ISSN 2278-3091

Volume 9 No.2, March - April 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse147922020.pdf

https://doi.org/10.30534/ijatcse/2020/147922020

Design and Implementation of Forensics Process Workflow on Compromised Linux Based Systems

T.NagaDivya Sirisha[1], Dr.S.Srinivasa Rao[2]

[1] MTech, Department of CSE(Cyber Security and Digital Forensics), KLEF, Vaddeswaram,A.P,India, tadiboinasirisha@gmail.com

[2] Associate Professor, Department of CSE,KLEF,Vaddeswaram,A.P,India,srinu1479cse@kluniversity.in

ABSTRACT

Today a diverse variety of devices like smart phones, tablets and IOT devices are being developed. Most of them are based on Linux based platform. Almost every website is deployed on Linux based server.Behind 90% of the websites and every IOT device the backend is Linux operating system. Linux is most popular for its presence in every organization's server room.In case of an incident the probability of us encountering a Linux, system is likely very high. It is also very popular with black hat hackers. When an event occurs in an organization or a hacker attacks a system or server, to determine the methodologies used by that hacker and to know the identity of that hacker we need to perform digital forensics. Digital forensics is playing a crucial role in identifying the vulnerabilities and root causes of the incidents and also help us improve the defense strategies. But unfortunately, there is no standard procedure for implementing this forensic process especially on Linux systems. In this paper a workflow for investigation of Linux operating system running devices is designed and implemented.

Key words: Digital Forensics, Linux forensic, hacking methodologies.

1.INTRODUCTION

Technology became a common word in 21st century. With the advent of laptops, smartphones and IOT devices technology is skyrocketing its pace. Like any other technology digital technology has its side effects too. Using digital device as a tool or targeting a digital device many people are doing illegal activities which are punishable offences.

The world segregated these punishable offences as "cybercrimes". In order to go against cybercrime and extract the root causes and procedures of crime and bring the criminal behind the computer into custody we need different strategies, and these are coined as digital forensics.

This includes various workflows for different kinds of devices and softwares that manage these devices. If an incident happens and a digital forensic investigator came for investigation, he would likely encounter a windows platform based machine. But with today's diversification of devices which are generally based on Linux platforms digital forensics became a challenging task.

Digital forensics is a branch of forensic science that deals with the crimes which are executed using computer as tool or computer as a target. In earlier times of digital enhancements this field is only limited to computers and its storage but due to rapid pace in technological development it has been expanded to cover investigations of all devices capable of storing and processing data[9].

The main aim of digital forensic process is to identify, acquire, collect and preserve data as evidence in a way that preserves its integrity. The entire process is reported in a document called chain of custody or 'Panchanama'.

The methods of digital forensic investigation is based on two factors. They are

1. Hardware
2. System Software (Operating systems).

The devices used in crimes and the operating systems running in those devices determine the method of forensic process work flow. For example, the process for windows operating systems running devices is different from Linux operating system running devices. Forensic experts face many hurdles when investigating a compromised Linux based system because there is no determined approach. Mostly there are well established workflows for investigations on windows-based platforms.

Investigating a compromised Linux operating system-based device is a tedious and perplexing task for investigators. This research is helpful for cyber investigations on systems running Linux operating systems. There are virtualization frameworks for detecting cyber threats[10].

Malware is a software which is used for illegal and malicious purposes. Finding malware is one of the key concept of digital forensics[4]. We experimented on different malware samples and intrusions for designing a workflow on compromised Linux based systems with the help of some tools and scripting we got desired and reliable results.

2. RELATED WORK

Digital investigators face many challenges if they face Linux operating system during investigations. For windows system there is a well-established and implemented forensics workflow for digital forensic investigation. Digital forensic images are used and the authentication of them during investigations is considered very important[3]. Implementation of a forensic workflow for Linux based systems. Conducted experiments on memory images for examining some of the high valued artifacts[5]. For the extraction of exact evidences in a way which are admissible by court the process should be done in a detailed way.

The tools used should be very efficient and reliable. Before doing our experiments, forensic tools are selected carefully for testing and validation. This workflow is designed in accordance with the ACPO principles so that the digital evidence integrity is preserved.

3.LINUX OPERATING SYSTEM

In order to retrieve evidences from a digital device requires complete understanding of the running operating system's architecture and file system structure. In Figure 1 we can see the complete architecture of Linux OS[1].

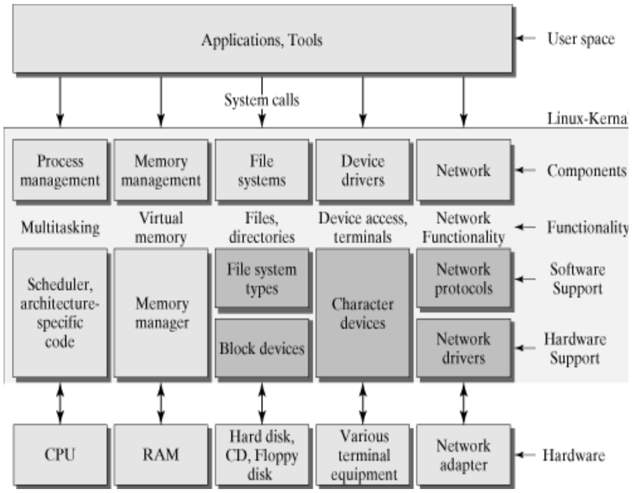


Figure1: Linux architecture

In Linux everything is a file. Linux uses file systems like ext family btfs etc. Present one is ext4.Hackers use timestamp based data hiding to avoid forensics[8].All the information about operations and processes running in the system are stored as logs in text files in /var/log directory.Linux logs provide a time line of events of the running OS,applications and system and this is the first thing a forensic expert should analyze.These logs are created by Linux system daemon 'syslogd' or 'rsyslogd'.Figure 2 shows the file system structure of Linux operating system[2].

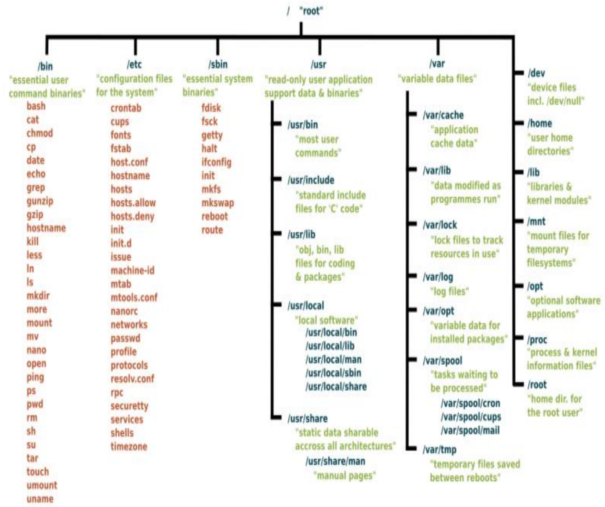


Figure 2: File system structure of Linux

4.FORENSIC WORKFLOW ON COMPROMISED LINUX BASED SYSTEMS

The most common workflow is that creating images of the hard disks acquired during search and seizure and analyzing it.This is done typically in the windows forensic workflows. Linux requires a more detailed and determined approach.During the workflow hash values are calculated before and after acquirement and other phases for authentication purposes[6].

A forensic workstation will be created to minimize the impact on the subject system.Figure 3 shows the designed process workflow.

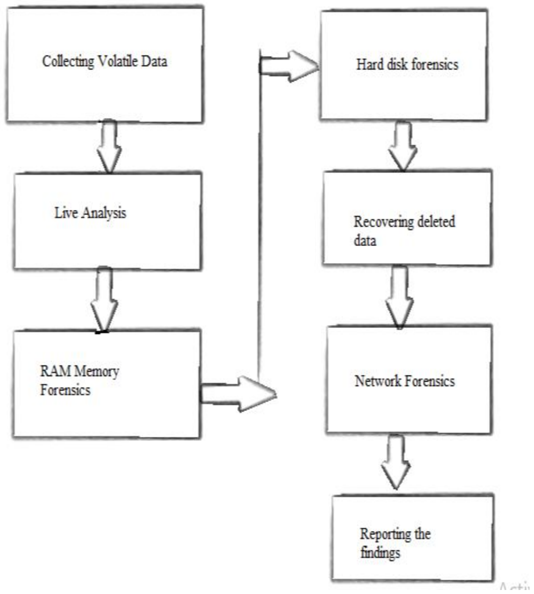


Figure 3: Designed Forensic Process workflow

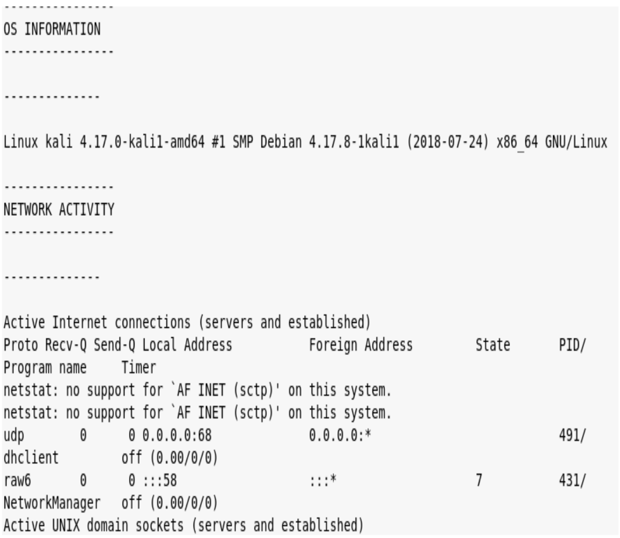
4.1Collecting Volatile Data

Collecting volatile data is the foremost step in the forensic process. This can contain important information and we can also find whether this information is altered in the process of anti-forensics.We can run some commands in the terminal to get this information.Table 1 shows the most common data we should collect..

Table 1:Commands for extracting useful volatile information

Data	Required Command
a.Date and time	Date
b.OS Information	uname -a
c.Open ports	Netstat -anp
d. Network Interfaces	ifconfig
e.Open files	Lsof -v
f.Running processes	ps -ef
g.Loaded kernel module	lsmod
h.mounted file systems	df,mount
e.Users past and present	W, history

We have written a shell script that automates the process of collecting volatile data and gives the output in a file. This will minimize the time taken for the process and the probability of losing important information to be declined.



```
---------------
OS INFORMATION
---------------

-------------

Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64 GNU/Linux

---------------
NETWORK ACTIVITY
---------------

-------------

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/
Program name     Timer
netstat: no support for `AF INET (sctp)' on this system.
netstat: no support for `AF INET (sctp)' on this system.
udp        0      0 0.0.0.0:68              0.0.0.0:*                           491/
dhclient         off (0.00/0/0)
raw6       0      0 :::58                   :::*                    7           431/
NetworkManager   off (0.00/0/0)
Active UNIX domain sockets (servers and established)
```

Screenshot 1: Result of the automated script for collecting volatile data.

After we have collected the volatile data we need to perform the file system analysis.As we have seen in the figure 1. In Linux operating system the data about the performed system actions are maintained in the file system. Analyzing these files can give a lead in finding helpful evidence in the activities performed by the user on the system.

The file descriptions which are given below are some of the files and directories from which a forensic investigator can get help in finding evidences and determining the root causes of the incident or the intrusion.

1. /etc/init.d:

There are various scripts written which are launched when a computer boot.These scripts are stored in inti.d. Intruders can embed malicious scripts in this file so that they can run as a service.

For the malicious scripts to remain running even after reboots intruders make use of some persistent mechanisms which are available in Linux systems consisting of scheduled tasks, drivers, services etc.So, a digital forensic investigator should analyze these files for evidences.

2./etc/passwd:
This file contains the information about the users who are accessing the machine-like usernames, startup programs which are executed when a user logs in and user's home directory. These can be of valuable information to the investigator.

3./etc/networks:
The networks list which are connected to the system are available in this file.

4./etc/hosts:
With the information present in this file the forensic investigator can conclude that when the system is connected to which network. This file contains information about the IP addresses of the system.

5./etc/shadow:
This file maintains the log in authentication information of the user.The data in this file are user login name and salted password. With this the investigator can get hold of any faulted login attempts by intruders.

6./etc/cron.d:
This directory contains scripts which are scheduled to run at regular intervals so that the system performance can be kept track of. This is one of the best places for an intruder or hacker to place his malicious codes. The investigator should have a look at these files to determine suspicious activity.

7./usr/lib:
This file consists of program libraries.These are collections of routines which are frequently used.

8./usr/bin:
In Linux based systems the information about the configurations of the applications installed on the machine. Using this information the examiner can get crucial data like the configurations of the programs a particular user installed on the system, the date of installation of certain application and it's modified date and timings and also the permissions it has and the size of the application.

9./var/log/syslog:
Syslog file maintains the login and shutdown timings of the users. It also contains the date and time of a particular network connection which is connected to the system.

This information can give an insight to the investigator to reconstruct the crime and to predict the criminal and his process of crime.

10. /var/lastlog:
The recent login information can be extracted from this file. The forensic investigator can be able to know who is logged in at the time of incident.

11. /var/faillog:
This file contains user failed login attempts. By this the target user can be identified.

12./proc/cpuinfo:
The information of the CPU will be in this file. By analyzing this data, we can get hold of any abnormal activity running in the system.This can be detected by activities like higher or lower CPU cycle rates, exhaustion of memory etc.

13. /proc/net/netstat:
This file maintains network information of the system. If there are any suspicious connections can be detected by the investigator.

14./proc/PID/exe:
This directory contains the Link to the executable of the process which is identified by PID i.e process id. If there are malicious programs running through this process they can be identified.

15. /dev:
The list of hardware devices which are attached to the machine are maintained by this directory. This information provides the investigator to identify any suspicious usb drives, cd drives, hard disks, and other biometric devices.

4.2. Live Analysis

After collecting the data, it is time to delve deeper into the system to determine if there is a malware or the system has been hacked. RAM represents the exact state of the running system. Therefore, it contains commands executed, drivers loaded and plethora of information regarding forensic investigation like running process,instant messages etc.

In this step we have taken the dump of the RAM memory and that acquired image file is analyzed in the RAM memory forensics phase.To dump the RAM of a Linux operating system running machine we used LiME tool.

This is a Loadable kernel module (LKM) which allows for volatile memory acquisition on Linux and Linux based devices.Its features are shown in Table 2.

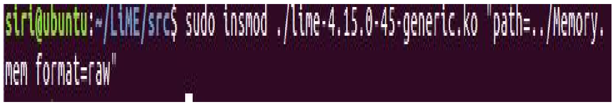
Table 2: Features of LiME

FEATURES OF LiME	
a.	Full memory acquisition
b.	Acquisition over network interfaces
c.	Minimal process footprint
d.	Hash of dumped memory

LiME can be cloned from git repository and executed. LiME utilizes insmod command to load the module.Required arguments for its execution are the path to store the memory image file and the format of the image file.

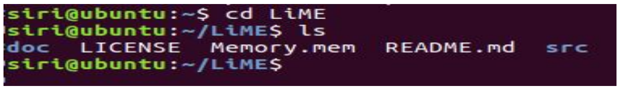
There are three different formats to choose padded,raw and LiME. In raw format every segment of memory is concatenated. In padded format blocks of zeros are not skipped like that of raw format. With that we can not only know the contents but file locations also. LiME format captures memory and it will store in structures with metadata. This supports two various paths a file or a network port.

The results of the RAM memory acquisition is show below



```
siri@ubuntu:~/LiME/src$ sudo insmod ./lime-4.15.0-45-generic.ko "path=../Memory.
mem format=raw"
```

Screenshot 2: Dumping RAM



```
siri@ubuntu:~$ cd LiME
siri@ubuntu:~/LiME$ ls
doc   LICENSE   Memory.mem   README.md   src
siri@ubuntu:~/LiME$
```

Screenshot 3: The acquired image

4.3.RAM Memory Forensics

To investigate malware infections and other sophisticated intrusions analyzing RAM is a must. Analyzing RAM in a way the evidences can be extracted is called RAM memory forensics. It plays a crucial role in the police case investigations.

Capturing memory completely on a compromised Linux system generally overcomes anti-forensics methods infused in malware by the attackers. With this the forensic investigator can get a more comprehensive view of the intrusion[7].

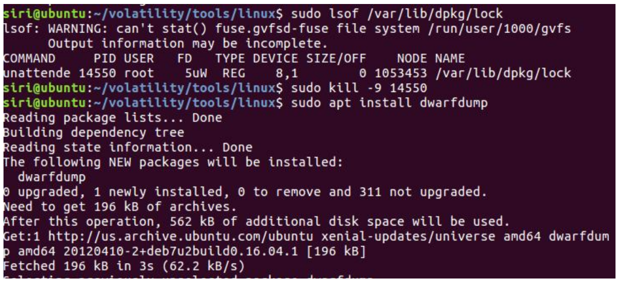
Often malware is designed to leave very little trace anywhere on the system, which is compromised, and the only exact indicators of compromise can be seen in RAM. So, RAM forensics plays an important role in extracting evidences that are not obtainable in traditional ways.

Memory analysis contributes a major part in digital forensics investigations in present and also in future. Volatility is a tool which is recognized worldwide for memory forensics.

Volatility is being developed and maintained by one of the biggest forensic communities. Every significant operating system such as Windows, MAC, Linux supports volatility.

Steps for analyzing dumped RAM memory image file through Volatility tool

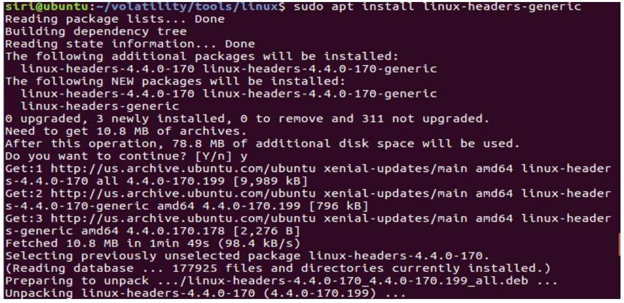
1.Clone Volatility from github repository
2.Creating profile for volatility.



```
siri@ubuntu:~/volatility/tools/linux$ sudo lsof /var/lib/dpkg/lock
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND     PID USER   FD   TYPE DEVICE SIZE/OFF    NODE NAME
unattende 14550 root    5uW  REG    8,1        0 1053453 /var/lib/dpkg/lock
siri@ubuntu:~/volatility/tools/linux$ sudo kill -9 14550
siri@ubuntu:~/volatility/tools/linux$ sudo apt install dwarfdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dwarfdump
0 upgraded, 1 newly installed, 0 to remove and 311 not upgraded.
Need to get 196 kB of archives.
After this operation, 562 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 dwarfdum
p amd64 20120410-2+deb7u2build0.16.04.1 [196 kB]
Fetched 196 kB in 3s (62.2 kB/s)
```

Screenshot 4: Result of creating profile for volatility

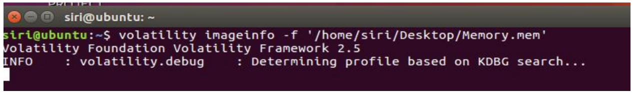
3.Installing Linux headers



```
siri@ubuntu:~/volatility/tools/linux$ sudo apt install linux-headers-generic
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  linux-headers-4.4.0-170 linux-headers-4.4.0-170-generic
The following NEW packages will be installed:
  linux-headers-4.4.0-170 linux-headers-4.4.0-170-generic
  linux-headers-generic
0 upgraded, 3 newly installed, 0 to remove and 311 not upgraded.
Need to get 10.8 MB of archives.
After this operation, 78.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 linux-header
s-4.4.0-170 all 4.4.0-170.199 [9,989 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 linux-header
s-4.4.0-170-generic amd64 4.4.0-170.199 [796 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 linux-header
s-generic amd64 4.4.0.170.178 [2,276 B]
Fetched 10.8 MB in 1min 49s (98.4 kB/s)
Selecting previously unselected package linux-headers-4.4.0-170.
(Reading database ... 177925 files and directories currently installed.)
Preparing to unpack .../linux-headers-4.4.0-170_4.4.0-170.199_all.deb ...
Unpacking linux-headers-4.4.0-170 (4.4.0-170.199) ...
```

Screenshot 5: Result of installing Linux headers

4.Analyzing through Volatility



```
siri@ubuntu:~$ volatility imageinfo -f '/home/siri/Desktop/Memory.mem'
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
```

Screenshot 6: Results of analyzing through volatality

4.4. Hard disk Forensics

To reconstruct the crime events the analysis of memory is an important step.Secondary memory is considered to be the most crucial part for evidence extraction.

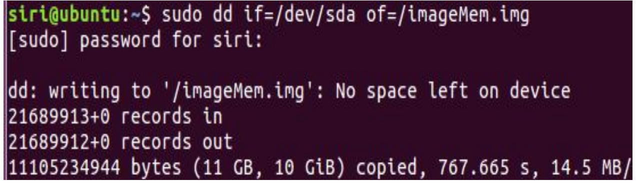
Hard disk is the secondary memory of the system while primary being RAM memory, CPU registers and buffers. This Hard disk contains valuable information which can be used as critical evidences like image files,text files and audio files.

This forensic process is done in two steps
4.4.1. Creating hard disk images
4.4.2. Analyzing created images

4.4.1. Creating hard disk images

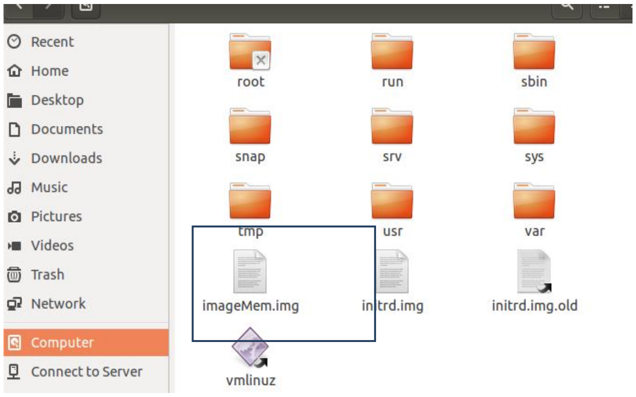
This is useful for analyzing the hard disk memory for evidences. As the folders of the system contain valuable information and can be treated as evidence. Since digital memory is very volatile and can be tampered easily while acquiring these images software or hardware write blocking is used.

We use dd tool to create images in Linux systems



```
siri@ubuntu:~$ sudo dd if=/dev/sda of=/imageMem.img
[sudo] password for siri:

dd: writing to '/imageMem.img': No space left on device
21689913+0 records in
21689912+0 records out
11105234944 bytes (11 GB, 10 GiB) copied, 767.665 s, 14.5 MB/
```

Screenshot 7: Creating disk image

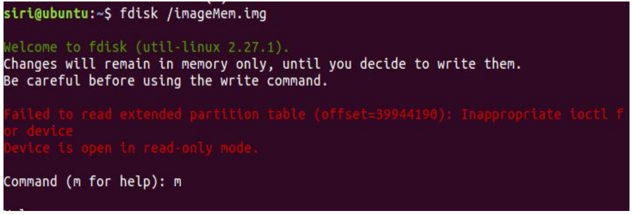


Screenshot 8: Result of the created memory image

4.4.2. Analyzing hard disk image

The subject system hard disk images are analyzed using fdisk and mount option in Linux distributions or we can clone the entire hard disk into another hard disk andcan view and verify the contents.

1.Mounting Partitions

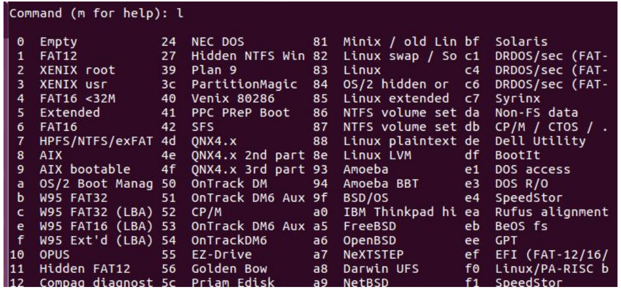


```
siri@ubuntu:~$ fdisk /imageMem.img

Welcome to fdisk (util-linux 2.27.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Failed to read extended partition table (offset=39944190): Inappropriate ioctl f
or device
Device is open in read-only mode.

Command (m for help): m
```

Screenshot 9: Mounting Partitions

There are list of commands to analyze the mounted images.

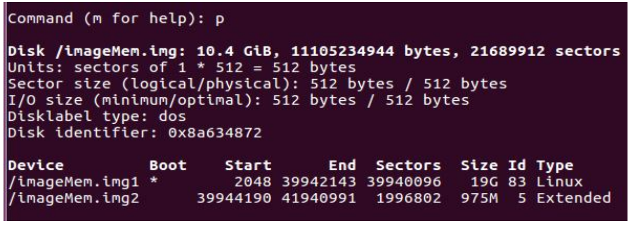
1.L – list known partition types



```
Command (m for help): l

 0  Empty           24  NEC DOS         81  Minix / old Lin bf  Solaris
 1  FAT12           27  Hidden NTFS Win 82  Linux swap / So c1  DRDOS/sec (FAT-
 2  XENIX root      39  Plan 9          83  Linux           c4  DRDOS/sec (FAT-
 3  XENIX usr       3c  PartitionMagic  84  OS/2 hidden or  c6  DRDOS/sec (FAT-
 4  FAT16 <32M      40  Venix 80286     85  Linux extended  c7  Syrinx
 5  Extended        41  PPC PReP Boot   86  NTFS volume set da  Non-FS data
 6  FAT16           42  SFS             87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS/exFAT 4d  QNX4.x          88  Linux plaintext de  Dell Utility
 8  AIX             4e  QNX4.x 2nd part 8e  Linux LVM       df  BootIt
 9  AIX bootable    4f  QNX4.x 3rd part 93  Amoeba          e1  DOS access
 a  OS/2 Boot Manag 50  OnTrack DM      94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       51  OnTrack DM6 Aux 9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 52  CP/M            a0  IBM Thinkpad hi ea  Rufus alignment
 e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         eb  BeOS fs
 f  W95 Ext'd (LBA) 54  OnTrackDM6      a6  OpenBSD         ee  GPT
10  OPUS            55  EZ-Drive        a7  NeXTSTEP        ef  EFI (FAT-12/16/
11  Hidden FAT12    56  Golden Bow      a8  Darwin UFS      f0  Linux/PA-RISC b
12  Compaq diagnost 5c  Priam Edisk     a9  NetBSD          f1  SpeedStor
```

Screenshot 10: Result of list of known partition types

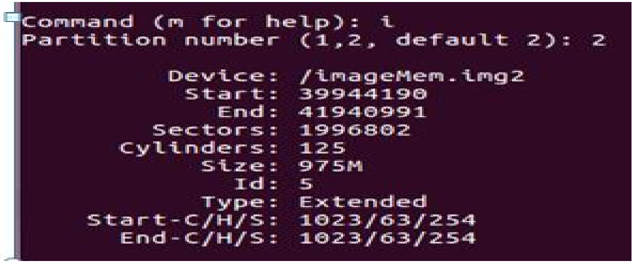
2.P – print partition tabe



```
Command (m for help): p

Disk /imageMem.img: 10.4 GiB, 11105234944 bytes, 21689912 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x8a634872

Device         Boot    Start      End  Sectors  Size Id Type
/imageMem.img1 *        2048 39942143 39940096   19G 83 Linux
/imageMem.img2      39944190 41940991  1996802  975M  5 Extended
```

Screenshot 11: Result of printing partition table

3. i – Information about particular partition



```
Command (m for help): i
Partition number (1,2, default 2): 2

         Device: /imageMem.img2
          Start: 39944190
            End: 41940991
        Sectors: 1996802
      Cylinders: 125
           Size: 975M
             Id: 5
           Type: Extended
    Start-C/H/S: 1023/63/254
      End-C/H/S: 1023/63/254
```

Screenshot 12: Result of information about particular partition

4.5. Recovering Deleted data

Data means information or any kind of file which was used to store important notes like dates, subjects, movies, videos and many more. All comes under data or information and some time the data will be deleted or may be lost by unknown actions performed on the system.

The intruders and hackers will delete crucial evidence information as a part of anti-forensic techniques so that he/she cannot be traced out. Recovering this data will be helpful in investigations. The data which is not overwritten by other data can only be recovered.

In windows the data deletion means that file is removed from the partition table. In Linux the file deletion means it is deleted from the inode. The complete destruction of data can only do when it is overwritten by another data in the memory. Thus, only data which is not over written can be recovered.

Sometimes the data will be deleted accidentally or because of some error corrections, data will be lost or deleted and not found in recycle bin also and that lost data is called as deleted data and it will only recovered with the help of the recovery tools only.

In windows there are many numbers of tools and in these tools, some are free, and some are paid ones. Just like that every other operating systems has their own data recover tools and as a part of our forensic workflow in this paper we are using one of the perfect tools to recover data as well as to test the data in the system which contains Linux operating system.

Extracting deleted data is an important task in forensics because it can contain valuable information for investigation purposes. The tool we used here is testdisk.

There are two ways to install this tool in ubuntu and the two ways are as follows

Step-1: Installation
Installing with command:
First open the terminal in ubuntu and then check it has all the packages to install a tool in it or not by performing installation operation. If it doesn't install, then it shows the needed things to install the software in Linux.Arch Linux users can install it from AUR.

After install the packages which are shown in the terminal with the given command and then type this command to install the tool in Ubuntu and the command is "sudo apt install testdisk".

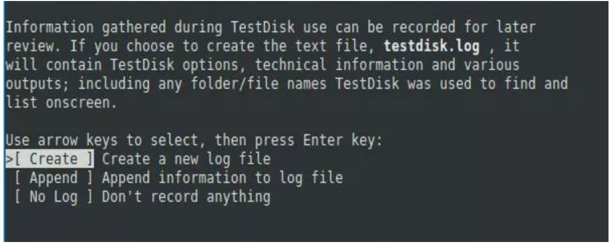
Installation with tool:
To install in this way user has to go to open the browser and then type testdisk and then many links appears and then we get the tool by opening this website called It's FOSS with a blue box. By clicking on the blue box, the tool will be downloaded.

And then user has to install the tool manually and it takes a minute to get installed and to be available for the access to recover data.

Step-2: To run this tool we have to open the terminal after installing the tool and then have to type this command "testdisk"

Step-3: After entering that command then a new interface will be appeared and then the tool will start from here. From this point the operation was only done by using arrow keys and enter button only.

The following will show three operations and from the three we have to choose option "Create"

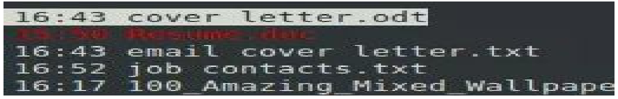


```
Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
 [ Append ] Append information to log file
 [ No Log ] Don't record anything
```

Screenshot 13: Executing testdisk

Step-4:After that it will directs to another screen in that it shows another three operation for next operation and then a drive is selected to create a log and then has to choose option "sudo" to complete and to go next.

Step-5:Then it shows the list of deleted files choose the files to get recovered.

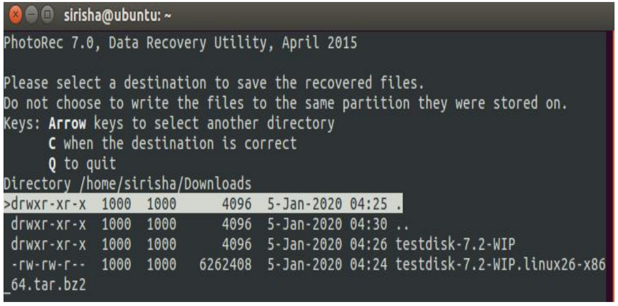


```
 16:43 cover letter.odt
 15:50 Resume.doc
 16:43 email cover letter.txt
 16:52 job contacts.txt
 16:17 100_Amazing_Mixed_Wallpape
```

Screenshot 14: List of deleted files in a particular file

Step-6: Click c to copy the selected files.

Step-7:Choose destination folder.



```
PhotoRec 7.0, Data Recovery Utility, April 2015

Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /home/sirisha/Downloads
>drwxr-xr-x  1000  1000      4096  5-Jan-2020 04:25 .
 drwxr-xr-x  1000  1000      4096  5-Jan-2020 04:30 ..
 drwxr-xr-x  1000  1000      4096  5-Jan-2020 04:26 testdisk-7.2-WIP
 -rw-rw-r--  1000  1000   6262408  5-Jan-2020 04:24 testdisk-7.2-WIP.linux26-x86
_64.tar.bz2
```

Screenshot 15: Destination folder selection

The results will be in the destination folder.

4.6.Network Forensics

Network forensics is a part of digital forensics investigation involving monitoring, capturing and analysis of suspicious system's or network's network traffic. This provides for legal evidence extraction, information gathering and intrusion detection.

Analyzing a compromised system's network connections and traffic delivers important pieces of evidences.Network forensic investigations unlike other analysis procedures deal with data which is highly volatile and dynamic.This information gets lost making network investigations crucial with time constraints.

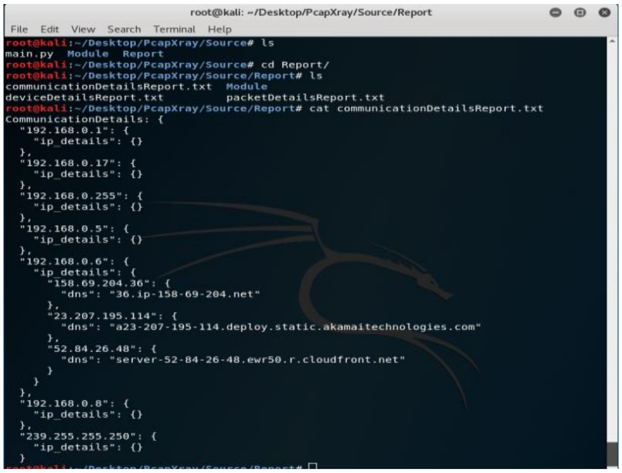
Network forensics can be done by live monitoring of traffic and also by capturing the network traffic into a pcap file. Pcap which means packet capture contains information about the packets and the data present in the packets which are transmitted along the network.This consists of an API(Application program interface) for capturing the traffic.

A pcap file is created to analyze the network traffic of the system. Browser artifacts are also collected along with the pcap file. Given a Pcap File, we can plot a network diagram displaying hosts in the network, network traffic, highlight important traffic and Tor traffic as well as potential malicious traffic including data involved in the communication.

A pcap file is generated using a tool called wireshark. Wireshark is widely tool and is very reliable for live monitoring of network and pcap file generation. This generated pcap file is used to analyze the network with the help of some tools like pcapxray and xplico.

In this workflow we used pcapxray tool for investigation of networks connected to the system and the packets travelled to and fro from the system. This tool is a command line inclined tool.

The results from the analysis of the pcap file generated in the suspicious network can be seen in the picture below.


root@kali: ~/Desktop/PcapXray/Source/Report
File Edit View Search Terminal Help

```
root@kali:~/Desktop/PcapXray/Source# ls
main.py  Module  Report
root@kali:~/Desktop/PcapXray/Source# cd Report/
root@kali:~/Desktop/PcapXray/Source/Report# ls
communicationDetailsReport.txt  Module
deviceDetailsReport.txt         packetDetailsReport.txt
root@kali:~/Desktop/PcapXray/Source/Report# cat communicationDetailsReport.txt
CommunicationDetails: {
  "192.168.0.1": {
    "ip_details": {}
  },
  "192.168.0.17": {
    "ip_details": {}
  },
  "192.168.0.255": {
    "ip_details": {}
  },
  "192.168.0.5": {
    "ip_details": {}
  },
  "192.168.0.6": {
    "ip_details": {
      "158.69.204.36": {
        "dns": "36.ip-158-69-204.net"
      },
      "23.207.195.114": {
        "dns": "a23-207-195-114.deploy.static.akamaitechnologies.com"
      },
      "52.84.26.48": {
        "dns": "server-52-84-26-48.ewr50.r.cloudfront.net"
      }
    }
  },
  "192.168.0.8": {
    "ip_details": {}
  },
  "239.255.255.250": {
    "ip_details": {}
  }
root@kali:~/Desktop/PcapXray/Source/Report# 
```

Screenshot 16: Results of an analysis of pcap file.

5.RESULTS

From this forensic process workflow on the compromised Linux based systems we can see important differences between windows forensic workflows and Linux forensic workflow.

With this process we can mount images acquired in acquisition phase in read-only mode without the help of software and hardware writeblockers which is usually a very important aspect in windows workflow. Mounting an image as a file system can show us the entire storage and without alteration, we can extract evidences.

This Linux based workflow uses bash scripts to minimize the disturbances on the subject system. The tools used in this workflow are inclined to command line and can be a competitive task to investigators.

From this workflow in every phase we can extract crucial information which can be submitted as evidences in court of law. In the first stage itself we can get a jist of the system situation to delve deeper. From live analysis we can get more crucial information from RAM memory. With the analysis of hard disk, we can get the entire storage in the system for analysis even deleted data with recovery.
We have injected several malware samples and identified their traces through this workflow and intrusions are also has been detected.

6.CONCLUSION

Linux operating system has a wide variety of tools for conducting forensic investigations. For each phase we have a dedicated tool with superior features which can be relied upon for modern day's hardware requirements. Most of them are free of cost. Investigation with knowledge of Linux architecture, file system and with the help of this workflow production and extraction of reliable evidences is proved.

REFERENCES

[1] https://www.Linux-india.org.

[2] https://www.Linux.com

[3] Somayeh Soltani and Seyed Amin Hosseini Seno "**A survey on digital evidence collection and analysis**" *Conference: 2017 7th International Conference on Computer and Knowledge Engineering (ICCKE)* https://doi.org/10.1109/ICCKE.2017.8167885

[4] Ahmed Amer, Normaziah A. Aziz, **"Malware Detection through Machine Learning Techniques"**,*International Journal of Advanced Trends in Computer Science and Engineering" , September- October 2016.2408-2413* . https://doi.org/10.30534/ijatcse/2019/82852019

[5] Moses Ashawa and MorrisNtonja **"Design and Implementation of Linux based Workflow for Digital Forensics Investigation"**, *International Journal of Computer Applications (0975 – 8887) Volume 181 – No. 49, April 2019.* https://doi.org/10.5120/ijca2019918684

[6] KoduruPrasada Rao, Dr G Lavanya Devi**," Information Security Using Hilbert With Hash Value"**, *International Journal of Advanced Trends in Computer Science andEngineering, September-October 2019.*

[7] Lorehttpnz Liebler and Frank Breitinger **"mrsh-mem: Approximate matching on raw memory dumps"**, *2018 11th International Conference on IT Security Incident Management & IT Forensics.* https://doi.org/10.1109/IMF.2018.00011

[8] Thomas Gobel, Harald Baier **"Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding"**, *DFRWS 2018 Europe d Proceedings of the Fifth Annual DFRWS Europe.* https://doi.org/10.1016/j.diin.2018.01.014

[9] Jeferson dos Santos Almeida, Leonardo de Santana Nascimento, Diogenes Antonio Marques Jose **"Computer Forensics: A Linux Case Study Applied to Pedophilia Crime Investigation in Brazil"** , *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 31-42,The Society of Digital Information and Wireless Communications (SDIWC), 2019.*

[10] D'Mita Levy, "**Design of Virtualization Framework to Detect Cyber Threats in Linux Environment", ***2017 IEEE 4th International Conference on Cyber Security and Cloud Computing.* https://doi.org/10.1109/CSCloud.2017.18