lscdLab 7: Recycle Bin and Anti-forensics

What You Need for this lab

- Install Virtualbox : https://www.virtualbox.org/wiki/Downloads
- Install Kali 2021.4. : https://old.kali.org/kali-images/kali-2021.4/
  - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
- Image "cfreds_2015_data_leakage_pc.dd" from Lab 5

1. Recycle Bin

Step 1.

- Examine 'Recycle Bin' data in PC.

```
┌──(duanhn㉿duanhn)-[~/lab5]
└─$ fls -rd -o 206848 cfreds_2015_data_leakage_pc.dd | grep -Ei "Recycle" | head
r/- * 0:        $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-1000/deskt
op.ini
-/r * 74311-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$I55Z163
-/r * 74312-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$IXWGVWC
-/r * 74313-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$I40295N
-/r * 74395-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$I9M7UMY
-/r * 74398-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RIQGWTT.ini
-/r * 74418-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RJEMT64.exe
-/r * 74418-128-4:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RJEMT64.exe:Zone.Identifier
-/r * 74620-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RKXD1U3.jpg
-/r * 74625-128-1:      $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RI3FM2A.jpg
```

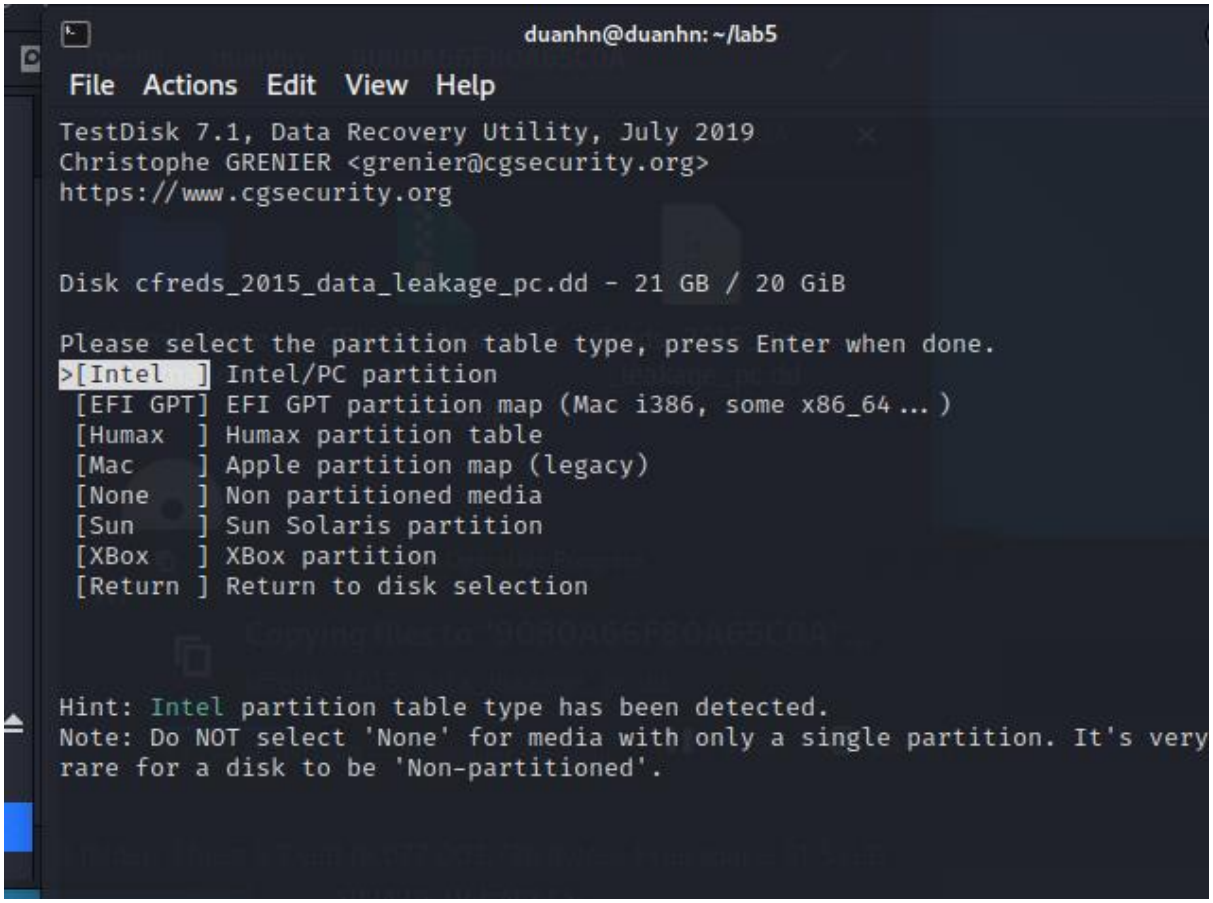
Step 2.

- Use *testdisk* to Recover *$Recyle.bin*

  Recover the image

```
┌──(duanhn㉿duanhn)-[~/lab5]
└─$ testdisk cfreds_2015_data_leakage_pc.dd
```

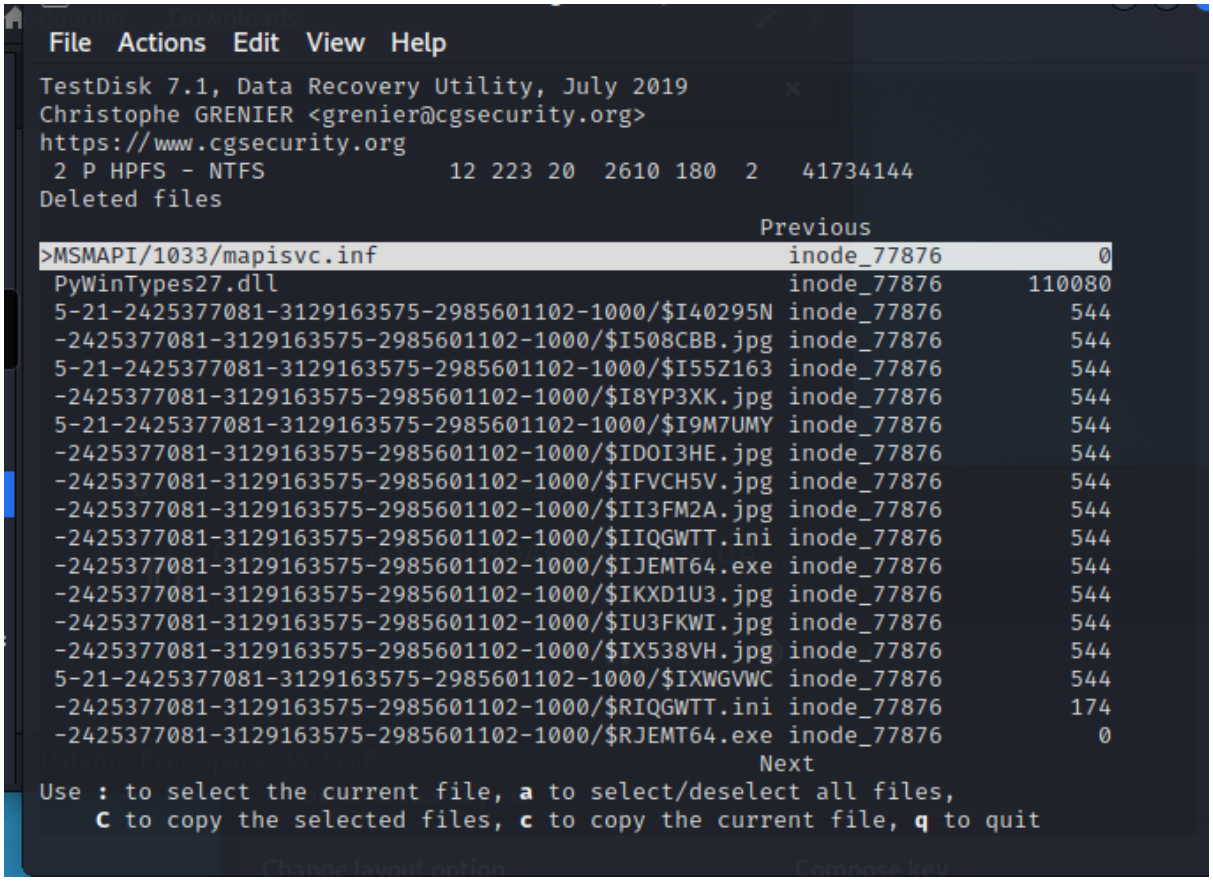

File Actions Edit View Help
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter):
>Disk cfreds_2015_data_leakage_pc.dd - 21 GB / 20 GiB


duanhn@duanhn: ~/lab5
File Actions Edit View Help
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
Disk cfreds_2015_data_leakage_pc.dd - 21 GB / 20 GiB
Please select the partition table type, press Enter when done.
>[Intel] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64 ...)
[Humax] Humax partition table
[Mac] Apple partition map (legacy)
[None] Non partitioned media
[Sun] Sun Solaris partition
[XBox] XBox partition
[Return] Return to disk selection
Hint: Intel partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.

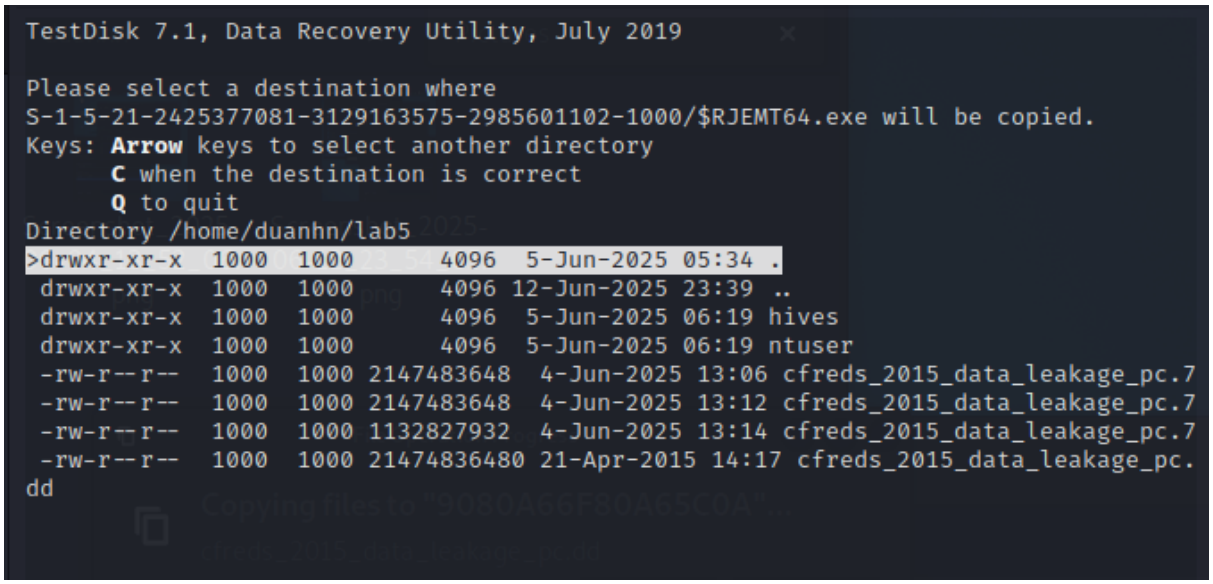
```
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org


Disk cfreds_2015_data_leakage_pc.dd - 21 GB / 20 GiB
     CHS 2611 255 63 - sector size=512

 [ Analyse  ] Analyse current partition structure and search for lost partitions
>[ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ MBR Code ] Write TestDisk MBR code to first sector
 [ Delete   ] Delete all data in the partition table
 [ Quit     ] Return to disk selection


Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

```
duanhn@duanhn: ~/lab5
File  Actions  Edit  View  Help
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk cfreds_2015_data_leakage_pc.dd - 21 GB / 20 GiB - CHS 2611 255 63

     Partition                  Start        End    Size in sectors
  1 * HPFS - NTFS              0  32 33    12 223 19     204800 [System Reserved]
> 2 P HPFS - NTFS             12 223 20  2610 180  2   41734144
```

– Use testDisk to recover files



– Choose the destination and copy



Quit all

ls S-1-5-21-2425377081-3129163575-2985601102-1000/ -l

```
┌──(duanhn㉿duanhn)-[~/lab5/restore]
└─$ ls S-1-5-21-2425377081-3129163575-2985601102-1000/ -l
total 60
-rw------- 1 root root 544 Mar 24  2015 '$I40295N'
-rw------- 1 root root 544 Mar 24  2015 '$I508CBB.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$I55Z163'
-rw------- 1 root root 544 Mar 24  2015 '$I8YP3XK.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$I9M7UMY'
-rw------- 1 root root 544 Mar 24  2015 '$IDOI3HE.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$IFVCH5V.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$II3FM2A.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$IIQGWTT.ini'
-rw------- 1 root root 544 Mar 24  2015 '$IJEMT64.exe'
-rw------- 1 root root 544 Mar 24  2015 '$IKXD1U3.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$IU3FKWI.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$IX538VH.jpg'
-rw------- 1 root root 544 Mar 24  2015 '$IXWGVWC'
-rw------- 1 root root 174 Mar 24  2015 '$RIQGWTT.ini'

┌──(duanhn㉿duanhn)-[~/lab5/restore]
└─$
```

– Match random file names with readable file names in the file

```
File  Actions  Edit  View  Help
└─$ strings -h
Usage: strings [option(s)] [file(s)]
 Display printable strings in [file(s)] (stdin by default)
 The options are:
  -a - --all                Scan the entire file, not just the data section [defaul
t]
  -d --data                 Only scan the data sections in the file
  -f --print-file-name      Print the name of the file before each string
  -n --bytes=[number]       Locate & print any NUL-terminated sequence of at
  -<number>                   least [number] characters (default 4).
  -t --radix={o,d,x}        Print the location of the string in base 8, 10 or 16
  -w --include-all-whitespace Include all whitespace as valid string characters
  -o                        An alias for --radix=o
  -T --target=<BFDNAME>     Specify the binary file format
  -e --encoding={s,S,b,l,B,L} Select character size and endianness:
                            s = 7-bit, S = 8-bit, {b,l} = 16-bit, {B,L} = 32-bit
  -s --output-separator=<string> String used to separate strings in output.
  @<file>                   Read options from <file>
  -h --help                 Display this information
  -v -V --version           Print the program's version number
strings: supported targets: elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 pei-i3
86 pe-x86-64 pei-x86-64 elf64-l1om elf64-k1om elf64-little elf64-big elf32-little e
lf32-big pe-bigobj-x86-64 pe-i386 srec symbolsrec verilog tekhex binary ihex plugin
Report bugs to <https://www.sourceware.org/bugzilla/>
```

ed: Today at 01:53:11 AM

Examine 'Recycle Bin' data in PC :

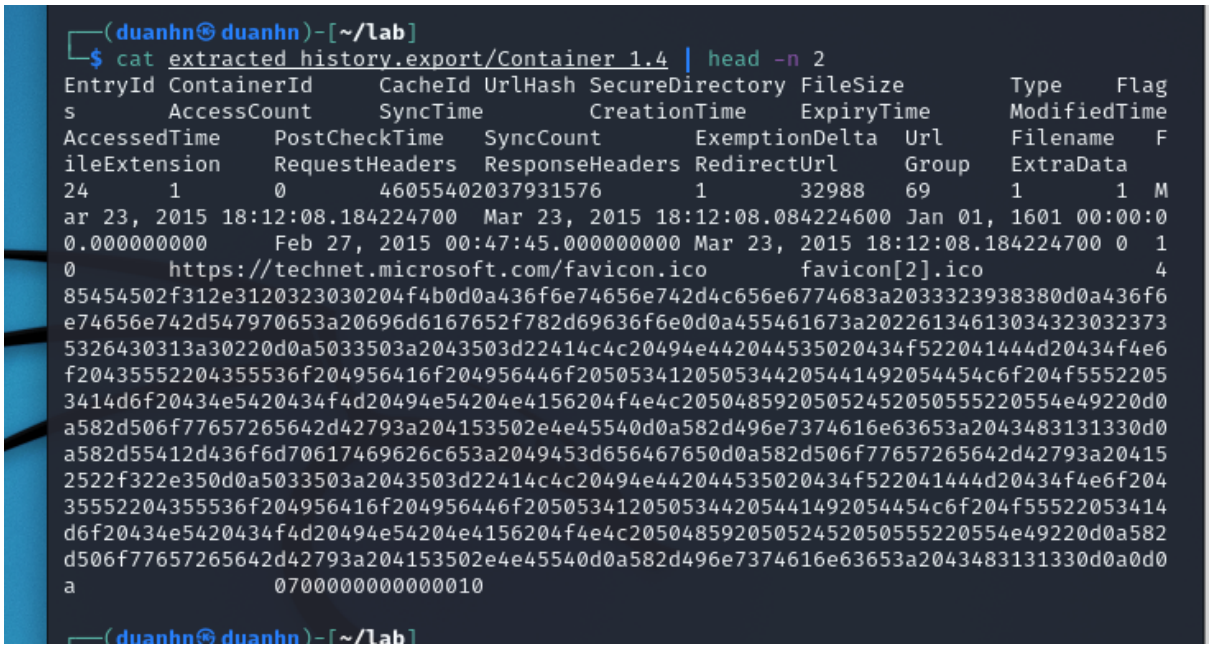
$I Name	Timestamp Deleted	Original File (or Directory) Path
$I40295N	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop
'$I55Z163'	2015-03-24 / 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd

$I9M7UMY	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr

2. What actions were performed for anti-forensics on PC at the last day '2015-03-25'?

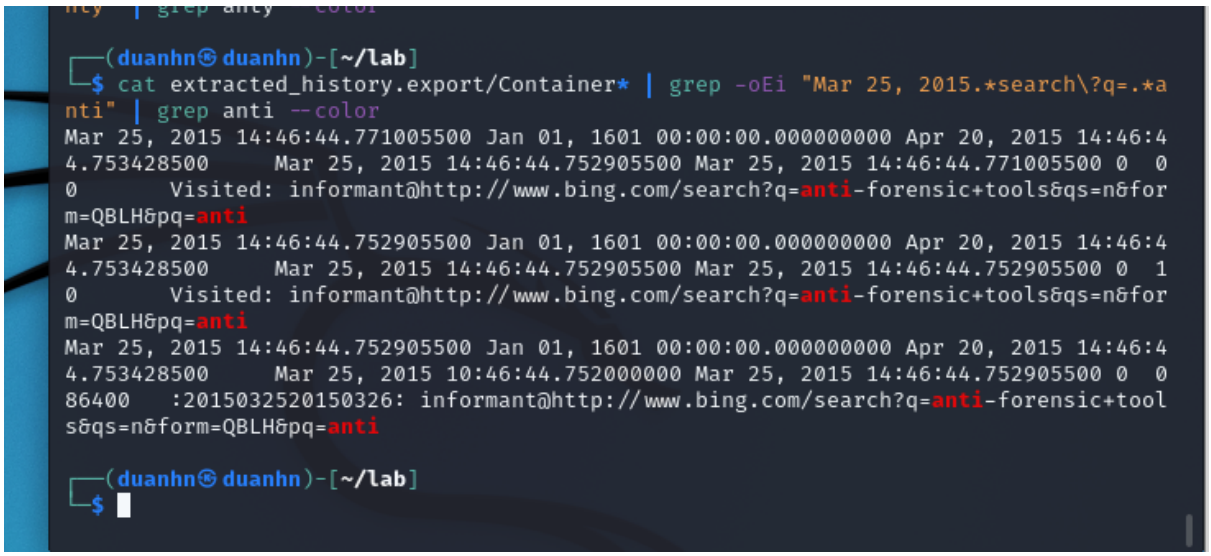
Step 1.

– Search IE anti-forensics using keyword



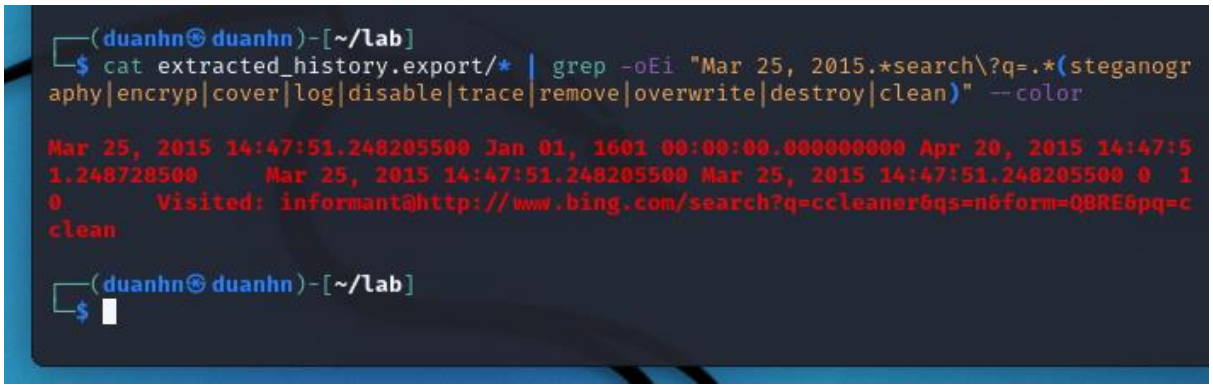
Three tasks:

1. Show all IE history
2. Grep date and with key word "anti"
3. Highlight anti in red



– Search a list of anti-forensic keywords :

cat webhistory/IE11.export/Container* | grep -oEi "Mar 25, 2015.*search\?q=.*(steganography|encryp|cover|log|diable|trace|cover|remove|overwrite|destroy|clean)"

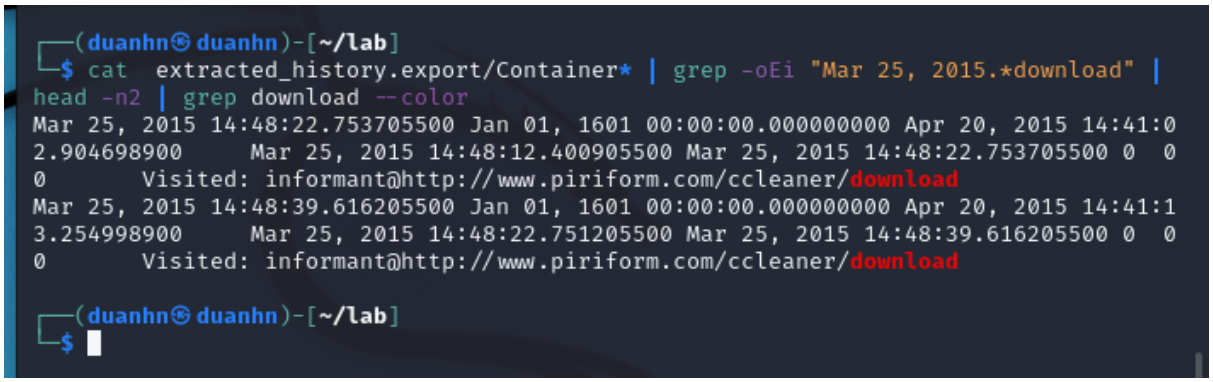


Step 2.

– Search IE download history

Search key word "*download*", only show first two records for the demonstration purpose :

cat webhistory/IE11.export/Container* | grep -oEi "Mar 25, 2015.*download" | head -n2 | grep download --color



– Search key word "*download*", only show last four records for the demonstration purpose

```
┌──(duanhn㉿duanhn)-[~/lab]
└─$ cat extracted_history.export/Container* | grep -oEi "Mar 25, 2015.*download" | t
ail -n4 | grep download --color
Mar 25, 2015 14:47:29.852305500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:47:2
9.850328500     Mar 25, 2015 10:47:29.849000000 Mar 25, 2015 14:47:29.852305500 0  0
86400   :2015032520150326: informant@http://sourceforge.net/projects/eraser/files/Er
aser%206/6.2/Eraser%206.2.0.2962.exe/download
Mar 25, 2015 14:48:22.753705500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:41:1
3.254998900     Mar 25, 2015 10:48:22.751205500 Mar 25, 2015 14:48:22.753705500 0  0
86400   :2015032520150326: informant@http://www.piriform.com/ccleaner/download
Mar 25, 2015 14:48:12.403405500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:41:0
2.904698900     Mar 25, 2015 10:48:12.400905500 Mar 25, 2015 14:48:12.403405500 0  0
86400   :2015032520150326: informant@http://www.piriform.com/ccleaner/download
Mar 25, 2015 14:47:35.008505500 iedownload      M       C:\\Users\\informant\\AppDat
a\\Roaming\\Microsoft\\Windows\\IEDownload

┌──(duanhn㉿duanhn)-[~/lab]
└─$
```

Step 3.

– Install download programs- *shimcache*

Check *shimcache* to monitor executed programs

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r SYSTEM -p shimcache | grep 2015-03-25
Launching shimcache v.20220921
LastWrite Time: 2015-03-25 15:31:05Z
C:\Users\informant\Desktop\Download\ccsetup504.exe  2015-03-25 14:48:28  Executed
C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe  2015-03-25 14:47:40  Exec
uted
C:\Users\INFORM~1\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40_Full_setup
.exe  2015-03-25 14:50:15  Executed
LastWrite Time: 2015-03-25 10:18:30Z
```

– Check if *eraser* or *cclearner* is managed by Win installer

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r SOFTWARE -p installer | grep -Ei "eraser|cclearn" -A 1 -B 2
Launching installer v.20200517
Key       : 1F782E6C74E20F54BB15498F51FCBF84
LastWrite: 2015-03-25 14:57:31Z
20150325 - Eraser 6.2.0.2962 6.2.2962 (The Eraser Project)
```

– Check Software registry hive

rip.pl -r SOFTWARE -p uninstall | grep 2015-03-25 -A 2 -B 2

rip.pl -r NTUSER_informant.DAT -p uninstall | grep 2015-03-25 -A 2 -B 2

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r SOFTWARE -p uninstall | grep 2015-03-25 -A 1 -B 2
Launching uninstall v.20200525
Microsoft\Windows\CurrentVersion\Uninstall

2015-03-25 14:57:31Z
  Eraser 6.2.0.2962 v.6.2.2962

2015-03-25 14:54:33Z
  Microsoft .NET Framework 4 Extended v.4.0.30319

2015-03-25 14:54:06Z
  Microsoft .NET Framework 4 Extended v.4.0.30319

2015-03-25 14:52:06Z
  Microsoft .NET Framework 4 Client Profile v.4.0.30319

2015-03-25 14:51:39Z
  Microsoft .NET Framework 4 Client Profile v.4.0.30319

2015-03-25 10:15:21Z
  DXM_Runtime

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

– Check *NTUSER_informant.DAT* registry hive

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r NTUSER informant.DAT  -p uninstall
Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hiv
es

Uninstall
```

Nothing found

– Check app paths registry

Check Software apppaths

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r SOFTWARE -p apppaths | grep 2015-03-25 -A 1 -B 2
Launching apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys

2015-03-25 14:57:31Z
  Eraser.exe - C:\Program Files\Eraser\Eraser.exe
2015-03-25 11:14:17Z
  cmmgr32.exe -

┌──(duanhn㉿duanhn)-[~/lab/ntuser]
```

Check NTUSER_informant apppaths

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r NTUSER_informant.DAT  -p apppaths
Launching apppaths v.20200511
apppaths v.20200511
(NTUSER.DAT,Software) Gets content of App Paths subkeys
```

Step 4

– Execute two programs : *userassist*

```
┌──(duanhn㉿duanhn)-[~/lab/ntuser]
└─$ ./rip.pl -r NTUSER_informant.DAT -p userassist | grep 2015-03-25 -A 1 --color
Launching userassist v.20170204
2015-03-25 15:28:47Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe (1)
2015-03-25 15:24:48Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\WINWORD.EXE (4)
2015-03-25 15:21:30Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Google\Drive\googledrivesync.exe (1)
2015-03-25 15:15:50Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\CCleaner\CCleaner64.exe (1)
2015-03-25 15:12:28Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Eraser\Eraser.exe (1)
2015-03-25 14:57:56Z
  C:\Users\informant\Desktop\Download\ccsetup504.exe (1)
2015-03-25 14:50:14Z
  C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe (1)
2015-03-25 14:46:05Z
  Microsoft.InternetExplorer.Default (5)
2015-03-25 14:42:47Z
  Microsoft.Windows.MediaPlayer32 (1)
2015-03-25 14:41:03Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\OUTLOOK.EXE (5)
--
2015-03-25 15:21:30Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Google Drive\Google Drive.lnk (1)
2015-03-25 15:15:50Z
  C:\Users\Public\Desktop\CCleaner.lnk (1)
2015-03-25 15:12:28Z
  C:\Users\Public\Desktop\Eraser.lnk (1)
2015-03-25 14:46:05Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer.lnk (5)
2015-03-25 14:42:47Z
  {9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Media Player.lnk (1)
2015-03-25 14:41:03Z
  {0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Outlook 2013.lnk (5)
```

Step 5

Search for deleted *.exe* files

Only search for 2015-03-25 from Download folder

fls -rd -o 206848 cfreds_2015_data_leakage_pc.dd -l | grep -i Users/informant/Desktop/Download/ | grep 2015-03-25 --color

```
┌──(duanhn㉿duanhn)-[~/lab]
└─$ fls -rd -o 206848 cfreds_2015_data_leakage_pc.dd -l | grep -i Users/informant/Desktop/Download/ | grep 2015-03-
25 --color
-/r * 75101-128-4:      Users/informant/Desktop/Download/Eraser 6.2.0.2962.exe  2015-03-25 10:47:40 (EDT)       201
5-03-25 10:47:40 (EDT)  2015-03-25 10:47:40 (EDT)       2015-03-25 10:47:40 (EDT)       8317032 0       0
-/r * 75101-128-5:      Users/informant/Desktop/Download/Eraser 6.2.0.2962.exe:Zone.Identifier  2015-03-25 10:47:40
 (EDT)  2015-03-25 10:47:40 (EDT)       2015-03-25 10:47:40 (EDT)       2015-03-25 10:47:40 (EDT)       26      0 0
-/r * 75186-128-4:      Users/informant/Desktop/Download/ccsetup504.exe 2015-03-25 10:48:28 (EDT)       2015-03-25
10:48:28 (EDT)  2015-03-25 10:48:28 (EDT)       2015-03-25 10:48:28 (EDT)       5344528 0       0
-/r * 75186-128-5:      Users/informant/Desktop/Download/ccsetup504.exe:Zone.Identifier 2015-03-25 10:48:28 (EDT) 2
015-03-25 10:48:28 (EDT)        2015-03-25 10:48:28 (EDT)       2015-03-25 10:48:28 (EDT)       26      0       0

┌──(duanhn㉿duanhn)-[~/lab]
└─$
```

– Only search for deleted *.exe* from *$UsnJrnl* on 2015-03-25

```
└─$ grep -Ei "\.exe.*2015-03-25.*delete" UsnJrnl2Csv/UsnJrnl_2025-06-19_10-17-49.csv --color
0×03E0C358|Eraser 6.2.0.2962.exe|65061720|2015-03-25 14:47:40.1253055|CLOSE+FILE_DELETE|75101|2|22273|3|archive|2|0|0×00000000|0
0×03E0C8F8|Eraser%206.2.0.2962[1].exe|65063160|2015-03-25 14:47:40.2033055|CLOSE+FILE_DELETE|75100|1|70424|1|archive+not_indexed|2|0|0×00000
000|0
0×03E19808|ccsetup504.exe|65116168|2015-03-25 14:48:28.8054055|CLOSE+FILE_DELETE|75186|1|22273|3|archive|2|0|0×00000000|0
0×03E19C80|ccsetup504[1].exe|65117312|2015-03-25 14:48:28.8678055|CLOSE+FILE_DELETE|75184|1|70423|1|archive+not_indexed|2|0|0×00000000|0
0×03E66AA8|TMPFF8D.tmp.exe|65432232|2015-03-25 14:50:47.3722055|CLOSE+FILE_DELETE|75477|3|75332|2|archive|2|0|0×00000000|0
0×03E66CD0|TMPFF8D.tmp.exe.tmp|65432784|2015-03-25 14:50:47.4658055|CLOSE+FILE_DELETE|75502|1|75332|2|directory+not_indexed|2|0|0×00000000|0
0×03E732C0|TMP5B99.tmp.exe|65483456|2015-03-25 14:50:55.6402055|CLOSE+FILE_DELETE|75559|6|75332|2|archive|2|0|0×00000000|0
0×03E736A0|TMP5B99.tmp.exe.tmp|65484448|2015-03-25 14:50:55.6402055|CLOSE+FILE_DELETE|75531|2|75332|2|directory+not_indexed|2|0|0×00000000|0
0×04067648|Microsoft.Workflow.Compiler.exe|67532360|2015-03-25 14:54:19.6102055|CLOSE+FILE_DELETE|77664|1|77663|2|normal|2|0|0×00000000|0
0×04103050|Setup.exe|68169808|2015-03-25 14:56:54.9550055|CLOSE+FILE_DELETE|75301|1|74869|5|normal|2|0|0×00000000|0
0×041030A0|SetupUtility.exe|68169888|2015-03-25 14:56:54.9550055|CLOSE+FILE_DELETE|75302|1|74869|5|normal|2|0|0×00000000|0
0×0410E708|dotNetFx40_Full_setup.exe|68216584|2015-03-25 14:57:49.2742055|CLOSE+FILE_DELETE|74812|5|70388|6|archive+not_indexed|2|0|0×000000
00|0
0×041252C0|$RJEMT64.exe|68309696|2015-03-25 15:14:45.0798055|CLOSE+FILE_DELETE|74418|7|15721|2|archive+not_indexed|2|0|0×00000000|0
0×04125318|$IJEMT64.exe|68309784|2015-03-25 15:14:45.0798055|CLOSE+FILE_DELETE|74761|3|15721|2|archive|2|0|0×00000000|0
0×04125B20|ccsetup504.exe|68311840|2015-03-25 15:15:45.4700055|CLOSE+FILE_DELETE|75186|2|22273|3|archive|2|0|0×00000000|0
0×04125B78|Eraser 6.2.0.2962.exe|68311928|2015-03-25 15:15:45.4700055|CLOSE+FILE_DELETE|75101|3|22273|3|archive|2|0|0×00000000|0
0×0412A448|CCleaner.exe|68330568|2015-03-25 15:18:36.9368055|CLOSE+FILE_DELETE|75248|3|75246|2|archive|2|0|0×00000000|0
0×0412A4A0|CCleaner64.exe|68330656|2015-03-25 15:18:36.9368055|CLOSE+FILE_DELETE|75250|2|75246|2|archive|2|0|0×00000000|0
0×0412A4F8|uninst.exe|68330744|2015-03-25 15:18:36.9524055|CLOSE+FILE_DELETE|75307|2|75246|2|archive|2|0|0×00000000|0
0×0424DCE0|ShellStreamsShortcut.exe|69524704|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74269|1|74268|1|archive|2|0|0×00000000|0
0×0424DEF0|iCloudIcon.exe|69525232|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74271|1|74268|1|archive|2|0|0×00000000|0
0×0424E000|MailIcon.exe|69525504|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74272|1|74268|1|archive|2|0|0×00000000|0
0×0424E118|ContactsIcon.exe|69525784|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74273|1|74268|1|archive|2|0|0×00000000|0
0×0424E238|CalendarIcon.exe|69526072|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74274|1|74268|1|archive|2|0|0×00000000|0
0×0424E368|FindMyiPhoneIcon.exe|69526376|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74275|1|74268|1|archive|2|0|0×00000000|0
0×0424E480|NotesIcon.exe|69526656|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74276|1|74268|1|archive|2|0|0×00000000|0
0×0424E598|RemindersIcon.exe|69526936|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74277|1|74268|1|archive|2|0|0×00000000|0
0×042724D0|main.exe.manifest|69674192|2015-03-25 15:23:00.8964055|CLOSE+FILE_DELETE|73720|2|6476|4|archive+not_indexed|2|0|0×00000000|0
```

What actions were performed for anti-forensics on PC at the last day '2015-03-25'?

Timestamp	Behavior	Description
2015-03-25 10:46:44	Search anti-forensic methods	anti-forensic tools
15:47:43	File Delete	Microsoft WorkFlow Compiler [exe] - application removal
6:46:59	File Delete	SetupUtility [exe] - setup file deletion
14:47:40	File Delete	Eraser v6.2.0.2962 [exe] - anti-forensic tool usage
15:47:13	File Delete	TMP files [tmp] - temporary file cleanup
14:48:28	File Delete	CCleaner v5.04 [exe] - anti-forensic tool usage

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 7.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 7 From YOUR NAME**", replacing "YOUR NAME" with your real name.