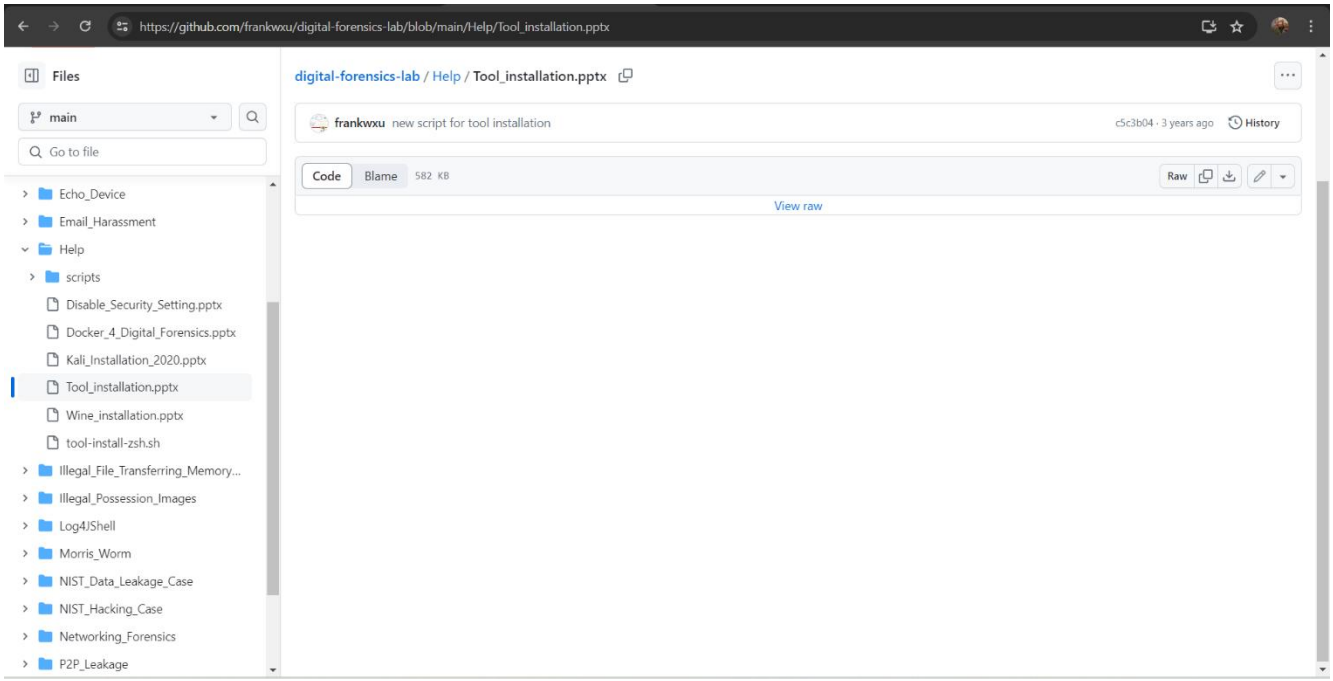
ITS60904

COMPUTER CRIME AND DIGITAL EVIDENCE

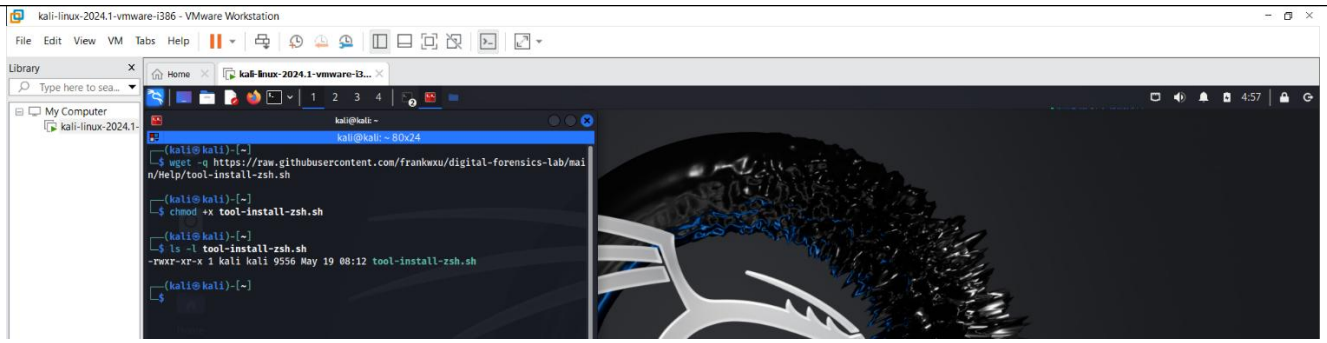
PRACTICAL 2 LAB REPORT

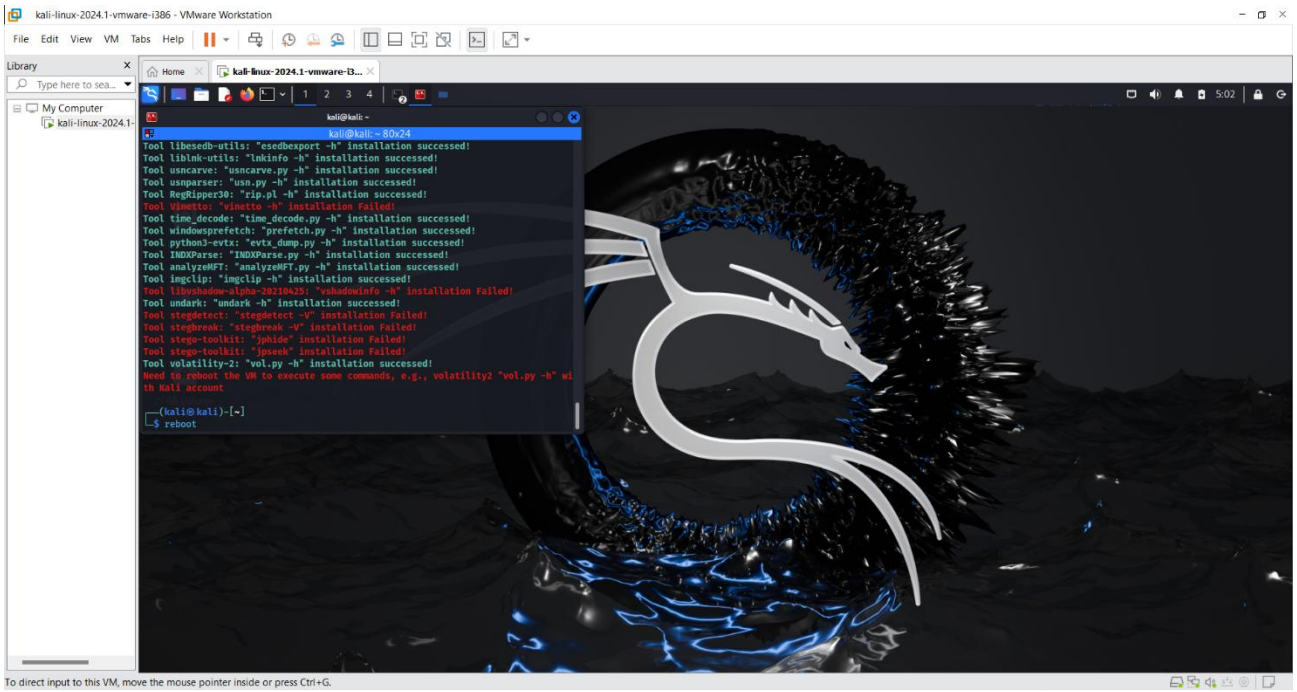
1. Install Kali (github).

- To be able to download the kali from the github under the username (frankxwu). User will need to search for 'Tool_installation.pptx' in this power point file there will be all the steps to download file from the kali-linux by using the terminal from terminator.



- The first step is to put the command 'wget -q' used to download files from the internet quietly, without showing any output in the terminal and insert with the link that you want to download the file from.
- The 'chmod +x' command is used to make a file executable after that the file will need to be list out with the command 'ls -l'. The download process will start.





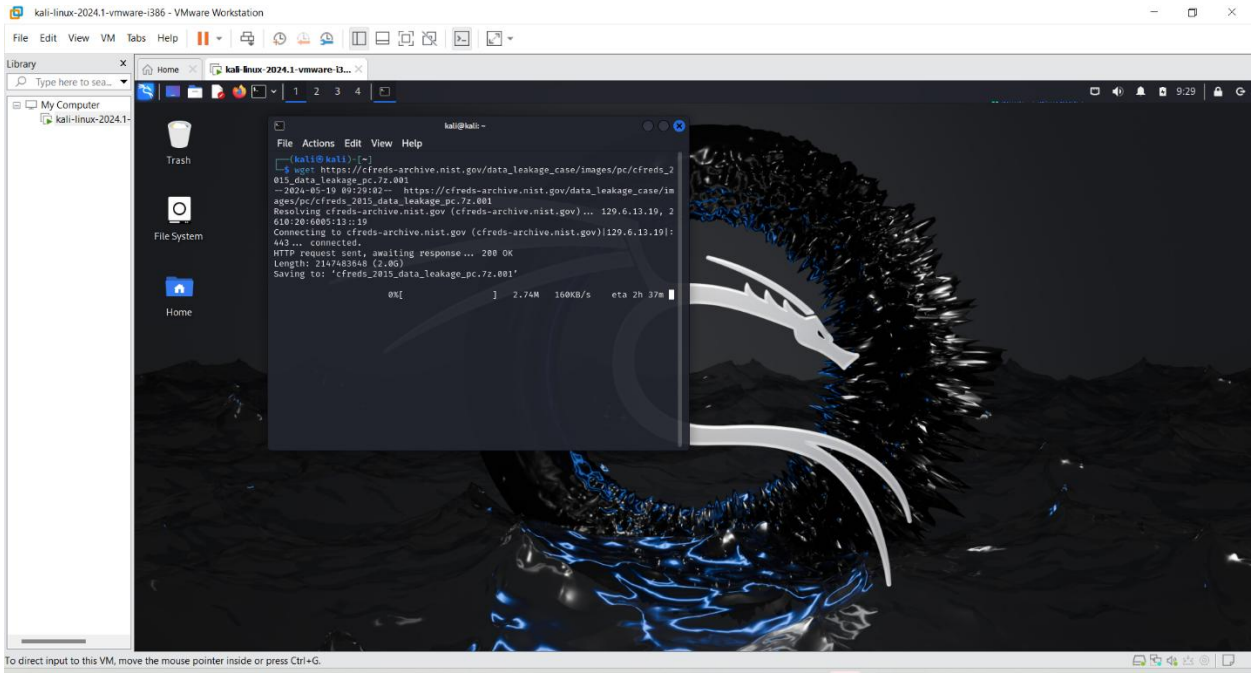
- After the download done the file will need to be reboot to able to use the command ‘vol.py -h’. All the necessary files like tree, RegRipper 3.0, Windows-Prefetch-Parser and Phyton-evtx successfully downloaded.

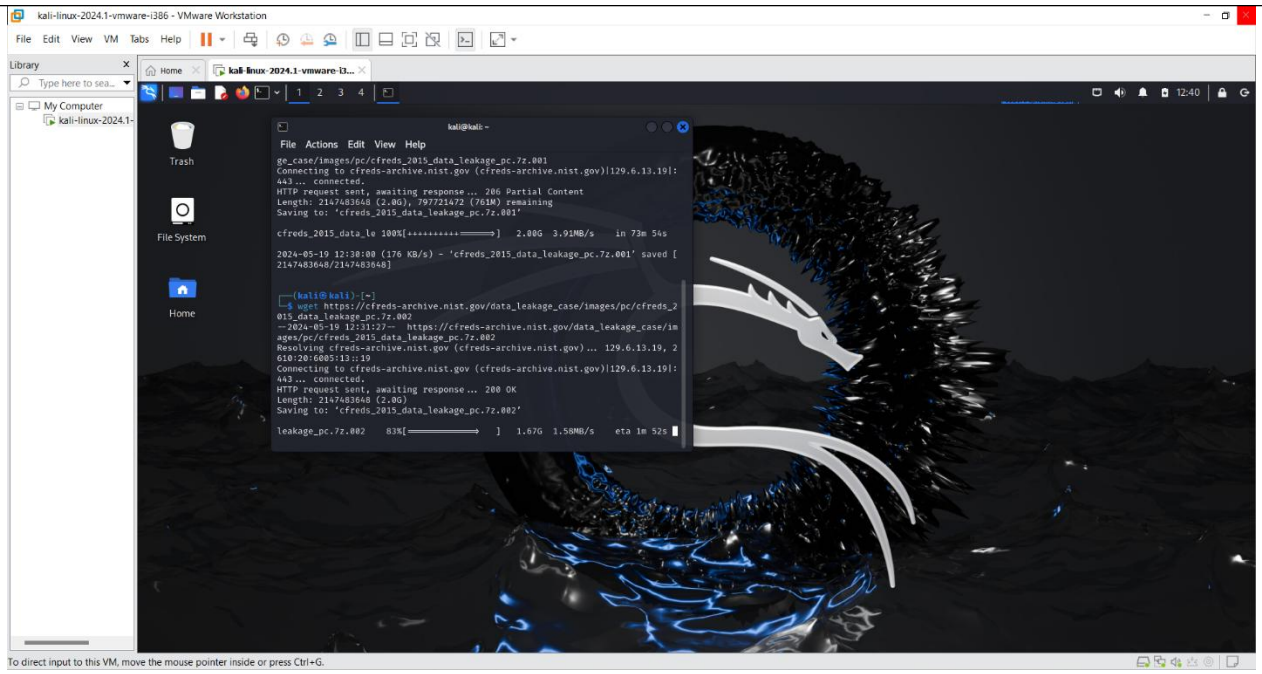
```
Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/home/kali/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/home/kali/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the (Olson) timezone for displaying timestamps
                        using pytz (if installed) or tzset
  -f FILENAME, --filename=FILENAME
```

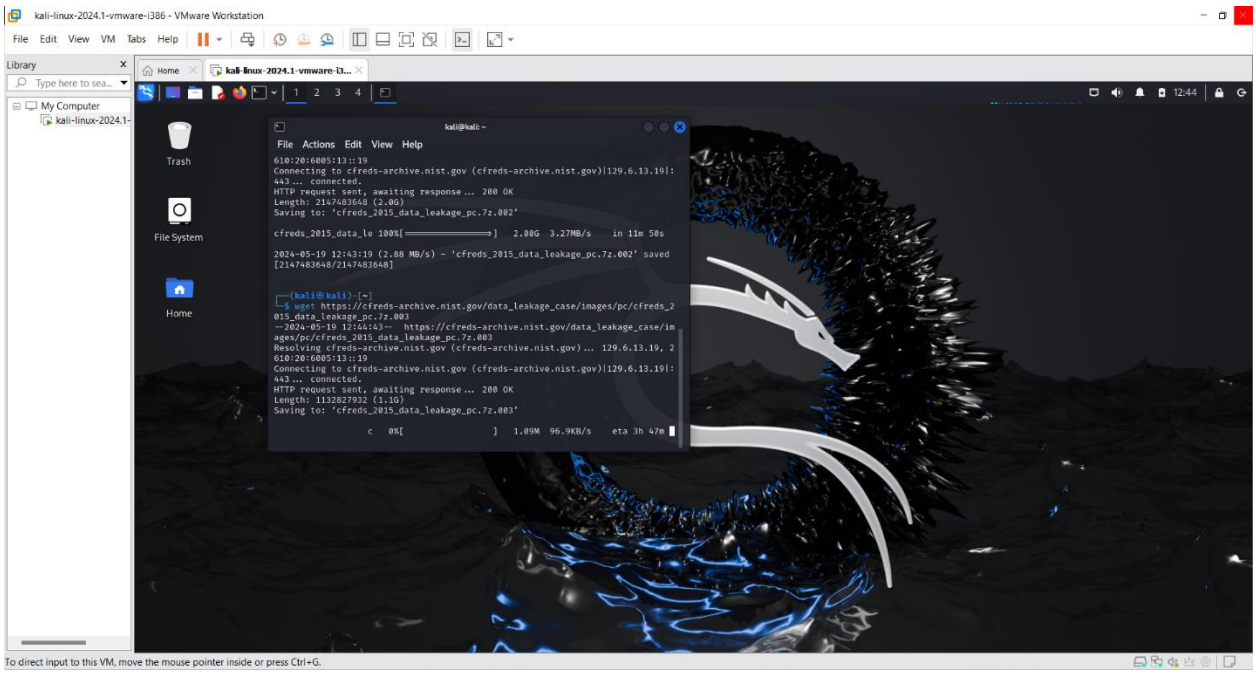
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Get the NIST data leakage DD image.

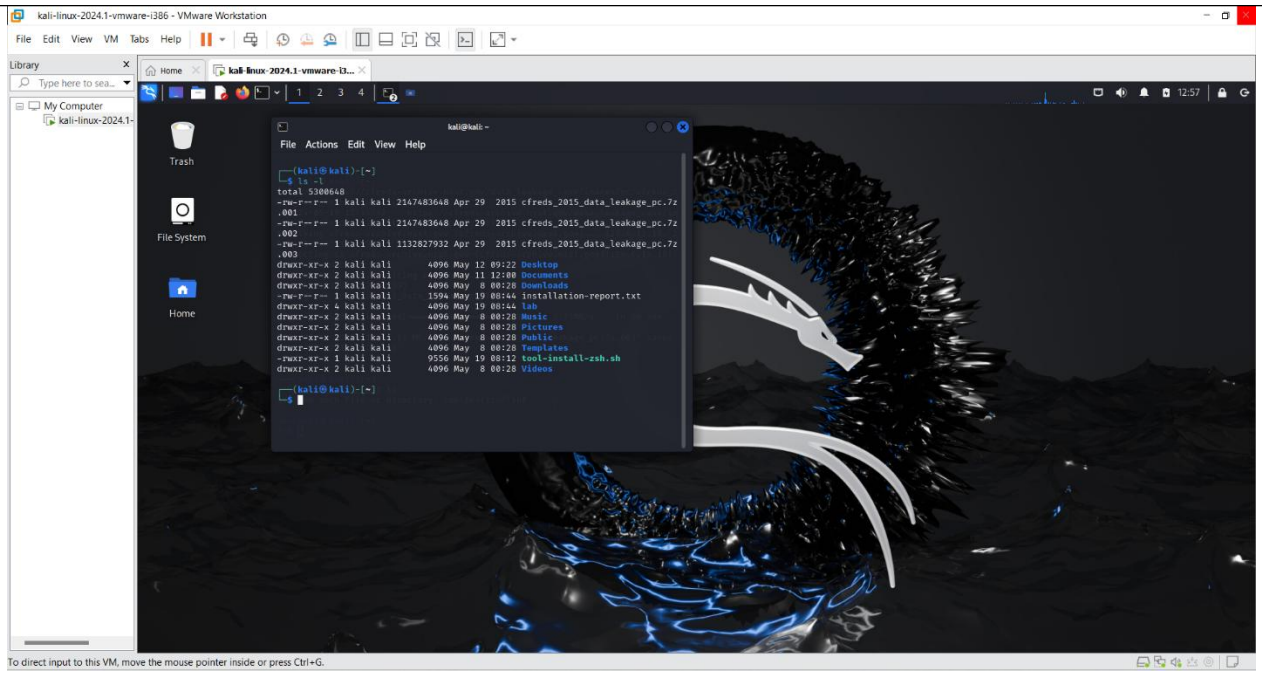
- There there link that must be downloaded first to be able to access the data leakage of the DD image. This particular file is part of a data leakage case scenario provided by NIST. The data leakage case involves simulated incidents where data might have been improperly accessed or exfiltrated from a computer system. The file has a .7z.001 extension, indicating it is part of a split archive compressed using the 7-Zip format. The three pictures below show the download process of the 3 files which are (001,002,003)



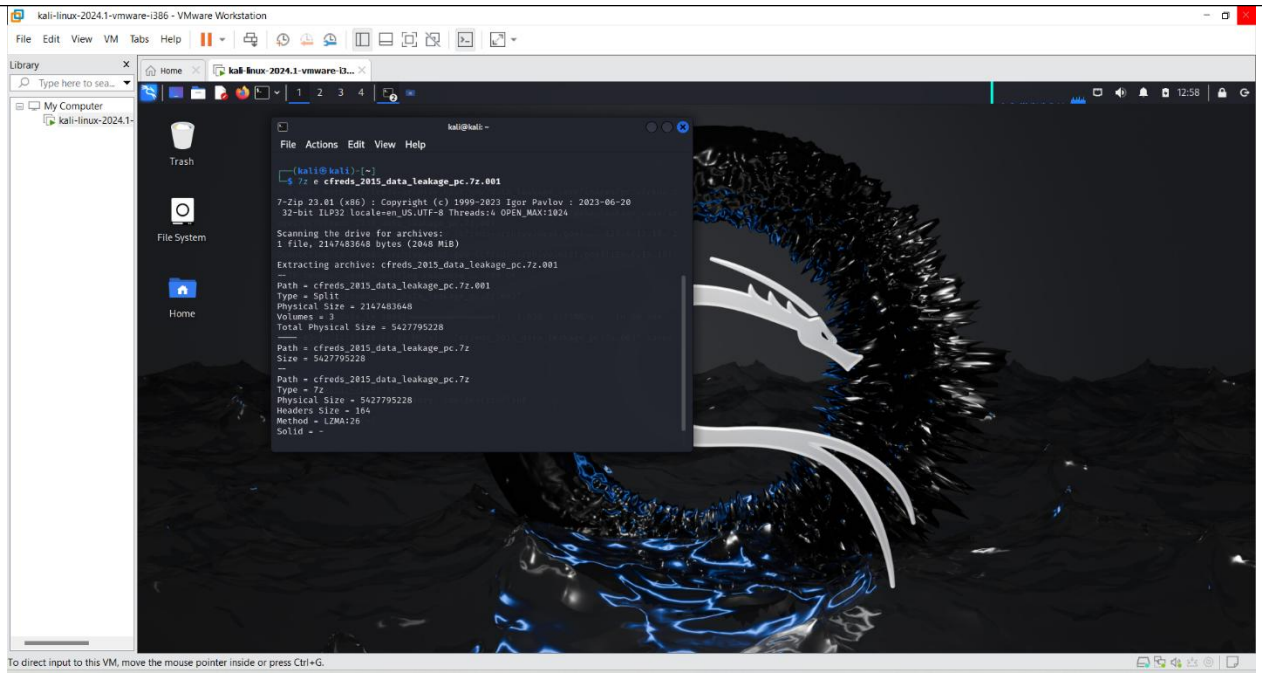




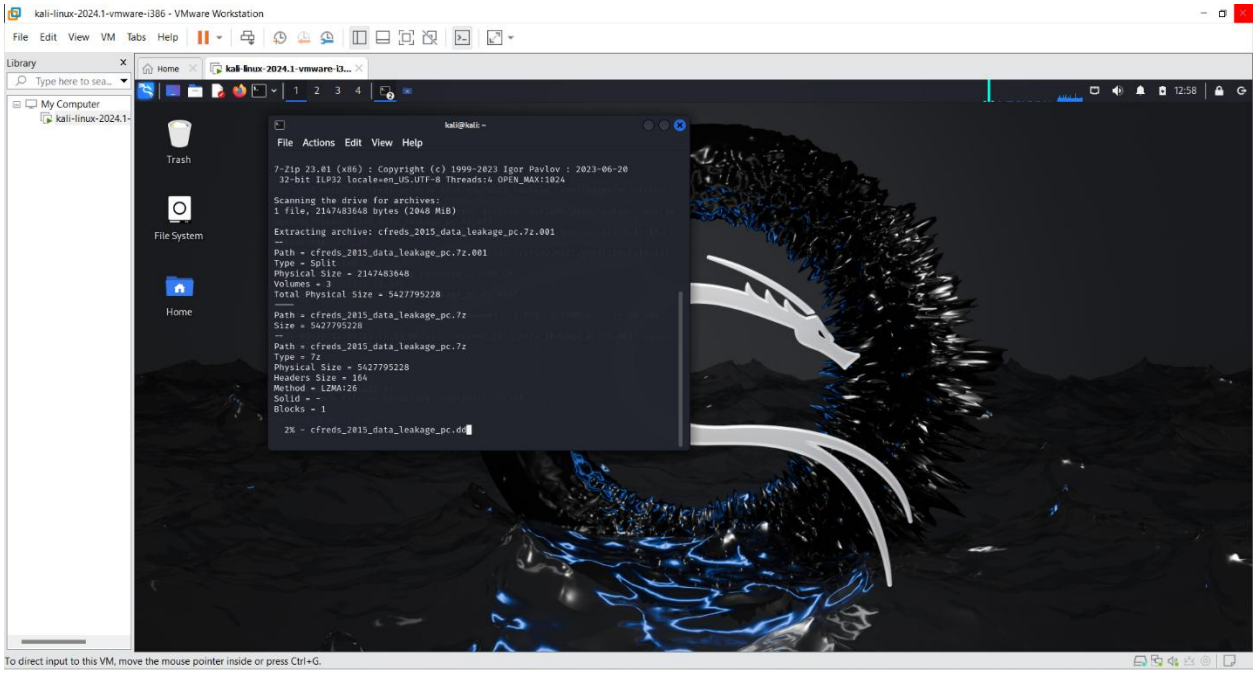
- To check if the zipped file is successfully downloaded, put in ‘ls -l’ which lists out the details of files and directories.



- After user done with the confirmation, now user need to unzip the file ‘001’. Before done it, it must be checked that all the three download files just now are in the same file. This will help to autamtically extract all three zip files together into the ‘.dd’ image file. This will need 20gb to proceed.

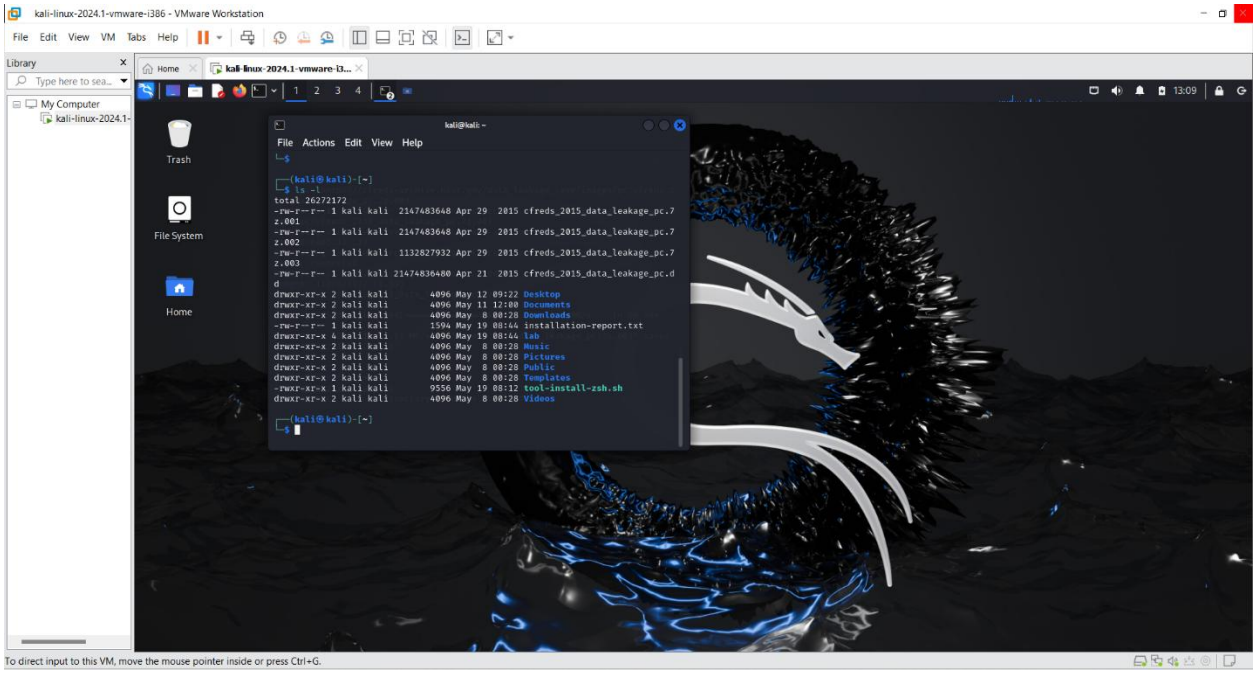

kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
1 2 3 4
12:58
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ 7z e cfreds_2015_data_leakage_pc.7z.001
7-Zip 23.01 (x86) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
32-bit ILP32 locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024
Scanning the drive for archives:
1 file, 2147483648 bytes (2048 MiB)
Extracting archive: cfreds_2015_data_leakage_pc.7z.001
--
Path = cfreds_2015_data_leakage_pc.7z.001
Type = Split
Physical Size = 2147483648
Volumes = 3
Total Physical Size = 5427795228

Path = cfreds_2015_data_leakage_pc.7z
Size = 5427795228
--
Path = cfreds_2015_data_leakage_pc.7z
Type = 7z
Physical Size = 5427795228
Headers Size = 164
Method = LZMA:26
Solid = -
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

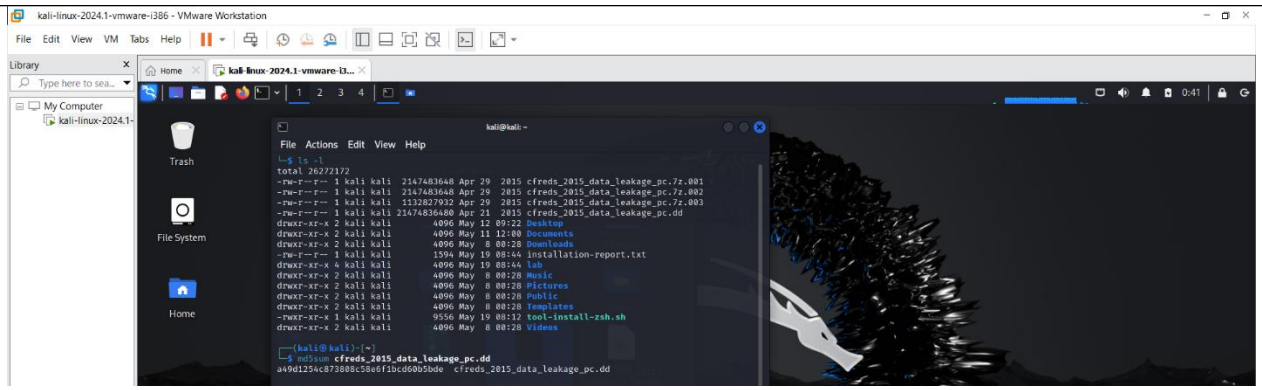

kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
1 2 3 4
12:58
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
7-Zip 23.01 (x86) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
32-bit ILP32 locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024
Scanning the drive for archives:
1 file, 2147483648 bytes (2048 MiB)
Extracting archive: cfreds_2015_data_leakage_pc.7z.001
--
Path = cfreds_2015_data_leakage_pc.7z.001
Type = Split
Physical Size = 2147483648
Volumes = 3
Total Physical Size = 5427795228

Path = cfreds_2015_data_leakage_pc.7z
Size = 5427795228
--
Path = cfreds_2015_data_leakage_pc.7z
Type = 7z
Physical Size = 5427795228
Headers Size = 164
Method = LZMA:26
Solid = -
Blocks = 1
2% - cfreds_2015_data_leakage_pc.de
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- To verify the unzipped DD image is successfully downloaded, put in ‘ls -l’ which lists out the details of files and directories. Here it shows that the steps had been succesfully.

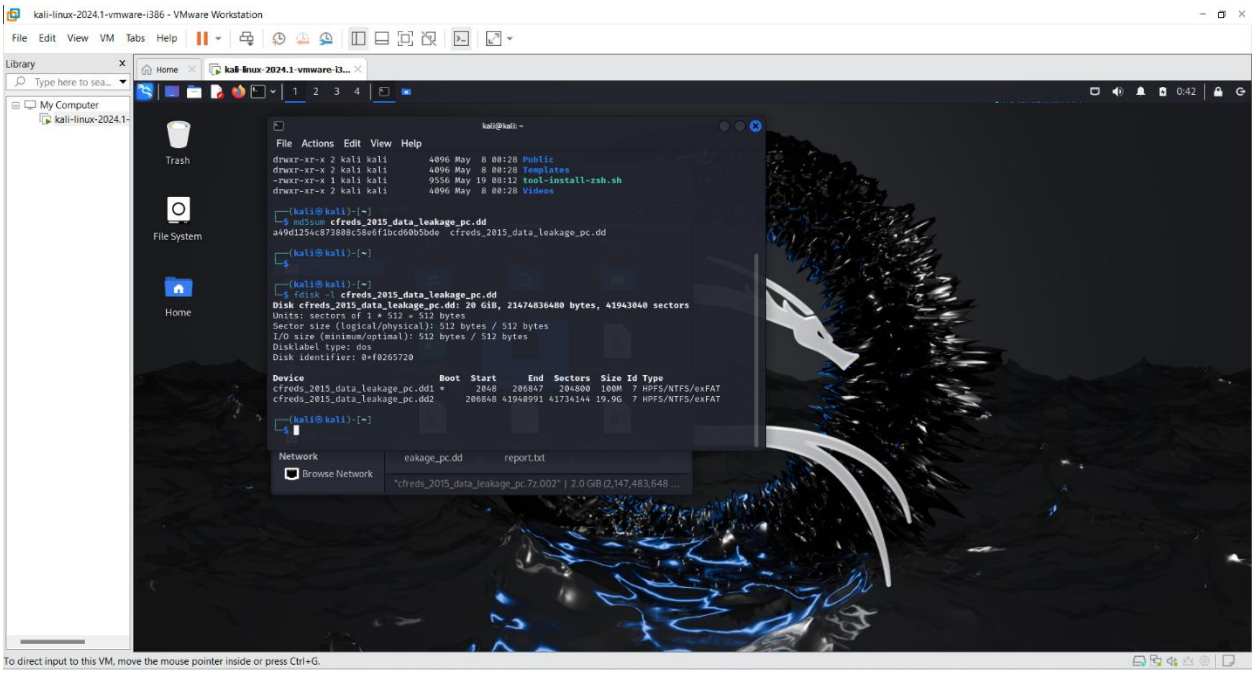


- To verify the unzipped DD image command ‘md5sum’ is used to generate and verify a unique fingerprint for a file. This fingerprint helps you check if the file has been altered or corrupted.

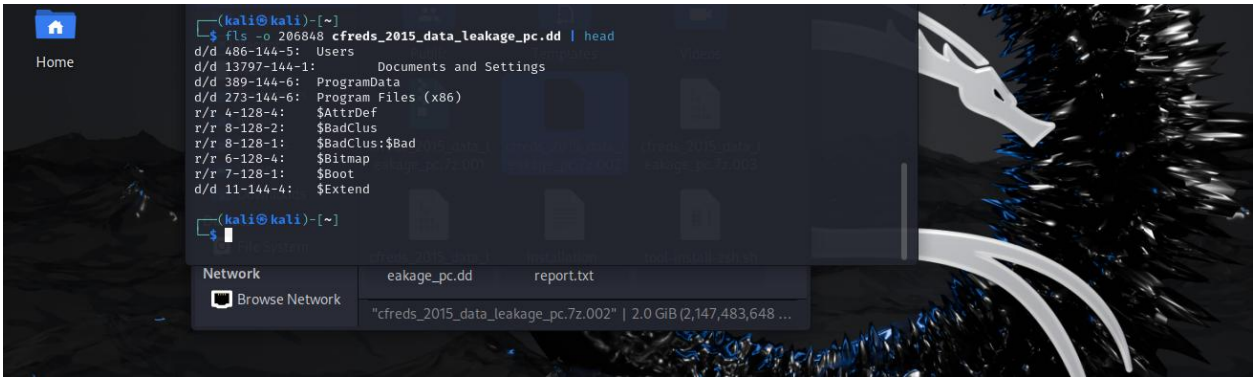


3. Exam files in DD image.

- In the next step user needs to examine the files in the DD image. The command used here is to examine the partitions of the DD image using fdisk (format disk). Below it can be seen that this device is bootable, not a boot partition. The ‘Value’ part is the “system” volume where configurations are required for the initial booting process and system startup. The ‘Device’ part is the “boot” volume where core operating system files are stored.

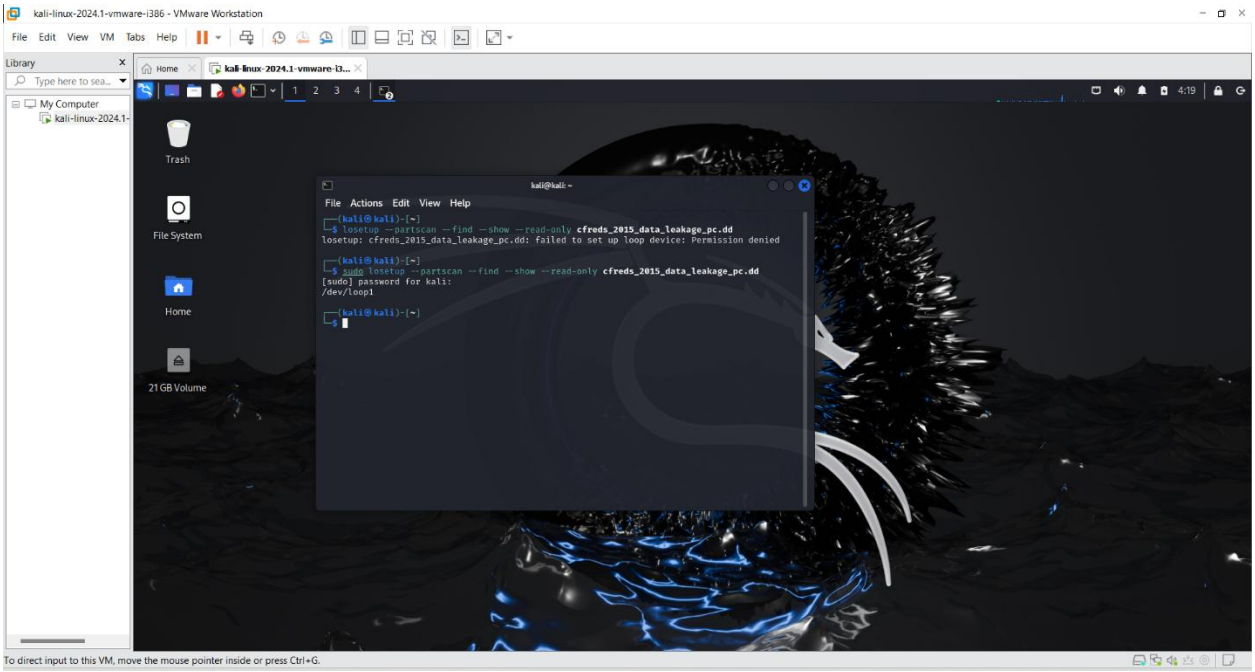


- The command ‘fls’ is to list out the file and directory names in a disk image.

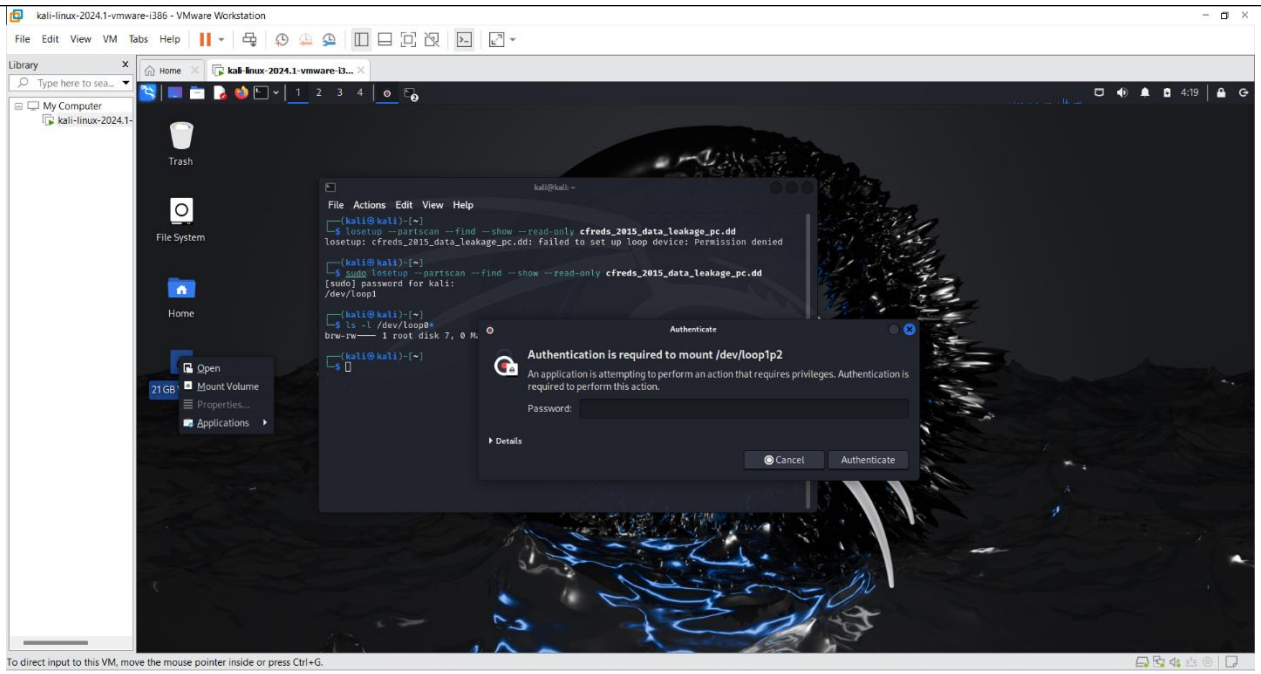


4. Extract key registry files from a DD image.

- The command use in here is to set up a loop device which is a pseudo-device that makes a file accessible as a block device. '—partscan' is use to scan the partition table on a newly created loop device. '—find' is to find the first unused loop device. '—show' print device name. '—read-only' is to setup read-only loop device. From the below image as I didn't have the admin privilege 'sudo' need to be added infront.

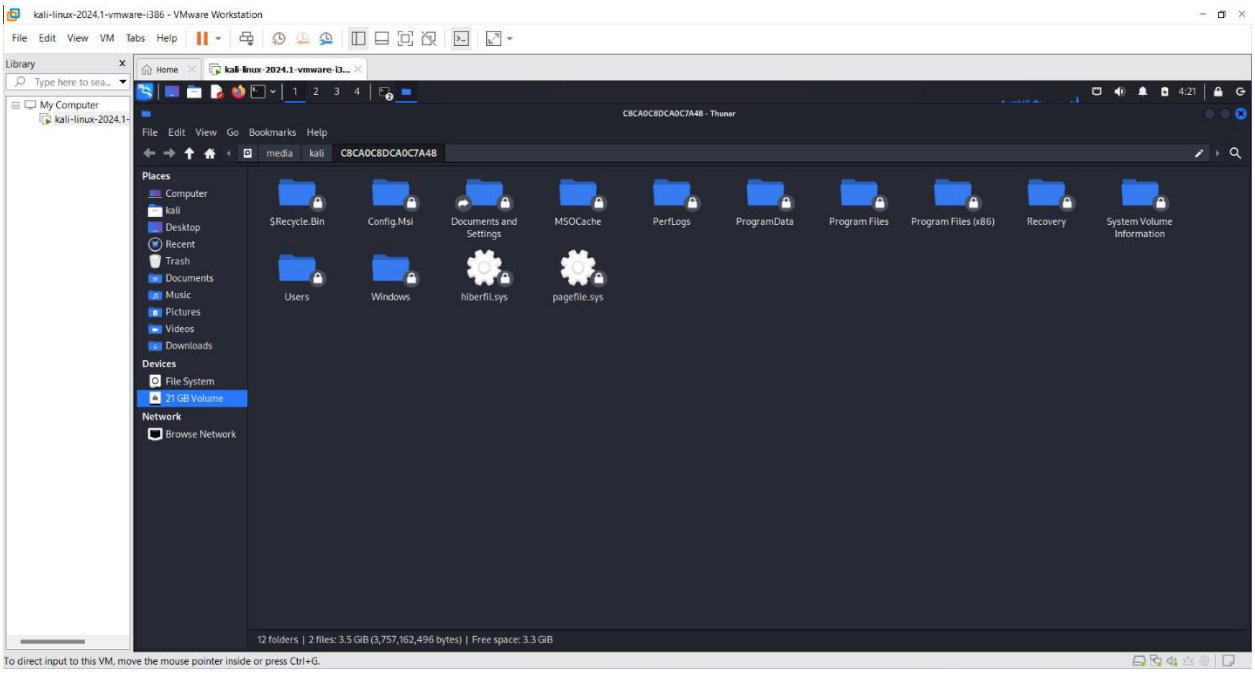


- This command is to show disk (loop0) (loop0p1 & p2) need a password user just need to key in kali.



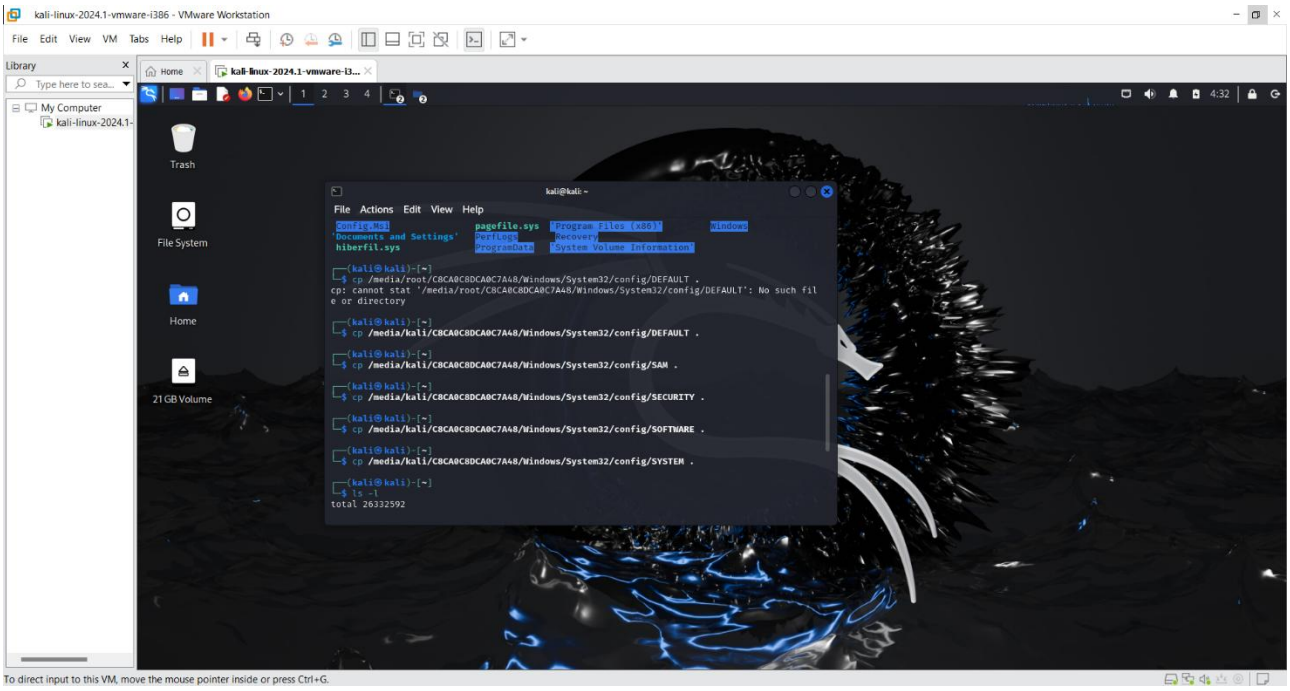
- The commnad ‘ls -l /dev/loop*’ is to show all disk files.

- Here is to show that file successfully available inside the kali-linux. The file will need to be mount volume first before able to open it.

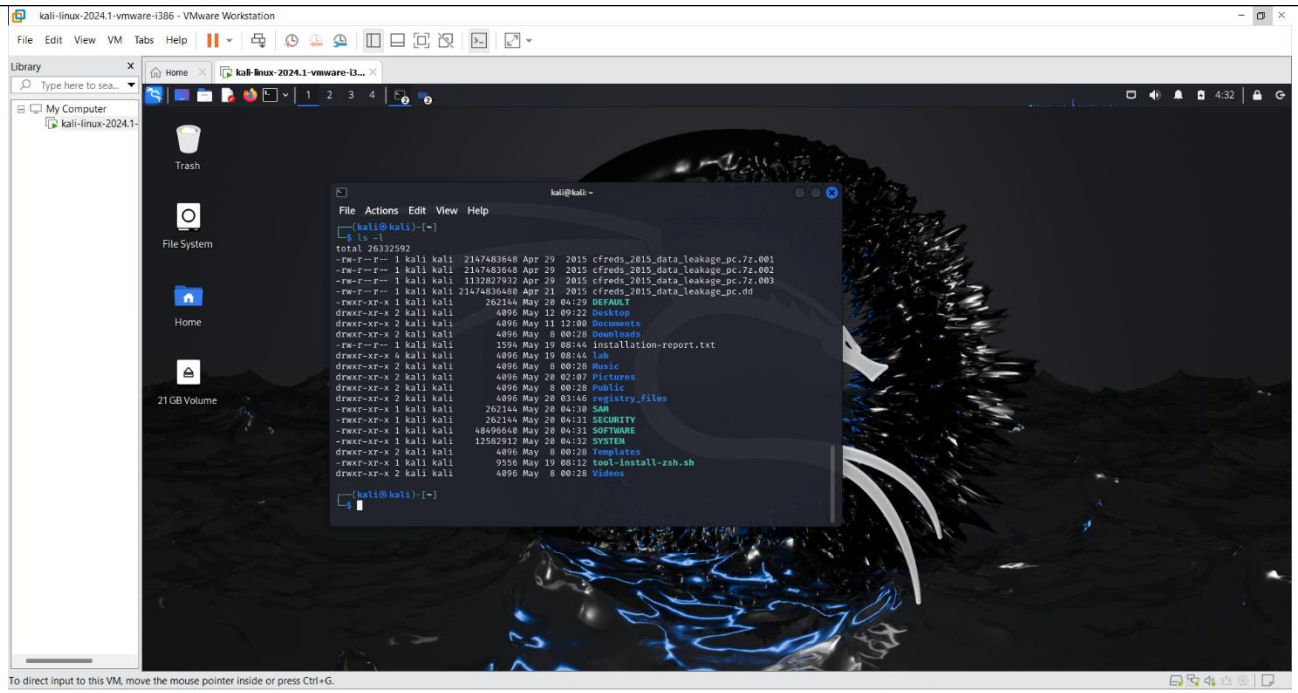


- The next step is to check the ounting point for my kali-linux I'm using kali to proceed with the step mine will be '/media/kali/C8CA0C8DCA0C7A48/'
- The next one is to list the command '/media/kali/C8CA0C8DCA0C7A48/' to checl the availability of file inside.

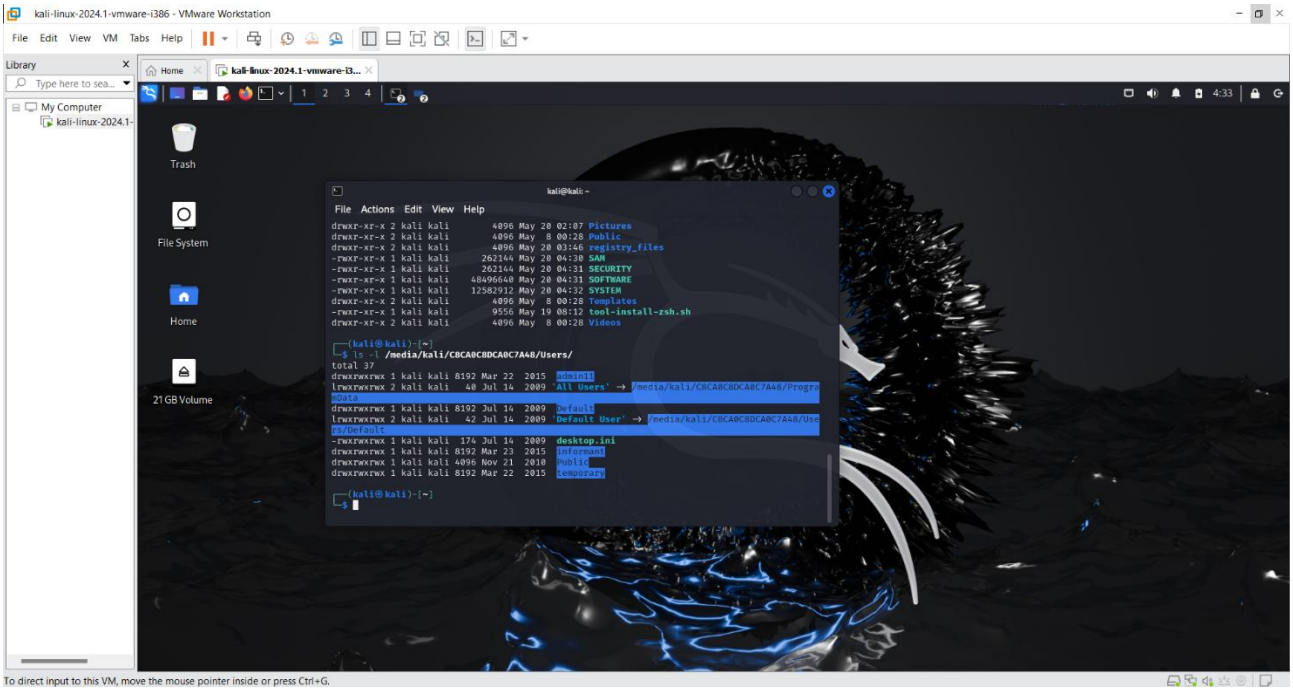
- In here user will need to cpy the file (Default,Sam,Security,Software,System) from the '21GB Volume' it will need to be put the command '/media/kali/C8CA0C8DCA0C7A48/' as the files are inside there. This will access the file config under system32 which is also under Windows that available inside the '21 GB Volume'



- The command ‘ls -l’ is to list out the file's name and directory. Here we can see that the files copied in previous step successfully done.



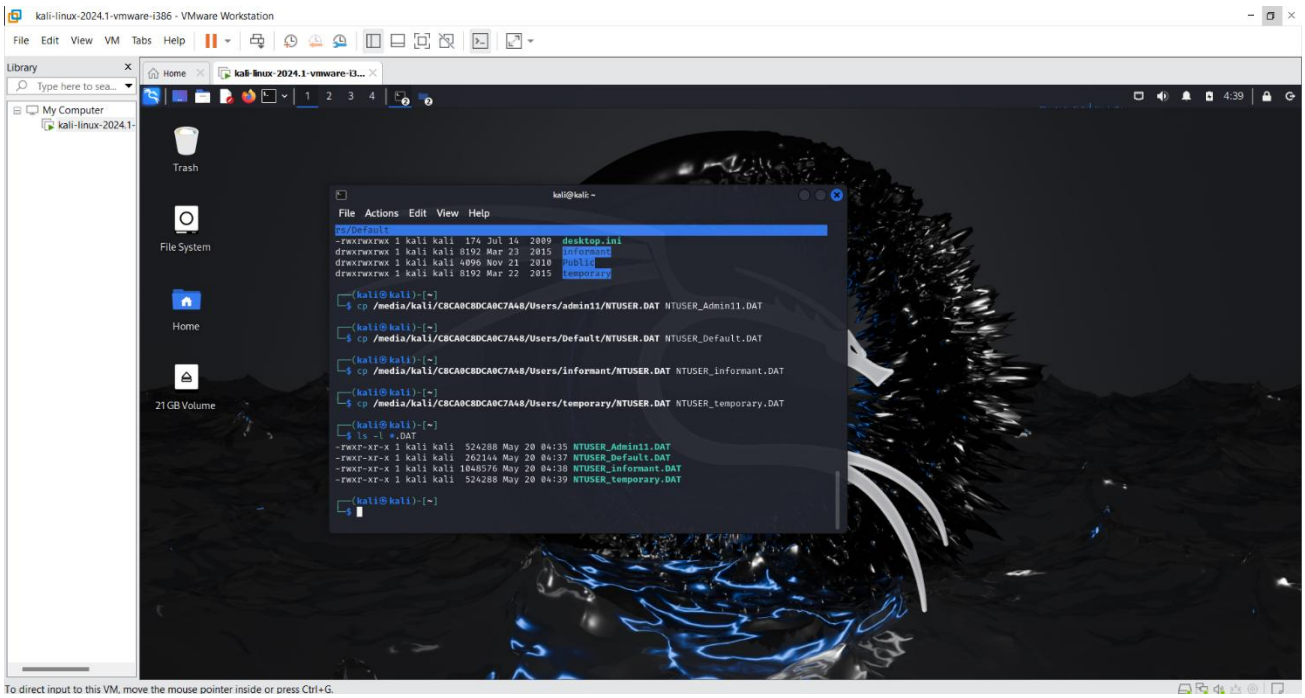
- *Here the command* '/media/kali/C8CA0C8DCA0C7A48/Users' is to find users in the PC.

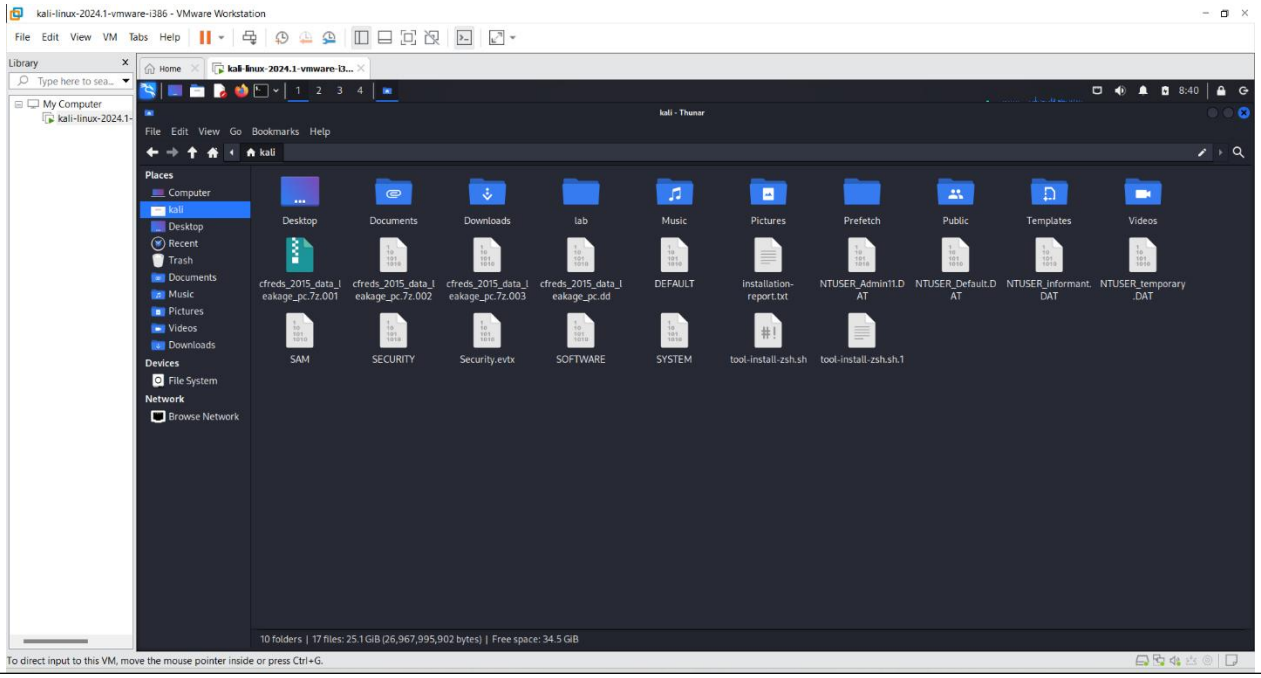


- In this next step users need to copy the HKEY_USERS hive files to \lab. The

command must be properly written without any wrong to avoid any error.

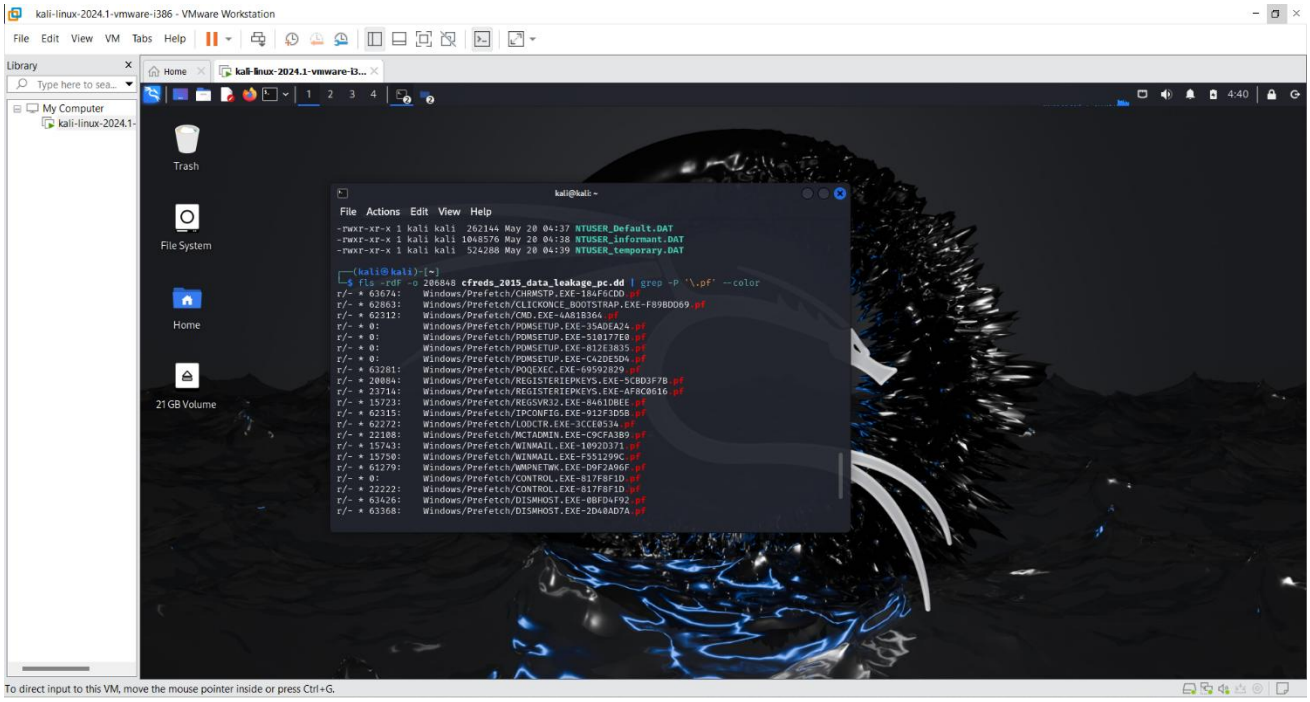
- After successfully copied, users can verify four of the file by putting in the command 'ls -l *.DAT'



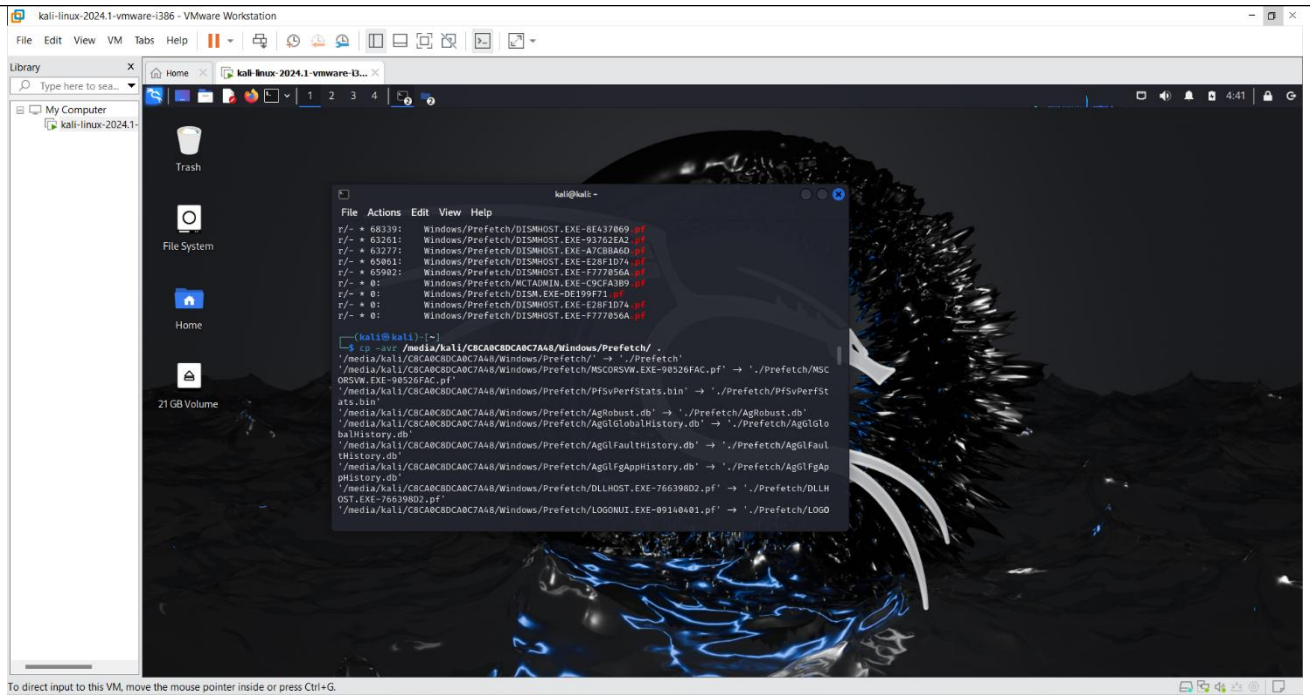


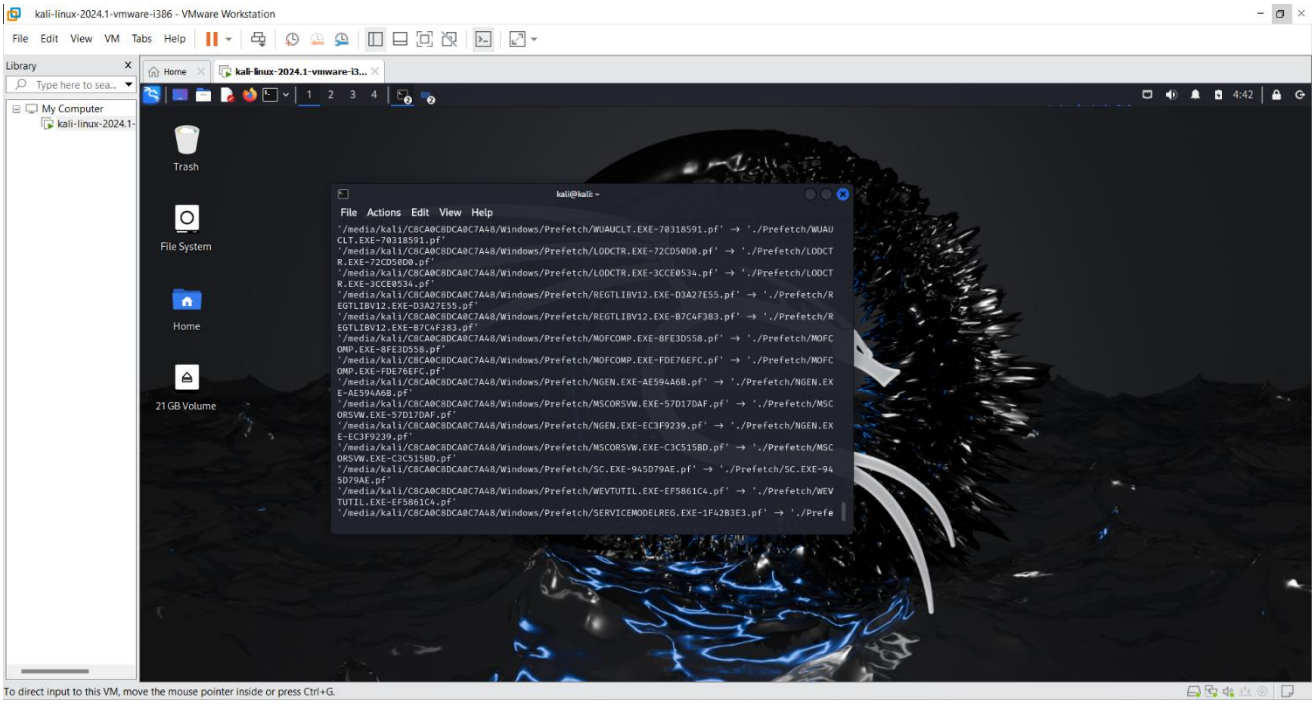
5. Extract prefetch event log files from a DD image.

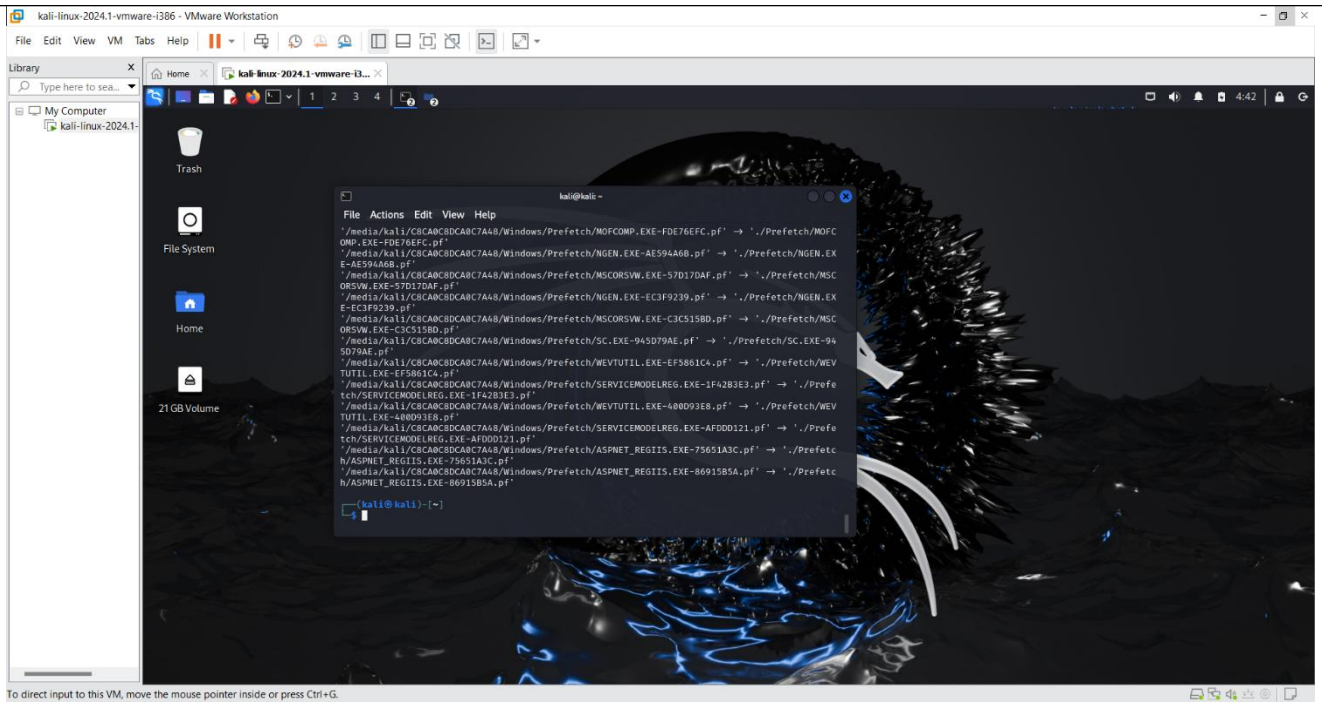
- The next step is to check the .pf files in a DD image the command '-P' is Perl-compatible with regular expressions. '\' is to escape a special character. '-rdF' are recursively,display only files, and deleted. In below pictures, shows the .pf files that are available inside the DD image.



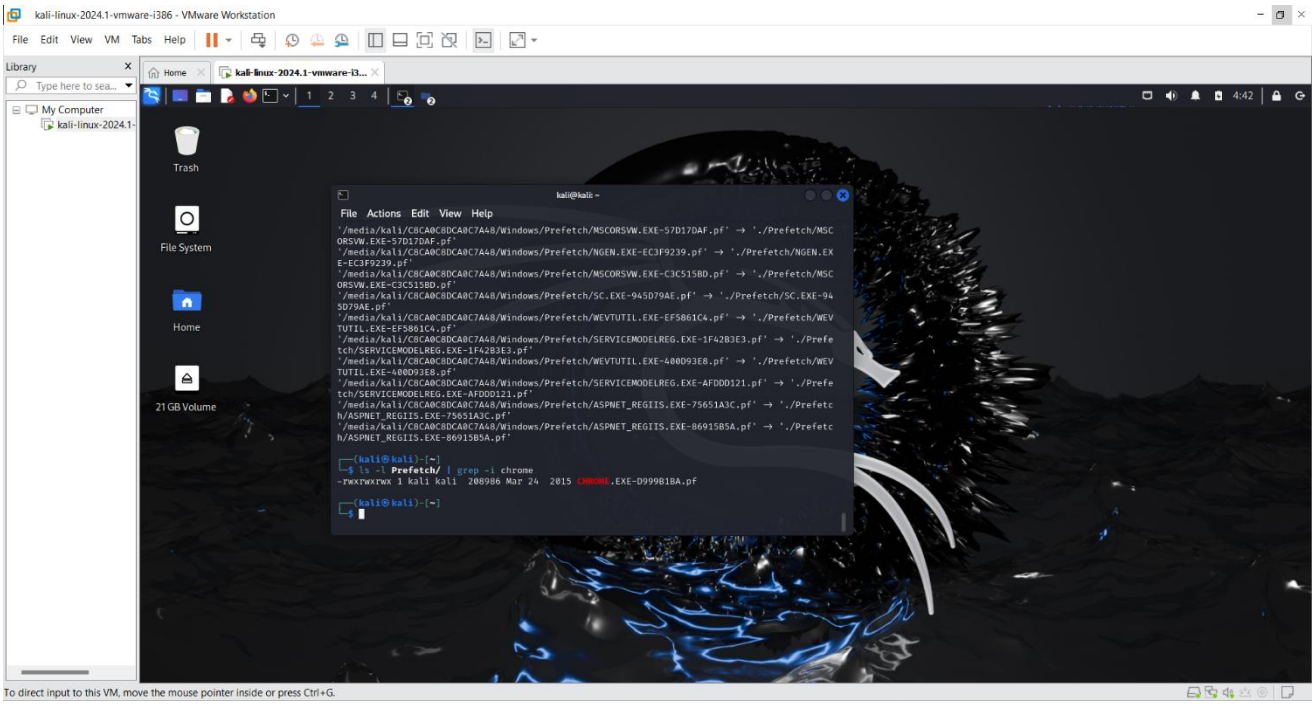
- In the next step user needs to copy all the prefetch folders that are available to '/Windows/Prefetch/. This prefetch log can be used for forensic analysis for example monitoring program execution.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
21 GB Volume
kali@kali: ~
File Actions Edit View Help
r/- * 68339: Windows/Prefetch/DISMHOST.EXE-8E437069.pf
r/- * 63261: Windows/Prefetch/DISMHOST.EXE-93762EA2.pf
r/- * 63277: Windows/Prefetch/DISMHOST.EXE-A7CB8A6D.pf
r/- * 65001: Windows/Prefetch/DISMHOST.EXE-E28F1D74.pf
r/- * 65002: Windows/Prefetch/DISMHOST.EXE-F777056A.pf
r/- * 0: Windows/Prefetch/MCTADMIN.EXE-C9CFA3B9.pf
r/- * 0: Windows/Prefetch/DISM.EXE-DE199F71.pf
r/- * 0: Windows/Prefetch/DISMHOST.EXE-E28F1D74.pf
r/- * 0: Windows/Prefetch/DISMHOST.EXE-F777056A.pf
┌──(kali㉿kali)-[~]
└─$ cp -avr /media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/ .
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/' → './Prefetch'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/MSCORSVW.EXE-90526FAC.pf' → './Prefetch/MSCORSVW.EXE-90526FAC.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/PfSvPerfStats.bin' → './Prefetch/PfSvPerfStats.bin'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/AgRobust.db' → './Prefetch/AgRobust.db'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/AgGlGlobalHistory.db' → './Prefetch/AgGlGlobalHistory.db'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/AgGlFaultHistory.db' → './Prefetch/AgGlFaultHistory.db'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/AgGlFgAppHistory.db' → './Prefetch/AgGlFgAppHistory.db'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/DLLHOST.EXE-766398D2.pf' → './Prefetch/DLLHOST.EXE-766398D2.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/LOGONUI.EXE-09140401.pf' → './Prefetch/LOGO
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
Trash
File System
Home
21 GB Volume
kali@kali: ~
File Actions Edit View Help
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/WUAUCLT.EXE-70318591.pf' → './Prefetch/WUAUCLT.EXE-70318591.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/LODCTR.EXE-72CD50D0.pf' → './Prefetch/LODCTR.EXE-72CD50D0.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/LODCTR.EXE-3CCE0534.pf' → './Prefetch/LODCTR.EXE-3CCE0534.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/REGTLIBV12.EXE-D3A27E55.pf' → './Prefetch/REGTLIBV12.EXE-D3A27E55.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/REGTLIBV12.EXE-B7C4F383.pf' → './Prefetch/REGTLIBV12.EXE-B7C4F383.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/MOFCOMP.EXE-8FE3D558.pf' → './Prefetch/MOFCOMP.EXE-8FE3D558.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/MOFCOMP.EXE-FDE76EFC.pf' → './Prefetch/MOFCOMP.EXE-FDE76EFC.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/NGEN.EXE-AE594A6B.pf' → './Prefetch/NGEN.EXE-AE594A6B.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/MSCORSVW.EXE-57D17DAF.pf' → './Prefetch/MSCORSVW.EXE-57D17DAF.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/NGEN.EXE-EC3F9239.pf' → './Prefetch/NGEN.EXE-EC3F9239.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/MSCORSVW.EXE-C3C515BD.pf' → './Prefetch/MSCORSVW.EXE-C3C515BD.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/SC.EXE-945D79AE.pf' → './Prefetch/SC.EXE-945D79AE.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/WEVTUTIL.EXE-EF5861C4.pf' → './Prefetch/WEVTUTIL.EXE-EF5861C4.pf'
'/media/kali/C8CA0C8DCA0C7A48/Windows/Prefetch/SERVICEMODELREG.EXE-1F42B3E3.pf' → './Prefe
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

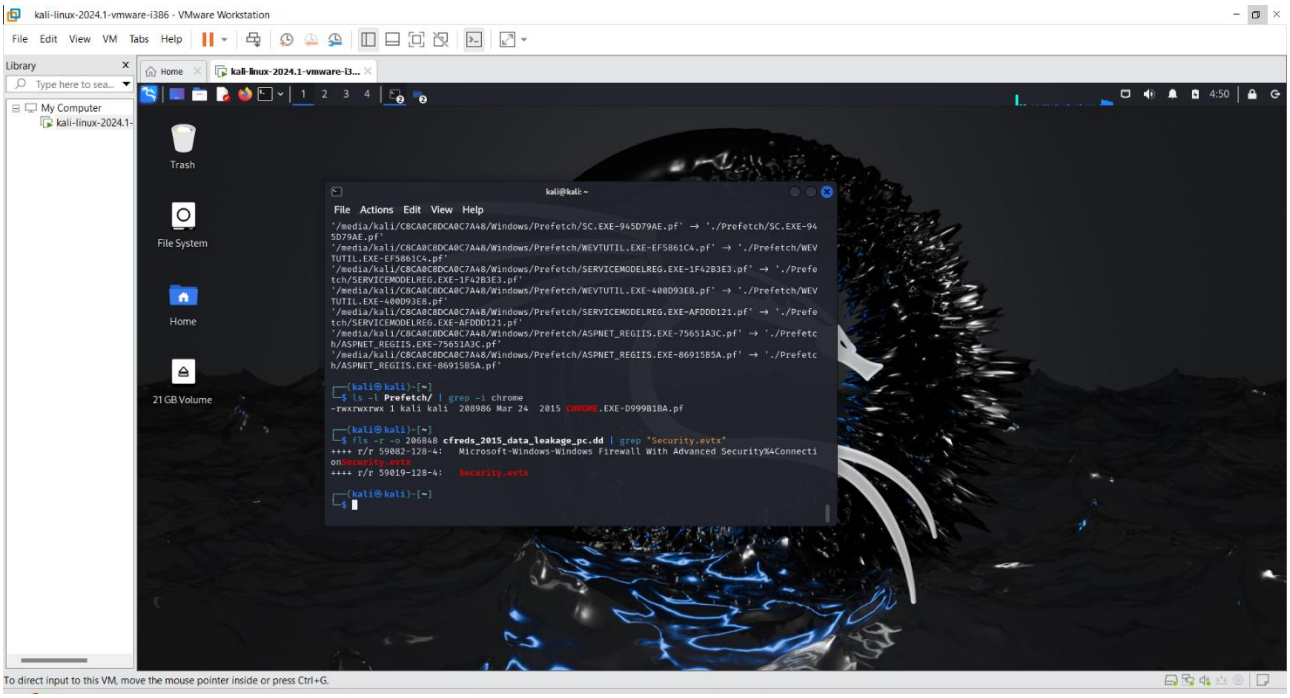


- This command will allow to verify and check that .pf of chrom.exe is in the ./Prefetch folder. The command ‘CHROME.EXE-D999B1BA.pf’ shows that the chrom.exe is exist.

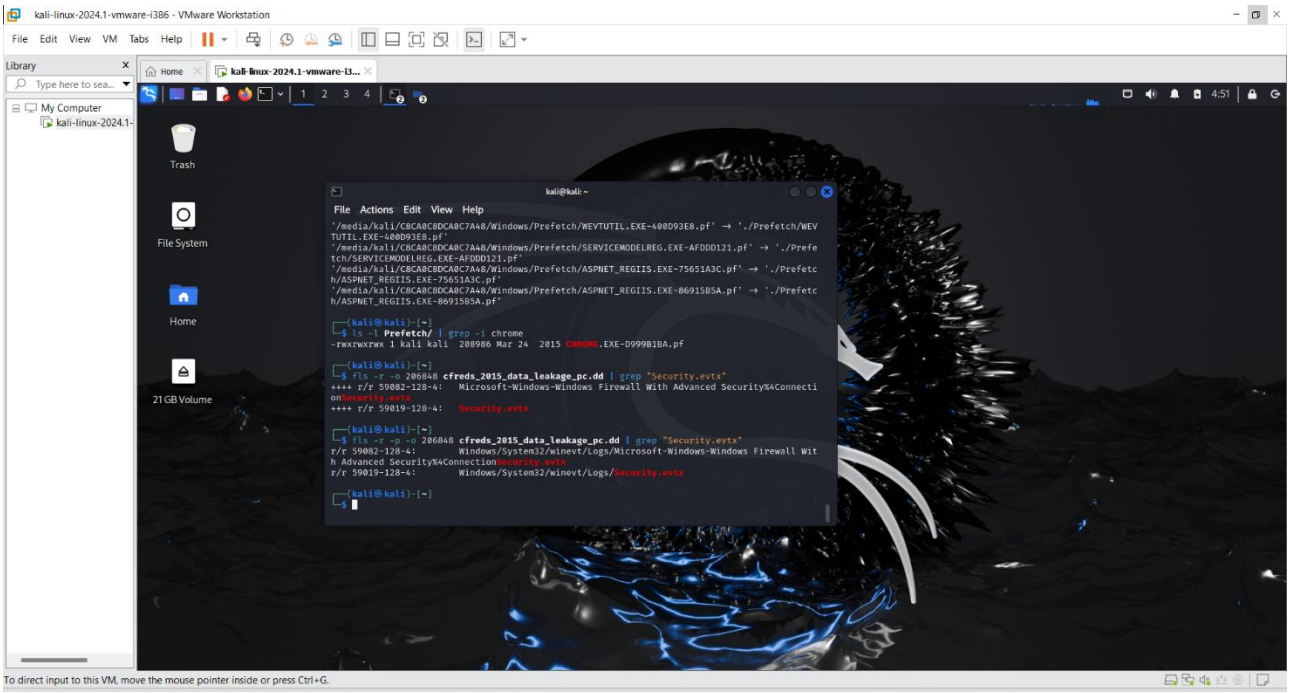


6. Extract security event log files from the DD image.

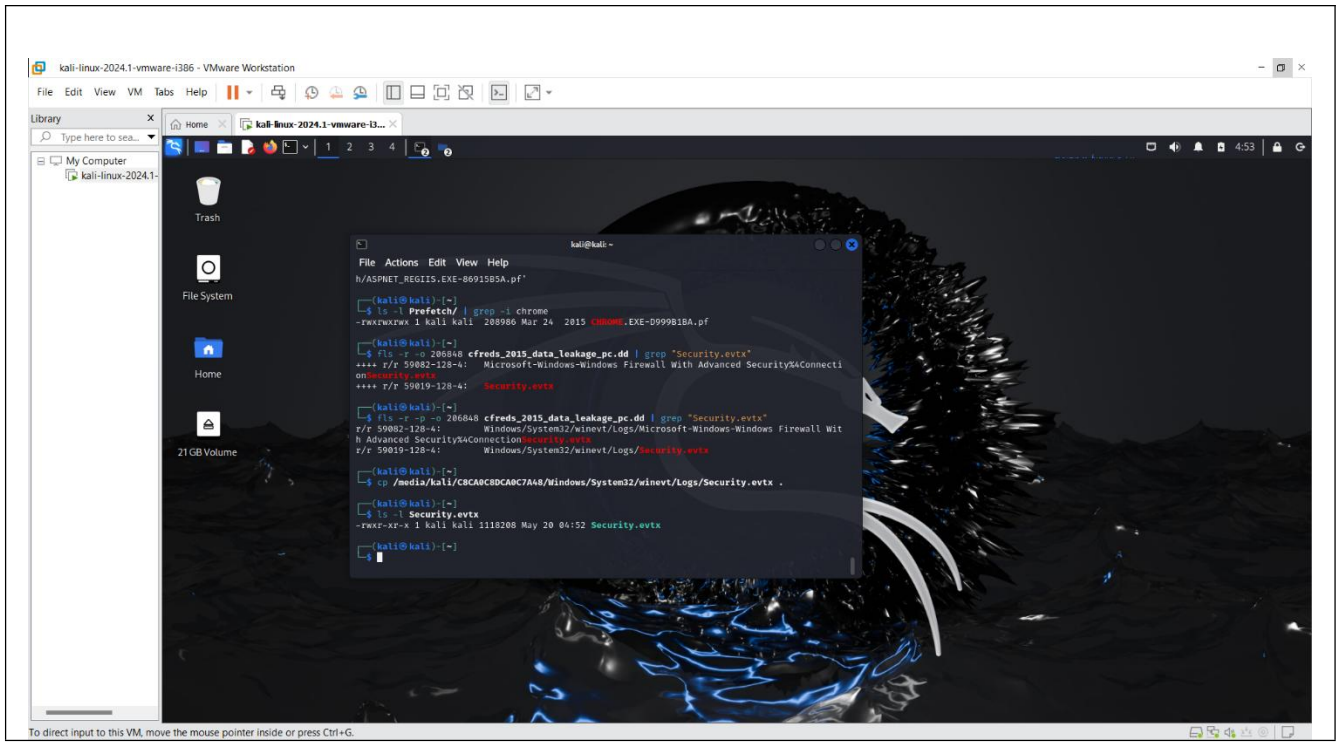
- Before I'm able to extract the security event log files from the DD image I will need to search for "Security.evtx" from the DD image. The command below will be use to show the directory entries (-r).



- After that I will need to search for “Security.evtx’ from the DD image with ‘-p’ which to show the full path of the file.



- Last step is to copy the “Security.evtx” from the DD image to the lab directory. The command ‘ls -l’ is to list out to verify the file. In this picture it’s succesfully being copied.


kali-linux-2024.1-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2024.1-
Home
kali-linux-2024.1-vmware-i3...
1 2 3 4
4:53
Trash
File System
Home
21 GB Volume
kali@kali: ~
File Actions Edit View Help
h/ASPNET_REGIIS.EXE-86915B5A.pf'
┌──(kali㉿kali)-[~]
└─$ ls -l Prefetch/ | grep -i chrome
-rwxrwxrwx 1 kali kali 208986 Mar 24 2015 CHROME.EXE-D999B1BA.pf
┌──(kali㉿kali)-[~]
└─$ fls -r -o 206848 cfreds_2015_data_leakage_pc.dd | grep "Security.evtx"
++++ r/r 59082-128-4: Microsoft-Windows-Windows Firewall With Advanced Security%4Connecti
onSecurity.evtx
++++ r/r 59019-128-4: Security.evtx
┌──(kali㉿kali)-[~]
└─$ fls -r -p -o 206848 cfreds_2015_data_leakage_pc.dd | grep "Security.evtx"
r/r 59082-128-4: Windows/System32/winevt/Logs/Microsoft-Windows-Windows Firewall Wit
h Advanced Security%4ConnectionSecurity.evtx
r/r 59019-128-4: Windows/System32/winevt/Logs/Security.evtx
┌──(kali㉿kali)-[~]
└─$ cp /media/kali/C8CA0C8DCA0C7A48/Windows/System32/winevt/Logs/Security.evtx .
┌──(kali㉿kali)-[~]
└─$ ls -l Security.evtx
-rwxr-xr-x 1 kali kali 1118208 May 20 04:52 Security.evtx
┌──(kali㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.