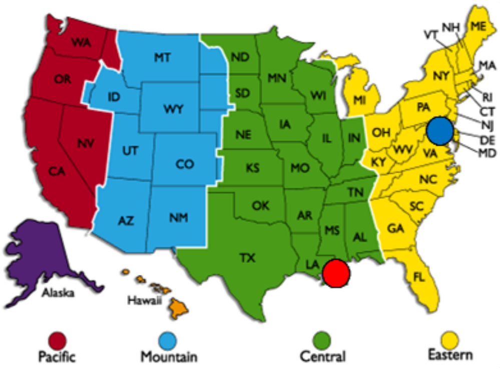
DFRWS 2009 Challenge Report

Jewan Bang, JungHeum Park, Kwonyoup Kim, and Sangjin Lee
Center for Information Security Technologies, Korea University.
jwbang@korea.ac.kr

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

· Timezone

After checking the /etc/timezone file for both systems, the timezone for nssal is "America/Chicago" and the timezone for jhuisi is "US/Eastern"



· Packet Analysis

1. After packet analysis, it was confirmed that jhuisi viewed the Playstation@Home profile on March 5th and on March 11th. Therefore, it is presumed that jhuisi and nssal had a conversation with each other on Playstation@Home.

2. nssal searched for “mardi gras” using sites such as Google on March 5th, 2009, and connected to the following sites. It can be deduced that he wanted to obtain information of products related to Mardi Gras.

http://www.mardigrasneworleans.com
http://www.toomeys-mardigras.com
http://www.mardigrasgalveston.com
http://www.mardigrasday.com
http://mardigrasday.makesparties.com
http://www.kingkingcakes.com
http://www.holidays.net

· Filesystem Analysis

jhuisi’s PS3’s goatboy created recipes on March 5th (/goatboy/Recipes/*). On the 6th, he created “customers”, a customer list (/goatboy/Recipes/customers/Tír na nÓg). On March 11th, he compressed the contents to a file named recipers.tar and transmitted it to nassal’s system (/home/goatboy/Recipes/recipes.tar).

The name of the recipes file is as follows, the contents of which is on how to make drugs.

Andromachi
bateman's
shéyòu
stanley's
stoughton's

In the customers folder, there exists a file named “Tír na nÓg”, the contents of which are as follows:

Ned Big-Ears, Market Street, Toytown, E4FZ10
Dinah Dole, Coronation Street, Toytown, E4FZ13
Dan Driver, Station Stop, Toytown, E4FZ21
Tessie Bard, Main Street, Toytown, E4FZ33
Tubby Bear, Honey Grove, Toytown, E4FZ08
Ernest Gobbo, Dark Forest Street, Toytown, E4FZ34
Graham Golly, Kettle Row, Toytown, E4FZ09
Missy Harriet, Half Pint Lane, Toytown, E4FZ45

```
Kevin Jumbo, Circus Avenue, Toytown, E4FZ22
Sam Little-Ears, Jingle Junction, Toytown, E4FZ20
Richard Milko, Dairy Way, Toytown, E4FZ12
CW Mouse, Holey Down, Toytown, E4FZ31
John Plod, Market Street, Toytown, E4FZ18
Martha Prim, Garden Lane, Toytown, E4FZ54
Harry Skittles, Bowling Green, Toytown, E4FZ33
Peter Sly, Back Street, Toytown, E4FZ34
Lucent Sparks, Hammer Row, Toytown, E4FZ01
Jerome Wobbly, Market Square, Toytown, E4FZ21
```

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

According to the file /var/log/auth.log (/auth_log folder), at 11:34:43 on March 11th, jhuisi user account was created (/home/jhuisi), and jhuisi connected using ssh from 128.220.249.83 (ps3.isi.jhu.edu). According to /home/jhuisi/.bash_history, the following commands were executed:

```
ls
cd Examples
ls
cd
cd ..
ls
cd nssal/
ls
cd Images/
ls
cd
ls
./backdoor
ls -l
~/backdoor
```

That is, jhuisi obtained root privileges and executed ./backd00r and ran the following commands on nssal's system (/backd00r files folder).

```
rm backboor
who
```

```
cd Recipes
ls
ls screenshots
ln –l /mnt/usb
```

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?

On March 6th, a user named goatboy created a folder named Recipes on jhuisi’s system, created Recipe that detailed how to make drugs and created a file related to purchasers. Also, in the /home/goatboy/.bash_history file, the following was entered (/goatboy's bash_history folder).

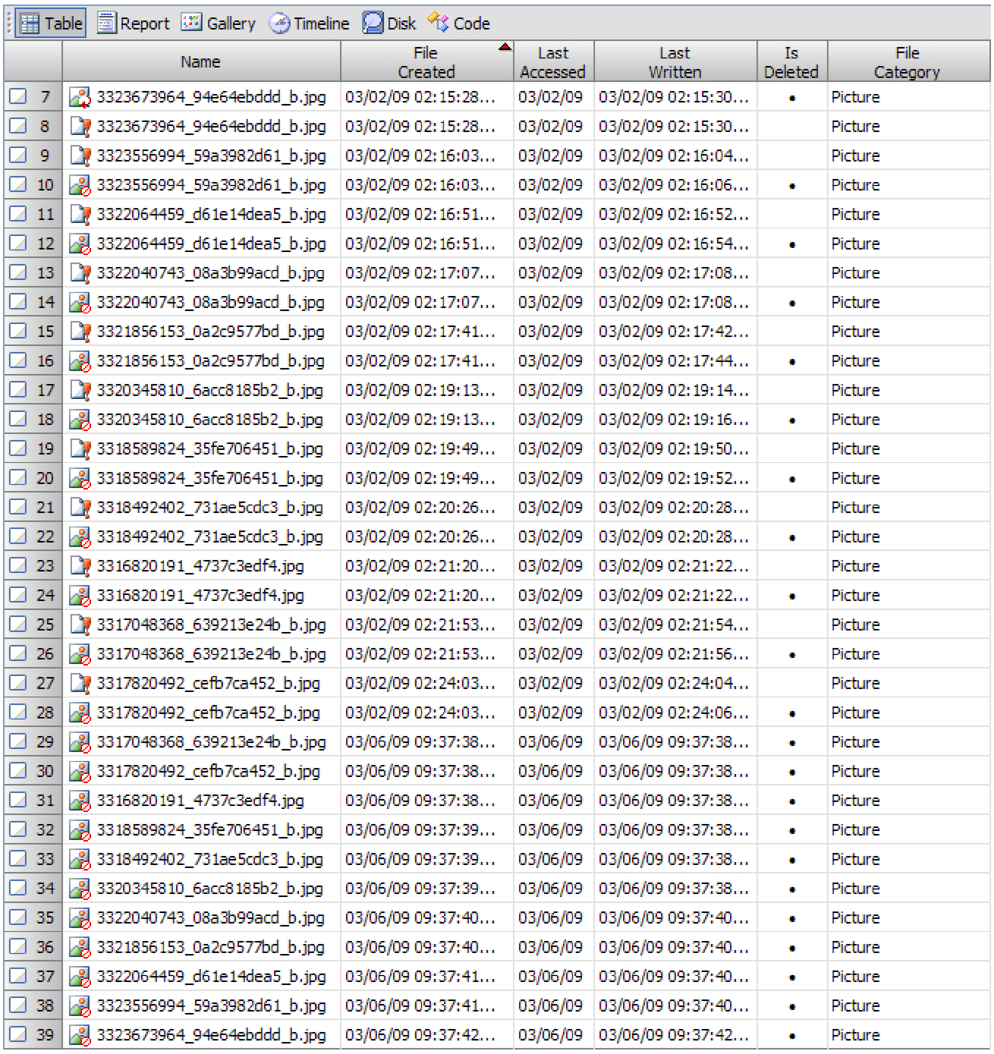
```
ls
mkdir Recipes
ls
cd Recipes/
ls
tar xvf recipes.tar
ls customers/
mv Tír\ na\ nÓg customers/
ls
rm recipes.tar
exit
ls
ls -l Recipes/
exit
ls
cd Examples
ls
cd ..
clear
ls
cd Recipes
ls
cat bateman\'s
talk
ytalk
```

```
ntalk
write jhuisi
ls
cat custmers
write jhuisi
cat customers
cd customers
ls
clear
ls -l
cat Tír\ na\ nÓg
ls
write jhuisi
I feel younger already!
write jhuisi
write
write jhuisi
Nice doing business with you!
clear
ls
cd
clear
ls
```

It can be known that jhuisi created a user account for goatboy and goatboy provided the recipes for this case.

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?

After analyzing nssal-thumb-fs.dd using EnCase, the image file that was created and deleted on March 2nd and March 6th was confirmed.



	Name	File Created	Last Accessed	Last Written	Is Deleted	File Category
☐ 7	3323673964_94e64ebddd_b.jpg	03/02/09 02:15:28...	03/02/09	03/02/09 02:15:30...	•	Picture
☐ 8	3323673964_94e64ebddd_b.jpg	03/02/09 02:15:28...	03/02/09	03/02/09 02:15:30...		Picture
☐ 9	3323556994_59a3982d61_b.jpg	03/02/09 02:16:03...	03/02/09	03/02/09 02:16:04...		Picture
☐ 10	3323556994_59a3982d61_b.jpg	03/02/09 02:16:03...	03/02/09	03/02/09 02:16:06...	•	Picture
☐ 11	3322064459_d61e14dea5_b.jpg	03/02/09 02:16:51...	03/02/09	03/02/09 02:16:52...		Picture
☐ 12	3322064459_d61e14dea5_b.jpg	03/02/09 02:16:51...	03/02/09	03/02/09 02:16:54...	•	Picture
☐ 13	3322040743_08a3b99acd_b.jpg	03/02/09 02:17:07...	03/02/09	03/02/09 02:17:08...		Picture
☐ 14	3322040743_08a3b99acd_b.jpg	03/02/09 02:17:07...	03/02/09	03/02/09 02:17:08...	•	Picture
☐ 15	3321856153_0a2c9577bd_b.jpg	03/02/09 02:17:41...	03/02/09	03/02/09 02:17:42...		Picture
☐ 16	3321856153_0a2c9577bd_b.jpg	03/02/09 02:17:41...	03/02/09	03/02/09 02:17:44...	•	Picture
☐ 17	3320345810_6acc8185b2_b.jpg	03/02/09 02:19:13...	03/02/09	03/02/09 02:19:14...		Picture
☐ 18	3320345810_6acc8185b2_b.jpg	03/02/09 02:19:13...	03/02/09	03/02/09 02:19:16...	•	Picture
☐ 19	3318589824_35fe706451_b.jpg	03/02/09 02:19:49...	03/02/09	03/02/09 02:19:50...		Picture
☐ 20	3318589824_35fe706451_b.jpg	03/02/09 02:19:49...	03/02/09	03/02/09 02:19:52...	•	Picture
☐ 21	3318492402_731ae5cdc3_b.jpg	03/02/09 02:20:26...	03/02/09	03/02/09 02:20:28...		Picture
☐ 22	3318492402_731ae5cdc3_b.jpg	03/02/09 02:20:26...	03/02/09	03/02/09 02:20:28...	•	Picture
☐ 23	3316820191_4737c3edf4.jpg	03/02/09 02:21:20...	03/02/09	03/02/09 02:21:22...		Picture
☐ 24	3316820191_4737c3edf4.jpg	03/02/09 02:21:20...	03/02/09	03/02/09 02:21:22...	•	Picture
☐ 25	3317048368_639213e24b_b.jpg	03/02/09 02:21:53...	03/02/09	03/02/09 02:21:54...		Picture
☐ 26	3317048368_639213e24b_b.jpg	03/02/09 02:21:53...	03/02/09	03/02/09 02:21:56...	•	Picture
☐ 27	3317820492_cefb7ca452_b.jpg	03/02/09 02:24:03...	03/02/09	03/02/09 02:24:04...		Picture
☐ 28	3317820492_cefb7ca452_b.jpg	03/02/09 02:24:03...	03/02/09	03/02/09 02:24:06...	•	Picture
☐ 29	3317048368_639213e24b_b.jpg	03/06/09 09:37:38...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 30	3317820492_cefb7ca452_b.jpg	03/06/09 09:37:38...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 31	3316820191_4737c3edf4.jpg	03/06/09 09:37:38...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 32	3318589824_35fe706451_b.jpg	03/06/09 09:37:39...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 33	3318492402_731ae5cdc3_b.jpg	03/06/09 09:37:39...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 34	3320345810_6acc8185b2_b.jpg	03/06/09 09:37:39...	03/06/09	03/06/09 09:37:38...	•	Picture
☐ 35	3322040743_08a3b99acd_b.jpg	03/06/09 09:37:40...	03/06/09	03/06/09 09:37:40...	•	Picture
☐ 36	3321856153_0a2c9577bd_b.jpg	03/06/09 09:37:40...	03/06/09	03/06/09 09:37:40...	•	Picture
☐ 37	3322064459_d61e14dea5_b.jpg	03/06/09 09:37:41...	03/06/09	03/06/09 09:37:40...	•	Picture
☐ 38	3323556994_59a3982d61_b.jpg	03/06/09 09:37:41...	03/06/09	03/06/09 09:37:40...	•	Picture
☐ 39	3323673964_94e64ebddd_b.jpg	03/06/09 09:37:42...	03/06/09	03/06/09 09:37:42...	•	Picture

It can be confirmed that in /home/nssal/Images of nssal's PS3 as well, 11 files with the same names were created on March 2nd (/Images folder).

3316820191_4737c3edf4.jpg
3317048368_639213e24b_b.jpg
3317820492_cefb7ca452_b.jpg
3318492402_731ae5cdc3_b.jpg
3318589824_35fe706451_b.jpg
3320345810_6acc8185b2_b.jpg
3321856153_0a2c9577bd_b.jpg
3322040743_08a3b99acd_b.jpg
3322064459_d61e14dea5_b.jpg
3323556994_59a3982d61_b.jpg
3323673964_94e64ebddd_b.jpg

It can be confirmed that in /home/jhuisi/Pictures of jhuisi's PS3 as well, 11 files with the same names were created on March 11nd

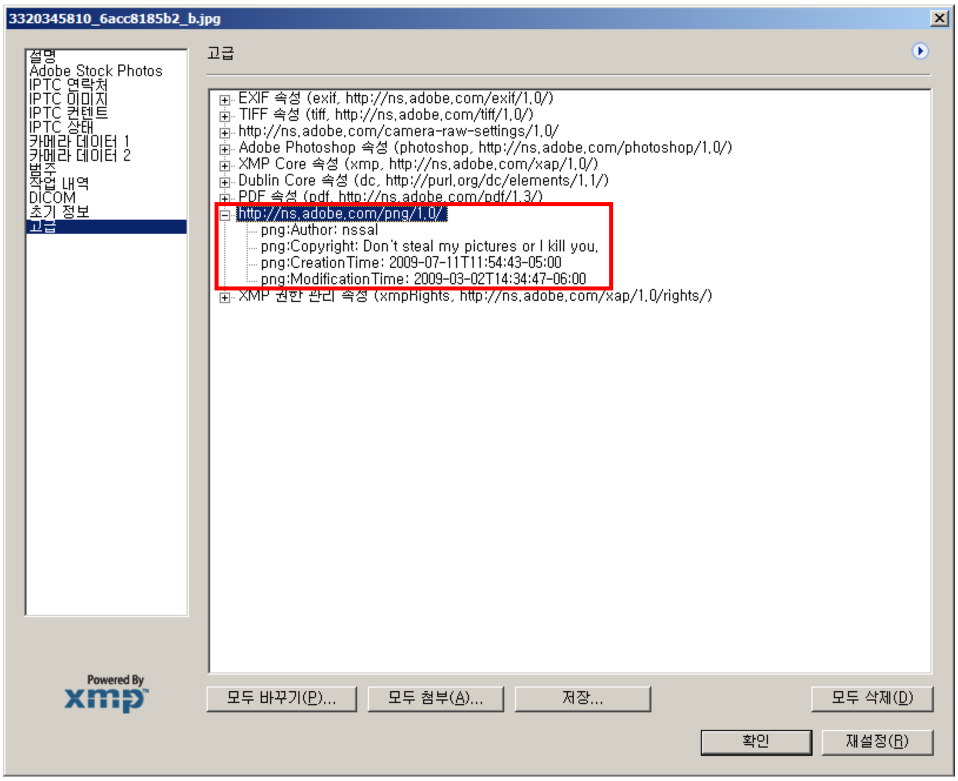
5. What data (if any) was provided by the Johns Hopkins PS3?

• recipes

It can be confirmed that a transmission took place, as the receipts located at /home/goatboy were created in nssal's system on March 11th.

• Images

Checking the images using Photoshop revealed that the nssal was the author, and a text string that says "Don't steal my pictures of i kill you" was found. Also, it was found that the date of edit was March 2nd, 2009.



3320345810_6acc8185b2_b.jpg

```
⊞ EXIF 속성 (exif, http://ns.adobe.com/exif/1.0/)
⊞ TIFF 속성 (tiff, http://ns.adobe.com/tiff/1.0/)
⊞ http://ns.adobe.com/camera-raw-settings/1.0/
⊞ Adobe Photoshop 속성 (photoshop, http://ns.adobe.com/photoshop/1.0/)
⊞ XMP Core 속성 (xmp, http://ns.adobe.com/xap/1.0/)
⊞ Dublin Core 속성 (dc, http://purl.org/dc/elements/1.1/)
⊞ PDF 속성 (pdf, http://ns.adobe.com/pdf/1.3/)
⊟ http://ns.adobe.com/png/1.0/
    png:Author: nssal
    png:Copyright: Don't steal my pictures or I kill you.
    png:CreationTime: 2009-07-11T11:54:43-05:00
    png:ModificationTime: 2009-03-02T14:34:47-06:00
⊞ XMP 권한 관리 속성 (xmpRights, http://ns.adobe.com/xap/1.0/rights/)
```

A text string that says "Don't steal my pictures of i kill you." was also found in the images found on jhuisi's system, and the author was all nssal. That is, it can be confirmed that jhuisi took the images from nssal's 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?

Summarizing the above analysis results, nssal provided the Mardi Gras images to jhuisi and jhuisi in turn provided the recipes.

Although nssal can argue that it was a backdoor intrusion to his system, examining the logs of /var/log/auth.log, it can be confirmed that he himself created the user account.

nssal’s /var/log/auth.log

```
Mar 11 11:33:47 nssal-ps3 sudo:       nssal : TTY=pts/0 ; PWD=/home/nssal ; USER=root ;
COMMAND=/bin/bash
Mar 11 11:34:43 nssal-ps3 groupadd[3132]: new group: name=jhuisi, GID=1001
Mar 11 11:34:43 nssal-ps3 useradd[3136]: new user: name=jhuisi, UID=1001, GID=1001,
home=/home/jhuisi, shell=/bin/bash
Mar 11 11:34:56 nssal-ps3 chfn[3144]: changed user `jhuisi' information
Mar 11 11:35:11 nssal-ps3 passwd[3149]: pam_unix(passwd:chauthtok): password changed for jhuisi
```

Therefore, it can be seen that the images were not taken by an intrusion but that it was an intentional act for data exchange.

Tools

The Autopsy Forensic Browser
http://www.sleuthkit.org

EnCase 6.13
http://www.guidancesoftware.com

Wireshark
http://www.wireshark.org

NetworkMiner
http://networkminer.sourceforge.net