

## Lab 5: Examining the Registry

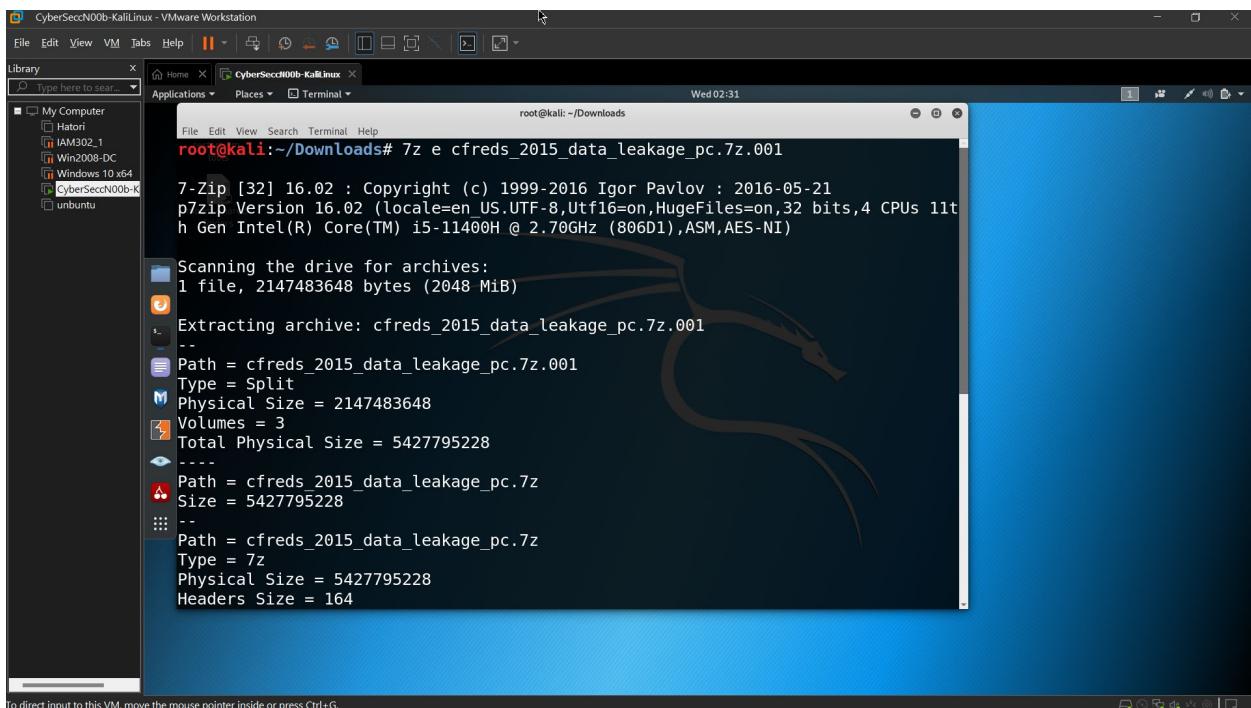
Group: CyberSec\_N00b

Member:

- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

### Step 1.

Unzipped the DD image



The screenshot shows a terminal window titled "root@kali: ~/Downloads" running on a Kali Linux desktop. The terminal displays the output of the command "7z e cfreds\_2015\_data\_leakage\_pc.7z.001". The output shows the extraction process of a 7z archive named "cfreds\_2015\_data\_leakage\_pc.7z.001". The archive contains one file, "cfreds\_2015\_data\_leakage\_pc.7z", which is a split file with a physical size of 2147483648 bytes (2048 MiB). The total physical size of the archive is 5427795228 bytes, and the headers size is 164 bytes. The terminal window is part of a VMware Workstation interface, with other virtual machines listed in the background.

```
root@kali:~/Downloads# 7z e cfreds_2015_data_leakage_pc.7z.001
7-Zip [32] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,Hugefiles=on,32 bits,4 CPUs 11t
h Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz (806D1),ASM,AES-NI)

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
```

Verify the unzipped DD image

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open in the Applications menu, titled 'Terminal'. The command being run is:

```
root@kali:~/Downloads# dd if=cfreds_2015_data_leakage_pc.dd of=cfreds_2015_data_leakage_pc.dd
```

The terminal displays the following output:

```
Would you like to replace the existing file:  
Path: ./cfreds_2015_data_leakage_pc.dd  
Size: 14113832960 bytes (14 GiB)  
Modified: 2024-09-23 23:44:15  
with the file from archive:  
Path: cfreds_2015_data_leakage_pc.dd  
Size: 21474836480 bytes (20 GiB)  
Modified: 2015-04-21 14:17:36  
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y  
Everything is Ok  
Size: 21474836480  
Compressed: 5427795228  
root@kali:~/Downloads# ls -l  
total 26272120  
-rw-r--r-- 1 root root 2147483648 Sep 23 23:07 cfreds_2015_data_leakage_pc.7z.0  
91  
-rw-r--r-- 1 root root 2147483648 Sep 23 23:11 cfreds_2015_data_leakage_pc.7z.0  
92  
...  
-rw-r--r-- 1 root root 1132827932 Sep 23 23:13 cfreds_2015_data_leakage_pc.7z.0  
93  
-rw-r--r-- 1 root root 21474836480 Apr 21 2015 cfreds_2015_data_leakage_pc.dd  
root@kali:~/Downloads#
```

Verify the unzipped DD image with MD5

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open in the Applications menu, titled 'Terminal'. The command being run is:

```
root@kali:~/Downloads# md5sum cfreds_2015_data_leakage_pc.dd
```

The terminal displays the following output:

```
a49d1254c873808c58e6f1bcd60b5bde cfreds_2015_data_leakage_pc.dd  
root@kali:~/Downloads#
```

Step 2.

Exam partitions of the DD image using *fdisk*

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open with the command `fdisk -l cfreds_2015_data_leakage_pc.dd`. The output shows a new partition (`cfreds_2015_data_leakage_pc.dd2`) has been created, which is 20 GiB in size.

```
root@kali:~/Downloads# fdisk -l cfreds_2015_data_leakage_pc.dd
Disk cfreds_2015_data_leakage_pc.dd: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0265720

Device      Boot  Start    End  Sectors  Size Id Type
cfreds_2015_data_leakage_pc.dd1 *      2048   206847   204800  100M  7 HPFS/NTFS
cfreds_2015_data_leakage_pc.dd2     206848 41940991 41734144 19.9G  7 HPFS/NTFS
root@kali:~/Downloads#
```

List file/directory names of the system volume

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window is open with the command `fls -o 206848 cfreds_2015_data_leakage_pc.dd | head`. The output lists directory entries from the specified partition.

```
-h: Include MD5 checksum hash in mactime output
-o imgoffset: Offset into image file (in sectors)
-p: Display full path for each file
-r: Recurse on directory entries
-u: Display undeleted entries only
-v: verbose output to stderr
-V: Print version
-z: Time zone of original machine (i.e. EST5EDT or GMT) (only useful with -l)
-s seconds: Time skew of original machine (in seconds) (only useful with -l & -m)
root@kali:~/Downloads# fls -o 206848 cfreds_2015_data_leakage_pc.dd | head
d/d 273-144-6: Program Files (x86)
d/c 273-144-5: Users
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot + Other Locations
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
root@kali:~/Downloads#
```

If your VM doesn't support auto-mounting

Create a folder as the mount point

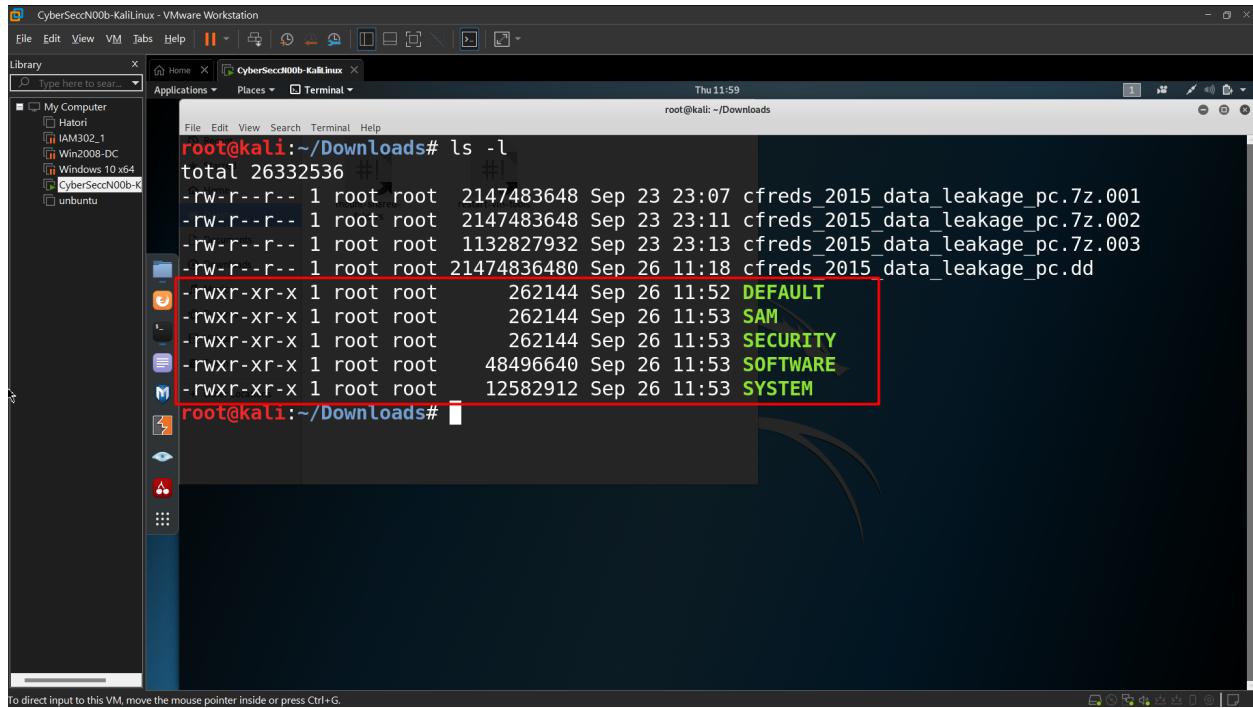
Mount partition 2 to the mounting point

```
root@kali:~/Downloads# losetup /dev/loop0p2 ^C
root@kali:~/Downloads# ls
mount.c
cfreds_2015_data_leakage_pc.7z.001 cfreds_2015_data_leakage_pc.7z.003
cfreds_2015_data_leakage_pc.7z.002 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# losetup /dev/loop0p2 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# mount /dev/loop0p2 /mnt/nist_dataleak_pc_dd2/
Mount is denied because the NTFS volume is already exclusively opened.
The volume may be already mounted, or another software may use it which
could be identified for example by the help of the 'fuser' command.
root@kali:~/Downloads# umount /dev/loop0p2
Killed
root@kali:~/Downloads# mount /dev/loop0p2 /mnt/nist_dataleak_pc_dd2/
```

Copy HKEY\_LOCAL\_MACHINE (Hive) files to \lab

```
root@kali:~/Downloads# cp /media/root/C8CA0C8DCA0C7A48/Windows/System32/config/DEFAULT .
root@kali:~/Downloads# cp /media/root/C8CA0C8DCA0C7A48/Windows/System32/config/SAM .
root@kali:~/Downloads# cp /media/root/C8CA0C8DCA0C7A48/Windows/System32/config/SECURITY .
root@kali:~/Downloads# cp /media/root/C8CA0C8DCA0C7A48/Windows/System32/config/SOFTWARE .
root@kali:~/Downloads# cp /media/root/C8CA0C8DCA0C7A48/Windows/System32/config/SYSTEM .
```

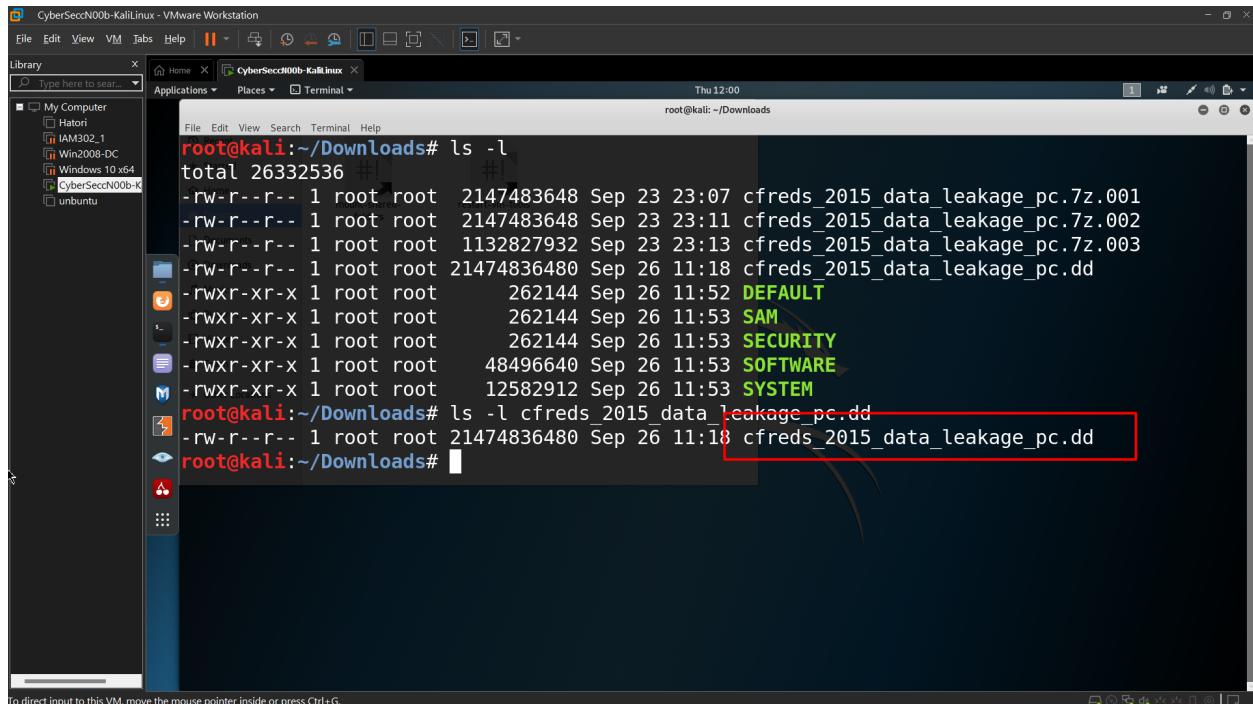
Verify five files



```
root@kali:~/Downloads# ls -l
total 26332536
-rw-r--r-- 1 root root 2147483648 Sep 23 23:07 cfreds_2015_data_leakage_pc.7z.001
-rw-r--r-- 1 root root 2147483648 Sep 23 23:11 cfreds_2015_data_leakage_pc.7z.002
-rw-r--r-- 1 root root 1132827932 Sep 23 23:13 cfreds_2015_data_leakage_pc.7z.003
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
-rwxr-xr-x 1 root root 262144 Sep 26 11:52 DEFAULT
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SAM
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SECURITY
-rwxr-xr-x 1 root root 48496640 Sep 26 11:53 SOFTWARE
-rwxr-xr-x 1 root root 12582912 Sep 26 11:53 SYSTEM
root@kali:~/Downloads#
```

### Step 3.

Verify you have the dd image



```
root@kali:~/Downloads# ls -l
total 26332536
-rw-r--r-- 1 root root 2147483648 Sep 23 23:07 cfreds_2015_data_leakage_pc.7z.001
-rw-r--r-- 1 root root 2147483648 Sep 23 23:11 cfreds_2015_data_leakage_pc.7z.002
-rw-r--r-- 1 root root 1132827932 Sep 23 23:13 cfreds_2015_data_leakage_pc.7z.003
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
-rwxr-xr-x 1 root root 262144 Sep 26 11:52 DEFAULT
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SAM
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SECURITY
-rwxr-xr-x 1 root root 48496640 Sep 26 11:53 SOFTWARE
-rwxr-xr-x 1 root root 12582912 Sep 26 11:53 SYSTEM
root@kali:~/Downloads# ls -l cfreds_2015_data_leakage_pc.dd
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads#
```

Compute MD5 and SHA1 of the DD image

```

root@kali:~/Downloads# ls -l
total 26332536
-rw-r--r-- 1 root root 2147483648 Sep 23 23:07 cfreds_2015_data_leakage_pc.7z.001
-rw-r--r-- 1 root root 2147483648 Sep 23 23:11 cfreds_2015_data_leakage_pc.7z.002
-rw-r--r-- 1 root root 1132827932 Sep 23 23:13 cfreds_2015_data_leakage_pc.7z.003
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
-rwxr-xr-x 1 root root 262144 Sep 26 11:52 DEFAULT
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SAM
-rwxr-xr-x 1 root root 262144 Sep 26 11:53 SECURITY
-rwxr-xr-x 1 root root 48496640 Sep 26 11:53 SOFTWARE
-rwxr-xr-x 1 root root 12582912 Sep 26 11:53 SYSTEM
root@kali:~/Downloads# ls -l cfreds_2015_data_leakage_pc.dd
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# md5sum cfreds_2015_data_leakage_pc.dd
0c3b2eaaff1e4f045ceda7bd0a0ff6c cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# shasum cfreds_2015_data_leakage_pc.dd
06f277bc0e0f75d3268288b92ba7d6c2164c9a48 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads#

```

Show partitions of the image

```

root@kali:~/Downloads# ls -l cfreds_2015_data_leakage_pc.dd
-rw-r--r-- 1 root root 21474836480 Sep 26 11:18 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# md5sum cfreds_2015_data_leakage_pc.dd
0c3b2eaaff1e4f045ceda7bd0a0ff6c cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# shasum cfreds_2015_data_leakage_pc.dd
06f277bc0e0f75d3268288b92ba7d6c2164c9a48 cfreds_2015_data_leakage_pc.dd
root@kali:~/Downloads# fdisk -l cfreds_2015_data_leakage_pc.dd
Disk cfreds_2015_data_leakage_pc.dd: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xf0265720

Device          Boot  Start    End  Sectors  Size Id Type
cfreds_2015_data_leakage_pc.dd1 *      2048  206847   204800 100M  7 HPFS/NTFS/exFAT
cfreds_2015_data_leakage_pc.dd2      206848 41940991 41734144 19.9G  7 HPFS/NTFS/exFAT
root@kali:~/Downloads#

```

Show partitions and unallocated space using *mmls*

The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window displays the output of the command `mmls cfreds_2015_data_leakage_pc.dd`. The output shows the DOS Partition Table for the specified disk image, listing four partitions:

Slot	Start	End	Length	Description
000:c	Meta	0000000000	0000000001	Primary Table (#0)
001:res	-----	0000000000	0000002047	Unallocated
002:as	000:000	0000002048	0000206847	0000204800 NTFS / exFAT (0x07)
003:Editor	000:001	0000206848	0041940991	0041734144 NTFS / exFAT (0x07)
004:Locat	-----	0041940992	0041943039	0000002048 Unallocated

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

Display file system statistics and metadata information from a disk image (first partition)

```
root@kali:~/Downloads# fsstat -b 512 -o 2048 cfreds_2015_data_leakage_pc.dd
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 4A180A15180A0125
OEM Name: NTFS
Volume Name: System Reserved
Version: Windows XP

METADATA INFORMATION
-----
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 - 256
Root Directory: 5

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 25598
```

```
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 25598
Total Sector Range: 0 - 204798
restart-vm-tools

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)  Size: No Limit  Flags: Non-resident
$FILE_NAME (48)  Size: 68-578  Flags: Resident,Index
$OBJECT_ID (64)  Size: 0-256  Flags: Resident
$SECURITY_DESCRIPTOR (80)  Size: No Limit  Flags: Non-resident
$VOLUME_NAME (96)  Size: 2-256  Flags: Resident
$VOLUME_INFORMATION (112)  Size: 12-12  Flags: Resident
$DATA (128)  Size: No Limit  Flags:
$INDEX_ROOT (144)  Size: No Limit  Flags: Resident
$INDEX_ALLOCATION (160)  Size: No Limit  Flags: Non-resident
$BITMAP (176)  Size: No Limit  Flags: Non-resident
$REPARSE_POINT (192)  Size: 0-16384  Flags: Non-resident
$EA_INFORMATION (208)  Size: 8-8  Flags: Resident
$EA (224)  Size: 0-65536  Flags:
$LOGGED.Utility_Stream (256)  Size: 0-65536  Flags: Non-resident
root@kali:~/Downloads#
```

List the second partition details

```
root@kali:~/Downloads# fsstat -b 512 -o 206848 cfreds_2015 data_leakage_pc.dd
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: C8CA0C8DCA0C7A48
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 78080
Root Directory: 5

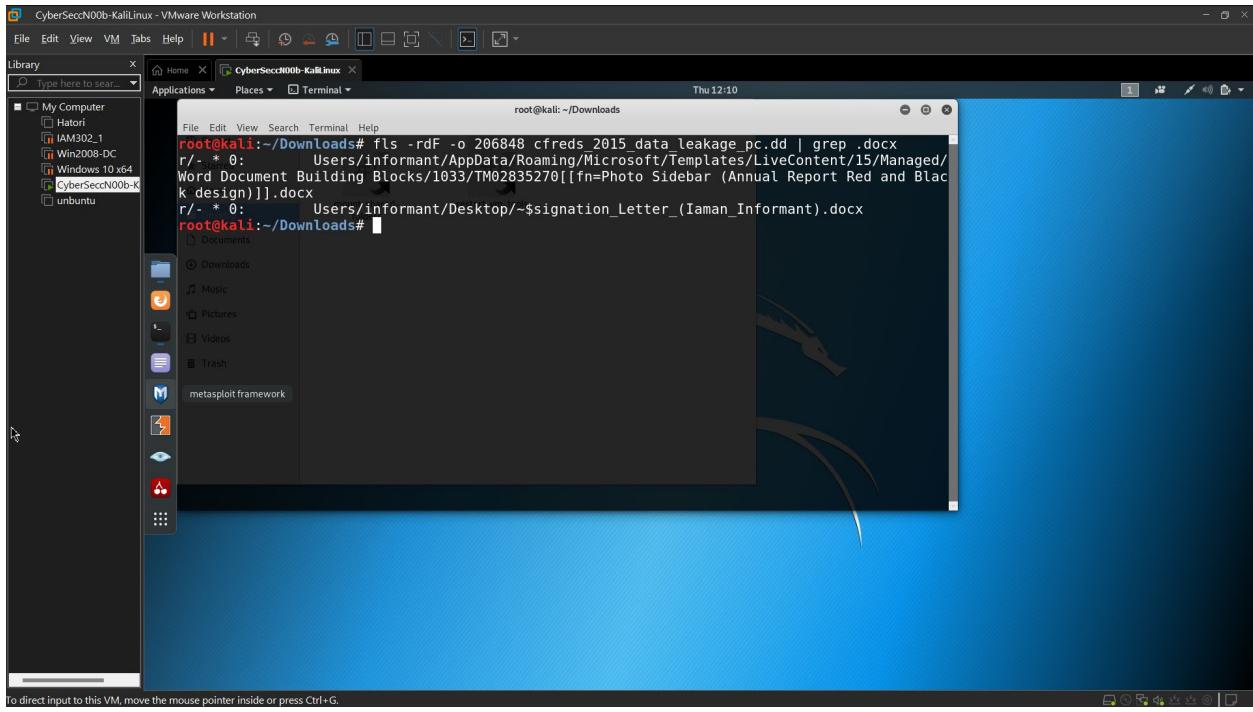
CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 5216766
Total Sector Range: 0 - 41734142
```

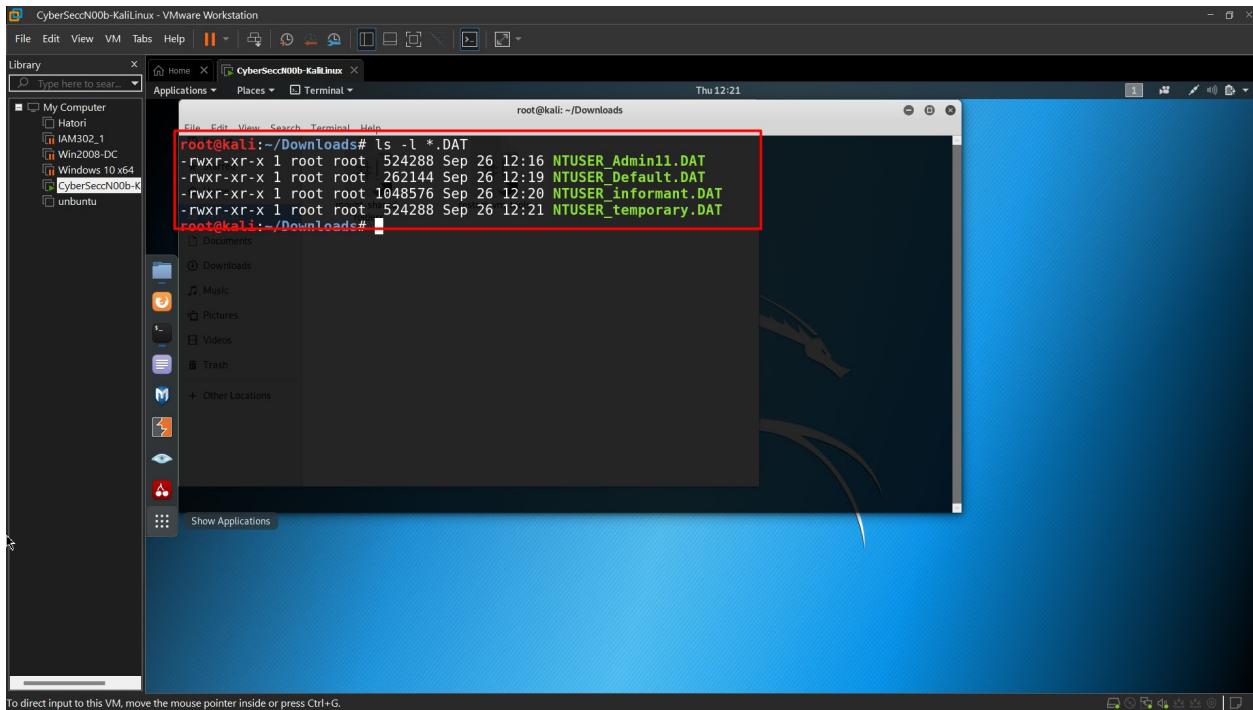
```
root@kali:~/Downloads#
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 5216766
Total Sector Range: 0 - 41734142 restart-vm-tools

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
$ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
$FILE_NAME (48) Size: 68-578 Flags: Resident,Index
$OBJECT_ID (64) Size: 0-256 Flags: Resident
$SECURITY_DESCRIPTOR (80) Size: No Limit Flags: Non-resident
$VOLUME_NAME (96) Size: 2-256 Flags: Resident
$VOLUME_INFORMATION (112) Size: 12-12 Flags: Resident
$DATA (128) Size: No Limit Flags:
$INDEX_ROOT (144) Size: No Limit Flags: Resident
$INDEX_ALLOCATION (160) Size: No Limit Flags: Non-resident
$BITMAP (176) Size: No Limit Flags: Non-resident
$REPARSE_POINT (192) Size: 0-16384 Flags: Non-resident
$EA_INFORMATION (208) Size: 8-8 Flags: Resident
$EA (224) Size: 0-65536 Flags:
$LOGGED.Utility_Stream (256) Size: 0-65536 Flags: Non-resident
root@kali:~/Downloads#
```

List all deleted .docx files in the whole partition?



Verify Users' information



What is the installed OS information in detail?