

Setting Up the Digital Forensic Lab

Our first task is to set up our digital forensic lab environment. We're instructed to install Oracle VM VirtualBox but I already have the vmware, so I used that to set up an Ubuntu virtual machine (VM). Here's the process I followed:

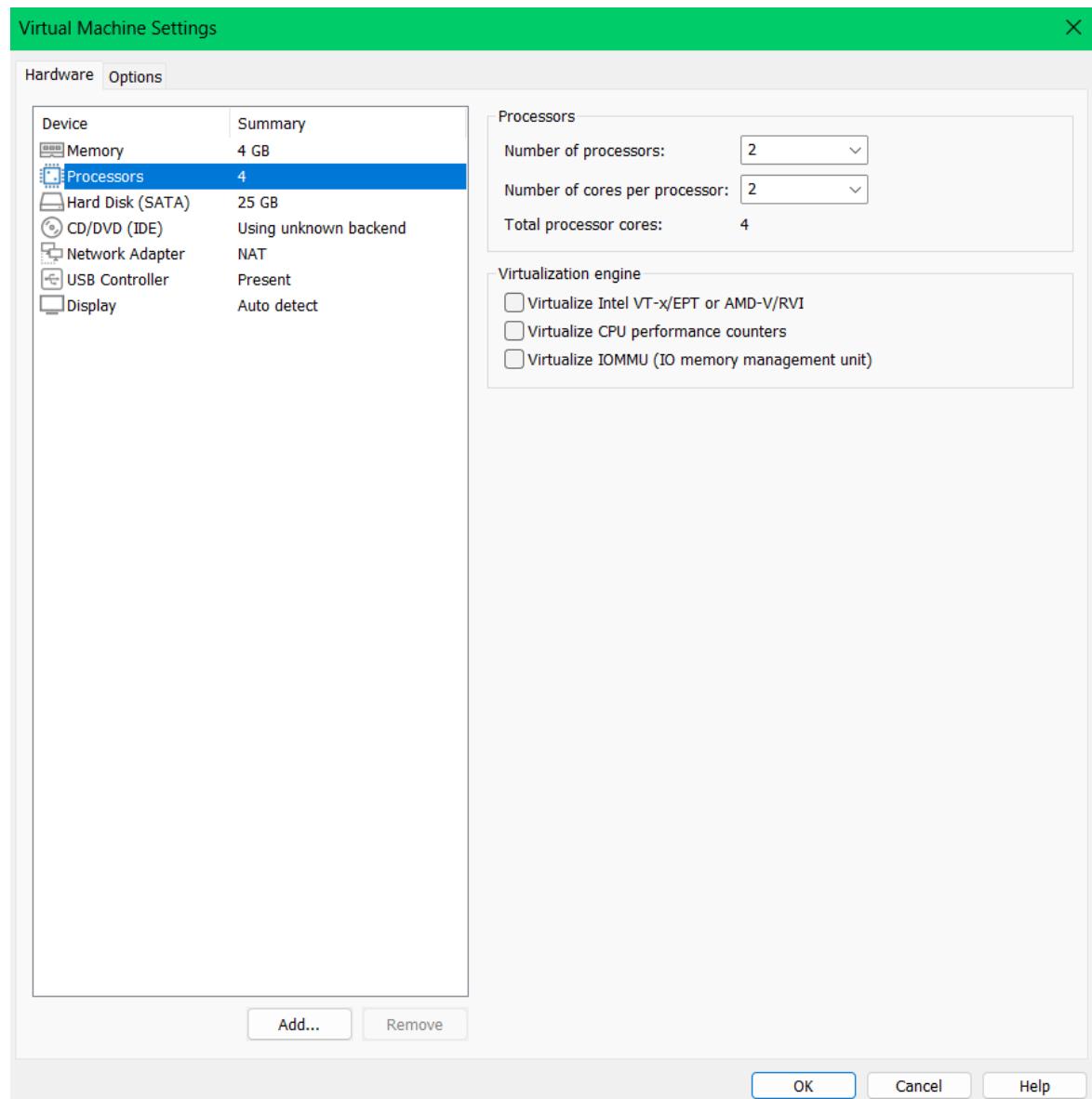
Download the Ubuntu VM: I then downloaded the virtual machine using the provided link and code

android-x86_64-9.0-r2.iso	4/22/2024 12:20 AM	Disc Image File	943,104 KB
DF.ova	6/5/2024 9:56 AM	Open Virtualizatio...	7,115,671 ...
kali-linux-2024.1-installer-purple-amd64	3/1/2024 12:34 AM	Disc Image File	4,042,896

Import the Ubuntu VM:

Then I simply right clicked the DF.ova file and opened it with the vmware. It got set up automatically in the vmware. I only had to configure the network and processor settings.

Processors



Network adapter

Virtual Machine Settings X

Hardware Options

Device	Summary
Memory	4 GB
Processors	4
Hard Disk (SATA)	25 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	NAT
USB Controller	Present
Display	Auto detect

Device status

Connected
 Connect at power on

Network connection

Bridged: Connected directly to the physical network
 Replicate physical network connection state

NAT: Used to share the host's IP address
 Host-only: A private network shared with the host
 Custom: Specific virtual network
VMnet0

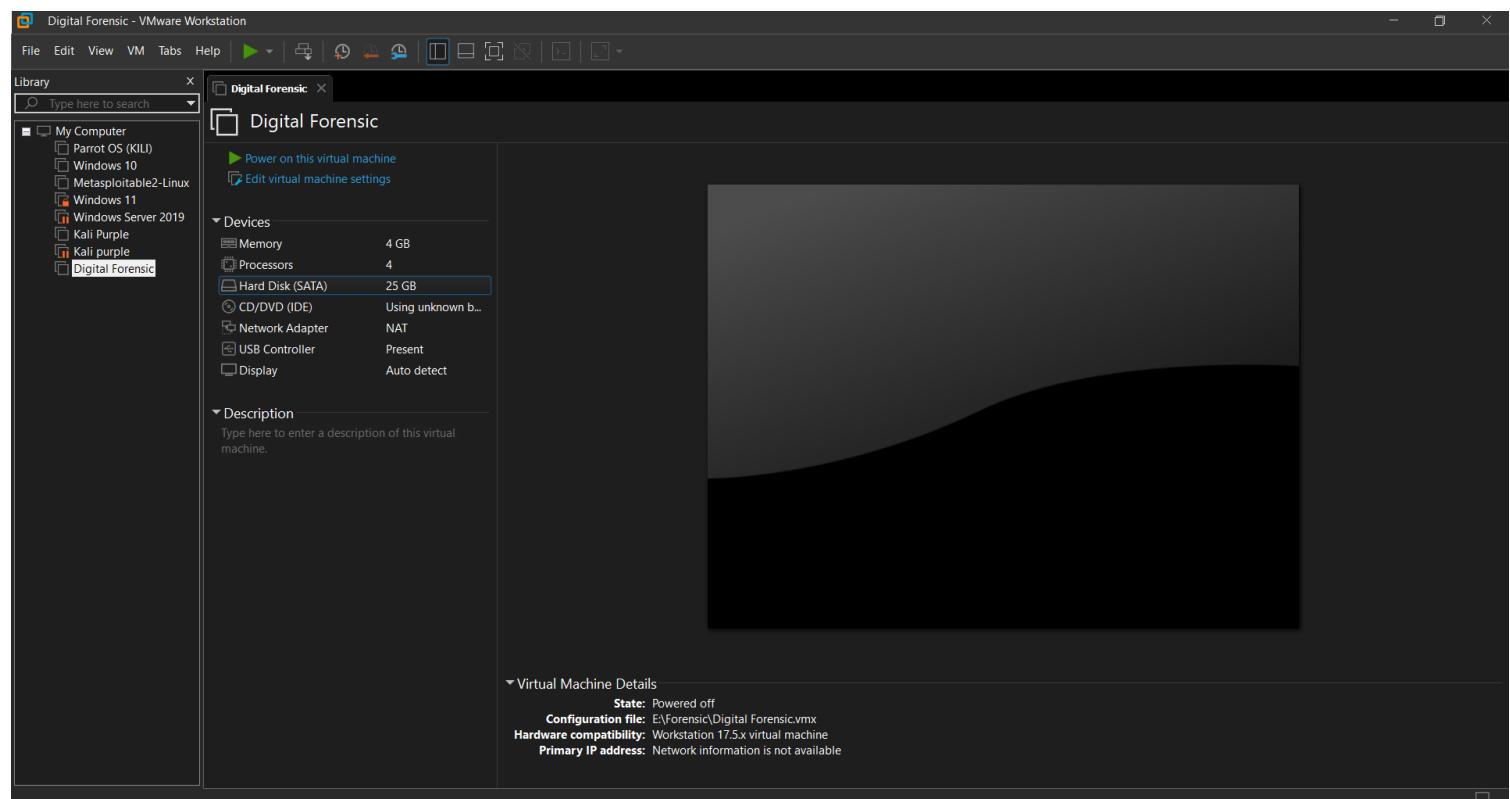
LAN segment:
[dropdown menu]

LAN Segments... Advanced...

Add... Remove

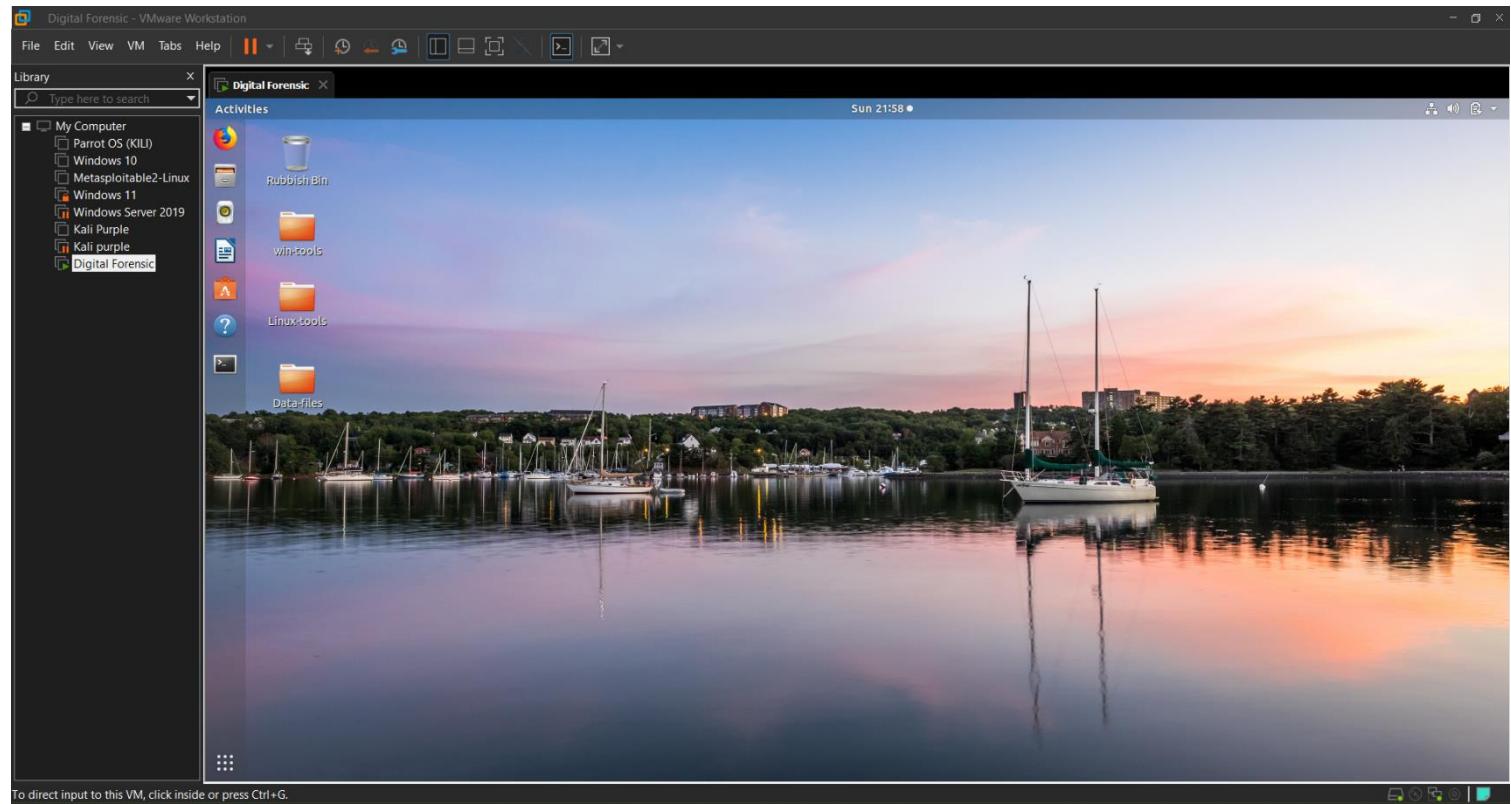
OK Cancel Help

After completing these steps, the Ubuntu virtual machine successfully appeared in Vmware



Running the Virtual Machine

Next, I selected the Ubuntu VM and clicked the green **Start** arrow to boot it up. It launched smoothly without requiring a password. I explored the pre-installed programs like Firefox, file explorer, and the terminal, which were pinned to the left-side Docker.



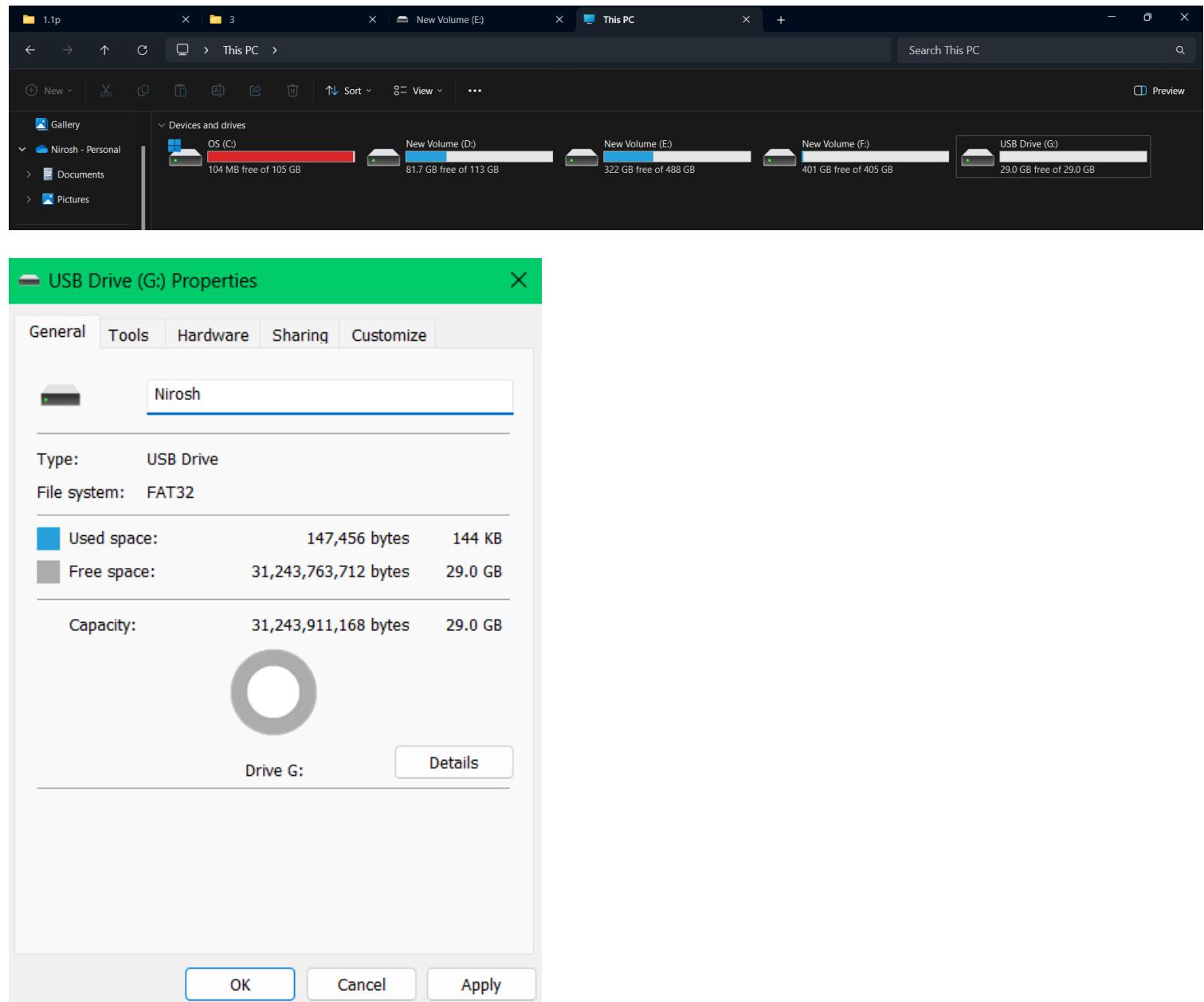
Accessing Personal Files

Vmware allows file sharing between the host and the virtual machine in several ways:

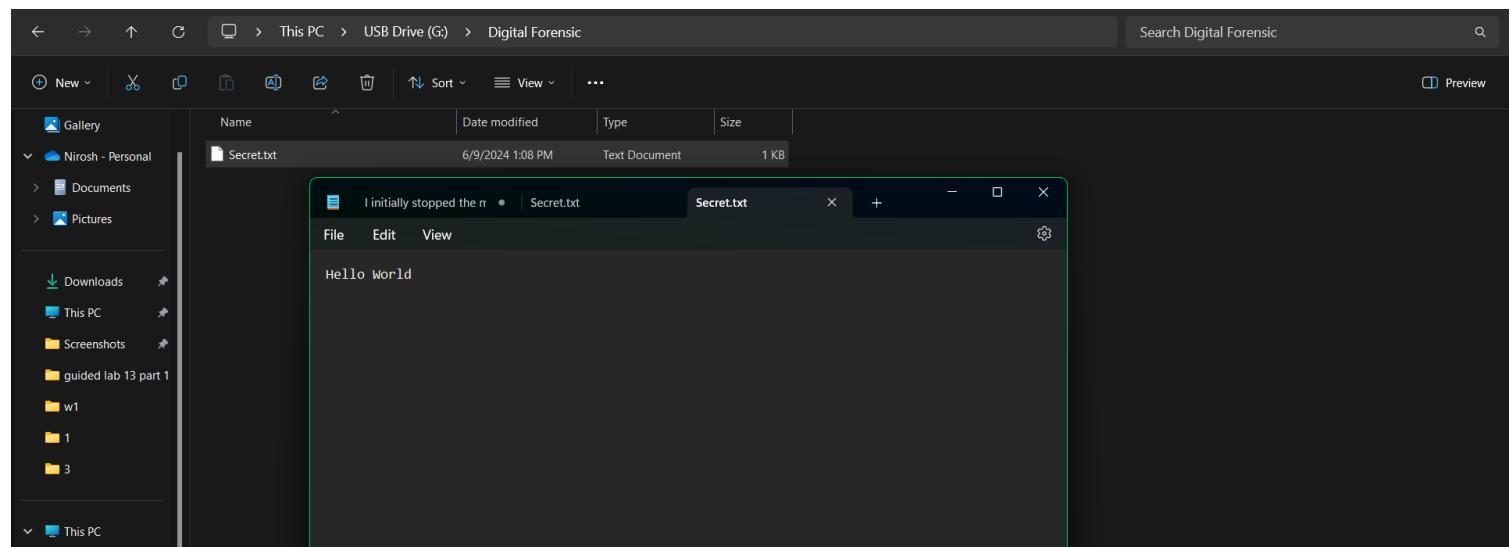
Using a USB Drive:

I Copied files from one system and pasted them to another system. I Ensured that the USB is formatted in FAT32 or ex-FAT.

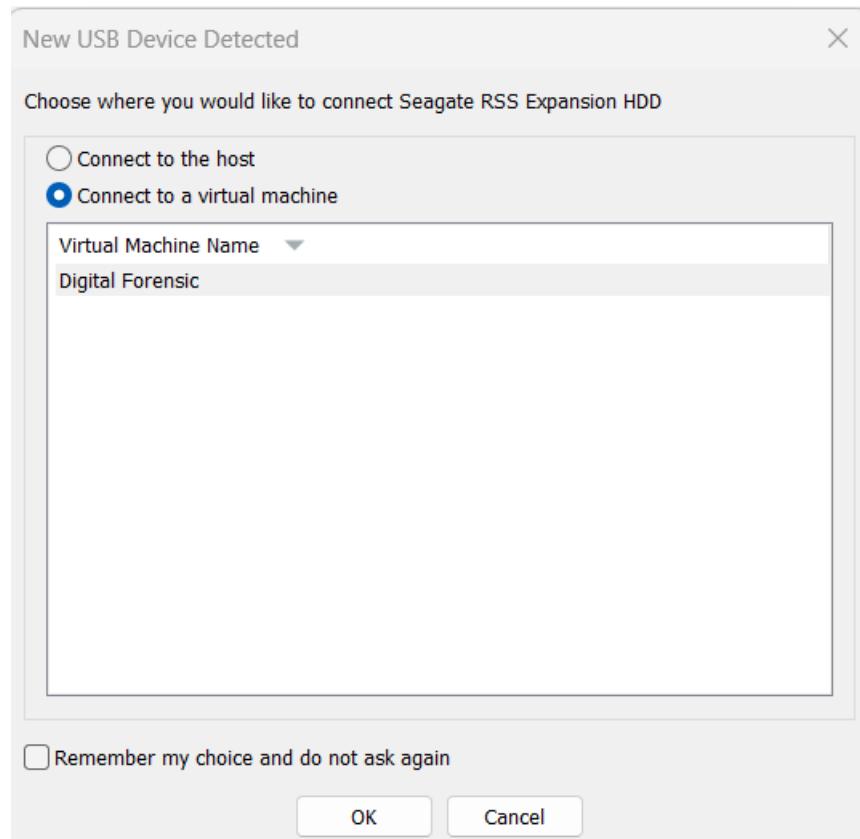
I first mounted the pendrive (USB Drive G:) to my main machine (Windows) to check the file format (FATT32) and added a text file inside called **secret**.



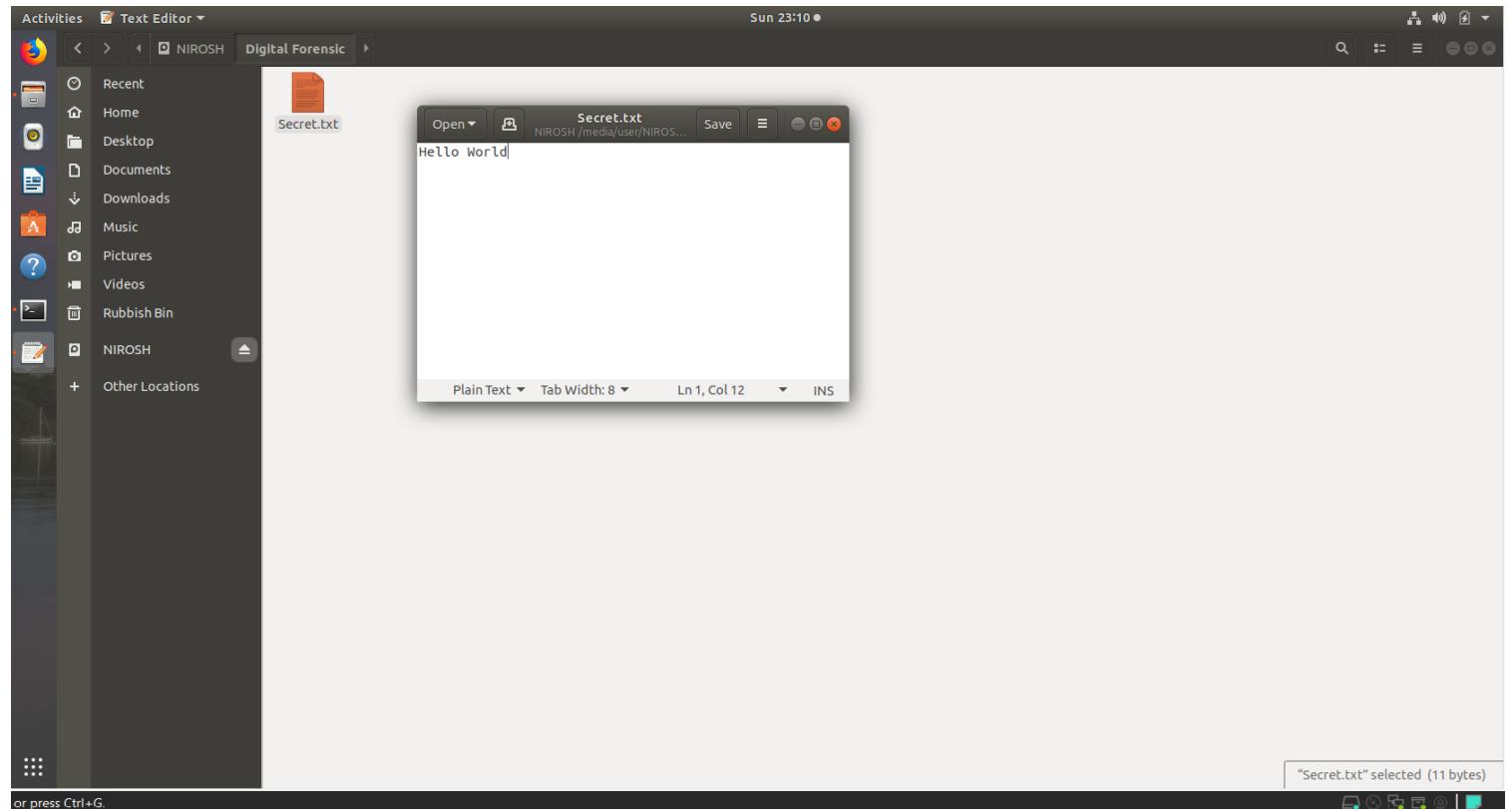
Inside the Secret.txt file I typed a message “Hello World”



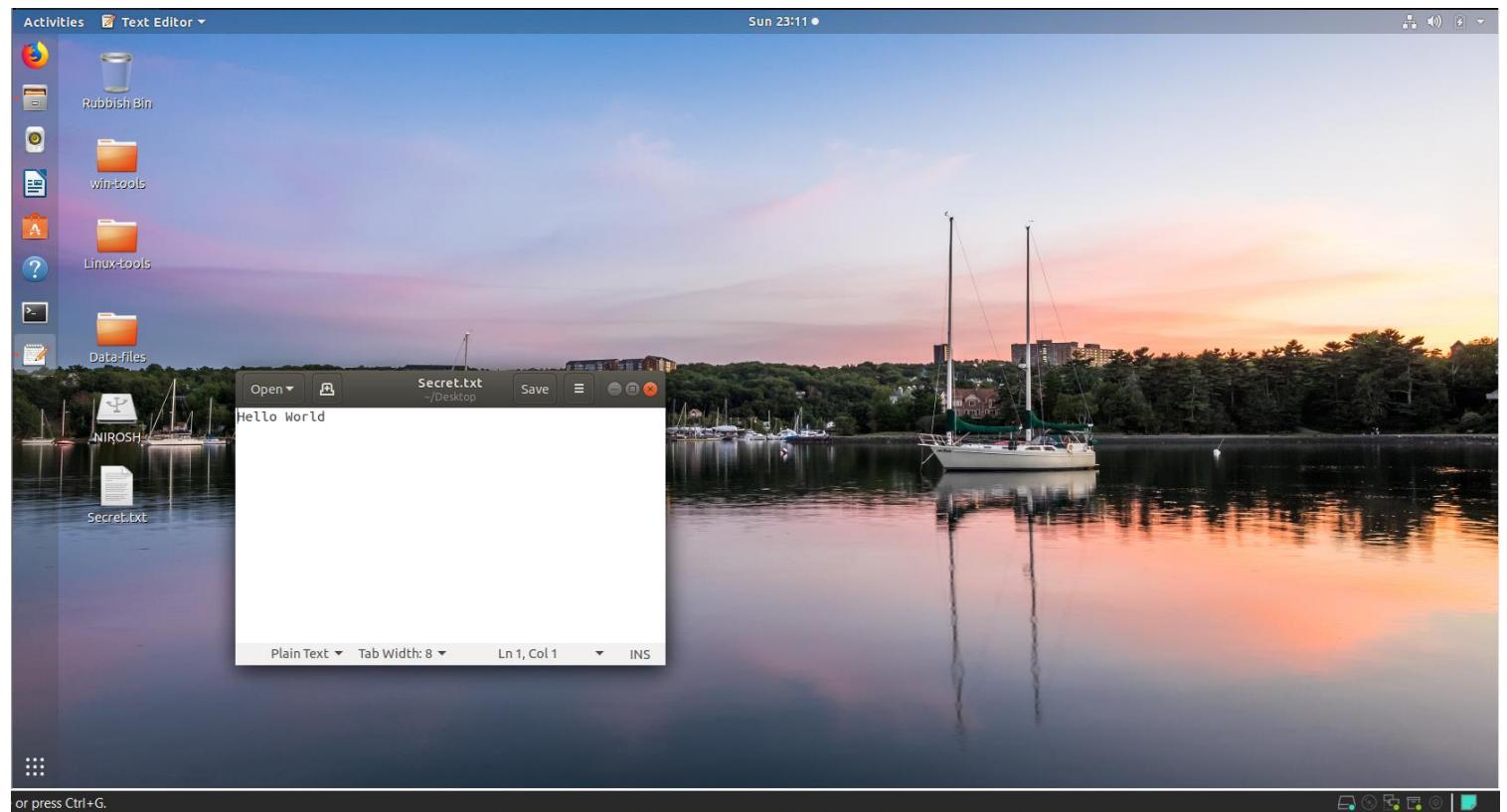
Now I ejected it from my main machine and mounted the drive to Ubuntu VM.



Then I navigated to the mounted drive and opened the text file I created and found the same text I typed in my main machine.



Now I copied the text file to my Ubuntu VM to check whether file sharing through USB works

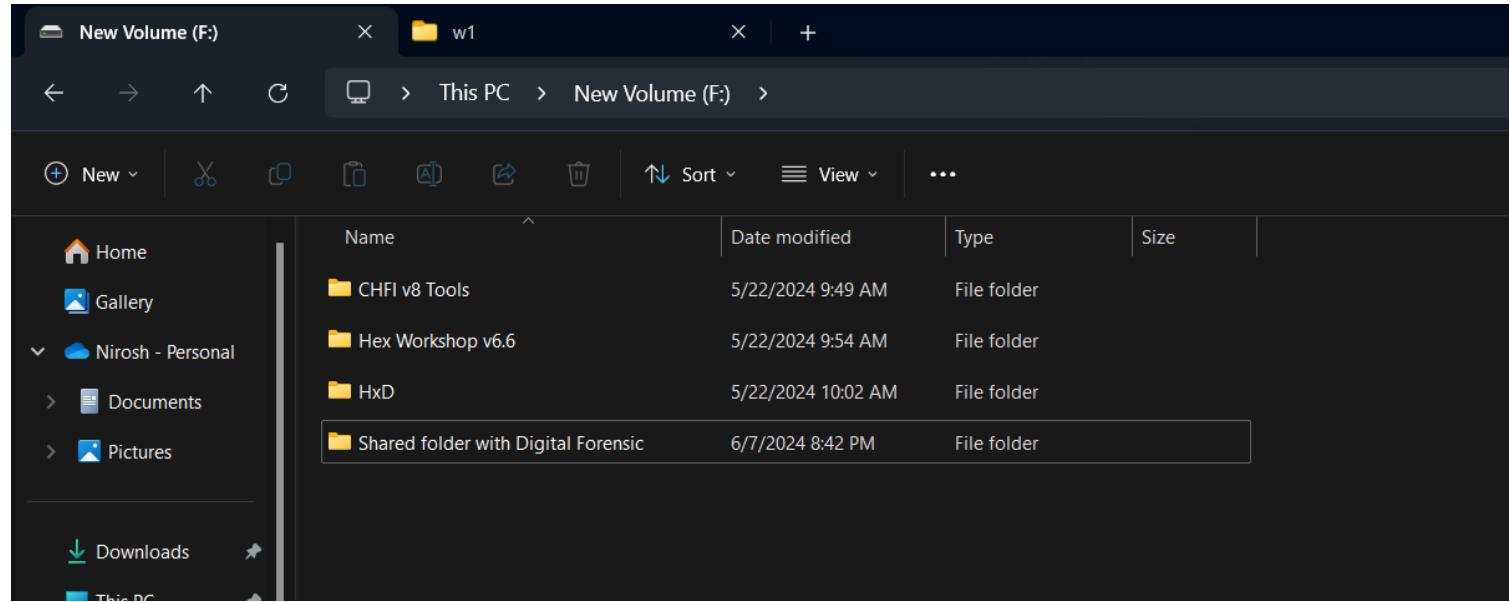


I pasted that file to my ubuntu VM and opened it, it shows the same text which means file sharing through USB works.

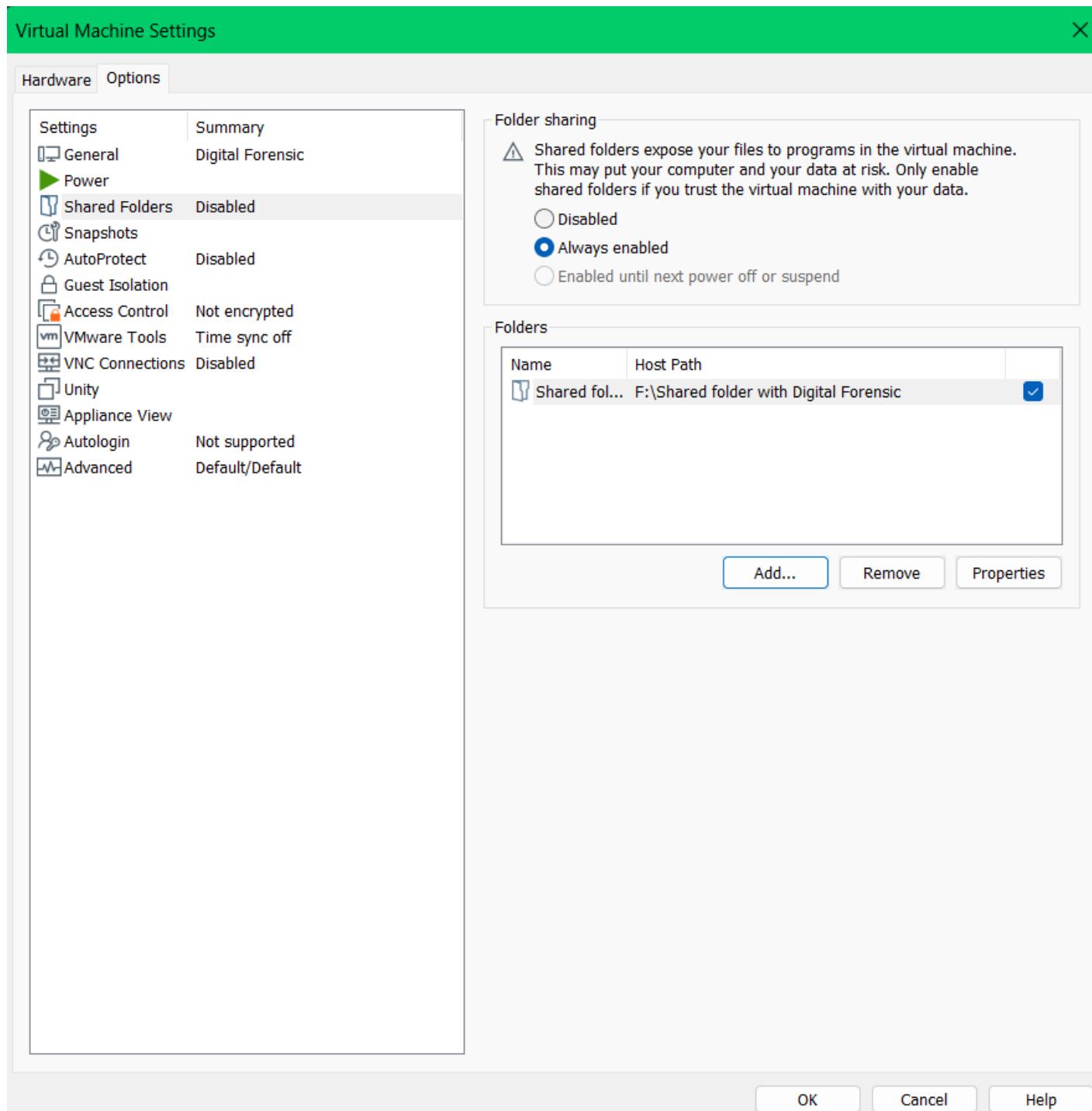
Directory Sharing

Now I want to share folder from the host machine to the ubuntu VM.

For that I first created a directory called **Shared folder with Digital Forensic**, this is the file path I created the folder in my host machine **F:\Shared folder with Digital Forensic**.

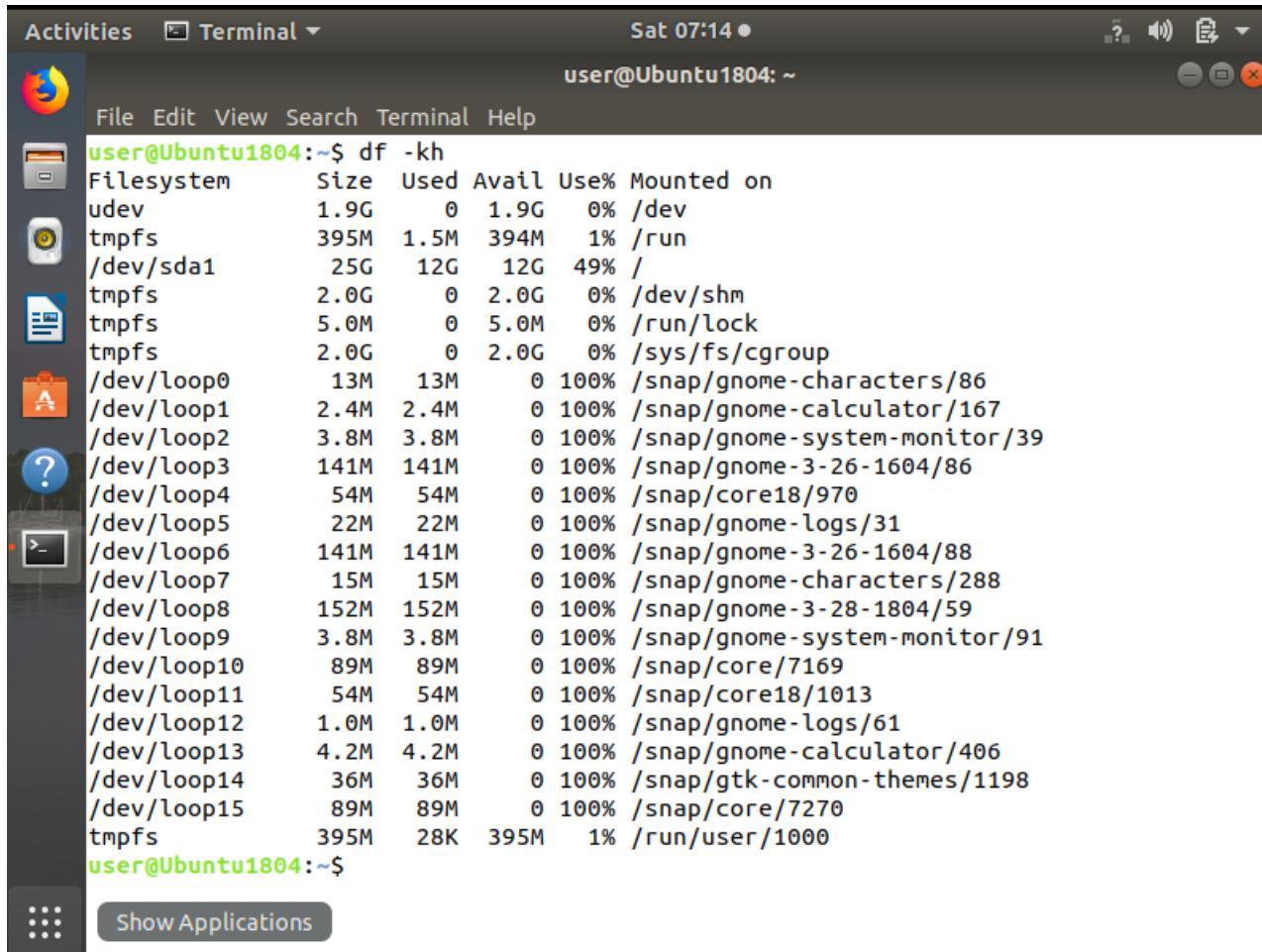


Now I configured the VM in order to allow folder sharing with the host machine. I also gave the destination of the directory to be shared with the VM.



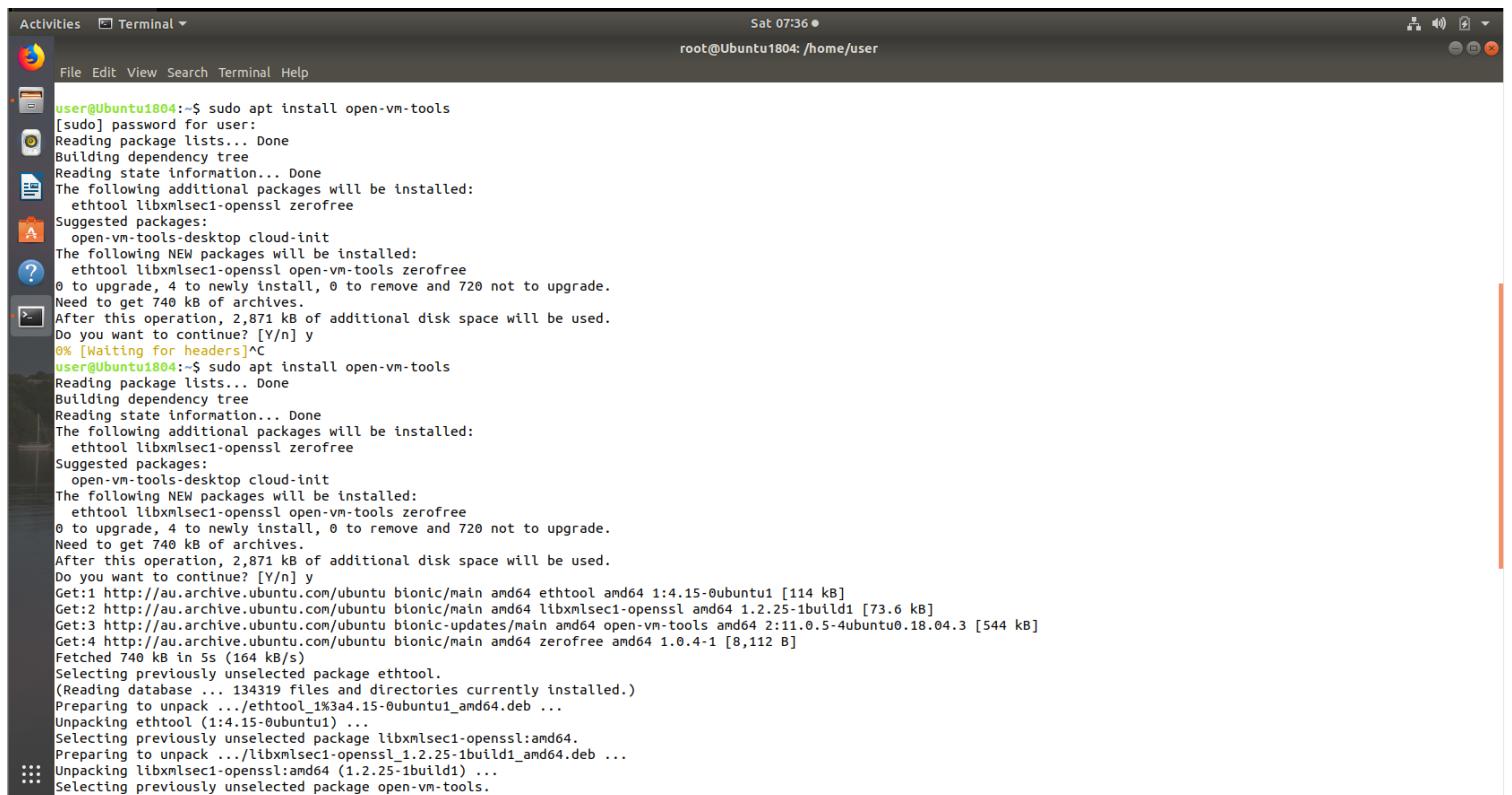
Now I switch on the VM and run some set of commands to mount the shared folder with the Ubuntu VM.

First, I run the **df -kh** command to check whether the folder is mounted, but it is not mounted yet, so we have to do it manually.



```
Activities Terminal Sat 07:14 ● user@Ubuntu1804: ~
File Edit View Search Terminal Help
user@Ubuntu1804:~$ df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G  0% /dev
tmpfs           395M  1.5M  394M  1% /run
/dev/sda1        25G   12G   12G  49% /
tmpfs           2.0G   0    2.0G  0% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
tmpfs           2.0G   0    2.0G  0% /sys/fs/cgroup
/dev/loop0       13M   13M   0  100% /snap/gnome-characters/86
/dev/loop1       2.4M  2.4M   0  100% /snap/gnome-calculator/167
/dev/loop2       3.8M  3.8M   0  100% /snap/gnome-system-monitor/39
/dev/loop3       141M  141M   0  100% /snap/gnome-3-26-1604/86
/dev/loop4       54M   54M   0  100% /snap/core18/970
/dev/loop5       22M   22M   0  100% /snap/gnome-logs/31
/dev/loop6       141M  141M   0  100% /snap/gnome-3-26-1604/88
/dev/loop7       15M   15M   0  100% /snap/gnome-characters/288
/dev/loop8       152M  152M   0  100% /snap/gnome-3-28-1804/59
/dev/loop9       3.8M  3.8M   0  100% /snap/gnome-system-monitor/91
/dev/loop10      89M   89M   0  100% /snap/core/7169
/dev/loop11      54M   54M   0  100% /snap/core18/1013
/dev/loop12      1.0M  1.0M   0  100% /snap/gnome-logs/61
/dev/loop13      4.2M  4.2M   0  100% /snap/gnome-calculator/406
/dev/loop14      36M   36M   0  100% /snap/gtk-common-themes/1198
/dev/loop15      89M   89M   0  100% /snap/core/7270
tmpfs           395M  28K   395M  1% /run/user/1000
user@Ubuntu1804:~$
```

So, for that, I first ran the **sudo apt install open-vm-tools**, the password prompt will be asked and I type it in. then the installation starts and ends automatically.



```
Activities Terminal Sat 07:36 ● root@Ubuntu1804: /home/user
File Edit View Search Terminal Help
root@Ubuntu1804:~$ sudo apt install open-vm-tools
[sudo] password for user:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ethtool libxmlsec1-openssl zerofree
Suggested packages:
open-vm-tools-desktop cloud-init
The following NEW packages will be installed:
ethtool libxmlsec1-openssl open-vm-tools zerofree
0 to upgrade, 4 to newly install, 0 to remove and 720 not to upgrade.
Need to get 740 kB of archives.
After this operation, 2,871 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Waiting for headers]~c
root@Ubuntu1804:~$ sudo apt install open-vm-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
ethtool libxmlsec1-openssl zerofree
Suggested packages:
open-vm-tools-desktop cloud-init
The following NEW packages will be installed:
ethtool libxmlsec1-openssl open-vm-tools zerofree
0 to upgrade, 4 to newly install, 0 to remove and 720 not to upgrade.
Need to get 740 kB of archives.
After this operation, 2,871 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://au.archive.ubuntu.com/ubuntu bionic/main amd64 ethtool amd64 1:4.15-0ubuntu1 [114 kB]
Get:2 http://au.archive.ubuntu.com/ubuntu bionic/main amd64 libxmlsec1-openssl amd64 1.2.25-1build1 [73.6 kB]
Get:3 http://au.archive.ubuntu.com/ubuntu bionic-updates/main amd64 open-vm-tools amd64 2:11.0.5-4ubuntu0.18.04.3 [544 kB]
Get:4 http://au.archive.ubuntu.com/ubuntu bionic/main amd64 zerofree amd64 1.0.4-1 [8,112 B]
Fetched 740 kB in 5s (164 kB/s)
Selecting previously unselected package ethtool.
(Reading database ... 134319 files and directories currently installed.)
Preparing to unpack .../ethtool_1%3a4.15-0ubuntu1_amd64.deb ...
Unpacking ethtool (1:4.15-0ubuntu1) ...
Selecting previously unselected package libxmlsec1-openssl:amd64.
Preparing to unpack .../libxmlsec1-openssl_1.2.25-1build1_amd64.deb ...
Unpacking libxmlsec1-openssl:amd64 (1.2.25-1build1) ...
Selecting previously unselected package open-vm-tools.
```

Then I type in the **vmware-hgfsclient** command to find out the shared folder, the folder name appears as the output. From that I become the root user and type in some commands like **gedit /etc/fstab**, to open a text editor to change some rules in that text editor, then I save it and run the command **mkdir /mnt/hgfs**, to create a directory in this machine in the given path to have the shared folder from the host machine.

This is a simple console application and can be run as any user. **vmware-hgfsclient** is a userspace HGFS client implementation.

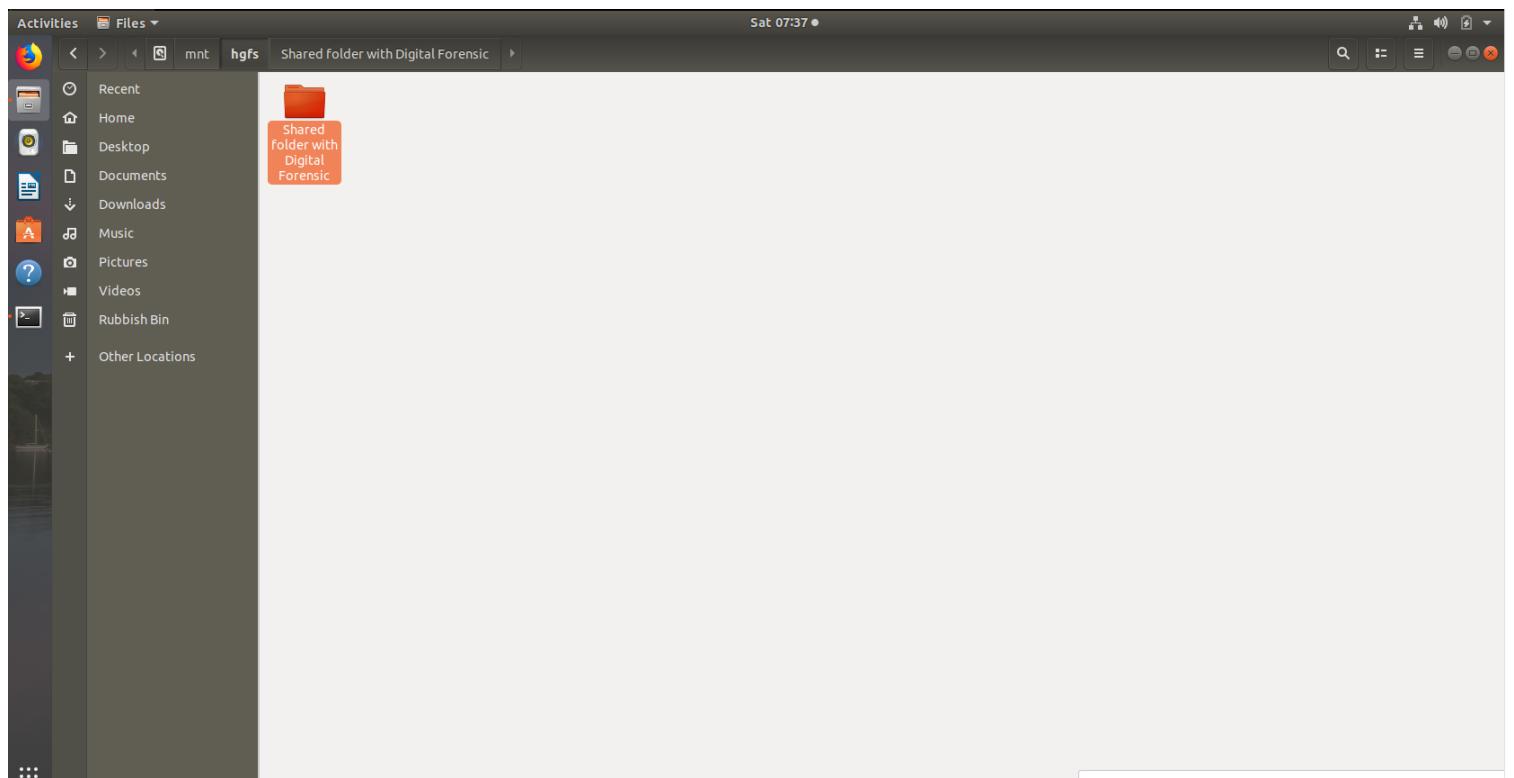
Finally mount the shared folder using **mount -a** command to mount it to the ubuntu VM.

The terminal window shows the following sequence of commands and outputs:

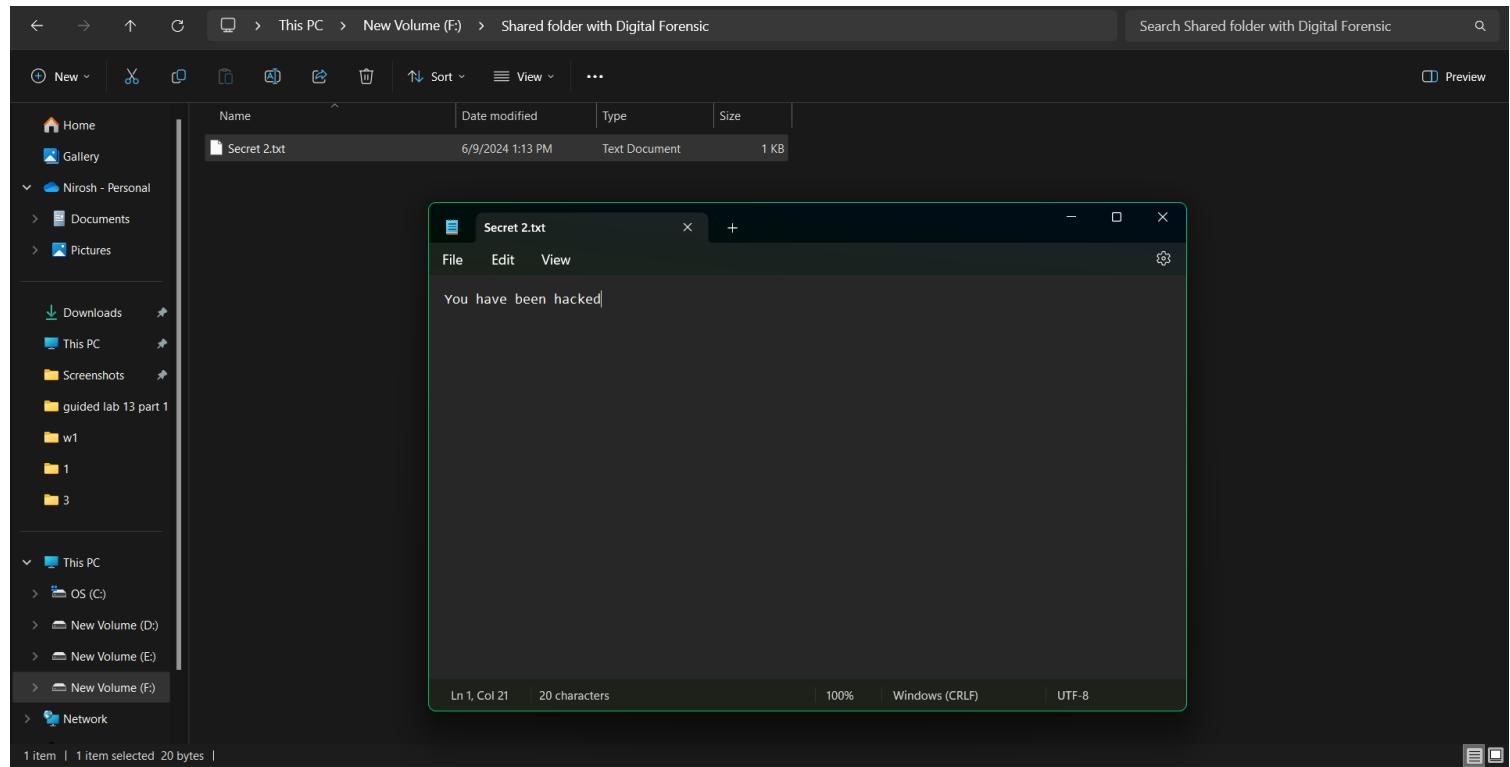
```
Activities Terminal Sat 07:36 ●
root@Ubuntu1804:/home/user
File Edit View Search Terminal Help
Fetching 740 kB in 5s (164 kB/s)
Selecting previously unselected package ethtool.
(Reading database ... 134319 files and directories currently installed.)
Preparing to unpack .../ethtool_1%3a4.15-0ubuntu1_amd64.deb ...
Unpacking ethtool (1:4.15-0ubuntu1) ...
Selecting previously unselected package libxmlsec1-openssl:amd64.
Preparing to unpack .../libxmlsec1-openssl_1.2.25-1build1_amd64.deb ...
Unpacking libxmlsec1-openssl:amd64 (1.2.25-1build1) ...
Selecting previously unselected package open-vm-tools.
Preparing to unpack .../open-vm-tools_2%3a11.0.5-4ubuntu0.18.04.3_amd64.deb ...
Unpacking open-vm-tools (2:11.0.5-4ubuntu0.18.04.3) ...
Selecting previously unselected package zerofree.
Preparing to unpack .../zerofree_1.0.4-1_amd64.deb ...
Unpacking zerofree (1.0.4-1) ...
Setting up zerofree (1.0.4-1) ...
Setting up libxmlsec1-openssl:amd64 (1.2.25-1build1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Setting up open-vm-tools (2:11.0.5-4ubuntu0.18.04.3) ...
Created symlink /etc/systemd/system/vmtoolsd.service → /lib/systemd/system/open-vm-tools.service.
Created symlink /etc/systemd/system/multi-user.target.wants/open-vm-tools.service → /lib/systemd/system/open-vm-tools.service.
Created symlink /etc/systemd/system/open-vm-tools.service.requires/vgauth.service → /lib/systemd/system/vgauth.service.
Processing triggers for libc-bin (2.27-3ubuntu0.23) ...
Processing triggers for systemd (237-3ubuntu0.23) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Setting up ethtool (1:4.15-0ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
user@Ubuntu1804:~$ vmware-hgfsclient
Shared folder with Digital Forensic
user@Ubuntu1804:~$ sudo su
root@Ubuntu1804:/home/user# user
Command 'user' not found, did you mean:
  Command 'fuser' from deb psmisc
  Command 'users' from deb coreutils
  Command 'luser' from deb iptutil
  Command 'userv' from deb userv
Try: apt install <deb name>
root@Ubuntu1804:/home/user# gedit /etc/fstab
root@Ubuntu1804:/home/user# mkdir /mnt/hgfs
root@Ubuntu1804:/home/user# mount -a
root@Ubuntu1804:/home/user#
```

or press Ctrl+G.

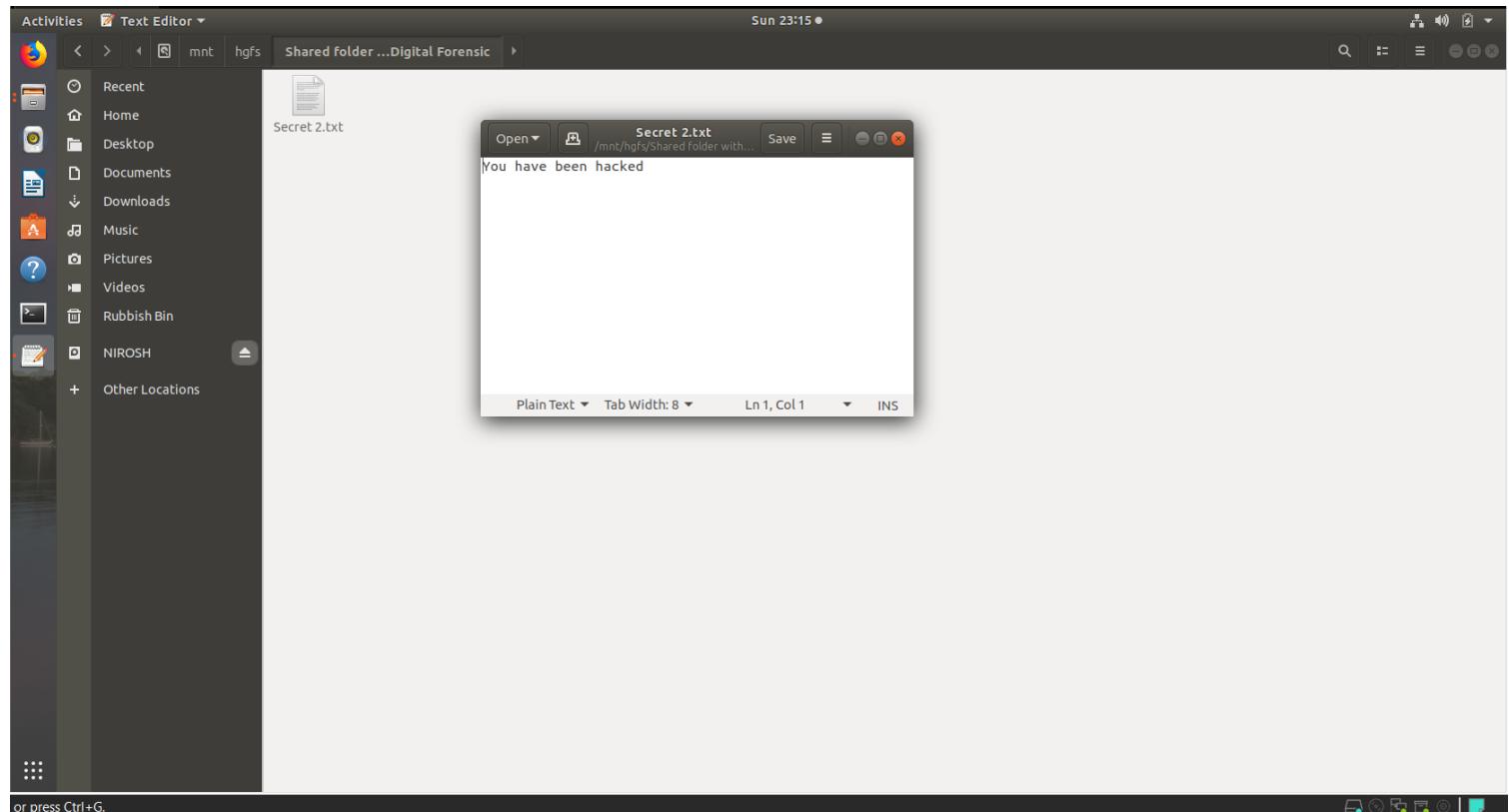
Now if I navigate to the directory I gave earlier, **computer/mnt/hgfs**, I can find the shared folder in this directory.



To test the file sharing through this method, I will first create another text file called **secret 2.txt** in my main machine with a secret called **You have been hacked**.



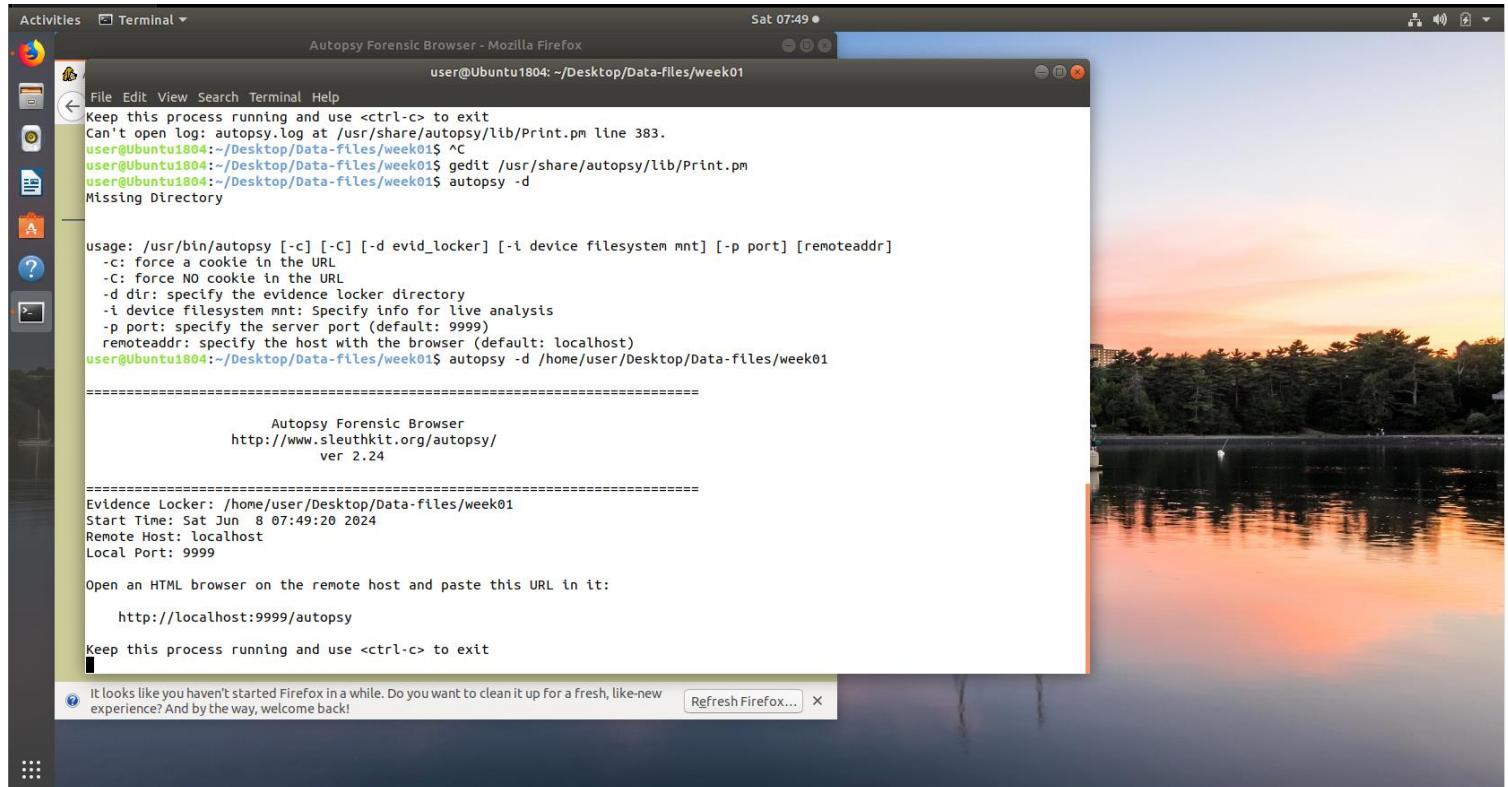
Now I switch back to the Ubuntu VM and checked the shared folder there. I found that the txt file has been shared there as well. So, this way of file sharing is also a success.



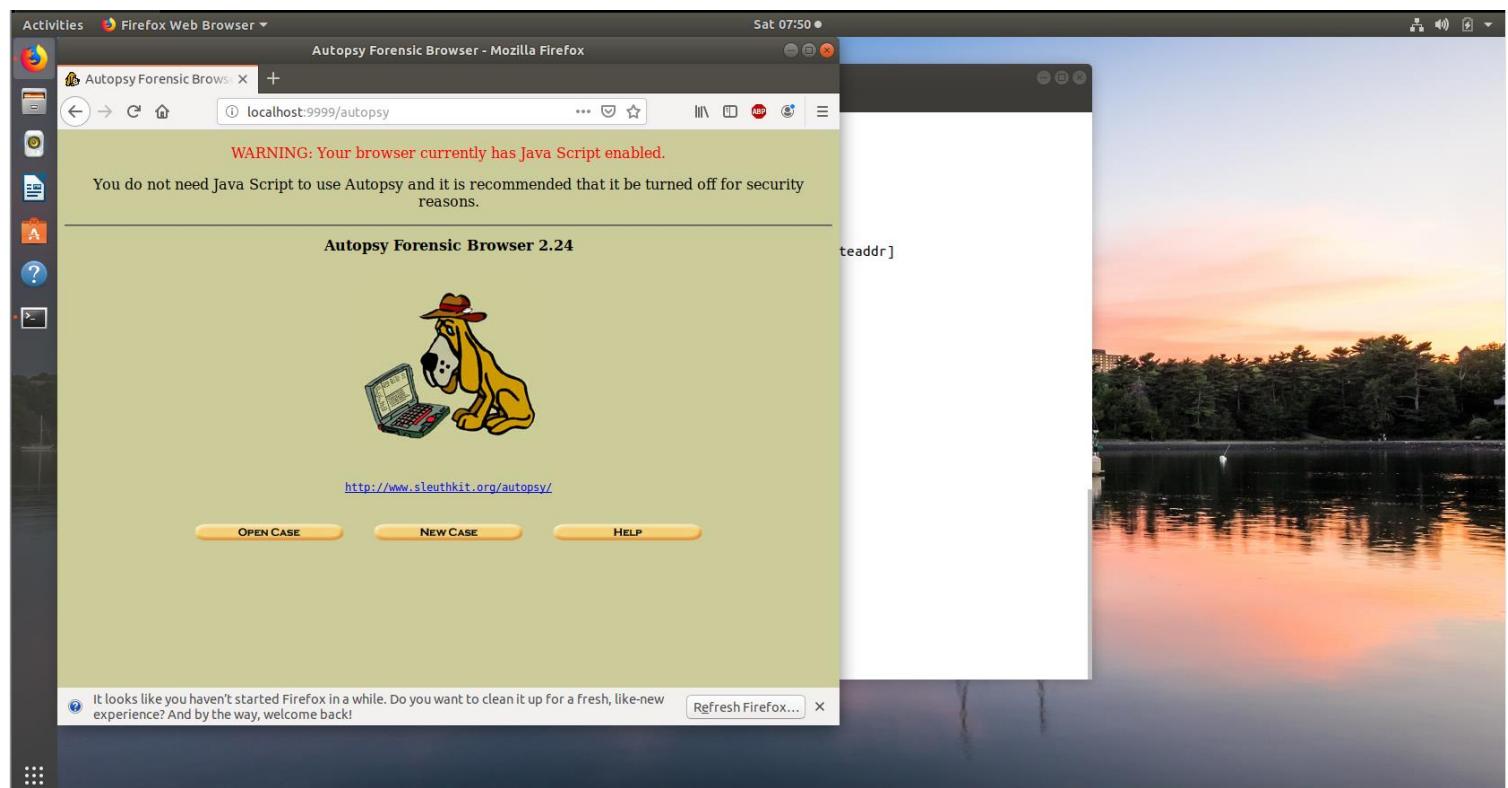
Forensic Investigation with Autopsy

Launch Terminal: I opened the terminal and navigated to the directory containing our data files with `cd ~/Desktop/Data-files/week01`.

Start Autopsy: Running the command `autopsy -d /home/user/Desktop/Data-files/week01/` started the Autopsy tool.

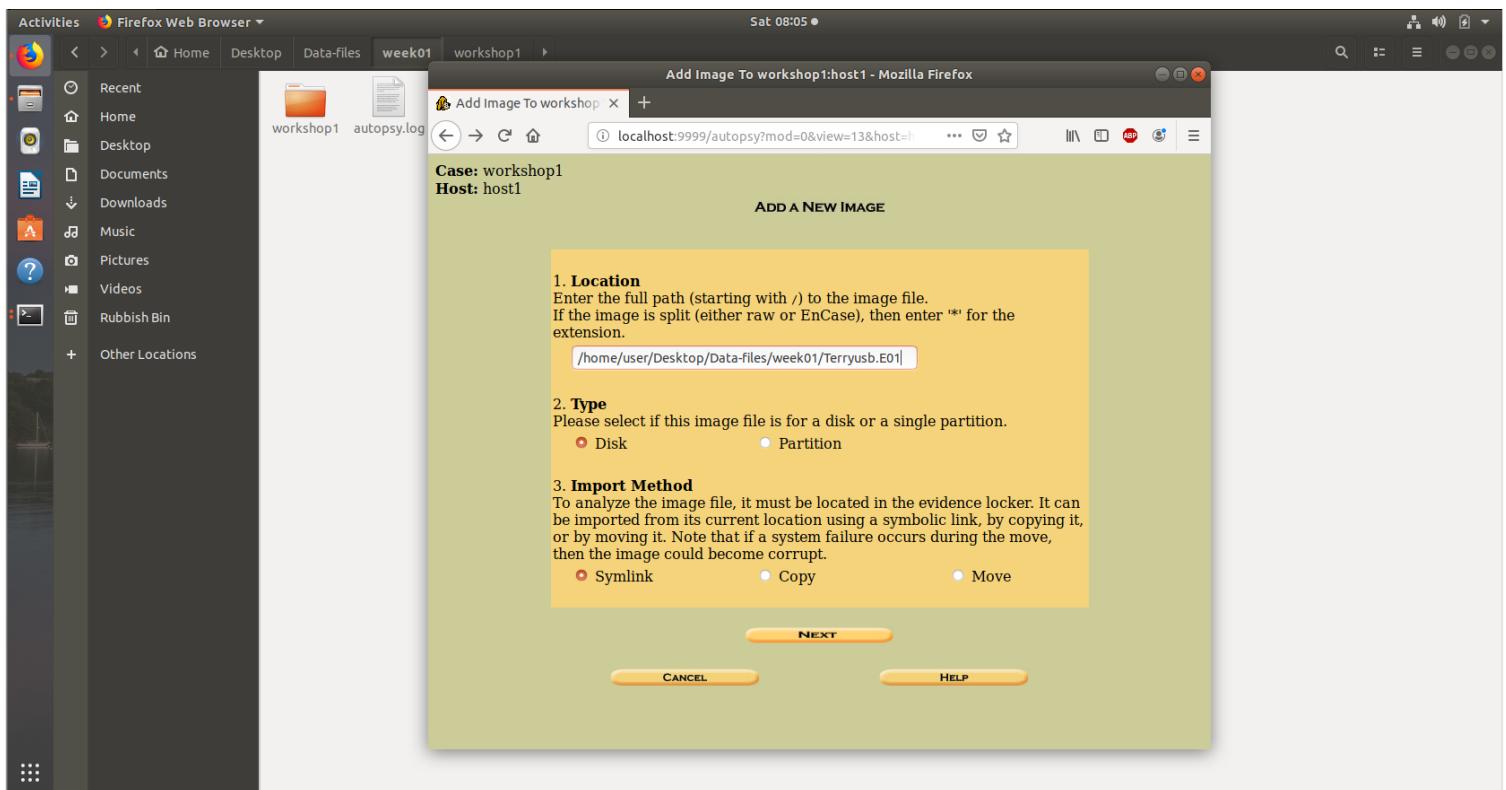
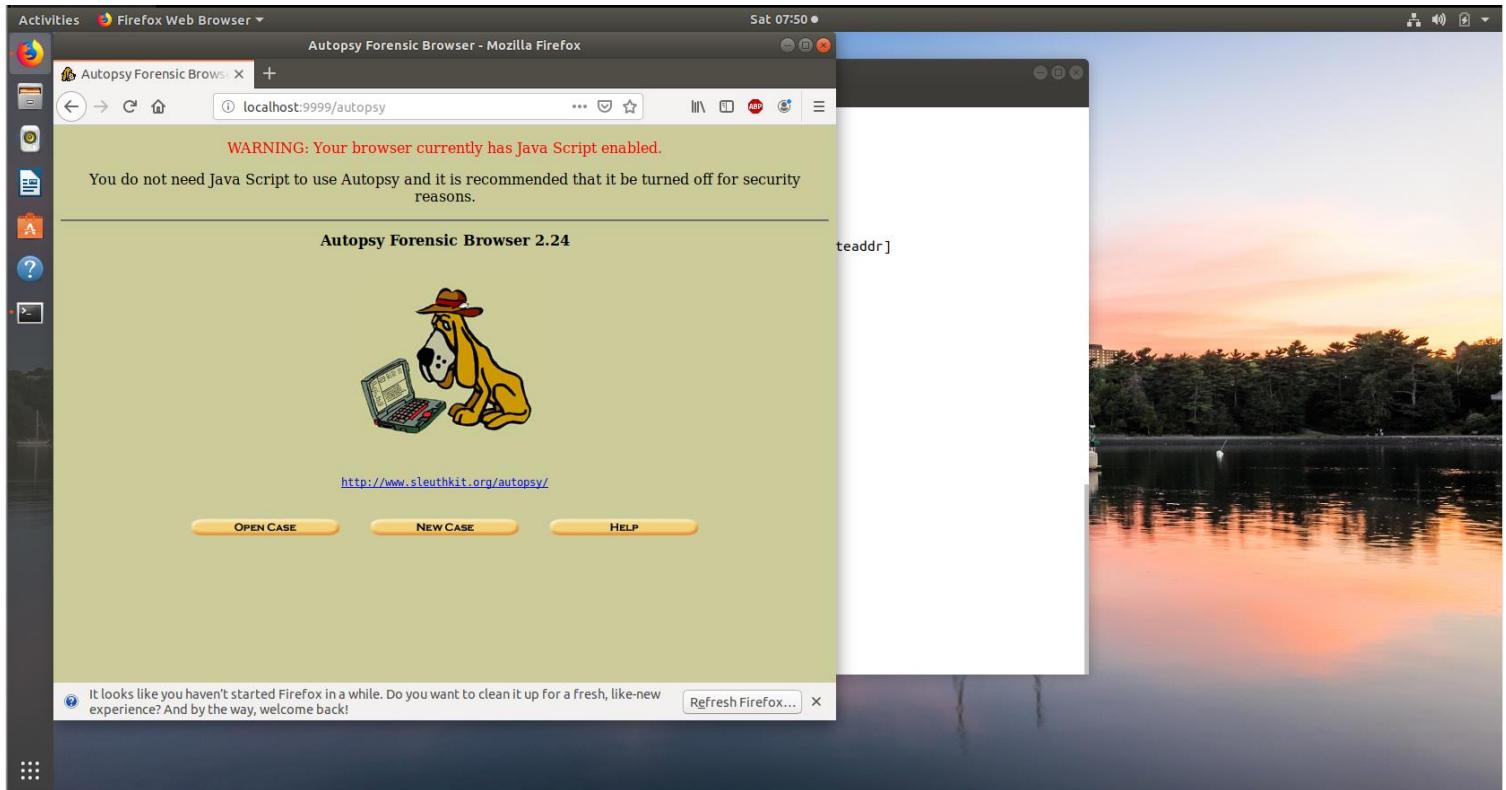


Access Autopsy in Browser: I opened <http://localhost:9999/autopsy> in Firefox.



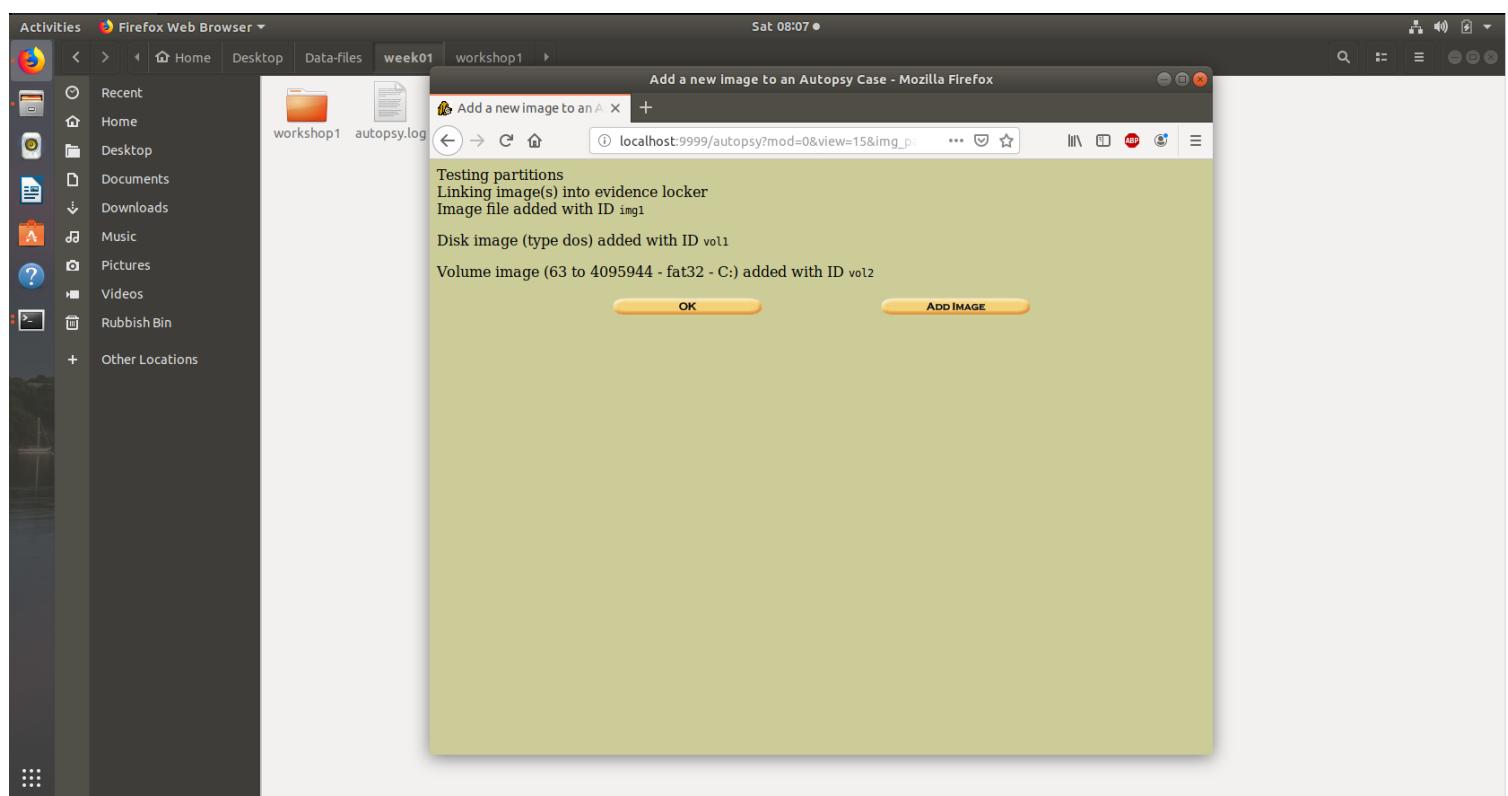
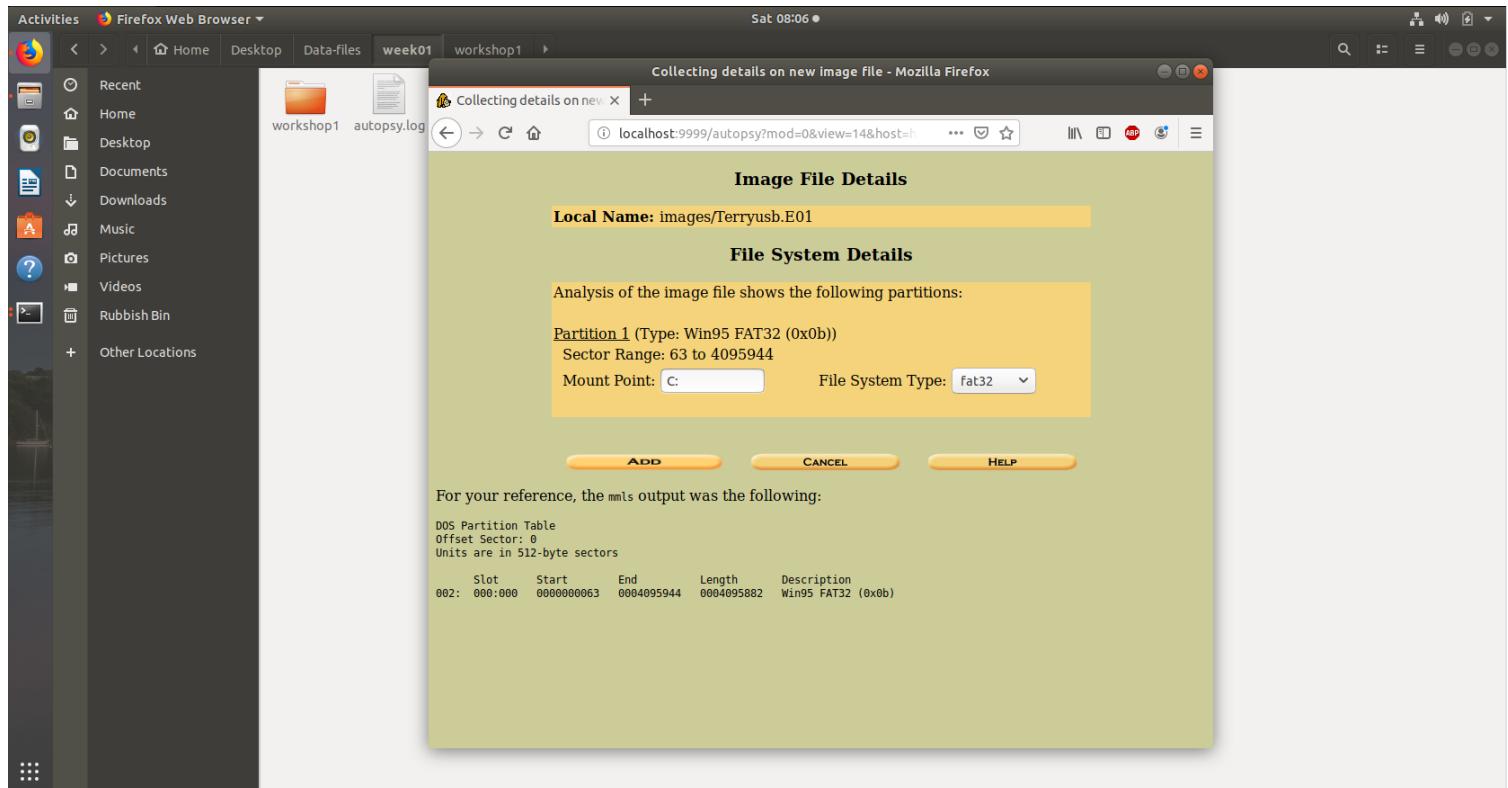
Clicked **New Case**, named the case and investigator, and then added a host.

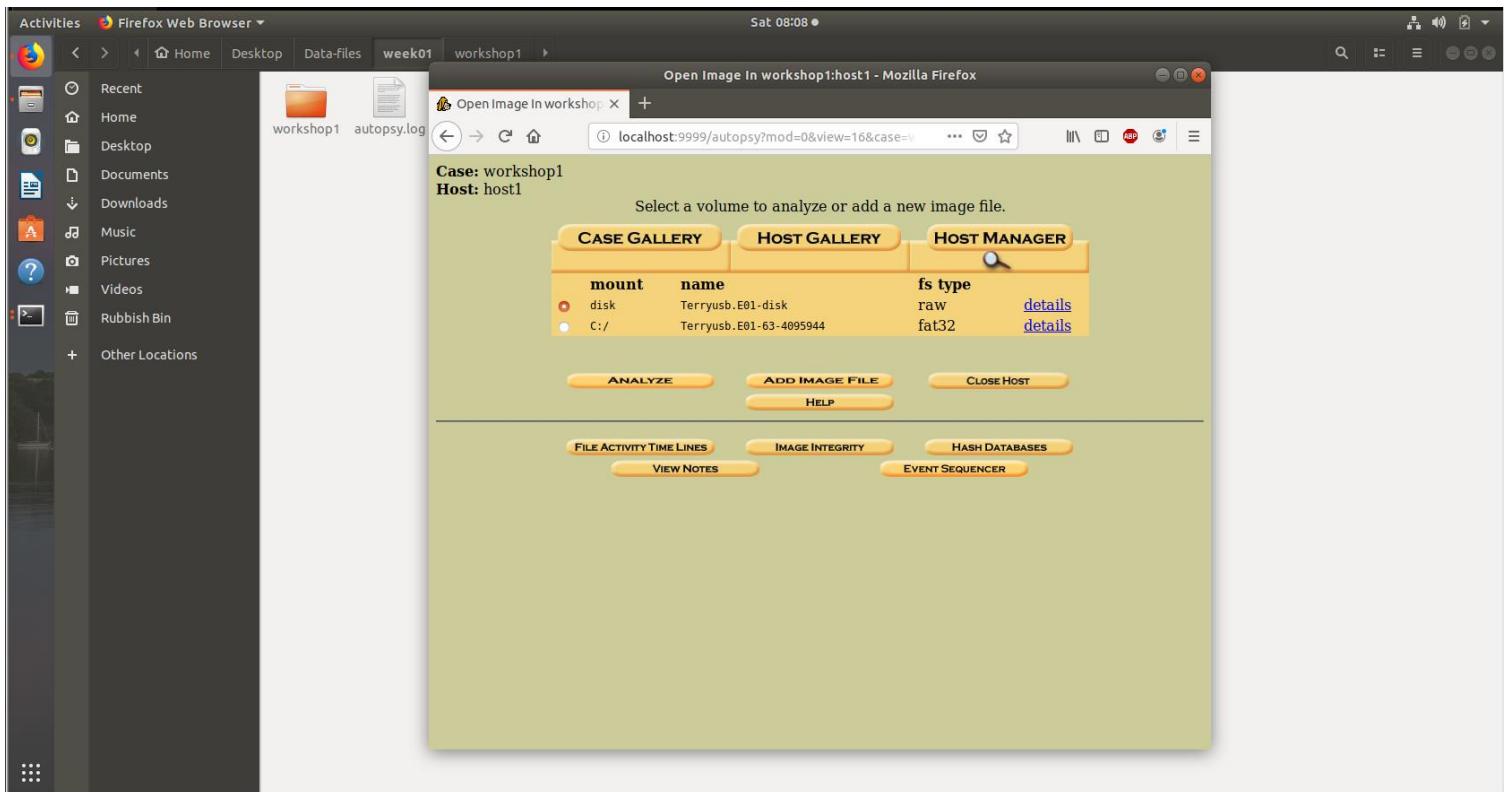
Added a forensic image by specifying the path **/home/user/Desktop/Data-files/week01/Terryusb.E01** and clicked **Next**



With the forensic image loaded, I began the analysis:

Checked the C:/ option under 'mount'.





Explored file analysis options, finding notable files like **xpadvancedkeylogger.exe**.

	File Path	Modified	Created	Last Accessed	Size	Permissions	Owner	
<input checked="" type="checkbox"/>	r/r xpadvancedkeylogger.exe	2009-11-16 14:23:38 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:43:57 (AEDT)	140	0	0	57
<input checked="" type="checkbox"/>	r/r R\$4492.EXE	2009-11-20 10:31:44 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-11-20 10:31:34 (AEDT)	4123504	0	0	62
<input checked="" type="checkbox"/>	r/r TERRYS WORK (Volume Label Entry)	2009-11-17 13:47:24 (AEDT)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	3
<input checked="" type="checkbox"/>	r/r urlscopyright.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	376766	0	0	46
<input checked="" type="checkbox"/>	r/r urlscryptography.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	299939	0	0	40
<input checked="" type="checkbox"/>	r/r urlspatents.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	5374583	0	0	34
<input checked="" type="checkbox"/>	r/r urlspersona.txt	2009-11-14 17:43:14 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:41:55 (AEDT)	1658	0	0	28
<input checked="" type="checkbox"/>	r/r urlstime_machine.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	1538990	0	0	20
<input checked="" type="checkbox"/>	r/r vnc-4_1_3-x86_win32.exe	2008-10-15 17:14:08 (AEDT)	2009-12-07 00:00:00 (AEDT)	2008-10-15 17:14:08 (AEDT)	741744	0	0	75
<input checked="" type="checkbox"/>	r/r webauto.py	2009-11-16 14:23:38 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:39:19 (AEDT)	2237	0	0	6
<input checked="" type="checkbox"/>	r/r xpadvancedkeylogger.exe	2009-12-03 09:40:44 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-12-03 09:41:16 (AEDT)	1580660	0	0	70

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: HTML document, ASCII text, with very long lines, with CRLF, CR line terminators
Deleted File Recovery Mode

Contents Of File: C:/xpadvancedkeylogger.exe

```

<style> body {SCROLLBAR-FACE-COLOR:#FFFFFF; SCROLLBAR-HIGHLIGHT-COLOR:#DFDFDF; SCROLLBAR-SHADOW-COLOR:#FFFFFF; SCROLLBAR-ARROW-COLOR:#666666; SCROLLBAR-BASE-COLOR:#333333; SCROLLBAR-DARK-SHADOW-COLOR:#000000;}</style>
<base target="_blank">
<hr noshade size="1" color="#C0C0C0">

<b><font face="Verdana" color="#FF0000" size="3">clipboard</font></b>
<BR>
<font face="Verdana" color="#0000FF" size="1">Window Title:</font>
<font face="Verdana" color="#B7B7B7" size="1"></font>
<BR>

```

Spent time exploring the case, taking notes on any anomalies or suspicious files.

Sat 08:10 • workshop1:host1:vol2 - Mozilla Firefox

localhost:9999/autopsy?mod=1&submod=2&case=workshop1&host=host1&inv=unknown&vol=vol2

FILE ANALYSIS **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW

File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH

ALL DELETED FILES
EXPAND DIRECTORIES

Current Directory: C:/
ADD NOTE **GENERATE MD5 LIST OF FILES**

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405828	
v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405829	
v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	65405827	
d / d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	65405830	
r / r	.._Trashes	2009-11-17 10:47:46 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 10:47:47 (AEDT)	4096	0	0	5	
r / r	.MS7biz.jpg	2009-11-17 10:49:24 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 10:49:25 (AEDT)	4096	0	0	17	
r / r	.patentauto.py	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:19 (AEDT)	4096	0	0	54	
r / r	.patentterms.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:19 (AEDT)	4096	0	0	60	
r / r	.urlscopyright.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:19 (AEDT)	4096	0	0	49	
r / r	.urlscryptography.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:19 (AEDT)	4096	0	0	43	
r / r	.urlspatents.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:18 (AEDT)	4096	0	0	37	
r / r	.urlspersona.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:18 (AEDT)	4096	0	0	31	
r / r	.urlstime_machine.txt	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:18 (AEDT)	4096	0	0	23	
r / r	.webauto.py	2009-11-17 13:47:18 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:47:18 (AEDT)	4096	0	0	25	
✓	d / d .fsevents/	2009-11-17 10:48:38 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 10:48:38 (AEDT)	0	0	0	10	

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Sat 08:11 • workshop1:host1:vol2 - Mozilla Firefox

localhost:9999/autopsy?mod=1&submod=2&case=workshop1&host=host1&inv=unknown&vol=vol2

FILE ANALYSIS **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

Directory Seek
Enter the name of a directory that you want to view.
C:/
VIEW

File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH

ALL DELETED FILES
EXPAND DIRECTORIES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
✓	d / d .078421/	2009-11-20 10:59:48 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:59:47 (AEDT)	0	0	0	65	
✓	d / d .189812/	2009-11-20 11:33:04 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 11:33:03 (AEDT)	0	0	0	67	
✓	d / d .452781/	2009-11-20 11:06:04 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 11:06:02 (AEDT)	0	0	0	66	
✓	d / d .461531/	2009-11-20 10:49:32 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:49:30 (AEDT)	0	0	0	63	
✓	r / r .54402.EXE	2009-11-20 10:31:36 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:31:34 (AEDT)	0	0	0	61	
✓	d / d .604468/	2009-11-20 10:51:54 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:51:53 (AEDT)	0	0	0	64	
d / d	Log/	2009-12-07 08:05:22 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-12-07 08:05:20 (AEDT)	643072	0	0	72	
r / r	MS7biz.jpg	2009-11-17 08:50:26 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-11-17 08:50:25 (AEDT)	379726	0	0	15	
r / r	patentauto.py	2009-11-17 13:37:00 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-16 14:16:49 (AEDT)	3673	0	0	51	
r / r	patentterms.txt	2009-11-16 14:29:38 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:43:57 (AEDT)	140	0	0	57	
r / r	RS4402.EXE	2009-11-20 10:31:44 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-11-20 10:31:34 (AEDT)	4123504	0	0	62	
r / r	TERRYS WORK (Volume Label Entry)	2009-11-17 13:47:24 (AEDT)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	3	
r / r	urlscopyright.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	376766	0	0	46	
r / r	urlscryptography.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	299939	0	0	40	
r / r	urlspatents.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	5374583	0	0	34	
r / r	urlspersona.txt	2009-11-14 17:43:14 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:41:55 (AEDT)	1658	0	0	28	
r / r	urlstime_machine.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	1538990	0	0	20	

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=21, baseline, precision 8, 1650x1275, frames 3]

C:/MS7biz.jpg

Thumbnail: [View Full Size Image](#)

Activities Firefox Web Browser Sat 08:11 ● workshop1:host1:vol2 - Mozilla Firefox

localhost:9999/autopsy?mod=1&submod=2&case=workshop1&host=host1&inv=unknown&vol=vol2

FILE ANALYSIS **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

		2009-11-17 10:47:40 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 10:59:47 (AEDT)	0	0	0	0	65	
✓	d / d	078421 /	2009-11-20 10:59:48 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:59:47 (AEDT)	0	0	0	0	65
✓	d / d	189812 /	2009-11-20 11:33:04 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 11:33:03 (AEDT)	0	0	0	0	67
✓	d / d	_452781 /	2009-11-20 11:06:04 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 11:06:02 (AEDT)	0	0	0	0	66
✓	d / d	_461531 /	2009-11-20 10:49:32 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:49:30 (AEDT)	0	0	0	0	63
✓	r / r	_54402.EXE	2009-11-20 10:31:36 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:31:34 (AEDT)	0	0	0	0	61
✓	d / d	_604468 /	2009-11-20 10:51:54 (AEDT)	2009-11-20 00:00:00 (AEDT)	2009-11-20 10:51:53 (AEDT)	0	0	0	0	64
	d / d	LogZ	2009-12-07 08:05:22 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-12-07 08:05:20 (AEDT)	643072	0	0	0	72
	r / r	M57biz.jpg	2009-11-17 08:50:26 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-11-17 08:50:25 (AEDT)	379726	0	0	0	15
	r / r	patentauto.py	2009-11-17 13:37:00 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-16 14:16:49 (AEDT)	3673	0	0	0	51
	r / r	patentterms.txt	2009-11-16 14:29:38 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:43:57 (AEDT)	140	0	0	0	57
	r / r	R54402.EXE	2009-11-20 10:31:44 (AEDT)	2009-12-07 00:00:00 (AEDT)	2009-11-20 10:31:34 (AEDT)	4123504	0	0	0	62
	r / r	TERRYS WORK (Volume Label Entry)	2009-11-17 13:47:24 (AEDT)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0	3
	r / r	urlscopyright.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	376766	0	0	0	46
	r / r	urlscryptography.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	299939	0	0	0	40
	r / r	urlspatents.txt	2009-11-17 10:40:56 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-17 10:40:57 (AEDT)	5374583	0	0	0	34
	r / r	urlspersona.txt	2009-11-14 17:43:14 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-14 17:41:55 (AEDT)	1658	0	0	0	28
	r / r	urlstime_machine.txt	2009-11-16 10:22:50 (AEDT)	2009-11-24 00:00:00 (AEDT)	2009-11-16 10:22:51 (AEDT)	1538990	0	0	0	20

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: ASCII text

Contents Of File: C:/patentterms.txt

```
time_2664052
quantum_50473
mortality_26619
cryptography_8431
machine_649955
math_13010
time+machine_4971
immortality_437
cryogenics_1385
```

Then went through the deleted files

Activities Firefox Web Browser Sat 08:31 ● workshop1:host1:vol2 - Mozilla Firefox

localhost:9999/autopsy?mod=1&submod=2&case=workshop1&host=host1&inv=unknown&vol=vol2

FILE ANALYSIS **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

Type	dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
d / d	C:/ Trashes/_01		2009-11-17 13:34:58 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:34:58 (AEDT)	0	0	0	133
r / r	C:/ Trashes/_501		2009-11-17 13:34:58 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:34:58 (AEDT)	4096	0	0	135
d / d	C:/ fsevents		2009-11-17 10:48:38 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 10:48:38 (AEDT)	0	0	0	10
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/-7.IND		2009-11-17 13:34:58 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:34:58 (AEDT)	4096	0	0	1433
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/journalAttr_1		2009-11-17 13:34:58 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:34:59 (AEDT)	0	0	0	1483
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/0.shadowIndexHead		2009-11-17 13:35:12 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:35:13 (AEDT)	4096	0	0	1493
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/tmp_0.cmpt_indexPostings		2009-11-17 13:35:14 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:35:14 (AEDT)	182	0	0	1525
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/tmp_0.cmpt_indexHead		2009-11-17 13:35:14 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:35:14 (AEDT)	4096	0	0	1528
r / r	C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/tmp_0.cmpt_indexPositions		2009-11-17 13:35:14 (AEDT)	2009-11-17 00:00:00 (AEDT)	2009-11-17 13:35:14 (AEDT)	4	0	0	1531

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note
File Type: AppleDouble encoded Macintosh file
Deleted File Recovery Mode

Contents Of File: C:/ Spotlight-V100/Store-V1/Stores/76800DE76-88D9-43B3-AC7E-3B02E7F38194/0.shadowIndexHead

```
Mac OS X
```

File system information

Activities Firefox Web Browser Sat 08:35 • workshop1:host1:vol2 - Mozilla Firefox

localhost:9999/autopsy X localhost:9999/autopsy X localhost:9999/autopsy X +

localhost:9999/autopsy?mod=1&submod=7&case=workshop1&host=host1&inv=unknown&vol=vol2

FILE SYSTEM INFORMATION

File System Type: FAT32

OEM Name: BSD 4.4

Volume ID: 0xa741208

Volume Label (Boot Sector): TERRYS WORK

Volume Label (Root Directory):

File System Type Label: FAT32

Next Free Sector (FS Info): 158074

Free Sector Count (FS Info): 3937808

Sectors before file system: 0

File System Layout (in sectors)

Total Range: 0 - 4095881

- * Reserved: 0 - 31
- ** Boot Sector: 0
- ** FS Info Sector: 1
- ** Backup Boot Sector: 6
- * FAT 0: 32 - 4024
- * FAT 1: 4025 - 8017
- * Data Area: 8018 - 4095881
- ** Cluster Area: 8018 - 4095881
- *** Root Directory: 8018 - 8025

METADATA INFORMATION

Range: 2 - 65405830

Root Directory: 2

CONTENT INFORMATION

Sector Size: 512

Cluster Size: 4096

Total Cluster Range: 2 - 510984

MD5 hash values

Activities Firefox Web Browser Sat 08:37 • Mozilla Firefox

localhost:9999/autopsy X localhost:9999/autopsy X localhost:9999/autopsy X +

localhost:9999/autopsy?mod=2&view=12&case=workshop1&host=host1&inv=unknown&vol=vol2&dir=/&meta=2

MDS Values for files in C:/ (Terryusb.E01-63-4095944)

d41dcd98700b204e800998ef8427e	- TERRYS WORK (Volume Label Entry)
Sead39c470178ebdef93e53ab6f0da	- ..Trashes
ce3231180e69f5a56c16459db0f1d531	- webauto.py
8ad51236538591f2a9e84a15bd89e01	- MS751z.jpg
7e1a2a2a2a2a2a2a2a2a2a2a2a2a2a2a2	- MS751z.jpg
64eeefbf48c835ce93df6bb7941a4b54	- urlstime_machine.txt
4ee3e800d4f4851ca7ec2bb409b977c3	- ..urlstime_machine.txt
5170de55bade423f1ed57b431a1fe4f	- ..webauto.py
D7D9E9A880B8A80B8A80B8A80B8A80B8A	- ..urlspatents.txt
Se1783e97289cc7dd9d93552738b101	- ..urlspersona.txt
95fa78acc9369d89a4513a0b8e4b26d	- ..urlspatents.txt
Se9f9d5280acfc4b4calec777880325f	- ..urlspatents.txt
321e55a02a2a2a2a2a2a2a2a2a2a2a2a2	- ..urlscryptography.txt
341e55a02a2a2a2a2a2a2a2a2a2a2a2a2	- ..urlscryptography.txt
02fcfb3f7b2b082lbecl0272508a32ea	- ..urlscopyright.txt
d4799d3877f0867c5b21f1217284aa05	- ..urlscopyright.txt
352e2d97831773d73d73d73d73d73d	- ..patentinfo.py
011a85464655546465554646555464655	- ..patentinfo.py
9345418513887494a8efef659093c6a07	- ..patentterms.txt
b02a2a4b05e80a80a1e38fc8bccfc1d1b	- ..patentterms.txt
55f9facfaeac8cf1d1b1f1fc8d4f3d2b754	- R54402.EXE
790856e8ae34f0a3e040e031c7fa47a	- vnc-4_1_3-x86_win32.exe

Key Findings:

xpadvancedkeylogger.exe: Given that this file is frequently linked to keylogging activities, its existence raises serious suspicions. This suggests that there may have been malicious intent to log and record keystrokes made on the infected machine.

The image contains a number of files and logs that indicate extensive user activity including possibly sensitive data. Reconstructing timelines and user behaviors can be aided by the examination of these records.

There were hints of obscured or concealed files, which would mean that critical information or proof was being tried to hide. provide a more accurate picture of any attempts to conceal actions.

Final Thoughts:

Comprehensive insights into the nature and scope of the suspicious activity on the studied system were obtained via the Autopsy-based investigation. I found important evidence by carefully examining the forensic image, which may be useful in determining the extent of the incident and avoiding similar ones in the future.