard return coming in but I am not sure.

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(7)(C) cambridgepolice.org
Sent: Tue Apr 05 15:26:20 2011
Subject: Response to Harvard Subpoena

(b)(3):Rule 6E,(b)(5)

Per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, April 05, 2011 3:26 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: Externa (b)(6),(b) @cambridgepolice.org
Subject: Response to Harvard Subpoena

(b)(3):Rule 6E,(b)(5)

Per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, April 04, 2011 3:02 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: (b)(6),(b)(7)(C)

per EOUSA

Can you give me a call. I need to schedule (b)(6),(b)(7)(C) on (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Monday, April 04, 2011 2:28 PM
To: Heymann, Stephen (USAMA) cambridgepolice.org
Subject: Re: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

Understood

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Sent: Mon Apr 04 11:32:24 2011
Subject: FW: (b)(6),(b)(7)(

(b)(3):Rule 6E,(b)(7)(C)

Per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Monday, April 04, 2011 11:30 AM
To: (b)(6), weinsteinlaw.com
Subject: (b)(6),(b)(7)(C)

(b)(3):Rule 6E,(b)(7)(C)

per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, April 04, 2011 11:32 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: FW: (b)(6),(b)(7)(C)

(b)(3):Rule 6E,(b)(7)(C)

per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Monday, April 04, 2011 11:30 AM
To: (b)(6), weinsteinlaw.com
Subject: (b)(6),(b)(7)(C)

(b)(3):Rule 6E,(b)(7)(C)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Thursday, March 31, 2011 1:29 PM
To: (b)(6),(b)(7)(C) BOS); External: (b)(6), @cambridgepolice.org
Subject: Re: (b)(6),(b)(7)(C)

Can you two do the 8th instead of the 15th for (b)(7)(C) per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, March 30, 2011 04:52 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C) cambridgepolice.org (b)(6),(b)(7)(C) cambridgepolice.org>
Subject: (b)(6),(b)(7)(C)

BTW, per EOUSA

Still no response from (b)(6),(b)(7)(C) to any of my inquiries, so I do not know what is going on with respect to (b)(6),(b)(7)(C) and the grand jury on the 7th.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, March 30, 2011 5:17 PM
To: (b)(6),(b)(7)(C) usdoj.gov>; (b)(6),(b)(7)(C) BOS)
Subject: Re: (b)(6),(b)(7)(C)

Well I'll be there the morning of the 7th to give him the opportunity to talk. If (b)(6),(is back, he'll be there or I'll have another person with me.

From: (b)(6),(b)(7)(C) (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C),P usss.dhs.gov>; (b)(6),(b)(7) @usss.dhs.gov>; (b)(6),(b)(7)(C),Per USSS
Sent: Wed Mar 30 16:52:05 2011
Subject: (b)(6),(b)(7)(C)

BTW, per EOUSA

Still no response from (b)(6),(b)(7)(C) to any of my inquiries, so I do not know what is going on with respect to (b)(6),(b)(7)(C) and the grand jury on the 7th.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, March 30, 2011 4:52 PM
To: (b)(6),(b)(7)(C) BOS); External-(b)(6),(b)(7)(C) cambridgepolice.org
Subject: (b)(6),(b)(7)(C)

BTW,

per EOUSA

Still no response from (b)(6),(b)(7)(C) to any of my inquiries, so I do not know what is going on with respect to (b)(6),(b)(7)(C) and the grand jury on the 7th.

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, March 24, 2011 7:19 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: FW (b)(3):Rule 6E
Attachments: (b)(3):Rule 6E

per EOUSA

From: (b)(3):Rule Legal [mailto:twitter-legal@(b) com]
Sent: Thursday, March 24, 2011 7:17 PM
To: Heymann, Stephen (USAMA)
Subject: per EOUSA (b)(3):Rule 6E

Dear Mr. Heymann:

(b)(3):Rule 6E,(b)(7)(C)

per EOUSA

Sincerely,

(b)(3):Rule 6E per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 23, 2011 9:46 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Either or both of you guys around an available to talk before 3:00?

I just put in a call to (b)(7)(C) per EOUS attorney. I'll let you know when I hear back from him.

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, March 23, 2011 9:44 AM
To: Heymann, Stephen (USAMA); (b)(6),(b) @cambridgepolice.org
Subject: Re: Either or both of you guys around an available to talk before 3:00?

(b)(6),(b) briefed me. All seems to be going well

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) BOS)
Sent: Wed Mar 23 09:34:19 2011
Subject: RE: Either or both of you guys around an available to talk before 3:00?

Sorry (b)(7)(C) called me directly and I thought you were (b)(7)(C) per EOUSA (b)(7)(C) per EOUSA but feel free to give me a call tomorrow if you want an update. I'm then out of pocket until April 4.

Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Tuesday, March 22, 2011 3:20 PM
To: Heymann, Stephen (USAMA); (b)(6),(b) @cambridgepolice.org
Subject: Re: Either or both of you guys around an available to talk before 3:00?

I dialed in but did not hear anyone else

(b)(6),(b)(7)(C)
Sent from Blackberry

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
To: Extema (b)(6),(b) @cambridgepolice.org (b)(6),(b)(7)(C) BOS)
Sent: Tue Mar 22 14:41:42 2011
Subject: RE: Either or both of you guys around an available to talk before 3:00?

Please dial (b)(7)(C) per EOUSA

Passcod(b)(7)(C) per EOUSA

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, March 22, 2011 2:13 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) @usss.dhs.gov'
Subject: Re: Either or both of you guys around an available to talk before 3:00?

I will be cutting it close for 3pm but should make it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C),Per (BOS) <(b)(6),(b)(7)(C), @usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Tue Mar 22 12:45:17 2011
Subject: Either or both of you guys around an available to talk before 3:00?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, March 23, 2011 9:34 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Either or both of you guys around an available to talk before 3:00?

Sorry (b)(7)(C) called me directly and I thought you were (b)(7)(C) per EOUSA but feel free to give me a call tomorrow if you want an update. I'm then out of pocket until April 4.
Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, March 22, 2011 3:20 PM
To: Heymann, Stephen (USAMA); (b)(6),(b) @cambridgepolice.org
Subject: Re: Either or both of you guys around an available to talk before 3:00?

I dialed in but did not hear anyone else

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: Externa (b)(6), @cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Sent: Tue Mar 22 14:41:42 2011
Subject: RE: Either or both of you guys around an available to talk before 3:00?

Please dial (b)(7)(C) per EOUSA
Passcode (b)(7)(C) per EOUSA

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @cambridgepolice.org]
Sent: Tuesday, March 22, 2011 2:13 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) @usss.dhs.gov
Subject: Re: Either or both of you guys around an available to talk before 3:00?

I will be cutting it close for 3pm but should make it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C),P usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Tue Mar 22 12:45:17 2011
Subject: Either or both of you guys around an available to talk before 3:00?

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 16, 2011 2:36 PM
To: (b)(6),(b)(7)(C) (BOS); External-(b)(6),(b) cambridgepolice.org
Subject: (b)(3):Rule 6E per EOUSA

(b)(3):Rule 6E per EOUSA

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, March 16, 2011 1:30 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: CID/CERT: Feedback from MIT case

Sounds good.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) Desk)
(Mobile)
412-288-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (CID)
Sent: Wed Mar 16 13:28:51 2011
Subject: Fw: CID/CERT: Feedback from MIT case

No 6E letter is necessary

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Mar 16 13:25:45 2011
Subject: RE: CID/CERT: Feedback from MIT case

(b)(5) per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, March 16, 2011 1:13 PM
To: Heymann, Stephen (USAMA)
Subject: Fw: CID/CERT: Feedback from MIT case

Question from CERT

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) (CID)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Mar 16 13:10:51 2011

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 16, 2011 1:26 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: CID/CERT: Feedback from MIT case

(b)(5) per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, March 16, 2011 1:13 PM
To: Heymann, Stephen (USAMA)
Subject: Fw: CID/CERT: Feedback from MIT case

Question from CERT

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) (CID)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Mar 16 13:10:51 2011
Subject: CID/CERT: Feedback from MIT case

Mike:

The guys here have some a report for you. However, their supervisor needs to review it before it goes out.

Should we add him to the 6e?

His name is (b)(6),(b)(7)(C) He is title is Technical Manager for the Digital Intelligence and Investigations Directorate. He has the same address as (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

All he is doing is reviewing the report.

Thanks.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Saturday, March 12, 2011 5:45 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Update

I heard. CONGRATULATIONS! Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, March 11, 2011 08:57 PM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C)
Cc: (b)(6),(b) @cambridgepolice.org <(b)(6),(b)(7)(C) cambridgepolice.org>
Subject: Re: Update

I apologize for not responding earlier. (b)(6),(b)(7)(C) I have not been able look for (b)(6),(b)(7)(C again. (b)(6),(b)(7 and I will come up with a plan.

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b) @cambridgepolice.org
Sent: Fri Mar 11 15:05:20 2011
Subject: Update

Anything further on locating (b)(6),(b)(7)(C) ? per EOUSA

(b)(3):Rule 6E

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, March 11, 2011 3:05 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External-(b)(6),(b) cambridgepolice.org
Subject: Update

Anything further on locating (b)(6),(b)(7)(C) **?** per EOUSA

(b)(3):Rule 6E

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, March 10, 2011 2:32 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Aaron Swartz

Thx.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, March 10, 2011 2:30 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Aaron Swartz

I re-faxed the original subpoena with a memorandum with the additional information they requested.

Today, I received the return from Equifax. It does list an American Express account. The Acer was bought from MicroCenter with an American Express.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, March 10, 2011 1:46 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Aaron Swartz

(b)(3):Rule 6E

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, March 09, 2011 10:58 AM
To: Heymann, Stephen (USAMA)
Subject: FW: Aaron Swartz
Importance: High

FYI

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Subpoena, Mail [mailto:subpoenamail@ (b)(3):Rule com]
Sent: Wednesday, March 09, 2011 10:57 AM
To: (b)(6),(b)(7)(C) (BOS); Subpoena, Mail
Subject: RE: Aaron Swartz
Importance: High

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, March 10, 2011 1:46 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Aaron Swartz

(b)(3):Rule 6E

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, March 09, 2011 10:58 AM
To: Heymann, Stephen (USAMA)
Subject: FW: Aaron Swartz
Importance: High

FYI

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Subpoena, Mail [mailto:subpoenamail@(b)(3):Rule 6E .com]
Sent: Wednesday, March 09, 2011 10:57 AM
To: (b)(6),(b)(7)(C) (BOS); Subpoena, Mail
Subject: RE: Aaron Swartz
Importance: High

(b)(6),(b)(7)(C)

We need the subpoena and the additional information under one cover. Once you submit this info, we will be happy to comply with your request.

Kind regards,

~~~
~~~

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, March 10, 2011 1:32 PM
To: (b)(3):Rule 6E,(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Failure to Respond to Grand Jury Subpoena

(b)(3):Rule 6E,(b)(7)(C)

per EOUSA

Stephen Heymann

Assistant U.S. Attorney

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) gov>
Sent: Thursday, March 10, 2011 12:23 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: (b)(6),(b)(7)(C)

Can you set up a time we can hear what happened?

From: (b)(6),(b)(7)(C) BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, March 09, 2011 7:54 PM
To: Heymann, Stephen (USAMA)
Subject: Fw: (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
Sent from Blackberry

---- Original Message ----
From: (b)(6),(b)(7)(C) (SFO)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Mar 09 19:19:09 2011
Subject: RE: (b)(6),(b)(7)(C)

Talked to (b)(6),(b) today. I'll give you a call tomorrow since it is after hours there, but (b)(6) basically stated that (b) doesn't know anything. Wasn't standoffish at all, very cooperative. I served (b) with the subpoena as well.

----Original Message----
From: (b)(6),(b)(7)(C) BOS)
Sent: Tuesday, March 08, 2011 4:29 PM
To: (b)(6),(b)(7)(C) SFO)
Subject: Re: (b)(6),(b)(7)(C)

Thank you very much

(b)(6),(b)(7)(C)

Sent from Blackberry

---- Original Message ----
From: (b)(6),(b)(7)(C) SFO)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Tue Mar 08 19:27:23 2011
Subject: (b)(6),(b)(7)(C)

Just an FYI, I have yet to interview (b)(6),(b)(7)(C),(b)(7)(E) (I can't believe I just wrote that) and (b)(6) flew from Oakland to JFK over the weekend. (b) flew back to Oakland last week and was only in town for a few days before flying back to NY, and that was when we only had the San Francisco address. I suspect (b) does this often for work, so I will stay on top of it until I can finally catch up with (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) @cert.org>
Sent: Wednesday, March 09, 2011 4:31 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Rough Chronology

Stephen,

We also wanted to pass along the username for the DynDNS account used on the Acer laptop. We identified the name after our phone call earlier.

host: ghost-laptop.dyndns-free.com
user: ghost4905

Please let us know if you have any questions.

(b)(6),(b)(7)(C)

From: "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) usdoj.gov>
Date: Wed, 9 Mar 2011 15:17:53 -0500
To: (b)(6),(b)(7)(C) cert.org>
Cc: (b)(6),(b)(7)(C) cert.org>, (b)(6),(b)(7)(C) usss.dhs.gov>
Subject: Rough Chronology

Attached is a rough chronological sketch which contains most of the relevant identities, MAC addresses and IP addresses identified to date used during the fraud and theft.

Steve

<<Rough Chronological Sketch.pdf>>

From:	Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent:	Wednesday, March 09, 2011 3:18 PM
To:	(b)(6),(b)(7)(C)
Cc:	(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (BOS)
Subject:	Rough Chronology
Attachments:	Rough Chronological Sketch.pdf

Attached is a rough chronological sketch which contains most of the relevant identities, MAC addresses and IP addresses identified to date used during the fraud and theft.

Steve

<<Rough Chronological Sketch.pdf>>

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, March 09, 2011 12:50 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Have we received the response to the (b) (3) Rule subpoena yet?

From: (b)(6),(b)(7)(C) @cert.org>
Sent: Wednesday, March 09, 2011 11:31 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID)
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

Follow Up Flag: Follow up
Flag Status: Completed

Here is the phone bridge information. I have booked the line from 1 to 2 Eastern.
Looking forward to speaking with you then.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Participant code

From: "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) @usdoj.gov>
Date: Wed, 9 Mar 2011 10:49:07 -0500
To: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) @usss.dhs.gov>, (b)(6),(b)(7)(C) @cert.org>
Cc: (b)(6),(b)(7)(C) @cert.org>
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Works for me, Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, March 09, 2011 10:37 AM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA)
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Would 1300 today work for everyone? Do you have the ability to host a conference call?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cert.org]
Sent: Wednesday, March 09, 2011 10:36 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

We can, but we haven't had the opportunity to look at much beyond the python script and the bash history.
Let us know what is a good time for you. We are free all day today.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) @usss.dhs.gov>
Date: Wed, 9 Mar 2011 10:23:06 -0500

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 09, 2011 10:49 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Works for me, Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, March 09, 2011 10:37 AM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA)
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Would 1300 today work for everyone? Do you have the ability to host a conference call?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7) [mailto (b)(6),(b)(7)(C) cert.org]
Sent: Wednesday, March 09, 2011 10:36 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: Re: bash history of Acer involved with MIT hack and downloading from JSTOR

We can, but we haven't had the opportunity to look at much beyond the python script and the bash history.
Let us know what is a good time for you. We are free all day today.

(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Wed, 9 Mar 2011 10:23:06 -0500
To: (b)(6),(b)(7)(C) cert.org>
Subject: RE: bash history of Acer involved with MIT hack and downloading from JSTOR

Do you mind if we have a conference call with the AUSA.

AUSA Heymann P Stephen
Chief Appellate and Computer Crime Section
(b)(6),(b)(7)(C) @usdoj.gov
Work
Cell

U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, March 08, 2011 8:57 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Update

(b)(6),(b)(7)(C)

I'm coming back later this evening, if your schedule will allow. I'll be available to get this interview completed.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, March 08, 2011 5:04 PM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject: Update

(b)(5),(b)(7)(C)

per EOUSA

Thanks, Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, March 08, 2011 5:04 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External-(b)(6),(b) cambridgepolice.org
Subject: Update

(b)(6),(b)(7)(C)

per EOUSA

Thanks, Steve

From: (b)(6),(b)(7)(C) >cambridgepolice.org>
Sent: Thursday, March 03, 2011 3:32 PM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) BOS)
Subject: (b)(6),(b)(7) Subpoena Review

Steve,

(b)(5)

per EOUSA

Other than that, it is complete and detailed.

Let it rip.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, March 02, 2011 6:03 PM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C)
Subject:

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

per EOUSA

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, March 02, 2011 7:35 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE:

Rec'd

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, March 02, 2011 6:03 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject:

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, March 02, 2011 6:03 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Attachments: (b)(6),(b)(7)(C) Subpoena Attachment 3-2 Draft.pdf

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 02, 2011 2:28 PM
To: Externa (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C) BOS)
Subject: RE: Fingerprint Verification Complete

Thank you for the update. I am preparing the additional subpoenas we need now.

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: Wednesday, March 02, 2011 2:25 PM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Subject: Fingerprint Verification Complete

(b)(6), (b)(7)(C) and Steve,

I received a phone call from CPD Criminalist (b)(6),(b)(7)(C) today. She told me that the Boston Police Identification unit has verified and concurs with her findings regarding a conclusive match of a print belonging to Aaron Swartz being found on the drive contained within the enclosure.

They are gathering all notes and generating formal reports of such, they will pass off all those to me in the beginning of next week.

I'm at Tampa Airport now trying to get on a flight, I'll be in tomorrow.

(b)(6), (b)(7)(C) I'm participating in a warrant sweep starting at 5:00am tomorrow. I should get to the office around 12:00pm.

Thanks

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, March 02, 2011 1:11 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Subpoenas

What telephone number of yours would you like as a contact number for individuals served with subpoenas?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, March 02, 2011 1:05 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Numbers of Interest

(b)(7)(C)
per EOUSA

Can you also check this number: Thx

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Tuesday, March 01, 2011 5:22 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Numbers of Interest

I checked with the NEU Star Law Enforcement Telephone Number Lookup for Ported Numbers:
(b)(6),(b)(7)(C) is a T-Mobile number
is a Verizon number

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, March 01, 2011 5:01 PM
To: External (b)(6),(b) cambridgepolice.org; (BOS)
Subject: RE: Numbers of Interest

(b)(7)(C) per EOUSA Worth interviewing. I'll also prepare a grand jury subpoena tomorrow.

(b)(7)(C) per EOUSA Can you double check these before I reissue subpoenas?

Steve

From: (b)(6),(b)(7)(C) [mailto: (b)(6), (b)(7)(C) @cambridgepolice.org]
Sent: Tuesday, February 22, 2011 11:07 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: Numbers of Interest

Hi Steve,

Below are the numbers we would like to have subpoenaed for ownership records.

AT&T numbers: (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Verizon:

T-Mobile:

Bandwith.com (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

Bandwidth (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

As a result of my conversation with T-Mobile last Friday I was able to glean the following facts.

Internet Addressing: Destination IP and Phone Number IP are generic IP addresses which state that the operator of the phone went out to the Internet. There is no other information available or stored by T-Mobile when an individual accesses the Internet. I asked 18 ways from Sunday for a way to get more information from three different T-Mobile representatives including a tech analyst.

Call Forwarding: When an abbreviation e.g. "SNFC MT – EV, CA" is listed in the Destination Column this indicates that the cell phone operator has placed his phone on "call forward" mode and the number listed under "Phone Number" column is the number the operator punched into the phone directing incoming calls to be forwarded to that number. In the majority of these instances, Swartz has forwarded his calls to (b)(6),(b)(7)(C)

Country Code: 356: Initially upon asking questions all three representatives stated that this was a call from Malta. When pressed that this was not reasonable or logical no explanation was given. In one instance the tech analyst stated that he would do further research and call me back. He never called back and his voicemail now indicates that he is away. After doing some internet research it would not be outlandish to believe that a person calling Swartz might be spoofing their number.

Conference Calling: The two conference calls placed during the month are calls Swartz initiated. He dialed the two numbers listed in the Phone Number column.

Hope this helps in clarification.

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, March 01, 2011 10:00 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Numbers of Interest

Thanks (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C)
Sent: Tue Mar 01 21:03:54 2011
Subject: Re: Numbers of Interest

I hope everything is OK

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) cambridgepolice.org>
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) usdoj.gov>; (b)(6),(b)(7)(C) BOS)
Sent: Tue Mar 01 17:35:24 2011
Subject: Re: Numbers of Interest

Copy that, I'll do an address and person history on him and the address.

I'm in Florida right now with my Father, I am scheduled to return tomorrow.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Tue Mar 01 17:01:04 2011
Subject: RE: Numbers of Interest

(b)(7)(C) per EOUSA Worth interviewing. I'll also prepare a grand jury subpoena tomorrow.

(b)(7)(C) per EOUSA Can you double check these before I reissue subpoenas?

Steve

From: (b)(6),(b)(7)(C) mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, February 22, 2011 11:07 AM
To: Heymann, Stephen (USAMA) (BOS)
Subject: Numbers of Interest (b)(6),(b)(7)(C)

Hi Steve,

Below are the numbers we would like to have subpoenaed for ownership records.

AT&T numbers (b)(6),(b)(7)(C)

Verizon:

T-Mobile:

Bandwith.com (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

Bandwidth (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

As a result of my conversation with T-Mobile last Friday I was able to glean the following facts.

Internet Addressing: Destination IP and Phone Number IP are generic IP addresses which state that the operator of the phone went out to the Internet. There is no other information available or stored by T-Mobile when an individual accesses the Internet. I asked 18 ways from Sunday for a way to get more information from three different T-Mobile representatives including a tech analyst.

Call Forwarding: When an abbreviation e.g. "SNFC MT – EV, CA" is listed in the Destination Column this indicates that the cell phone operator has placed his phone on "call forward" mode and the number listed under "Phone Number" column is the number the operator punched into the phone directing incoming calls to be forwarded to that number. In the majority of these instances, Swartz has forwarded his calls to 415-680-3910.

Country Code: 356: Initially upon asking questions all three representatives stated that this was a call from Malta. When pressed that this was not reasonable or logical no explanation was given. In one instance the tech analyst stated that he would do further research and call me back. He never called back and his voicemail now indicates that he is away. After doing some internet research it would not be outlandish to believe that a person calling Swartz might be spoofing their number.

Conference Calling: The two conference calls placed during the month are calls Swartz initiated. He dialed the two numbers listed in the Phone Number column.

Hope this helps in clarification.

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, March 01, 2011 5:35 PM
To: (b)(6),(b)(7)(C) usdoj.gov'; (b)(6),(b)(7)(C) (BOS)
Subject: Re: Numbers of Interest

Copy that, I'll do an address and person history on him and the address.

I'm in Florida right now with my Father, I am scheduled to return tomorrow.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) dhs.gov>
Sent: Tue Mar 01 17:01:04 2011
Subject: RE: Numbers of Interest

(b)(7)(C) per EOUSA Worth interviewing. I'll also prepare a grand jury subpoena tomorrow.

(b)(7)(C) per EOUS er. Can you double check these before I reissue subpoenas?

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, February 22, 2011 11:07 AM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) BOS)
Subject: Numbers of Interest

Hi Steve,

Below are the numbers we would like to have subpoenaed for ownership records.

AT&T numbers: (b)(6),(b)(7)(C)

Verizon:

T-Mobile:

Bandwith.com (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

Bandwidth (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

As a result of my conversation with T-Mobile last Friday I was able to glean the following facts.

Internet Addressing: Destination IP and Phone Number IP are generic IP addresses which state that the operator of the phone went out to the Internet. There is no other information available or stored by T-Mobile when an individual accesses the Internet. I asked 18 ways from Sunday for a way to get more information from three different T-Mobile representatives including a tech analyst.

Call Forwarding: When an abbreviation e.g. "SNFC MT – EV, CA" is listed in the Destination Column this indicates that the cell phone operator has placed his phone on "call forward" mode and the number listed under "Phone Number" column is the number the operator punched into the phone directing incoming calls to be forwarded to that number. In the majority of these instances, Swartz has forwarded his calls to (b)(6),(b)(7)(C)

Country Code: 356: Initially upon asking questions all three representatives stated that this was a call from Malta. When pressed that this was not reasonable or logical no explanation was given. In one instance the tech analyst stated that he would do further research and call me back. He never called back and his voicemail now indicates that he is away. After doing some Internet research it would not be outlandish to believe that a person calling Swartz might be spoofing their number.

Conference Calling: The two conference calls placed during the month are calls Swartz initiated. He dialed the two numbers listed in the Phone Number column.

Hope this helps in clarification.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, March 01, 2011 5:01 PM
To: External-(b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: Numbers of Interest

(b)(7)(C) per EOUSA Worth interviewing. I'll also prepare a grand jury subpoena tomorrow.

(b)(7)(C) per EOUSA Can you double check these before I reissue subpoenas?

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, February 22, 2011 11:07 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: Numbers of Interest

Hi Steve,

Below are the numbers we would like to have subpoenaed for ownership records.

AT&T numbers: (b)(6),(b)(7)(C)

Verizon:

T-Mobile:

Bandwith.com (competitive local exchange carrier / internet telephony) (b)(6),(b)(7)(C)

Bandwidth (competitive local exchange carrier / internet telephony (b)(6),(b)(7)(C)

As a result of my conversation with T-Mobile last Friday I was able to glean the following facts.

Internet Addressing: Destination IP and Phone Number IP are generic IP addresses which state that the operator of the phone went out to the Internet. There is no other information available or stored by T-Mobile when an individual accesses the Internet. I asked 18 ways from Sunday for a way to get more information from three different T-Mobile representatives including a tech analyst.

Call Forwarding: When an abbreviation e.g. "SNFC MT – EV, CA" is listed in the Destination Column this indicates that the cell phone operator has placed his phone on "call forward" mode and the number listed under "Phone Number" column is the number the operator punched into the phone directing incoming calls to be forwarded to that number. In the majority of these instances, Swartz has forwarded his calls to (b)(6),(b)(7)(C)

Country Code: 356: Initially upon asking questions all three representatives stated that this was a call from Malta. When pressed that this was not reasonable or logical no explanation was given. In one instance the tech analyst stated that he would do further research and call me back. He never called back and his voicemail now indicates that he is away. After doing some internet research it would not be outlandish to believe that a person calling Swartz might be spoofing their number.

Conference Calling: The two conference calls placed during the month are calls Swartz initiated. He dialed the two numbers listed in the Phone Number column.

Hope this helps in clarification.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, March 01, 2011 11:00 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Subpoena Response

(b)(3):Rule 6E

Per EOUSA

From: (b)(6),(b)(7)(C) (CID)
Sent: Monday, February 28, 2011 2:29 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Can you call if you get a chance

I'm tied up in a meeting, I forwarded the memo to (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) for feedback.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (CID)
Sent: Mon Feb 28 14:18:09 2011
Subject: Can you call if you get a chance

The attached memo looks fine to me. AUSA Heymann wanted to get your approval before he submitted it to the judge

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Saturday, February 26, 2011 7:24 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7) (CID)
Subject: Motion for Grand Jury Disclosure

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

Per EOUSA

Thanks, Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 28, 2011 2:20 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Harvard Search affidavit
Attachments: Supplemental SW Affidavit.pdf

(b)(3):Rule 6E per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Monday, February 28, 2011 2:11 PM
To: Heymann, Stephen (USAMA)
Subject: Harvard Search affidavit

Could you send me the electronic copy of the affidavit for the application for search warrant for the search of Swartz's office at Harvard?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Sunday, February 27, 2011 6:04 AM
To: External:(b)(6),(b)(cambridgepolice.org
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Swartz report

(b)(5),(b)(7)(C) per EOUSA

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) cambridgepolice.org]
Sent: Saturday, February 26, 2011 12:16 PM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Subject: FW: Swartz report

Steve,

The documentation from JSTOR is the result of a GJ subpoena. 6E comes into play.

Ideas on how to deal with that? DO I call (b)(6),(b) and ask him to subpoena the values from JSTOR directly?

Thanks
(b)(6),
(b)(7)(C)

From: (b)(6),(b)(7) (C) [mailto:(b)(6),(b) (7)(C) MIT.EDU]
Sent: Friday, February 25, 2011 2:38 PM
To: (b)(6),(b)(7)(C)
Subject: Swartz report

(b)(6),(b)
(7)(C)

Attached are all narratives from the Swartz case; not sure what, if anything, you already had. The last two supplements deal with the ID at the student center.

I still need to get photos and reports from your crime scene people, and (b)(6), (b)(7) said he had documentation from J-Stor relating to the value of downloaded items. I'll need that stuff for our B&E arrest.

Have a good weekend...

Det. (b)(6),(b)(7)(C)
MIT Police Dept.

Investigations Unit

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Saturday, February 26, 2011 8:39 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: Filter Team Review

Please contact me after the filter team process is complete and before either of you begin your forensic examinations of the iMac computer and hard drive seized at Harvard. Steve

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov]
Sent: Saturday, February 26, 2011 7:28 AM
To: (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) BOS)
Subject: Read This One Instead
Attachments: JSTOR Memorandum in Support of 6e Disclosure.pdf

<<JSTOR Memorandum in Support of 6e Disclosure.pdf>> Sorry, forgot to save to .pdf the final typographical corrections before I sent it to you two. sph

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Saturday, February 26, 2011 7:24 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (CID)
Subject: Motion for Grand Jury Disclosure
Attachments: JSTOR Memorandum in Support of 6e Disclosure.pdf

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

Per EOUSA

Thanks, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 25, 2011 5:56 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Good news, bad news

Thanks for the update.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, February 25, 2011 05:47 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) @cambridgepolice.org; (b)(6),(b)(7)(C) cambridgepolice.org>
Subject: Good news, bad news

The bad news is my first attempt to image the 2TB drive from the enclosure crashed. The good news is after it crashed I used FTK imager to preview the disk and many, many, many, PDF files are in the clear and unencrypted.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 25, 2011 12:31 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Expertise

(b)(6)

per EOUSA

From: (b)(6),(b)(7)(C)
Sent: Thursday, February 24, 2011 5:10 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Sub20458 Response
Attachments: Sub20458 - Aaron Swartz.pdf

(b)(6),(b)(7)(C)
Special Agent
US Secret Service
10 Causeway Street
Suite (b)(6),
Boston, MA 0222

Re: Swartz – Sub20458

Dear Special Agent (b)(6),(b)(7)(C)

(b)(3):Rule 6E

per EOUSA

(b)(6),(b)(7)(C)
(b)(6),(b) Litigation Paralegal
440 Terry Avenue North
Seattle, WA 98109

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, February 24, 2011 9:35 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: CID/CERT: USAO Correspondence

I'll call (b)(6),(b)(7)(C) and talk it through. Steve

-----Original Message-----
From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, February 24, 2011 9:29 AM
To: Heymann, Stephen (USAMA)
Subject: FW: CID/CERT: USAO Correspondence

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) (CID)
Sent: Thursday, February 24, 2011 8:48 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: CID/CERT: USAO Correspondence
(b)(6),(b)(7)(C)

I got a couple of forms from the Boston USAO. Why is it we have to sign these again?

If this is a requirement, I will need forms for:

Software Engineering Institute
CERT (b)(6),(b)(7)(C)
ATTN:
4500 Fifth Avenue
CERT (b)(6),(b)(7)(C)
Pittsburgh, PA 15213

Software Engineering Institute
CERT (b)(6),(b)(7)(C)
ATTN:
4500 Fifth Avenue
CERT (b)
Pittsburgh, PA 15213

Thanks.

(b)(6),(b)(7)(C)

Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, February 23, 2011 5:07 PM
To: Heymann, Stephen (USAMA (b)(6),(b)(7)(C) (BOS)
Subject: RE: Revised Paragraph

Looks good

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 23, 2011 4:59 PM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C)
Subject: Revised Paragraph

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground and fled. The backpack in Swartz's possession at the time he was caught and arrested appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 23, 2011 4:59 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: Revised Paragraph

25. An MIT police officer who had seen several pictures taken by the covert camera in Building 16's network wiring closet saw Aaron Swartz on a bicycle near MIT, approximately half an hour after the "ghost laptop" had been connected in Building W20. The officer stopped his car, activated its blue lights and displayed his wallet badge. When he sought to question Swartz, Swartz dropped his bike to the ground and fled. The backpack in Swartz's possession at the time he was caught and arrested appeared to be the same one he had with him on each occasion he was videotaped in the wiring closet at MIT.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, February 23, 2011 12:53 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Proposed additional paragraph for the affidavit

26. On February 9, 2011, the Court issued warrants to search the PREMISES, the ACER LAPTOP, the WESTERN DIGITAL HARD DRIVE, and the USB DRIVE. The warrant to search the PREMISES was executed on February 11, 2011. The warrants to search the ACER LAPTOP, the WESTERN DIGITAL DRIVE, and the USB DRIVE were not executed prior to their expiration on February 22, 2011. At the time the warrant was issued for these pieces of electronic equipment, they were secured within the Identification Unit Laboratory of the Cambridge Police Department. Throughout the period of February 9, 2011, to the present, they have remained within secure areas at Cambridge Police Headquarters, first in the Identification Unit Laboratory, then in the Evidence/Property Unit.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 23, 2011 12:30 PM
To: External (b)(6),(b) cambridgepolice.org
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Evidence Movement

More than suffice. Let me write up a proposed paragraph and get it to you both to review.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: Wednesday, February 23, 2011 11:52 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) usss.dhs.gov
Subject: Evidence Movement

Please consider this email as written chronology for four pieces of evidence seized on January 6, 2011. These four items are

1 Acer Netbook/Laptop

1 Hard Drive Enclosure with cords

1 Hard Disk Drive – Western Digital

1 USB Thumb/Flash Drive

These items were grouped into two lots as they were recovered from two locations, the Netbook, HDD enclosure and HDD is one group and the USB Thumb/Drive being the other group.

The Cambridge Police headquarters has two secure areas with limited access on the third floor. One area being called the Property / Evidence Unit and the other being the Identification Unit Laboratory. The wall between these units has an installed evidence locker designed as a pass through system from Evidence to Indentifation for processing. Upon completion of analysis the items are passed back through the locker system from the Identification Unit back to Evidence.

February 3, 2011 at approximately 11:00am Special Agent (b)(6),(b)(7)(and I (b)(6),(b)(7)(C) received the four evidence items from MIT Police (b)(6),(b)(7)(C)

We drove directly from MIT PD to Cambridge Police HQ

February 3, 2011 @ 11:27am the USB Thumb / Flash Drive was logged into Evidence and placed in the evidence locker.

February 3, 2011 @ 11:31am the Netbook, enclosure and HDD were logged into evidence and placed in the evidence locker.

February 3, 2011 @ 11:35am the USB Thumb / Flash Drive was taken from the locker and placed in the ID unit lab.

February 3, 2011 @ 11:35am the Netbook, enclosure and HDD were taken from the locker and placed in the ID unit lab.

February 11, 2011 @ 3:50pm the USB Thumb / Flash Drive was taken from the ID unit lab and placed in the locker.

February 11, 2011 @ 3:09pm the Netbook, enclosure and HDD were taken from the ID unit lab and placed in the locker.

Since February 11, 2011 the above mentioned items have been in the custody of the Evidence / Property Unit and been secured.

Will this timeline suffice? I have printed out the Custody Information reports from CPD's database and will add those forms to the records being kept.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 23, 2011 11:03 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: What do you think your timing is today?

I am flexible too. Let's set a time, though, once we get the additional facts from (b)(6) so I can get the new applications down to the judge.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, February 23, 2011 10:44 AM
To: Heymann, Stephen (USAMA)
Subject: Re: What do you think your timing is today?

I am flexible. 1300 works for me. How about you

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) ambridgepolice.org
Sent: Wed Feb 23 09:52:50 2011
Subject: What do you think your timing is today?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 22, 2011 4:40 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Search Warrants for Acer Laptop, Western Digital Hard Drive and HP USB Drive

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C)@usdoj.gov>
Sent: Tuesday, February 22, 2011 4:05 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Draft of Search Warrant Return

We can just attach your Word documents to the warrant returns. Remember, in each case, you will need all of the information called for on the return page, a copy of which you have with each of your copies of the warrants.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Tuesday, February 22, 2011 3:53 PM
To: Heymann, Stephen (USAMA)
Subject: Draft of Search Warrant Return

(b)(5)

(b)(6),(b)(7)(C)
U.S. Secret Service

Boston Field Office

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 22, 2011 4:03 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Draft of Search Warrant Return

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) busss.dhs.gov]
Sent: Tuesday, February 22, 2011 3:53 PM
To: Heymann, Stephen (USAMA)
Subject: Draft of Search Warrant Return

(b)(5)

(b)(6),(b)(7)(C)
U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 22, 2011 1:23 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Office IMac and Hard Drive Forensics

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 22, 2011 12:43 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b) cambridgepolice.org; (b)(6), bpd@cityofboston.gov; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Office IMac and Hard Drive Forensics

The filter examiner will be Detective (b)(6), (b)(7)(It will take him approximately a week to examine the image and develop a filter hash set in accordance with the filter team memo.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 22, 2011 11:05 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External(b)(6),(b)(cambridgepolice.org
Subject: Office IMac and Hard Drive Forensics

(b)(6),(b)(7)(C)

(b)(5) per EOUSA

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 22, 2011 1:22 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External: (b)(6),(b) cambridgepolice.org; External: (b)(6), bpd@cityofboston.gov; (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Office IMac and Hard Drive Forensics

(b)(6),(b)(7)(C)

per EOUSA (b)(5)

Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 22, 2011 12:43 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b) cambridgepolice.org; (b)(6), bpd@cityofboston.gov; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Office IMac and Hard Drive Forensics

The filter examiner will be Detective (b)(6), (b)(7)(C) It will take him approximately a week to examine the image and develop a filter hash set in accordance with the filter team memo.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 22, 2011 11:05 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External: (b)(6),(b)(cambridgepolice.org
Subject: Office IMac and Hard Drive Forensics

(b)(6),(b)(7)(C)

(b)(5)

per EOUSA

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 22, 2011 11:05 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(cambridgepolice.org
Subject: Office IMac and Hard Drive Forensics

(b)(6),(b)(7)(C)

(b)(5)

per EOUSA

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 18, 2011 12:38 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Carrier

(b)(3):Rule 6E

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 18, 2011 9:08 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Can you two talk sometime this a.m.?

(b)(3):Rule 6E,(b)(5) Per EOUSA

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, February 18, 2011 9:07 AM
To: Heymann, Stephen (USAMA); (b)(6),(b) cambridgepolice.org
Subject: RE: Can you two talk sometime this a.m.?

Yes. Does 10 work?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Friday, February 18, 2011 8:30 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b) cambridgepolice.org
Subject: Can you two talk sometime this a.m.?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Friday, February 18, 2011 8:39 AM
To: (b)(6),(b)(7)(C) @usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: Re: Can you two talk sometime this a.m.?

I can, name the time

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) @hsss.dhs.gov>
(b)(6),(b)(7)(C)
Sent: Fri Feb 18 08:29:31 2011
Subject: Can you two talk sometime this a.m.?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Friday, February 18, 2011 8:30 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) @cambridgepolice.org
Subject: Can you two talk sometime this a.m.?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, February 17, 2011 1:06 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: T-Mobile Subpoenas
Attachments: T-MobileSubpoena1.pdf; T-MobileSubpoena2.pdf

(b)(3):Rule 6E,(b)(5)

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, February 17, 2011 12:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Telephone subpoenas

(b)(3):Rule 6E

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, February 17, 2011 9:11 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: (b)(3):Rule 6E ERT Procedures

(b)(6), (b)(7)(C) please see me about this.

(b)(6),(b)(7)(C)

Assistant to the Special Agent in Charge
United States Secret Service
Boston Field Office
10 Causeway Street, Suite 447
Boston, MA 02222
office: (617) 565-5640
fax: (617) 565-5659
cell (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, February 17, 2011 7:27 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: FW: (b)(3):Rule 6E ERT Procedures

AUSA Heymann would like the Service to pay for an expedited response from (b)(3):Rule 6E is there a mechanism for us to pay (b)(3):Rule 6E

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, February 17, 2011 6:52 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: FW: (b)(3):Rule 6E ERT Procedures

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, February 16, 2011 9:42 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: (b)(3):Rule 6E ERT Procedures

(b)(5)

per EOUSA

From: (b)(7)(C) (USMS)
Sent: Tuesday, February 15, 2011 10:34 AM

To: Heymann, Stephen (USAMA)
Subject: T Mobile ERT Procedures

Steve:

(b)(7)(E)

per USMS

(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, February 17, 2011 7:41 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Re: (b)(3):Rule ERT Procedures

I would suggest checking with CID, but wait for (b)(6),(to make the call.

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Sent: Thu Feb 17 07:27:22 2011
Subject: FW: (b)(3):Rule ERT Procedures

AUSA Heymann would like the Service to pay for an expedited response from (b)(3):Rule Is there a mechanism for us to pay (b)(3):Rule ?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, February 17, 2011 6:52 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: (b)(3):Rule ERT Procedures

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, February 16, 2011 9:42 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: (b)(3):Rul ERT Procedures

(b)(5)

per EOUSA

From: (b)(7)(C) (USMS)
Sent: Tuesday, February 15, 2011 10:34 AM
To: Heymann, Stephen (USAMA)
Subject: (b) ERT Procedures

Steve:

(b)(7)(E)

per USMS

(b)(7)(E)

per USMS

(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Thursday, February 17, 2011 6:52 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: (b)(3):Rule ERT Procedures
Attachments: (b)(3):Rule Expedited Response Intake Sheet - interactive.pdf

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, February 16, 2011 9:42 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: FW: (b)(3):Rule ERT Procedures

(b)(5)

From: (b)(7)(C) (USMS)
Sent: Tuesday, February 15, 2011 10:34 AM
To: Heymann, Stephen (USAMA)
Subject: (b) ERT Procedures

Steve:

(b)(7)(E)

per USMS

(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Wednesday, February 16, 2011 5:12 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Revised Draft Filter Memo

D

(b)(6),(b)(7)(C)
SA
US Secret Service
Boston Field Office

From: (b)(6),(b)(7)(C) (BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) usdoj.gov>
Cc: External (b)(6),(b) cambridgepolice.org; External (b)(6),(bpd@cityofboston.gov; (b)(6),(b)(7)(C) BOS)
Sent: Wed Feb 16 16:59:45 2011
Subject: RE: Revised Draft Filter Memo

It looks OK to me

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 16, 2011 4:54 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Revised Draft Filter Memo

<<Draft Filter Team Memo 2-16 revised.pdf>> Please review this revised draft filter team memo and let me know your thoughts.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 4:54 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Revised Draft Filter Memo
Attachments: Draft Filter Team Memo 2-16 revised.pdf

<<Draft Filter Team Memo 2-16 revised.pdf>> Please review this revised draft filter team memo and let me know your thoughts.

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 16, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Local Rules Letters

(b)(6),(b)(7)(C)

I'd like to get the local rules letters out tomorrow. Can you prioritize getting me the list of names of those involved in the searches and will be involved in the forensics? Thank you

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Haymann, Stephan (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 3:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b) pcambridgepolice.org
Attachments: Draft Filter Team Memo 2-16.pdf

Attached is a draft filter team memo. <<Draft Filter Team Memo 2-16.pdf>> Please review it carefully and discuss it with the agent(s) who will comprise the filter team. I would like to make sure that it is technically practicable at your end or if there are any changes you would suggest before finalizing the memo.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 1:55 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Local Rules Letters

(b)(6),(b)(7)(C)

I'd like to get the local rules letters out tomorrow. Can you prioritize getting me the list of names of those involved in the searches and will be involved in the forensics? Thank you

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 11:23 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Identifiers

Thank you. (I wanted to identify them in the filter team memo.)

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, February 16, 2011 11:21 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Identifiers

Apple iMac model A1311 with serial number W80254XGD87
Western Digital hard drive model WD1200 with serial number WMANN1006724
Sony Micro Vault Tiny 8GB with the marking SDK USM8GH(8)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, February 16, 2011 10:47 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Identifiers

(b)(5)

per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 10:47 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Identifiers

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, February 16, 2011 9:45 AM
To: (b)(6),(b)(7)(C) @usdoj.gov; (b)(6),(b)(7)(C) BOS)
Subject: Re: USB Drive Seized from Swartz's Wallet

It was on a table in the "Main" room of the unit, sitting on a table. It was NOT on his person.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: MICHAEL PICKETT (BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Wed Feb 16 09:37:14 2011
Subject: USB Drive Seized from Swartz's Wallet

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 9:42 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: FW: T Mobile ERT Procedures
Attachments: (b)(3):Rule 6E Expedited Response Intake Sheet - interactive.pdf

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) (USMS)
Sent: Tuesday, February 15, 2011 10:34 AM
To: Heymann, Stephen (USAMA)
Subject: (b)(3):Rule ERT Procedures

Steve:

(b)(7)(E)

Per USMS

(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 9:40 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Taint Team

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: USB Drive Seized from Swartz's Wallet

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 16, 2011 8:37 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Search List sph 2-15 draft.doc
Attachments: Search List sph 2-15 draft.rtf

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 15, 2011 4:20 PM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b) cambridgepolice.org
Subject: Initial List of Search Terms
Attachments: Search List sph 2-15 draft.pdf

(b)(5),(b)(7)(C)

Steve

per EOUSA

<<Search List sph 2-15 draft.pdf>>

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, February 15, 2011 4:01 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) (BOS)
Subject: Re: Micro Center Subpoena

Will do.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Tue Feb 15 15:55:13 2011
Subject: Micro Center Subpoena

(b)(3):Rule 6E,(b)(5)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 15, 2011 3:55 PM
To: (b)(6),(b)(7)(C) (BOS); External-(b)(6),(b) cambridgepolice.org
Subject: Micro Center Subpoena

(b)(3):Rule 6E,(b)(5)

Per EOUSA

From: (b)(6),(b)(7)(C) (CID)
Sent: Tuesday, February 15, 2011 12:44 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C) is working on it now.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-6226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (CID)
Sent: Tue Feb 15 12:31:07 2011
Subject: FW: Packet traffic to/from the Acer Laptop

How is it going?
Has anybody had a chance to look at the packet capture from the MIT intrusion case 102-775-60071?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 15, 2011 9:56 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(cambridgepolice.org
Subject: FW: Packet traffic to/from the Acer Laptop

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, February 02, 2011 11:56 AM
To: (b)(6),(b)(7)(C) (CID)
Cc: (b)(6),(b)(7) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

(b)(5)

Per EOUSA

Steve

From: (b)(6),(b)(7)(C) (CID) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),(b)(7)(C)
4500 Fifth Avenue
Pittsburgh, PA 15213
TEL: (b)(6),(b)(7)(C)

We are eager to help in any way that we are able.

(b)(6),(b)(7)(C)

Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-208-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) usdoj.gov>
Cc: (b)(6),(b)(7)(C) CID); External (b)(6),(b) cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the flow data has enough detail to show remote connections into the laptop but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5) per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Haymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 15, 2011 11:12 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External-(b)(6),(b) cambridgepolice.org
Subject: Running to-do list
Attachments: Things to be Done 2-15.pdf

<<Things to be Done 2-15.pdf>> I thought a list could be helpful to us both. Attached is my running to do list (absent the subpoenas on my desk, which I am getting in motion.)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 15, 2011 9:56 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External-(b)(6),(b) cambridgepolice.org
Subject: FW: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Wednesday, February 02, 2011 11:56 AM
To: (b)(6),(b)(7)(C) (CID)
Cc: (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

(b)(5)

per EOUSA

Steve

From: (b)(6),(b)(7)(C) CID) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, February 02, 2011 10:55 AM

To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Cc: (b)(6),(b) @cambridgepolice.org
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),
(b)(7)(

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C
CERT - CIC Room (b)(6),(b)(7)(C)
4500 Fifth Avenue
Pittsburgh, PA 15213
TEL: (b)(6),(b)(7)(C

We are eager to help in any way that we are able.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5228 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: 'Heymann, Stephen (USAMA)' <(b)(6),(b)(7)(C) @usdoj.gov>
Cc: (b)(6),(b)(7)(C) (CID); External (b)(6),(b) cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the flow data has enough detail to show remote connections into the laptop but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5) per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 14, 2011 4:11 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Smartphone Seized on Friday

Thank you

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Monday, February 14, 2011 4:04 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Smartphone Seized on Friday

The two phones that were being charged when we entered apartment (b)(6),(were a HTC G2 and a Nokia 1661

The Nokia 1661 had a IMEI of 012185001723274

Even though the Nokia 1661 is normally a T-Mobile cell phone the SIM Card inside the phone was marked as AT&T Go the AT&T prepaid cell phone service.

The SIM card had an ICCID of: 89014104233710767564
The SIM card had an IMSI of 310410371076756

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, February 14, 2011 8:16 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Smartphone Seized on Friday

What is the make and model of the phone seized on Friday

What is its IMSI,MEID,IMEI

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (ISD)
Sent: Monday, February 14, 2011 12:48 PM
To: 'Heymann, Stephen (USAMA)'
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) @cambridgepolice.org)'
Subject: RE: SWARTZ - Accounts

It's the billing address for the card.

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, February 14, 2011 12:45 PM
To: (b)(6),(b)(7)(C) (ISD)
Subject: RE: SWARTZ - Accounts

Is that the billing address of the card or the address given by (b)(6),(b)(7)(C), whom I would like to locate.

From: (b)(6),(b)(7)(C) (ISD) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Monday, February 14, 2011 12:32 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7) @cambridgepolice.org
Subject: SWARTZ - Accounts

Steve –
Steve –

I gave a call into AMEX – SWARTZ is the supplemental card holder on an AMEX card for (b)(6),(b)(7)(C) at the 950 Mass Ave (b) Cambridge MA 02139 address. According to AMEX the card is a Premier Reward Gold card opened in September 2010. Let me know if you need/want the actual card number. Subpoena should be directed to:

American Express Subpoena Compliance (by mail only, NO faxes)
43 Butterfield Circle
El Paso, TX 79906

Citibank had no cards for him under his SSN.

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (ISD)
Sent: Monday, February 14, 2011 12:33 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: Credit Bureau Subpoena
Attachments: Credit Bureau Subpoena Information as 7.doc; SWARTZ-DCS.pdf

---

From: (b)(6),(b)(7)(C) (ISD)
Sent: Monday, February 14, 2011 12:33 PM
To: (b)(6),(b)(7)(C) (MCH); (b)(6),(b)(7)(C) cambridgepolice.org)
Subject: FW: Credit Bureau Subpoena

FYI

From: (b)(6),(b)(7)(C) (ISD)
Sent: Monday, February 14, 2011 10:24 AM
To: (b)(6),(b)(7)(C) usdoj.gov'
Subject: FW: Credit Bureau Subpoena

Steve –

Attached is the most recent info on credit bureau subpoena requests. I'm also attaching the return on a credit header search.

Let me know if I can be of assistance.

Be well –

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (ISD)
Sent: Monday, February 14, 2011 12:32 PM
To: (b)(6),(b)(7)(C) @usdoj.gov'
Cc: BOS);(b)(6),(b)(7)(C) cambridgepolice.org)'
Subject: SWARTZ - Accounts

Steve –
Steve –

I gave a call into AMEX – SWARTZ is the supplemental card holder on an AMEX card for (b)(6),(b)(7)(C) at the 950 Mass Ave (b) Cambridge MA 02139 address. According to AMEX the card is a Premier Reward Gold card opened in September 2010. Let me know if you need/want the actual card number. Subpoena should be directed to:

American Express Subpoena Compliance (by mail only, NO faxes)
43 Butterfield Circle
El Paso, TX 79906

Citibank had no cards for him under his SSN.

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Monday, February 14, 2011 9:45 AM
To: External-(b)(6),(b) @cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: When would be good for you two to talk a bit?

I'll figure that you two will call me when you get there. If it looks like it will be an issue, let me know, and I will get the call in number.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @cambridgepolice.org]
Sent: Monday, February 14, 2011 9:39 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) @usss.dhs.gov'
Subject: Re: When would be good for you two to talk a bit?

I'll try to be at the lab.

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) @usss.dhs.gov (b)(6),(b)(7)(C) @usss.dhs.gov>
Sent: Mon Feb 14 09:36:07 2011
Subject: RE: When would be good for you two to talk a bit?

3:00 it is then. Will you be at the lab or should I see if I can grab the conference call center?

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @cambridgepolice.org]
Sent: Monday, February 14, 2011 9:20 AM
To: (b)(6),(b)(7)(C) @usss.dhs.gov'; Heymann, Stephen (USAMA)
Subject: Re: When would be good for you two to talk a bit?

I can do 3pm.

First Responder / CPR recertification today.

From: (b)(6),(b)(7)(C) (BOS) [(b)(6),(b)(7)(C) @usss.dhs.gov>
To: Heymann, Stephen (USAMA (b)(6),(b)(7)(C) @usdoj.gov>
Cc: (b)(6),(b)(7)(C)
Sent: Mon Feb 14 09:04:48 2011
Subject: RE: When would be good for you two to talk a bit?

I know (b) has training today but he may be free after 3pm

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, February 14, 2011 8:59 AM
To: (b)(6),(b)(7)(C) (BOS); External-(b)(6),(b) @cambridgepolice.org
Subject: When would be good for you two to talk a bit?

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Monday, February 14, 2011 9:39 AM
To: (b)(6),(b)(7)(C) @usdoj.gov'; (b)(6),(b)(7)(C) (BOS)
Subject: Re: When would be good for you two to talk a bit?

I'll try to be at the lab.

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) @usss.dhs.gov (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Mon Feb 14 09:36:07 2011
Subject: RE: When would be good for you two to talk a bit?

3:00 it is then. Will you be at the lab or should I see if I can grab the conference call center?

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Monday, February 14, 2011 9:20 AM
To: (b)(6),(b)(7)(C) @usss.dhs.gov'; Heymann, Stephen (USAMA)
Subject: Re: When would be good for you two to talk a bit?

I can do 3pm.

First Responder / CPR recertification today.

From: (b)(6),(b)(7)(C) (BOS) [(b)(6),(b)(7)(C) usss.dhs.gov>
To: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Cc: (b)(6),(b)(7)(C)
Sent: Mon Feb 14 09:04:48 2011
Subject: RE: When would be good for you two to talk a bit?

I know (b) has training today but he may be free after 3pm

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, February 14, 2011 8:59 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(cambridgepolice.org
Subject: When would be good for you two to talk a bit?

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 14, 2011 9:36 AM
To: External-(b)(6),(b)(cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: When would be good for you two to talk a bit?

3:00 it is then. Will you be at the lab or should I see if I can grab the conference call center?

From: (b)(6),(b)(7)(C) [mailto:(b)(6), cambridgepolice.org]
Sent: Monday, February 14, 2011 9:20 AM
To: (b)(6),(b)(7)(C) usss.dhs.gov'; Heymann, Stephen (USAMA)
Subject: Re: When would be good for you two to talk a bit?

I can do 3pm.

First Responder / CPR recertification today.

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Cc: (b)(6),(b)(7)(C)
Sent: Mon Feb 14 09:04:48 2011
Subject: RE: When would be good for you two to talk a bit?

I know (b) has training today but he may be free after 3pm

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, February 14, 2011 8:59 AM
To: (b)(6),(b)(7)(C) BOS); External-(b)(6),(b) cambridgepolice.org
Subject: When would be good for you two to talk a bit?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 14, 2011 8:19 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: (b)(3):Rule 6E Subpoena Response

This one should come in this week. Please let me know when it (and others) come in. Thanks again, steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 14, 2011 8:18 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: (b)(3):Rule 6E Subpoena

Follow Up Flag: Follow up
Flag Status: Flagged

(b)(3):Rule 6E

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 14, 2011 8:16 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Smartphone Seized on Friday

What is the make and model of the phone seized on Friday

What is its IMSI,MEID,IMEI

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Sunday, February 13, 2011 8:49 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: What was the serial number on the Macbook box?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, February 10, 2011 10:37 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Cell Phone Subpoena

(b)(3):Rule 6E,(b)(5)

Per EOUSA

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, February 09, 2011 6:34 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: Condo is dark

Nope, i'll check back periodicaLly.

From: (b)(6),(b)(7)(C) (BOS) <(b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C)
Sent: Wed Feb 09 18:21:34 2011
Subject: Re: Condo is dark

Roger. Maybe out for dinner. Can I help?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) cambridgepolice.org>
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) sdoj.gov>; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Sent: Wed Feb 09 18:19:32 2011
Subject: Condo is dark

The curtains are open and the condo is dark. Will advise again later.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Wed Feb 09 16:37:15 2011
Subject: Tomorrow's Search

(b)(5)

Steve

Per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, February 09, 2011 6:20 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Condo is dark

The curtains are open and the condo is dark. Will advise again later.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Wed Feb 09 16:37:15 2011
Subject: Tomorrow's Search

(b)(5)

per EOUSA

Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, February 09, 2011 5:03 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: Re: Tomorrow's Search

Rec'd

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) ss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Wed Feb 09 16:37:15 2011
Subject: Tomorrow's Search

(b)(5)

Per EOUSA

Steve

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 09, 2011 4:37 PM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b) cambridgepolice.org
Subject: Tomorrow's Search

(b)(5)

Steve

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 09, 2011 1:23 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b) cambridgepolice.org
Subject: Federal Rules on Executing a Search Warrant

Mike,

I have just e-mailed you the full text of Rule 41 of the Federal Rules of Criminal Procedure concerning search warrants, which you should read before tomorrow. Below is the subsection on the execution of warrants.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(A) Noting the Time. The officer executing the warrant must enter on it the exact date and time it was executed.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

(C) Receipt. The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property.

(D) Return. The officer executing the warrant must promptly return it--together with a copy of the inventory--to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

Steve

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, February 08, 2011 3:17 PM
To: (b)(6),(b)(7)(C) BOS)
Cc: (b)(6),(b)(7)(C)
Subject: Swearing out the warrants

Please be here at 9:30 a.m. tomorrow. We will go down to the courtroom at 9:45 a.m. to swear out the warrants.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, February 08, 2011 6:02 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Swearing out the warrants

Did you get a copy of the final drafted warrant?

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 08, 2011 4:37 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Swearing out the warrants

I am definitely going. I don't think you need to be there unless you want to.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, February 08, 2011 4:35 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: Swearing out the warrants

(b)(6),
(b)(7)

Just to be sure, you're going tomorrow morning and I am not?

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 08, 2011 3:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C)
Subject: Swearing out the warrants

Please be here at 9:30 a.m. tomorrow. We will go down to the courtroom at 9:45 a.m. to swear out the warrants.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, February 08, 2011 4:41 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Swearing out the warrants

If I don't need to be there then I won't.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 08, 2011 4:37 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Swearing out the warrants

I am definitely going. I don't think you need to be there unless you want to.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) cambridgepolice.org]
Sent: Tuesday, February 08, 2011 4:35 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: FW: Swearing out the warrants

(b)(6),(b)(7)(C)

Just to be sure, you're going tomorrow morning and I am not?

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, February 08, 2011 3:17 PM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject: Swearing out the warrants

Please be here at 9:30 a.m. tomorrow. We will go down to the courtroom at 9:45 a.m. to swear out the warrants.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, February 08, 2011 4:35 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: Swearing out the warrants

(b)(6),
(b)(7)

Just to be sure, you're going tomorrow morning and I am not?

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 08, 2011 3:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: Swearing out the warrants

Please be here at 9:30 a.m. tomorrow. We will go down to the courtroom at 9:45 a.m. to swear out the warrants.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 08, 2011 3:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: Externa (b)(6),(b) cambridgepolice.org
Subject: Swearing out the warrants

Please be here at 9:30 a.m. tomorrow. We will go down to the courtroom at 9:45 a.m. to swear out the warrants.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C)@usdoj.gov>
Sent: Tuesday, February 08, 2011 12:51 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Everything is down with the Judge

6:00 a.m. is the earliest the warrant will permit

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Tuesday, February 08, 2011 12:49 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Everything is down with the Judge

We are planning to execute the warrant as early as possible Thursday morning even if it is signed today

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, February 08, 2011 12:47 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Everything is down with the Judge

I will let you know when I hear anything.

Are you planning to go tomorrow a.m. If we are able to get the warrant signed today, or hold off until Thursday a.m. in any case?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 08, 2011 12:47 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Everything is down with the Judge

I will let you know when I hear anything.

Are you planning to go tomorrow a.m. if we are able to get the warrant signed today, or hold off until Thursday a.m. in any case?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 08, 2011 11:52 AM
To: (b)(6),(b)(7)(C) [BOS]; External (b)(6),(b) cambridgepolice.org
Subject: Instructions to Agents Executing Warrants

(b)(5)

Per EOUSA

Steve

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 08, 2011 11:28 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Sorry--Important Clarification

Thanks. Steve

-----Original Message-----
From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @MIT.EDU]
Sent: Tuesday, February 08, 2011 8:56 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Sorry--Important Clarification
Importance: High

Morning Steve - replies inline - and don't hesitate to let me know if you have additional questions:

On Feb 8, 2011, at 6:39 AM, Heymann, Stephen (USAMA) wrote:

(b)(5),(b)(7)(C)

Per EOUSA

(b)(5)

Per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 08, 2011 10:11 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Copy for Agents to initial

Yes. Can you call me please.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Tuesday, February 08, 2011 10:09 AM
To: Heymann, Stephen (USAMA)
Subject: Copy for Agents to initial

Whenever you get a chance, could you email the final copy of the affidavit so I can have the search team read it.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, February 08, 2011 9:54 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: RE: Let's discuss this proposed re-write

Paragraph 12 is further revised here

(b)(5)

Per EOUSA

(b)(5)

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Tuesday, February 08, 2011 9:51 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C)@cambridgepolice.org
Subject: RE: Let's discuss this proposed re-write

The changes look good to both of us. I will call you in a minuet

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

per EOUSA

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, February 08, 2011 9:34 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@cambridgepolice.org
Subject: Let's discuss this proposed re-write

(b)(5)

Per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information

that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

(b)(5)

Per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 08, 2011 9:54 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External:(b)(6),(b) cambridgepolice.org
Subject: RE: Let's discuss this proposed re-write

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 08, 2011 9:34 AM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Let's discuss this proposed re-write

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) @MIT.EDU>
Sent: Tuesday, February 08, 2011 8:56 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Sorry--Important Clarification

Importance: High

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 08, 2011 7:18 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: FW: Search Warrant Applications

FYI, sph

From: Heymann, Stephen (USAMA)
Sent: Tuesday, February 08, 2011 7:09 AM
To: (b)(6),(b)(7)(C) mad.uscourts.gov
Subject: Search Warrant Applications

(b)(6),(b)(7)(C)

I am waiting to confirm two facts, in our applications for search warrants. I will bring them down as soon as they are confirmed (or any necessary changes are made). I am sorry, but this will be later in the day than I had hoped. Once you get them, please just let me know whether the Judge will still have the opportunity to review them today or I should let the agency know it will be sometime tomorrow, instead.

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 08, 2011 7:17 AM
To: (b)(6),(b)(7)(C)
Cc: (BOS)
Subject: RE: Sorry--Important Clarification

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA)
Sent: Tuesday, February 08, 2011 6:40 AM
To: (b)(6),(b)(7)(C)
Cc: (BOS)
Subject: Sorry--Important Clarification
Importance: High

(b)(6),(b)(7)

(b)(5)

per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 08, 2011 6:40 AM
To: (b)(6),(b)(7)(C)
Cc: BOS)
Subject: Sorry--Important Clarification

Importance: High

(b)(6),(b)(7)(C)

(b)(5)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 4:20 PM
To: (b)(6),(b)(7)(C) BOS); External-(b)(6),(b) cambridgepolice.org
Subject: For planning purposes

If we are able to finalize the affidavit tonight at whatever time, so I can drop the applications off at the clerk's office tomorrow at 8:30, we should still be able to get the warrants in the course of the day tommorow absent horrendous weather.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Monday, February 07, 2011 1:37 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: Can you confirm something quickly for me?
Attachments: MIT Abuse - RCA.pdf

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @ithaka.org]
Sent: Monday, February 07, 2011 1:31 PM
To: Heymann, Stephen (USAMA)
Subject: FW: Can you confirm something quickly for me?

Hi Steve,

In response to your question, << The abuse from 18.55.6.215 began on September 24th and continued until it was blocked by JSTOR that evening.

Then abuse began the next morning, on the September 26th, and continued in turn until it was blocked.>>

I am forwarding you a PDF of our incident report for the MIT activity, which contains the answer to these questions. We don't know if the activity started on the 24th (although do the other materials we sent show this?) but

9/25
We first noticed it from 18.55.6.215 on the 25th, circa 7 PM.
We blocked this IP circa 9 PM

9/26
This activity started again, this time from 18.55.6.216 around 8 AM
We noticed it around 10 AM
We blocked 18.55.6.216 at 12 PM
We saw activity start from another IP around 1 PM
We blocked their class C 18.55.6.0/24 around 6 PM

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 1:00 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: Review of MIT Records

Please review the MIT records we have just received this afternoon and make sure that our current draft of the search warrant affidavit is fully consistent with them. Let me know either that no changes are needed or whatever changes may be necessary in light of the records; I'll wait to send the warrant applications down to the Magistrate Judge until after you have finished your review.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 12:21 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: FW: MIT Documents

I should have noted, please keep them in files clearly marked "grand jury" to distinguish them from other materials received in the case. The same applies to the materials we received earlier from JSTOR.

From: Heymann, Stephen (USAMA)
Sent: Monday, February 07, 2011 12:00 PM
To: (b)(6),(b)(7)(C) BOS)'; (b)(6),(b)(cambridgepolice.org
Subject: MIT Documents

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 12:00 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: MIT Documents

(b)(3):Rule 6E,(b)(5),(b)(7)(C)

Per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 11:19 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) ambridgepolice.org
Subject: FW: MIT Update: It's worse than we know

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @ithaka.org]
Sent: Wednesday, February 02, 2011 9:59 AM
To: Heymann, Stephen (USAMA)
Subject: RE: MIT Update: It's worse than we know

The counts are for PDF downloads, so the 1,385,569 figure represents full articles.

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, February 02, 2011 9:06 AM
To: (b)(6),(b)(7)(C)
Subject: RE: MIT Update: It's worse than we know

(b)(6),(b)(7)(C)

In (b)(6),(b)(7)(C)'s numbers below, does 1,385,569 represent separate research articles, or parts (like some title pages, some parts of multi-part articles, etc) or is it impossible to tell for the moment? If you don't know for the moment, is it possible to estimate the number of separate articles?

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @ithaka.org]
Sent: Friday, January 28, 2011 3:05 PM
To: Heymann, Stephen (USAMA)
Subject: FW: MIT Update: It's worse than we know

... and this too.

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 3:02 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: RE: MIT Update: It's worse than we know

I do know from (b)(6),(b)(7)(C)'s initial analysis that the downloading was done systematically using sequential increases in our stable URLs. That is, get stable URL 12345, get stable URL 12346, 12347, 12348 and so on.

This tells us a few things. One, that the previous activity was similar to the pattern (b)(6),(b)(7)(C) is seeing. That is, not targeted towards types. Two, it lends credence to an entire corpus grab approach. Don't care what it is I am getting, just get me the next one.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:50 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Re: MIT Update: It's worse than we know

This doesn't appear to be targeted towards research articles or any particular titles, collections, or disciplines. For the 2.8 million in Nov and Dec, the breakdown by article type is:
Research articles – 1,385,569
Reviews – 938,063
Misc – 459,457
News – 62,127
Editorial – 9,472

Those numbers more or less correlate to the corpus as a whole. I'd say the he was going after everything.

From: (b)(6),(b)(7)(C) ithaka.org>
Date: Fri, 28 Jan 2011 14:28:43 -0500
To: (b)(6),(b)(7)(C) ithaka.org>, (b)(6),(b)(7)(C) ithaka.org>
Cc: (b)(6),(b)(7)(C) ithaka.org>
Subject: Re: MIT Update: It's worse than we know

Attached are 2 screen shots depicting PDF download activity from MIT for November and December. One show's all downloads and totals 2,854,824 for the 2 months. The other filters out downloads from the 3 IP's that look to be associated with the download abuse (b)(6),(b)(7)(C) and totals 17,865 for the 2 month period. Recognizing that some legitimate downloads may have occurred from the 3 filtered IP's, it would still be safe to say that about 2.8 million illegal downloads occurred during November and December. We know that some illegal downloading occurred prior to November and into January. I don't have those numbers yet. But looking at the graph you can see that some pretty aggressive downloading was taking place the last week of Dec (over 100k/day). It seems likely this extended into January for some period of time. It wouldn't be much of a stretch to say that as much of a million or more additional downloads may have occurred that are not reflected on this chart. I expect to have January data available for review by Monday. I'll also start loading Oct and Sept numbers as well to complete the picture.

(b)(6),
(b)(7)(C

From: (b)(6),(b)(7)(C) ithaka.org>
Date: Fri, 28 Jan 2011 14:13:57 -0500
To: (b)(6),(b)(7)(C) ithaka.org>
Cc: ithaka.org>, (b)(6),(b)(7)(C) ithaka.org>
Subject: RE: MIT Update: It's worse than we know

So, with September and October, what does the number look like? Still looking like the entire corpus?

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:10 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: RE: MIT Update: It's worse than we know

(b)(6),(b)
(7)(C)

Hi (b)(6), (b)(7)(

Speaking with (b)(6),(b)(7)(C) just now about making sure we have (b)(6),(b)(7)(C) time as needed for the MIT evaluation currently underway and discovering that the IP addresses associated with these specific incidents have numerous additional days of mass downloading.

It would take some time to normalize against usual MIT usage, but at first glance, it is reasonably safe to assume from what (b) and I covered that the individual responsible has already acquired the entire JSTOR corpus. Glad to have a call ASAP if you think it useful and I let (b) know that I thought you might be calling him shortly after receiving this message for clarification. In light of this information, it would seem that we need to try and understand the full picture outside of the identified incidents going forward. Certainly our tack here merits some re-evaluation, both concerning this case and the potential for additional measures of prevention as we move forward. Also copying in (b) at this juncture.

(b)(6),(b)(7)(C)

Thanks,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) thaka.org

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, February 07, 2011 11:18 AM
To: (b)(6),(b)(7)(C) [BOS]; Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: FW: MIT Update: It's worse than we know

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) ithaka.org]
Sent: Friday, January 28, 2011 5:02 PM
To: Heymann, Stephen (USAMA)
Subject: FW: MIT Update: It's worse than we know

Breakdown of downloading:

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 4:57 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: Re: MIT Update: It's worse than we know

Here are the totals for each IP during Nov/Dec. All but a few thousand of these are probably attributed to the downloader.

(b)(6),(b)(7)(C)

2,341,267 (periods of activity 11/29 – 12/26)
306,984 (periods of activity 12/27 - ??)
188,708 (periods of activity 11/6 – 11/11)

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Sunday, February 06, 2011 9:03 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Notes and Reports

Good Morning,

Message received (b)(6),(b) and I will split this up, relay the instructions and collect the copies. Additionally the names of participants will be forwarded forthwith.

(b)(6),
(b)(7)(C

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Sunday, February 06, 2011 6:16 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Notes and Reports

(b)(5)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Sunday, February 06, 2011 8:20 AM
To: External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) BOS)
Subject: Revised Search Warrant Affidavit
Attachments: Comparison of 2-6 and 2-1 SW Affidavit Drafts.pdf; SW Affidavit 2-6-11 draft.pdf

The attached .pdfs include (a) my proposed revised search warrant affidavit and (b) a comparison which shows the changes since the last draft you looked at. Please review them as early as you can on Monday. I would like to get the applications down to the Judge by midday, if at all possible. Thx, Steve

<<Comparison of 2-6 and 2-1 SW Affidavit Drafts.pdf>> <<SW Affidavit 2-6-11 draft.pdf>>

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Sunday, February 06, 2011 6:16 AM
To: External-(b)(6),(b)(7)(C) cambridgepolice.org (b)(6),(b)(7)(C) (BOS)
Subject: Notes and Reports

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 04, 2011 9:22 AM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: Revised Search Warrant Affidavit
Attachments: SW Affidavit Changes.pdf; SW Affidavit 2-4-11 draft.pdf

Attached is the revised search warrant affidavit and a comparison document comparing this version to the last one you had. Please read it again very carefully for any changes or corrections that need to be made.

Thank you, Steve

<<SW Affidavit Changes.pdf>> <<SW Affidavit 2-4-11 draft.pdf>>

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, February 04, 2011 9:12 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Ploease give me a call when you are at your computer, Steve

From: (b)(6),(b)(7)(C) @mit.edu>
Sent: Thursday, February 03, 2011 11:34 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Accepted: Conference Call

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, February 03, 2011 6:18 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: January 4th

Please check in the morning

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, February 03, 2011 5:59 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b) cambridgepolice.org
Subject: Re: January 4th

The photo I am referencing is one of the ones I took. There might be a better one I don't know about

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Sent: Thu Feb 03 17:54:37 2011
Subject: RE: January 4th

Who took the photo? Do we have any others? And might whomever took the photo have other details on it?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, February 03, 2011 5:53 PM
To: Heymann, Stephen (USAMA); (b)(6),(b) cambridgepolice.org
Subject: Re: January 4th

I have a picture from the 4th of the drive that shows it is the same enclosure and a different disk but no serial number is visible in the picture I am looking at. I can tell the hard drive on the 4 is different because the portion shown in the photo is very dirty where as the hard drive in the enclosure seized on the 6th is clean

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Sent: Thu Feb 03 17:45:08 2011
Subject: January 4th

(b)(5)

per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF
2218

From: (b)(6),(b)(7)(C) (CID)
Sent: Thursday, February 03, 2011 6:12 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Linux Forensics

Sounds good.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) Desk)
Mobile)
412-268-5226 (Fax)

----- Original Message -----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b)(7)(C) (CID)
Sent: Thu Feb 03 17:56:12 2011
Subject: Linux Forensics

My Linux forensics experience is limited. We will probably have the warrant for the Acer running Ubuntu next week. I will probably be asking for advice and help with that next week

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) (CID)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Feb 03 17:41:24 2011
Subject: Re: Dropbox upload

(b)(6),
(b)(7)(C

To follow-up:

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)
CERT - CIC Room (b)(6),(
4500 Fifth Avenue
Pittsburgh, PA 15213
(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
Desk)
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) (Mobile)
412-268-5226 (Fax)

----- Original Message -----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b) cert.org (b)(6),(b)(7)(ert.org> (b)(6),(b)(7)(C) CID)
Sent: Thu Feb 03 17:36:18 2011
Subject: Re: Dropbox upload

What is best address to send disk with packet capture

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) @cert.org>
To: (b)(6),(b)(7)(C) BOS)
Sent: Wed Feb 02 18:10:12 2011
Subject: RE: Dropbox upload

Thanks, sir. We'll look for the cd.

Sent from a mobile device

-----Original Message-----
From: (b)(6),(b)(7)(C) BOS] (b)(6),(b)(7)(C) usss.dhs.gov]
Received: Wednesday, 02 Feb 2011, 5:55pm
To: (b)(6),(b)(7)(C) cert.org]
Subject: RE: Dropbox upload

I just stopped the transfer.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) mailto: (b)(6),(b) (7)(C) cert.org]
Sent: Wednesday, February 02, 2011 5:36 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Dropbox upload

Hi (b)(6),(b) (7)(C)

We're still show that we are receiving PCAP data into the dropbox, FYI.

Regards,

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS usdoj.gov>
Sent: Thursday, February 03, 2011 5:55 PM
To: (b)(6),(b)(7)(C),Per USSS BOS); External (b)(6),(b) cambridgepolice.org
Subject: RE: January 4th

Who took the photo? Do we have any others? And might whomever took the photo have other details on it?

From: (b)(6),(b)(7)(C),Per USSS (BOS) [mailto:(b)(6),(b)(7) usss.dhs.gov]
Sent: Thursday, February 03, 2011 5:53 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(cambridgepolice.org
Subject: Re: January 4th

I have a picture from the 4th of the drive that shows it is the same enclosure and a different disk but no serial number is visible in the picture I am looking at. I can tell the hard drive on the 4 is different because the portion shown in the photo is very dirty where as the hard drive in the enclosure seized on the 6th is clean

(b)(6),(b)(7)
(C),Per USSS

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS usdoj.gov>
To: (b)(6),(b)(7)(C),Per (BOS); External (b)(6),(b)(cambridgepolice.org
Sent: Thu Feb 03 17:45:08 2011
Subject: January 4th

(b)(5)

per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Thursday, February 03, 2011 5:50 PM
To: (b)(6),(b)(7)(C) usdoj.gov'; (b)(6),(b)(7)(C) BOS)
Subject: Re: January 4th

It was identified as a usb enclosure, but not opened. It was processed on scene.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS @usdoj.gov>
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) @usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Thu Feb 03 17:45:08 2011
Subject: January 4th

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS usdoj.gov>
Sent: Thursday, February 03, 2011 5:45 PM
To: (b)(6),(b)(7)(C),Per USSS BOS); External (b)(6),(b) cambridgepolice.org
Subject: January 4th

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C)
Sent: Thursday, February 03, 2011 5:41 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Dropbox upload

(b)(6),(b)(7)(C)

To follow-up:

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),
4500 Fifth Avenue
Pittsburgh, PA 15213
(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) ert.org' (b)(6),(b) cert.org>; (b)(6),(b)(7)(C) (CID)
Sent: Thu Feb 03 17:36:18 2011
Subject: Re: Dropbox upload

What is best address to send disk with packet capture

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) @cert.org>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Feb 02 18:10:12 2011
Subject: RE: Dropbox upload

Thanks, sir. We'll look for the cd.

Sent from a mobile device

-----Original Message-----

From: (b)(6),(b)(7)(C) (BOS) [(b)(6),(b)(7)(C) @usss.dhs.gov]
Received: Wednesday, 02 Feb 2011, 5:55pm
To: (b)(6),(b)(7)(C) @cert.org]
Subject: RE: Dropbox upload

I just stopped the transfer.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cert.org]
Sent: Wednesday, February 02, 2011 5:36 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Dropbox upload

Hi (b)(6),(b)(7)

We're still show that we are receiving PCAP data into the dropbox, FYI.

Regards,

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cert.org>
Sent: Wednesday, February 02, 2011 6:10 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Dropbox upload

Thanks, sir. We'll look for the cd.

Sent from a mobile device

-----Original Message-----
From: (b)(6),(b)(7)(C) BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Received: Wednesday, 02 Feb 2011, 5:55pm
To: (b)(6),(b)(7)(C) @cert.org]
Subject: RE: Dropbox upload

I just stopped the transfer.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @cert.org]
Sent: Wednesday, February 02, 2011 5:36 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Dropbox upload

HI (b)(6),(b)(7)(C)

We're still show that we are receiving PCAP data into the dropbox, FYI.

Regards,

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: no-reply-dropbox@cert.org
Sent: Wednesday, February 02, 2011 5:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Submission received to CERT dropbox

We have received your submission to the CERT dropbox.
It was uploaded as capXXXXt 4 (name sanitized) and the file's SHA1 hash is 4590305470a8ebffd88e14be008fef38b2262f14.
Please correspond with us at forensics@cert.org if you have questions or issues.

From: (b)(6),(b)(7)(C) @cert.org>
Sent: Wednesday, February 02, 2011 5:36 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Dropbox upload

Hi (b)(6),(b

We're still show that we are receiving PCAP data into the dropbox, FYI.

Regards,

(b)(6),(b)(7)(C)

From: no-reply-dropbox@cert.org
Sent: Wednesday, February 02, 2011 4:46 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Submission received to CERT dropbox

We have received your submission to the CERT dropbox.
It was uploaded as capXXXXt 2 (name sanitized) and the file's SHA1 hash is df7dc8b82d579c29fcb562633cd26beb82723153.
Please correspond with us at forensics@cert.org if you have questions or issues.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Wednesday, February 02, 2011 3:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b) cambridgepolice.org
Subject: Re: grace host and ghost macbook registration email

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Host Lookup

visitor registration
name: Gary Host
email: ghost42@mailinator.com
phone:
days remaining:4
last expiration date: 13-Oct-2010
MAC address: 00235a735ffc
status: inactive
comment:
please include
contact info
record last updated by (b)(6),(b)(7)(C) mit.edu at Wed Oct 13 06:54:22 2010 EDT

- From the DHCP logs:

dhcplogger/dhcp-20101009.gz:Oct 8 23:02:05 installer dhcpd: DHCPACK on 18.55.7.48 to 00:23:5a:73:5f:fc (ghost-laptop) via 18.55.0.1 dhcplogger/dhcp-20101009.gz:Oct 8 23:13:49 installer dhcpd: DHCPACK on 18.55.7.47 to 00:17:f2:2c:b0:74 (ghost-macbook) via eth0

On Feb 2, 2011, at 1:04 PM, (b)(6),(b)(7)(C) (BOS) wrote:

> Do remember what email was used on 10/08/10 when ghost macbook and Grace Host was registered?
>
> (b)(6),(b)(7)(C)
>
> U.S. Secret Service
> Boston Field Office
>
> (b)(6),(b)(7)(C)
>
>
> All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: no-reply-dropbox@cert.org
Sent: Wednesday, February 02, 2011 2:14 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Submission received to CERT dropbox

We have received your submission to the CERT dropbox.
It was uploaded as capXXXXasc (name sanitized) and the file's SHA1 hash is 84c1d606eaf59310ec6f5fcbb22c3bc7f5c8ec0b.
Please correspond with us at forensics@cert.org if you have questions or issues.

From: no-reply-dropbox@cert.org
Sent: Wednesday, February 02, 2011 2:11 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Submission received to CERT dropbox

We have received your submission to the CERT dropbox.
It was uploaded as capXXXXe-1 (name sanitized) and the file's SHA1 hash is dc9efb447d640da688b4c0f7345b90b6af0a29f3.
Please correspond with us at forensics@cert.org if you have questions or issues.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 02, 2011 11:56 AM
To: (b)(6),(b)(7)(C) CID)
Cc: External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) BOS)
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

(b)(5) per EOUSA

Steve

From: (b)(6),(b)(7)(C) (CID) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),(b)(7)(C)
4500 Fifth Avenue
Pittsburgh, PA 15213

(b)(6),(b)(7)(C)

We are eager to help in any way that we are able.

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5228 (Fax)

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usdoj.gov>
To: 'Heymann, Stephen (USAMA)'
Cc: (b)(6),(b)(7)(C) (CID); External (b)(6),(b)(cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe (b)(5) (b)(5) but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5)

per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) pcert.org>
Sent: Wednesday, February 02, 2011 11:34 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID)
Subject: RE: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

If the total size of the data we will receive is still 80GB, it would be much faster (and better) to FedEx it to us.

Thanks, sir.

Best
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, February 02, 2011 11:26 AM
To: (b)(6),(b)(7)(C) (CID)
Cc:
Subject: RE: Packet traffic to/from the Acer Laptop

I broke it up into smaller chunks and it is starting to upload now. If it does not finish, I will FedEx a copy to you tomorrow.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, February 02, 2011 11:21 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),
(b)(7)(C

You'll need to FEDEX something that big.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5228 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (CID)
Cc: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) @usdoj.gov>; External (b)(6),(b)(7)(C) @cambridgepolice.org
Sent: Wed Feb 02 11:03:09 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I am working on uploading the packet capture now. It is a nearly 80GB file. I am getting an error message now. 550 failed to capture directory. I will keep working on it. I will put together the information on the IP addresses and MAC addresses. One of the things I would like to know is if the suspect was controlling the laptop remotely and if so, an IP address that we might be able trace to a physical location. Also, I would like to know if the laptop was uploading the documents it was downloading to any other location.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) @usdoj.gov'
Cc: External; (b)(6),(b) @cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),
(b)(7)(

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN: (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),(b)(7)(C)
4500 Fifth Avenue
Pittsburgh, PA 15213
TEL: (b)(6),(b)(7)(C)

We are eager to help in any way that we are able.

(b)(6),
(b)(7)(C
(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-288-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) @usdoj.gov>
Cc: (b)(6),(b)(7)(C) (CID); External; (b)(6),(b) @cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the flow data has enough detail to show remote connections into the laptop but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C)
U.S. Secret Service

Boston Field Office

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5) per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, February 02, 2011 11:21 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6), (b)(7)

You'll need to FEDEX something that big.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (CID)
Cc: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C) usdoj.gov>; External-(b)(6),(b)(7)(C) cambridgepolice.org
Sent: Wed Feb 02 11:03:09 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I am working on uploading the packet capture now. It is a nearly 80GB file. I am getting an error message now. 550 failed to capture directory. I will keep working on it. I will put together the information on the IP addresses and MAC addresses. One of the things I would like to know is if the suspect was controlling the laptop remotely and if so, an IP address that we might be able trace to a physical location. Also, I would like to know if the laptop was uploading the documents it was downloading to any other location.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usdoj.gov'
Cc: Externa (b)(6),(b)(cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),(b)
4500 Fifth Avenue
Pittsburgh, PA 15213

TEL: (b)(6),(b)(7)(C),Per USSS

We are eager to help in any way that we are able.

(b)(6),(b)(7)(C),Per USSS

Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C),Per USSS (Desk)
(Mobile)
412-288-5226 (Fax)

From: (b)(6),(b)(7)(C),Per USSS (BOS)
To: 'Heymann, Stephen (USAMA)' (b)(6),(b)(7)(C),Per USSS @usdoj.gov>
Cc: (b)(6),(b)(7)(C), CID); External (b)(6),(b)(cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the flow data has enough detail to show remote connections into the laptop but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C),Per USSS
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C),Per USSS

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C),Per USSS @usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C),Per (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5) per EOUSA

From: no-reply-dropbox@cert.org
Sent: Wednesday, February 02, 2011 11:12 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Submission received to CERT dropbox

We have received your submission to the CERT dropbox.
It was uploaded as .htXXXXess (name sanitized) and the file's SHA1 hash is f1a71ca88bf4c93baa6612a1ed7d8142ae0811db.
Please correspond with us at forensics@cert.org if you have questions or issues.

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, February 02, 2011 10:55 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usdoj.gov'
Cc: External (b)(6),(b) cambridgepolice.org
Subject: Re: Packet traffic to/from the Acer Laptop

(b)(6),(b)(7)(C)

This request is well within our capabilities. We'll need some information in terms of authorized / unauthorized IPs and MAC addresses, but it is all stuff you already have. Also, we'll need to know what your objective is for the analysis - my assumption is to reconstruct the offender's observed activity. Finally, we need a rough time line of when the analysis is needed by the USAO.

You could upload the data to our ftp server as you've done in the past or FEDEX it to me.

USSS Resident Affiliate
ATTN (b)(6),(b)(7)(C)
CERT - CIC Room (b)(6),
4500 Fifth Avenue
Pittsburgh, PA 15213
TEL (b)(6),(b)(7)(C)

We are eager to help in any way that we are able.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C)
To: 'Heymann, Stephen (USAMA)' usdoj.gov>
Cc: (b)(6),(b)(7)(C) CID); External (b)(6),(b) cambridgepolice.org
Sent: Wed Feb 02 09:54:25 2011
Subject: RE: Packet traffic to/from the Acer Laptop

I uploaded the flow data to CERT. I have not uploaded the packet capture yet. I do not believe the flow data has enough detail to show remote connections into the laptop but the packet capture should if the connection was active while the capture was running. I will check with CERT to see if they have the resources available to analyze the packet capture.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, February 02, 2011 9:47 AM

To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 02, 2011 9:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Packet traffic to/from the Acer Laptop

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, February 02, 2011 9:05 AM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) (BOS)
Subject: RE: Please review very carefully

Will do

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) Per USSS @usdoj.gov]
Sent: Wednesday, February 02, 2011 8:37 AM
To: (b)(6),(b)(7)(C),Per USSS (BOS)
Subject: Please review very carefully

Attached is a draft affidavit in support of search warrants. Please review it very, very carefully and let me know anything that needs corrected, edited, modified, added or deleted in any way in light of what you know at this time.

<<SW Affidavit 2-1-11 draft.pdf>>

From: (b)(6),(b)(7)(C) (IRM)
Sent: Wednesday, February 02, 2011 8:43 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Setting up conference call

Sounds good.

Later:
(b)(6),(b)
Spelling errors accepted while communicating with a BlackBerry!
Thank U

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (IRM)
Sent: Wed Feb 02 08:26:19 2011
Subject: Re: Setting up conference call

The AUSA set up a line to dial in

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (IRM)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Feb 02 08:21:27 2011
Subject: Re: Setting up conference call

H (b)(6),(b)(7)(
We do have some capabilities to do this, stop by when you get in and we can discuss the options in better detail.
(b)(6),(b)(7)(C)
Spelling errors accepted while communicating with a BlackBerry!
Thank U

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)((IRM)
Sent: Wed Feb 02 07:45:36 2011
Subject: Setting up conference call

Do we have the ability to host a conference call in our office?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To (b)(6),(b)(7)(C) BOS)
Sent: Wed Feb 02 06:00:02 2011
Subject: RE: Time Check

Are you going to set up the conference line or should I see whether ours is free again?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:29 PM
To (b)(6), mit.edu; Heymann, Stephen (USAMA) (b)(6),(b) @cambridgepolice.org
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

(b)(6),(b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS usdoj.gov>
Sent: Wednesday, February 02, 2011 8:37 AM
To: Extemal (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: Please review very carefully
Attachments: SW Affidavit 2-1-11 draft.pdf

Attached is a draft affidavit in support of search warrants. Please review it very, very carefully and let me know anything that needs corrected, edited, modified, added or deleted in any way in light of what you know at this time.

<<SW Affidavit 2-1-11 draft.pdf>>

Those numbers more or less correlate to the corpus as a whole. I'd say the he was going after everything.

From: (b)(6),(b)(7)(C) ithaka.org>
Date: Fri, 28 Jan 2011 14:28:43 -0500
To: (b)(6),(b)(7)(C) ithaka.org> (b)(6),(b)(7)(C) ithaka.org>
Cc: (b)(6),(b)(7)(C) ithaka.org>
Subject: Re: MIT Update: It's worse than we know

Attached are 2 screen shots depicting PDF download activity from MIT for November and December. One show's all downloads and totals 2,854,824 for the 2 months. The other filters out downloads from the 3 IP's that look to be associated with the download abuse (b)(6),(b)(7)(C) and totals 17,865 for the 2 month period. Recognizing that some legitimate downloads may have occurred from the 3 filtered IP's, it would still be safe to say that about 2.8 million illegal downloads occurred during November and December. We know that some illegal downloading occurred prior to November and into January. I don't have those numbers yet. But looking at the graph you can see that some pretty aggressive downloading was taking place the last week of Dec (over 100k/day). It seems likely this extended into January for some period of time. It wouldn't be much of a stretch to say that as much of a million or more additional downloads may have occurred that are not reflected on this chart. I expect to have January data available for review by Monday. I'll also start loading Oct and Sept numbers as well to complete the picture.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) ithaka.org>
Date: Fri, 28 Jan 2011 14:13:57 -0500
To: (b)(6),(b)(7)(C) ithaka.org>
Cc: (b)(6),(b)(7)(C) ithaka.org> (b)(6),(b)(7)(C) ithaka.org>
Subject: RE: MIT Update: It's worse than we know

So, with September and October, what does the number look like? Still looking like the entire corpus?

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:10 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: MIT Update: It's worse than we know

(b)(6),(b)(7)(C)

Still digging and (b)(6) is going to pass along a screen shot of what he is seeing for November and December. It appears as though the activity was less impactful in November, but just these two months ballpark ~2 million + PDFs over their normal usage. (b)(6) is also seeking out data prior and since for review.

(b)(6),

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 1:53 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: RE: MIT Update: It's worse than we know

I will call in a moment.

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 1:43 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: MIT Update: It's worse than we know
Importance: High

Hi (b)(6), (b)(7)(C)

Speaking with (b)(6),(b)(7)(C) just now about making sure we have (b)(6),(b)(7)(C) time as needed for the MIT evaluation currently underway and discovering that the IP addresses associated with these specific incidents have numerous additional days of mass downloading.

It would take some time to normalize against usual MIT usage, but at first glance, it is reasonably safe to assume from what (b)(6), and I covered that the individual responsible has already acquired the entire JSTOR corpus. Glad to have a call ASAP if you think it useful and I let (b)(6), know that I thought you might be calling him shortly after receiving this message for clarification. In light of this information, it would seem that we need to try and understand the full picture outside of the identified incidents going forward. Certainly our tack here merits some re-evaluation, both concerning this case and the potential for additional measures of prevention as we move forward. Also copying in (b)(6), at this juncture.

(b)(6),(b)(7)(C)

Thanks,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) thaka.org

Hi (b)(6),(b)(7)(C)

Speaking with (b)(6),(b)(7)(C) just now about making sure we have (b)(6),(b)(7)(C) time as needed for the MIT evaluation currently underway and discovering that the IP addresses associated with these specific incidents have numerous additional days of mass downloading.

It would take some time to normalize against usual MIT usage, but at first glance, it is reasonably safe to assume from what (b) and I covered that the individual responsible has already acquired the entire JSTOR corpus. Glad to have a call ASAP if you think it useful and I let (b) know that I thought you might be calling him shortly after receiving this message for clarification. In light of this information, it would seem that we need to try and understand the full picture outside of the identified incidents going forward. Certainly our tack here merits some re-evaluation, both concerning this case and the potential for additional measures of prevention as we move forward. Also copying in (b)(6 at this juncture.

(b)(6),(b)(7)(C)

Thanks,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 02, 2011 8:31 AM
To: External (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) BOS)
Subject: FW: MIT Update: It's worse than we know

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) ithaka.org]
Sent: Friday, January 28, 2011 5:02 PM
To: Heymann, Stephen (USAMA)
Subject: FW: MIT Update: It's worse than we know

Breakdown of downloading:

From: (b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 4:57 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: Re: MIT Update: It's worse than we know

Here are the totals for each IP during Nov/Dec. All but a few thousand of these are probably attributed to the downloader.

(b)(6),(b)(7)(C)

2,341,267 (periods of activity 11/29 – 12/26)
306,984 (periods of activity 12/27 - ??)
188,708 (periods of activity 11/6 – 11/11)

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 02, 2011 8:29 AM
To: External [(b)(6),(b) cambridgepolice.org [(b)(6),(b)(7)(C) (BOS)
Subject: FW: MIT abuse
Attachments: MIT NovDec all IP's.png; MIT NovDec excluding abuse IP's.png

---

From: [(b)(6),(b)(7)(C) [mailto [(b)(6),(b)(7)(C) ithaka.org]
Sent: Friday, January 28, 2011 2:58 PM
To: Heymann, Stephen (USAMA)
Subject: MIT abuse

FYI

From: [(b)(6),(b)(7)(C)
Sent: Friday, January 28, 2011 2:29 PM
To:
Cc: [(b)(6),(b)(7)(C)
Subject: Re: MIT Update: It's worse than we know

Attached are 2 screen shots depicting PDF download activity from MIT for November and December. One show's all downloads and totals 2,854,824 for the 2 months. The other filters out downloads from the 3 IP's that look to be associated with the download abuse [(b)(6),(b)(7)(C) and totals 17,865 for the 2 month period. Recognizing that some legitimate downloads may have occurred from the 3 filtered IP's, it would still be safe to say that about 2.8 million illegal downloads occurred during November and December. We know that some illegal downloading occurred prior to November and into January. I don't have those numbers yet. But looking at the graph you can see that some pretty aggressive downloading was taking place the last week of Dec (over 100k.day). It seems likely this extended into January for some period of time. It wouldn't be much of a stretch to say that as much of a million or more additional downloads may have occurred that are not reflected on this chart. I expect to have January data available for review by Monday. I'll also start loading Oct and Sept numbers as well to complete the picture.

[(b)(6),
(b)(7)(C)

From: (b)(6),(b)(7)(C) (IRM)
Sent: Wednesday, February 02, 2011 8:21 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Setting up conference call

H (b)(6), We do have some capabilities to do this, stop by when you get in and we can discuss the options in better detail.

(b)(6), (b)(7)
Spelling errors accepted while communicating with a BlackBerry!
Thank U

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (IRM)
Sent: Wed Feb 02 07:45:36 2011
Subject: Setting up conference call

Do we have the ability to host a conference call in our office?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Wed Feb 02 06:00:02 2011
Subject: RE: Time Check

Are you going to set up the conference line or should I see whether ours is free again?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:29 PM
To: (b)(6), mit.edu; Heymann, Stephen (USAMA); (b)(6),(b) (7)(C) cambridgepolice.org
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

(b)(6),(b)(7)(C)
Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF
2259

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) sdoj.gov>
Sent: Wednesday, February 02, 2011 7:53 AM
To: External:(b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(mit.edu
Subject: RE: Time Check

Works for me as well, steve

(b)(6),(b)(7)(C)

Dial: (b)(6),(b)(7)(C)

Passcode: (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, February 01, 2011 7:30 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6), mit.edu; Heymann, Stephen (USAMA)
Subject: RE: Time Check

Yes for me!

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:29 PM
To: (b)(6), mit.edu; (b)(6),(b)(7)(C) usdoj.gov; (b)(6),(b)(7)(C)
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

(b)(6),(b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, February 02, 2011 6:00 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Time Check

Are you going to set up the conference line or should I see whether ours is free again?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @uss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:29 PM
To: (b)(6), mit.edu; Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

(b)(6),(b)(7)(C)
Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephan (USAMA) (b)(6),(b)(7)(C) sa.doj.gov>
Sent: Wednesday, February 02, 2011 5:59 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: [BULK] Accepted: Conference Call

Importance: Low

From: (b)(6),(b)(7)(C) >cambridgepolice.org>
Sent: Tuesday, February 01, 2011 7:32 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Accepted: Conference Call

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, February 01, 2011 7:30 PM
To: (b)(6),(b)(7)(C) (BOS); (b) mit.edu; (b)(6),(b)(7)(C) usdoj.gov
Subject: RE: Time Check

Yes for me!

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:29 PM
To: (b) mit.edu; (b)(6),(b)(7)(C) usdoj.gov; (b)(6),(b)(7)(C)
Subject: Time Check

Would a 10AM Conference Call work for everyone's schedule?

(b)(6),(b)(7)(C)
Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, February 01, 2011 12:31 PM
To: (b)(6),(b)(7)(C) @usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: 2nd set of attachments
Attachments: DSC01395.JPG; DSC01403.JPG; DSC01404.JPG; MapView950Mass.pdf

Anything else concerning property that either of you believe I should add?

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, February 01, 2011 12:29 PM
To: (b)(6),(b)(7)(C) @usdoj.gov; (b)(6),(b)(7)(C) BOS)
Subject: 1st set of attachments
Attachments: 950 MassAve.jpg; 950-Mass-Ave-FrontDoor.jpg; CityPropertyDatabase950Mass.pdf

See attached

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, February 01, 2011 12:28 PM
To: (b)(6),(b)(7)(C) usdoj.gov (BOS); (b)(6),(b)(7)(C)
Subject: 950 Mass Ave Description

Dwelling and Storage Locker Description

950 Massachusetts Avenue in Cambridge Massachusetts has three streets that abut the property, Massachusetts Avenue, Bay Street and Green Street. 950 Mass Ave is also known as the Bay Square Condominiums. It contains 109 residential and 4 commercial condominium units. The main entrance to the building is from Massachusetts Avenue. Upon entering the front door there is a foyer between doors that contain a list of resident's last name that show a door bell number for the resident. The door bell numbers do not reflect the actual unit number of the resident. Door bell number (b)(6) has the name Swartz on it.

The building has two lower levels and seven stories above ground on the Massachusetts Avenue side of the building. The two lower levels are garages known as lower garage and upper garage. Floor one is the ground level floor when entering from the Massachusetts Avenue side of the building. The six floors above that are floors 2 through 6 and the 7th floor is referred to as the Penthouse floor.

Unit (b)(6), (Swartz) is located on the (b)(6), floor. It has a dark brown wood grained door with the number (b)(6), attached to it just above the peep hole. It is described as a 586 square foot three room one bedroom, one bathroom corner unit condominium. Aaron Swartz is the listed tenant of unit (b)(6), The owners of the unit are listed as (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

There are storage lockers located on the following levels, lower garage, upper garage, first floor and penthouse floor (aka 7th floor). The storage lockers can be described as large locked cages. The occupants place their own locks on the locker doors. Unit (b)(6), is deeded and assigned locker (b)(6), which is located on the (b)(6), floor in a room behind the front concierge desk. The locker is marked with the letter and numeral (b)(6),(b)(7)(C)

950 Massachusetts Avenue aka Bay Square Condominiums is managed by Thayer and Associates located at 1812 Massachusetts Avenue Cambridge, MA 02140 with a telephone number of 617-354-6480.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, February 01, 2011 8:48 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: warrant

Thank you

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, February 01, 2011 7:59 AM
To: Heymann, Stephen (USAMA)
Subject: RE: warrant

I am still working on the flash drive

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, February 01, 2011 7:48 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: warrant

(b)(5) per EOUSA

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, February 01, 2011 7:48 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: warrant

(b)(5) per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Monday, January 31, 2011 2:11 PM
To: (b)(6),(b)(7)(C),Per USSS (BOS)
Subject: What year did you become a special agent with the Secret Service?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C),Per USSS usdoj.gov>
Sent: Monday, January 31, 2011 2:08 PM
To: (b)(6),(b)(7)(C),Per USSS (BOS)
Subject: USB drive

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) sdoj.gov>
Sent: Monday, January 31, 2011 11:17 AM
To: (b)(6),(b)(7)(C) BOS)
Subject:

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Monday, January 31, 2011 11:09 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please give me a call when you have a moment. Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Thursday, January 27, 2011 4:44 PM
To: (b)(6),(b)(7)(C) @usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: Re: Anything you would add to these?

Just finished, sorry for delay. Yes that looks comprehensive/good.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
Sent: Thu Jan 27 15:00:03 2011
Subject: RE: Anything you would add to these?

(b)(6), (b)(7)(

You good with them too? sph

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 27, 2011 2:04 PM
To: Heymann, Stephen (USAMA); (b)(6),(b) @cambridgepolice.org
Subject: RE: Anything you would add to these?

I don't have anything to add

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, January 27, 2011 1:56 PM
To: (b)(6),(b)(7)(C) (BOS); Extema (b)(6),(b) cambridgepolice.org
Subject: Anything you would add to these?

I'd like to get them out this p.m. Thx. Sph

<<MITattachment.pdf>> <<JSTORattachment.pdf>>

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 27, 2011 3:00 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: RE: Anything you would add to these?

(b)(6),(b)(7)(C)

You good with them too? sph

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 27, 2011 2:04 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(cambridgepolice.org
Subject: RE: Anything you would add to these?

I don't have anything to add

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 27, 2011 1:56 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: Anything you would add to these?

I'd like to get them out this p.m. Thx. Sph

<<MITattachment.pdf>> <<JSTORattachment.pdf>>

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Thursday, January 27, 2011 2:12 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) MIT.EDU'
Subject: Re: Conf Call

I can do 1pm tomorrow as well.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C) @MIT.EDU>
Cc: (b)(6),(b)(7)(C)
Sent: Thu Jan 27 13:18:25 2011
Subject: RE: Conf Call

Could we do 1:00 p.m. on Friday instead?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 27, 2011 1:16 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
Cc: (b)(6),(b) @cambridgepolice.org
Subject: RE: Conf Call

I am clear all Friday afternoon.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, January 27, 2011 1:14 PM
To: (b)(6),(b)(7)(C)
Cc: BOS); External (b)(6),(b)(7)(C) @cambridgepolice.org
Subject: RE: Conf Call

(b)(6),(b)(7)(C)

Would it be possible to talk tomorrow, instead? What's your schedule? I've just had something develop at this end.

Apologies. Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @MIT.EDU]
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) BOS); (b)(6),(b) @cambridgepolice.org
Subject: Re: Conf Call

Check and delivery confirmed.

(b)(6),(b)(7)(C)

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) usdoj.gov> wrote:

Same number. Don't know where the last one got lost in the ether, but no worries. Steve

---

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b) cambridgepolice.org; Heymann, Stephen (USAMA)
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C) gmail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)
PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b) @cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) @MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial: (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b) MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6),(b)(7)(C) I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 27, 2011 1:51 PM
To: (b)(6),(b)(7)(C) BOS (b)(6),(b)(7)(C) External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call--Change of time/date

Importance: High

Off for this afternoon. We are set for 12:00 noon tomorrow, Friday.
Same call in number and passcode.

Dial: (b)(6),(b)(7)(C)
Passcode (b)(6),(b)(7)(C)

Steve

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 27, 2011 1:16 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

I am clear all Friday afternoon.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 27, 2011 1:14 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

(b)(6),(b)(7)(C)

Would it be possible to talk tomorrow, instead? What's your schedule? I've just had something develop at this end.

Apologies. Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

Check, and delivery confirmed.

(b)(6),(b)(7)(C)

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) usdoj.gov> wrote:

Same number. Don't know where the last one got lost in the ether, but no worries. Steve

---

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) cambridgepolice.org; Heymann, Stephen (USAMA)
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable a (b)(6),(b)(7)(C) mail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--

(b)(6),(b)(7)(C)
IT Security Systems & Services, ISDA
MIT
(b)(6),(b)(7)(C)
PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial: (b)(6),(b)(7)(C)

Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6), I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),
(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) <(b)(6),(b)(7)(C) @usdoj.gov>
Sent: Thursday, January 27, 2011 1:56 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) @cambridgepolice.org
Subject: Anything you would add to these?
Attachments: MITattachment.pdf; JSTORattachment.pdf

I'd like to get them out this p.m. Thx. Sph

<<MITattachment.pdf>> <<JSTORattachment.pdf>>

From: (b)(6),(b)(7)(C) @MIT.EDU>
Sent: Thursday, January 27, 2011 1:38 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Re: Conf Call

I do have a class at that time, but can make it happen if we keep it relatively short (or if you have some specifics, I can prep ahead of time) - thoughts??

(b)(6),(b)(7)(C)
Consultant
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
PGP Fingerprint:

Please excuse typos sent via my portable.

On Jan 27, 2011, at 1:19 PM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) usdoj.gov> wrote:

> Could we do 1:00 p.m. on Friday instead?
>
> ---
> **From:** (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
> **Sent:** Thursday, January 27, 2011 1:16 PM
> **To:** Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
> **Cc:** (b)(6),(b)(cambridgepolice.org
> **Subject:** RE: Conf Call
>
> I am clear all Friday afternoon.
>
> (b)(6),(b)(7)(C)
> U.S. Secret Service
> Boston Field Office
> (b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 27, 2011 1:14 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

(b)(6),(b)(7)(

Would it be possible to talk tomorrow, instead? What's your schedule? I've just had something develop at this end.

Apologies. Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @MIT.EDU]
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(cambridgepolice.org
Subject: Re: Conf Call

Check, and delivery confirmed.
(b)(6),(b)(7)(C)

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) usdoj.gov> wrote:

> Same number. Don't know where the last one got lost in the ether, but no worries. Steve
>
> From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @MIT.EDU]
> Sent: Thursday, January 27, 2011 2:37 AM
> To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7 cambridgepolice.org; Heymann, Stephen (USAMA)
> Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C)@gmail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--

(b)(6),(b)(7)(C)

IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID (b)(6),(b)(7)(C) http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C)
(BOS) (b)(6),(b) MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. M & M, I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 27, 2011 1:18 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Cc: Externa (b)(6),(b) @cambridgepolice.org
Subject: RE: Conf Call

Could we do 1:00 p.m. on Friday instead?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thursday, January 27, 2011 1:16 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
Cc: (b)(6),(b) @cambridgepolice.org
Subject: RE: Conf Call

I am clear all Friday afternoon.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 27, 2011 1:14 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

(b)(6),(b)(7)(C

Would it be possible to talk tomorrow, instead? What's your schedule? I've just had something develop at this end.

Apologies. Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @MIT.EDU]
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); (b)(6),(b) @cambridgepolice.org
Subject: Re: Conf Call

Check, and delivery confirmed.

(b)(6),(b)(7)(C)

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) @usdoj.gov> wrote:

Same number. Don't know where the last one got lost in the ether, but no worries. Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@MIT.EDU]
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b) cambridgepolice.org; Heymann, Stephen (USAMA)
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b) gmail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--

(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)
PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b)(7)(C)@cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial: (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU

Cc: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C)
Subject: Follow-up questions with

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6), (b)(7)(C) I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) [redacted]usdoj.gov>
Sent: Thursday, January 27, 2011 1:14 PM
To: [redacted](BOS); External [redacted]@cambridgepolice.org
Cc:
Subject: RE: Conf Call

[redacted]

Would it be possible to talk tomorrow, instead? What's your schedule? I've just had something develop at this end.

Apologies. Steve

From: [redacted] [mailto:[redacted]MIT.EDU]
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: [redacted](BOS); [redacted]cambridgepolice.org
Subject: Re: Conf Call

Check, and delivery confirmed.

[redacted]

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" [redacted]usdoj.gov> wrote:

> Same number. Don't know where the last one got lost in the ether, but no worries. Steve
>
> ---
>
> **From:** [redacted] [mailto:[redacted]MIT.EDU]
> **Sent:** Thursday, January 27, 2011 2:37 AM
> **To:** [redacted](BOS); [redacted]cambridgepolice.org; Heymann, Stephen (USAMA)
> **Subject:** Re: Conf Call
>
> This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable a[redacted]mail.com).
>
> I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--

(b)(6),(b)(7)(C)

IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b)(7)(C)@cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6),(b)(7)(C) I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret

Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 27, 2011 1:07 PM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Re: Conf Call

Check, and delivery confirmed.
(b)(6), (b)(7)(C

On Jan 27, 2011, at 6:56 AM, "Heymann, Stephen (USAMA)" (b)(6),(b)(7)(C) sdoj.gov> wrote:

Same number. Don't know where the last one got lost in the ether, but no worries. Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 27, 2011 7:37 AM
To: (b)(6),(b)(7)(C) (BOS (b)(6),(b)(7)(C) epolice.org; Heymann, Stephen (USAMA)
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C) gmail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--

(b)(6),(b)(7)(C)

IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)
PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM

To: External (b)(6),(b)(7)(C) @cambridgepolice.org (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial: (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: TUESDAY, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) BOS (b)(6),(b) MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6),(b)(7)(C) I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) sdoj.gov>
Sent: Thursday, January 27, 2011 6:56 AM
To: (b)(6),(b)(7)(C) BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Conf Call

Same number. Don't know where the last one got lost in the ether, but no worries. Steve

---

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @MIT.EDU]
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) cambridgepolice.org; Heymann, Stephen (USAMA)
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C) gmail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--
(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: (b)(6),(b)(7)(C) http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.
(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?
(b)(6),(b)(7)(C)
U.S. Secret Service

Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C)@usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External:(b)(6),(b)(7)(C)@cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial: 877-876-7643
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)@MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today (b)(6),(b)(7)(C) I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Thursday, January 27, 2011 6:43 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usdoj.gov
Subject: RE: Conf Call

4pm – I got it.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) usdoj.gov
Subject: Re: Conf Call

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C) mail.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),

--
(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: (b)(6),(b)(7)(C) http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM, (b)(6),(b)(7)(C) BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)
U.S. Secret Service

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 27, 2011 2:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) usdoj.gov
Subject: [BULK] Re: Conf Call

Importance: Low

This is disconcerting - Steve, I didn't receive the below email from you confirming the call time. Have you sent me any other emails, because I have none at all from you. (As I apparently may not get your reply, I'm also reachable at (b)(6),(b)(7)(C) email.com).

I've put 4pm Thursday on my calendar. Same number?

Best,
(b)(6),(b)(7)(C)

--
(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 26, 2011, at 4:48 PM, (b)(6),(b)(7)(C) (BOS) wrote:

Let me know if either 4pm on Thursday or 1pm on Friday is a good time to have a conference call.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

On Jan 26, 2011, at 4:07 PM (b)(6),(b)(7)(C) (BOS) wrote:

Are you able to make the conference call?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 25, 2011 7:19 AM
To: External (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) MIT.EDU
Cc: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6), I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

PGP Fingerprint: (b)(6),(b)(7)(C)

On Jan 24, 2011, at 6:25 PM (b)(6),(b)(7)(C) BOS) wrote:

When would be a good time for you to have a conference call on Wednesday?

Also, if it works for you, I would like to drop by your office sometime tomorrow to get a copy of the packet data capture and the video surveillance file. When would be a good time?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 24, 2011 5:45 PM
To: (b)(6),(b)(7)(C) BOS); External (b)(6),(b) cambridgepolice.org
Subject: Follow-up questions with (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Can you two arrange a time on Wednesday when we can get on the phone with (b)(6),(b)(7)(C) both with some follow-up questions and to confirm our understanding of some facts? He will want to be on a speakerphone so he can access the network logs while we talk. My schedule is flexible all day, but all things being equal, the morning would work better for me. Also, our conference line is booked all week, can you arrange one from there?

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, January 26, 2011 3:28 PM
To:
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: SW Reconnaissance

Lt. and (b)(6),(b)(7)(C) and I are meeting CFD Captain (b)(6),(b)(7) at 10:00am on Friday.

I'll be donning CFD paraphilia and doing a fire prevention inspection of 950 Mass Ave to gather information for an affidavit we're writing.

Thanks for the hookup.

R/S
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, January 26, 2011 3:19 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Accepted: Reconnaissance

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, January 26, 2011 9:34 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Subpoenas

Follow Up Flag: Follow up
Flag Status: Completed

(b)(3):Rule 6E,(b)(5)

(b)(5)

steve per EOUSA

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, January 25, 2011 6:33 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Just got out

Thanks once again...

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 25, 2011 5:28 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Just got out

Long but done with

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) cambridgepolice.org>
To: (b)(6),(b)(7)(C) BOS)
Sent: Tue Jan 25 17:23:24 2011
Subject: Just got out

How did it go?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, January 25, 2011 5:23 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Just got out

How did it go?

From: (b)(6),(b)(7)(C) ithaka.org>
Sent: Tuesday, January 25, 2011 4:32 PM
To: (b)(6),(b)(7)(C) BOS)
Cc: @usdoj.gov'
Subject: Contacts @ JSTOR

Hi (b)(6),(b)(7)(C)

Please find the information requested below...

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) ithaka.org

(b)(6),(b)(7)(C) Office of General Counsel
(b)(6),(b)(7)(C) ithaka.org

(b)(6),(b)(7)(C) Public Systems

(b)(6),(b)(7)(C) Public Systems

From: (b)(6),(b)(7)(C) ithaka.org>
Sent: Tuesday, January 25, 2011 3:03 PM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) usdoj.gov; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: RE: Conference Call

Please dial int (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 25, 2011 2:59 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C)
Cc:
Subject: Re: Conference Call

Are we calling you or are you calling us?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) ithaka.org> (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) ithaka.org>; BOS)
Sent: Tue Jan 25 12:47:47 2011
Subject: RE: Conference Call

3:00 works for me, as well. Thank you for setting up the call. Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) ithaka.org]
Sent: Tuesday, January 25, 2011 12:35 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov'; (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA)
Subject: Re: Conference Call

Works for me too.

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 25, 2011 12:33 PM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Subject: Conference Call

I changed my other meeting. 3pm works for me

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) ithaka.org]
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 25, 2011 12:48 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: RE: Conference Call

3:00 works for me, as well. Thank you for setting up the call. Steve

---

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @ithaka.org]
Sent: Tuesday, January 25, 2011 12:35 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov'; (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA)
Subject: Re: Conference Call

Works for me too.

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 25, 2011 12:33 PM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Subject: Conference Call

I changed my other meeting. 3pm works for me

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @ithaka.org]
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)
JSTOR | Portico

(b)(6),(b)(7)(C) @ithaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 25, 2011 12:46 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Conference Call

Thx, sph

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 25, 2011 12:34 PM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA)
Subject: Conference Call

I changed my other meeting. 3pm works for me

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @ithaka.org]
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)
JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @ithaka.org>
Sent: Tuesday, January 25, 2011 12:35 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Cc: @usdoj.gov'
Subject: Re: Conference Call

Works for me too.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Tuesday, January 25, 2011 12:33 PM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Subject: Conference Call

I changed my other meeting. 3pm works for me

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) @ithaka.org]
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)
JSTOR | Portico
(b)(6),(b)(7)(C) @ithaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, January 25, 2011 12:30 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re:

I don't know if I am going to be ready or released at that time.

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C)
Sent: Tue Jan 25 12:21:10 2011
Subject: Fw:

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) @ithaka.org>
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) @ithaka.org>
Sent: Tue Jan 25 12:07:11 2011
Subject:
Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)
JSTOR | Portico
(b)(6),(b)(7)(C) ithaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 25, 2011 12:22 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Conference Call

(b)(6),(b)(7)(C)

Can you move your pick up time earlier. I'm tight at this end, if we don't start 'till 3:30.

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) @uss.dhs.gov]
Sent: Tuesday, January 25, 2011 12:15 PM
To: (b)(6),(b)(7)(C)
Cc: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C)
Subject: Conference Call

I have a meeting at 3pm at MIT to pick up some files but I should be able to join a conference call anytime after 3:30

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) ithaka.org]
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)
JSTOR | Portico
(b)(6),(b)(7)(C) thaka.org

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @ithaka.org>
Sent: Tuesday, January 25, 2011 12:07 PM
To: (b)(6),(b)(7)(C) (SOS)
Cc:

Hi (b)(6),(b)(7)(C)

We have arranged for resources from our side and it looks as though 3-4 would be optimal for us today. Is that reasonable on your side? I'll send a meeting invite and a conference line once you have confirmed.

Best,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) @ithaka.org

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 25, 2011 7:19 AM
To: External: (b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) MIT.EDU
Subject: RE: Follow-up questions with (b)(6),(b)(7)(C)

4:00 Wednesday it is. (If it starts to run too long, we can always pick up on Thursday.)

Dial (b)(6),(b)(7)(C)
Passcode: (b)(6),(b)(7)(C)

steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)(C)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6), I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) <cambridgepolice.org>
Sent: Tuesday, January 25, 2011 6:14 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b) MIT.EDU
Cc: Heymann, Stephen (USAMA)
Subject: Follow-up questions with (b)(6),(b)(7)

I have commitments today and tomorrow. I could possibly make the 3:00pm today. (b)(6), , I'll keep you posted on that.

That being said, I would be available after 4pm on both days. Could we make that work for a conference call?

(b)(6),(b)(7)(C)

To: (b)(6),(b)(7)(C) (BOS); External-(b)(6),(b)(7)(C) cambridgepolice.org
Subject: Follow-up questions with (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

Can you two arrange a time on Wednesday when we can get on the phone with (b)(6),(b)(7)(C), both with some follow-up questions and to confirm our understanding of some facts? He will want to be on a speakerphone so he can access the network logs while we talk. My schedule is flexible all day, but all things being equal, the morning would work better for me. Also, our conference line is booked all week, can you arrange one from there?

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 24, 2011 5:45 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: Follow-up questions with (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

Can you two arrange a time on Wednesday when we can get on the phone with (b)(6),(b)(7)(C), both with some follow-up questions and to confirm our understanding of some facts? He will want to be on a speakerphone so he can access the network logs while we talk. My schedule is flexible all day, but all things being equal, the morning would work better for me. Also, our conference line is booked all week, can you arrange one from there?

Steve

From: (b)(6),(b)(7)(C) (CHI)
Sent: Friday, January 21, 2011 4:30 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

Wow! – from ethics.harvard.edu – pretty high-profile defendant. He also has his own Wikipedia entry. Surprised this didn't make it into the news. Also weird that he couldn't just afford to buy articles, or have a JSTOR account at Harvard...! - (b)(6),

Aaron Swartz

Lab Fellow, 2010-2011
Aaron Swartz is a writer, hacker, and activist. He co-authored the RSS 1.0 specification, helped develop standards for the Semantic Web, and designed the metadata system for Creative Commons. He co-founded Reddit.com, an online news startup acquired by Condé Nast, and architected OpenLibrary.org. His writing has appeared in a variety of magazines and journals and he has been profiled in Wired and Newsweek. He is on the board of Change Congress and is the co-founder of the Progressive Change Campaign Committee. During the fellowship year, he will conduct experimental and ethnographic studies of the political system to prepare a monograph on the mechanisms of political corruption.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 3:16 PM
To: (b)(6),(b)(7)(C) (CHI)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

No. Never a student or associated with MIT. He is a lab fellow of Harvard's Safra Center for Ethics. His father is listed as an associate of MIT but we are still researching the details of that.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CHI)
Sent: Friday, January 21, 2011 4:11 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

Very nice! Is the perp an MIT student?

H.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 3:03 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C)

(CID)
Subject: FW: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

FYI

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: BOS
Sent: Friday, January 21, 2011 2:59 PM
To: CID
Cc: ISD; BOS
Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM:	BOSTON FIELD OFFICE	FILE: 102-775-60071-S
TO:	CRIMINAL INVESTIGATIVE DIVISION	X-REF: N/A
INFO:	INVESTIGATIVE SUPPORT DIVISION	SEIZURE#: N/A

SUBJECT: OPENING REPORT

CASE TITLE:	AARON SWARTZ
CASE TYPE:	775.510
SECONDARY TYPES:	848.191, 848,304, 848.930
CONTROLLING OFFICE:	BOSTON FIELD OFFICE
REPORT MADE BY:	SA (b)(6),(b)(7)(C)
DATE CASE OPENED:	01/07/11
PREVIOUS REPORT:	N/A
REPORTING PERIOD:	01/04/11 - 01/21/11
STATUS:	CONTINUED

SYNOPSIS:

On 01/04/11, MIT police requested assistance from members of the New England Electronic Crime Task Force regarding an investigation into a computer that was found in a locked closet at MIT and was connected to the MIT Network without authorization. Further investigation revealed that a subject later identified as Aaron Swartz, intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR.

On 01/06/11, Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering. The investigation of Swartz's unauthorized intrusion into the MIT network and the theft of documents from JSTOR continue.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology (MIT) Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and that Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Continuing on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) of the MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security Analyst, and (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, in the basement of building 16. Criminalist (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from the Cambridge Police Department processed the scene for fingerprints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Network traffic indicated that the netbook was using two IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male, later identified as Aaron Swartz (DOB 11/08/86), enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7)(C) was able to provide SA (b)(6),(b)(7)(C) with the following timeline regarding this investigation:

On 09/26/10, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) Manager, stating that excessive downloading of journals had been detected from MIT, and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) Security Analyst, discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" registered on the network on 09/24/10. (b)(6),(b)(7) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff, emailed (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Libraries, to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b)(7) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security and Support Services for MIT, notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) Operations and Infrastructure, that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can use to host a Virtual Machine.

On 01/03/11, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) Network Operations, and (b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b)(7)(C) located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard drive. (b)(6),(b)(7)(C) established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(7)(C) also provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b)(

provided SA (b)(6),(b)(7)(C) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7)(C) of the MIT Police Department and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) detained the suspect and he was subsequently placed under arrest. A search of the backpack the suspect was wearing revealed a U.S. passport in the name of Aaron Swartz and one (1) USB Thumb Drive. No computer was found in the backpack. Swartz was transported by Cambridge Police to Cambridge Police headquarters and subsequently charged with violation of Massachusetts General Law (MGL) for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations containing the word "ghost". Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) mit.edu) an (b)(6),(b)(7)(C) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) and (b)(6),(b)(traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(7)(contacted (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7)(met (b)(6),(b)(7)(and (b)(6),(b)(7)(at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves, SA (b)(6),(b)(7) examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Continuing on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters, SA (b)(6),(b)(7)(met (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) com). (b)(6),(b)(7)(C) informed SA (b)(6),(b)(7)(that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department and charged with violation of Massachusetts General Law (MGL) Chapter 266, Section 18, Breaking and Entering.

On 01/06/11, SA (b)(6),(b)(7)(C) contacted AUSA Steven Heymann, District of Massachusetts, to brief him on the above investigation.

On 01/07/11, Aaron Swartz was arraigned in Cambridge, MA District Court for violation of MGL Chapter 266, Section 18, Breaking and Entering. The case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C)
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Yes
1599A:	No
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	
ADDRESS:	
EMAIL:	

DATABASE CHECKS: 01/07/11

EXAMS CONDUCTED:

ECSAP:	Pending
POLY: N/A	
PSD:	N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11

LOCAL LE: 01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently being held at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

USSS / BOSTON (b)(6),(b)(7)(C) / RICCIARDI

From: (b)(6),(b)(7)(C) (CHI)
Sent: Friday, January 21, 2011 4:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

Ethics! Can't make this stuff up!

H.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 3:16 PM
To: (b)(6),(b)(7)(C) (CHI)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

No. Never a student or associated with MIT. He is a lab fellow of Harvard's Safra Center for Ethics. His father is listed as an associate of MIT but we are still researching the details of that.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CHI)
Sent: Friday, January 21, 2011 4:11 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

Very nice! Is the perp an MIT student?

H.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 3:03 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)
Subject: FW: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

FYI

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: BOS
Sent: Friday, January 21, 2011 2:59 PM
To: CID

Cc: ISD; BOS
Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE FILE: 102-775-60071-S
TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A
INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A

SUBJECT: OPENING REPORT

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.510
SECONDARY TYPES: 848.191, 848,304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: N/A
REPORTING PERIOD: 01/04/11 - 01/21/11
STATUS: CONTINUED

SYNOPSIS:

On 01/04/11, MIT police requested assistance from members of the New England Electronic Crime Task Force regarding an investigation into a computer that was found in a locked closet at MIT and was connected to the MIT Network without authorization. Further investigation revealed that a subject later identified as Aaron Swartz, intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR.

On 01/06/11, Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering. The investigation of Swartz's unauthorized intrusion into the MIT network and the theft of documents from JSTOR continue.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology (MIT) Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and that Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Continuing on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) of the MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security Analyst, and (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, in the basement of building 16. Criminalist (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from the Cambridge Police Department processed the scene for fingerprints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Network traffic indicated that the netbook was using two IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male, later identified as Aaron Swartz (DOB 11/08/86), enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7)(C) was able to provide SA (b)(6),(b)(7)(C) with the following timeline regarding this investigation:

On 09/26/10, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) stating that excessive downloading of journals had been detected from MIT, and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) of Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu), (b)(6),(b)(7)(C) Security Analyst, discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" registered on the network on 09/24/10. (b)(6),(b)(7) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff, emailed (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) detained the suspect and he was subsequently placed under arrest. A search of the backpack the suspect was wearing revealed a U.S. passport in the name of Aaron Swartz and one (1) USB Thumb Drive. No computer was found in the backpack. Swartz was transported by Cambridge Police to Cambridge Police headquarters and subsequently charged with violation of Massachusetts General Law (MGL) for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations containing the word "ghost". Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) mit.edu) an (b)(6),(b)(7)(C) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) and (b)(6),(b)(7 traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(7) contacted (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7)(met (b)(6),(b)(7) and (b)(6),(b)(7) at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves, SA (b)(6),(b)(7) examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Continuing on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters, SA (b)(6),(b)(7) met Philip G Cormier (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) goodcormier.com). Cormier informed SA (b)(6),(b)(7)(that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department and charged with violation of Massachusetts General Law (MGL) Chapter 266, Section 18, Breaking and Entering.

On 01/06/11, SA (b)(6),(b)(7)(C) contacted AUSA Steven Heymann, District of Massachusetts, to brief him on the above investigation.

On 01/07/11, Aaron Swartz was arraigned in Cambridge, MA District Court for violation of MGL Chapter 266, Section 18, Breaking and Entering. The case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C) 1374
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Yes
1599A:	No
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	
ADDRESS:	
EMAIL:	

DATABASE CHECKS: 01/07/11

EXAMS CONDUCTED:

ECSAP:	Pending
POLY: N/A	
FSD:	N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11
LOCAL LE:	01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently being held at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

USSS / BOSTON

(b)(6),(b)(7)(C) / RICCIARDI

From: (b)(6),(b)(7)(C) (CHI)
Sent: Friday, January 21, 2011 4:11 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

Very nice! Is the perp an MIT student?

H.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 3:03 PM
To: (b)(6),(b)(7)(C) BOS)
Cc: (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)
Subject: FW: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

FYI

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: BOS
Sent: Friday, January 21, 2011 2:59 PM
To: CID
Cc: ISD; BOS
Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE FILE: 102-775-60071-S
TO: CRIMINAL INVESTIGATIVE DIVISION X-REF: N/A
INFO: INVESTIGATIVE SUPPORT DIVISION SEIZURE#: N/A

SUBJECT: OPENING REPORT

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.510
SECONDARY TYPES: 848.191, 848,304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: N/A
REPORTING PERIOD: 01/04/11 - 01/21/11
STATUS: CONTINUED

SYNOPSIS:

On 01/04/11, MIT police requested assistance from members of the New England Electronic Crime Task Force regarding an investigation into a computer that was found in a locked closet at MIT and was connected to the MIT Network without authorization. Further investigation revealed that a subject later identified as Aaron Swartz, intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR.

On 01/06/11, Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering. The investigation of Swartz's unauthorized intrusion into the MIT network and the theft of documents from JSTOR continue.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology (MIT) Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and that Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Continuing on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) of the MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security Analyst, and (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, in the basement of building 16. Criminalist (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from the Cambridge Police Department processed the scene for fingerprints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Network traffic indicated that the netbook was using two IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male, later identified as Aaron Swartz (DOB 11/08/86), enter the wire closet. Based on the surveillance video, Swartz appeared

to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7)(C) was able to provide SA (b)(6),(b)(7)(C) with the following timeline regarding this investigation:

On 09/26/10, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) stating that excessive downloading of journals had been detected from MIT, and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) of Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu), (b)(6),(b)(7)(C) (b)(6),(b)(7)(C), discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" registered on the network on 09/24/10 (b)(6),(b)(7)(C) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff, emailed (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of "ghost-laptop" (b)(6),(b)(7)(C) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security and Support Services for MIT, notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) MIT Operations and Infrastructure, that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can use to host a Virtual Machine.

On 01/03/11, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) Network Operations, and (b)(6),(b)(7)(C) it.edu) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Network and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b)(7) located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard drive. (b)(6),(b)(7) established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(7)(C) also provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b) provided SA (b)(6),(b)(7) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7)(C) of the MIT Police Department and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) detained the suspect and he was subsequently placed under arrest. A search of the backpack the suspect was wearing revealed a U.S. passport in the name of Aaron Swartz and one (1) USB Thumb Drive. No computer was found in the backpack. Swartz was transported by Cambridge Police to Cambridge Police headquarters and subsequently charged with violation of Massachusetts General Law (MGL) for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations containing the word "ghost". Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) mit.edu) an (b)(6),(b)(7)(C) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) and (b)(6),(b) traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(7)(contacted (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7) met (b)(6),(b)(7) and

(b)(6),(b)(7)(C) at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves, SA (b)(6),(b) examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Continuing on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters, SA (b)(6),(b)(7) met Philip G Cormier (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) goodcormier.com). Cormier informed SA (b)(6),(b)(7) that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department and charged with violation of Massachusetts General Law (MGL) Chapter 266, Section 18, Breaking and Entering.

On 01/06/11, SA (b)(6),(b)(7)(C) contacted AUSA Steven Heymann, District of Massachusetts, to brief him on the above investigation.

On 01/07/11, Aaron Swartz was arraigned in Cambridge, MA District Court for violation of MGL Chapter 266, Section 18, Breaking and Entering. The case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C)
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown

1599: Yes
1599A: No
PHOTO: Yes
PRINTS: Yes
POB: Chicago, IL
DL/STATE:
ADDRESS:
EMAIL:
DATABASE CHECKS: 01/07/11

EXAMS CONDUCTED:

ECSAP: Pending
POLY: N/A
FSD: N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI: 01/07/11
NCIC/NLETS: 01/07/11
CCS/CFT: 01/07/11
LOCAL LE: 01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently being held at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

USSS / BOSTON (b)(6),(b)(7)(C) / RICCIARDI

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 21, 2011 4:03 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)
Subject: FW: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

FYI

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: BOS
Sent: Friday, January 21, 2011 2:59 PM
To: CID
Cc: ISD; BOS
Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
INFO: INVESTIGATIVE SUPPORT DIVISION

FILE: 102-775-60071-S
X-REF: N/A
SEIZURE#: N/A

SUBJECT: OPENING REPORT

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.510
SECONDARY TYPES: 848.191, 848.304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: N/A
REPORTING PERIOD: 01/04/11 - 01/21/11
STATUS: CONTINUED

SYNOPSIS:

On 01/04/11, MIT police requested assistance from members of the New England Electronic Crime Task Force regarding an investigation into a computer that was found in a locked closet at MIT and was connected to the MIT Network without authorization. Further investigation revealed that a subject later identified as Aaron Swartz, intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR.

On 01/06/11, Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering. The investigation of Swartz's unauthorized intrusion into the MIT network and the theft of documents from JSTOR continue.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7)(C) MIT.EDU) of the Massachusetts Institute of Technology (MIT) Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and that Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Continuing on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7)(C) of the MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security Analyst, and (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, in the basement of building 16. Criminalist (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from the Cambridge Police Department processed the scene for fingerprints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAX0D001001100E1601. Network traffic indicated that the netbook was using two IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male, later identified as Aaron Swartz (DOB 11/08/86), enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7)(C) was able to provide SA (b)(6),(b)(7)(C) with the following timeline regarding this investigation:

On 09/26/10, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) stating that excessive downloading of journals had been detected from MIT, and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores

them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) Scholarly Publishing and Licensing, regarding excessive downloading from two IP addresses (b)(6),(b)(7)(C) and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) Security Analyst, discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" registered on the network on 09/24/10. (b)(6),(b)(7) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff, emailed (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address (b)(6),(b)(7)(C)

On 10/13/10, (b)(6),(b)(7)(C) traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b)(7) disabled the host registrations identified as bogus. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Security and Support Services for MIT, notified (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) MIT Operations and Infrastructure, that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can use to host a Virtual Machine.

On 01/03/11, (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) forwarded from (b)(6),(b)(7)(C) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(7)(C) emailed (b)(6),(b)(7)(C) Network Operations, and (b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) Network and Infrastructure Services for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b)(7) located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard drive. (b)(6),(b)(7) established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(7)(C) also provided SA (b)(6),(b)(7)(C) with a copy of historical network flow data concerning IP addresses (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b)(7)(C) contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b)(7) provided SA (b)(6),(b)(7)(C) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7)(C) of the MIT Police Department and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge, Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7)(C) responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) detained the suspect and he was subsequently placed under arrest. A search of the backpack the suspect was wearing revealed a U.S. passport in the name of Aaron Swartz and one (1) USB Thumb Drive. No computer was found in the backpack. Swartz was transported by Cambridge Police to Cambridge Police headquarters and subsequently charged with violation of Massachusetts General Law (MGL) for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) checked the DHCP logs for computer registrations containing the word "ghost". Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) mit.edu) and (b)(6),(b)(7)(C) traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)(7)(C) and (b)(6),(b)(7) traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(7) contacted (b)(6),(b)(7)(C) to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b)(7) met (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves, SA (b)(6),(b)(7) examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Continuing on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters, SA (b)(6),(b)(7)(C) met (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) goodcormier.com). (b)(6),(b)(7)(C) informed SA (b)(6),(b)(7)(C) that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7)(C) AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department and charged with violation of Massachusetts General Law (MGL) Chapter 266, Section 18, Breaking and Entering.

On 01/06/11, SA (b)(6),(b)(7)(C) contacted AUSA Steven Heymann, District of Massachusetts, to brief him on the above investigation.

On 01/07/11, Aaron Swartz was arraigned in Cambridge, MA District Court for violation of MGL Chapter 266, Section 18, Breaking and Entering. The case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C)
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Yes
1599A:	No
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	
ADDRESS:	
EMAIL:	

DATABASE CHECKS: 01/07/11

EXAMS CONDUCTED:

ECSAP: Pending

POLY: N/A
FSD: N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11
LOCAL LE:	01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently being held at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

USSS / BOSTON (b)(6),(b)(7)(C) / RICCIARDI

From: (b)(6),(b)(7)(C) CambridgePolice.Org>
Sent: Friday, January 21, 2011 9:23 AM
To: External: (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) BOS)
Subject: RE: Photographs of laptop found in MIT on 01-04-11

I'll have a disk ready for you (b)(6),(so you can pick it up and send it along. It will be certified as all photos maintained by this office with this file #.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) Manager

Cambridge Police Department
125 Sixth Street
Cambridge, MA 02142
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Thursday, January 20, 2011 5:18 PM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C)
Subject: RE: Photographs of laptop found in MIT on 01-04-11

(b)(6),(b)(7)(C)

If it would help, you can burn a disk with these and I'll pick them up tomorrow morning?

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 20, 2011 5:16 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: Photographs of laptop found in MIT on 01-04-11

Would it be possible for me to get copies of the photographs taken of room 04T of Building 16, the Durance Building of MIT on 01/01/11 including the photographs of the computer found?

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) <cambridgepolice.org>
Sent: Thursday, January 20, 2011 5:18 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: RE: Photographs of laptop found in MIT on 01-04-11

(b)(6), (b)(7)(C)

If it would help, you can burn a disk with these and I'll pick them up tomorrow morning?

(b) (6),(b

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C)@usss.dhs.gov]
Sent: Thursday, January 20, 2011 5:16 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Photographs of laptop found in MIT on 01-04-11

Would it be possible for me to get copies of the photographs taken of room 04T of Building 16, the Durance Building of MIT on 01/01/11 including the photographs of the computer found?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 20, 2011 5:16 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: Re: Photos of Swartz Laptop taken at Stratton Center

(b)(6),(b)(7)(C) no problem will see (b)(6),(b)(7)(C) in the morning. (b)(6),(

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 20, 2011 05:13 PM
To: (b)(6),(b)(7)(C)
Subject: Photos of Swartz Laptop taken at Stratton Center

Would it be possible for me to get copies of the photographs taken of Swartz's laptop when we found it at the Stratton Center?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Thursday, January 20, 2011 7:16 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Cambridge District Court Roster January 2011.doc
Attachments: cdc roster January 2011.doc

I left a few messages with ADA (b)(6),(b)(7)(C) who's contact information is on the attached roster.

From: (b)(6),(b)(7)(C)
Sent: Thursday, January 20, 2011 7:02 AM
To: *All PD Sworn Officers
Subject: cdc roster January 2011.doc

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, January 19, 2011 10:43 AM
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usdoj.gov'
Subject: Re: Updates

Copy

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov> (b)(6),(b)(7)(C)
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wed Jan 19 10:22:06 2011
Subject: Re: Updates

OK

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To: Extemal (b)(6),(b)(cambridgepolice.org; (b)(6),(b)(7)(C) BOS)
Sent: Wed Jan 19 10:20:40 2011
Subject: RE: Updates

Why don't you two give me a call from the lab again. 2:00?

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b) cambridgepolice.org]
Sent: Wednesday, January 19, 2011 9:52 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: Updates

Early afternoon works for me, before 3:00pm

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Wednesday, January 19, 2011 9:41 AM
To: (b)(6),(b)(7)(C) (BOS);
Subject: Updates (b)(6),(b)(7)(C)

Would it be better to talk again this afternoon or tomorrow morning on our respective follow-ups?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: Heymann, Stephen (USAMA) [redacted]sdoj.gov>
Sent: Wednesday, January 19, 2011 10:21 AM
To: External [redacted]cambridgepolice.org; [redacted]BOS)
Subject: RE: Updates

Why don't you two give me a call from the lab again. 2:00?

From: [redacted] [mailto:[redacted]@cambridgepolice.org]
Sent: Wednesday, January 19, 2011 9:52 AM
To: Heymann, Stephen (USAMA); [redacted](BOS)
Subject: RE: Updates

Early afternoon works for me, before 3:00pm

From: Heymann, Stephen (USAMA) [mailto:[redacted]@usdoj.gov]
Sent: Wednesday, January 19, 2011 9:41 AM
To: [redacted](BOS); [redacted]
Subject: Updates

Would it be better to talk again this afternoon or tomorrow morning on our respective follow-ups?

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Wednesday, January 19, 2011 9:52 AM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) (BOS)
Subject: RE: Updates

Early afternoon works for me, before 3:00pm

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Wednesday, January 19, 2011 9:41 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Updates (b)(6),(b)(7)(C)

Would it be better to talk again this afternoon or tomorrow morning on our respective follow-ups?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, January 19, 2011 9:41 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Updates

Would it be better to talk again this afternoon or tomorrow morning on our respective follow-ups?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Wednesday, January 19, 2011 8:57 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Telephone Record Subpoena

(b)(3):Rule 6E,(b)(5)

(b)(3):Rule 6E,(b)(5)

Steve

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, January 18, 2011 8:54 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b) cambridgepolice.org
Subject: FW: one more link

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 18, 2011 8:54 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: FW: link

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 18, 2011 8:12 AM
To: External (b)(6),(b) @cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: When can I get the two of you on the phone this a.m.?

I'll call you guys a bit after 10:00

From: (b)(6),(b)(7)(C) [mailto: (b)(6),(b)(7)(C) @cambridgepolice.org]
Sent: Tuesday, January 18, 2011 8:01 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: When can I get the two of you on the phone this a.m.?

On my cell phone, (b)(6),(b)(7)(C) Or in about a two hours, (b)(6),(and I should be in the same room.

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, January 18, 2011 7:45 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: When can I get the two of you on the phone this a.m.?

I am free any time except 11:00-12:00. Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, January 18, 2011 8:01 AM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (BOS)
Subject: RE: When can I get the two of you on the phone this a.m.?

On my cell phone (b)(6),(b)(7)(C) Or in about a two hours, (b)(6), and I should be in the same room.

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Tuesday, January 18, 2011 7:45 AM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: When can I get the two of you on the phone this a.m.?

I am free any time except 11:00-12:00. Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Tuesday, January 18, 2011 7:45 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: When can I get the two of you on the phone this a.m.?

I am free any time except 11:00-12:00. Steve

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 13, 2011 6:08 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Aaron Swartz and the stolen laptop

Thanks (b)(6), (b)(7) However I do think some of the information that will be discussed would helpful to our investigation. (b)(6),

On Jan 13, 2011, at 5:55 PM, (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) @usss.dhs.gov> wrote:

> I don't think there was any reason. I think the AUSA wanted to have a meeting on just the technical computer network part of the case. I am sure he will want to talk to everyone eventually.
>
> (b)(6),(b)(7)(C)
>
> U.S. Secret Service
>
> Boston Field Office
> (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 13, 2011 5:47 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: Aaron Swartz and the stolen laptop

Ok, 1300 should be ok give my cell a call. (b)(6), any reason MIT Police were not invited to the meeting (b)

On Jan 13, 2011, at 5:11 PM, (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) @usss.dhs.gov> wrote:

> AUSA Heymann, DET (b)(6), (b)(7)(C and myself are meeting (b)(6),(b)(7)(C) and (b)(6), (b)(7)(from IS&T tomorrow, 1/14/11 at 1100 at the Office of the General Counsel conference room. (b)(6),(b)(7)(C) and I could probably meet with you right after that meeting. I am not sure how long the first meeting will take but I think we could plan on meeting you around 1300.
>
> (b)(6),(b)(7)(C)
>
> U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)MIT.EDU]
Sent: Thursday, January 13, 2011 5:00 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); (b)(6),(b)(7)(C)
Subject: Re: Aaron Swartz and the stolen laptop

All, Det. (b)(6),(b)(7)(C) is working to re interview the reporting party, I will check on status in the AM. The student who saw Swartz in the student center is coming to view a photo array sometime tomorrow. Harvard Police is checking for any reports they have on Swartz and what is his job at Harvard, I should have any info in the morning. I also should have camera footage of the student center that might show Swartz entering W-20 after he cleaned out his equipment from building 16 on and reinstalled same onThursday (b)(6), here is my cell (b)(6),(b)(7)(C) I would like to set a meeting with you, Sgt. (b)(6), and (b)(6),(b)(7) to discuss a game plan. I will call Middlesex ADA to get a time when we can have a sit down with him also. (b)(6),

On Jan 13, 2011, at 3:36 PM, (b)(6),(b)(7)(C) mit.edu> wrote:

(b)(6),
(b)(7)

Not sure, i am forwarding this email to (b)(6) and (b)(6),(b)(7)(C) They are running the invest.

J

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) (BOS)"
(b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 13, 2011 3:31 pm
Subject: Aaron Swartz and the stolen laptop
To: (b)(6),(b)(7)(C) mit.edu>

Any luck re-interviewing the victim for the serial number?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C),Per USSS

From: Heymann, Stephen (USAMA)
[mailto:(b)(6),(b)(7)(C),Per usdoj.gov]
Sent: Thursday, January 13, 2011 3:27 PM
To: (b)(6),(b)(7)(C),Per (BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

Can you or (b)(6), touch base with him, whomever is appropriate

---

From: (b)(6),(b)(7)(C),Per USSS (BOS) [mailto:(b)(6),(b)(7)(C),Per USSS usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from (b)(6),(b)(7)(C),Per USSS yet

(b)(6),(b)(7)(C),Per USSS

U.S. Secret Service

Boston Field Office

(b)(6),(b)(7)(C),Per USSS

From: Heymann, Stephen (USAMA)
[mailto:(b)(6),(b)(7)(C),Per usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C),Per (BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any

inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (CID)
Sent: Thursday, January 13, 2011 5:57 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Out of Office AutoReply: CCFinder

I will be out of the office from 01/11 through 01/17/2011 with limited access to voicemail/email. Please direct CERT inquiries to ATSAIC (b)(6),(b)(7)(C) r (b)(6),(b)(7)(C) sss.dhs.gov) during this time.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 13, 2011 5:47 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Aaron Swartz and the stolen laptop

Ok, 1300 should be ok give my cell a call. (b)(6),(b)(7)(C) any reason MIT Police were not invited to the meeting. (b)(6),(b)(7)(C)

On Jan 13, 2011, at 5:11 PM, (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) usss.dhs.gov> wrote:

> AUSA Heymann, DET (b)(6),(b)(7)(C) and myself are meeting (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from IS&T tomorrow, 1/14/11 at 1100 at the Office of the General Counsel conference room. (b)(7)(C) and I could probably meet with you right after that meeting. I am not sure how long the first meeting will take but I think we could plan on meeting you around 1300.
>
> (b)(6),(b)(7)(C)
>
> U.S. Secret Service
>
> Boston Field Office
> (b)(6),(b)(7)(C)
>
> ---
> **From:** (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
> **Sent:** Thursday, January 13, 2011 5:00 PM
> **To:** (b)(6),(b)(7)(C)
> **Cc:** (b)(6),(b)(7)(C) (BOS);
> **Subject:** Re: Aaron Swartz and the stolen laptop
>
> Ali, Det (b)(6),(b)(7)(C) is working to re interview the reporting party, I will check on status in the AM. The student who saw Swartz in the student center is coming to view a photo array sometime tomorrow. Harvard Police is checking for any reports they have on Swartz and what is his job at Harvard, I should have any info in the morning. I also should have camera footage of the student center that might show Swartz entering W-20 after he cleaned out his equipment from building 16 on and reinstalled same on Thursday. (b)(6), here is my cell (b)(6),(b)(7)(C) I would like to set a meeting with you, Sgt (b)(6), and (b)(6),(b)(7)(C) to discuss a game plan. I will call Middlesex ADA to get a time when we can have a sit down with him also. (b)(6)
>
> On Jan 13, 2011, at 3:36 PM, (b)(6),(b)(7)(C) mit.edu> wrote:
>
> (b)(6),(b)(7)(C)

Not sure, i am forwarding this email to (b)(6) and (b)(6),(b)(7)(C) They are running the invest.

J

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) [BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 13, 2011 3:31 pm
Subject: Aaron Swartz and the stolen laptop
To: (b)(6),(b)(7)(C) mit.edu>

Any luck re-interviewing the victim for the serial number?

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, January 13, 2011 3:27 PM
To: (b)(6),(b)(7)(C) [BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

Can you or (b)(6) touch base with him, whomever is appropriate

---

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from (b)(6),(b)(7)(C) yet

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: Haymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Do we know the serial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 13, 2011 5:00 PM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS);
Subject: Re: Aaron Swartz and the stolen laptop

All, Det. (b)(6), (b)(7)(is working to re interview the reporting party, I will check on status in the AM. The student who saw Swartz in the student center is coming to view a photo array sometime tomorrow. Harvard Police is checking for any reports they have on Swartz and what is his job at Harvard, I should have any info in the morning. I also should have camera footage of the student center that might show Swartz entering W-20 after he cleaned out his equipment from building 16 on and reinstalled same on Thursday (b)(6), here is my cell (b)(6),(b)(7) (b)(6),(b)(7) (C) I would like to set a meeting with you, Sgt (b)(6), and (b)(6),(b)(7) (C) to discuss a game plan. I will call Middlesex ADA to get a time when we can have a sit down with him also. (b)(6

On Jan 13, 2011, at 3:36 PM, (b)(6),(b)(7)(C) mit.edu> wrote:

(b)(6),(b) (7)(C)

Not sure, i am forwarding this email to (b) (6) and (b)(6), (b)(7)(They are running the invest.

J

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 13, 2011 3:31 pm
Subject: Aaron Swartz and the stolen laptop
To: (b)(6),(b)(7)(C) mit.edu>

Any luck re-interviewing the victim for the serial number?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 13, 2011 3:27 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

per EOUSA Can you or (b) (6), touch base with him, whomever is appropriate

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from Captain (b)(6), (b)(7)(C) yet

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 13, 2011 4:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

(b)(5),(b)(7)(C)

Per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from Captain (b)(6), (b)(7)(C) yet

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) @MIT.EDU>
Sent: Thursday, January 13, 2011 3:36 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C)
Subject: Re: Aaron Swartz and the stolen laptop

(b)(6),(b)(7)(C)

Not sure, i am forwarding this email to (b)(6), and (b)(6),(b)(7)(C). They are running the invest.

(b)(5),(b)(7)(C)

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 13, 2011 3:31 pm
Subject: Aaron Swartz and the stolen laptop
To: (b)(6),(b)(7)(C) @mit.edu>

Any luck re-interviewing the victim for the serial number?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, January 13, 2011 3:27 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

Can you or (b)(6), touch base with him, whomever is appropriate

---

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from Captain (b)(6),(b)(7)(C) yet

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) sdoj.gov]
Sent: Thursday, January 13, 2011 3:27 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Do we know the seial number of the stolen laptop yet?

Can you or (b)(5) touch base with him, whomever is appropriate

---

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 13, 2011 2:12 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Do we know the seial number of the stolen laptop yet?

I have not heard from (b)(6),(b)(7)(C) yet

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 13, 2011 1:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Do we know the seial number of the stolen laptop yet?

Does it mesh with the one used by Swartz?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 13, 2011 11:24 AM
To: (b)(6),(b)(7)(C) (BOS); External-(b)(6),(b)(7)(C) ambridgepolice.org
Subject: I will meet you two at MIT tomorrow. steve

You both were cc'd with directions yesterday, right?

(b)(6),(b)(7)(C)

(b)(5),(b)(7)(C)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 11, 2011 11:04 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Stolen Laptop Report

Do you have a copy of the police report made when the laptop was stolen, or do we need to wait for (b)(6),(b)(7)(C) return on that one?

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 11, 2011 10:06 AM
To: (b)(6),(b)(7)(C) [BOS]; External-(b)(6),(b)(7)(C) cambridgepolice.org
Cc:
Subject: RE: Confirming Interviews on Friday

(b)(5),(b)(7)(C)

Per EOUSA

Steve

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Tuesday, January 11, 2011 8:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) [BOS]; (b)(6),(b)(7)(C)
Subject: RE: Confirming Interviews on Friday

Steve –

Friday does work for us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to 11:00). Hopefully that's okay.

I have been in contact with the folks in IS&T and they came up with a slightly different list of names of people you'd probably want to speak with. They suggested (b)(6),(b)(7)(C) and (b)(6),(b)(7) they've advised me that (b) would likely be able to provide the same information that (b)(6),(b)(7)(C) and (b)(6),(b)(7) could provide). Also, (b)(6), (b)(6),(b)(7)(C) advised me that he probably can't provide much information beyond what you could get from (b)(6),(b)(7)(C) (b)(6),(b)(7)(C). If you still want to speak to everyone, I'm sure we can make it work, but I just want to be sure we're being as efficient as possible. Let me know your thoughts.

We can hold the meeting in the Office of General Counsel conference room, located in room 10-370. To get here, walk through the main entrance of 77 Massachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a long corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large quad facing the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confuse things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General Counsel. Follow the hallway until you see another sign for the entrance to the Office of the General Counsel.

I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Tuesday, January 11, 2011 9:19 AM
To: (b)(6),(b)(7)(C) BOS); (b)(6), MIT.EDU'; (b)(6),(b)(7)(C) usdoj.gov'
Cc: (b)(6),(b)(7) MIT.EDU'
Subject: Re: Confirming Interviews on Friday

Ditto with time, place and participants.

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) sss.dhs.gov>
To: (b)(6),(b)(7)(C) MIT.EDU>; Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Cc: (b)(6),(b)(7)(C) @MIT.EDU>
Sent: Tue Jan 11 09:15:04 2011
Subject: RE: Confirming Interviews on Friday

1100 works for me. I am OK with keeping the interview to (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7) @MIT.EDU]
Sent: Tuesday, January 11, 2011 8:27 AM
To: Heymann, Stephen (USAMA)
Cc: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: RE: Confirming Interviews on Friday

Steve –

Friday does work for us, although it might be easier to start at 11:00 (our conference room is booked from 9:30 to 11:00). Hopefully that's okay.

I have been in contact with the folks in IS&T and they came up with a slightly different list of names of people you'd probably want to speak with. They suggested (b)(6),(b)(7)(C) and (b)(6),(b)(7) they've advised me that (b)(6) would likely be able to provide the same information that (b)(6),(b)(7)(C) and (b)(6),(b)(7) could provide). Also, (b)(6), (b)(6),(b)(7)(C) advised me that he probably can't provide much information beyond what you could get from (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) If you still want to speak to everyone, I'm sure we can make it work, but I just want to be sure we're being as efficient as possible. Let me know your thoughts.

We can hold the meeting in the Office of General Counsel conference room, located in room 10-370. To get here, walk through the main entrance of 77 Massachusetts Avenue. You will enter a large lobby (known as Lobby 7) and see a long corridor directly in front of you (known as the Infinite Corridor). Follow the Infinite Corridor until you enter another large open lobby, known as Lobby 10 (you will see a large set of doors on the right that look out onto a large quad facing the Back Bay, called Killian Court). When you're in Lobby 10, there will be two elevators on your left (to further confuse things, you may see a sign that says "Lobby 13" with an arrow, but you're in Lobby 10 at that point). Take either of the elevators to the third floor. When you exit the elevators, immediately turn left and you will see a sign for the Office of the General Counsel. Follow the hallway until you see another sign for the entrance to the Office of the General Counsel.

I'm in meetings the bulk of today, so I will be somewhat inaccessible, but we can coordinate any additional details tomorrow.

(b)(6),(b)(7)(C)

Office of the General Counsel
Massachusetts Institute of Technology
77 Massachusetts Avenue, Building 10-370
Cambridge, MA 02139
tel: (b)(6),(b)(7)(C)
fax: 617-258-0267
(b)(6),(b)(7) mit.edu

This message and any attached documents contain information which may be confidential, subject to privilege, or exempt from disclosure under applicable law. These materials are intended only for the use of the intended recipient. Delivery of this message to any person other than the intended recipient shall not compromise or waive such confidentiality, privilege, or exemption from disclosure as to this communication.

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 4:30 PM
To: (b)(6),(b)(7)(C)
Cc: (BOS); (b)(6),(b)(7)(C)
Subject: Confirming Interviews on Friday

(b)(6),(b)(7)(C)

If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).

(b)(6),(b)(7)(C)

(b)(5),(b)(7)(C)

Per EOUSA

Thank you, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 11, 2011 9:09 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Aaron Schwartz

What is the name of the task force?

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 11, 2011 9:07 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Aaron Schwartz

The same address as me should work

10 Causeway Street
(b)(6),(b)(7)
Boston, MA 02222
(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 11, 2011 7:50 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Aaron Schwartz

What mailing address should I use for (b)(6),(b)(7)(C) at your offices?

(b)(6),(b)(7)(C)
Cambridge Police Department
(whatever you tell me the name of the task force is)
(your office address)

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 11, 2011 7:43 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Aaron Schwartz

USSS case number is J-102-775-60071-S

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto: (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 11, 2011 7:27 AM

To: (b)(6),(b)(7)(C) (BOS)
Subject: Aaron Schwartz

What is your case number on this investigation? (I need to know it to open an investigation on our end with a victim.) Thanks, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) ithaka.org>
Sent: Tuesday, January 11, 2011 8:50 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc:
Subject: MIT & JSTOR

Good Morning (b)(6),(b)(7)(C)

Per a conversation I had with our legal counsel after yesterday's call, we are requesting that all future inquiries be made through our legal counsel's office. I have CCed (b)(6),(b)(7)(C) on this message.

Best,

(b)(6),(b)(7)(C)

JSTOR | Portico

(b)(6),(b)(7)(C) ithaka.org

To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Confirming Interviews on Friday

(b)(6),(b)(7)(C)

If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).

(b)(6),(b)(7)(C)

(b)(5),(b)(7)(C)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 11, 2011 7:50 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Aaron Schwartz

What mailing address should I use for (b)(6),(b)(7)(C) at your offices?

(b)(6),(b)(7)(C)
Cambridge Police Department
(whatever you tell me the name of the task force is)
(your office address)

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Tuesday, January 11, 2011 7:43 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Aaron Schwartz

USSS case number is J-102-775-60071-S

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) doj.gov]
Sent: Tuesday, January 11, 2011 7:27 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Aaron Schwartz

What is your case number on this investigation? (I need to know it to open an investigation on our end with a victim.) Thanks, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Tuesday, January 11, 2011 7:44 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Aaron Schwartz

Thx

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) sss.dhs.gov]
Sent: Tuesday, January 11, 2011 7:43 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Aaron Schwartz

USSS case number is J-102-775-60071-S

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Tuesday, January 11, 2011 7:27 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Aaron Schwartz

What is your case number on this investigation? (I need to know it to open an investigation on our end with a victim.) Thanks, Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) sdoj.gov>
Sent: Tuesday, January 11, 2011 7:27 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Aaron Schwartz

What is your case number on this investigation? (I need to know it to open an investigation on our end with a victim.) Thanks, Steve

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Tuesday, January 11, 2011 2:20 AM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject: Re: Meeting
Attachments: PGP.sig

Hey (b)(6), unfortunately, I have a conflict as I'll be in a training at 9am (on Wed., too) -- I am available at 12:00 on Wed/Fri and it's over at 3; Thursday is fairly clean, except for a 10:30.

Best,

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)

PGP public key ID: (b)(6),(b)(7)(C) | http://pgp.mit.edu

On Jan 10, 2011, at 2:43 PM, (b)(6),(b)(7)(C) (BOS) wrote:

FYI

AUSA Steve Heymann is scheduling interviews between MIT staff and Detective (b)(6),(b)(7)(C) and myself to go over the logs. He is going to set it up for 0930 on Friday. You will probably get the call later.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further

disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) (BOS)
Sent: Monday, January 10, 2011 6:22 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Re: Draft Notification of State Arrest

I'll look at it tomorrow. Thanks

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Sent: Mon Jan 10 18:20:53 2011
Subject: Draft Notification of State Arrest

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM:	BOSTON FIELD OFFICE	FILE:	J-102-775-60071-S
TO:	CRIMINAL INVESTIGATIVE DIVISION	X-REF:	N/A
INFO:	INVESTIGATIVE SUPPORT DIVISION	SEIZURE#:	N/A

SUBJECT: NOTIFICATION OF STATE ARREST
AARON H. SWARTZ - DATE OF ARREST : 01/06/11

ACTUAL LOSS: $TBD POTENTIAL LOSS: $50,000.00

STATUTES VIOLATED: BRAKING AND ENTERING C266 S18

CASE TITLE:	AARON SWARTZ
CASE TYPE:	775.426 - UNAUTHORIZED ACCESS UNIVERSITIES
SECONDARY TYPES:	848.191, 848,304, 848.930
CONTROLLING OFFICE:	BOSTON FIELD OFFICE
REPORT MADE BY:	SA (b)(6),(b)(7)(C)
DATE CASE OPENED:	01/07/11
PREVIOUS REPORT:	N/A
REPORTING PERIOD:	01/04/11 - 01/10/11
STATUS:	CONTINUED

SYNOPSIS:

Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force for breaking and entering.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 09/26/10 at approximately 12:31 (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) the JSTOR (b)(6),(b)(7)(C) stating that at 0800 excessive downloading of journals had been detected from MIT and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT

drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves SA (b)(6),(b)(examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Also on 01/06/11, SA (b)(6),(b) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters SA (b)(6),(b) met Philip G Cormier (b)(6),(b)(7)(C) goodcormier.com). Cormier informed SA (b)(6),(b)(7)(C) that he represented Swartz and that his client would not make a statement.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was booked by Cambridge Police Department for violation of Massachusetts General Law chapter 266 section 18, Breaking and Entering in the daytime for felony.

On 01/07/11, Aaron Swartz was arraigned in Cambridge District court for violation of MGL C266 S18, breaking and entering and his case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

AARON H SWARTZ - DEPENDENT - ARRESTED (STATE)

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C)
FBI:	675304KD0
SID:	MA10556559
HT:	5' - 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Pending
1599A:	Pending
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	N/A
ADDRESS:	
EMAIL:	N/A
DATABASE CHECKS:	01/07/11

EXAMS CONDUCTED:

ECSAP: Pending
Poly: N/A
FSD: N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11
LOCAL LE:	01/07/11

Results of database searches have been reported under "Details of Investigation".

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation.

(b)(6),(b)(7)(C) / Ricciardi

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 4:30 PM
To: (b)(6),(b)(7 MIT.EDU
Cc: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Subject: Confirming Interviews on Friday

(b)(6),(b)(7)(C)

If you can make it work from your end, let's do the interviews on Friday beginning at 10:00 a.m. I anticipate (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) joining me. Tentatively, we would like to speak with the following five people in the order listed (as well as anyone else you may think useful or appropriate).

(b)(6),(b)(7)(C)

(b)(5),(b)(7)(C)

Per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 4:20 PM
To: External (b)(6),(b) cambridgepolice.org
Cc: (b)(6),(b)(7)(C) BOS)
Subject: RE: MIT Interviews

I'll set it up for 10:00 on Friday then. Location to follow. Steve

---

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b) cambridgepolice.org]
Sent: Monday, January 10, 2011 4:09 PM
To: Heymann, Stephen (USAMA)
Subject: Re: MIT Interviews

I can be at MIT at 10:00 with a 9:30

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C)
Sent: Mon Jan 10 15:37:09 2011
Subject: RE: MIT Interviews

Could you be at MIT by 10:00 with a 9:30, or is the 9:30 on the phone?

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Monday, January 10, 2011 3:34 PM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT Interviews

10:00am start would work better for me. I have a 8:30 to 9:30 already set up.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Mon Jan 10 14:32:10 2011
Subject: RE: MIT Interviews

I'll set up the interviews for Friday at MIT then. Both of you wide open. If so, I'll propose starting at 9:30 or 10:00 and going as long as they take.

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Monday, January 10, 2011 2:30 PM
To: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT Interviews

I travel back on Thursday and will be working Friday.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS) (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)

Sent: Mon Jan 10 12:16:04 2011
Subject: MIT Interviews

Is my memory correct that (b) is out until Friday, but back on Friday? per EOUSA

If so, are you both free on Friday to interview the core MIT people and (b)(5)

Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Monday, January 10, 2011 3:34 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: Re: MIT Interviews

10:00am start would work better for me. I have a 8:30 to 9:30 already set up.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Mon Jan 10 14:32:10 2011
Subject: RE: MIT Interviews

I'll set up the interviews for Friday at MIT then. Both of you wide open. If so, I'll propose starting at 9:30 or 10:00 and going as long as they take.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) @cambridgepolice.org]
Sent: Monday, January 10, 2011 2:30 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT Interviews

I travel back on Thursday and will be working Friday.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Mon Jan 10 12:16:04 2011
Subject: MIT Interviews

Is my memory correct that (b)(6) is out until Friday, but back on Friday? per EOUSA

If so, are you both free on Friday to interview the core MIT people and (b)(6) ?

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 3:02 PM
To: External (b)(6),(b) cambridgepolice.org; (b)(6),(b)(7)(C) OS)
Subject: RE: MIT Interviews

per EOUSA

(b)(5)

Steve

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Monday, January 10, 2011 2:30 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT Interviews

I travel back on Thursday and will be working Friday.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Mon Jan 10 12:16:04 2011
Subject: MIT Interviews

per EOUSA

Is my memory correct that (b) is out until Friday, but back on Friday?

If so, are you both free on Friday to interview the core MIT people and (b)(5) ?

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 2:53 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: JStor

I would still like to talk with him about the events themselves. Can we set up a time later today or tomorrow morning? From his perspective, it will also inform his discussion on Wednesday.

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) uss.dhs.gov]
Sent: Monday, January 10, 2011 2:49 PM
To: Heymann, Stephen (USAMA)
Subject: RE: JStor

I just got through to him. He did receive my email. JSTOR has a meeting scheduled for Wednesday to discuss just how they are going to value the items in this case. He also said they are preparing the logs for us.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 2:42 PM
To: (b)(6),(b)(7)(C) BOS)
Cc: External (b)(6),(b) cambridgepolice.org
Subject: JStor

(b)(6),(b)(7)(C)

Have you been able to make contact with JSTOR? I have been given the name (b)(6),(b)(7)(C) (b)(6),(b)(7) as the right person to which to reach out, if you do not have an independent point of contact. His number is (b)(6),(b)(7)(C)

Can you find some times during which you and I could talk to him together over the phone, presuming he is out of state.

Thanks, steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 2:42 PM
To: (b)(6),(b)(7)(C) BOS)
Cc: External (b)(6), @cambridgepolice.org
Subject: JStor

Mike,

Have you been able to make contact with JSTOR? I have been given the name (b)(6),(b)(7)(C) (b)(6),(b)(7) as the right person to which to reach out, if you do not have an independent point of contact. His number is (b)(6),(b)(7)(C)

Can you find some times during which you and I could talk to him together over the phone, presuming he is out of state.

Thanks, steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 2:32 PM
To: External-(b)(6),(b)(7)(C) cambridgepolice.org; (b)(6),(b)(7)(C) (BOS)
Subject: RE: MIT Interviews

I'll set up the interviews for Friday at MIT then. Both of you wide open. If so, I'll propose starting at 9:30 or 10:00 and going as long as they take.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Monday, January 10, 2011 2:30 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT Interviews

I travel back on Thursday and will be working Friday.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Mon Jan 10 12:16:04 2011
Subject: MIT Interviews

per EOUSA

Is my memory correct that (b)(6) is out until Friday, but back on Friday?

If so, are you both free on Friday to interview the core MIT people and (b)(5)

Steve

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Monday, January 10, 2011 2:30 PM
To: (b)(6),(b)(7)(C) usdoj.gov (b)(6),(b)(7)(C) BOS)
Subject: Re: MIT Interviews

I travel back on Thursday and will be working Friday.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>; (b)(6),(b)(7)(C)
Sent: Mon Jan 10 12:16:04 2011
Subject: MIT Interviews

Is my memory correct that (b)(6), is out until Friday, but back on Friday? per EOUSA

If so, are you both free on Friday to interview the core MIT people and (b)(5) ?

Steve

From: Heymann, Stephen (USAMA) [(b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 12:50 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: MIT Interviews

Please check

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Monday, January 10, 2011 12:21 PM
To: Heymann, Stephen (USAMA)
Subject: RE: MIT Interviews

I believe he is traveling back on Friday but will not return to the office until next Monday.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, January 10, 2011 12:16 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: MIT Interviews

Is my memory correct that (b)(6),(is out until Friday, but back on Friday? per EOUSA

If so, are you both free on Friday to interview the core MIT people and (b)(5) ?

Steve

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) sdoj.gov>
Sent: Monday, January 10, 2011 12:16 PM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b) cambridgepolice.org
Subject: MIT Interviews

per EOUSA

Is my memory correct that (b)(6),(7)(C) is out until Friday, but back on Friday?

If so, are you both free on Friday to interview the core MIT people and (b)(5) ?

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 12:14 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Please contact Postal

Thx

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) sss.dhs.gov]
Sent: Monday, January 10, 2011 11:54 AM
To: Heymann, Stephen (USAMA)
Subject: RE: Please contact Postal

USPI (b)(6),(b)(7)(C) is running it now.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) @usdoj.gov]
Sent: Monday, January 10, 2011 8:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please contact Postal

Please contact Postal and see if they are delivering mail to Aaron Swartz at 950 Massachusetts Ave, Apt (b)(6),(b)(7)(C)
Cambridge 02139

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Monday, January 10, 2011 10:49 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Who is on Postal Task Force?

We do not have anyone assigned right now. What do you need? You may be able to call USPI (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) She is very helpfull.

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Cc: (BOS)
Sent: Mon Jan 10 10:34:15 2011
Subject: Who is on Postal Task Force?

Who do we have on the Postal Task Force?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto:(b)(6),(b)(7)(C) usdoj.gov]
Sent: Monday, January 10, 2011 8:47 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please contact Postal

Please contact Postal and see if they are delivering mail to Aaron Swartz at 950 Massachusetts Ave, Ap (b)(6),(b)(7)(C) Cambridge 02139

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Monday, January 10, 2011 8:47 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Please contact Postal

Please contact Postal and see if they are delivering mail to Aaron Swartz at 950 Massachusetts Ave, Apt (b)(6),(b)(7)(C) Cambridge 02139

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Saturday, January 08, 2011 1:37 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: Theft of material from JSTOR
Attachments: PGP.sig

Hey (b)(6), - just saw this - it's (b)(6),(b)(7)(C) ithaka.org>. I'm hoping to have the pcap/flows/video/logs all in by to me Monday, possibly sooner - if you don't already have a copy of the video or pcap, I'll make sure you get one.

Have a good weekend –
(b)(6),(b)

On Jan 7, 2011, at 11:59 AM, (b)(6),(b)(7)(C) (BOS) wrote:

(b)(6),(b)(7)(C)

I am an agent with the U.S. Secret Service in the Boston Field Office. I am investigating the theft of property from JSTOR through an unauthorized intrusion into the MIT network. I was given your contact information from (b)(6),(b)(7) Could you please estimate for me the monetary value of the documents that may have been downloaded by Aaron Swartz from November of 2010 until yesterday?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Saturday, January 08, 2011 1:28 AM
To: (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C)
Subject: Finalized timeline of events on JSTOR incident
Attachments: jstor_incident_timeline.docx; Untitled attachment 00022.txt; PGP.sig

Attached is the timeline, finalized and seen by the network operations staff involved.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, January 07, 2011 5:55 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Evidence Preservation

AT&T, correct?

From: (b)(6),(b)(7)(C) BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, January 07, 2011 4:58 PM
To: Heymann, Stephen (USAMA)
Subject: RE: Evidence Preservation

The phone number (b)(6),(b)(7)(C) has not been ported

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) [mailto (b)(6),(b)(7)(C) usdoj.gov]
Sent: Friday, January 07, 2011 4:30 PM
To: External (b)(6),(b) cambridgepolice.org (b)(6),(b)(7)(C) BOS)
Subject: Evidence Preservation

per EOUSA

(b)(5)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Friday, January 07, 2011 5:47 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External-(b)(6),(b @cambridgepolice.org; (b)(6),(b)(7)(C) (USAMA)
Subject: FW: Library Network Electronic Journal Theft

FYI, Steve

From: Heymann, Stephen (USAMA)
Sent: Friday, January 07, 2011 12:04 PM
To: (b)(6),(b)(7)(C)
Subject: Library Network Electronic Journal Theft

(b)(5),(b)(6),(b)(7)(C)

per EOUSA

Thank you, Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Friday, January 07, 2011 5:46 PM
To: (b)(6),(b)(7)(C) (BOS)
Cc: External (b)(6),(b)(@cambridgepolice.org (b)(6),(b)(7)(C) SAMA)
Subject: MIT Records

(b)(5),(b)(6),(b)(7)(C)

per EOUSA

Thank you, Steve

From: (b)(6),(b)(7)(C) >cambridgepolice.org>
Sent: Friday, January 07, 2011 4:58 PM
To: (b)(6),(b)(7)(C) @usdoj.gov; (b)(6),(b)(7)(C) BOS)
Subject: Re: Evidence Preservation

Copy that.

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
To: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) @uscg.dhs.gov>
Sent: Fri Jan 07 16:30:20 2011
Subject: Evidence Preservation

(b)(5)

per EOUSA

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) sdoj.gov>
Sent: Friday, January 07, 2011 4:30 PM
To: Externa (b)(6),(b) @cambridgepolice.org (b)(6),(b)(7)(C) BOS)
Subject: Evidence Preservation

(b)(5)

per EOUSA

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Friday, January 07, 2011 2:31 PM
To: (b)(6),(b)(7)(C) usdoj.gov; (b)(6),(b)(7)(C) usdoj.gov; (b)(6),(b)(7)(C) OS); (b)(6),(b)(7)(C) BOS)
Subject: Fw: Updated: Timeline of JSTOR-related events from September through today

---

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Sent: Fri Jan 07 13:47:09 2011
Subject: FW: Updated: Timeline of JSTOR-related events from September through today

(b)(6), (b)(7)(- Not sure this public knowledge, but I wanted you to have this info.

(b) (6),(b

From: (b)(6),(b)(7)(C) [mailto:(b)(6), (b)(7)(C) plant.mit.edu]
Sent: Friday, January 07, 2011 8:46 AM
To: (b)(6),(b)(7)(C)
Subject: FW: Updated: Timeline of JSTOR-related events from September through today

(b)(6),(b)(7)(C)

FYI.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Friday, January 07, 2011 7:24 AM
To: (b)(6),(b)(7)(C)
Subject: Fwd: Updated: Timeline of JSTOR-related events from September through today

Sent from my iPhone

Begin forwarded message:

From: (b)(6),(b)(7)(C) mit.edu>
Date: January 7, 2011 3:46:04 AM EST
To: (b)(6),(b)(7)(C) @mit.edu, (b)(6),(b)(7)(C) mit.edu>
Subject: Updated: Timeline of JSTOR-related events from September through today

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Timeline of JSTOR-related events

People involved:

(b)(6),(b)(7)(C)

JSTOR (b)(6),(b)(7)(C)
JSTOR
Cambridge Police Detective
United States Secret Service Special Agent
MIT (b)(6),(b)(7)(C)
MIT
MIT
MIT Campu (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)
MIT (b)(6),(b)(7)(C)
MIT
MIT (b)(6),(b)(7)(C)
MIT
MIT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)
MIT TT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)
MIT (b)(6),(b)(7)(C)

Sun 9/26/10 | 12:31pm (b)(6), receives email from (b)(6), (b)(7)(at JSTOR stating that at 8am excessive downloading of journals
started and that all of MIT's access to JSTOR has been blocked.

Mon 9/27/10 | 10:28am Security team receives email from (b)(6), (b)(7)(regarding excessive downloading from two IP addresses
(b)(6),(b)(7)(C) & 18.55.6.215 and needs help identifying the user of those addresses. (b)(6),(
follows up with (b) (6),(b, that we're looking into identifying user.

Mon 9/27/10 | pm JSTOR restores MIT's access having changed their blocking to just (b)(6),(b)(7) (C) user information
discovered reveals bogus guest network registration named Gary Host (ghost@mailinator.com)
with host registration occurring on Fri 9/24/10.

Mon 9/27/10 | pm Computer registration for bogus host disabled.

Tue 9/28/10 | am (b) (6),(b emails (b)(6), (b)(7) to speak to issues regarding the bogus registration info as well as the IP
blocking approach and thinks a call with JSTOR might be fruitful in determining JSTOR's
future courses of action around blocking, as a) blocking is usually a temporary solution and b) this problem would most likely reocour because IP addresses are easily
changed.

It becomes clear that this is willful and intentional abuse for possible purpose of spidering JSTOR

without being identified. All bogus host registrations are disabled.

Wed 10/13/10 | 3:12pm [redacted] emails [redacted] and [redacted] with the information that it appears to be the same unknown person

using our guest registration capability from a wired connection in building 16.

Wed 10/13/10 | 3:42pm [redacted] responds to [redacted] and Security team that she will pursue the Libraries moving to the proxy/

econtrol system for accessing JSTOR.

Wed 10/13/10 | 10:41pm [redacted] sends email to [redacted] and [redacted] that the offending machine is no longer seen on the network.

Thu 10/14/10 | 10:47am [redacted] emails [redacted] to inquire as to whether JSTOR is still seeing continued excessive downloading.

Voices support for the Libraries to move to econtrol/proxy system for MIT's access to JSTOR.

Thu 10/14/10 | 5:05pm [redacted] emails [redacted] and [redacted] to let us know of JSTOR's wanting some sort of indication that we've

identified the user or any expectation of being able to identify in the future.

Thu 10/14/10 | 9:09pm [redacted] responds to [redacted] email with reasons for difficulties of identifying random guest user

making attempts to thwart detection when using our wired network.

Thu 10/14/10 | 11:26pm [redacted] asks [redacted] for any updates to share with [redacted] and [redacted]

Thu 10/14/10 | 11:33pm [redacted] emails facts of case to date to [redacted] around extreme robotic activity of JSTOR at MIT.

Fri 10/15/10 | 1:31am [redacted] emails [redacted] and [redacted] to keep eye out for the host so their physical location can be

determined if they show up again.

Fri 10/15/10 | 11:26am [redacted] forwards email from JSTOR to MIT Security team; JSTOR would like assurances that we could

monitor for this type of behavior. [redacted] responds to JSTOR that it is not technically feasible

for us to do that kind of monitoring. I point out that JSTOR has many more capabilities than we do

to facilitate that kind of monitoring.

Meanwhile, there are emails between [redacted] and [redacted] that speak to risk management and

protection, both technically and practically, of our own assets and resources against this type

of threat.

Fri 10/22/10 | 4:48pm (b)(6), (b)(7) from JSTOR sets up conference for 10/26 with (b)(6), (b)(7) from JSTOR (b)(6),(b)(7) and (b)(6),(

Tue 10/26/10 | 2:00pm Conference call with JSTOR; next moves to econtrol/proxy system for authentication to JSTOR was discussed. (b) sends email with update and next steps: JSTOR will make landing page to smooth access for users who try to access JSTOR directly from MIT's network rather than using proxy.

Libraries would then go ahead and communicate with users (drafts were already ready). Proxy server configuration changes would be made. JSTOR would be contacted and would change the list of permitted IPs to only MIT's proxy servers.

Mon 11/29/10 | 6:47pm Security team receives notice from IEEE that journal spidering is occurring on their site. It is tracked to the SIPB XVM cluster, a group of computers that are shared and that anyone in the MIT community can host a Virtual Machine on.

Tue 11/30/10 | 2:40am The user running the Virtual Machine on SIPB's cluster is notified; his Virtual Machine had been compromised and scripts placed on it that were downloading journals from JSTOR, IEEE and APS.

The machines were taken offline.

Mon 01/03/11 | 10:49am (b)(6), (b)(7)(receives email forwarded via (b) from (b)(6), (b)(7)(at JSTOR regarding an incident on 12/26 at 9pm of (b)(6),(b)(7) excessively downloading JSTOR journals again; surprising, as under impression that authentication had been set up and proxy was being used. Discovers that hold-up has been JSTOR's difficulties with setting up landing page to make it easier for our users.

Tue 01/04/11 | 1:34am (b)(6), (b)(7)(pings (b)(6), (b)(7)(regarding incident; (b) (6),(b had starting to look into incident at that time. Can find zero information regarding this IP address, not even bogus guest registration data as found before. Started email reply to (b)(6), (b)(7)(then started examining older emails - all former abuses had come from 18.55. With recent network infrastructure access and tools given to Security team to enable self-sufficient discovery/protection of network and users, more investigation into the (b)(6),(b)(7) address and its possible physical location was pursued.

The user was now not using any of the typical methods to access MIT-net to avoid all usual methods of being disabled, including assigning himself an additional IP address (b)(6),(b)(7)(C)

so communication wouldn't be interrupted if we disabled (b)(6),(b)(7)(C) which had been doing the downloading.

Tue 01/04/11 | 2:49am (b)(6),(b) sends email to (b)(6),(b) and (b)(6),(b)(7) containing findings to see if they could further pinpoint location in building 16.

Tue 01/04/11 | 3:24am (b)(6),(b)(7) sends email to (b)(6),(b)(7) with update, concurs that move to econtrol/proxy system is prudent, and that further information should be known with (b)(6),(and (b)(6),(b)(7)(help.

Tue 01/04/11 | 3:42am (b)(6),(b)(7)(emails (b)(6),(b)(7)(and (b)(6),(with copy of email to (b)(6),(b)(7) and copy of email to (b)(6 and (b)(6),(

Tue 01/04/11 | 8:08am (b)(6),(b)(7)(emails (b)(6),(b with news that he's found the offending computer; an Acer netbook hidden under a box in the network closet in the basement of building 16. Under the netbook is an external hard drive.

(b)(6),(b)(7) arrives to assist (b)(6),(b)(7)(Traffic to/from the netbook is captured on (b)(6),(b)(7)(C laptop. The only traffic destined for the netbook is a single ping from Chinese address space.

9:44am (b)(6),(b)(7)(and (b)(6),(b talk via phone. (b)(6),(b calls (b)(6),(b)(7)(C) to advise and for counsel around legality of possibly having MIT police seize laptop.

(b)(6),(b)(7)(is notified by (b)(6),(b)(7)(C) and notifies MIT police.

10:30am (b)(6),(b)(7)(and (b)(6),(join (b)(6),(b)(7)(and (b)(6),(b in building 16, along with two MIT uniformed officers who are guarding scene. We are told that Det. (b)(6),(b)(7)(C) has notified Cambridge police who are en route.

~11:00am Det. (b)(6),(b)(7)(arrives with additional uniformed officers, Det. (b)(6),(b)(7)(C) Crime Scene Investigators and USSS Agent (b)(6),(b)(7)(C) and (b)(6),(detail events. (b)(6),(b)(7)(C) handles computer forensics for the Secret Service.

CSI folks fume for prints and photograph the scene. Prints are found and lifted from netbook.

Scene is released for further investigation.

(b)(6),(b)(7)(C) arrives with an IP-based video camera for surveillance after it's decided, at the recommendation of (b)(6),(b)(7)(C) that the netbook be left in place to continue to monitor traffic to/from it. At that time, it is observed that the netbook is still reaching out

to JSTOR and downloading journals.

It was also observed that connections were now being made to the computer from an IP address in China. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) arrive to assist.

~12:30pm (b)(6), and (b)(6),(b) stop by General Counsel's office to advise MIT's counsel of law enforcement's presence on campus and discuss what data is in-scope to provide them for the investigation that OI has stewardship over. (b)(6),(b)(7)(C) advises that turning over this evidence poses no violation of rights.

~1:30pm (b)(6),(b)(7)(C) and SA (b)(6), (b)(7)(C) continue to observe netbook; two open ports are discovered on netbook, both allowing for remote access. Strategy is determined for continual monitoring of traffic to/from the netbook. Camera is set up; (b)(6),(and (b)(6),(b restore scene to original condition as it had been discovered.

~2:30pm Paths diverge; (b)(6),(b and SA (b)(6), (b)(7) return to N42.

~3:00pm (b)(6), and (b)(6),(b speak with (b)(6),(b)(7)(C) to verify specific data to be turned over to Secret Service is within scope of investigation and poses no legal risks.

(b)(6), (b)(7) provides SA (b)(6), (b)(7)(with historical network flow data concerning 18.55.6.240 & 7.240 dating from 12/14 until present and relevant DHCP log information from prior occurrences of ghost-macbook and ghost-laptop JSTOR downloading incidents (from Sept. and Oct.).

~3:00pm Scene is restored to the way it was found and all involved clear out from building 16.

3:26pm Suspect is seen on camera entering network closet, noticeably unaware of what had occurred all morning. He's observed swapping out the external hard disk drive with a different one. He left before police could arrive. On his way out, the suspect shuts off the lights. As this will hurt video quality and possibly work against the motion activation of the camera, (b)(6),(returns to closet and turns lights back on.

~4:00pm SA (b)(6), (b)(7)(leaves campus; (b)(6),(b calls (b)(6),(b to inquire if he needs anything further. (b)(6), is waiting to hear of location to transmit captured network traffic to for further analysis.

Thu 01/06/11 | 12:32pm Suspect enters network closet while covering his face with bike helmet, presumably thinking video cameras
may be in hallway. Once inside and with the door closed, he hurriedly removes his netbook, hard drive,
and network cable and stows them in his backpack. While leaving, he covers his face again with the helmet
and is out within 2 minutes with not enough time for police to respond to the area quickly enough to
apprehend.

2:15pm (b)(6), (b)(7)(at home, calls (b)(6), seeing 2nd IP address that had been used by laptop, (b)(6),(b)(7)(C) in use on the 4th
floor of building 16. (b)(6),(verifies location of IP address. The MAC address was different, however the
suspect had been observed in the past changing his MAC address. It is plausible, given the circumstance,
that the laptop was moved up there when it had been removed from the basement.

2:22pm (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) drive to building 16 to attempt to recover the netbook.
(b)(6), calls (b)(6),(b)(7) on the way to inform him and for police presence while the attempt is made to locate
the netbook. (b)(6),(informs them that he and SA (b)(6), (b)(7) had just apprehended the suspect near Central Square
attempting to flee. Detective (b)(6), (b)(7)(C joins us with a uniformed officer.

~2:40pm (b)(6), (b)(7) is called and joins us quickly in 16 to aid in tracing the punched-down wires in the TR to the possible
location of the netbook. The netbook could not be located on the 4th floor; instead, a Dell laptop in an
office belonging to students is identified as having leased the (b)(6),(b)(7)(C) address, by happenstance, after
the suspect's netbook stopped using it.

~3:15pm The group returns to W92. The netbook had been using a statically assigned IP address, however, because
it moved, it was possible that it had been reconfigured to use DHCP services for network access. (b)(6), checks
today's DHCP logs for "ghost", part of the laptop's name that had been used over the past months.
ghost-laptop is seen in the logs, with the same MAC address that had been used on Tuesday. (b)(6), verifies
that the netbook is still active on the network. (b)(6),(finds the netbook seems to be on the network in
building W20 on the 5th floor. The log shows:

Jan 6 12:48:31 wall-street dhcpd: DHCPOFFER on 18.53.6.12 to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.53.0.1

Jan 6 13:27:01 installer dhcpd: DHCPOFFER on 18.187.7.213 to 00:4c:e5:a0:c7:56 (ghost-laptop) via 18.187.0.1

At 12:42 the netbook was re-registered on the network in building 4, 8 minutes after being picked up from building 16. 39 minutes later, at 1:26, it was plugged into a network jack in building W20.

3:20pm (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) arrive at W20. The network closet is examined and jack location determined. (b)(6),(b)(7)(C) and (b)(6),(b)(7)(determine the network drop location is in the SIPB office, room 557.

3:42pm (b)(6),(b)(7)(calls Det. (b)(6),(b)(7) to request police presence prior to the group entering the SIPB offices to check the room for the netbook.

4:00pm Det. (b)(6),(b)(7)(C and SA (b)(6),(b)(7) arrive outside W20 room 557. The students present are asked by Det. (b)(6), if they saw anyone drop off a silver laptop computer; they all respond they'd only been there ~15-20 minutes and had seen no computer. The room is searched by all - (b)(6),(locates the laptop, neatly placed under a table in a corner abutting a filing cabinet. The netbook is plugged in to a network jack about 6 feet away and is sitting on an external hard drive, attached, the same way it had been when in building 16.

SA (b)(6),(b)(7)(dons gloves and proceeds to examine the netbook. It appeared to be in a halfway shutdown state and all attempts to access a terminal on the machine were unsuccessful. It was determined that there was no feasible way to do live forensics on the computer in an attempt to capture a snapshot of current memory. The laptop is shutdown and bagged as evidence. SA (b)(6),(b)(7)(placed a call to the Cambridge police to inquire about getting another fingerprint exam for the netbook.

4:45pm The group returns to W92 and meets with (b)(6),(b)(7)(to debrief.

5:30pm (b)(6),(b)(7)(C) and (b)(6),(b)(7)(go to (b)(6),(b)(7)(C) office to join a conference call with (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) to brief them on the technical details of the work, the staff involved and sequence of events which enabled the group to locate the netbook. The call was concluded ~6:00.

A rough approximation of MIT's staff's time spent on incident since September: 160 hours in aggregate.

--

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 07, 2011 2:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Draft NOSA

Looks good. There are a few corrections and questions for you. I left it on your chair.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Friday, January 07, 2011 1:49 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Subject: Draft NOSA

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
INFO: INVESTIGATIVE SUPPORT DIVISION

FILE: J-102-775-60071-S
X-REF: N/A
SEIZURE#: N/A

SUBJECT: NOTIFICATION OF STATE ARREST
AARON H. SWARTZ - DATE OF ARREST : 01/06/11

ACTUAL LOSS: $TBD

POTENTIAL LOSS: $50,000.00

STATUTES VIOLATED: BRAKING AND ENTERNING C266 S18

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.426 - UNAUTHORIZED ACCESS UNIVERSITIES
SECONDARY TYPES: 848.191, 848,304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: N/A
REPORTING PERIOD: 01/04/11 - 01/10/11
STATUS: CONTINUED

SYNOPSIS:

Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force for breaking and entering

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) (MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building

16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department.

Also on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b)(7)(C) and Detective (b)(6),(b)(7)(C) of the Boston Police traveled to MIT and met with (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu) of the MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu) (b)(6),(b)(7)(C) Consultant for MIT IT Security Systems & Services and (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT. (b)(6),(b)(7)(C) stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. (b)(6),(b)(7)(C) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) went to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Also on 01/04/11, at approximately 1526, the surveillance camera was able to record a white male later identified as Aaron Swartz (DOB 11/08/86) enter the wire closet. Based on the surveillance video Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Also on 01/04/11, (b)(6),(b) provided SA (b)(6),(b) with a copy of flow traffic from the MIT network. SA (b)(6),(b)(7 contacted SA (b)(6),(b)(7)(C) (CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6), provided SA (b)(6),(b) with instructions to upload the data to the CERT drop box.

On 01/06/11, at approximately 1232, video surveillance viewed Swartz return to the wire closet and remove the netbook and external hard drive. At approximately 1411 (b)(6),(b)(7)(C) of the MIT police Department called (b)(6),(b)(7)(C) of the MIT Police and stated that he had located Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge Massachusetts. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) responded to Lee Street to assist (b)(6),(b)(7)(C) attempted to interview the Swartz however; Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)(C) and SA (b)(6),(b)(7) detained Swartz. Swartz was transported by Cambridge Police to Cambridge Police headquarters to be booked for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(7)(C) edu) and (b)(6),(b)(7)(C) contacted (b)(6),(b)(7)(C) to inform him that they found that the signature of the same Acer Aspire netbook had been discovered again coming from the Stratton Student Center. SA (b)(6),(b) met (b)(6),(b)(7 and (b)(6),(b)(at the student center and found the Acer Aspire netbook and external hard drive under a table, powered on and connected to the MIT LAN by a RJ-45 cable. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Also on 01/06/11, SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Headquarters SA (b)(6),(b)(met (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) .com). (b)(6),(b)(7)(C) informed SA (b)(6),(b)(7) that he represented Swartz and that his client would not make a statement.

JUDICIAL ACTION:

No significant judicial action during this reporting period.

SUSPECTS / DEFENDANTS:

(b)(6),(b)(7)(C) - DEFENDANT - SENTENCED (STATE)

1599:	YES
1599A:	YES

AARON H SWARTZ - DEFENDENT - ARRESTED (STATE)

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(7)(C)
FBI:	675304KD0
SID:	MA10556559
HT:	5'- 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Pending
1599A:	Pending
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	N/A
ADDRESS:	
EMAIL:	N/A
DATABASE CHECKS:	01/07/11

EXAMS CONDUCTED:

ECSAP: Pending
Poly: N/A
PSD: N/A

DATABASE SEARCHES CONDUCTED:

NCI / CI:	01/07/11
NCIC/NLETS:	01/07/11
CCS/CFT:	01/07/11
LOCAL LE:	01/07/11

Results of database searches have been reported under "Details of Investigation".

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation.

(b)(6),(b)(7)(C) / Ricciardi

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Friday, January 07, 2011 12:55 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet Capture

Hi,
I noticed I didn't have the correct name in the apache web server config. I fixed it and restarted it so you should be able to access it now.

Thanks

(b)(6),
(b)(7)(C

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, January 07, 2011 11:40 AM
To: (b)(6),(b)(7)(C)
Subject: RE: Packet Capture

I have not been able to access the packet capture. Is the site still up?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) mailto:(b) MIT.EDU]
Sent: Thursday, January 06, 2011 3:40 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet Capture

I am actually out of the office today. I could be there in an hour, if that would be OK.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 06, 2011 3:25 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Packet Capture

I am at MIT PD HQ now. I brought an external with me. I can drop by after I interview suspect if you will still be around

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 15:22:24 2011
Subject: RE: Packet Capture

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Friday, January 07, 2011 11:43 AM
To: (b)(6),(b)(7)(C) BOS)
Cc:
Subject: Re: http://www.nytimes.com/2009/02/13/us/13records.html

This is from a few years back -- in the first 30 seconds of this video:

http://blogs.law.harvard.edu/mediaberkman/2007/10/25/aaron-swartz-on-the-open-library-2/

Really intelligent kid that just got buried under an avalanche of dumb.

For the ultimate irony, check out that video again: just before the second picture-in-picture they cut to, 4 or so minutes in... "we want to be able to say, 'oh, just down the street there's a library that has a copy; go visit them'... this allows us to pull people into physical libraries. Our motto is, kind of on the side of every book, we have a little option where you can buy, borrow or down- steal.. err download, I guess."

No wonder he didn't talk at all -- seems like he might be quite familiar with how questioning works... that, and he hangs out with (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)
Consultant
IT Security Systems & Services, IS&T
MIT
(b)(6),(b)(7)(C)
PGP Fingerprint: (b)(6),(b)(7)(C)

Please excuse typos sent via my portable.

On Jan 7, 2011, at 7:48 AM, (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) @usss.dhs.gov> wrote:

FYI

(b)(6),(b)(7)(C)

U.S. Secret Service

Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto: (b)(6),(b)(7)(C) gmail.com]
Sent: Friday, January 07, 2011 7:34 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: http://www.nytimes.com/2009/02/13/us/13records.html

http://www.nytimes.com/2009/02/13/us/13records.html

Americans have grown accustomed to finding just about anything they want online fast, and free. But for those searching for federal court decisions, briefs and other legal papers, there is no Google.

Instead, there is Pacer, the government-run Public Access to Court Electronic Records system designed in the bygone days of screechy telephone modems. Cumbersome, arcane and not free, it is everything that Google is not.

Pacer is just so awful," said Carl Malamud, the leader of the effort and founder of a nonprofit group, Public.Resource.org. "The system is 15 to 20 years out of date."

Worse, Mr. Malamud said, Pacer takes information that he believes should be free — government-produced documents are not covered by copyright — and charges 8 cents a page. Most of the private services that make searching easier, like Westlaw and Lexis-Nexis, charge far more, while relative newcomers like AltLaw.org, Fastcase.com and Justia.com, offer some records cheaply or even free. But even the seemingly cheap cost of Pacer adds up, when court records can run to thousands of pages. Fees get plowed back to the courts to finance technology, but the system runs a budget surplus of some $150 million, according to recent court reports.

To Mr. Malamud, putting the nation's legal system behind a wall of cash and kludge separates the people from what he calls the "operating system for democracy." So, using $600,000 in contributions in 2008, he bought a 50-year archive of papers from the federal appellate courts and placed them online. By this year, he was ready to take on the larger database of district courts.

Those courts, with the help of the Government Printing Office, had opened a free trial of Pacer at 17 libraries around the country. Mr. Malamud urged fellow activists to go to those libraries, download as many court documents as they could, and send them to him for republication on the Web, where Google could get to them.

Aaron Swartz, a 22-year-old Stanford dropout and entrepreneur who read Mr. Malamud's appeal, managed to download an estimated 20 percent of the entire database: 19,856,160 pages of text.

Then on Sept. 29, all of the free servers stopped serving. The government, it turns out, was not pleased.

A notice went out from the Government Printing Office that the free Pacer pilot program was suspended, "pending an evaluation." A couple of weeks later, a Government Printing Office official, Richard G. Davis, told librarians that "the security of the Pacer service was compromised. The F.B.I. is conducting an investigation."

Recently, however, a small group of dedicated open-government activists teamed up to push the court records system into the 21st century — by simply grabbing enormous chunks of the database and giving the documents away, to the great annoyance of the government.

Lawyers for Mr. Malamud and Mr. Swartz told them that they appeared to have broken no laws, noting nonetheless that it was impossible to say what angry government officials might do.

At the administrative office of the courts, a spokeswoman, Karen Redmond, said she could not comment on the fate of the free trial of Pacer, or whether there had been a criminal investigation into the mass download.

The free program "is not terminated," Ms. Redmond said. "We'll just have to see what happens after the evaluation." As for the system's cost, she said: "We're about as cheap as we can get it. We're talking pennies a page."

Meanwhile, the 50 years of appellate decisions remain online and Google-friendly, and the 20 million pages of lower court decisions are available in bulk form, but are not yet easily searchable. "I want the whole database in 2009," Mr. Malamud said.

Mr. Malamud, 49, has a long record of trying to balance openness with privacy, and has also pushed the Securities and Exchange Commission and the Patent and Trademark Office to put their records online free. But the issue is a thorny one with court documents, which often contain personal information.

Daniel J. Solove, a professor at the George Washington University Law School, noted that marketers skim court records for personal data, and making records easier to troll will put even more data at risk. "It's taking away this middle ground that offered a lot of protection, practically, and throwing it into this radically wide open box," he said.

But this argument for what is known as "practical obscurity" does not convince Peter A. Winn, a privacy expert who is an assistant United States attorney in Washington State. Noting that he was speaking only for himself, he argued that the courts developed rules over the last 400 years to protect privacy.

"It worked in the bricks-and-mortar age — it should work in the electronic age," Mr. Winn said. The administrative office of the courts, he said, should take on the role of policing privacy on its databases. "This is going to take focus and a lot of hard work," he said.

Mr. Malamud agrees that the court system needs to do a better job of protecting privacy. He found thousands of documents in which the lawyers and courts had not properly redacted personal information like Social Security numbers, a violation of the courts' own rules. There was data on children in Washington, names of Secret Service agents, members of pension funds and more.

"They're pretty spectacular blunders," he said. He sent letters to the clerks of individual courts around the country. After some initial inaction, and repeated and increasingly spirited notices

from Mr. Malamud, most of the offending documents were pulled from the databases to be redacted.

Ms. Redmond, of the administrative office of the courts, said the courts comb through the documents "on a regular basis" and tell lawyers to redact confidential information. The number of violations, she noted, was relatively small.

Mr. Malamud scoffed at that. "This is a large number of transgressions, and this is illegal," he said. "The law doesn't say that you should only publish a small number of Social Security numbers!"

Mr. Malamud said his years of activism had led him to set a long-shot goal: serving in the Obama administration, perhaps even as head of the Government Printing Office. The thought might seem far-fetched — Mr. Malamud is, by admission, more of an at-the-barricades guy than a behind-the-desk guy. But he noted that he published more pages online last year than the printing office did.

Mr. Malamud represents a perspective of openness and transparency that is much in tune with the new administration's, said Lawrence Lessig, a law professor at Harvard who is a leading advocate for free culture. "The principles are those that Carl has been at the center of defining," he said.

The idea also seems to have a measure of appeal for John D. Podesta, a longtime fan of Mr. Malamud and head of the Obama transition team, who stopped short, however, of anything resembling an endorsement. "He would certainly shake things up," Mr. Podesta said, laughing.

Mr. Malamud says he is not counting on the new administration's being quite that bold. Besides, he said, he keeps himself awfully busy doing what he believes the government ought to be doing anyway.

"If called, I will certainly serve," he said. "But if not called, I will probably serve anyway."

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Friday, January 07, 2011 11:04 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Surveilance Video

I will ask is&t to get together

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) BOS)" <(b)(6),(b)(7)(C) usss.dhs.gov>
Date: Fri, Jan 7, 2011 10:28 am
Subject: Surveilance Video
To: (b)(6),(b)(7)(C) @mit.edu (b)(6),(b)(7)(C)
Cc: it.edu>, mit.edu>

Would it be possible for me to get a copy of the surveillance Video from the camera in the wire closet?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b) MIT.EDU]
Sent: Friday, January 07, 2011 1:18 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: 1st hard drive from suspect

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Just wanted to check in regarding potentially recovering the hard drive that was reported seen, on the video feed, being swapped out by the suspect on Tuesday; may/may not be moot at this point if he's already been bailed out, but I'd think that's where a lot of the JSTOR property might be sitting.

I'm super impressed with all the good work that went into this coming together. Hopefully it works like this most of the time for you all.

Best,
(b)(6),

(b)(6),(b)(7)(C)
Security Analyst
IT Security Systems & Services
MIT
(b)(6),(b)(7)(C)

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, January 07, 2011 9:11 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Swartz Case

(b)(5),(b)(6),(b)(7)(C)

per EOUSA

Steve

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Friday, January 07, 2011 7:57 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: http://www.nytimes.com/2009/02/13/us/13records.html

Please call (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Friday, January 07, 2011 7:41 AM
To: Heymann, Stephen (USAMA)
Subject: FW: http://www.nytimes.com/2009/02/13/us/13records.html

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) mailto (b)(6),(b)(7)(C) gmail.com]
Sent: Friday, January 07, 2011 7:34 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: http://www.nytimes.com/2009/02/13/us/13records.html

http://www.nytimes.com/2009/02/13/us/13records.html

FYI

http://www.nytimes.com/2009/02/13/us/13records.html

Pacer is just so awful," said Carl Malamud, the leader of the effort and founder of a nonprofit group, Public.Resource.org. "The system is 15 to 20 years out of date."

Worse, Mr. Malamud said, Pacer takes information that he believes should be free — government-produced documents are not covered by copyright — and charges 8 cents a page. Most of the private services that make searching easier, like Westlaw and Lexis-Nexis, charge far more, while relative newcomers like AltLaw.org, Fastcase.com and Justia.com, offer some records cheaply or even free. But even the seemingly cheap cost of Pacer adds up, when court records can run to thousands of pages. Fees get plowed back to the courts to finance technology, but the system runs a budget surplus of some $150 million, according to recent court reports.

To Mr. Malamud, putting the nation's legal system behind a wall of cash and kludge separates the people from what he calls the "operating system for democracy." So, using $600,000 in contributions in 2008, he bought a 50-year archive of papers from the federal appellate courts and placed them online. By this year, he was ready to take on the larger database of district courts.

Those courts, with the help of the Government Printing Office, had opened a free trial of Pacer at 17 libraries around the country. Mr. Malamud urged fellow activists to go to those libraries, download as many court documents as they could, and send them to him for republication on the Web, where Google could get to them.

Aaron Swartz, a 22-year-old Stanford dropout and entrepreneur who read Mr. Malamud's appeal, managed to download an estimated 20 percent of the entire database: 19,856,160 pages of text.

Then on Sept. 29, all of the free servers stopped serving. The government, it turns out, was not pleased.

A notice went out from the Government Printing Office that the free Pacer pilot program was suspended, "pending an evaluation." A couple of weeks later, a Government Printing Office official, Richard G. Davis, told librarians that "the security of the Pacer service was compromised. The F.B.I. is conducting an investigation."

Americans have grown accustomed to finding just about anything they want online fast, and free. But for those searching for federal court decisions, briefs and other legal papers, there is no Google.

Instead, there is Pacer, the government-run Public Access to Court Electronic Records system designed in the bygone days of screechy telephone modems. Cumbersome, arcane and not free, it is everything that Google is not.

Recently, however, a small group of dedicated open-government activists teamed up to push the court records system into the 21st century — by simply grabbing enormous chunks of the database and giving the documents away, to the great annoyance of the government.

Lawyers for Mr. Malamud and Mr. Swartz told them that they appeared to have broken no laws, noting nonetheless that it was impossible to say what angry government officials might do.

At the administrative office of the courts, a spokeswoman, Karen Redmond, said she could not comment on the fate of the free trial of Pacer, or whether there had been a criminal investigation into the mass download.

The free program "is not terminated," Ms. Redmond said. "We'll just have to see what happens after the evaluation." As for the system's cost, she said: "We're about as cheap as we can get it. We're talking pennies a page."

Meanwhile, the 50 years of appellate decisions remain online and Google-friendly, and the 20 million pages of lower court decisions are available in bulk form, but are not yet easily searchable. "I want the whole database in 2009," Mr. Malamud said.

Mr. Malamud, 49, has a long record of trying to balance openness with privacy, and has also pushed the Securities and Exchange Commission and the Patent and Trademark Office to put their records online free. But the issue is a thorny one with court documents, which often contain personal information.

Daniel J. Solove, a professor at the George Washington University Law School, noted that marketers skim court records for personal data, and making records easier to troll will put even more data at risk. "It's taking away this middle ground that offered a lot of protection, practically, and throwing it into this radically wide open box," he said.

But this argument for what is known as "practical obscurity" does not convince Peter A. Winn, a privacy expert who is an assistant United States attorney in Washington State. Noting that he was speaking only for himself, he argued that the courts developed rules over the last 400 years to protect privacy.

"It worked in the bricks-and-mortar age — it should work in the electronic age," Mr. Winn said. The administrative office of the courts, he said, should take on the role of policing privacy on its databases. "This is going to take focus and a lot of hard work," he said.

R I F

Mr. Malamud agrees that the court system needs to do a better job of protecting privacy. He found thousands of documents in which the lawyers and courts had not properly redacted personal information like Social Security numbers, a violation of the courts' own rules. There was data on children in Washington, names of Secret Service agents, members of pension funds and more.

"They're pretty spectacular blunders," he said. He sent letters to the clerks of individual courts around the country. After some initial inaction, and repeated and increasingly spirited notices from Mr. Malamud, most of the offending documents were pulled from the databases to be redacted.

Ms. Redmond, of the administrative office of the courts, said the courts comb through the documents "on a regular basis" and tell lawyers to redact confidential information. The number of violations, she noted, was relatively small.

Mr. Malamud scoffed at that. "This is a large number of transgressions, and this is illegal," he said. "The law doesn't say that you should only publish a small number of Social Security numbers!"

Mr. Malamud said his years of activism had led him to set a long-shot goal: serving in the Obama administration, perhaps even as head of the Government Printing Office. The thought might seem far-fetched — Mr. Malamud is, by admission, more of an at-the-barricades guy than a behind-the-desk guy. But he noted that he published more pages online last year than the printing office did.

Mr. Malamud represents a perspective of openness and transparency that is much in tune with the new administration's, said Lawrence Lessig, a law professor at Harvard who is a leading advocate for free culture. "The principles are those that Carl has been at the center of defining," he said.

The idea also seems to have a measure of appeal for John D. Podesta, a longtime fan of Mr. Malamud and head of the Obama transition team, who stopped short, however, of anything resembling an endorsement. "He would certainly shake things up," Mr. Podesta said, laughing.

Mr. Malamud says he is not counting on the new administration's being quite that bold. Besides, he said, he keeps himself awfully busy doing what he believes the government ought to be doing anyway.

"If called, I will certainly serve," he said. "But if not called, I will probably serve anyway."

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Friday, January 07, 2011 7:40 AM
To: undisclosed-recipients
Subject: Booking Sheet Attached
Attachments: AaronSwartz.pdf

I have attached the booking sheet of Aaron Swartz.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Friday, January 07, 2011 1:18 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (BOS)
Subject: 1st hard drive from suspect

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Just wanted to check in regarding potentially recovering the hard drive that was reported seen, on the video feed, being swapped out by the suspect on Tuesday; may/may not be moot at this point if he's already been bailed out, but I'd think that's where a lot of the JSTOR property might be sitting.

I'm super impressed with all the good work that went into this coming together. Hopefully it works like this most of the time for you all.

Best,
(b)(6),(b)(

(b)(6),(b)(7)(C) Security Analyst IT Security Systems & Services MIT

PGP Fingerprint: (b)(6),(b)(7)(C)

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.8 (Darwin)

IEYEARECAAYFAk0msCUACgkQxnTkuJ5I0ObIkwCffqwPgywH+1I7ImX1zlytenIn
4kgAoKozedr559kAnhbUUimt9abGI6y5
=6JST
-----END PGP SIGNATURE-----

From: (b)(6),(b)(7)(C) gmail.com>
Sent: Thursday, January 06, 2011 10:59 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Swartz and Pacer

Home > Aaron Swartz >

Subject of FBI Investigation Reveals Government Concerns About Access to Federal Courts' Public PACER System

Posted on October 6, 2009 by Aaron Wright

Reddit co-founder Aaron Swartz was apparently the subject of an FBI investigation for "participating in a project to take the publicly owned US court records from the PACER database (where they were very expensive to access) and put them on the web."

Mr. Swartz has made this information public by releasing the contents of his FBI file, obtained through a Freedom of Information Act request. His file reveals that the FBI was treating his access of PACER as a crime which cost the victim, the Administrative Office of the US Courts, approximately $1.5 million. The file suggests, but does not explicitly sate, that the crime may have been a violation of the Computer Fraud and Abuse Act (18 U.S.C. §1030), as the FBI apparently asked the Administrative Office of the US Courts how Mr. Swartz would have know his access was unauthorized.

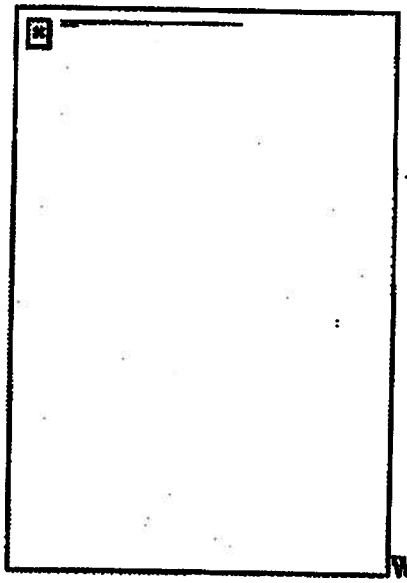
The FBI closed its investigation of Mr. Swartz without filing charges. The investigation of Swartz's activity, coupled with questions about what constitutes accessing a computer "without authorization" under anti-hacking statutes (as I previously discussed here), suggests that future efforts to open the PACER system (as well as existing efforts, like RECAP) may meet with some government resistance.

For more on efforts to make the PACER system more accessible to the public se our previous posts on the subject.

From: (b)(6),(b)(7)(C) gmail.com>
Sent: Thursday, January 06, 2011 10:45 PM
To: (b)(6),(b)(7)(C) POS)
Subject: FBI Investigated Coder for Liberating Paywalled Court Records

FBI Investigated Coder for Liberating Paywalled Court Records

- By Ryan Singel
- October 5, 2009 |
- 8:48 pm |
- Categories: Sunshine and Secrecy, The Ridiculous



When 22-year-old programmer Aaron Swartz decided last fall to help an open-government activist amass a public and free copy of millions of federal court records, he did not expect he'd end up with an FBI agent trying to stake out his house.

But that's what happened, as Swartz found out this week when he got his FBI file through a Freedom of Information Act request. A partially-redacted FBI report shows the feds mounted a serious investigation of Swartz for helping put public documents onto the public web.

The FBI ran Swartz through a full range of government databases starting in February, and drove by his home, after the U.S. court system told the feds he'd pilfered approximately 18 million pages of documents worth $1.5 million dollars. That's how much the public records would have cost through the federal judiciary's pay-walled PACER record system, which charges eight cents a page for most legal filings.

"I think its pretty silly they go after people who use the library to try to get access to public court documents," Swartz said. "It is pretty silly that instead of calling me up, they sent an FBI agent to my house."

The feds also checked Swartz's Facebook page, ran his name against the Department of Labor to figure out his work history, looked for outstanding warrants and prior convictions, checked to see if his mobile phone number had ever come up in a federal wiretap or pen register, and checked him against the records in a private data broker's database.

399diggsdigg

The Great Court Records Caper began last year when the judiciary and the Government Printing Office experimented with giving away free access to PACER at 17 select libraries around the country. Swartz decided to use the trial to grab as many of the public court records as he could and, perversely, release them to the public.

He visited one of the libraries — the 7th U.S. Circuit Court of Appeals library in Chicago — and installed a small PERL script he'd written. The code cycled sequentially through case numbers, requesting a new document from PACER every three seconds. In this manner, Swartz got nearly 20 million pages of court documents, which his script uploaded to Amazon's EC2 cloud computing service.

Or, as the FBI report put it, the public records were "exfiltrated."

The script ran for a couple of weeks — from September 4 to 22, until the court system's IT department realized something was wrong. Someone was downloading *everything*. None of the records, of course, were private or sealed, and Lexis Nexis has a copy of of PACER's database that it sells a high markup. But Swartz wasn't paying anything.

The Government Printing Office abruptly shut down the free trial and reported to the FBI that PACER was "compromised," the FBI file reveals. The Administrative Office of the U.S. Courts told the FBI in March that Swartz had gained unauthorized access to the free PACER account.

"AARON SWARTZ would have known his access was unauthorized because it was with a password that did not belonged [sic] to him," reads the FBI report summarizing the judiciary's position.

Swartz says his script only ran on the library computer. It didn't use a password at all, but used the PACER authentication cookie set in the PC's browser.

He donated the 19,856,160 pages to public.resource.org, an open government initiative spearheaded by Carl Malamud as part of a broader project to make public as many government databases as Malamud can find. It was Malamud who previously shamed the SEC into putting all its EDGAR filings online in the '90s, and he used $600,000 in donations to buy 50 years of documents from the nation's appeals court, which he promptly put on the internet for anyone to download in bulk.

The Washington bureau of the FBI opened their investigation of Swartz just a week or so before the *New York Times* published its account of the caper. The bureau didn't contact him then, but in April, the FBI asked to interview the code jock — saying it needed his help to close the "security hole" he'd exploited. When Swartz declined, on the advice of counsel, the feds dropped the investigation after the Justice Department's Computer Crime and Intellectual Property Section closed the case.

Swartz, a former employee of Reddit — a sister company of Wired.com — requested his FBI file in August, and describes it as the "usual mess of confusions that shows the FBI's lack of sense of humor." (Threat Level notes that the FBI's filled Swartz's FOIA request at an admirable speed that would have been unheard of as recently as last year.)

RIF

That's how Swartz learned that a Chicago-based FBI agent got Swartz's driver's license photo, and considered a stakeout of his home. But any surveillance, the agent concluded, would be conspicuous, since so few cars were parked on Swartz's dead-end street in Highland Park, Illinois.

The feds evidently identified Swartz in the first place by approaching Amazon, which provided his name, phone number and address. It's not clear if the feds got a subpoena to learn his identity, but they may not have needed one; Amazon's user agreement for its cloud computing solutions gives it the right to turn over customer information to the government on request.

Amazon did not reply to a call and online request for comment.

Two months after opening an investigation, the feds finally called Swartz on April 14. He declined to speak to them, and demurred again through his lawyer two days later.

The investigation was closed on April 20.

PACER records still cost eight cents a page, but now PACER users running the Firefox browser can donate their downloads to the public domain with a simple plug-in called RECAP.

Use of the plug-in is not likely to start an investigation of you.

But then again, who knows.

RIF
2464

From: (b)(6),(b)(7)(C) gmail.com>
Sent: Thursday, January 06, 2011 10:25 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Aaron Swartz

Aaron Swartz, co-founder of Reddit, was investigated by the FBI for participating in a project to take the publicly owned US court records from the PACER database (where they were very expensive to access) and put them on the web. He's requested his FBI file and put it on the web:
AARON SWARTZ has a profile on the website LINKEDIN, at www.linkedin.com/in/aaronsw. SWARTZ is listed as a writer, hacker and activist based in the San Francisco Bay Area. SWARTZ's education includes Stanford University, Sociology, 2004. SWARTZ's experience includes the following:

SWARTZ has a profile on the website FACEBOOK. His networks include Stanford '08 and Boston, MA. The picture used in his profile was also used in an article about SWARTZ in THE NEW YORK TIMES.

SWARTZ's personal webpage, www.aaronsw.com, includes a section titled "Aaron Swartz: a life time of dubious accomplishments". In 2007, SWARTZ began working full-time as a member of the Long-Term Planning Committee for the Human Race (LTPCHR).

February 19, Manassas, VA:

On February 17, 2008 [sic], SA [REDACTED] received an email from [REACTED] Administrative Office of the US Courts, with links to two published articles regarding the compromise of the PACER system.

On February 12, 2009, [REACTED] published an article in THE NEW YORK TIMES titled "An Effort to Upgrade a Court Archive to Free and Easy". For the article, [REDACTED] interviewed [REDACTED] and AARON SWARTZ regarding the compromise of the PACER system.

From: (b)(6),(b)(7)(C) gmail.com>
Sent: Thursday, January 06, 2011 8:58 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: http://openlibrary.org/about/people

http://openlibrary.org/about/people

Aaron Swartz *Former Project Leader*
The Open Library wouldn't exist without Aaron. He wrote the backbone of the system you see today. He has also worked on specs like RSS, startups like Reddit.com, and software projects like web.py. He worked from San Francisco to architect the site, put together the team, and attempt to keep things organized, and we couldn't have come this far without his crucial expertise.

Aaron Swartz: a lifetime of dubious accomplishments

home page • life story • contact info

the early years

Aaron Swartz was born in Chicago, Illinois before his parents quickly whisked him away to the northern suburb of Highland Park, where he was kept safe from the infectious effects of the lower classes for over a decade.

He was enrolled for a short time at the Creative Children's Academy but then was moved the North Shore Country Day School of Winnetka. After providing the correct answers on a standardized test he was offered a scholarship to the same school for high school, which he reluctantly accepted but only for a year.

After a year of high school he found it intolerable and refused to go back. His family told the state of Illinois that they were "homeschooling" him and he enrolled in a handful of classes at nearby Lake Forest College (Physics, Chemistry, Logic, and Number Theory) but spent most of his time on his own.

the middle years

After taking a course from Philip Greenspun, he built his first database-backed web site (based around the same idea as what is now called Wikipedia) and entered it in the ArsDigita Prize, where he received runner-up status. As part of his second project, an early web-based news aggregator, he joined the RSS-DEV working group where he co-authored the RSS 1.0 spec.

RSS 1.0 was based around a technology known as RDF, which was being developed as part of the Semantic Web project at the W3C, the standards body for the Web. Aaron learned more and more about RDF, eventually becoming a member of the RDF 1.0 Working Group, where he wrote RFC3870.

In 2002 he read an article about the Creative Commons project then being started by Lawrence Lessig. He wrote Lessig an email saying that he thought RDF would be appropriate for the project and Lessig invited him to become the project's RDF lead.

In subsequent years he became increasingly interested in the law, the major part of Creative Common's work, and then in politics. The summer before college he became especially engaged in radical politics.

the recent years

On the recommendation of Lessig, who is a professor of law there, he was accepted to Stanford University, where he planned to study sociology. He documented his first year at Stanford extensively on his blog.

Towards the end of the year, he received an email from Paul Graham who suggested he apply for his Summer Founders Program. With Simon Carstensen, he did, and was accepted, and moved to Cambridge for the summer, where they stayed in beautiful Simmons Hall.

Simon left at the end of the summer to return to school in Denmark but Aaron decided to stay in Cambridge and take a leave of absence from Stanford after receiving several funding offers. However, he spent months trying to find a new partner and close down a funding deal, eventually giving up and merging with Steve Huffman and Alexis Ohanian of Reddit to form Not a Bug.

right now

He was a co-founder of Reddit, whose traffic doubled six times from when he joined in October 2005 to when it was purchased by Condé Nast in October 2006.

He left in early 2007 and since then has co-founded Open Library, Watchdog.net, and the Progressive Change Campaign Committee.

He is currently executive director of Demand Progress.

Aaron Swartz (born November 8, 1986) is a writer, activist, and programmer. He is currently co-founder of the Progressive Change Campaign Committee.

At age 14, he was a co-author of the RSS 1.0 specification. Since then he has become a member of the W3C's RDF Core Working Group, co-designed the formatting language Markdown with John Gruber, and has been involved in many other projects.

Swartz was the founder of Infogami, a startup that was part of Y Combinator's first Summer Founders Program. Previously, he attended Stanford University for a year, leaving to work on his company full-time. Infogami merged with reddit to form *not a bug* but failed to take off.

In late 2006, reddit was sold to CondéNet (the online arm of Condé Nast Publications and the owners of *Wired*) and Swartz moved with his company to San Francisco. In January 2007, Swartz was asked to resign from his position at Wired Digital.[1]

In September 2007, Swartz, together with Simon Carstensen, launched Jottit, a website service quite similar to Infogami. Jottit was launched from bitbots.net, a project by Swartz and Carstensen. Swartz is also the creator of

RIF 2467

the web.py web application framework, based on the Python programming language, which is used by Jottit (and previously reddit).

Swartz is an active blogger and has written a number of widely read essays on his blog. Two of his more well-known pieces are "Who Writes Wikipedia",[2] an article examining the contributions to Wikipedia articles written during his candidacy for the Wikimedia Foundation board election in 2006, and "HOWTO: Be More Productive",[3] an article on personal productivity.

Swartz currently lives in Cambridge, Mass. He works on watchdog.net and is on the board of Change Congress, and previously worked on Open Library.

RIF 2468

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 7:01 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: SWARTZ

(b)(6),(b)(7)(C)

Looks like he is a big hacker, i googled him

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) BOS)" (b)(6),(b)(7)(C) ss.dhs.gov>
Date: Thu, Jan 6, 2011 3:55 pm
Subject: SWARTZ
To: (b)(6),(b)(7)(C) mit.edu>

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) ISD)
To: (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 15:52:54 2011
Subject: SWARTZ

(b)(6),(b)(7)(- I printed out and passed along the attached report to (b)(6),(b)(7) (via (b)(6),(b)(7) to glean the appropriate info for you. I'm also attaching his expired IL DL printout. In checking for DL or vehicles for his possible (b)(6),(b)(7)(C) there was nothing in the registry.
Let me know if you need anything else.
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, January 06, 2011 5:24 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Update

(b)(6), (b)(7) good work!

---- Original Message ----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b)(7)(C) BOS)
Sent: Thu Jan 06 17:11:27 2011
Subject: Re: Update

He never made any statement but Attorney told me he is a current Cambridge resident.

(b)(6),(b)(7)(C)

Sent from Blackberry

---- Original Message ----
From: (b)(6),(b)(7)(C BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 17:07:13 2011
Subject: Re: Update

(b)(6), (b)(7) Did he ever give an address?

---- Original Message ----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b)(7)(C BOS)
Sent: Thu Jan 06 17:05:03 2011
Subject: Re: Update

His attorney arrived and did not give permission for an interview.

(b)(6),(b)(7)(C)

Sent from Blackberry

---- Original Message ----
From: (b)(6),(b)(7) BOS)
To: (b)(6),(b)(7)(C) BOS)
Sent: Thu Jan 06 16:43:45 2011
Subject: Re: Update

(b)(6),(b)(7)(C) good luck. Let me know if you are successful

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:42:03 2011
Subject: Re: Update

In a computer room off of the student center.
Going to ask for interview now

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7) BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:39:29 2011
Subject: Re: Update

Where was it?
Have you had a chance to interview?
Phone?

----- Original Message -----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b)(7)(C) BOS)
Sent: Thu Jan 06 16:34:14 2011
Subject: Update

Laptop and external drive found. Being processed by MIT now. Will be dusted for prints by Cambridge tomorrow. I will examine it as soon as I have a warrant

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 06, 2011 5:13 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) USAMA)
Subject: RE: FYI Swartz council

As I understand it, we still have no role in this matter. But, thank you for the information.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thursday, January 06, 2011 5:10 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) USAMA)
Subject: FYI Swartz council

FYI
In reference to the Aaron Swartz arrested by MIT for B and E. Swartz is now represented by (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, January 06, 2011 5:07 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Update

(b)(6), (b)(7)(C) Did he ever give an address?

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 17:05:03 2011
Subject: Re: Update

His attorney arrived and did not give permission for an interview.

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:43:45 2011
Subject: Re: Update

(b)(6), (b)(7)(good luck. Let me know if you are successful

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:42:03 2011
Subject: Re: Update

In a computer room off of the student center.
Going to ask for interview now

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:39:29 2011

Subject: Re: Update

Where was it?
Have you had a chance to interview?
Phone?

---- Original Message ----
From: (b)(6),(b)(7)(C) BOS)
To: (b)(6),(b)(7)(C) BOS)
Sent: Thu Jan 06 16:34:14 2011
Subject: Update

Laptop and external drive found. Being processed by MIT now. Will be dusted for prints by Cambridge tomorrow. I will examine it as soon as I have a warrant

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, January 06, 2011 4:44 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Update

(b)(6), (b)(7)(C) good luck. Let me know if you are successful

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (BOS)
Sent: Thu Jan 06 16:42:03 2011
Subject: Re: Update

In a computer room off of the student center.
Going to ask for interview now

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:39:29 2011
Subject: Re: Update

Where was it?
Have you had a chance to interview?
Phone?

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 16:34:14 2011
Subject: Update

Laptop and external drive found. Being processed by MIT now. Will be dusted for prints by Cambridge tomorrow. I will examine it as soon as I have a warrant

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, January 06, 2011 4:39 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Update

Where was it?
Have you had a chance to interview?
Phone?

---- Original Message ----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (BOS)
Sent: Thu Jan 06 16:34:14 2011
Subject: Update

Laptop and external drive found. Being processed by MIT now. Will be dusted for prints by Cambridge tomorrow. I will examine it as soon as I have a warrant

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 4:13 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: 1-6-11 at 1232

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

(b)(6),(b)(7) skyfire /var/log/dhcplogger $ grep ghost dhcp
Jan 6 12:42:49 installer dhcpd: DHCPOFFER on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C) Jan 6 12:42:49 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7) Jan 6 12:42:49 installer dhcpd: DHCPACK on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) Jan 6 12:44:32 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7) from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:44:32 installer dhcpd: DHCPACK on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:45:22 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7 from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:45:22 installer dhcpd: DHCPACK on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:46:22 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:46:22 installer dhcpd: DHCPACK on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via eth0 Jan 6 12:48:31 wall-street dhcpd: DHCPOFFER on (b)(6),(b) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) Jan 6 12:48:31 wall-street dhcpd: DHCPREQUEST for (b)(6),(b)(7) (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) Jan 6 12:48:31 wall-street dhcpd: DHCPACK on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) Jan 6 12:48:31 installer dhcpd: DHCPOFFER on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(1 Jan 6 12:48:32 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(1 Jan 6 12:50:56 wall-street dhcpd: DHCPREQUEST for (b)(6),(b)(7 from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6), 1 Jan 6 12:50:56 wall-street dhcpd: DHCPACK on (b)(6),(b) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(1 Jan 6 13:27:01 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) 1 Jan 6 13:27:01 installer dhcpd: DHCPREQUEST for (b)(6),(b)(7) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b 1 Jan 6 13:27:01 installer dhcpd: DHCPACK on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b) 1 Jan 6 13:27:02 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b 1 Jan 6 13:27:02 wall-street dhcpd: DHCPOFFER on (b)(6),(b)(7) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)

On Jan 6, 2011, at 1:47 PM, (b)(6),(b)(7)(C) (BOS) wrote:

>
> (b)(6),(b)(7)(C)
>
>
> Sent from Blackberry
>
> From: (b)(6),(b)(7)(C) gmail.com>
> To (b)(6),(b)(7)(C) (BOS)
> Sent: Thu Jan 06 13:39:27 2011
> Subject: 1-6-11 at 1232
>
>
>

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 06, 2011 3:49 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: FYI an update

(b)(5) per EOUSA

From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 06, 2011 3:38 PM
To: Heymann, Stephen (USAMA); (b)(6),(b)(7)(C) (USAMA)
Subject: FYI an update

FYI.
At approximately 1232 today the suspect was seen on video surveillance returning to the wire closet and taking the laptop and external drive. The suspect fled the scene before authorities could detain him. However at 1411 the suspect was identified. On Massachusetts Avenue in Cambridge. Detectives and this agent found the suspect and detained him. The suspect was arrested by MIT Police for breaking and entering. A passport in his backpack identifies the suspect as Aaron H Swartz, with a DOB of 8 NOV 86. The booking is ongoing. Swartz has made no statements yet. I am still working to find the right person to make the call for MIT if they want Federal involvement beyond my assistance.

(b)(6),(b)(7)(C)

Sent from Blackberry

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
To: (b)(6),(b)(7)(C) BOS)
Sent: Thu Jan 06 09:48:44 2011
Subject: Please call. Steve (b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: prvs=198013c80b(b)(6),(b)(7)(C) @ci.boston.ma.us on behalf of (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) @ci.boston.ma.us>
Sent: Thursday, January 06, 2011 3:47 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Aaron Swartz

Can you get the video footage of the apprehension? I want to put it into Camtasia and put it to theme music.

Thank you,

(b)(6),(b)(7)(C)
Detective
Boston Police, Forensic Group
New England Electronic Crimes Task Force
10 Causeway St, Suite (b)(6),
Boston Ma, 02222
(b)(6),(b)(7)(C) Office)
Cell)
617-565-5659 (Fax)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Thu 1/6/2011 2:46 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Cc: (b)(6),(b)(comcast.net
Subject: Aaron Swartz

An Aaron Swartz has been taken into custody and will initial be charged with B and E. Swartz matches the description of the suspect in video surveillance

(b)(6),(b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

The substance of this message, including any attachments, may be confidential, legally privileged and/or exempt from disclosure pursuant to Massachusetts law. It is intended solely for the addressee. If you received this in error, please contact the sender and delete the material from any computer.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 3:40 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Packet Capture

I am actually out of the office today. I could be there in an hour, if that would be OK.

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 06, 2011 3:25 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Packet Capture

I am at MIT PD HQ now. I brought an external with me. I can drop by after I interview suspect if you will still be around

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C) (BOS)
Sent: Thu Jan 06 15:22:24 2011
Subject: RE: Packet Capture

Hi there,
I've setup a web server on the machine containing the files so you can download them. They are in a standard tcpdump format. The URL is

(b)(3):Rule 6E

We've got plenty of bandwidth over here, however, if downloading this much data is a problem for you I could put them on a SATA drive and bring them down to your office. Let me know.

Thanks
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) [mailto:(b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Thursday, January 06, 2011 2:09 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Packet Capture

How could I get a copy of the network traffic?

(b)(6),(b)(7)(C)

Sent from Blackberry

(b)(6),(b)(7)(C)

(b)(6), (b)(7) (C) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Thursday, January 06, 2011 2:26 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Call me

When you get a second regarding MIT

From: (b)(6),(b)(7)(C) CambridgePolice.Org>
Sent: Thursday, January 06, 2011 1:33 PM
To: External (b)(6),(b) cambridgepolice.org (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7) mit.edu (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) comcast.net'; (b)(6),(b)(7)(C) (BOS)
Subject: RE: MIT - Bld 16

FYI:
Agent (b)(6), and I spoke today. He was notified by (b)(6),(b)(7)(C) that the perpetrator was caught on tape again and removed the laptop so our services were not needed at this time.

Respectfully,
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C)
Sent: Thursday, January 06, 2011 11:13 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b) mit.edu'; (b)(6),(b)(7)(C) usss.dhs.gov'; (b)(6),(b)(7)(C) comcast.net'; (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Fw: MIT - Bld 16

(b)(6),(b)(7)(C)

The thread below has the status of the investigation to date.

As I am on a day off today I would request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external hard drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, the operation is being shut down and we will continue the investigation just not with the computer hooked up and downloading data.

(b)(6),(b)(7)(C) cell phone number is (b)(6),(b)(7)(C)

(b)(6), and (b)(6), can you call (b)(6),(b)(7)(C) and hook up with her and (b)(6),(b)(7)(C

Respectfully Submitted,
(b)(6),(b)

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C) MIT.EDU>; (b)(6),(b)(7)(C) mit.edu>; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) mit.edu>; (b)(6),(b)(7)(C) mit.edu>; (b)(6),(b)(7)(C) mit.edu>; (b)(6),(b)(7)(C); (b)(6),(b) (BOS); (b)(6),(b)(7)(C) usss.dhs.gov>
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bld 16

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF
2489

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 12:55 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: MIT - Bld 16

It is gone, he just left-my guys are looking for him

Sent from my HTC on the Now Network from Sprint!

---- Reply message ----
From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 6, 2011 12:46 pm
Subject: MIT - Bld 16
To: (b)(6),(b)(7)(C) mit.edu>

I just spoke with Cambridge Crime Scene (b)(6),(b)(7)(C) cal (b)(6),(b)(7)(C) ffice) and they are ready to grab the laptop and hard drive and process it for prints again as soon as someone lets them into the wire closet.

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, January 06, 2011 11:23 AM
To: Externa (b)(6),(b) cambridgepolice.org
Cc: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) BOS)
Subject: RE: MIT - Bld 16

I will talk with (b)(6),(b)(7)(and make sure my approach is a sound practice; if so I will cal (b)(6),(b)(7) nd meet him over there.

I really appreciate all the help.

(b)(6),(b)(7)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Thursday, January 06, 2011 11:20 AM
To: (b)(6),(b)(7)(C)
Cc: Ames, Paul; (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT - Bld 16

(b)(6),(b)(7)(hat is certainly your call and sounds good. (b)(6),(will be responding either way.

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(
Sent: Thu Jan 06 11:17:02 2011
Subject: RE: MIT - Bld 16

(b)(6), – We can bag, tag and deliver if that works. I am thinking that if we are leaving the camera up, we should be in and out rather quickly incase the suspect ventures by. I would imagine (b)(6), could process it in her lab.

(b)(6), (b)(7)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Thursday, January 06, 2011 11:13 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) @usss.dhs.gov'; (b)(6),(b)(7)(C) @comcast.net'; (b)(6),(b)(7)(C) @usss.dhs.gov'
Subject: Fw: MIT - Bid 16

(b)(6),(b)(7)(C)

The thread below has the status of the investigation to date.

As I am on a day off today I would request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external hard drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, the operation is being shut down and we will continue the investigation just not with the computer hooked up and downloading data.

(b)(6),(b)(7)(C) cell phone number is (b)(6),(b)(7)(C)

(b)(6), (b)(7)(C) and (b)(6), can you call (b)(6),(b)(7)(C) and hook up with her and (b)(6), (b)(7)(C)

Respectfully Submitted;

(b)(6), (b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) @usss.dhs.gov>
To: (b)(6),(b)(7)(C) @MIT.EDU>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) @mit.edu>
Cc: (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) @usss.dhs.gov>
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bid 16

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External: (b)(6),(b)(7)(C) @cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bid 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).<

R I F

From: (b)(6),(b)(7)(C) @MIT.EDU>
Sent: Thursday, January 06, 2011 11:23 AM
To: External (b)(6),(b)(cambridgepolice.org
Cc: Ames, Paul (b)(6),(b)(7)(C) (BOS)
Subject: RE: MIT - Bid 16

I will talk with (b)(6), (b)(7) and make sure my approach is a sound practice; if so I will call (b)(6), and meet him over there.

I really appreciate all the help.

(b)(6), (b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Thursday, January 06, 2011 11:20 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Re: MIT - Bid 16

(b)(6),(that is certainly your call and sounds good. (b)(6),(will be responding either way.

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Sent: Thu Jan 06 11:17:02 2011
Subject: RE: MIT - Bid 16

(b)(6),(b - We can bag, tag and deliver if that works. I am thinking that if we are leaving the camera up, we should be in and out rather quickly incase the suspect ventures by. I would imagine (b)(6), could process it in her lab.

(b)

From: (b)(6),(b)(7)(C) [mailto (b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Thursday, January 06, 2011 11:13 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) usss.dhs.gov' (b)(6),(b)(7)(C) comcast.net';
(b)(6),(b)(7)(C) usss.dhs.gov'
Subject: Fw: MIT - Bid 16

(b)(6),(b)(7)(C)

The thread below has the status of the investigation to date.

As I am on a day off today I would request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external hard drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, the operation is being shut down and we will continue the investigation just not with the computer hooked up and downloading data.

(b)(6),(b)(7)(C) cell phone number is (b)(6),(b)(7)(C)

(b)(6), (b)(7) and (b) (6), can you call (b)(6),(b)(7)(C) and hook up with her and (b)(6), (b)(7)(C)

Respectfully Submitted,

(b)(6),

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
To: (b)(6),(b)(7)(C) MIT.EDU> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) usss.dhs.gov>
Cc: (b)(6),(b)(7)(C)
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bid 16

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) mailto: (b)(6), (b)(7) @MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambiddenpolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bid 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(6), (b)(7)(C

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

Thank you

(b)(6),(b)(7)(C)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS): External; (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bid 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(6),
(b)(7)

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) uess.dhs.gov; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

Thank you

(b)(6),(b)(7)(C)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(C)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in

response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Thursday, January 06, 2011 11:13 AM
To: (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) mit.edu (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) @comcast.net (b)(6),(b)(7)(C) (BOS)
Subject: Fw: MIT - Bld 16

(b)(6),(b)(7)(C)

The thread below has the status of the investigation to date.

As I am on a day off today I would request that CPD Crime Scene personnel hook up with SA (b)(6),(b)(7)(C) and process the newest external hard drive for prints that the suspect left the other day after we cleared the scene.

As you'll notice from the thread, the operation is being shut down and we will continue the investigation just not with the computer hooked up and downloading data.

(b)(6),(b)(7)(C) cell phone number is (b)(6),(b)(7)(C)

(b)(6), (b)(7)(and (b) (6) can you call (b)(6),(b)(7)(C) at (b)(6),(b)(7)(C) and hook up with her and (b)(6),(b)(7)(C)

Respectfully Submitted,
(b)(6), (b)(7)(

From: (b)(6),(b)(7)(C) (BOS) - (b)(6),(b)(7)(C) @usss.dhs.gov>
To: (b)(6),(b)(7)(C) @MIT.EDU>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C) @mit.edu>; (b)(6),(b)(7)(C)
(b)(6),(b)(7) BOS); (b)(6),(b)(7)(C) @usss.dhs.gov>
Sent: Thu Jan 06 10:00:07 2011
Subject: RE: MIT - Bld 16

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) @MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) BOS); External-(b)(6),(b)(7)(C) @cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bld 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) usss.dhs.gov; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

Thank you

(b)(6),(b)(7)(C)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)(7)(
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6),(b) mit.edu

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 10:22 AM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: MIT - Bld 16

(b)(6),(b)(7)(C)

I have a possible, i am looking for him to try to make an id. Can you see if the name (b)(6),(b)(7)(C) shows up on any download sites?

I am not sure we will be able to get an additional camera up, my guy is on vaca for the rest of the week.

(b)(6),(b)

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) (BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>
Date: Thu, Jan 6, 2011 10:01 am
Subject: MIT - Bld 16
To: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu>, (b)(6),(b)(7)(@cambridgepolice.org> (b)(6),(b)(7) @cambridgepolice.org>
Cc: (b)(6),(b)(7)(C) mit.edu> (b)(6),(b)(7)(C) mit.edu>, (b)(6),(b)(7)(C) (b)(6),(b)(7)(mit.edu> (b)(6),(b)(7)(C) BOS)" (b)(6),(b)(7)(C) usss.dhs.gov>

I agree with taking the laptop offline today and imaging it. Any leads with identification? I wanted to look at what options we have to get a better picture of his face. I mentioned the case to our Technical Security Division Specialist. He is working on another case this morning but will be available this afternoon. Do you have any other surveillance options to capture a better image of his face?

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:jperault@MIT.EDU]
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); Externa (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bld 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

From: Heymann, Stephen (USAMA) (b)(6),(b)(7)(C) usdoj.gov>
Sent: Thursday, January 06, 2011 9:49 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Please call. Steve (b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 9:39 AM
To: (b)(6),(b)(7)(C) (BOS)
Cc: Externa (b)(6),(b) @cambridgepolice.org
Subject: FW: macaddr reg screenshot
Attachments: Screen shot 2011-01-05 at 5.18.49 PM.png

Not sure of the email address in the page he filled out to register the laptop at MIT is worth anyting.
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:32 PM
To: (b)(6),(b)(7)(C)
Subject: FW: macaddr reg screenshot

Hi there,
So the MAC address in question is 00:4c:e5:a0:c7:56 and it looks like it was registered for a guest account on Nov 28th and has 13 days left on the registration. But it counts days in use and he is currently using a static IP address which doesn't affect that countdown. So the bottom line is that it does not look like the MAC address was previously registered by someone else.

Attached is a screen shot of our tool that looks up the MAC address registration information.

Thanks
(b)(6),(b)(7)(C)

-----Original Message-----
From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Wednesday, January 05, 2011 5:21 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: macaddr reg screenshot

Here you go. The email address ends in .com

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Thursday, January 06, 2011 9:37 AM
To: (b)(6),(b)(7)(C) (BOS); External (b)(6),(b)(7)(C) cambridgepolice.org
Cc: (b)(6),(b)(7)(C)
Subject: MIT - Bid 16

All,

I am going to suggest that we take the laptop and hard drive offline today. I think the amount of network traffic captured is sufficient and would like to remove the laptop to see if he comes back to retrieve it. I will be able to put some people there for a short time in an attempt to ID.

I am following up a couple of possible ID's this morning and will get back to you on my success (or not).

The open questions will be if we decide to take it offline, is this something I can do with instruction or will I need help? Also, do we want to have the new drive printed?

(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C)
Sent: Wednesday, January 05, 2011 5:02 PM
To: (b)(6),(b)(7)(C) ussa.dhs.gov; (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C)
Subject: Packet Capture

Hi there,
I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. I've done some initial checking of the capture and I don't see anything that identifies a command and control channel. I was just wondering what the next step is.

Thank you

(b)(6),(b)(7)(C)
Network & Infrastructure Services
Information Services and Technology (IS&T)
Massachusetts Institute of Technology
Room (b)(6),(b)
Cambridge, MA 02139
(b)(6),(b)(7)(C)
(b)(6), mit.edu

From: (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) @state.ma.us>
Sent: Thursday, January 06, 2011 8:12 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Unauthorized Activity on MIT network

Let me know if you need me to look deeper into other statutes. Good luck (b)(6), (b)(7)

From (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, January 05, 2011 05:58 PM
To (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) state.ma.us>
Subject: Re: Unauthorized Activity on MIT network

We are working on identification now

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) state.ma.us>
To: (b)(6),(b)(7)(C) BOS)
Sent: Wed Jan 05 17:53:43 2011
Subject: Re: Unauthorized Activity on MIT network

Do you have an identification (b)(6), (b)(7) (b)(5)
(b)(5)
(b)(5) I would need to know a bit more though.

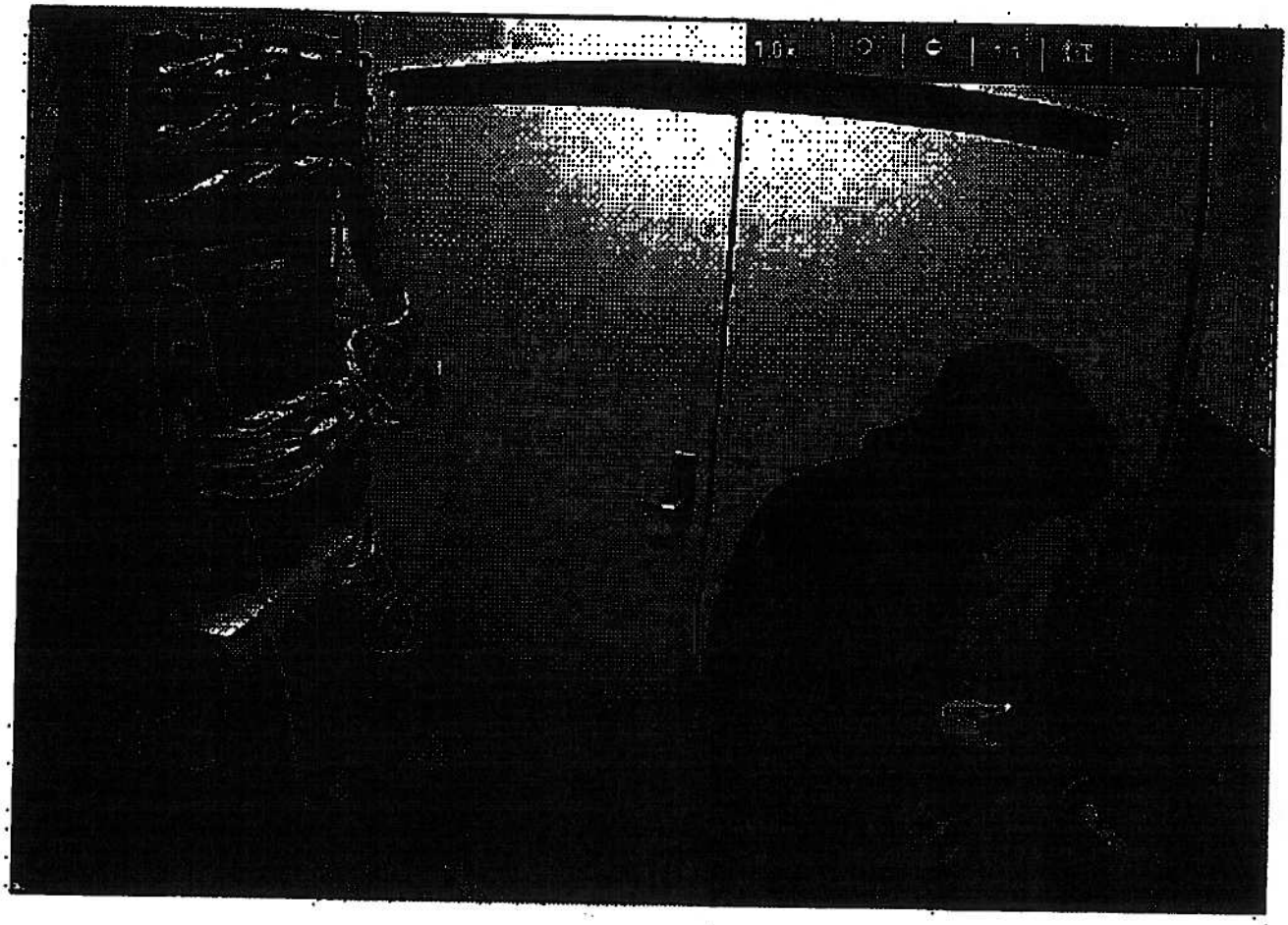
From (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, January 05, 2011 11:19 AM
To (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) state.ma.us>
Subject: Unauthorized Activity on MIT network

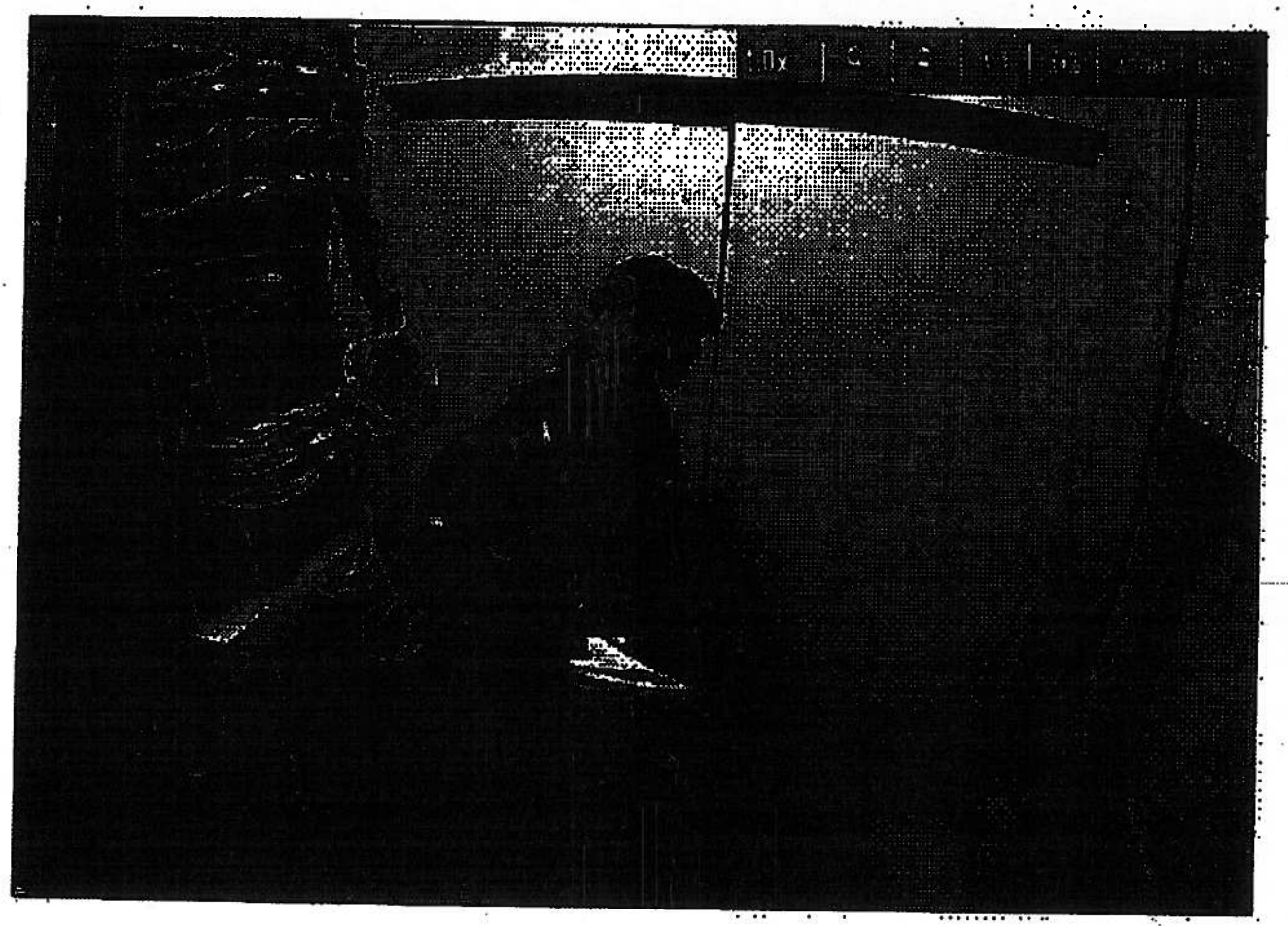
I would like to get your opinion on what offenses the suspect could be charged with in this case and what evidence would best support prosecution.

On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department (b)(6),(b)(7)(C) mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11, (b)(6), (b)(6),(b (b)(6),(b)(7)(C) (b)(6),(b)(7 mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as

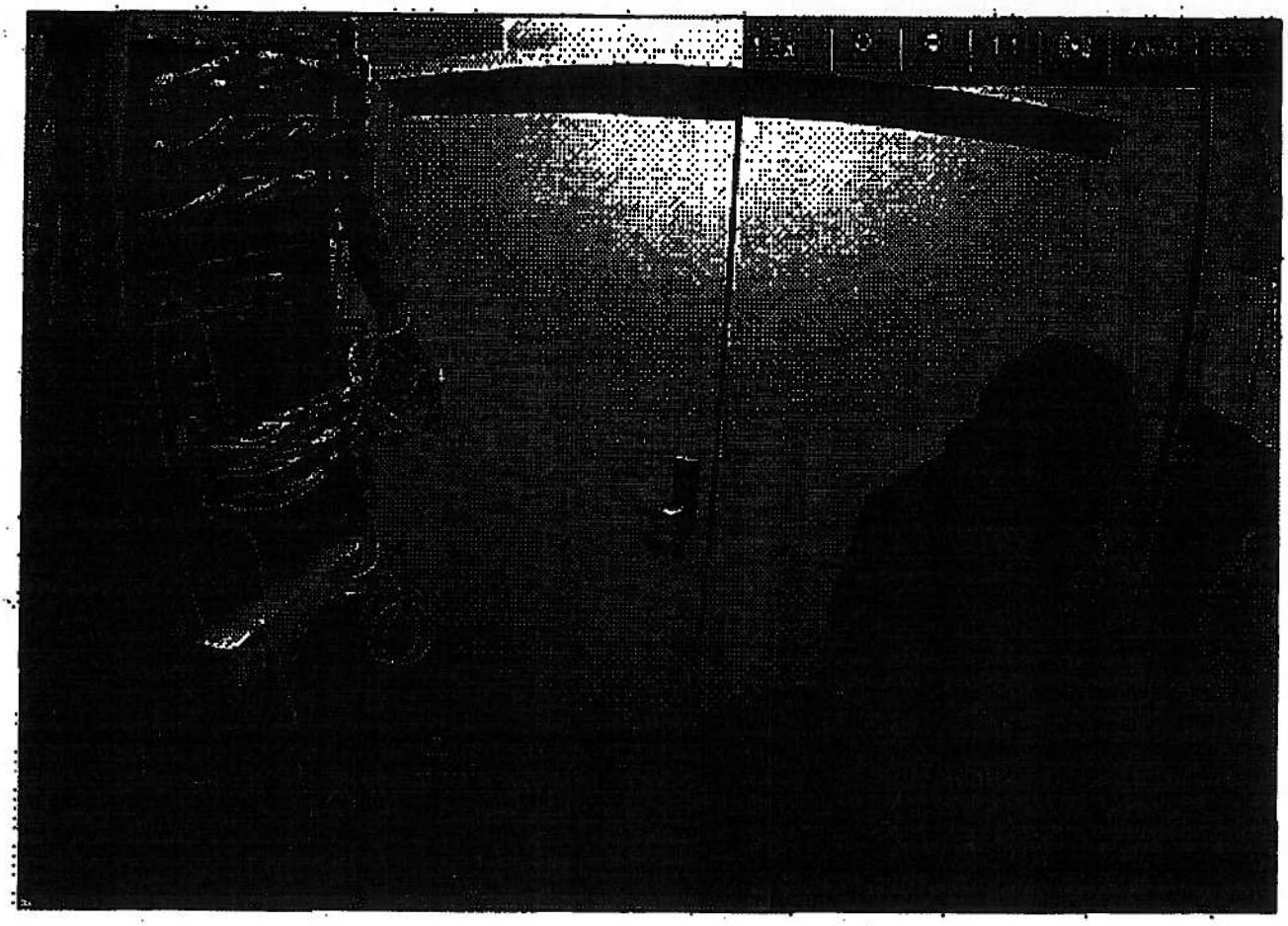
stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing. (b)(6),(b)(7)(provided SA (b)(6), with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

At 1526 on 01/04/11 this individual came back and appears to be replacing the external drive:



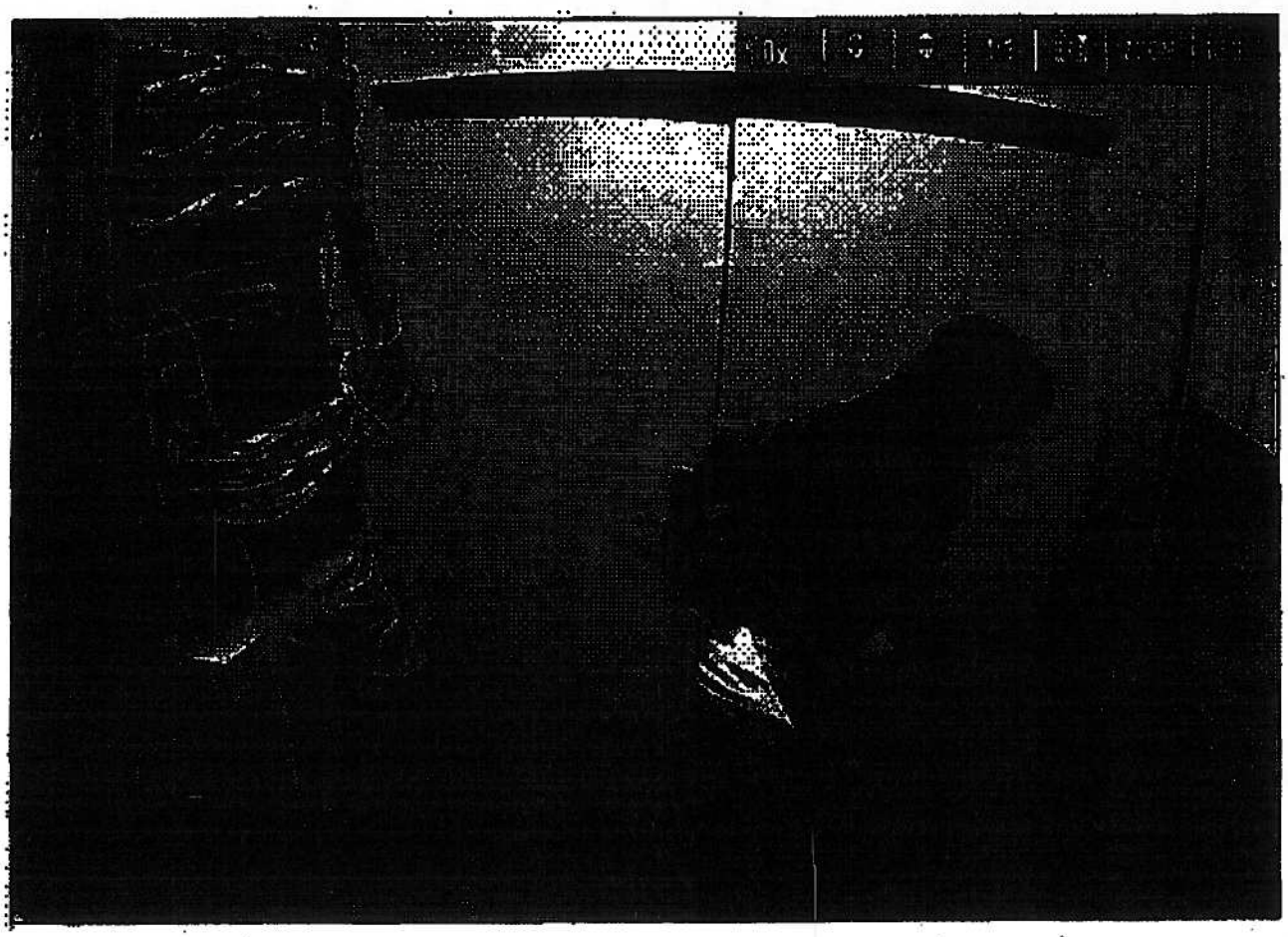


RIF

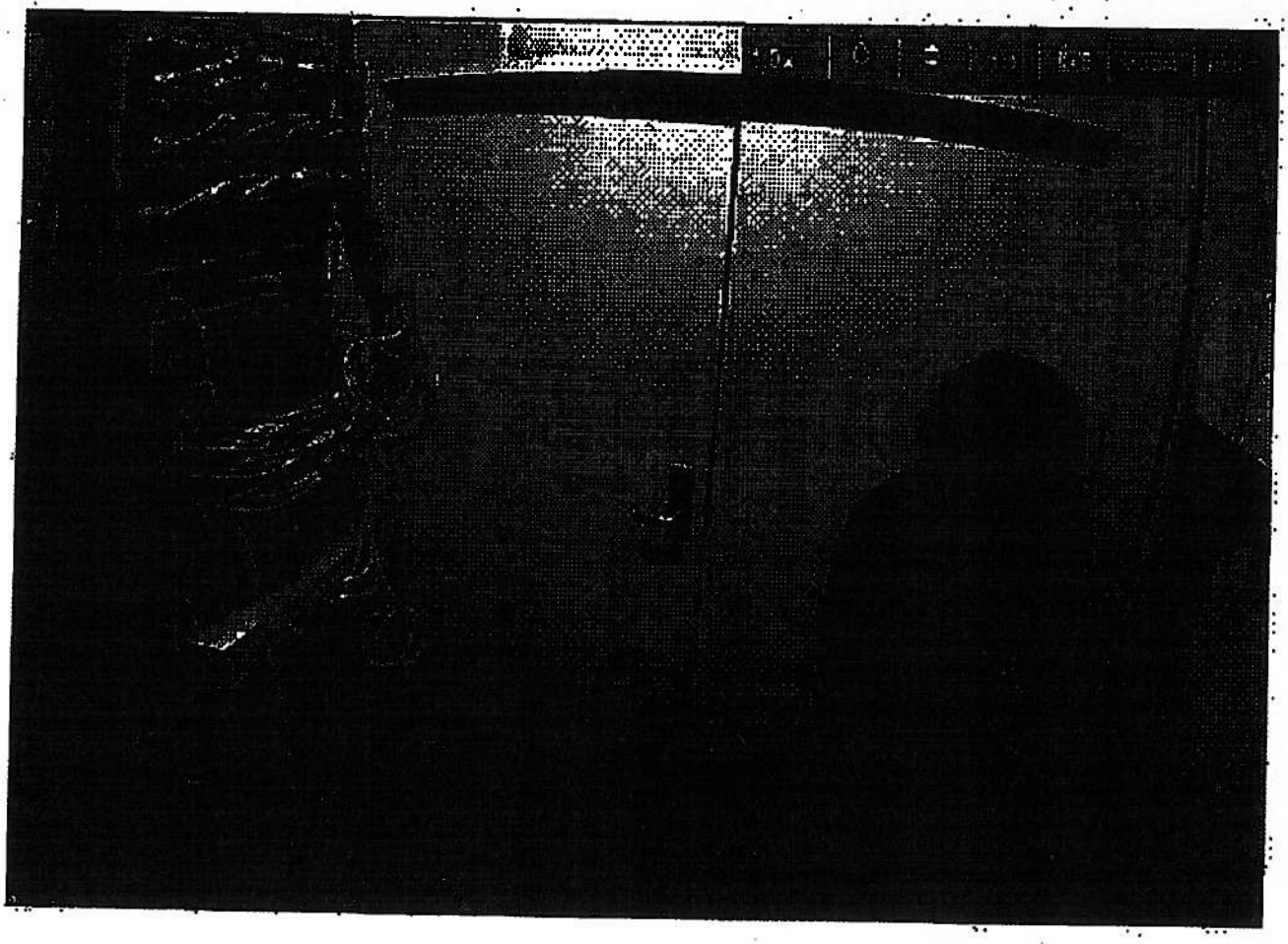


RIF
2511

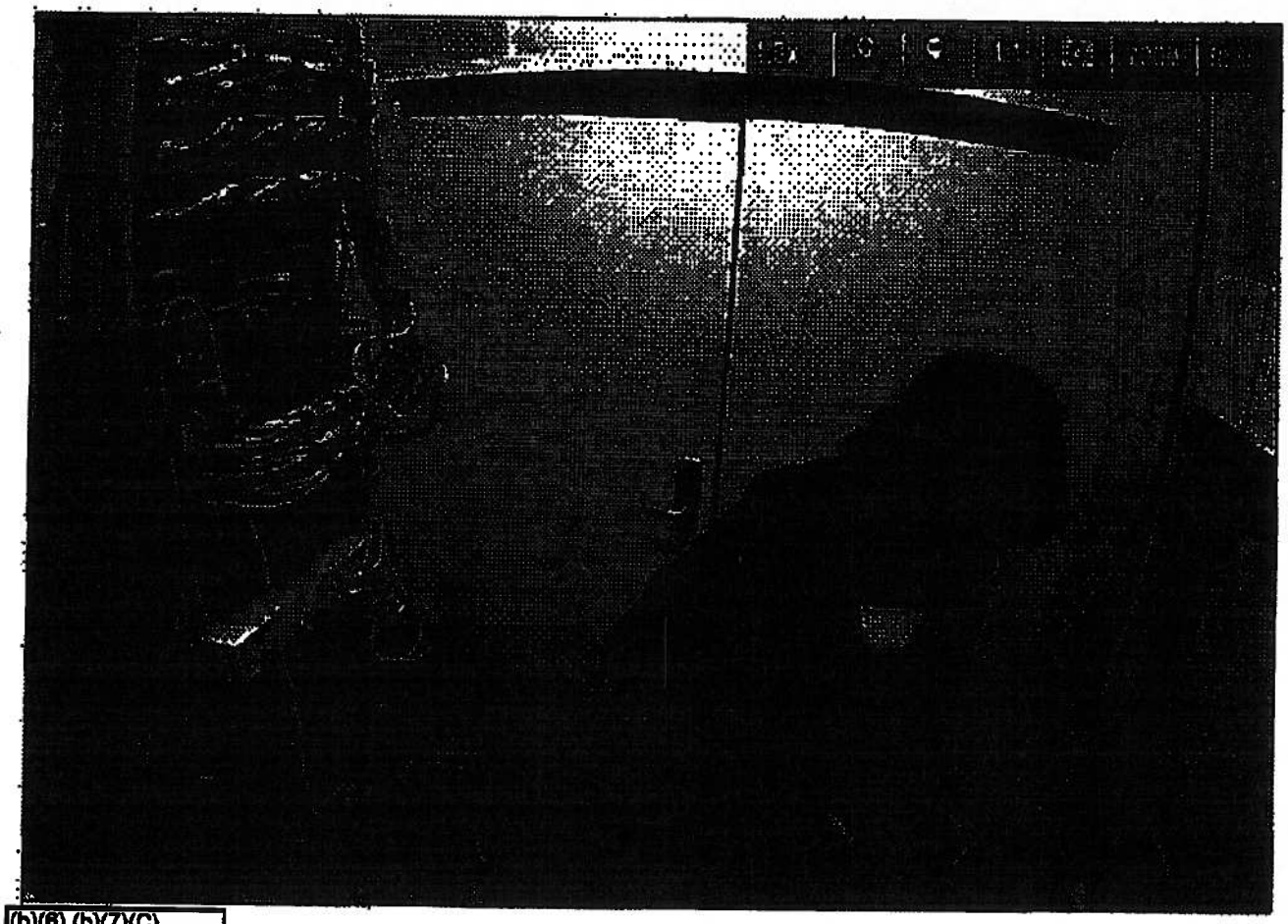
RIF
2512



RIF



RIF
2514



(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) @state.ma.us>
Sent: Wednesday, January 05, 2011 5:54 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Unauthorized Activity on MIT network

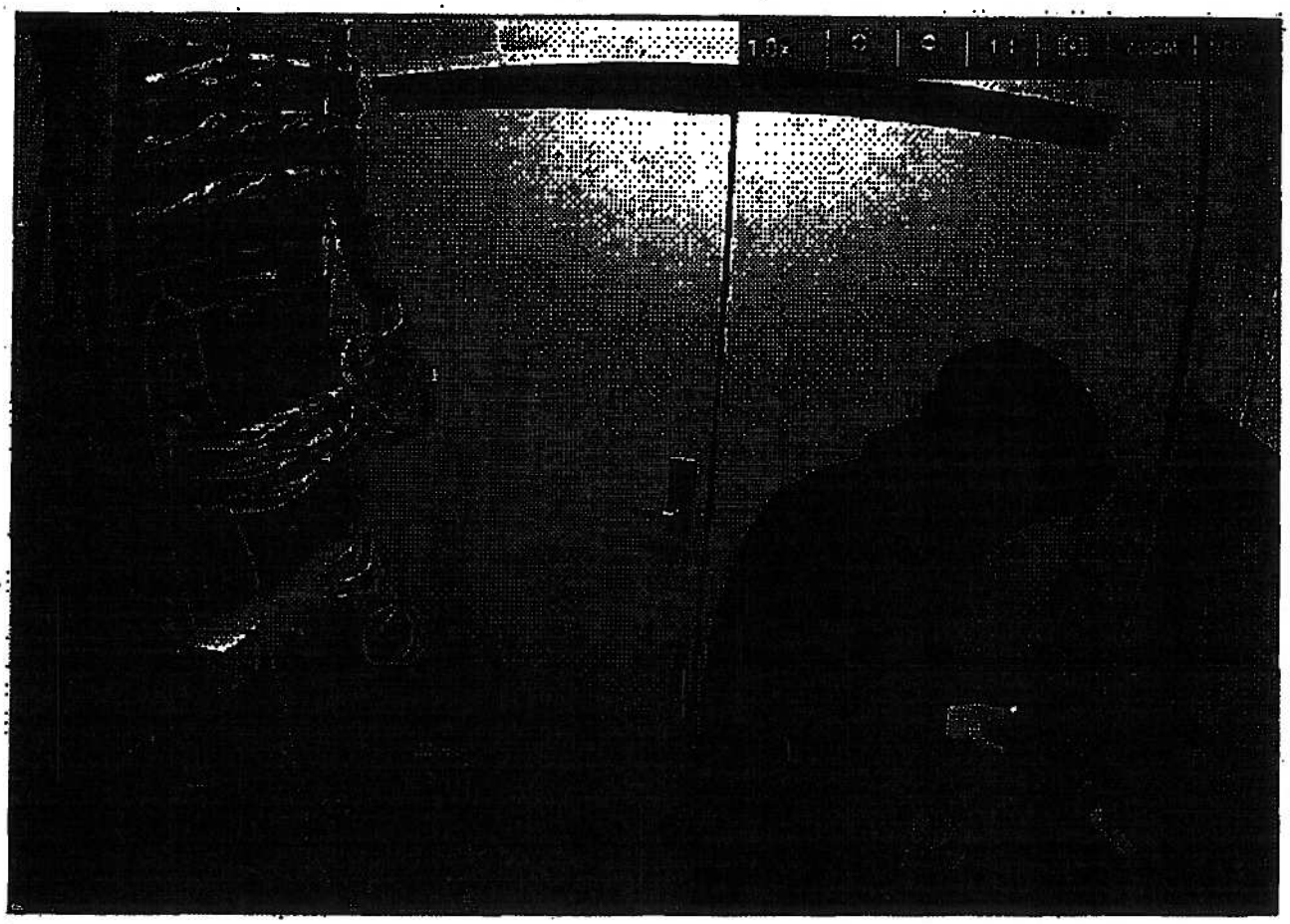
Do you have an identification (b)(6), (b)(7)(C) (b)(5) (b)(5) (b)(5) I would need to know a bit more though.

From: (b)(6),(b)(7)(C) (BOS) [mailto: (b)(6),(b)(7)(C) @usss.dhs.gov]
Sent: Wednesday, January 05, 2011 11:19 AM
To: (b)(6),(b)(7)(C) (AGO) (b)(6),(b)(7)(C) @state.ma.us>
Subject: Unauthorized Activity on MIT network

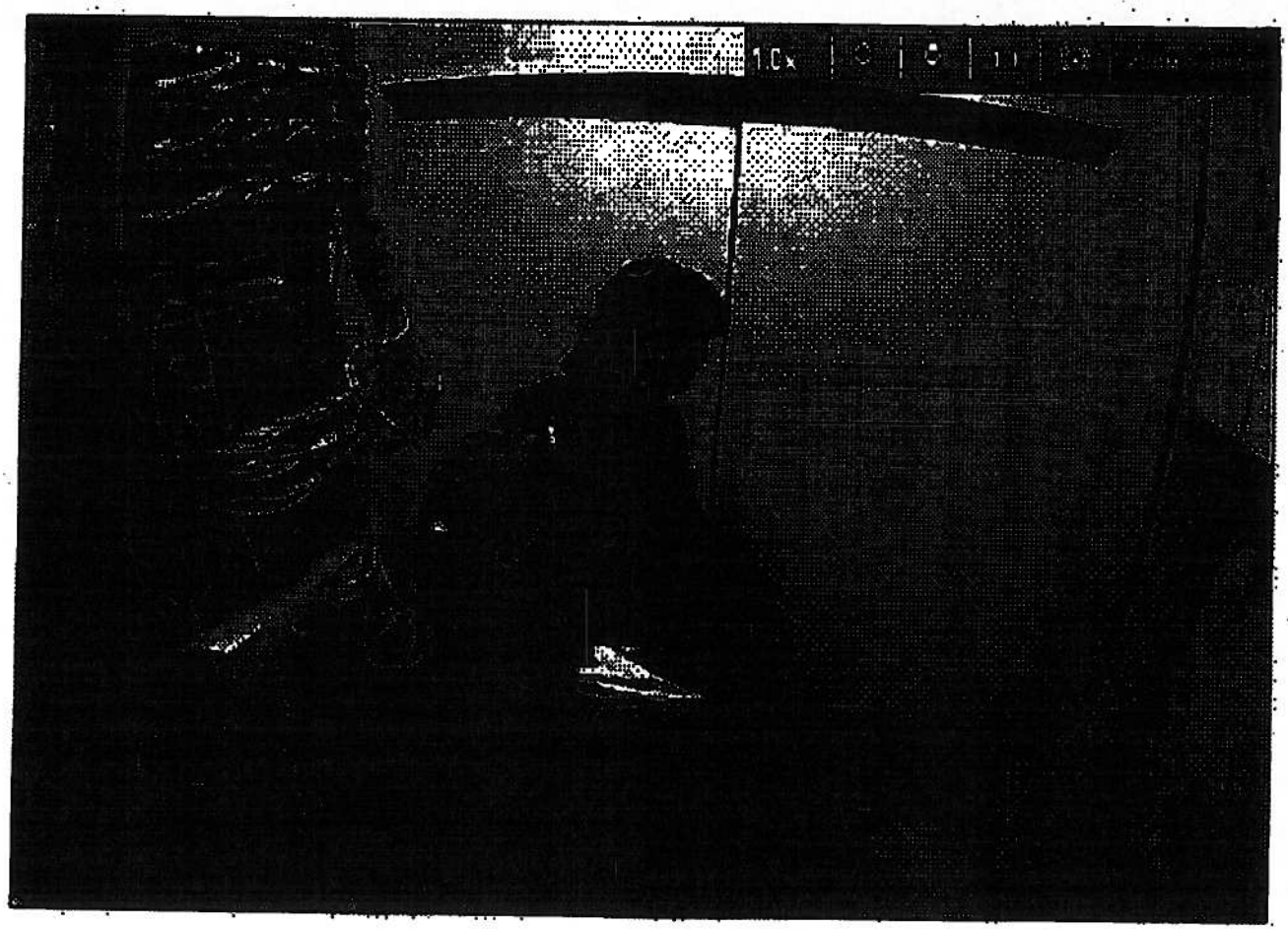
I would like to get your opinion on what offenses the suspect could be charged with in this case and what evidence would best support prosecution.

On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) (MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department (b)(6),(b)(7)(C) @mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(6),(b (b)(6),(b)(7) @mit.edu) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing. (b)(6),(b)(7)(provided SA (b)(6),(with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

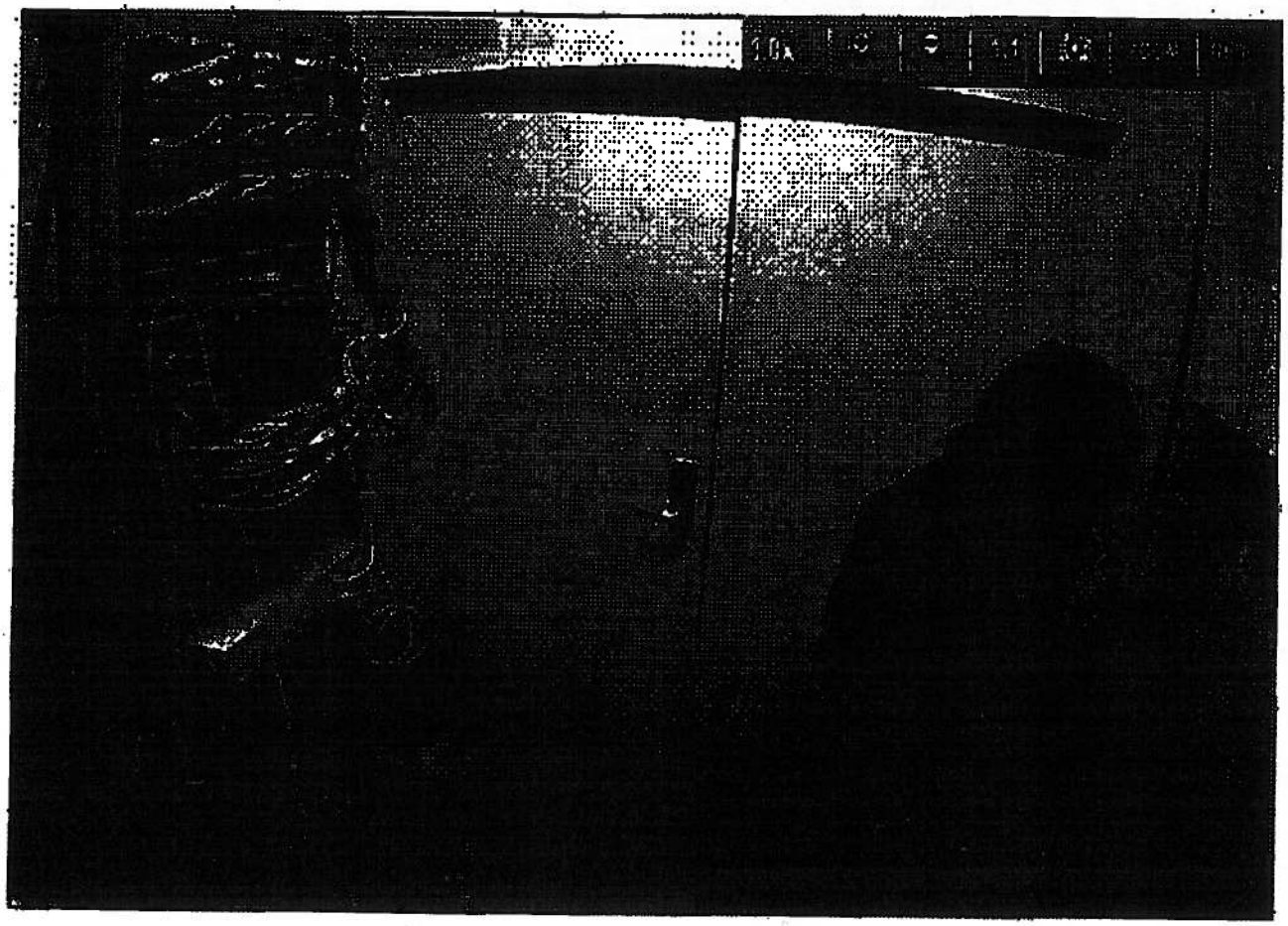
At 1526 on 01/04/11 this individual came back and appears to be replacing the external drive:



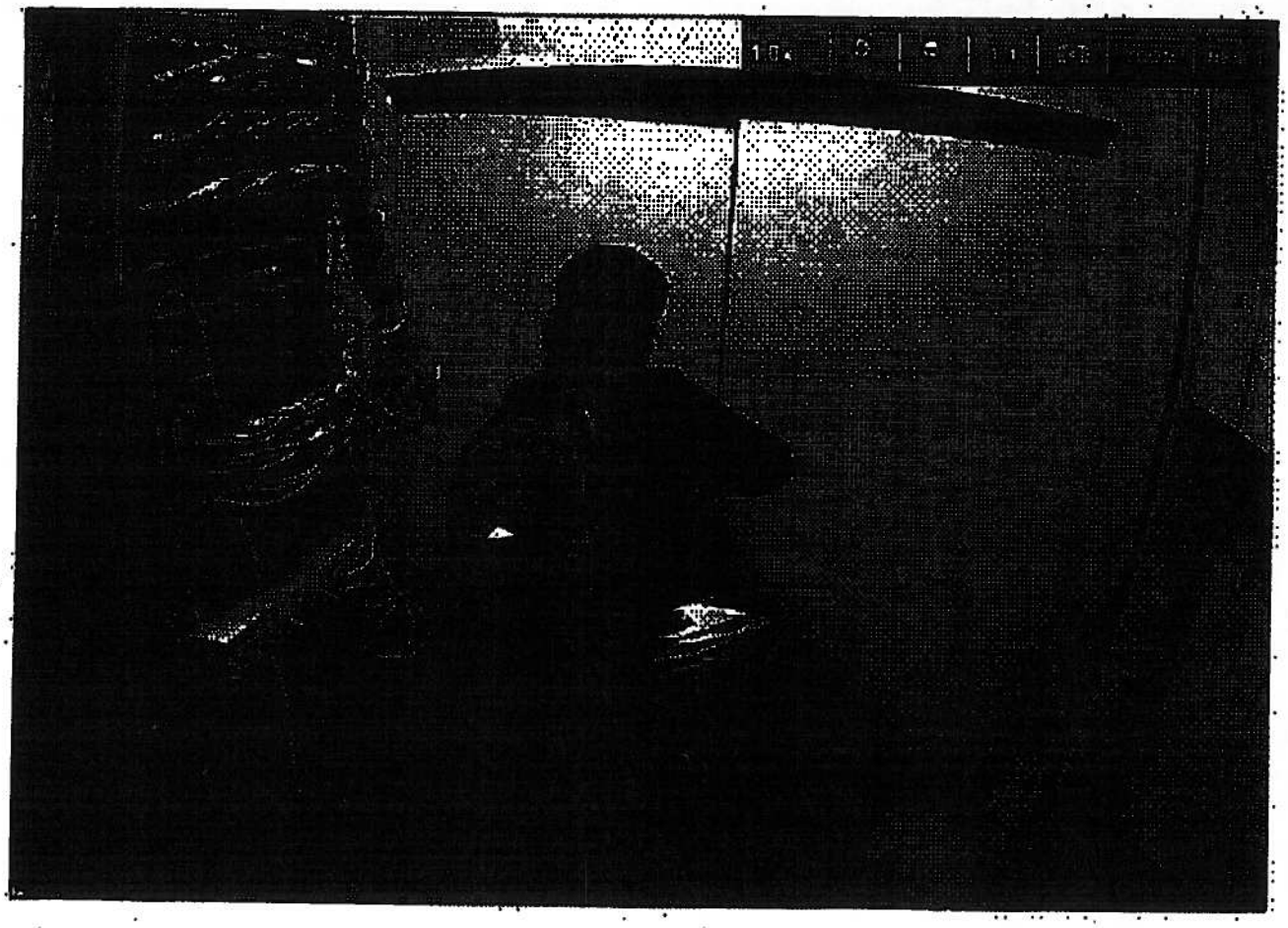
RIF

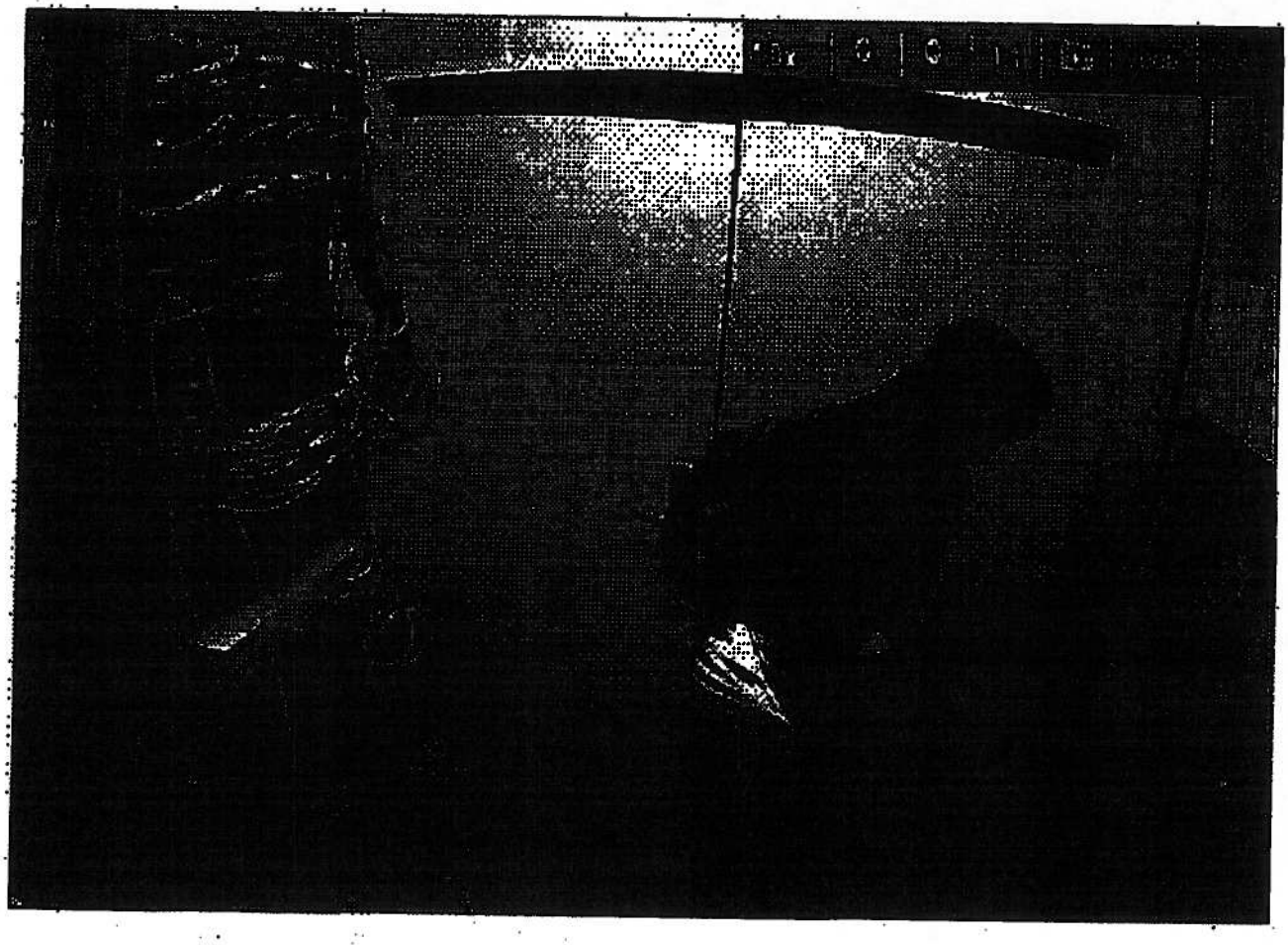


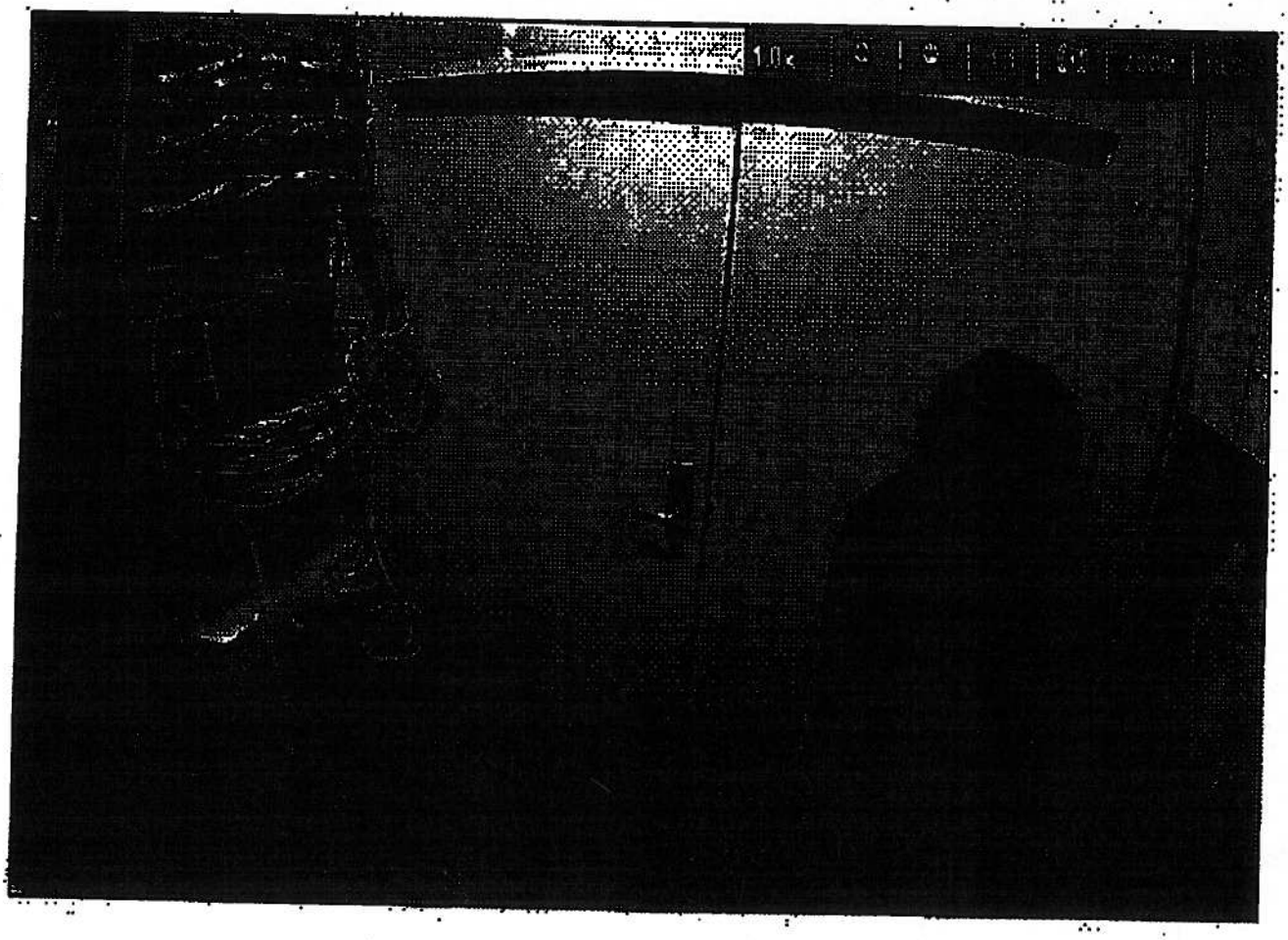
RIF

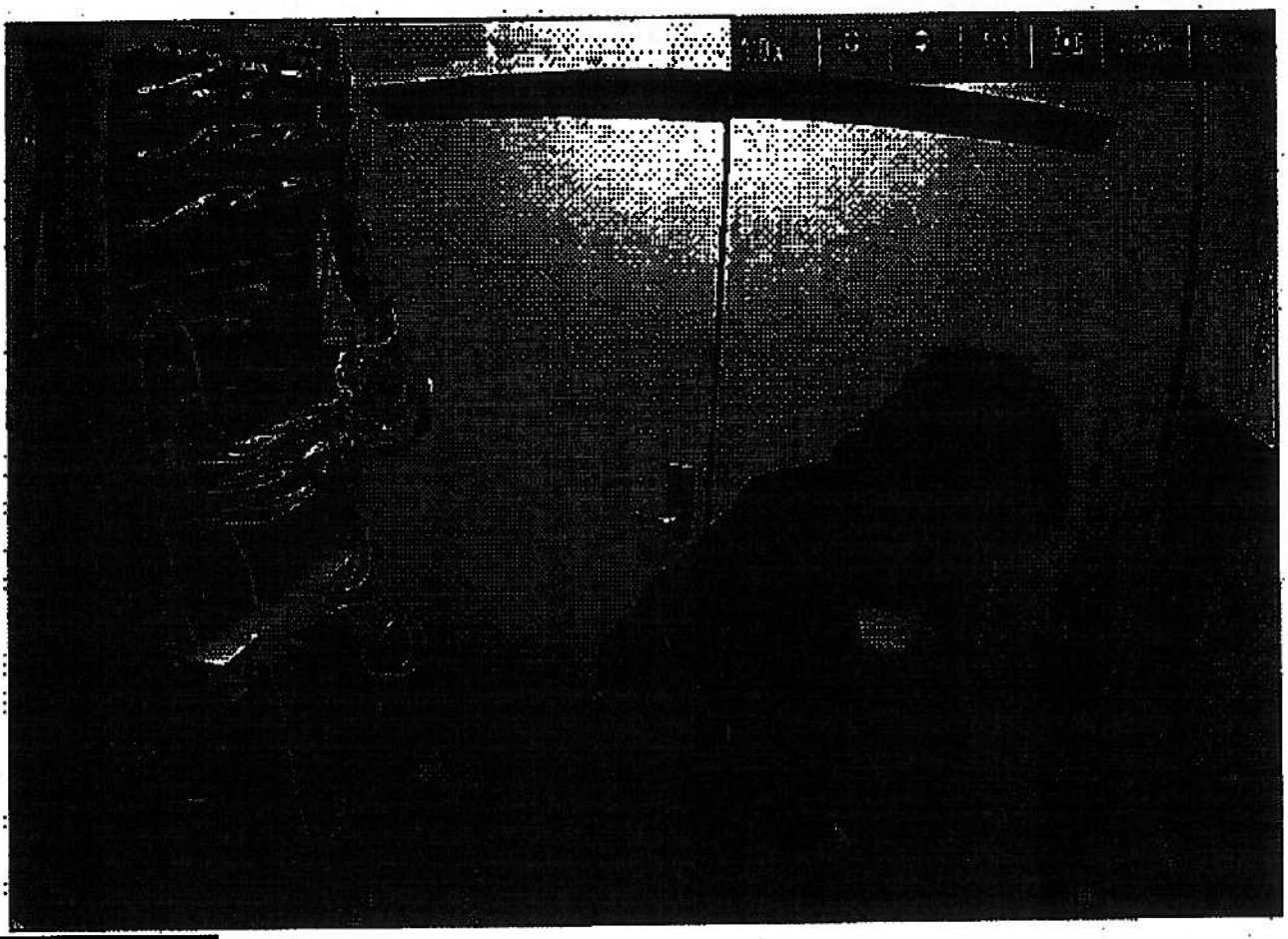


RIF









(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (CHI)
Sent: Wednesday, January 05, 2011 12:42 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: FW: [responses to HTCC posting on MIT incident]
Attachments: Re: [HTCC] Live Capture of Linux Box with out Admin Rights; Re: [HTCC] Live Capture of Linux Box with out Admin Rights; Re: [HTCC] Live Capture of Linux Box with out Admin Rights; Re: [HTCC] Live Capture of Linux Box with out Admin Rights; Re: [HTCC] Live Capture of Linux Box with out Admin Rights

See attached.

HTH

(b)(6),

(b)(6),(b)(7)(C)

ASSISTANT TO THE SPECIAL AGENT IN CHARGE US SECRET SERVICE CHICAGO FIELD OFFICE

-----Original Message-----
From: htcc-bounces@htcc.secport.com [mailto:htcc-bounces@htcc.secport.com] On Behalf Of htcc-request@htcc.secport.com
Sent: Wednesday, January 05, 2011 11:00 AM
To: htcc@htcc.secport.com
Subject: HTCC Digest, Vol 96, Issue 6

Send HTCC mailing list submissions to
htcc@htcc.secport.com

To subscribe or unsubscribe via the World Wide Web, visit
https://htcc.secport.com/mailman/listinfo/htcc
or, via email, send a message with subject or body 'help' to
htcc-request@htcc.secport.com

You can reach the person managing the list at
htcc-owner@htcc.secport.com

When replying, please edit your Subject line so it is more specific than "Re: Contents of HTCC digest..."

From: (b)(6),(b)(7)(C) USAMA) (b)(6),(b)(7)(C) @usdoj.gov>
Sent: Wednesday, January 05, 2011 11:32 AM
To: (b)(6),(b)(7)(C) BOS)
Cc: Heymann, Stephen (USAMA)
Subject: RE: Unauthorized Activity on the MIT network

Thanks for all of the detail -- very helpful. Steve and I will discuss this and get back to you by the end of the day.

(b)(6),(b)(7)(C)

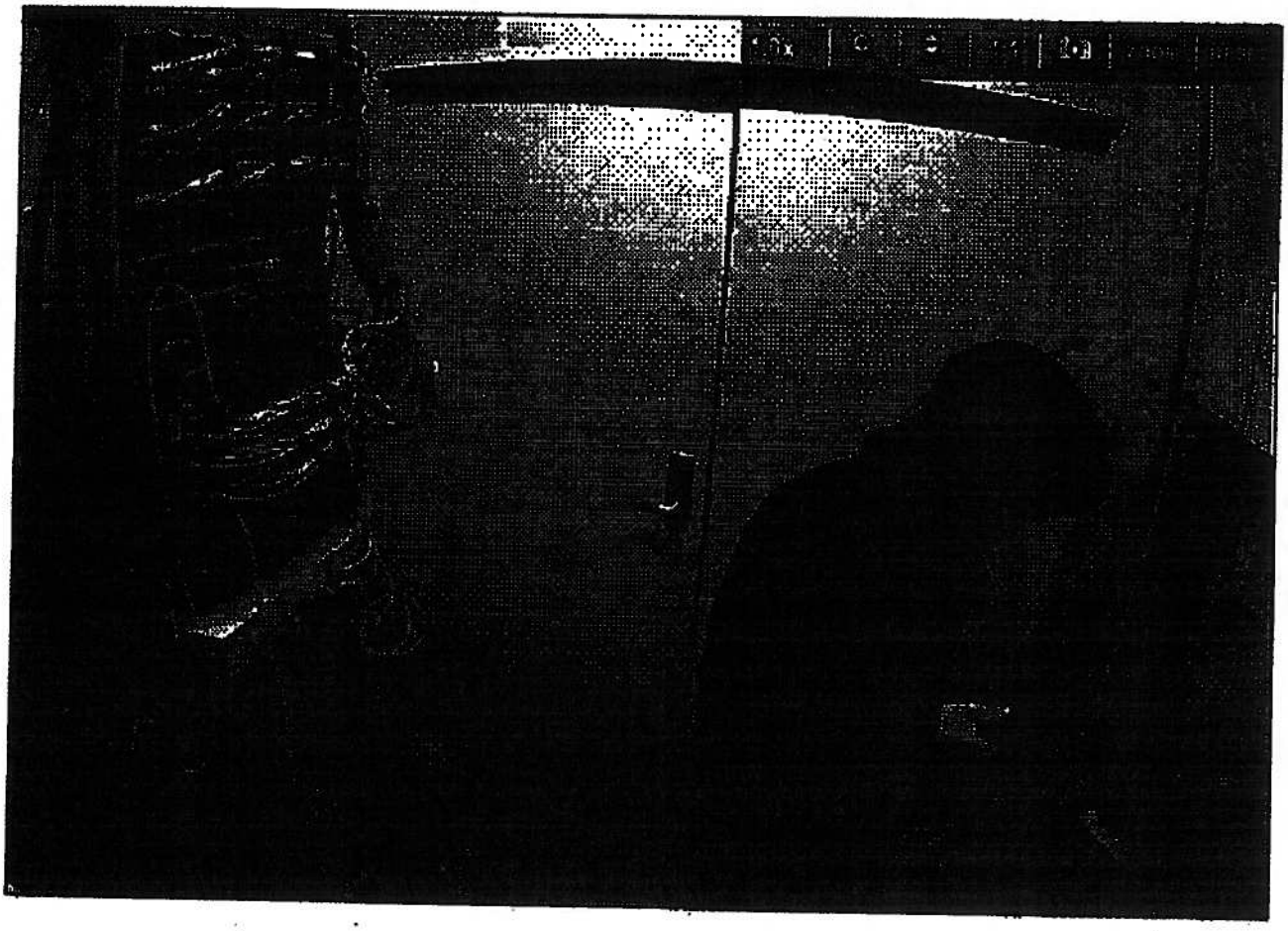
From: (b)(6),(b)(7)(C) (BOS) [mailto (b)(6),(b)(7)(C) usss.dhs.gov]
Sent: Wednesday, January 05, 2011 11:23 AM
To: (b)(6),(b)(7)(C) (USAMA)
Subject: Unauthorized Activity on the MIT network

If you have the time, I would appreciate if you would take a look at a new development that came to our attention yesterday. I would like to get your opinion on what offenses the suspect could be charged with in this case and what evidence would best support prosecution.

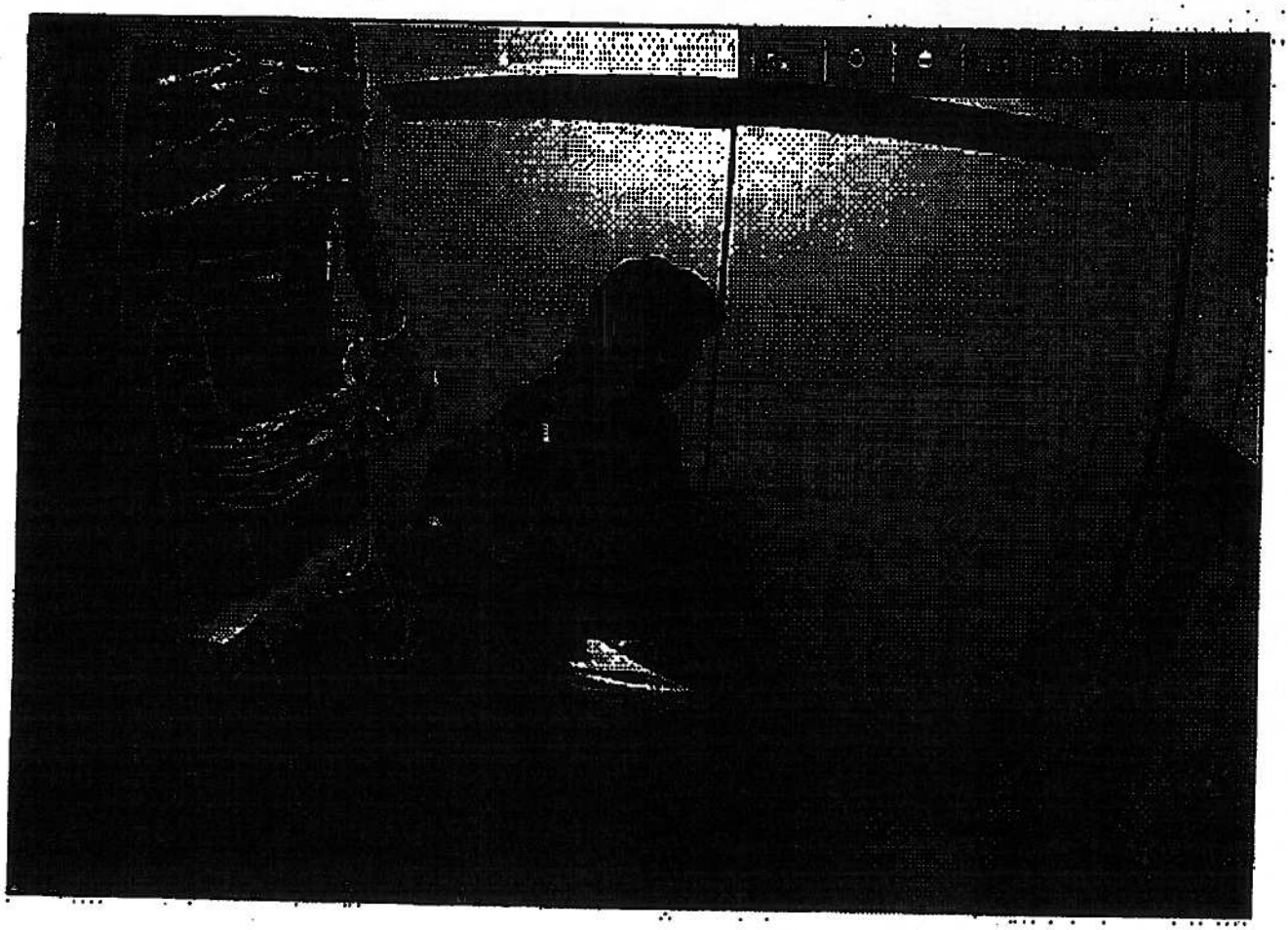
On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department (b)(6),(b)(7)(C) mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(7)(C (b)(6),(b) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) (b)(6),(b mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(and (b)(6),(b)(7)(C which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing (b)(6),(b)(7)(provided SA (b)(6), with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to

view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

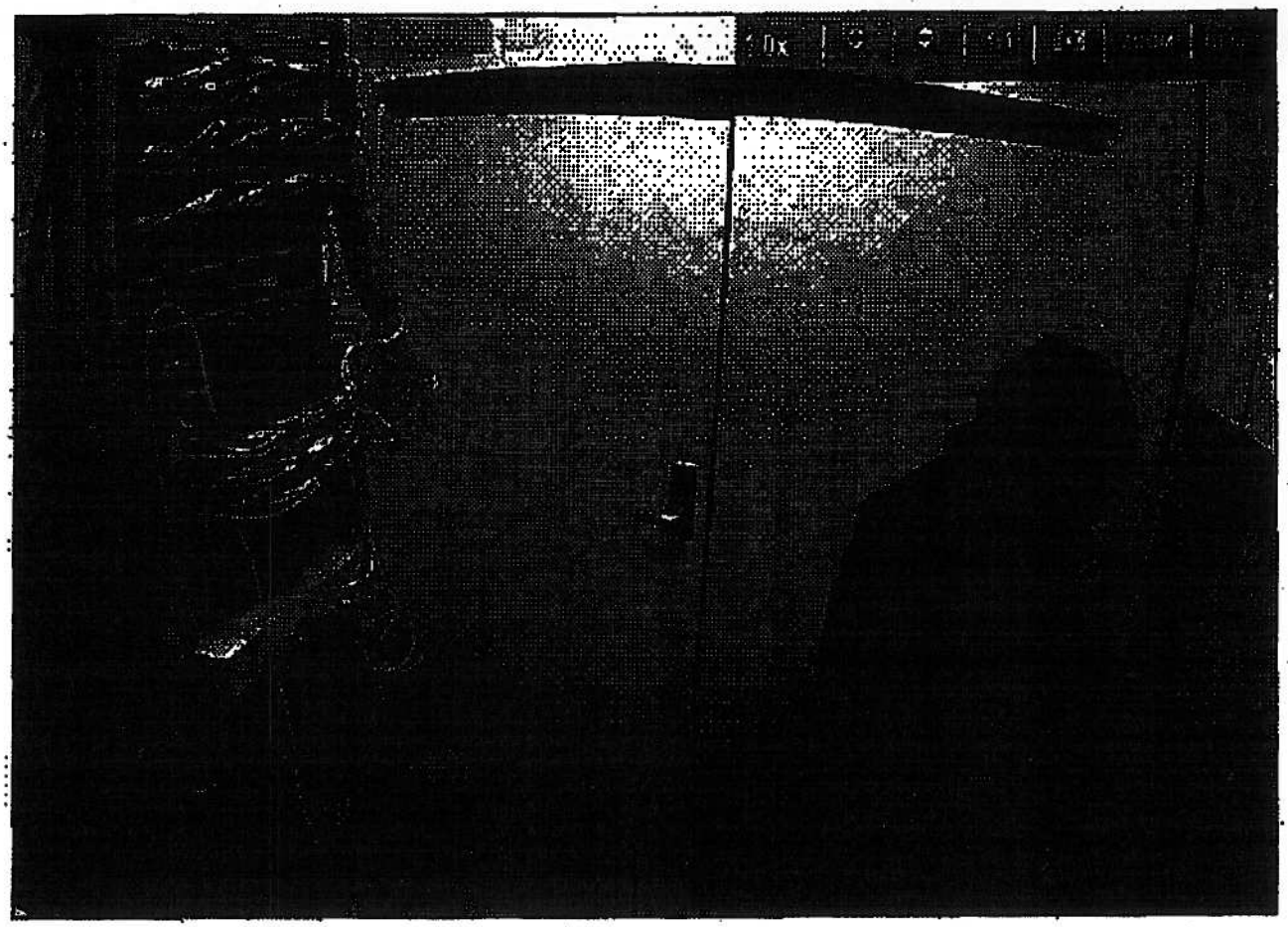
At 1526 on 01/04/11 this individual came back and appears to be replacing the external drive:



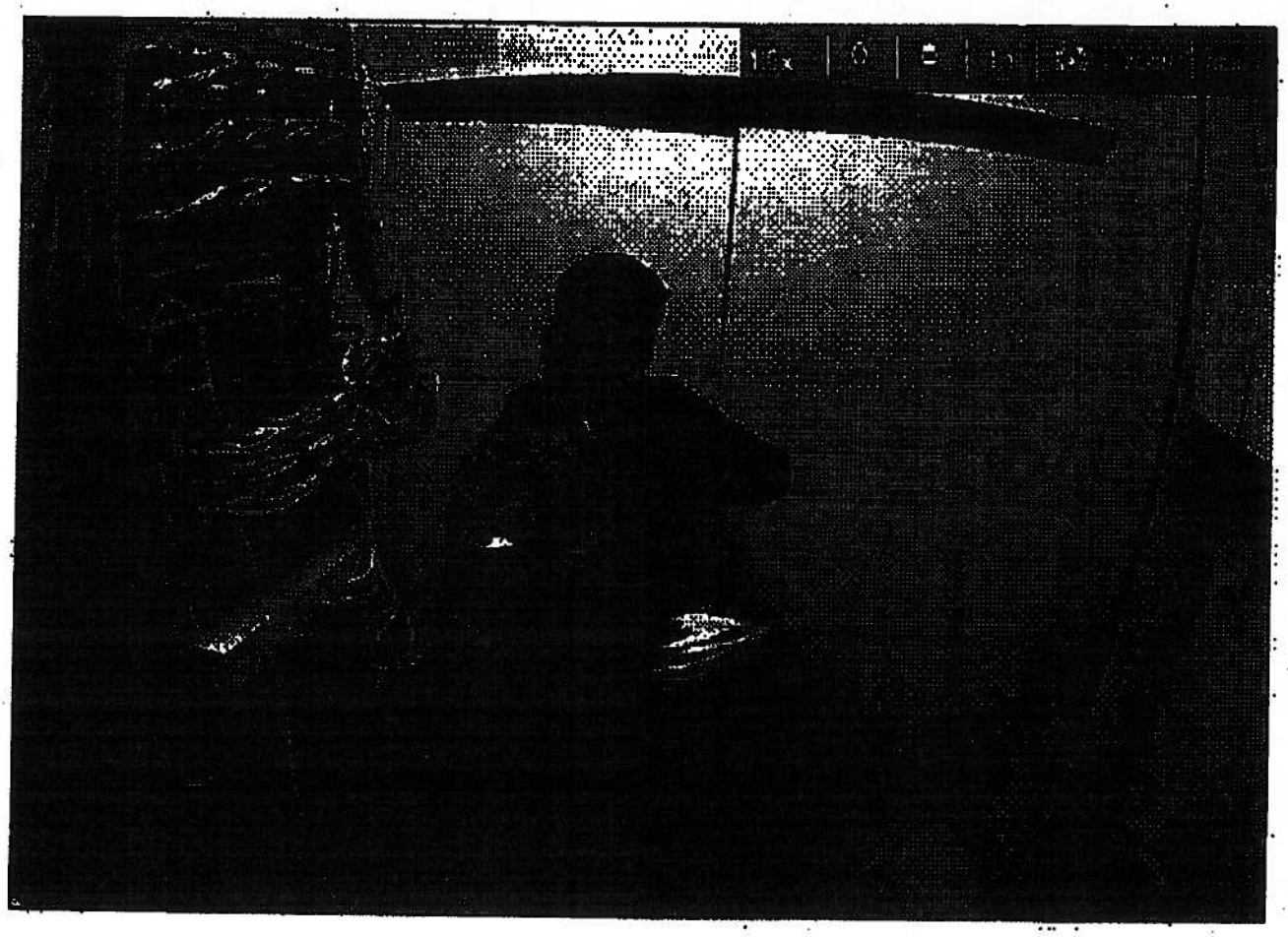
RIF 2527



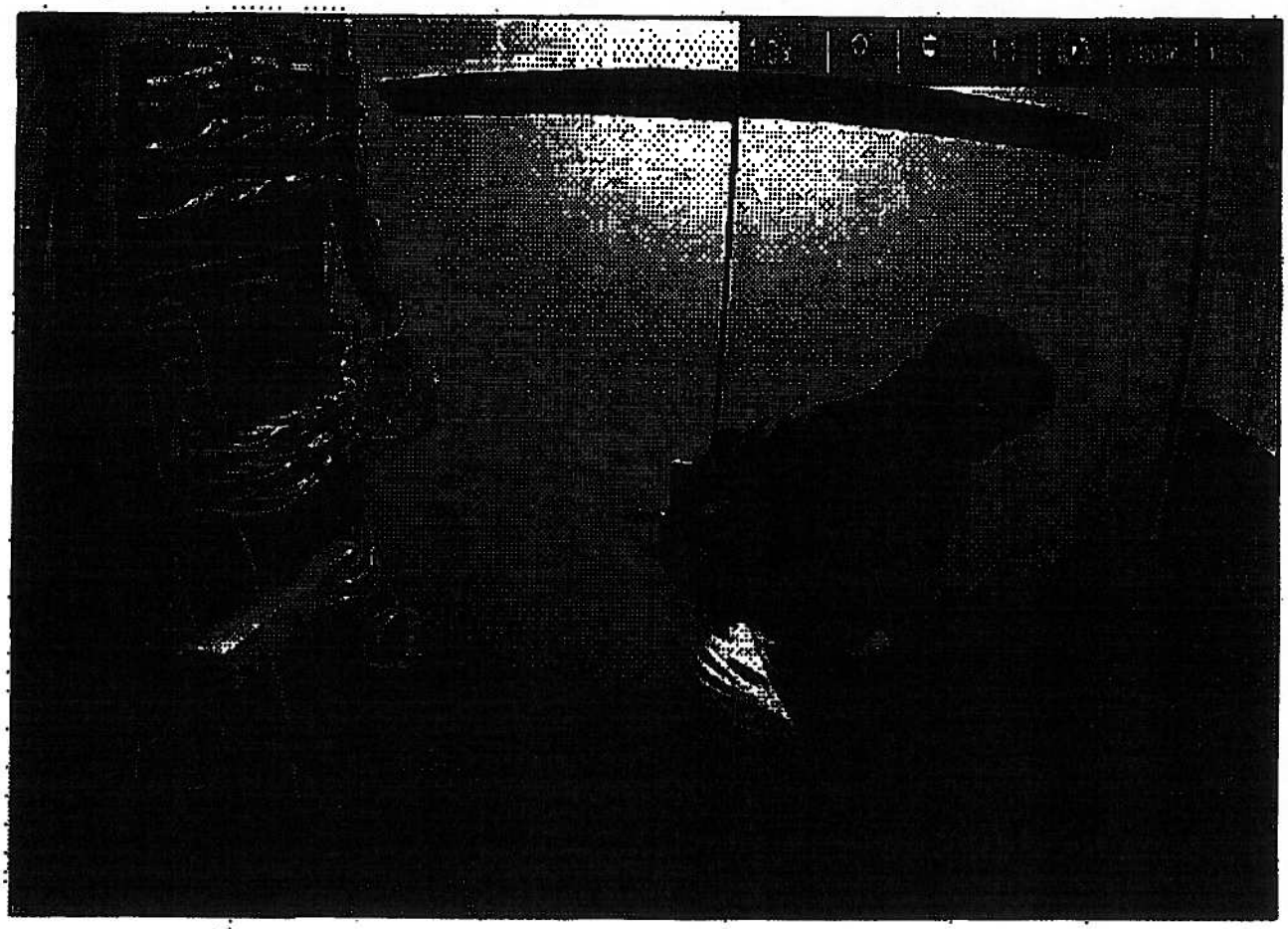
RIF
2528



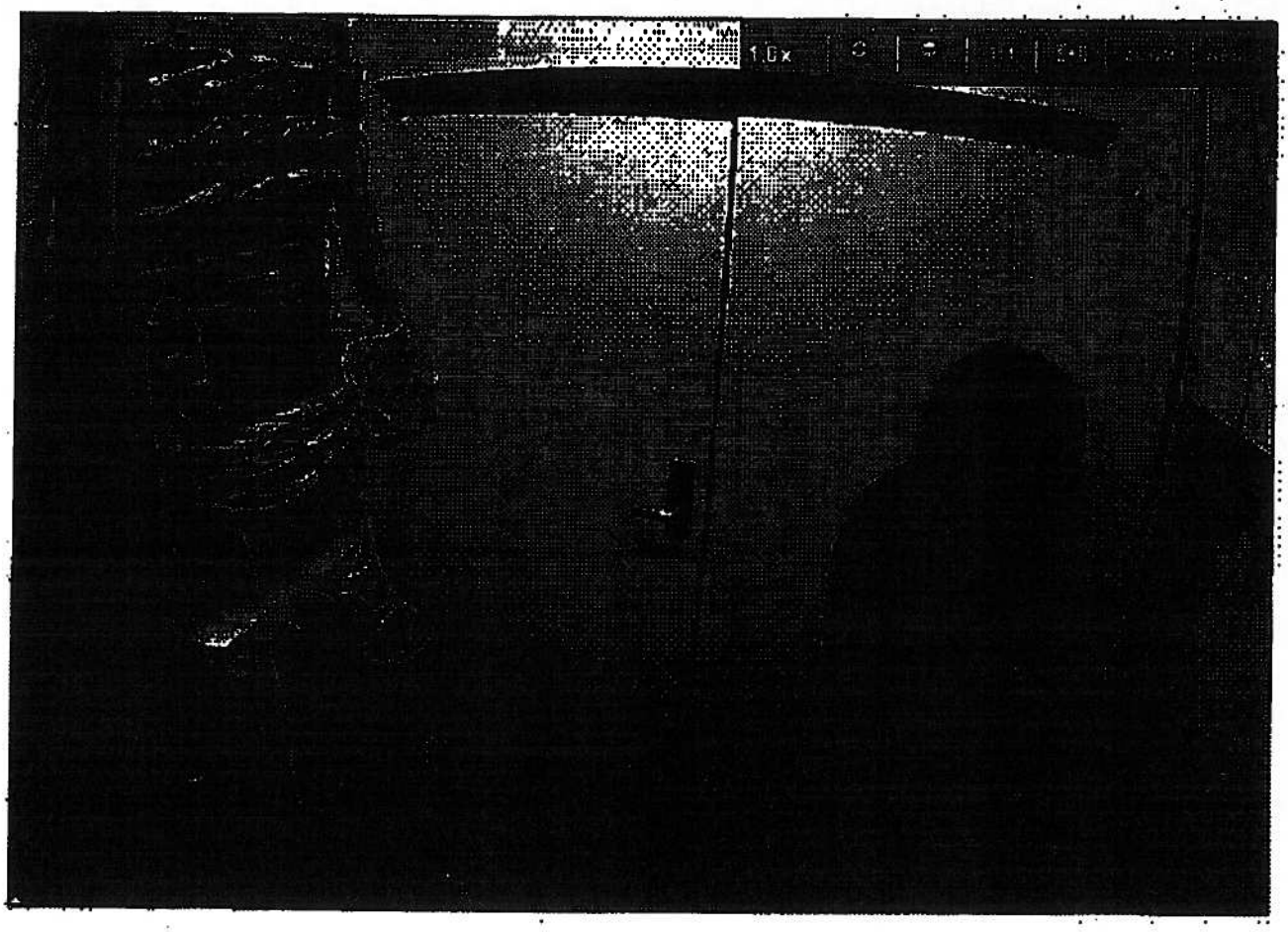
RIF



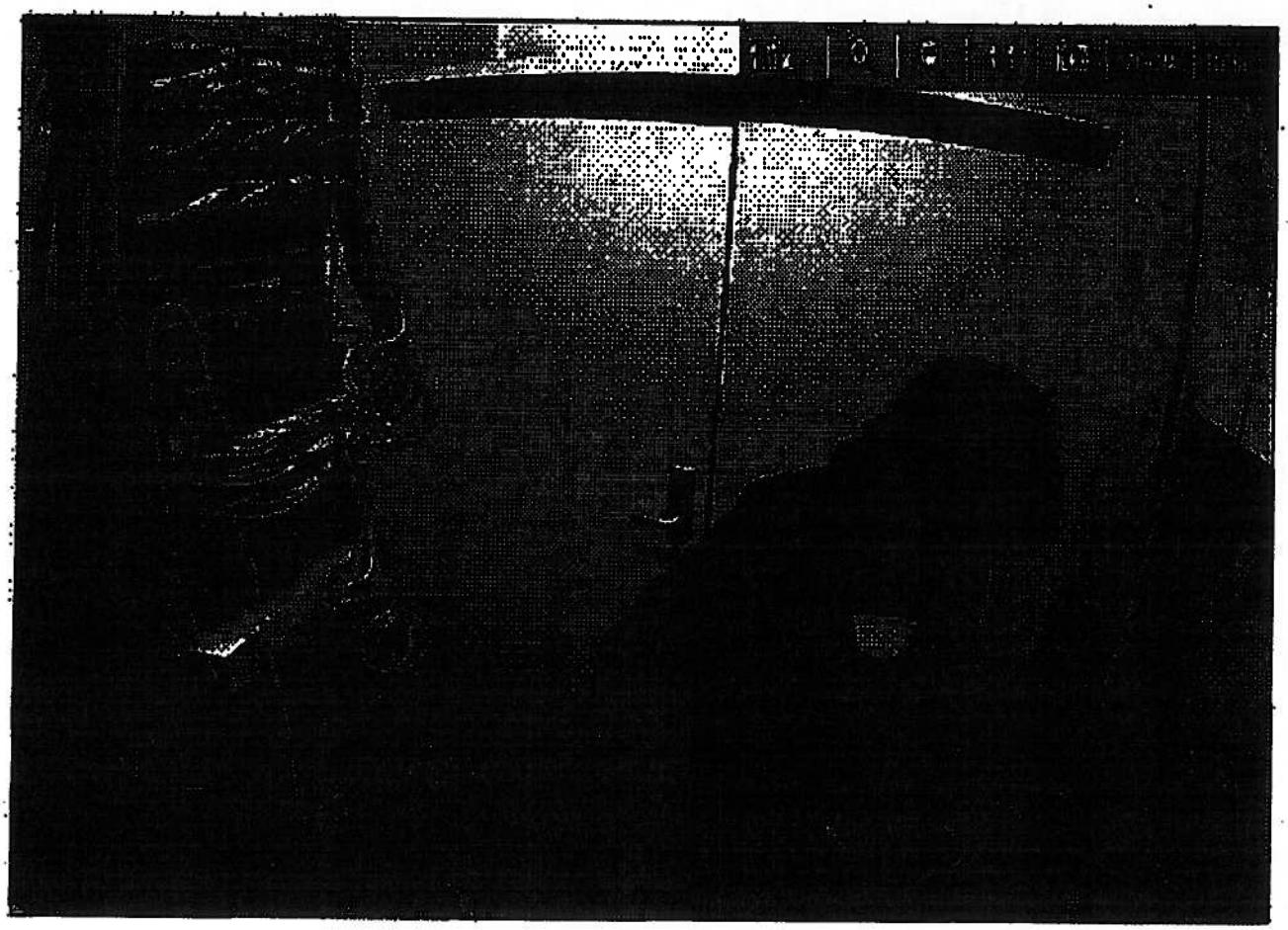
RIF



RIF



RIF



(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

RIF

From: (b)(6),(b)(7)(C) (CID)
Sent: Wednesday, January 05, 2011 10:22 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Unauthorized activity on Massachusetts Institute of Technology network

(b)(6),(b)(7)(C)

Thanks for the info about the case...its' sounds very interesting. If you wouldn't mind, please keep me posted as it develops. Let me know if we can assist here. Thanks.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Tue 1/4/2011 6:45 PM
To: (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID)
Cc: (WFO); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) (REN)
Subject: Unauthorized activity on Massachusetts Institute of Technology network

FYI

Unauthorized activity on Massachusetts Institute of Technology network
On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department. (b)(6),(b)(7)(C) @mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(7)(C) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile. (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing. (b)(6),(b)(7) provided SA (b)(6), with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet

to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (BOS)
Sent: Wednesday, January 05, 2011 8:13 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Building 16

Got it, thanks

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Sent: Wed Jan 05 07:37:58 2011
Subject: FW: Building 16

Please see below

(b)(6),(b)(7)(C)
U.S. Secret Service
Boston Field Office
(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Wednesday, January 05, 2011 6:48 AM
To: undisclosed-recipients
Subject: FW: Building 16

Suspect as of yet unidentified.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@MIT.EDU]
Sent: Tuesday, January 04, 2011 3:51 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Building 16

(b)(6),(b)(7)(C) - here are the screenshots from the camera setup on the laptop at MIT. Looks like he added a drive, but it is still on the network.

(b)(6),

We did not get the call until he left the room.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, January 04, 2011 3:48 PM
To:
Cc: (b)(6),(b)(7)(C)
Subject: Building 16

Here are screenshots from 3:26pm

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Information Services & Technology, MIT

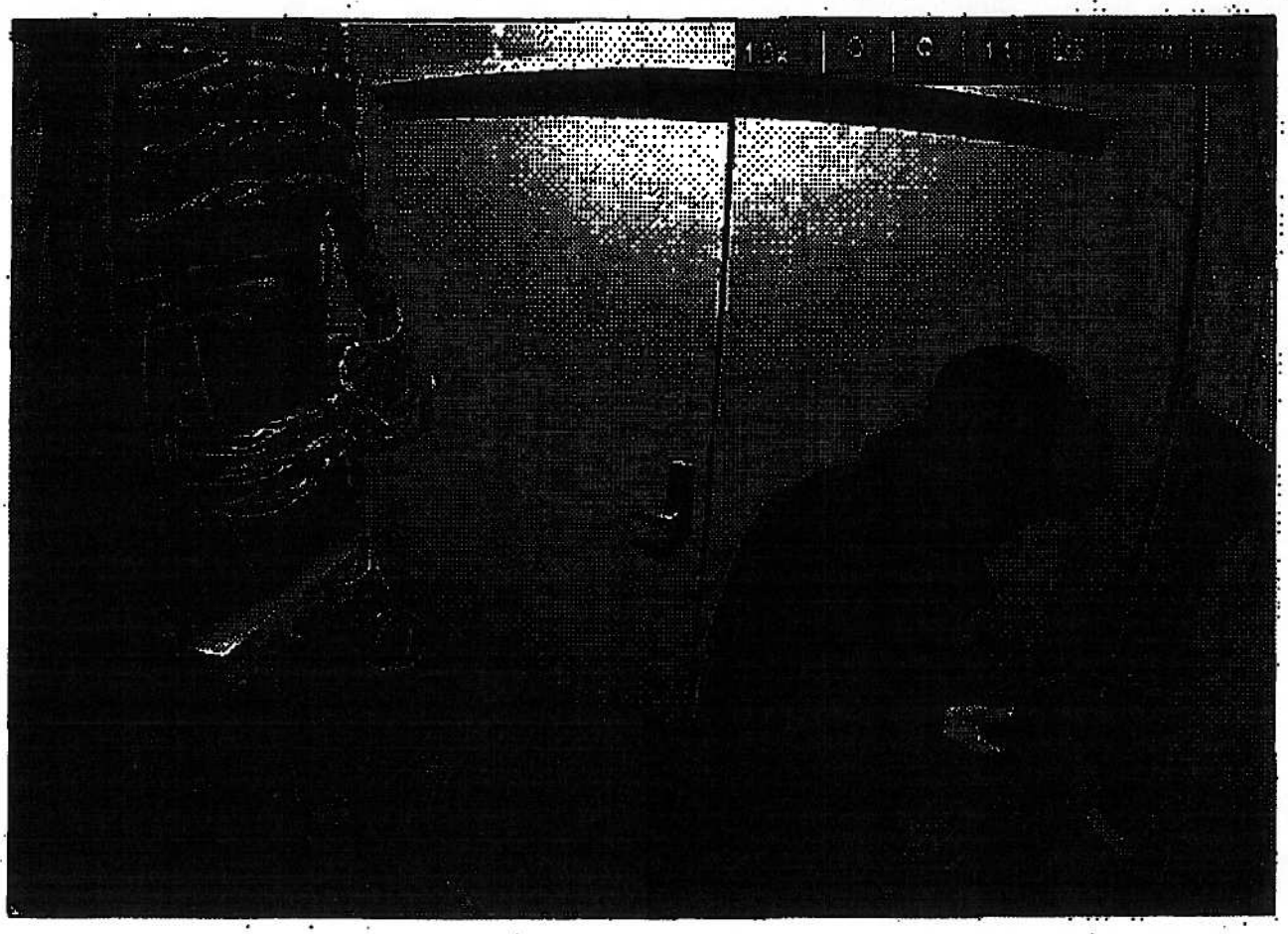
(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) mit.edu

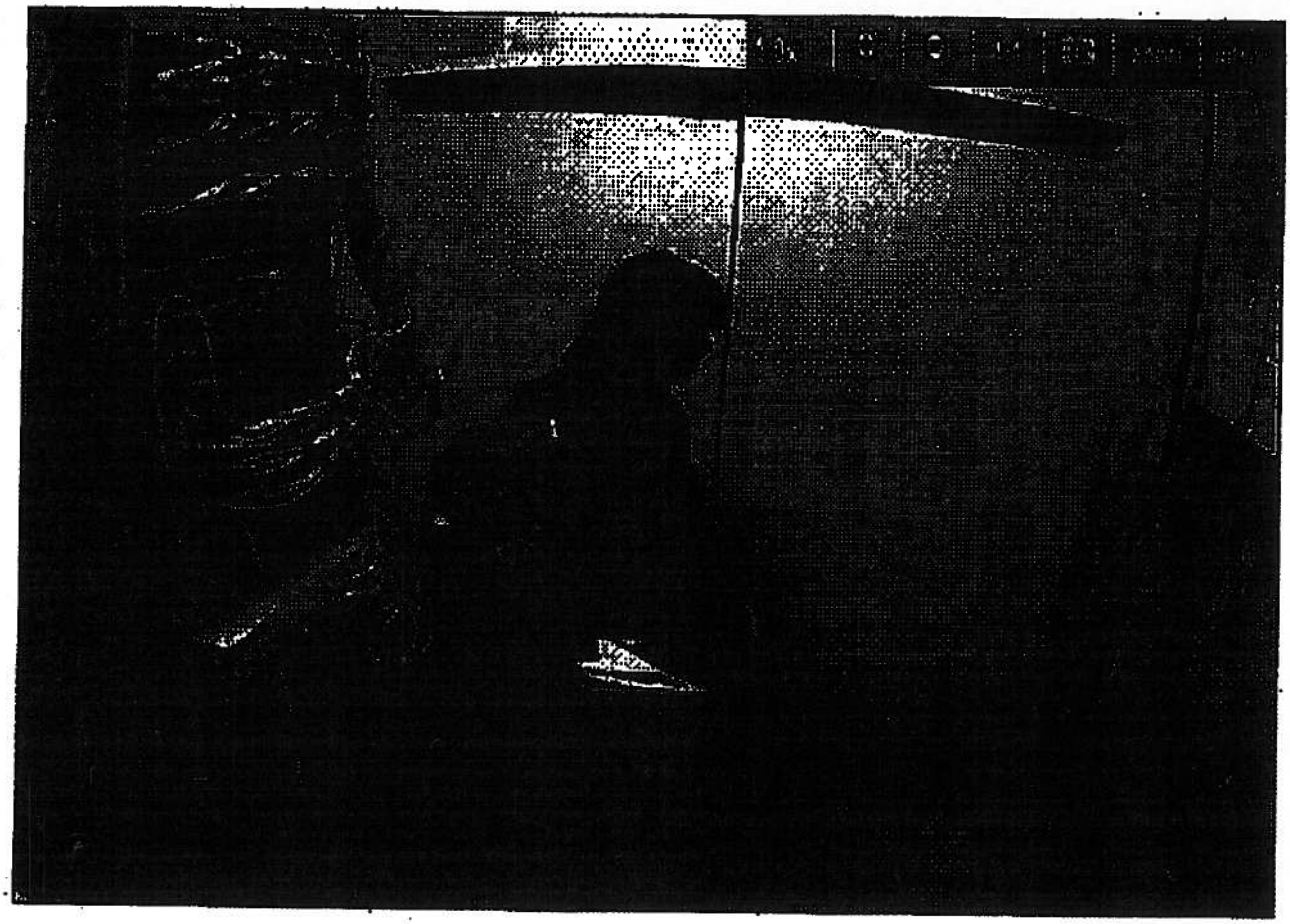
(b)(6),(b)(7)(C)

Begin forwarded message:

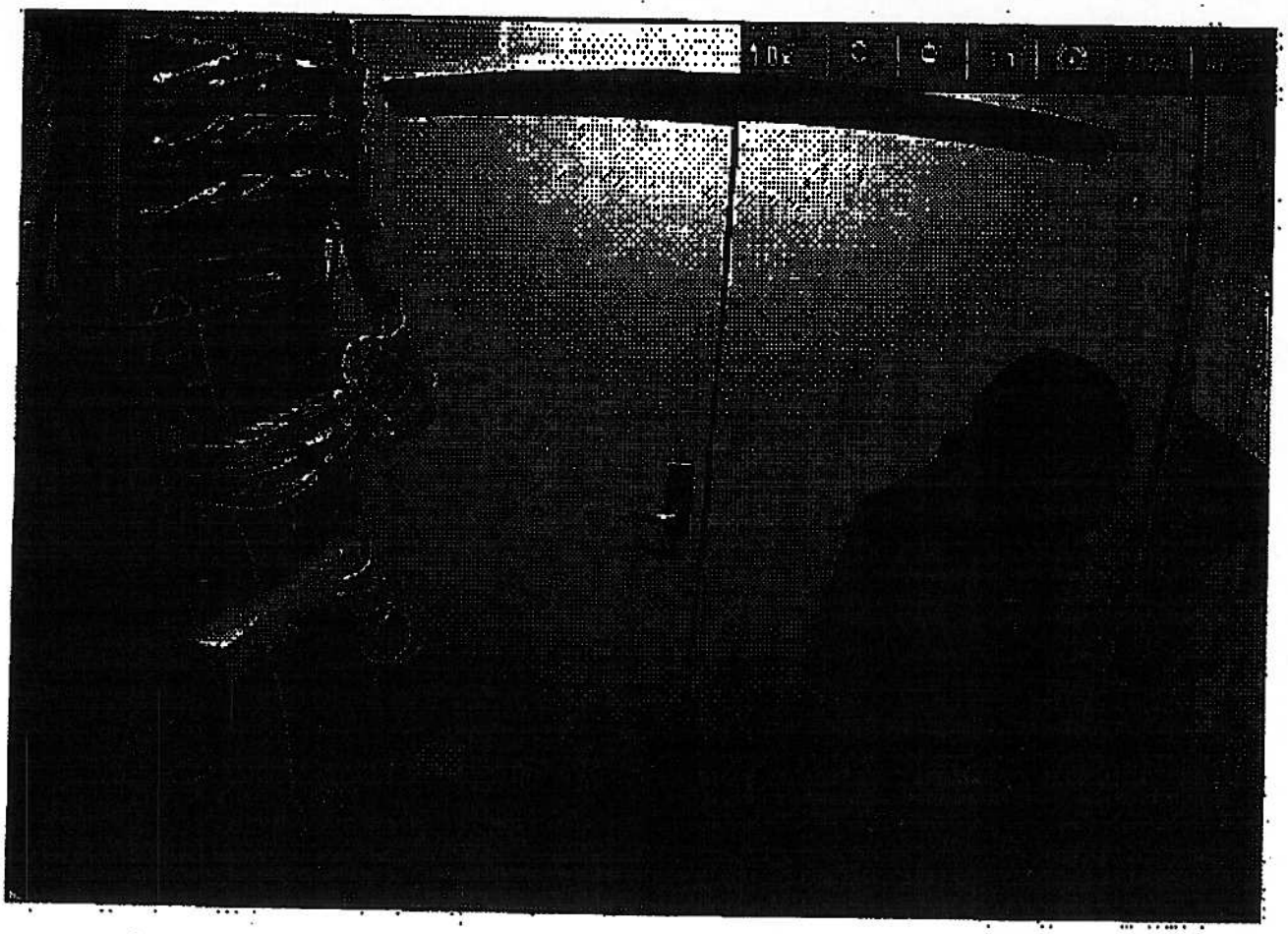
From: (b)(6),(b)(7)(C) mit.edu>
Date: January 4, 2011 3:46:18 PM EST
To: (b)(6),(b)(7)(C) mit.edu>



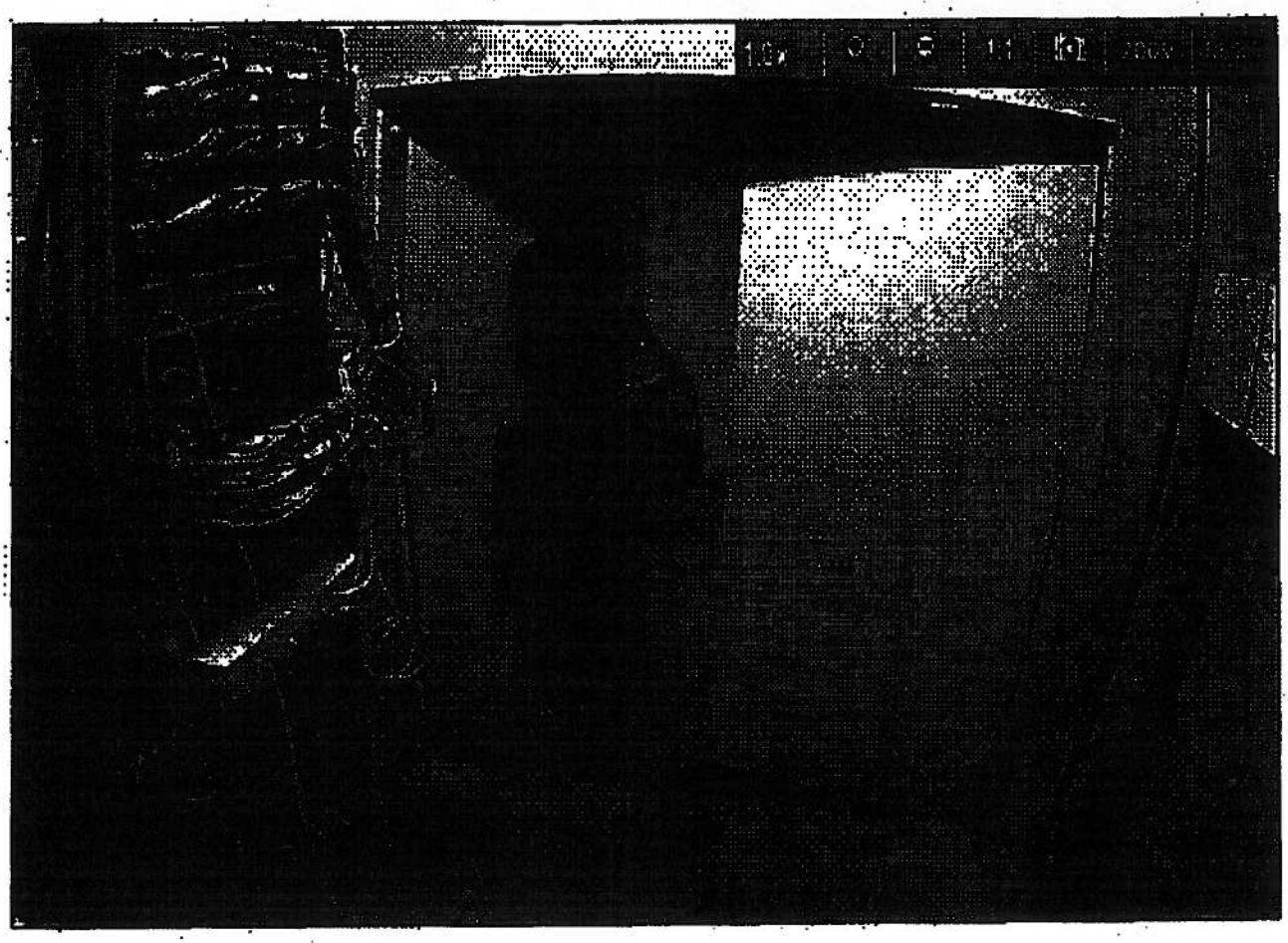
RIF 2538



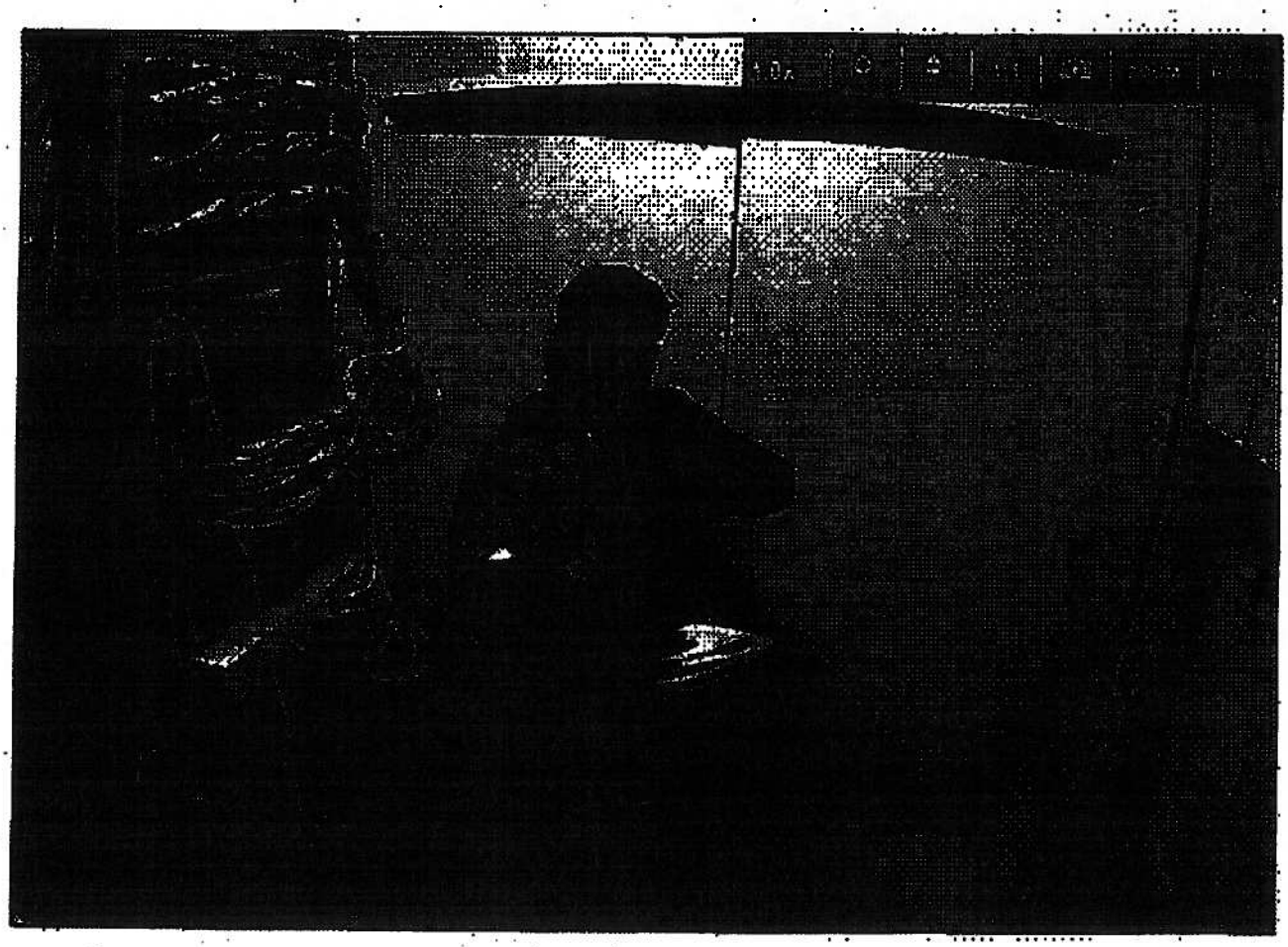
RIF



RIF

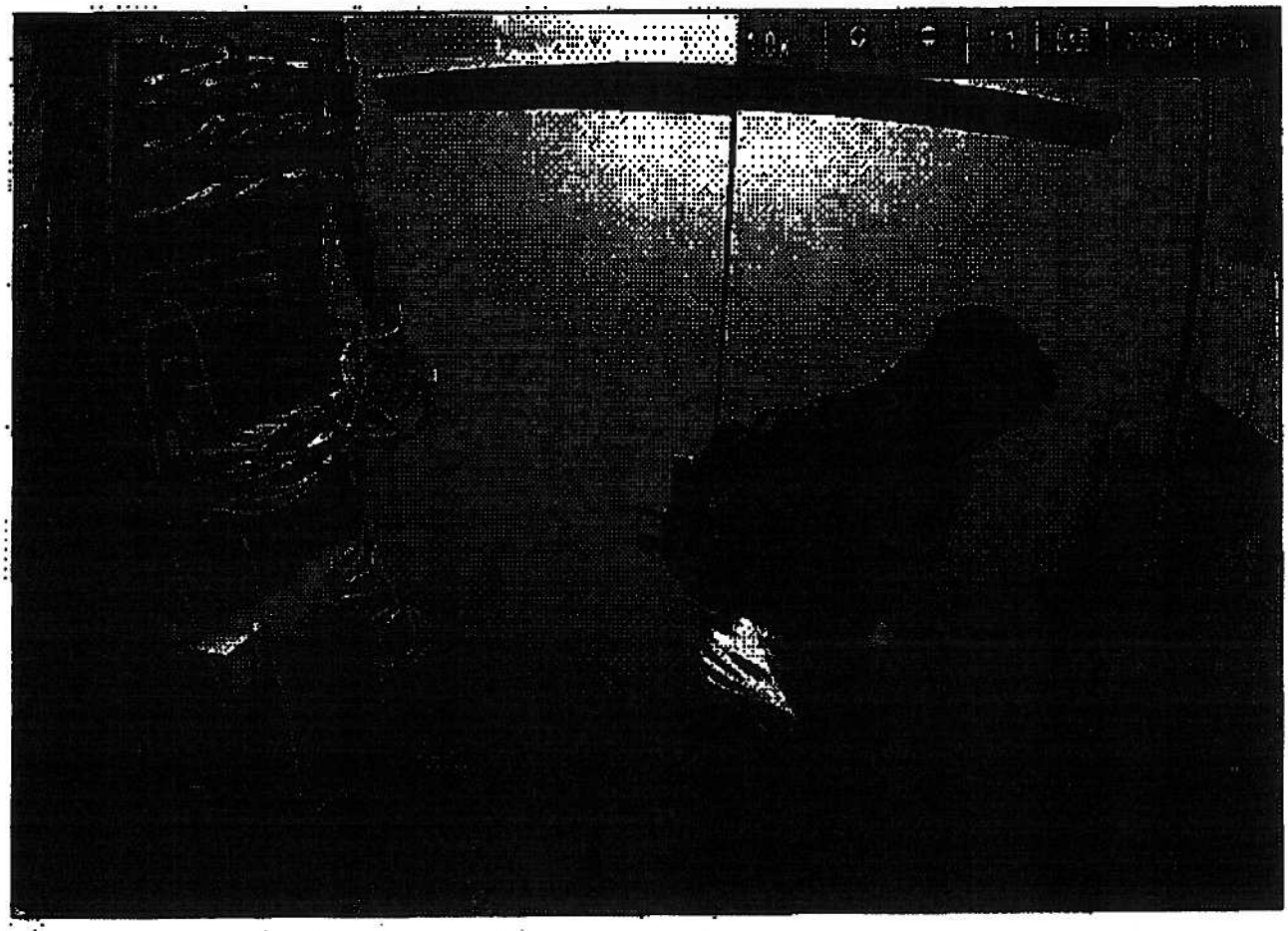


RIF

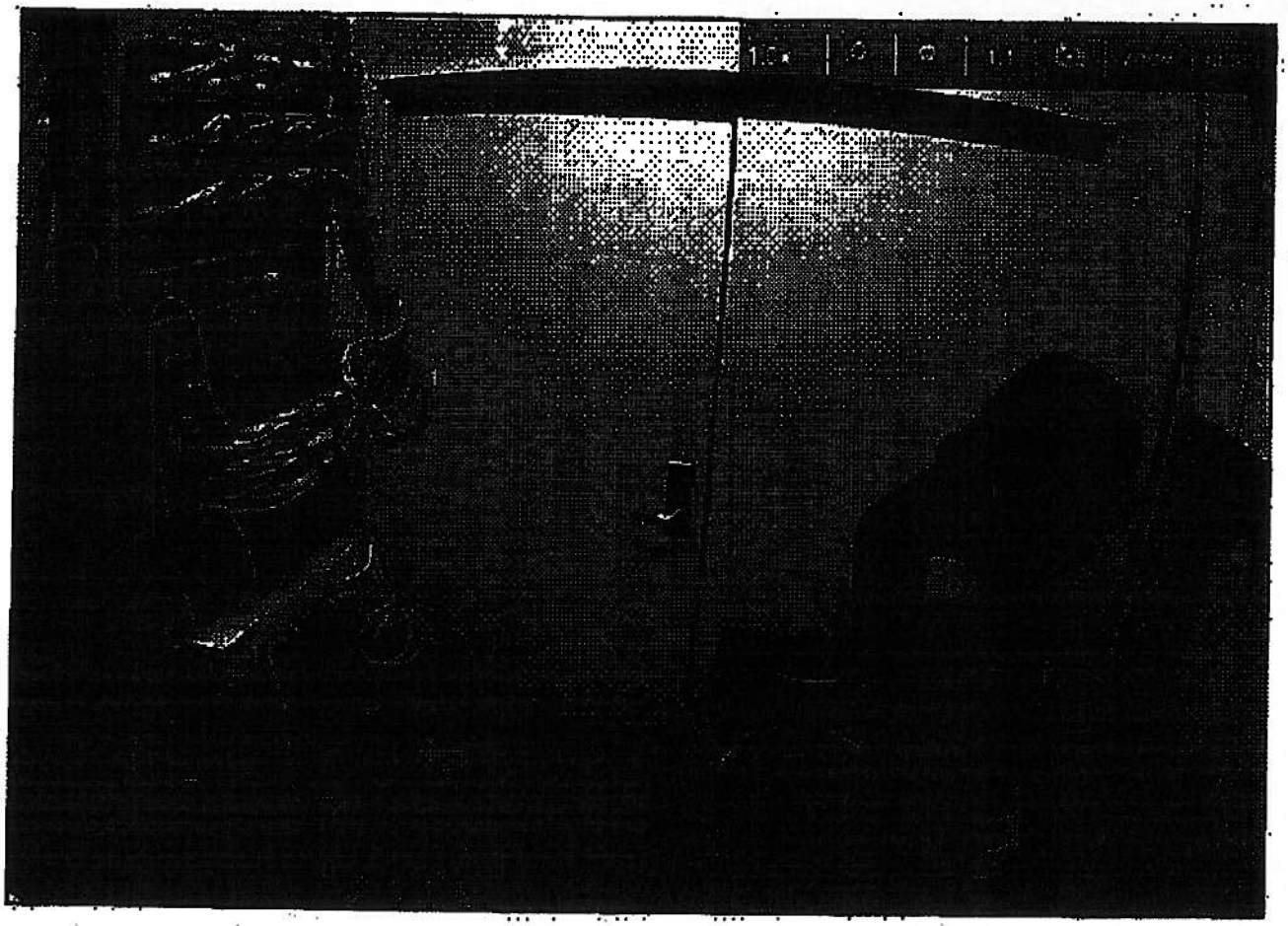


RIF

2542

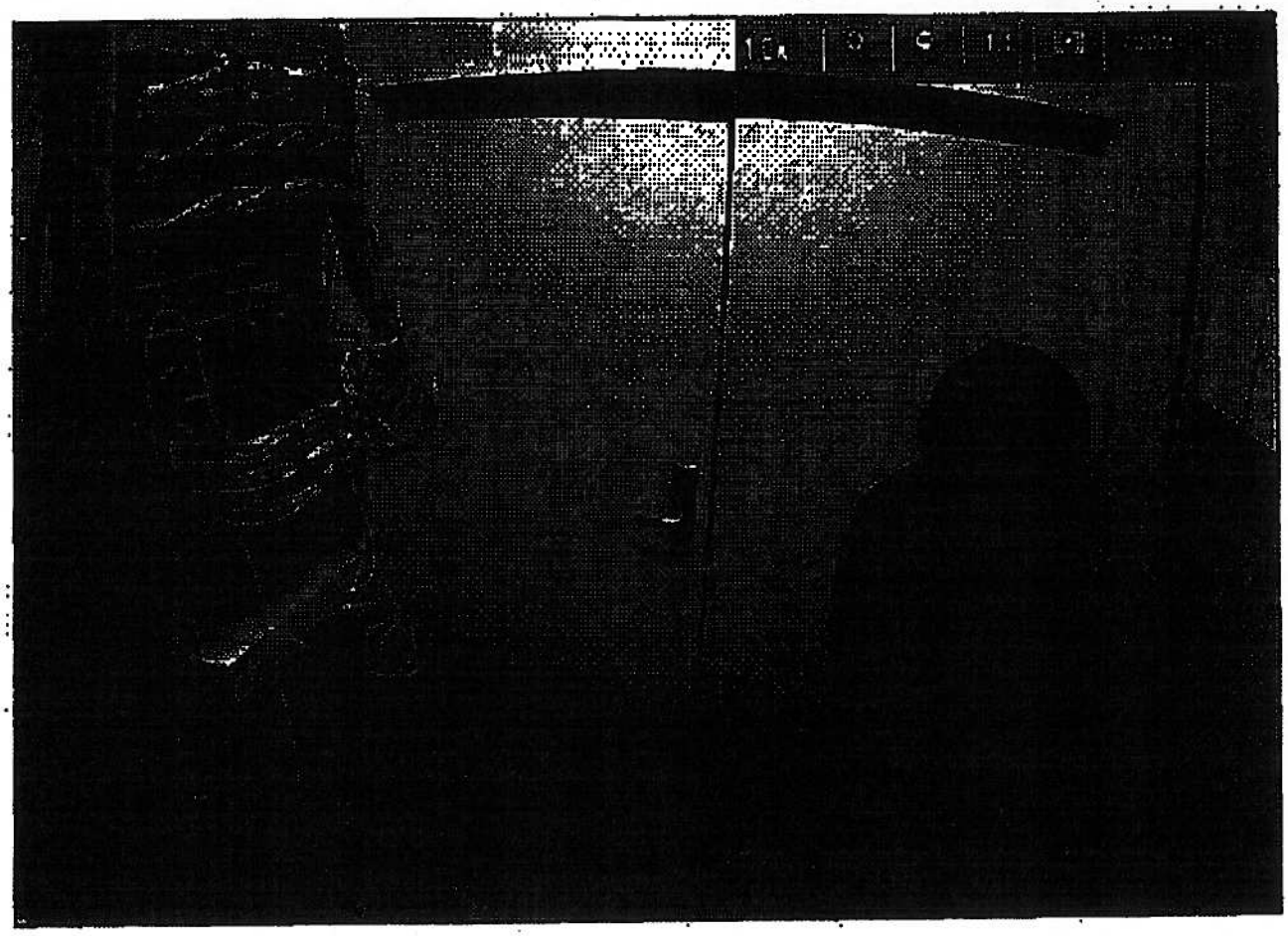


RIF

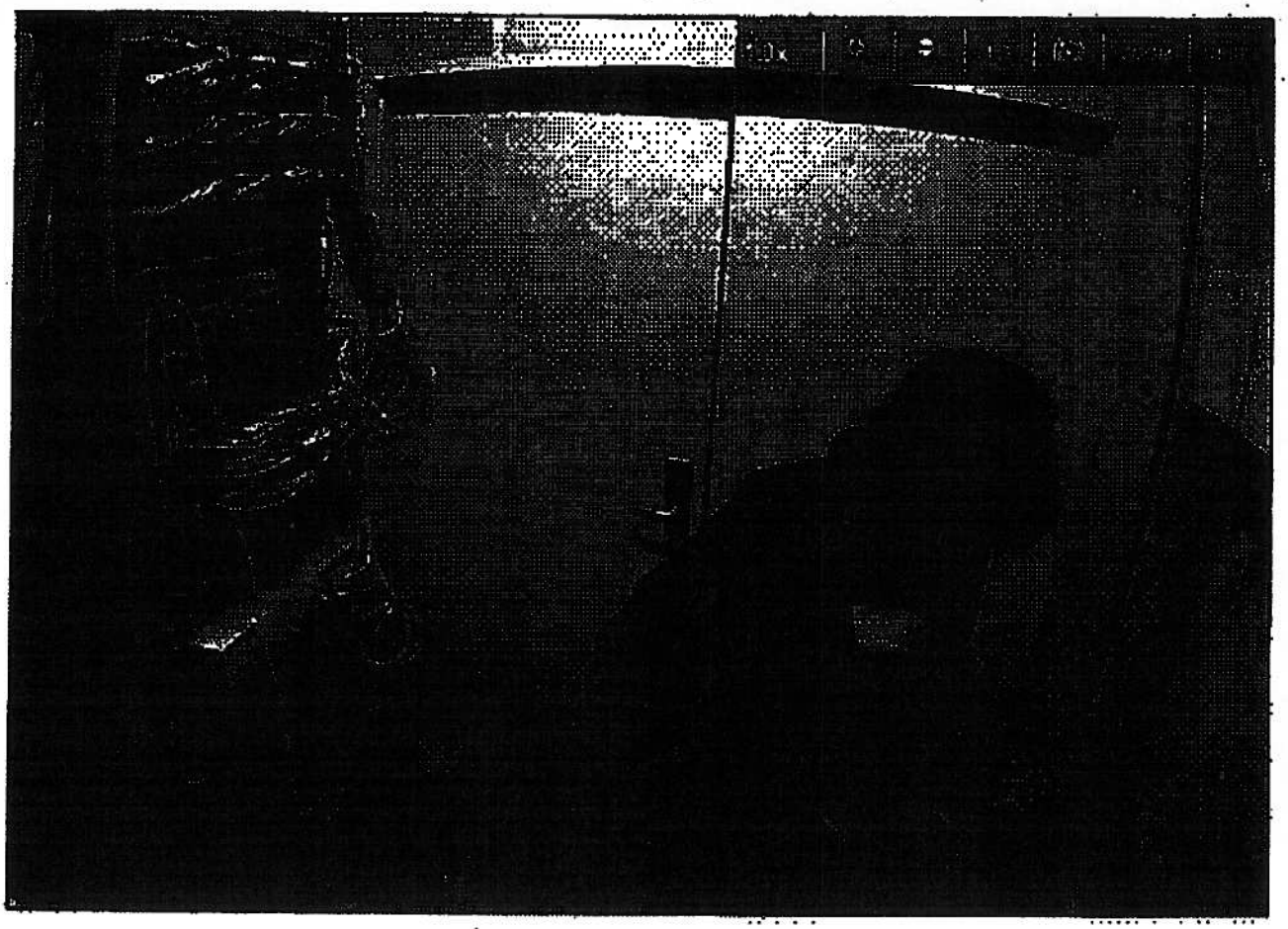


RIF

2544



RIF



RIF

From: (b)(6),(b)(7)(C) cambridgepolice.org>
Sent: Wednesday, January 05, 2011 6:48 AM
To: undisclosed-recipients
Subject: FW: Building 16

Suspect as of yet unidentified.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) MIT.EDU]
Sent: Tuesday, January 04, 2011 3:51 PM
To: (b)(6),(b)(7)(C)
Subject: FW: Building 16

(b)(6), here are the screenshots from the camera setup on the laptop at MIT. Looks like he added a drive, but it is still on the network.

(b)(6),

We did not get the call until he left the room.

From: (b)(6),(b)(7)(C)
Sent: Tuesday, January 04, 2011 3:48 PM
To: (b)(6),(b)(7)(C)
Cc:
Subject: Building 16

Here are screenshots from 3:26pm

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

Information Services & Technology, MIT

(b)(6),(b)(7)(C)

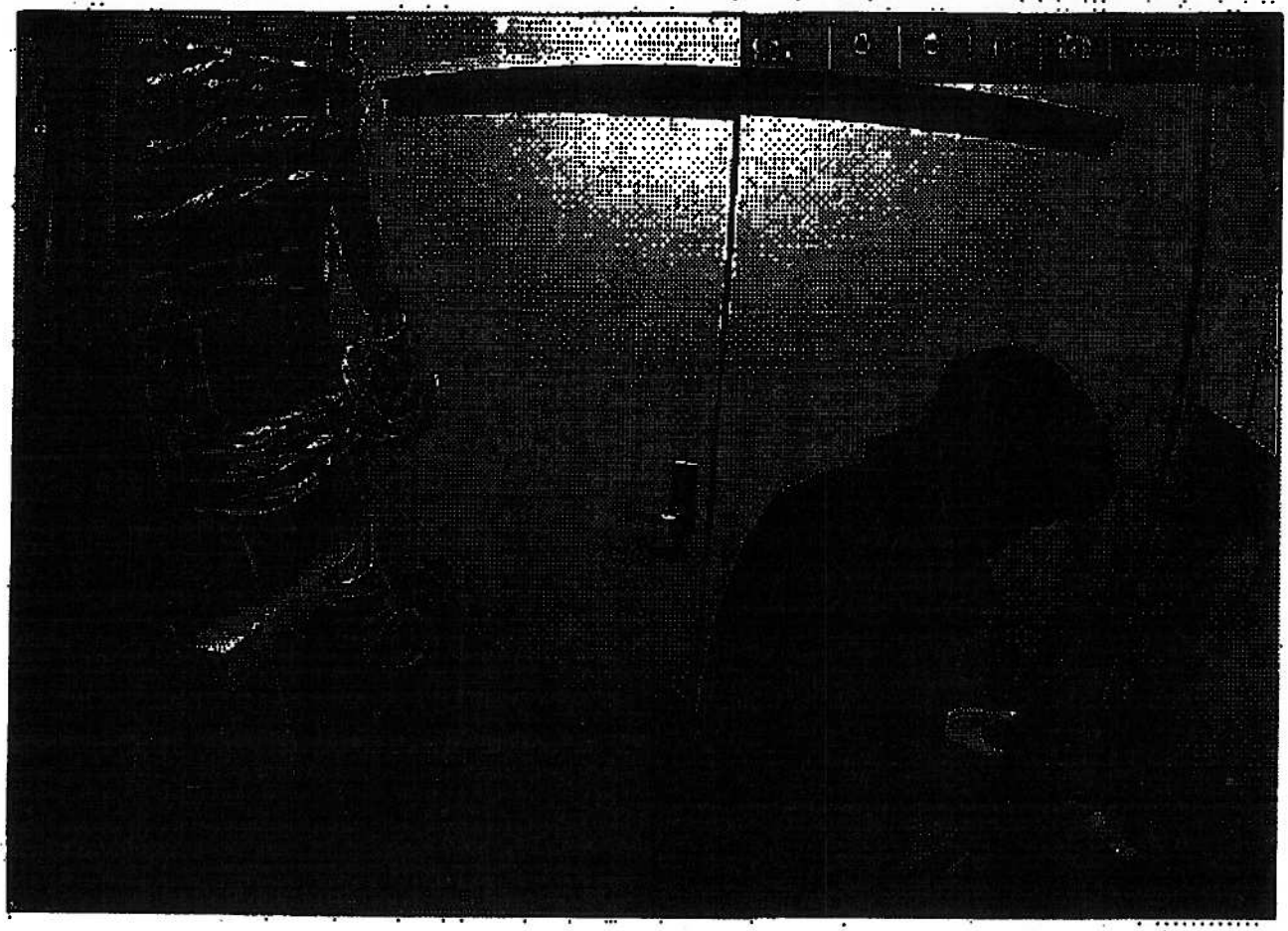
(b)(6),(b)(7)(C) mit.edu

(b)(6),(b)(7)(C)

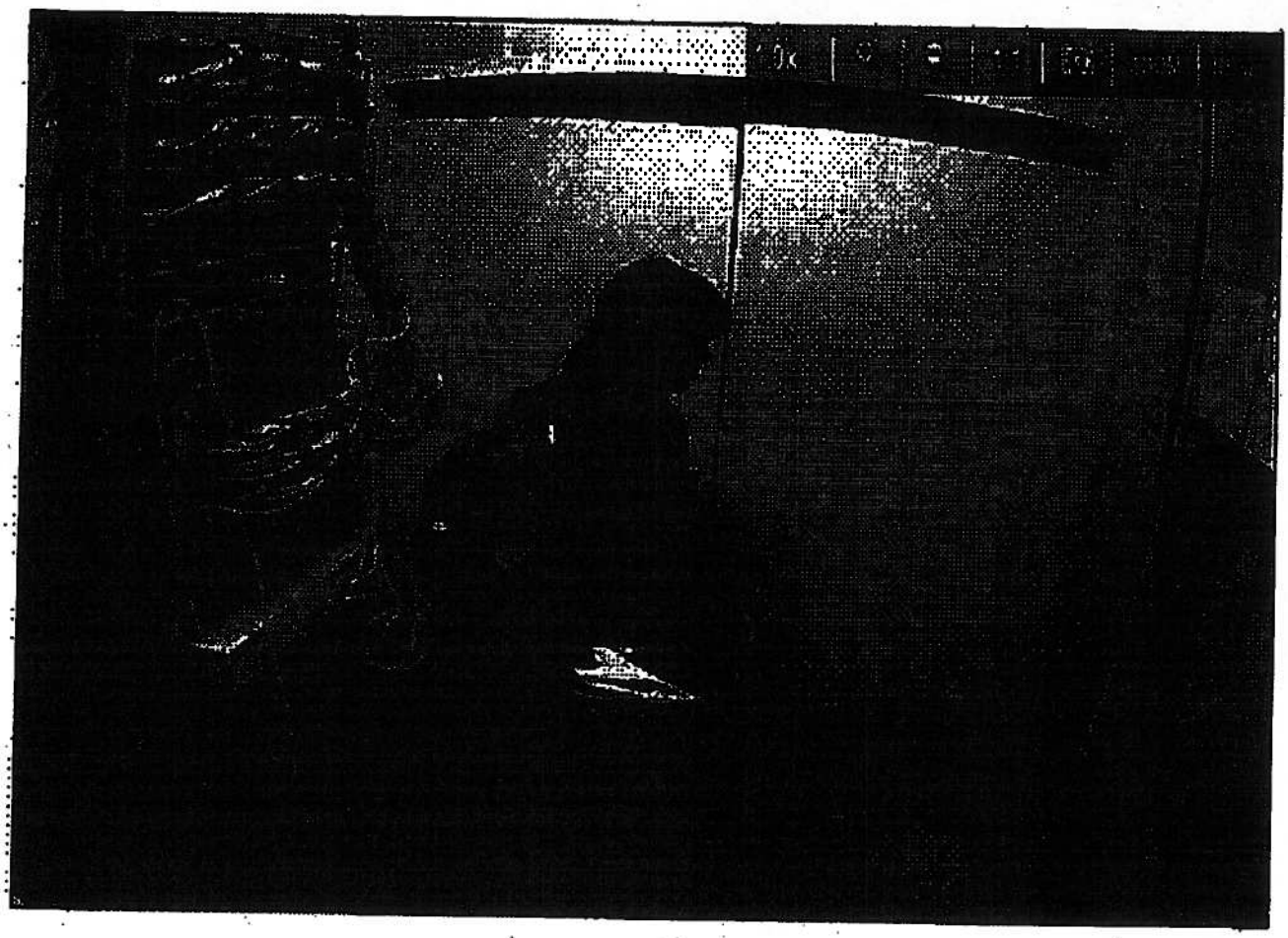
Begin forwarded message:

From: (b)(6),(b)(7)(C) @mit.edu>
Date: January 4, 2011 3:46:18 PM EST
To: mit.edu>

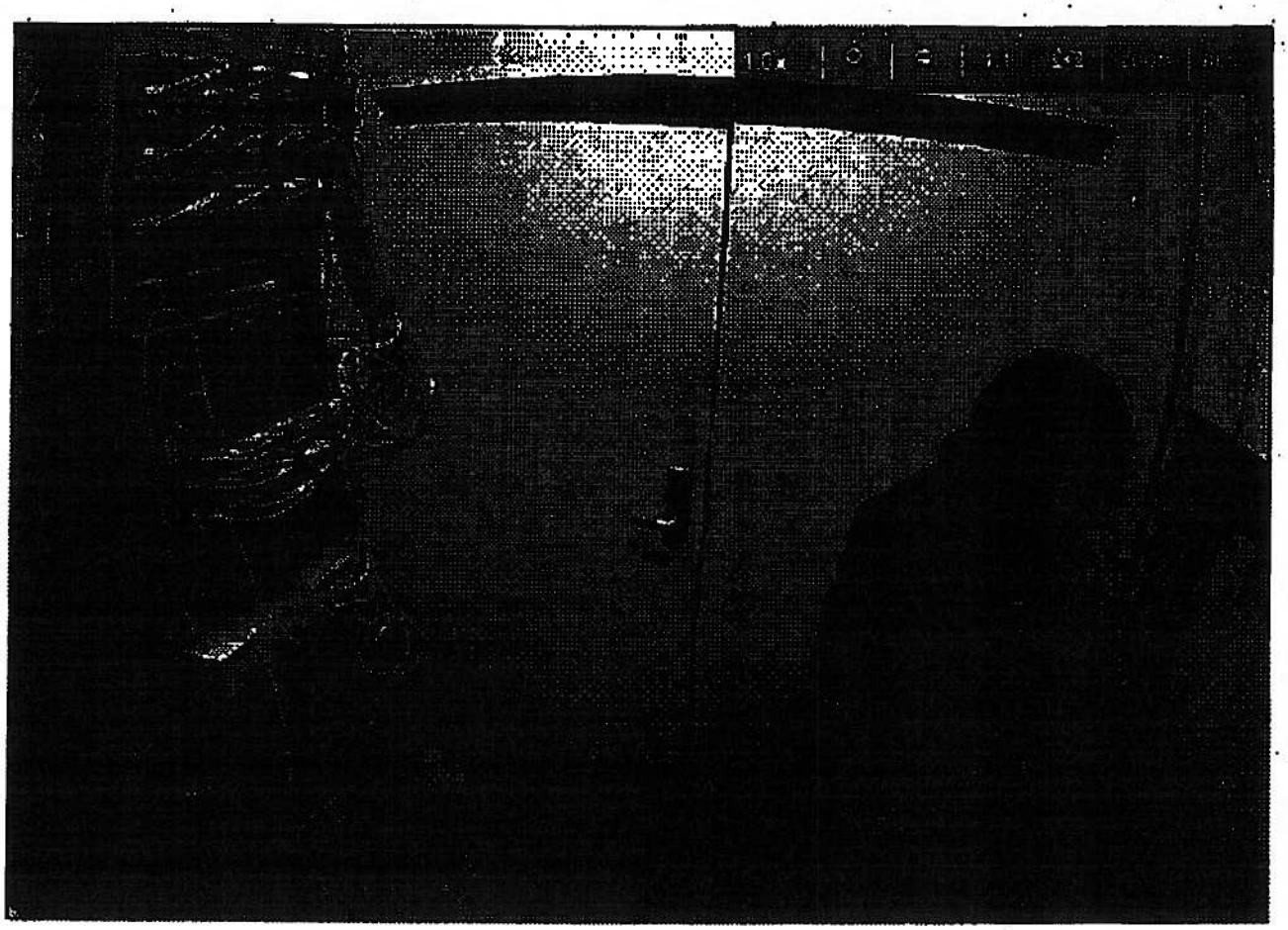
(b)(6),(b)(7)(C)



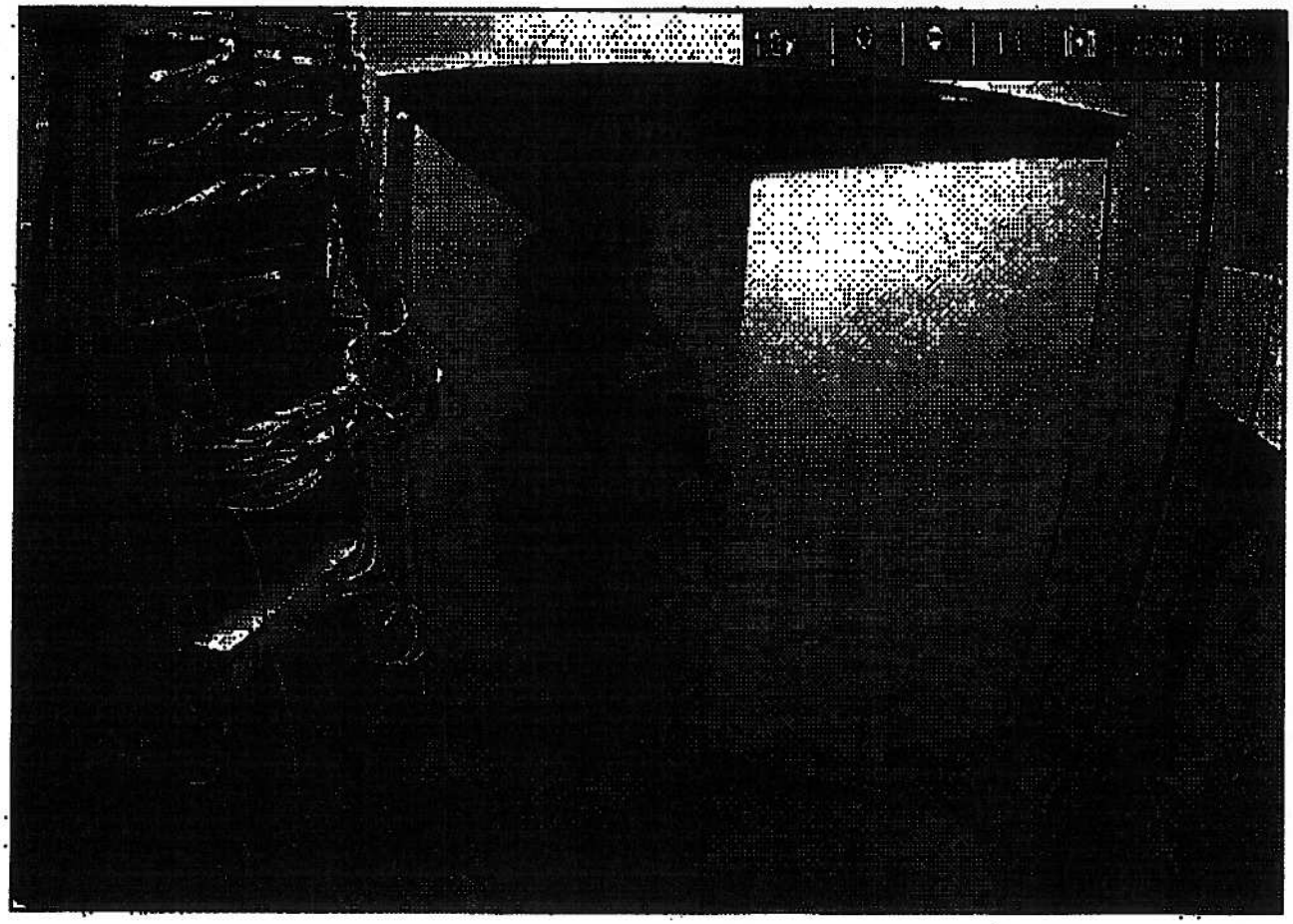
RIF



RIF



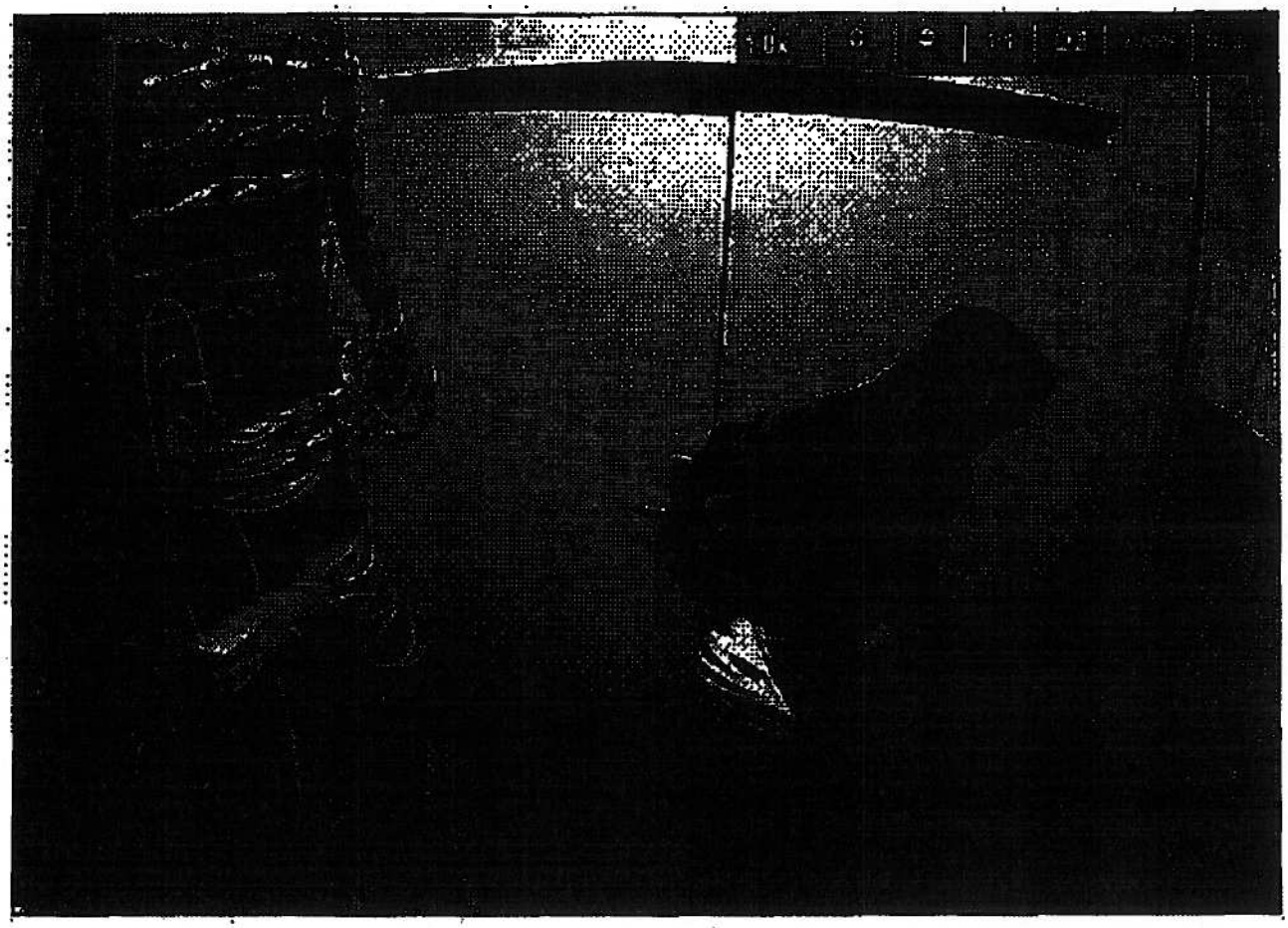
RIF



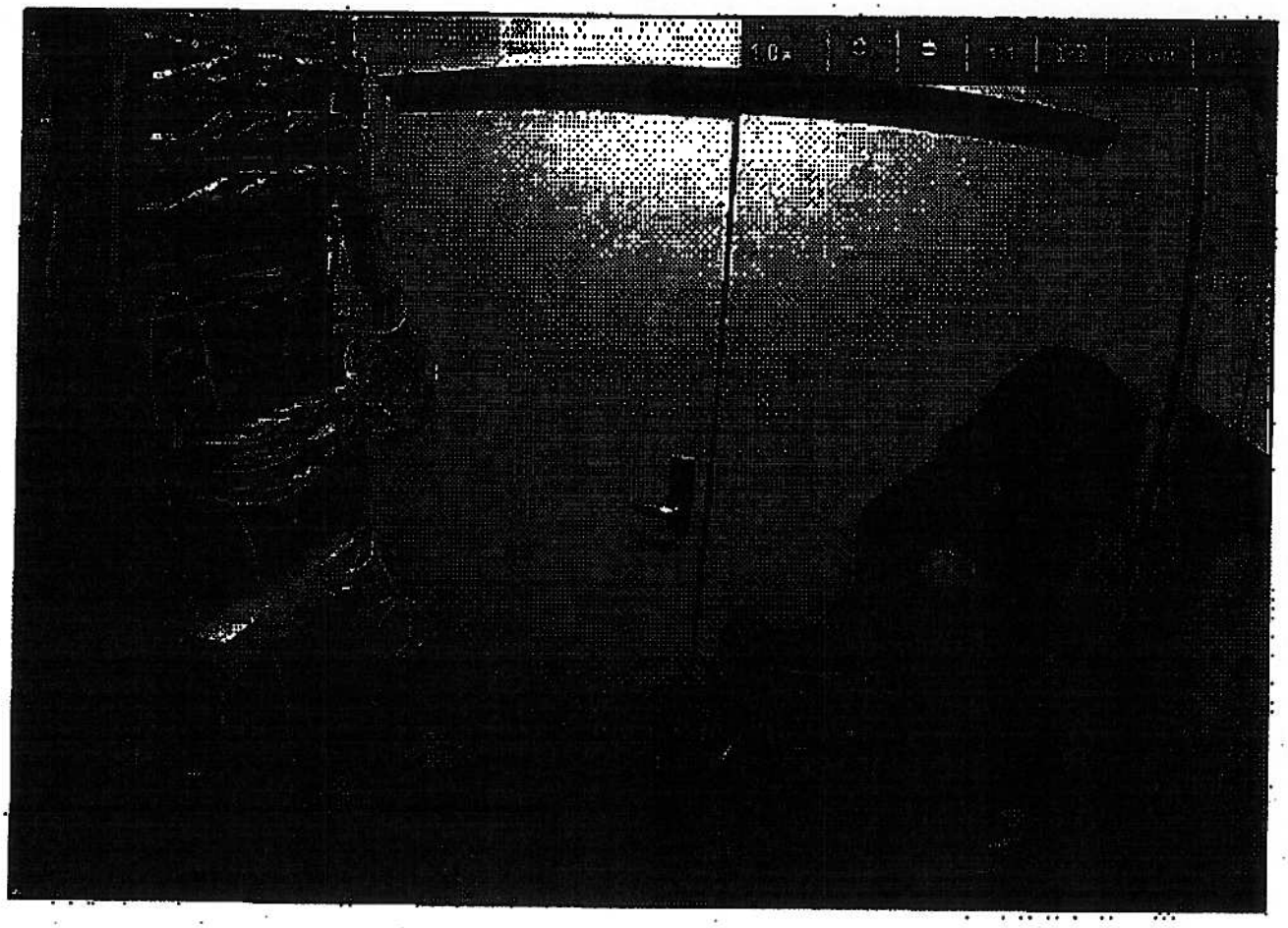
RIF

2551

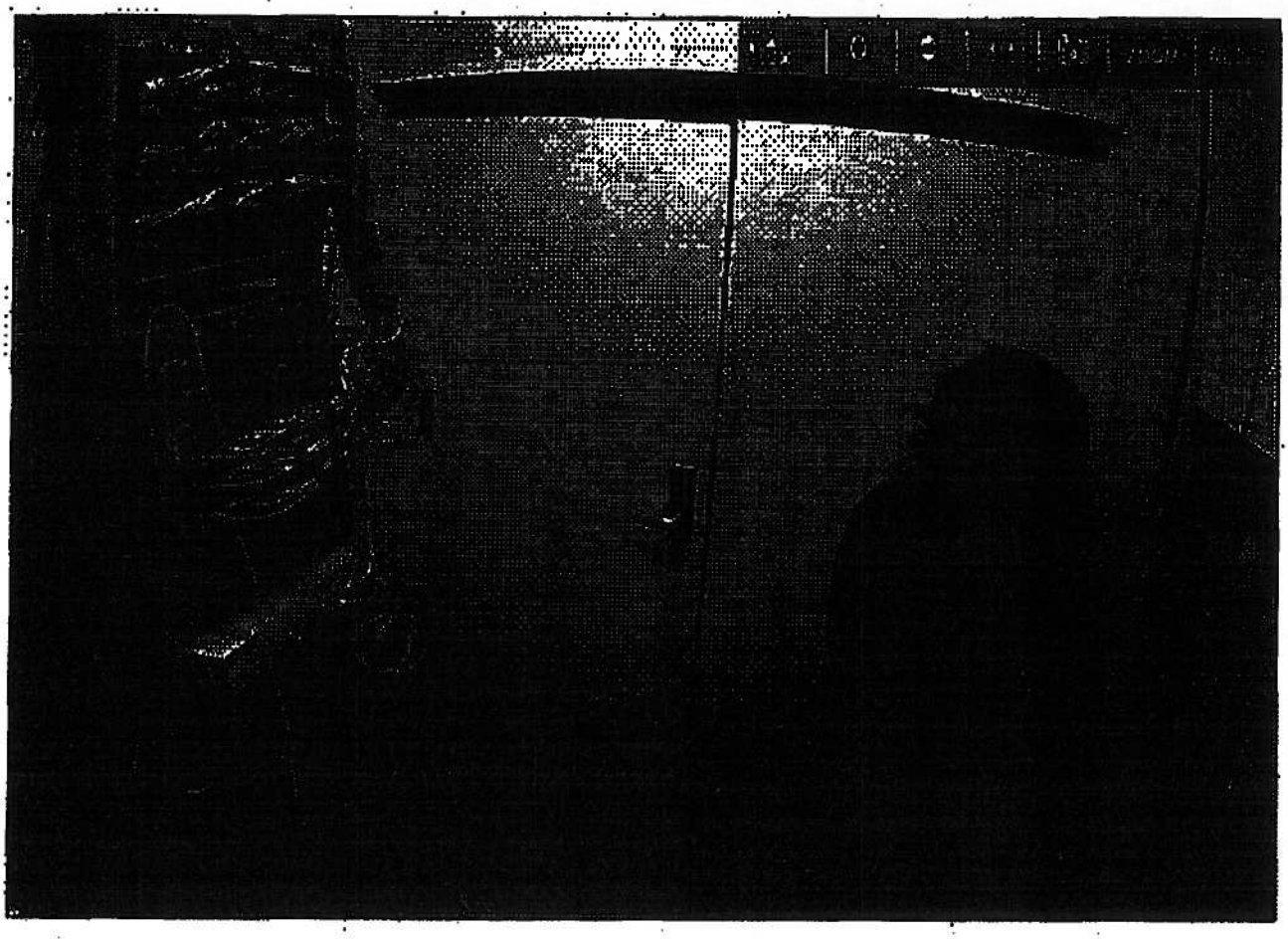
RIF



RIF



RIF



RIF

2555

RIF

2556

From: (b)(6),(b)(7)(C) MIT.EDU>
Sent: Tuesday, January 04, 2011 11:51 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: another response - FW: Re linux box

Hey (b)(6), - not that I know of (to execute a script off a stick); there does exist an autorun configuration utility in Ubuntu, but it's for media files so they'll automagically play (you can specify filetype and player), so not the same notion of autorun as Windows has. But yeah, there exists no way I know of to get a script to autorun off a USB stick upon hotplug.

I'm thinking two things to get a prompt on that machine currently:

a) I'm currently fuzzing CherryPy for the heck of it -- there's no current vuln info on the app; that's a long shot at best...

b) MITM the sshd (might be a winner, if he, or someone else connecting, doesn't spook about fingerprint mismatch) with an sshd that dumps passwords. Or, if last resort, take netbook offline temporarily, mount the disk and grab the host's keys, and set up MITM with those keys so they'll match...

--
(b)(6),(b)(7)(C)
IT Security Systems & Services, IS&T MIT

PGP public key ID (b)(6),(b)(7)(C) http://pgp.mit.edu

On Jan 4, 2011, at 6:29 PM, (b)(6),(b)(7)(C) BOS) wrote:

> You can try with a usb and a cron job script set to open a shell
> window in some versions it may work

>> You wouldn't happen to know where I could find an example of the
>> script to run
>> (b)(6),(b)(7)(C)
>>
>> U.S. Secret Service
>> Boston Field Office
>> (b)(6),(b)(7)(C)
>>
>> -----Original Message-----
>> From: (b)(6),(b)(7)(C) (CHI)
>> Sent: Tuesday, January 04, 2011 6:15 PM
>> To: (b)(6),(b)(7)(C) BOS)
>> Subject: another response - FW: Re linux box
>>
>> From: (b)(6),(b)(7)(C) who is actually one of the NYC TFO's - you could
>> contact him at his vzw addy, or his USSS associate addy:
>> (b)(6),(b)(7)(C) associates.usss.dhs.gov

From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 9:54 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Summary

Thanks (b)(6),(Great work today, again.
(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (BOS)
Cc: External(b)(6),(b cambridgepolice.org; External(b)(6),(b)(7)(C) gcityofboston.gov (b)(6),(b)(7)(C) BOS); (b)(6),(b)(7)(C) BOS)
Sent: Tue Jan 04 18:35:08 2011
Subject: Summary

Unauthorized activity on Massachusetts Institute of Technology network

On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department (b)(6),(b)(7)(C) mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(7 (b)(6),(b)(7)(was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) (b)(6),(b)(7 mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D001001100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP addres (b)(6),(b)(7)(and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing. (b)(6),(b)(7) provided SA (b)(6), with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network.

(b)(6),(b)(7)(C)
U.S. Secret Service

Boston Field Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) (CHI)
Sent: Tuesday, January 04, 2011 7:00 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: RE: Unauthorized activity on Massachusetts Institute of Technology network

Thanks – ok if I share this with my squad? I want to show them how a proper incident response is done!

H.

From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 5:46 PM
To: (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) CID); (b)(6),(b)(7)(C) CID)
Cc: (b)(6),(b)(7)(C) WFO); (b)(6),(b)(7)(C) (CHI); (b)(6),(b)(7)(C) REN)
Subject: Unauthorized activity on Massachusetts Institute of Technology network

FYI

Unauthorized activity on Massachusetts Institute of Technology network
On 01/04/11 Detective (b)(6),(b)(7)(C) of the Cambridge Police Department and a member of the New England Electronic Crimes Task Force received a call from the (b)(6),(b)(7)(C) MIT.EDU) of Massachusetts Institute of Technology Police that an unauthorized computer had been found in a wire closet on MIT grounds and Network Traffic suggested that the computer was being used to download technical journals. The computer was found in a wire closet of in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue) which has MIT Biological Engineering Department. (b)(6),(b)(7)(C) mit.edu), an (b)(6),(b)(7)(C) Security Analyst for MIT stated that on 01/03/11 the library had notified him that someone was downloading large numbers of journals from the library without authorization. Large amounts of unauthorized downloading was first noticed by the library on 09/29/10 and on 11/23/10 there was another incident of excessive downloading. From 01/03/11 to 01/04/11 (b)(6),(b)(7) (b)(6),(b)(7) was able to trace the activity to a particular switch in the wire closet. When (b)(6),(b)(7)(C) (b)(6),(b)(mit.edu) when to examine the wire closet he found the unauthorized computer connected to the switch. An external hard drive was connected to the netbook. The netbook was an Acer Aspire One with a serial number LUSAX0D0010011100E1601. The netbook matches the description of an Acer netbook (b)(6),(b)(7)(C) reported as stolen to MIT Police on 12/31/10. The netbook appeared to be using two IP address (b)(6),(b)(7)(and (b)(6),(b)(7)(C) which are IP address belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open . Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 that is often associated with TCP (Transmission Control Protocol) traffic. Cambridge Police processed the scene for prints. Stickers on the outside of the netbook showed that it was originally loaded with Windows 7 starter edition but an examination of the screen indicated that the current operating system was Ubuntu, a type of Linux. The login screen showed a computer name of "ghost-laptop" with the user "Gene Host" logged in. The login screen had a password. All efforts to bypass the login screen were futile (b)(6),(b)(7)(C) started a wireshark packet capture of traffic on the switch around 9AM on 01/04/11 and the packet capture is continuing (b)(6),(b)(7)(provided SA (b)(6),(with a copy of flow traffic on the network. The flow traffic is currently being uploaded to the CERT dropbox. MIT decided to leave the netbook running in place with the hopes of capturing more network traffic to show if a suspect was controlling the netbook through a SSH channel and if the network traffic can show where the suspect is controlling the netbook from. MIT placed a camera in the wire closet to observe if the suspect returns for the netbook. MIT also established an alarm to notify MIT if the netbook is removed from the network. The technical journals being downloaded have a monetary value. All MIT students have access to view the journals but are limited as to how much they can download and anyone outside of MIT including students after they graduate have to pay a substantial subscription to access the files. The price for downloading one file can vary from $200.00 to $3,000.00. Total value of the downloaded files could be in excess of $50,000.00.

(b)(6),(b)(7)(C)

U.S. Secret Service
Boston Field Office

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, January 04, 2011 6:07 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Fw: Person Inquiry

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Sent: Tue Jan 04 10:13:04 2011
Subject: RE: Person Inquiry

(b)(6), (b)(7)(C)

Can you give me a buzz? I have a crazy one to run by you.

I tried the number I had for you, it is not working.

(b)(6),(b)(7)(C)

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C) cambridgepolice.org]
Sent: Friday, December 10, 2010 2:22 PM
To: (b)(6),(b)(7)(C)
Subject: Re: Person Inquiry

Be very afraid

From: (b)(6),(b)(7)(C) MIT.EDU>
To: (b)(6),(b)(7)(C)
Sent: Fri Dec 10 13:34:43 2010
Subject: Re: Person Inquiry

I am almost afraid to check the site. You have a good weekend as well.

(b)(6),(b

Sent from my HTC on the Now Network from Sprint!

----- Reply message -----
From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Date: Fri, Dec 10, 2010 12:44 pm
Subject: Person Inquiry
To: (b)(6),(b)(7)(C) mit.edu>

Hi (b)(6),(

Originally her name came across my desk from IRS, there is some financial activity that triggered us to look at her. The banking address had her out of a Cambridge address.

It has to do with her little side business.

(b)(6),(b)(7)(C)

Believe it or not she is making a few extra bucks. In my IRS Task Force capacity I am not sure if we'll take action since she is claiming her income but I still might refer the case out to Vice.

Life is stranger than fiction.

Thanks for the follow up information, have a good weekend.

(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)MIT.EDU]
Sent: Friday, December 10, 2010 11:48 AM
To: (b)(6),(b)(7)(C)
Subject: RE: Person Inquiry

I am not sure the rules of keeping email addresses--She is a (b)(6),(b graduate and our Alumni listing has her living in (b)(6),(b)(7)(C) no exact address given. She also has an association with our radio station (WMBR) which is in the basement of Walker Memorial (corner of Mem and Ames).

Hope this helps.

(b)
(6),(b

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)cambridgepolice.org]
Sent: Thursday, December 09, 2010 1:24 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Person Inquiry

(b)(6),
(b)(7)(C

Sorry, I assumed she was an employee since she uses (b)(6),(b)(7)(C) mit.edu as an email address. Do alumni get to keep their email address account?

Thanks

(b)(6),
(b)(7)(

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)MIT.EDU]
Sent: Thursday, December 09, 2010 12:35 PM
To: (b)(6),(b)(7)(C)
Subject: RE: Person Inquiry

(b)(6),
(b)(7)(

I do not have one in the current employee or student directory. These are the (b)(6),(b)(7)(C) have:

What is the email address she is using? I may be able to look at that way. She could work at MIT as a contractor, temp or some other capacity. I will check to see if she has an MIT ID.

(b)(6),(b)(7)(C)

There were 17 matches to your request.

(b)(6),(b)(7)(C)

MIT Affiliate
..Non-Institute Harvard, year G
.....Health Sciences & Technology, year G
...Technology Licensing Office
..Lincoln Laboratory
MIT Affiliate
Computer Science & Artificial Intelligence Lab
Technology Review
.MIT Affiliate
...Dept of Electrical Engineering & Computer Science
..MIT Affiliate
Dept of Earth, Atmospheric, & Planetary Sciences
...Harvd-MIT Division of Health Sciences & Technology
....Office of the Provost
...MIT Affiliate
...Management, year G
....Department of Biology

Student data loaded as of Dec 9, Staff data loaded as of Dec 9.

From: (b)(6),(b)(7)(C) [mailto:(b)(6),(b)(7)(C)@cambridgepolice.org]
Sent: Thursday, December 09, 2010 12:04 PM
To: (b)(6),(b)(7)(C)
Subject: Person Inquiry

Hi (b)(6),(b)(7)(C)

Can you give me some biographical info on the attached person?

Thanks

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) @cambridgepolice.org>
Sent: Tuesday, January 04, 2011 6:06 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Name of MIT Contact

(b)(6),(b)(7)(C) at MIT PD do you need his info?

From: (b)(6),(b)(7)(C) (BOS) (b)(6),(b)(7)(C) @usss.dhs.gov>
To: (b)(6),(b)(7)(C)
Sent: Tue Jan 04 17:27:32 2011
Subject: Name of MIT Contact

Who was the first person to contact you from MIT
(b)(6),(b)(7)(C)

Sent from Blackberry

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

From: (b)(6),(b)(7)(C) (CID)
Sent: Tuesday, January 04, 2011 2:50 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C) (CID); (b)(6),(b)(7)(C)
Cc: (b)(6),(b)(7)(C) (CID)
Subject: MIT

It was forwarded to CIS that you are responding to an intrusion case at MIT. If you need any assistance give us a call at (b)(6),(b)(7)(C) Or our BBs after hours. Good Luck.

(b)(6),(b)(7)(C)

From: (b)(6),(b)(7)(C) pcert.org>
Sent: Tuesday, January 04, 2011 2:21 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Instructions to Use CERT FTP Dropbox
Attachments: secure_ftp_server_dropbox_submission_instructions.doc

(b)(6),(b)(7)(C)

Please refer to the attached document to submit data to CERT.

From: (b)(6),(b)(7)(C) (WAC)
Sent: Tuesday, January 04, 2011 1:24 PM
To: (b)(6),(b)(7)(C) (BOS); (b)(6),(b)(7)(C) (WFO)
Subject: Re: Live Capture of Linux Box with out Admin Rights

Sounds like a (b)(6),(b)(7)(C) expertise area...
(b)(6),(b)(7)(C)
*** Sent from Blackberry ***

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: ecsap (b)(6),(b)(7)(C) (CID)
Sent: Tue Jan 04 13:12:30 2011
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (CID)
Sent: Tuesday, January 04, 2011 1:21 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: Live Capture of Linux Box with out Admin Rights

Mike:

We're discussing it here.

(b)(6),(b)(7)(C)
Special Agent
U.S. Secret Service
(b)(6),(b)(7)(C) (Desk)
(Mobile)
412-268-5226 (Fax)

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: ecsap (b)(6),(b)(7)(C) (CID)
Sent: Tue Jan 04 13:12:30 2011
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (WFO)
Sent: Tuesday, January 04, 2011 1:19 PM
To: (b)(6),(b)(7)(C) BOS)
Subject: Re: Live Capture of Linux Box with out Admin Rights

Not likely (b)(7)(E)
(b)(7)(E)

Regards,
(b)(6),(b)(

----- Original Message -----
From: (b)(6),(b)(7)(C) BOS)
To: ecsap (b)(6),(b)(7)(C) (CID)
Sent: Tue Jan 04 13:12:30 2011
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (REN)
Sent: Tuesday, January 04, 2011 1:18 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Live Capture of Linux Box with out Admin Rights

Can you log in as a different user? The user root has no password by default on ubuntu.

(b)(6),(b)(7)(C)

Reno Resident Office
(b)(6),(b)(7)(C) Office
Cell

-----Original Message-----
From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 10:13 AM
To: ecsap; (b)(6),(b)(7) (CID)
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (CHI)
Sent: Tuesday, January 04, 2011 1:17 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Live Capture of Linux Box with out Admin Rights

Ok - stand by....

(b)(6),(b)(7)(C)

ASSISTANT TO THE SPECIAL AGENT IN CHARGE US SECRET SERVICE CHICAGO FIELD OFFICE

-----Original Message-----
From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 12:16 PM
To: (b)(6),(b)(7)(C) (CHI)
Subject: Re: Live Capture of Linux Box with out Admin Rights

Sure

(b)(6),(b)(7)(C)

Sent from Blackberry

----- Original Message -----
From: (b)(6),(b)(7)(C) (CHI)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Tue Jan 04 13:14:58 2011
Subject: RE: Live Capture of Linux Box with out Admin Rights

I can blast this out on the HTCC and CFID boards (with the victim name redacted) if you want. Would you like me to do that?

(b)(6),(

-----Original Message-----
From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 12:13 PM
To: ecsap (b)(6),(b)(7)(C) (CID)
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (CHI)
Sent: Tuesday, January 04, 2011 1:15 PM
To: (b)(6),(b)(7)(C) (BOS)
Subject: RE: Live Capture of Linux Box with out Admin Rights

I can blast this out on the HTCC and CFID boards (with the victim name redacted) if you want. Would you like me to do that?

H.

-----Original Message-----
From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 12:13 PM
To: ecsap-(b)(6),(b)(7)(C) (CID)
Subject: Live Capture of Linux Box with out Admin Rights

I have an Acer Aspire that has some version Ubuntu loaded on it. It is physically patched into a switch at MIT and has been downloading technical journals from the Network. The laptop is on but the login screen has a password. Does anyone know a way to capture the RAM or live image with out logging in or a way to bypass the login password in Linux?

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 11:44 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: MIT

Call me when you get a chance

----- Original Message -----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7) (BOS)
Sent: Tue Jan 04 11:04:32 2011
Subject: MIT

(b)(6),(b)(7)(C) and I are in route to MIT

(b)(6),(b)(7)(C)

Sent from Blackberry

From: (b)(6),(b)(7)(C) (BOS)
Sent: Tuesday, January 04, 2011 11:18 AM
To: (b)(6),(b)(7)(C) (BOS)
Subject: Re: MIT

(b)(6),(b)(7)(C) just told (b)(6),(b)(7)(C)

---- Original Message ----
From: (b)(6),(b)(7)(C) (BOS)
To: (b)(6),(b)(7)(C) (BOS)
Sent: Tue Jan 04 11:04:32 2011
Subject: MIT

(b)(6),(b)(7)(C) and I are in route to MIT

(b)(6),(b)(7)(C)

Sent from Blackberry