Digital Forensics Research Workshop Challenge 2009

Wouter van Dongen, Alain van Hoof

Research Project 2

1 July 2009

- **Introduction**
  - Challenge details
  - Research questions
- **Method**
- **Time zones and Linux time stamps**
- **SSH traces**
- **Recovery of deleted files**
- **The big picture**
- **Questions**

Challenge details

- Connecting from an IP adress in New Orleans
- Advanced knowledge of Linux and digital forensics

NSSAL (Suspect)

Captured: March 11, 2009

Thumb drive

FAT16
512 MB

PS3

Linux Ubuntu 8.10
EXT3 10 GB

Physical Mem

240 MB

PCAP 1

Early surveillance

PCAP 2

Make illicit Mardi Gras images available to other ps3 users

- Baltimore

PCAP 1

PS3

Linux Ubuntu 8.10
EXT3 10 GB

JHUISI (John Hopkins University)

Research questions

1. What relevant user activity can be reconstructed from the available forensic data and what does it show?

2. Is there evidence of inappropriate or suspicious activity on the system?

3. Is there evidence of collaboration with an outside party? If so, what can be determined about the identity of the outside party? How was any collaboration conducted?

4. Is there evidence that illicit data (specifically, Mardi Gras images) was exchanged? If so, what can be determined about that data and the manner of transfer?

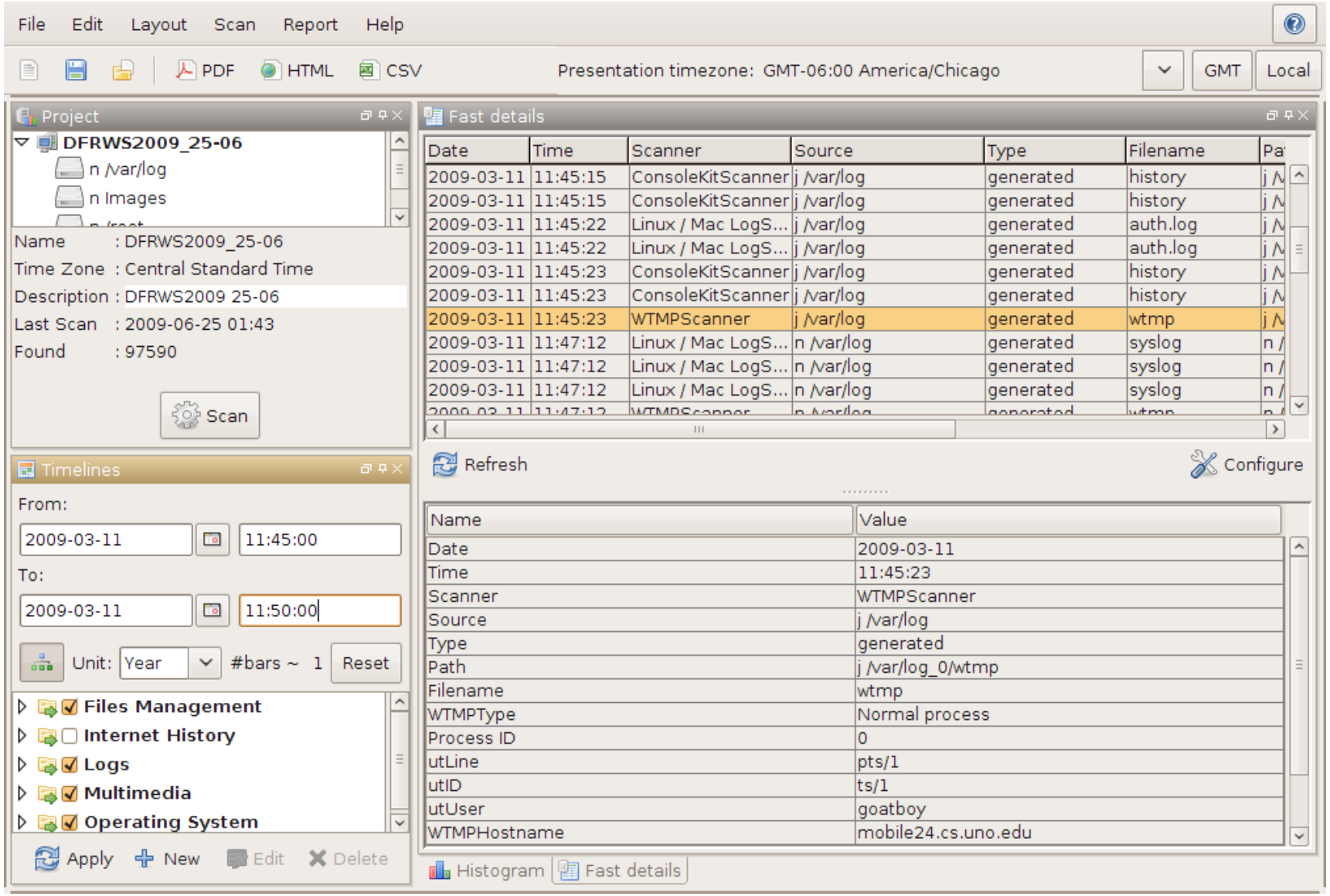
5. What data (if any) was provided by the Johns Hopkins PS3?

6. The suspect claims that he was not responsible for any transfer of data. What evidence do you have to show that remote, unauthorized access to the system might have occurred, and does this evidence exonerate the suspect?

Method (1)

- Standard Linux commands on read-only mounted images
- Additional Linux utilities
- Restored images on Playstation 3 to observe and test behaviour
- Aftertime to parse and export 100,000 log entries of both systems
- Excel to quickly filter and search
- Created timeline

Method (2)


File Edit Layout Scan Report Help
PDF HTML CSV
Presentation timezone: GMT-06:00 America/Chicago
GMT Local
Project
DFRWS2009_25-06
n /var/log
n Images
Name : DFRWS2009_25-06
Time Zone : Central Standard Time
Description : DFRWS2009 25-06
Last Scan : 2009-06-25 01:43
Found : 97590
Scan
Timelines
From:
2009-03-11 11:45:00
To:
2009-03-11 11:50:00
Unit: Year #bars ~ 1 Reset
Files Management
Internet History
Logs
Multimedia
Operating System
Apply New Edit Delete
Fast details
Date Time Scanner Source Type Filename
2009-03-11 11:45:15 ConsoleKitScanner j /var/log generated history
2009-03-11 11:45:15 ConsoleKitScanner j /var/log generated history
2009-03-11 11:45:22 Linux / Mac LogS... j /var/log generated auth.log
2009-03-11 11:45:22 Linux / Mac LogS... j /var/log generated auth.log
2009-03-11 11:45:23 ConsoleKitScanner j /var/log generated history
2009-03-11 11:45:23 ConsoleKitScanner j /var/log generated history
2009-03-11 11:45:23 WTMPScanner j /var/log generated wtmp
2009-03-11 11:47:12 Linux / Mac LogS... n /var/log generated syslog
2009-03-11 11:47:12 Linux / Mac LogS... n /var/log generated syslog
2009-03-11 11:47:12 Linux / Mac LogS... n /var/log generated syslog
Refresh
Configure
Name Value
Date 2009-03-11
Time 11:45:23
Scanner WTMPScanner
Source j /var/log
Type generated
Path j /var/log_0/wtmp
Filename wtmp
WTMPType Normal process
Process ID 0
utLine pts/1
utID ts/1
utUser goatboy
WTMPHostname mobile24.cs.uno.edu
Histogram
Fast details

Timezones

- 1 hour time difference
- Summertime: 8th of March
- Aftertime

Disk Image	Physical Location	/etc/timezone	Code	UTC Offset Summertime (DST)	UTC Offset Wintertime
nssal-linux-fs	New Orleans	America/Chicago	CDT	-5	-6
jhuis-linux-fs	Baltimore	US/Eastern	EST	-4	-5

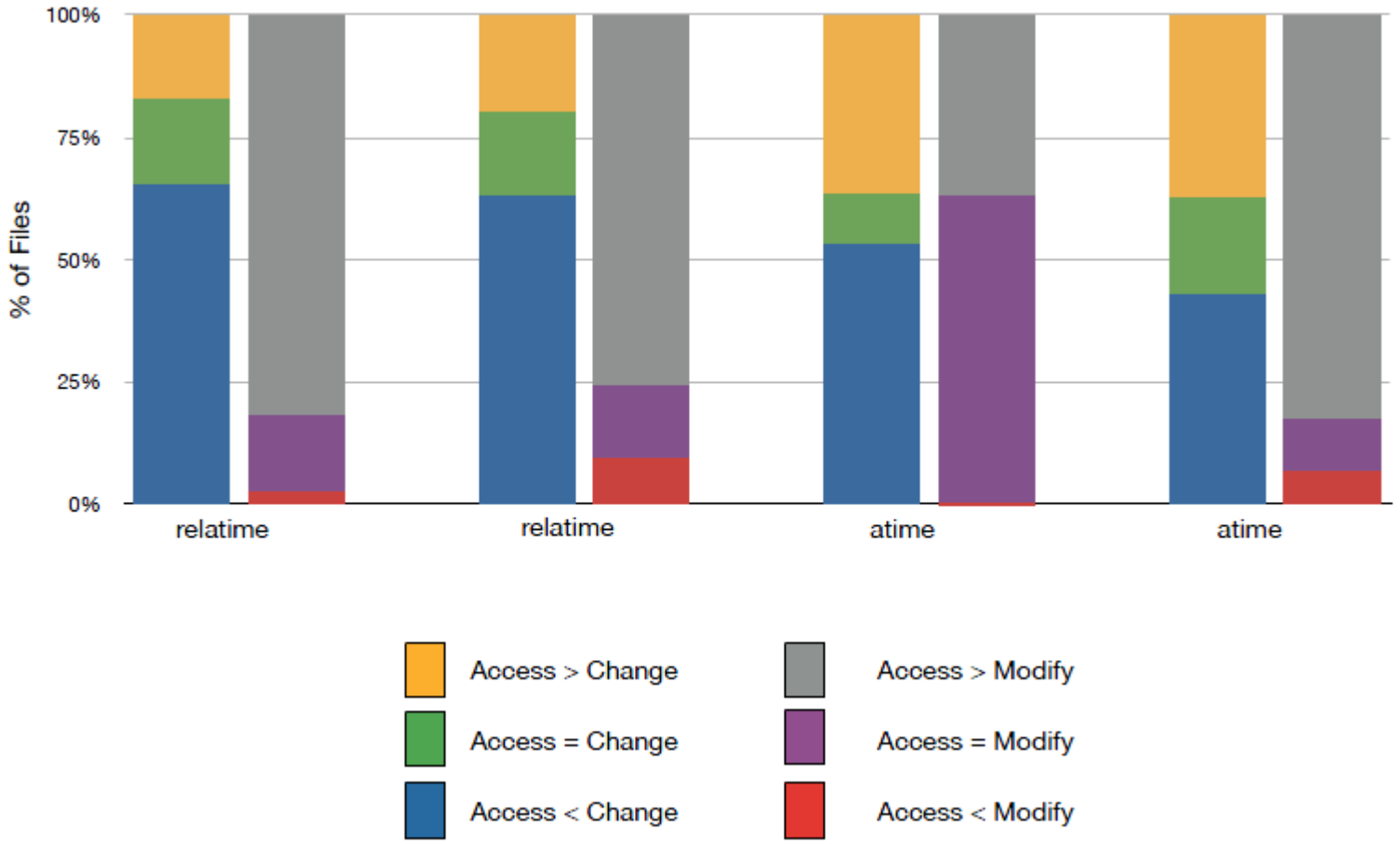
Linux time stamps (1)

- Modified, Access and Change time stamps, crucial for investigation.
- Mount options affect behaviour, not mentioned in literature!
  - relatime
  - noatime
  - nodiratime
- /etc/fstab

Action	Updated time stamp(s)		
Creation	Access	Modify	Change
Read	Access*		
Modify Content		Modify	Change
Copy (source)	Access*		
Copy (target does not exist)	Access	Modify	Change
Copy (target does exist)	**	Modify	Change
Move (target does not exist)			Change
Move (target does exist)			Change

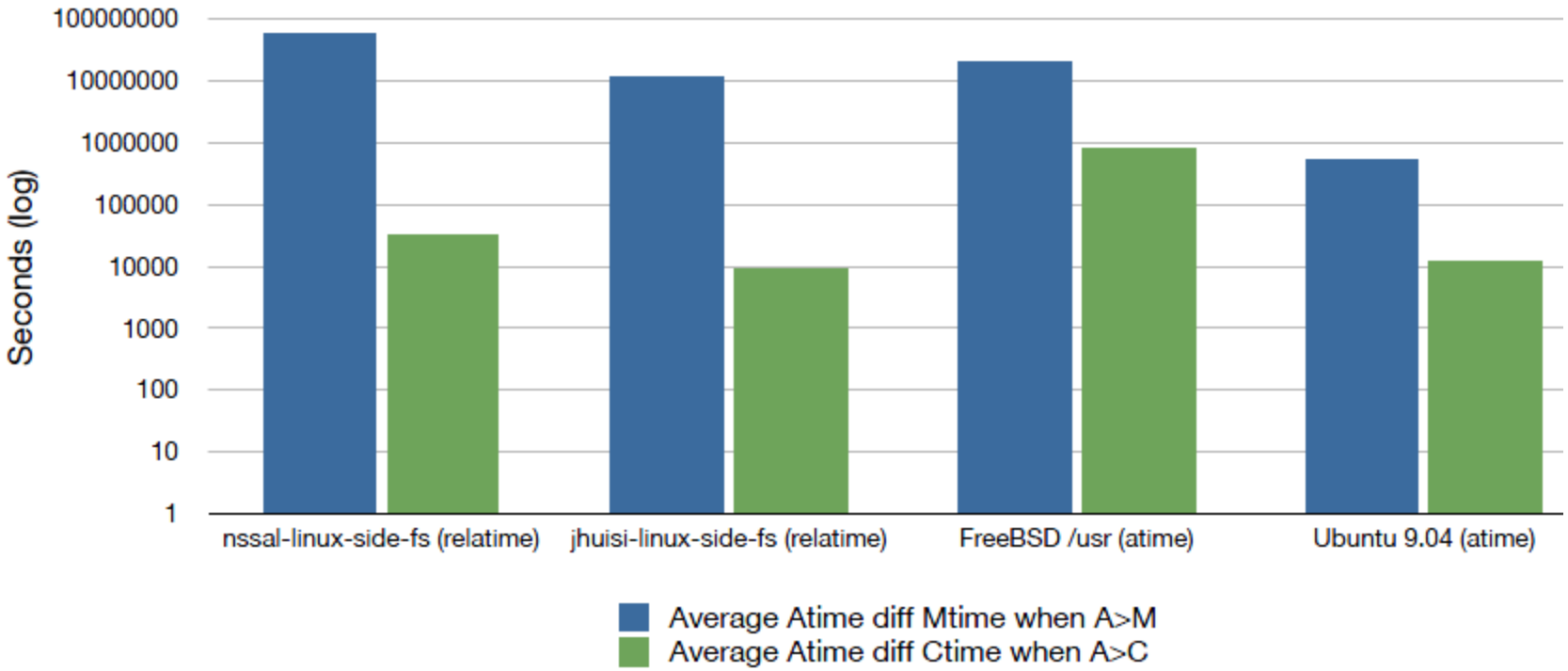
Linux time stamps (2)

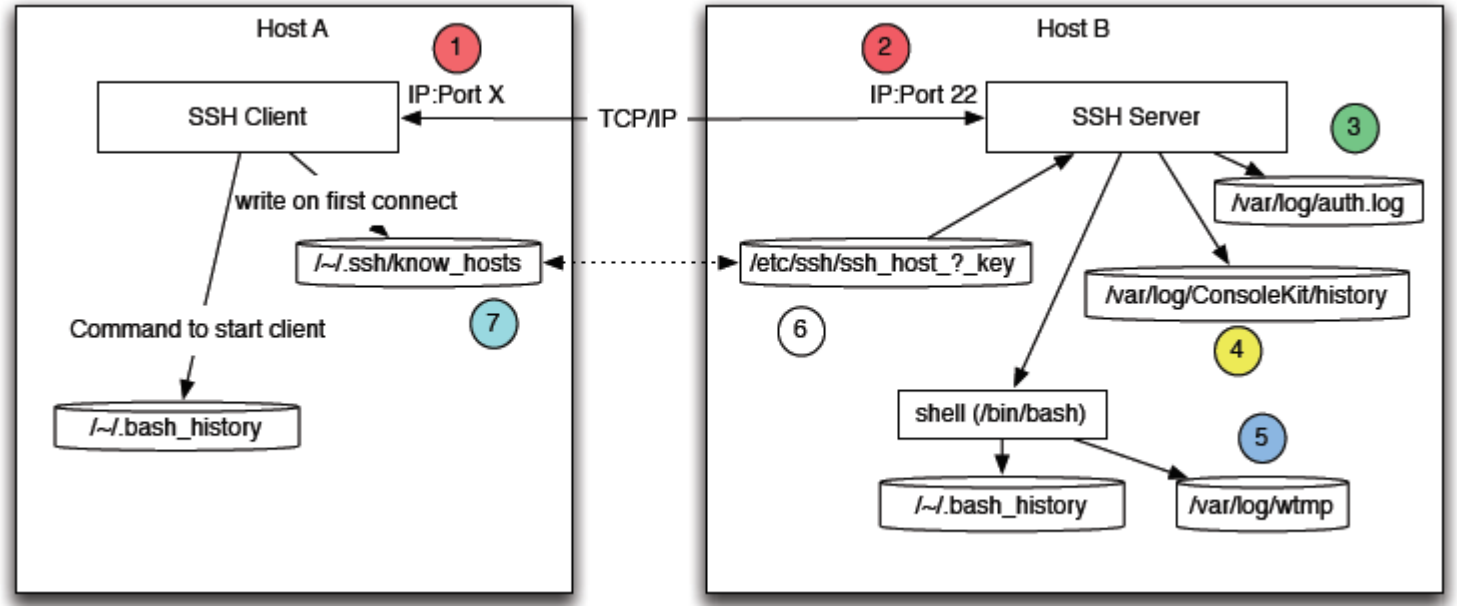
Determining the mount options using time stamps



Linux time stamps (3)

Determining the mount options using time stamps

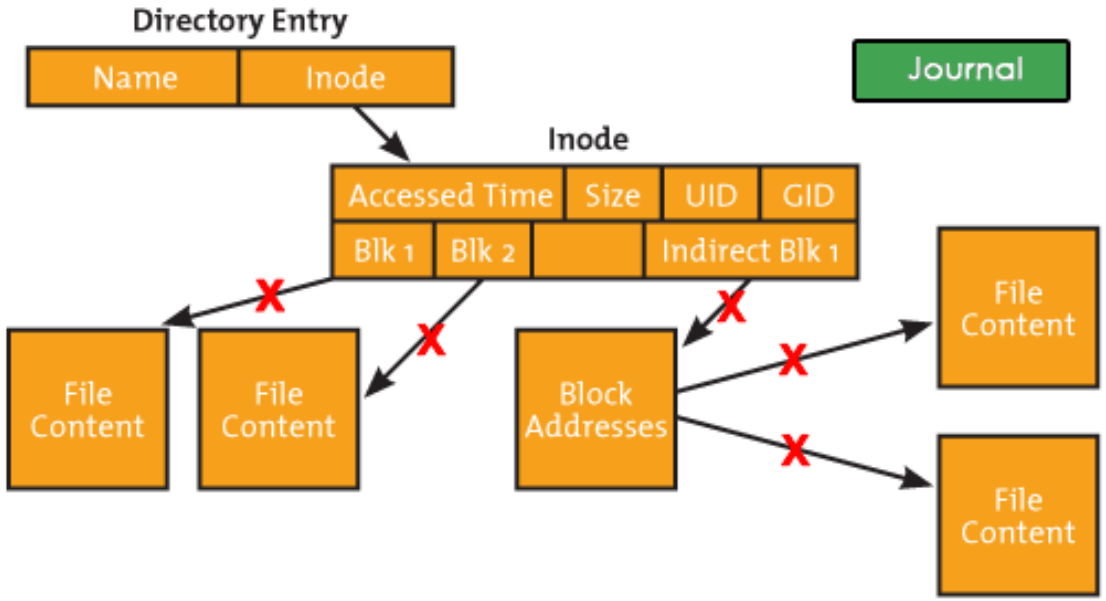




1 & 2	Network Trace nssal-capture-2.pcap	2009-03-11 11:49:37 128.220.249.83 137.30.123.40 TCP 51874 > ssh [SYN] 2009-03-11 11:49:37 137.30.123.40 128.220.249.83 TCP ssh > 51874 [SYN, ACK] 2009-03-11 11:49:37 128.220.249.83 137.30.123.40 TCP 51874 > ssh [ACK]
3	auth.log nssal-linux-side-fs.dd	Mar 11 11:49:45 nssal-ps3 sshd[3208]: Accepted password for jhuisi from 128.220.249.83 port 51874 ssh2 Mar 11 11:49:45 nssal-ps3 sshd[3208]: pam_unix(sshd:session): session opened for user jhuisi by (uid=0)
4	ConsoleKit/history nssal-linux-side-fs.dd	1236790186.127 type=SEAT_SESSION_ADDED : seat-id='Seat2' session-id='Session2' session-type='' session-x11-display='' session-x11-display-device='' session-display-device='/dev/ssh' session-remote-host-name='128.220.249.83' session-is-local=FALSE session-unix-user=1001 session-creation-time='2009-03-11T16:49:45.880532Z'
5	wtmp nssal-linux-side-fs.dd	jhuisi pts/2 128.220.249.83 Wed Mar 11 11:49 - 12:09 (00:20)
7	known_hosts (7) jhuisi-linux-side-fs.dd	stat /home/jhuisi/.ssh/known_hosts Access: 2009-03-11 11:51:57.000000000 -0500 Modify: 2009-03-11 11:49:40.000000000 -0500 Change: 2009-03-11 11:49:40.000000000 -0500

Investigation - Recovery of deleted files (1)

- ext3 zeros out block pointer on deletion
- Journaling: inode (entire block!) update is first recorded in journal



Investigation - Recovery of deleted files (2)

Carving is not always possible → journal based recovery

- Search for deleted files and their inode address in directory entries

```
 505479  (16) Recipes    503339  (16) .lesshst
 503412  (2688) memdump-powerpc.tar   <505465> (2660) .ICEauthority-n
<505482> (20) andromachi   <505483> (2604) bateman's
<505484> (20) stanley's   <505485> (2564) stoughton's
```

- Find inode copies in journal

Investigation - Recovery of deleted files (3)

No directory entries?

- Search journal for old entries (e.g. with 'ext3grep –search')
- Read all results (ext3grep --ls –block):

```
Indx Next |  Inode   | Deletion time                          Mode        File name
==========+==========+---------------data-from-inode------+----------+=========
   0    1 d  502947                                        drwxr-xr-x  .
   1    2 d  502945                                        drwxr-xr-x  ..
   2    3 r  502948                                        rrw-r--r--  .profile
   3    4 l  502949                                        lrwxrwxrwx  Examples -> /u
   4    5 r  502950                                        rrw-r--r--  .bash_logout
   5    6 r  502951                                        rrw-r--r--  .bashrc
<SNIP>
  34   35 d  503073                                        drwx------  .update-notifi
  35   36 d  505446                                        drwxr-xr-x  kmem
  36   37 r  503023                                        rrw-r--r--  .sudo_as_admin
  37   38 r  503148  D 1236805424 Wed Mar 11 16:03:44 2009  rrw-------  .bash_history
<SNIP>
  46   47 r  503434  D 1236805688 Wed Mar 11 16:08:08 2009  rrw-r--r--  mem.find.pics
```

- Try restoring the inode

Investigation - Recovery of deleted files (4)

File still not recovered?

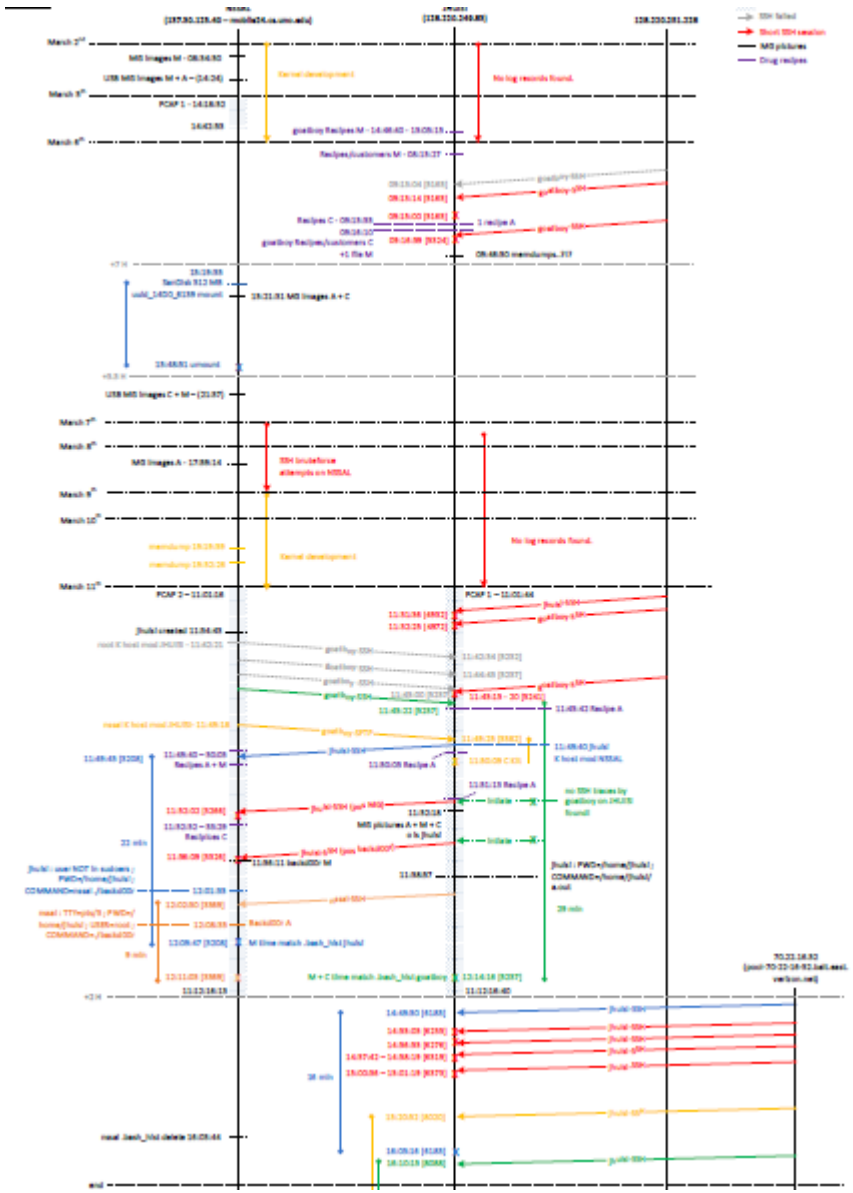
- Calculate block group data range and export the block (e.g. with dd) and try searching.

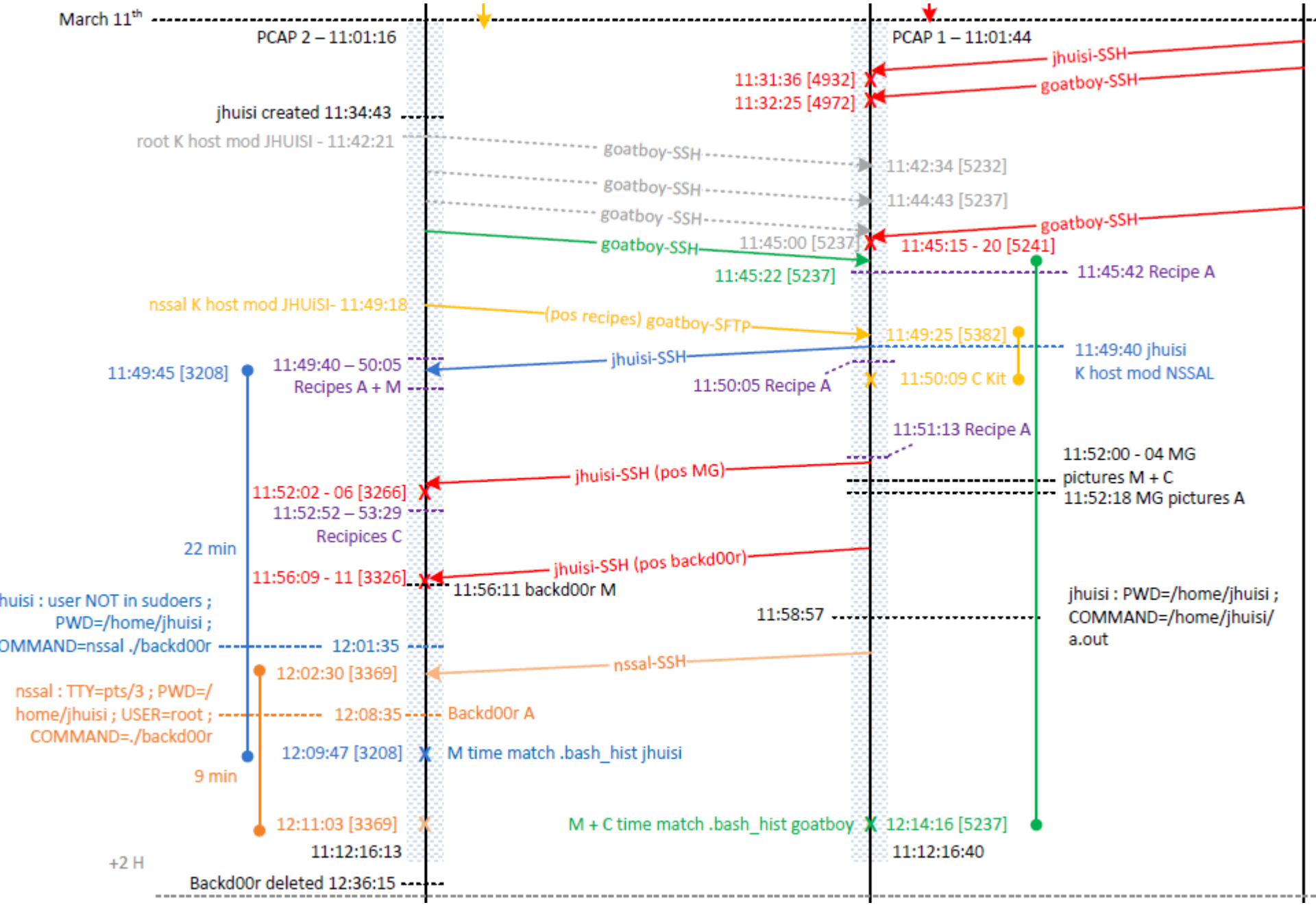
Recovered:

- Bash history
- Drug recipes
- Backdoor software

```
481  exit
482  pwd
483  ls
484  sudo ./backd00r &
485  fg
486  exit
487  adduser
488  adduser --help
489  ls /home
490  adduser --home /home/jhuisi jhuisi
491  passwd jhuisis
492  passwd jhuisi
493  ssh goatboy@ps3.isi.jhu.edu
494  ifconfig
```

The big picture




March 11th
PCAP 2 – 11:01:16
PCAP 1 – 11:01:44
jhuisi-SSH
goatboy-SSH
11:31:36 [4932]
11:32:25 [4972]
jhuisi created 11:34:43
root K host mod JHUISI - 11:42:21
goatboy-SSH
11:42:34 [5232]
goatboy-SSH
11:44:43 [5237]
goatboy -SSH
goatboy-SSH
11:45:00 [5237]
goatboy-SSH
11:45:15 - 20 [5241]
11:45:22 [5237]
11:45:42 Recipe A
nssal K host mod JHUiSI- 11:49:18
(pos recipes) goatboy-SFTP
11:49:25 [5382]
11:49:40 jhuisi
K host mod NSSAL
jhuisi-SSH
11:49:45 [3208]
11:49:40 – 50:05
Recipes A + M
11:50:05 Recipe A
11:50:09 C Kit
11:51:13 Recipe A
11:52:00 - 04 MG
pictures M + C
11:52:18 MG pictures A
jhuisi-SSH (pos MG)
11:52:02 - 06 [3266]
11:52:52 – 53:29
Recipices C
22 min
jhuisi-SSH (pos backd00r)
11:56:09 - 11 [3326]
11:56:11 backd00r M
huisi : user NOT in sudoers ;
PWD=/home/jhuisi ;
OMMAND=nssal ./backd00r
12:01:35
11:58:57
jhuisi : PWD=/home/jhuisi ;
COMMAND=/home/jhuisi/
a.out
nssal-SSH
12:02:30 [3369]
nssal : TTY=pts/3 ; PWD=/
home/jhuisi ; USER=root ;
COMMAND=./backd00r
12:08:35
Backd00r A
12:09:47 [3208]
M time match .bash_hist jhuisi
9 min
12:11:03 [3369]
M + C time match .bash_hist goatboy
12:14:16 [5237]
11:12:16:13
11:12:16:40
+2 H
Backd00r deleted 12:36:15

Questions?

Thanks!

NEDERLANDSFORENSISCHINSTITUUT