2009 DFRWS CHALLENGE REPORT

Authors: Byungkil Lee (nullhat@gmail.com), Hongsuk Yang (eininondumak@gmail.com), Hyeon Yu (hyeony@gmail.com)

Analysis Targets

There are 6 different files uploaded on the DFRWS Forensic Challenge Details website (http://www.dfrws.org/2009/challenge/submission.shtml). Details of the files are following;

No.	Name of file	Hash value	Format
1	nssal-capture-1.pcap	e6ba905d4a0630915600b00ab9712499	Network packet
2	nssal-capture-2.pcap	fd28ae8fff1430b19ceec9785c2b027b	Network packet
3	jhuisi-capture-1.pcap	9bb90b7e6c5b8d7401b7621969017b01	Network packet
4	nssal-linux-side-fs.dd	a64f017400123b7eff2c5868f8e784e1	Hard drive image
5	jhuisi-linux-side-fs.dd	3ee30c25e5bca832b93ddf9eee88cb1b	Hard drive image
6	nssal-thumb-fs.dd	d4a8ff499355d82c9df76254dcb0cb1d	Thumb drive image
7	nssal-physicalmem.dd	5ffa6839dbab169c9c44436c80f8ea9b	Physical memory image

List 1: Evidences list

Those 6 files are our main analysis targets and to do actual analysis, we used 3 different programs, one is the Autopsy (www.sleuthkit.org/autopsy), the other is Wireshark (http://www.wireshark.com) and the last one is Networkminer (http://sourceforge.net/projects/networkminer).

We had set up a Linux box for the analysis and mounted the 2 hard drive images in the list and while doing so, we also used the autopsy program for the analysis. We used Wireshark and Networkminer programs to analyze 3 network packet files above.

Preview of the evidences

The No. 1 evidence in the Evidences List above, nssal-capture-1.pcap file, has 23,528 counts of packets including communication records of nssal's computer for 24 minutes and 01 second, between 5 MAR 2009 20:18:52 Universal Time Coordinated (UTC) and 5 MAR 2009 20:42:53 UTC.

The No. 2 evidence, nssal-capture-2.pcap file, has 43,538 counts of packets including communication records of nssal's computer between 11 MAR 2009 16:01:16 and 17:16:13 on the same day.

The No. 3 evidence, jhuisi-capture-1.pcap file, has 174,451 counts of packets including communication records of jhuisi computer between 11 MAR 2009 16:01:44 and 17:16:40 on the same day.

The No. 4 evidence, nssal-linux-side-fs.dd file, indicates that Ubuntu Operating System (OS) ver. 8.10 is installed on the PS3, time zone is set to be the "America/Chicago" and IP address is configured to use DHCP. The registered users are "nssal" which has been created in the process of OS installation and "jhuisi" which has been created on 11 Mar 16:34:43.

```
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
```

The No. 5 evidence, jhuisi-linux-side-fs.dd file, indicates that Ubuntu Operating System (OS) ver. 8.10 is installed on the PS3, time zone is set to be the "US/Eastern" and IP address is configured to use the static IP address of 128.220.249.83. The registered users are "jhuisi" which has been created in the process of OS installation and "goatboy" which has been created on 22 Jan 2009 18:15:59.

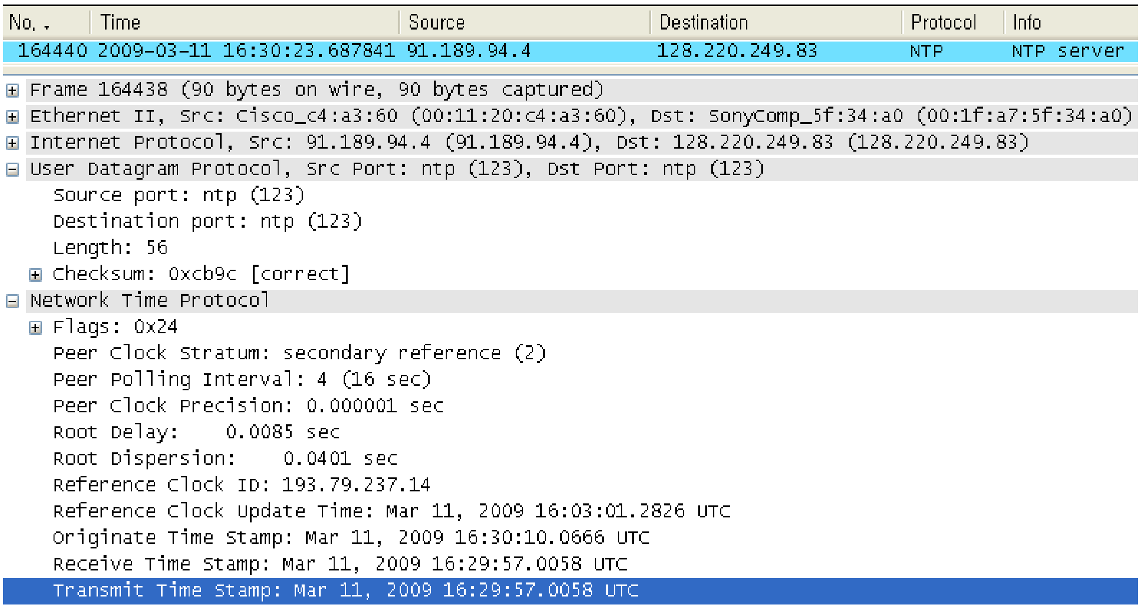
```
Jan 22 13:15:59 ps3 groupadd[5263]: new group: name=goatboy, GID=1001
Jan 22 13:15:59 ps3 useradd[5267]: new user: name=goatboy, UID=1001, GID=1001, home=/home/goatboy,
shell=/bin/bash
```

The No. 6 evidence, nssal-thumb-fs.dd file, is the USB Thumb drive which has 34 different files including 3316820191_4737c3edf4.jpg file and the capacity of it is 488.1 Mbytes.

The No. 7 evidence, nssal-physicalmem.dd file, is the physical memory dump file of nssal's PS3 Linux box on arrest, and the capacity of it is 240 Mbytes.

Setting the Basic Time

As we can see at the screen capture below, the packet captured time was Mar 11, 2009 16:29:57 (UTC) and the packet capture program recorded the time as Mar 11, 16:30:23, so we can see that the time in the jhuisi-capture-1.pcap file is 26 seconds faster than the standard UTC time.

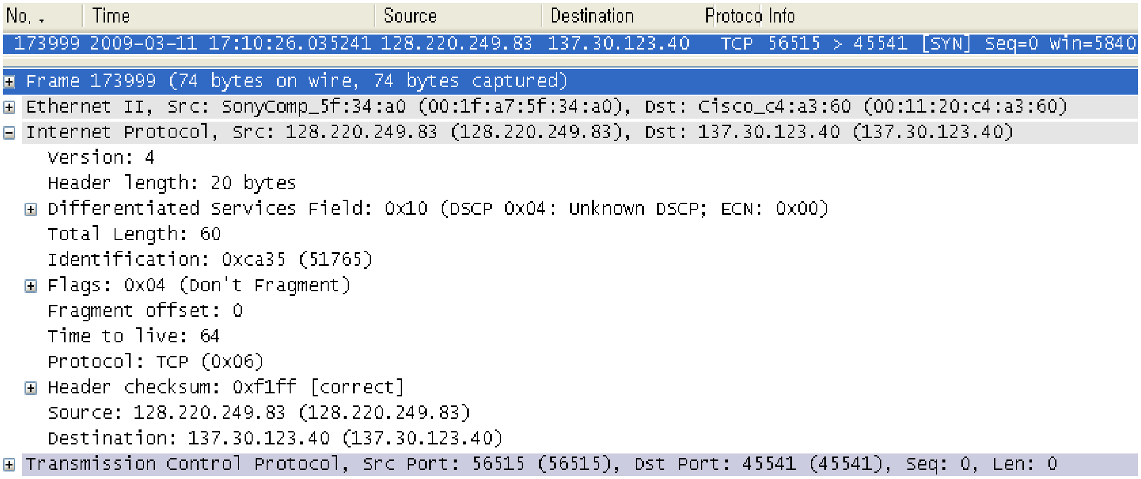


```
No. .   Time                        Source          Destination      Protocol  Info
164440 2009-03-11 16:30:23.687841 91.189.94.4     128.220.249.83   NTP       NTP server

⊞ Frame 164438 (90 bytes on wire, 90 bytes captured)
⊞ Ethernet II, Src: Cisco_c4:a3:60 (00:11:20:c4:a3:60), Dst: SonyComp_5f:34:a0 (00:1f:a7:5f:34:a0)
⊞ Internet Protocol, Src: 91.189.94.4 (91.189.94.4), Dst: 128.220.249.83 (128.220.249.83)
⊟ User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
    Source port: ntp (123)
    Destination port: ntp (123)
    Length: 56
  ⊞ Checksum: 0xcb9c [correct]
⊟ Network Time Protocol
  ⊞ Flags: 0x24
    Peer Clock Stratum: secondary reference (2)
    Peer Polling Interval: 4 (16 sec)
    Peer Clock Precision: 0.000001 sec
    Root Delay:    0.0085 sec
    Root Dispersion:    0.0401 sec
    Reference Clock ID: 193.79.237.14
    Reference Clock Update Time: Mar 11, 2009 16:03:01.2826 UTC
    Originate Time Stamp: Mar 11, 2009 16:30:10.0666 UTC
    Receive Time Stamp: Mar 11, 2009 16:29:57.0058 UTC
    Transmit Time Stamp: Mar 11, 2009 16:29:57.0058 UTC
```

Picture 1: 164,440th number of packet of the jhuisi-capture-1.pcap file

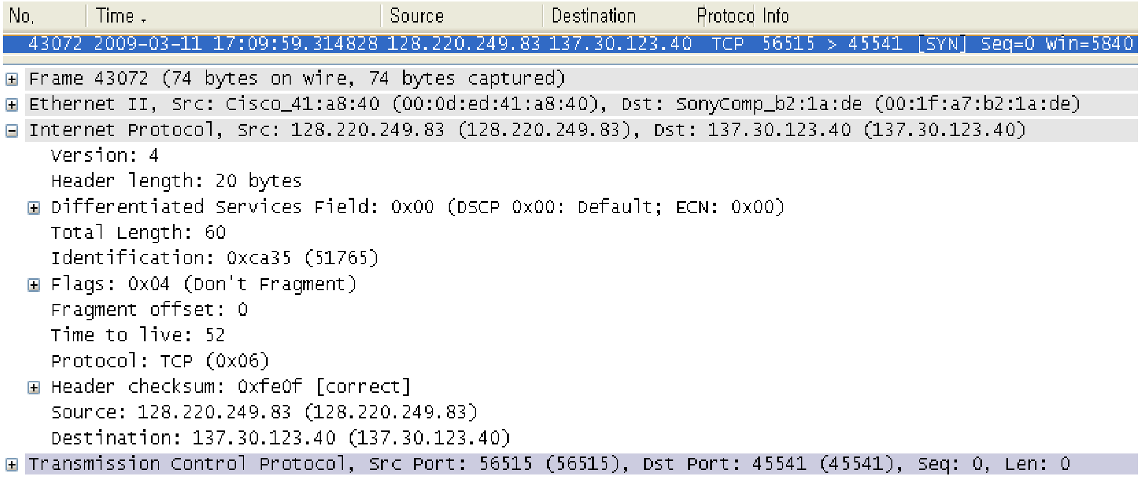
When we see the following screen captures, we can find that 173,999th number of packets in the jhuisi-capture-1.pcap file has been recorded on Mar 11 17:10:26 2009, so the packet was created actually on UTC Mar 11 17:10:00 2009 because jhuisi-capture-1.pcap file is 26 seconds faster than UTC. We can also see that the identical packet has been captured on the 43,072th number of packets in the nssal-capture-2.pcap file and it has the time of Mar 11 17:09:59 2009, so the nssal-capture-2.pcap file is 1 second slower than UTC. We could not find NTP packet in the nssal-capture-1.pcap file and we assume the file is 1 second slower than UTC, just like the nssal-capture-2.pcap file, because the system which had been used to capture packets of nssal's computer was the only one and identical.



```
No. .  Time                        Source          Destination     Protoco Info
173999 2009-03-11 17:10:26.035241 128.220.249.83 137.30.123.40    TCP  56515 > 45541 [SYN] Seq=0 Win=5840

⊞ Frame 173999 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: SonyComp_5f:34:a0 (00:1f:a7:5f:34:a0), Dst: Cisco_c4:a3:60 (00:11:20:c4:a3:60)
⊟ Internet Protocol, Src: 128.220.249.83 (128.220.249.83), Dst: 137.30.123.40 (137.30.123.40)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
    Total Length: 60
    Identification: 0xca35 (51765)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0xf1ff [correct]
    Source: 128.220.249.83 (128.220.249.83)
    Destination: 137.30.123.40 (137.30.123.40)
⊞ Transmission Control Protocol, Src Port: 56515 (56515), Dst Port: 45541 (45541), Seq: 0, Len: 0
```

Picture 2: 173,999th number of packets of jhuisi-capture-1.pcap file



```
No.      Time .                     Source          Destination     Protoco Info
  43072 2009-03-11 17:09:59.314828 128.220.249.83 137.30.123.40  TCP  56515 > 45541 [SYN] Seq=0 Win=5840

⊞ Frame 43072 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_41:a8:40 (00:0d:ed:41:a8:40), Dst: SonyComp_b2:1a:de (00:1f:a7:b2:1a:de)
⊟ Internet Protocol, Src: 128.220.249.83 (128.220.249.83), Dst: 137.30.123.40 (137.30.123.40)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0xca35 (51765)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 52
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0xfe0f [correct]
    Source: 128.220.249.83 (128.220.249.83)
    Destination: 137.30.123.40 (137.30.123.40)
⊞ Transmission Control Protocol, Src Port: 56515 (56515), Dst Port: 45541 (45541), Seq: 0, Len: 0
```

Picture 3: 43,072th number of packets of nssal-capture-2.pcap file

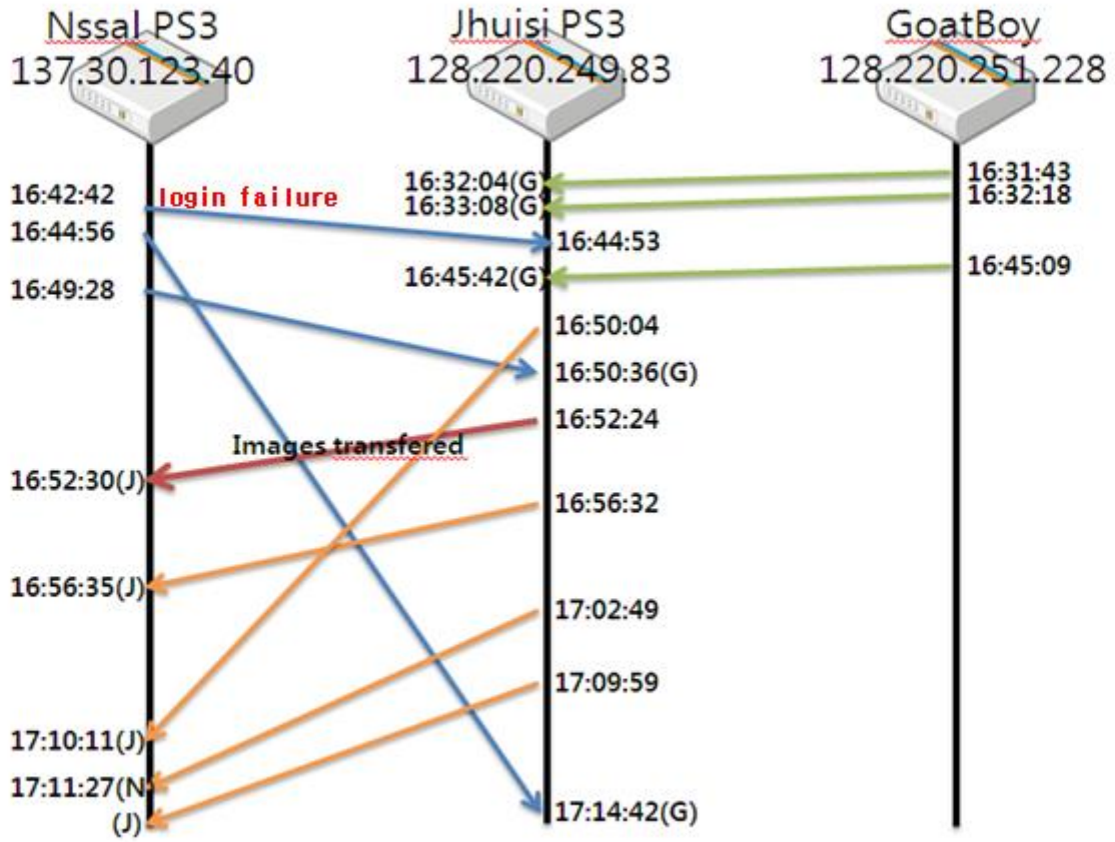
To summarize it up, we can see the time gap from the UTC of each file at the following list.

	Files	Time gap
1	nssal-capture-1.pcap	UTC-1 Second
2	nssal-capture-2.pcap	UTC-1 Second
3	jhuisi-capture-1.pcap	UTC+26 Seconds
4	nssal-linux-side-fs.dd	UTC+8 Seconds
5	jhuisi-linux-side-fs.dd	UTC+20 Seconds
6	nssal-thumb-fs.dd	Unknown

List 2: Time gap from UTC of each file

The Case Summary

Nssal has the Mardi Gras images in his system on Mar. 2, 2009. On Mar. 11, 2009, nssal created "jhuisi" account in his PS3 system and at 16:52 on that day, jhuisi has transferred Mardi Gras images to his PS3 system through SSH encrypted channel.



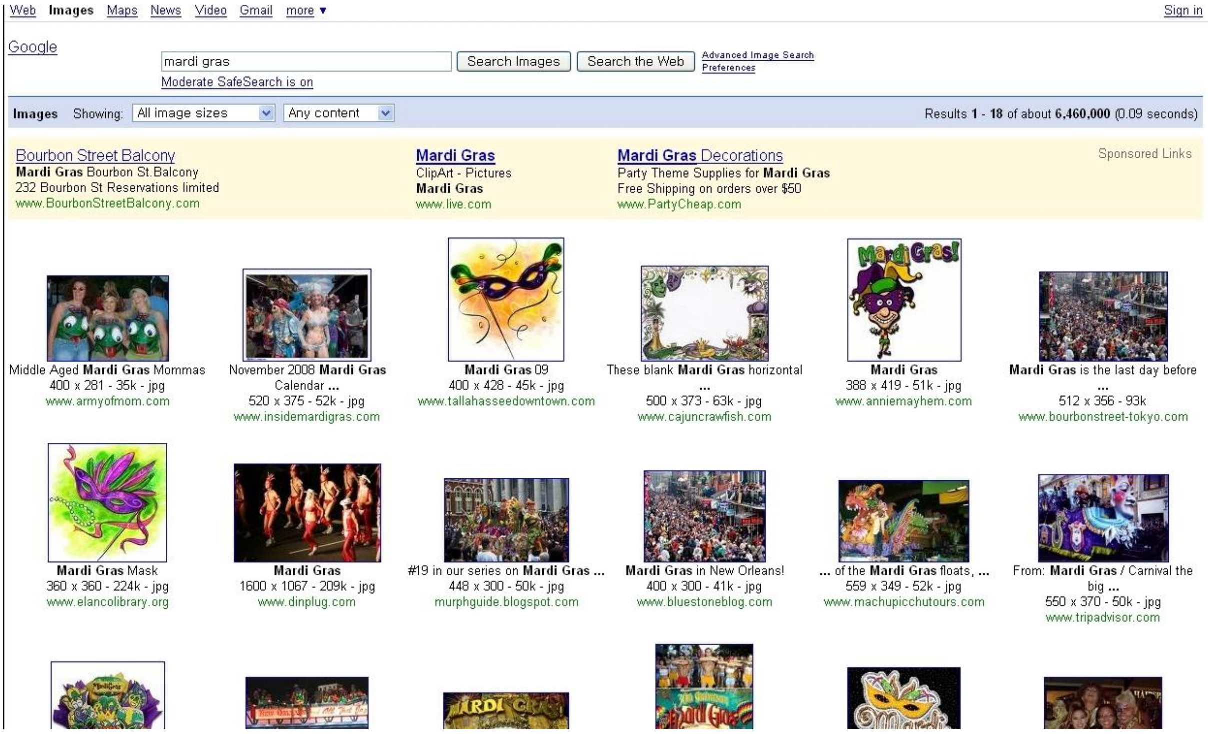
Answers to the DFRWS question

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

A. Nssal's activity

On Mar. 2 14:34:50 2009, he created Mardi Gras images in the directory of "/home/nssal/Images" in his PS3 system. Between some times on Mar. 5 20:19 2009, he searched the Mardi Gras images from the google website. On Mar. 6 21:37 2009, he deleted Mardi Gras images in the USB Thumb drive.

On Mar. 11 16:42 2009, he had booted his PS3 system using Ubuntu 9.10 Linux OS and was assigned IP address of 137.30.123.40. He created "jhuisi" account in his PS3 system. Between 16:44 and 17.14 on Mar. 11, 2009, nssal has connected to the jhuisi's PS3 system using "goatboy" account. Jhuisi and nssal tried to send a message of "Nice doing business with you!", which was recorded in the ".bash_history" file.



Web **Images** Maps News Video Gmail more ▾ Sign in

Google

mardi gras | Search Images | Search the Web | Advanced Image Search Preferences

Moderate SafeSearch is on

Images Showing: All image sizes ▾ Any content ▾ Results **1** - **18** of about **6,460,000** (0.09 seconds)

Bourbon Street Balcony
Mardi Gras Bourbon St.Balcony
232 Bourbon St Reservations limited
www.BourbonStreetBalcony.com

Mardi Gras
ClipArt - Pictures
Mardi Gras
www.live.com

Mardi Gras Decorations
Party Theme Supplies for **Mardi Gras**
Free Shipping on orders over $50
www.PartyCheap.com

Sponsored Links

Middle Aged **Mardi Gras** Mommas
400 x 281 - 35k - jpg
www.armyofmom.com

November 2008 **Mardi Gras** Calendar ...
520 x 375 - 52k - jpg
www.insidemardigras.com

Mardi Gras 09
400 x 428 - 45k - jpg
www.tallahasseedowntown.com

These blank **Mardi Gras** horizontal ...
500 x 373 - 63k - jpg
www.cajuncrawfish.com

Mardi Gras
388 x 419 - 51k - jpg
www.anniemayhem.com

Mardi Gras is the last day before ...
512 x 356 - 93k
www.bourbonstreet-tokyo.com

Mardi Gras Mask
360 x 360 - 224k - jpg
www.elancolibrary.org

Mardi Gras
1600 x 1067 - 209k - jpg
www.dinplug.com

#19 in our series on **Mardi Gras** ...
448 x 300 - 50k - jpg
murphguide.blogspot.com

Mardi Gras in New Orleans!
400 x 300 - 41k - jpg
www.bluestoneblog.com

... of the **Mardi Gras** floats, ...
559 x 349 - 52k - jpg
www.machupicchutours.com

From: **Mardi Gras** / Carnival the big ...
550 x 370 - 50k - jpg
www.tripadvisor.com

B. Jhuisi's activity

On Jan. 22 18:15 2009, he created "goatboy" account in his system. On Mar. 11 16:30 2009, he had booted his PS3 system using Ubuntu 9.10 Linux OS using the static IP address of 128.220.249.83. He had a connection to nssal's PS3 system using "jhuisi" account between 16:50 and 17:10 on Mar. 11, 2009. At the time of Mar. 11 17:02 2009, jhuisi had connected to the nssal's PS3 system using "nssal" account and logged off after executing a backdoor program. On Mar. 11 16:52:24 2009, he had Mardi Gras images transferred to his sytem from nssal's PS3 system using "scp" command. On Mar. 11 17:09 2009, he connected to a backdoor port of nssal's PS3 system.

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

In the 3 evidence files, nssal-linux-side-fs.dd file, jhuisi-linux-side-fs.dd file and nssal-thumb-fs.dd file, we can find Mardi Gras images is being stored or has been stored and related analysis report is attached as the Analysis Result, A, B and C. When we see the meta tag of the Mardi Gras images, we find that the file has last stored using Photoshop program and it is the file nssal has created as we can find "nssal" or "Don't steal my pictures or I kill you." strings in the file.

When we read the Timeline analysis report, P and Q, we can find that the Mardi Gras images has been transferred from nssal-thumb-fs.dd file to nssal-linux-side-fs.dd file and finally from nssal-linux-side-fs.dd to jhuisi-linux-side-fs.dd file. The transmission from nssal-thumb-fs.dd file to nssal-linux-side-fs.dd file was made by nssal's USB Thumb drive and the transmission from nssal-linux-side-fs.dd to jhuisi-linux-side-fs.dd file was made by jhuisi using encrypted channel from nssal's PS3 system at the time of Mar. 11 16:52:24, 2009.

On the directory of /home/jhuisi in the nssal-linux-side-fs.dd, we could find out that there had been a "backd00r" executable file which opens TCP/IP port 45,541 and opens a root shell when it receives strings of "jhuisi" and "mac" continuously, but now it was deleted. On the directory of /home/jhuisi in the jhuisi-linux-side-fs.dd file, the source code of the backdoor is preserved as "backd00r.c" file and the output file of the source code compilation, "a.out" is also preserved in the system. The backdoor program had been executed at the nssal-linux-side-fs.dd file system and jhuisi had the connection to the nssal's PS3 system using the backdoor from Mar. 11 17:09 2009. We can identify it on the Time Line Analysis result, P and Q.

On the directory of /home/nssal/Recipes/ in the nssal-linux-side-fs.dd file and on the directory of /home/goatboy/Recipes/ in the jhuisi-linux-side-fs.dd file, we could find a file named "andromachi" which has the recipe of opium poppy, so it seems like that we need additional investigation to the drug clue. Through the timeline analysis report, the file has been transferred from jhuisi's PS3 computer to the nssal's PS3 computer on Mar. 5, 2009. On the /Recipes/customers folder in the file, there is a file named "Tí   r na nOǵ   " in which the customers' address is being kept.

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?

When we look at the log in record, we can see that nssal connected to the jhuisi's PS3 system using "goatboy" account right after somebody had connection to the jhuisi's PS3 system using "goatboy" account from the IP address of 128.220.251.228 for about 20 seconds at Mar. 11 16:32 2009 and for about 10 seconds at 16:33 on the same day. So the person who used the IP address of 128.220.251.228 to the connection is another accomplice different from nssal and jhuisi.

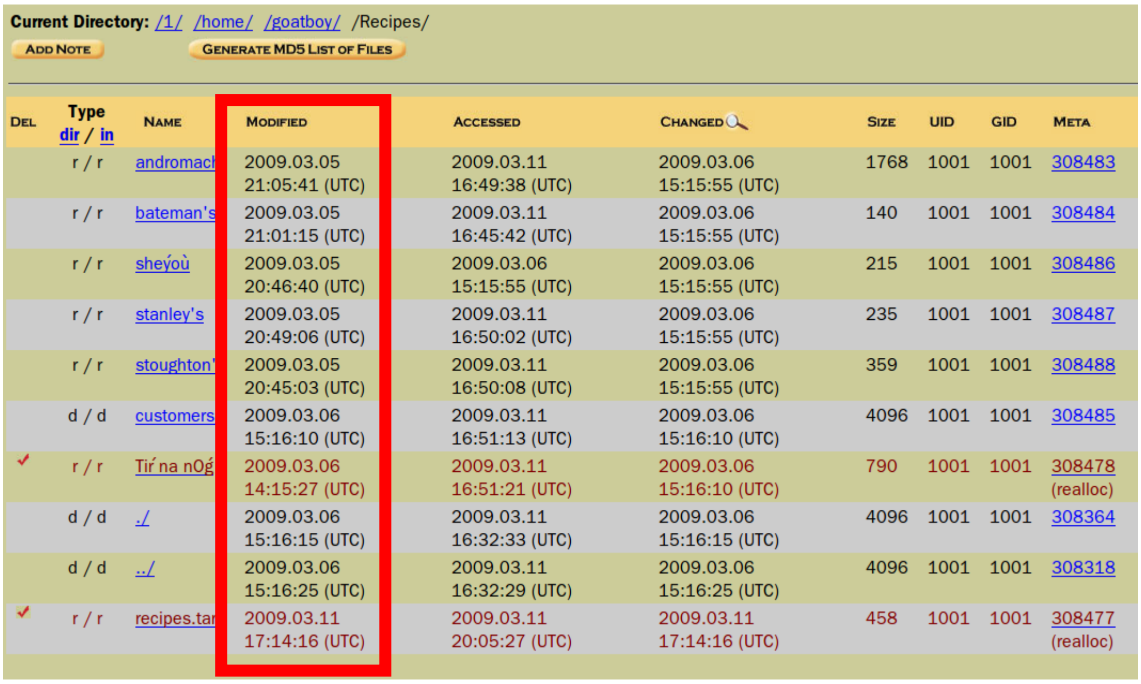
4. Is there evidence that illicit data (specifically, Mardi Gras images) was exchanged? If so, what can be determined about that data and the manner of transfer?

According to the log in records, the size of the data jhuisi has transferred for about 6 seconds after connecting to the nssal's PS3 from his own PS3 is 4,165,581 bytes which is almost same with the total size of Mardi Gras images, 3,954,938 bytes. And the creation time of the Mardi Gras images on the jhuisi PS3 system is Mar. 11 16:52 2009. The owner of the Mardi Gras images is jhuisi and when the Mardi Gras images were created, there are 2 login users in the system, one is jhuisi account from local system and goatboy account which is the nssal's account being logged in from remote connection. When we assume that nssal had a ssh connection to the jhuisi system using goatboy account, then ssh_host file would have been created in the home directory of goatboy account. Based on the fact that the file is not created, so we concluded the connection user is "jhuisi".

To summarize it, jhuisi connected to his own PS3 local system at the time of Mar. 11 16:52, 2009 using jhuisi account and transferred the Mardi Gras images from nssal's PS3 system to his system.

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

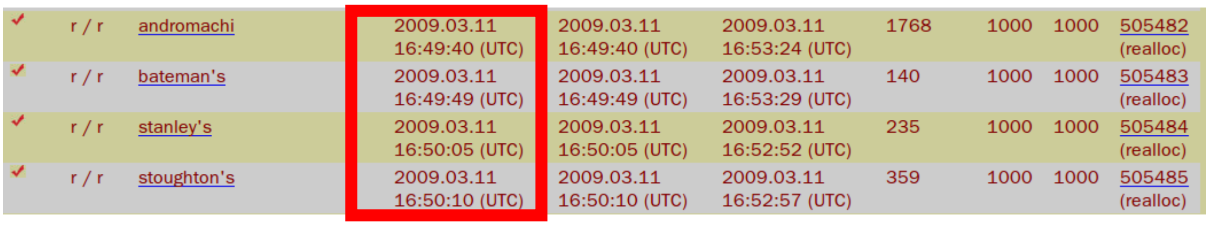
The folder of /home/nssal/Recipes/ and files in the folder, in the nssal-linux-side-fs.dd file is identical to the folder of /home/goatboy/Recipes/ and files in it, in jhuisi-linux-side-fs.dd file. We could find that the files had been created on Mar. 5, 2009 in jhuisi's PS3 system and transferred to nssal's PS3 system on Mar. 11, 2009.



Current Directory: /1/ /home/ /goatboy/ /Recipes/

Del	Type dir / in	Name	Modified	Accessed	Changed	Size	UID	GID	Meta
	r / r	andromach	2009.03.05 21:05:41 (UTC)	2009.03.11 16:49:38 (UTC)	2009.03.06 15:15:55 (UTC)	1768	1001	1001	308483
	r / r	bateman's	2009.03.05 21:01:15 (UTC)	2009.03.11 16:45:42 (UTC)	2009.03.06 15:15:55 (UTC)	140	1001	1001	308484
	r / r	sheýoù	2009.03.05 20:46:40 (UTC)	2009.03.06 15:15:55 (UTC)	2009.03.06 15:15:55 (UTC)	215	1001	1001	308486
	r / r	stanley's	2009.03.05 20:49:06 (UTC)	2009.03.11 16:50:02 (UTC)	2009.03.06 15:15:55 (UTC)	235	1001	1001	308487
	r / r	stoughton'	2009.03.05 20:45:03 (UTC)	2009.03.11 16:50:08 (UTC)	2009.03.06 15:15:55 (UTC)	359	1001	1001	308488
	d / d	customers	2009.03.06 15:16:10 (UTC)	2009.03.11 16:51:13 (UTC)	2009.03.06 15:16:10 (UTC)	4096	1001	1001	308485
✓	r / r	Tiŕ na nOǵ	2009.03.06 14:15:27 (UTC)	2009.03.11 16:51:21 (UTC)	2009.03.06 15:16:10 (UTC)	790	1001	1001	308478 (realloc)
	d / d	./	2009.03.06 15:16:15 (UTC)	2009.03.11 16:32:33 (UTC)	2009.03.06 15:16:15 (UTC)	4096	1001	1001	308364
	d / d	../	2009.03.06 15:16:25 (UTC)	2009.03.11 16:32:29 (UTC)	2009.03.06 15:16:25 (UTC)	4096	1001	1001	308318
✓	r / r	recipes.tar	2009.03.11 17:14:16 (UTC)	2009.03.11 20:05:27 (UTC)	2009.03.11 17:14:16 (UTC)	458	1001	1001	308477 (realloc)

Picture 4: The contents of Recipes folder of goatboy account

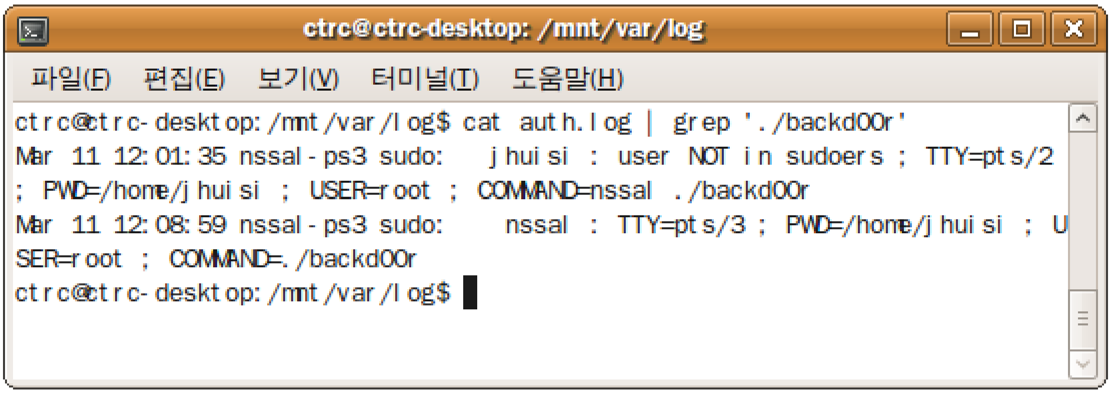


✓	r / r	andromachi	2009.03.11 16:49:40 (UTC)	2009.03.11 16:49:40 (UTC)	2009.03.11 16:53:24 (UTC)	1768	1000	1000	505482 (realloc)
✓	r / r	bateman's	2009.03.11 16:49:49 (UTC)	2009.03.11 16:49:49 (UTC)	2009.03.11 16:53:29 (UTC)	140	1000	1000	505483 (realloc)
✓	r / r	stanley's	2009.03.11 16:50:05 (UTC)	2009.03.11 16:50:05 (UTC)	2009.03.11 16:52:52 (UTC)	235	1000	1000	505484 (realloc)
✓	r / r	stoughton's	2009.03.11 16:50:10 (UTC)	2009.03.11 16:50:10 (UTC)	2009.03.11 16:52:57 (UTC)	359	1000	1000	505485 (realloc)

Picture 5: Deleted contents in the nssal's account

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?

As we already explained, Jhuisi transferred the Mardi Gras images through ssh encrypted channel. When we see the auth.log file, we can find that on Mar. 11 12:01:35 2009, jhuisi tried to execute backd00r executable using jhuisi account, but it was not normally executed because the jhuisi account is not SUDO user account, so jhuisi connected to nssal's PS3 system again using nssal account and executed the backd00r executable.

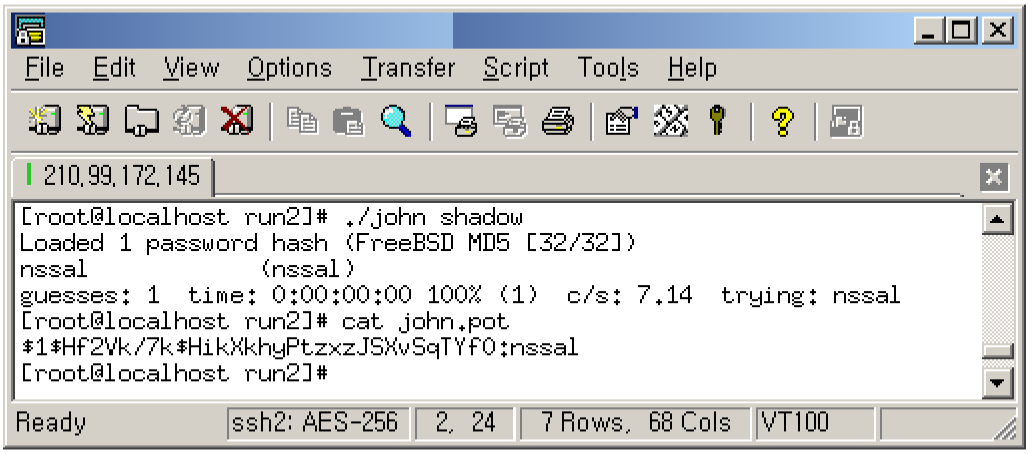

ctrc@ctrc-desktop: /mnt/var/log
파일(F) 편집(E) 보기(V) 터미널(T) 도움말(H)

```
ctrc@ctrc-desktop:/mnt/var/log$ cat auth.log | grep './backd00r'
Mar 11 12:01:35 nssal-ps3 sudo:   jhuisi : user NOT in sudoers ; TTY=pts/2
; PWD=/home/jhuisi ; USER=root ; COMMAND=nssal ./backd00r
Mar 11 12:08:59 nssal-ps3 sudo:    nssal : TTY=pts/3 ; PWD=/home/jhuisi ; U
SER=root ; COMMAND=./backd00r
ctrc@ctrc-desktop:/mnt/var/log$
```

Picture 6: auth.log analysis

Additional analysis

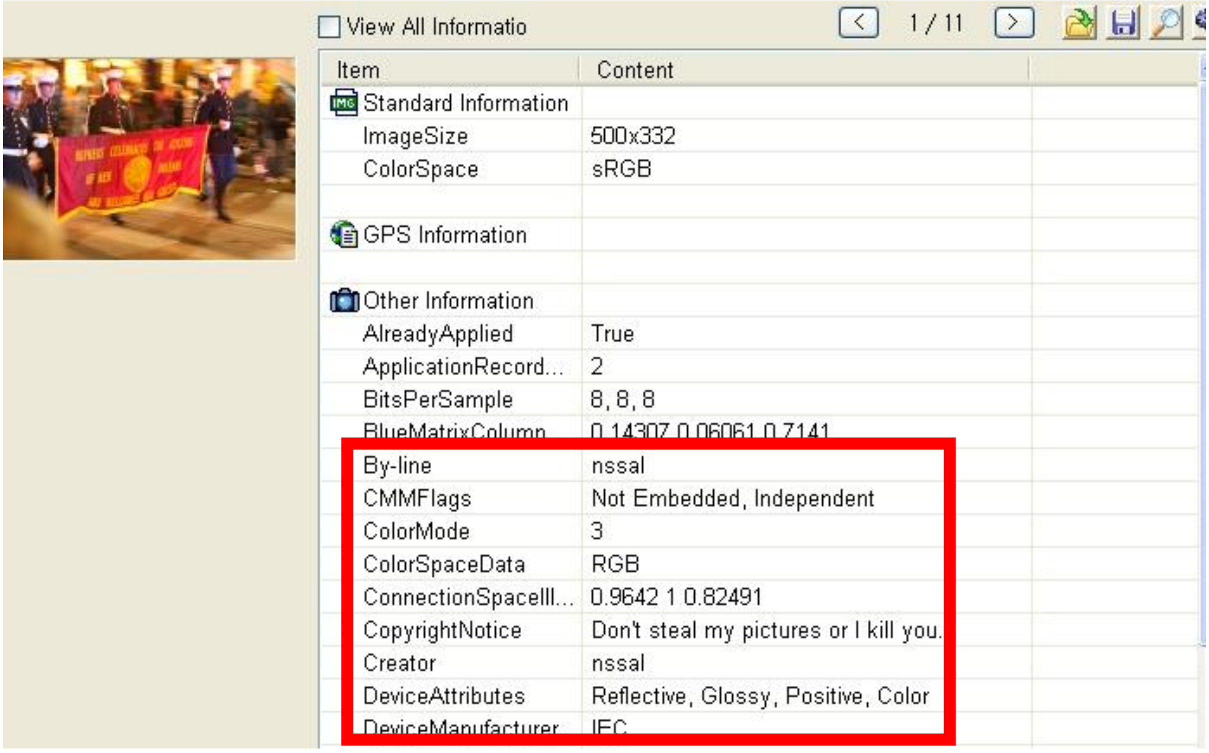
The ID/Passwords in the "/etc/shadow" file in nssal-linux-side-fs.dd and jhuisi-linux-side-fs.dd file has been found out using John the ripper program: the ID is "nssal" and the password is "nssal".



```
[root@localhost run2]# ./john shadow
Loaded 1 password hash (FreeBSD MD5 [32/32])
nssal            (nssal)
guesses: 1  time: 0:00:00:00 100% (1)  c/s: 7.14  trying: nssal
[root@localhost run2]# cat john.pot
$1$Hf2Vk/7k$HikXkhyPtzxzJSXvSqTYf0:nssal
[root@localhost run2]#
```

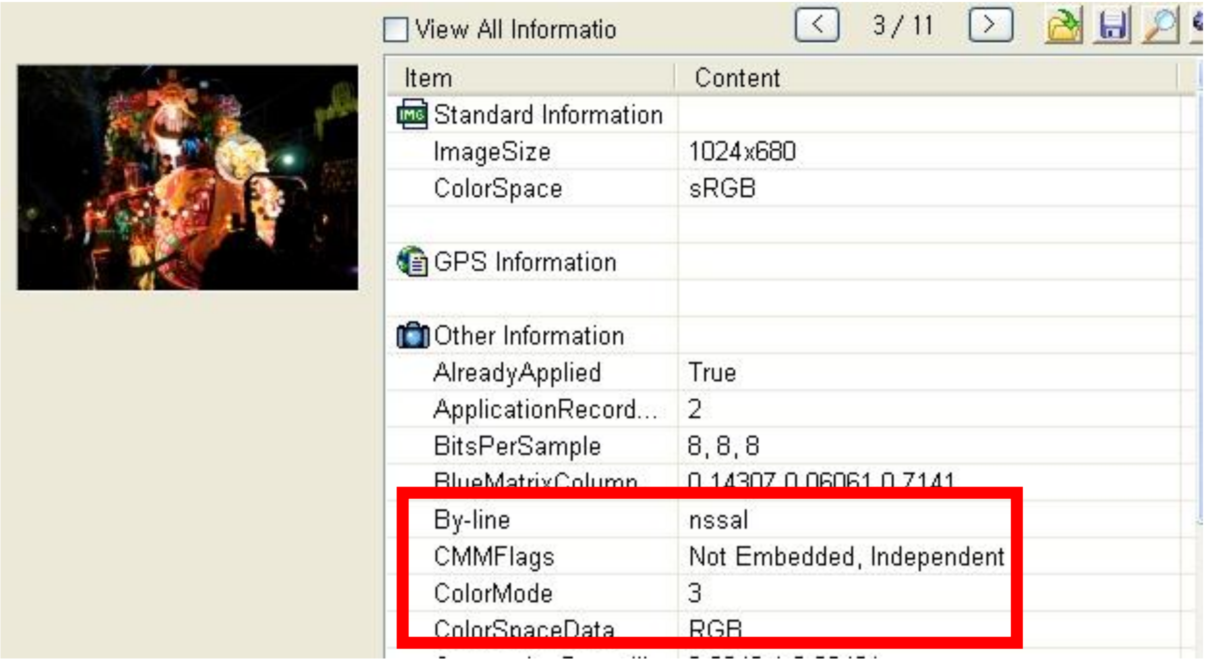
Picture 7: Using John the Ripper to crack password

We could also find exif information of Mardi Gras images to incriminate the creation of the images.



Item	Content
Standard Information	
ImageSize	500x332
ColorSpace	sRGB
GPS Information	
Other Information	
AlreadyApplied	True
ApplicationRecord...	2
BitsPerSample	8, 8, 8
BlueMatrixColumn	0.14307 0.06061 0.7141
By-line	nssal
CMMFlags	Not Embedded, Independent
ColorMode	3
ColorSpaceData	RGB
ConnectionSpaceIl...	0.9642 1 0.82491
CopyrightNotice	Don't steal my pictures or I kill you.
Creator	nssal
DeviceAttributes	Reflective, Glossy, Positive, Color
DeviceManufacturer	IEC

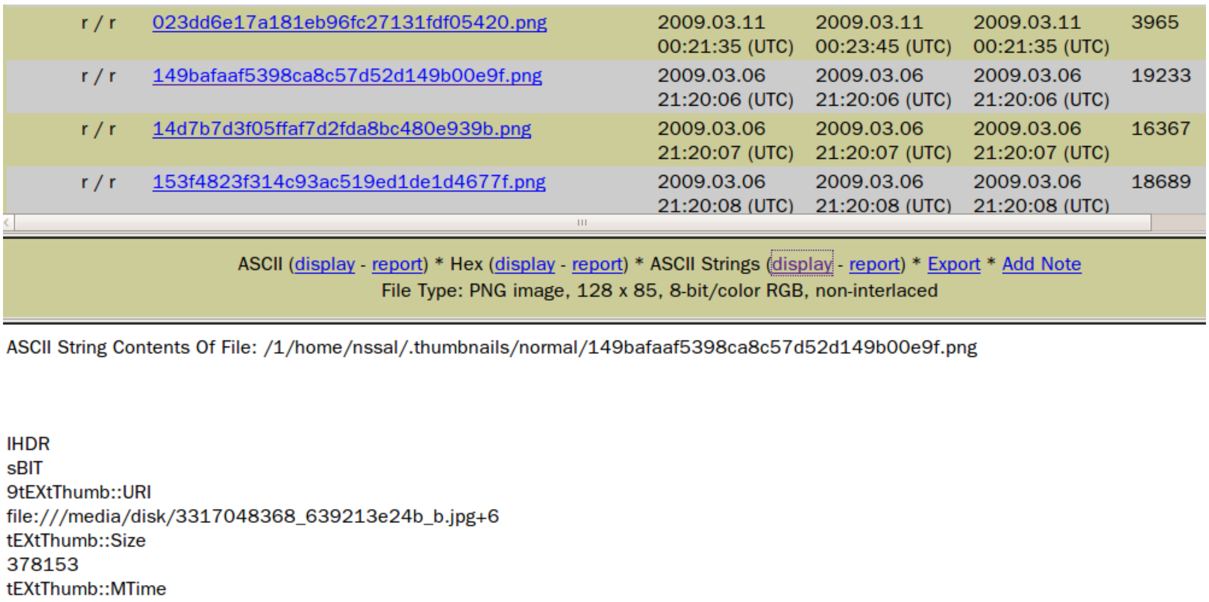
Picture 8: exif information of the Mardi Gras image



Item	Content
Standard Information	
ImageSize	1024x680
ColorSpace	sRGB
GPS Information	
Other Information	
AlreadyApplied	True
ApplicationRecord...	2
BitsPerSample	8, 8, 8
BlueMatrixColumn	0.14307 0.06061 0.7141
By-line	nssal
CMMFlags	Not Embedded, Independent
ColorMode	3
ColorSpaceData	RGB

Picture 9: exif information of the Mardi Gras image

Also we could find a thumbnail which assumes to be the thumbnail in the nssal's USB drive under the /home/nssal/.thumbnails/normal directory.



r / r	023dd6e17a181eb96fc27131fdf05420.png	2009.03.11 00:21:35 (UTC)	2009.03.11 00:23:45 (UTC)	2009.03.11 00:21:35 (UTC)	3965
r / r	149bafaaf5398ca8c57d52d149b00e9f.png	2009.03.06 21:20:06 (UTC)	2009.03.06 21:20:06 (UTC)	2009.03.06 21:20:06 (UTC)	19233
r / r	14d7b7d3f05ffaf7d2fda8bc480e939b.png	2009.03.06 21:20:07 (UTC)	2009.03.06 21:20:07 (UTC)	2009.03.06 21:20:07 (UTC)	16367
r / r	153f4823f314c93ac519ed1de1d4677f.png	2009.03.06 21:20:08 (UTC)	2009.03.06 21:20:08 (UTC)	2009.03.06 21:20:08 (UTC)	18689

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: PNG image, 128 x 85, 8-bit/color RGB, non-interlaced

ASCII String Contents Of File: /1/home/nssal/.thumbnails/normal/149bafaaf5398ca8c57d52d149b00e9f.png

```
IHDR
sBIT
9tEXtThumb::URI
file:///media/disk/3317048368_639213e24b_b.jpg+6
tEXtThumb::Size
378153
tEXtThumb::MTime
```

Picture 10: Thumbnail found at the /home/nssal/.thumbnails/normal directory

Conclusion

To summarize the analysis result, the Mardi Gras images had been originally generated by nssal, but jhuisi transferred the files without authorization through ssh channel. To clearly confirm it, we had had to decrypt the encrypted ssh channel, but we couldn't because communication entities generate large size of a prime number and delete it right after creating a session key by exchanging public keys.