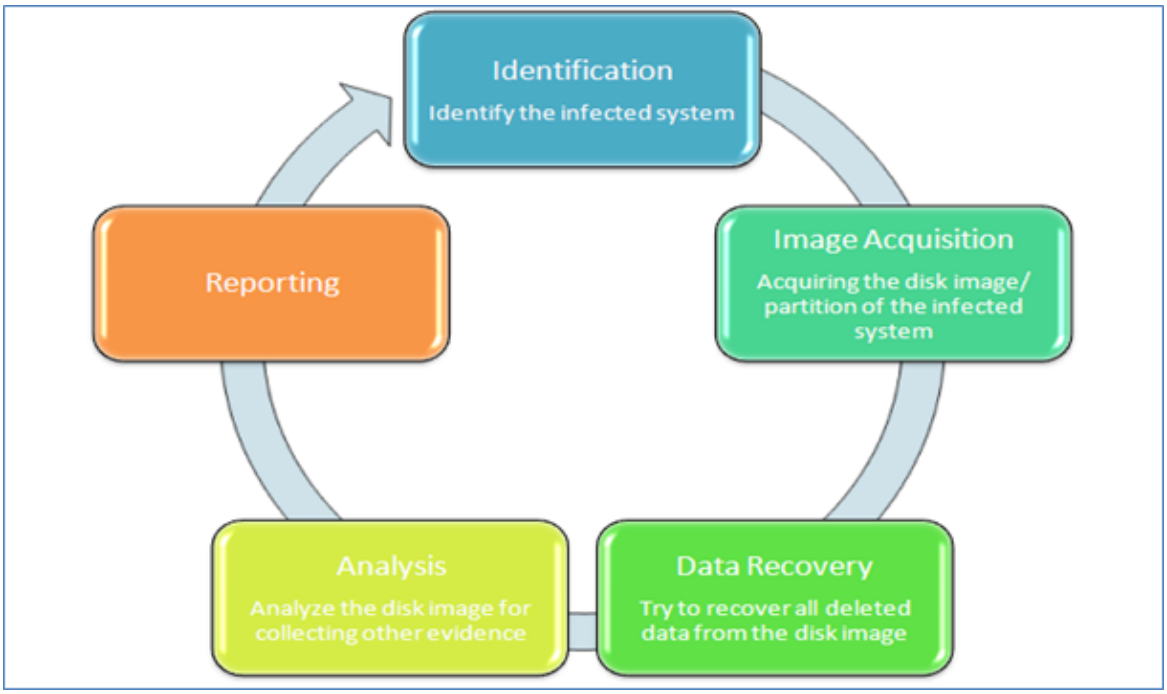
Linux and Disk Forensics

POSTED IN DATA RECOVERY, FORENSICS ON JUNE 6, 2013

Introduction:

A digital forensic investigation generally consists of five major steps [Figure-1]:

- Identification
- Data Acquisition
- Data Recovery
- Analysis
- Reporting



[Figure-1: Forensics steps]

A brief about various Linux tools available:

There are multiple Linux tools used for imaging and analysis of disks and drives. They also come as several distributions containing all necessary tools to carry out Forensics, e.g. BackTrack, FIRE, Knoppix-STD, Linux LEO, Penguin Sleuth. All of them have an excellent collection of tools required for forensics. Some useful tools we

Forensics Analysis tools: bulk_extractor, Miss Identify, RegLookup, readpst

Forensics suites: Autopsy, Sleuth Kit, PTK

As published elsewhere, the complete description of tools and their uses are out of scope of this article, we'll be just using them for our forensics, as you may get a fair idea about them during our process. We shall be using BackTrack(BT) for our analysis. You could pretty much use any distribution available as all have mostly common necessary tools. You could use any normal Linux flavors such as Fedora, RedHat, and Ubuntu as well, but the advantage of using distributions like BT is that they already have a fair collection of these tools. Otherwise you may need to install them.

To keep our work neat, clean, and easily understandable, we will create a few directories in order to organize the data. We may need one directory for collecting our proofs, and another directory to browse the suspected image of the disk. We shall redirect all of the results from our analysis to the proof directory. The location of the directories is completely arbitrary but I prefer them on the root's home:

 # mkdir /evidence

Now make a directory where we'll be doing our most of the analysis:

 # mkdir /mnt/investigation

Here we are creating the folder 'investigation' under 'mnt' directory, where we will mount all the external data for our investigation. You are completely free to create your own folder at any place; this is just for sake of better organization.

Acquire the Image:

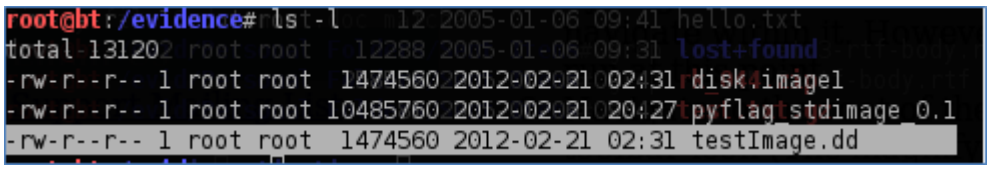
Identify the machine which needs to be investigated, and take an image of the hard disk. You can capture the disk and connect to your forensics machine in order to take its image. The disk may be anything from a hard disk to a floppy. That way, you'll have two copies of the suspected disk-one image as well as the physical disk itself. We'll be examining both images one by one. The tool 'dd' can be used to take an image of the disk by using this command:

dd if=<media/partition on a media> of=<image file>,

Here, we are taking image of the disk sdc and saving it as image.dd. You can give the image any name, and .dd is an extension just to denote that it's an image taken through 'dd' tool.

Now for this article, we'll use sample test images already available on few open source sites such as http://dftt.sourceforge.net/ , http://pyflag.sourceforge.net or http://linuxleo.com/ etc. They list excellent test images in every format to carry out test forensics. Download any disk images and unzip it in the 'evidence' directory already created.

I shall be using one of the images already downloaded from similar sites at my PC. This was created using the same command *dd if=/dev/sdc of= pyflag_stdimage_0.1,* where we have taken image of disk sdc [Figure-2]:



[Figure-2: List of sample images]

Once you download the above image copy it in blank floppy disk, we may require it later on:

 # dd if=

pyflag_stdimage_0.1 of=/dev/fd0

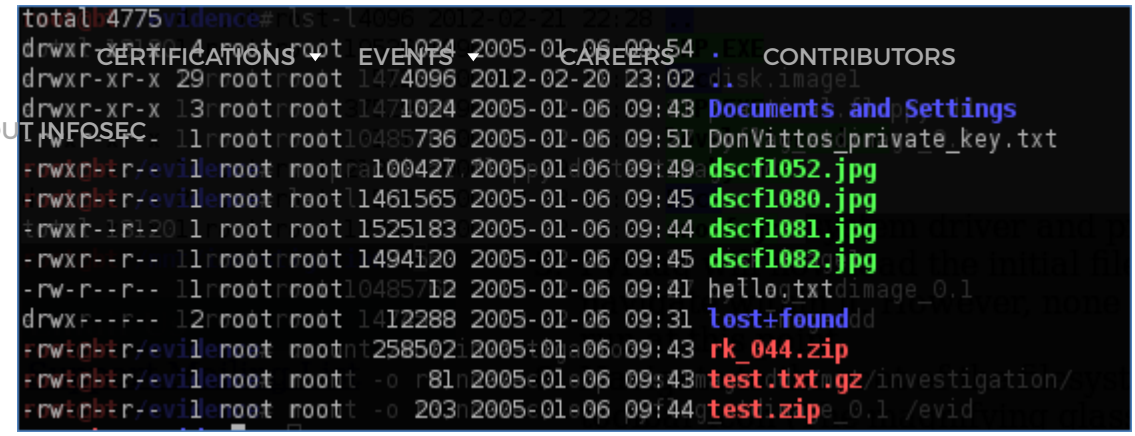
So, the image is copied into your floppy device(/dev/fd0). Now we have two copies, one in the /evidence directory and one in physical floppy device.

Image Analysis:

Now that an image has been captured, let's mount the contents to see how we can use tools. We'll mount it in our /investigation directory:

 # mount -o ro,noexec,loop pyflag_stdimage_0.1 /mnt/investigation

Here 'ro' and 'noexec' denotes that the file should be mounted as read-only and non-executable.



[Figure-3: File system in the disk image]

Now you can redirect the above output to a simple file and place it into your evidence directory. This file can be used for analyzing the files and their various attributes [Figure-4].

#ls -Ralit > /evidence/ListOfFiles

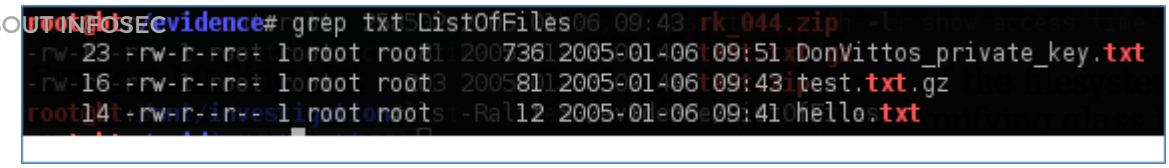
```
root@bt:/evidence# cat ListOfFiles
.:
total 4775
522242 drwxr-xr-x 4 root root    4096 2012-02-21 22:51 ..
     2 drwxr-xr-x 4 root root    1024 2005-01-06 09:54 .
    23 -rw-r--r-- 1 root root     736 2005-01-06 09:51 DonVittos_private_key.txt
    22 -rwxr--r-- 1 root root  100427 2005-01-06 09:49 dscf1052.jpg
    20 -rwxr--r-- 1 root root 1461565 2005-01-06 09:45 dscf1080.jpg
    19 -rwxr--r-- 1 root root 1494120 2005-01-06 09:45 dscf1082.jpg
    18 -rwxr--r-- 1 root root 1525183 2005-01-06 09:44 dscf1081.jpg
    17 -rw-r--r-- 1 root root     203 2005-01-06 09:44 test.zip
    16 -rw-r--r-- 1 root root      81 2005-01-06 09:43 test.txt.gz
    15 -rw-r--r-- 1 root root  258502 2005-01-06 09:43 rk_044.zip
  1281 drwxr-xr-x 3 root root    1024 2005-01-06 09:43 Documents and Settings
    14 -rw-r--r-- 1 root root      12 2005-01-06 09:41 hello.txt
    11 drwx------ 2 root root   12288 2005-01-06 09:31 lost+found

./Documents and Settings:
total 3
   2 drwxr-xr-x 4 root root 1024 2005-01-06 09:54 ..
1282 drwxr-xr-x 3 root root 1024 2005-01-06 09:54 Administrator
1281 drwxr-xr-x 3 root root 1024 2005-01-06 09:43 .

./Documents and Settings/Administrator:
total 1434
1282 drwxr-xr-x 3 root root    1024 2005-01-06 09:54 .
1285 -rwxr-xr-x 1 root root  147456 2005-01-06 09:53 outlook.pst
1283 drwxr-xr-x 2 root root    1024 2005-01-06 09:43 Local Settings
1281 drwxr-xr-x 3 root root    1024 2005-01-06 09:43 ..
  13 -rw-r--r-- 1 root root 1310720 2005-01-06 09:41 NTUSER.DAT

./Documents and Settings/Administrator/Local Settings:
```

 # grep txt ListOfFiles

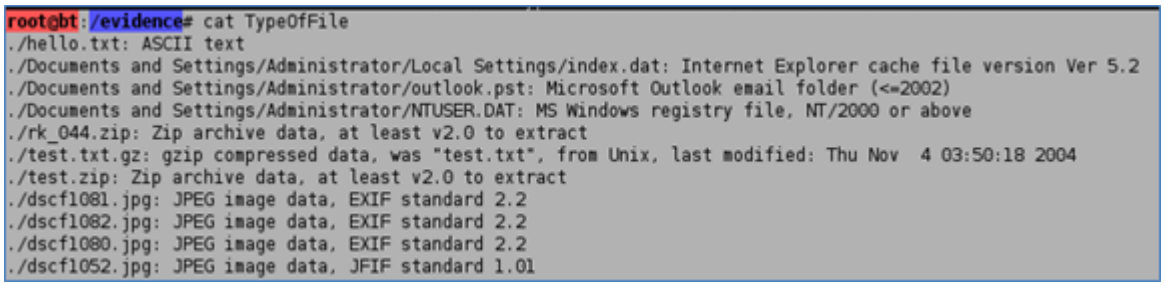


[Figure-5: Using grep to search specific files]

Another useful command might be for checking the file types. This would be useful in the scenarios where file extensions are modified. So if any .txt file is modified as a .jpg, the grep command won't be able to find it. Go to your investigation folder and provide the following command and again redirect the results in your 'evidence' directory:

 # find. -type f -exec file {} \; > /evidence/TypeOfFile

Go to evidence directory and see the contents of TypeOfFile, you get the nice view of file types [Figure-6]:



[Figure-6: Type of files]

Now we may want to view the contents of the files:

 # less hello.txt

 # strings hello.txt

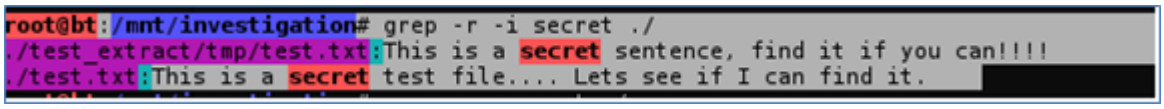
Or, if you want to see HexDump:

 # xdd hello.txt

Searching strings can be also useful in the cases where you might want to look for notoriously used terms that may give you some idea about the incident and

The following commands now can be used for searching a term [Figure-7]:

 # grep -r -i secret ./, It will look for term 'secret' in all the files of current directory

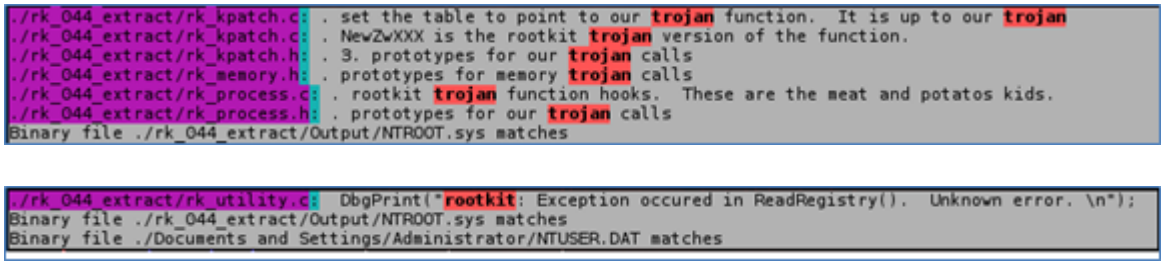


[Figure-7: Looking for suspicious keywords through the image]

 # grep –r –i rootkit ./ [Figure-8]:

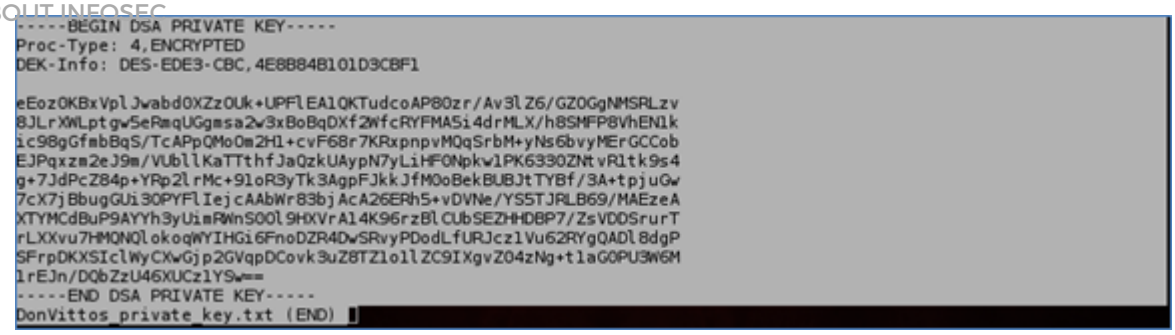
[Figure-8: Looking for suspicious keywords]

It seems that a rootkit has also been injected to the system. But where is the file? If we search through the file, at the bottom we find path of rootkit binary file. Finding of NTROOT.sys suggest that the system was infected from process hiding Trojans. So here's another search [Figure-9]:



which might have been used to get access the machine [Figure-10]:

 # less DonVittos_private_key.txt



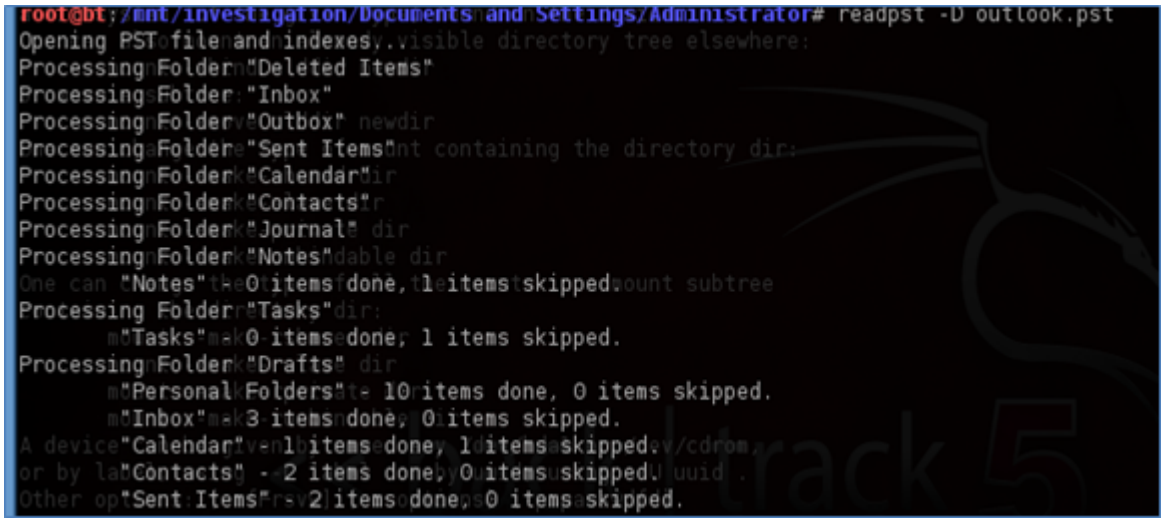
[Figure-10: View of a private key file]

Let's drill into other folders such as 'Document and Settings'. One file 'index.dat' under 'Document and Settings/ Administrator/ Local Settings' gives tracking information about sites visited. Keep looking other folders. We found something more interesting, one outlook.pst file under 'Document and Settings/ Administrator/'. This may give us more information. We will use a tool called 'readpst' available in BackTrack. 'readpst' is a command line tool which converts pst files into mbox format which in turn can be viewed and manipulated using any mail reading software.

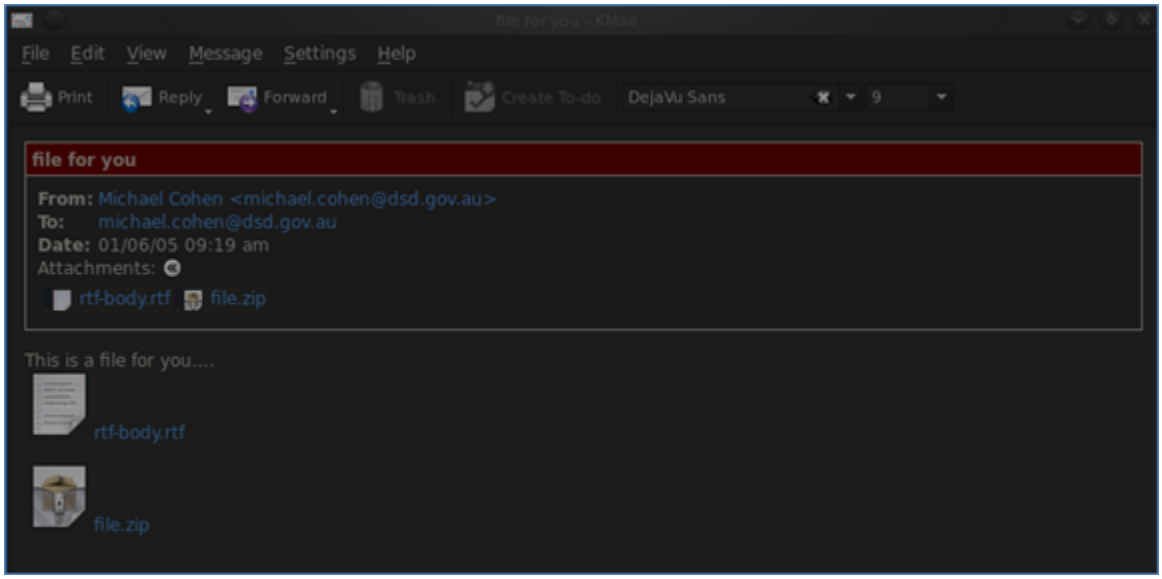
 # readpst -D outlook.pst

Option 'D' includes deleted items in the output.

This creates several folders Inbox, Sent Items, MailBox, Deleted Items etc [Figure-11].

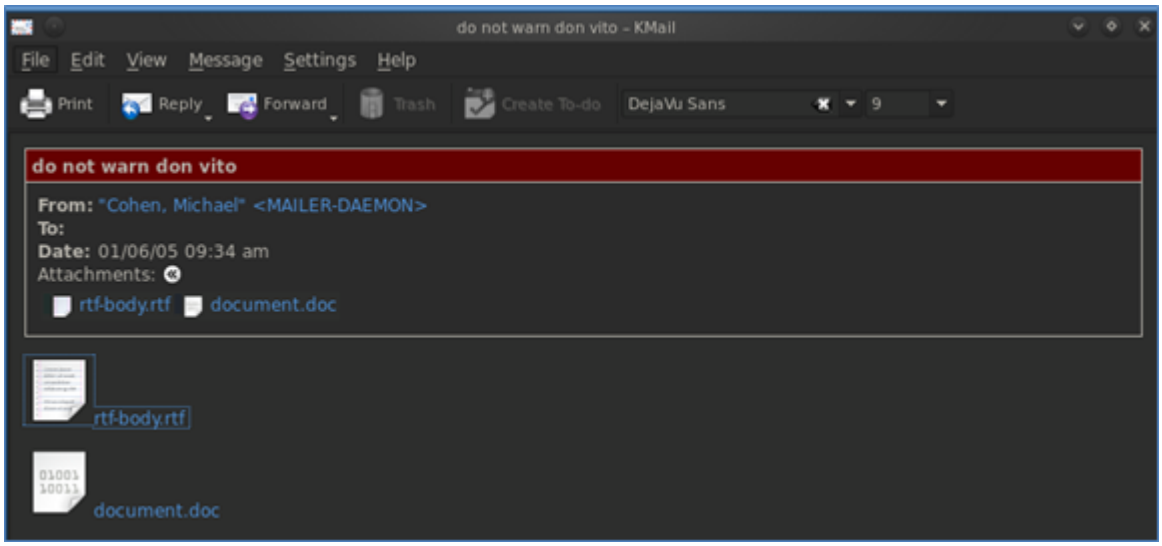


show the path of the folders and it will open them in your client interface. So if there are any attachments in the mail you can easily open it and download for further evidence. So, while examining Inbox we can see the mails, one of the mails says [Figure-12]:



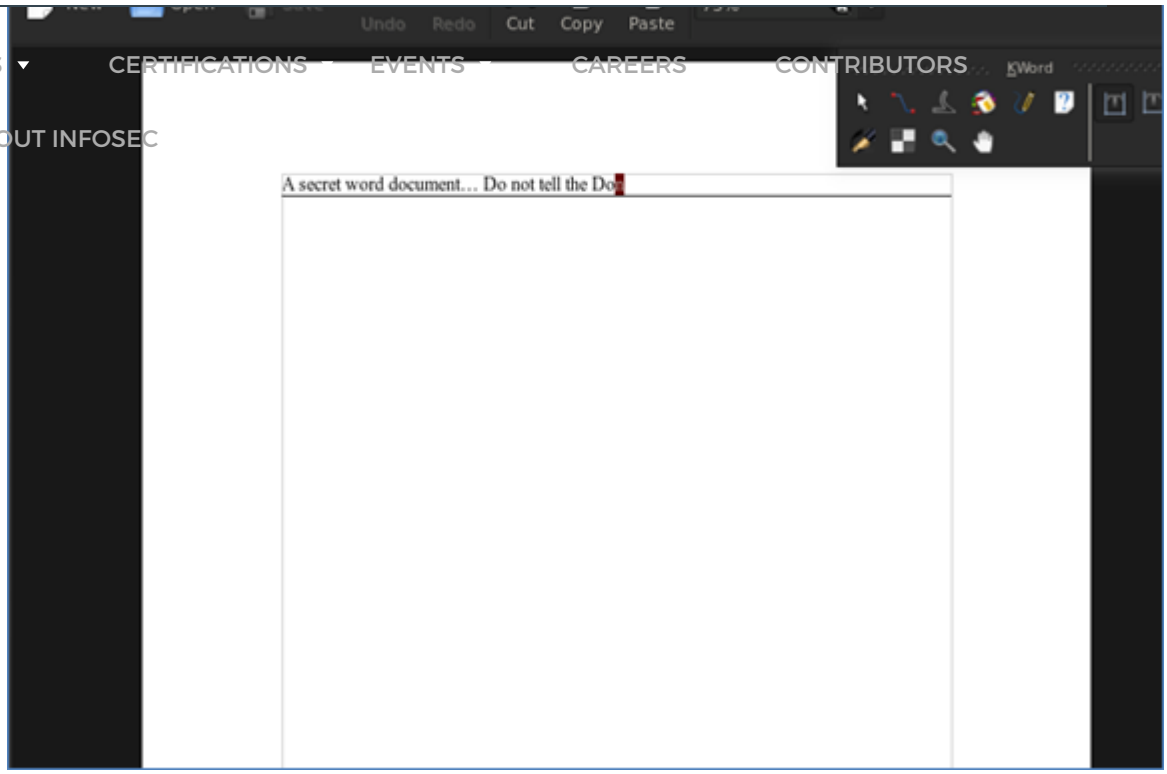
[Figure-12: View of one received mail]

We can view any attachment now easily. Similarly let's examine Sent Items folder now [Figure-13].



[Figure-13: View of a mail in Sent Items]

The above mail appears to be threatening. We can see the contents of the files as well. Let's open 'document.doc' above attached above to see its contents [Figure-14].



[Figure-14: View of an attachment in the mail]

Further, we would like to redirect all the mail items to our 'Evidence' directory in order to collect them for producing proof:

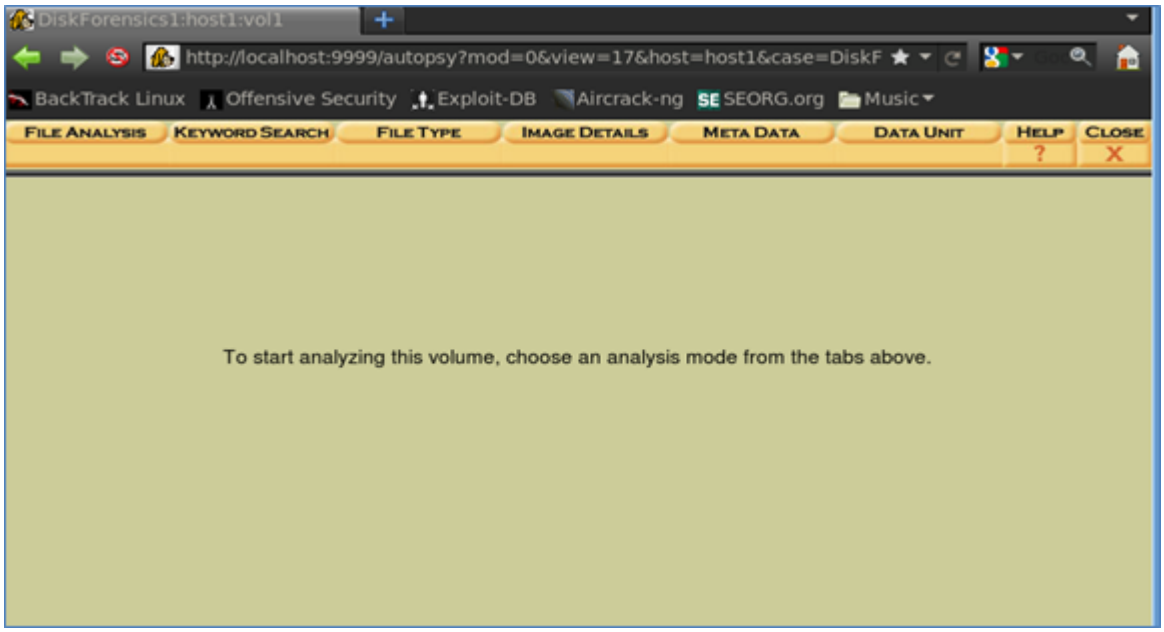
 # readpst -D outlook.pst -o /evidence/MailsEvidence

Data Recovery:

Now, I shall introduce one more tool which has a nice GUI—Autopsy. Autopsy analyzes the disk image and helps you browse the file contents and recover the data. It even has capabilities for retrieving deleted files as well. So, once you are done with the image acquisition, we can use Autopsy to analyze the image [Figure-15.

[Figure-15: Autopsy tool]

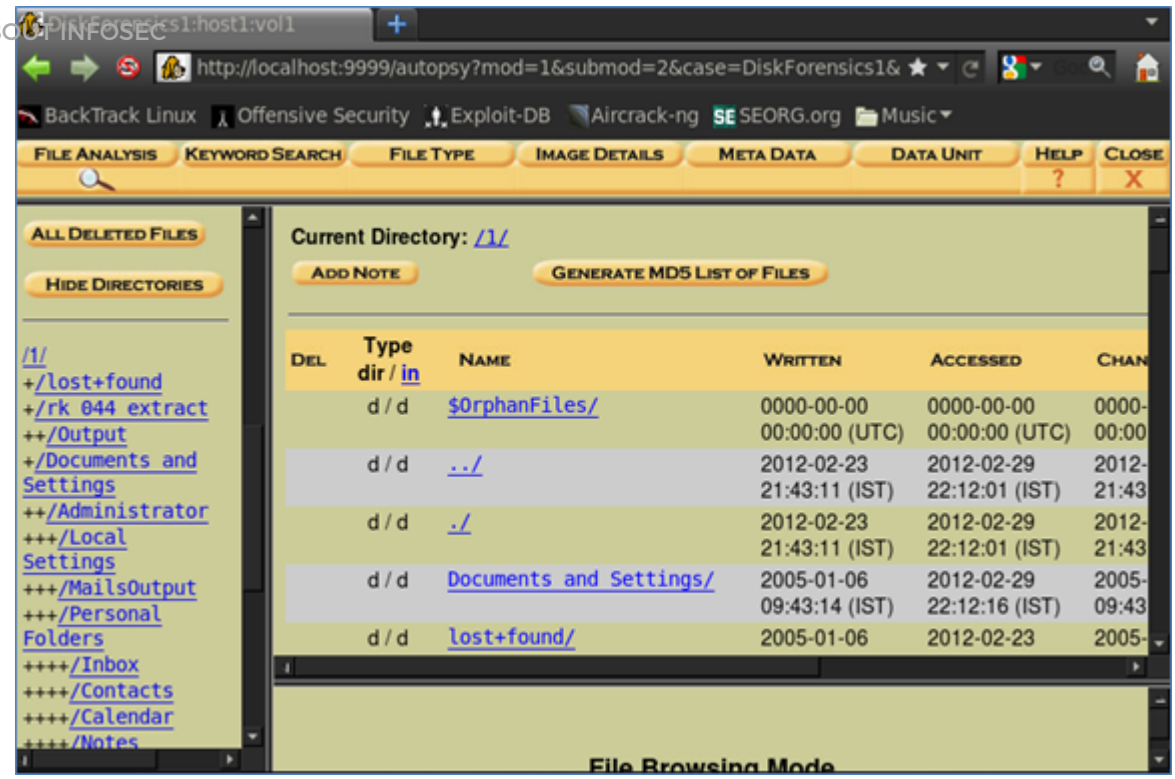
We'll open a new case, provide the case name, description and investigator names at the second step, then add a host in the third step. In fourth step, you need to give path of the image stored at your machine. In few next steps, it will ask you to select the file system and partition, etc. Once done, click on 'Analyze' button, the following screen will appear [Figure-16].



[Figure-16: Autopsy functions]

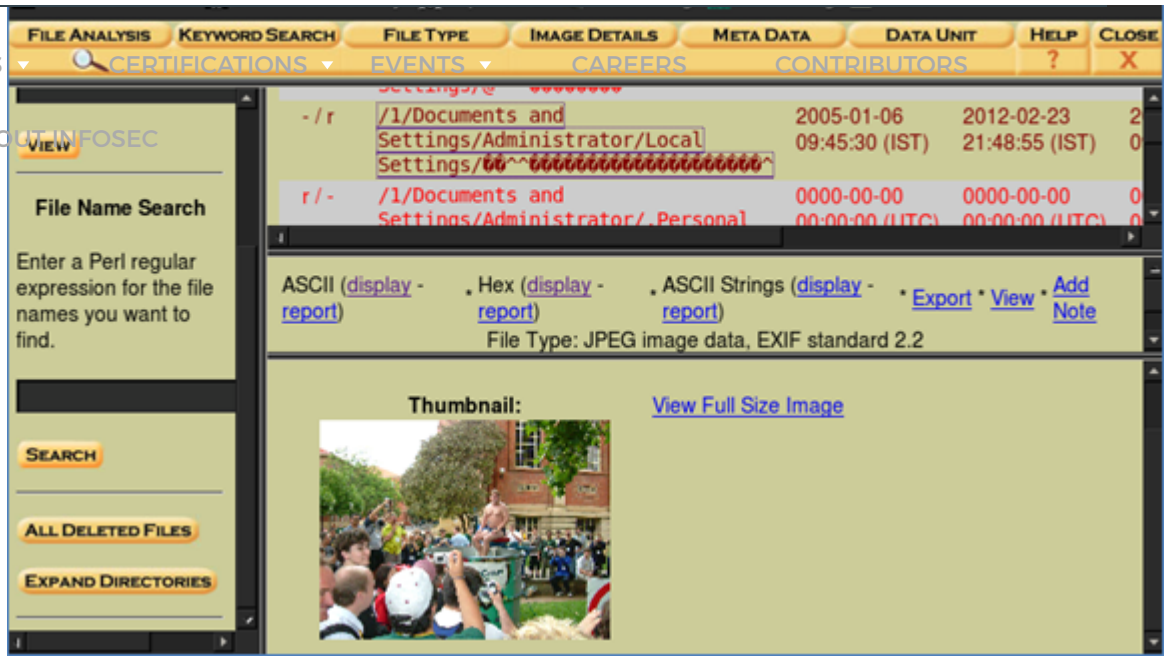
'File Analysis' lets you browse through the entire file system, 'Keyword Search' can be

about Inodes, "Data Unit" shows contents of any fragment. We're interested in File Analysis and Keyword Search, let's click File Analysis tab [Figure-17].



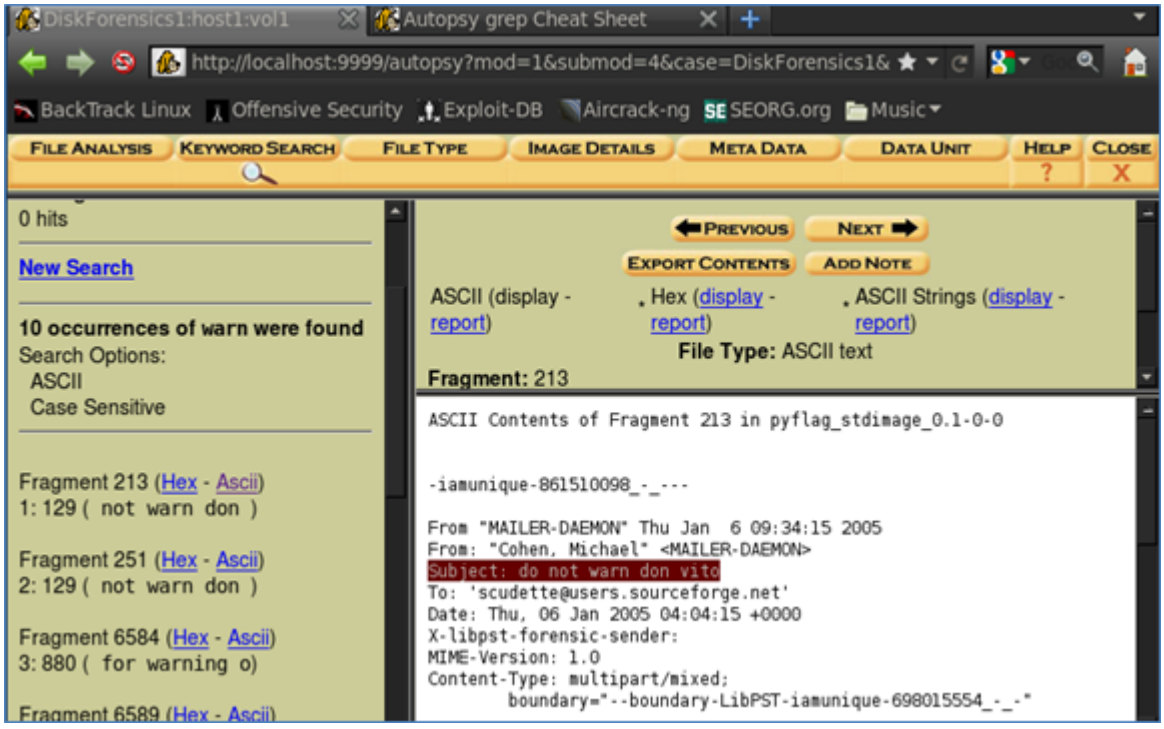
[Figure-17: Browsing the file system]

We can browse and view contents of the entire file system. The files in blue are existing files and if in red, they are deleted. We can see the contents of the files by clicking on them. Autopsy also gives you much information about dates of access, change, size, name etc of the files. Let's click on of the red files, which were deleted. It shows the contents of the deleted file, file type, and various options for displaying it in ASCII, HEX or exporting the file [Figure-18].



[Figure-18: View of deleted files]

Now we'll go to Keyword Search tab and try to search some important terms such as SSN, ransom, virus, Trojan, secret etc. Actually, it's suggested to create a list of terms or regular expressions, which can give vital clues about the file. We searched for the term 'warn' here; it shows all of the hits it found in the entire file system. We can show the contents of the file after clicking on them [Figure-19].



useful evidence as far as possible. It's not possible to cover all of the tools and their functionalities in single article; hence we may look at them in future articles.

References:

http://dftt.sourceforge.net/

http://pyflag.sourceforge.net

http://linuxleo.com/

http://www.deftlinux.net/

and more...

AUTHOR

Ninj@S3c

Ninj@S3c is a Security Analyst with a leading MNC. He is predominantly focused on Application Security, Network Security and Wireless Security. Beyond this, he's interested in Reverse Engineering and Forensics.

- Keeping your cybersecurity skills relevant in 2019
- Top 50 Network Administrator Interview Questions [Updated for 2019]
- CISSP Certification – The Ultimate Guide
- Anonymization and pseudonymization of personal data
- Cybersecurity engineer resume tips
- What does an IT auditor do?
- ICS Protocols
- Phish testing: What to do about so-called “repeat offenders”
- Does it make sense to make a career move from law to data privacy?
- Why diversity of thought matters in cybersecurity
- CySA+: History
- Analyzing Packed Malware
- CySA+: Examination Process
- CySA+ requirements
- Reverse Engineering Packed Malware

RELATED JOB TITLES

Ethical Hacker

Computer Forensics Investigator

MORE POSTS BY AUTHOR

Exploiting Heartbleed

Reversing Firmware Part 1

Ajax Security Issues

5 responses to “Linux and Disk Forensics”

SImon Thornton says:
June 10, 2013 at 11:12 am
With dd you need to add the “noerror” (keeps going on read error) and “notrunc” (stops the output being truncated if a read error occurs). e.g.:
dd if= of= conv=noerror,notrunc
(Adding a blocksize ‘bs’ of 1M to this also speeds up the transfer. The optimal size depends on the disk geometry and memory in the system).
I would also suggest splitting the output into chunks no bigger than 2GB, which makes them easier to split across media. Using a single large file for capture can cause problems with many file systems. . The simplest way is to pipe the output of dd through split:
dd if= conv=noerror,notrunc | split -b2047M – .
This will produce output files on the name:
image_file.xx where xx =aa,ab,ac etc etc
A further refinement would be to use the excellent ‘dcfldd’ which is an enhanced version of dd which includes many features for forensic work such as automatic md5 of the output stream.
Reply

alex says:
June 10, 2013 at 1:15 pm
Well .. What will you get with these products if i use a laptop with no HDD in it, and i always use a free wifi connection from a live Ubunutu CD ?
Reply

Reply

Ceative Designer says:
October 12, 2015 at 6:24 am
why not adding the correct commands in your comment to help others???
Reply

OneEyedMonk says:
March 22, 2014 at 9:14 pm
Thank you for sharing your knowledge. I like to learn and appreciate a person that is unselfish enough to take the time to help.
Reply

Leave a Reply
Your email address will not be published. Required fields are marked *

Comment
Name *
Email *
Website
Save my name, email, and website in this browser for the next time I comment.
× 8 = 40
Post Comment

About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We provide the best certification and skills development training for IT and security professionals, as well as employee security awareness training and phishing simulations. Learn more at infosecinstitute.com.

INFOSEC INFOSEC IQ TECHEXAMS

Connect with us

Stay up to date with Infosec

Like 211

Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YOUR SUBSCRIBE