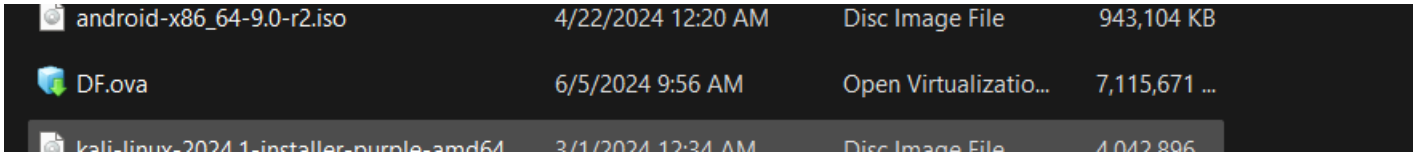
Setting Up the Digital Forensic Lab

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:

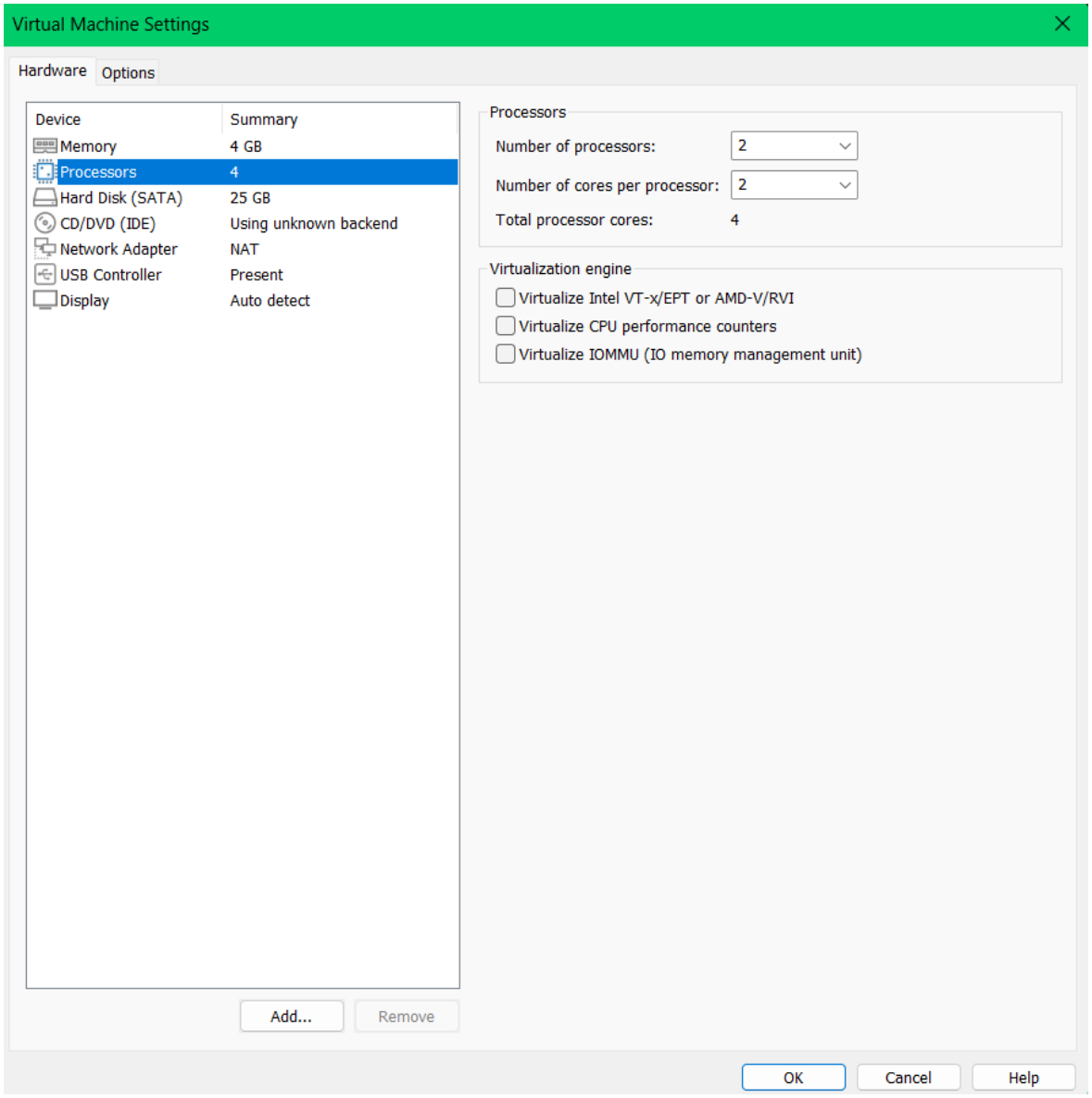
Download the Ubuntu VM: I then downloaded the virtual machine using the provided link and code



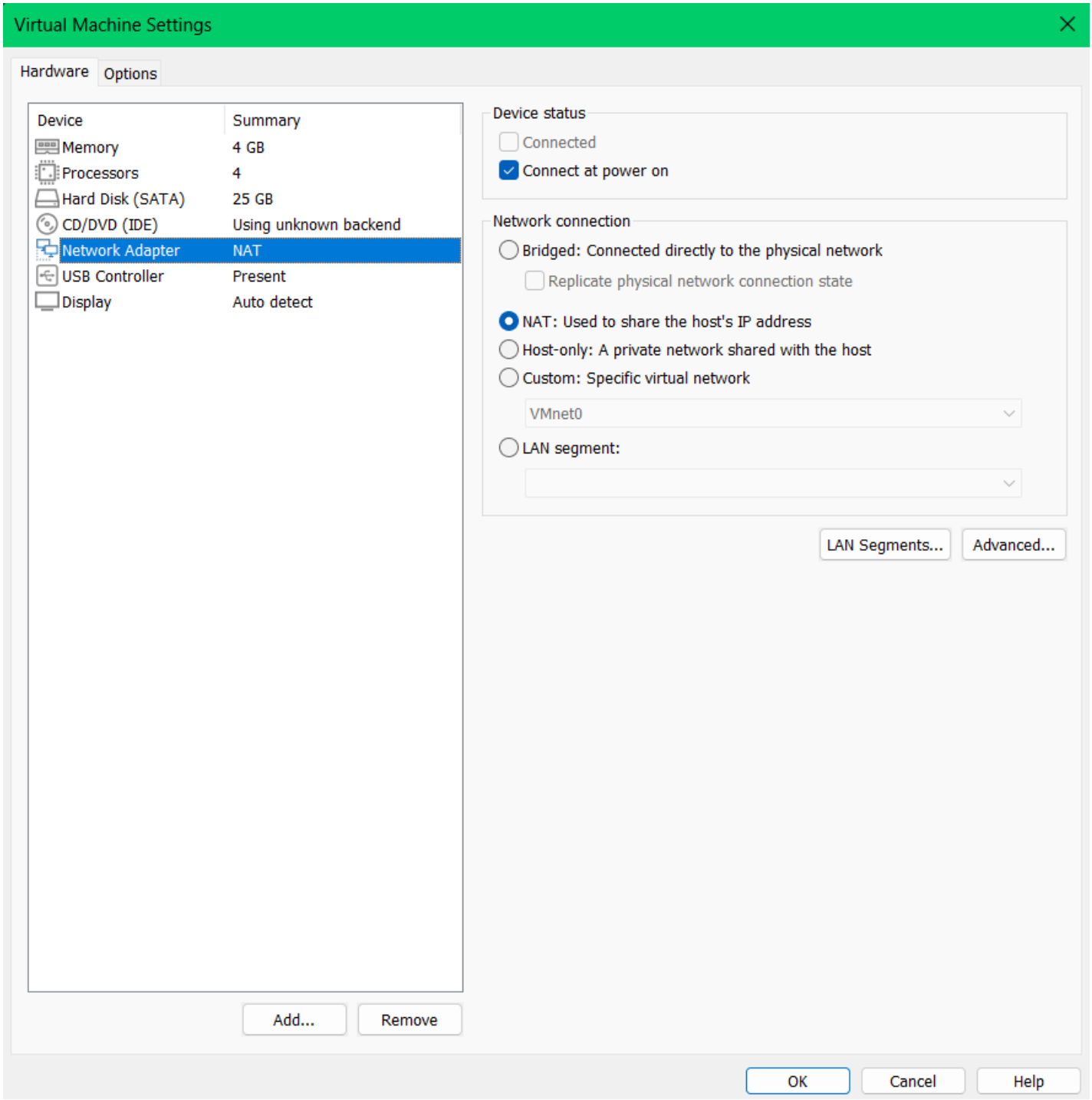
Import the Ubuntu VM:

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

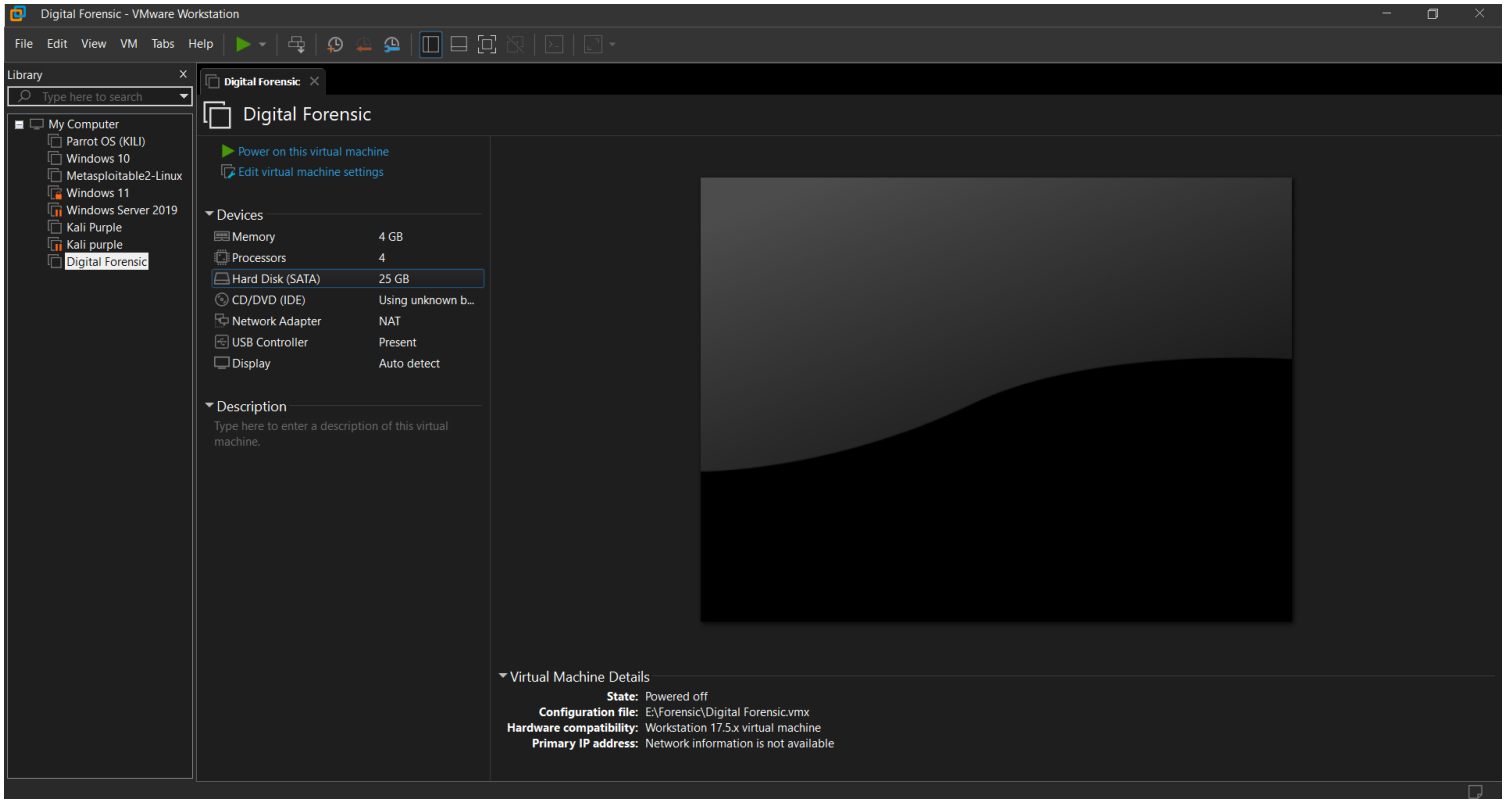
Processors



Network adapter

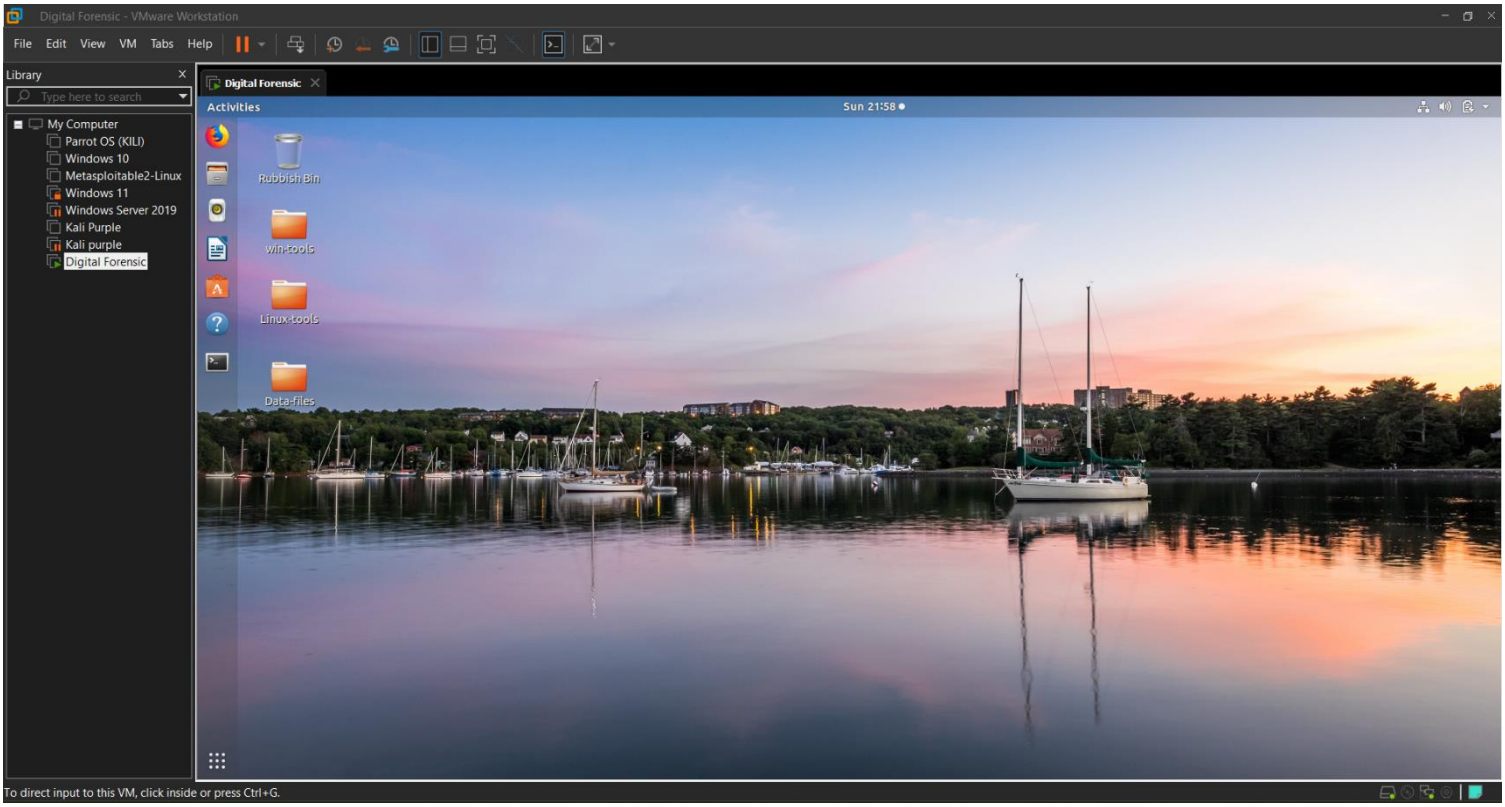


After completing these steps, the Ubuntu virtual machine successfully appeared in Vmware



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.



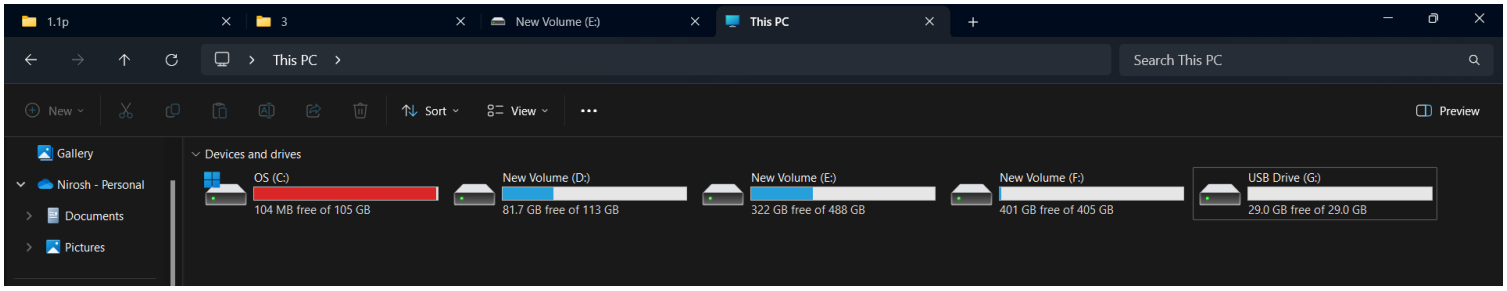
Accessing Personal Files

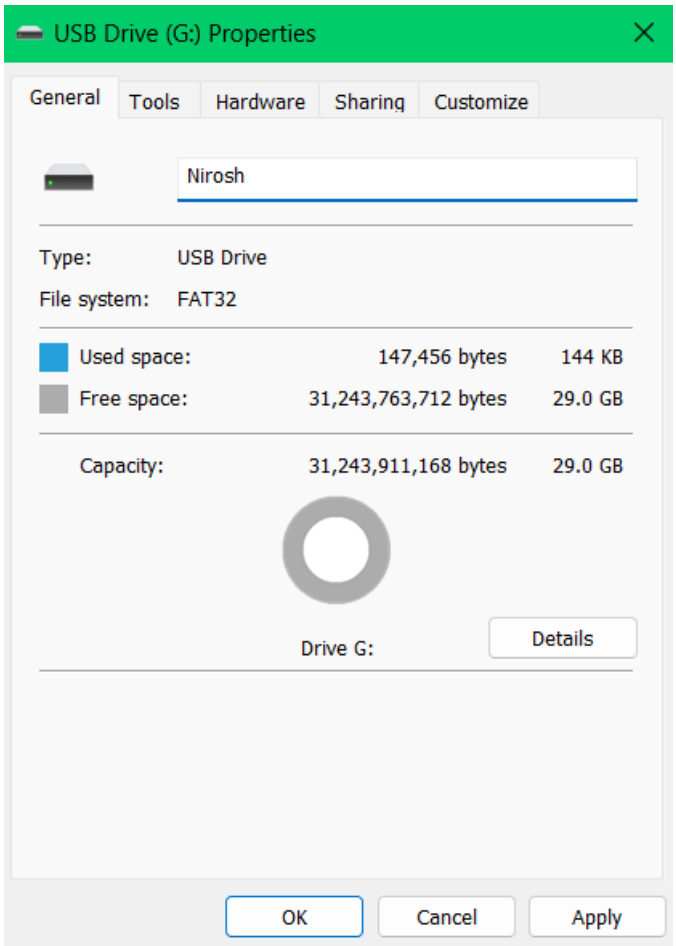
Vmware allows file sharing between the host and the virtual machine in several ways:

Using a USB Drive:

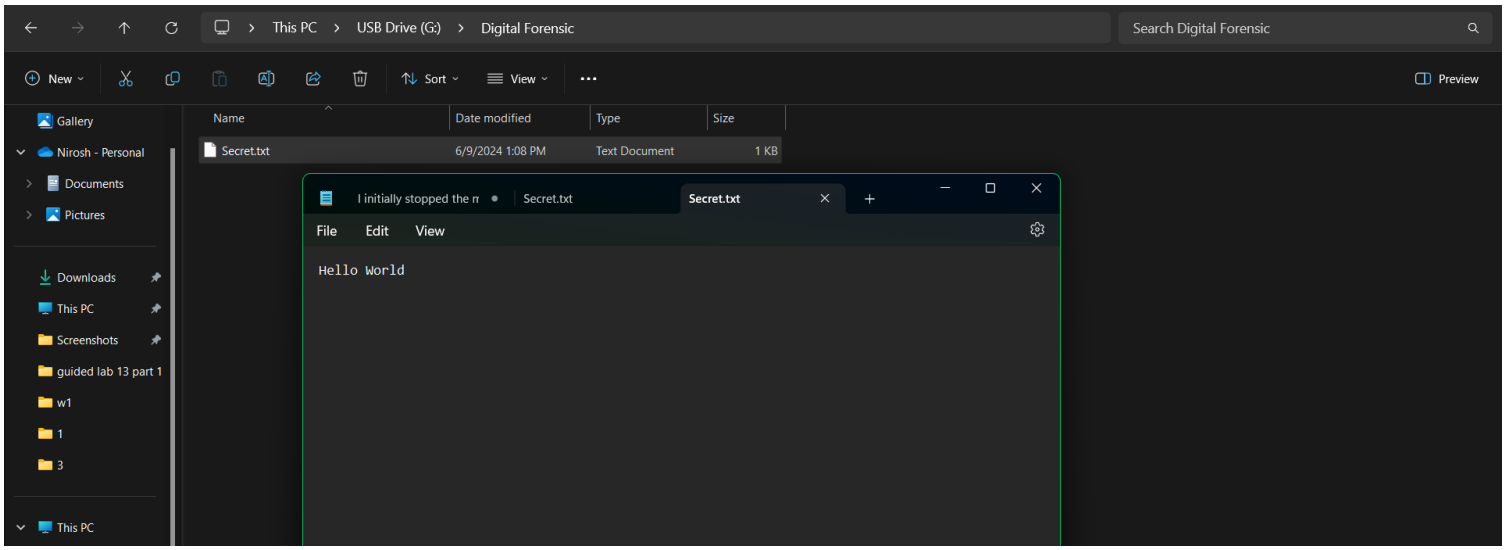
I Copied files from one system and pasted them to another system. I Ensured that the USB is formatted in FAT32 or ex-FAT.

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.**

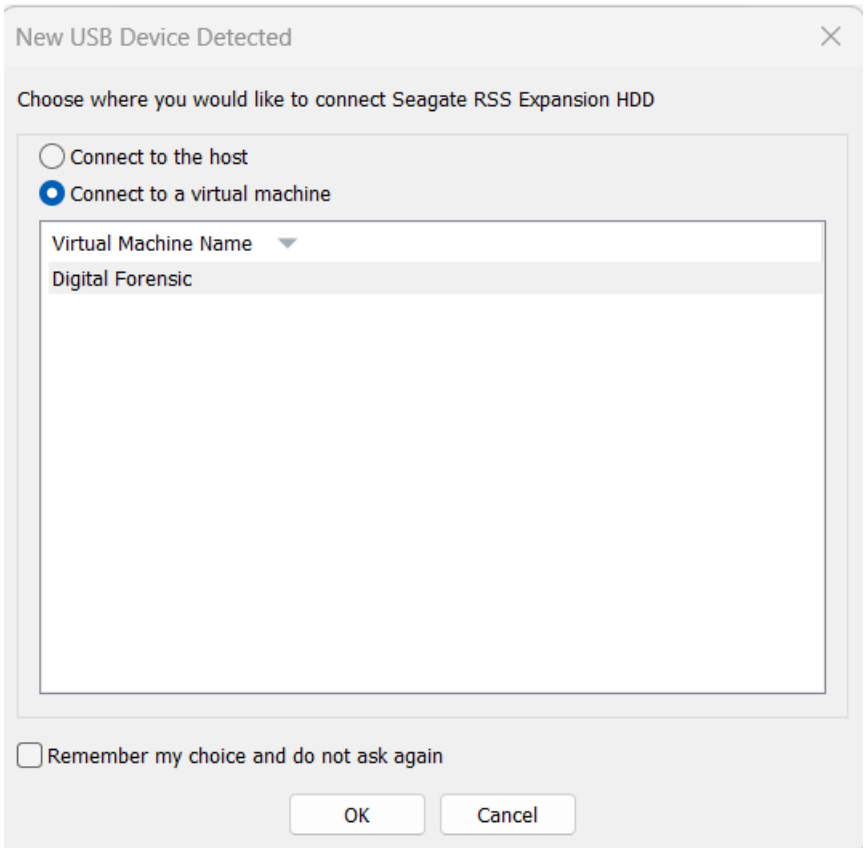




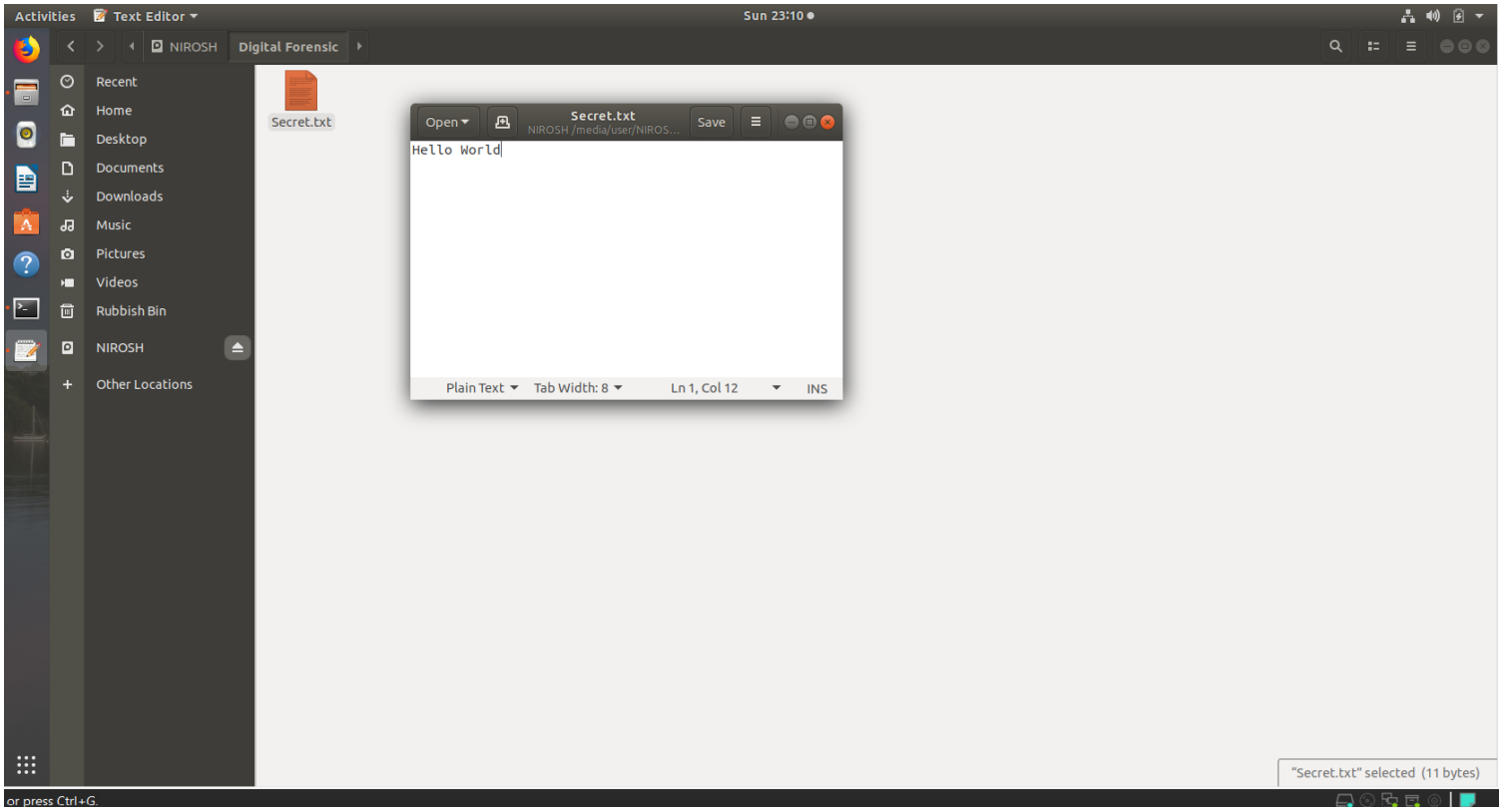
Inside the Secret.txt file I typed a message **“Hello World”**



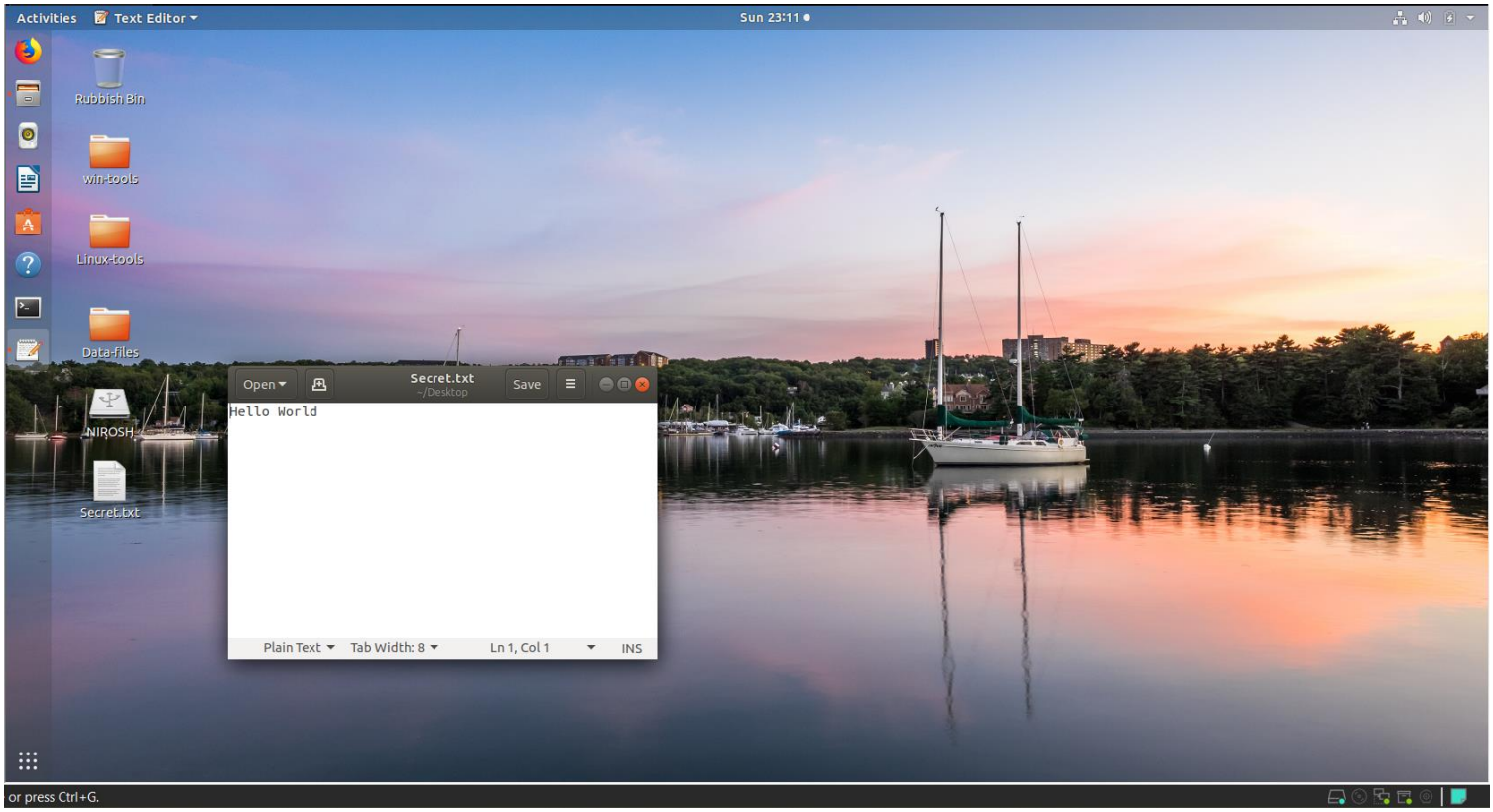
Now I ejected it from my main machine and mounted the drive to Ubuntu VM.



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

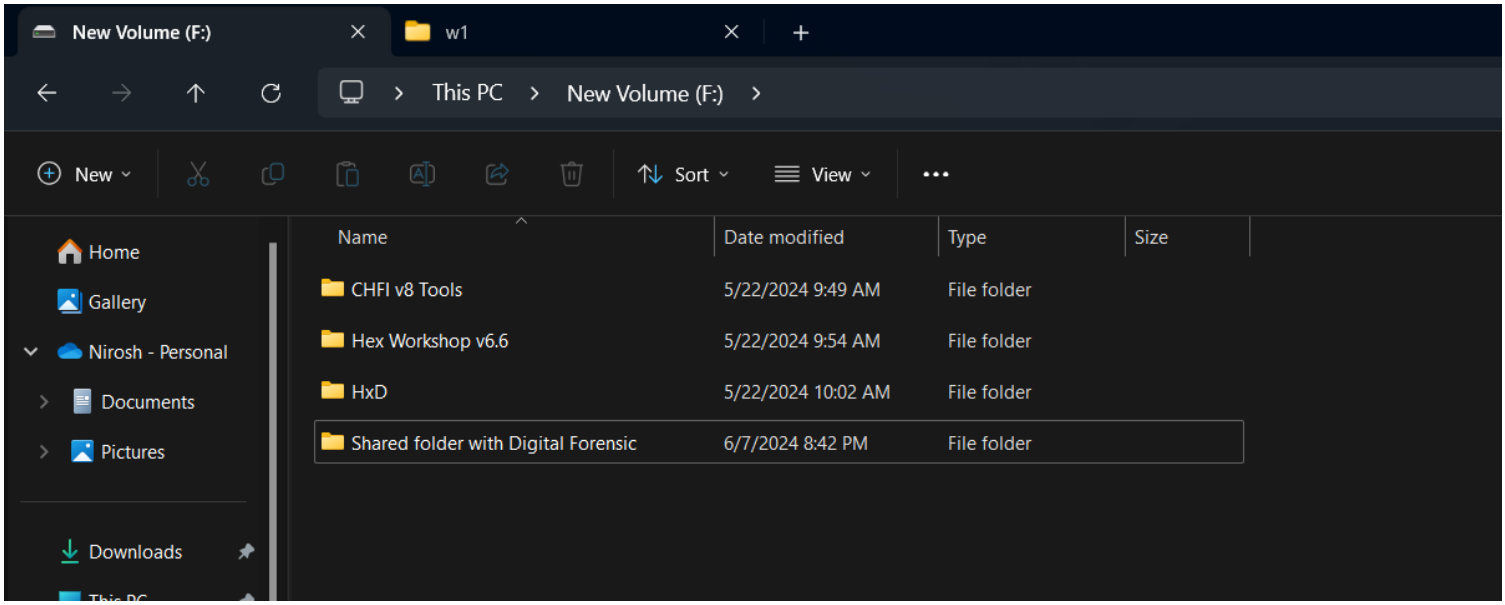


I pasted that file to my ubuntu VM and opened it, it shows the same text which means file sharing through USB works.

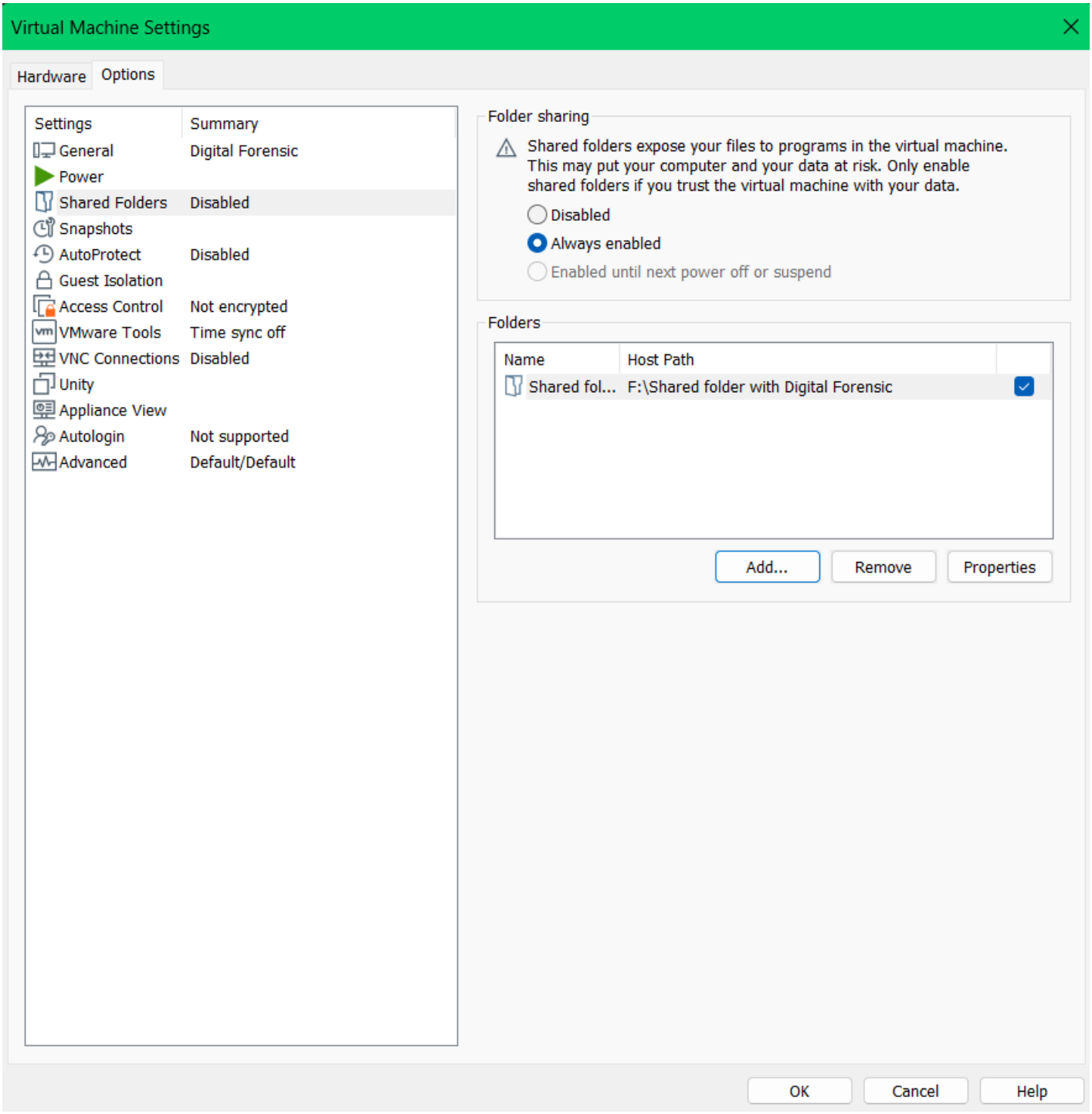
Directory Sharing

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.**

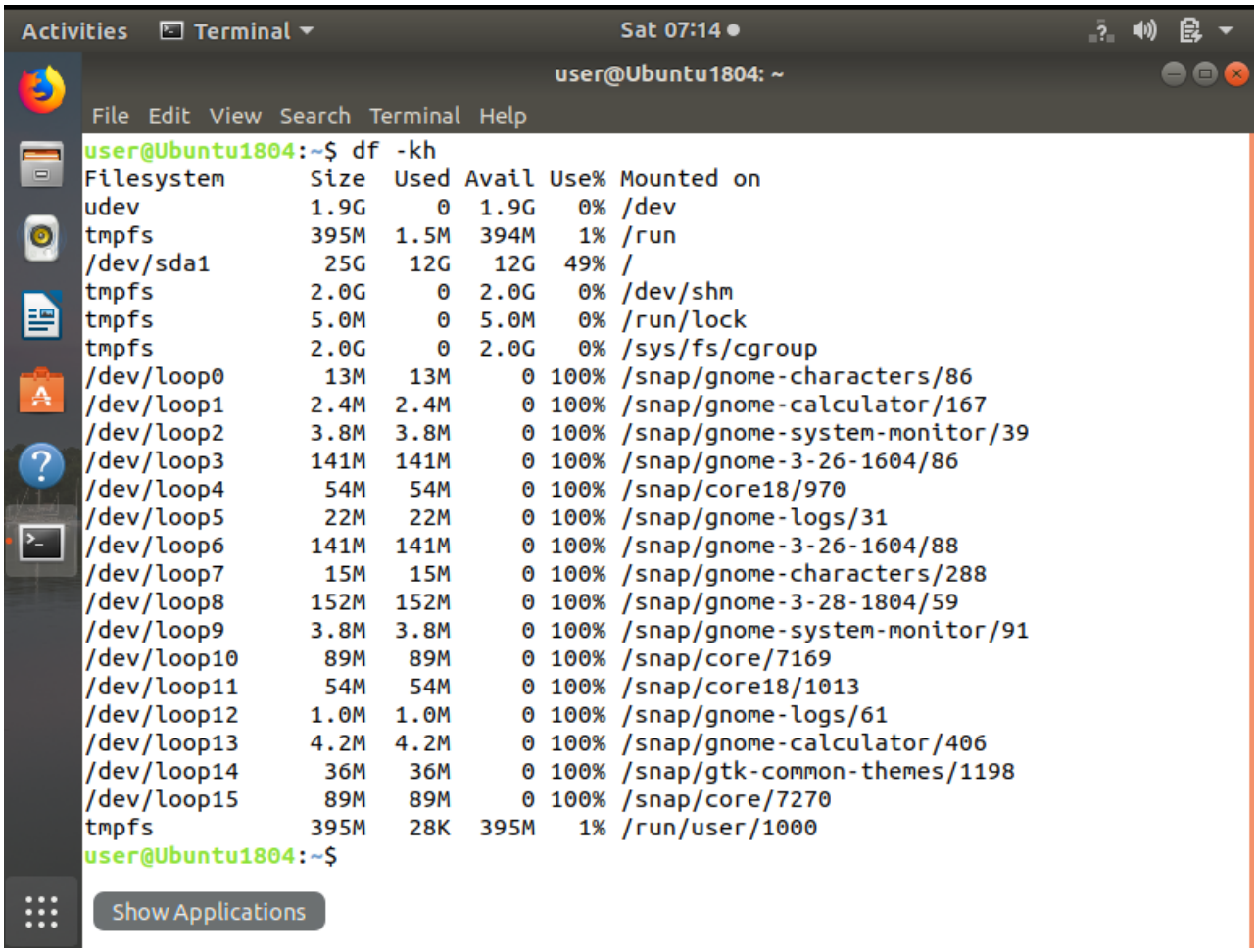


Now I configured the VM in order to allow folder sharing with the host machine. I also gave the destination of the directory to be shared with the VM.

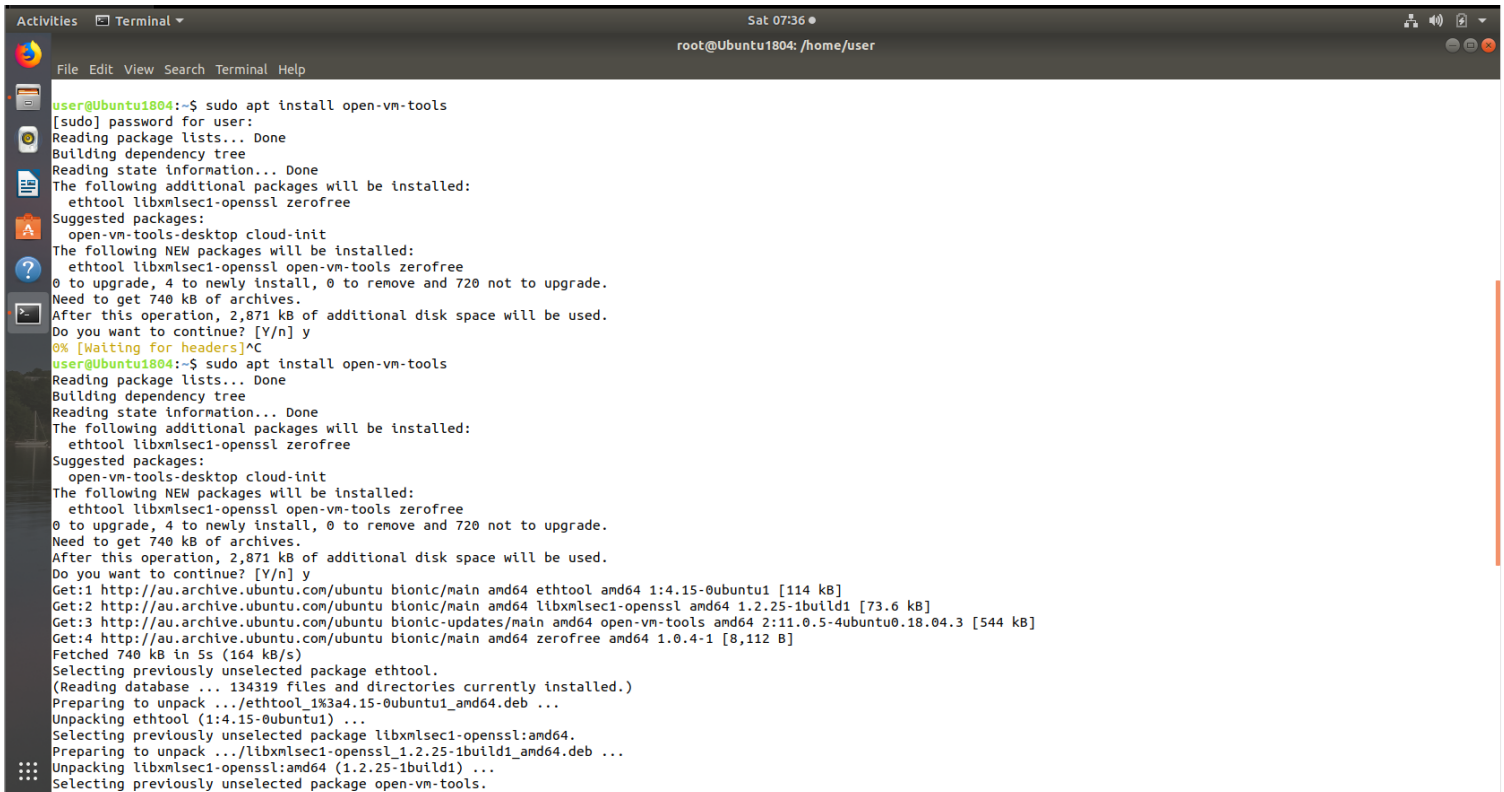


Now I switch on the VM and run some set of commands to mount the shared folder with the Ubuntu VM.

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.



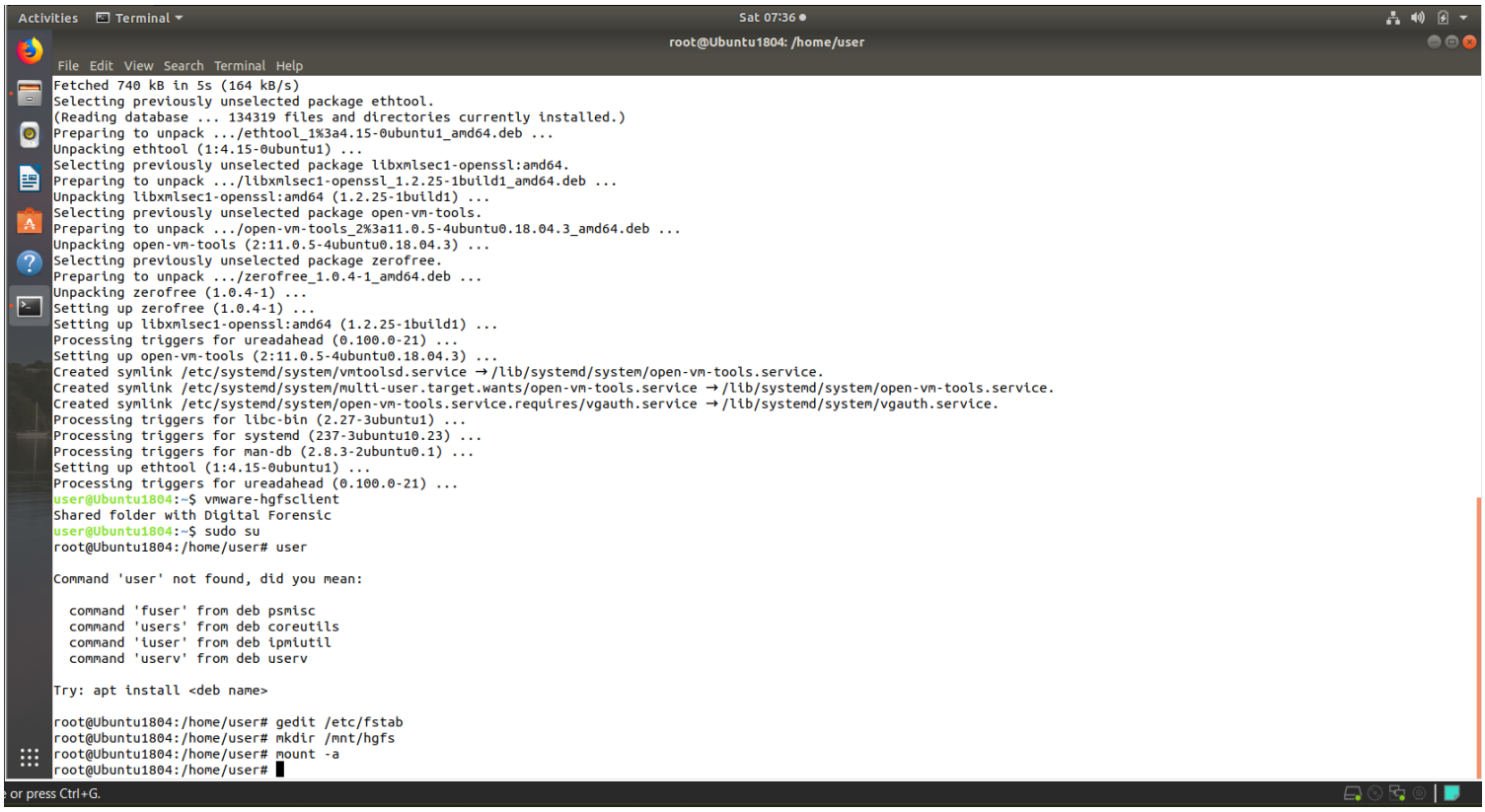
So, for that, I first ran the **sudo apt install open-vm-tools,** the password prompt will be asked and I type it in. then the installation starts and ends auomatically.



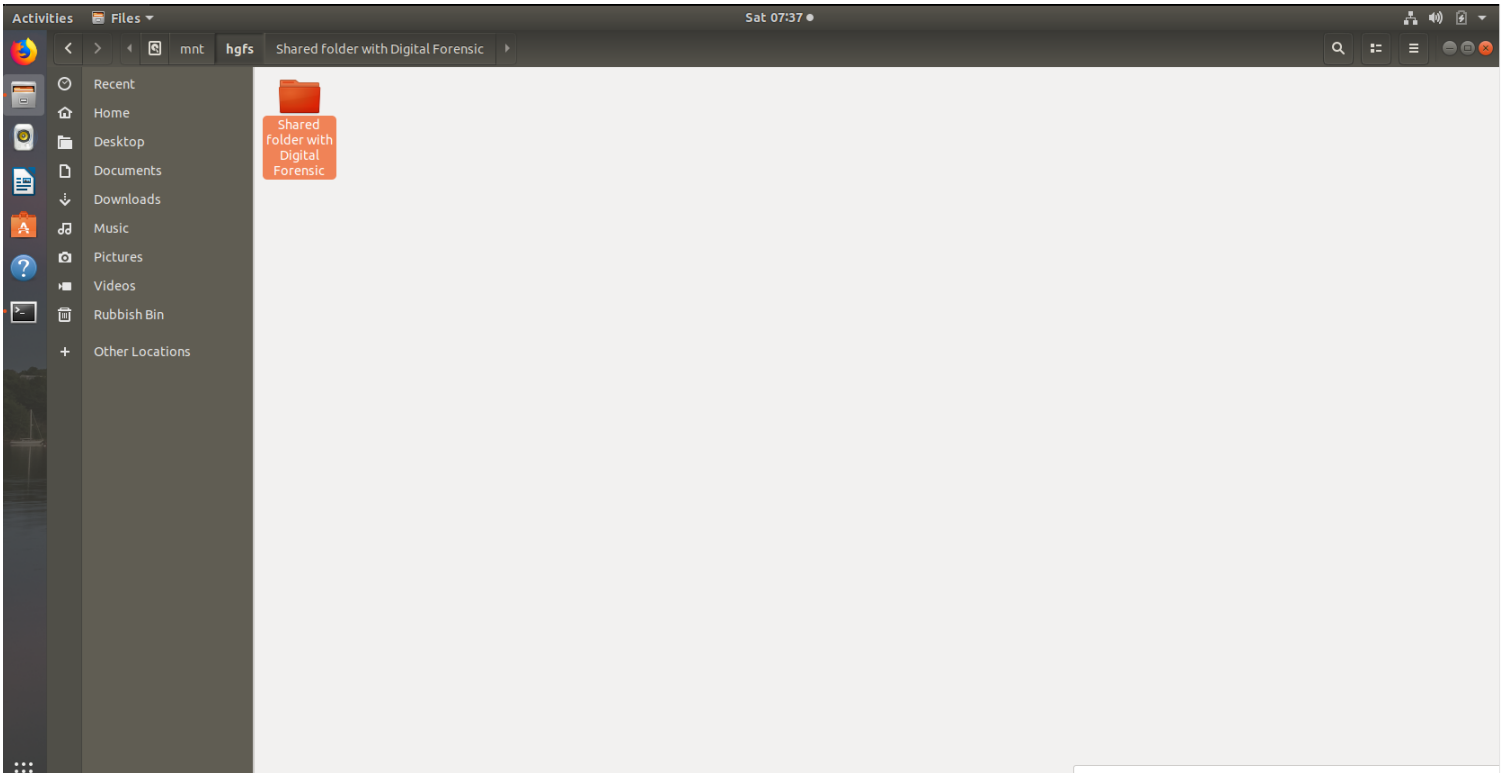
Then I type in the **vmware-hgfsclient** command to find out the shared folder, the folder name appears as the output. From that I become the root user and type in some commands like **gedit /etc/fstab,** to open a text editor to change some rules in that text editor, then I save it and run the command **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.

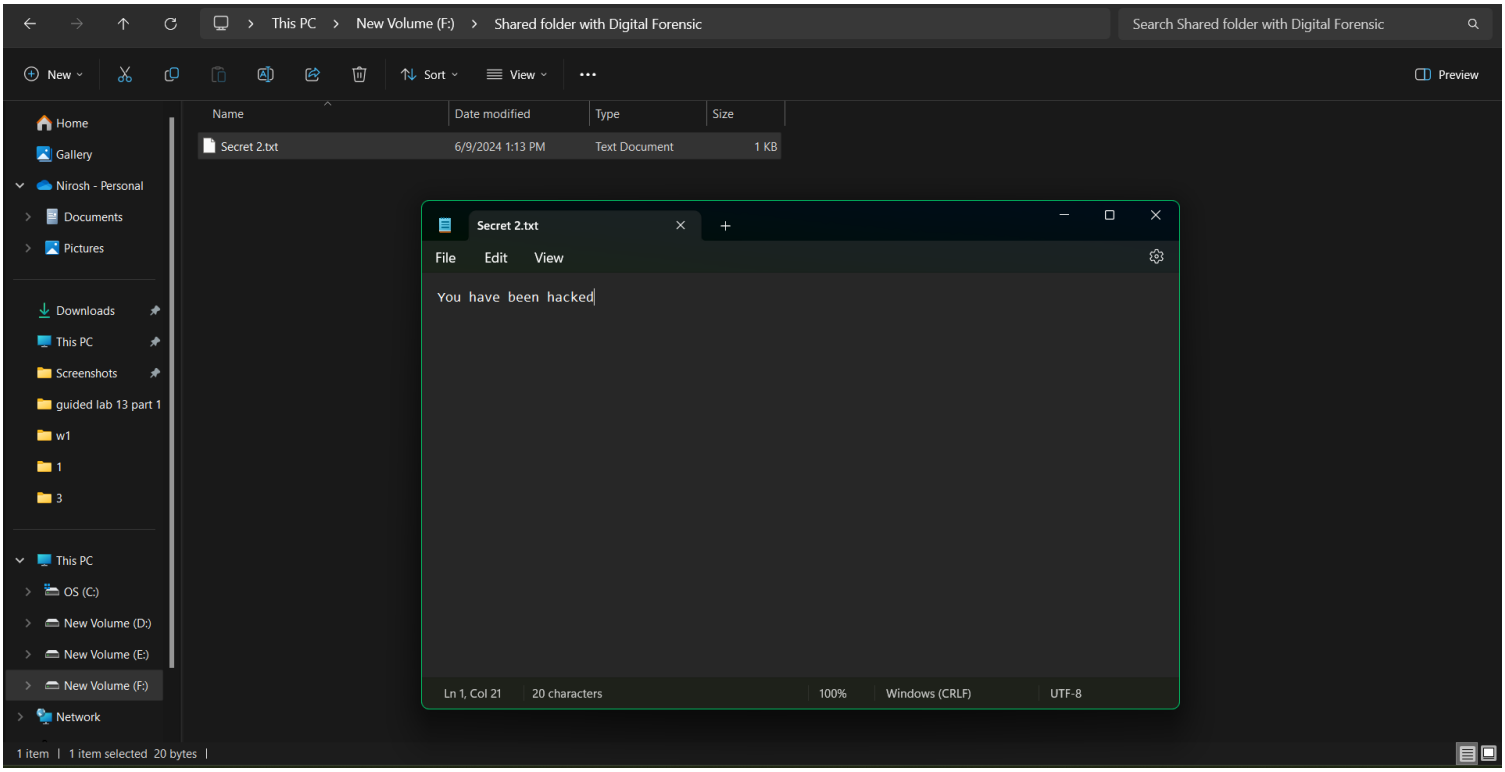
Finally mount the shared folder using **mount -a** command to mount it to the ubuntu VM.



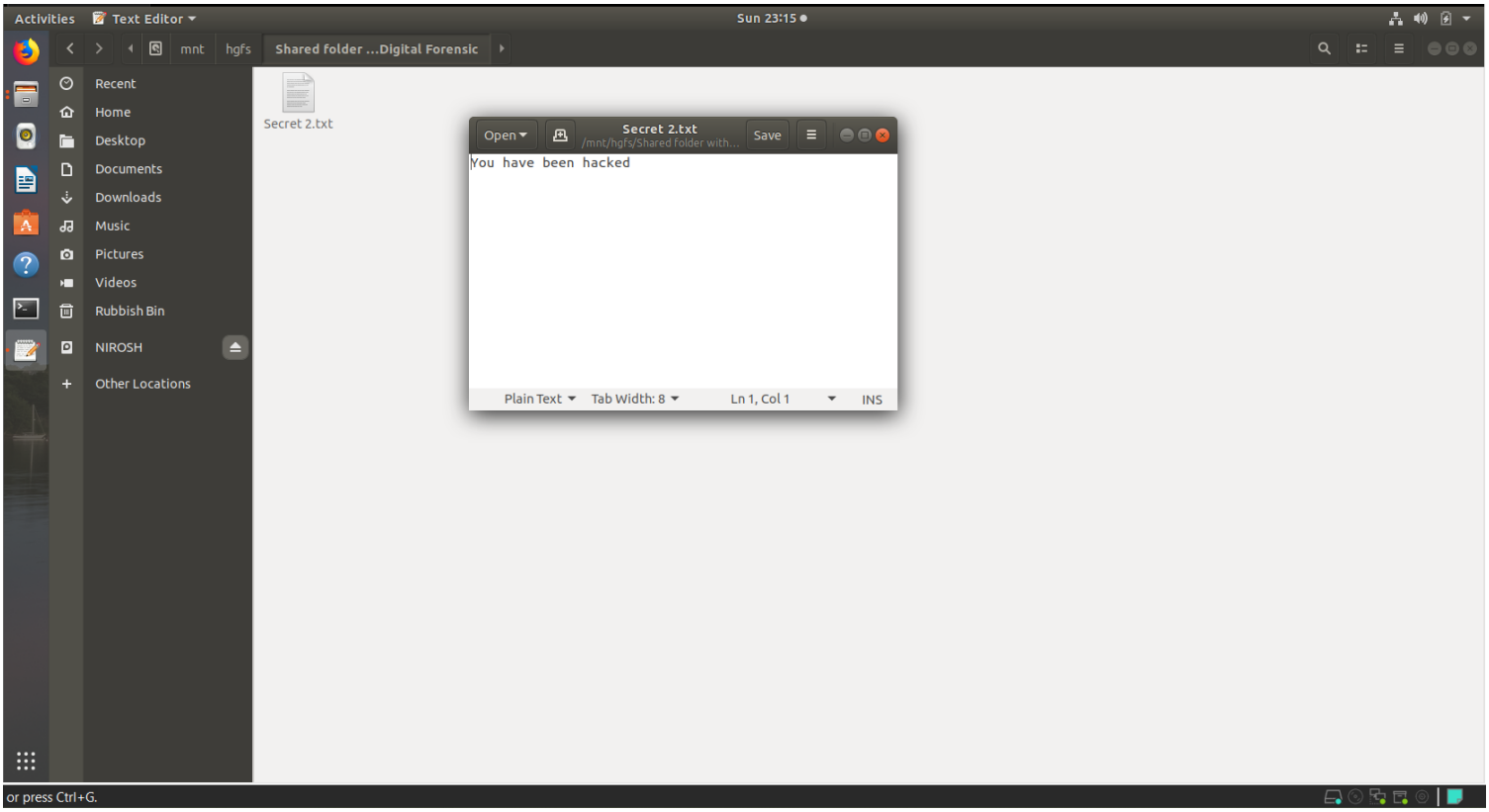
Now if I navigate to the directory I gave earlier, **computer/mnt/hgfs,** I an find the shared folder in this directory.



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**.



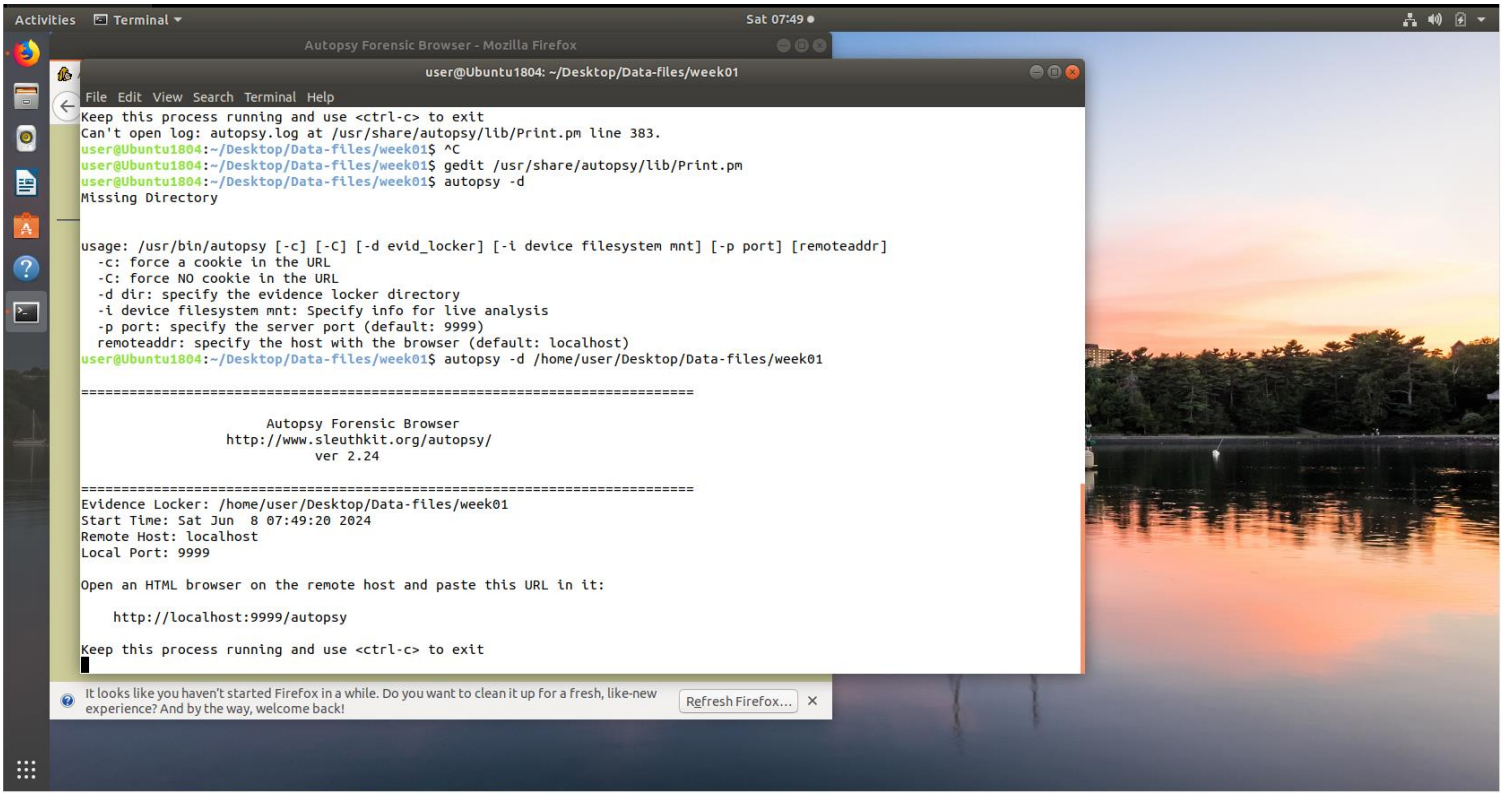
Now I switch back to the Ubuntu VM and checked the shared folder there. I found that the txt file has been shared there as well. So, this way of file sharing is also a success.



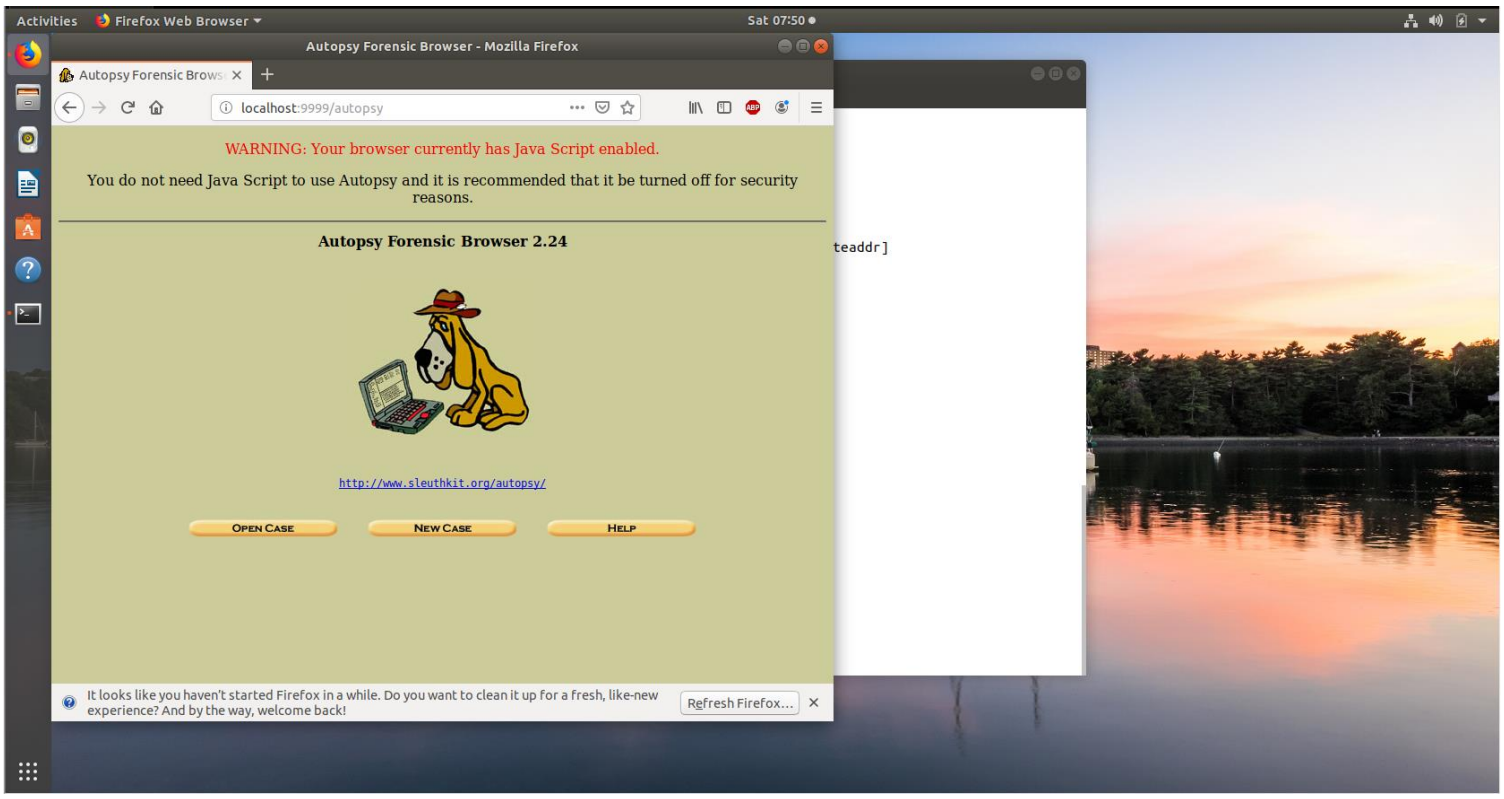
Forensic Investigation with Autopsy

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.

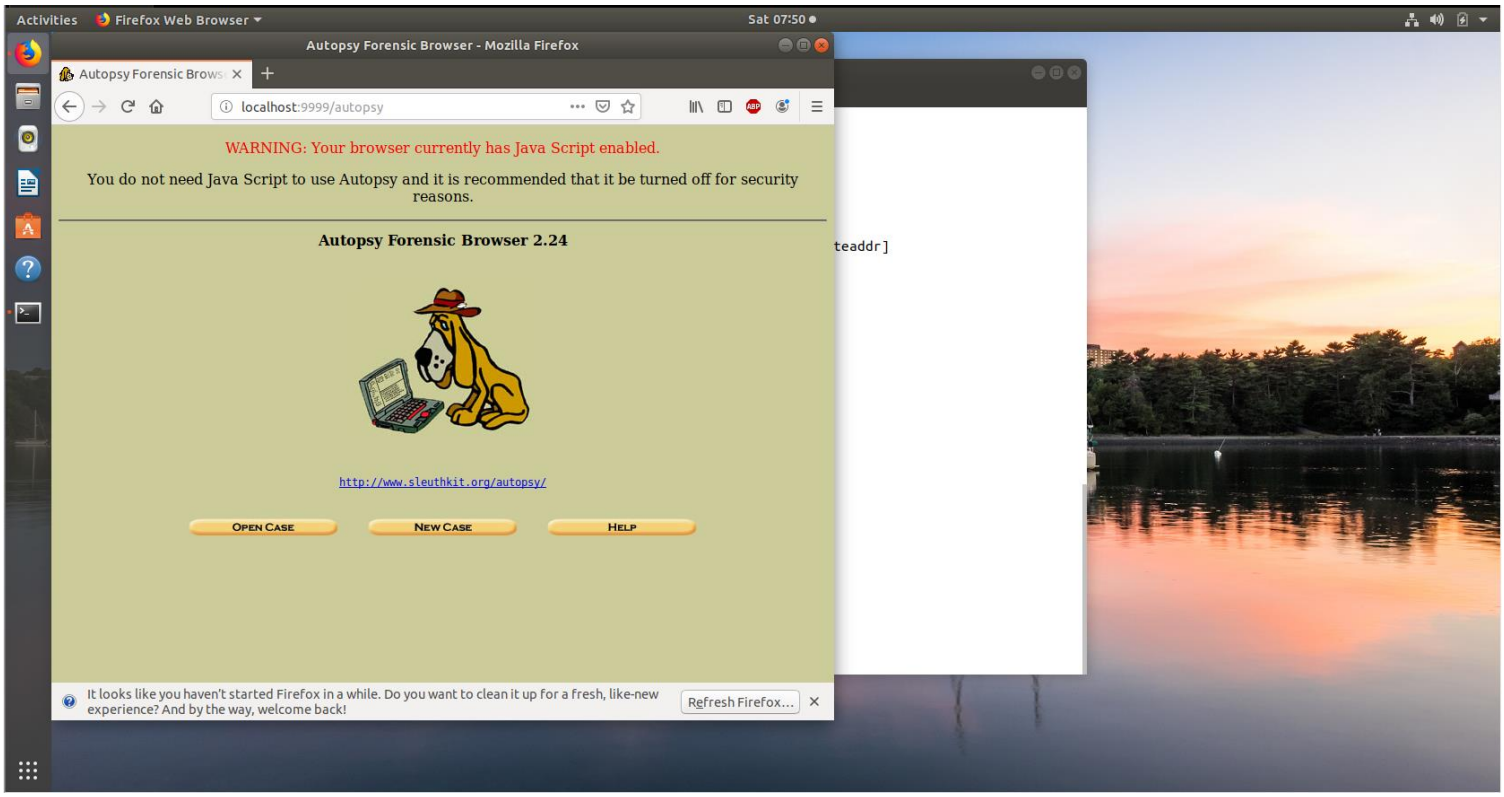


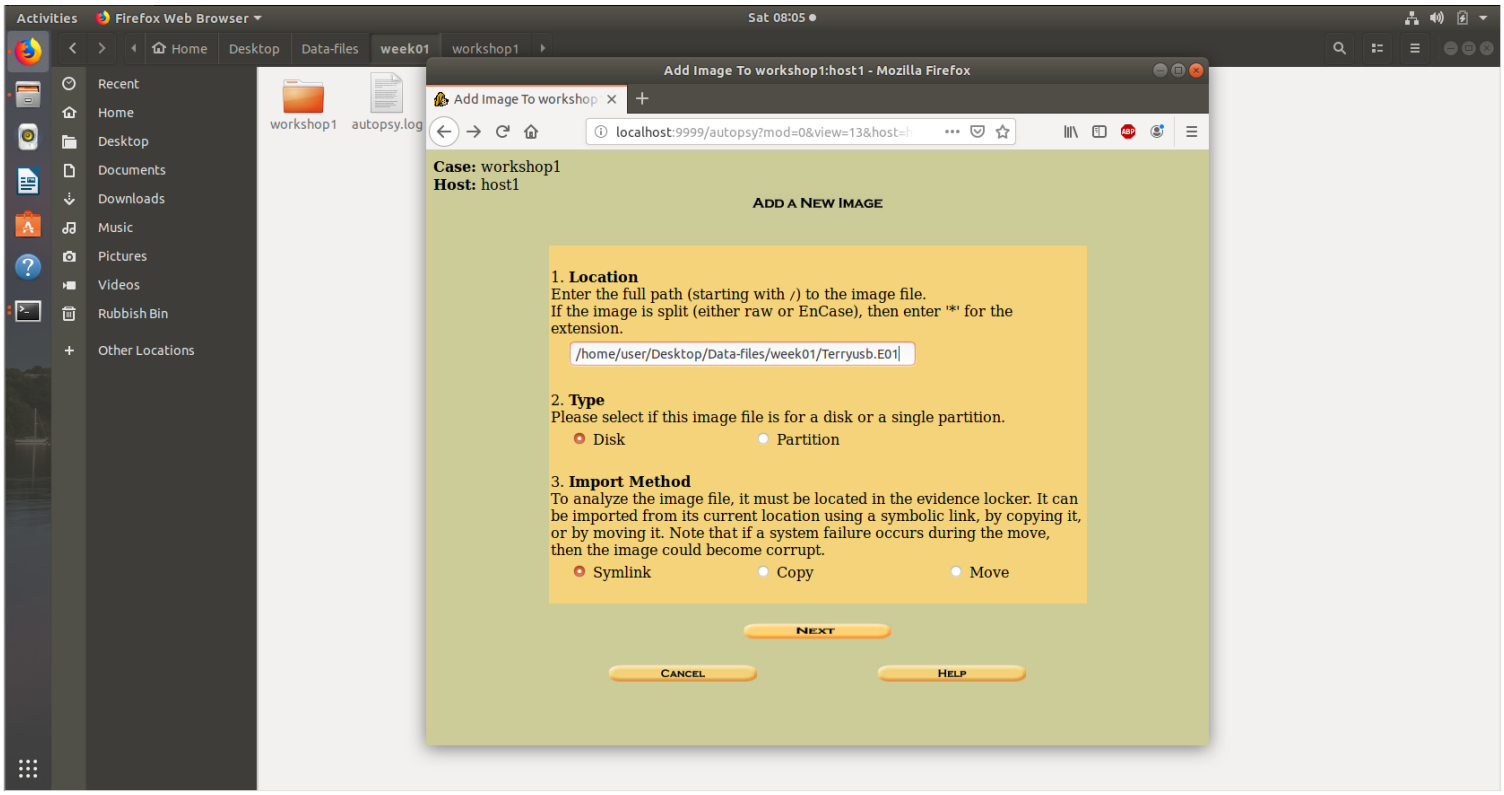
Access Autopsy in Browser: I opened http://localhost:9999/autopsy in Firefox.



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

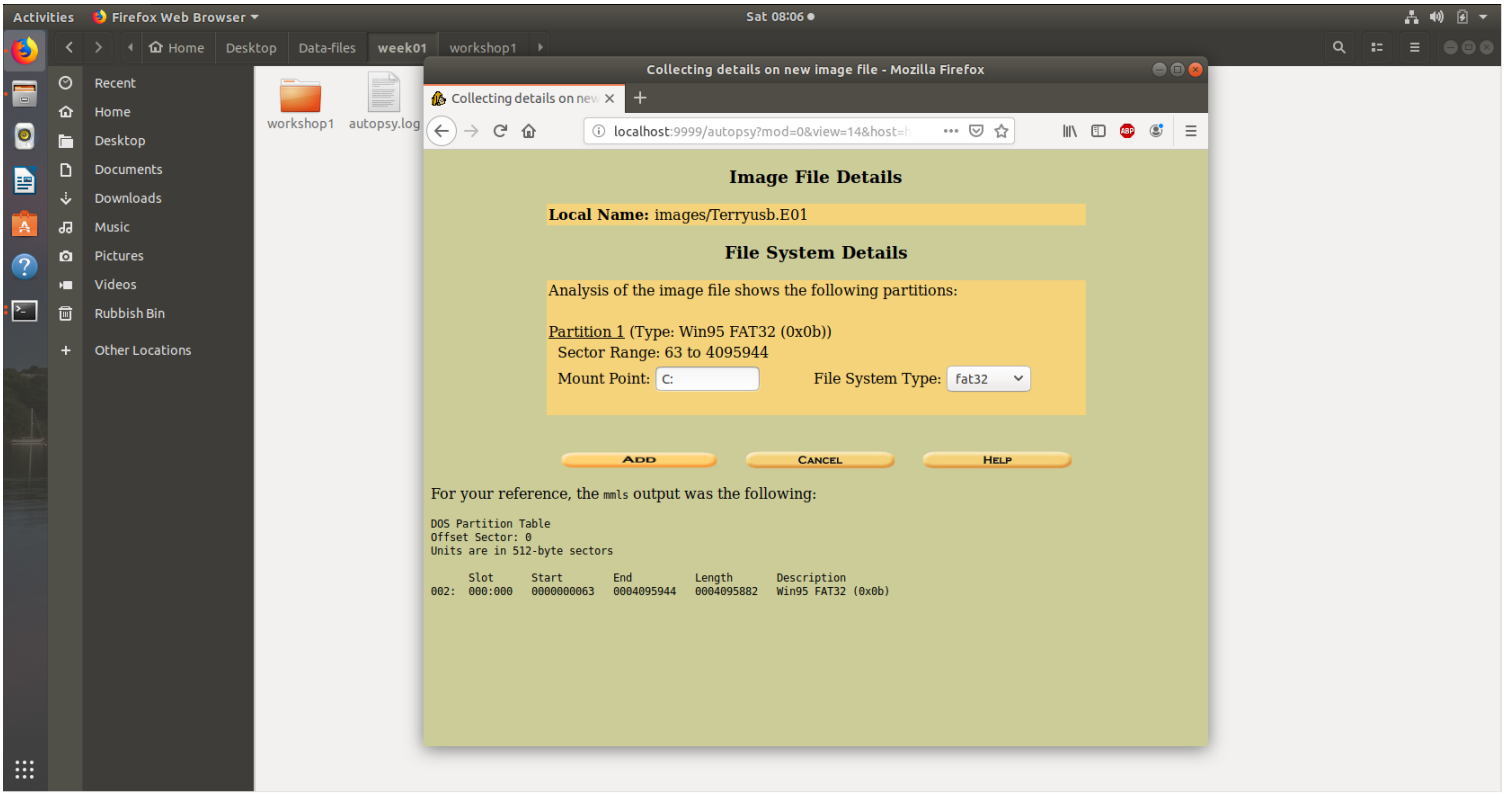
Added a forensic image by specifying the path **/home/user/Desktop/Data-files/week01/Terryusb.**E01 and clicked Next

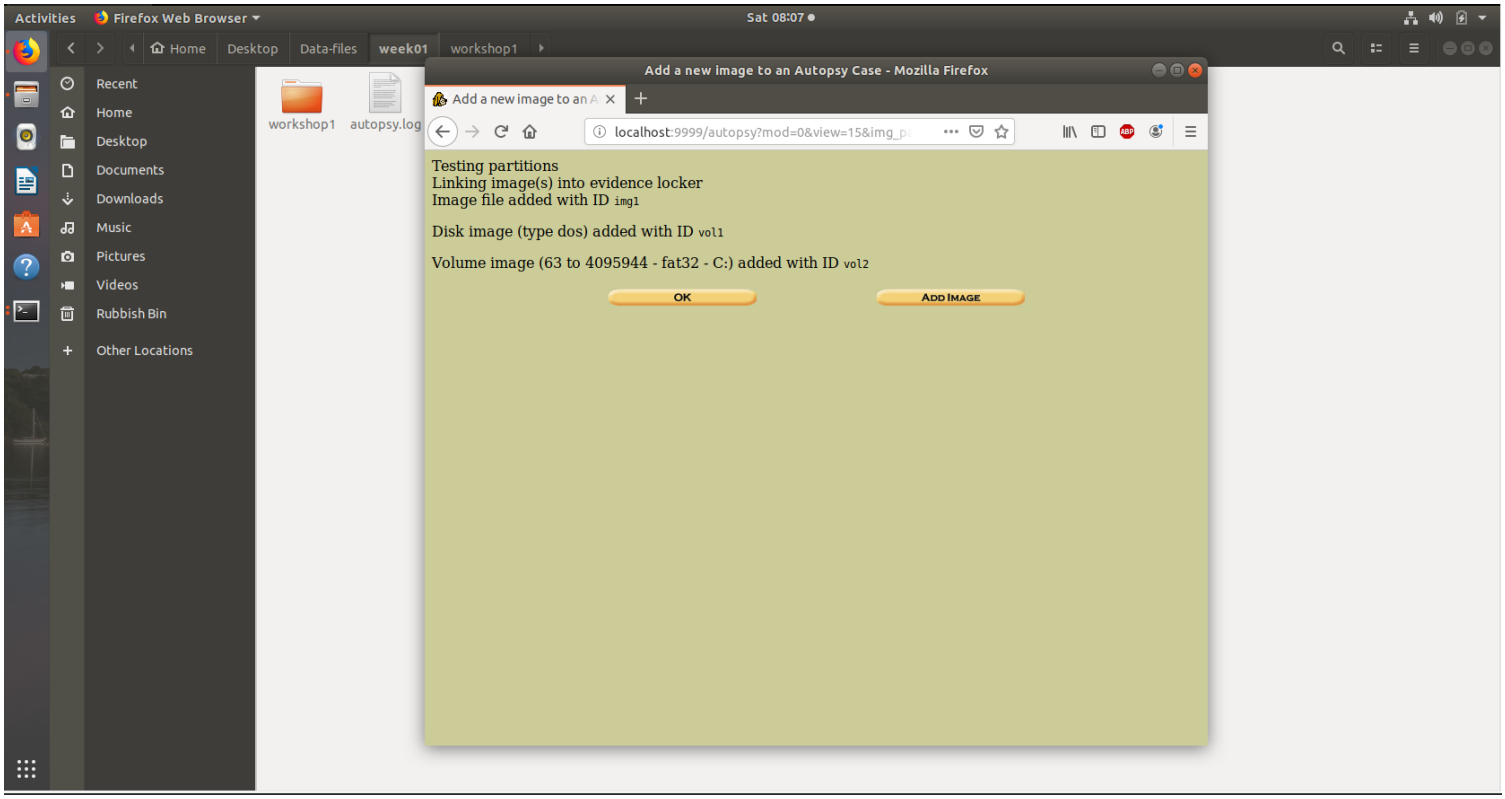


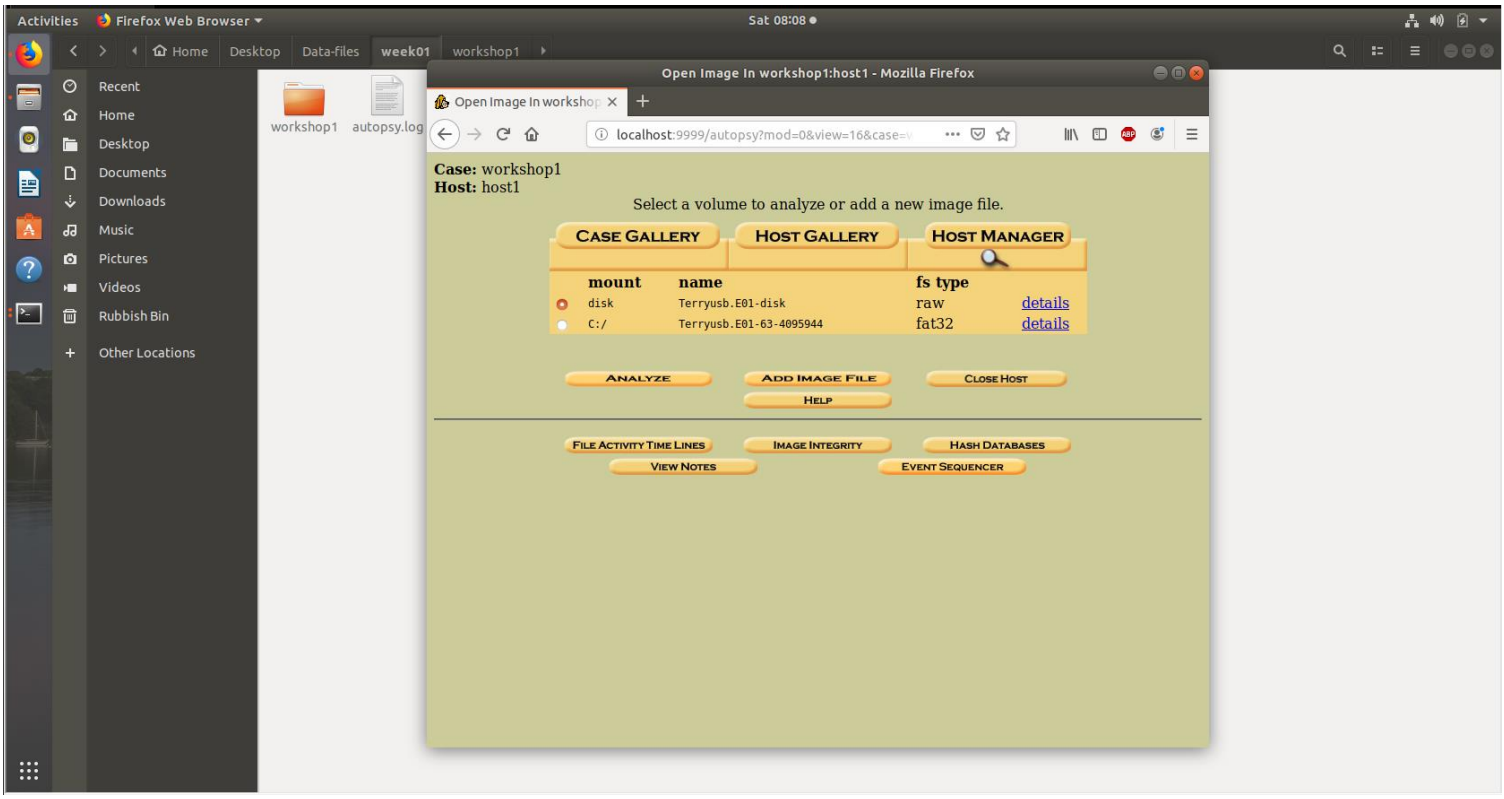


With the forensic image loaded, I began the analysis:

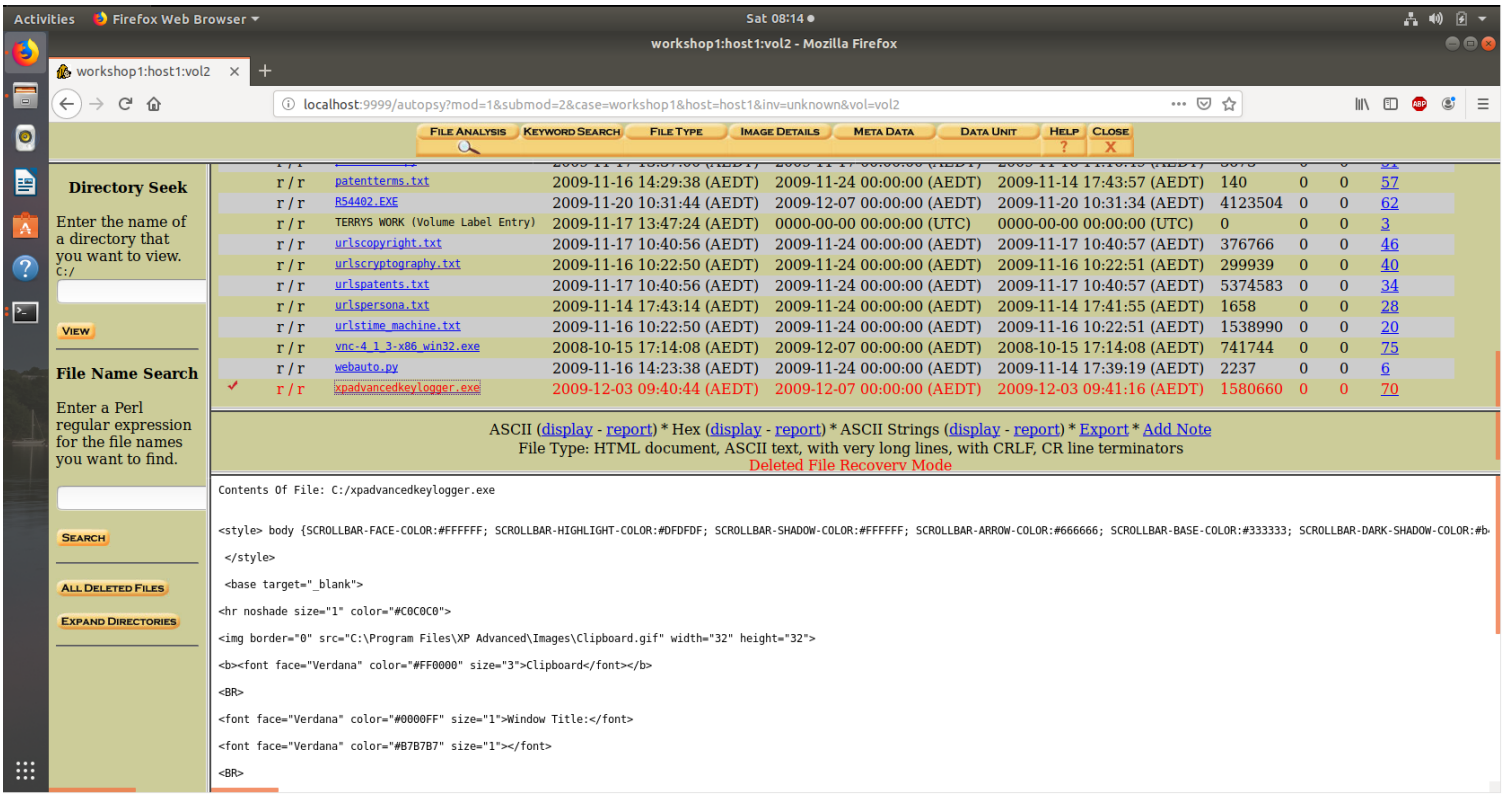
Checked the C:/ option under 'mount'.



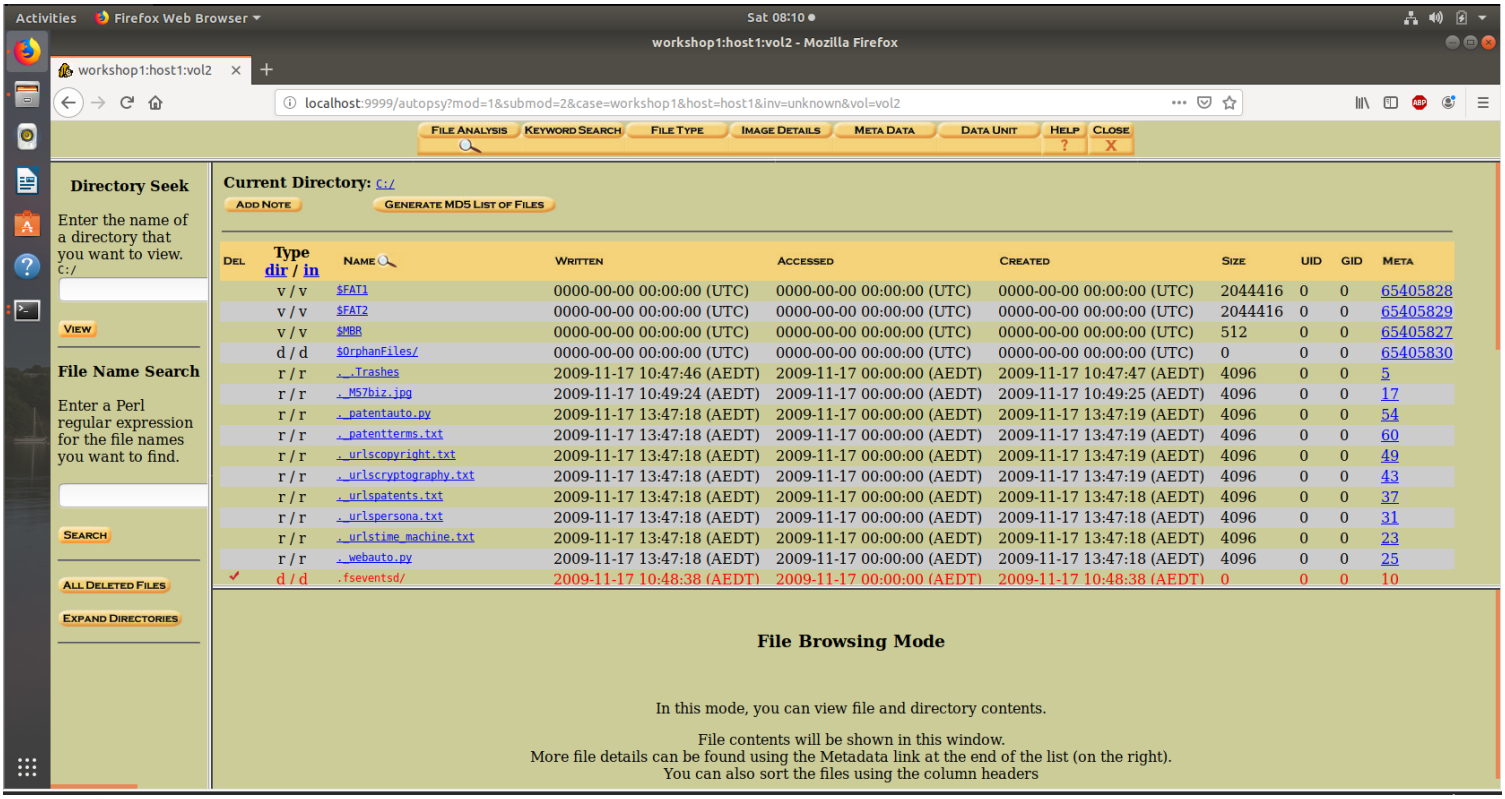


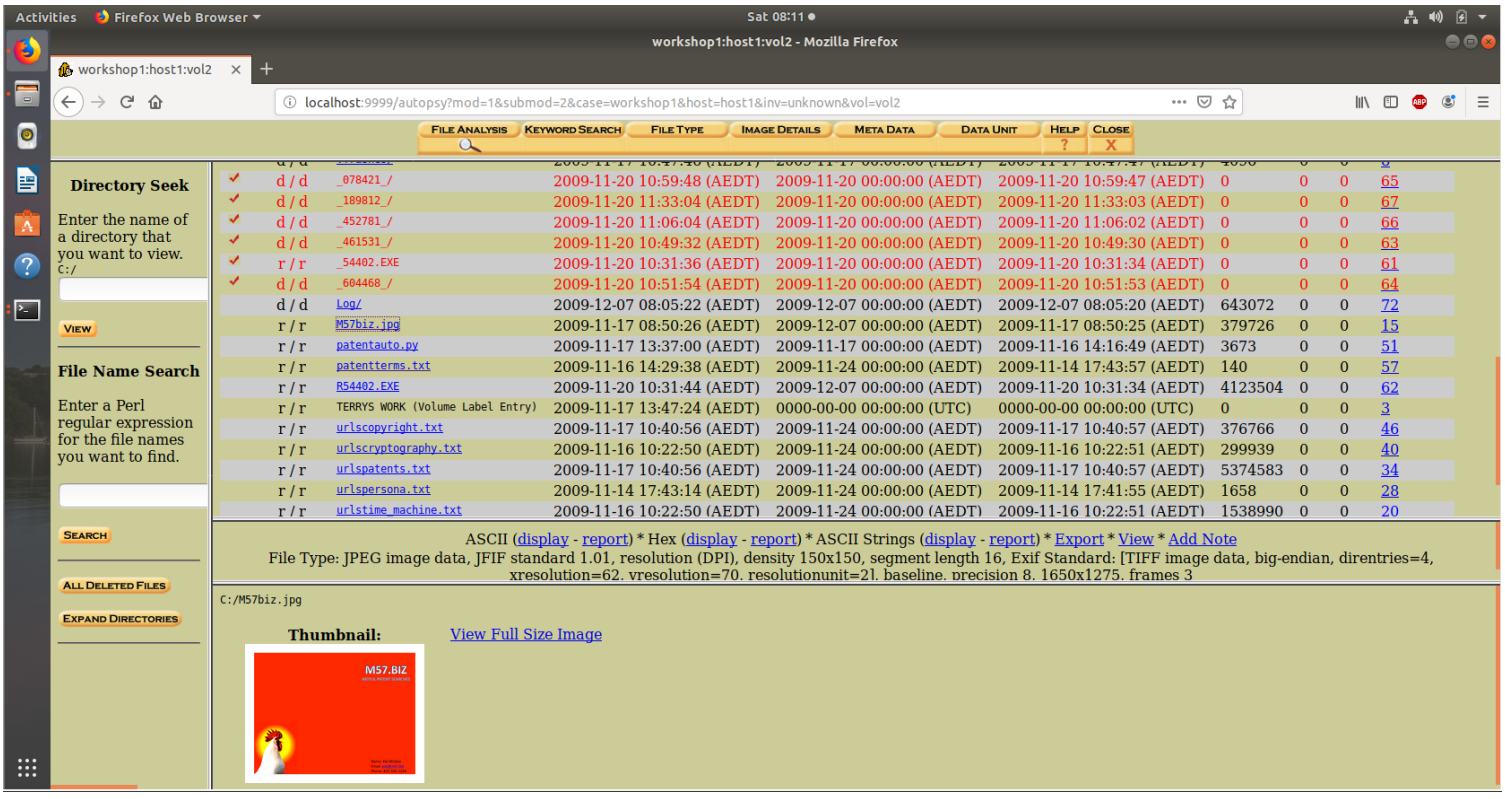


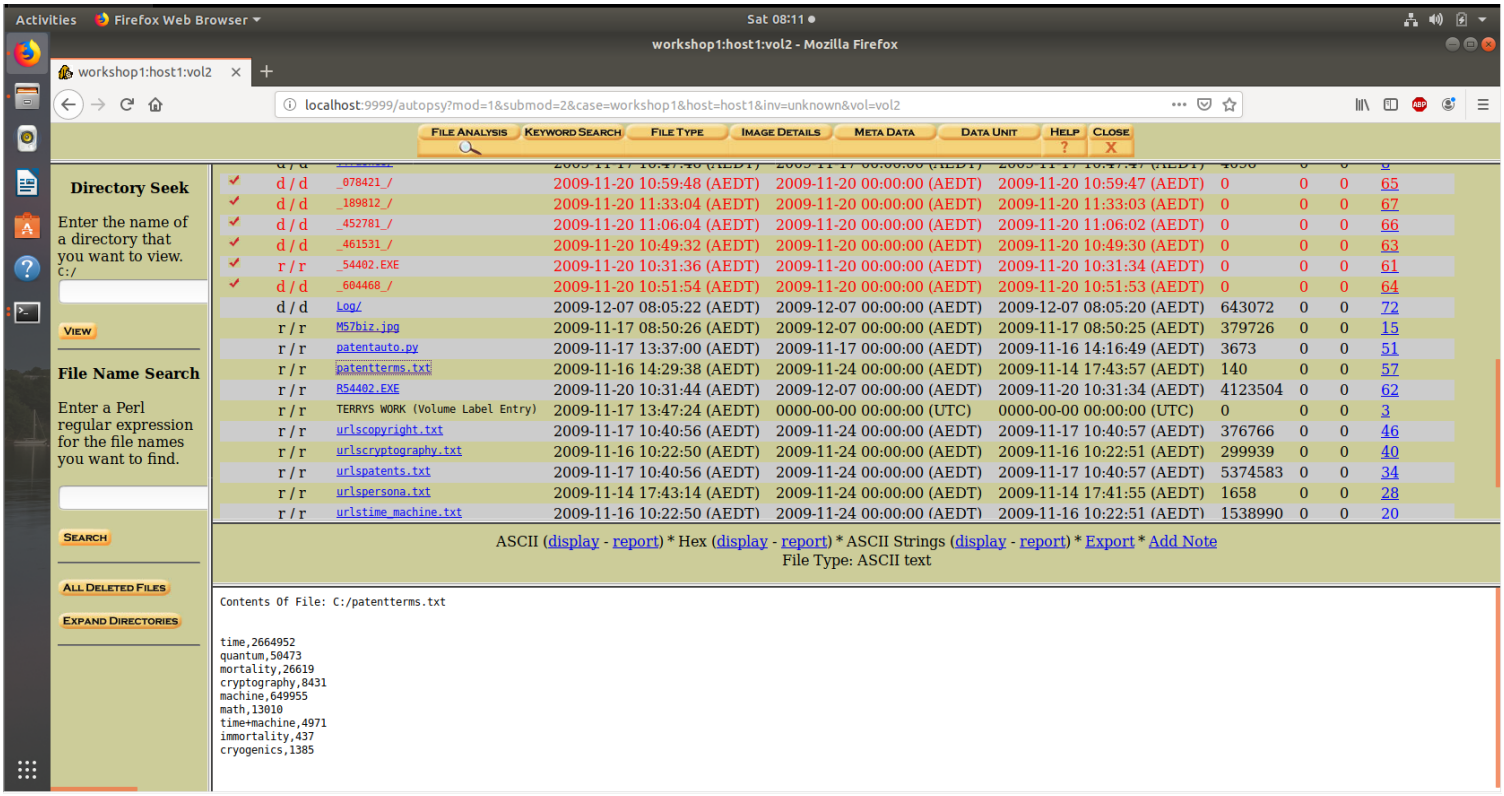
Explored file analysis options, finding notable files like **xpadvancedkeylogger.exe**.



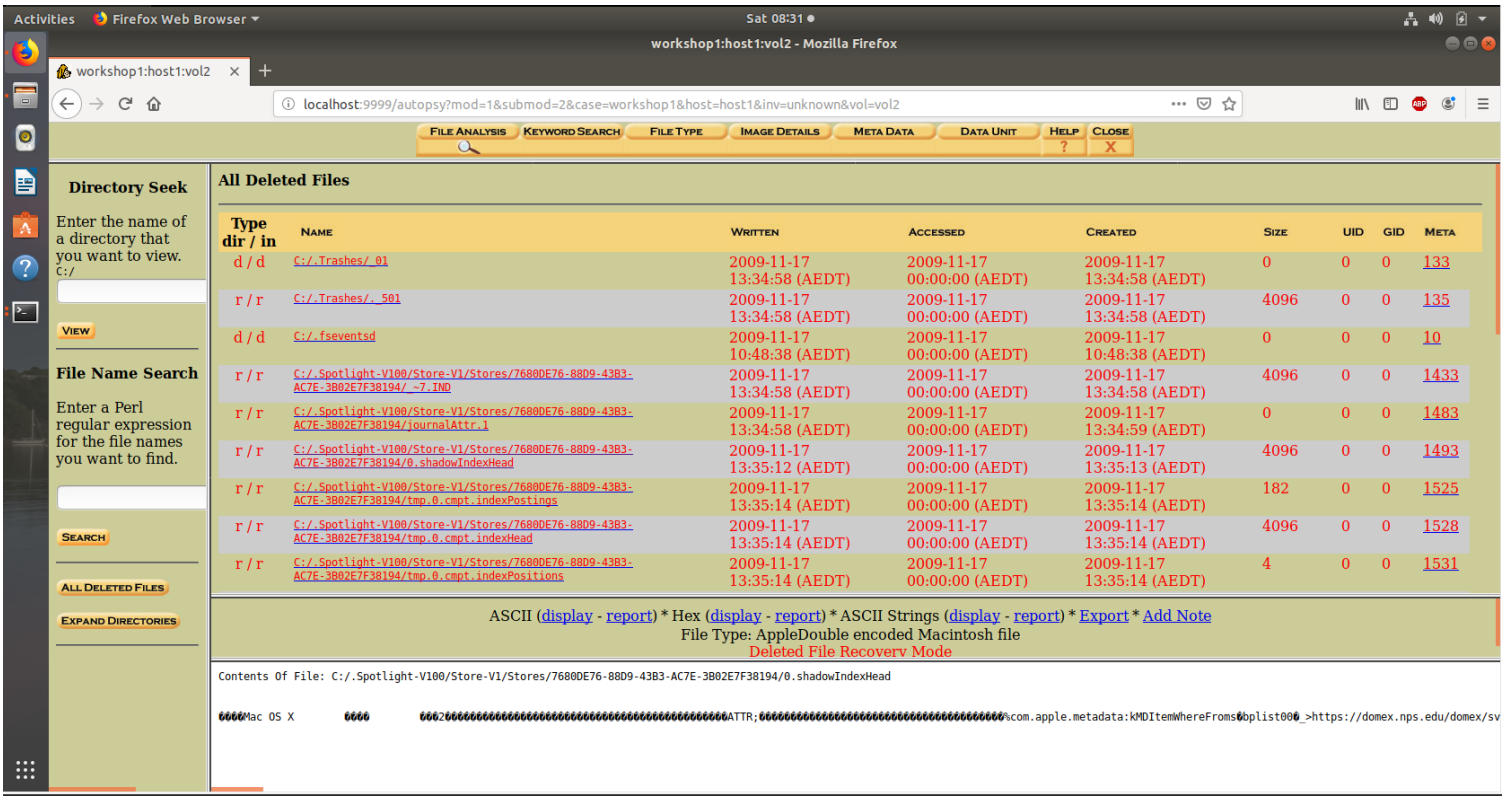
Spent time exploring the case, taking notes on any anomalies or suspicious files.



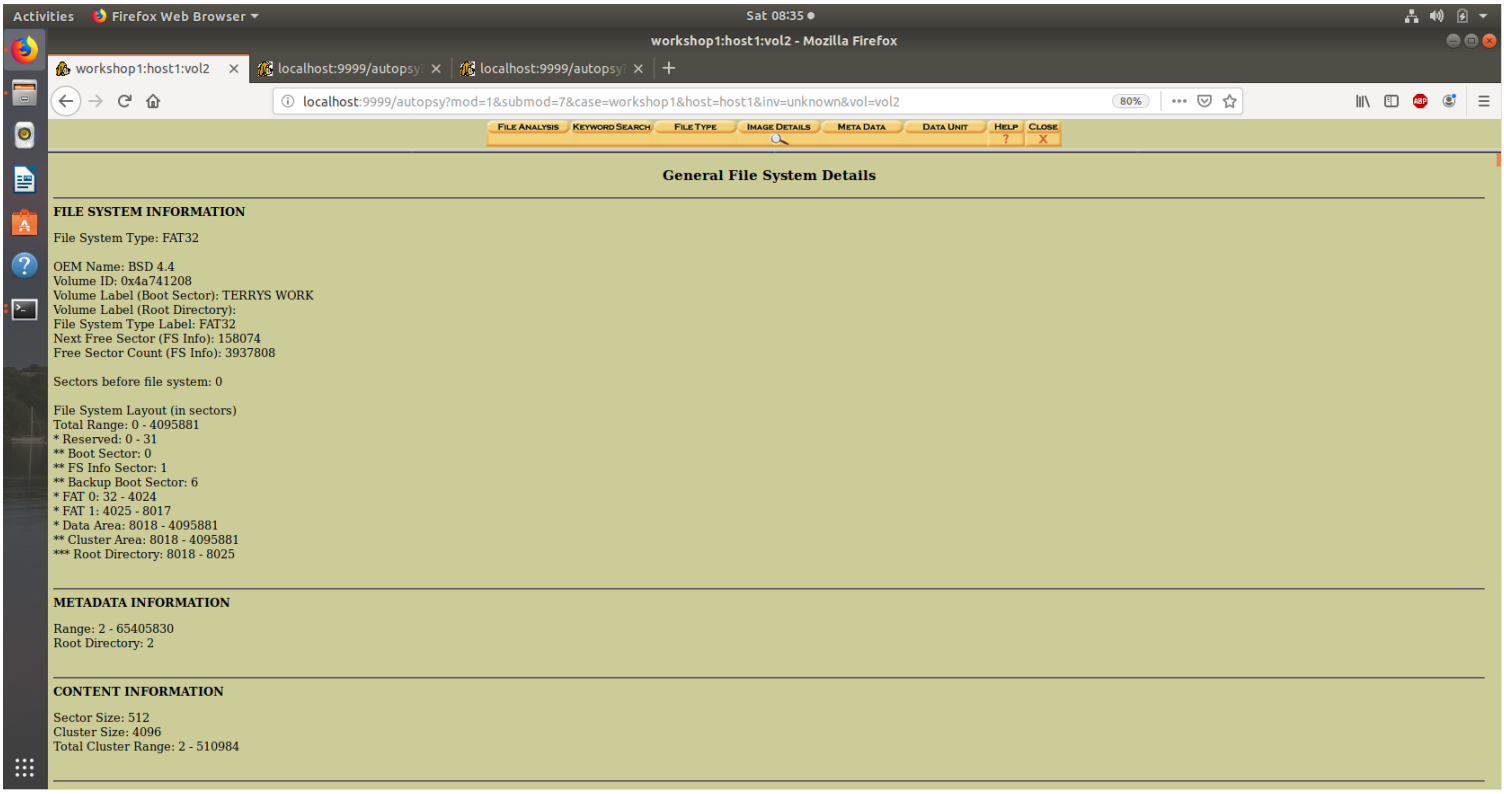




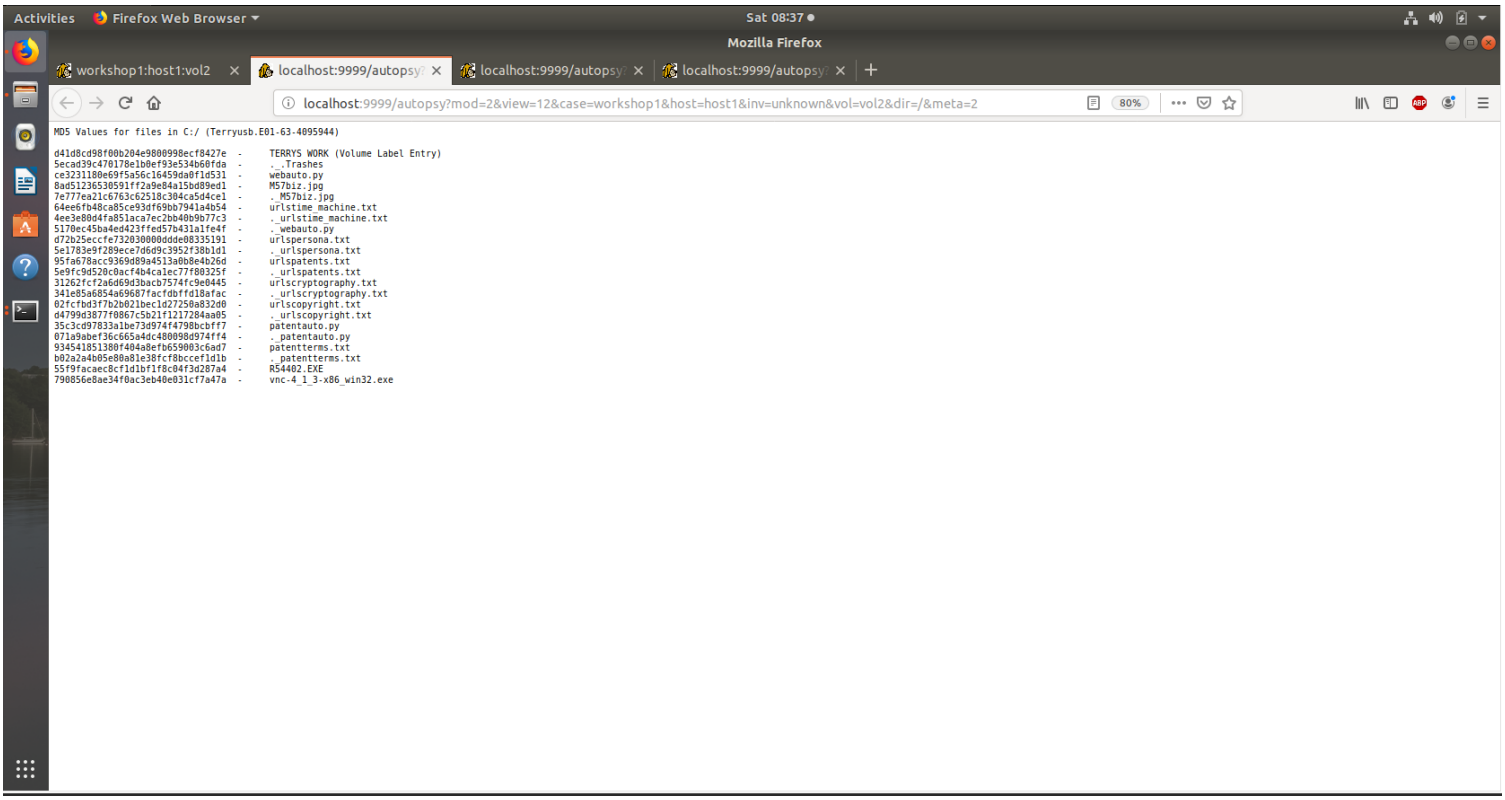
Then went through the deleted files



File system information



MD5 hash values



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.