ITS60904

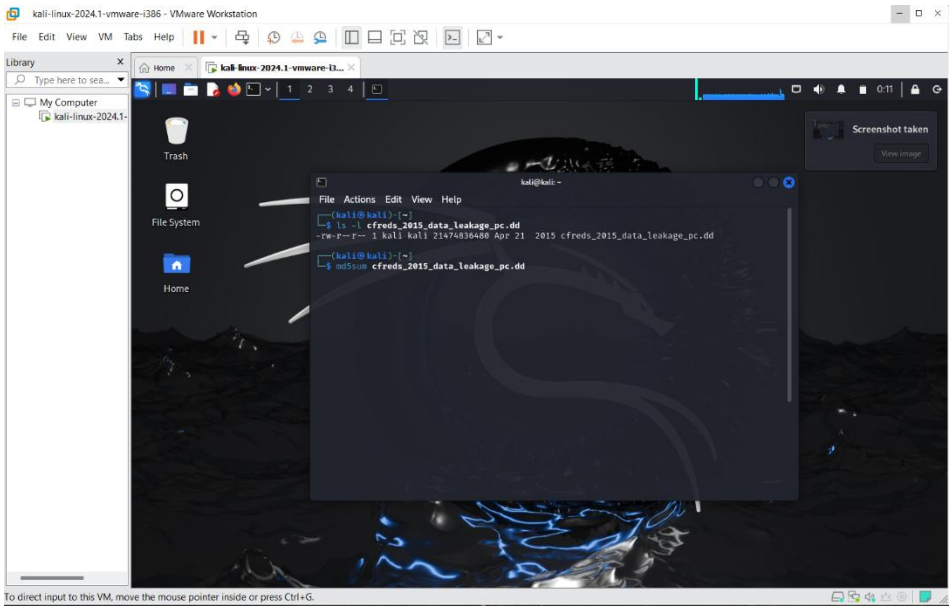
COMPUTER CRIME AND DIGITAL EVIDENCE

PRACTICAL 3 LAB REPORT

1. What are the hash values (MD5 & SHA-1) of the image? (Linux)

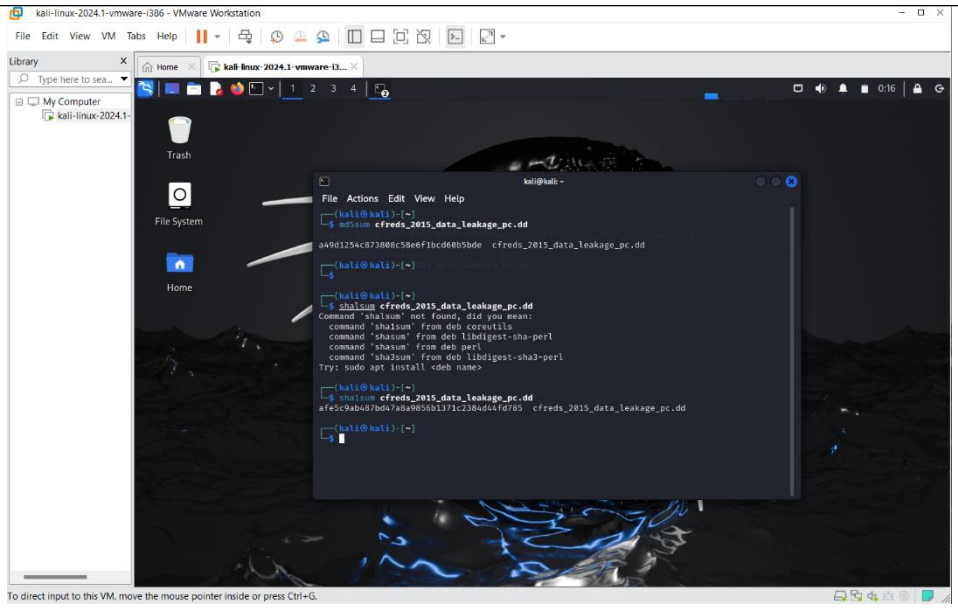
Verify you have the dd image:

The phrase "Verify you have the dd image" is significant because it highlights how crucial it is to make sure you have a disc image made using the `dd} command. This is essential because the disc image contains a byte-by-byte replica of the original storage device, which is necessary for data recovery, forensic investigation, or system restoration. The precision and thoroughness of any recovery or analysis procedure could be jeopardised without this image.



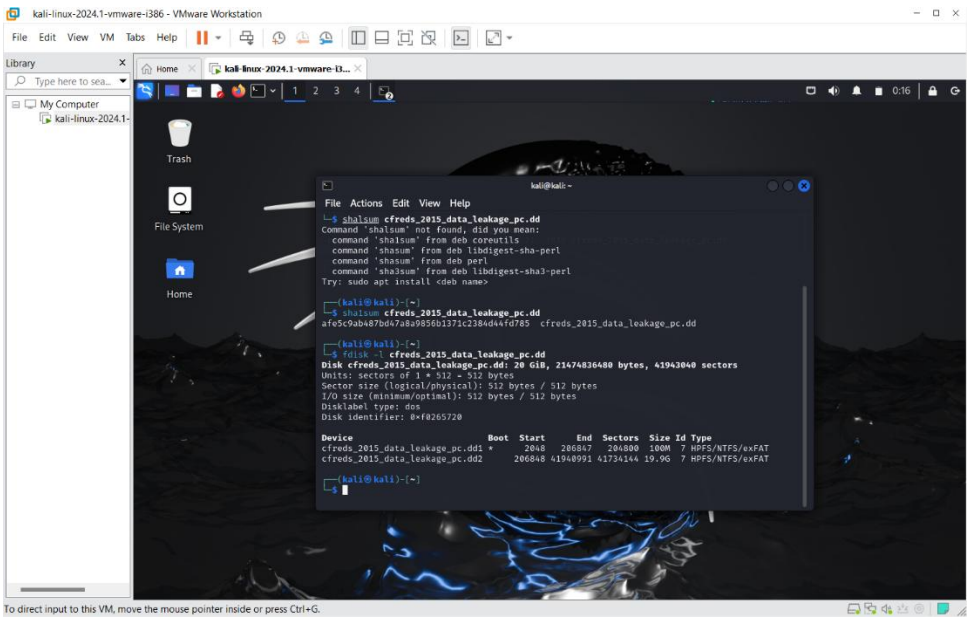
Compute MD5 and SHA1 of the DD image:

Data integrity and authenticity are guaranteed by calculating the MD5 and SHA1 hashes of a DD image, which is a bit-by-bit replica of a storage device. By acting as distinct digital fingerprints, these hashes confirm that the image hasn't been tampered with or distorted. In domains where preserving the original state of data is critical, such as digital forensics and data recovery, this procedure is essential.



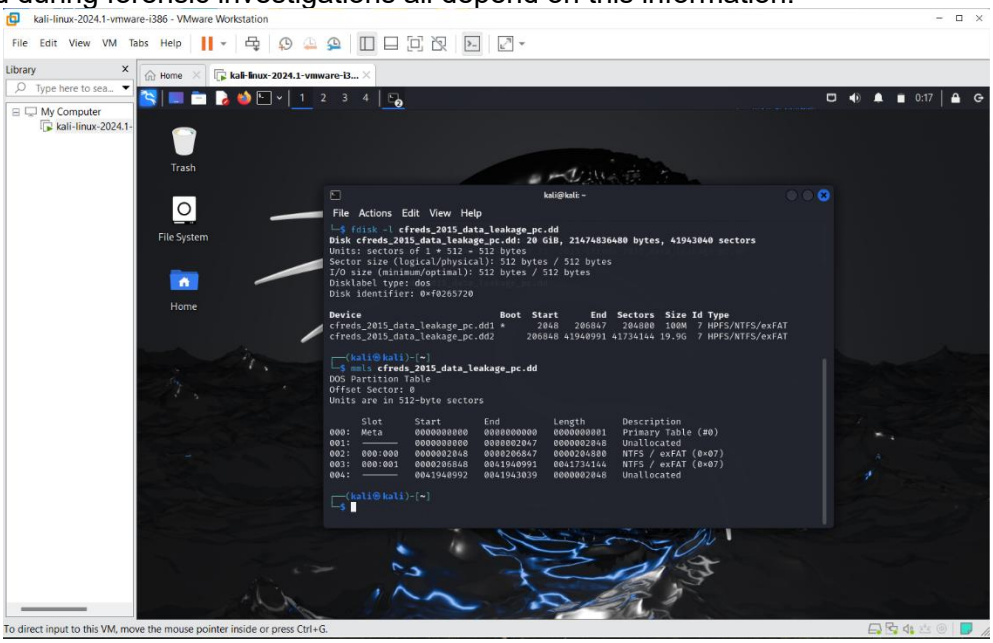
2.1 How to identify the partition information of PC image? (Method 1 -fdisk)

Show partitions of the image:
Partitioning an image means breaking it up into separate areas or sections. This procedure is crucial for a number of applications, including computer vision, object recognition, and image analysis, as it reduces the intricacy of the image and facilitates the study and processing of particular regions. Algorithms can more successfully detect patterns, objects, and pertinent elements in a picture by concentrating on particular segments.



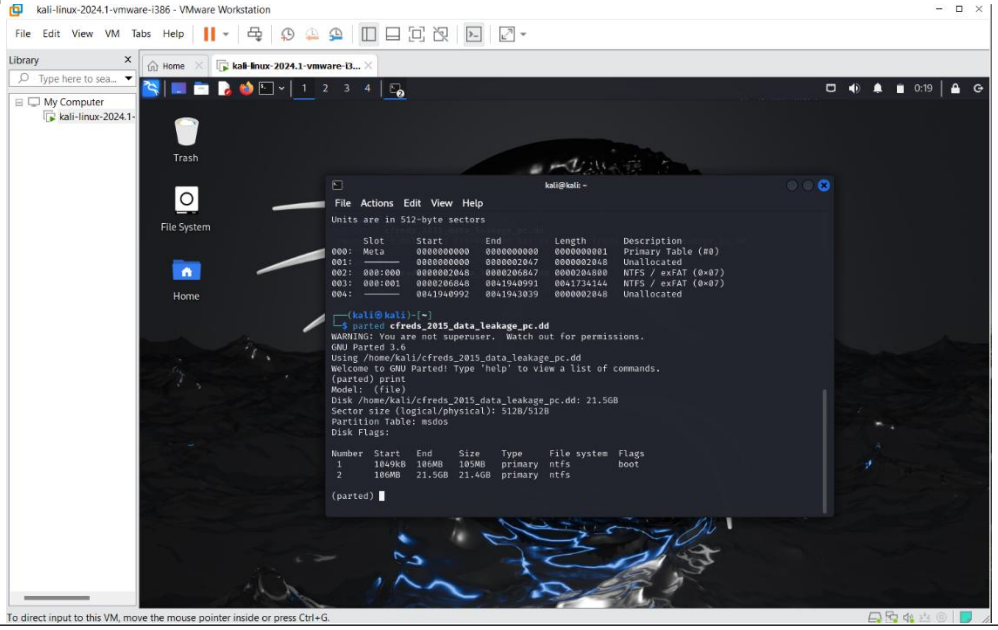
Show partitions and unallocated space using mmls:
Digital forensics and system management depend heavily on the ability to display partitions

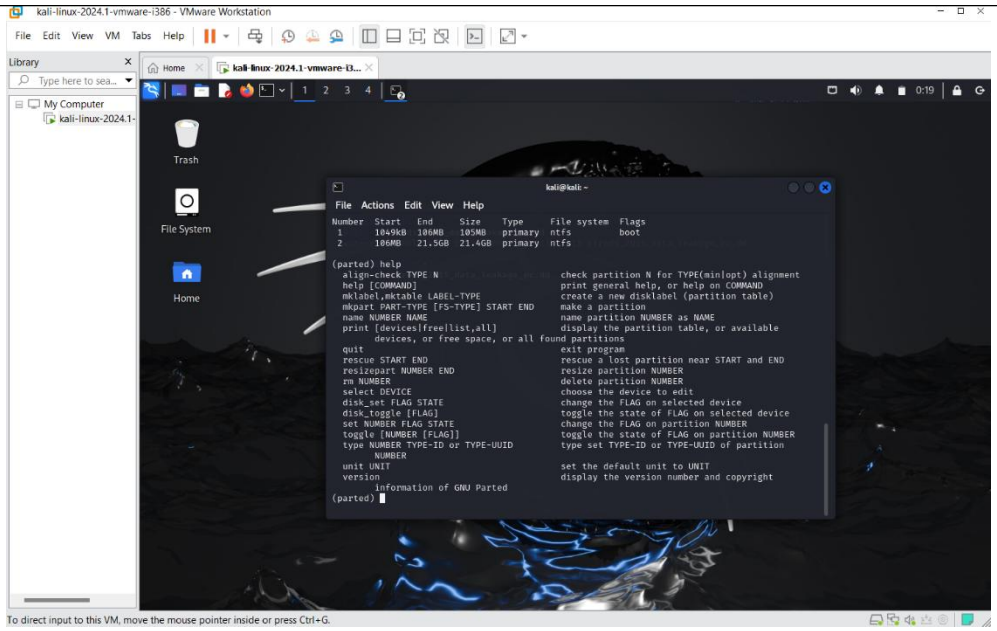
and unallocated space on a disc using {mmls} (Media Management Listing). It facilitates the identification of a disk's structure, including its primary and extended partitions as well as any unallocated space. Data recovery, disc utilisation analysis, and making sure no important data is missed during forensic investigations all depend on this information.



Identify the partition information of PC image:

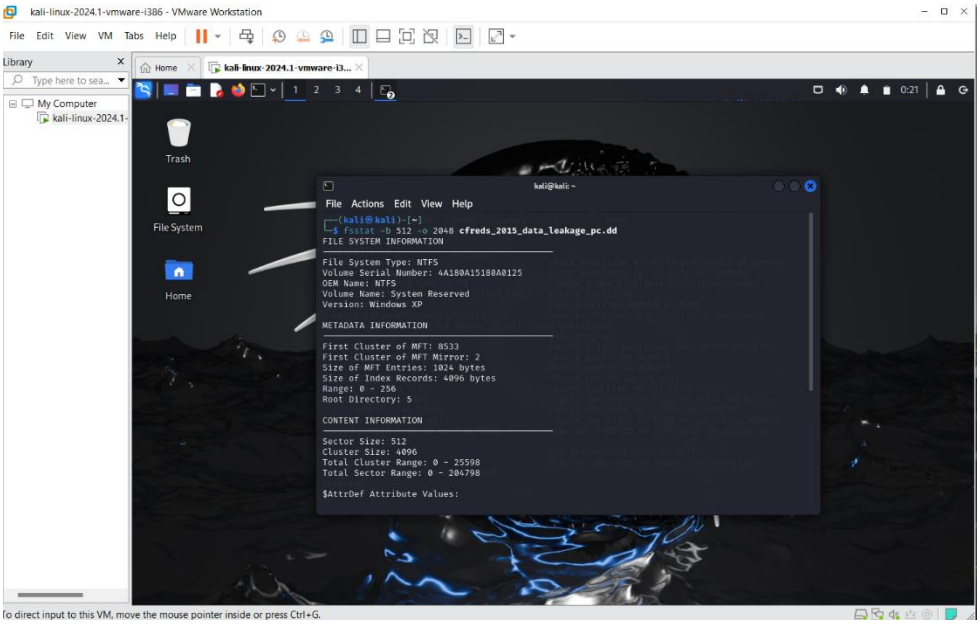
The specifics of how the storage device is split up into different sections, each functioning as an independent storage unit, are referred to as the partition information of a PC image. The way that data is arranged, maintained, and retrieved on the device is determined by this information, which has an effect on the effectiveness and dependability of data retrieval and storage processes.

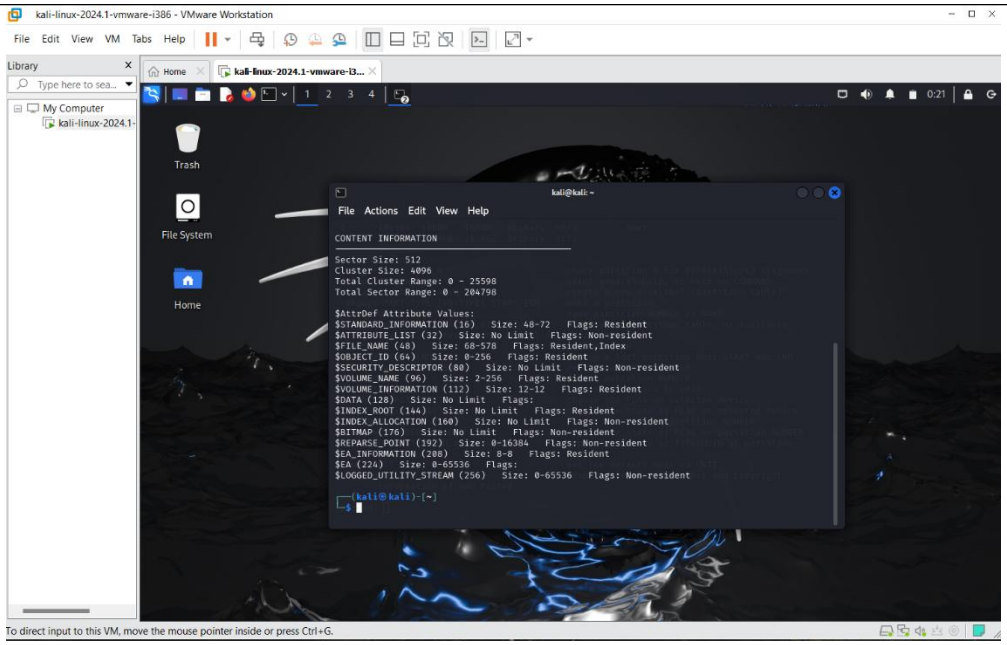




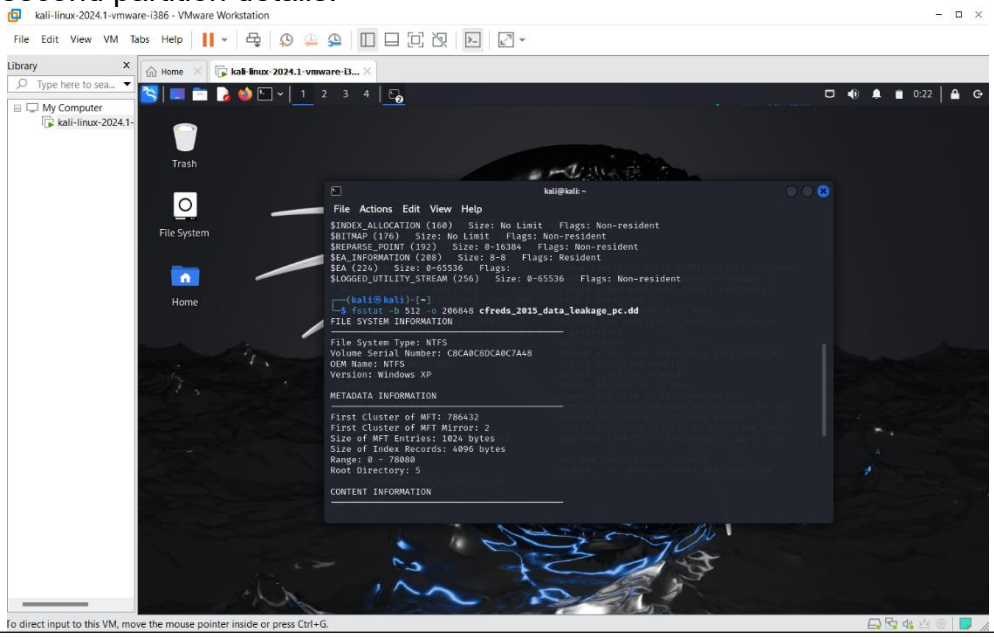
List the first partition details using file system stat (fsstat):

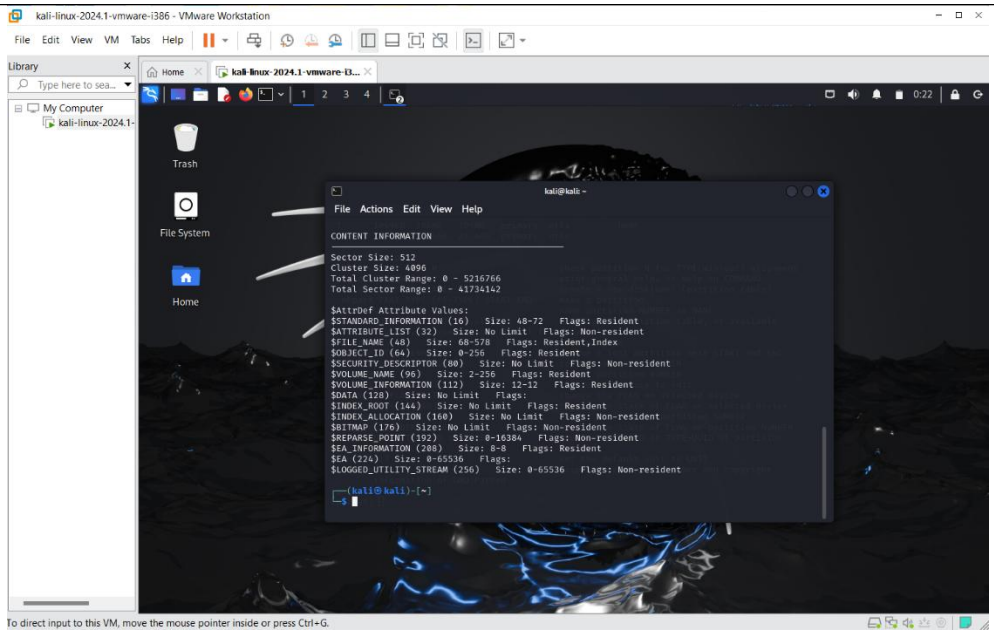
To view comprehensive file system information, use the `fsstat` command. `fsstat` on a disc image displays a variety of file system characteristics, including partition information. Using `fsstat` to list the first partition details reveals details about the file system, including its size, layout, and type. These details are critical for activities related to system management, forensic analysis, and data recovery. Comprehension of how data is arranged on the disc and carrying out operations like mounting the file system or examining its contents require a basic comprehension of this information.



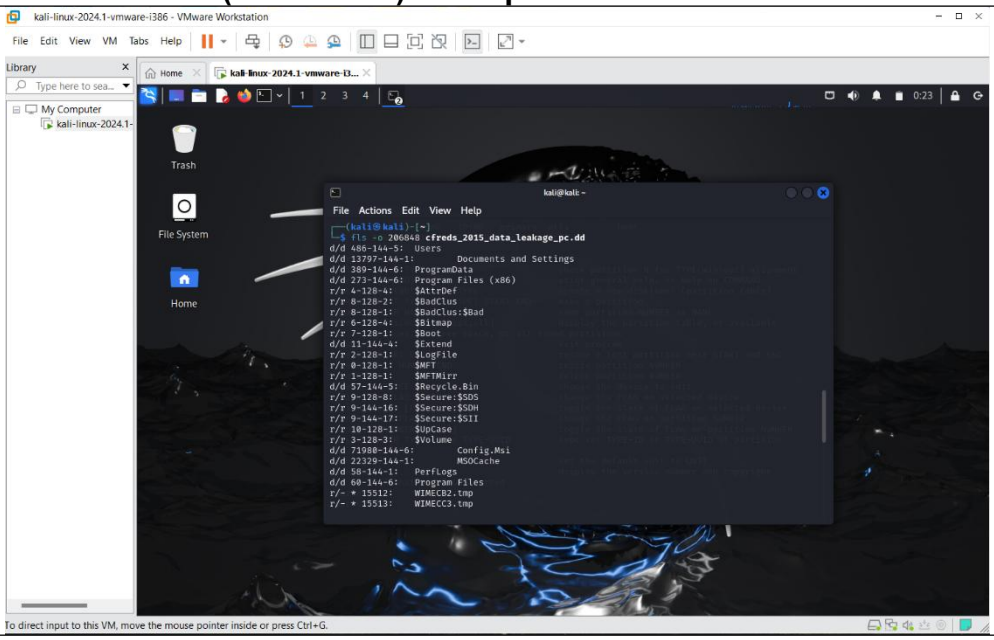


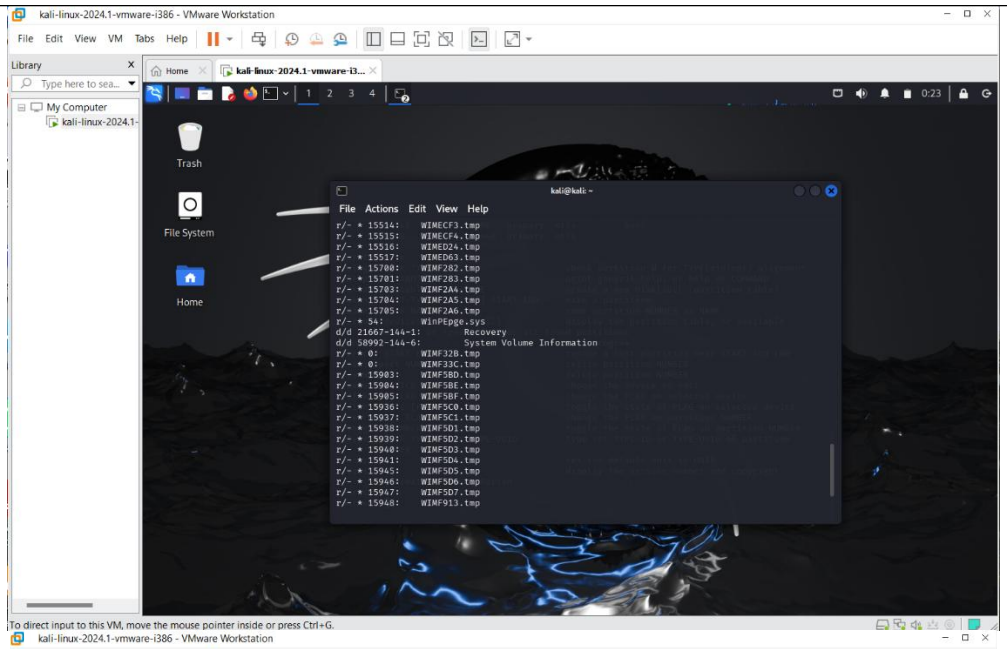
List the second partition details:

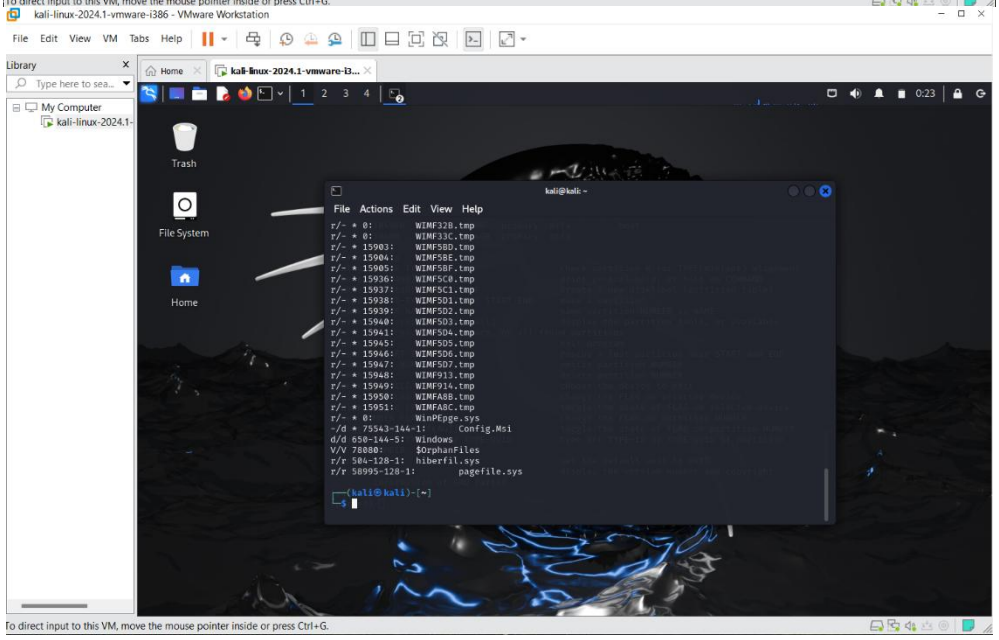




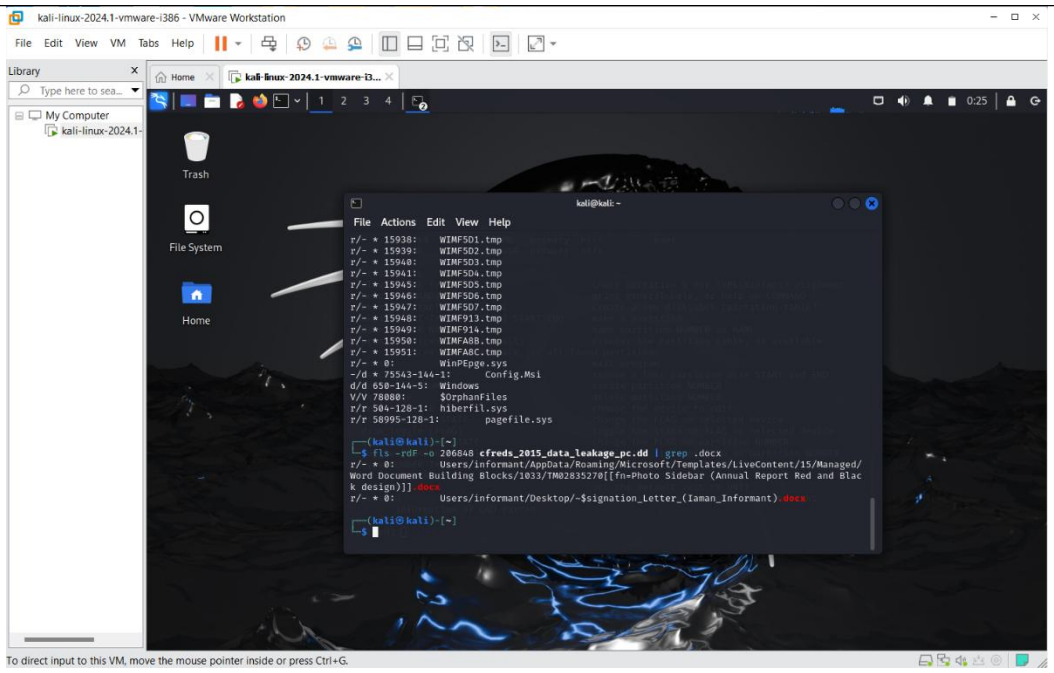
2.2 How to show files (directories) in 2nd partition?



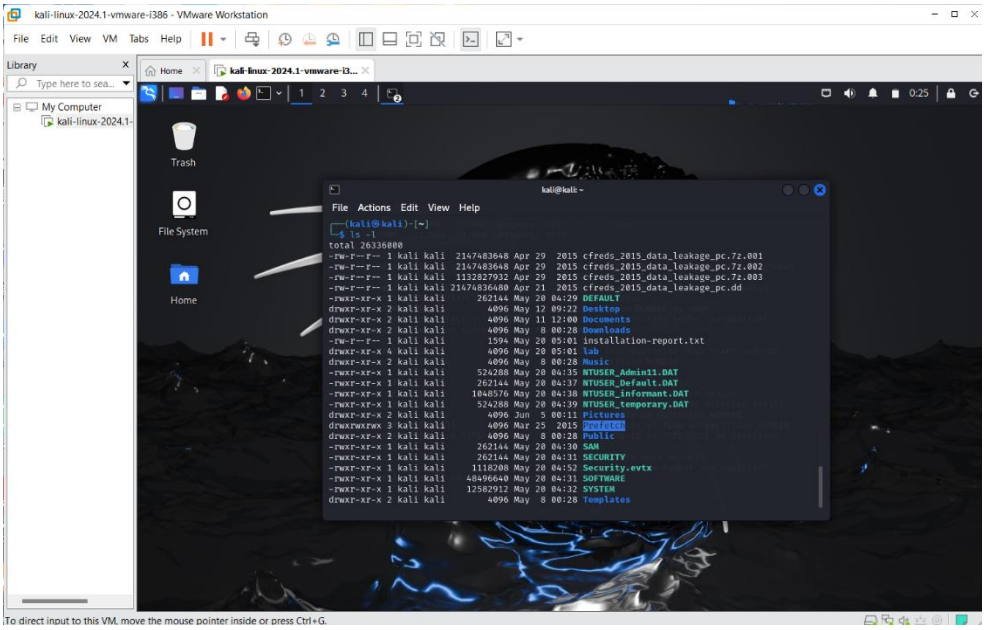


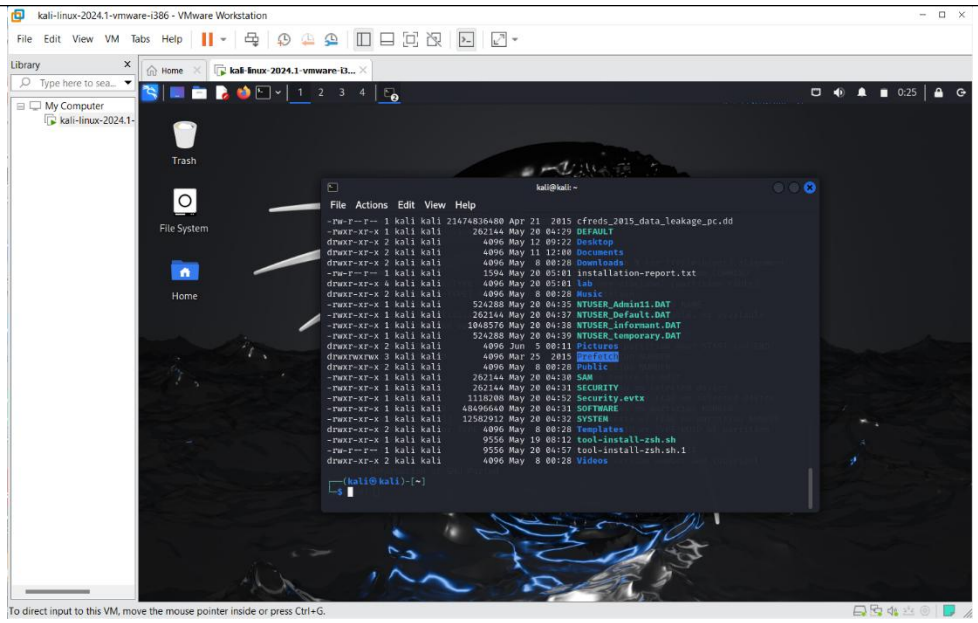


2.3 How to list all deleted .docx files in the whole partition?

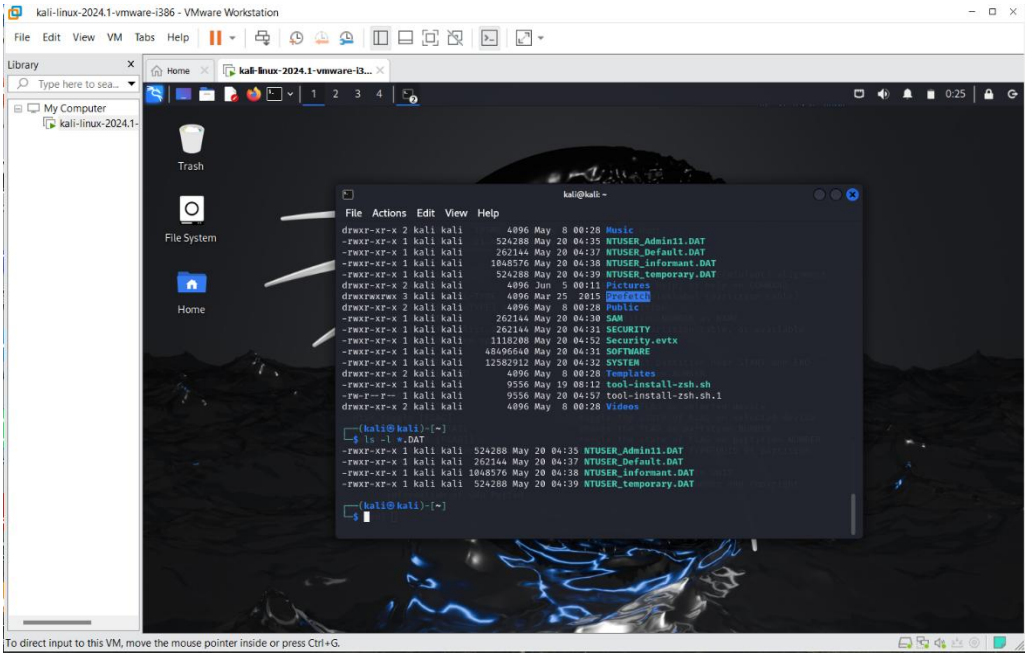


Verify system information:

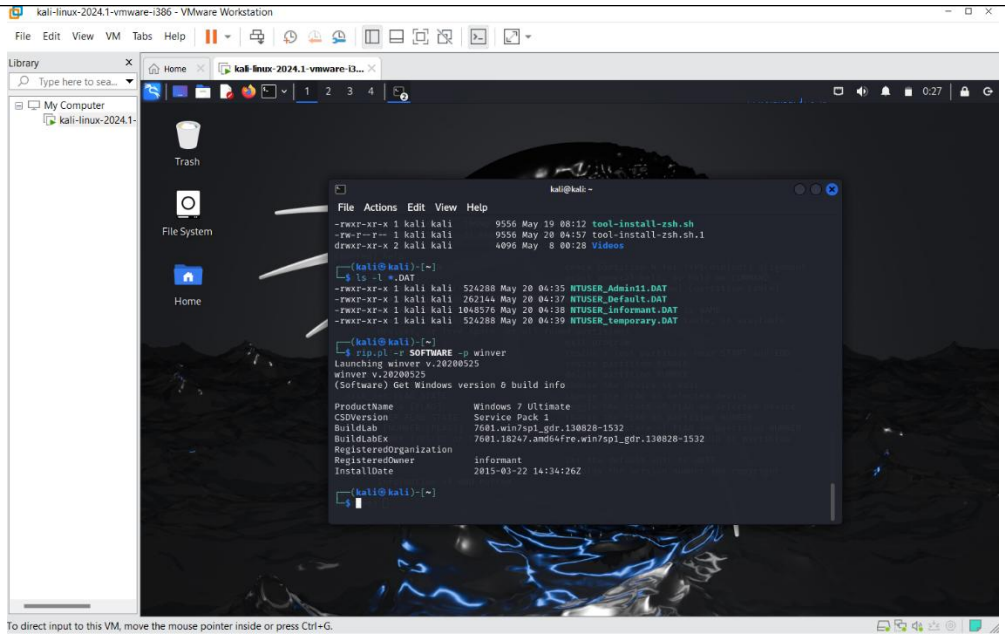




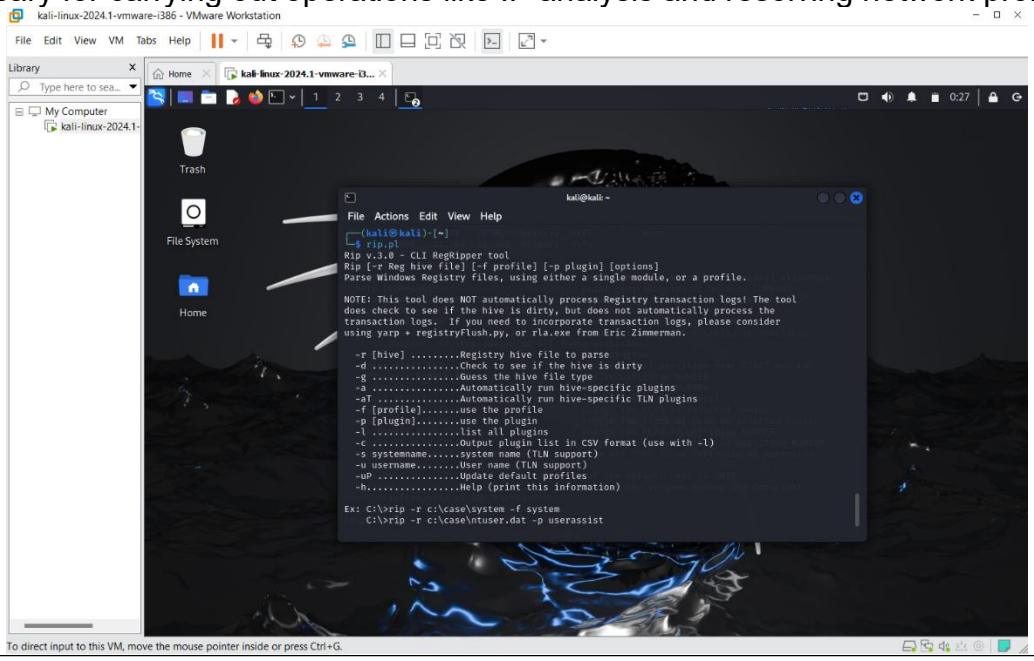
Verify Users' information:

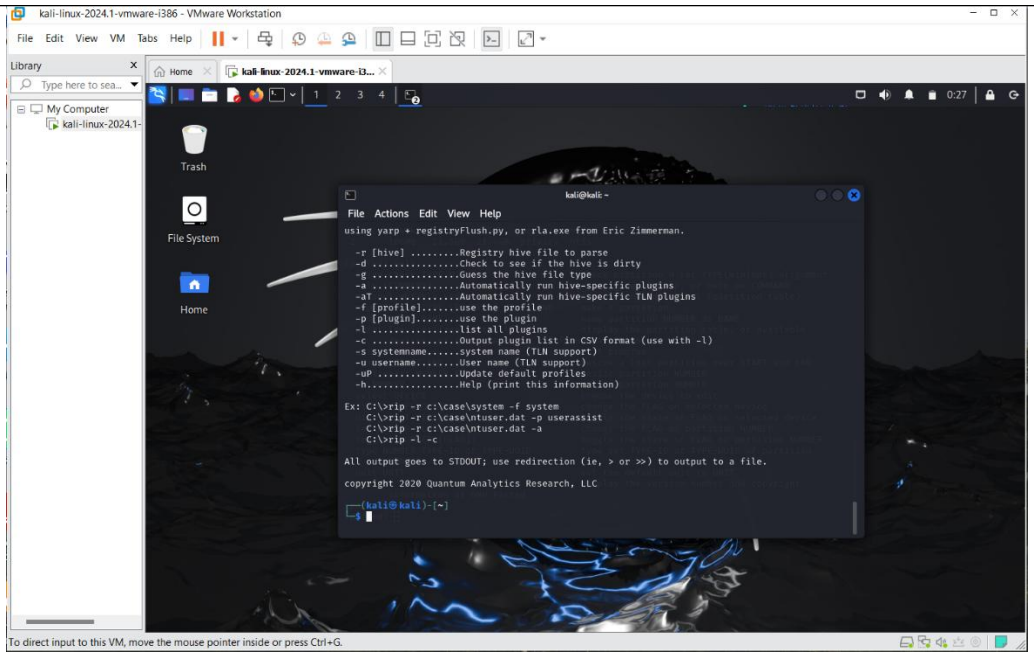


3. What is the installed OS information in detail?

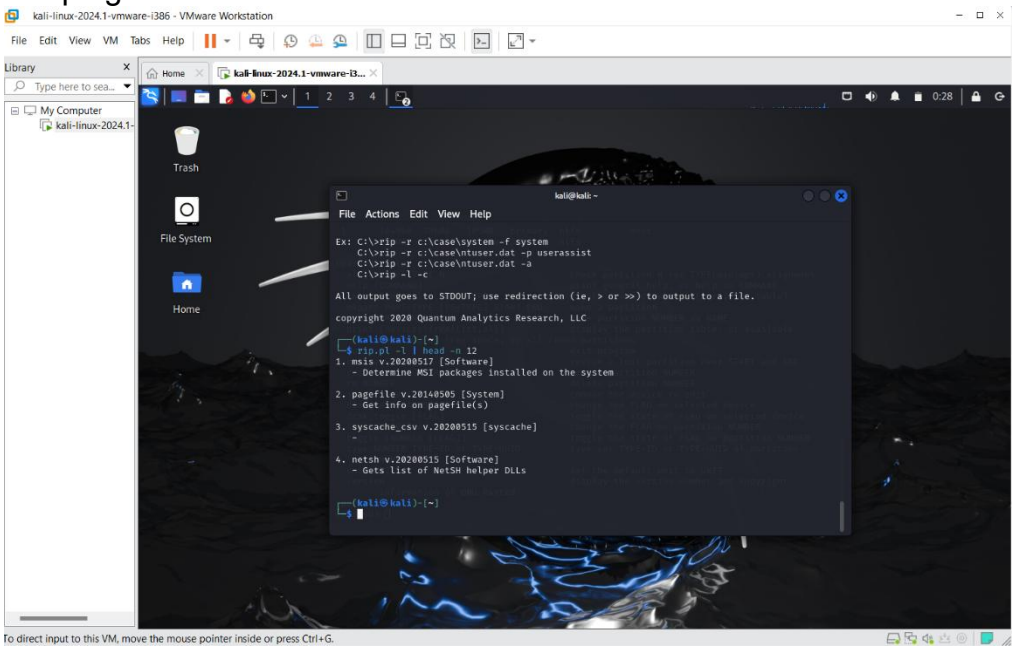


Show rip.pl command help:
Users must comprehend the help command (rip.pl -h) to use the script efficiently. It gives the necessary instructions on how to use the capabilities of the script, which is necessary for carrying out operations like IP analysis and resolving network problems.



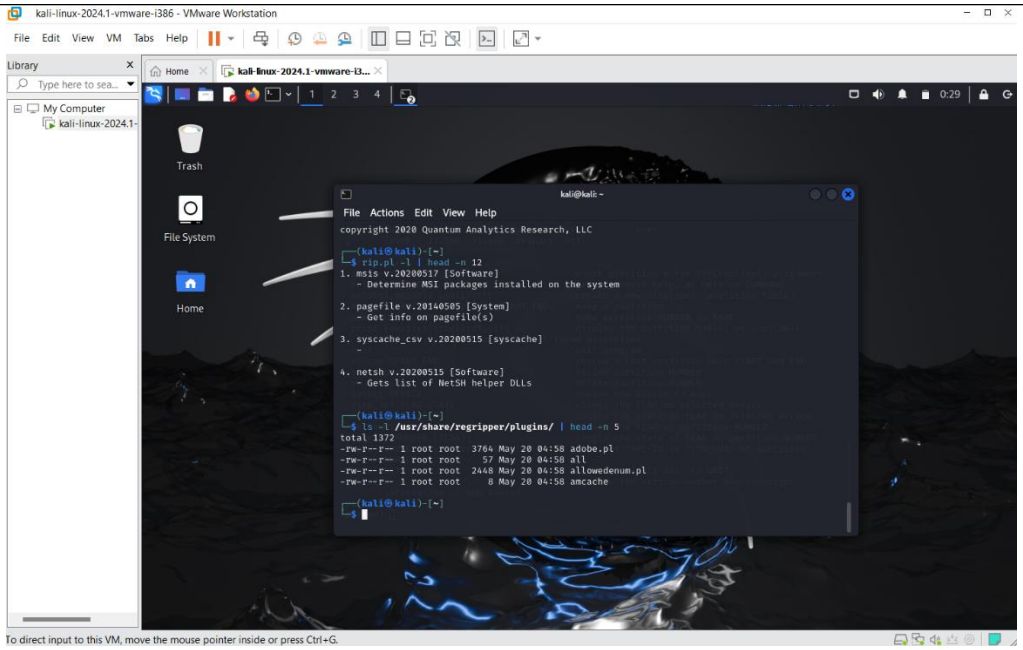


List all 243 plugins of SOFTWARE:



Show the location of all plugins:

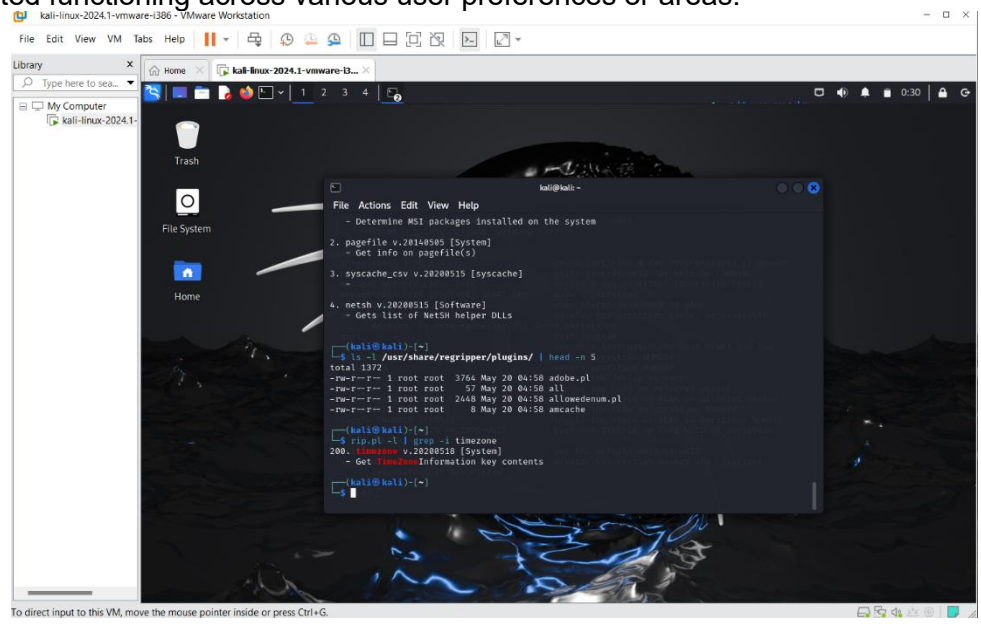
For developers or system administrators in charge of a software environment, "Show the location of all plugins" is an essential command, particularly when working with intricate systems or programs that have a large number of plugins. It is easier to debug, update, and ensure compatibility and security inside the system when you know where each plugin is located. This information improves the software's general stability and performance and makes maintenance easier.



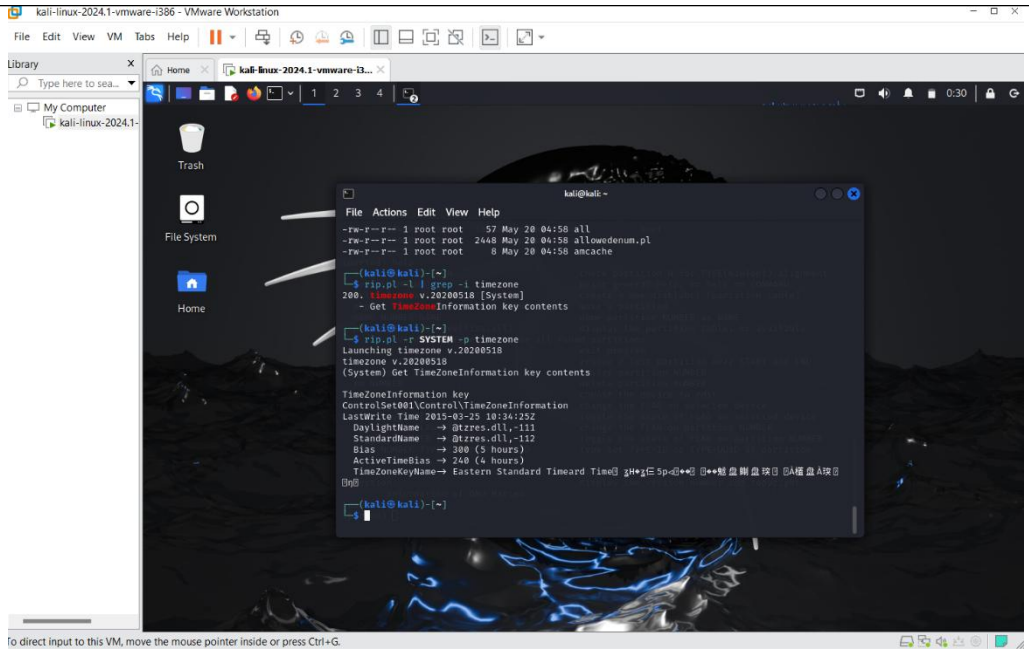
4. What is the time zone setting?

Search for timezone plugin and the file that contains timezone:

Comprehending this data is essential for tasks related to software development and system management, particularly for systems that require precise handling of several time zones or include time-sensitive procedures. The plugin and associated file probably make it easier to convert, manage, or configure time zones inside of software systems, guaranteeing accurate time-related functioning across various user preferences or areas.

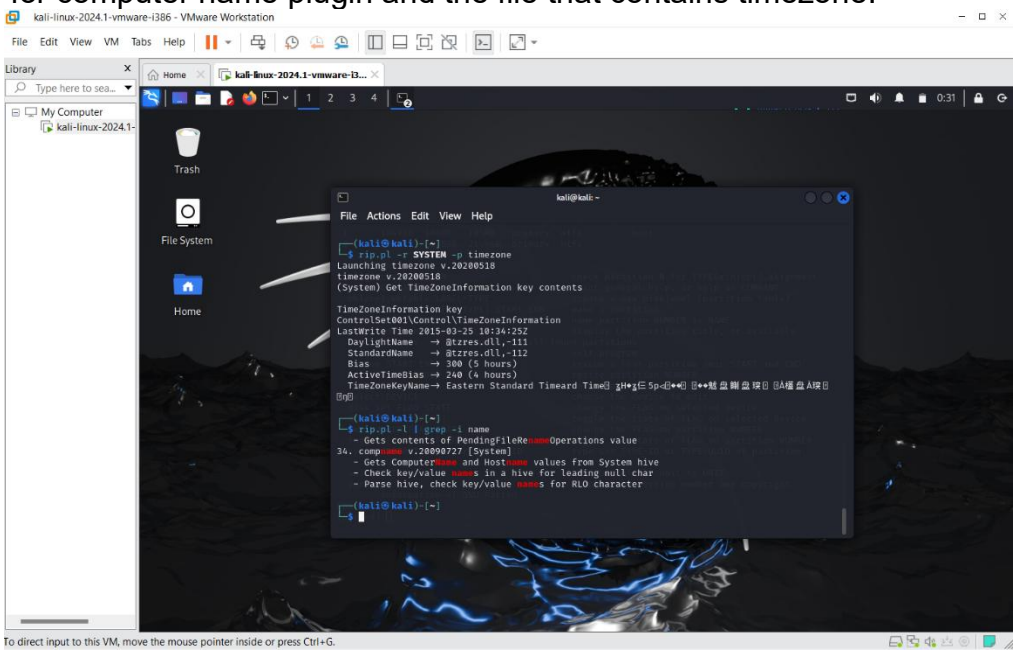


Run timezone plugin:

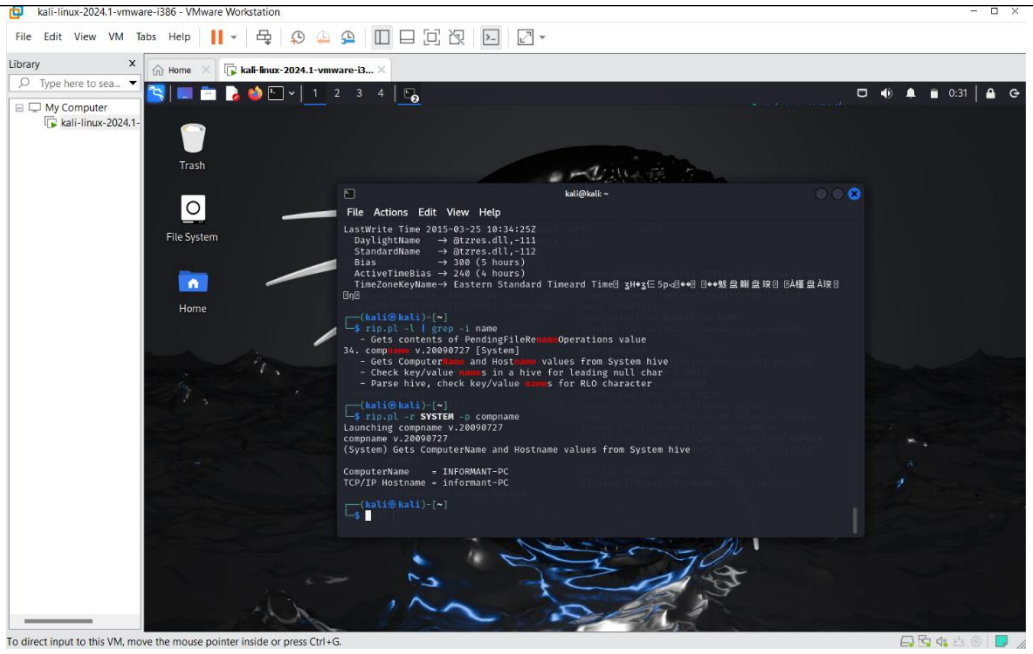


5. What is the computer name?

Search for computer name plugin and the file that contains timezone:

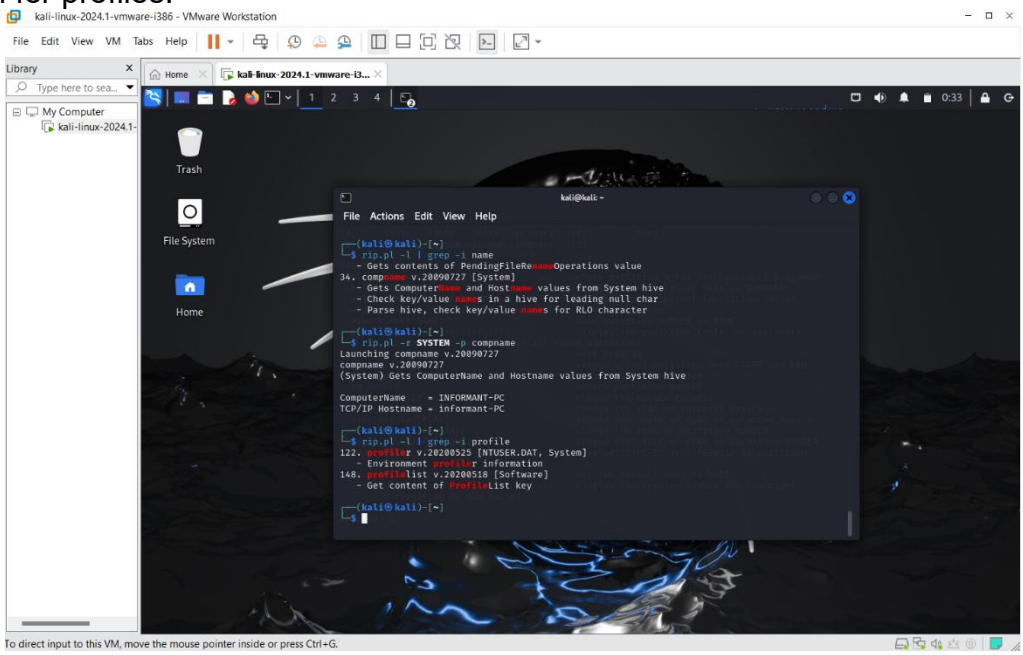


Run compname plugin:



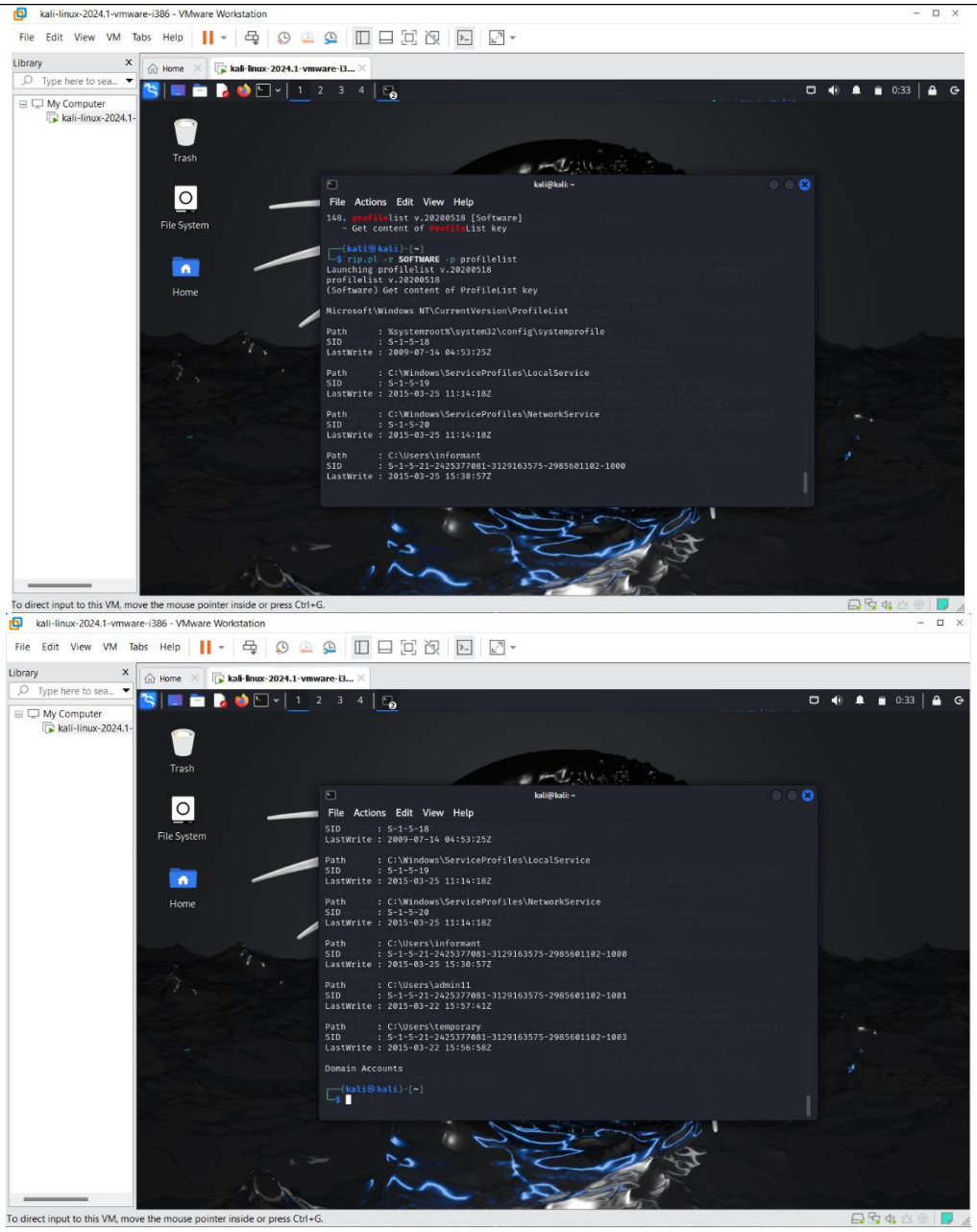
6. How many accounts does the system have?

Search for profiles:

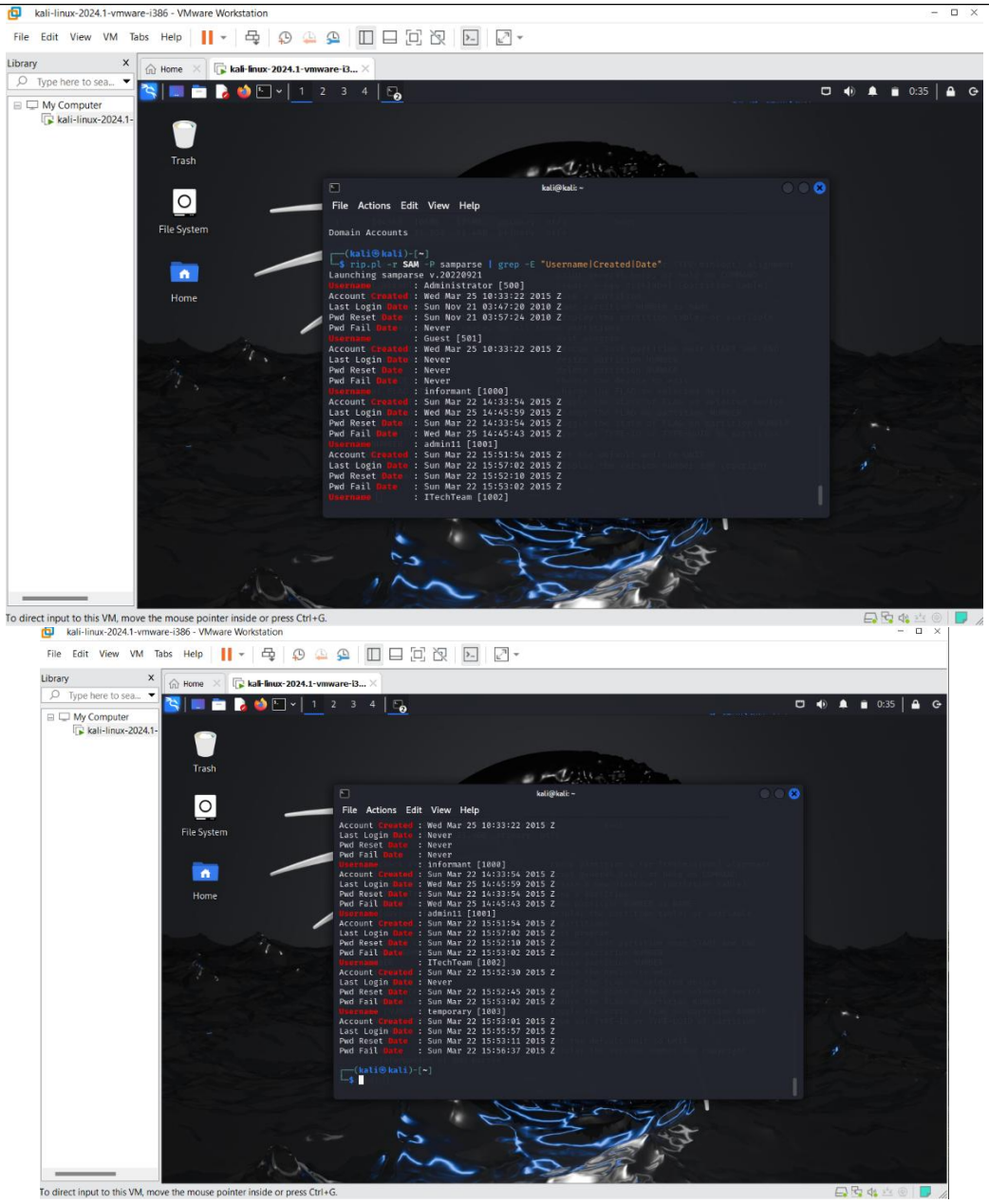


resolve SIDs to user:

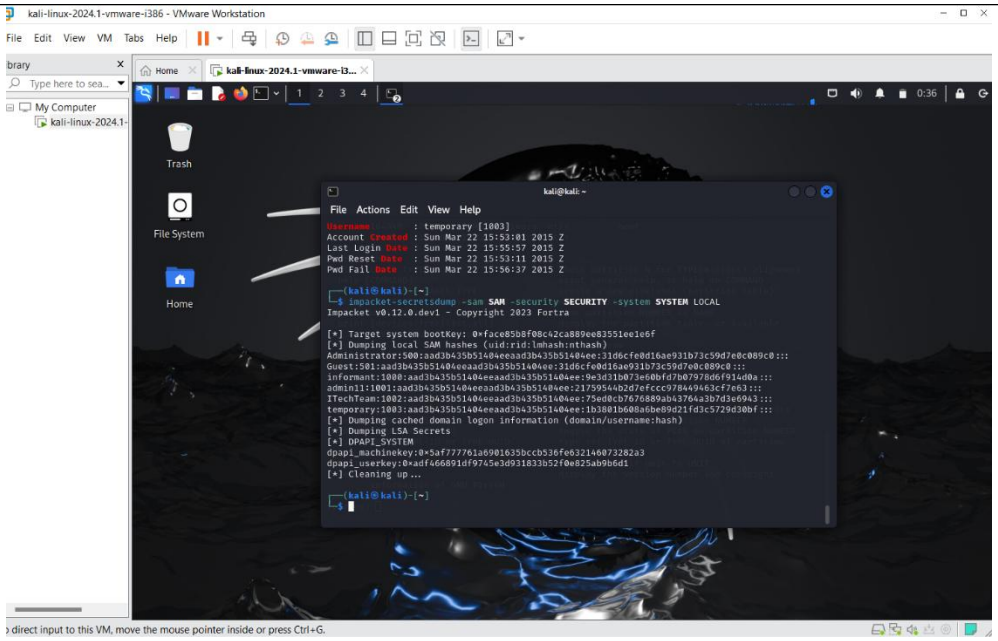
Managing access and permissions in a computer system requires resolving Security Identifiers (SIDs) to user accounts. By monitoring and managing user activity, administrators can make sure that resources are secured and used effectively. Administrators can identify users linked to particular actions or permissions through this method, which is crucial for security, auditing, and troubleshooting. This helps to preserve the integrity and confidentiality of the system.



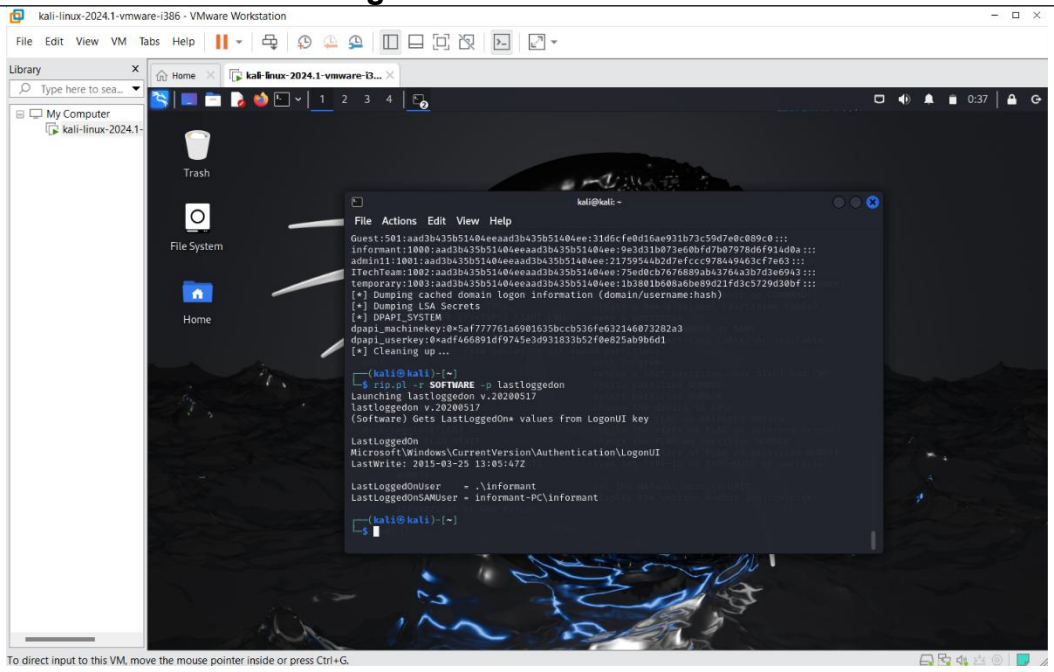
Find and search for Security Accounts Manager (SAM) information:



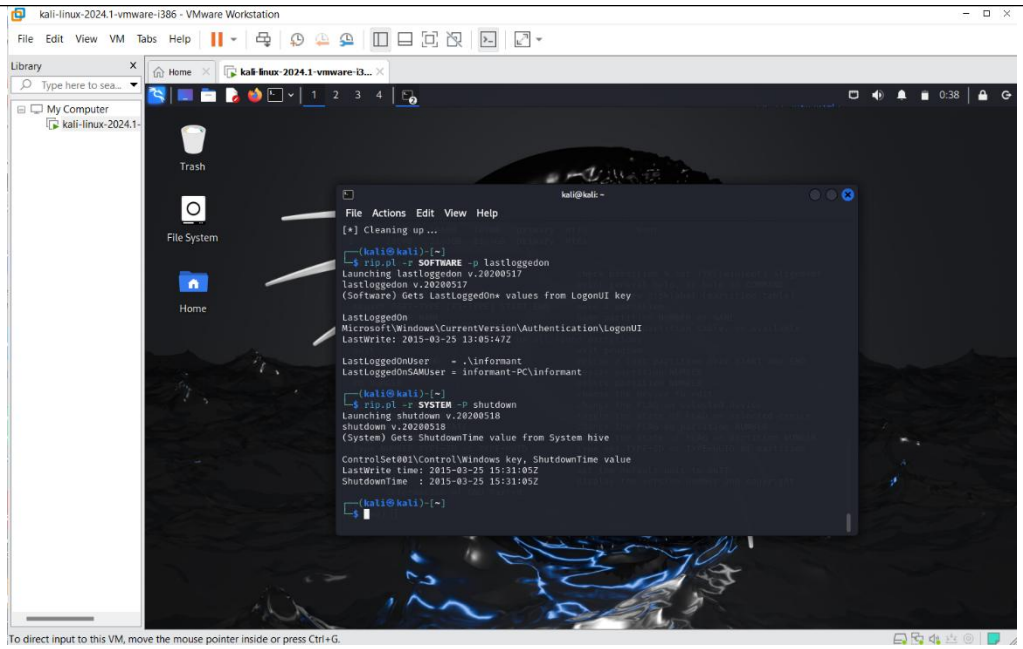
6.1 What are the NTLM of these accounts?



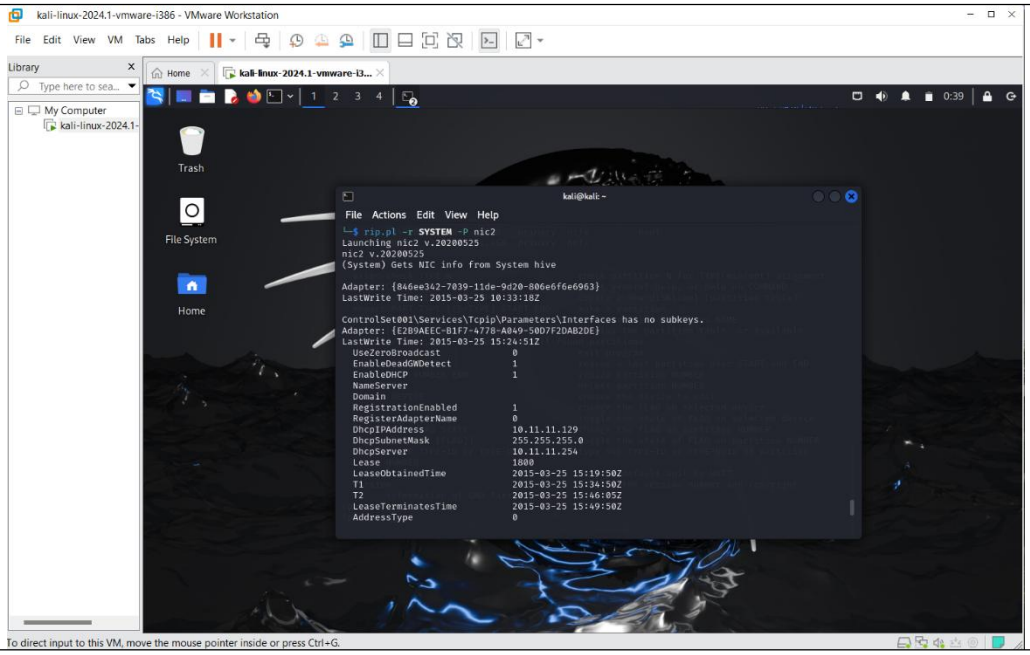
7. Who was the last user to logon into PC?

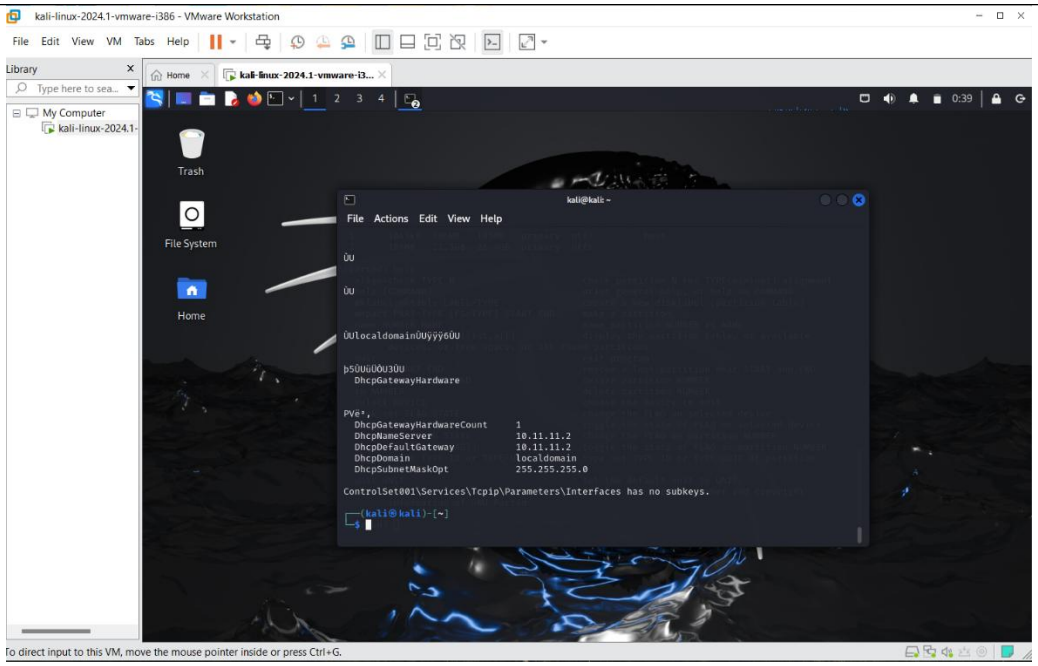


8. When was the last recorded shutdown date/time?

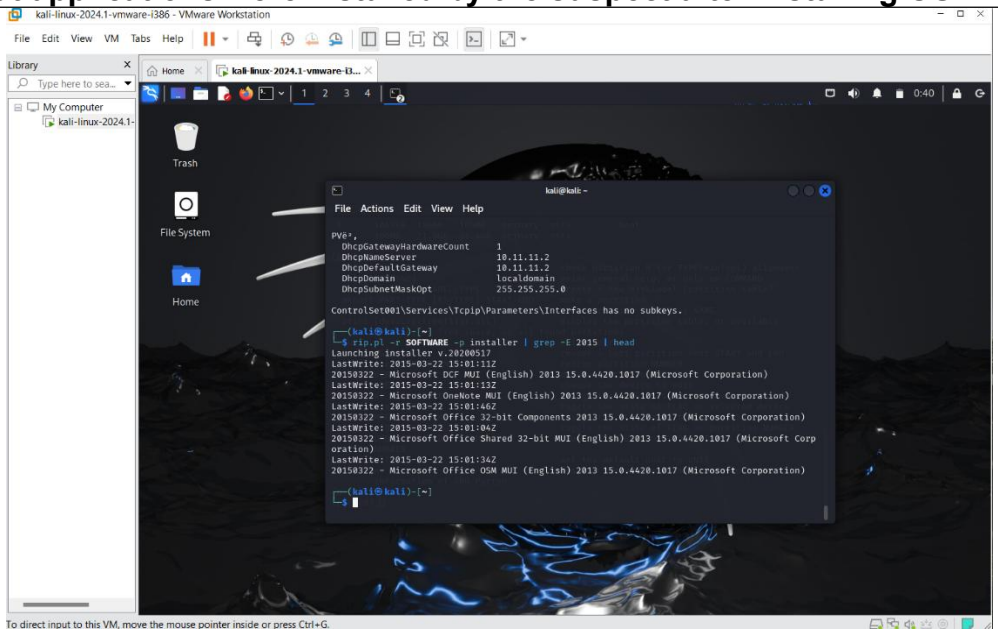


9. Explain the information of network interface(s) with an IP address assigned by DHCP.

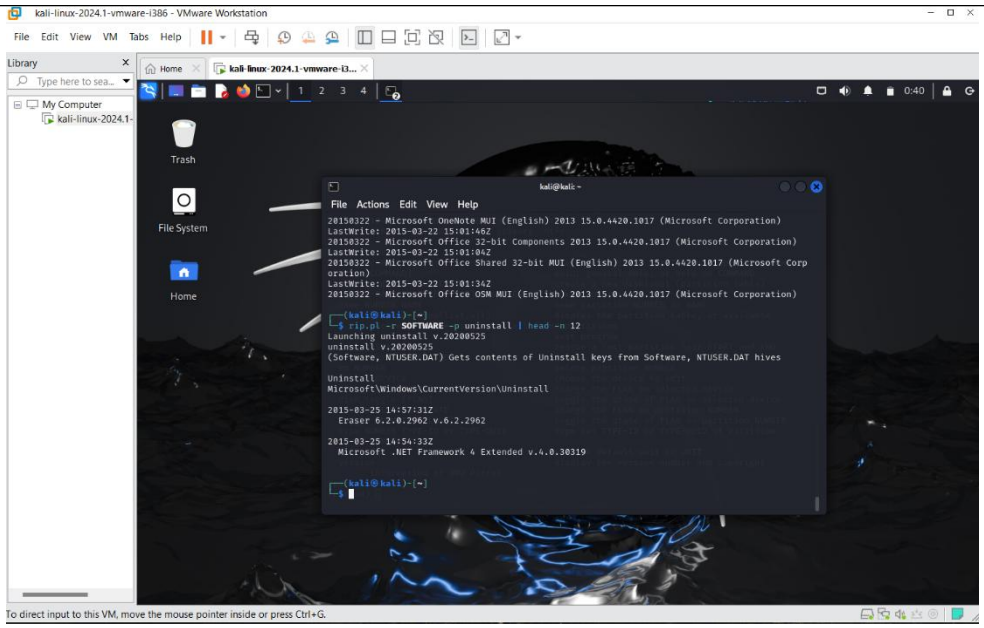




10. What applications were installed by the suspect after installing OS?



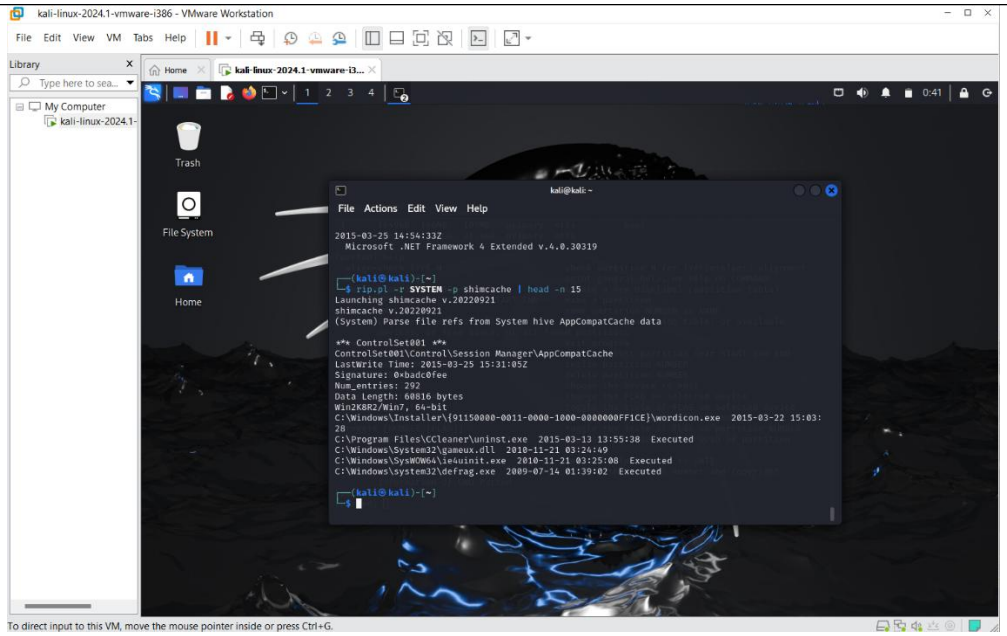
10.1 What applications can be uninstalled by the suspect after installing OS?



11.1 Shimcache

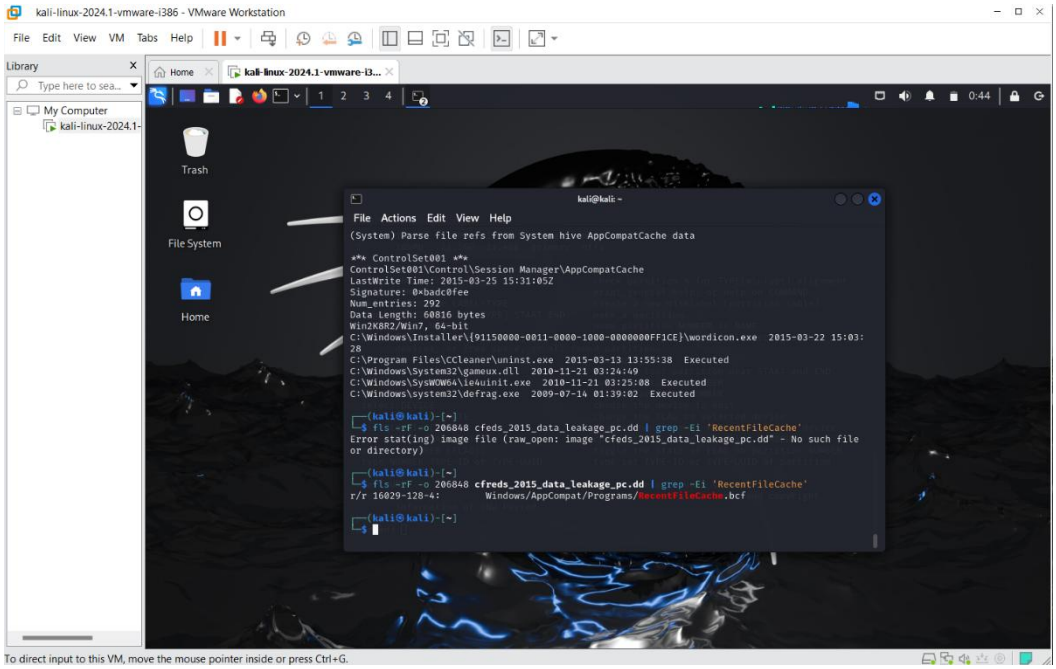
Extract shimcache from registry:

The command "extract shimcache from registry" describes obtaining information about the Application Compatibility Shim Database, which keeps track of running programmes, from the Windows Registry. This is important because it can provide a history of programmes that have been run, which helps in understanding system activity, identifying malicious software, and reconstructing timelines of events during investigations. It is particularly useful in digital forensics and incident response.

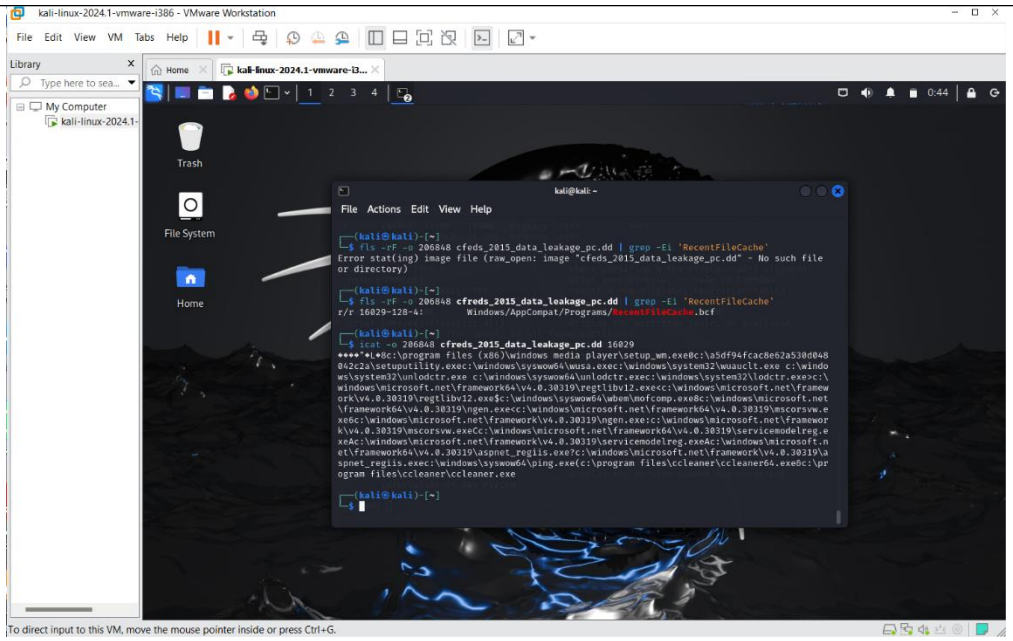


11.2 RecentFileCache.bcf/Amcache

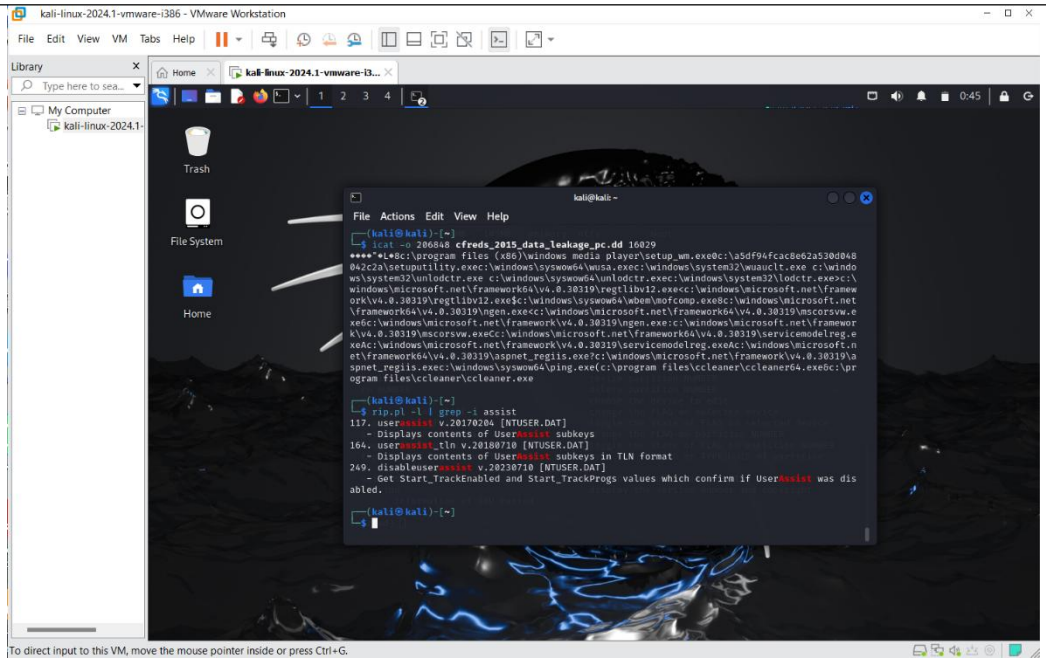
Find the location of RecenfFileCache.bcf:



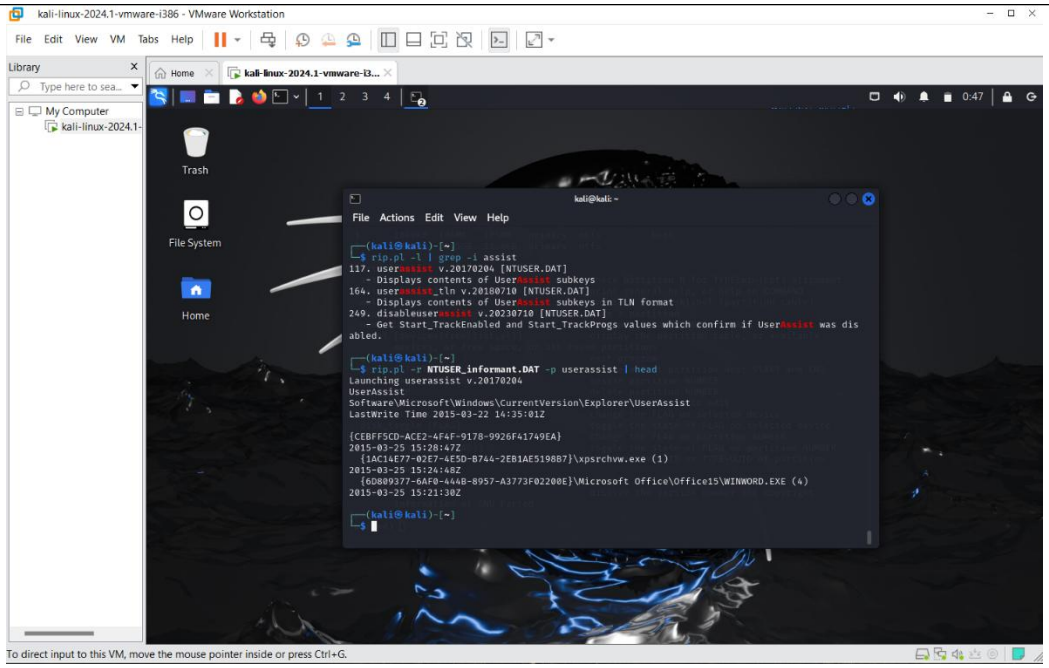
Show RecenfFileCache.bcf:



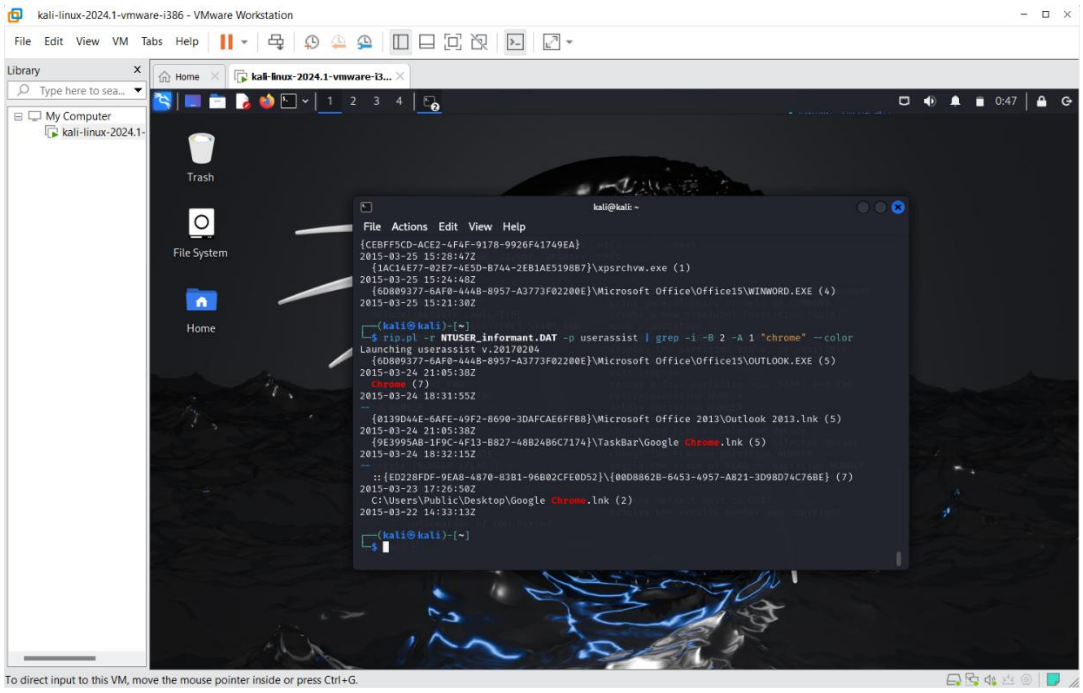
11.3 UserAssist



List executed programs by the user informant:



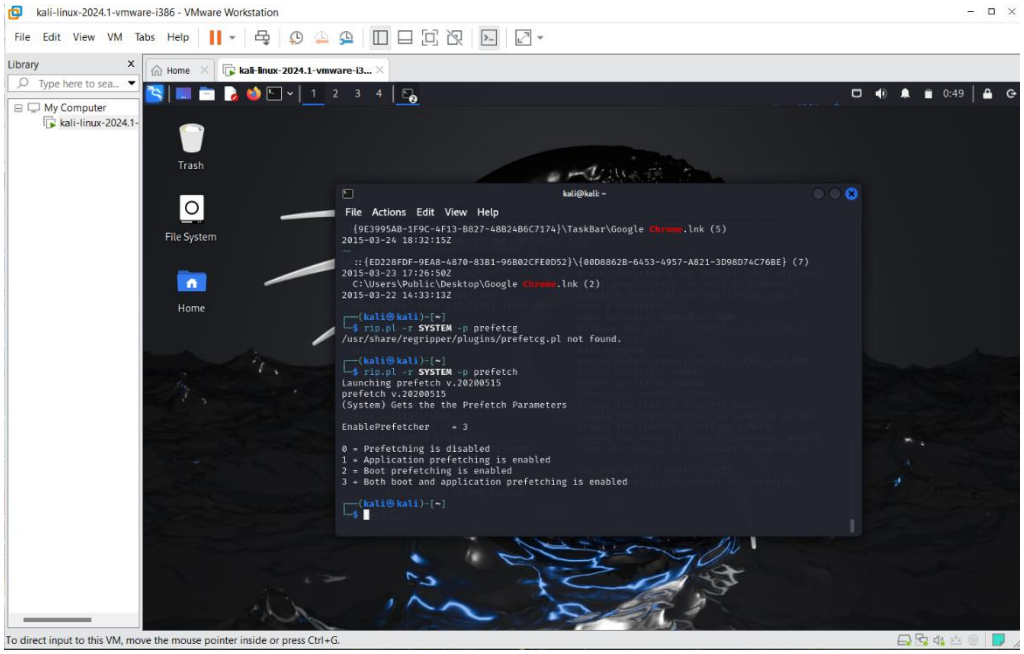
Search if “chrome” has been executed by the user informant. Show lines before and after the matches:



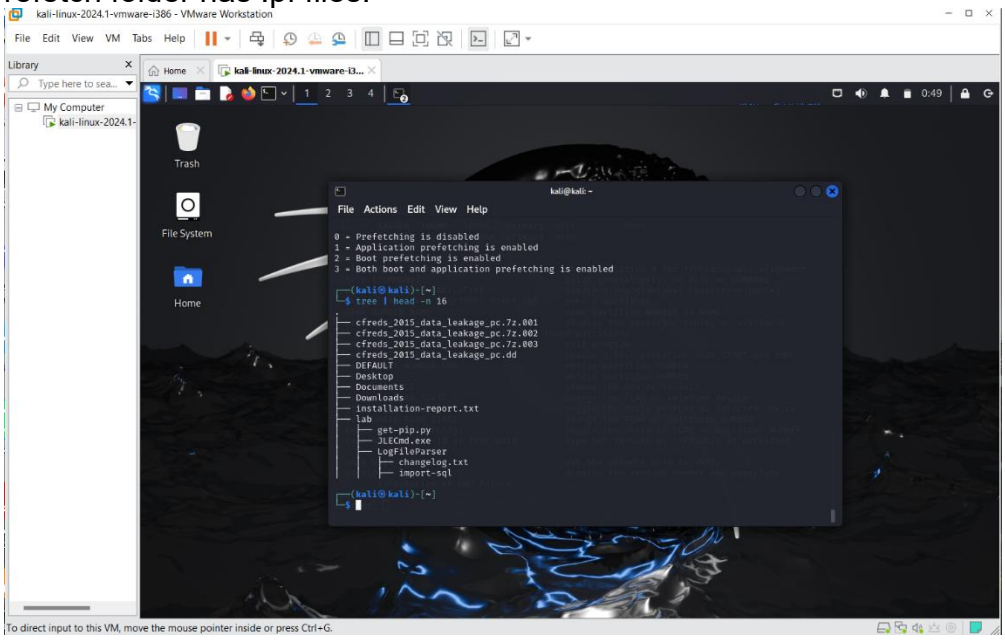
11.4 Prefetch

Exam prefetch setting from registry:
It is likely the case that the "exam prefetch setting from registry" relates to a system configuration pertaining to the administration of exams or tests, perhaps in a professional or educational context. Changing this registry value may have an effect on how exam-related

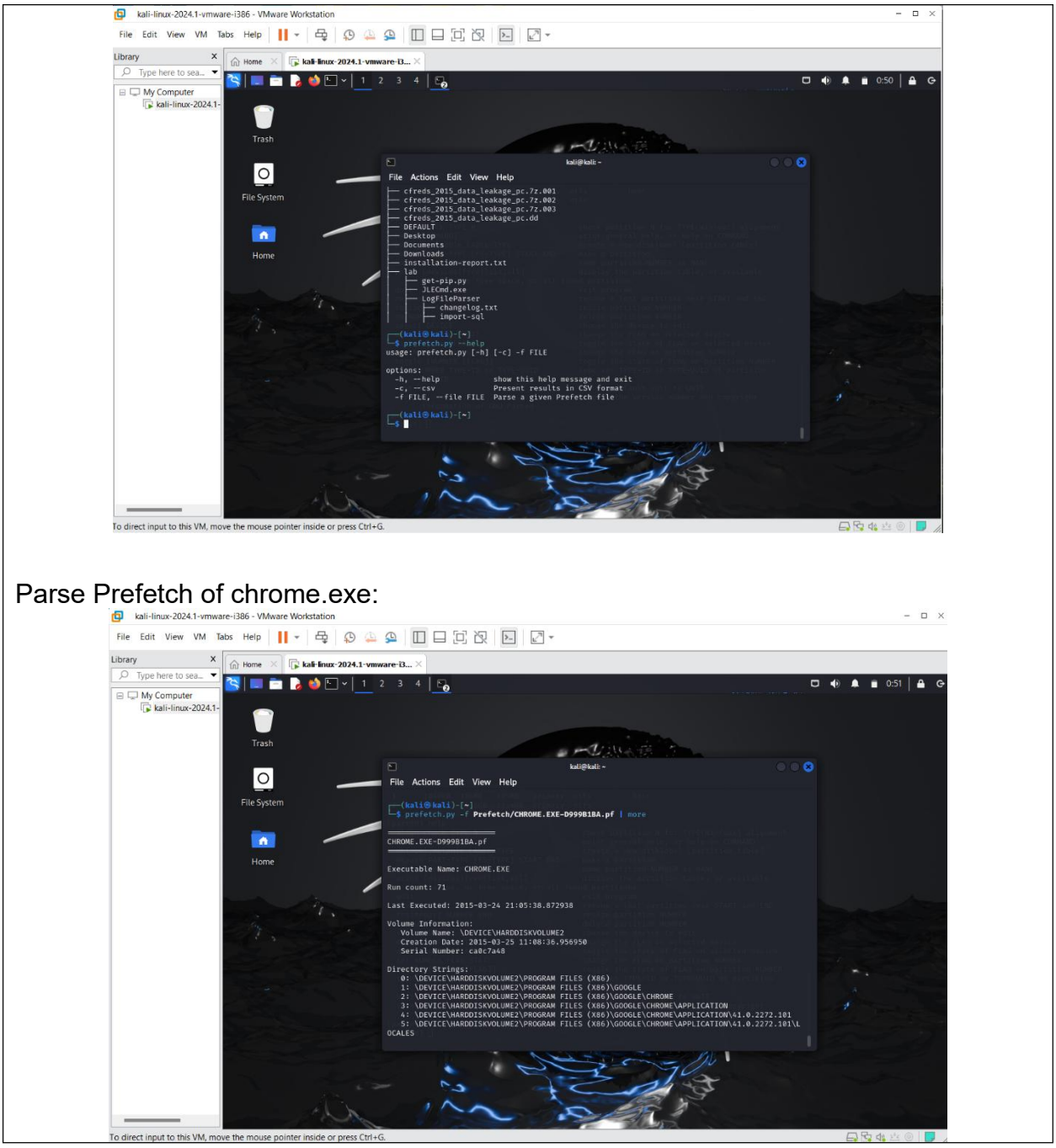
data is managed, which may improve security or performance throughout the test process. Maintaining the integrity and effectiveness of exam delivery systems requires proper configuration, which protects against possible problems like data loss or unauthorised access during crucial assessment times.



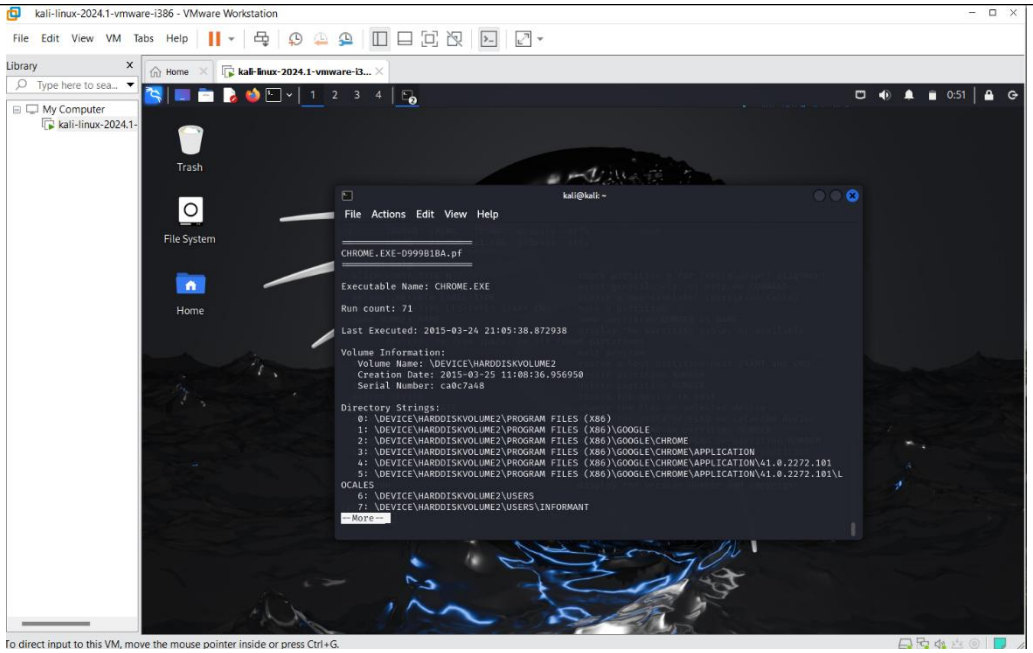
Verify Prefetch folder has .pf files:



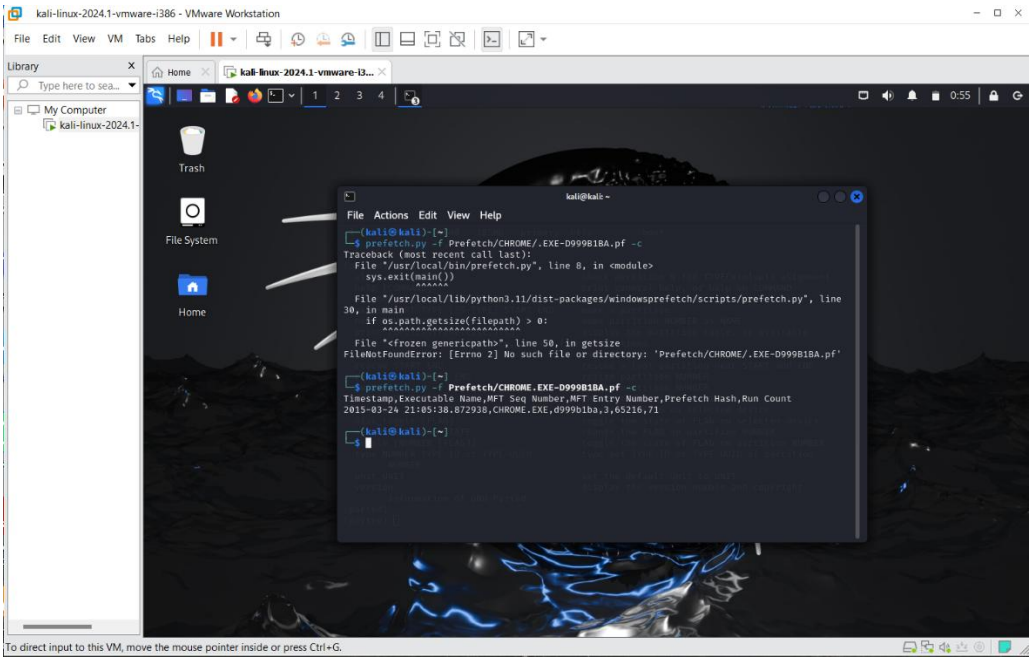
Verify prefetch command:



Parse Prefetch of chrome.exe:

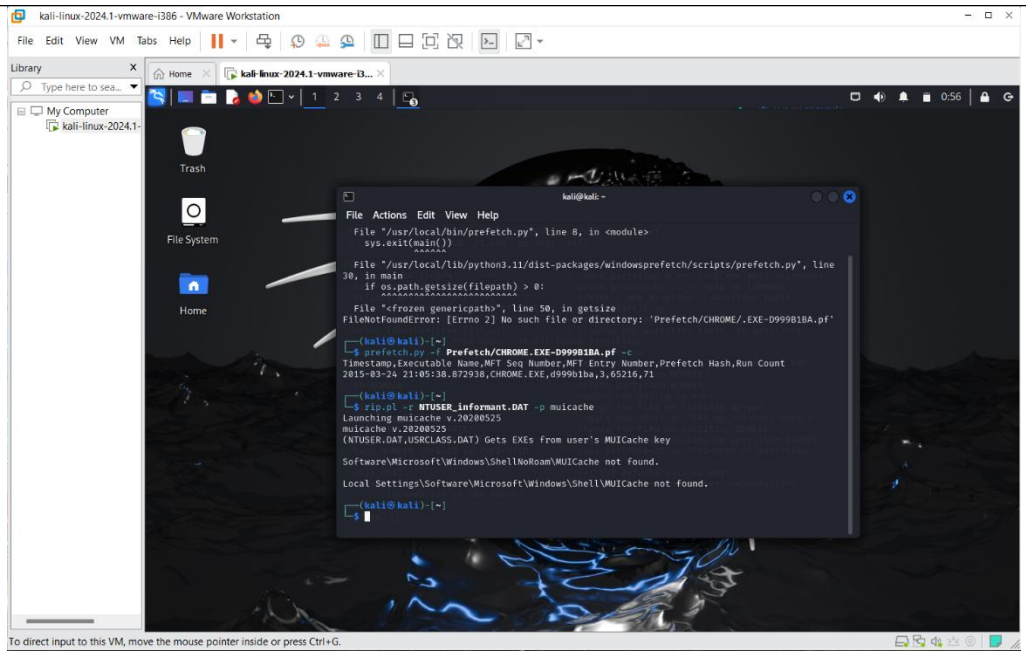


Parse Prefetch of chrome.exe and save the results to .CSV:

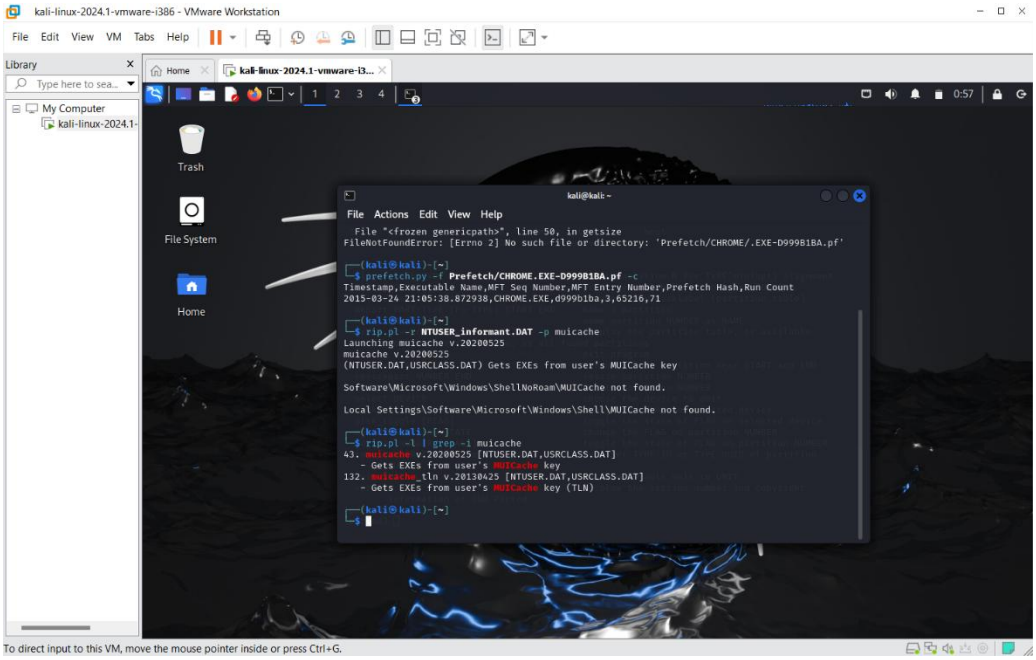


11.5 MuiCache: Multilingual User Interface

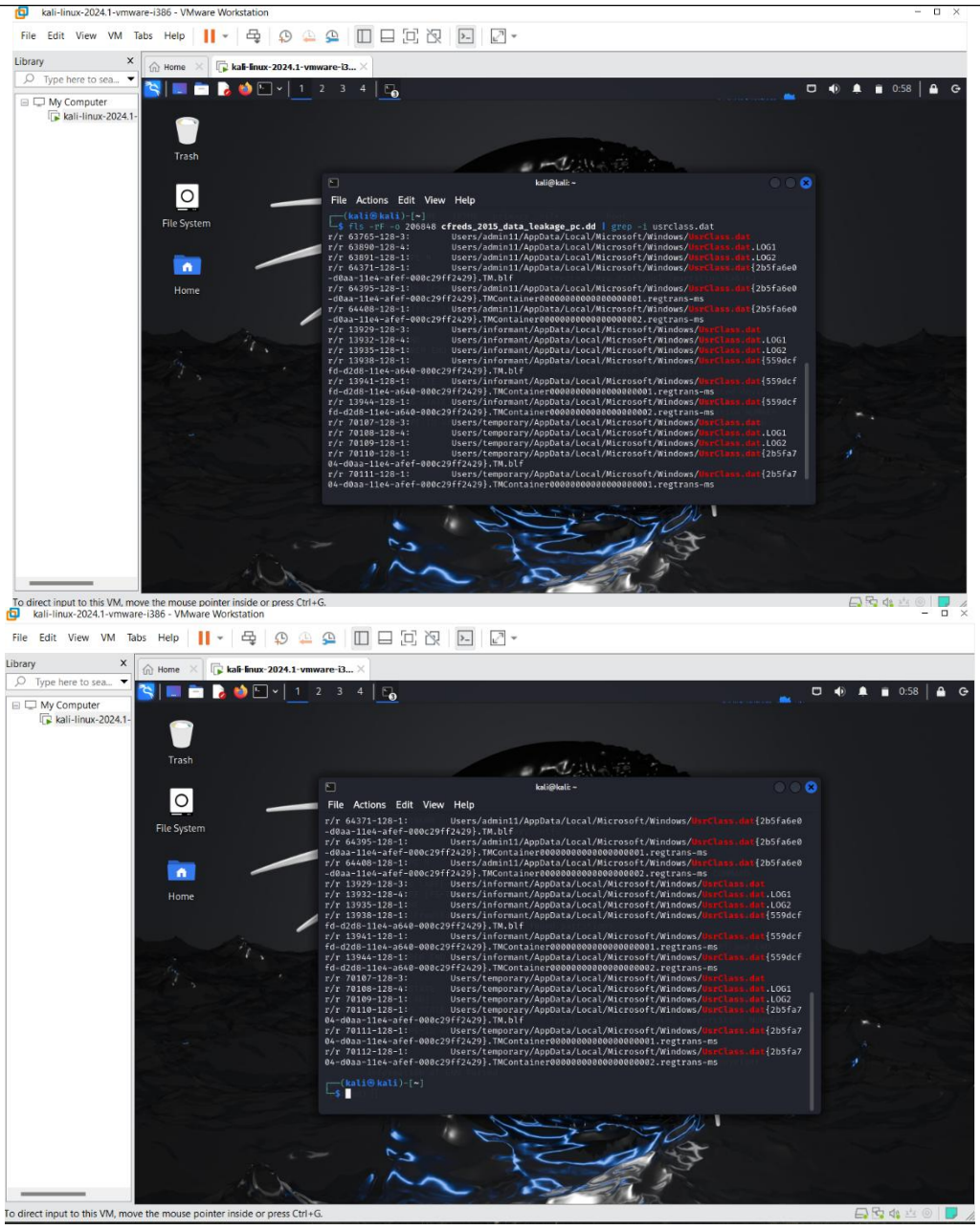
Search for muicache plugin:



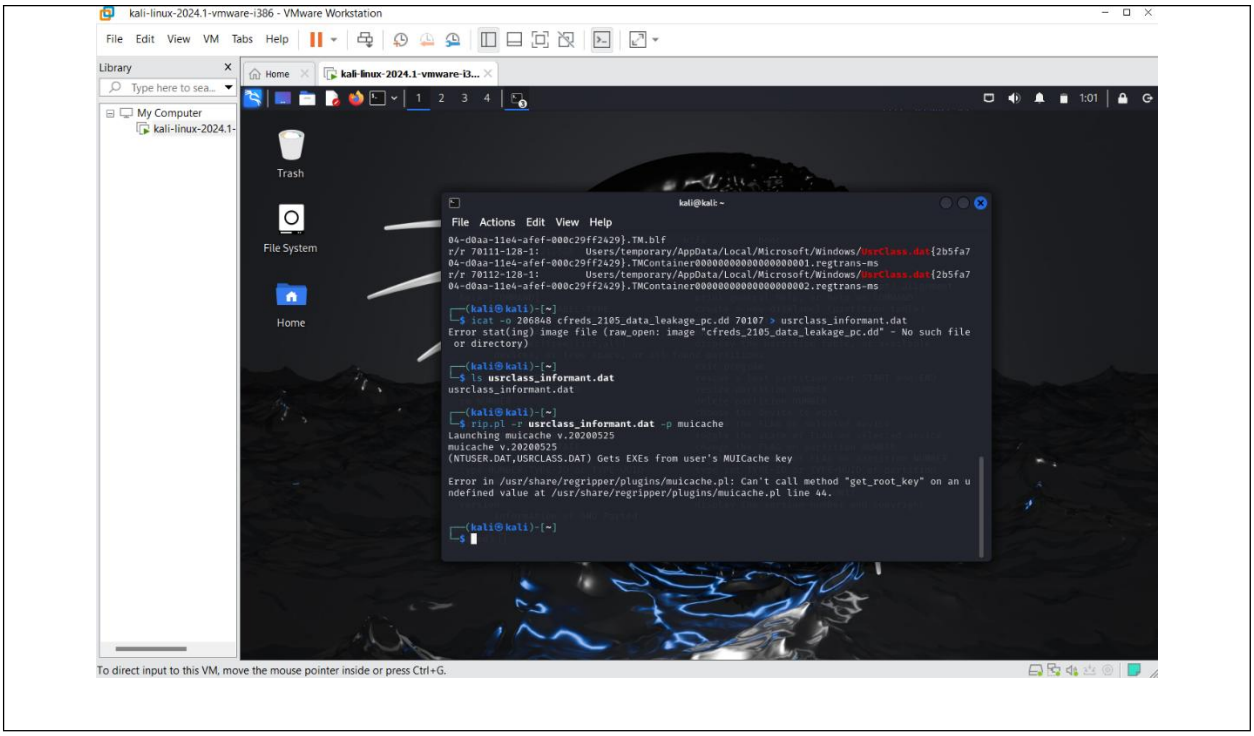
Exam muicache:



Search usrclass.dat:



Extract usrclass.dat & Search muicache from usrclass.dat:


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
1:01
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
04-d0aa-11e4-afef-000c29ff2429}.TM.blf
r/r 70111-128-1: Users/temporary/AppData/Local/Microsoft/Windows/UsrClass.dat{2b5fa7
04-d0aa-11e4-afef-000c29ff2429}.TMContainer00000000000000001.regtrans-ms
r/r 70112-128-1: Users/temporary/AppData/Local/Microsoft/Windows/UsrClass.dat{2b5fa7
04-d0aa-11e4-afef-000c29ff2429}.TMContainer00000000000000002.regtrans-ms
┌──(kali㉿kali)-[~]
└─$ icat -o 206848 cfreds_2105_data_leakage_pc.dd 70107 > usrclass_informant.dat
Error stat(ing) image file (raw_open: image "cfreds_2105_data_leakage_pc.dd" - No such file
or directory)
┌──(kali㉿kali)-[~]
└─$ ls usrclass_informant.dat
usrclass_informant.dat
┌──(kali㉿kali)-[~]
└─$ rip.pl -r usrclass_informant.dat -p muicache
Launching muicache v.20200525
muicache v.20200525
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key
Error in /usr/share/regripper/plugins/muicache.pl: Can't call method "get_root_key" on an u
ndefined value at /usr/share/regripper/plugins/muicache.pl line 44.
┌──(kali㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.