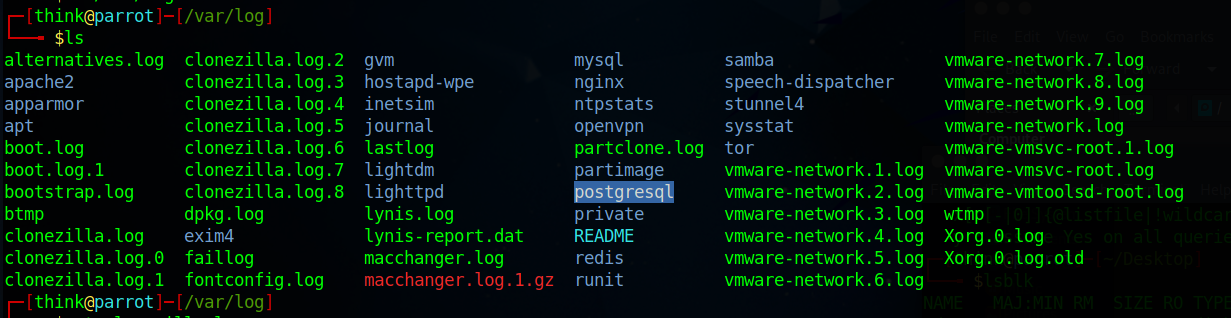
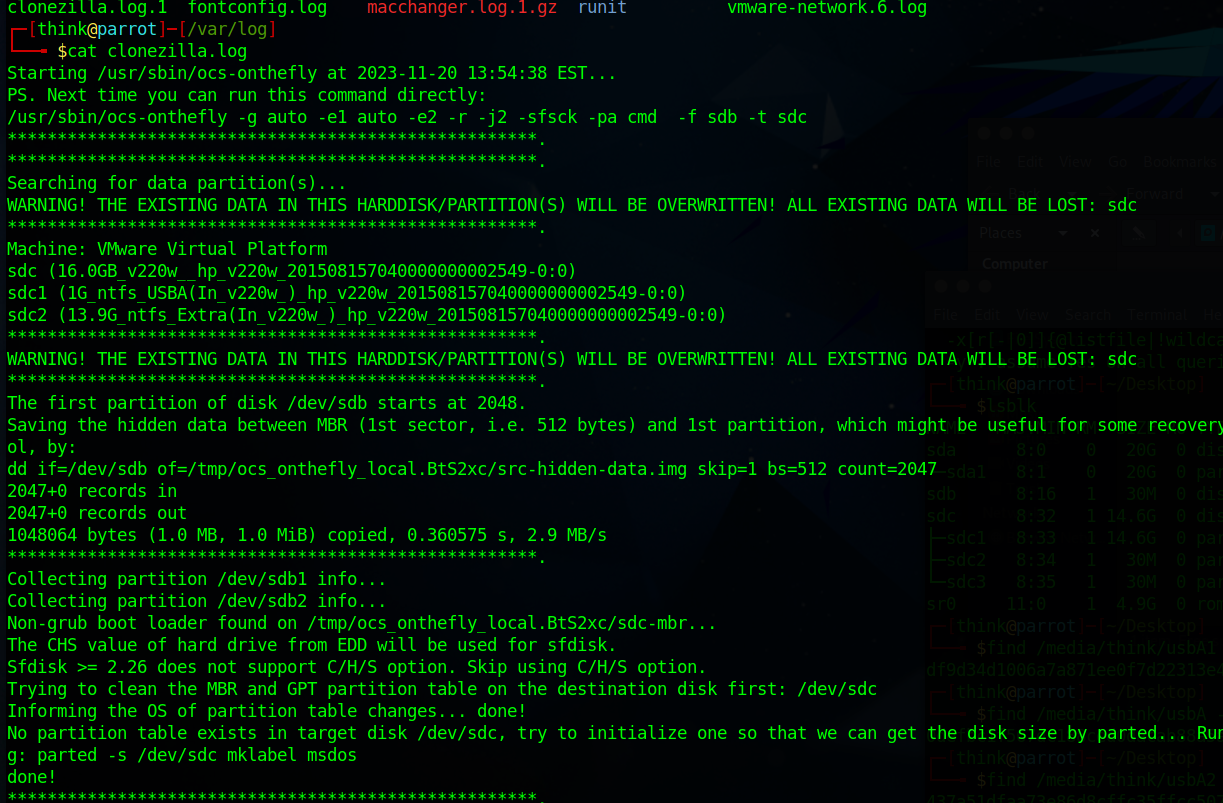
Lab-5 Events

Linux:

I’m using Parrot OS, below are the list of logs available to me



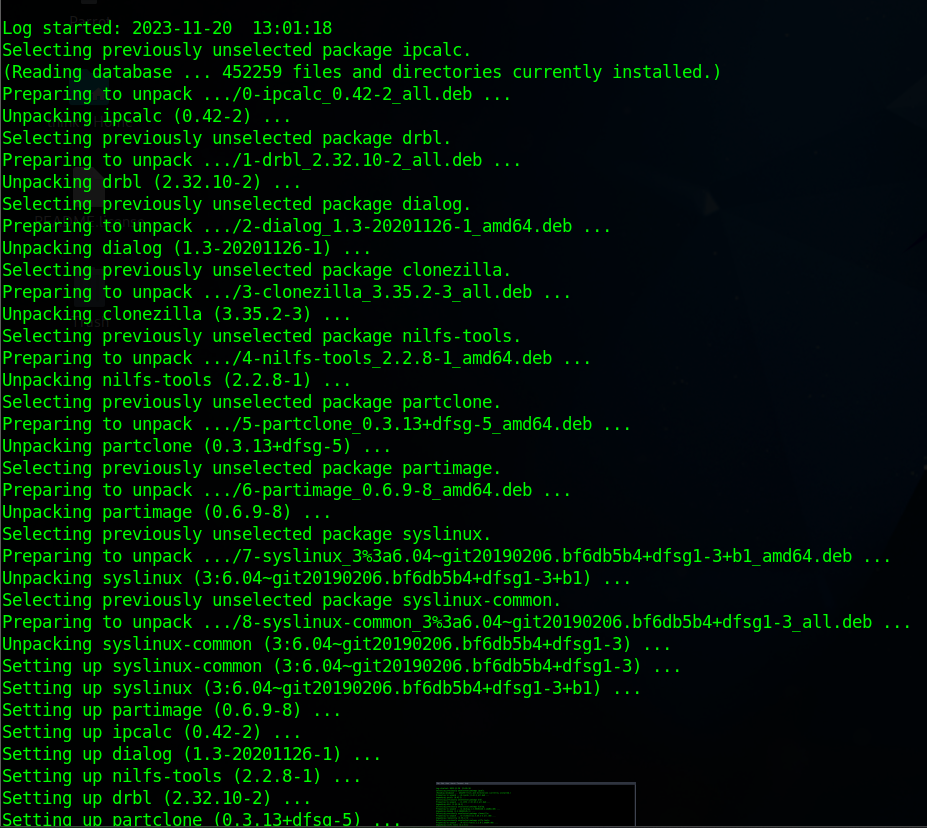
Clonezilla log:

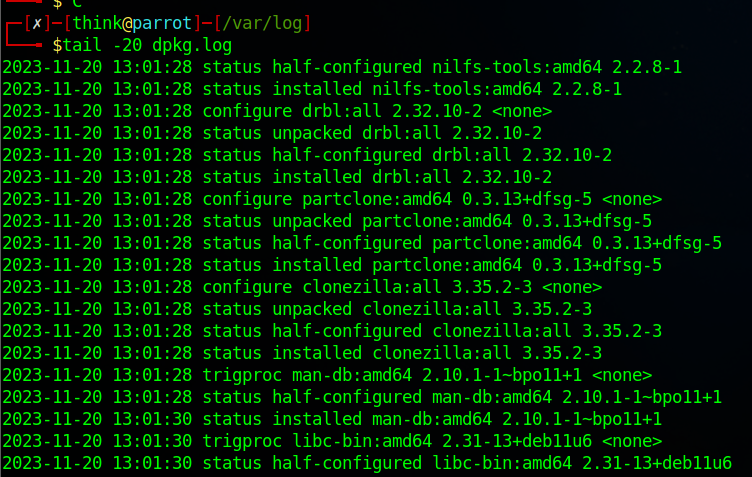


This one more log showing I did cloning not sure what I method is used.

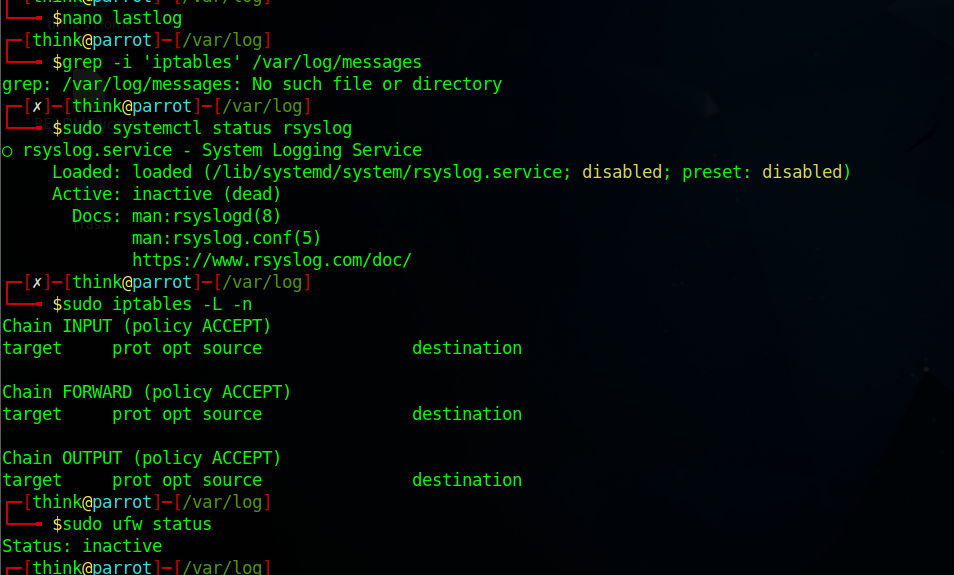


Below is the logs of apt/term.log  
we can see when I installed Clonezilla. Apparently I installed it around 13:00 and used it to clone the partition around 13.54 from the above screenshot.

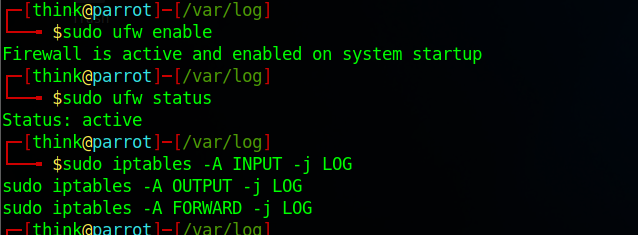


And From dpkg logs: we are able to find when our clonezilla is unpacked.  


We can see that I don’t syslog enabled by default. So, I’m providing the alternative logs pointing out that I have done the lab.

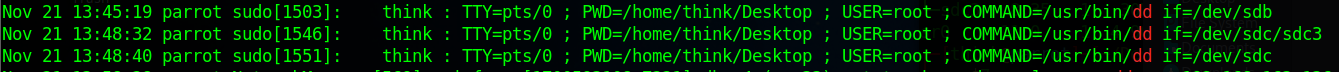


Now I have enable it now.



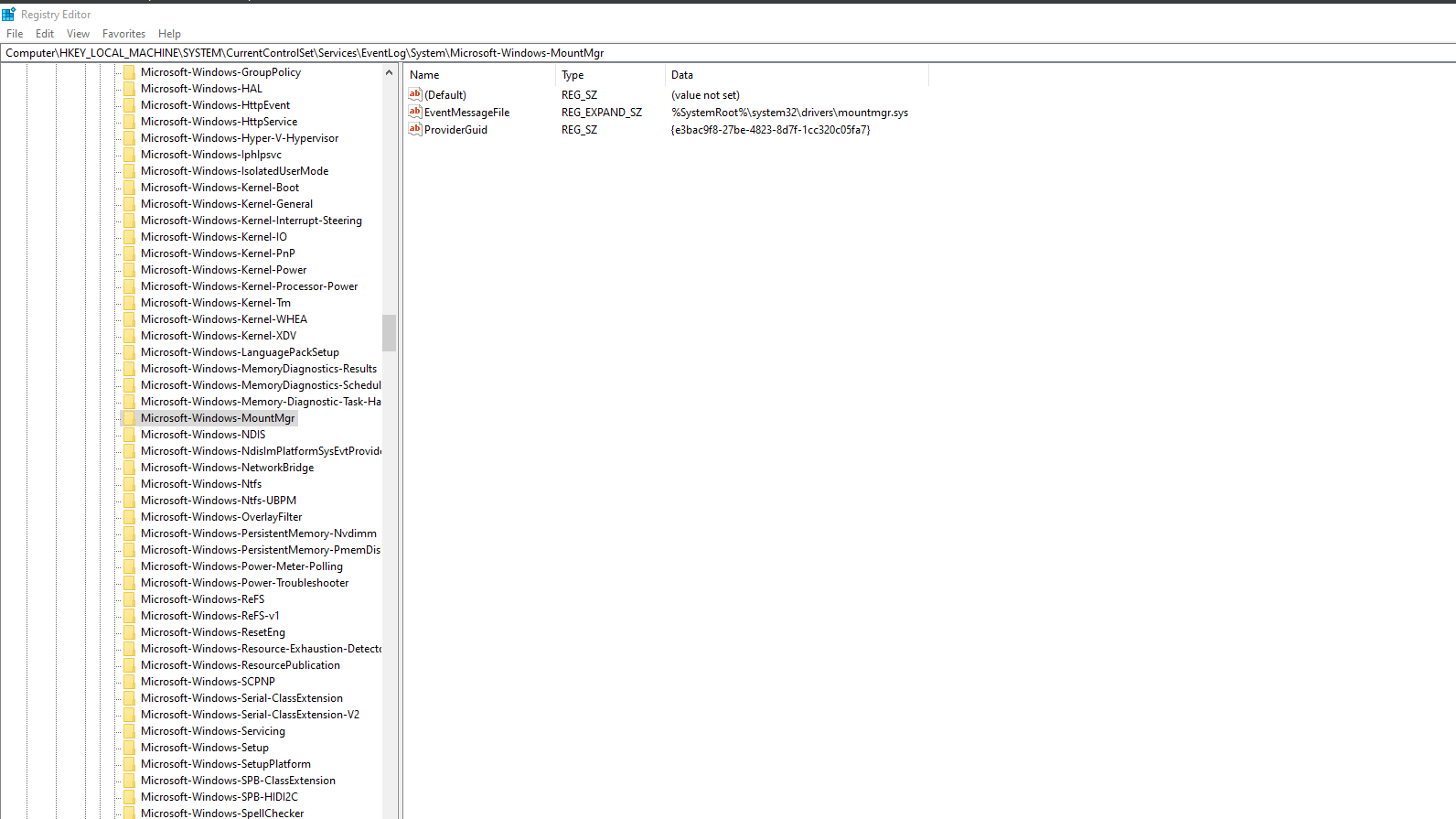
Now is used: sudo journalctl | grep dd

I found the following log pointing it out.

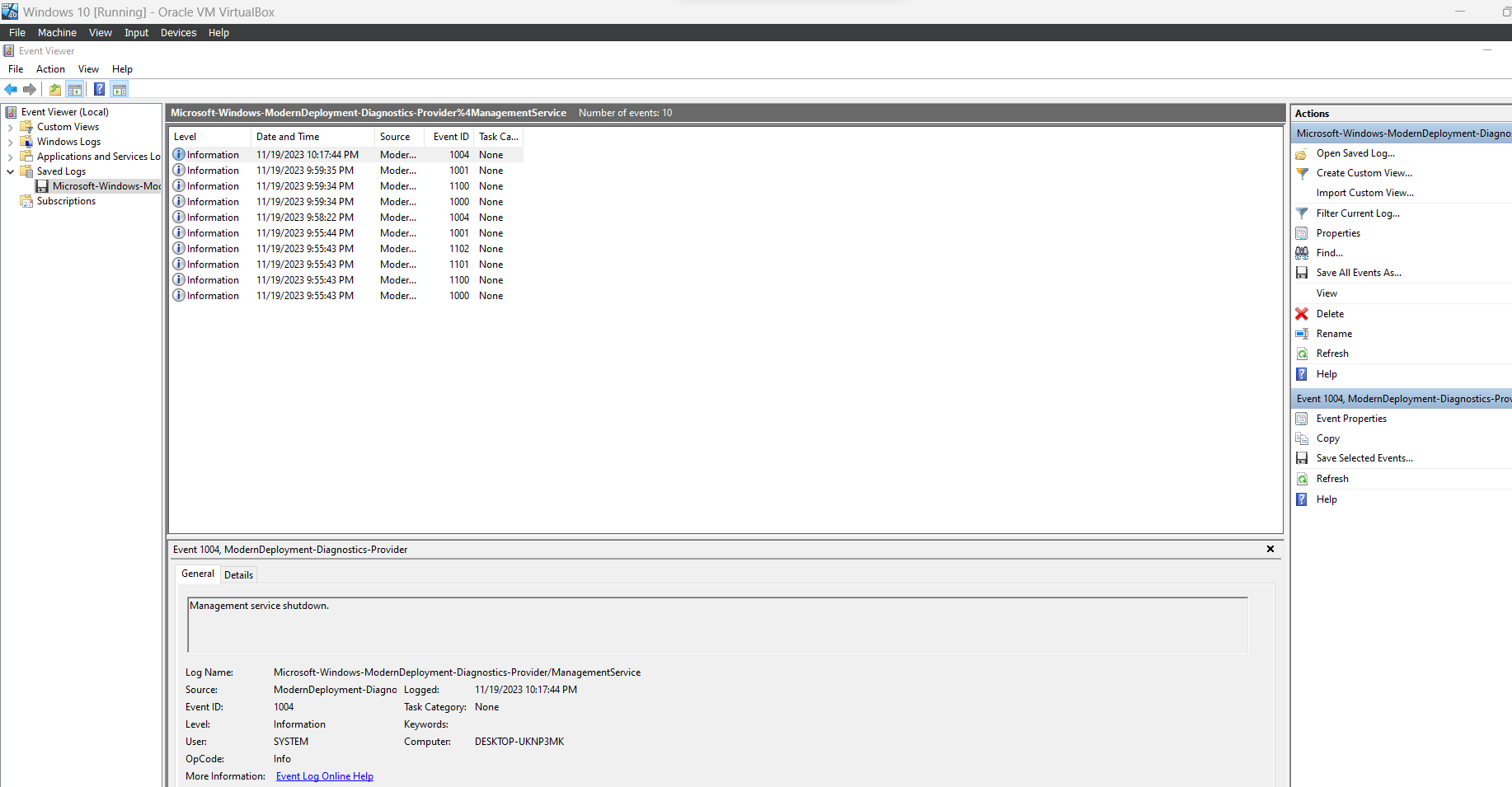


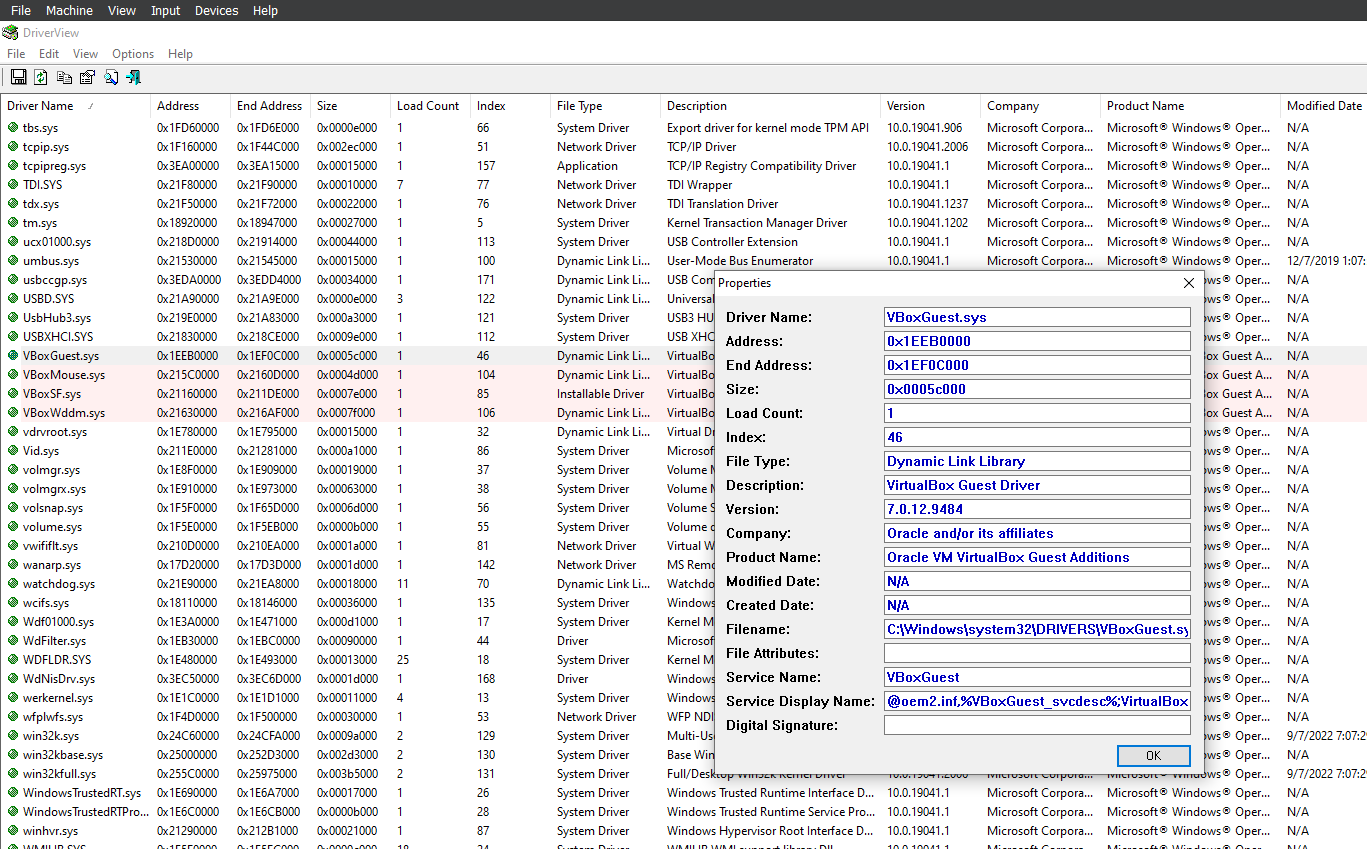
Windows:

1. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\<find your log>

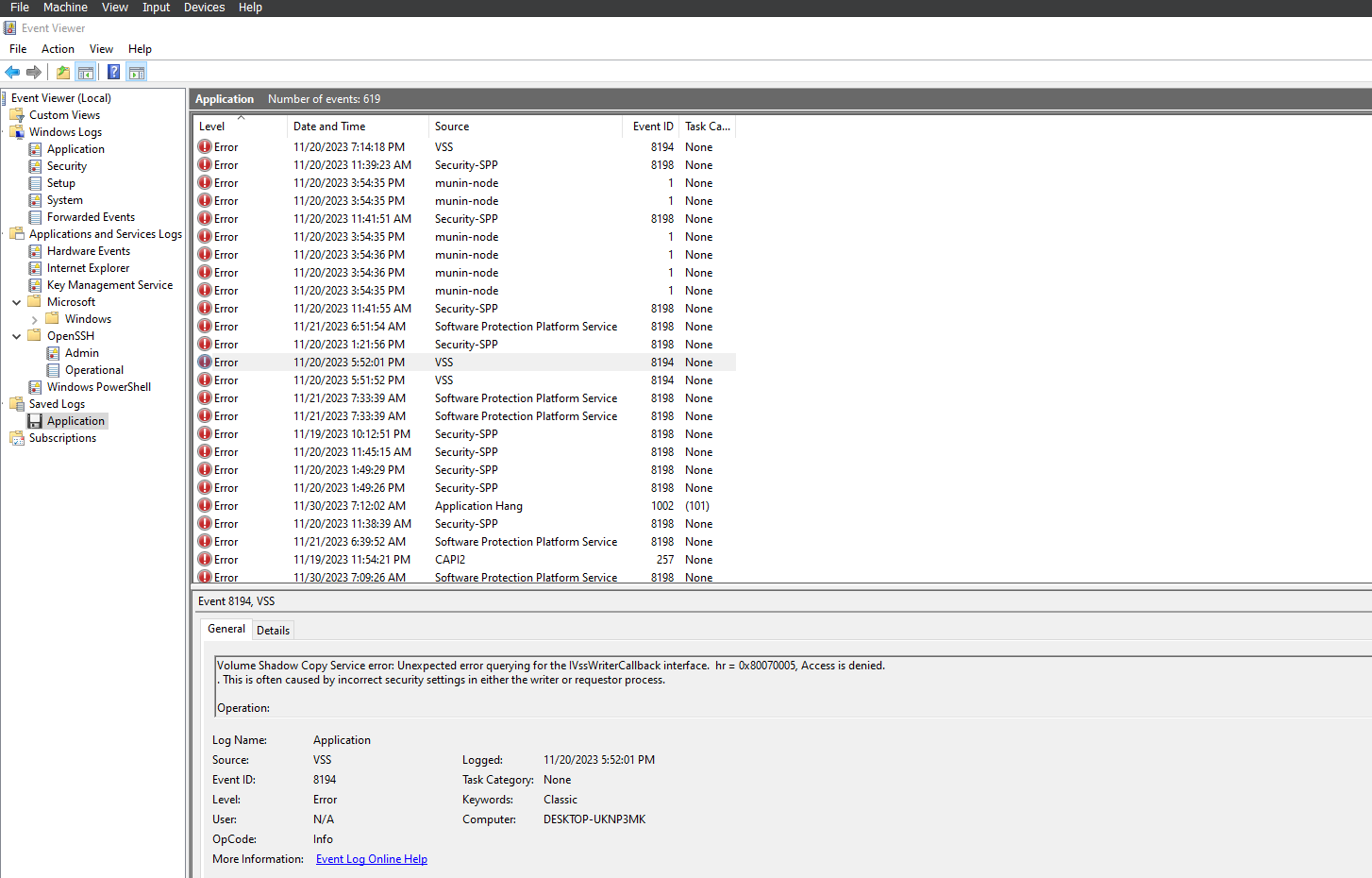


1. C:\Windows\System32\winevt\Logs <again find your logs>

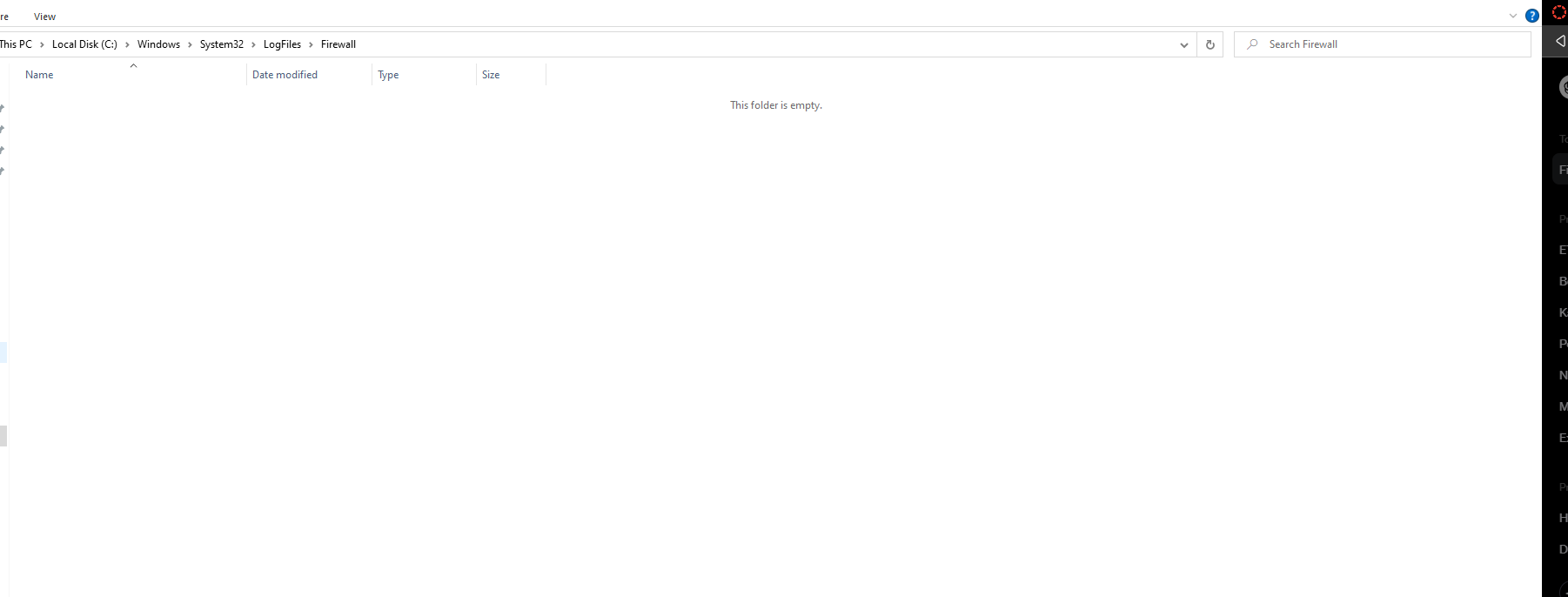


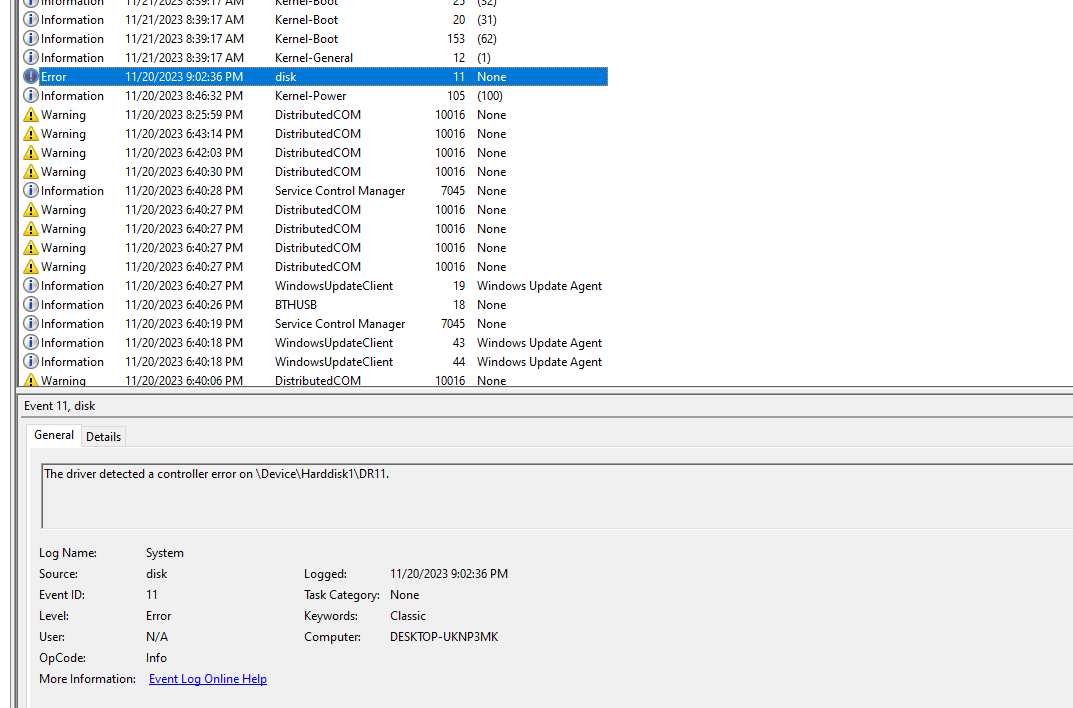


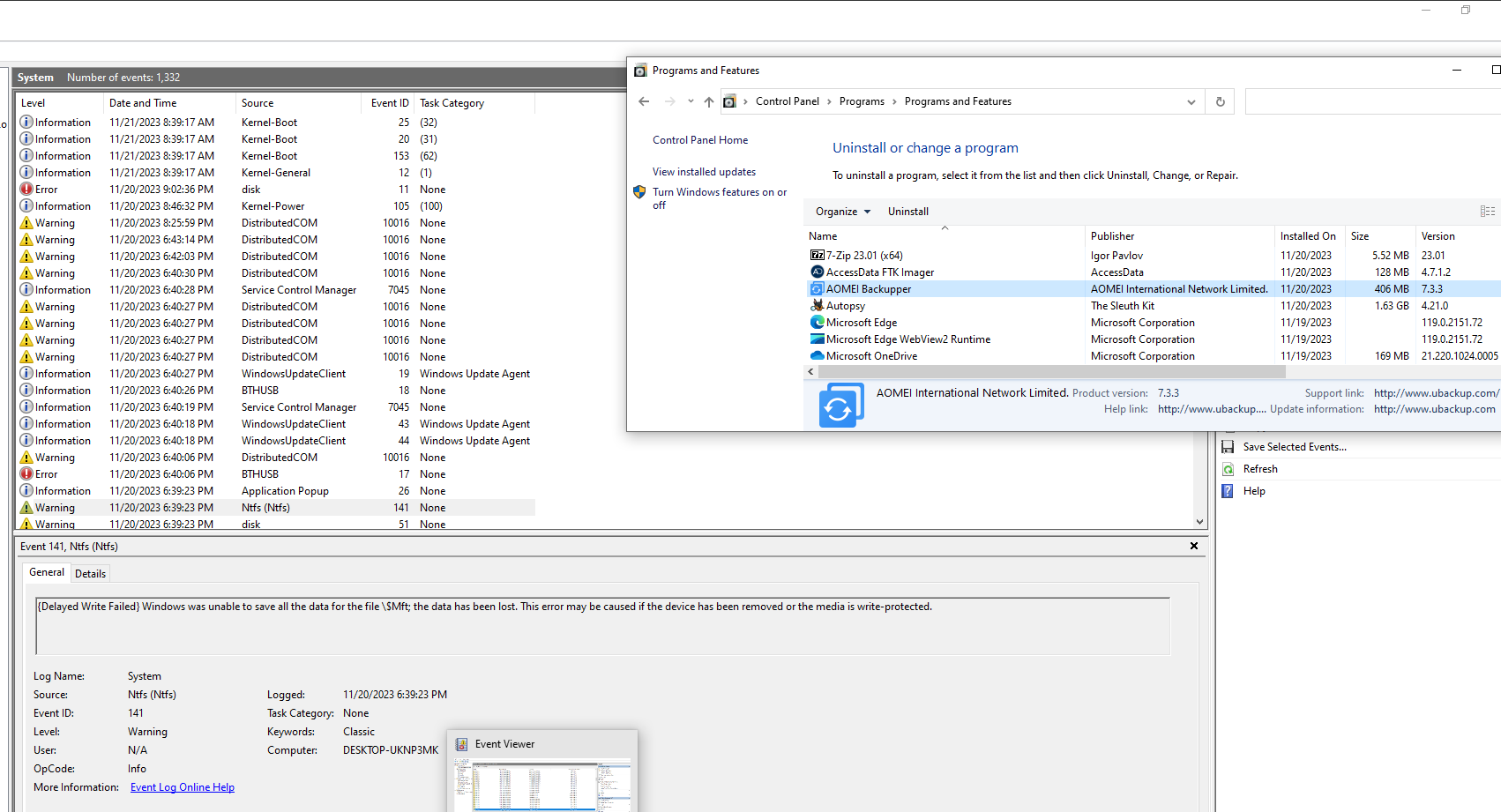
1. C:\Windows\System32\Logfiles\Firewall\pfirewall.log



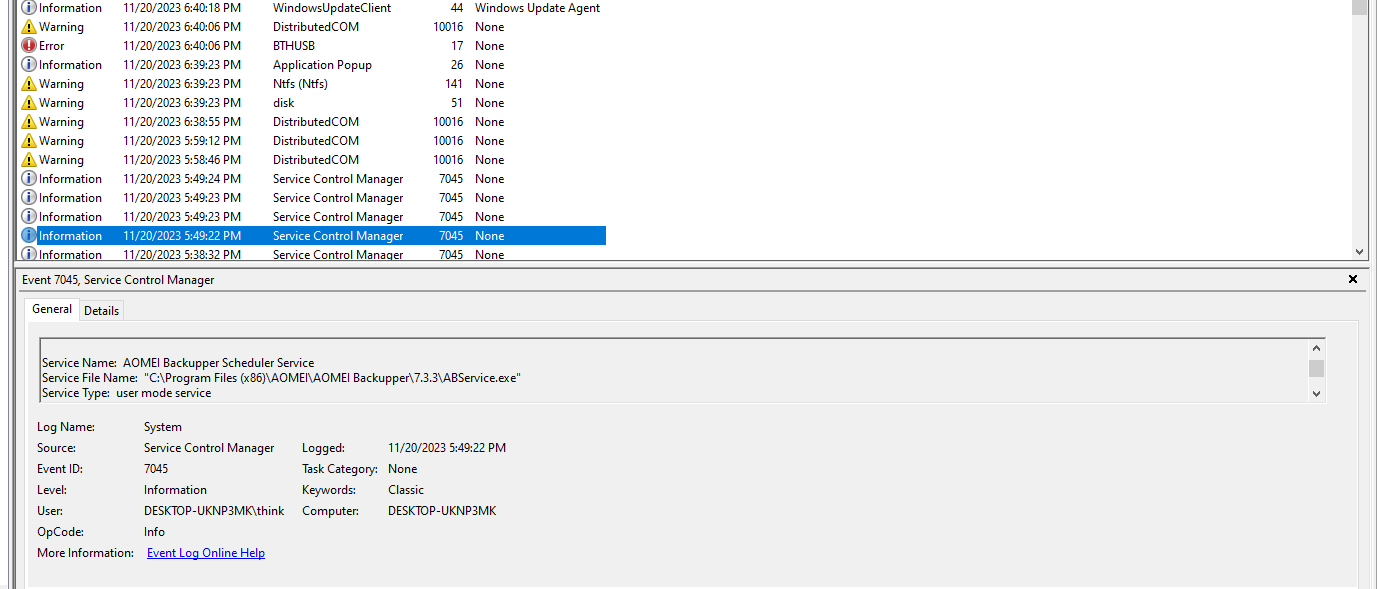
My firewall logs are empty:



Logs pointing to lab-4 in windows:  




The above screenshot show I have write protected the drive and control panel screenshot for backing up that I have done after I installed Aomei backupper.

  
Here is the log showing I installed Aomei backupper application.

Note: The firewall is disabled in my system. So, I don’t have any firewall logs. I have attached the screenshot of it.