SIFT Workstation for Digital Forensics and Incident Response

Name: Sharvari Dubey

Group: A

Topic: SIFT-week 2 assignment

Index

1. Introduction
2. SIFT Workstation
3. Demonstration
4. Tools
5. Case Study
6. Assessment Answers

Introduction

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Digital Forensics and Incident Response (DFIR) are two critical components of the cybersecurity field, focused on investigating and responding to cyber incidents and breaches.

1. **Digital Forensics:**

Digital forensics involves the systematic investigation and analysis of digital devices, networks, and data in order to gather evidence related to a cyber incident or criminal activity. This process aims to identify, preserve, recover, and present digital evidence that can be used in legal proceedings, incident analysis, or to better understand the nature of a cyber attack.

Key aspects of digital forensics include:

- Evidence Collection: Identifying and preserving potential evidence from various digital sources like computers, smartphones, servers, cloud storage, network logs, etc.
- Data Recovery: Extracting and recovering data from storage media, even if attempts have been made to delete or hide information.
- Analysis: Examining the collected data to reconstruct events, determine the cause of the incident, and identify the parties involved.
- Chain of Custody: Maintaining a secure and documented chain of custody to ensure the integrity and admissibility of the evidence in legal proceedings.

Tutelr.

2. **Incident Response:**

Incident Response (IR) is a structured approach to managing and mitigating the impact of cybersecurity incidents, such as data breaches, malware infections, system compromises, or network intrusions. The primary goal of incident response is to minimize the damage, contain the incident, and restore normal operations as quickly as possible.

Key elements of incident response include:

- Detection and Identification: Recognizing signs of potential security incidents and distinguishing them from normal network activity.
- Containment: Isolating affected systems or networks to prevent further spread of the incident and mitigate potential damage.
- Eradication: Identifying the root cause of the incident and eliminating the source of the problem from the affected systems.
- Recovery: Restoring affected systems to a secure state and resuming normal operations.
- Lessons Learned: Analyzing the incident response process to identify weaknesses and areas for improvement in the organization's security posture.

Both digital forensics and incident response play crucial roles in enhancing an organization's cybersecurity capabilities. Digital forensics helps to understand the nature and scope of an incident, while incident response helps to effectively manage and recover from the incident while also preventing future occurrences. These two disciplines work hand-in-hand to strengthen an organization's ability to detect, respond, and recover from cyber threats.

SIFT Workstation

The SIFT (SANS Investigative Forensic Toolkit) Workstation is a specialized Linux distribution developed and maintained by the SANS Institute, a leading provider of cybersecurity training and certification. The SIFT Workstation is designed specifically for digital forensics, incident response, and media exploitation.

Key features and components of the SIFT Workstation include:

1. Forensics Tools: The SIFT Workstation comes pre-installed with a wide range of open-source digital forensics tools and utilities, making it a comprehensive platform for conducting forensic investigations. These tools cover areas such as disk and memory analysis, network forensics, file carving, metadata analysis, and more.
2. User-Friendly Interface: Despite being a Linux distribution, the SIFT Workstation is designed with a user-friendly interface, making it accessible to both experienced forensic analysts and those new to digital forensics.
3. Virtual Appliance: The SIFT Workstation is available as a virtual appliance, allowing users to run it within a virtualization environment like VMware or VirtualBox. This makes it easy to integrate into existing forensic workflows and reduces the need for dedicated hardware.
4. Constantly Updated: The SIFT Workstation is actively maintained by SANS, and updates are released regularly to ensure it remains current and effective in handling the latest forensic challenges.
5. Community Support: SANS maintains an active community around the SIFT Workstation, offering support, sharing knowledge, and providing valuable resources for digital forensics professionals.
6. Training and Certification: SANS offers various training courses related to digital forensics and incident response, and the SIFT Workstation is often used in conjunction with these courses to provide hands-on experience in real-world scenarios.

It's worth noting that the SIFT Workstation is just one of many digital forensics tools and distributions available. Digital forensics professionals often choose their toolkits based on their specific needs, the type of cases they handle, and personal preferences. Other popular forensic distributions include Kali Linux and DEFT (Digital Evidence & Forensics Toolkit).

Demonstration

1) Go to the official website of SANS and download SIFT Workstation → SIFT-Workstation
2) To download the file you need to login to your SANS account and if you don't have one then create a SANS account to login.
3) The file will be downloaded with the .ova extension.

Option 1: SIFT Workstation VM Appliance

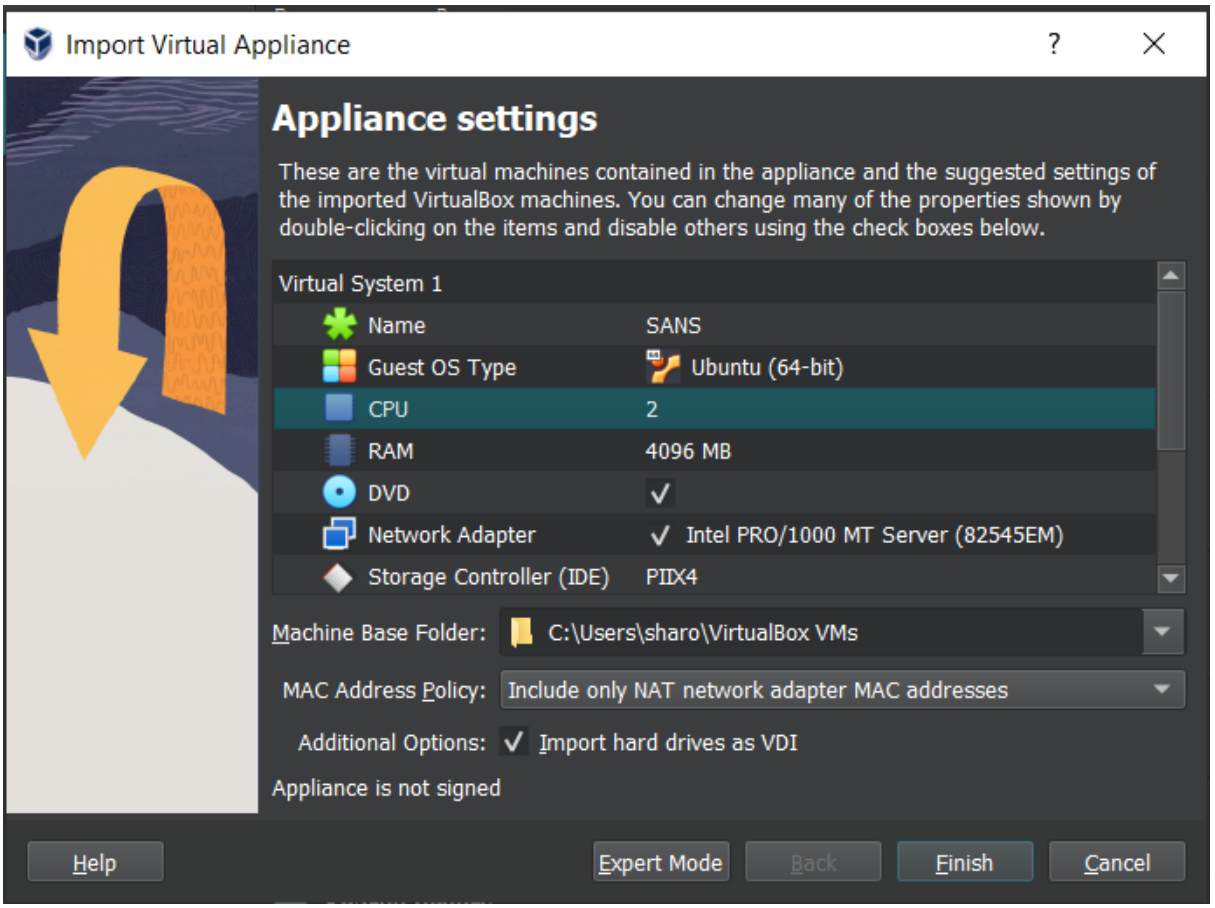
Login to download

Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine. Once you have booted the virtual machine, use the credentials below to gain access.

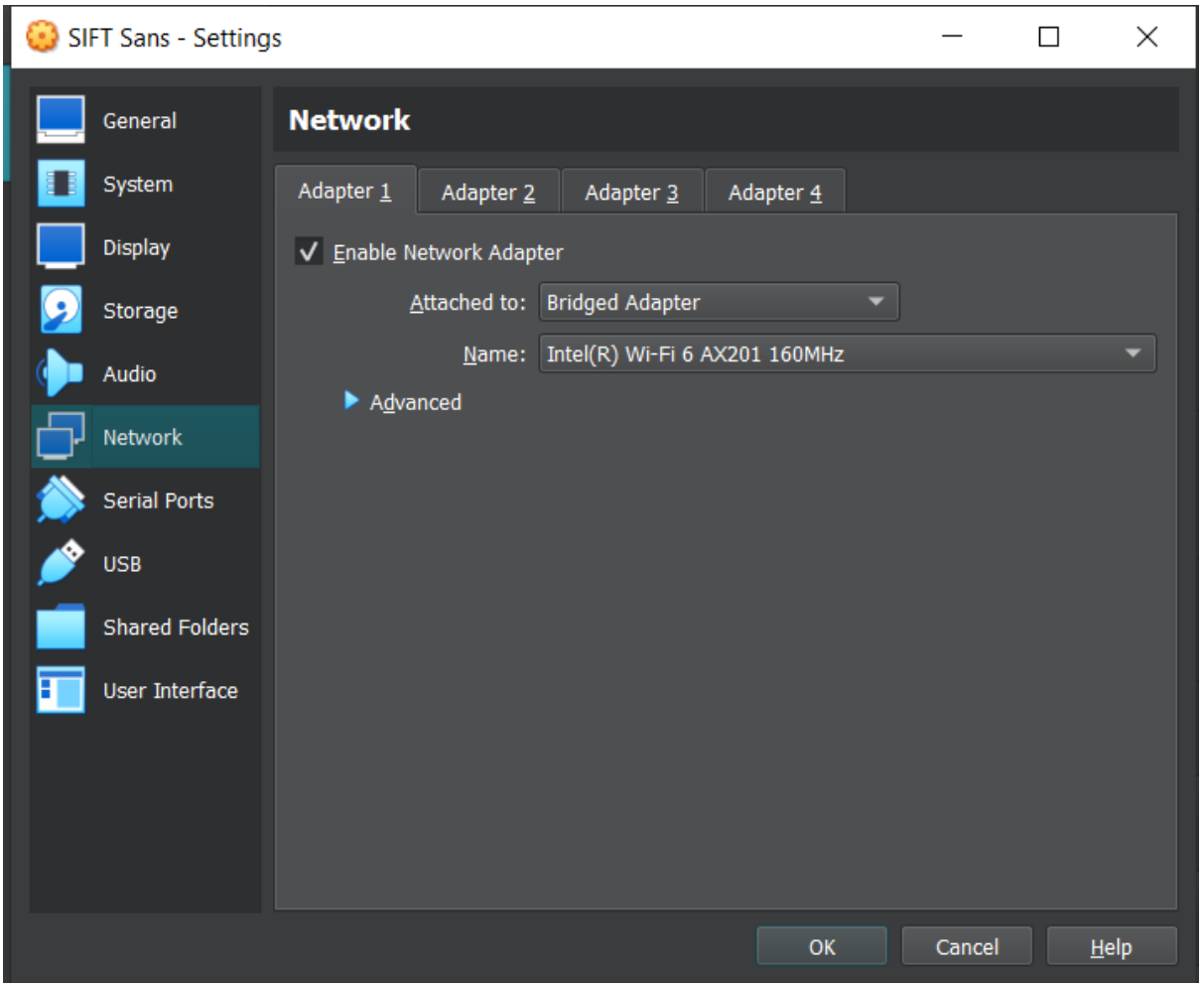
- Login = **sansforensics**
- Password = **forensics**
- $ **sudo su -**
  - Use to elevate privileges to root while mounting disk images.
- Hash Values
  - MD5: b838d44bd56ad0e8f4f6a5a6b00b7c8d SIFT-Workstation.ova
  - SHA256: 27fac07e95498db5eaaa2c6c0b85ef9ca96090fb0964e552a7792a441ebe4d74 SIFT-Workstation.ova

Having trouble downloading SIFT?

If you are having trouble downloading the SIFT Workstation VM, please contact sift-support@sans.org and include the URL you were given, your public IP address, browser type, and if you are using a proxy of any kind.



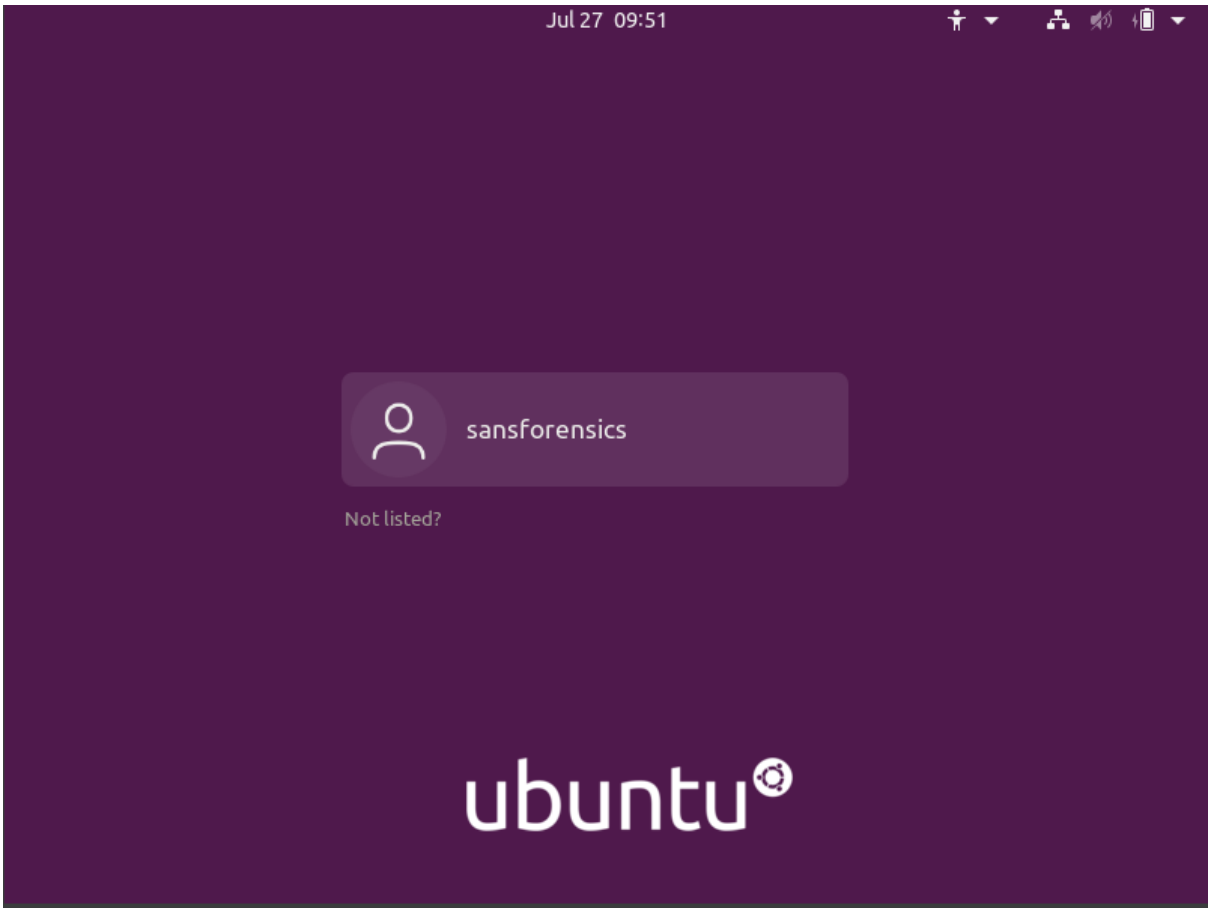
4) Double click on it, and it will redirect you to your VirtualBox or VM ware machine which you have in your system.
5) Configure the basic settings like:
   - Change its name.
   - Set OS type to Ubuntu(64bit).
   - Set RAM and CPU according to your computer's capability.
6) Click on "Finish".



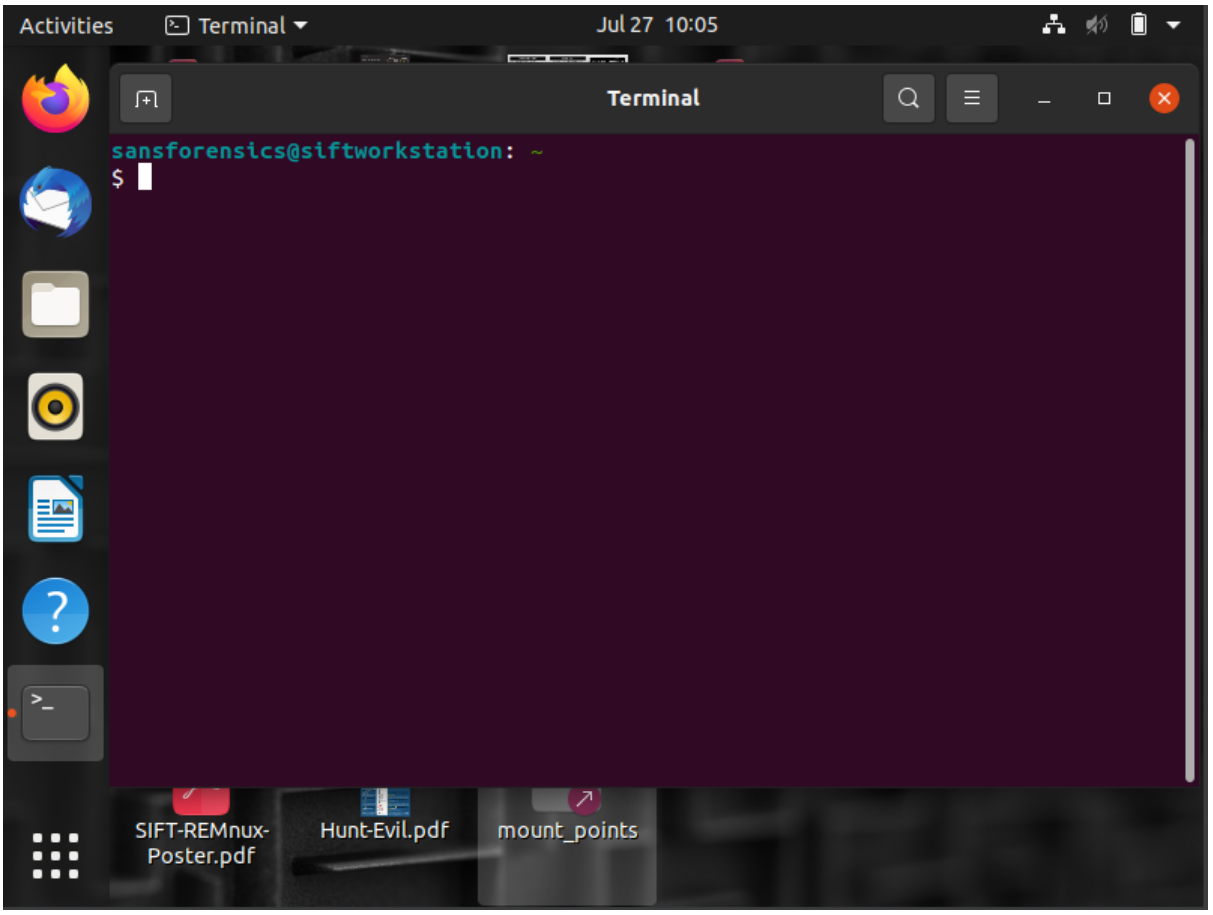
7) Now go to the settings and configure some other basic settings.
8) Go to Settings --> General --> Advanced --> Now set "Shared clipboard" and "Drag n' Drop" to "Bidirectional".
9) Display --> Video memory to max (128MB).
10) Network --> Attached to --> Set it to "Bridged Adapter" (For VirtualBox).

    Note: In case of VMWare - Attached to --> NAT (only).

11) Click on "Ok".
12) Start the machine.



13) The login page will Show up.
14) Login with the following credentials:
    - Login = sansforensics
    - Password = forensics



15) As shown in the figure a terminal window will open.

16) A pop-up window will appear asking to update the Ubuntu. Click on "Upgrade Now".

17) After upgrading it run the following commands:

- sudo su - To gain root access.
- sudo apt update && sudo apt upgrade - To update all your packages.
- Install the tools that you require, for example,
    - sudo apt install gparted - to install the GParted tool.

Tools

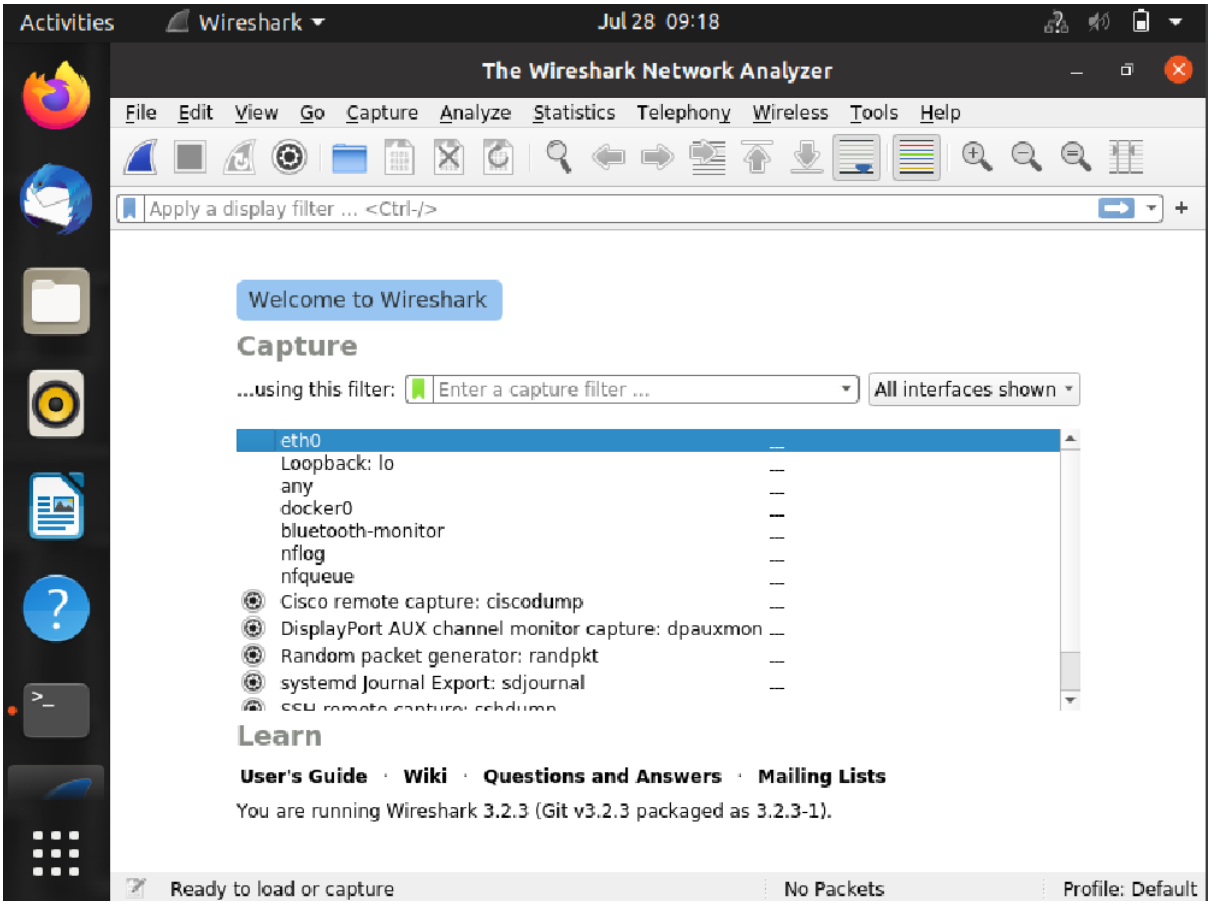
1) Autopsy: A graphical interface for The Sleuth Kit, a powerful open-source digital forensics tool. Autopsy enables investigators to perform in-depth analysis on disk images and aids in the identification of potential evidence.
2) The Sleuth Kit: A collection of command-line tools for digital forensics, including disk imaging, file system analysis, and file recovery. It's a robust and widely used tool in the DFIR community.
3) Wireshark: Although primarily known as a network protocol analyzer, Wireshark is also valuable for network forensics and analyzing packet-level data during an investigation.
4) Guymager: Guymager is an open-source forensic imaging tool used for creating bit-by-bit copies (forensic images) of digital media such as hard drives, USB drives, memory cards, and other storage devices.
5) Volatility: An open-source memory forensics framework used to analyze memory dumps and investigate the state of a system, identify running processes, and detect malicious activities.

1) **Wireshark**: In SANS, Wireshark is included with all the other tools. Whenever data or network packets are transferred between endpoints, wireshark assists in sniffing them or monitoring them.

a) Just enter into root mode and type "wireshark" to get the tool running.

```
sansforensics@siftworkstation: ~
$ sudo su
root@siftworkstation:/home/sansforensics# wireshark
```

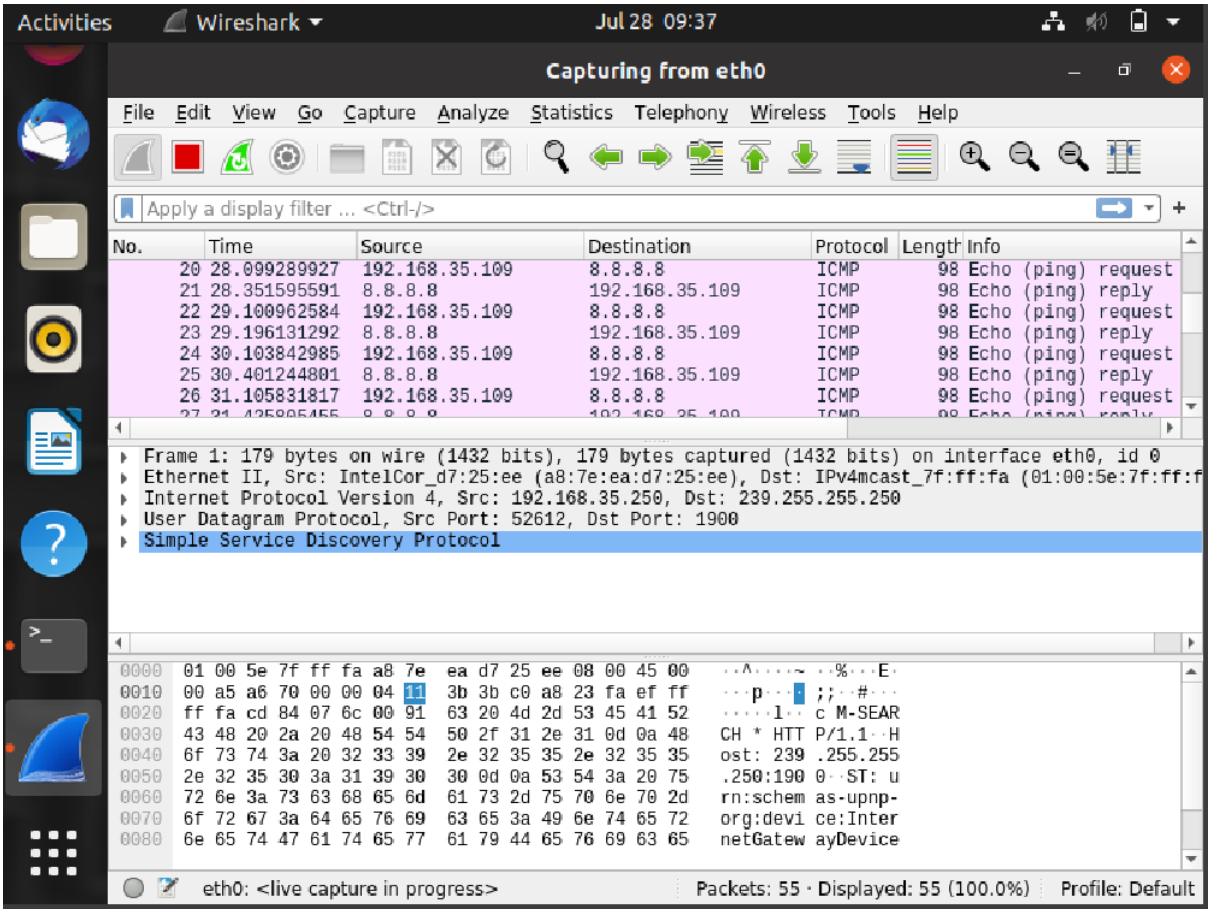
b) You would be able to see a welcome page as shown below. It shows all the interfaces that would be in a device.



c) If we go to the terminal and send packets like the one below.

```
root@siftworkstation:/home/sansforensics# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=248 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=252 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=95.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=297 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=320 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=93.6 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5031ms
```

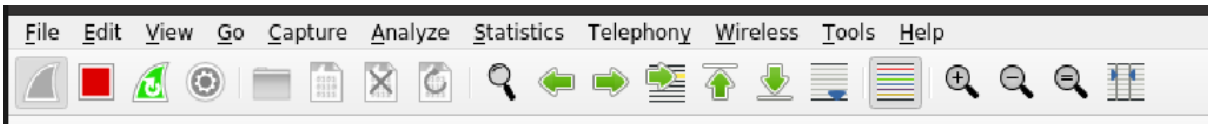
d) We would be able to see it in Wireshark.



e) You can perform various operations with Wireshark's toolbar, as shown below. The description of the option can be seen by hovering your mouse over it:

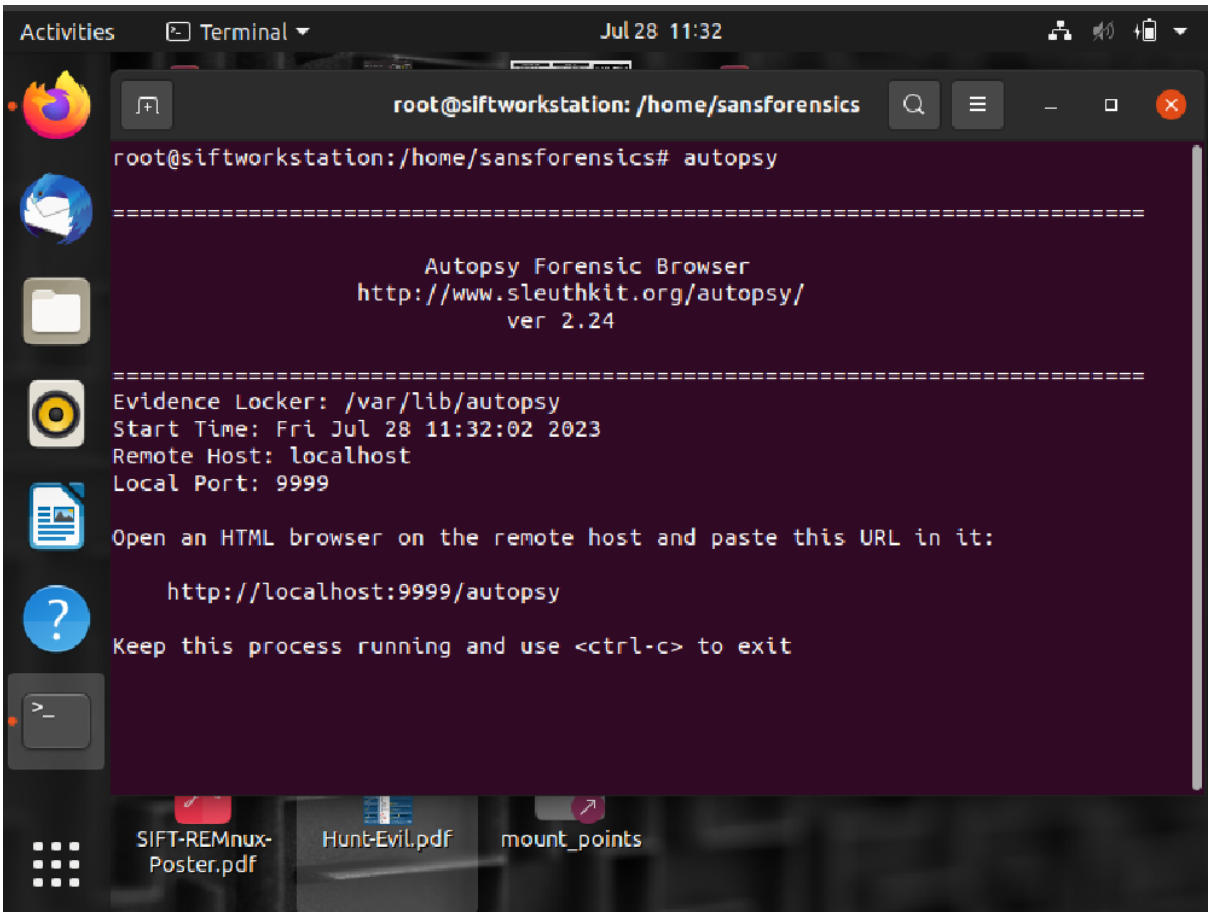
Some examples:

i) Blue shark fin - Start capturing packets.
ii) Red square - Stop capturing the packets.
iii) Green shark fin - Restart current capture.



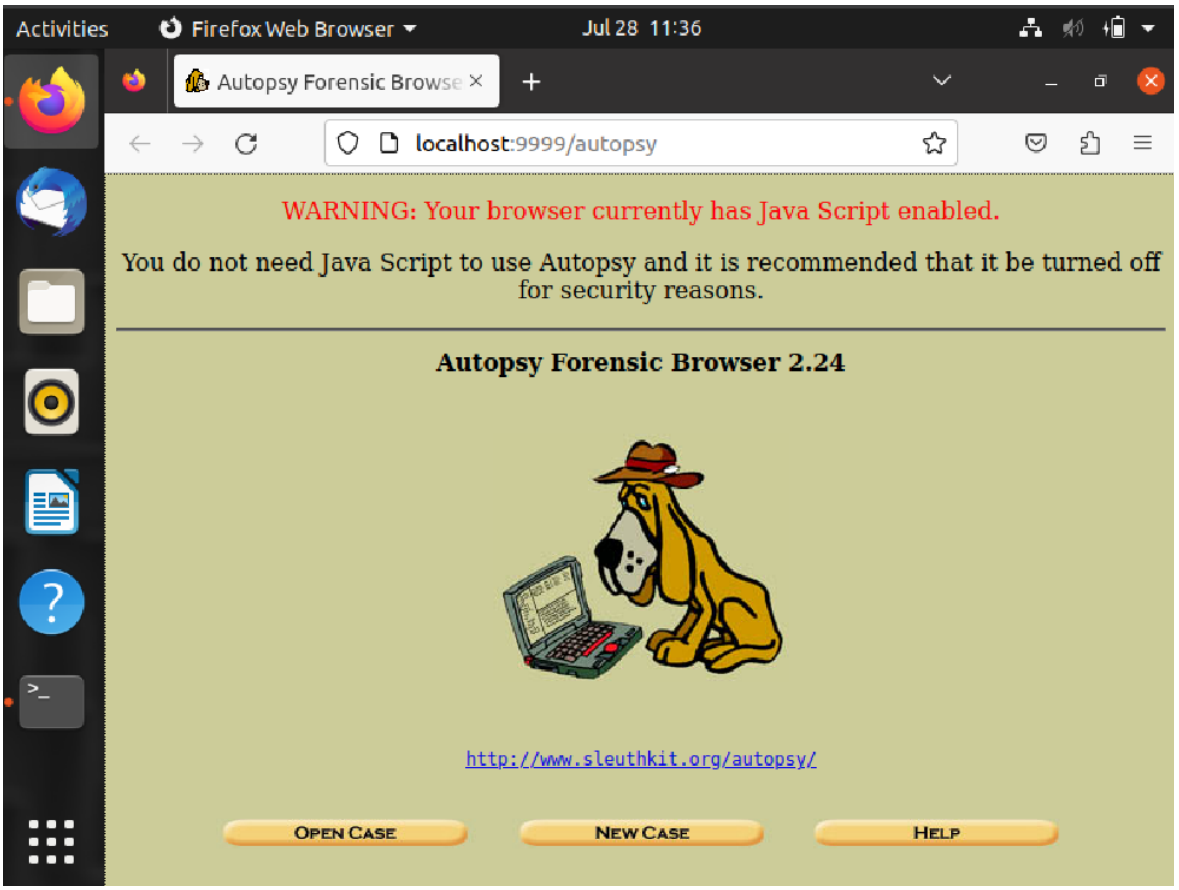
2) **Autopsy**: Autopsy is a feature-rich, open-source digital forensics platform that provides a graphical interface for conducting in-depth forensic analysis. It allows investigators to analyze disk images, perform keyword searches, examine file system artifacts, and visualize data relationships.

a) Type "autopsy" in your terminal to launch the tool.



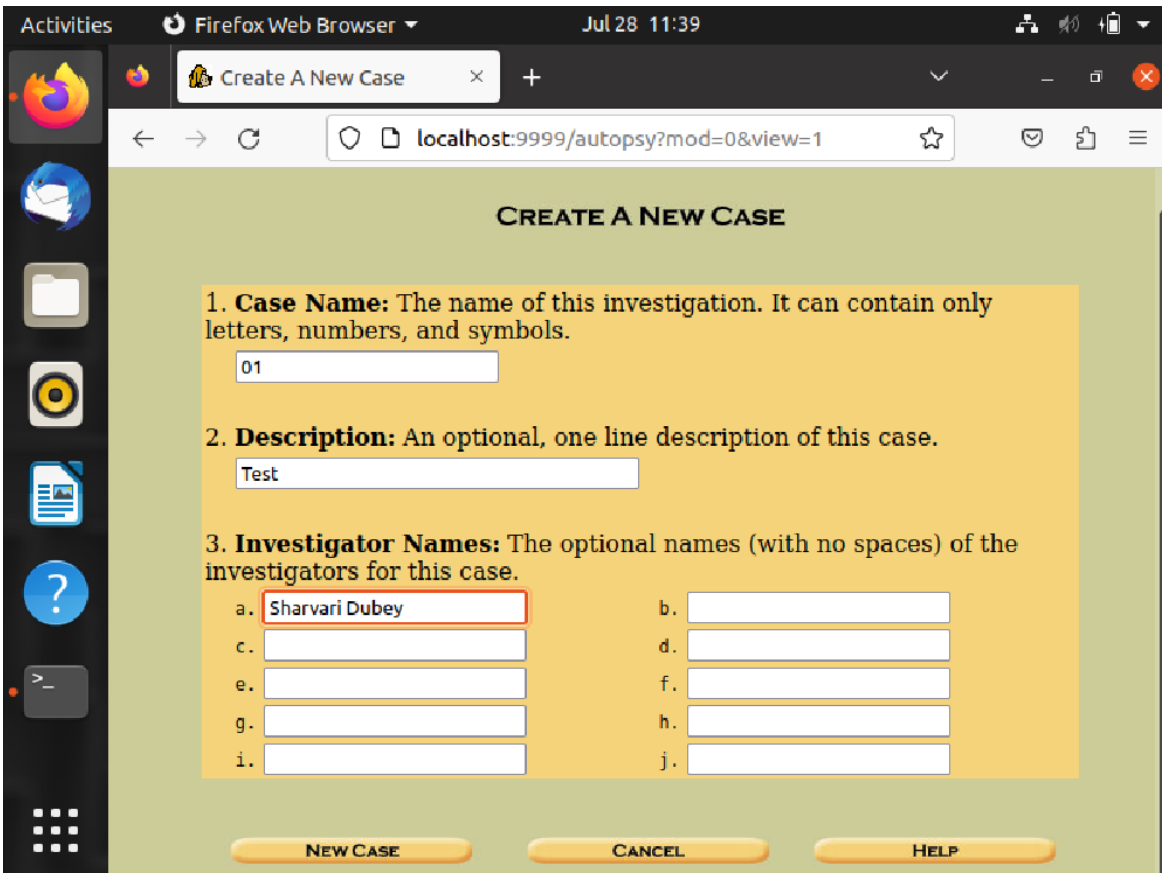
b) Open the link in any browser - http://localhost:999/autopsy

c) The following interface will show up:



d) If you have an existing case click on "Open Case" or else click on "New Case".

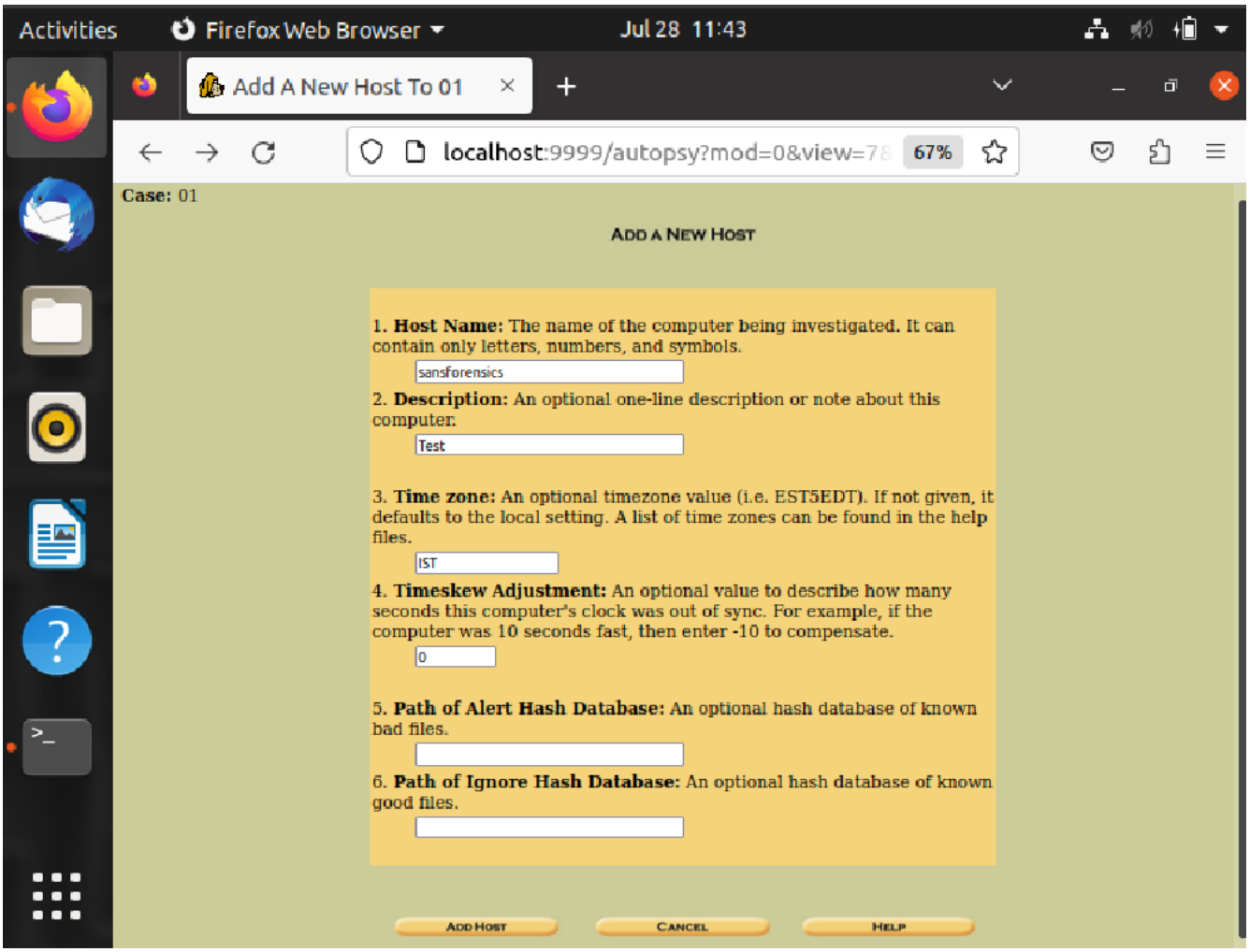
e) Fill in the basic details regarding the case in their respective columns.



f) Click on “New Case”.

g) Then click on “Add Host”.

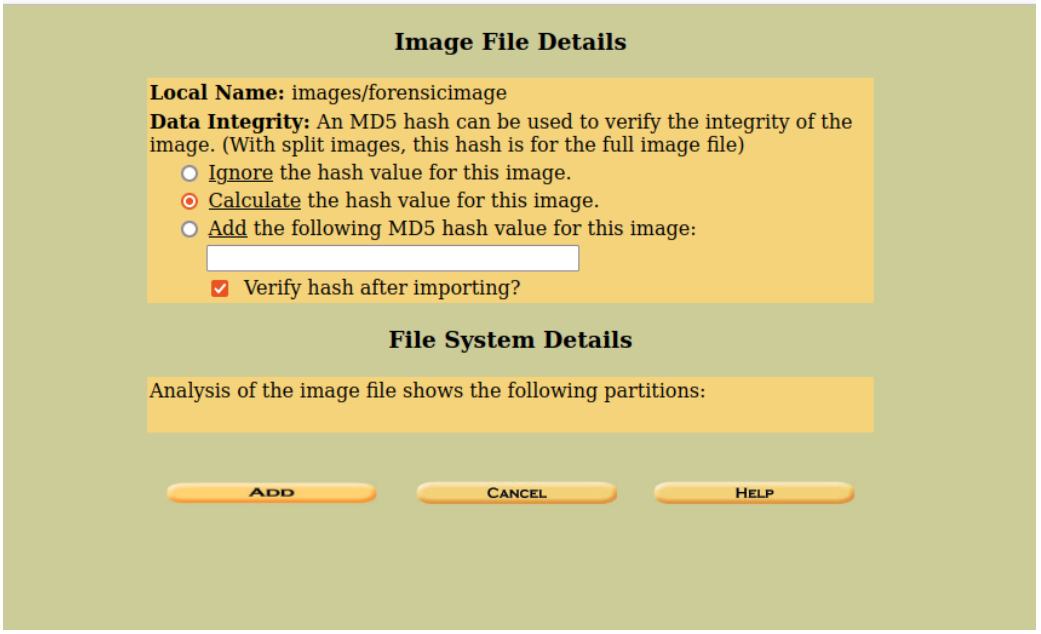
h) Fill in the details about the Host.



i) click on “Add Host”.

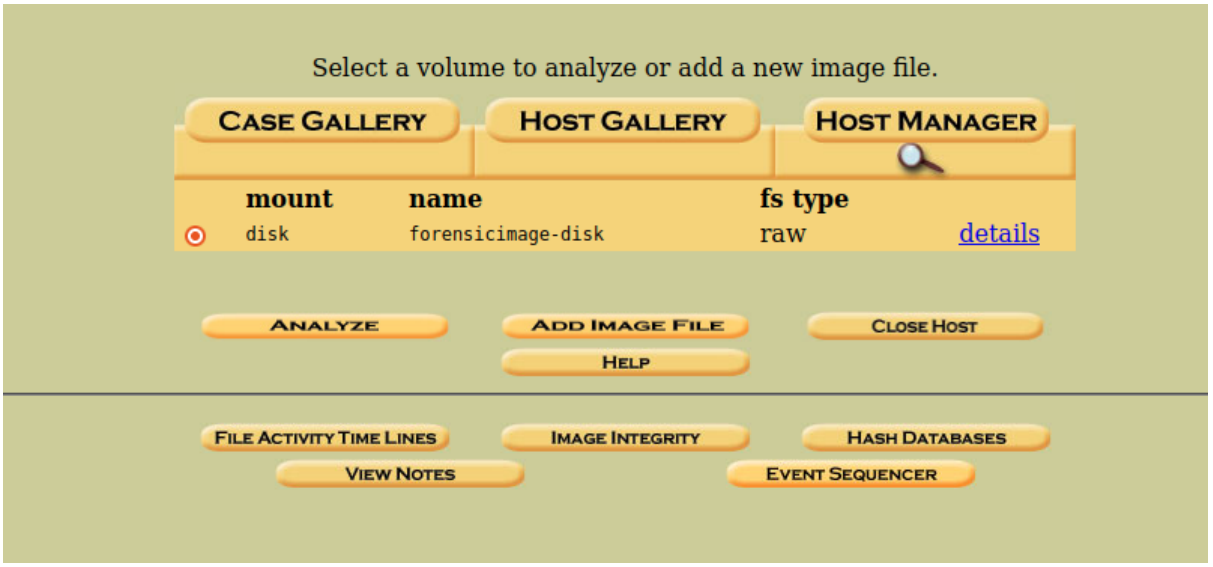
j) Add the path for the image, select its type & import method.

k) Add Image file details. Then Click on "Add".

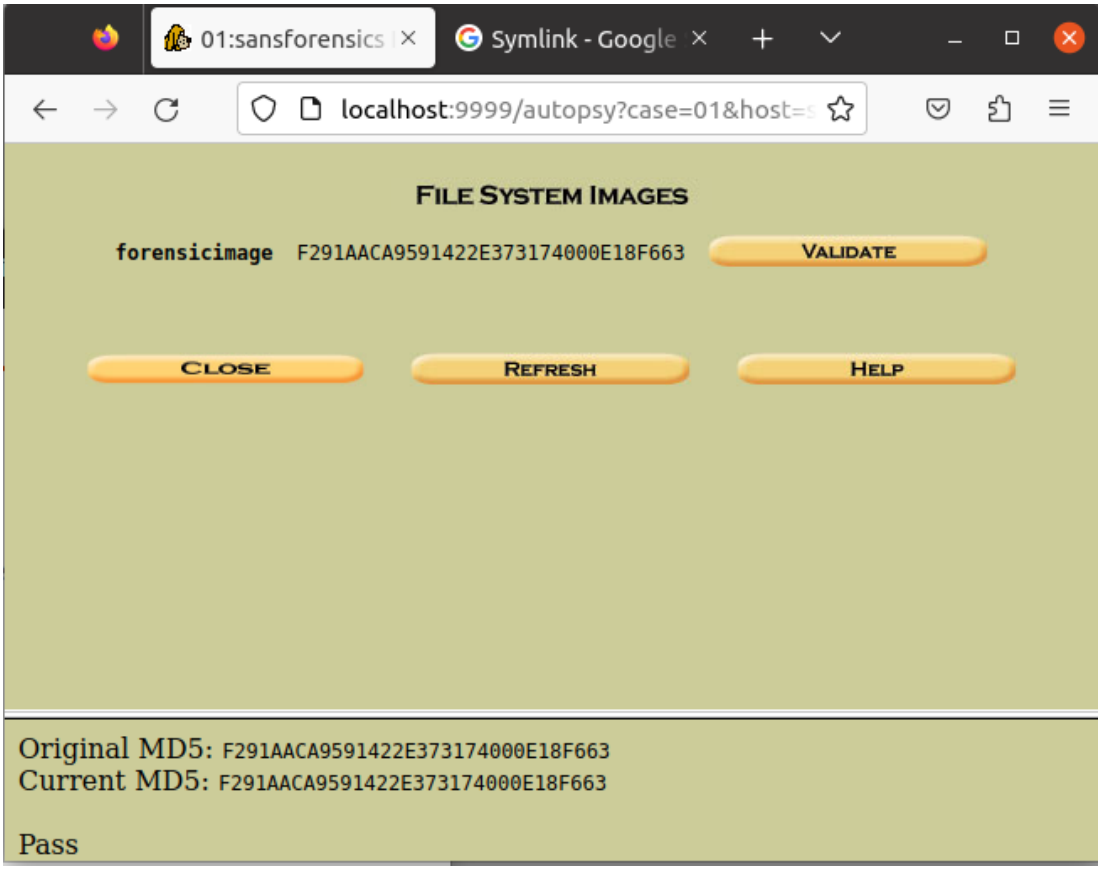


l) It will calculate and show the details of the hash, click on “OK”.

m) A window similar to below would be shown, select the operation that you need to perform.



n) For instance, we select “Image Integrity”. It will calculate and compare its hash value to the original one.



o) Similarly, you can use different options.

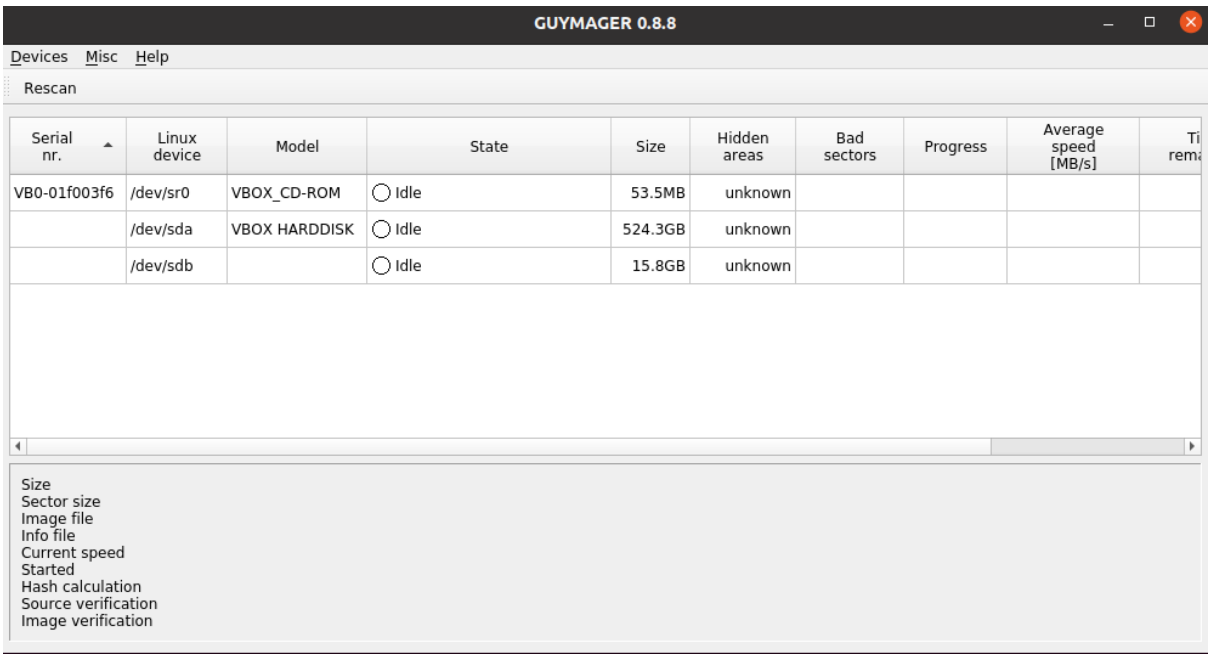
3) **Guymager:** Guymager is an open-source forensic imaging tool used for creating bit-by-bit copies (forensic images) of digital media such as hard drives, USB drives, memory cards, and other storage devices. It is commonly used in digital forensics and incident response investigations to acquire and preserve evidence from potential sources without altering the original data.

a) Install the Guymager tool with the following command:
"sudo apt install guymager"

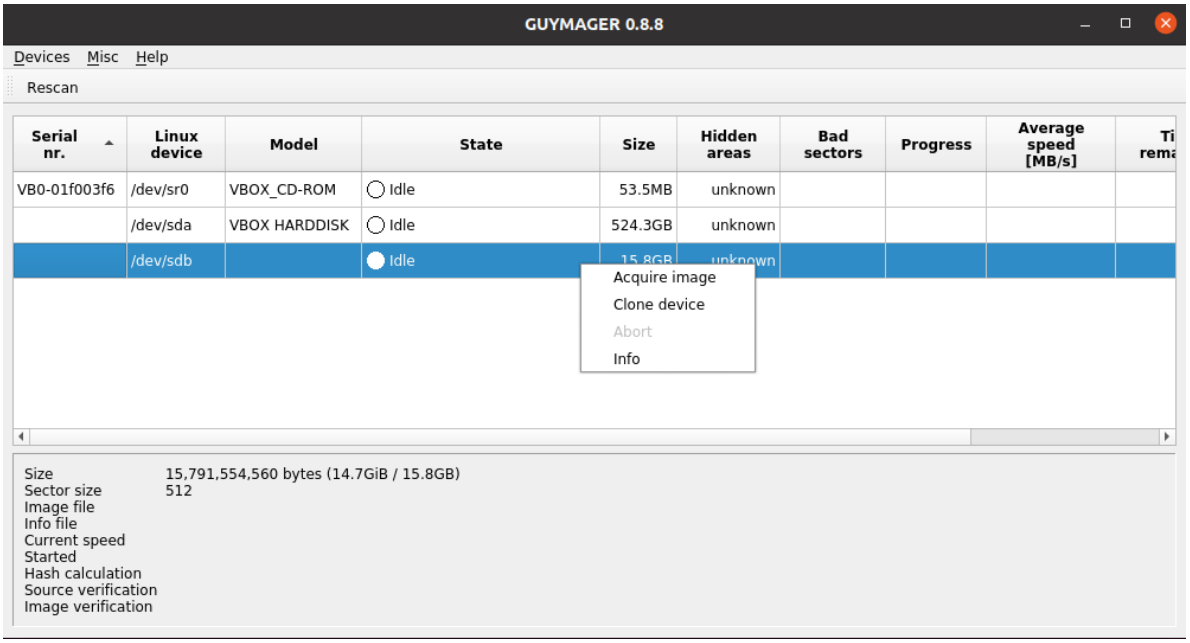
```
root@siftworkstation:/home/sansforensics# sudo apt install guymager
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  artifacts-data libbde-python3 libcreg libcreg-python3 libesedb-python3 libevt-python3 libevtx-python3 libfsapfs-python3 libfsext libfsext-python3 libfshfs libfshfs-python3 libfsntfs libfsntfs-pytho
  libfsxfs libfsxfs-python3 libfvde-python3 libfwnt libfwnt-python3 libfwsi libfwsi-python3 liblnk liblnk-python3 libluksde libluksde-python3 libmodi libmodi-python3 libmsiecf-python3 libolecf-python
  libphdi libphdi-python3 libqcow libqcow-python3 libregf-python3 libscca libscca-python3 libsigscan libsigscan-python3 libsmdev libsmdev-python3 libsmraw libsmraw-python3 libvhdi libvhdi-python3
  libvmdk libvmdk-python3 libvsgpt libvsgpt-python3 libvshadow-python3 libvslvm libvslvm-python3 plaso-data python3-artifacts python3-bencode python3-defusedxml python3-dfdatetime python3-dfwinreg
  python3-dtfabric python3-lz4 python3-opensearch python3-pbr python3-pefile python3-pyparsing python3-pytsk3 python3-pyxattr python3-yara
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  guymager
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 325 kB of archives.
After this operation, 1,084 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 guymager amd64 0.8.8-3 [325 kB]
Fetched 325 kB in 1s (233 kB/s)
Selecting previously unselected package guymager.
(Reading database ... 241953 files and directories currently installed.)
Preparing to unpack .../guymager_0.8.8-3_amd64.deb ...
Unpacking guymager (0.8.8-3) ...
Setting up guymager (0.8.8-3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
root@siftworkstation:/home/sansforensics# guymager

Using default log file name /var/log/guymager.logQStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

b) Type "guymager" on the terminal to launch it.

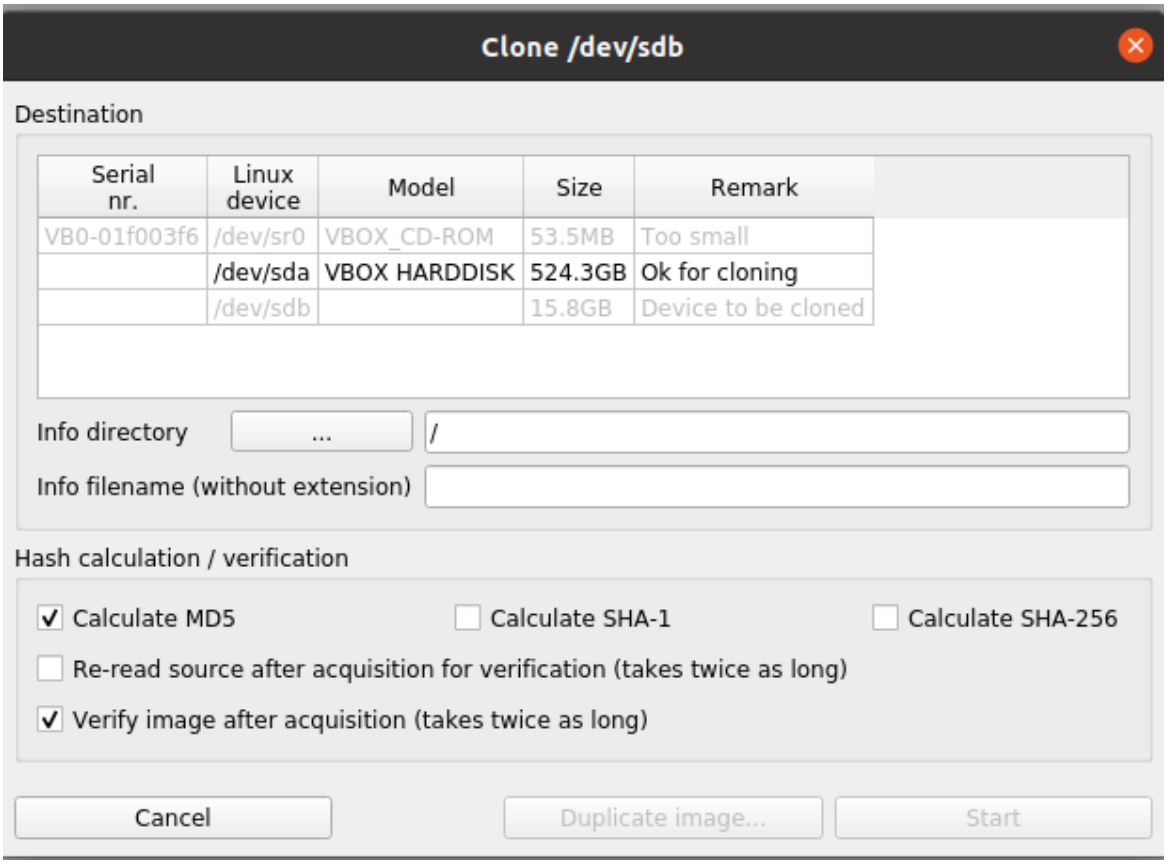
c) The following interface will be shown.



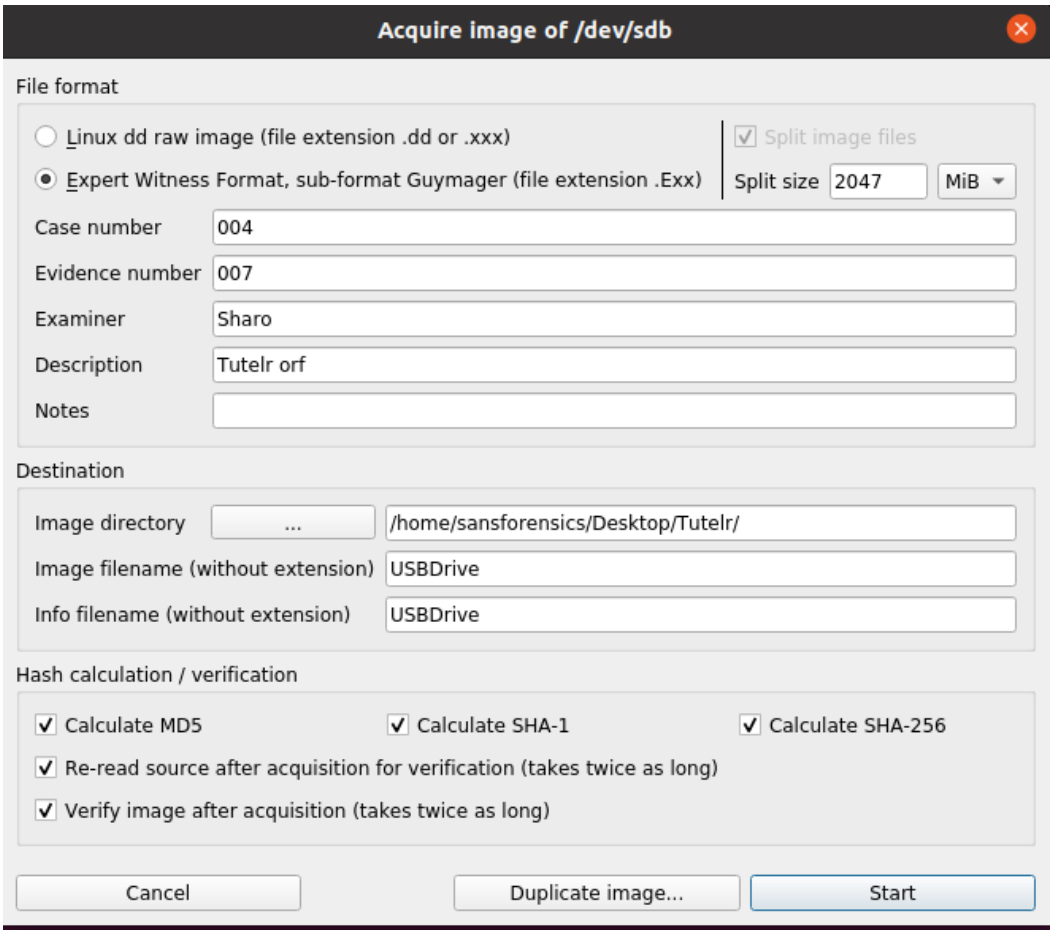
d) After right-clicking on a device we get different options such as:



e) After selecting Clone image we can perform various operations shown below:



f) Here we will acquire its image, after selecting the "Acquire image" option



g) Fill in the details accordingly, and check the boxes according to your need for hash calculation/verification.

h) Now click on "Start". It can take time according to the size of your drive.

i) You can see the status of the process.

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
VB0-01f003f6	/dev/sr0	VBOX_CD-ROM	Idle	53.5MB	unknown					
	/dev/sda	VBOX HARDDISK	Idle	524.3GB	unknown					
	/dev/sdb		Running	15.8GB	unknown	0	1%	4.68	01:46:06	r 0 h 0 c 0 w

Size	15,791,554,560 bytes (14.7GiB / 15.8GB)
Sector size	512
Image file	/home/sansforensics/Desktop/Tutelr/USBDrive.Exx
Info file	/home/sansforensics/Desktop/Tutelr/USBDrive.info
Current speed	4.69 MB/s
Started	30. July 08:29:14 (00:01:07)
Hash calculation	MD5, SHA-1 and SHA-256
Source verification	on
Image verification	on

j) Once it is done it will show the following:

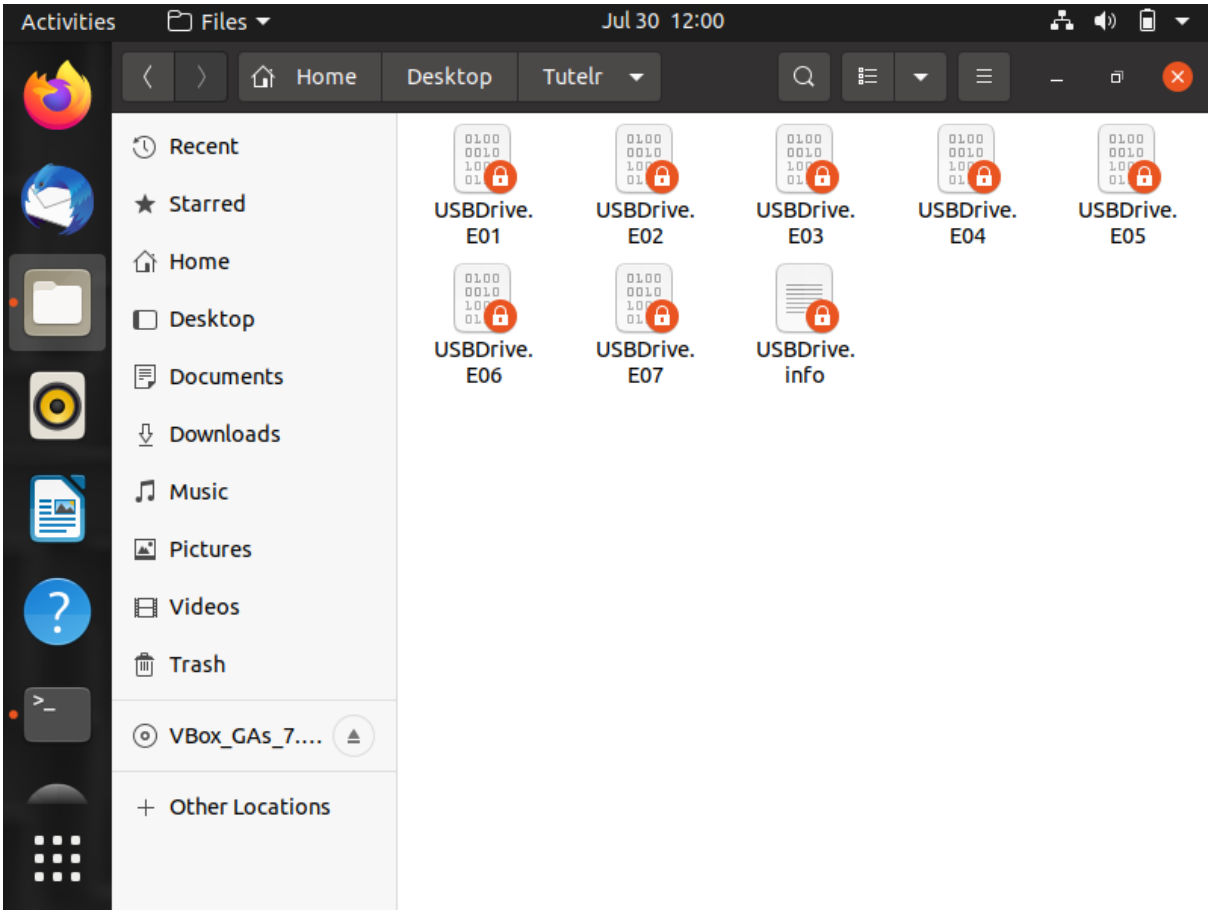
Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
VB0-01f003f6	/dev/sr0	VBOX_CD-ROM	Idle	53.5MB	unknown					
	/dev/sda	VBOX HARDDISK	Idle	524.3GB	unknown					
4C530000110315101170	/dev/sdb	SanDisk Cruzer_Blade	Finished - Verified & ok	15.8GB	unknown	0	100%	4.61		

Size 15,791,554,560 bytes (14.7GiB / 15.8GB)
Sector size 512
Image file /home/sansforensics/Desktop/Tutelr/USBDrive.Exx

k) You will be able to see 2 folders in the directory that you have selected to acquire your image.



l) In the .info folder you will find all the details regarding the acquired image

Open

USBDrive.info [Read-Only]
~/Desktop/Tutelr

```
GUYMAGER ACQUISITION INFO FILE
==============================

Guymager
========

Version              : 0.8.8-3
Compilation timestamp: 2019-02-20-15.50.35
Compiled with        : gcc 8.2.0
libewf version       : 20140807 (not used as Guymager is configured to use its own EWF module)
libguytools version  : 2.0.5
Host name            : siftworkstation
Domain name          : (none)
System               : Linux siftworkstation 5.4.0-155-generic #172-Ubuntu SMP Fri Jul 7 16:10:02 UTC 2023 x86_64


Device information
==================
Command executed: bash -c "search="`basename /dev/sdb`: H..t P.......d A..a de.....d" && dmesg | grep -A3 "$search" || echo "No kernel HPA messages for /dev/sdb""
Information returned:
-----------------------------------------------------------------------------------------------
   No kernel HPA messages for /dev/sdb

Command executed: bash -c "smartctl -s on /dev/sdb ; smartctl -a /dev/sdb"
Information returned:
-----------------------------------------------------------------------------------------------
   smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.4.0-155-generic] (local build)
   Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

   /dev/sdb: Unknown USB bridge [0x0781:0x5567 (0x100)]
   Please specify device type with the -d option.

   Use smartctl -h to get a usage summary

   smartctl 7.1 2019-12-30 r5022 [x86_64-linux-5.4.0-155-generic] (local build)
   Copyright (C) 2002-19, Bruce Allen, Christian Franke, www.smartmontools.org

   /dev/sdb: Unknown USB bridge [0x0781:0x5567 (0x100)]
   Please specify device type with the -d option.

   Use smartctl -h to get a usage summary

Command executed: bash -c "hdparm -I /dev/sdb"
Information returned:
-----------------------------------------------------------------------------------------------
   SG_IO: bad/missing sense data, sb[]:  70 00 05 00 00 00 00 14 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

4) **The Sleuth Kit:** The Sleuth Kit is a collection of command-line tools designed for digital investigation purposes. It allows examiners to perform file system analysis, conduct timeline analysis, recover deleted files, and extract metadata from various file types. TSK is a fundamental tool for many forensic investigations.

a) To install the Sleuth kit type the following command:
"sudo apt install sleuthkit"

```
root@siftworkstation:/home/sansforensics# sudo apt install sleuthkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libguytools2 smartmontools
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sleuthkit
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,065 kB of archives.
After this operation, 16.5 MB of additional disk space will be used.
Get:1 http://ppa.launchpad.net/sift/stable/ubuntu focal/main amd64 sleuthkit am
d64 4.7.0-2ppa3~focal [1,065 kB]
Fetched 1,065 kB in 3s (391 kB/s)
Selecting previously unselected package sleuthkit.
(Reading database ... 241315 files and directories currently installed.)
Preparing to unpack .../sleuthkit_4.7.0-2ppa3~focal_amd64.deb ...
```

b) You can also check its version through the command:
"mmls -V"

```
root@siftworkstation: /home/sansforensics
root@siftworkstation:/home/sansforensics# mmls -V
The Sleuth Kit ver 4.7.0
root@siftworkstation:/home/sansforensics#
```

c) By using the disk image of the disk, we are able to analyze the disk using Sleuth Kit.

d) There is a command to get to know which type of image is.

```
root@siftworkstation: /home/sansforensics/forensics
root@siftworkstation:/home/sansforensics/forensics# ls
diskimg  forensicimage
root@siftworkstation:/home/sansforensics/forensics# img_stat diskimg
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 2046820352
Sector size:    512
root@siftworkstation:/home/sansforensics/forensics#
```

e) Sleuth Kit supports a number of image types which can be listed with the following command.

```
root@siftworkstation:/home/sansforensics/forensics# fls -i list
Supported image format types:
        raw (Single or split raw file (dd))
        aff (Advanced Forensic Format)
        afd (AFF Multiple File)
        afm (AFF with external metadata)
        afflib (All AFFLIB image formats (including beta ones))
        ewf (Expert Witness Format (EnCase))
        vmdk (Virtual Machine Disk (VmWare, Virtual Box))
        vhd (Virtual Hard Drive (Microsoft))
root@siftworkstation:/home/sansforensics/forensics#
```

f) We can do Partition Identification, File System Identification, Offset Calculation, Disk Image Analysis Planning.

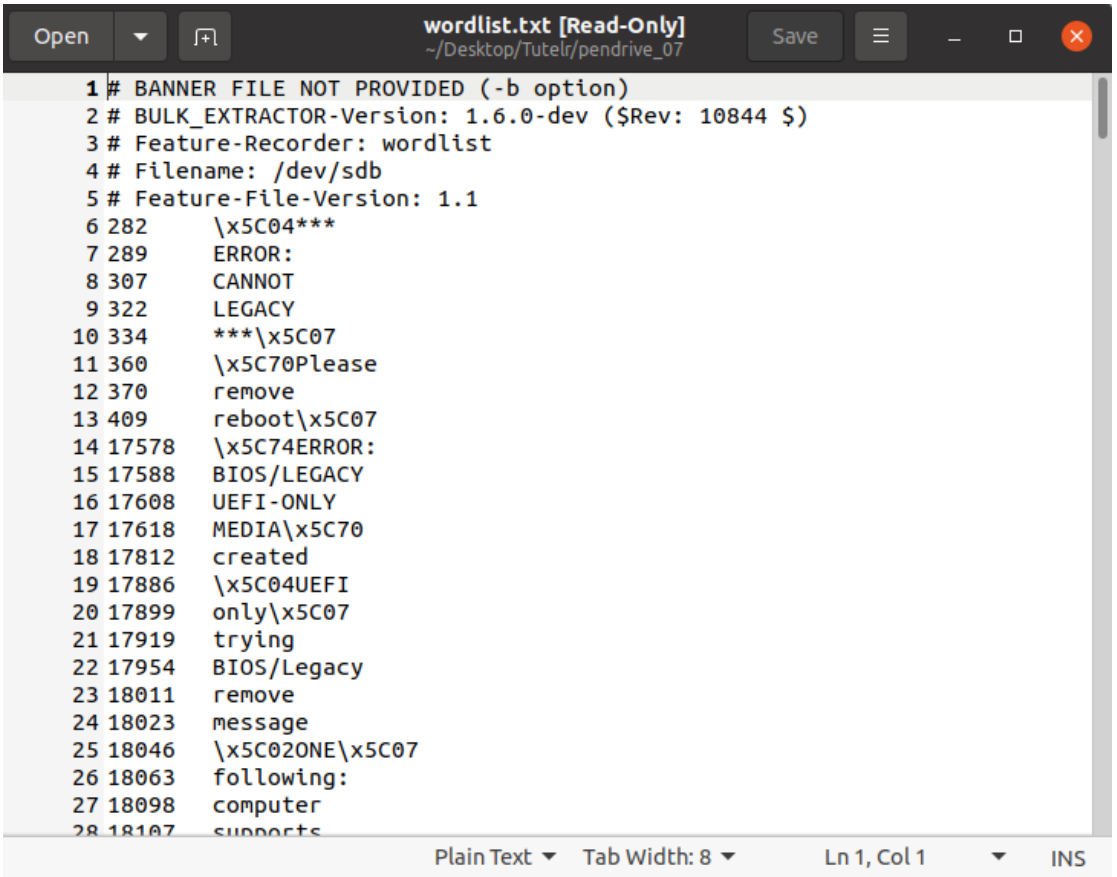
```
root@siftworkstation:/home/sansforensics/Desktop/Tutelr# mmls USBDrive.E07
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Safety Table
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  Meta      0000000001   0000000001   0000000001   GPT Header
003:  Meta      0000000002   0000000033   0000000032   Partition Table
004:  000       0000002048   0030842846   0030840799   Main Data Partition
005:  -------   0030842847   0030842879   0000000033   Unallocated
root@siftworkstation:/home/sansforensics/Desktop/Tutelr#
```

5) **Bulk Extractor:** It is a powerful digital forensics tool designed to extract valuable information from large volumes of data quickly and efficiently. It is commonly used by forensic investigators and cybersecurity professionals to scan various types of digital media, such as disk images, memory dumps, and network packet captures, to uncover evidence and artifacts related to potential security incidents or investigations.
    a) For this tutorial we are going to use the bulk extractor to scan our disk image.
    b) Now we scan our disk image. Scanning of the image may take time according to the size, contents of the image, and mainly on the type of scans you have enabled or disabled.

```
root@siftworkstation:/home/sansforensics/Desktop/Tutelr# ls
USBDrive.E01  USBDrive.E02  USBDrive.E03  USBDrive.E04  USBDrive.E05  USBDrive.E06  USBDrive.E07  USBDrive.info
root@siftworkstation:/home/sansforensics/Desktop/Tutelr# bulk_extractor -o case-07 USBDrive.E07
bulk_extractor version: 1.6.0-dev
Hostname: siftworkstation
Input file: USBDrive.E07
Output directory: case-07
Disk Size: 1956955325
Threads: 2
Attempt to open USBDrive.E07
17:28:20 Offset 67MB (3.43%) Done in  0:03:11 at 17:31:31
17:28:27 Offset 150MB (7.72%) Done in  0:02:45 at 17:31:12
17:28:37 Offset 234MB (12.00%) Done in  0:02:54 at 17:31:31
17:28:44 Offset 318MB (16.29%) Done in  0:02:39 at 17:31:23
17:28:53 Offset 402MB (20.58%) Done in  0:02:36 at 17:31:29
17:29:00 Offset 486MB (24.86%) Done in  0:02:21 at 17:31:21
17:29:09 Offset 570MB (29.15%) Done in  0:02:17 at 17:31:26
17:29:16 Offset 654MB (33.44%) Done in  0:02:06 at 17:31:22
17:29:25 Offset 738MB (37.72%) Done in  0:02:00 at 17:31:25
17:29:32 Offset 822MB (42.01%) Done in  0:01:48 at 17:31:20
17:29:42 Offset 905MB (46.29%) Done in  0:01:43 at 17:31:25
17:29:48 Offset 989MB (50.58%) Done in  0:01:33 at 17:31:21
17:29:57 Offset 1073MB (54.87%) Done in  0:01:25 at 17:31:22
17:30:03 Offset 1157MB (59.15%) Done in  0:01:16 at 17:31:19
17:30:13 Offset 1241MB (63.44%) Done in  0:01:09 at 17:31:22
17:30:19 Offset 1325MB (67.73%) Done in  0:01:00 at 17:31:19
17:30:28 Offset 1409MB (72.01%) Done in  0:00:52 at 17:31:20
17:30:35 Offset 1493MB (76.30%) Done in  0:00:44 at 17:31:19
17:30:44 Offset 1577MB (80.59%) Done in  0:00:36 at 17:31:20
17:30:50 Offset 1660MB (84.87%) Done in  0:00:28 at 17:31:18
17:30:59 Offset 1744MB (89.16%) Done in  0:00:20 at 17:31:19
17:31:06 Offset 1828MB (93.45%) Done in  0:00:12 at 17:31:18
17:31:14 Offset 1912MB (97.73%) Done in  0:00:04 at 17:31:18
All data are read; waiting for threads to finish...
Time elapsed waiting for 2 threads to finish:
     (timeout in 60 min.)
All Threads Finished!
Producer time spent waiting: 172.306 sec.
Average consumer time spent waiting: 0.247388 sec.
*****************************************
** bulk_extractor is probably CPU bound. **
**    Run on a computer with more cores  **
**      to get better performance.       **
*****************************************
MD5 of Disk Image: a93cf8d986425c42294c291cddab9d5b
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 185.974 sec.
Total MB processed: 1956
Overall performance: 10.5227 MBytes/sec (5.26136 MBytes/sec/thread)
Total email features found: 0
root@siftworkstation:/home/sansforensics/Desktop/Tutelr#
```

c) We can also perform scanning operations on a USB drive.

d) Using the pendrive connected to the computer, we will attempt to create a wordlist. It has generated the following wordlist with the help of tool.




```
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
# Feature-Recorder: wordlist
# Filename: /dev/sdb
# Feature-File-Version: 1.1
282     \x5C04***
289     ERROR:
307     CANNOT
322     LEGACY
334     ***\x5C07
360     \x5C70Please
370     remove
409     reboot\x5C07
17578   \x5C74ERROR:
17588   BIOS/LEGACY
17608   UEFI-ONLY
17618   MEDIA\x5C70
17812   created
17886   \x5C04UEFI
17899   only\x5C07
17919   trying
17954   BIOS/Legacy
18011   remove
18023   message
18046   \x5C02ONE\x5C07
18063   following:
18098   computer
18107   supports
```

e) You can see the types of scans and how to enable or disable them with the command:

"bulk_extractor -h"

```
root@siftworkstation:/home/sansforensics/Desktop/Tutelr# bulk_extractor -h
bulk_extractor version 1.6.0-dev
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
   -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 status at all
   -s frac[:passes] - Set random sampling parameters

Tuning parameters:
   -C NN         - specifies the size of the context window (default 16)
   -S fr:<name>:window=NN   specifies context window for recorder to NN
   -S fr:<name>:window_before=NN  specifies context window before to NN for recorder
   -S fr:<name>:window_after=NN   specifies context window after to NN for recorder
   -G NN         - specify the page size (default 16777216)
   -g NN         - specify margin (default 4194304)
   -j NN         - Number of analysis threads to run (default 2)
   -M nn         - sets max recursion depth (default 7)
   -m <max>      - maximum number of minutes to wait after all data read
                    default is 60

Path Processing Mode:
   -p <path>/f   - print the value of <path> with a given format.
                    formats: r = raw; h = hex.
                    Specify -p - for interactive mode.
                    Specify -p -http for HTTP mode.

Parallelizing:
   -Y <o1>       - Start processing at o1 (o1 may be 1, 1K, 1M or 1G)
   -Y <o1>-<o2> - Process o1-o2
   -A <off>      - Add <off> to all reported feature offsets
```

f) You can all use its GUI interface but for that, you need to download its GitHub repo and configure it accordingly.

Case Study - Social Engineering and Phishing Campaign

Scenario:

A medium-sized company falls victim to a sophisticated phishing campaign. Attackers send convincing emails to employees, pretending to be from the company's IT department, asking them to click on a link and log in to verify their credentials due to a supposed security upgrade. Several employees unknowingly provide their login credentials on a fraudulent website, allowing attackers to gain unauthorized access to the company's internal network.

Investigation and Analysis:

- ➔ The incident response team first identifies the phishing email and investigates the email headers to determine the source and the path of the attack.
- ➔ They analyze the malicious website's code and hosting information to understand the attack infrastructure and possible attribution of the threat actors.
- ➔ The team checks the company's network logs to determine the extent of the intrusion and identify any lateral movement by the attackers.
- ➔ Memory analysis using tools like Volatility helps uncover any evidence of running malicious processes or the presence of keyloggers.
- ➔ File carving may be employed to identify any malware artifacts or attachments that might have been downloaded by employees.

Outcome:

The incident response team learns the full scope of the phishing campaign, identifies the affected accounts, and takes immediate measures to contain the attack. They educate employees about phishing threats and implement multi-factor authentication to enhance security.

Assessment Answers

1. What is the SIFT Workstation?

a) A digital forensic toolkit

b) A cloud-based data storage platform

c) A malware analysis tool

d) A social media monitoring tool

2. What is the primary use of the SIFT Workstation?

a) Data recovery

b) Network monitoring

c) Incident response

d) Web application testing

3. Which operating system is the SIFT Workstation based on?

a) Windows

b) MacOS

c) Linux

d) Android

4. Which tool is included in the SIFT Workstation for file carving?

a) FTK Imager

b) Wireshark

c) Autopsy

d) Scalpel

5. Which file system can the SIFT Workstation analyze?

a) NTFS

b) FAT32

c) EXT4

d) All of the above

6. What is the purpose of the SIFT Workstation's log2timeline tool?

a) To analyze network traffic

b) To recover deleted files

c) To create a timeline of system events

d) To analyze web traffic

7. Which tool in the SIFT Workstation is used for memory analysis?

a) Volatility

b) Autopsy

c) Wireshark

d) FTK Imager

8. Which forensic tool in the SIFT Workstation is used for database analysis?

a) SQLite

b) MySQL

c) Oracle

d) SQL Server

9. What is the function of the SIFT Workstation's bulk_extractor tool?

a) To analyze email headers

b) To recover deleted files

c) To extract metadata from files

d) To analyze network traffic

10. Which type of investigation is the SIFT Workstation commonly used for?

a) Cybersecurity incident response

b) Physical security assessment

c) Fraud investigation

d) Employee misconduct investigation