LAB Manual
PART A
(PART A : TO BE REFFERED BY STUDENTS)

Experiment No. 7

A.1 Aim:
To Perform Forensic Analysis of deleted files.
A.2 Prerequisite:
Data recovery, Digital Forensic, kali linux

A.3 Outcome:
After successful completion of this experiment students will be able to
1. Appreciate foremost as a forensic tool to recover the data.
2. Explorer kali linux as penetration testing Operating system.

A.4 Theory:

Virtual Machine: With a virtual machine, the sandbox is isolated from the underlying physical hardware but has access to the installed operating system. Virtualized environment. Usually, a sandbox is on a virtual machine so that it has no access to physical resources but can access virtualized hardware.

Kali Linux: Kali Linux is a Debian -derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

Forensic: Digital forensics is a branch of forensic science encompassing the recovery, investigation, examination and analysis of material found in digital devices, often in relation to mobile devices and computer crime.

Foremost is a digital forensic application that is used to recover lost or deleted files. Foremost can recover the files for hard disk, memory card, pen drive, and another mode of memory devices easily. It can also work on the image files that are being generated by any other Application. It is a free command-line tool that is pre-installed in Kali Linux. This tool comes pre-installed in Kali Linux. Foremost is a very useful software that is used to recover the deleted files, if some files are deleted accidentally or in any case files are deleted. You can recover the deleted files from foremost only if the data in the device is not overridden, which means after deleting the files no more data is added to the storage device because in that case data may be overridden and the chances of recovery also get reduced and data must get corrupted.

Installing the Foremost Tool:
Use the following command to install this tool in any Debian based Linux Operating System or in any other Operating System using the APT package manager.

sudo apt install foremost

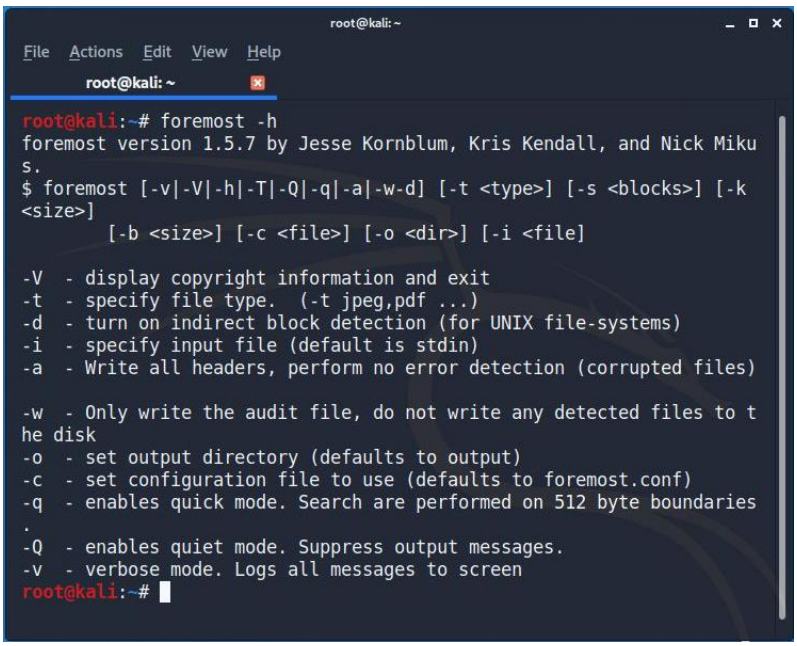
Use the following command to install this tool using dnf package manager

sudo dnf install foremost

Use the following command to install this tool using Pacman package manager or in Arch Linux.

sudo pacman -S foremost

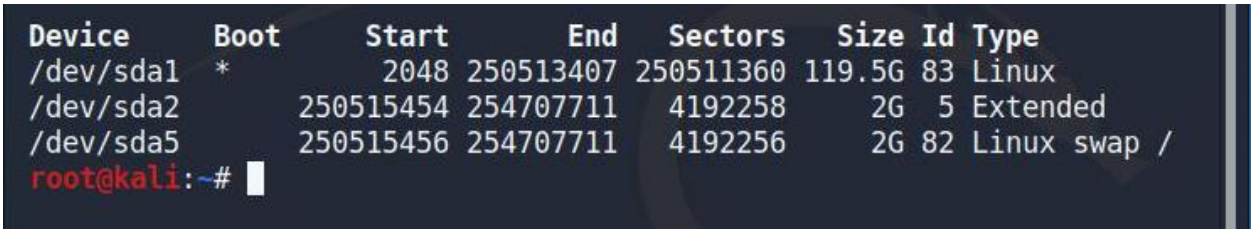
Syntax:
foremost [options]



Here you can check the options available and their functions. Let us now see how to recover deleted files using foremost:

Recovering from USB/Hard Disk:

- Connect the External memory storage with the system.
- First, you need to know the path of your external memory device, for that use the command fdisk -1



Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1	*	2048	250513407	250511360	119.5G	83	Linux
/dev/sda2		250515454	254707711	4192258	2G	5	Extended
/dev/sda5		250515456	254707711	4192256	2G	82	Linux swap /

root@kali:~#

- After copying the device path, now we have to recover the files from that device.

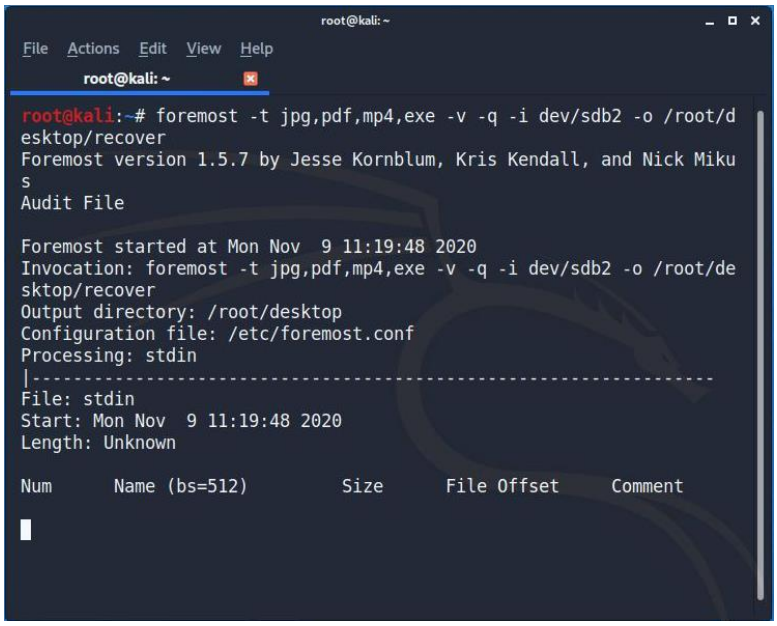
Use the options available by the “foremost -h” command.

For example :

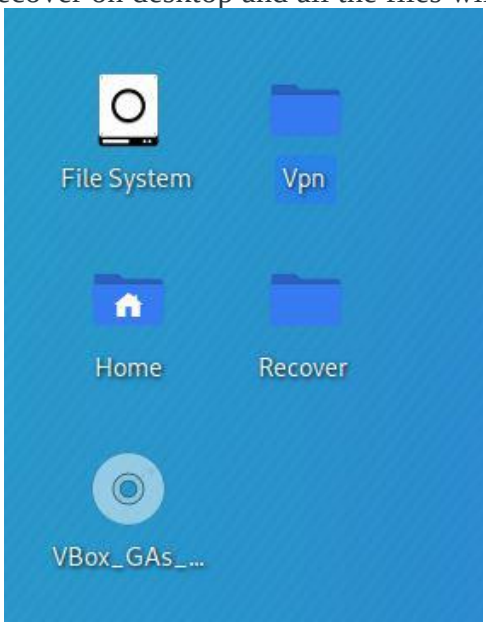
foremost -t jpg,pdf,mp4,exe -v -q -i /dev/sdb2 -o /root/desktop/recover

Here use this command to recover the data from the device.

- **-t**: It is the type of files we want to recover. Here I want to recover jpg, pdf,mp4, and exe files.
- **-q**: It is a quick scan for the device
- **-i**: It means the input as in this case external memory.
- **-o**: It is the output folder, where to save the recovered files.



Hereafter running this command, all the files will be saved in the folder name as mentioned. Here you can see the folder recover on desktop and all the files will be stored here.



PART B

(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

Roll. No. A016	Name: Varun Khadayate
Class B.Tech CsBs	Batch:1
Date of Experiment: 18-02-2022	Date of Submission:18002-2022
Grade:	

B.1 Software installation issues faced:

B.2 Input and Output:

(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output in due course of time. Students will be graded accordingly.)

Input and Output

We will work with a freely available evidence file named terry-work- usb-2009-12-11.E01.

Using bulk_extractor

bulk_extractor -h

```
┌──(root💀varun)-[/home/varun]
└─# bulk_extractor -h
bulk_extractor version 1.6.0
Usage: bulk_extractor [options] imagefile
  runs bulk extractor and outputs to stdout a summary of what was found where

Required parameters:
   imagefile     - the file to extract
 or  -R filedir  - recurse through a directory of files
                   HAS SUPPORT FOR E01 FILES
                   HAS SUPPORT FOR AFF FILES
   -o outdir    - specifies output directory. Must not exist.
                  bulk_extractor creates this directory.
Options:
   -i           - INFO mode. Do a quick random sample and print a report.
   -b banner.txt- Add banner.txt contents to the top of every output file.
   -r alert_list.txt  - a file containing the alert list of features to alert
                        (can be a feature file or a list of globs)
                        (can be repeated.)
   -w stop_list.txt   - a file containing the stop list of features (white list
                        (can be a feature file or a list of globs)s
                        (can be repeated.)
   -F <rfile>   - Read a list of regular expressions from <rfile> to find
   -f <regex>   - find occurrences of <regex>; may be repeated.
                  results go into find.txt
   -q nn        - Quiet Rate; only print every nn status reports. Default 0; -1 for no statu
s at all
   -s frac[:passes] - Set random sampling parameters

Tuning parameters:
```

```
bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01
```

```
┌──(root💀varun)-[/home/varun]
└─# bulk_extractor -o bulk_output terry-work-usb-2009-12-11.E01            1 ×
bulk_extractor version: 1.6.0
Hostname: varun
Input file: terry-work-usb-2009-12-11.E01
Output directory: bulk_output
Disk Size: 2097152000
Threads: 1
10:39:36 Offset 67MB (3.20%) Done in  0:05:43 at 10:45:19
10:39:41 Offset 150MB (7.20%) Done in  0:03:18 at 10:42:59
10:39:42 Offset 234MB (11.20%) Done in  0:02:14 at 10:41:56
10:39:43 Offset 318MB (15.20%) Done in  0:01:41 at 10:41:24
10:39:45 Offset 402MB (19.20%) Done in  0:01:21 at 10:41:06
10:39:46 Offset 486MB (23.20%) Done in  0:01:08 at 10:40:54
10:39:47 Offset 570MB (27.20%) Done in  0:00:58 at 10:40:45
10:39:48 Offset 654MB (31.20%) Done in  0:00:51 at 10:40:39
10:39:50 Offset 738MB (35.20%) Done in  0:00:45 at 10:40:35
10:39:51 Offset 822MB (39.20%) Done in  0:00:39 at 10:40:30
10:39:52 Offset 905MB (43.20%) Done in  0:00:35 at 10:40:27
10:39:53 Offset 989MB (47.20%) Done in  0:00:31 at 10:40:24
10:39:55 Offset 1073MB (51.20%) Done in  0:00:28 at 10:40:23
10:39:56 Offset 1157MB (55.20%) Done in  0:00:25 at 10:40:21
10:39:57 Offset 1241MB (59.20%) Done in  0:00:22 at 10:40:19
10:39:58 Offset 1325MB (63.20%) Done in  0:00:19 at 10:40:17
10:40:00 Offset 1409MB (67.20%) Done in  0:00:16 at 10:40:16
10:40:01 Offset 1493MB (71.20%) Done in  0:00:14 at 10:40:15
10:40:02 Offset 1577MB (75.20%) Done in  0:00:12 at 10:40:14
10:40:03 Offset 1660MB (79.20%) Done in  0:00:10 at 10:40:13
10:40:05 Offset 1744MB (83.20%) Done in  0:00:07 at 10:40:12
10:40:06 Offset 1828MB (87.20%) Done in  0:00:05 at 10:40:11
10:40:07 Offset 1912MB (91.20%) Done in  0:00:04 at 10:40:11
10:40:08 Offset 1996MB (95.20%) Done in  0:00:02 at 10:40:10
10:40:10 Offset 2080MB (99.20%) Done in  0:00:00 at 10:40:10
```

```
10:40:01 Offset 1493MB (71.20%) Done in  0:00:14 at 10:40:15
10:40:02 Offset 1577MB (75.20%) Done in  0:00:12 at 10:40:14
10:40:03 Offset 1660MB (79.20%) Done in  0:00:10 at 10:40:13
10:40:05 Offset 1744MB (83.20%) Done in  0:00:07 at 10:40:12
10:40:06 Offset 1828MB (87.20%) Done in  0:00:05 at 10:40:11
10:40:07 Offset 1912MB (91.20%) Done in  0:00:04 at 10:40:11
10:40:08 Offset 1996MB (95.20%) Done in  0:00:02 at 10:40:10
10:40:10 Offset 2080MB (99.20%) Done in  0:00:00 at 10:40:10
All data are read; waiting for threads to finish...
Time elapsed waiting for 1 thread to finish:
     (timeout in 60 min.)
All Threads Finished!
Producer time spent waiting: 28.724 sec.
Average consumer time spent waiting: 0.161821 sec.
*****************************************
** bulk_extractor is probably CPU bound. **
**    Run on a computer with more cores  **
**      to get better performance.       **
*****************************************
MD5 of Disk Image: e07f26954b23db1a44dfd28ecd717da9
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 45.4044 sec.
Total MB processed: 2097
Overall performance: 46.1883 MBytes/sec (46.1883 MBytes/sec/thread)
Total email features found: 3
```

Viewing the results of bulk_extractor

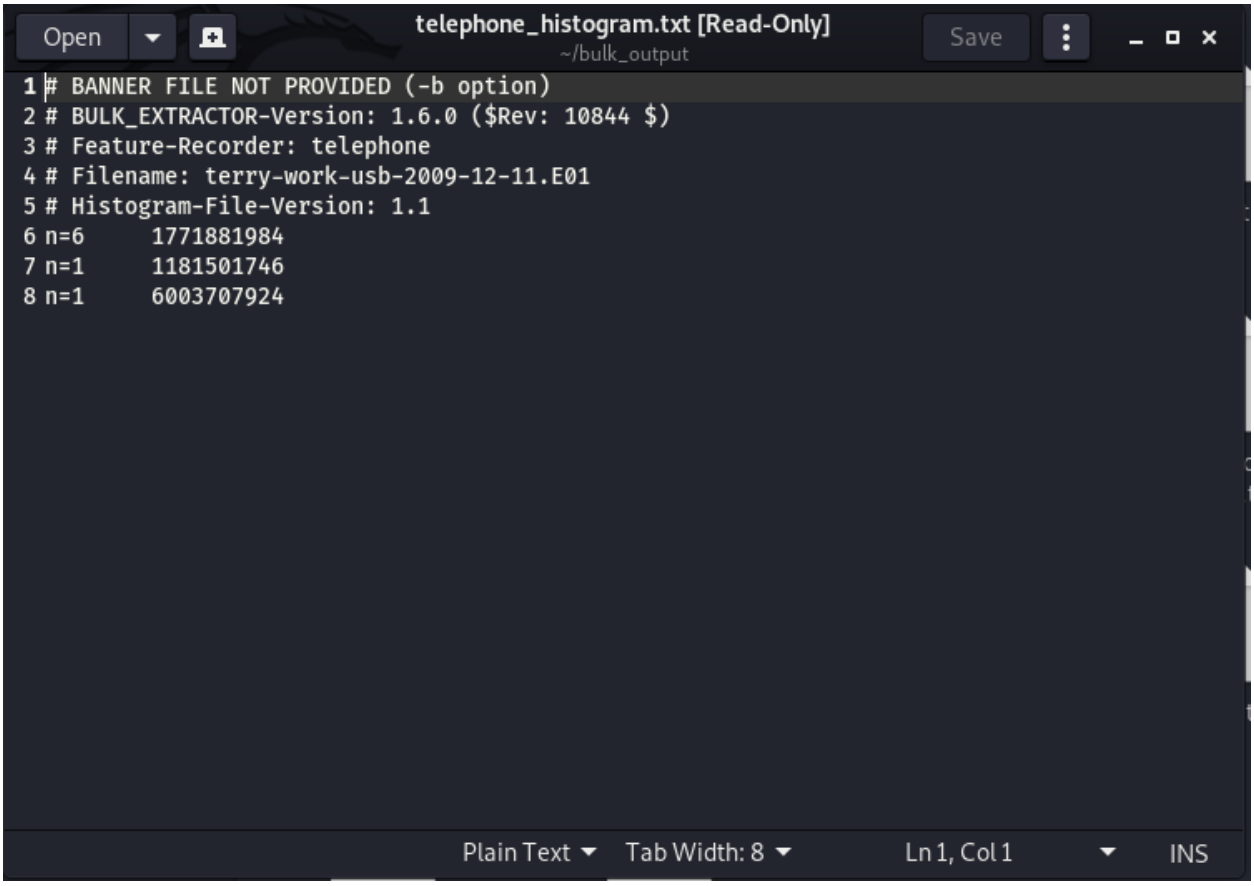
```
┌──(root💀varun)-[/home/varun]
└─# ls -l
total 32756
drwxr-xr-x 3 root  root      4096 Feb 18 10:40 bulk_output
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Desktop
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Documents
drwxr-xr-x 2 varun varun     4096 Feb 18 10:32 Downloads
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Music
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Pictures
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Public
drwxr-xr-- 2 varun varun     4096 Feb 18 10:22 scalpelOutput
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Templates
-rw-r--r-- 1 varun varun 33499203 Feb 18 10:32 terry-work-usb-2009-12-11.E01
drwxr-xr-x 2 varun varun     4096 Feb  4 10:22 Videos
```

ls -l bulk_output

```
┌──(root💀varun)-[/home/varun]
└─# ls -l bulk_output
total 30600
-rw-r--r-- 1 root root        0 Feb 18 10:39 aes_keys.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 alerts.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 ccn_histogram.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 ccn_track2_histogram.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 ccn_track2.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 ccn.txt
-rw-r--r-- 1 root root    68136 Feb 18 10:40 domain_histogram.txt
-rw-r--r-- 1 root root  7603388 Feb 18 10:39 domain.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 elf.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 email_domain_histogram.txt
-rw-r--r-- 1 root root      256 Feb 18 10:40 email_histogram.txt
-rw-r--r-- 1 root root     1112 Feb 18 10:39 email.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 ether_histogram.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 ether.txt
-rw-r--r-- 1 root root      513 Feb 18 10:39 exif.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 find_histogram.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 find.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 gps.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 httplogs.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 ip_histogram.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 ip.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 jpeg_carved.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 json.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 kml.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 ntfsusn_carved.txt
-rw-r--r-- 1 root root        0 Feb 18 10:40 pii_teamviewer.txt
-rw-r--r-- 1 root root        0 Feb 18 10:39 pii.txt
```

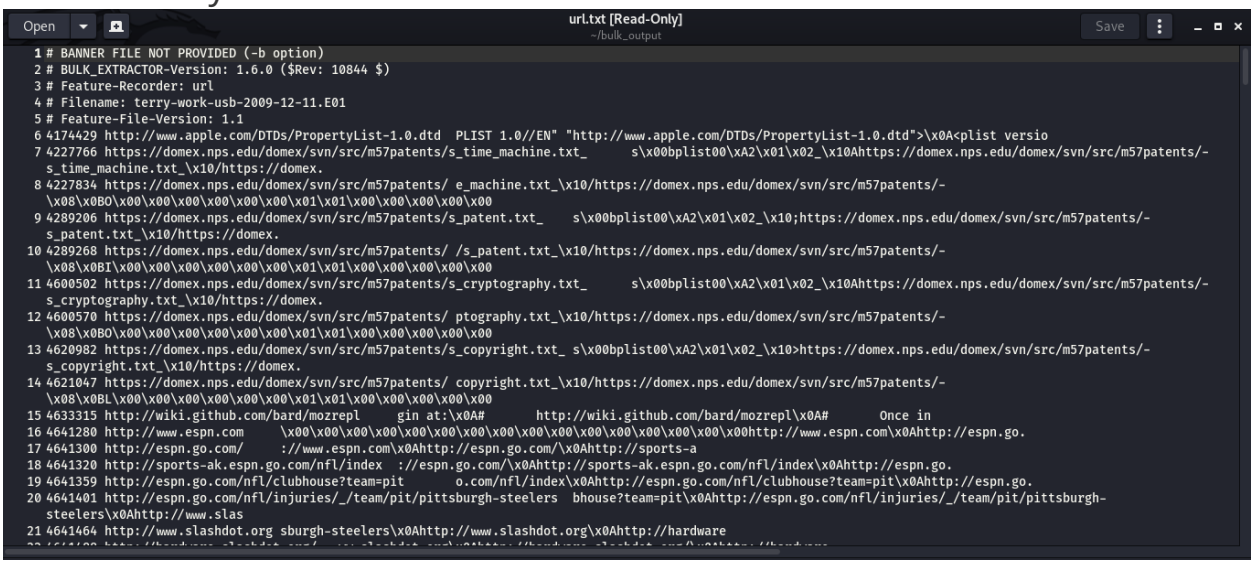
telephone_histogram.txt

reveals telephone numbers:



url.txt

Reveals many of the websites and links visited:



B.3 Observations and learning:

(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)

bulk_extractor is a wonderful tool that carves data and also finds useful information, such as email addresses, visited URLs, Facebook URLs, credit card numbers, and a variety of other information.

B.4 Conclusion:

(Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)
Hence we were able to perform the lab.

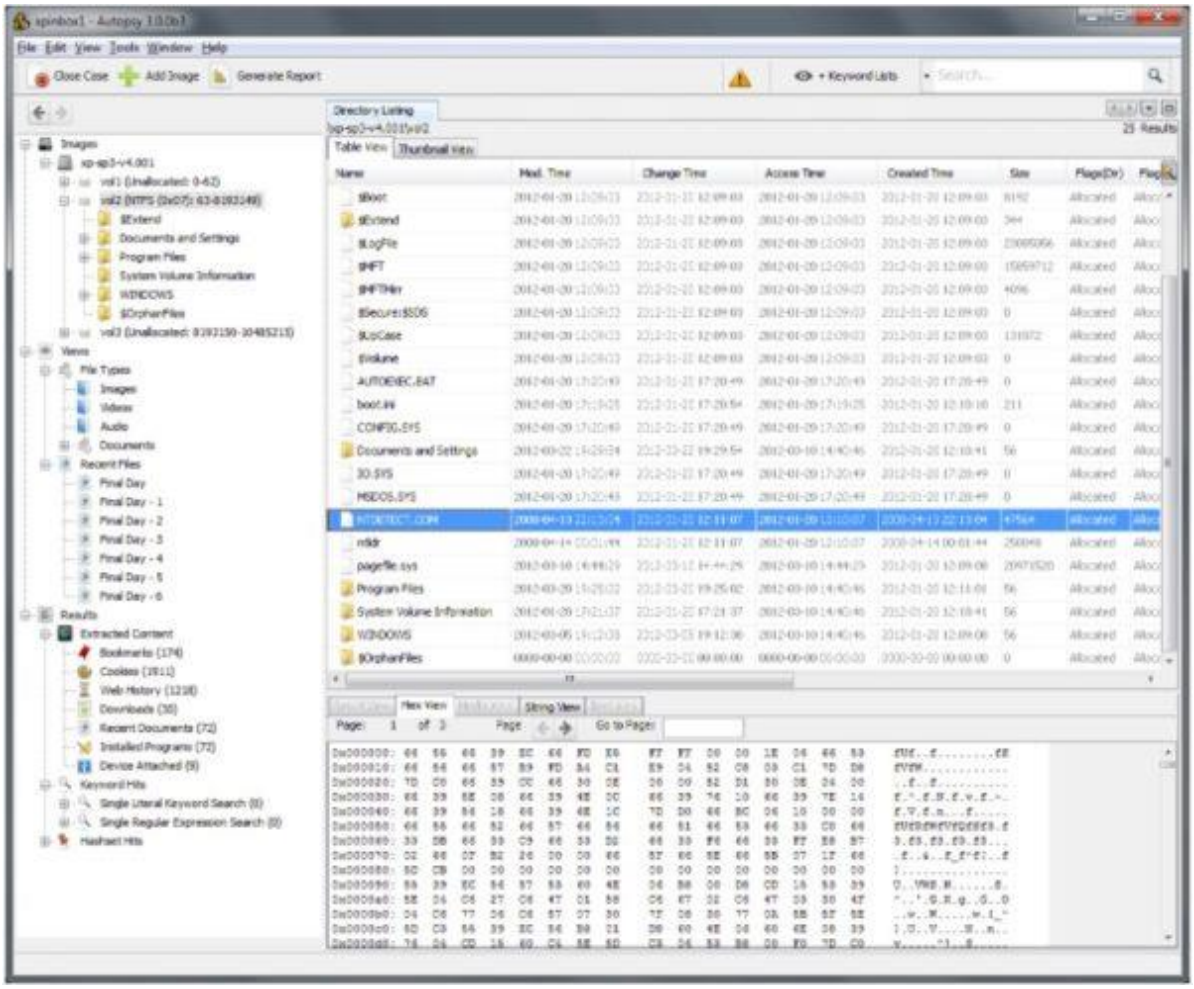
Questions of Curiosity

(To be answered by student based on the practical performed and learning/observations)

Q1: what are open source and proprietary forensic tools for multimedia recovery?

1. Autopsy

Autopsy is a GUI-based open source digital forensic program to analyze hard drives and smart phones effectively. Autospy is used by thousands of users worldwide to investigate what actually happened in the computer.

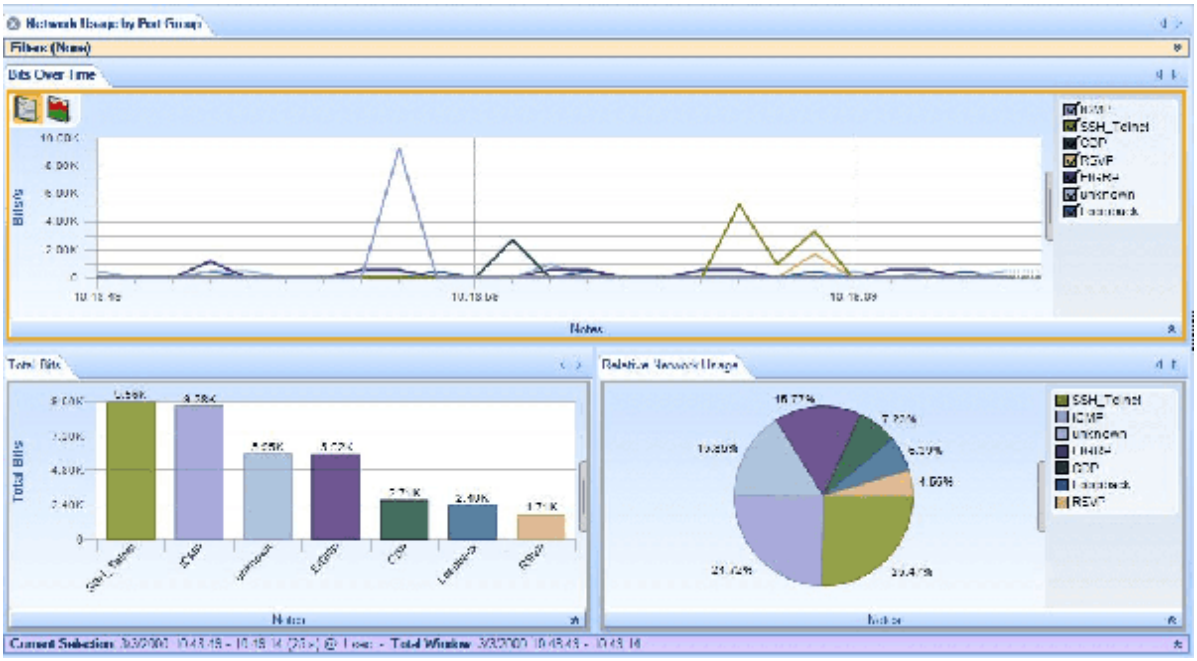


2. Encrypted Disk Detector

Encrypted Disk Detector can be helpful to check encrypted physical drives. It supports TrueCrypt, PGP, Bitlocker, Safeboot encrypted volumes.

3. Wireshark

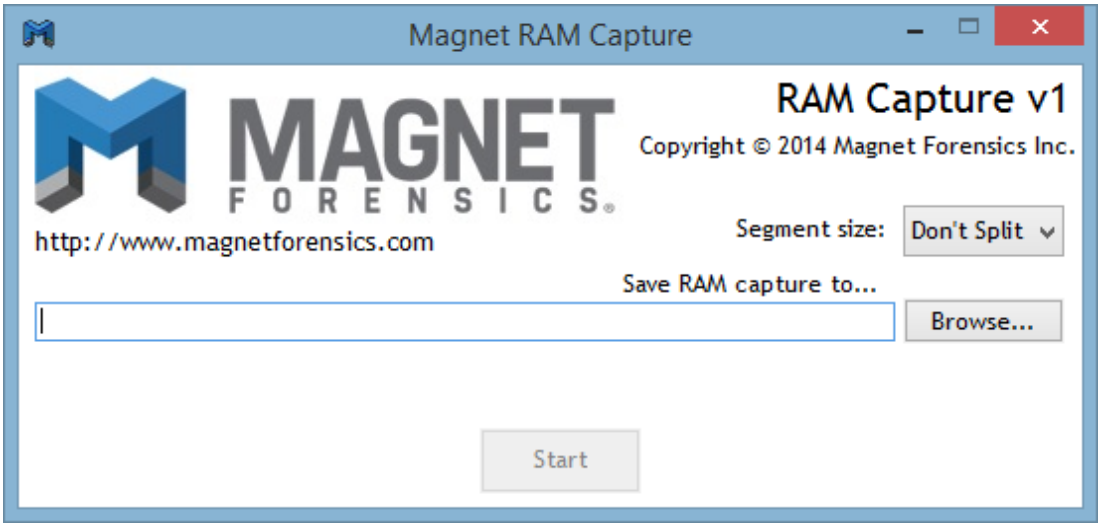
Wireshark is a network capture and analyzer tool to see what's happening in your network. Wireshark will be handy to investigate network related incident.



4. Magnet RAM Capture

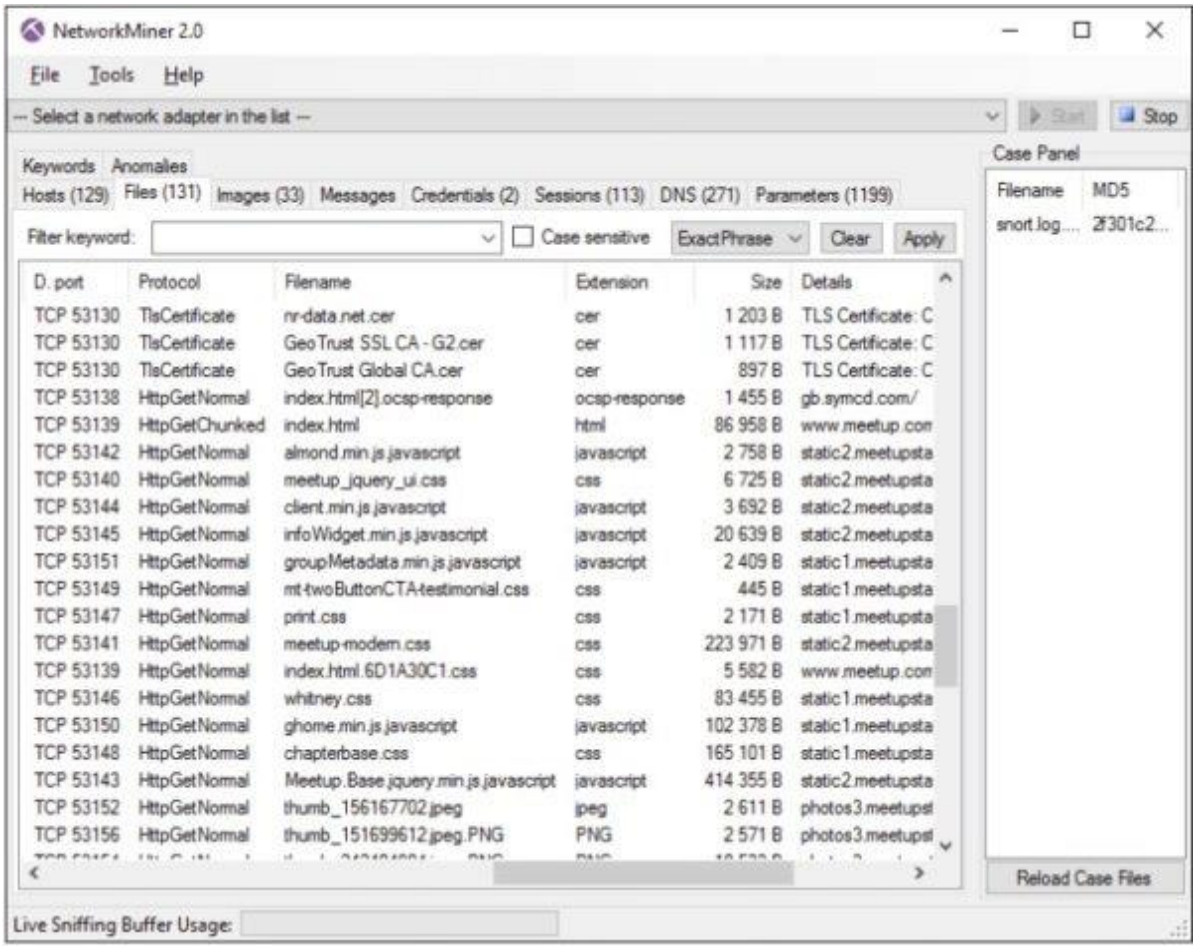
You can use Magnet RAM capture to capture the physical memory of a computer and analyze artifacts in memory.

It supports Windows operating system.



5. Network Miner

An interesting network forensic analyzer for Windows, Linux & MAC OS X to detect OS, hostname, sessions and open ports through packet sniffing or by PCAP file. Network Miner provide extracted artifacts in an intuitive user interface.

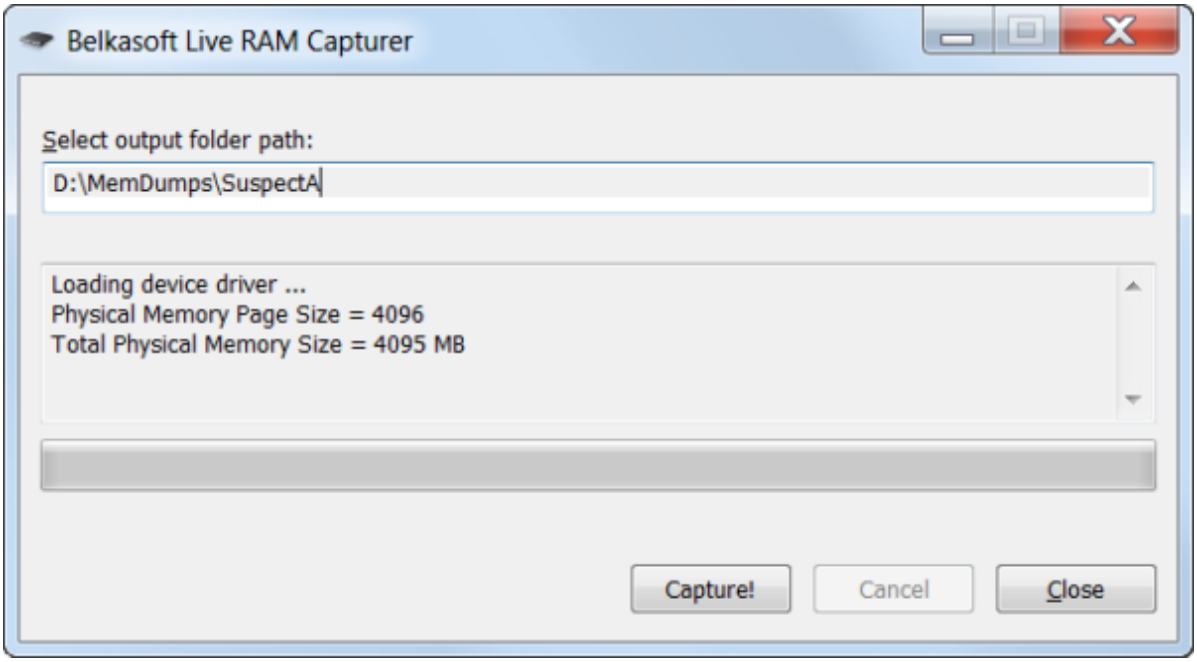


6. NMAP

NMAP (Network Mapper) is one of the most popular networks and security auditing tools. NMAP is supported on most of the operating systems including Windows, Linux, Solaris, MAC OS, HP-UX etc. It's open source so free.

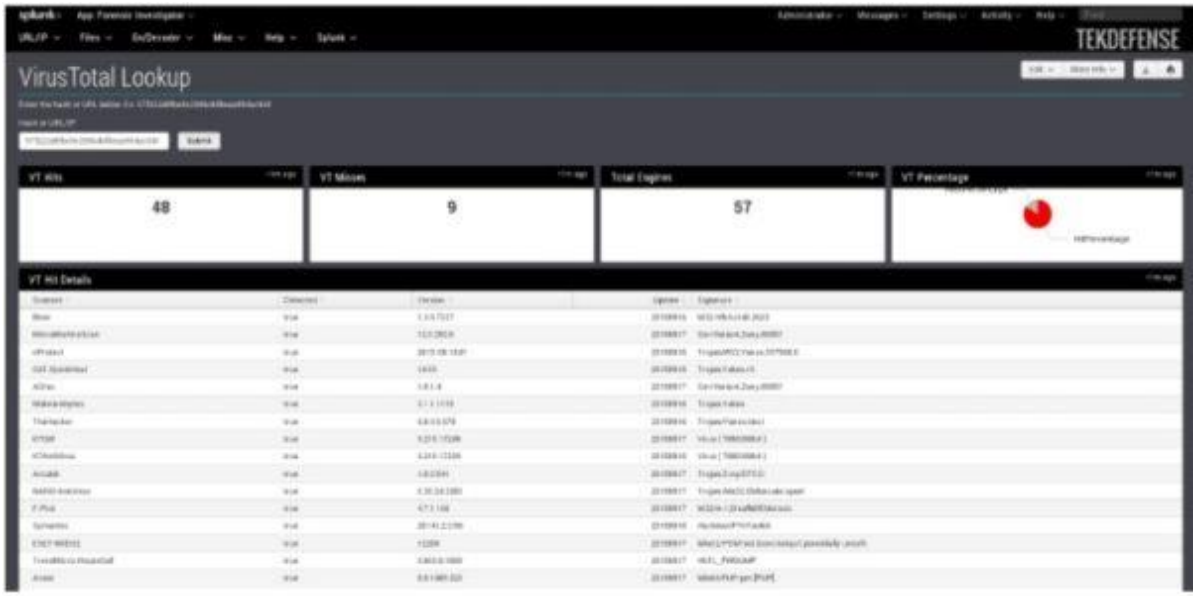
7. RAM Capturer

RAM Capturer by Belkasoft is a free tool to dump the data from computer's volatile memory. It's compatible with Windows OS. Memory dumps may contain encrypted volume's password and login credentials for webmails and social network services.



8. Forensic Investigator

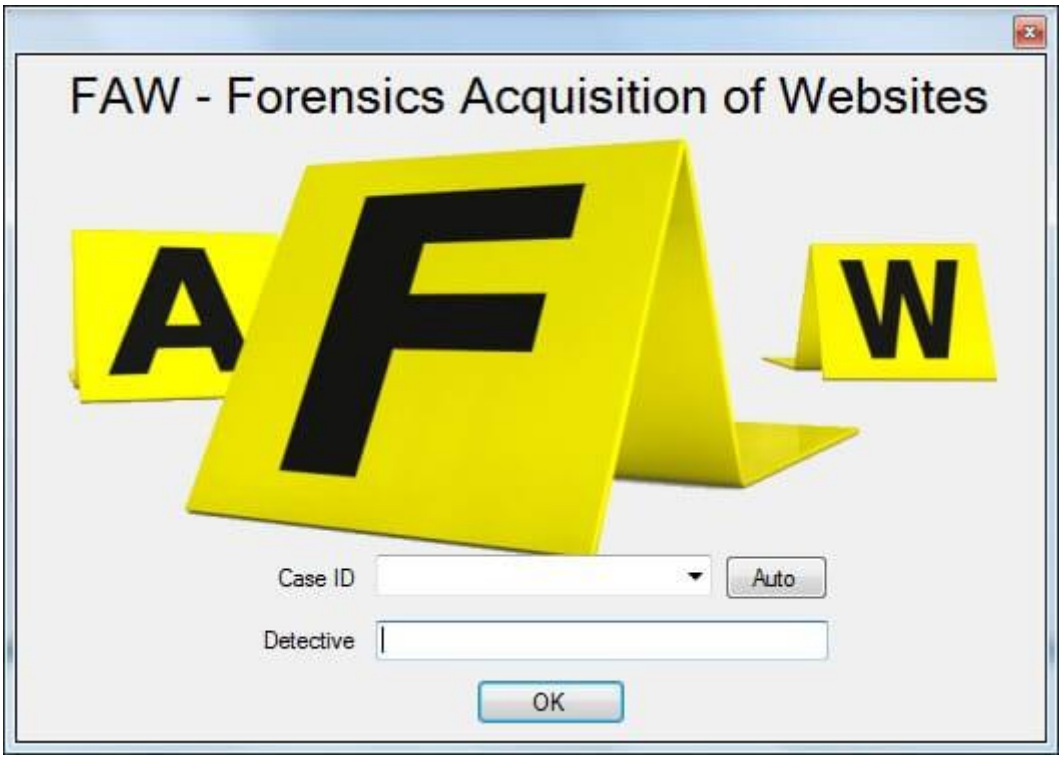
If you are using Splunk then Forensic Investigator will be a very handy tool. It's Splunk app and has many tools combined.



9. FAW

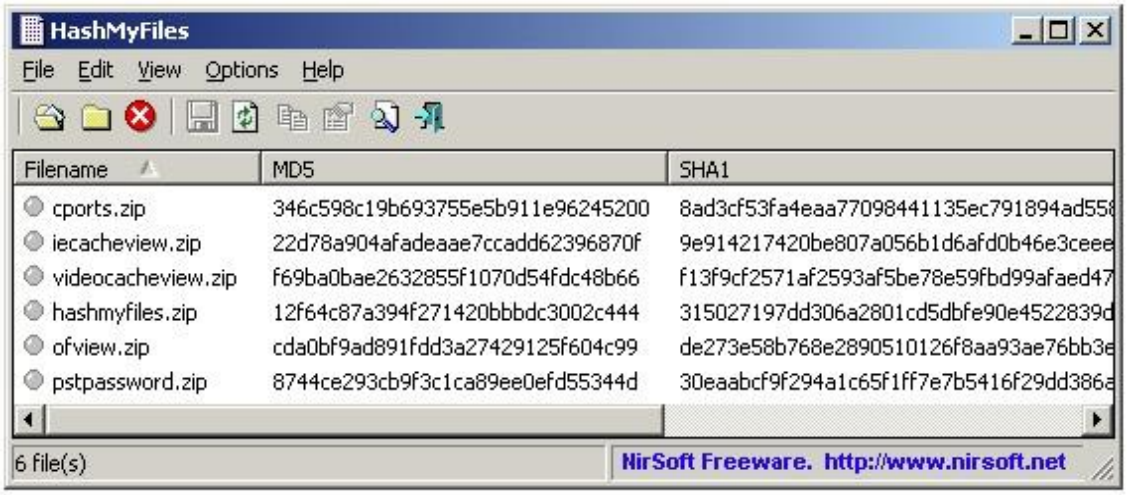
FAW (Forensics Acquisition of Websites) is to acquire web pages for forensic investigation which has the following features.

- Capture the entire or partial page
- Capture all types of image
- Capture HTML source code of the web page
- Integrate with Wireshark



10. HashMyFiles

HashMyFiles will help you to calculate the MD5 and SHA1 hashes. It works on almost all latest Windows OS.



11. USB Write Blocker

View the USB drives content without leaving the fingerprint, changes to metadata and timestamps. USB Write Blocker use Windows registry to write-block USB devices.

12. Crowd Response

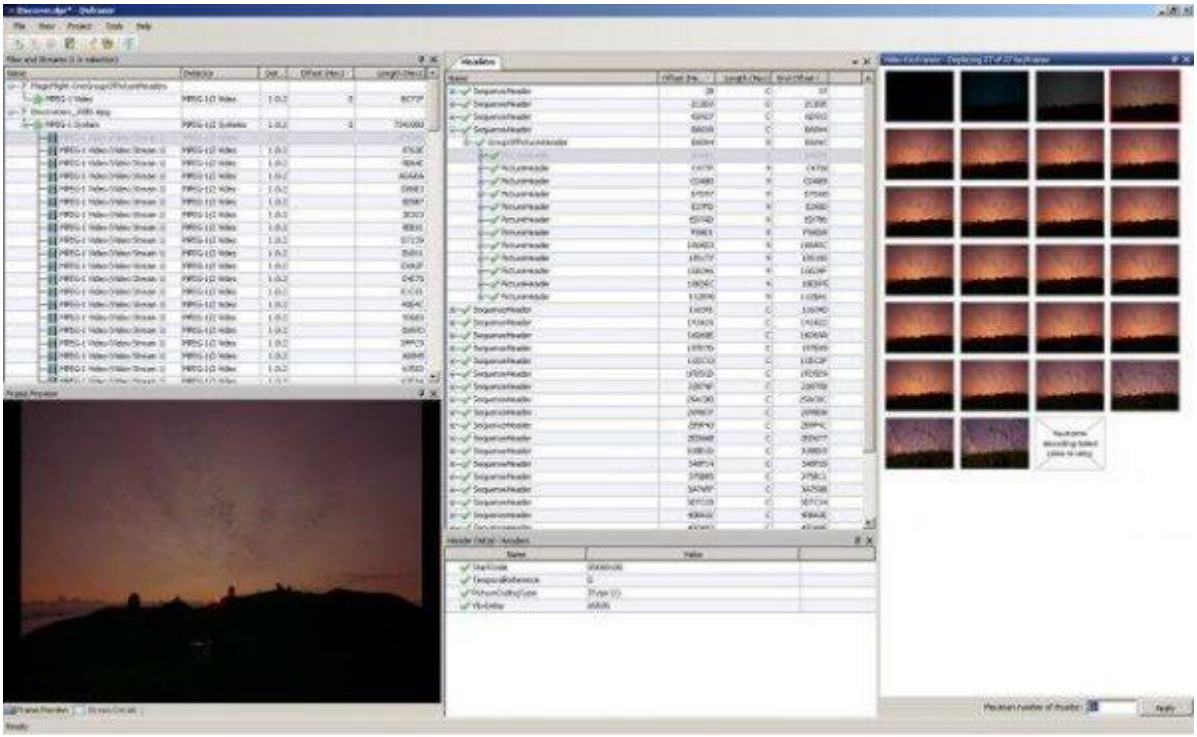
Response by Crowd Strike is a windows application to gather system information for incident response and security engagements. You can view the results in XML, CSV, TSV or HTML with help of CRConvert. It runs on 32 or 64 bit of Windows XP above.

Crowd Strike has some other nice tools for investigation.

- Totrtilla – anonymously route TCP/IP and DNS traffic through TOR.
- Shellshock Scanner – scan your network for shellshock vulnerability
- Heartbleed scanner – scan your network for OpenSSL heart bleed vulnerability

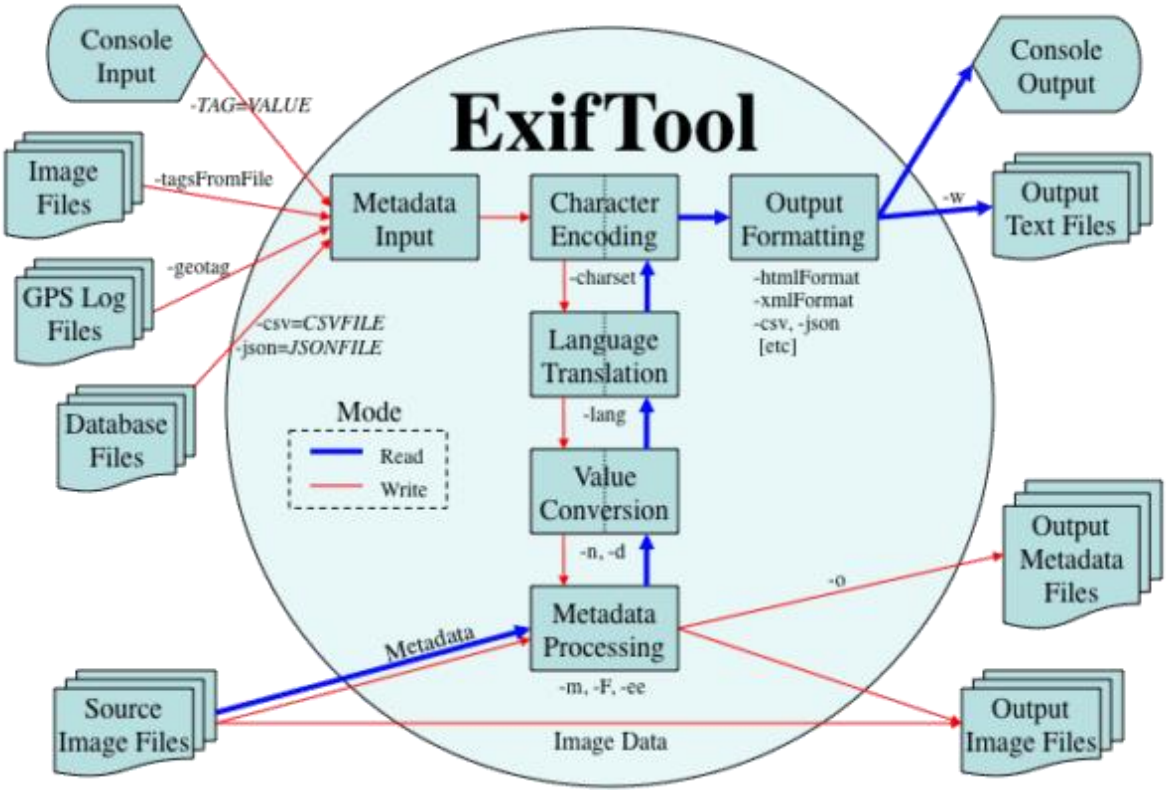
13. NFI Defraser

Defraser forensic tool may help you to detect full and partial multimedia files in the data streams.



14. ExifTool

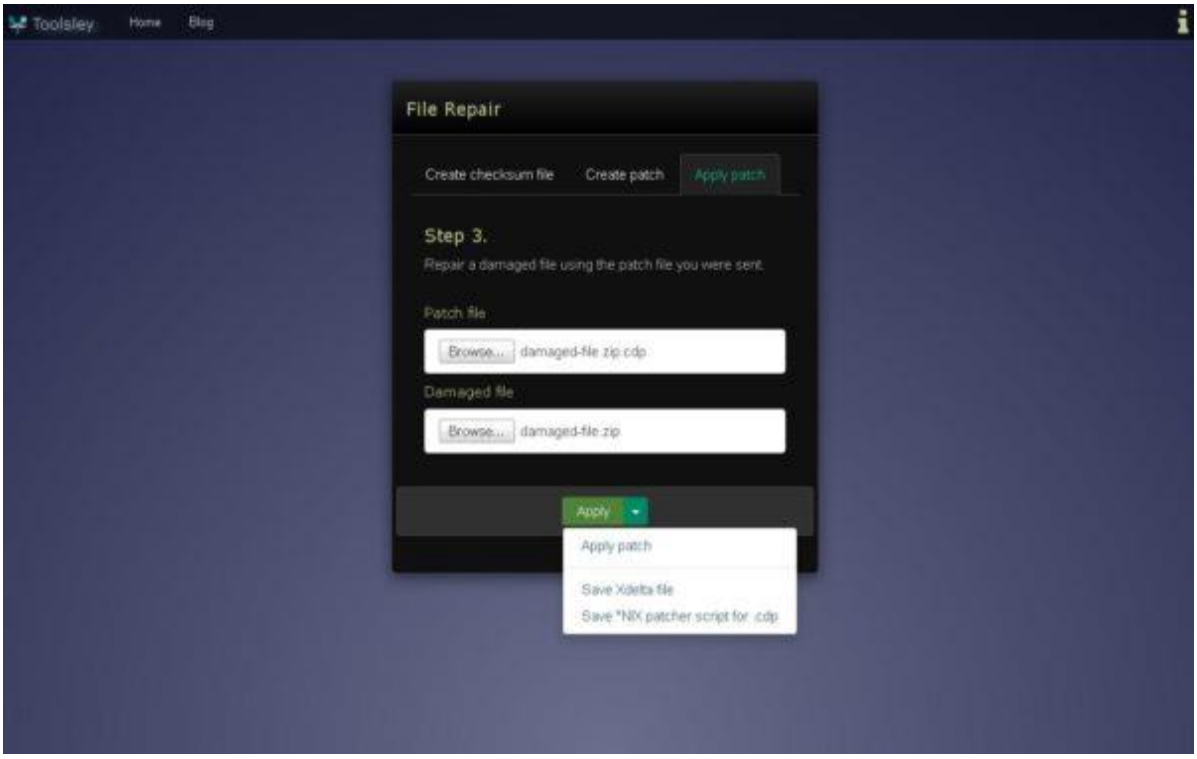
ExifTool helps you to read, write and edit meta information for a number of file types. It can read EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Photoshop IRB, FlashPix, etc.



15. Toolsley

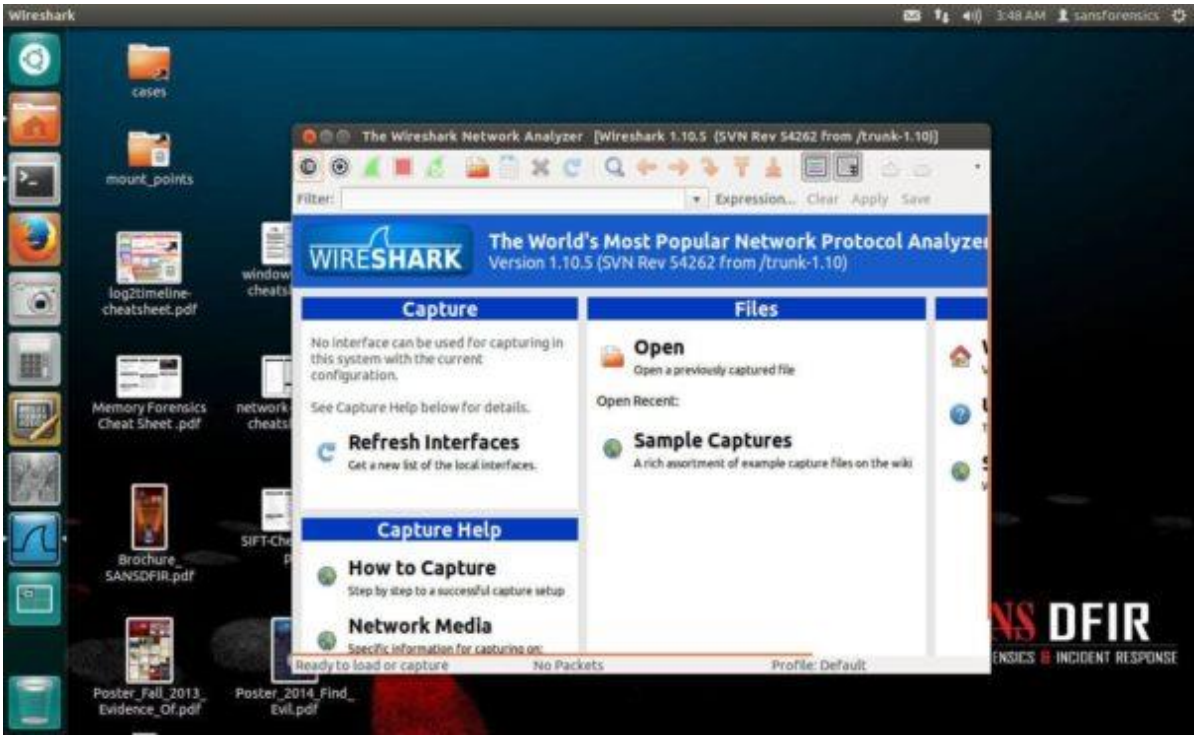
Toolsley got more than 10 useful tools for investigation.

- File signature verifier
- File identifier
- Hash & Validate
- Binary inspector
- Encode text
- Data URI generator
- Password generator



16. SIFT

SIFT (SANS investigative forensic toolkit) workstation is freely available as Ubuntu 14.04. SIFT is a suite of forensic tools you need and one of the most popular open source incident response platform.



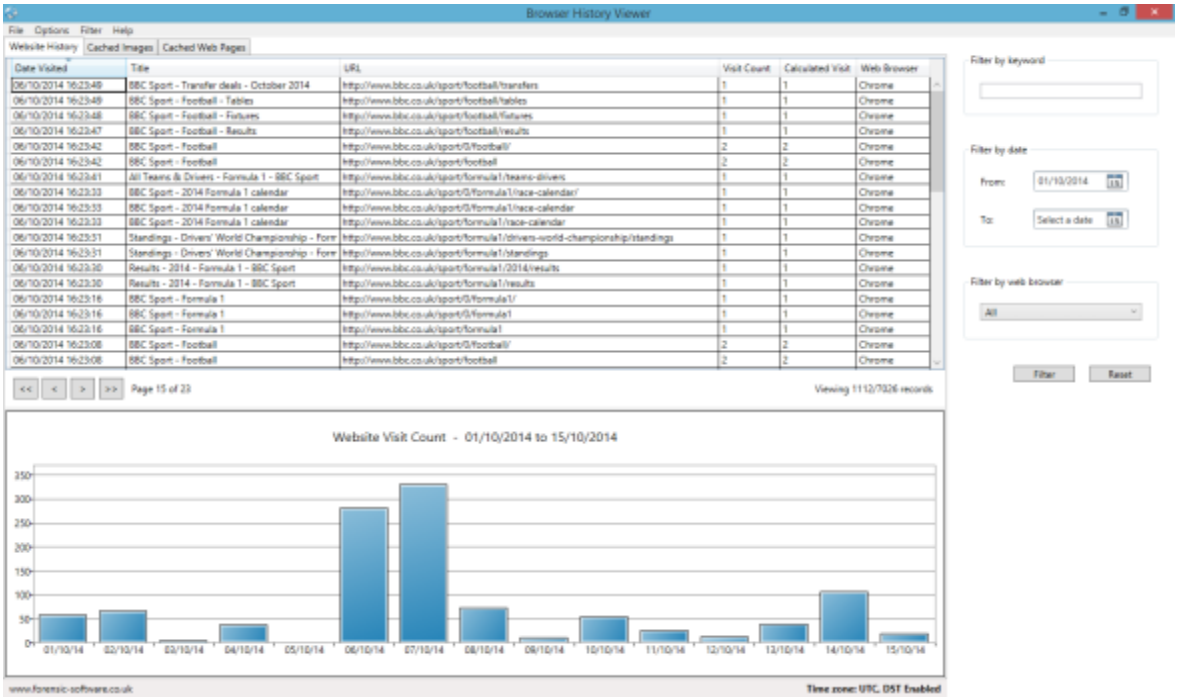
17. Dumpzilla

Extract all interesting information from Firefox, Iceweasel and Seamonkey browser to be analyzed with Dumpzilla.

18. Browser History

Foxton has two free interesting tools.

1. Browser history capturer – capture web browser (chrome, firefox, IE & edge) history on Windows OS.
2. Browser history viewer – extract ana analyze internet activity history from most of the modern browsers. Results are shown in the interactive graph and historical data can be filtered.



19. ForensicUserInfo

Extract the following information with [ForensicUserInfo](#).

- RID
- LM/NT Hash
- Password reset/Account expiry date
- Login count/fail date
- Groups
- Profile path

woanware

20. Kali Linux

[Kali Linux](#) is one of the most popular platforms for penetration testing but it has forensic capability too.

21. Paladin

PALADIN forensic suite – the world's most popular Linux forensic suite is a modified Linux distro based on Ubuntu available in 32 and 64 bit.

22. Sleuth Kit

The Sleuth Kit is a collection of command line tools to investigate and analyze volume and file systems to find the evidence.

23. CAINE

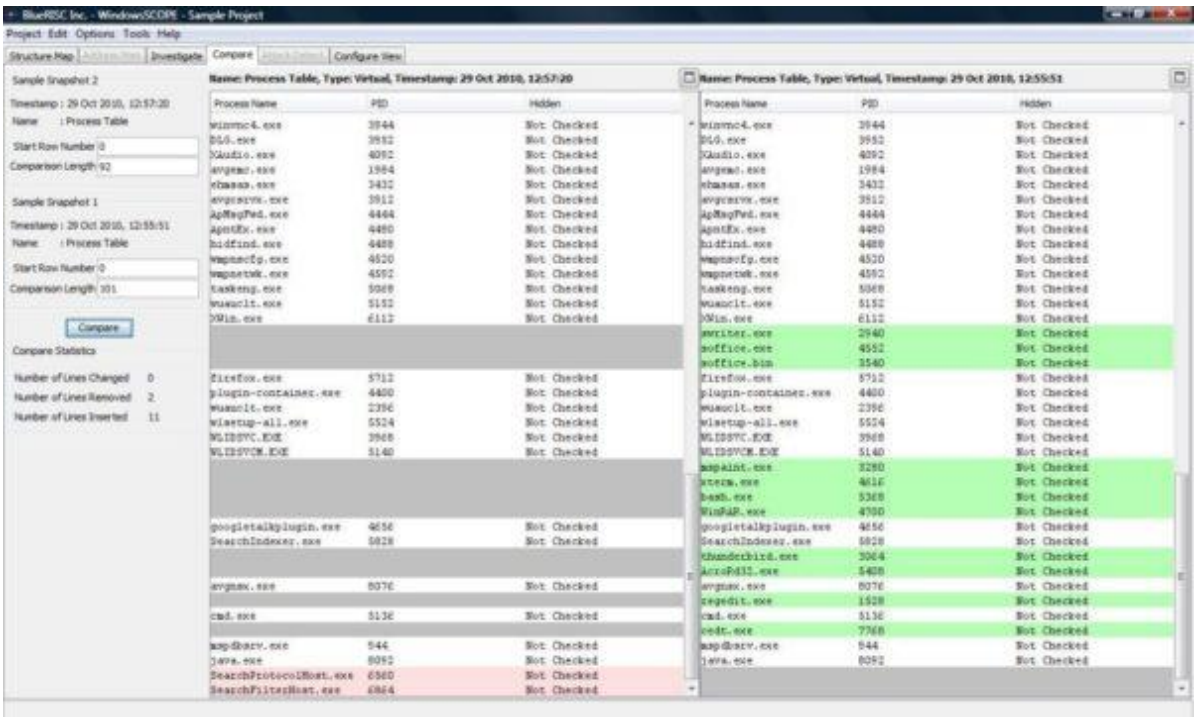
CAINE (**C**omputer **A**ided **In**vestigate **E**nvironment) is Linux distro that offers the complete forensic platform which has more than 80 tools for you to analyze, investigate and create an actionable report.

24. Volatility

Volatility is the memory forensics framework. It used for incident response and malware analysis. With this tool, you can extract information from running processes, network sockets, network connection, DLLs and registry hives. It also has support for extracting information from Windows crash dump files and hibernation files. This tool is available for free under GPL license.

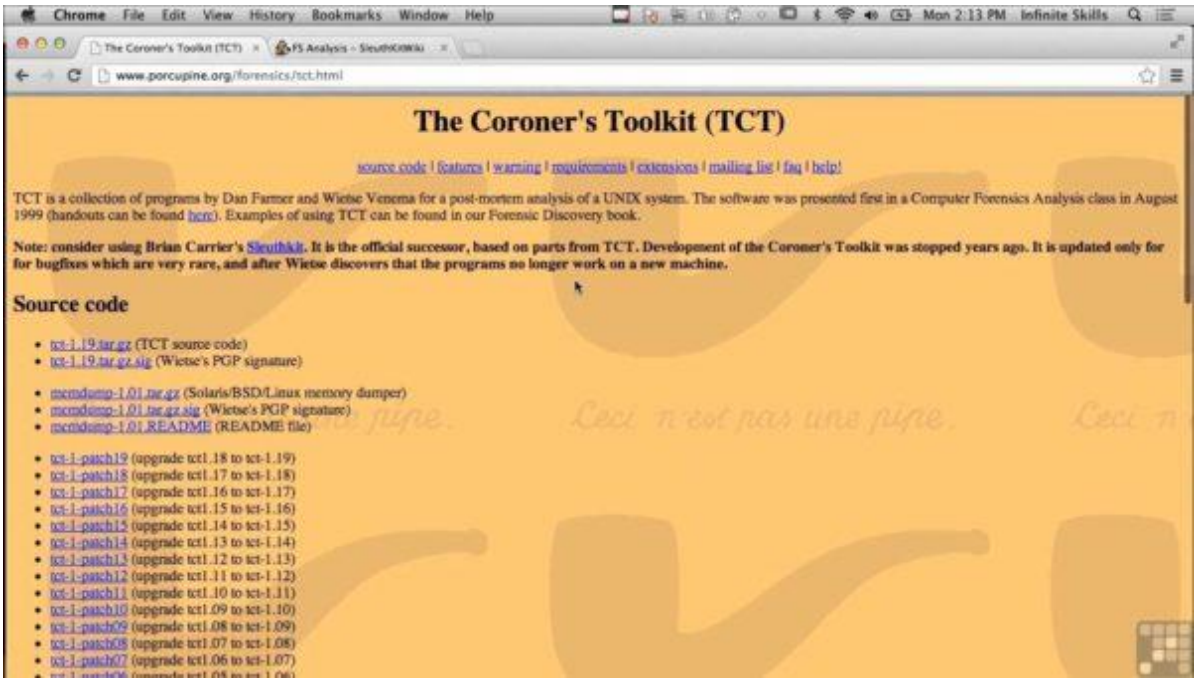
25. WindowSCOPE

WindowsSCOPE is another memory forensics and reverse engineering tool used for analyzing volatile memory. It is basically used for reverse engineering of malwares. It provides the capability of analyzing the Windows kernel, drivers, DLLs, virtual and physical memory.



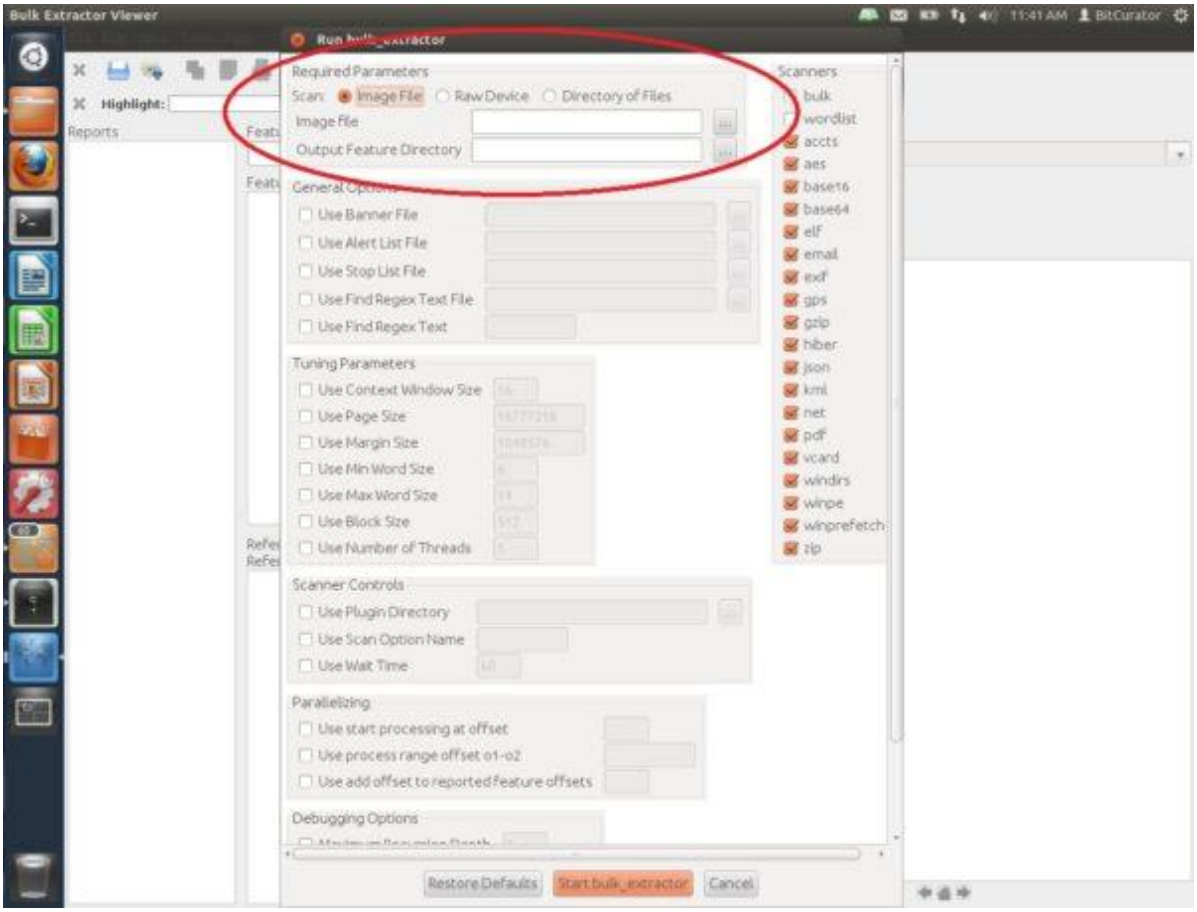
26. The Coroner’s Toolkit

The Coroner’s Toolkit or TCT is also a good digital forensic analysis tool. It runs under several Unix-related operating systems. It can be used to aid analysis of computer disasters and data recovery.



27. Bulk Extractor

Bulk Extractor is also an important and popular digital forensics tool. It scans the disk images, file or directory of files to extract useful information. In this process, it ignores the file system structure, so it is faster than other available similar kinds of tools. It is basically used by intelligence and law enforcement agencies in solving cyber crimes.

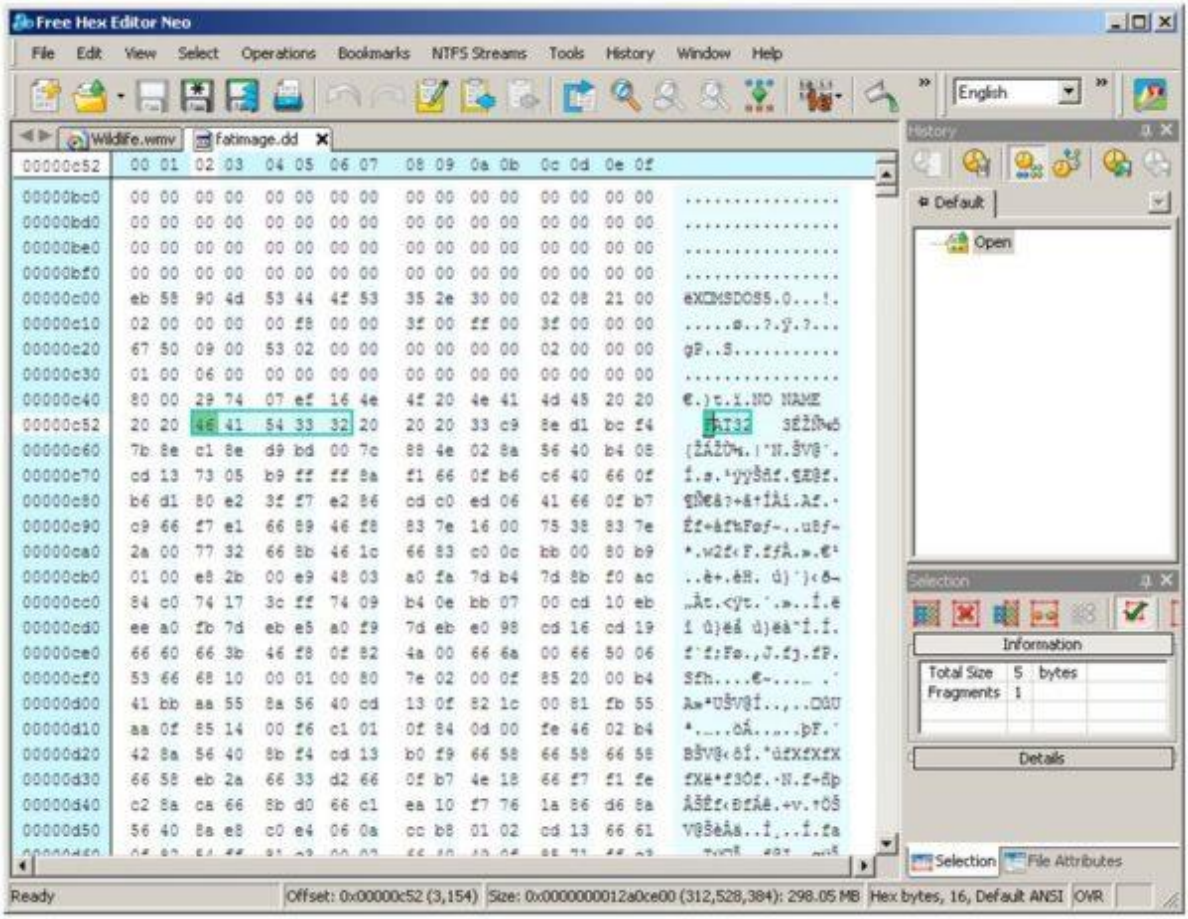


28. Oxygen Forensic Suite

If you are investigating a case that requires you to gather evidence from a mobile phone to support your case, Oxygen Forensics Suite (Standard Edition) is a tool that will help you achieve this.

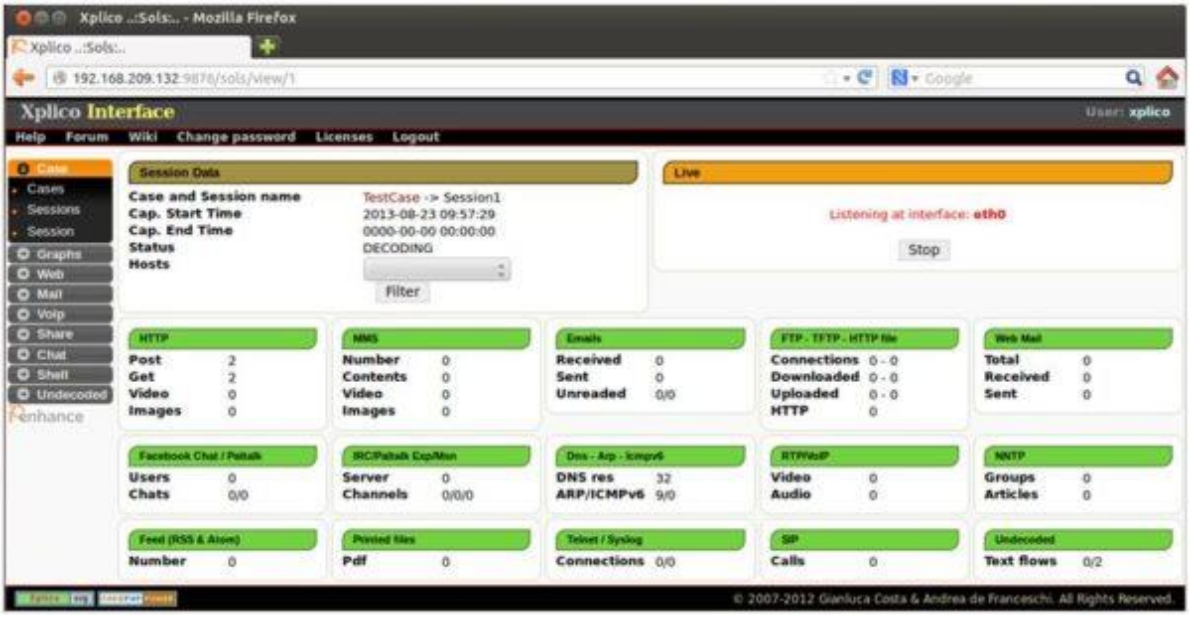
29. Free Hex Editor Neo

Free Hex Editor Neo is a basic hex editor that was designed to handle very large files. While a lot of the additional features are found in the commercial versions of Hex Editor Neo, I find this tool useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.



30. Xplico

Xplico is an open source Network Forensic Analysis Tool (NFAT) that aims to extract applications data from internet traffic (e.g. Xplico can extract an e-mail message from POP, IMAP or SMTP traffic). Features include support for a multitude of protocols (e.g. HTTP, SIP, IMAP, TCP, UDP), TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.


Xplico ..:Sols:.. - Mozilla Firefox
Xplico ..:Sols:..
192.168.209.132:9876/sols/view/1
Google
Xplico Interface
User: xplico
Help Forum Wiki Change password Licenses Logout
Case
Cases
Sessions
Session
Graphs
Web
Mail
Voip
Share
Chat
Shell
Undecoded
Enhance
Session Data
Case and Session name TestCase -> Session1
Cap. Start Time 2013-08-23 09:57:29
Cap. End Time 0000-00-00 00:00:00
Status DECODING
Hosts
Filter
Live
Listening at interface: eth0
Stop
HTTP
Post 2
Get 2
Video 0
Images 0
NNS
Number 0
Contents 0
Video 0
Images 0
Emails
Received 0
Sent 0
Unreaded 0/0
FTP - TFTP - HTTP file
Connections 0 - 0
Downloaded 0 - 0
Uploaded 0 - 0
HTTP 0
Web Mail
Total 0
Received 0
Sent 0
Facebook Chat / Paltalk
Users 0
Chats 0/0
IRC/Paltalk Exp/Msn
Server 0
Channels 0/0/0
Dns - Arp - Icmpv6
DNS res 32
ARP/ICMPv6 9/0
RTP/VoIP
Video 0
Audio 0
NNTP
Groups 0
Articles 0
Feed (RSS & Atom)
Number 0
Printed files
Pdf 0
Telnet / Syslog
Connections 0/0
SIP
Calls 0
Undecoded
Text flows 0/2
© 2007-2012 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.