

ITS60904

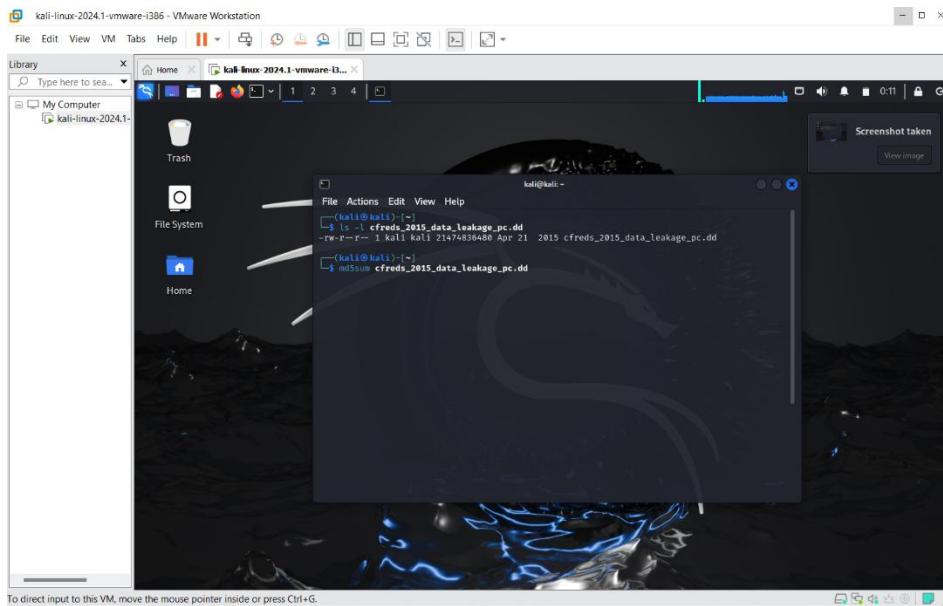
COMPUTER CRIME AND DIGITAL EVIDENCE

PRACTICAL 3 LAB REPORT

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

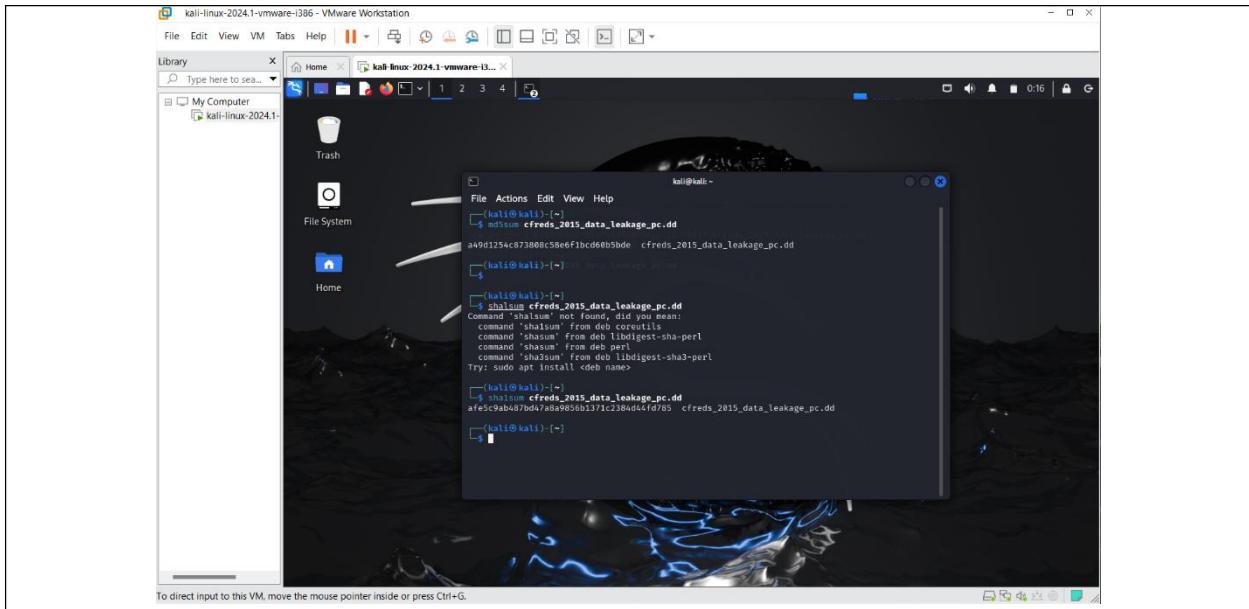
Verify you have the dd image:

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:

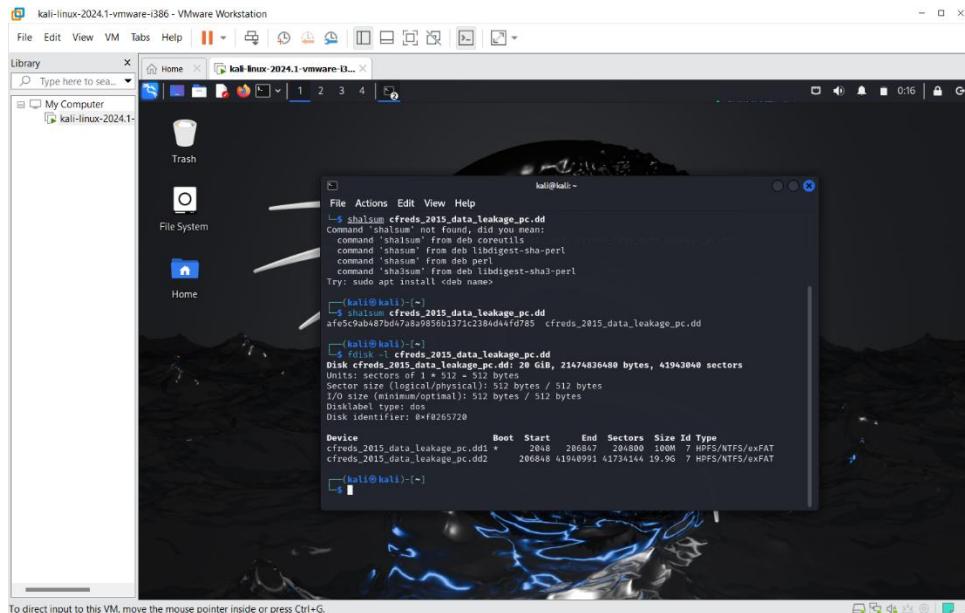
Data integrity and authenticity are guaranteed by calculating the MD5 and SHA1 hashes of a DD image, which is a bit-by-bit replica of a storage device. By acting as distinct digital fingerprints, these hashes confirm that the image hasn't been tampered with or distorted. In domains where preserving the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

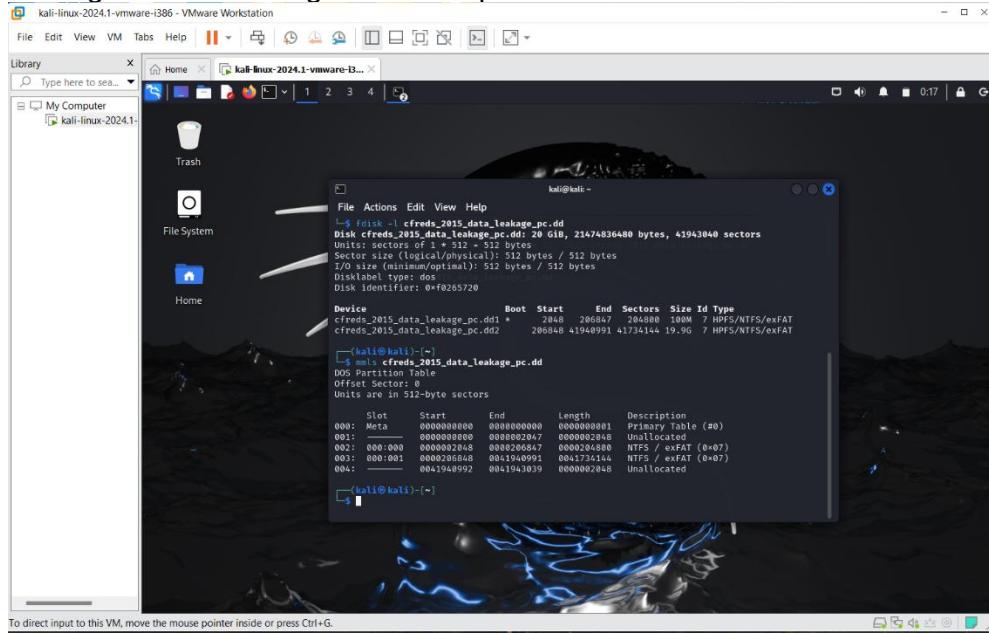
Partitioning an image means breaking it up into separate areas or sections. This procedure is crucial for a number of applications, including computer vision, object recognition, and image analysis, as it reduces the intricacy of the image and facilitates the study and processing of particular regions. 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:

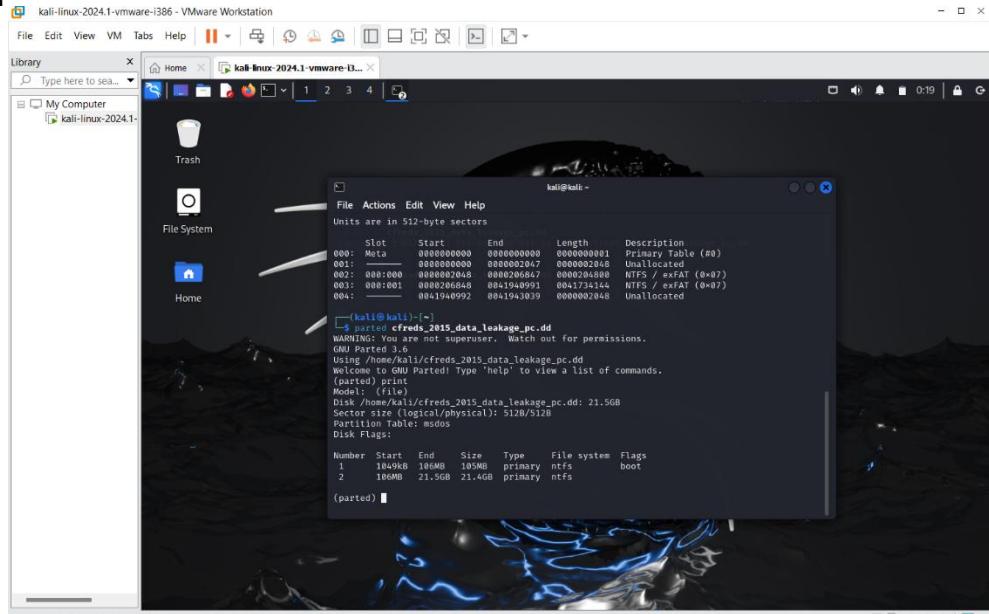
Digital forensics and system management depend heavily on the ability to display partitions

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.



```

kali@kali:~$ parted help
(parted) help
  align-check [TYPE] N           check partition N for TYPE(minopt) alignment
  help [COMMAND]                print general help, or help on COMMAND
  mklabel,mktable,LABEL-TYPE   create a new disklabel (partition table)
  mkpart,--mkpart [FS-TYPE] START END
  name [NUMBER] NAME           name partition NUMBER as NAME
  print [devices|free|list,all]  display the partition table, or available
  devices, or free space, or all found partitions
  quit                        exit parted
  rescue START END             rescue a lost partition near START and END
  resizepart NUMBER END        resize partition NUMBER
  rm NUMBER                     delete partition NUMBER
  select DEVICE                 choose a device to edit
  set FLAG STATE               change the FLAG on selected device
  disk_toggle [FLAG]
  set NUMBER FLAG STATE        change the FLAG on partition NUMBER
  toggle [NUMBER [FLAG]]
  type NUMBER TYPE-ID or TYPE-UUID
  unit UNIT                     set the default unit to UNIT
  version                      display the version number and copyright
(parted) 

```

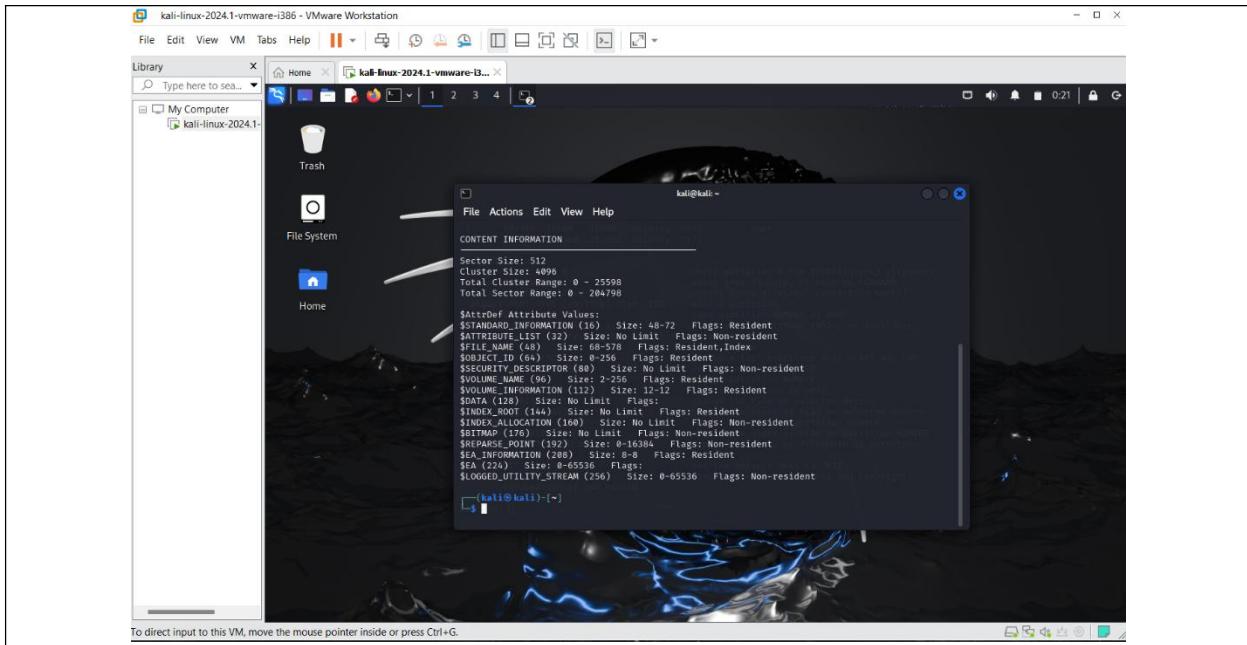
List the first partition details using file system stat (fsstat):

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.

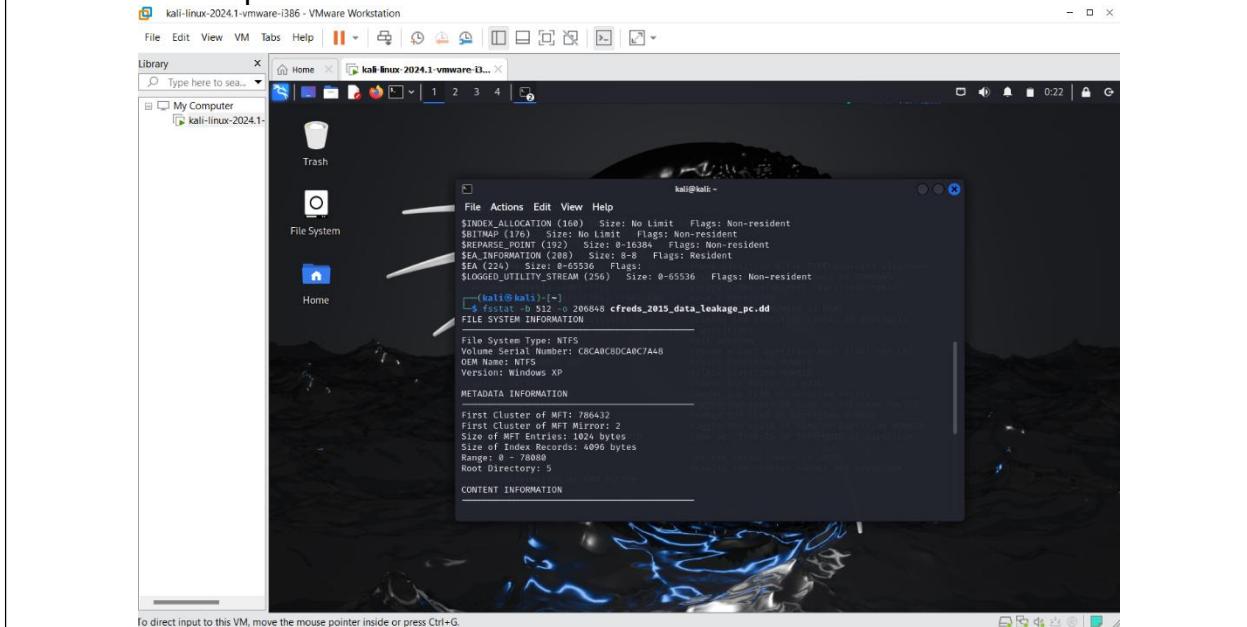
```

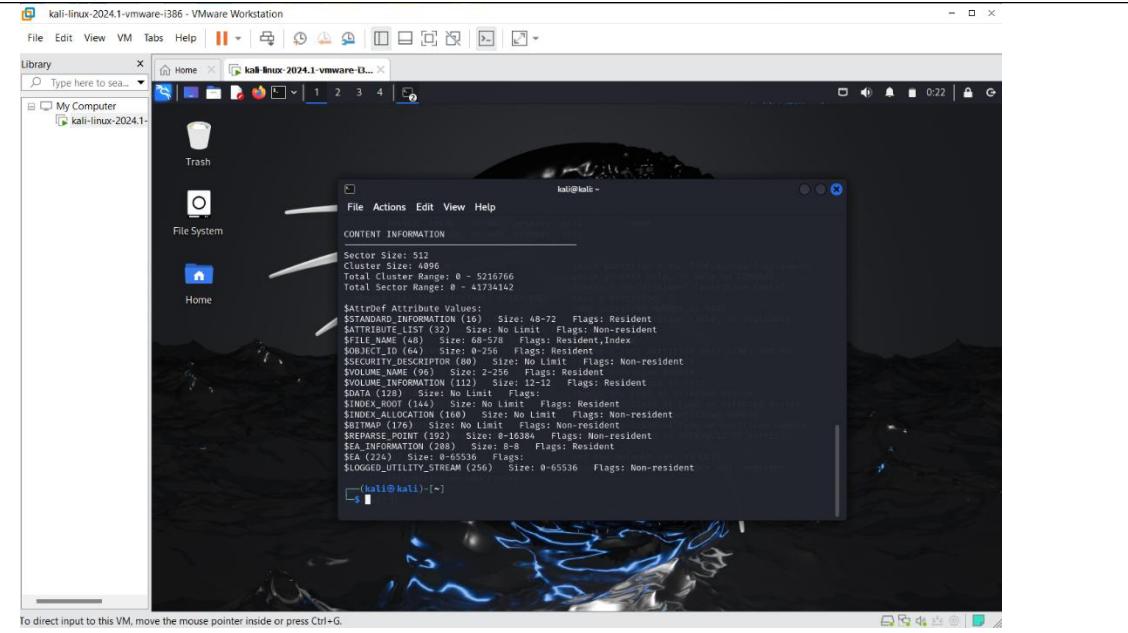
kali@kali:~$ fsstat -b 512 -o 2048 cfreds_2015_data_leakage_pc.dd
FILE SYSTEM INFORMATION
File System Type: NTFS
Volume Serial Number: 4A1B0A15180A0125
OEM Name: NTFS
Volume Name: System Reserved
Cluster Size: 4096 bytes
First Cluster of MFT: 8533
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 25598
Root Directory: 5
METADATA INFORMATION
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 25598
Total Sector Range: 0 - 204798
CONTENT INFORMATION
$AttrDef Attribute Values:

```

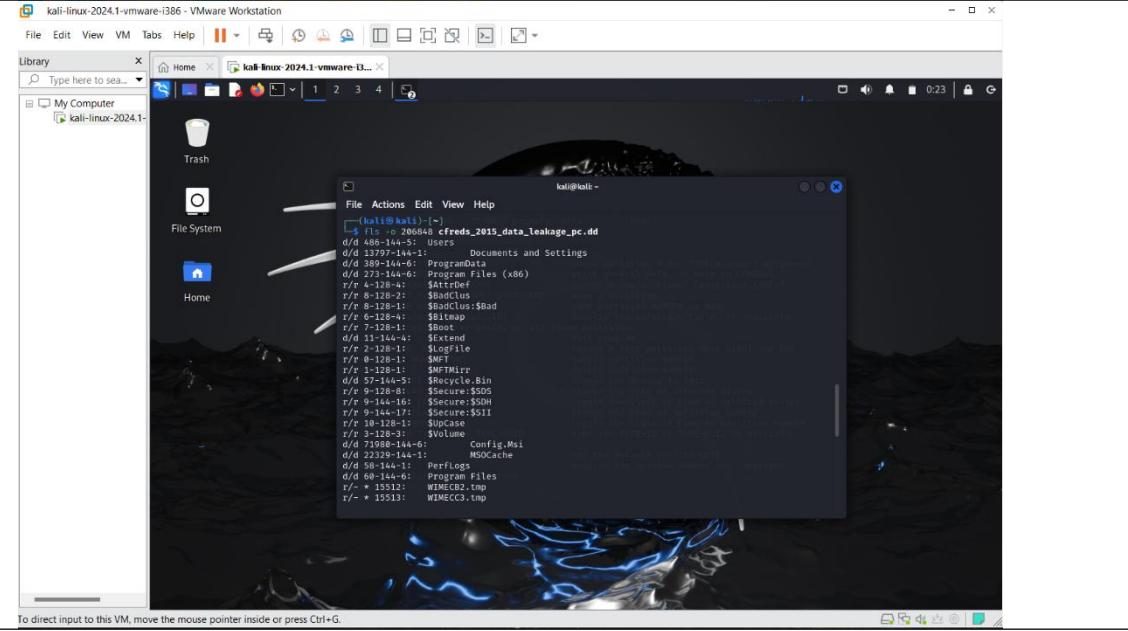


List the second partition details:





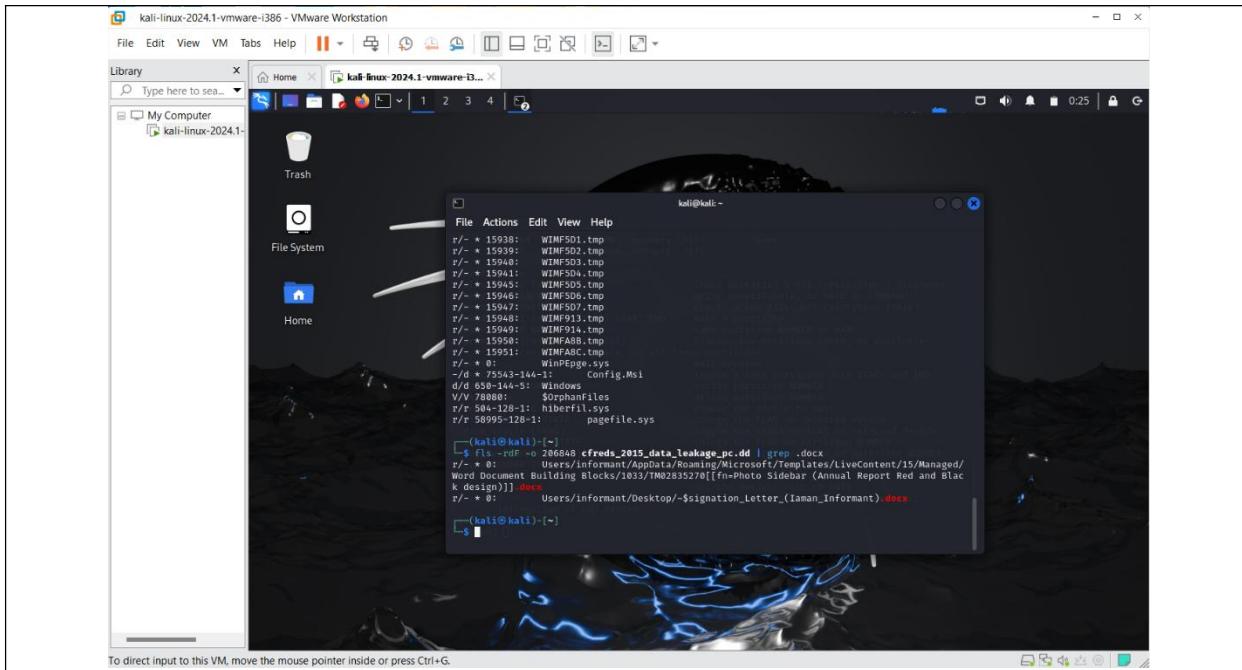
2.2 How to show files (directories) in 2nd partition?



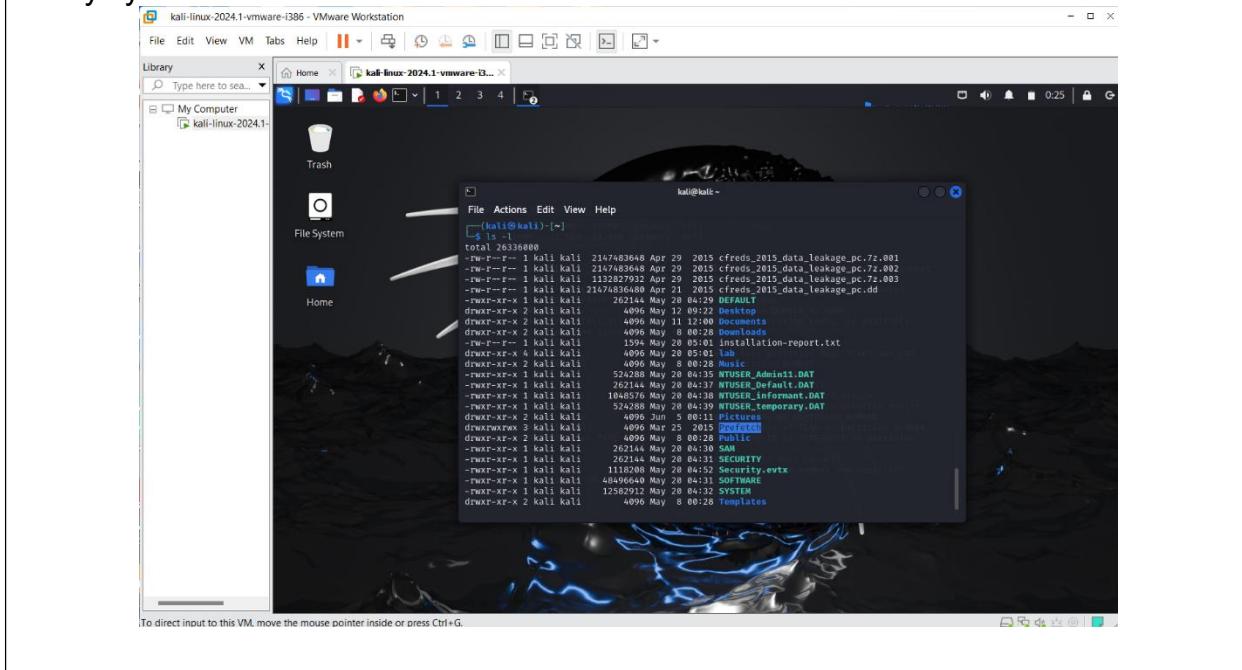
The screenshot shows a terminal window titled "kali@kali ~" with the following command and output:

```
File Actions Edit View Help
r/.* * 0: WIMF32B.tmp
r/.* * 0: WIMF33C.tmp
r/.* * 19903: WIMF34D.tmp
r/.* * 15904: WIMF38E.tmp
r/.* * 15905: WIMF50F.tmp
r/.* * 15936: WIMF5CB.tmp
r/.* * 15937: WIMF5D0.tmp
r/.* * 15938: WIMF5D1.tmp
r/.* * 15939: WIMF5D2.tmp
r/.* * 15940: WIMF5D3.tmp
r/.* * 15941: WIMF5D4.tmp
r/.* * 15945: WIMF5D5.tmp
r/.* * 15946: WIMF5D6.tmp
r/.* * 15947: WIMF5D7.tmp
r/.* * 15948: WIMF5D8.tmp
r/.* * 15949: WIMF5D9.tmp
r/.* * 15950: WIMFA8B.tmp
r/.* * 15951: WIMFABC.tmp
r/.* * 0: WiPePEasy.sys
d/d 6543-144-3: Windows Config.Msi
d/d 650-144-3: Windows
V/V 70808: $orphanfiles
r/r 584-128-1: hiberfil.sys
r/r 58995-128-1: pagefile.sys
```

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



Verify system information:



kali@kali:~

```
-rw-r--r-- 1 kali kali 21474835680 Apr 21 2015 cfreds_2015_data_leakage_pc.dd
drwxr-xr-x 2 kali kali 4996 May 12 09:22 Desktop
drwxr-xr-x 2 kali kali 4996 May 12 12:00 Documents
drwxr-xr-x 2 kali kali 4996 May 12 09:22 Downloads
-rw-r--r-- 1 kali kali 1594 May 20 05:01 installation-report.txt
drwxr-xr-x 4 kali kali 4996 May 20 05:01 lab
drwxr-xr-x 2 kali kali 4996 May 20 05:01 music
-rw-r--r-- 1 kali kali 524288 May 20 04:55 NTUSER_Admin11.DAT
drwxr-xr-x 1 kali kali 262144 May 20 04:57 NTUSER_Default.DAT
-rw-r--r-x 1 kali kali 1048576 May 20 04:58 NTUSER_Informant.DAT
-rw-r--r-x 1 kali kali 524288 May 20 04:59 NTUSER_Temporary.DAT
drwxrwxrwx 3 kali kali 4996 Jun 5 09:11 Pictures
drwxr-xr-x 2 kali kali 4996 May 25 2015 Public
drwxr-xr-x 2 kali kali 4996 May 8 08:28 SECURITY
drwxr-xr-x 1 kali kali 262144 May 20 04:51 SECURITY
-rw-r--r-x 1 kali kali 1118208 May 20 04:52 Security.evtx
drwxr-xr-x 1 kali kali 4849640 May 20 04:52 SOFTWARE
-rw-r--r-x 1 kali kali 12582012 May 20 04:53 SYSTEM
drwxr-xr-x 2 kali kali 4996 May 8 08:28 Templates
-rw-r--r-x 1 kali kali 9556 May 19 08:12 tool-install-zsh.sh
-rw-r--r-- 1 kali kali 9556 May 20 04:57 tool-install-zsh.sh.i
drwxr-xr-x 2 kali kali 4996 May 8 08:28 Videos
```

Verify Users' information:

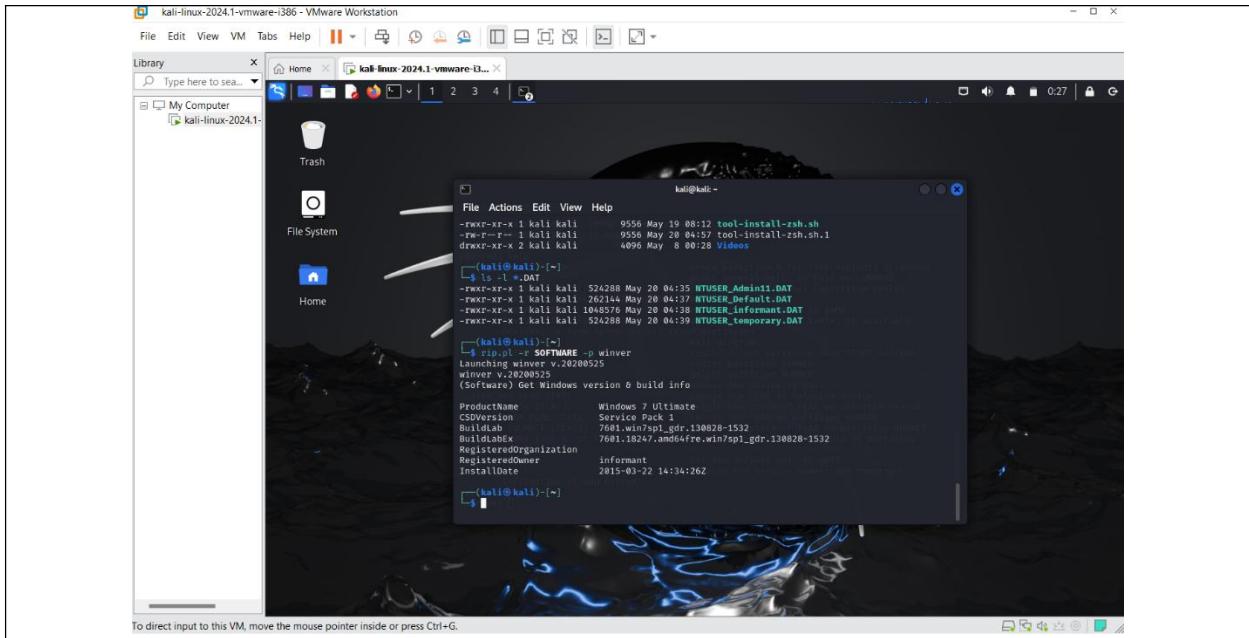
kali@kali:~

```
drwxr-xr-x 2 kali kali 4996 May 8 00:28 Music
-rw-r--r-x 1 kali kali 524288 May 20 04:35 NTUSER_Admin11.DAT
-rw-r--r-x 1 kali kali 262144 May 20 04:35 NTUSER_Default.DAT
-rw-r--r-x 1 kali kali 1048576 May 20 04:38 NTUSER_Informant.DAT
-rw-r--r-x 1 kali kali 524288 May 20 04:39 NTUSER_Temporary.DAT
drwxr-xr-x 2 kali kali 4996 Jun 5 00:11 Pictures
drwxrwxrwx 3 kali kali 4996 May 8 00:28 Public
drwxr-xr-x 1 kali kali 262144 May 20 04:30 SAM
-rw-r--r-x 1 kali kali 262144 May 20 04:31 SECURITY
-rw-r--r-x 1 kali kali 1118208 May 20 04:52 Security.evtx
drwxr-xr-x 1 kali kali 4849640 May 20 04:52 SOFTWARE
-rw-r--r-x 1 kali kali 12582012 May 20 04:53 SYSTEM
drwxr-xr-x 2 kali kali 4996 May 8 00:28 Templates
-rw-r--r-x 1 kali kali 9556 May 19 08:12 tool-install-zsh.sh
-rw-r--r-- 1 kali kali 9556 May 20 04:57 tool-install-zsh.sh.i
drwxr-xr-x 2 kali kali 4996 May 8 00:28 Videos
```

ls -l *.DAT

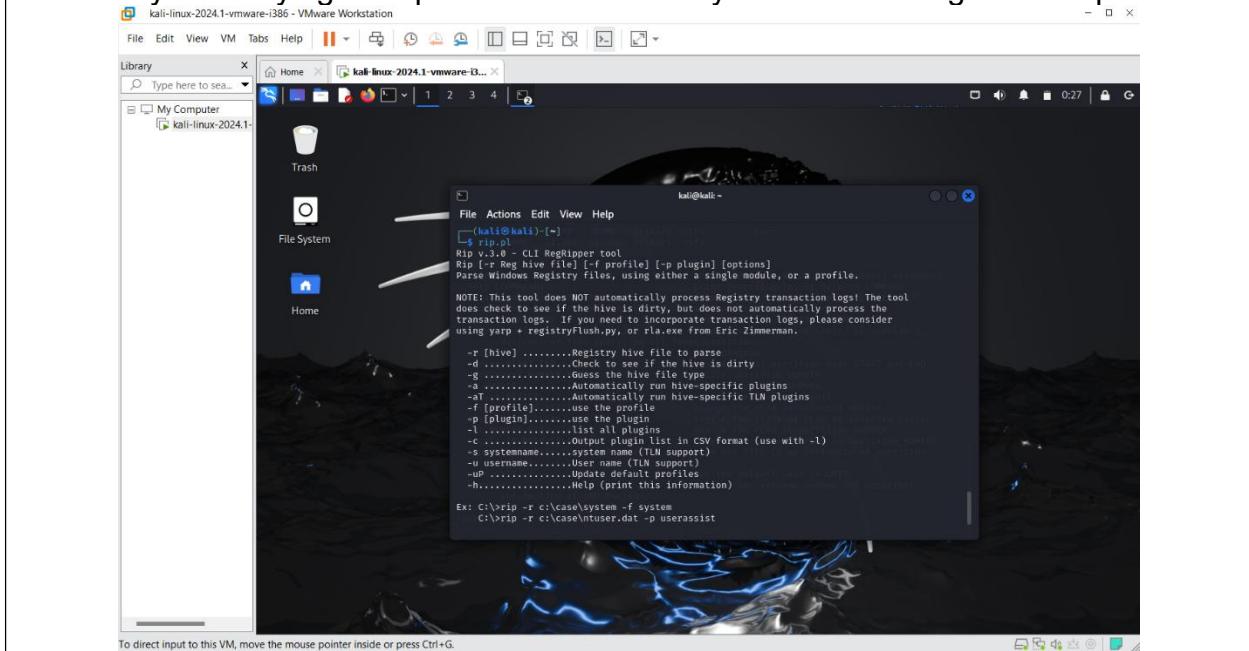
```
-rw-r--r-x 1 kali kali 524288 May 20 04:25 NTUSER_Admin11.DAT
-rw-r--r-x 1 kali kali 262144 May 20 04:37 NTUSER_Default.DAT
-rw-r--r-x 1 kali kali 1048576 May 20 04:38 NTUSER_Informant.DAT
-rw-r--r-x 1 kali kali 524288 May 20 04:39 NTUSER_Temporary.DAT
```

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.



```

kali@kali: ~
File Actions Edit View Help
using yarp + registryFlush.py, or rla.exe from Eric Zimmerman.
-p [hive] ..... Registry hive file to parse
-g ..... Check to see if the hive is dirty
-g ..... Guess the hive file type
-a ..... Automatically run hive-specific plugins
-T ..... Automatically run hive-specific TLN plugins
-f [profile] ..... Use the profile
-l [plugin] ..... List all the plugin
-l ..... List all the plugin
-c ..... Output plugin list in CSV format (use with -l)
-s systemname ..... System name (TLM support)
-u userassist ..... Userassist name (TLM support)
-d ..... Update default profiles
-h ..... Help (print this information)

Ex: C:\>yarp -r c:\case\sysmet -f system
C:\>yarp -r c:\case\ntuser.dat -p userassist
C:\>yarp -r c:\case\ntuser.dat -a
C:\>yarp -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
copyright 2020 Quantum Analytics Research, LLC

```

List all 243 plugins of SOFTWARE:

```

kali@kali: ~
File Actions Edit View Help
Ex: C:\>rip -r c:\case\sysmet -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -r c:\case\ntuser.dat -a
C:\>rip -l -c

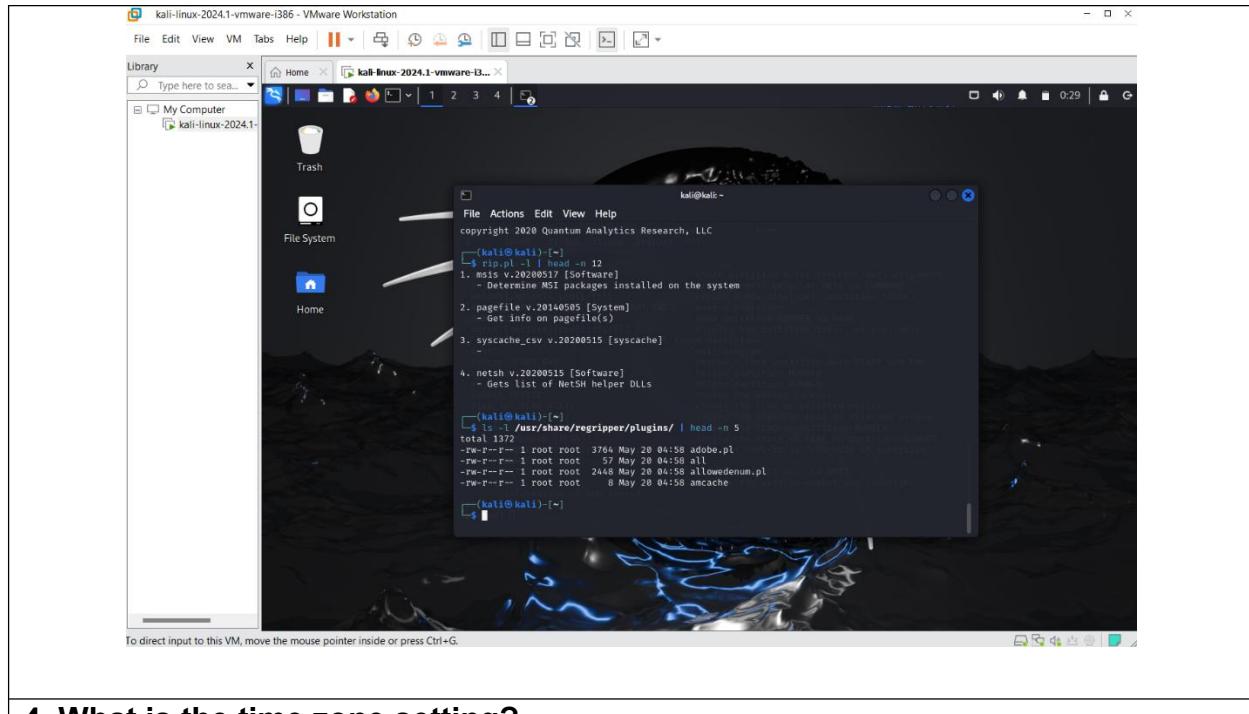
All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
copyright 2020 Quantum Analytics Research, LLC

```

1.	msasn1 v.20200517 [Software]	- Determine MSI packages installed on the system
2.	pagefile v.20140505 [System]	- Get info on pagefile(s)
3.	syscache.csv v.20200515 [syscache]	
4.	netsh v.20200515 [Software]	- Gets list of NetSH helper DLLs

Show the location of all plugins:

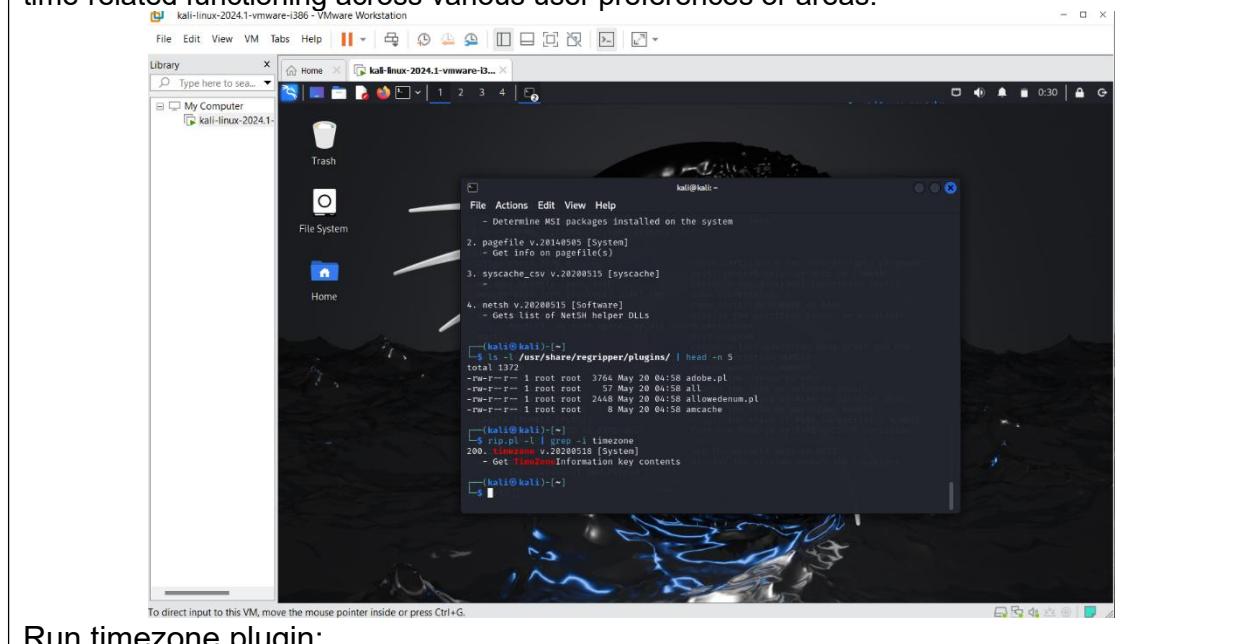
For developers or system administrators in charge of a software environment, "Show the location of all plugins" is an essential command, particularly when working with intricate systems or programs that have a large number of plugins. It is easier to debug, update, and ensure compatibility and security 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:

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open, displaying the following command and its output:

```
-rw-r--r-- 1 root root 57 May 20 04:58 all  
-rw-r--r-- 1 root root 2448 May 20 04:58 allowedenum.pl  
-rw-r--r-- 1 root root 8 May 20 04:58 amcache  
[kali㉿kali:~] $ rip.pl -l | grep -i timezone  
200. timezone v.20200518 [System]  
- Get TimezoneInformation key contents  
[kali㉿kali:~] $ rip.pl -r SYSTEM -p timezone  
Launching timezone v.20200518  
timezone v.20200518  
(System) Get TimeZoneInformation key contents  
TimezoneInformation Key  
ControlSet001\Control\TimeZoneInformation  
LastWrite Time 2015-03-25 10:34:25Z  
DaylightName → @tzres.dll,_111  
StandardName → @tzres.dll,_112  
Bias → 300 (5 hours)  
ActiveTimeBias → 240 (4 hours)  
TimeZoneKeyName → Eastern Standard Time@0 gH+gE5p-0++@ 0++魅盤驅盤快日 GA磁盤A快日  
[kali㉿kali:~]
```

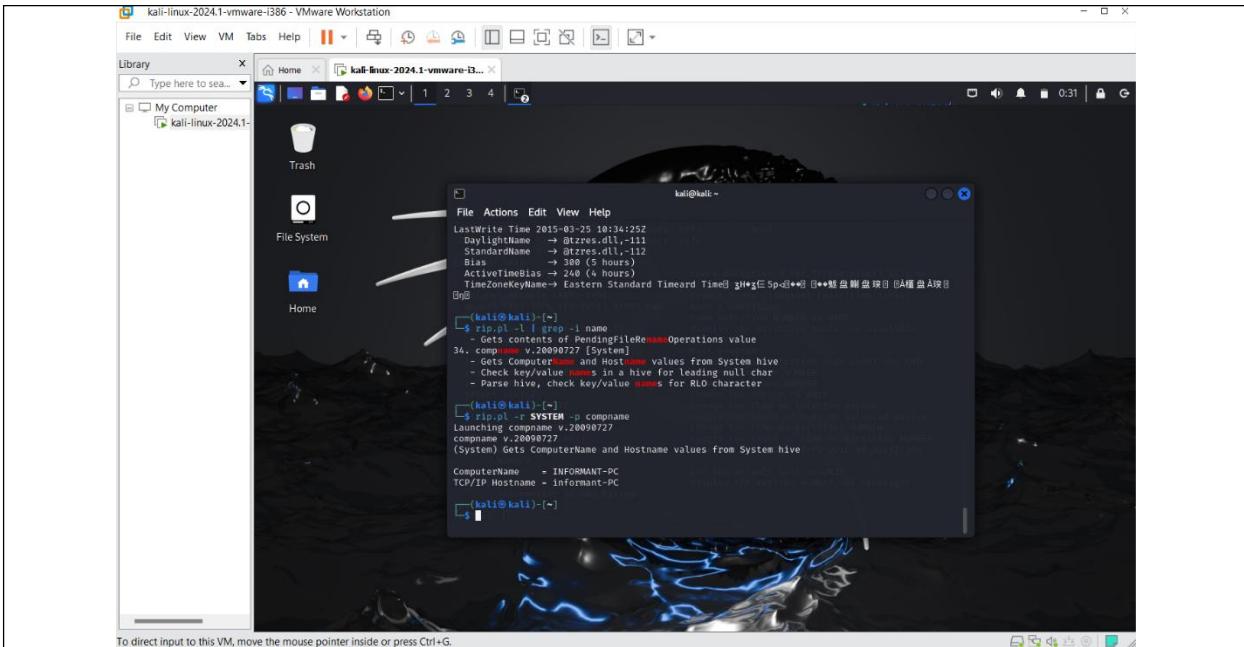
5. What is the computer name?

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

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open, displaying the following command and its output:

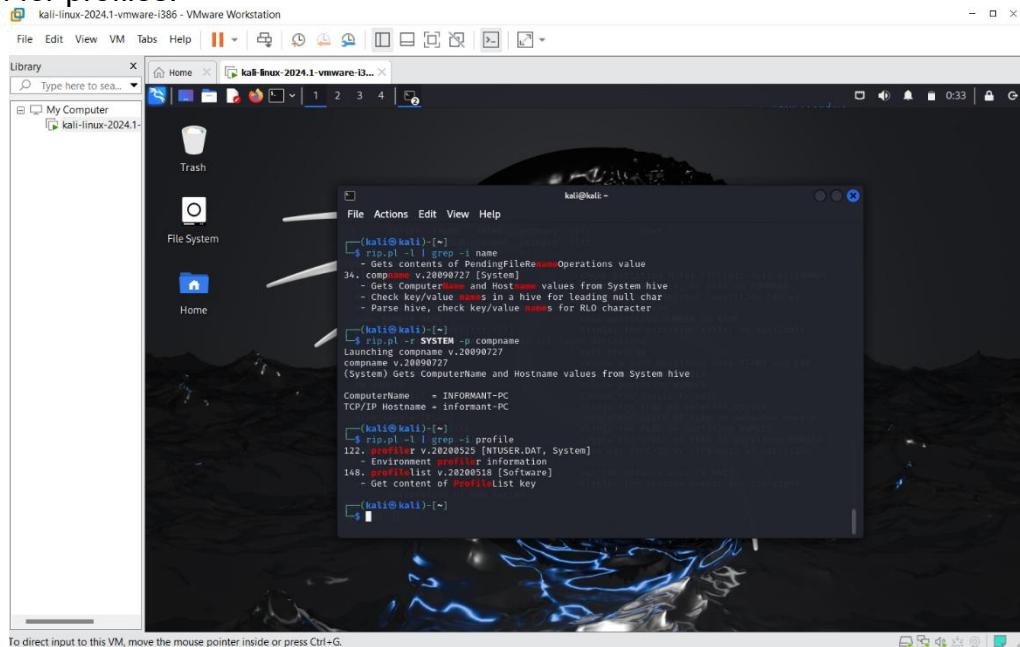
```
[kali㉿kali:~] $ rip.pl -r SYSTEM -p timezone  
Launching timezone v.20200518  
timezone v.20200518  
(System) Get TimeZoneInformation key contents  
TimezoneInformation Key  
ControlSet001\Control\TimeZoneInformation  
LastWrite Time 2015-03-25 10:34:25Z  
DaylightName → @tzres.dll,_111  
StandardName → @tzres.dll,_112  
Bias → 300 (5 hours)  
ActiveTimeBias → 240 (4 hours)  
TimeZoneKeyName → Eastern Standard Time@0 gH+gE5p-0++@ 0++魅盤驅盤快日 GA磁盤A快日  
[kali㉿kali:~] $ rip.pl -l | grep -i name  
- Get contents of PendingFileRenameOperations value  
34. comp v.20090727 [System]  
- Gets ComputerName and HostName values from System hive  
- Check key/value names in a hive for leading multi char  
- Parse hive, check key/value names for RLO character  
[kali㉿kali:~]
```

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.

The image shows two windows of a Kali Linux virtual machine in VMware Workstation. Both windows have the title "kali-linux-2024.1-vmware-13..." and are displaying terminal sessions.

Terminal Session 1 (Top Window):

```

File Actions Edit View Help
148. profilelist v.20200518 [Software]
  - Get content of ProfileList key
[kali㉿kali] ~
$ ripgrep -r SOFTWARE -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows\NT\CurrentVersion\ProfileList
Path : %systemroot%\system32\config\systemprofile
SID : S-1-5-18
LastWrite : 2009-07-16 04:53:252

Path : C:\Windows\ServiceProfiles\LocalService
SID : S-1-5-19
LastWrite : 2015-03-25 11:14:182

Path : C:\Windows\ServiceProfiles\NetworkService
SID : S-1-5-20
LastWrite : 2015-03-25 11:14:182

Path : C:\Users\informant
SID : S-1-5-21-2425377881-3129163575-2985601102-1000
LastWrite : 2015-03-25 15:30:572
  
```

Terminal Session 2 (Bottom Window):

```

File Actions Edit View Help
SID : S-1-5-18
LastWrite : 2009-07-16 04:53:252

Path : C:\Windows\ServiceProfiles\LocalService
SID : S-1-5-19
LastWrite : 2015-03-25 11:14:182

Path : C:\Windows\ServiceProfiles\NetworkService
SID : S-1-5-20
LastWrite : 2015-03-25 11:14:182

Path : C:\Users\informant
SID : S-1-5-21-2425377881-3129163575-2985601102-1000
LastWrite : 2015-03-25 15:30:572

Path : C:\Users\admin11
SID : S-1-5-21-2425377881-3129163575-2985601102-1001
LastWrite : 2015-03-22 15:57:412

Path : C:\Users\temporary
SID : S-1-5-21-2425377881-3129163575-2985601102-1003
Lastwrite : 2015-03-22 15:58:582

Domain Accounts
[kali㉿kali] ~
$ 
  
```

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

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

```
kali@kali:~$ sam -r SAM | grep -E "Username|Created|Date"
Launching samparse v.20200211
=====
Username : Administrator [500]
Account_created : Wed Mar 25 10:33:22 2015 Z
Last_Login_date : Sun Nov 21 03:47:20 2018 Z
Pwd_Reset_date : Sun Nov 21 03:57:24 2018 Z
Pwd_Fail_date : Never
Username : Guest [501]
Account_created : Wed Mar 25 10:33:22 2015 Z
Last_Login_date : Never
Pwd_Reset_date : Never
Pwd_Fail_date : Never
Username : informant [1000]
Account_created : Sun Mar 22 14:33:54 2015 Z
Last_Login_date : Wed Mar 25 14:45:43 2015 Z
Pwd_Reset_date : Sun Mar 22 14:33:54 2015 Z
Pwd_Fail_date : Wed Mar 25 14:45:43 2015 Z
Username : admin11 [1001]
Account_created : Sun Mar 22 15:51:54 2015 Z
Last_Login_date : Sun Mar 22 15:53:02 2015 Z
Pwd_Reset_date : Sun Mar 22 15:53:02 2015 Z
Pwd_Fail_date : Sun Mar 22 15:53:02 2015 Z
Username : iTechTeam [1002]
Account_created : Sun Mar 22 15:52:30 2015 Z
Last_Login_date : Never
Pwd_Reset_date : Sun Mar 22 15:52:45 2015 Z
Pwd_Fail_date : Sun Mar 22 15:53:02 2015 Z
=====
(kali㉿kali)-[~]
```

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

```
kali@kali:~$ sam -r SAM | grep -E "Username|Created|Date"
Launching samparse v.20200211
=====
Username : Administrator [500]
Account_created : Wed Mar 25 10:33:22 2015 Z
Last_Login_date : Never
Pwd_Reset_date : Never
Pwd_Fail_date : Never
Username : Guest [501]
Account_created : Sun Mar 22 14:33:54 2015 Z
Last_Login_date : Wed Mar 25 14:45:59 2015 Z
Pwd_Reset_date : Sun Mar 22 14:33:54 2015 Z
Pwd_Fail_date : Wed Mar 25 14:45:43 2015 Z
Username : informant [1000]
Account_created : Sun Mar 22 14:33:54 2015 Z
Last_Login_date : Sun Mar 22 15:53:18 2015 Z
Pwd_Reset_date : Sun Mar 22 14:33:54 2015 Z
Pwd_Fail_date : Sun Mar 22 15:53:02 2015 Z
Username : admin11 [1001]
Account_created : Sun Mar 22 15:51:54 2015 Z
Last_Login_date : Sun Mar 22 15:53:02 2015 Z
Pwd_Reset_date : Sun Mar 22 15:51:54 2015 Z
Pwd_Fail_date : Sun Mar 22 15:53:02 2015 Z
Username : iTechTeam [1002]
Account_created : Sun Mar 22 15:52:30 2015 Z
Last_Login_date : Never
Pwd_Reset_date : Sun Mar 22 15:52:45 2015 Z
Pwd_Fail_date : Sun Mar 22 15:53:02 2015 Z
=====
(kali㉿kali)-[~]
```

6.1 What are the NTLM of these accounts?

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

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays the following output:

```
Guest:501:aad3b435b51404eaaad3b435b51404eae:31d6cfe8d76a971b73:59d7e0c889c0:::  
informant:1000:aad3b435b51404eaaad3b435b51404eae:9e3d1b073660bd7b7978df9f14d0a:::  
admin1:1001:aad3b435b51404eaaad3b435b51404eae:2179594ab2dfeffcc9784a943c7f14d0a:::  
ITechTeam:1002:aad3b435b51404eaaad3b435b51404eae:75edcb767689ab3784a3b7d3d6e943:::  
User1:1003:aad3b435b51404eaaad3b435b51404eae:1b3881b68a0a6e8921fd3c5729d30bf:::  
[*] Dumping cached domain logon information (domain/username/hash)  
[*] Dumping LSA Secrets  
[*] DPAPI_SYSTEM  
dpapi_machinekey@kad1468891df9745e3d93183352f0e825a9b96d1  
dpapi_userkey@kad1468891df9745e3d93183352f0e825a9b96d1  
[*] Cleaning up ...  
[+] (kali㉿kali)-[~]  
$ rip.pl -r SOFTWARE -p lastloggedon  
Launching lastloggedon v.20200517  
lastloggedon v.20200517  
(Software) Gets LastLoggedOn values from LogonUI key  
LastLoggedOn  
Microsoft\Windows\CurrentVersion\Authentication\LogonUI  
LastWrite: 2015-03-25 13:05:47Z  
LastLoggedOnUser -> informant  
LastLoggedOnsAMUser -> informant-P\informant  
[+] (kali㉿kali)-[~]  
$
```

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

```

kali@kali: ~
[*] Cleaning up ...
[+] (kali㉿kali)-[~]
$ tipcl -l -r SOFTWARE
Launching lastloggedon v.20200517
lastloggedon v.20200517
(Software) Gets LastloggedOnUser values from LogonUI key

LastloggedOnUser   = \Informat
LastloggedOnSAMUser = informant-PC\informant

[+] (kali㉿kali)-[~]
$ tipcl -l -r SYSTEM
Launching shutdown v.20200518
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
Lastwrite time: 2015-03-25 15:31:05Z
ShutdownTime : 2015-03-25 15:31:05Z

[+] (kali㉿kali)-[~]

```

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

```

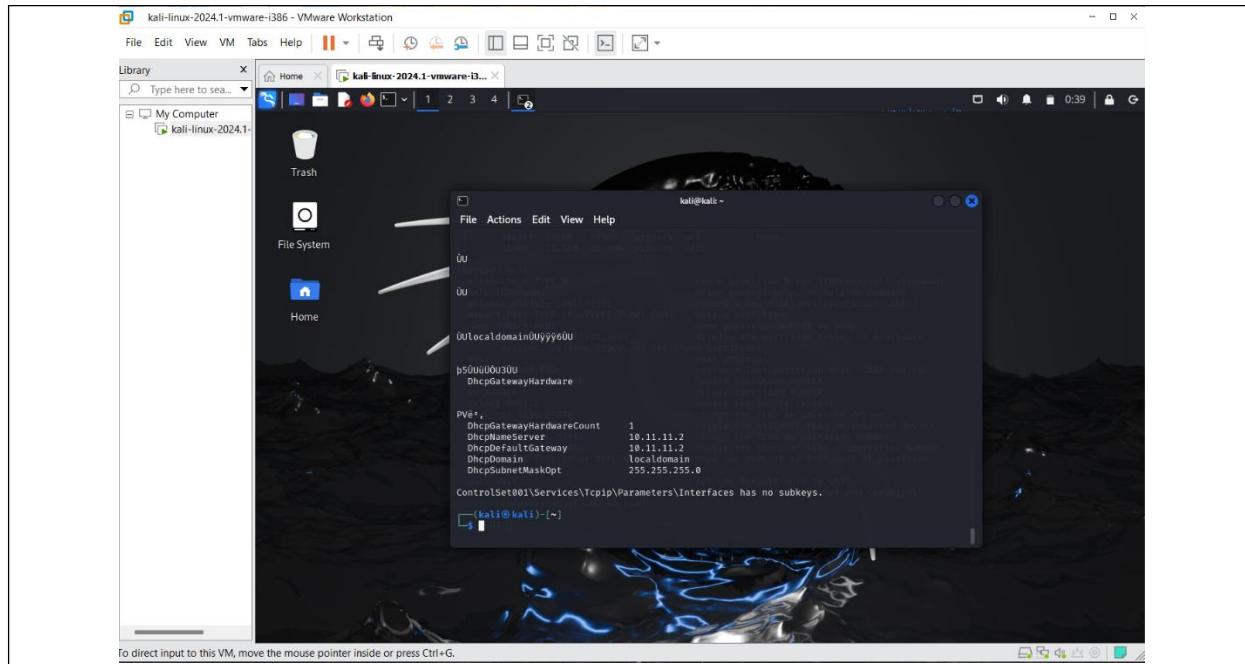
[+] (kali㉿kali)-[~]
$ tipcl -l -r SYSTEM
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {846e3b2-7839-11d0-920-000e6f6e6963}
Lastwrite Time: 2015-03-25 10:33:10Z

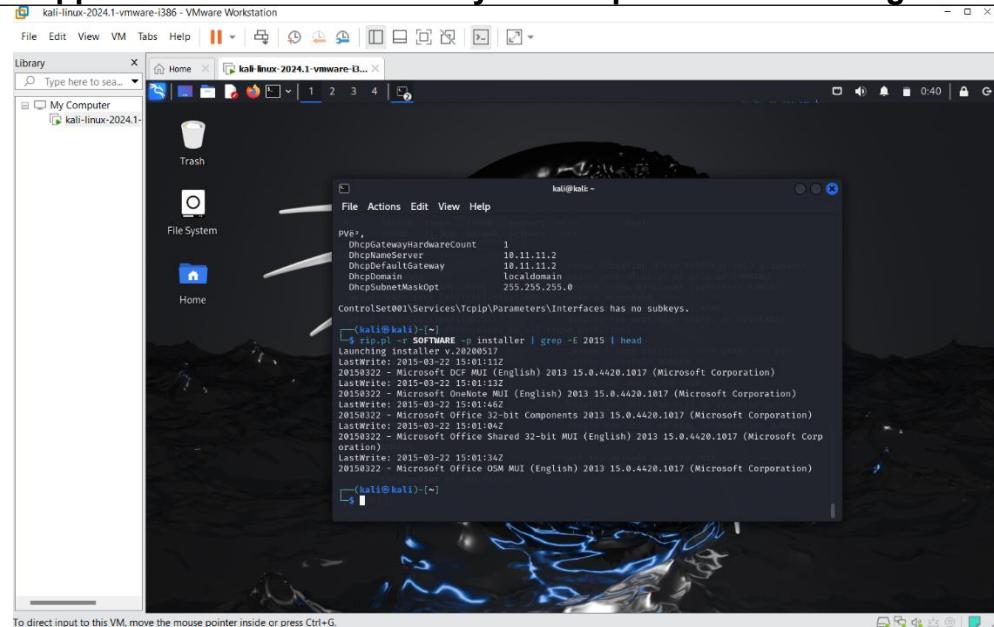
ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.

Adapter: {E9AEC-E817-478-A049-5D07F2DAB20E}
Lastwrite Time: 2015-03-25 15:24:51Z
UseZeroBroadcast
EnableDeadGwDetect
EnableDHCP
EnableDHCPv6
NameServer
Domain
RegistrationEnabled
RegisterAdapterName
DhcpIPAddress
DhcpNetmask
DhcpServer
Lease
LeaseObtainedTime
T1
T2
LeaseTerminatesTime
AddressType

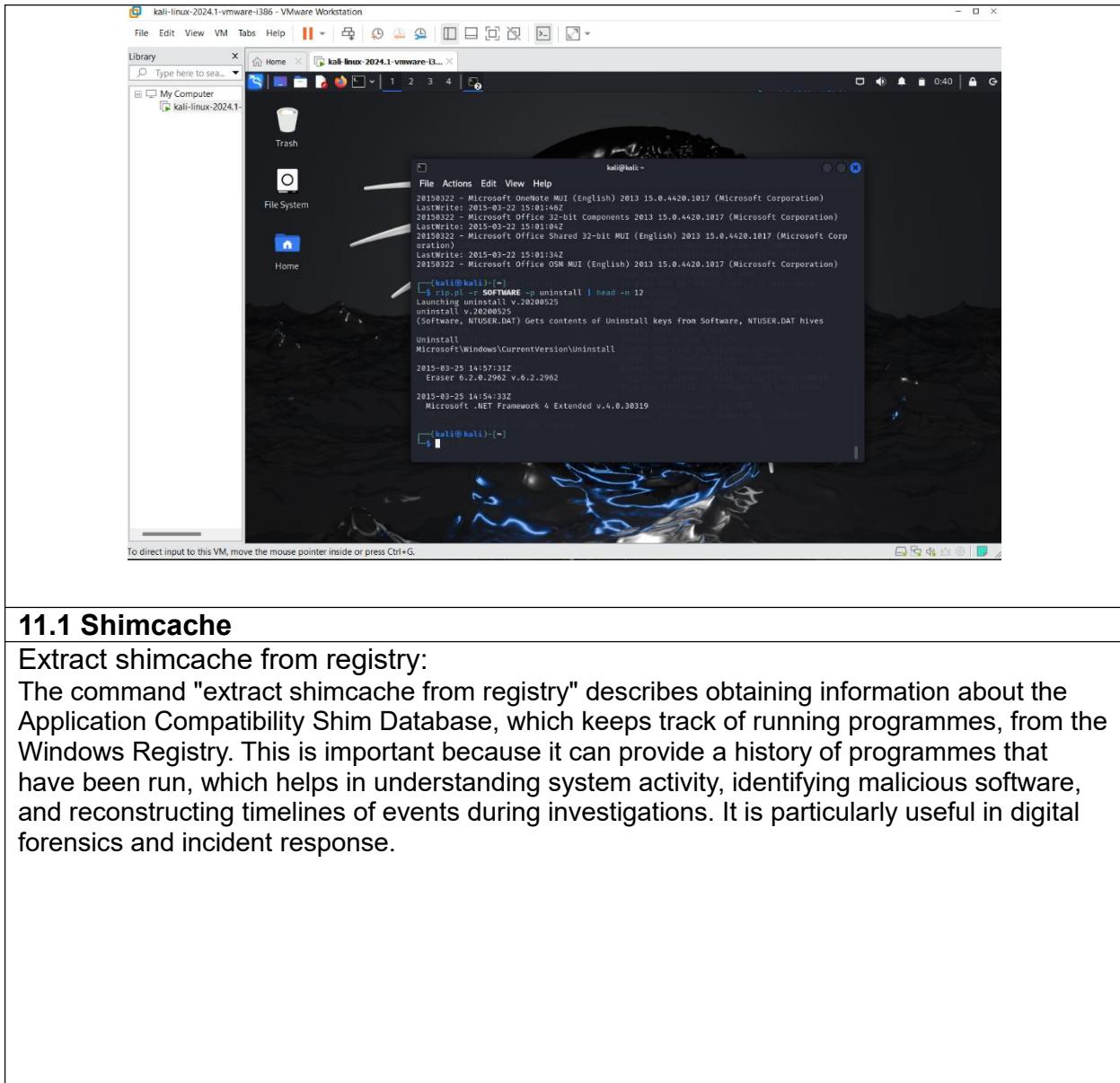
```



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.

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The desktop background is a dark landscape scene. A terminal window titled 'kali@kali' is open, displaying a command-line session. The user runs the command 'fipa.al -r SYSTEM -o shimcache | head -n 15' to launch the shimcache tool. The output shows the dump of the System hive's AppCompatCache data, including file names, sizes, and timestamps. The terminal window has a dark theme with white text. The desktop interface includes a taskbar at the top with icons for File, Edit, View, VM, Tabs, Help, and various system status indicators. A sidebar on the left contains icons for Library, Home, My Computer, and the current VM (kali-linux-2024.1). A bottom status bar indicates 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

11.2 RecentFileCache.bcf/Amcache

Find the location of RecenfFileCache.bcf:

kali-linux-2024.1-vmware-i386 - VMware Workstation

File Edit View VM Tabs Help

Library X

Type here to search

My Computer

kali-linux-2024.1-

Home kalli@kali:~

File Actions Edit View Help

(System) Parse file refs from System hive AppCompatCache data

```
*/* ControlSet001 */
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2015-03-25 15:31:05Z
Signature: 0xbadc0fee
Name: AppCompatCache
Data Length: 60016 bytes
Win32K8R2\Win3, 64-bit

C:\Windows\Installer\{91150800-0011-0000-1000-00000000FF1C}\wordicon.exe 2015-03-22 15:03:
28

C:\Program Files\xCleaner\uninst.exe 2015-03-13 13:55:38 Executed
C:\Windows\System32\gamerux.dll 2010-11-21 03:24:40
C:\Windows\System32\ieauinit.exe 2010-11-21 03:25:08 Executed
C:\Windows\system32\defrag.exe 2009-07-14 01:39:02 Executed

[kali㉿kali] ~]
# file -c -o 206848 cfreds_2015.data_leakage_pc.dd | grep -Ei 'RecentFileCache'
Error starting image file (raw_open: image "cfreds_2015.data_leakage_pc.dd" - No such file or directory)

[kali㉿kali] ~]
# file -c -o 206848 cfreds_2015.data_leakage_pc.dd | grep -Ei 'RecentFileCache'
r/x 16029-128:4 Windows/AppCompat/Programs/RecentFileCache.bcf

[kali㉿kali] ~]
```

Show RecentFileCache.bcf:

11.3 UserAssist

List executed programs by the user informant:

```

File Edit View VM Tabs Help
Library Type here to search
My Computer kali-linux-2024.1...
Trash
File System
Home
File Actions Edit View Help
kali@kali: ~
[(kali㉿kali)-~]
$ rip.pl -l | grep -i assist
117. userassist v.20170204 [NTUSER.DAT]
- Displays contents of UserAssist registry
164. userassist_Lnk v.20170204 [NTUSER.DAT]
- Displays contents of UserAssist subkeys in TLN format
249. disableuserassist v.20230710 [NTUSER.DAT]
- Get Start_TrackEnabled and Start_TrackProgs values which confirm if UserAssist was disabled.

[(kali㉿kali)-~]
$ rip.pl -r NTUSER.informant.DAT -p userassist | head
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2015-03-22 14:35:01Z
(CEBF5CD-ACE2-4F4F-9178-9926F41749EA)
2015-03-25 15:21:38Z
[1AC1E77-4E7-E45D-B744-2EB1AE519B87]\xpsrchvw.exe (1)
2015-03-25 15:24:48Z
{6D809377-6AF0-44AB-8957-A3773F02200E}\Microsoft Office\Office15\WINWORD.EXE (4)
2015-03-25 15:21:30Z
[(kali㉿kali)-~]
$ 

```

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

```

File Edit View VM Tabs Help
Library Type here to search
My Computer kali-linux-2024.1...
Trash
File System
Home
File Actions Edit View Help
kali@kali: ~
[(kali㉿kali)-~]
$ rip.pl -r NTUSER.informant.DAT -p userassist | grep -i -B 2 -A 1 "chrome" --color
Launching userassist v.20170204
{6D809377-6AF0-44AB-8957-A3773F02200E}\Microsoft Office\Office15\OUTLOOK.EXE (5)
2015-03-24 21:05:38Z
Chrome (7)
2015-03-24 18:31:55Z
{013904AE-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Outlook 2013.lnk (5)
2015-03-24 21:05:38Z
{9E3995AB-1F9C-4F13-B827-48B2486C7174}\TaskBar\Google Chrome.lnk (5)
2015-03-24 18:32:15Z
:::{ED28BDFD-0E48-4870-83B1-96B02CFE0052}\{0008862B-6453-4957-A821-3D98074C76BE} (7)
2015-03-23 17:26:50Z
C:\Users\Public\Desktop\Google Chrome.lnk (2)
2015-03-22 14:33:13Z
[(kali㉿kali)-~]
$ 

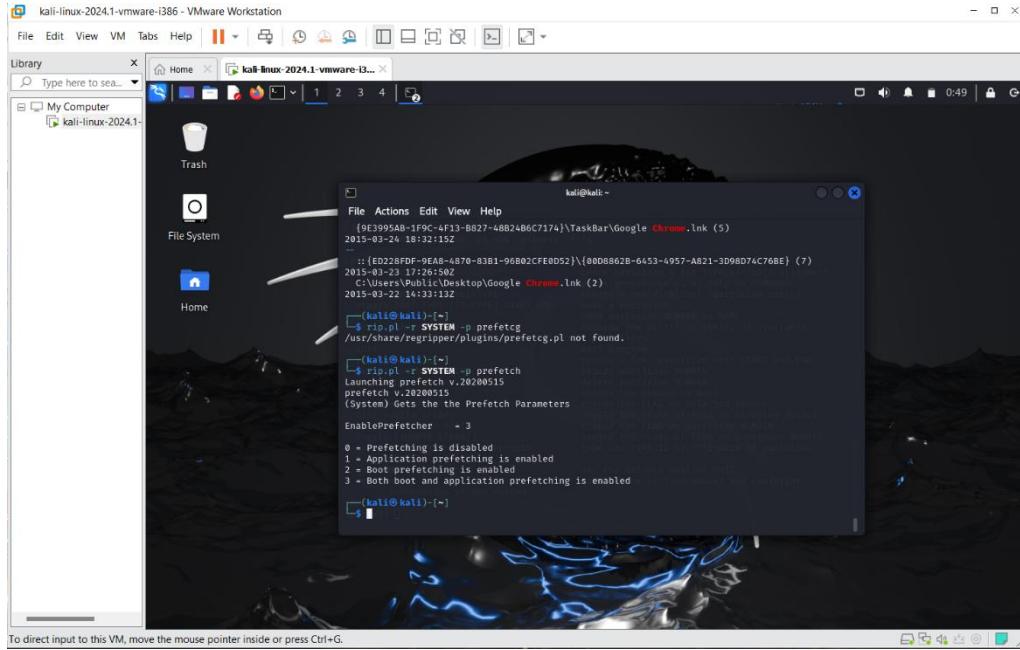
```

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.



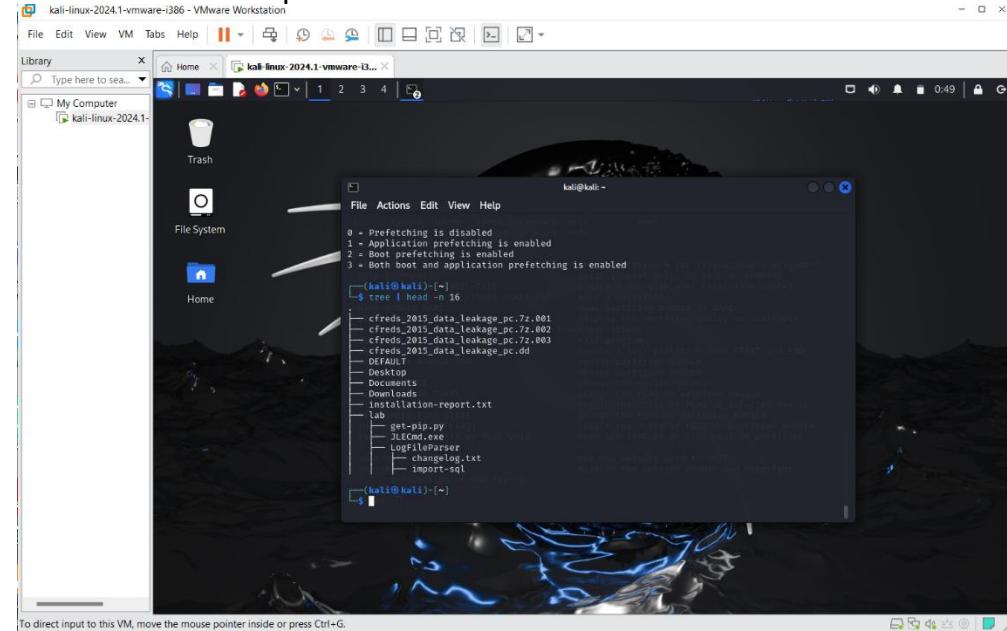
```
(kali㉿kali)-[~]
$ rip.pl -r SYSTEM -p prefetch
/usr/share/regripper/plugins/prefetchcg.pl not found.

(kali㉿kali)-[~]
$ rip.pl -r SYSTEM -p prefetch
Launching prefetch v.20200519
prefetch V.20200519
(System) Gets the Prefetch Parameters
EnablePrefetcher = 3

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled

(kali㉿kali)-[~]
```

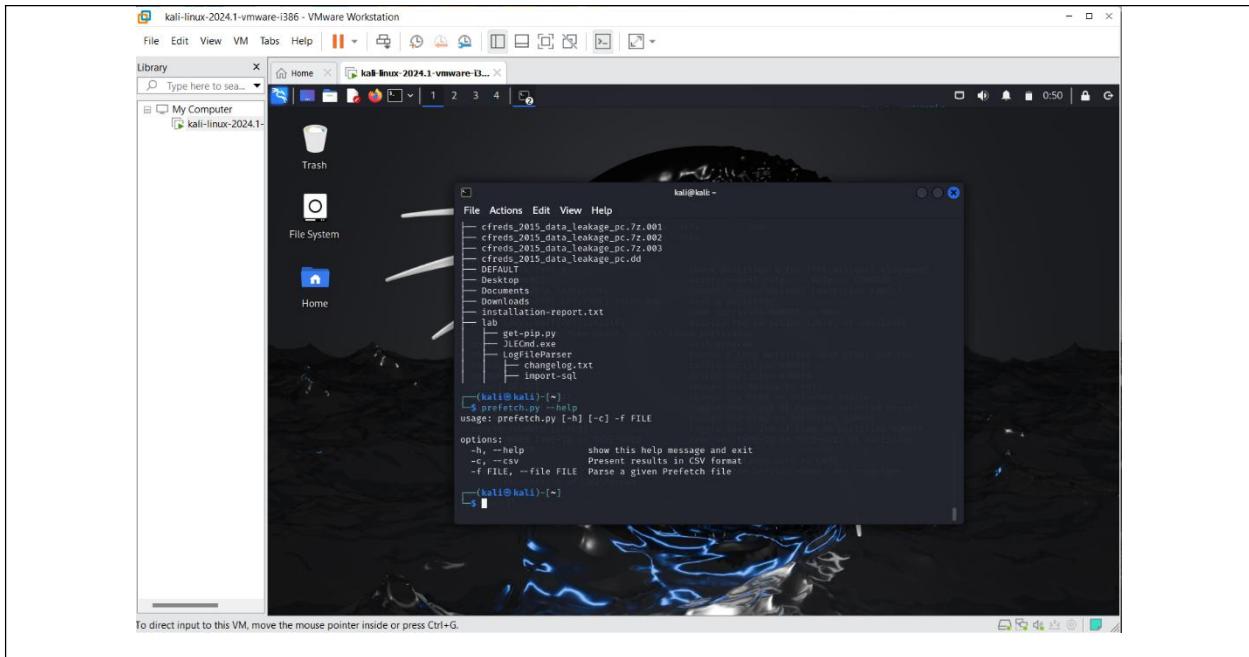
Verify Prefetch folder has .pf files:



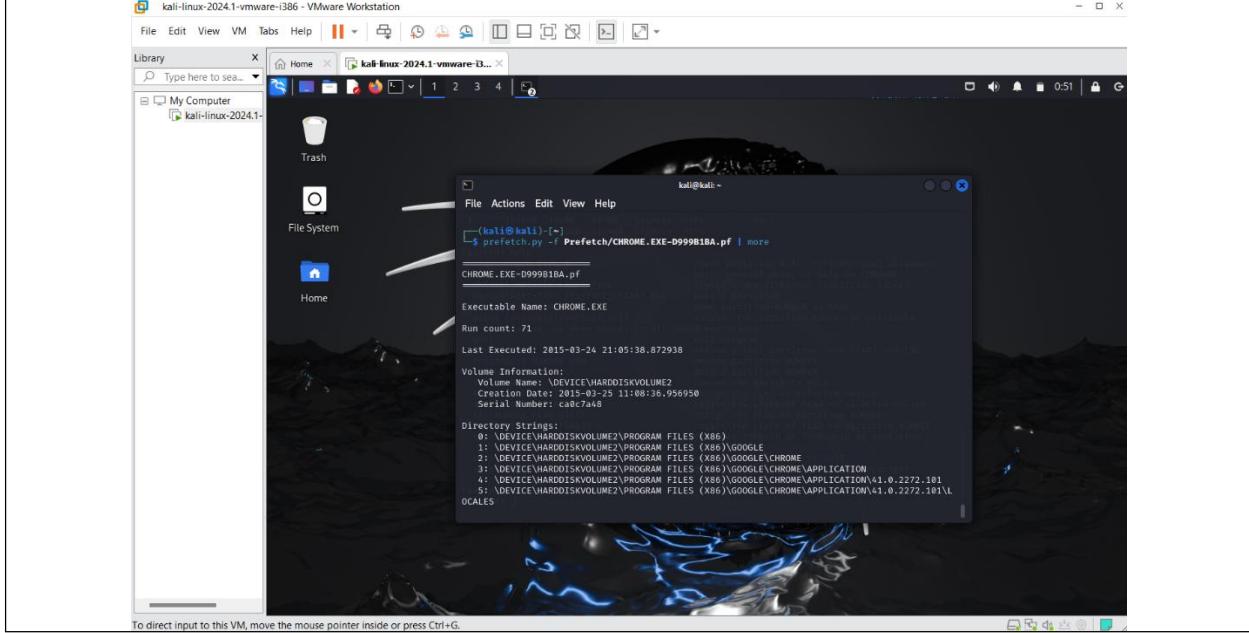
```
(kali㉿kali)-[~]
$ tree | head -n 16
.
├── cfreds_2015_data_leakage_pc_7z.001
├── cfreds_2015_data_leakage_pc_7z.002
├── cfreds_2015_data_leakage_pc_7z.003
├── cfreds_2015_data_leakage_pc.dd
├── DEFAULT
├── Desktop
├── Documents
├── Downloads
├── Installation-report.txt
└── lab
    ├── get.py
    └── Jupyter
        └── LogFileParser
            └── changelog.txt
                └── import-sql

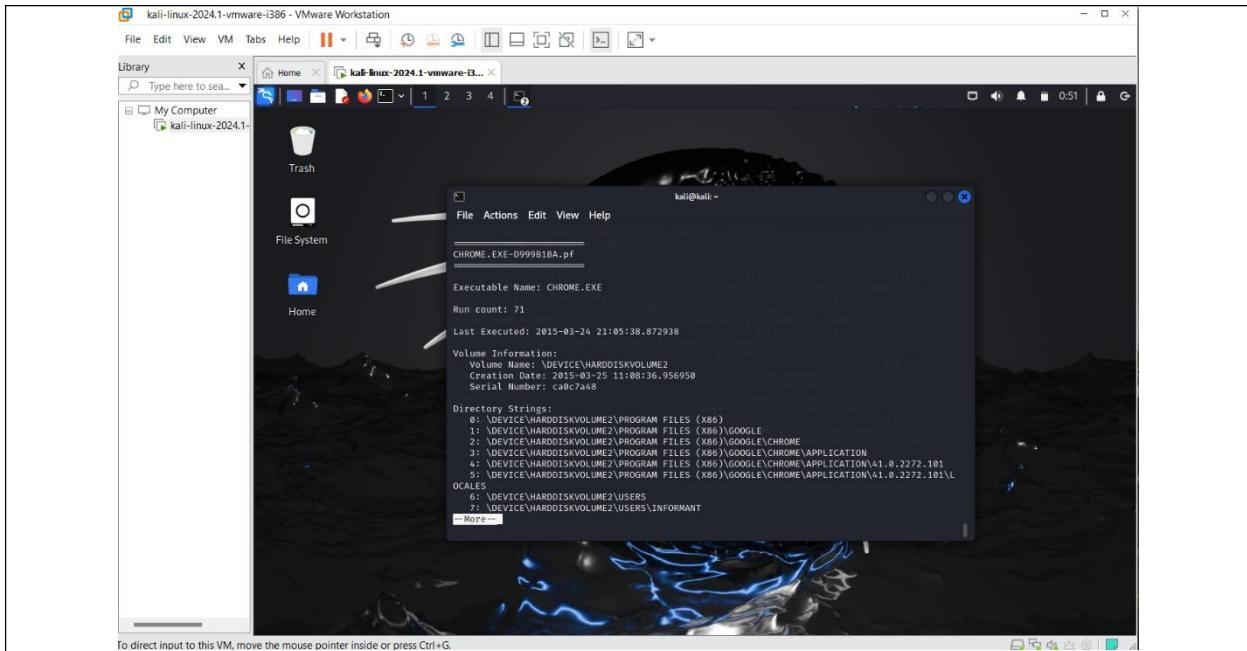
(kali㉿kali)-[~]
```

Verify prefetch command:

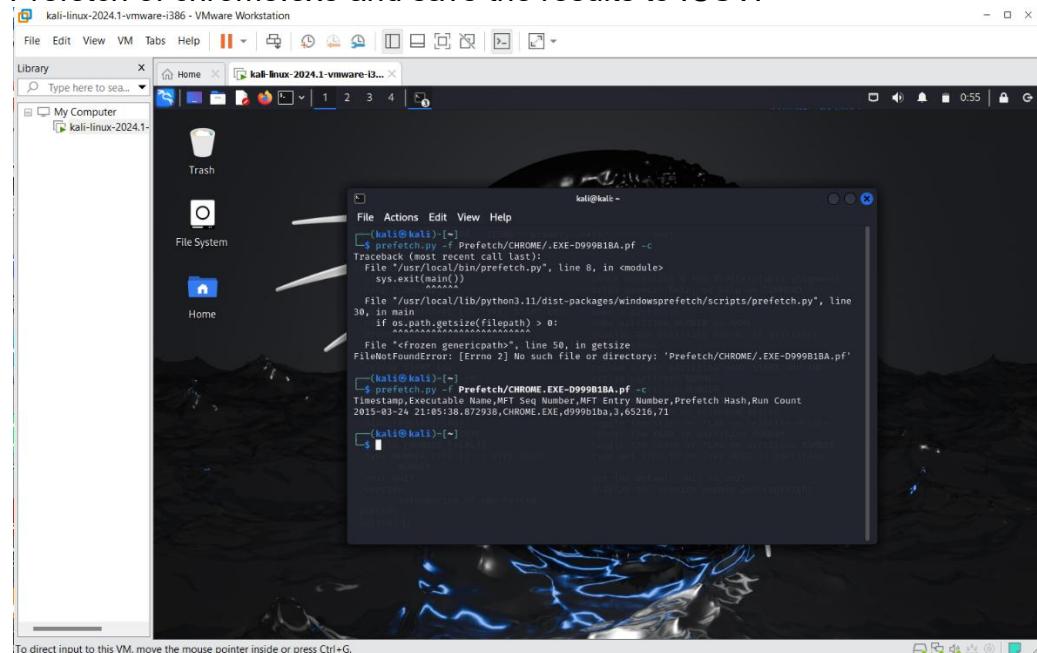


Parse Prefetch of chrome.exe:





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



11.5 MuCache: Multilingual User Interface

Search for muicache plugin:

The screenshot shows a Kali Linux 2024.1 VM running in VMware Workstation. The desktop environment is Unity. A terminal window is open, showing the following command and output:

```
$ prefetch.py -r Prefetch\CHROME.EXE-D999B1BA.pf --c  
Timestamp,Executable Name,.NET Seq Number,.NET Entry Number,Prefetch Hash,Run Count  
2015-03-24 21:05:38.872938,CHROME.EXE,d999b1ba,3,65216,71  
  
[kali㉿kali:~] $ ribol -t NTUSER_informant.DAT -p mucache  
Launching mucache v.20280525  
mucache v.20280525  
(NTUSER.DAT,USKCLASS.DAT) Gets EXEs from user's MUICache key  
Software\Microsoft\Windows\ShellNoRoam\MUICache not found.  
Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
```

Exam muicache:

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The desktop background is a dark space-themed image. A terminal window titled 'kali@kali: ~' is open, displaying a command-line session with a tool named 'rip'. The user has run 'rip.pl -r' and is interacting with the resulting output, which includes file paths like 'Prefetch/CHROME.EXE-D99981BA.pf' and 'NTUSER.informant.DAT'. The terminal also shows the user navigating through directory structures such as 'Software\Microsoft\Windows\ShellNoRoam\Shell\'. The top of the screen features the VMware toolbar with icons for file operations, and the bottom has the standard Windows-style taskbar.

Search usrclass.dat:

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

