

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: $Recycle.Bin/S-1-5-21-2425377081-3129163575-2985601102-10
00/$RIQWTT.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 \$Recycle.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
System Volume - CFHVL2 Module 0 - cfreds_2015_data

[ 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

Copying files to "9080A66F80A65C0A"...
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

```

File Actions Edit View Help
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
2 P HPFS - NTFS 12 223 20 2610 180 2 41734144
Deleted files

Previous
>MSMAPI/1033/mapisvc.inf inode_77876 0
PyWinTypes27.dll inode_77876 110080
5-21-2425377081-3129163575-2985601102-1000/$I40295N inode_77876 544
-2425377081-3129163575-2985601102-1000/$I508CBB.jpg inode_77876 544
5-21-2425377081-3129163575-2985601102-1000/$I55Z163 inode_77876 544
-2425377081-3129163575-2985601102-1000/$I8YP3XK.jpg inode_77876 544
5-21-2425377081-3129163575-2985601102-1000/$I9M7UMY inode_77876 544
-2425377081-3129163575-2985601102-1000/$IDOI3HE.jpg inode_77876 544
-2425377081-3129163575-2985601102-1000/$IFVCH5V.jpg inode_77876 544
-2425377081-3129163575-2985601102-1000/$II3FM2A.jpg inode_77876 544
-2425377081-3129163575-2985601102-1000/$IIQGWTT.ini inode_77876 544
-2425377081-3129163575-2985601102-1000/$IJEMT64.exe inode_77876 544
-2425377081-3129163575-2985601102-1000/$IKXD1U3.jpg inode_77876 544
-2425377081-3129163575-2985601102-1000/$IU3FKWI.jpg inode_77876 544
-2425377081-3129163575-2985601102-1000/$IX538VH.jpg inode_77876 544
5-21-2425377081-3129163575-2985601102-1000/$IXWGVWC inode_77876 544
-2425377081-3129163575-2985601102-1000/$RIQGWTT.ini inode_77876 174
-2425377081-3129163575-2985601102-1000/$RJEMT64.exe inode_77876 0

Next
Use : to select the current file, a to select/deselect all files,
C to copy the selected files, c to copy the current file, q to quit

```

- Choose the destination and copy

```

TestDisk 7.1, Data Recovery Utility, July 2019
Please select a destination where
S-1-5-21-2425377081-3129163575-2985601102-1000/$RJEMT64.exe will be copied.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory /home/duanhn/lab5
>drwxr-xr-x 1000 1000 4096 5-Jun-2025 05:34 .
drwxr-xr-x 1000 1000 4096 12-Jun-2025 23:39 ..
drwxr-xr-x 1000 1000 4096 5-Jun-2025 06:19 hives
drwxr-xr-x 1000 1000 4096 5-Jun-2025 06:19 ntuser
-rw-r--r-- 1000 1000 2147483648 4-Jun-2025 13:06 cfreds_2015_data_leakage_pc.7
-rw-r--r-- 1000 1000 2147483648 4-Jun-2025 13:12 cfreds_2015_data_leakage_pc.7
-rw-r--r-- 1000 1000 1132827932 4-Jun-2025 13:14 cfreds_2015_data_leakage_pc.7
-rw-r--r-- 1000 1000 21474836480 21-Apr-2015 14:17 cfreds_2015_data_leakage_pc.
dd

```

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-rw-rw- 1 root root 544 Mar 24 2015 '$I40295N'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$I508CBB.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$I55Z163'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$I8YP3XK.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$I9M7UMY'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$ID0I3HE.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IFVCH5V.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$II3FM2A.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IIQGWTT.ini'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IJEMT64.exe'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IKXD1U3.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IU3FKWI.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IX538VH.jpg'
-rw-rw-rw- 1 root root 544 Mar 24 2015 '$IXWGVWC'
-rw-rw-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 [default]
-t                Only scan the data sections in the file
-d --data
-f --print-file-name Print the name of the file before each string
-n --bytes=[number] Locate & print any NUL-terminated sequence of at
                    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 --tabsize=[N] Specify the binary file format
-e --encoding={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 --version      Print the program's version number
strings: supported targets: elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 pei-i386
pe-x86-64 pei-x86-64 elf64-l1om elf64-k1om elf64-little elf64-big elf32-little elf32-big
pe-bigobj-x86-64 pe-i386 srec symbolsrec verilog tekhex binary ihex plugin
Report bugs to <https://www.sourceware.org/bugzilla/>

(duanhn@duanhn) - [~/lab5/restore]
```

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

```
(duanh@duanh)-[~/lab]
$ cat extracted_history.export/Container 1.4 | head -n 2
EntryId ContainerId CacheId UrlHash SecureDirectory FileSize Type Flag
s AccessCount SyncTime CreationTime ExpiryTime ModifiedTime
AccessedTime PostCheckTime SyncCount ExemptionDelta Url Filename F
ileExtension RequestHeaders ResponseHeaders RedirectUrl Group ExtraData
24 1 0 46055402037931576 1 32988 69 1 1 M
ar 23, 2015 18:12:08.184224700 Mar 23, 2015 18:12:08.084224600 Jan 01, 1601 00:00:0
0.000000000 Feb 27, 2015 00:47:45.000000000 Mar 23, 2015 18:12:08.184224700 0 1
0 https://technet.microsoft.com/favicon.ico favicon[2].ico 4
85454502f312e3120323030204f4b0d0a436f6e74656e742d4c656e6774683a2033323938380d0a436f6
e74656e742d547970653a20696d6167652f782d69636f6e0d0a455461673a20226134613034323032373
5326430313a30220d0a5033503a2043503d22414c4c20494e442044535020434f522041444d20434f4e6
f20435552204355536f204956416f204956446f2050534120505344205441492054454c6f204f5552205
3414d6f20434e5420434f4d20494e54204e4156204f4e4c20504859205052452050555220554e49220d0
a582d506f77657265642d42793a204153502e4e45540d0a582d496e7374616e63653a2043483131330d0
a582d55412d436f6d70617469626c653a2049453d656467650d0a582d506f77657265642d42793a20415
2522f322e350d0a5033503a2043503d22414c4c20494e442044535020434f522041444d20434f4e6f204
35552204355536f204956416f204956446f2050534120505344205441492054454c6f204f55522053414
d6f20434e5420434f4d20494e54204e4156204f4e4c20504859205052452050555220554e49220d0a582
d506f77657265642d42793a204153502e4e45540d0a582d496e7374616e63653a2043483131330d0a0d0
a 07000000000000010
(duanh@duanh)-[~/lab]
```

Three tasks:

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

```
(duanh@duanh)-[~/lab]
$ cat extracted_history.export/Container* | grep -oEi "Mar 25, 2015.*search?q=.*a
nti" | grep anti --color
Mar 25, 2015 14:46:44.771005500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:46:4
4.753428500 Mar 25, 2015 14:46:44.752905500 Mar 25, 2015 14:46:44.771005500 0 0
0 Visited: informant@http://www.bing.com/search?q=anti-forensic+tools&q=
m=QBLH&pq=anti
Mar 25, 2015 14:46:44.752905500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:46:4
4.753428500 Mar 25, 2015 14:46:44.752905500 Mar 25, 2015 14:46:44.752905500 0 1
0 Visited: informant@http://www.bing.com/search?q=anti-forensic+tools&q=
m=QBLH&pq=anti
Mar 25, 2015 14:46:44.752905500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:46:4
4.753428500 Mar 25, 2015 10:46:44.752000000 Mar 25, 2015 14:46:44.752905500 0 0
86400 :2015032520150326: informant@http://www.bing.com/search?q=anti-forensic+tool
s&q=
s&q=
s&q=
m=QBLH&pq=anti
(duanh@duanh)-[~/lab]
$
```

- Search a list of anti-forensic keywords :

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

```
(duanhn@duanhn)-[~/Lab]
$ cat extracted_history.export/* | grep -oEi "Mar 25, 2015.*search\?q=.*(steganography|encryp|cover|log|diab|trace|cover|remove|overwrite|destroy|clean)" --color
Mar 25, 2015 14:47:51.248205500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:47:51.248728500 Mar 25, 2015 14:47:51.248205500 Mar 25, 2015 14:47:51.248205500 0 1
0 Visited: informant@http://www.bing.com/search?q=ccleaner&q=nb&form=QBRE&pq=cclean
(duanhn@duanhn)-[~/Lab]
$
```

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

```
(duanhn@duanhn)-[~/Lab]
$ cat extracted_history.export/Container* | grep -oEi "Mar 25, 2015.*download" | head -n2 | grep download --color
Mar 25, 2015 14:48:22.753705500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:41:02.904698900 Mar 25, 2015 14:48:12.400905500 Mar 25, 2015 14:48:22.753705500 0 0
0 Visited: informant@http://www.piriform.com/ccleaner/download
Mar 25, 2015 14:48:39.616205500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:41:13.254998900 Mar 25, 2015 14:48:22.751205500 Mar 25, 2015 14:48:39.616205500 0 0
0 Visited: informant@http://www.piriform.com/ccleaner/download
(duanhn@duanhn)-[~/Lab]
$
```

- 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" | tail -n4 | grep download --color
Mar 25, 2015 14:47:29.852305500 Jan 01, 1601 00:00:00.000000000 Apr 20, 2015 14:47:29.850328500 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/Eraser%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 14:41:13.254998900 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 14:41:02.904698900 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 ie download M C:\Users\informant\AppDataa\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 Executed
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 *ccleaner* 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 hives
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) 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) 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) 5344528 0 0
-r * 75186-128-5: Users/informant/Desktop/Download/ccsetup504.exe:Zone.Identifier 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
0x03E0C358|Eraser 6.2.0.2962.exe|65061720|2015-03-25 14:47:40.1253055|CLOSE+FILE_DELETE|75101|2|22273|3|archive|2|0|0x00000000|0
0x03E0C8F8|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|0x00000000|0
0x03E19808|ccsetup504.exe|65116168|2015-03-25 14:48:28.8054055|CLOSE+FILE_DELETE|75186|1|22273|3|archive|2|0|0x00000000|0
0x03E19C80|ccsetup504|1|.exe|65117312|2015-03-25 14:48:28.8678055|CLOSE+FILE_DELETE|75184|1|70423|1|archive+not_indexed|2|0|0x00000000|0
0x03E66AA8|TMPFF8D.tmp.exe|65432232|2015-03-25 14:50:47.3722055|CLOSE+FILE_DELETE|75477|3|75332|2|archive|2|0|0x00000000|0
0x03E66CD0|TMPFF8D.tmp.exe.tmp|65432784|2015-03-25 14:50:47.4658055|CLOSE+FILE_DELETE|75502|1|75332|2|directory+not_indexed|2|0|0x00000000|0
0x03E732C0|TMP5899.tmp.exe|65483456|2015-03-25 14:50:55.6402055|CLOSE+FILE_DELETE|75559|6|75332|2|archive|2|0|0x00000000|0
0x03E736A0|TMP5899.tmp.exe.tmp|65484448|2015-03-25 14:50:55.6402055|CLOSE+FILE_DELETE|75531|2|75332|2|directory+not_indexed|2|0|0x00000000|0
0x04067648|Microsoft.Workflow.Compiler.exe|67532360|2015-03-25 14:54:19.6102055|CLOSE+FILE_DELETE|77664|1|77663|2|normal|2|0|0x00000000|0
0x04103050|Setup.exe|68169808|2015-03-25 14:56:54.9550055|CLOSE+FILE_DELETE|75301|1|74869|5|normal|2|0|0x00000000|0
0x041030A0|SetupUtility.exe|68169808|2015-03-25 14:56:54.9550055|CLOSE+FILE_DELETE|75302|1|74869|5|normal|2|0|0x00000000|0
0x0410E708|dotNetFx40_Full_setup.exe|68216584|2015-03-25 14:57:49.2742055|CLOSE+FILE_DELETE|74812|5|70388|6|archive+not_indexed|2|0|0x00000000|0
0x041252C0|$RJEMT64.exe|68309696|2015-03-25 15:14:45.0798055|CLOSE+FILE_DELETE|74418|7|15721|2|archive+not_indexed|2|0|0x00000000|0
0x04125318|$IJEMT64.exe|68309784|2015-03-25 15:14:45.0798055|CLOSE+FILE_DELETE|74761|3|15721|2|archive|2|0|0x00000000|0
0x04125B20|ccsetup504.exe|68311840|2015-03-25 15:15:45.4700055|CLOSE+FILE_DELETE|75186|2|22273|3|archive|2|0|0x00000000|0
0x04125B78|Eraser 6.2.0.2962.exe|68311920|2015-03-25 15:15:45.4700055|CLOSE+FILE_DELETE|75101|3|22273|3|archive|2|0|0x00000000|0
0x0412A448|CCleaner.exe|68330560|2015-03-25 15:18:36.9368055|CLOSE+FILE_DELETE|75248|3|75246|2|archive|2|0|0x00000000|0
0x0412A4A0|CCleaner64.exe|68330656|2015-03-25 15:18:36.9368055|CLOSE+FILE_DELETE|75250|2|75246|2|archive|2|0|0x00000000|0
0x0412A4F8|uninst.exe|68330744|2015-03-25 15:18:36.9524055|CLOSE+FILE_DELETE|75307|2|75246|2|archive|2|0|0x00000000|0
0x0424DCE0|ShellStreamsShortcut.exe|69524704|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74269|1|74268|1|archive|2|0|0x00000000|0
0x0424DEF0|iCloudIcon.exe|69525232|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74271|1|74268|1|archive|2|0|0x00000000|0
0x0424E000|MailIcon.exe|69525504|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74272|1|74268|1|archive|2|0|0x00000000|0
0x0424E118|ContactsIcon.exe|69525784|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74273|1|74268|1|archive|2|0|0x00000000|0
0x0424E238|CalendarIcon.exe|69526072|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74274|1|74268|1|archive|2|0|0x00000000|0
0x0424E368|FindMyiPhoneIcon.exe|69526376|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74275|1|74268|1|archive|2|0|0x00000000|0
0x0424E480|NotesIcon.exe|69526656|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74276|1|74268|1|archive|2|0|0x00000000|0
0x0424E598|RemindersIcon.exe|69526936|2015-03-25 15:19:16.9906055|CLOSE+FILE_DELETE|74277|1|74268|1|archive|2|0|0x00000000|0
0x042724D0|main.exe.monifest|69674192|2015-03-25 15:23:00.8984055|CLOSE+FILE_DELETE|73720|2|6476|4|archive+not_indexed|2|0|0x00000000|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.