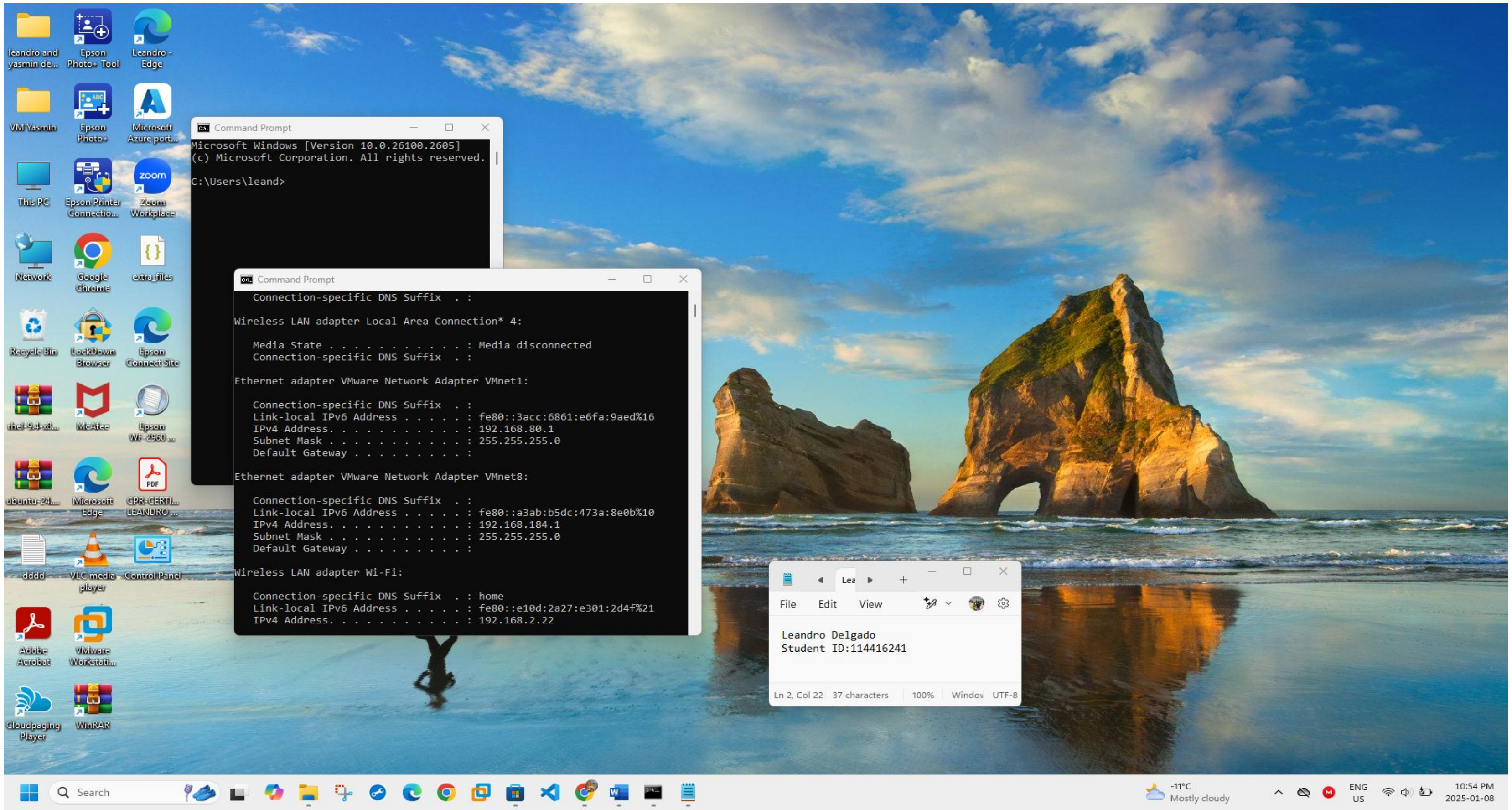
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
LEANDRO DELGADO	114416241	As Posted	6%

Name	Lab 1: SIFT Workstation
Instructions	• It is an Individual assignment. Put your name + Student ID in the file you submit • 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**". • Submit your report name: CYT215-Lab1-Student Name & ID
Students Work required for this activity	• Install a virtualization platform (VMware or Virtual Box) • Make sure to Enable shared folders between your host and VM and test it. • Set up your workspace inside the SIFT virtual machine & familiarize yourself with some simple Linux commands. • Download and 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 some tools & utilities of your choice on SIFT to test your workspace.

	• Show screenshots of the tools & utilities you used in your workspace (at least 2 tools) • Provide a brief description of what the tools are and what they are used for. • You need to provide screenshots for every step of the assignment.

Desktop background with **Date/Time** and **your name + IP**".



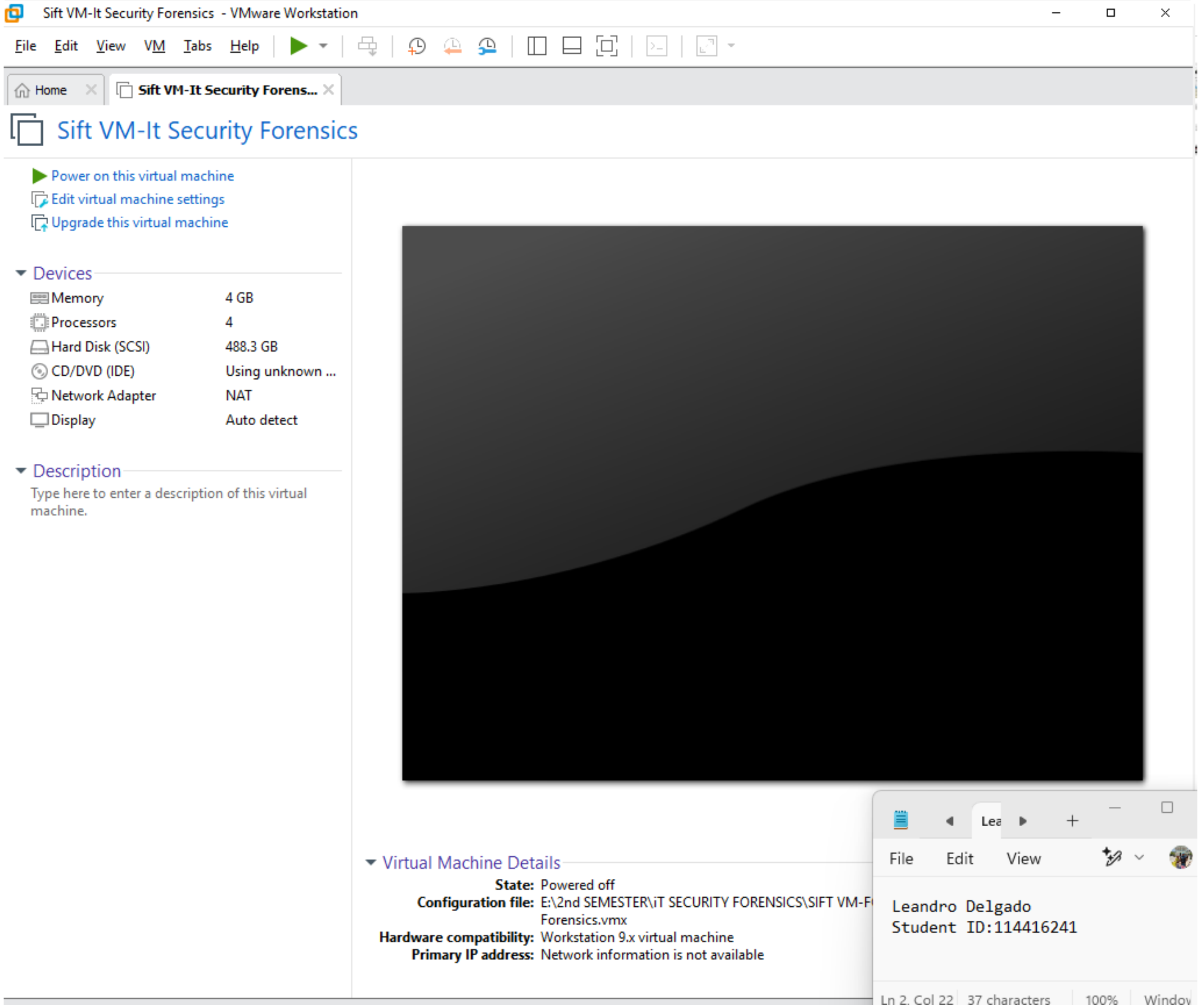
```
Microsoft Windows [Version 10.0.26100.2605]
(c) Microsoft Corporation. All rights reserved.

C:\Users\leand>
```

```
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3acc:6861:e6fa:9aed%16
   IPv4 Address. . . . . . . . . . . : 192.168.80.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a3ab:b5dc:473a:8e0b%10
   IPv4 Address. . . . . . . . . . . : 192.168.184.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::e10d:2a27:e301:2d4f%21
   IPv4 Address. . . . . . . . . . . : 192.168.2.22
```

```
Leandro Delgado
Student ID:114416241
```

Ln 2, Col 22 | 37 characters | 100% | Windov | UTF-8

The next screenshots below show the process of workspace inside the SIFT virtual machine.


Sift VM-It Security Forensics - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Sift VM-It Security Forens...
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Lea
File
Edit
View

Sift VM-It Security Forensics

Devices

Memory	4 GB
Processors	4
Hard Disk (SCSI)	488.3 GB
CD/DVD (IDE)	Using unknown ...
Network Adapter	NAT
Display	Auto detect

Description

Type here to enter a description of this virtual machine.

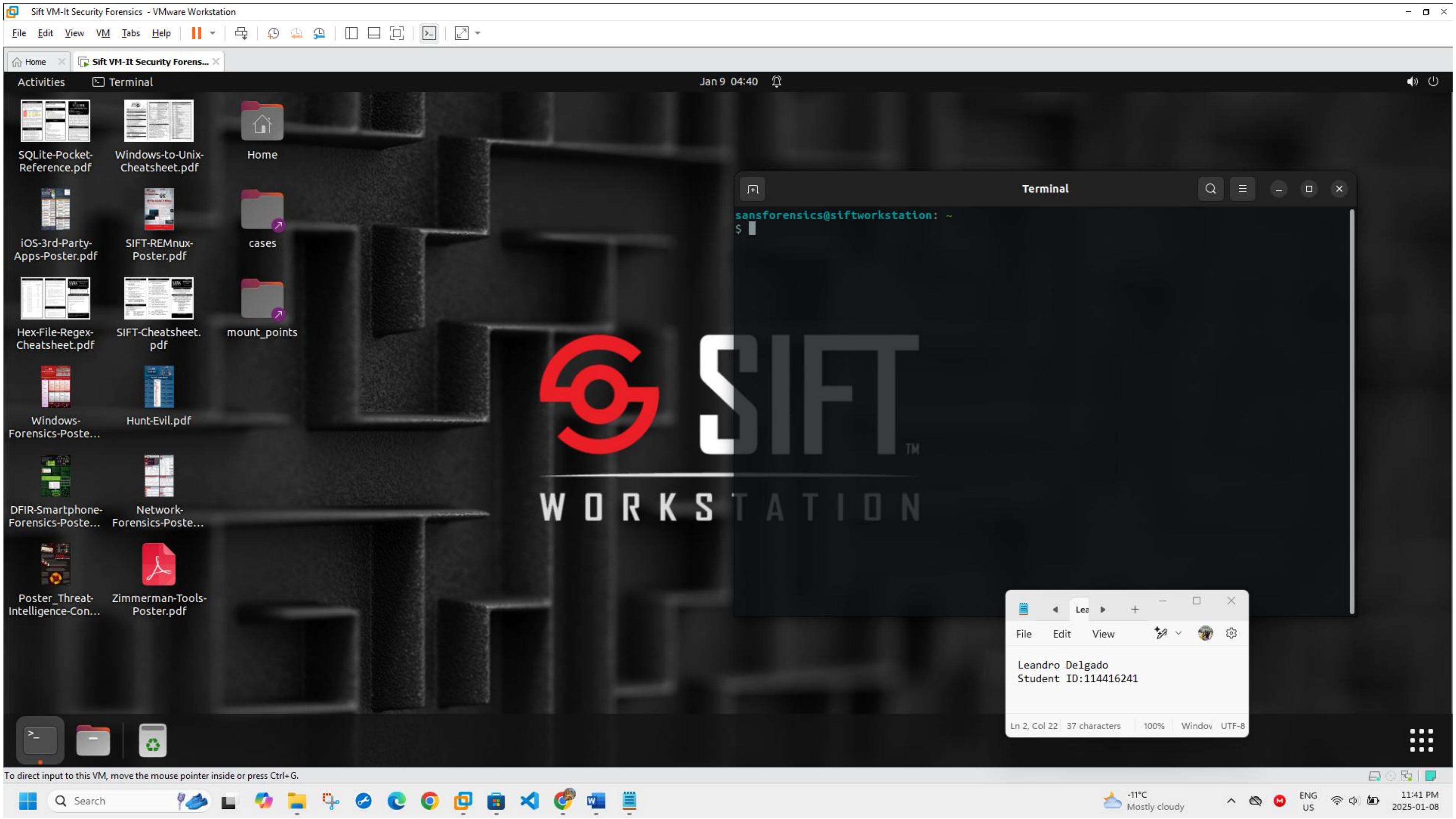
Virtual Machine Details

State:	Powered off
Configuration file:	E:\2nd SEMESTER\iT SECURITY FORENSICS\SIFT VM-F Forensics.vmx
Hardware compatibility:	Workstation 9.x virtual machine
Primary IP address:	Network information is not available

```
Leandro Delgado
Student ID:114416241
```

Ln 2, Col 22 | 37 characters | 100% | Windov

Figure 1- Vm Sift security Forensics setting.



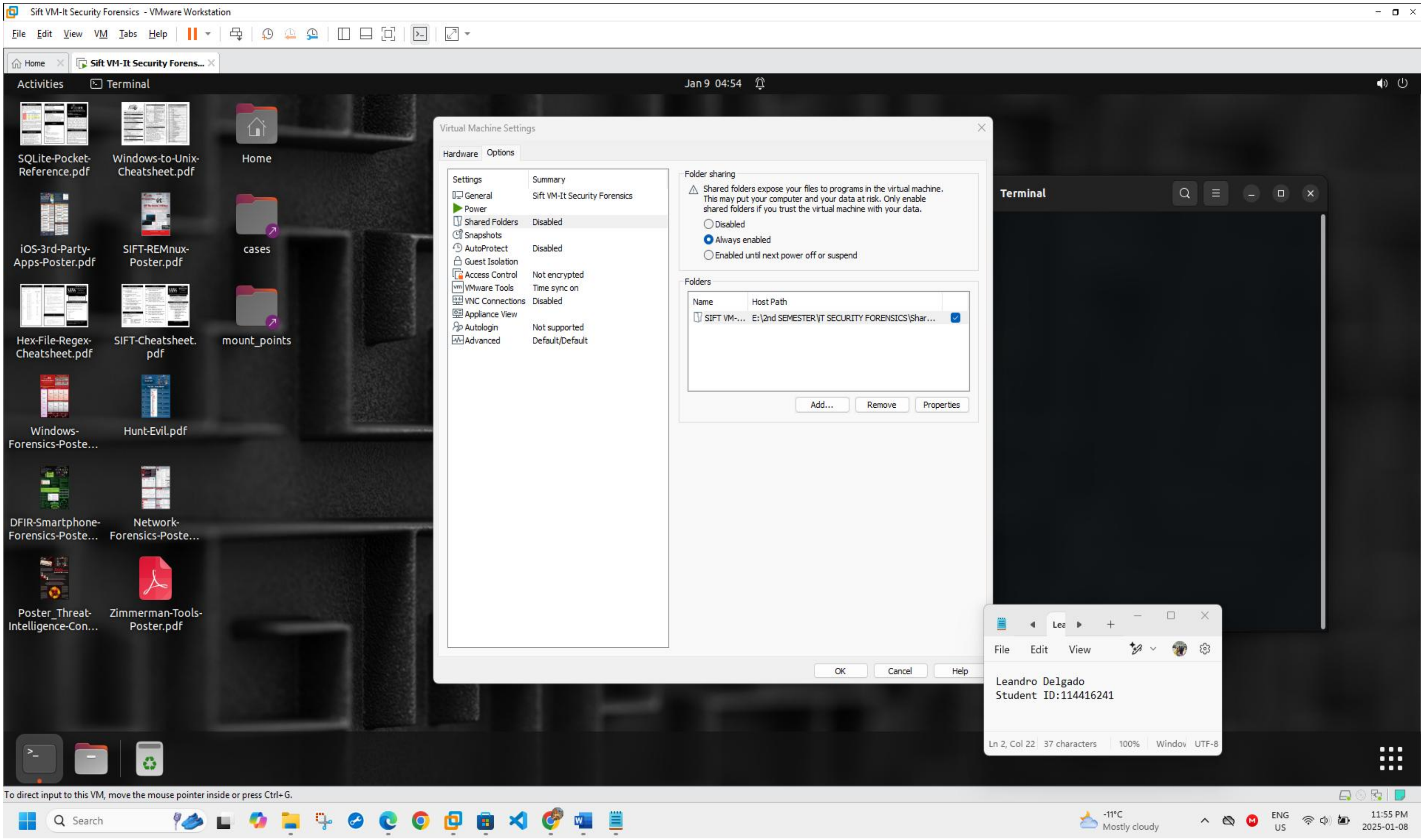
Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 04:40
SQLite-Pocket-Reference.pdf
Windows-to-Unix-Cheatsheet.pdf
Home
iOS-3rd-Party-Apps-Poster.pdf
SIFT-REMnux-Poster.pdf
cases
Hex-File-Regex-Cheatsheet.pdf
SIFT-Cheatsheet.pdf
mount_points
Windows-Forensics-Poste...
Hunt-Evil.pdf
DFIR-Smartphone-Forensics-Poste...
Network-Forensics-Poste...
Poster_Threat-Intelligence-Con...
Zimmerman-Tools-Poster.pdf
SIFT
WORKSTATION
Terminal
Lea
File Edit View
Ln 2, Col 22 37 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
-11°C
Mostly cloudy
ENG
US
11:41 PM
2025-01-08

```
sansforensics@siftworkstation: ~
$ 
```

```
Leandro Delgado
Student ID:114416241
```

Figure 2- Vm Sift security Forensics created.

Shared folders between your host and VM is enable.



Virtual Machine Settings

Settings	Summary
General	Sift VM-It Security Forensics
Power	
Shared Folders	Disabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync on
VNC Connections	Disabled
Appliance View	
Autologin	Not supported
Advanced	Default/Default

Folder sharing

⚠ Shared folders expose your files to programs in the virtual machine. This may put your computer and your data at risk. Only enable shared folders if you trust the virtual machine with your data.

○ Disabled
● Always enabled
○ Enabled until next power off or suspend

Folders

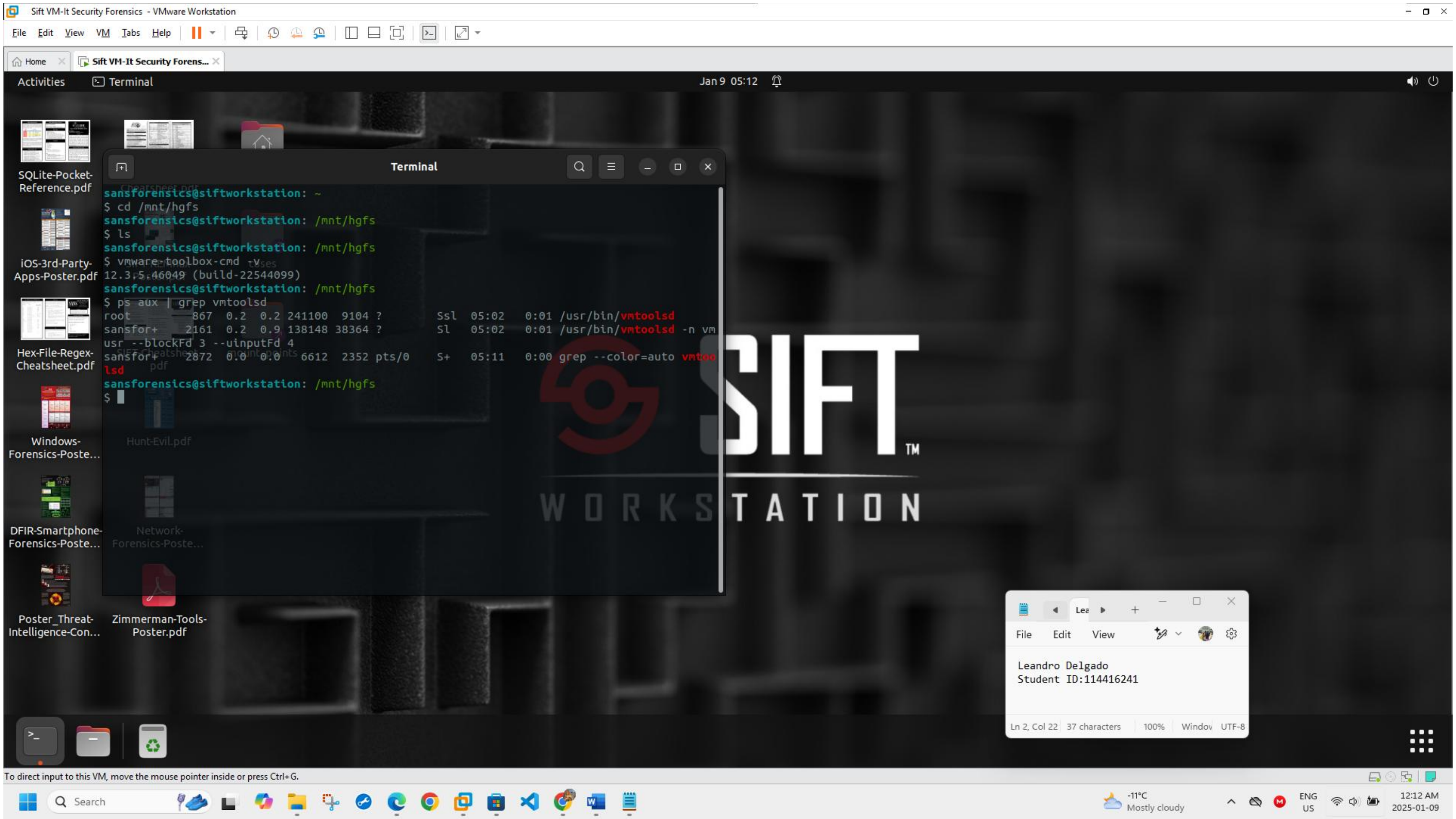
Name	Host Path	
SIFT VM-...	E:\2nd SEMESTER\IT SECURITY FORENSICS\Shar...	☑

Leandro Delgado
Student ID:114416241

Sift VM-It Security Forensics - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 04:54
SQLite-Pocket-Reference.pdf
Windows-to-Unix-Cheatsheet.pdf
Home
iOS-3rd-Party-Apps-Poster.pdf
SIFT-REMnux-Poster.pdf
cases
Hex-File-Regex-Cheatsheet.pdf
SIFT-Cheatsheet.pdf
mount_points
Windows-Forensics-Poste...
Hunt-Evil.pdf
DFIR-Smartphone-Forensics-Poste...
Network-Forensics-Poste...
Poster_Threat-Intelligence-Con...
Zimmerman-Tools-Poster.pdf
Hardware
Options
Add...
Remove
Properties
OK
Cancel
Help
Terminal
Lea
File
Edit
View
Ln 2, Col 22
37 characters
100%
Windov
UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
-11°C
Mostly cloudy
ENG
US
11:55 PM
2025-01-08

Figure 3- Vm Sift security Forensics shared folders.

In this section was verifying the Workspace Inside SIFT and Test Shared Folders



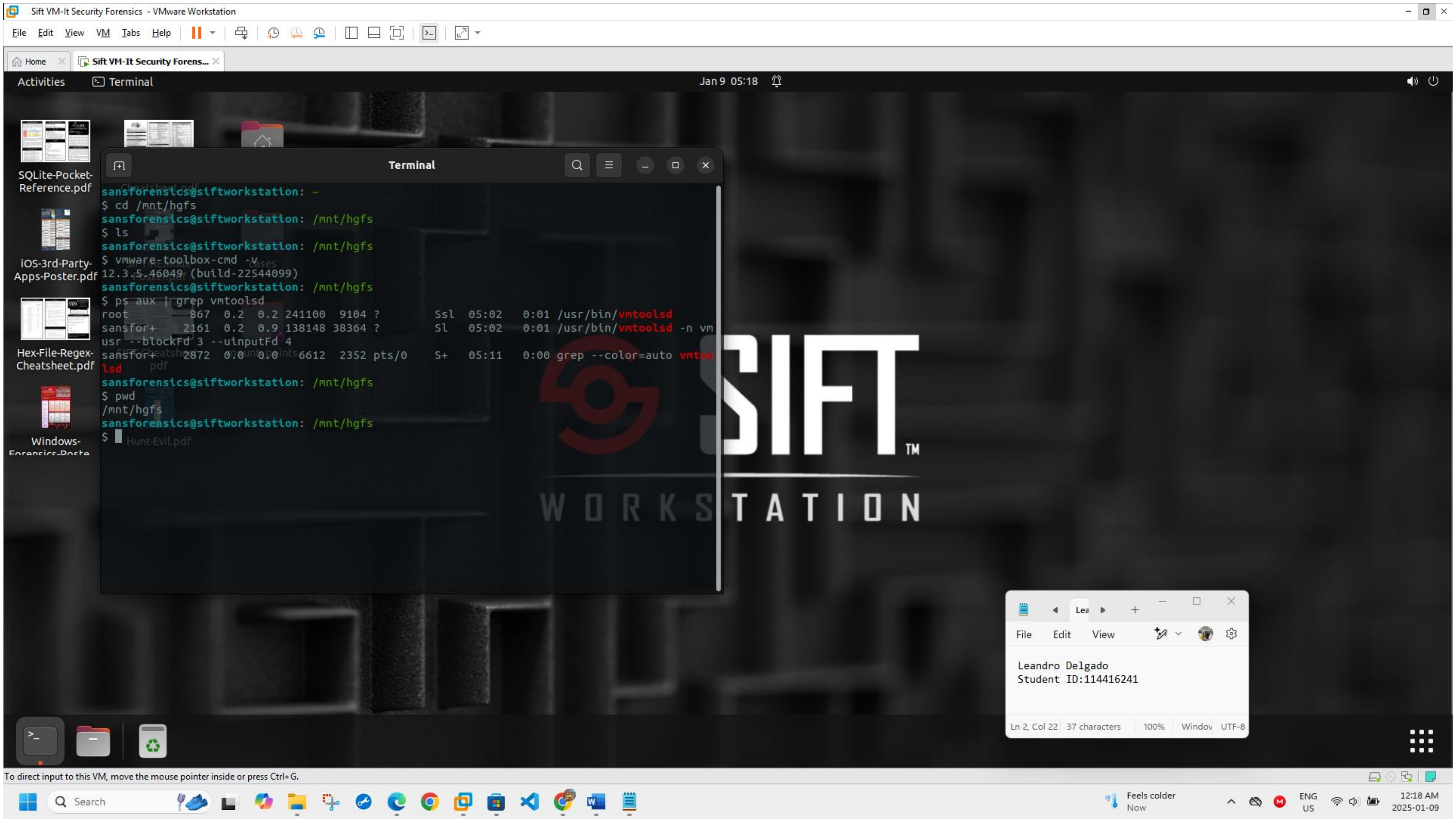
```
sansforensics@siftworkstation: ~
$ cd /mnt/hgfs
sansforensics@siftworkstation: /mnt/hgfs
$ ls
sansforensics@siftworkstation: /mnt/hgfs
$ vmware-toolbox-cmd -v
12.3.5.46049 (build-22544099)
sansforensics@siftworkstation: /mnt/hgfs
$ ps aux | grep vmtoolsd
root         867  0.2  0.2 241100  9104 ?        Ssl  05:02   0:01 /usr/bin/vmtoolsd
sansfor+    2161  0.2  0.9 138148 38364 ?        Sl   05:02   0:01 /usr/bin/vmtoolsd -n vm
usr --blockFd 3 --uinputFd 4
sansfor+    2872  0.0  0.0   6612  2352 pts/0    S+   05:11   0:00 grep --color=auto vmtoo
lsd
sansforensics@siftworkstation: /mnt/hgfs
$ 
```

Leandro Delgado
Student ID:114416241

Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 05:12
SQLite-Pocket-Reference.pdf
iOS-3rd-Party-Apps-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Poste...
DFIR-Smartphone-Forensics-Poste...
Poster_Threat-Intelligence-Con...
Zimmerman-Tools-Poster.pdf
Hunt-Evil.pdf
Network-Forensics-Poste...
SIFT WORKSTATION
File Edit View
Ln 2, Col 22 37 characters 100% Windov UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
-11°C Mostly cloudy
ENG US
12:12 AM 2025-01-09

Figure 4- Vm Sift security Forensics test shared folders.

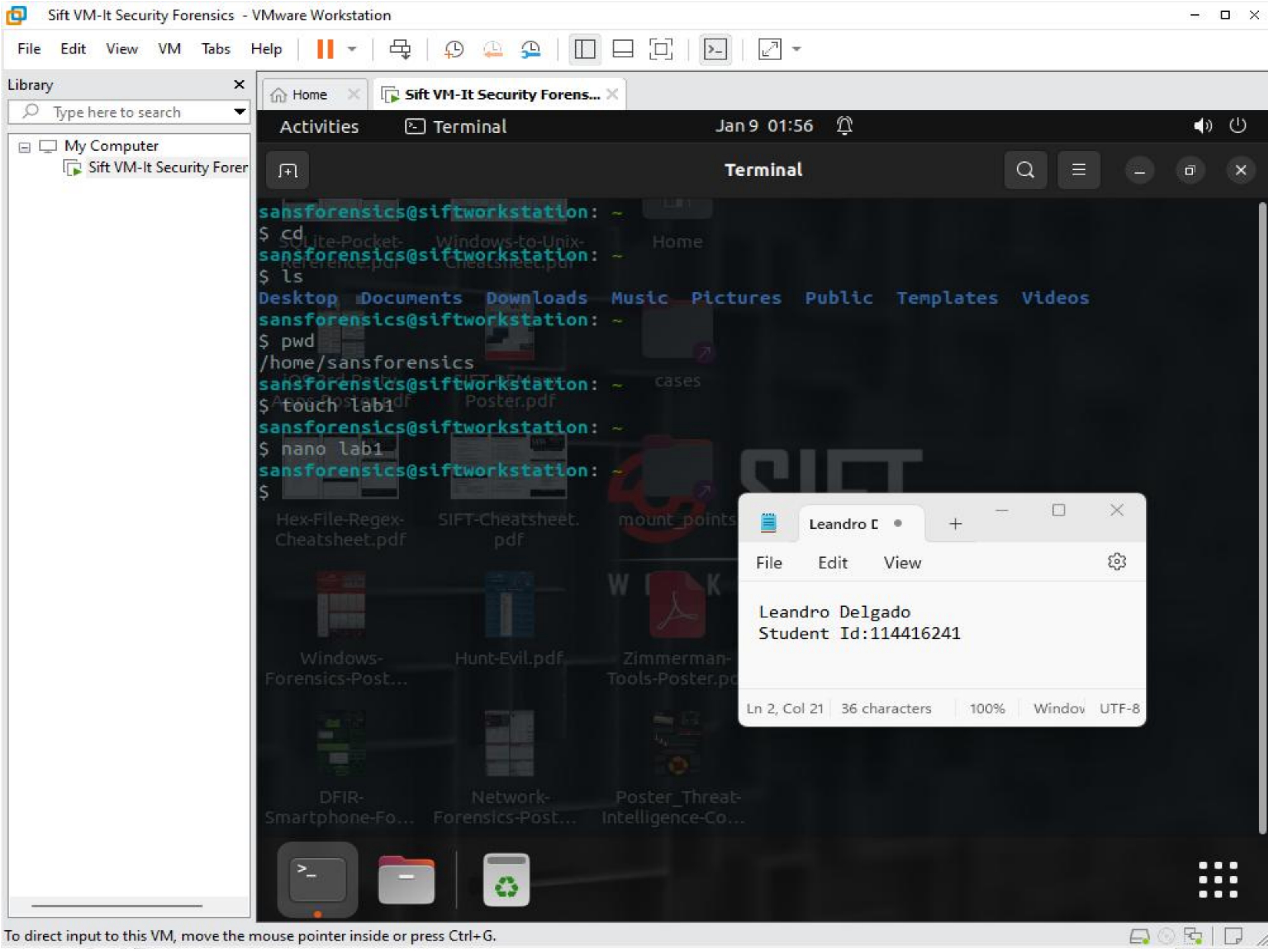
Familiarize yourself with basic Linux commands in SIFT:


Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 05:18
SQLite-Pocket-Reference.pdf
iOS-3rd-Party-Apps-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Poste
Terminal
SIFT™
WORKSTATION
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
Feels colder
Now
ENG
US
12:18 AM
2025-01-09

```
sansforensics@siftworkstation: ~
$ cd /mnt/hgfs
sansforensics@siftworkstation: /mnt/hgfs
$ ls
sansforensics@siftworkstation: /mnt/hgfs
$ vmware-toolbox-cmd -v
12.3.5.46049 (build-22544099)
sansforensics@siftworkstation: /mnt/hgfs
$ ps aux | grep vmtoolsd
root         867  0.2  0.2 241100  9104 ?        Ssl  05:02   0:01 /usr/bin/vmtoolsd
sansfor+    2161  0.2  0.9 138148 38364 ?        Sl   05:02   0:01 /usr/bin/vmtoolsd -n vm
usr --blockFd 3 --uinputFd 4
sansfor+    2872  0.0  0.0   6612  2352 pts/0    S+   05:11   0:00 grep --color=auto vmtoo
lsd
sansforensics@siftworkstation: /mnt/hgfs
$ pwd
/mnt/hgfs
sansforensics@siftworkstation: /mnt/hgfs
$
```

Leandro Delgado
Student ID:114416241

Figure 5- Vm Sift security Forensics basic Linux commands.



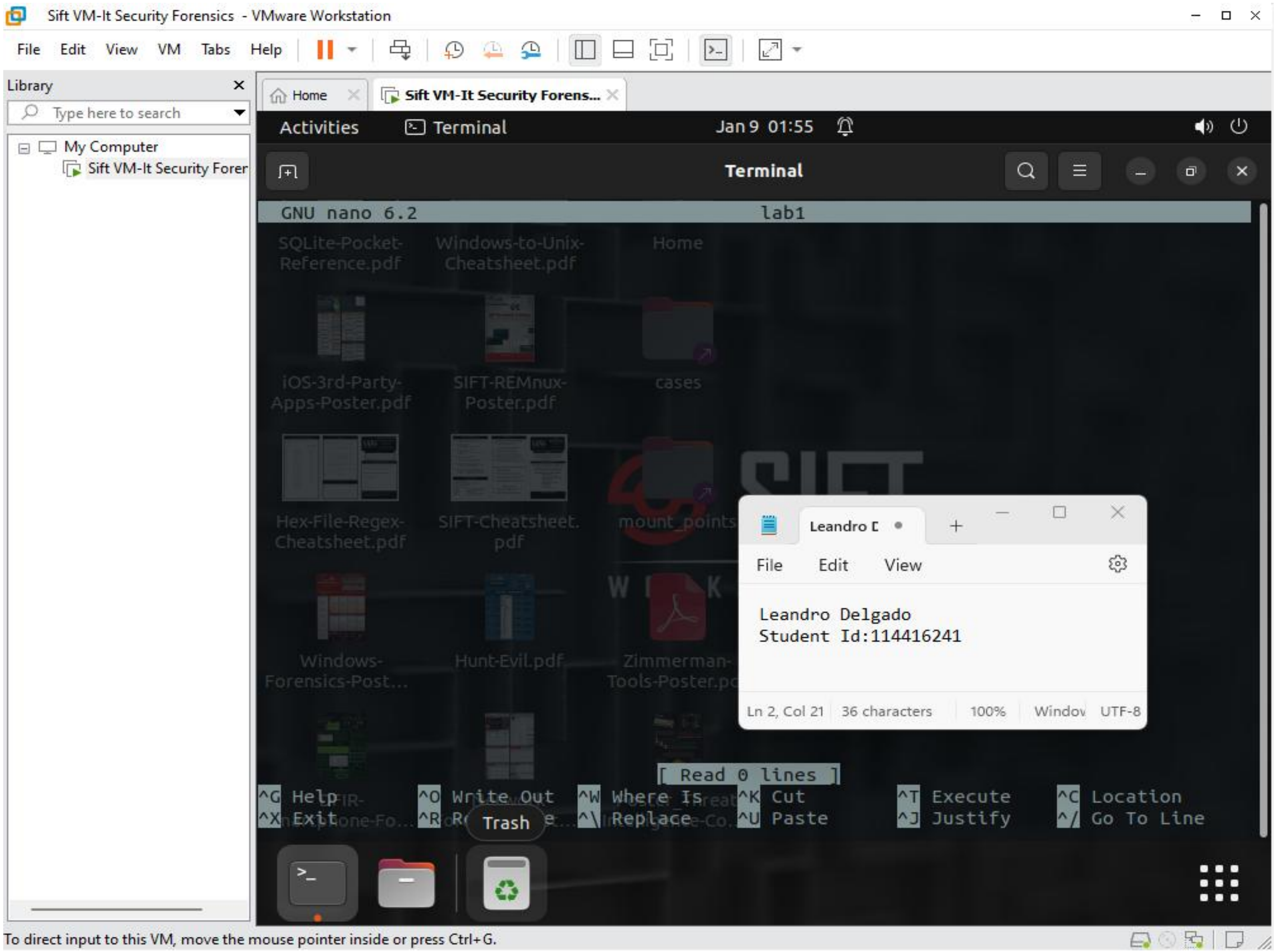
Sift VM-It Security Forensics - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
Sift VM-It Security Forer
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 01:56
Terminal

```
sansforensics@siftworkstation: ~
$ cd
sansforensics@siftworkstation: ~
$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
sansforensics@siftworkstation: ~
$ pwd
/home/sansforensics
sansforensics@siftworkstation: ~
$ touch lab1
sansforensics@siftworkstation: ~
$ nano lab1
sansforensics@siftworkstation: ~
$
```

Leandro Delgado
Student Id:114416241

Ln 2, Col 21
36 characters
100%
Windov
UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Figure 6- Vm Sift security Forensics basic Linux commands.

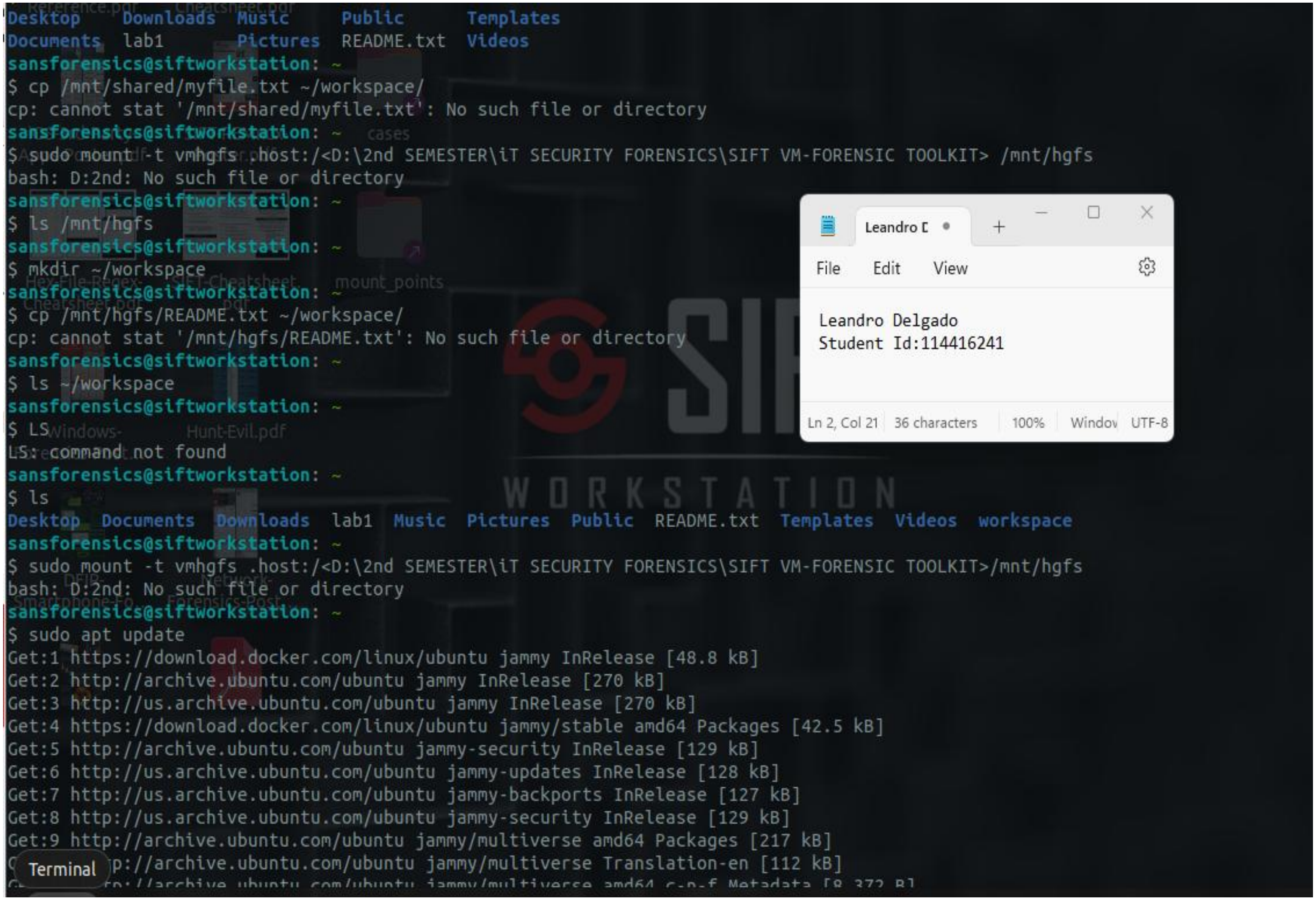

Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Sift VM-It Security Forer
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 01:55
Terminal
Trash
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
GNU nano 6.2                                        lab1

                                         [ Read 0 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

```
Leandro Delgado
Student Id:114416241
```

Ln 2, Col 21 | 36 characters | 100% | Windov | UTF-8

Figure 7- Vm Sift security Forensics basic Linux commands.

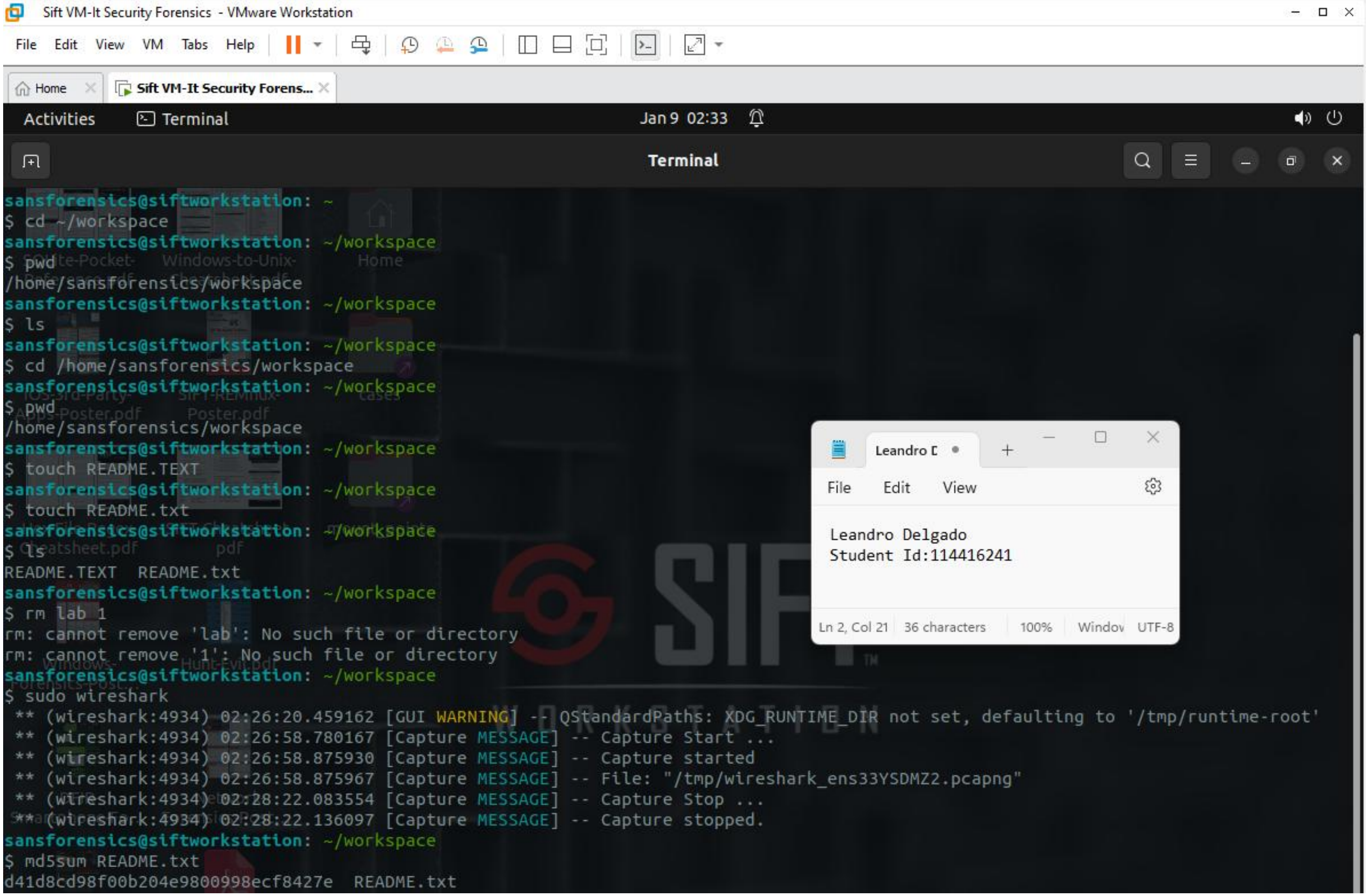


```
Desktop    Downloads  Music      Public      Templates
Documents  lab1       Pictures   README.txt  Videos
sansforensics@siftworkstation: ~
$ cp /mnt/shared/myfile.txt ~/workspace/
cp: cannot stat '/mnt/shared/myfile.txt': No such file or directory
sansforensics@siftworkstation: ~
$ sudo mount -t vmhgfs .host:/<D:\2nd SEMESTER\iT SECURITY FORENSICS\SIFT VM-FORENSIC TOOLKIT> /mnt/hgfs
bash: D:2nd: No such file or directory
sansforensics@siftworkstation: ~
$ ls /mnt/hgfs
sansforensics@siftworkstation: ~
$ mkdir ~/workspace
sansforensics@siftworkstation: ~
$ cp /mnt/hgfs/README.txt ~/workspace/
cp: cannot stat '/mnt/hgfs/README.txt': No such file or directory
sansforensics@siftworkstation: ~
$ ls ~/workspace
sansforensics@siftworkstation: ~
$ LS
LS: command not found
sansforensics@siftworkstation: ~
$ ls
Desktop  Documents  Downloads  lab1  Music  Pictures  Public  README.txt  Templates  Videos  workspace
sansforensics@siftworkstation: ~
$ sudo mount -t vmhgfs .host:/<D:\2nd SEMESTER\iT SECURITY FORENSICS\SIFT VM-FORENSIC TOOLKIT>/mnt/hgfs
bash: D:2nd: No such file or directory
sansforensics@siftworkstation: ~
$ sudo apt update
Get:1 https://download.docker.com/linux/ubuntu jammy InRelease [48.8 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:4 https://download.docker.com/linux/ubuntu jammy/stable amd64 Packages [42.5 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
G          p://archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
G      tp://archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8,372 B]
```

Leandro Delgado
Student Id:114416241

Figure 8- Vm Sift security Forensics basic Linux commands.

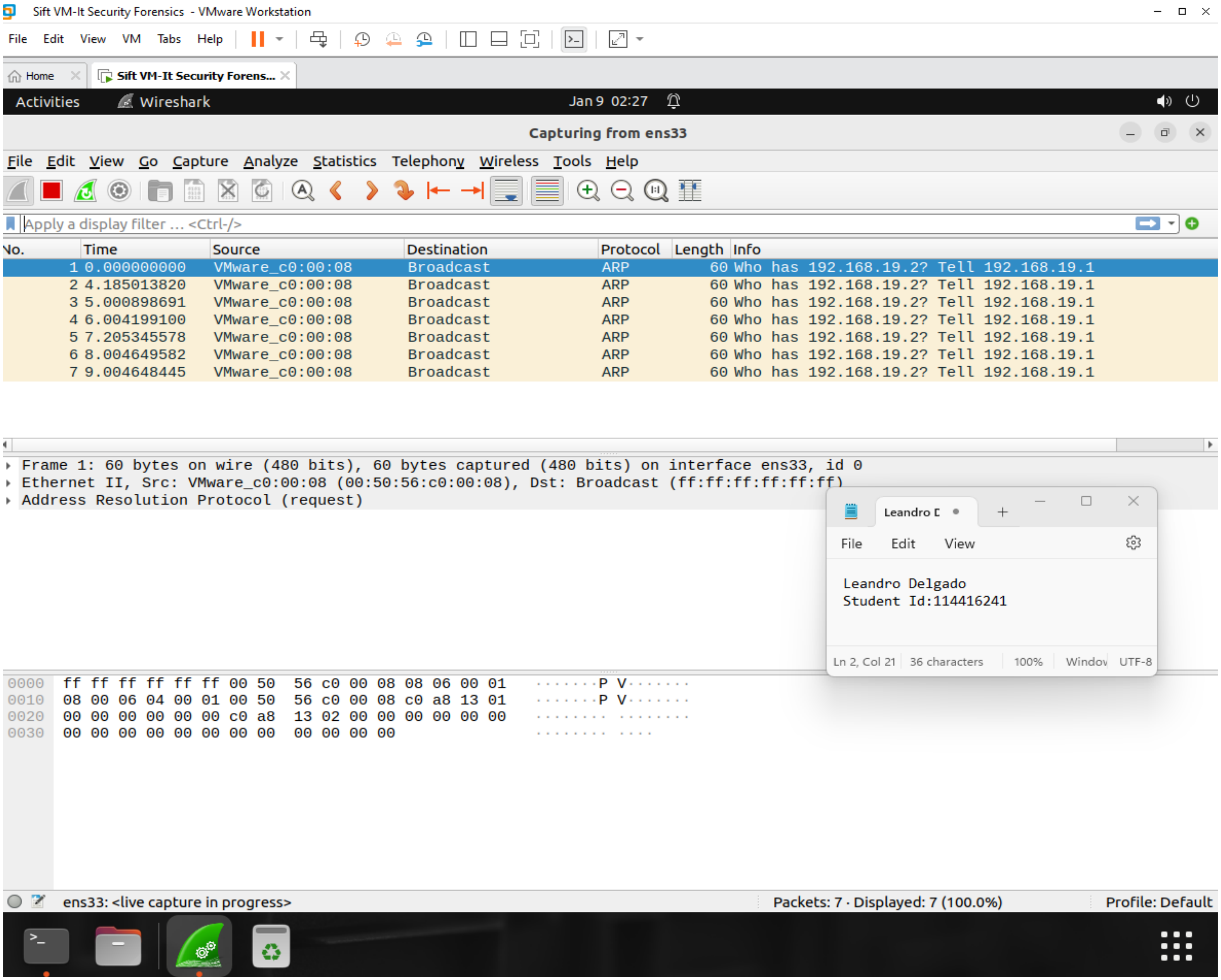
Screenshots of the tools & utilities you used in your workspace (at least 2 tools)



```
sansforensics@siftworkstation: ~
$ cd ~/workspace
sansforensics@siftworkstation: ~/workspace
$ pwd
/home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ ls
sansforensics@siftworkstation: ~/workspace
$ cd /home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ pwd
/home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ touch README.TEXT
sansforensics@siftworkstation: ~/workspace
$ touch README.txt
sansforensics@siftworkstation: ~/workspace
$ ls
README.TEXT  README.txt
sansforensics@siftworkstation: ~/workspace
$ rm lab 1
rm: cannot remove 'lab': No such file or directory
rm: cannot remove '1': No such file or directory
sansforensics@siftworkstation: ~/workspace
$ sudo wireshark
 ** (wireshark:4934) 02:26:20.459162 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:4934) 02:26:58.780167 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:4934) 02:26:58.875930 [Capture MESSAGE] -- Capture started
 ** (wireshark:4934) 02:26:58.875967 [Capture MESSAGE] -- File: "/tmp/wireshark_ens33YSDMZ2.pcapng"
 ** (wireshark:4934) 02:28:22.083554 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:4934) 02:28:22.136097 [Capture MESSAGE] -- Capture stopped.
sansforensics@siftworkstation: ~/workspace
$ md5sum README.txt
d41d8cd98f00b204e9800998ecf8427e  README.txt
```

Leandro Delgado
Student Id:114416241

Figure 8- Vm Sift security Forensics tools/ Wireshark.


Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Wireshark
Jan 9 02:27
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Leandro D
File Edit View
Ln 2, Col 21 36 characters 100% Window UTF-8

```
No.  Time         Source            Destination  Protocol  Length  Info
   1 0.000000000  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   2 4.185013820  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   3 5.000898691  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   4 6.004199100  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   5 7.205345578  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   6 8.004649582  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
   7 9.004648445  VMware_c0:00:08   Broadcast    ARP           60  Who has 192.168.19.2? Tell 192.168.19.1
```

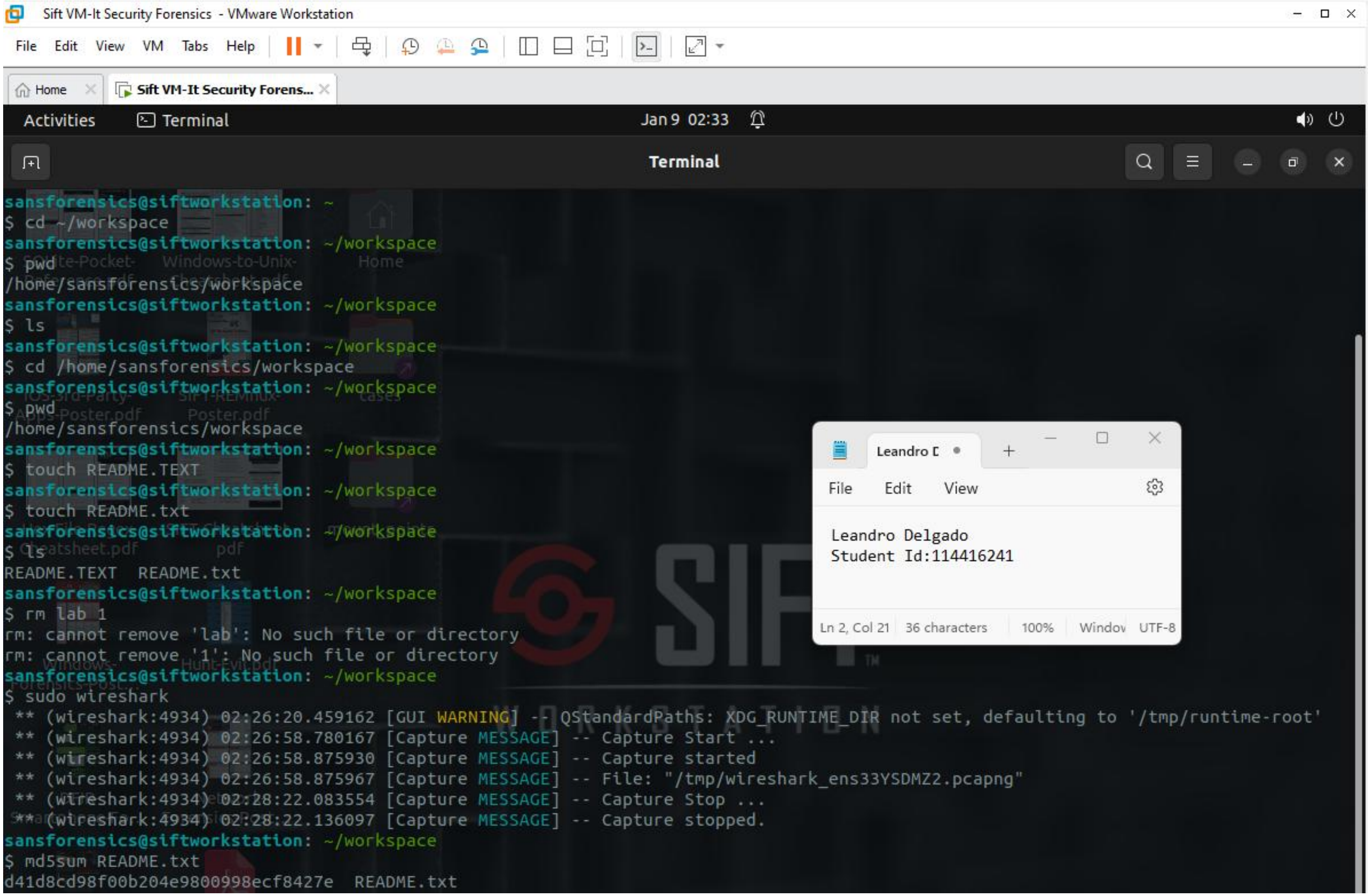
```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens33, id 0
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   ·······P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0 a8 13 01   ·······P V·······
0020  00 00 00 00 00 00 c0 a8  13 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

```
Leandro Delgado
Student Id:114416241
```

```
ens33: <live capture in progress>        Packets: 7 · Displayed: 7 (100.0%)        Profile: Default
```

Figure 9- Vm Sift security Forensics tools/ Wireshark.

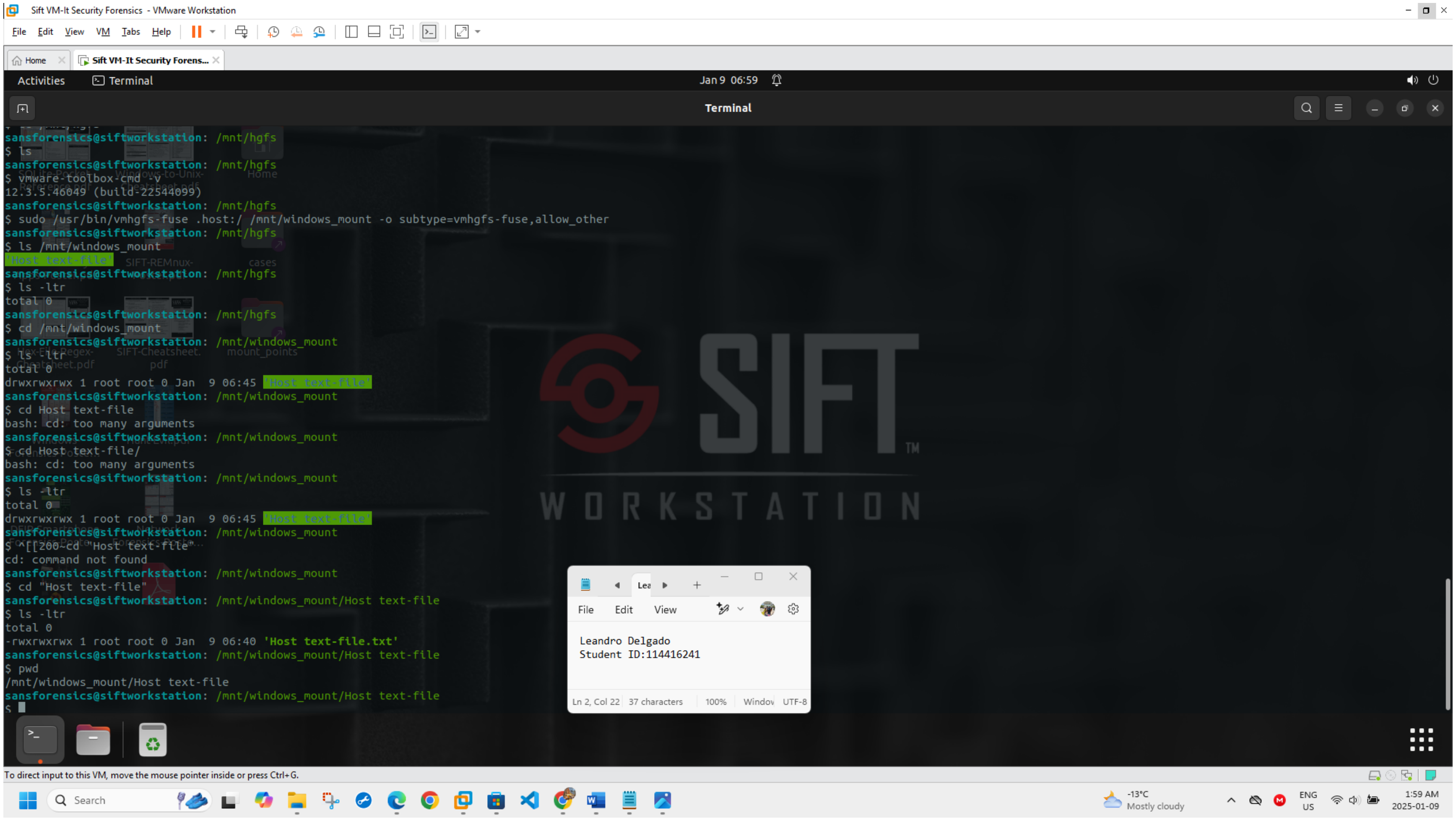


```
sansforensics@siftworkstation: ~
$ cd ~/workspace
sansforensics@siftworkstation: ~/workspace
$ pwd
/home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ ls
sansforensics@siftworkstation: ~/workspace
$ cd /home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ pwd
/home/sansforensics/workspace
sansforensics@siftworkstation: ~/workspace
$ touch README.TEXT
sansforensics@siftworkstation: ~/workspace
$ touch README.txt
sansforensics@siftworkstation: ~/workspace
$ ls
README.TEXT  README.txt
sansforensics@siftworkstation: ~/workspace
$ rm lab 1
rm: cannot remove 'lab': No such file or directory
rm: cannot remove '1': No such file or directory
sansforensics@siftworkstation: ~/workspace
$ sudo wireshark
 ** (wireshark:4934) 02:26:20.459162 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:4934) 02:26:58.780167 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:4934) 02:26:58.875930 [Capture MESSAGE] -- Capture started
 ** (wireshark:4934) 02:26:58.875967 [Capture MESSAGE] -- File: "/tmp/wireshark_ens33YSDMZ2.pcapng"
 ** (wireshark:4934) 02:28:22.083554 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:4934) 02:28:22.136097 [Capture MESSAGE] -- Capture stopped.
sansforensics@siftworkstation: ~/workspace
$ md5sum README.txt
d41d8cd98f00b204e9800998ecf8427e  README.txt
```

Leandro Delgado
Student Id:114416241

Figure 10- Vm Sift security Forensics tools/ md5sum.

Mounting process to test the Vm sift



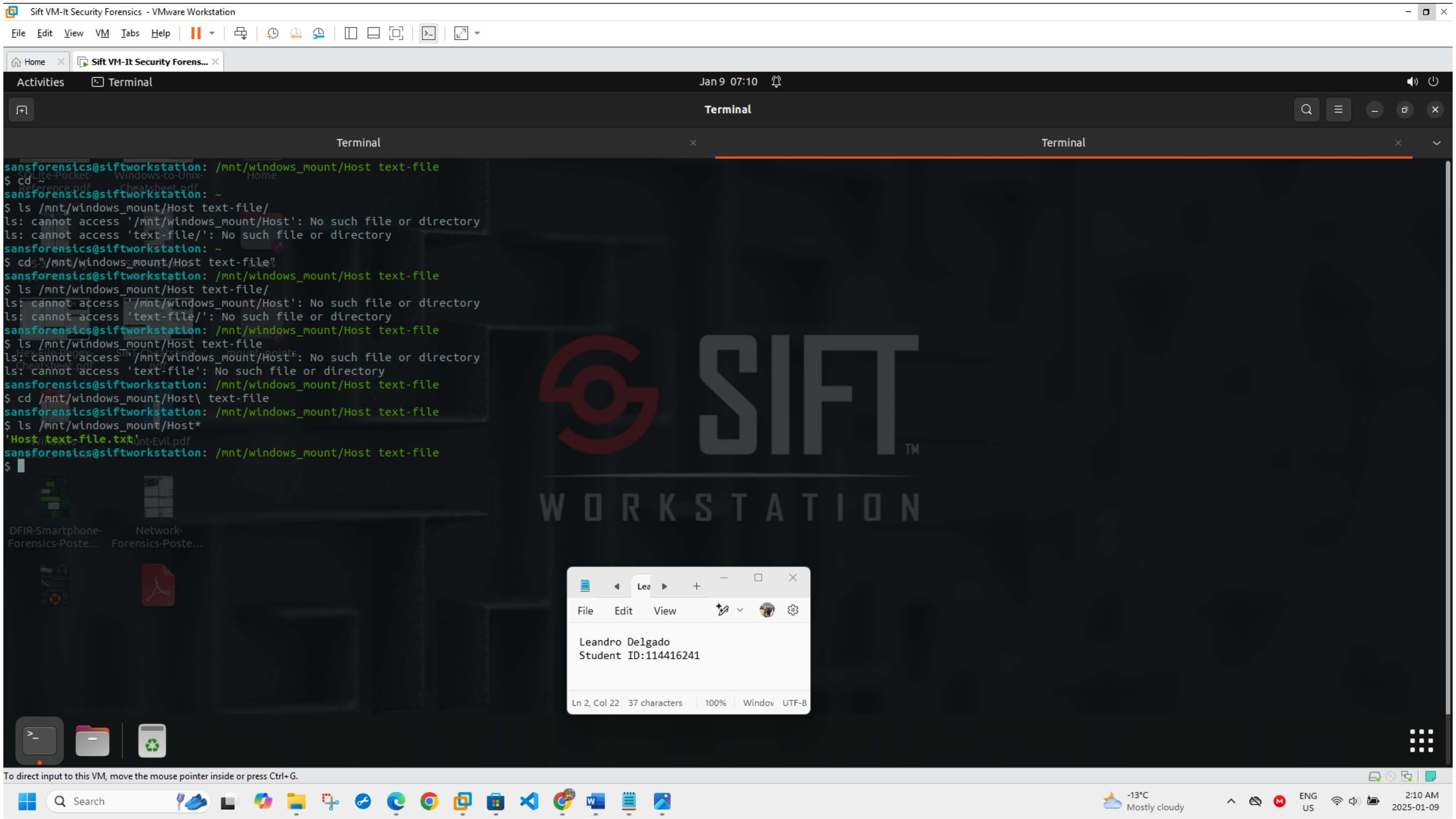
Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 06:59
Terminal
SIFT
WORKSTATION
File Edit View
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
-13°C
Mostly cloudy
ENG
US
1:59 AM
2025-01-09

```
sansforensics@siftworkstation: /mnt/hgfs
$ ls
sansforensics@siftworkstation: /mnt/hgfs
$ vmware-toolbox-cmd -v
12.3.5.46049 (build-22544099)
sansforensics@siftworkstation: /mnt/hgfs
$ sudo /usr/bin/vmhgfs-fuse .host:/ /mnt/windows_mount -o subtype=vmhgfs-fuse,allow_other
sansforensics@siftworkstation: /mnt/hgfs
$ ls /mnt/windows_mount
'Host text-file'
sansforensics@siftworkstation: /mnt/hgfs
$ ls -ltr
total 0
sansforensics@siftworkstation: /mnt/hgfs
$ cd /mnt/windows_mount
sansforensics@siftworkstation: /mnt/windows_mount
$ ls -ltr
total 0
drwxrwxrwx 1 root root 0 Jan  9 06:45 'Host text-file'
sansforensics@siftworkstation: /mnt/windows_mount
$ cd Host text-file
bash: cd: too many arguments
sansforensics@siftworkstation: /mnt/windows_mount
$ cd Host text-file/
bash: cd: too many arguments
sansforensics@siftworkstation: /mnt/windows_mount
$ ls -ltr
total 0
drwxrwxrwx 1 root root 0 Jan  9 06:45 'Host text-file'
sansforensics@siftworkstation: /mnt/windows_mount
$ ^[[200~cd "Host text-file"
cd: command not found
sansforensics@siftworkstation: /mnt/windows_mount
$ cd "Host text-file"
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ ls -ltr
total 0
-rwxrwxrwx 1 root root 0 Jan  9 06:40 'Host text-file.txt'
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ pwd
/mnt/windows_mount/Host text-file
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ 
```

```
Leandro Delgado
Student ID:114416241
```

Ln 2, Col 22 | 37 characters | 100% | Windov | UTF-8

Figure 10- Vm Sift security Forensics tools/ md5sum.



```
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ cd ~
sansforensics@siftworkstation: ~
$ ls /mnt/windows_mount/Host text-file/
ls: cannot access '/mnt/windows_mount/Host': No such file or directory
ls: cannot access 'text-file/': No such file or directory
sansforensics@siftworkstation: ~
$ cd "/mnt/windows_mount/Host text-file"
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ ls /mnt/windows_mount/Host text-file/
ls: cannot access '/mnt/windows_mount/Host': No such file or directory
ls: cannot access 'text-file/': No such file or directory
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ ls /mnt/windows_mount/Host text-file
ls: cannot access '/mnt/windows_mount/Host': No such file or directory
ls: cannot access 'text-file': No such file or directory
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ cd /mnt/windows_mount/Host\ text-file
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ ls /mnt/windows_mount/Host*
'Host text-file.txt'
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ 
```

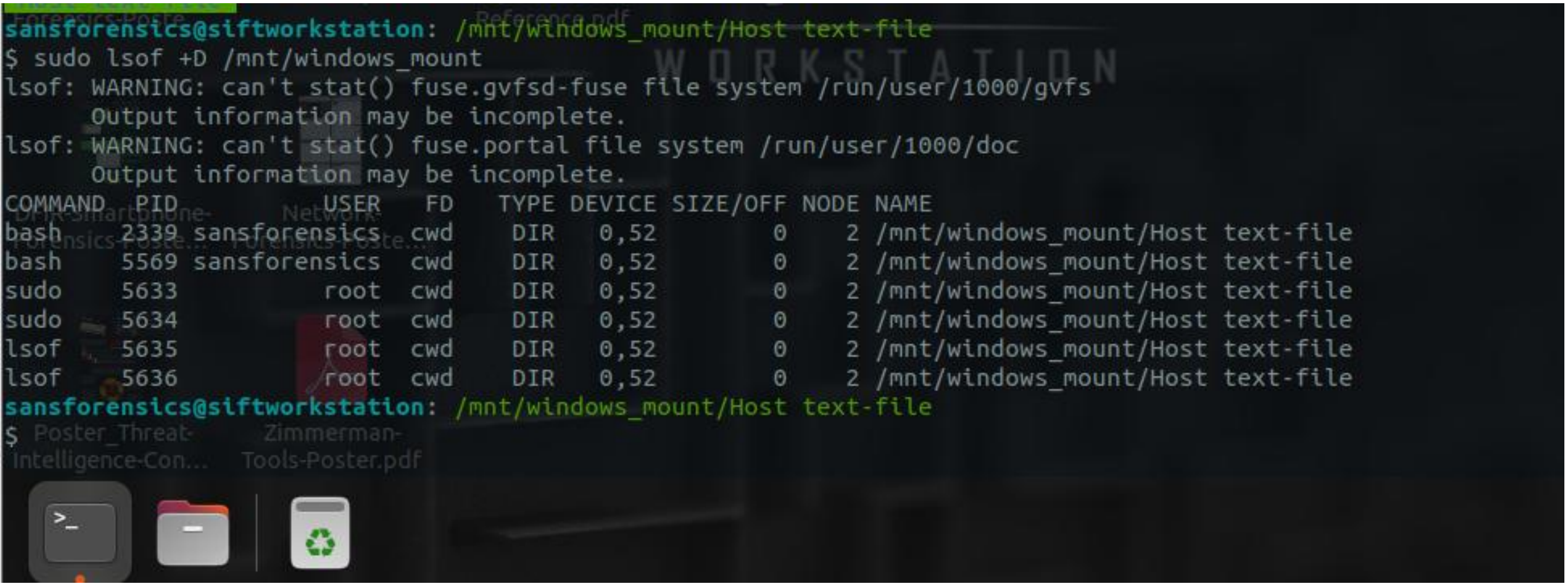
Leandro Delgado
Student ID:114416241

Sift VM-It Security Forensics - VMware Workstation
File Edit View VM Tabs Help
Home
Sift VM-It Security Forens...
Activities
Terminal
Jan 9 07:10
Terminal
Terminal
Terminal
SIFT
WORKSTATION
File Edit View
Ln 2, Col 22
37 characters
100%
Windov
UTF-8
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
-13°C
Mostly cloudy
ENG
US
2:10 AM
2025-01-09

Figure 11- Vm Sift security Forensics tools/ md5sum.

Unmounting process to test the Vm sift.

The image below shows the list of active process that are using the directory on the bash process. This process was preventing to unmounting the directory. So, using the command [sudo fuser -km /mnt/windows_mount/Host\ text-file] im killing all the process to proceed to unmount the folder using the command [sudo umount /mnt/windows_mount]. After this, the folder is unmounted.



```
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$ sudo lsof +D /mnt/windows_mount
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1000/doc
      Output information may be incomplete.
COMMAND  PID         USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
bash    2339 sansforensics  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
bash    5569 sansforensics  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
sudo    5633          root  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
sudo    5634          root  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
lsof    5635          root  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
lsof    5636          root  cwd    DIR   0,52        0    2 /mnt/windows_mount/Host text-file
sansforensics@siftworkstation: /mnt/windows_mount/Host text-file
$
```

Figure 12- Vm Sift security Forensics tools/ md5sum.

Description of the tools used during the test:

1. **Wireshark** is a powerful tool that helps people monitor and analyze network traffic. It allows you to capture data as it moves across the network, which is useful for troubleshooting issues or spotting security concerns.
2. **Md5sum**, on the other hand, helps you ensure that files haven't been altered. By generating a unique hash value for a file, you can easily check if it's been changed or corrupted by comparing the hash to the original one.