DFRWS Forensic Challenge 2009

Knut Kröger[1] · Sven Wegner[2]

[1] University of Applied Sciences Brandenburg
kroeger@fh-brandenburg.de

[2] University of Applied Sciences Brandenburg
wegners@fh-brandenburg.de

Summary

The findings of a forensic investigations are summarized in this document. The investigations occurred in connection with the DFRWS Forensic Challenge 2009. Forensic duplicates (Images) and network monitoring were examined. Definitively the questions formulated by the DFRWS are answered.

Introduction

In this short report, the results of a forensic investigation of the annual DFRWS Conference Forensic Challenge 2009[1] are presented. The two authors participated in this Challenge in within the scope of a practical student project as part of the course IT- and Media Forensics at the University of Applied Sciences in Brandenburg, Germany in summer term 2009. Professors C. Vielhauer and R. Creutzburg, whom the authors would like to express their thankfulness, have supervised the course.

Since the findings reported here have been accomplished only shortly before the submission deadline and due to the fact, that English is not the authors native language, we hope for the understanding in case of any stylistic and grammatical shortcomings in this report. Authors will gladly provide a revised version at a later point in time, if required by the reviewing committee.

The authors handle the following forensic investigations with according to the Investigative Process Model of Casey[2] . Here the forensic duplicates were provided, so the authors put first with the categorie Harveresting and work the model up to the Reporting. First of all the hidden, deleted or camouflaged data are put out. After this in the Reduction in order to be able to organize the large amount of data separated the wheat from the chaff. In the phase Organization and Search irrelevant data are eliminated. In the extensive Analysis phase find instead of detailed analyses and the file contents are considered the first time. The contents and contexts become evaluate and then the data should fused, correlated and validated. The forensic investigation is closed with a report.

[1] http://www.dfrws.org/

[2] Casey Eoghan: Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet. *Academic Press*, 2004, Second Edition

Not only the findings are supposed to be kept also the reconstruction of the results must be guaranteed through a detailed documentation.

1. Tools

For the forensic investigation of the storage medium copies and the network monitoring files were used several tools. The two forensic tools FTK by AccessData[3] and X-Ways Forensics[4] were used for the post mortem analysis of the images, IrfanView[5] v4.23 and EXIF-Viewer[6] v2.4 for the analyse of Exif meta data and the network analysis tools Wireshark[7], NetworkMiner and the dsniff[8] collection for the network monitoring files.

1.1 Tools for the post-mortem investigation

The forensic tool FTK were used in version 1.7 and X-Ways Forensics in version 1.3. Two tools were used, because it is important to evaluate the found Data. Besides they have extensive options and can be automatised in many fields strongly.

With the help of the Tools FTK and X-Ways Forensics it is shown which investigations were carried out and which options were activated.

The first step was the integration of the storage medium, this happens at FTK with the help of a Wizard. In the Wizard the options were set as the follows.

I. Case Log Options: all boxes were checked (see figure 1)

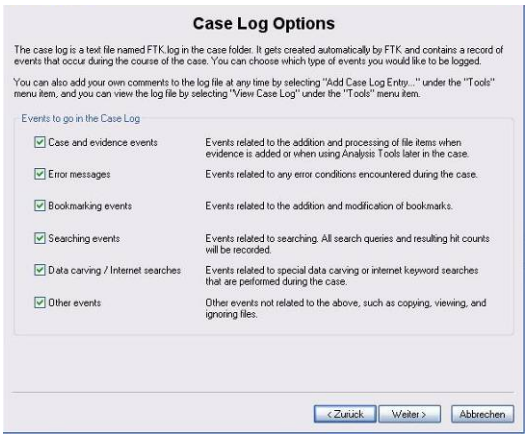


figure 1 Case Log Options

II. Processes to Perform: all boxes were checked (see figure 2)

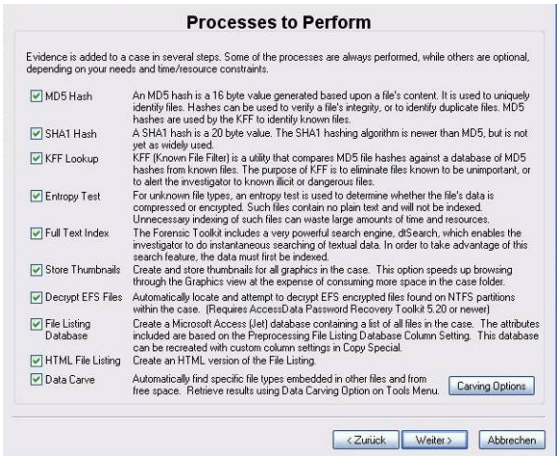


figure 2 Processes to Perform

a. for Data Carve: all file types were selected, the minimum file size was set to 1kb and the box „automatically add carves items to case“ was checked (see figure 3)

[3] Forensic Toolkit v1.7 http://www.accessdata.com/forensictoolkit.html

[4] X-Ways Forensics v1.3 http://www.x-ways.net/forensics/index-d.html

[5] http://www.irfanview.de/

[6] http://www.amarra.de/exif.htm

[7] Wireshark v1.0.8 http://www.wireshark.org/

[8] Dsniff v2.3 http://naughty.monkey.org/~dugsong/dsniff/

figure 3 Data Carve

III. Refine Case – Default: it was pressed only the button „Include all items“ (see figure 4)

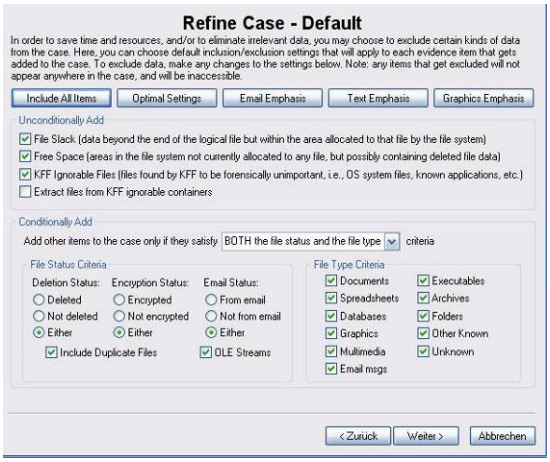


figure 4 Refine Case

IV. Refine Index – Default: do not change anything check the box „kff ignorable files“ (see figure 5)

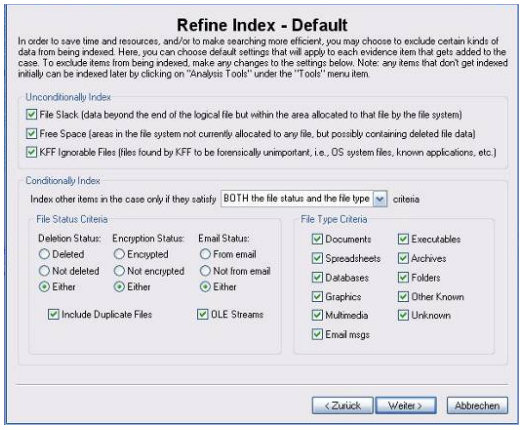


figure 5 Refine Index

V. Add evidence: all of one Person and change TimeZone to “Europe/Berlin“ (see figure 6)

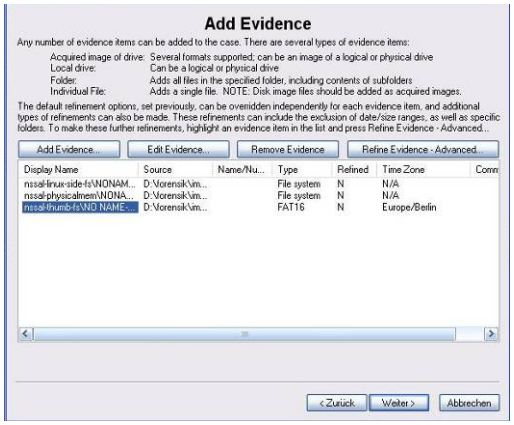


figure 6 Add evidence

With X-Ways Forensics a new case was created. No options were changed. All storage medium belonging to a person were bound into the case and traversing automatically (see figure 7). After the integration of the images, an index was created and the file carving was carried out.

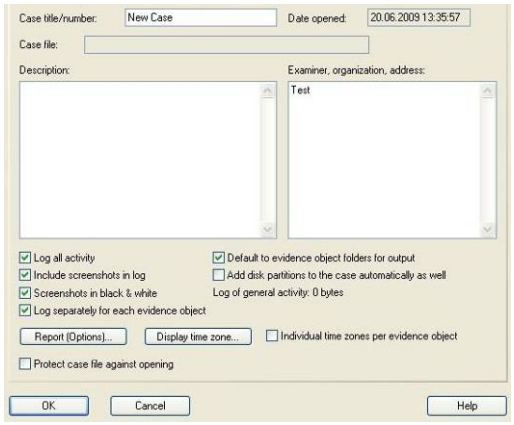


figure 7 X-Ways Forensics

Summary

Both forensic tools are well suitable for the analysis. For the investigation of a large volume of data the tool FTK is the better one. FTK carries out with the integration of the storage medium a file Carving automatically. During the integration of the storage medium FTK

does a file carving automatically. Additional an index for all storage media was created and they are represented sortedly. These operation steps must be carried out with X-Ways Forensics manually. A further advantage of FTK is the filter database[9] provided by Access-Data, these can downloaded for free on the manufacturer page and will integrate into the tool FTK. The database contains signatures of known files and program's and make these immediately visible during the analysis of a storage medium.

1.2 Network Tools

The following section are supposed to be imagined used network tools, for the evaluation of the *.pcap files, shortly. Focus during the selection of used tools lay onto open source programs or free solutions. Subsequently description are supposed to be particularly to the needed function of the forensic analysis, no complete function report.

dsniff - Suite

The dsniff - suite[10] is a collection of tools for network analysis. There are also programs to fake or slow down network traffic and to be able to a man-in-the-middle-attack.

The console programs are interesting for the later network analysis will be presented. These are in addition to the live analysis in the situation to read and evaluate *.pcap files.

- dsniff
  - searching the network monitoring according to passwords of unencoded protocols (ftp, telnet, smtp, http, …)
  - exemplary call:

```
dsniff -p nssal-capture-1.pcap > output_dsniff_nssal_1.txt
```

- mailsnarf
  - makes possible to extract e-mails from pop- and smtp-traffic
  - exemplary call:

```
mailsnarf -p nssal-capture-1.pcap > output_mailsnarf_nssal_1.txt
```

- urlsnarf
  - filter the requested url's from the network monitoring
  - exemplary call:

```
urlsnarf -p nssal-capture-1.pcap > output_urlsnarf_nssal_1.txt
```

- msgsnarf
  - filter chat-news from Messengern (AOL Instant Messenger, ICQ 2000, IRC, MSN Messenger, Yahoo Messenger)
  - exemplary call:

```
msgsnarf –p nssal-capture-1.pcap > output_msgsnarf_nssal_1.txt
```

Network Miner

This open source tool, with graphic user interface, designates itself on the own internet presence[11] as a "Network Forensic Analysis Tool" (NFAT). It is made possible for the forensic observer to provide a first comprehensive survey of the network. Network Miner can be a passive network sniffer or can used to read in capture pakets files, in order to carry out an offline analysis. In this case Network Miner can identify the used operating systems, sessions, host names, open ports and so on. It is also possible to reconstruct the sent files in a folder structure. Thus e.g. a complete web page with their embedded contents can be considered.

Wireshark

The successor of ethereal is an extensive paket sniffer which one can combine TCP/IP packets and analyze them. Wireshark[12] offers filter techniques in order to reduce the mostly quite extensive raw of data to the essential informa-

[9] kff-kff_library_file-29_sep_2008.exe (http://www.accessdata.com/downloads.html)

[10] http://www.monkey.org/~dugsong/dsniff/

[11] http://networkminer.sourceforge.net/

[12] http://www.wireshark.org

tion. The gui-program keeps on offering different output formats and the extraction guarantees in this way to different data. The function „Follow TCP Stream" is especially, because with this opinion it is possibly to unite a coherent data stream. Furthermore a summary and a protocol hierarchy of the recorded pcap files can be created. You can find this options under “Analyse” and “Statistics”. A other reasonable feature is the automatized name resolution for TCP/IP pakets, which to be found at “View-> Name Resolution-> Enabe for Network Layer”.

2. Analysis

This chapter deals with the methods which were used for the analysis.

For the data carriers used techniques were the file carving, the analysis of the Exif meta data and searching the index.

During the analysis of the network monitoring is proceeded chronological. First of all that pcap file (nssal-capture-1.pcap.bz2) is examined that activated the investigations. Following the second monitoring (nssal-capture-2.pcap.bz2) of the suspect. At last the network monitoring (jhuisi-capture-1.pcap.bz2) of the John Hopkins University is considered. In this chapter only the used techniques are presented, the evaluation of the analysis happens with the aid of the questions in the chapter 3.

2.1 Analysis the images

The following image were investigated:
- jhuisi-linux-side-fs.dd
- nssal-linux-side-fs.dd
- nssal-physicalmem.dd
- nssal-thumb-fs.dd

A file carving was done and the found data were sorted by type and arranged contents.

The pictures classified as interesting were analysed with IrfanView v4.23 und EXIF-Viewer v2.4 to find possible meta data. With the search function were searched for search words like Mardi Gras, John Hopkins, Backdoor, nssal und darkXside.

File carving

The following files were searched and saved at the file carving (See figure 8)

I. X-Ways Forensics: go to tools -> disk tools and click „file recovery by type“

   It was searched for the file types: microsoft office, openoffice, rtf, html, all archive file types, mpg, avi, wav, jpg, png, tiff, bmp, gif.

   X-Ways Forensics sorts the found files into separately created folders, these folders must be screened and evaluated separately

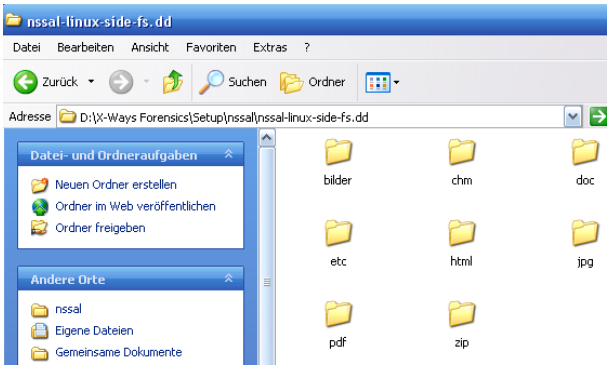


figure 8 files searched and saved at the file carving

II. FTK: The file carving can be carried on already at the integration of the storage medium (see figure 2 and 3). It was searched for the file types: BMP, GIF, JPEG, PNG, EMF, PDF, HTML, AOL/AIM, OLE.

   At FTK the found files were classified into the program structure and could be analysed directly (see figure 9).

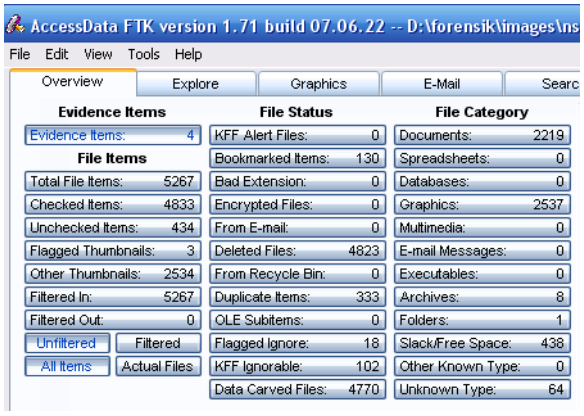


figure 9 Assortment and editing of the found data

All found files were examined and sorted concerning the problem definition. It was found, e.g., more than 10k images, 30 archive files and 4k documents. These were sorted, evaluated and stored in the File folder. For a detailed listing see table 1 .

Found file types	Number of files (approx.)
Graphics	4700
HTML documents	4500
PDF documents	50
CHM documents	2
Archive (zip, rar…)	30

Table 1 Number of found files

Use of the paging function

With the paging function were searched for terms witch are interesting to answer the questions.

Search terms were, e.g.: Mardi Gras, John Hopkins, Backdoor, nssal and concerning the network analysis darkXside.

Investigation for possible metadata in pictures

The Exchangeable image file format (Exif) is a specification for the image file format used by digital cameras. Exif add a specific metadata tag to an JPEG,TIFF and RIFF file. It is not supported in JPEG 2000, PNG, or GIF. The metadata tags defined in Exif cover a broad spectrum of information for example date and time, camera settings, a thumbnail for previewing the picture on the camera's LCD screen, in file managers, or in photo manipulation software, and descriptions and copyright information. All images which used for closer investigating were examined for Exif-information.

2.2 Analysis the pcap files

During the analysis of the network monitoring is proceeded chronological. First of all that pcap file (nssal-capture-1.pcap.bz2) is examined that activated the investigations. Following the second monitoring (nssal-capture-2.pcap.bz2) of the suspect. At last the network monitoring (jhuisi-capture-1.pcap.bz2) of the John Hopkins University is considered. At every *.pcap file the presented console programs are used first of all. These are designed to a certain task for the overcoming and can supply so interesting starting points. If too many data accumulate, they are only consulted if required.

nssal-capture-1.pcap

The programs „dsniff", „mailsnaff" and „msgsnaff" could not extract any information. On the other hand „urlsnaff" extracted onto 800 url's from the *.pcap file. These outputs are redirected into text files and only consulted at to become needs.

The introduced tool "Network Miner" extracts extensive data from the "nssal-capture-1.pcap" file. These files could be assigned to 81 ip-addresses and held in a folder structure. That in extracted website to be seen in figure 10 could be reconstructed with the aid of "Network Miner". A comparison with the original web site (see figure 10), underlines the correctness of the extracted data.

figure 10 network miner – extracted website

figure 11 original website

This is supposed to show how was proceeded in order to comprehend the held communication exemplary. The program “Wireshark” identified the suitable url’s to the single ip-addresses (when which ones existed) and so the orientation facilitated which web pages were called.

The result page of a search at google.com could be extracted from the logged traffic. It could comprehend that syntax „mardi gras" was searched. The found results were visited by the user after each other. Departure from the gained findings seeing in table 2.

url	Comment
www.google.com	search for „mardi gras"
	results of the search
www.mardigrasday.com	visit the site “About Mardi Gras Madness, Official Site of Mardi Gras 2009”
Mardigras-day.makeparties.com	Advertising on www.mardigrasday.com
Mardigras-day.makeparties.com	visit the announced online shop for costume
www.mardigrasgalveston.com **www.holidays.net** **www.toomeys-mardigras.com**	visit another result from that google search "Referer: http://www.google.com/search?hl=en&q=mardi+gras&start=40&sa=N"
www.huffingtonpost.com	website contains flash elements of the site sharethis.com

table 2 departure url's

The listed calls above could dedicated a client in the „Network Security and System's Administration Lab”[13] at the University of New Orleans[14].

In addition numerous connections could be identified of the client to the domain „homeps3.svo.online.scee.com". These are to be assigned to “SONY COMPUTER ENTERTAINMENT EUROPE".

nssal-capture-2.pcap

In this monitoring a lot of traffic falls on two url’s. On one *.playstation.net, which with the assist of whois tools[15] could be related to „Sony Computer Entertainment INC." On the other hand several url’s could be assigned to the company called Akamai. This is an business which offers load distribution of WWW contents.

The console programs “dsniff”, “mailsnarf“ and “msgsnarf“ had no findings only “urlsnarf“

[13] http://cs.uno.edu/facilities/nssal.htm

[14] http://www.cs.uno.edu/

[15] http://whois.domaintools.com/

could extract data, but would only used if required.

The client with the ip-address 137.30.123.78 (mobile62.cs.uno.edu) requested the files in table 3 over „scea-home.playstation.net".

MaleNinja_Signage_9x16Portait.jpg
Listen@Home_Home_256x256.jpg
Killzone2_Home_billboard2_template.jpg
Killzone2_Home_billboard5_template.jpg
Killzone2_Home_billboard4_template.jpg
WelcomeOpenBeta_Home_billboard_9x16.jpg
WarHawk_Home-PriceDrop_HomePoster_USFR.jpg
MaleNinja_Signage_9x16Portait.jpg
NinjaVsPirate_Home_512x512_v1.jpg
Fireworks_Home_billboard_01.jpg
Killzone2_Home_billboard6_template.jpg
FemaleNinja_Signage_9x16Portait.jpg

table 3 requested files

Some of the files could be extracted. In this case one recognize that the extracted file „Killzone2_tv_spot_w_arg10.mp4" is approx 10 Megabyte large and forms so an essential part of the 24 Megabyte large nssal-capture-2.pcap file.

Also an encoded communication being find in the monitoring between the ip-addresses 128.220.249.83 and 137.30.123.40. Both addresses could be identified, see table4.

ip-address	name resolution	location
128.220.249.83	ps3.isi.jhu.edu	The Johns Hopkins University Information Security institutes (JHUISI) [16]
137.30.123.40	nssal-ps3.local /mobile24. cs.uno.edu	University of New Orleans

table4 identified ip-adresses

The communication between the two ip-addresses was examined in "Wireshark" more precisely.

In this case the focus was onto the not encoded communication (see figure 122). With the option „Follow TCP Stream" packets were joined and examined for interesting contents. If no interesting contents could be identified, the TCP Stream would extracted. After several repetitions of these steps a plain text communication could be identified in a TCP Stream.

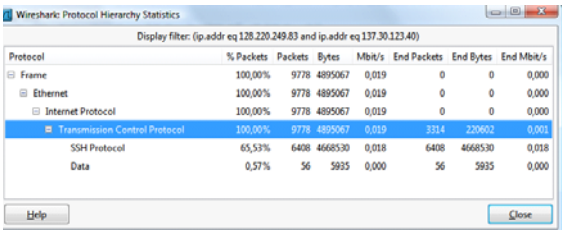


figure 122 Protocol Hierarchy Statistics of the communication between ps3.isi.jhu.edu and nssal-ps3.local

In figure 133 that one combined TCP stream is to be recognized. The communication between the two suspicious systems occurs onto the ports 56515 and 45541. With the following filter, this communication can be called directly.

(ip.addr eq 128.220.249.83 and ip.addr eq 137.30.123.40) and (tcp.port eq 56515 and tcp.port eq 45541)

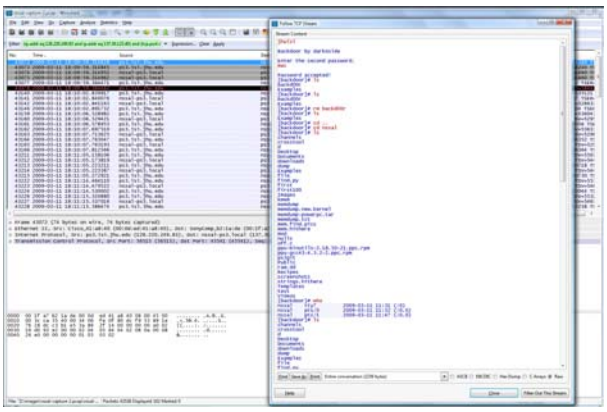


figure 13 identified „Backdoor by darkXside"

[16] http://web.jhu.edu/jhuisi/

The communications begins at 18:09:59 o'clock and end at 18:16:13 o'clock, because to this time the network monitoring ends. The script is extracted as RAW file.

jhuisi-capture-1.pcap

In this network dump a great part of the traffic fells again on ip-addresses witch could be assigned to „Sony Computers Entertainment INC". The console program “dsniff” identifies one udp communication between the suspicious systems.
The programs “Wireshark” and “Network Miner” extracted pictures (table 5) from the network monitoring.

The names of these files are releated with the requested pictures from the second capture file (nssal-capture-2.pcap).

A0019.png
FemaleNinja_Signage_9x16Portait.jpg
FemalePirate_Signage_9x16Portait.jpg
Fireworks_Home_billboard_01.jpg
Fireworks_Home_billboard_02.jpg
I0025.png
Killzone2_Home_billboard1_template.jpg
Killzone2_Home_billboard2_template.jpg
Killzone2_Home_billboard3_template.jpg
Killzone2_Home_billboard4_template.jpg
Killzone2_Home_billboard5_template.jpg
Killzone2_Home_billboard6_template.jpg
Listen@Home_Home_256x256.jpg
MaleNinja_Signage_9x16Portait.jpg
MalePirate_Signage_9x16Portait.jpg
NinjaVPirate_Home_512x512_v2.jpg
NinjaVsPirate_Home_512x512_v1.jpg
ResidentEvil_StudioLot_16x9_Billboard684x384.png
TheUglyTruthposter.jpg
WarHawk_Home-PriceDrop_HomePoster_USFR.jpg
WelcomeOpenBeta_Home_billboard_9x16.jpg

table 5 extracted files

Through the above introduced filter for “Wireshark” can be searched directly, for the interesting communication between the two suspicious clients. Also here the script is found. The monitoring goes until 18:16:40 o'clock, few seconds longer than the nssal-capture-1.pcap file. But does not contain any new informationen about the script. Definitively the script is extracted as RAW file, too.

3. Evaluation of the results

In this chapter the results are evaluated. For it the questions from the conceptual formulation are used. The following questions have been asked to assist investigators:

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?

Answer of the question 1 and 5:

On the data carriers a big number of information was reconstructed, primarily graphics and html files. The figures and html files extracted from the images were mostly parts of tutorials and manuals. From it the following user activities can be conducted:

Both users (from the nssal and the jhuisi PS3) had the same interests or on user has used the same data on both systems. Because on both computers were found the same HTML and image files. Concerning the contents the on or both were interested for linux (e.g. ubuntu), programming (e.g. magick++) and network technologies like packet filtering. In addition, SSH -protocols and -files were found on both computers. So it can be suspected that an en-

coded connection was carried out. For a detailed listing see the folder of results. The Analysis of the users activities points out that the two users knew each other.

From the network dumps could also extract a number of same pictures. It looks like as there play the same PS3 Game. Some graphics seem to be avatars. This icons was found on both suspicious clients.

The extracted mardi gras picture from network monitoring nssal_1 are from a google search. This pictures wasn´t shared by the PS3's.

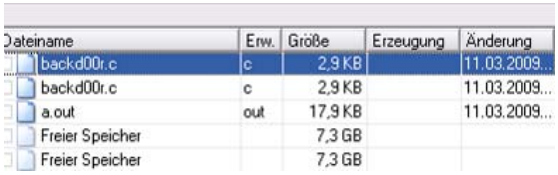
Answer of the question 2:

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

On both computers were found an indication for the use of a BitTorrent client[17] (see figure 8)

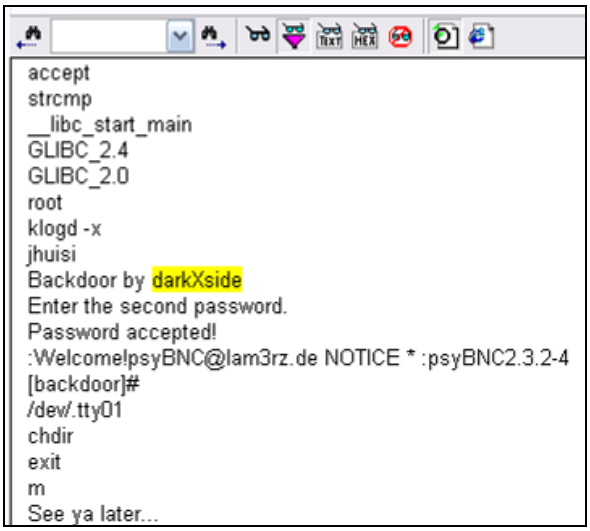
figure 14 fast, easy, and free multi-platform BitTorrent client

Also it was found a c-programmed backdoor script in the file backd00r.c. It was found in two of three network dumps (nssal2 and jhuisi) and on the jhuisi PS3 image. The script is even told to „Backdoor by darkXside". After a short internet research a website[18] was be found which provides the supposed script. On the computer of the nssal PS3 the program was executed and logged in the klogd. On the nssal PS3 the backd00r.c was not found. See figure 11 for the found backd00r.c and figure 12 for the klogd on the nssal PS3.



Dateiname	Erw.	Größe	Erzeugung	Änderung
backd00r.c	c	2,9 KB		11.03.2009...
backd00r.c	c	2,9 KB		11.03.2009...
a.out	out	17,9 KB		11.03.2009...
Freier Speicher		7,3 GB		
Freier Speicher		7,3 GB		

figure 15 the found backd00r.c on the jhuisi System



```
accept
strcmp
__libc_start_main
GLIBC_2.4
GLIBC_2.0
root
klogd -x
jhuisi
Backdoor by darkXside
Enter the second password.
Password accepted!
:Welcome!psyBNC@lam3rz.de NOTICE * :psyBNC2.3.2-4
[backdoor]#
/dev/.tty01
chdir
exit
m
See ya later...
```

figure 16 the klogd on the nssal PS3

Answer of the question 3:

Is there evidence of collaboration with an outside party? From the point of view of the data carrier analysis the third question cannot be answered. The images and dumps haven´t any information about an outside party.

Answer of the question 4:

Is there evidence that illicit data (specifically, Mardi Gras images) was exchanged? If so,

[17] http://www.transmissionbt.com/

[18] http://www.packetstormsecurity.org/UNIX/penetration/rootkits/

what can be determined about that data and the manner of transfer?

With the file carving were found pictures on the two computers and inside the first network monitoring. These were identified as mardi grass pictures and guaranteed for certain. Founded pictures were identical on the two computers. See figure 11 exemplarily. How the data were exchanged between both computers, cannot be found out in the data carrier analysis. For a detailed listing see the folder of results.

figure 17 a found Mardi Gras Picture on the nssal PS3

figure 18 found the same Mardi Gras Picture on the jhuisi PS3

Answer of the question 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?

It were guaranteed 2 Html files were classified by McAffee as an “Exploit-ObscuredHtml” and “ObfuscatedHtml” (see table 2). If it really concerns exploit files, there can be a tip to an remote or unauthorized access to the nssal system.

File	McAfee+Artemis
DriveFreeSpace310[2476]--HTML_16142768[313][2476].htm	Exploit-ObscuredHtml
DriveFreeSpace342[2671]--HTML_5693490[345][2671].htm	ObfuscatedHtml

table 6 exploit html files

Another important clue is the guaranteed backdoor script. It was evident that the Script was only on the jhuisi system as a source code and could be found on the nssal system only as a call in the logging files. The communication was kept where the script is executed. In the network monitoring nssal_2 and jhuisi the script could be proved. Out of this can be closed that an access of the jhuisi system to the nssal system was carried out (see also reply to question 2). From the point of view of the data carrier analysis there are two essential clues these the accused be able to relieve.

All results were stored in the folder named DFRWS_Challenge_Results.