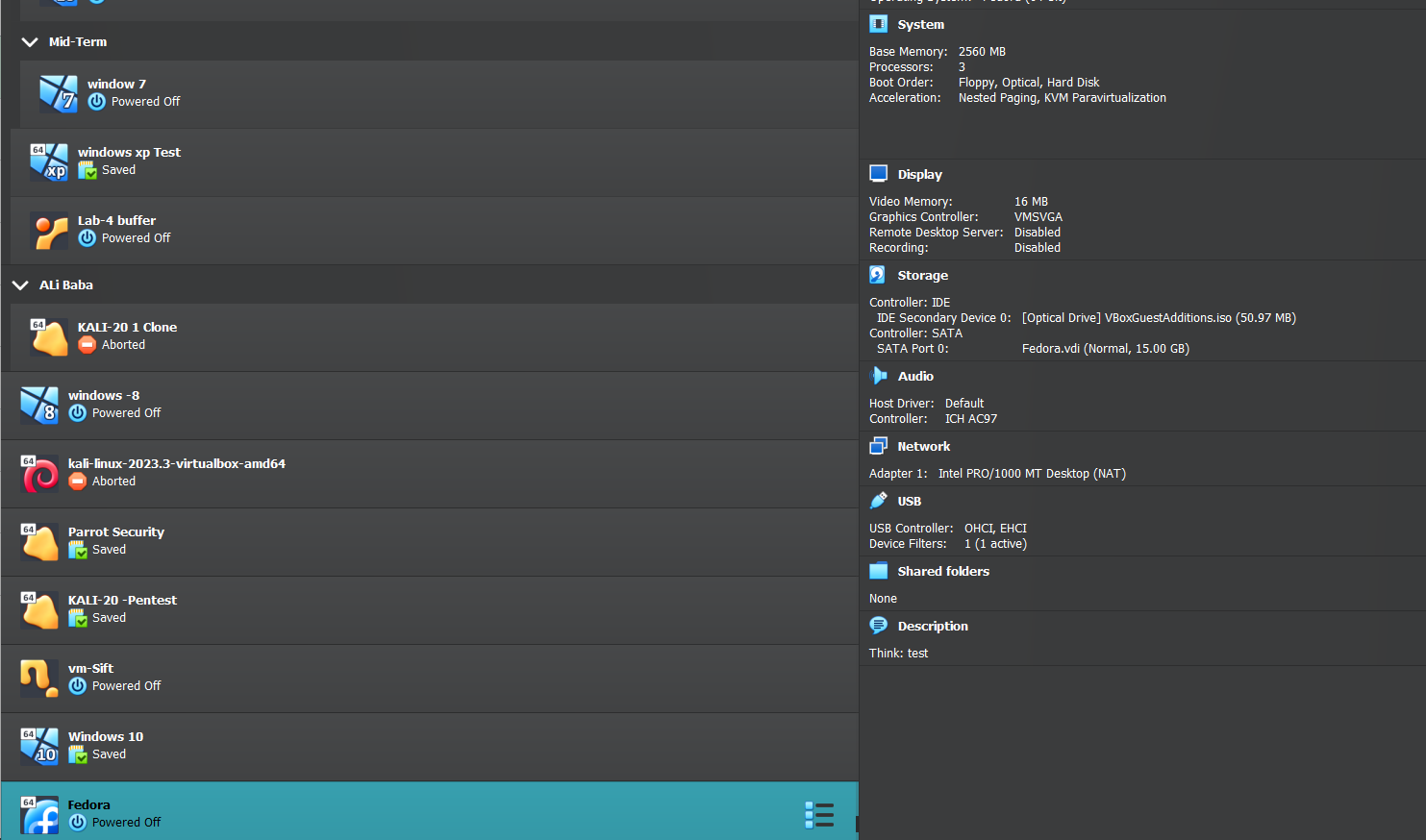
Lab-6 Final

Write a report - this report should reflect a using your preferred platform (windows or Linux) to live capture of a USB partition (needs 2 files on it).

You need the following in your report - a description of what you did..

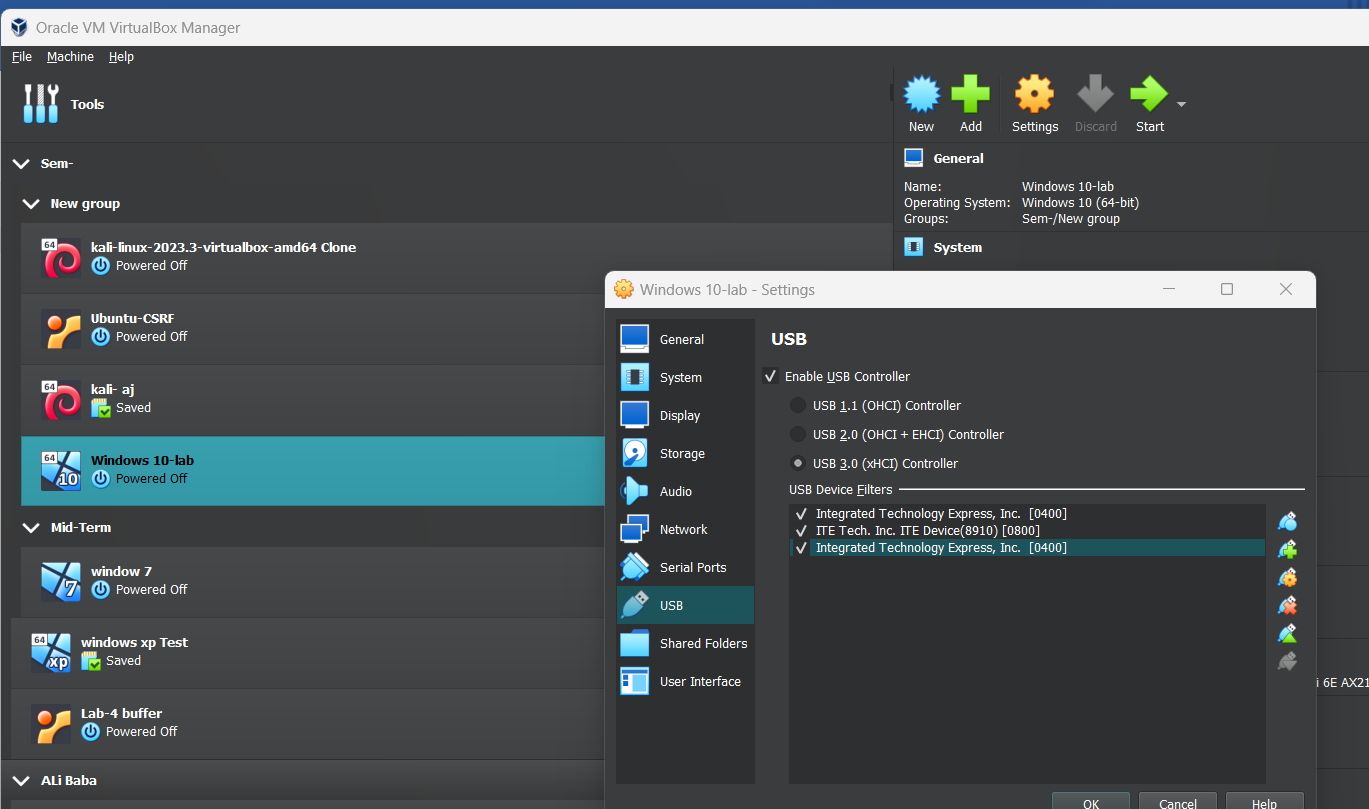
Include the following:

* My preferred platform for working is Linux. Because it’s easy to use and I can use command to basically to everything from Terminal and started hating windows after going through the logs.
* I used Virtual box and VMware for doing my labs. I like Virtual box because I have been using for long time and got used to its interface, but I think VMware is good and trying to learn how to use it, they give pop-up whenever we try to external device to the host machine giving us option asking you want to connect it host machine or to the VM. Which isn’t case with Virtual box.
* I use kali almost all the time, as we are told not use kali for doing the labs. I started again using my old favorite Parrot OS after long time and tried using SIFT OS (not installed, but going to try once done with finals).



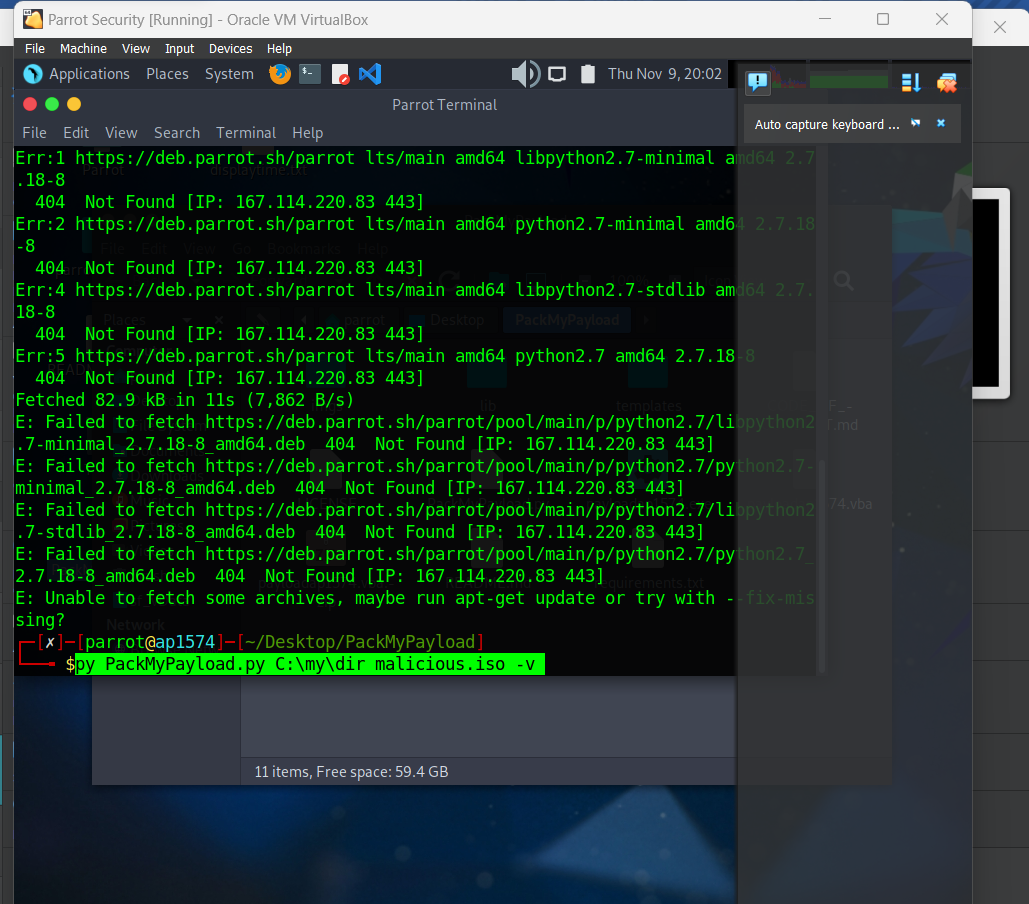
Screenshot of Virtual box showing that I have fedora, parrot os, sift(need to setup) and ubunut(aka Lab-4 buffer)

* The below screenshot is from virtual box showing option to add the USB drivers to the vm.

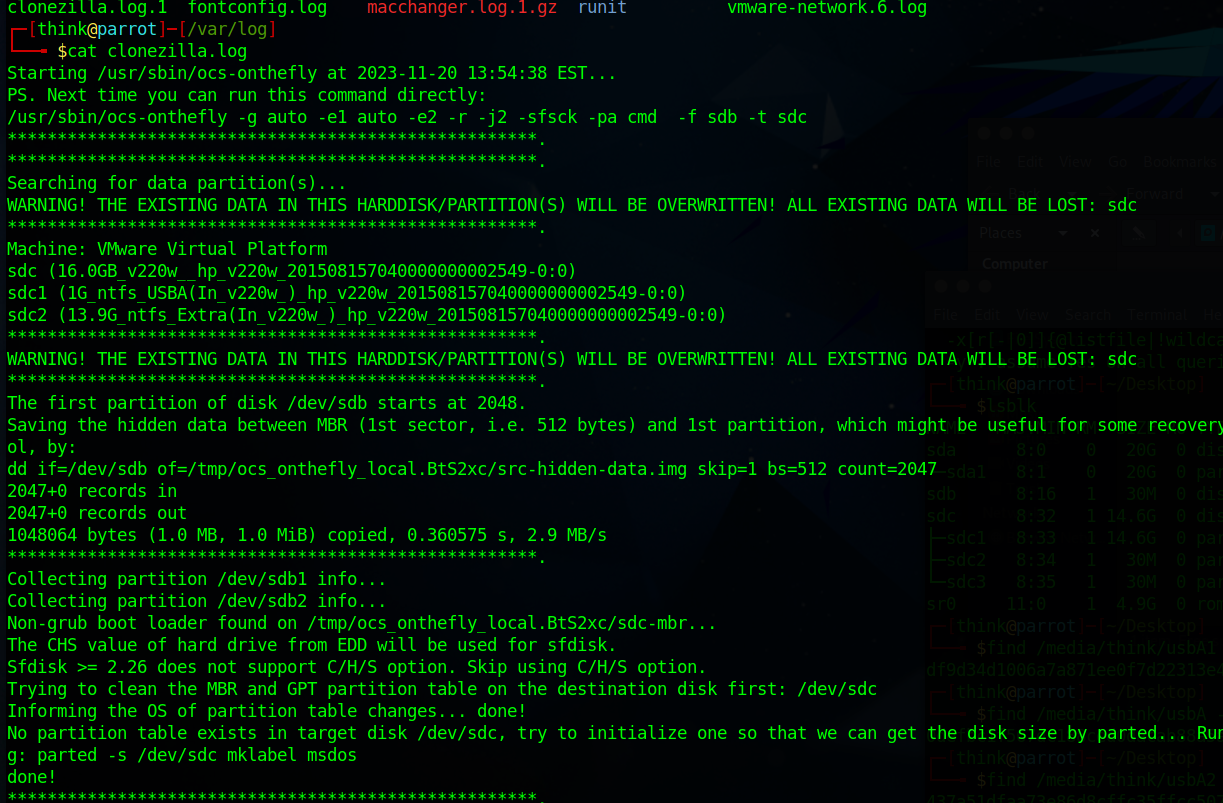


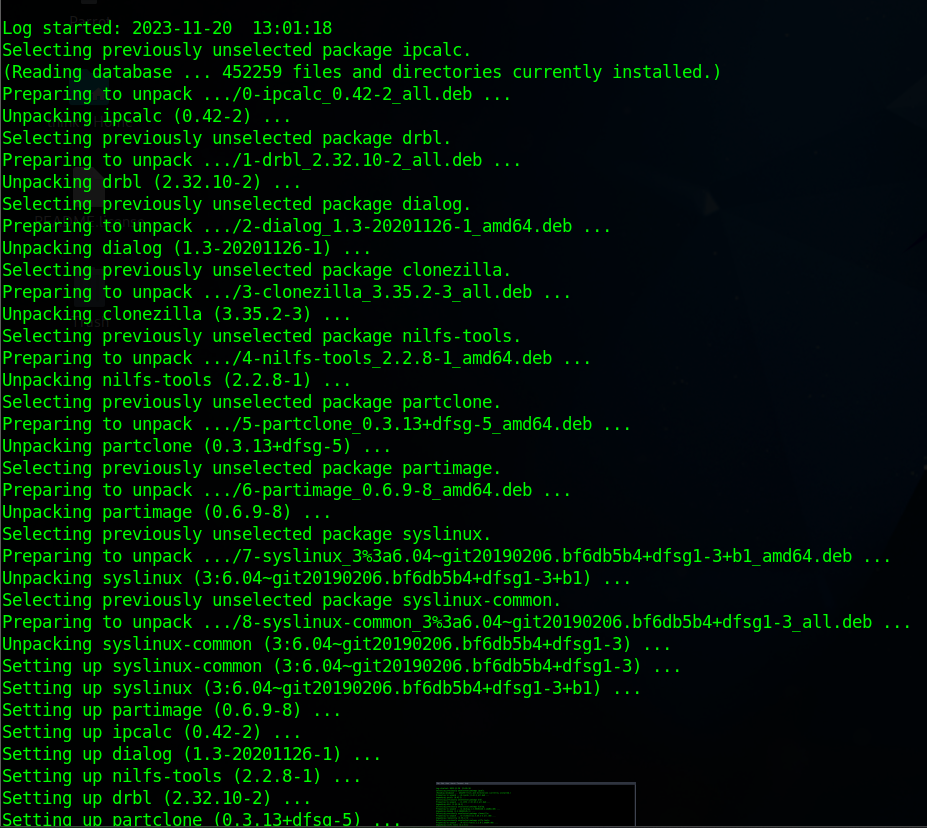
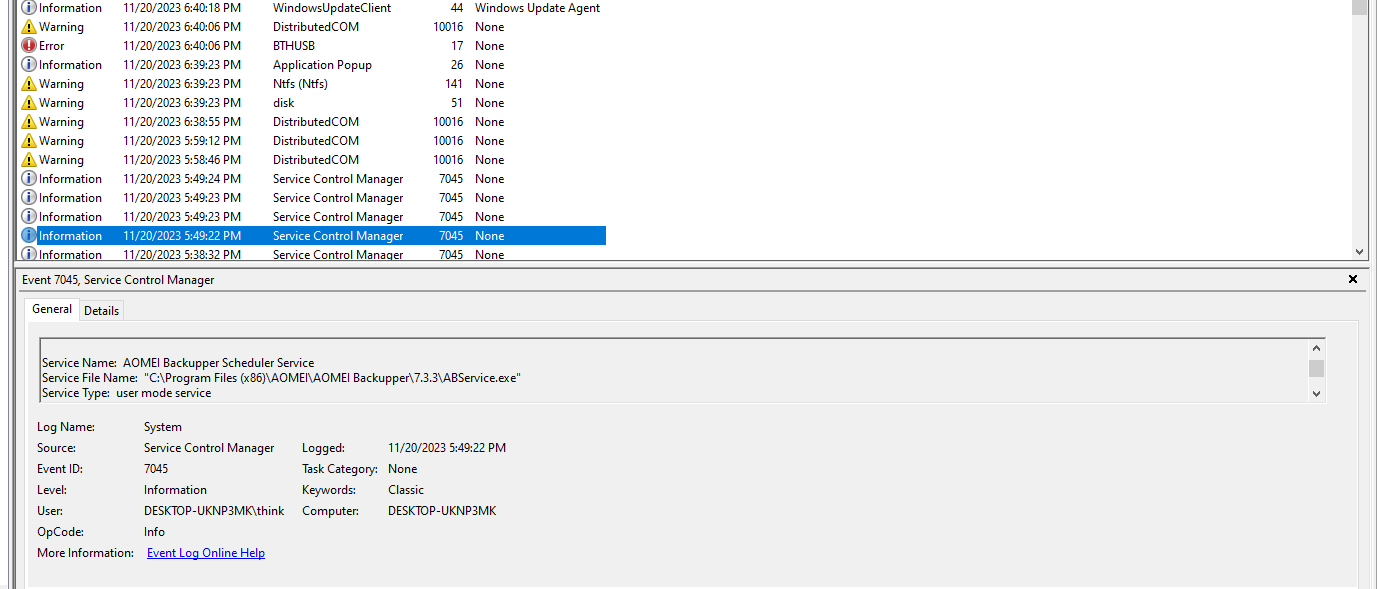
For VMware I just get popup like I mentioned earlier, no need to configure in beforehand for it.

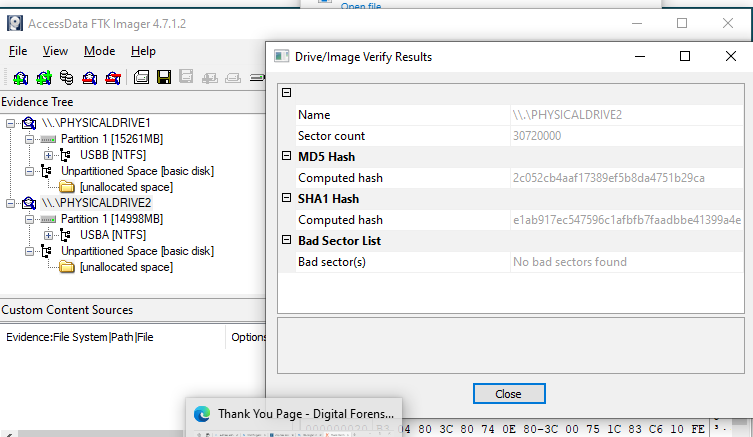
* Used Windows and Parrot OS for doing the labs.



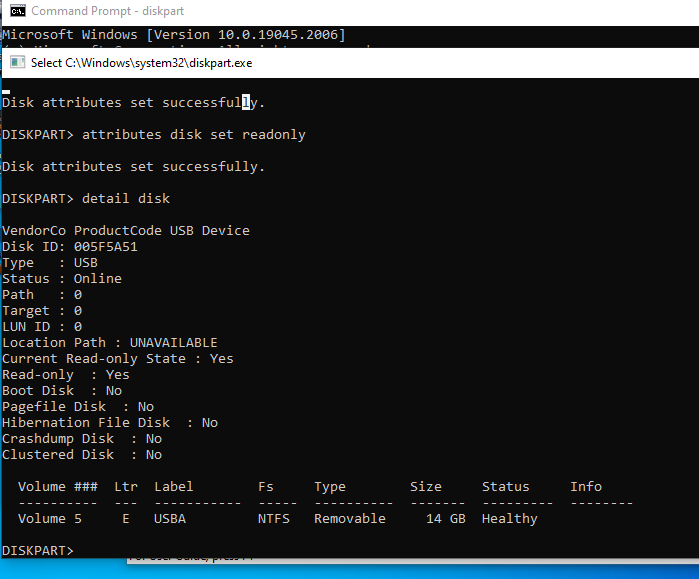
* I used Clonezilla and dd command in linux for doing the lab, below is the screenshot that I have used it.

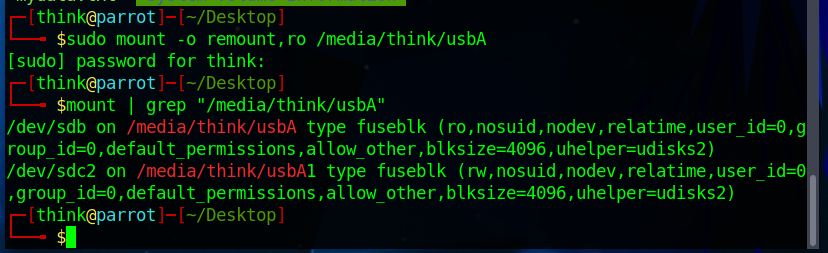


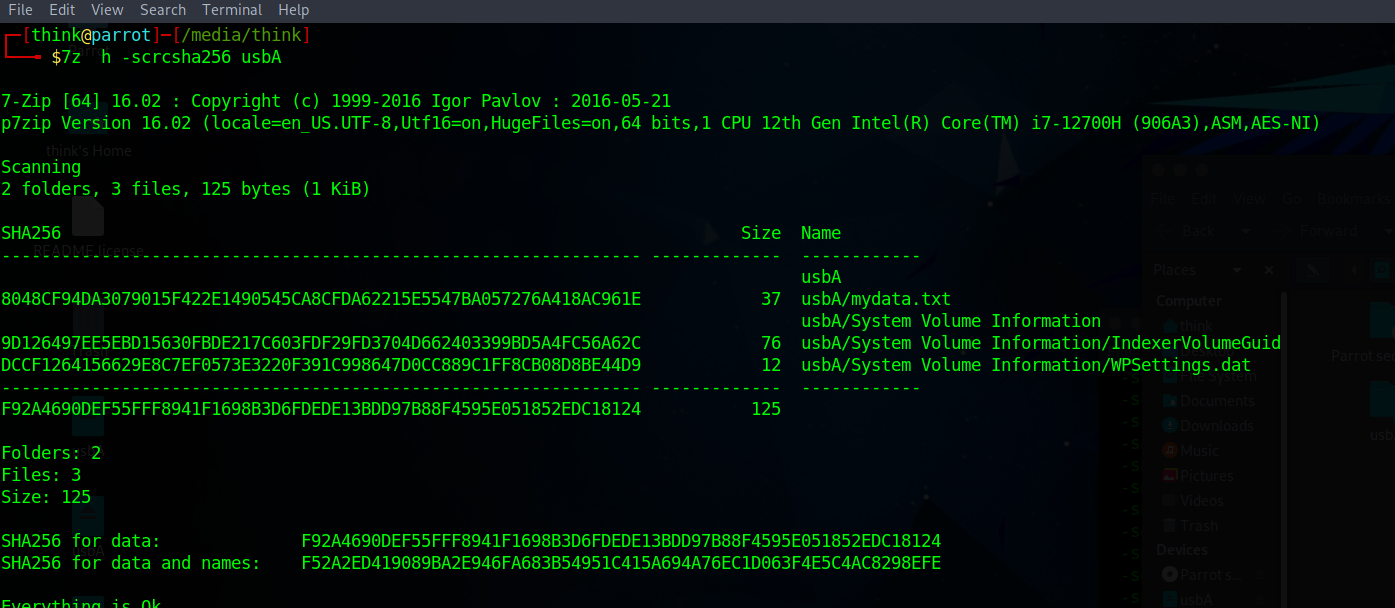
* I used 7zip for getting the hash value in both windows and linux.
* Event logs:  
  for linux:  
    
  for windows:  
  
* I used diskpart command in windows for write protecting it. So, It’s a software write blocker.



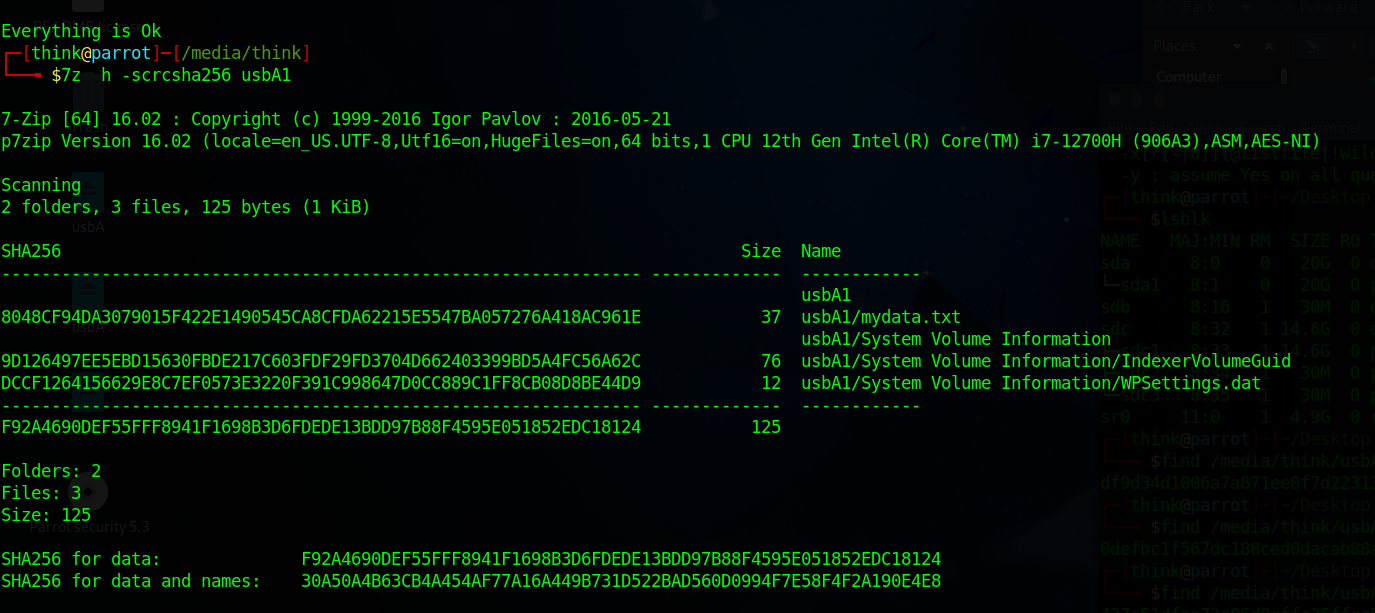
Diskpart :



In Linux:  


Sha screenshot before and after the task is done.   
Linux:  
h

Data cloned drive hash value:



We can see the hash value of two drives after it’s cloned. The sha value is same for the data, but the drives cannot have same name when both are connected, so the hash value is different for combination of data and name for the drives.