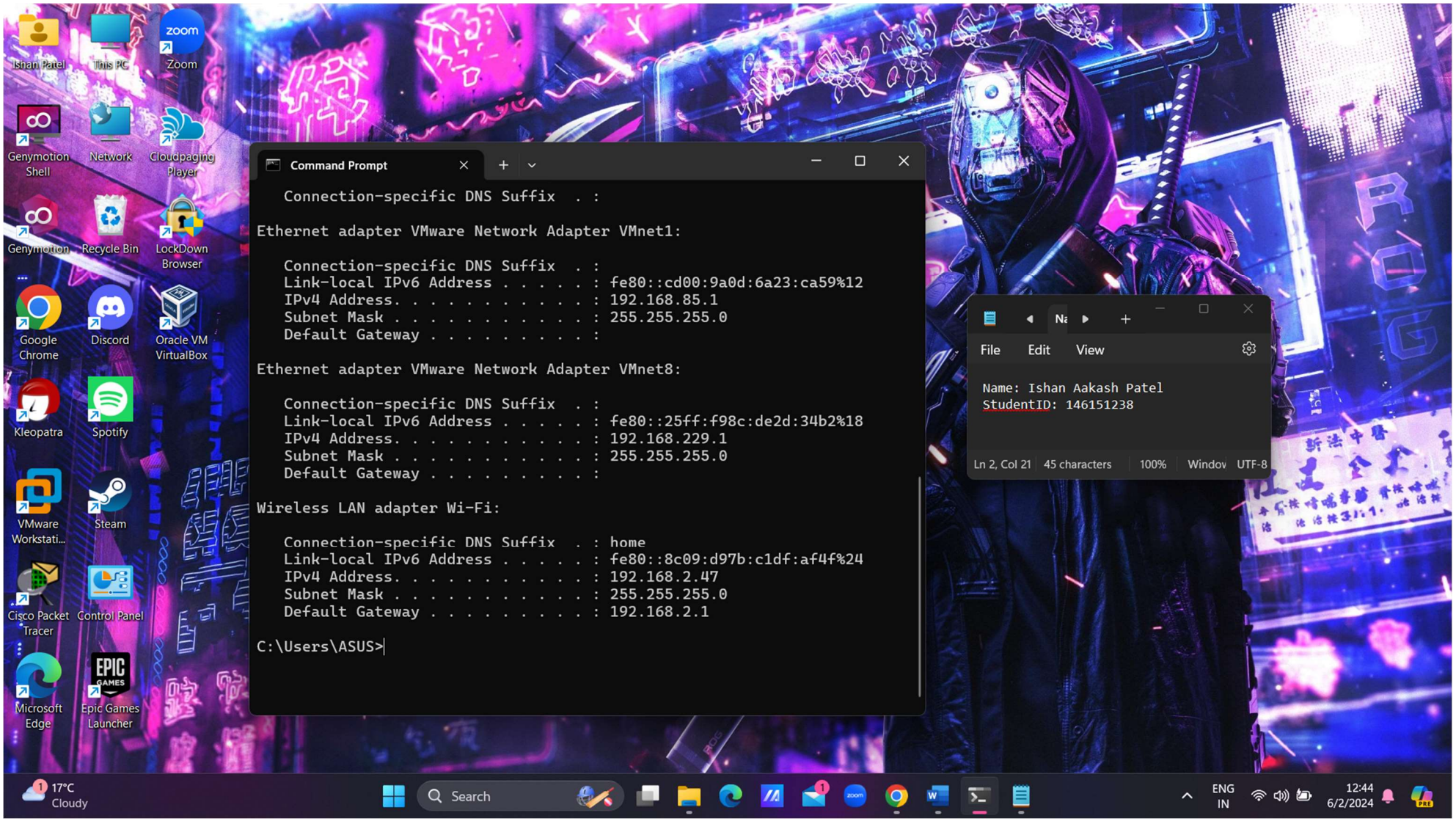
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Ishan Aakash Patel	146151238	As Posted	6%

Name	Lab2: SIFT Workstation

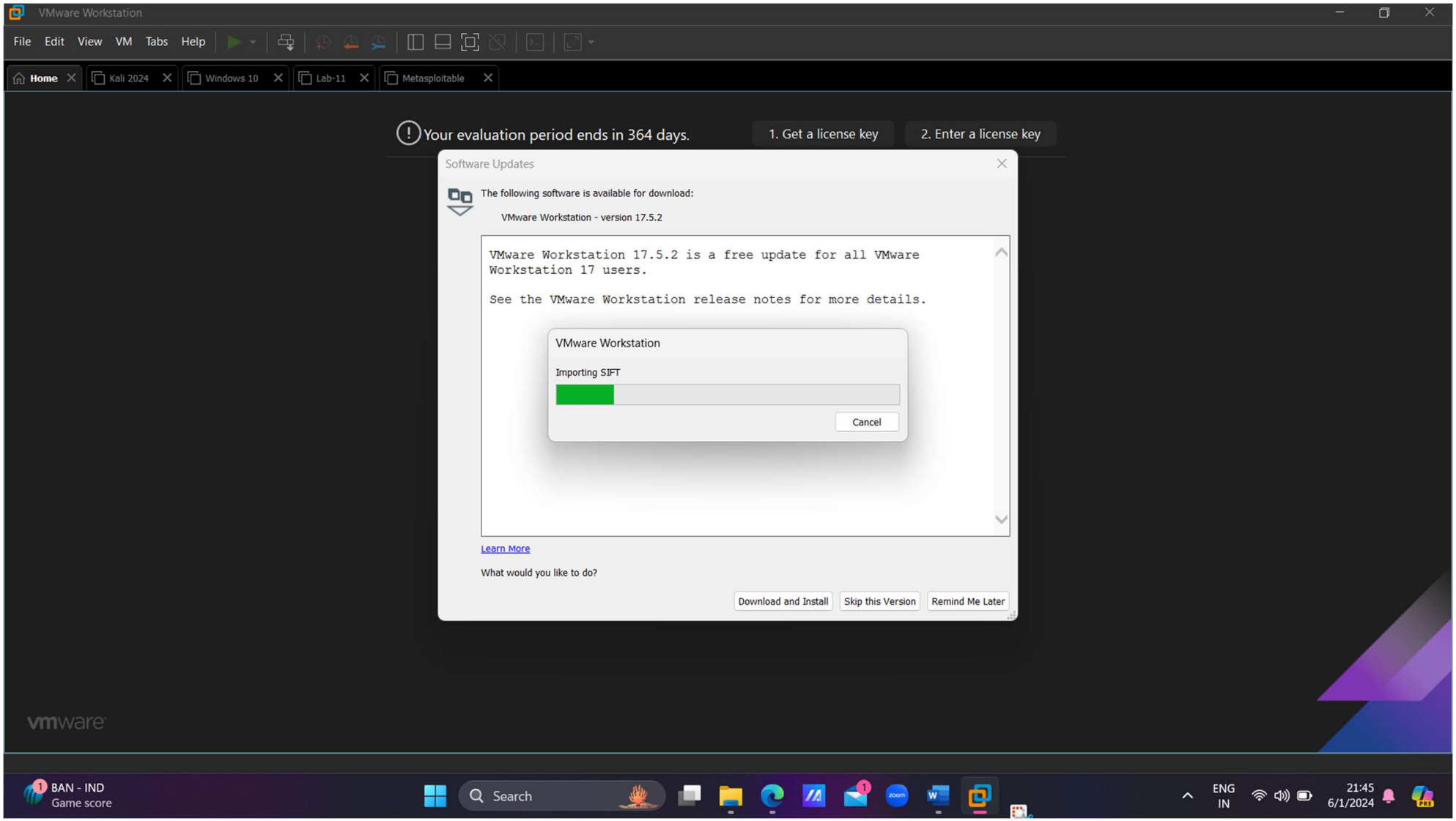
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above.
	• Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
	• Show your genuine signs of your work is done on your machine. This includes:
	  ○ Screenshots that show your desktop background with Date/Time
	  ○ Show a pop-up bx that shows "your name + IP".
	  ○ Show your logged account when applicable.
	  ○ Optional: Your photo.
	• Submit your report name: CYT215-Lab2-Student Name & ID

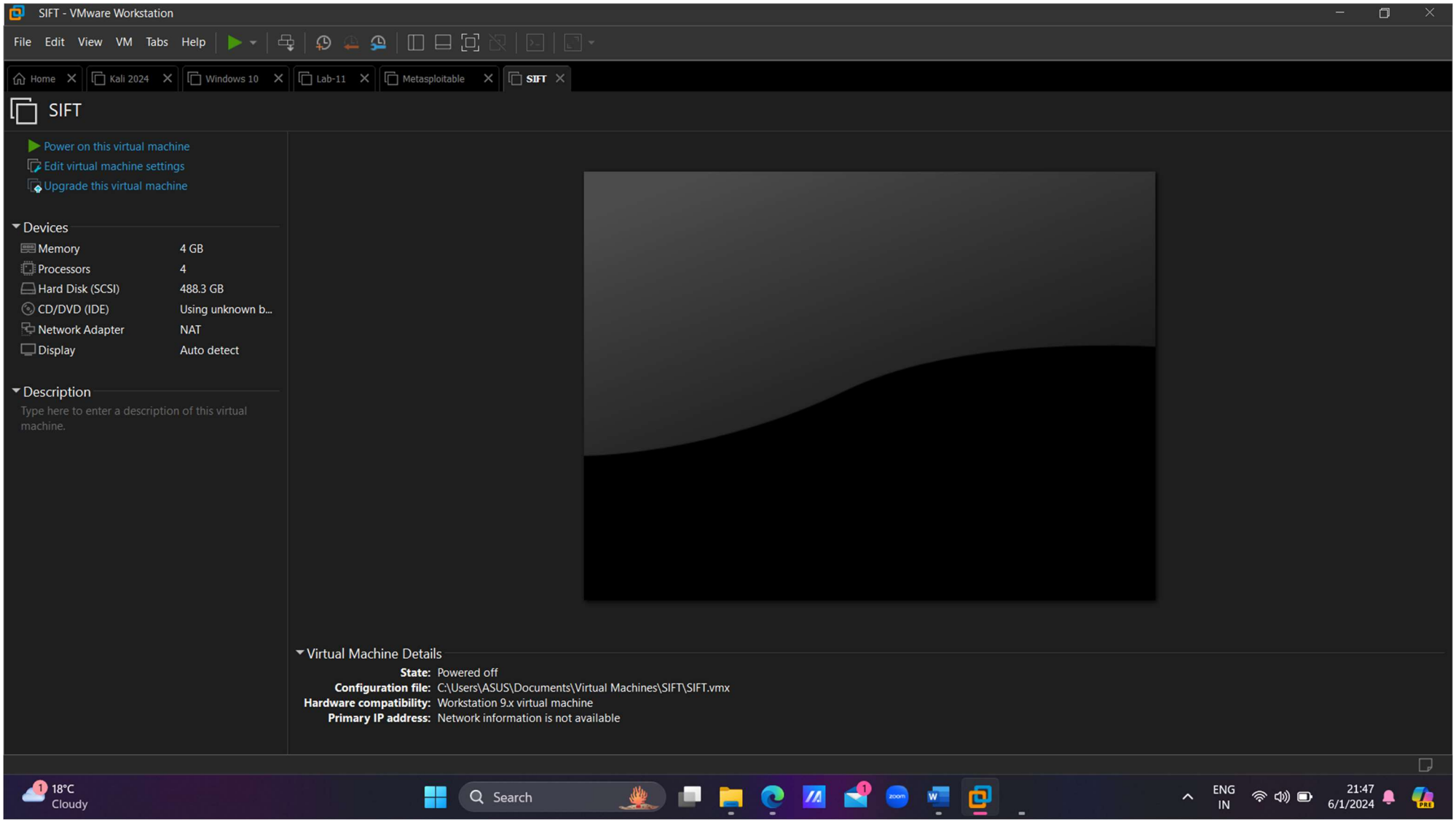
Students Work required for this activity	• You will setup your workspace inside the SIFT virtual machine & familiarize yourself with some simple Linux commands.
	• You will need to get/install SIFT Workstation https://digital-forensics.sans.org/community/downloads
	• Resources to help:
	  1. How To Use SIFT Workstation https://robots.net/tech/how-to-use-sift-workstation/
	  2. How To Install SIFT Workstation Getting Started https://www.youtube.com/watch?v=ZtRtLGDWIz0
	  3. Setting Up SANS Windows SIFT Workstation https://www.youtube.com/watch?v=PYjUbTwuH4I&ab_channel=OvieCarroll
	  4. How to Install SIFT Workstation on VirtualBox https://www.youtube.com/watch?v=GscgY0eDZyk&ab_channel=Pham
	• Keep SIFT Workstation installation on your machines for future analysis:
	  ○ File system.
	  ○ Memory.
	  ○ Network Traffic.
	  ○ Malware.
	  ○ Network.
	• Practice few tools & utilities (upon your wish) to test your workspace.
	• Show screenshots of all your installation steps. Show screenshots of the tools & utilities you used in your workspace.
	• Briefly write your experience and answer the following.:
	  ○ Any challenges?
	  ○ How useful & easy to use?

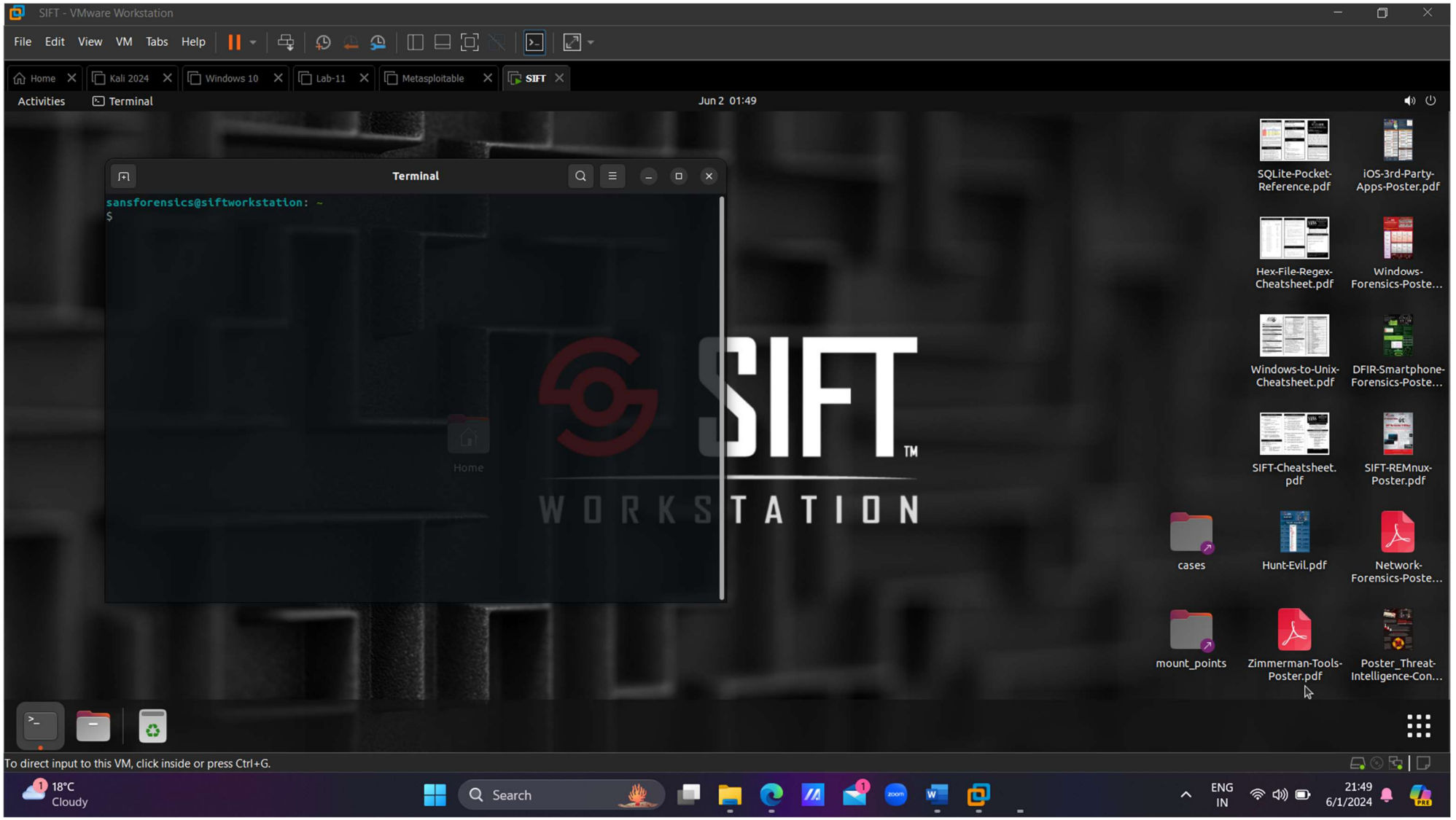
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.


Ishan Patel
This PC
Zoom
Genymotion Shell
Network
Cloudpaging Player
Genymotion
Recycle Bin
LockDown Browser
Google Chrome
Discord
Oracle VM VirtualBox
Kleopatra
Spotify
VMware Workstati...
Steam
Cisco Packet Tracer
Control Panel
Microsoft Edge
Epic Games Launcher
Command Prompt
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::cd00:9a0d:6a23:ca59%12
IPv4 Address. . . . . : 192.168.85.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::25ff:f98c:de2d:34b2%18
IPv4 Address. . . . . : 192.168.229.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
Link-local IPv6 Address . . . . . : fe80::8c09:d97b:c1df:af4f%24
IPv4 Address. . . . . : 192.168.2.47
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\Users\ASUS>
File
Edit
View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21
45 characters
100%
Windov
UTF-8
17°C
Cloudy
Search
ENG
IN
12:44
6/2/2024

Installation of SIFT

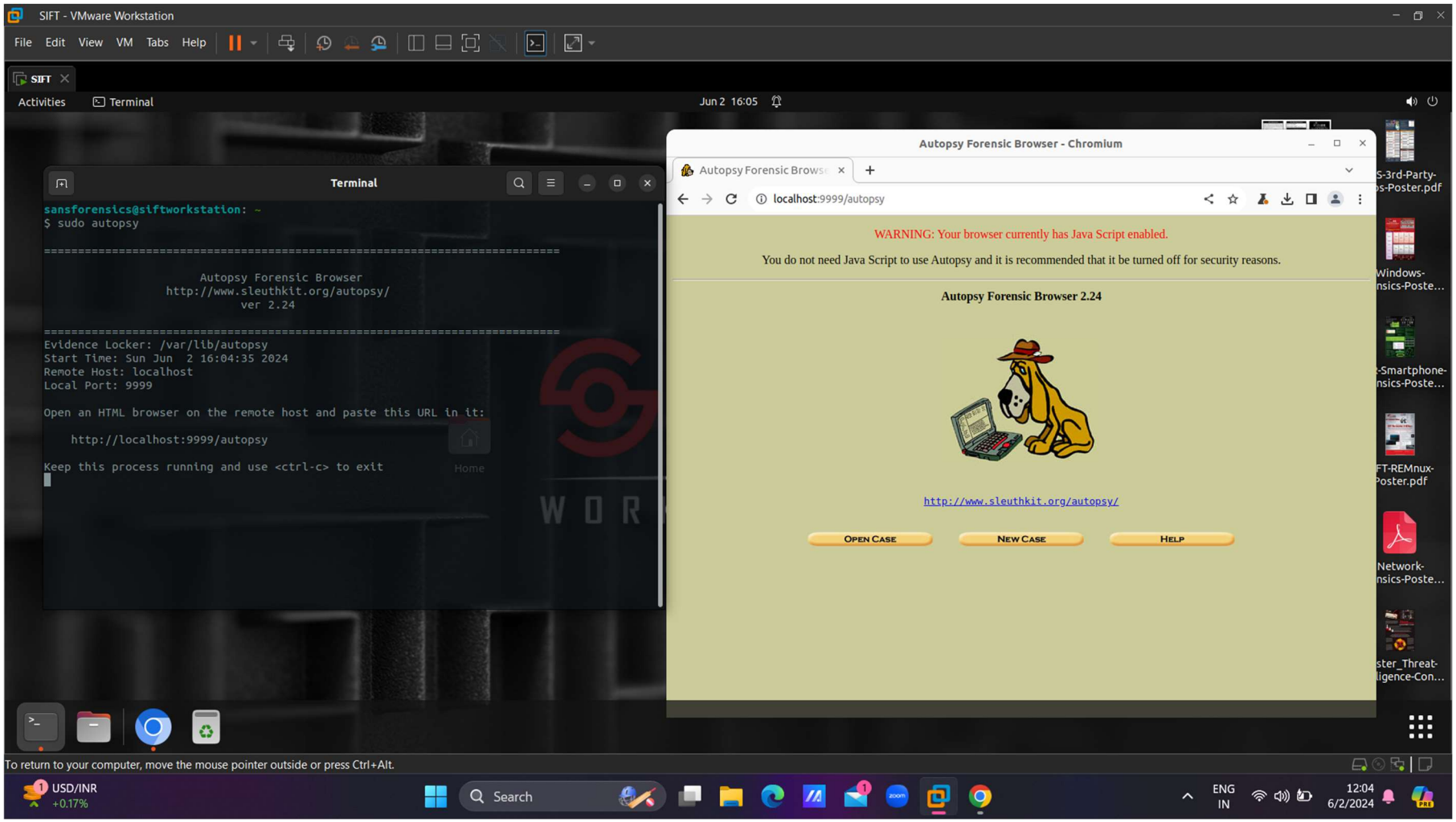


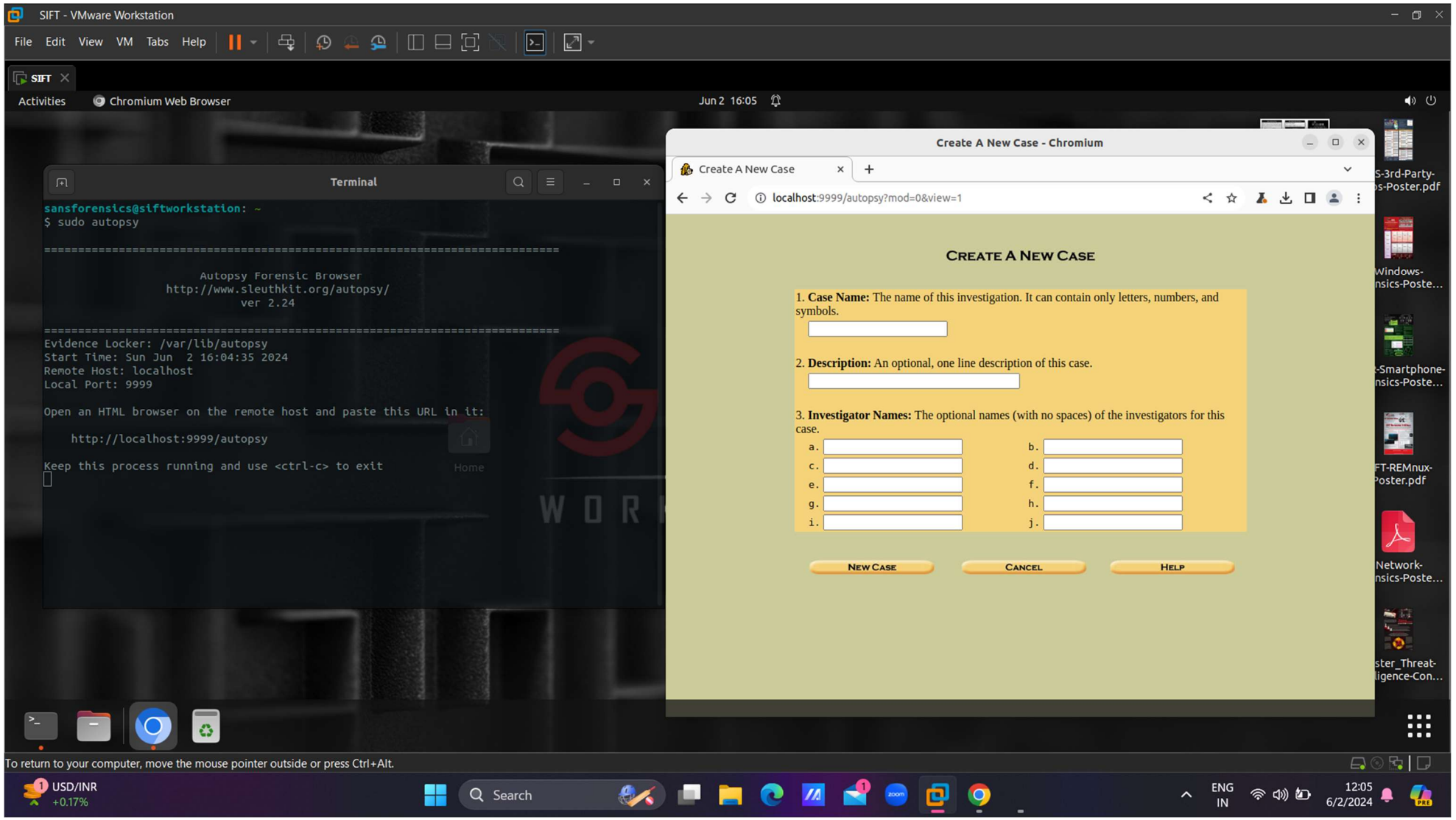

SIFT - VMware Workstation
File Edit View VM Tabs Help
Home
Kali 2024
Windows 10
Lab-11
Metasploitable
SIFT
SIFT
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 4 GB
Processors 4
Hard Disk (SCSI) 488.3 GB
CD/DVD (IDE) Using unknown b...
Network Adapter NAT
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\ASUS\Documents\Virtual Machines\SIFT\SIFT.vmx
Hardware compatibility: Workstation 9.x virtual machine
Primary IP address: Network information is not available
18°C
Cloudy
Search
ENG
IN
21:47
6/1/2024

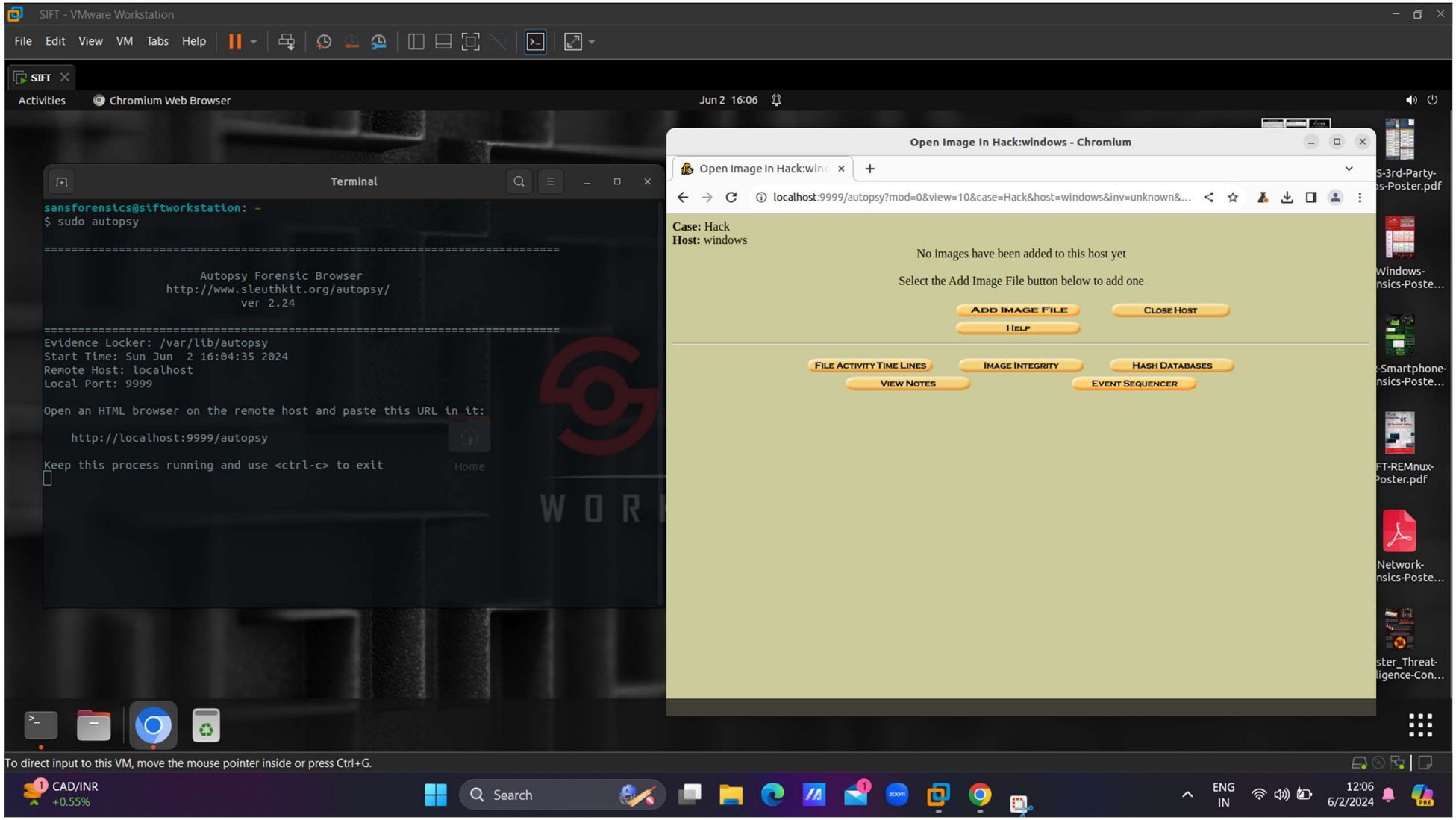

SIFT - VMware Workstation
File Edit View VM Tabs Help
Home
Kali 2024
Windows 10
Lab-11
Metasploitable
SIFT
Activities
Terminal
Jun 2 01:49
Terminal
sansforensics@siftworkstation: ~
$
SIFT
WORKSTATION
Home
SQLite-Pocket-Reference.pdf
iOS-3rd-Party-Apps-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Poste...
Windows-to-Unix-Cheatsheet.pdf
DFIR-Smartphone-Forensics-Poste...
SIFT-Cheatsheet.pdf
SIFT-REMnux-Poster.pdf
cases
Hunt-Evil.pdf
Network-Forensics-Poste...
mount_points
Zimmerman-Tools-Poster.pdf
Poster_Threat-Intelligence-Con...
To direct input to this VM, click inside or press Ctrl+G.
18°C
Cloudy
Search
ENG
IN
21:49
6/1/2024

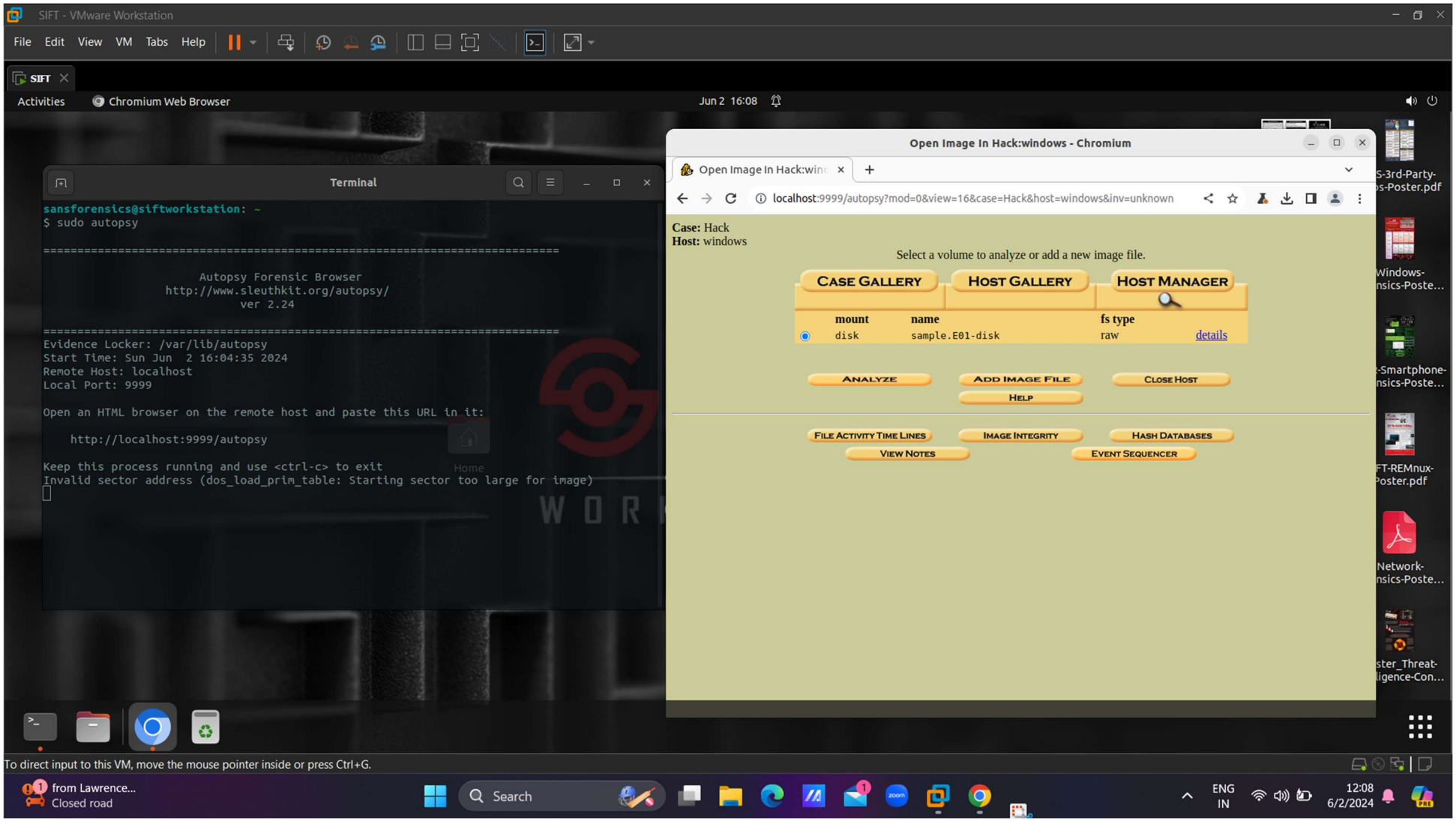
Tools

1) Autopsy : Autopsy is a digital forensics platform that provides a graphical interface for the Sleuth Kit, a collection of command-line tools for forensic analysis. It enables investigators to analyze disk images and perform in-depth investigations into file systems, recover deleted files, extract artifacts, and generate reports.

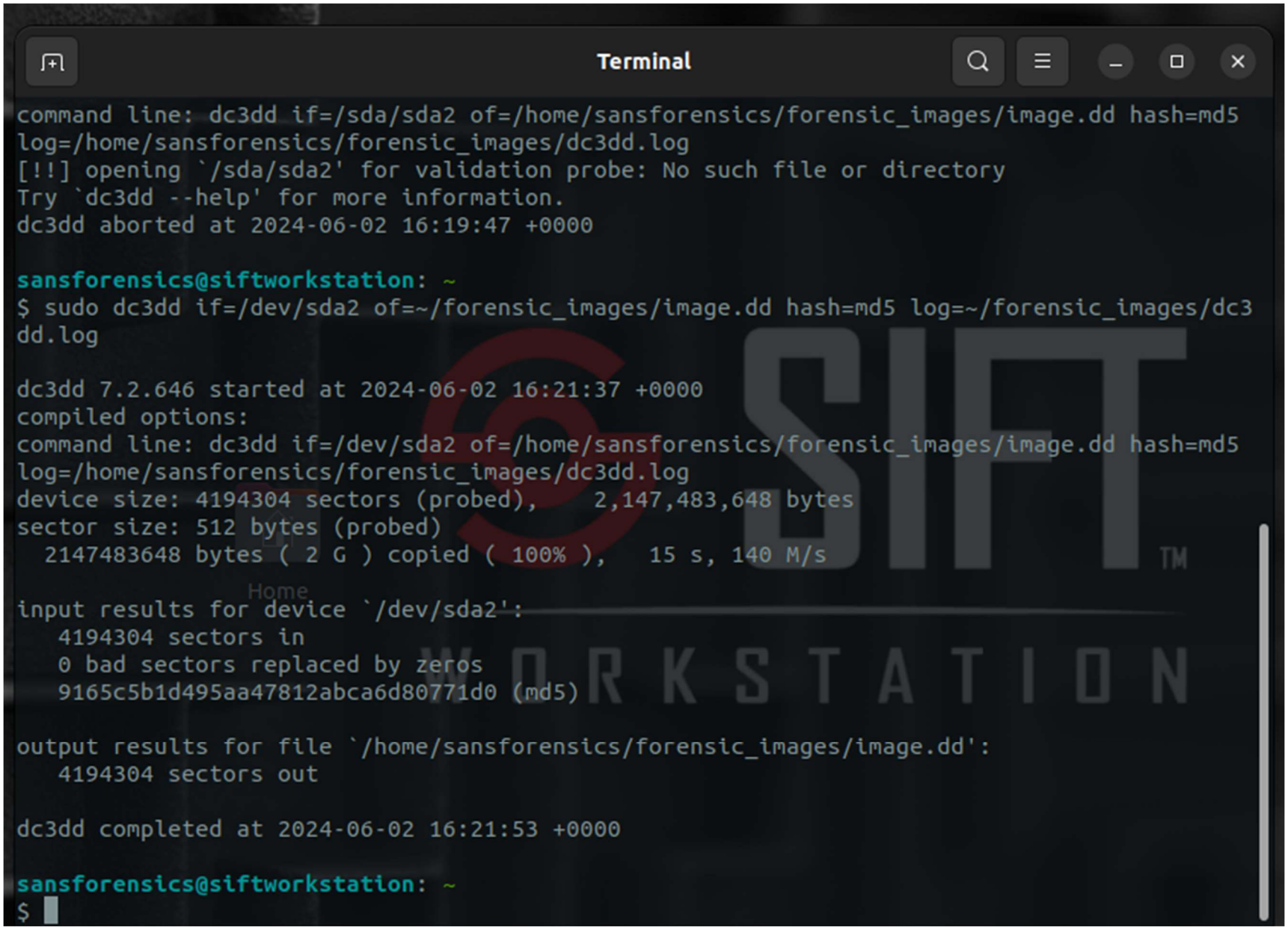


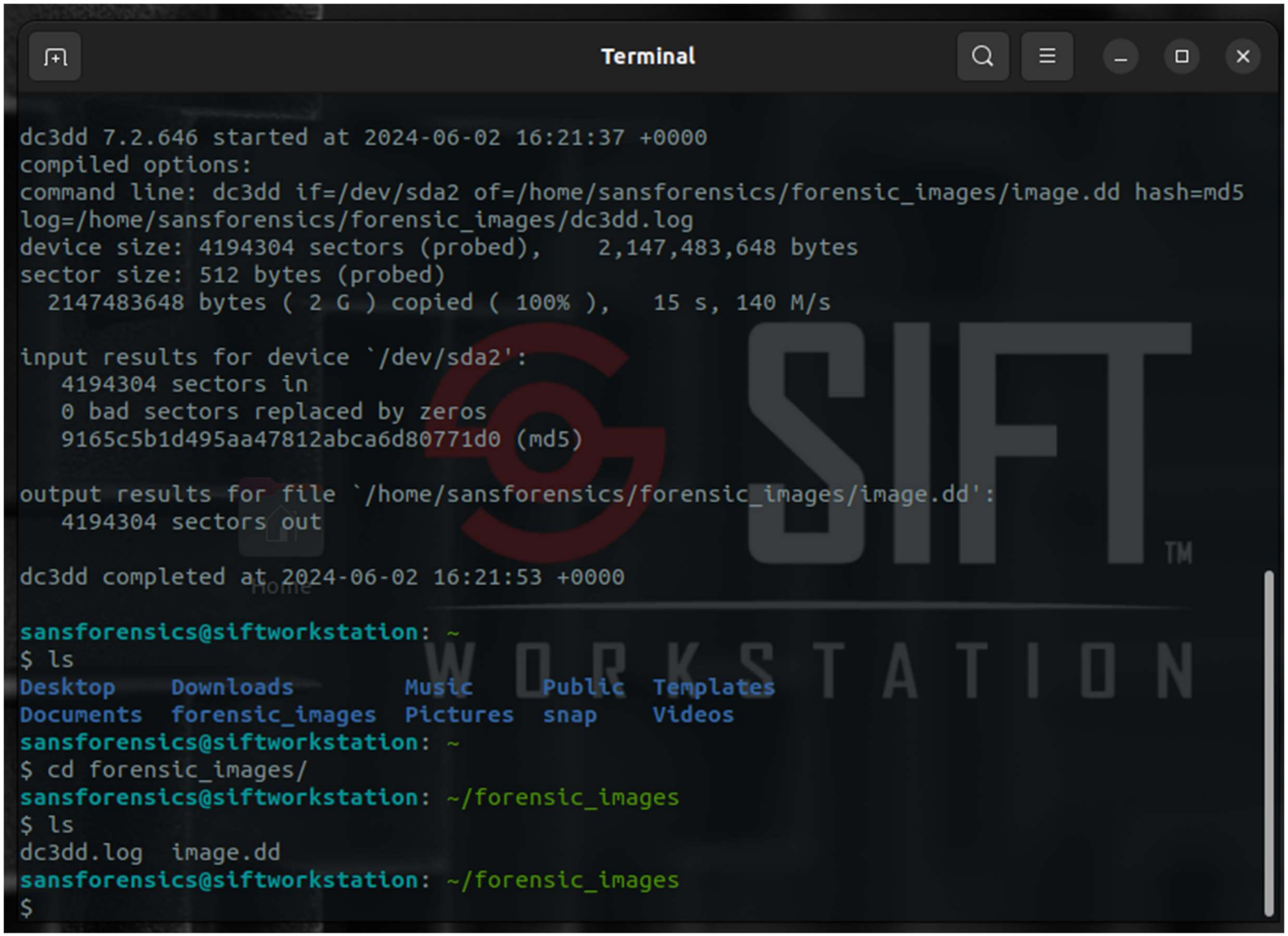

SIFT - VMware Workstation
File Edit View VM Tabs Help
SIFT
Activities
Chromium Web Browser
Jun 2 16:05
Terminal
sansforensics@siftworkstation: ~
$ sudo autopsy
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Sun Jun 2 16:04:35 2024
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
Create A New Case - Chromium
Create A New Case
localhost:9999/autopsy?mod=0&view=1
CREATE A NEW CASE
1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols.
2. Description: An optional, one line description of this case.
3. Investigator Names: The optional names (with no spaces) of the investigators for this case.
a. b.
c. d.
e. f.
g. h.
i. j.
NEW CASE
CANCEL
HELP
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
USD/INR
+0.17%
Search
ENG
IN
12:05
6/2/2024


SIFT - VMware Workstation
File Edit View VM Tabs Help
SIFT
Activities
Chromium Web Browser
Jun 2 16:06
Terminal
sansforensics@siftworkstation: ~
$ sudo autopsy
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Sun Jun 2 16:04:35 2024
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
Open Image In Hack:windows - Chromium
localhost:9999/autopsy?mod=0&view=10&case=Hack&host=windows&inv=unknown&...
Case: Hack
Host: windows
No images have been added to this host yet
Select the Add Image File button below to add one
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
CAD/INR
+0.55%
Search
ENG
IN
12:06
6/2/2024

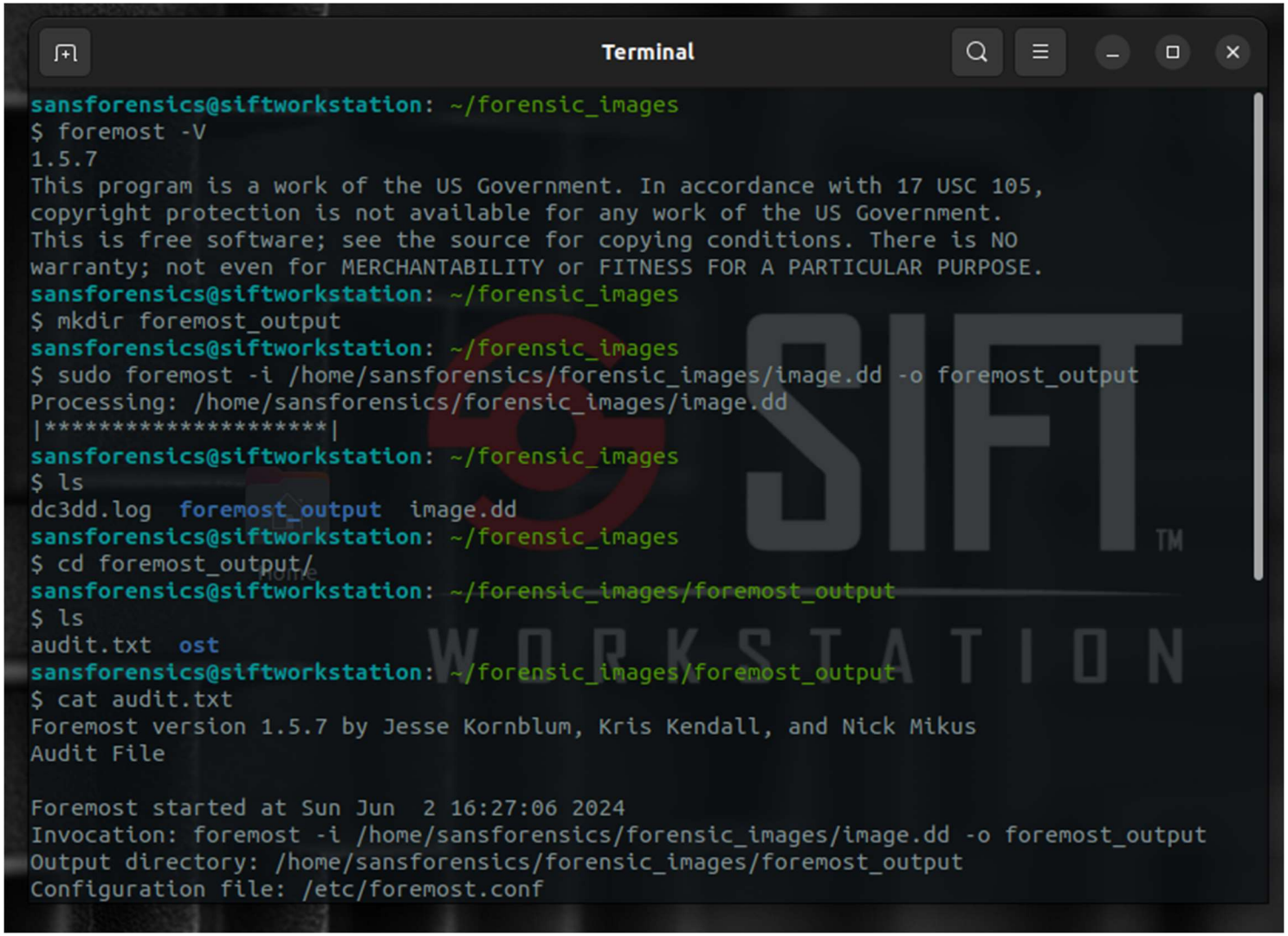

SIFT - VMware Workstation
File Edit View VM Tabs Help
SIFT
Activities
Chromium Web Browser
Jun 2 16:08
Terminal
sansforensics@siftworkstation: ~
$ sudo autopsy
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
Evidence Locker: /var/lib/autopsy
Start Time: Sun Jun 2 16:04:35 2024
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
Invalid sector address (dos_load_prim_table: Starting sector too large for image)
Open Image In Hack:windows - Chromium
Open Image In Hack:win
localhost:9999/autopsy?mod=0&view=16&case=Hack&host=windows&inv=unknown
Case: Hack
Host: windows
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
disk
sample.E01-disk
raw
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
from Lawrence...
Closed road
Search
ENG
IN
12:08
6/2/2024

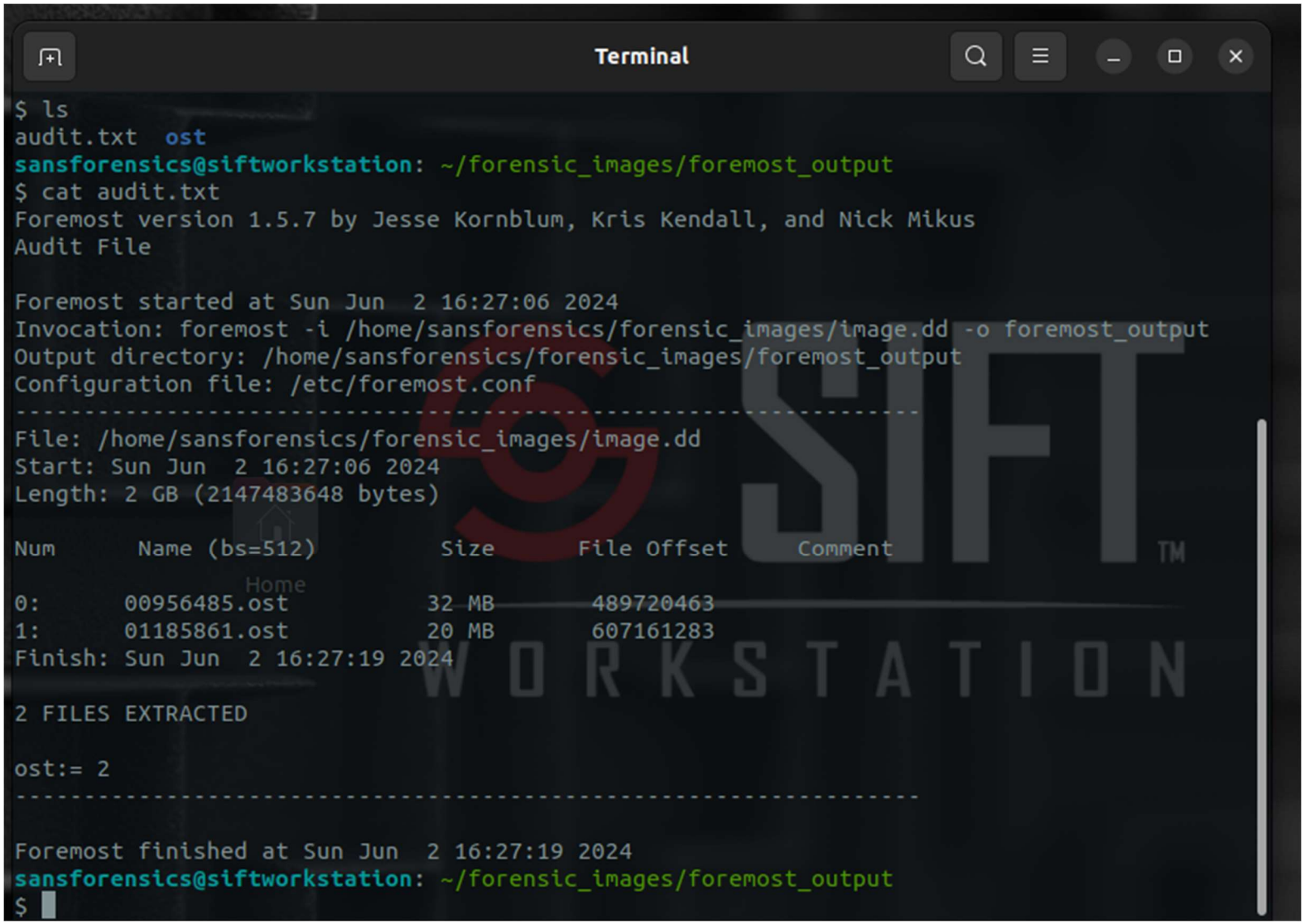
2) dc3dd : dc3dd is an enhanced version of the dd command, specifically designed for forensic imaging tasks. It allows users to create disk images bit by bit, with options for hashing, logging, and error handling. dc3dd is commonly used in digital forensics to create forensically sound disk images for analysis.


Terminal
command line: dc3dd if=/sda/sda2 of=/home/sansforensics/forensic_images/image.dd hash=md5
log=/home/sansforensics/forensic_images/dc3dd.log
[!!] opening `/sda/sda2' for validation probe: No such file or directory
Try `dc3dd --help' for more information.
dc3dd aborted at 2024-06-02 16:19:47 +0000
sansforensics@siftworkstation: ~
$ sudo dc3dd if=/dev/sda2 of=~/forensic_images/image.dd hash=md5 log=~/forensic_images/dc3
dd.log
dc3dd 7.2.646 started at 2024-06-02 16:21:37 +0000
compiled options:
command line: dc3dd if=/dev/sda2 of=/home/sansforensics/forensic_images/image.dd hash=md5
log=/home/sansforensics/forensic_images/dc3dd.log
device size: 4194304 sectors (probed), 2,147,483,648 bytes
sector size: 512 bytes (probed)
2147483648 bytes (2 G) copied (100%), 15 s, 140 M/s
input results for device `/dev/sda2':
4194304 sectors in
0 bad sectors replaced by zeros
9165c5b1d495aa47812abca6d80771d0 (md5)
output results for file `/home/sansforensics/forensic_images/image.dd':
4194304 sectors out
dc3dd completed at 2024-06-02 16:21:53 +0000
sansforensics@siftworkstation: ~
$

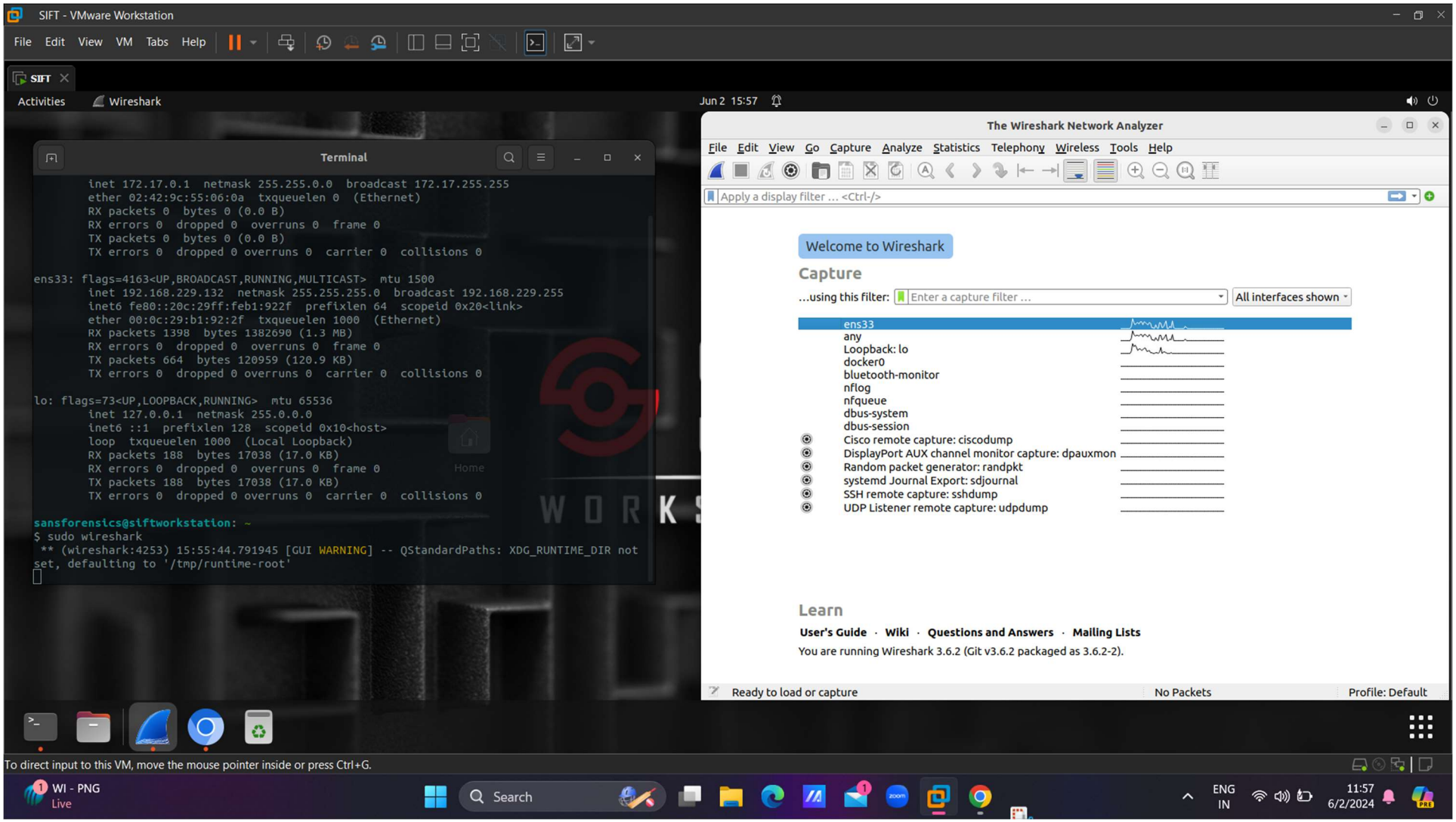

Terminal
dc3dd 7.2.646 started at 2024-06-02 16:21:37 +0000
compiled options:
command line: dc3dd if=/dev/sda2 of=/home/sansforensics/forensic_images/image.dd hash=md5
log=/home/sansforensics/forensic_images/dc3dd.log
device size: 4194304 sectors (probed), 2,147,483,648 bytes
sector size: 512 bytes (probed)
2147483648 bytes (2 G) copied (100%), 15 s, 140 M/s
input results for device `/dev/sda2':
4194304 sectors in
0 bad sectors replaced by zeros
9165c5b1d495aa47812abca6d80771d0 (md5)
output results for file `/home/sansforensics/forensic_images/image.dd':
4194304 sectors out
dc3dd completed at 2024-06-02 16:21:53 +0000
sansforensics@siftworkstation: ~
$ ls
Desktop Downloads Music Public Templates
Documents forensic_images Pictures snap Videos
sansforensics@siftworkstation: ~
$ cd forensic_images/
sansforensics@siftworkstation: ~/forensic_images
$ ls
dc3dd.log image.dd
sansforensics@siftworkstation: ~/forensic_images
$
SIFT
WORKSTATION

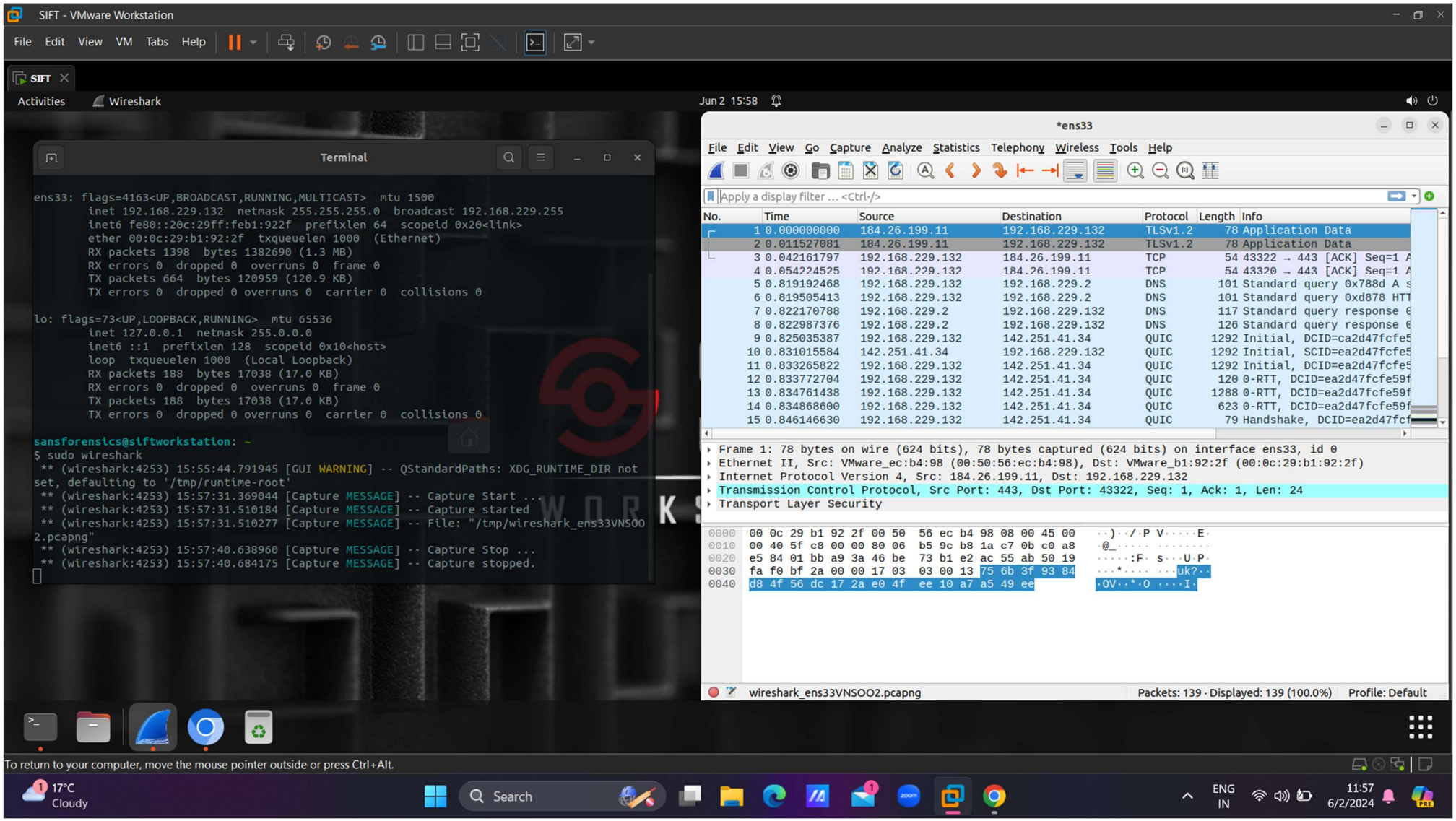
3) Foremost : Foremost is a forensic data recovery tool used to extract files from disk images or raw data files based on their headers, footers, and internal data structures. It can recover various types of files, such as documents, images, and archives, even if they have been deleted or corrupted.

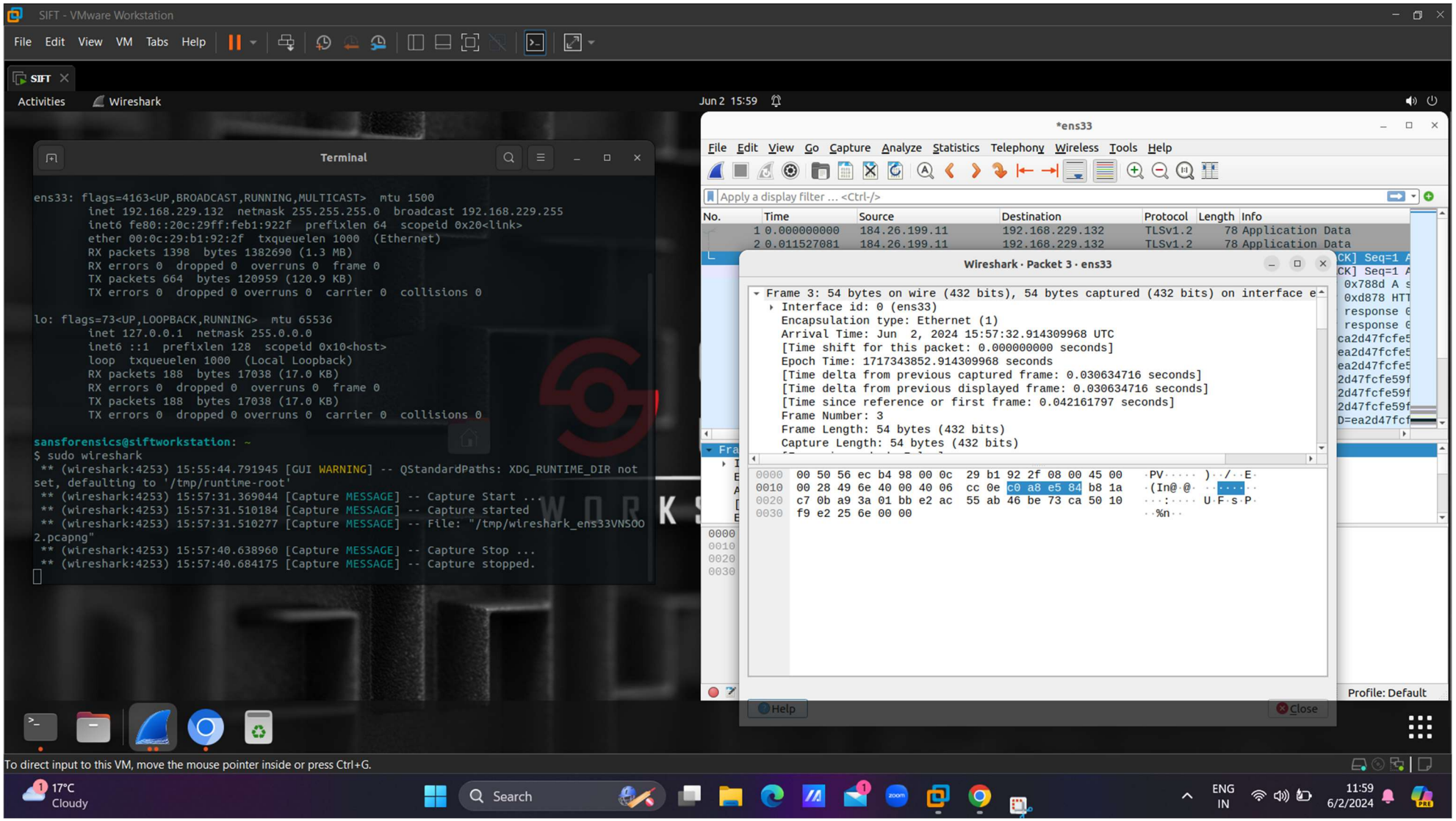



Terminal
$ ls
audit.txt ost
sansforensics@siftworkstation: ~/forensic_images/foremost_output
$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Sun Jun 2 16:27:06 2024
Invocation: foremost -i /home/sansforensics/forensic_images/image.dd -o foremost_output
Output directory: /home/sansforensics/forensic_images/foremost_output
Configuration file: /etc/foremost.conf
File: /home/sansforensics/forensic_images/image.dd
Start: Sun Jun 2 16:27:06 2024
Length: 2 GB (2147483648 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00956485.ost 32 MB 489720463
1: 01185861.ost 20 MB 607161283
Finish: Sun Jun 2 16:27:19 2024
2 FILES EXTRACTED
ost:= 2
Foremost finished at Sun Jun 2 16:27:19 2024
sansforensics@siftworkstation: ~/forensic_images/foremost_output
$

4) Wireshark : Wireshark is a network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It supports a wide range of protocols and provides detailed information about network packets, allowing users to troubleshoot network issues, analyze security threats, and conduct network forensics.




SIFT - VMware Workstation
File Edit View VM Tabs Help
SIFT
Activities
Wireshark
Jun 2 15:58
Terminal
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.229.132 netmask 255.255.255.0 broadcast 192.168.229.255
inet6 fe80::20c:29ff:feb1:922f prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:b1:92:2f txqueuelen 1000 (Ethernet)
RX packets 1398 bytes 1382690 (1.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 664 bytes 120959 (120.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 188 bytes 17038 (17.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 188 bytes 17038 (17.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sansforensics@siftworkstation: ~
$ sudo wireshark
** (wireshark:4253) 15:55:44.791945 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:4253) 15:57:31.369044 [Capture MESSAGE] -- Capture Start ...
** (wireshark:4253) 15:57:31.510184 [Capture MESSAGE] -- Capture started
** (wireshark:4253) 15:57:31.510277 [Capture MESSAGE] -- File: "/tmp/wireshark_ens33VNSOO2.pcapng"
** (wireshark:4253) 15:57:40.638960 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:4253) 15:57:40.684175 [Capture MESSAGE] -- Capture stopped.
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 184.26.199.11 192.168.229.132 TLSv1.2 78 Application Data
2 0.011527081 184.26.199.11 192.168.229.132 TLSv1.2 78 Application Data
3 0.042161797 192.168.229.132 184.26.199.11 TCP 54 43322 → 443 [ACK] Seq=1 A
4 0.054224525 192.168.229.132 184.26.199.11 TCP 54 43320 → 443 [ACK] Seq=1 A
5 0.819192468 192.168.229.132 192.168.229.2 DNS 101 Standard query 0x788d A s
6 0.819505413 192.168.229.132 192.168.229.2 DNS 101 Standard query 0xd878 HTT
7 0.822170788 192.168.229.2 192.168.229.132 DNS 117 Standard query response 6
8 0.822987376 192.168.229.2 192.168.229.132 DNS 126 Standard query response 6
9 0.825035387 192.168.229.132 142.251.41.34 QUIC 1292 Initial, DCID=ca2d47fcfe5
10 0.831015584 142.251.41.34 192.168.229.132 QUIC 1292 Initial, SCID=ea2d47fcfe5
11 0.833265822 192.168.229.132 142.251.41.34 QUIC 1292 Initial, DCID=ea2d47fcfe5
12 0.833772704 192.168.229.132 142.251.41.34 QUIC 120 0-RTT, DCID=ea2d47fcfe59f
13 0.834761438 192.168.229.132 142.251.41.34 QUIC 1288 0-RTT, DCID=ea2d47fcfe59f
14 0.834868600 192.168.229.132 142.251.41.34 QUIC 623 0-RTT, DCID=ea2d47fcfe59f
15 0.846146630 192.168.229.132 142.251.41.34 QUIC 79 Handshake, DCID=ea2d47fcf
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface ens33, id 0
Ethernet II, Src: VMware_ec:b4:98 (00:50:56:ec:b4:98), Dst: VMware_b1:92:2f (00:0c:29:b1:92:2f)
Internet Protocol Version 4, Src: 184.26.199.11, Dst: 192.168.229.132
Transmission Control Protocol, Src Port: 443, Dst Port: 43322, Seq: 1, Ack: 1, Len: 24
Transport Layer Security
0000 00 0c 29 b1 92 2f 00 50 56 ec b4 98 08 00 45 00
0010 00 40 5f c8 00 00 80 06 b5 9c b8 1a c7 0b c0 a8
0020 e5 84 01 bb a9 3a 46 be 73 b1 e2 ac 55 ab 50 19
0030 fa f0 bf 2a 00 00 17 03 03 00 13 75 6b 3f 93 84
0040 d8 4f 56 dc 17 2a e0 4f ee 10 a7 a5 49 ee
wireshark_ens33VNSOO2.pcapng
Packets: 139 · Displayed: 139 (100.0%)
Profile: Default
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
17°C
Cloudy
Search
ENG
IN
11:57
6/2/2024


SIFT - VMware Workstation
File Edit View VM Tabs Help
SIFT
Activities
Wireshark
Jun 2 15:59
Terminal
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.229.132 netmask 255.255.255.0 broadcast 192.168.229.255
inet6 fe80::20c:29ff:feb1:922f prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:b1:92:2f txqueuelen 1000 (Ethernet)
RX packets 1398 bytes 1382690 (1.3 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 664 bytes 120959 (120.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 188 bytes 17038 (17.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 188 bytes 17038 (17.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sansforensics@siftworkstation: ~
$ sudo wireshark
** (wireshark:4253) 15:55:44.791945 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (wireshark:4253) 15:57:31.369044 [Capture MESSAGE] -- Capture Start ...
** (wireshark:4253) 15:57:31.510184 [Capture MESSAGE] -- Capture started
** (wireshark:4253) 15:57:31.510277 [Capture MESSAGE] -- File: "/tmp/wireshark_ens33VN5002.pcapng"
** (wireshark:4253) 15:57:40.638960 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:4253) 15:57:40.684175 [Capture MESSAGE] -- Capture stopped.
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 184.26.199.11 192.168.229.132 TLSv1.2 78 Application Data
2 0.011527081 184.26.199.11 192.168.229.132 TLSv1.2 78 Application Data
Wireshark · Packet 3 · ens33
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface e
Interface id: 0 (ens33)
Encapsulation type: Ethernet (1)
Arrival Time: Jun 2, 2024 15:57:32.914309968 UTC
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1717343852.914309968 seconds
[Time delta from previous captured frame: 0.030634716 seconds]
[Time delta from previous displayed frame: 0.030634716 seconds]
[Time since reference or first frame: 0.042161797 seconds]
Frame Number: 3
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
0000 00 50 56 ec b4 98 00 0c 29 b1 92 2f 08 00 45 00
0010 00 28 49 6e 40 00 40 06 cc 0e c0 a8 e5 84 b8 1a
0020 c7 0b a9 3a 01 bb e2 ac 55 ab 46 be 73 ca 50 10
0030 f9 e2 25 6e 00 00
Help
Close
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
17°C Cloudy
Search
ENG IN
11:59 6/2/2024

Answer

Setting up the SIFT Workstation on my virtual machine was straightforward following the installation guides and video tutorials provided. I downloaded the SIFT Workstation from the official website and installed it using VirtualBox. During the installation process, I encountered no significant challenges, and the setup was relatively easy to complete. Once installed, I familiarized myself with basic Linux commands and explored the SIFT Workstation's file system, memory analysis tools, network traffic analysis tools, malware analysis tools, and network utilities.

Overall, I found the SIFT Workstation to be highly useful and user-friendly. The interface was intuitive, and the pre-installed tools provided comprehensive capabilities for digital forensics analysis. The step-by-step tutorials and resources available online were instrumental in guiding me through the setup and usage of the SIFT Workstation.

Learning Experience

My learning experience was enriching as I gained practical knowledge of setting up a forensic analysis environment and using various tools to investigate digital evidence. The hands-on practice allowed me to understand the importance of each tool and how they work together to conduct thorough forensic examinations.