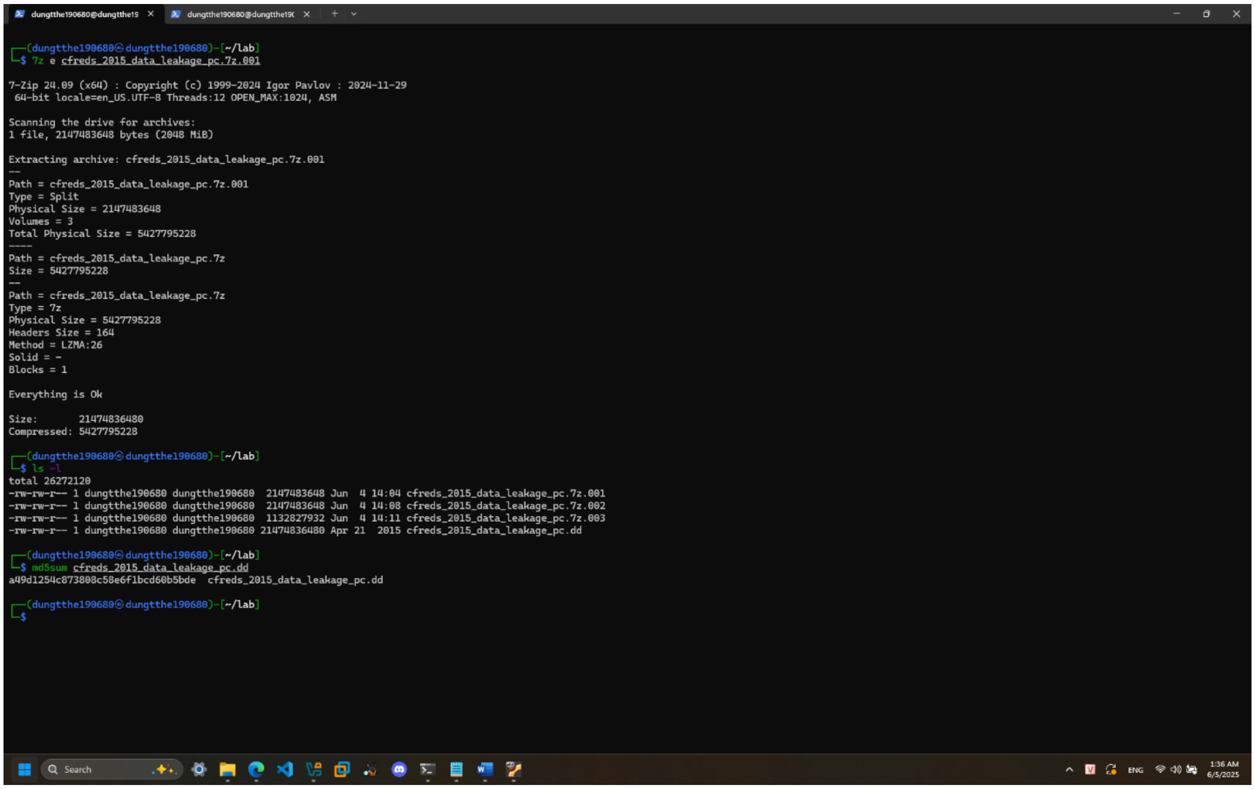
Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

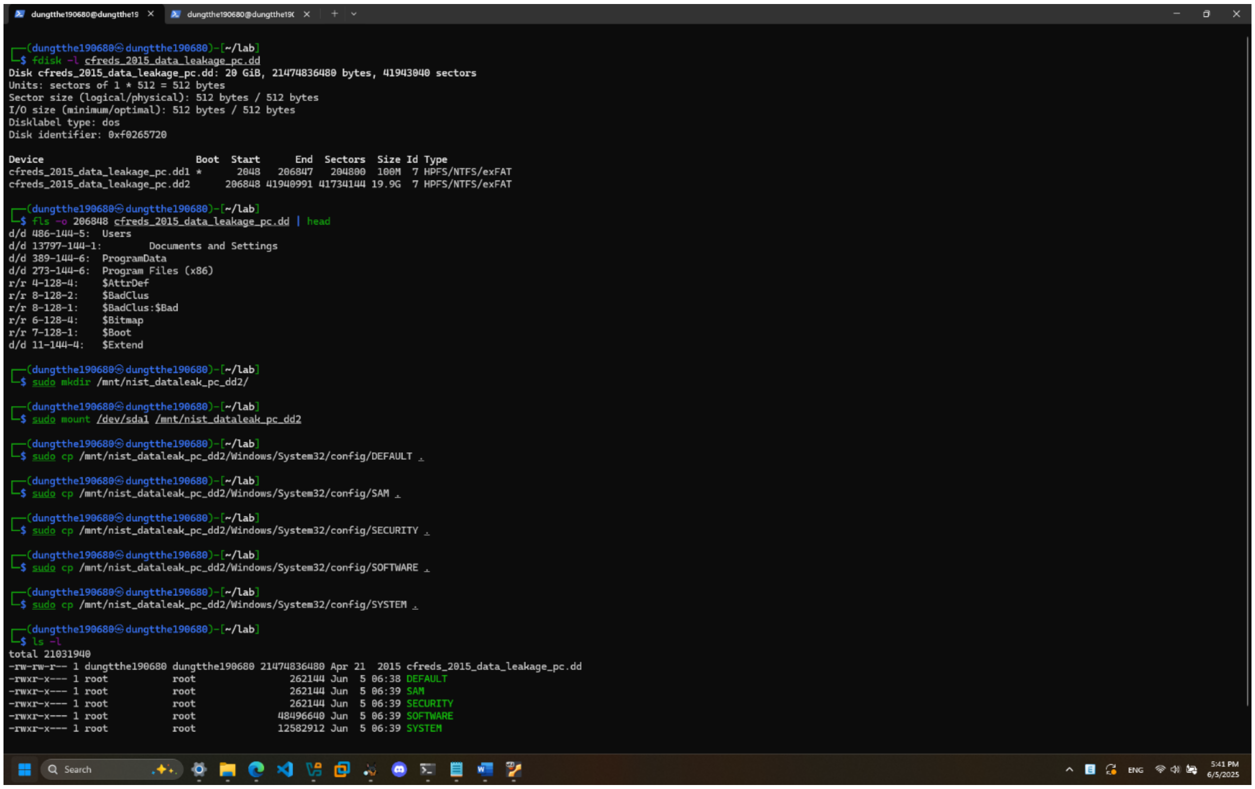
Lab 5: Examining the Registry

Step 1:



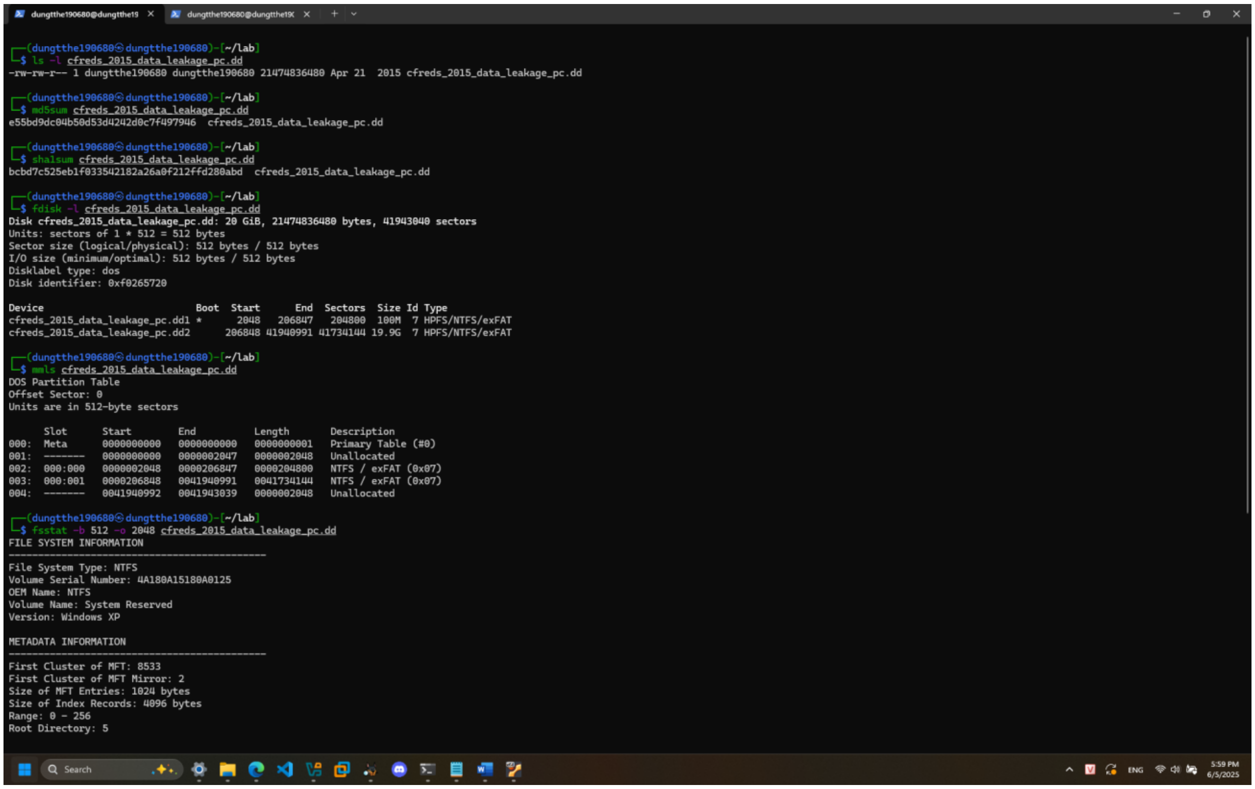
```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ 7z e cfreds_2015_data_leakage_pc.7z.001

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=en_US.UTF-8 Threads:12 OPEN_MAX:1024, ASM

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

Everything is Ok

Size:       21474836480
Compressed: 5427795228

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ ls -l
total 26272120
-rw-rw-r-- 1 dungtthe190680 dungtthe190680  2147483648 Jun  4 14:04 cfreds_2015_data_leakage_pc.7z.001
-rw-rw-r-- 1 dungtthe190680 dungtthe190680  2147483648 Jun  4 14:08 cfreds_2015_data_leakage_pc.7z.002
-rw-rw-r-- 1 dungtthe190680 dungtthe190680  1132827932 Jun  4 14:11 cfreds_2015_data_leakage_pc.7z.003
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 21474836480 Apr 21  2015 cfreds_2015_data_leakage_pc.dd

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ md5sum cfreds_2015_data_leakage_pc.dd
a49d1254c873808c58e6f1bcd60b5bde  cfreds_2015_data_leakage_pc.dd

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$
```

Step 2:

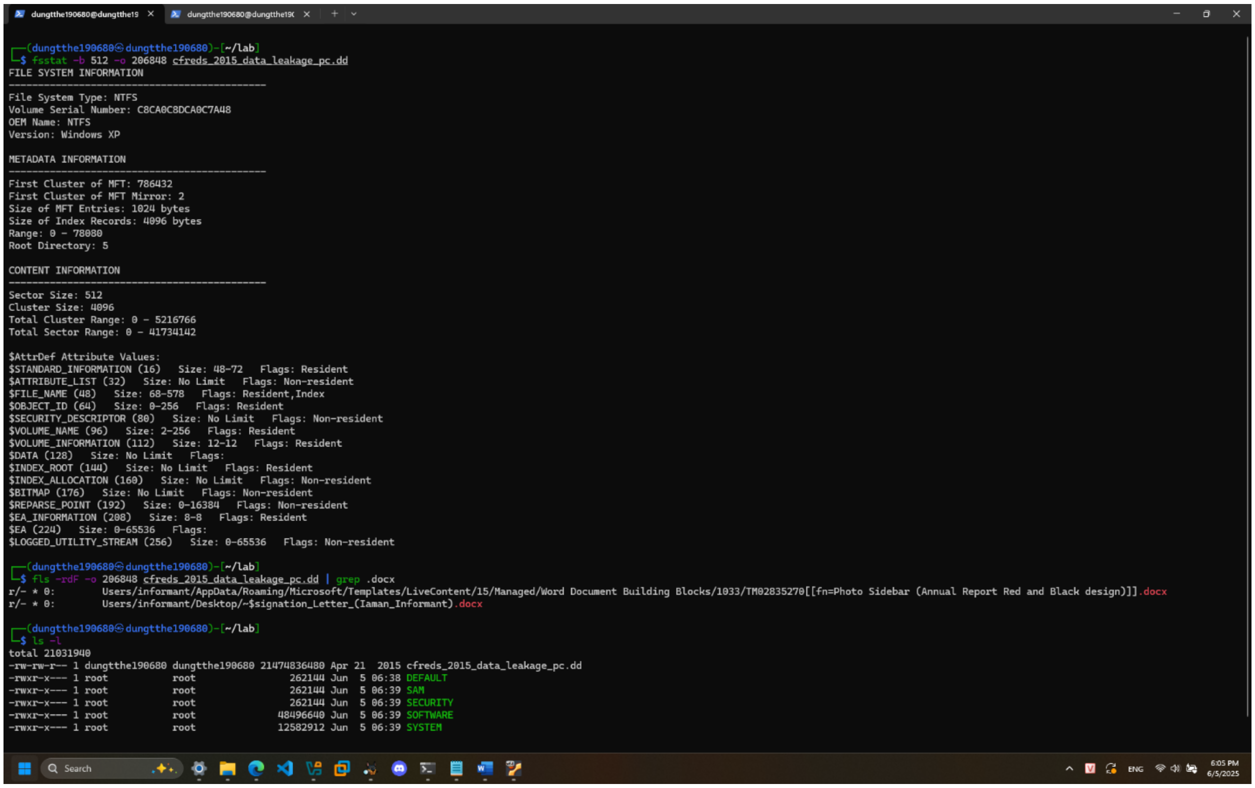


```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ fdisk -l cfreds_2015_data_leakage_pc.dd
Disk cfreds_2015_data_leakage_pc.dd: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 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

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ fls -o 206848 cfreds_2015_data_leakage_pc.dd | head
d/d 486-144-5:  Users
d/d 13797-144-1:        Documents and Settings
d/d 389-144-6:  ProgramData
d/d 273-144-6:  Program Files (x86)
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
d/d 11-144-4:   $Extend

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo mkdir /mnt/nist_dataleak_pc_dd2/

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo mount /dev/sda1 /mnt/nist_dataleak_pc_dd2

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo cp /mnt/nist_dataleak_pc_dd2/Windows/System32/config/DEFAULT .

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo cp /mnt/nist_dataleak_pc_dd2/Windows/System32/config/SAM .

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo cp /mnt/nist_dataleak_pc_dd2/Windows/System32/config/SECURITY .

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo cp /mnt/nist_dataleak_pc_dd2/Windows/System32/config/SOFTWARE .

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo cp /mnt/nist_dataleak_pc_dd2/Windows/System32/config/SYSTEM .

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ ls -l
total 21031940
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 21474836480 Apr 21  2015 cfreds_2015_data_leakage_pc.dd
-rwxr-x--- 1 root           root                262144 Jun  5 06:38 DEFAULT
-rwxr-x--- 1 root           root                262144 Jun  5 06:39 SAM
-rwxr-x--- 1 root           root                262144 Jun  5 06:39 SECURITY
-rwxr-x--- 1 root           root              48496640 Jun  5 06:39 SOFTWARE
-rwxr-x--- 1 root           root              12582912 Jun  5 06:39 SYSTEM
```

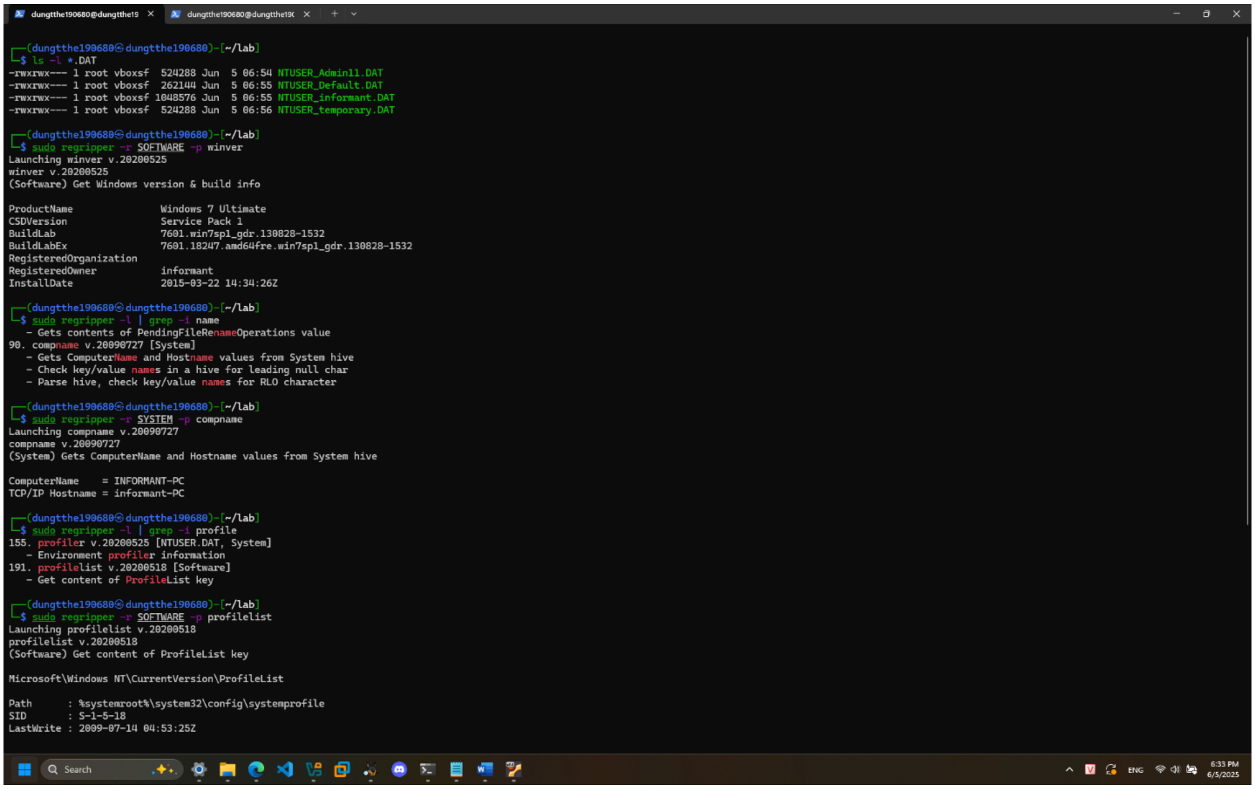
Step 3:



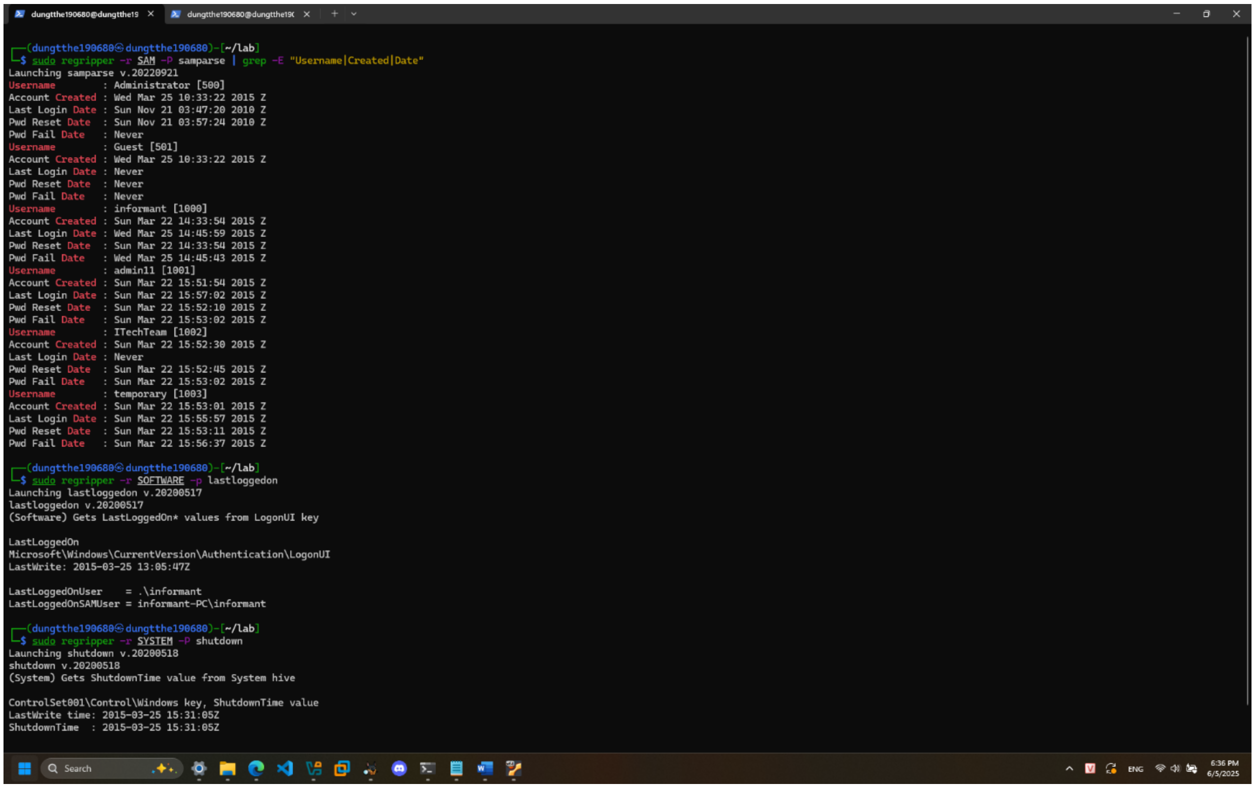
```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ ls -l cfreds_2015_data_leakage_pc.dd
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 21474836480 Apr 21  2015 cfreds_2015_data_leakage_pc.dd

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ md5sum cfreds_2015_data_leakage_pc.dd
e55bd9dc04b50d53d4242d0c7f497946  cfreds_2015_data_leakage_pc.dd

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sha1sum cfreds_2015_data_leakage_pc.dd
bcbd7c525eb1f033542182a26a0f212ffd280abd  cfreds_2015_data_leakage_pc.dd

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ 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

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ mmls cfreds_2015_data_leakage_pc.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

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

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ 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
```



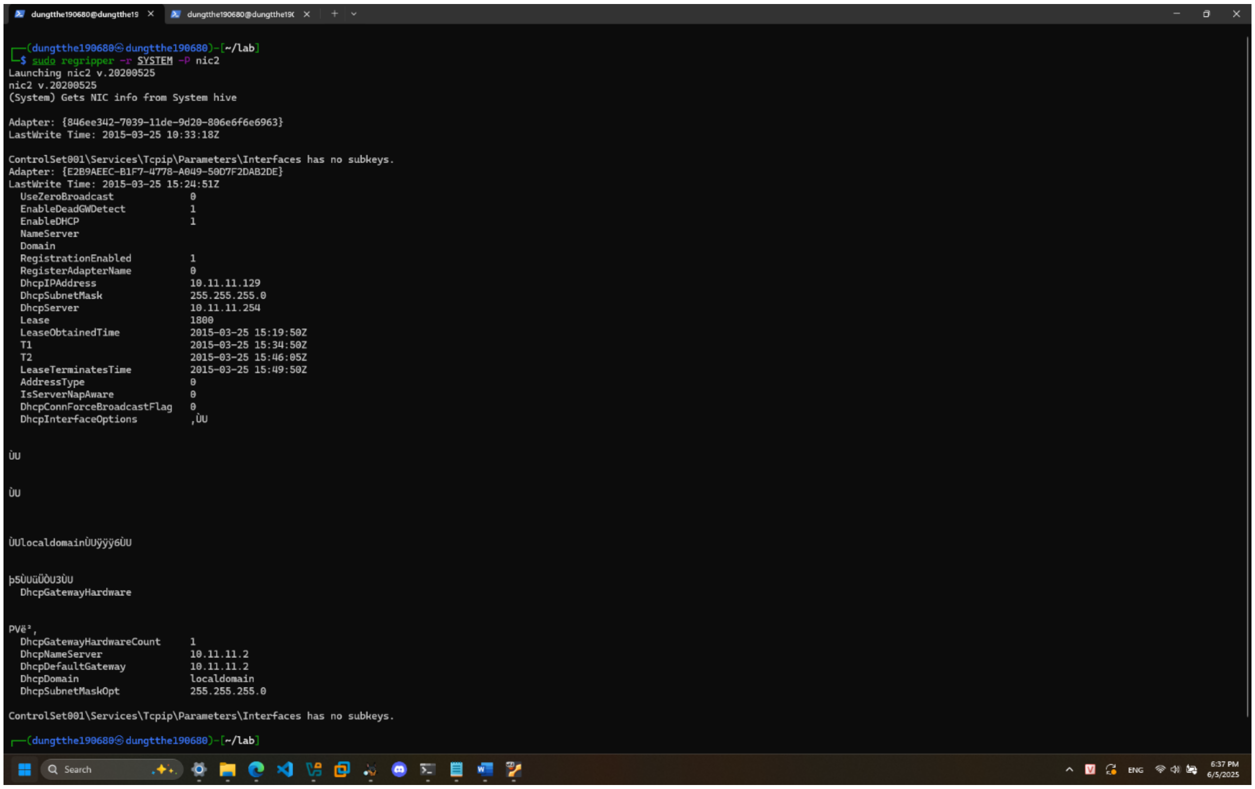
```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ fsstat -b 512 -o 206848 cfreds_2015_data_leakage_pc.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: C8CA0C8DCA0C7A48
OEM Name: NTFS
Version: Windows XP

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

$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

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ fls -rdF -o 206848 cfreds_2015_data_leakage_pc.dd | grep .docx
r/- * 0:        Users/informant/AppData/Roaming/Microsoft/Templates/LiveContent/15/Managed/Word Document Building Blocks/1033/TM02835270[[fn=Photo Sidebar (Annual Report Red and Black design)]].docx
r/- * 0:        Users/informant/Desktop/~$signation_Letter_(Iaman_Informant).docx

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ ls -l
total 21031940
-rw-rw-r-- 1 dungtthe190680 dungtthe190680 21474836480 Apr 21  2015 cfreds_2015_data_leakage_pc.dd
-rwxr-x--- 1 root           root                262144 Jun  5 06:38 DEFAULT
-rwxr-x--- 1 root           root                262144 Jun  5 06:39 SAM
-rwxr-x--- 1 root           root                262144 Jun  5 06:39 SECURITY
-rwxr-x--- 1 root           root              48496640 Jun  5 06:39 SOFTWARE
-rwxr-x--- 1 root           root              12582912 Jun  5 06:39 SYSTEM
```



```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ ls -l *.DAT
-rwxrwx--- 1 root vboxsf  524288 Jun  5 06:54 NTUSER_Admin11.DAT
-rwxrwx--- 1 root vboxsf  262144 Jun  5 06:55 NTUSER_Default.DAT
-rwxrwx--- 1 root vboxsf 1048576 Jun  5 06:55 NTUSER_informant.DAT
-rwxrwx--- 1 root vboxsf  524288 Jun  5 06:56 NTUSER_temporary.DAT

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -r SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName               Windows 7 Ultimate
CSDVersion                Service Pack 1
BuildLab                  7601.win7sp1_gdr.130828-1532
BuildLabEx                7601.18247.amd64fre.win7sp1_gdr.130828-1532
RegisteredOrganization
RegisteredOwner           informant
InstallDate               2015-03-22 14:34:26Z

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -l | grep -i name
   - Gets contents of PendingFileRenameOperations value
90. compname v.20090727 [System]
   - Gets ComputerName and Hostname values from System hive
   - Check key/value names in a hive for leading null char
   - Parse hive, check key/value names for RLO character

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -r SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = INFORMANT-PC
TCP/IP Hostname = informant-PC

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -l | grep -i profile
155. profiler v.20200525 [NTUSER.DAT, System]
   - Environment profiler information
191. profilelist v.20200518 [Software]
   - Get content of ProfileList key

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -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 : 2009-07-14 04:53:25Z
```



```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -r SAM -P samparse | grep -E "Username|Created|Date"
Launching samparse v.20220921
Username        : Administrator [500]
Account Created : Wed Mar 25 10:33:22 2015 Z
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 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 14:45:59 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        : admin11 [1001]
Account Created : Sun Mar 22 15:51:54 2015 Z
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date  : Sun Mar 22 15:52:10 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
Username        : temporary [1003]
Account Created : Sun Mar 22 15:53:01 2015 Z
Last Login Date : Sun Mar 22 15:55:57 2015 Z
Pwd Reset Date  : Sun Mar 22 15:53:11 2015 Z
Pwd Fail Date   : Sun Mar 22 15:56:37 2015 Z

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -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-PC\informant

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -r SYSTEM -P shutdown
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
```



```
┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
└─$ sudo regripper -r SYSTEM -P nic2
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive

Adapter: {846ee342-7039-11de-9d20-806e6f6e6963}
LastWrite Time: 2015-03-25 10:33:18Z

ControlSet001\Services\Tcpip\Parameters\Interfaces has no subkeys.
Adapter: {E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}
LastWrite Time: 2015-03-25 15:24:51Z
  UseZeroBroadcast              0
  EnableDeadGWDetect            1
  EnableDHCP                    1
  NameServer
  Domain
  RegistrationEnabled           1
  RegisterAdapterName           0
  DhcpIPAddress                 10.11.11.129
  DhcpSubnetMask                255.255.255.0
  DhcpServer                    10.11.11.254
  Lease                         1800
  LeaseObtainedTime             2015-03-25 15:19:50Z
  T1                            2015-03-25 15:34:50Z
  T2                            2015-03-25 15:46:05Z
  LeaseTerminatesTime           2015-03-25 15:49:50Z
  AddressType                   0
  IsServerNapAware              0
  DhcpConnForceBroadcastFlag    0
  DhcpInterfaceOptions          ,ÙU


ÙU


ÙU



ÙUlocaldomainÙUÿÿÿ6ÙU


þ5ÙUüÛÒU3ÙU
  DhcpGatewayHardware


PVë²,
  DhcpGatewayHardwareCount      1
  DhcpNameServer                10.11.11.2
  DhcpDefaultGateway            10.11.11.2
  DhcpDomain                    localdomain
  DhcpSubnetMaskOpt             255.255.255.0

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

┌──(dungtthe190680㉿dungtthe190680)-[~/lab]
```

- Installed OS information in detail:

- ProductName: Windows 7 Ultimate
- CSDVersion: Service Pack 1
- BuildLab: 7601.win7sp1_gdr.130828-1532
- BuildLabEx: 7601.18247.amd64fre.win7sp1_gdr.130828-1532
- RegisteredOrganization:
- RegisteredOwner: informant
- InstallDate: 2015-03-22 14:34:26

- Computer name: INFORMANT-PC.

- The system has 6 accounts.

- Security Accounts Manager (SAM) information:

- Administrator (500)
- Guest (501)
- informant (1000)
- admin11 (1001)
- ITechTeam (1002)
- temporary (1003)

- Login time: 2015-03-25 13:05:47Z

- Last user to logon into PC: informant

- Last recorded shutdown date/time: 2015-03-25 15:31:05Z

- Explain the information of network interface(s) with an IP address assigned by DHCP: Network interface (nic2) has IP 10.11.11.129, subnet mask 255.255.255.0, DHCP server 10.11.11.254. DHCP enabled, dead gateway detection enabled, registration enabled, zero broadcast disabled. Last write time: 2015-03-25 15:24:51Z.