DOGGY INVESTIGATION TOOLKIT:

Acquisition Tools:

1. DD

This is a famous Forensic copying tool.

The basic purpose of this command is to transfer data from one drive to another while also making sure that the data itself is not changed.

The ability of this tool to accurately move data from one device to another makes it a popular tool for backing up your data.

Usage:

- If=DEST: This parameter takes the file from the destination DEST.
- of=DEST: This parameter saves the file to the destination DEST.
- If=DEST: | split -b 1000m: This parameter splits the disk into multiple files.

Example:

dd if= C:\Users\<name>\Drive.1 of= C:\Users\<name>\Desktop\Drive.1_copy

2. Dcode

Dcode is a forensic utility designed to calculate date/time values from timestamps found inside data files

To download Dcode and learn more on how to use, visit website: https://www.digital-detective.net/dcode/

3. OfficeMalScanner

The purpose of the OfficeMalScanner is to scan Office documents and extract items such as shellcode and VBA macros. It can handle both doc and docx formats.

Getting Help:

Typing the command: officemalscanner.exe -h will display the help page for this program, See below.

```
+-------------------------------------------+
|           OfficeMalScanner v0.62          |
|  Frank Boldewin / www.reconstructer.org   |
+-------------------------------------------+

Usage:
------
OfficeMalScanner <PPT, DOC or XLS file> <scan | info> <brute> <debug>

Options:
  scan    - scan for several shellcode heuristics and encrypted PE-Files
  info    - dumps OLE structures, offsets+length and saves found VB-Macro code
  inflate - decompresses Ms Office 2007 documents, e.g. docx, into a temp dir
Switches: (only enabled if option "scan" was selected)
  brute - enables the "brute force mode" to find encrypted stuff
  debug - prints out disassembly resp hexoutput if a heuristic was found

Examples:
  OfficeMalScanner evil.ppt scan brute debug
  OfficeMalScanner evil.ppt scan
  OfficeMalScanner evil.ppt info

Malicious index rating:
  Executables: 20
  Code       : 10
  STRINGS    :  2
  OLE        :  1

--------------------------------------------------------------------------------
    I strongly suggest you to scan malicious files in a safe environment
 like VMWARE, as this tool is written in C and might have exploitable bugs!
--------------------------------------------------------------------------------
```

Scanning:

- Using the previous steps in the Exiftool, we will scan an .xml file and check for malicious code. We will type the following command in the following syntax:

OfficeMalScanner.exe <File-Directory> scan

```
C:\Windows\System32\cmd.exe
C:\Users\squidward\Desktop\OfficeMalScanner>OfficeMalScanner.exe "C:\Users\squidward\Downloads\module\Lab 6\test.xls" sc
an

+-------------------------------------------+
|           OfficeMalScanner v0.62          |
|  Frank Boldewin / www.reconstructer.org   |
+-------------------------------------------+

[*] SCAN mode selected
[*] Opening file C:\Users\squidward\Downloads\module\Lab 6\test.xls
[*] Filesize is 3072 (0xc00) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Scanning now...

FLDZ/FSTENV [esp-12] signature found at offset: 0x23c


Analysis finished!

---------------------------------------------------------
test.xls seems to be malicious! Malicious Index = 10
---------------------------------------------------------

C:\Users\squidward\Desktop\OfficeMalScanner>
```

- We can see that the file is malicious. Sometimes running the “scan” option doesn’t return us with results, we can then run “info” and hope for results.
- When we use brute in combination with scan, we can sometimes find encrypted shellcode inside the file.

```
C:\Windows\System32\cmd.exe

C:\Users\squidward\Desktop\OfficeMalScanner>OfficeMalScanner.exe "C:\Users\squidward\Downloads\module\Lab 6\test.xls" sc
an brute

+-------------------------------------------+
|           OfficeMalScanner v0.62          |
|  Frank Boldewin / www.reconstructer.org   |
+-------------------------------------------+

[*] SCAN mode selected
[*] Opening file C:\Users\squidward\Downloads\module\Lab 6\test.xls
[*] Filesize is 3072 (0xc00) Bytes
[*] Ms Office OLE2 Compound Format document detected
[*] Scanning now...

FLDZ/FSTENV [esp-12] signature found at offset: 0x23c

Brute-forcing for encrypted PE- and embedded OLE-files now...
Bruting XOR Key: 0xff
Bruting ADD Key: 0xff
Bruting ROL Key: 0x08


Analysis finished!

---------------------------------------------------------
test.xls seems to be malicious! Malicious Index = 10
---------------------------------------------------------

C:\Users\squidward\Desktop\OfficeMalScanner>
```

- After getting our results, we can see that we have a signature at offset: 0x23c, let's use Disview.exe to see what it is.

```
C:\Users\squidward\Desktop\OfficeMalScanner>DisView.exe "C:\Users\squidward\Downloads\module\Lab 6\test.xls" 0x23c
Filesize is 3072 (0xc00) Bytes

0000023C: D9EE                  fldz
0000023E: D97424F4              fstenv [esp-0Ch]
00000242: BA45E41BA0            mov edx, A01BE445h
00000247: 5E                    pop esi
00000248: 2BC9                  sub ecx, ecx
0000024A: B147                  mov cl, 47h
0000024C: 83EEFC                sub esi, FFFFFFFCh
0000024F: 315614                xor [esi+14h], edx
00000252: 035651                add edx, [esi+51h]
00000255: 06                    push es
00000256: EE                    out dx, al
00000257: 5C                    pop esp
00000258: B144                  mov cl, 44h
0000025A: 119D41299B78          adc [ebp+789B2941h], ebx
00000260: 7069                  jo $+6Bh
00000262: FF09                  dec [ecx]
00000264: 22598B                and bl, [ecx-75h]
00000267: 5C                    pop esp
00000268: CE                    into
00000269: 12D9                  adc bl, cl
0000026B: 7445                  jz $+47h
0000026D: 56                    push esi
0000026E: F67BEE                idiv byte ptr [ebx-12h]
00000271: DD20                  frstor [eax]
00000273: B5EF                  mov ch, EFh
00000275: 4E                    dec esi
00000276: 10D4                  adc ah, dl
00000278: 738D                  jnb $-71h
0000027A: 45                    inc ebp
0000027B: 364A                  dec edx
0000027D: 5E                    pop esi
0000027E: 98                    cwde
0000027F: 37                    aaa
00000280: 8B83516544CF          mov eax, [ebx-30BB9AAFh]
00000286: C49AE185D411          les ebx, [edx+11D485E1h]
0000028C: B9085DC509            mov ecx, 09C55D08h
00000291: 2A4C5802              sub cl, [eax+ebx*2+02h]
00000295: 754E                  jnz $+50h
00000297: 5A                    pop edx
00000298: C70DC744042B91FFFEC7  invalid
000002A2: 20D6                  and dh, dl
000002A4: CF                    iretd
000002A5: 288E17E0DACE          sub [esi-31251FE9h], cl
000002AB: 50                    push eax
000002AC: C604A5A835B8BE6E      mov [*4]
000002B4: 44                    inc esp
000002B5: 664A                  dec dx
000002B7: 75EE                  jnz $-10h
--------------------------------------------------------------------------------


C:\Users\squidward\Desktop\OfficeMalScanner>
```

4. Exif-tool

Exif-tool is a command line tool used for reading and writing metadata in many file formats.

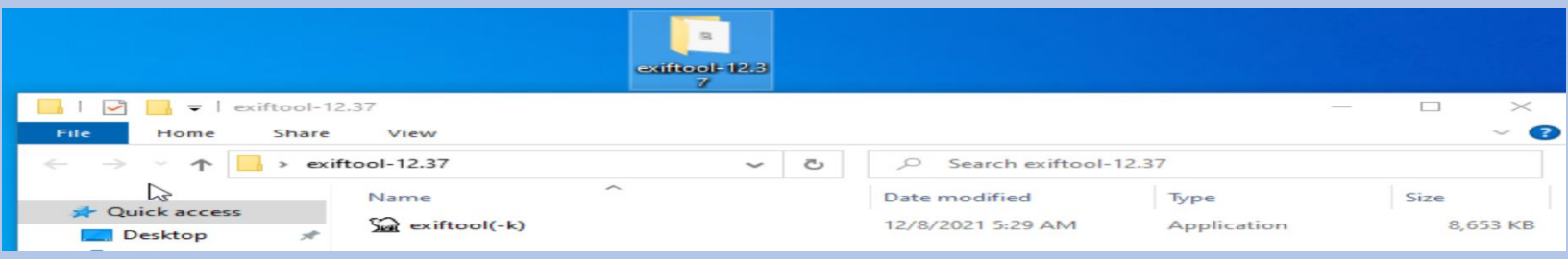
Getting Help:

To see how we can use this tool, we will type the following command into our linux terminal or Windows cmd:

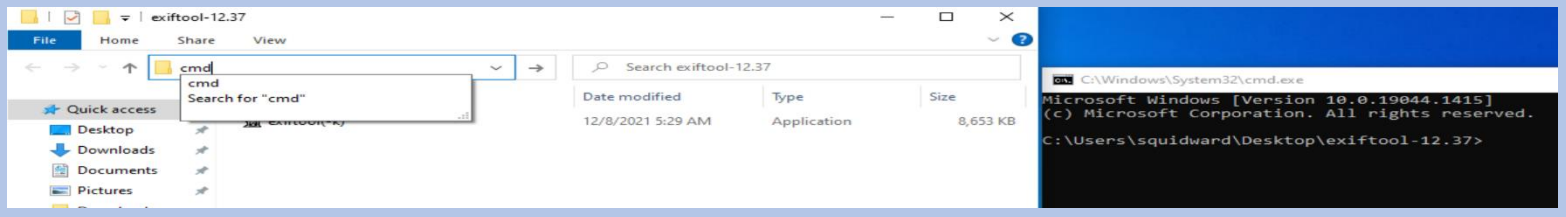
- Exiftool -h

Usage:

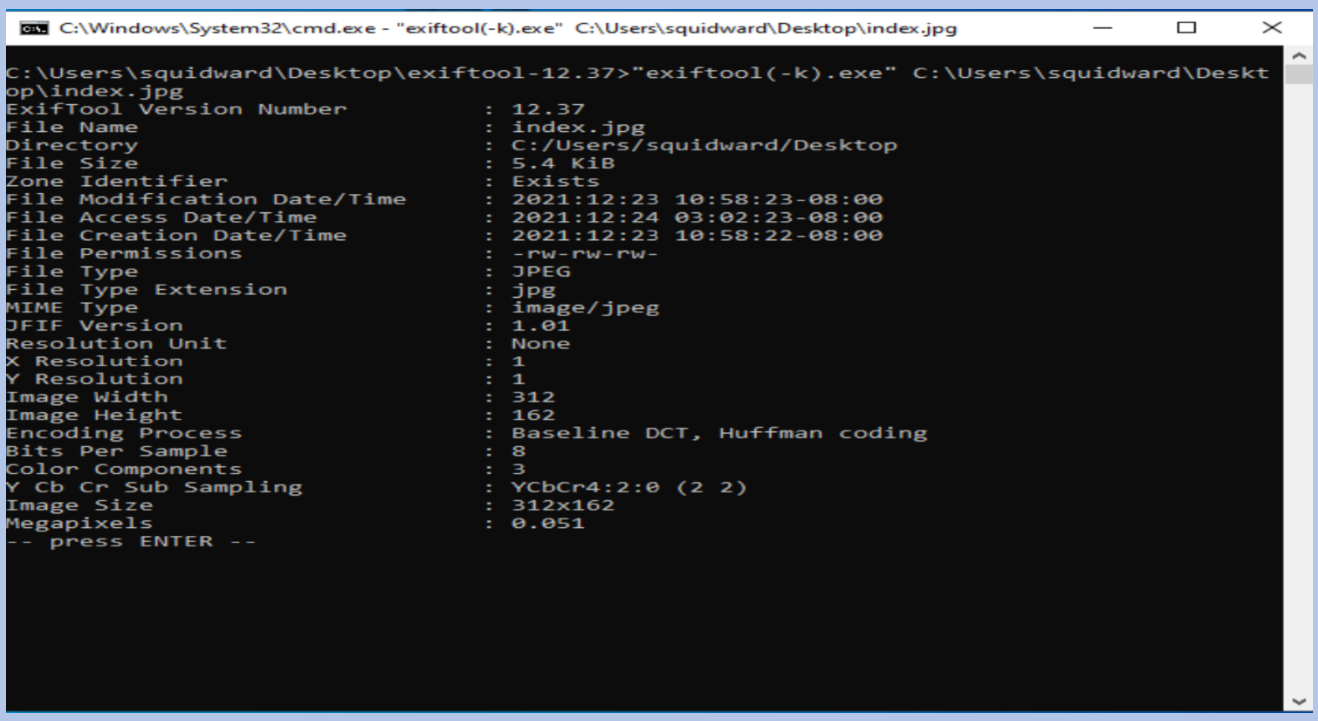
- Find the exif-tool file



- Go to the file directory and type “cmd” instead of “exiftool-12.37”



- To start scanning, type “exif” and press tab so the cmd completes the name of the program, then select a picture to scan and drag&drop it in the cmd terminal, then press enter to run the scan.



We can generate a single report on one file using the command:

"exiftool(-k).exe" -a -u -g1 -w %f.txt *.jpg

And we can also generate a single report in a Comma Separated Value (CSV) format with all the information within it by using the following command:

"exiftool(-k).exe" *.jpg -csv > report.csv

To Learn more on how to use Exif-tool, visit the website:
https://linuxhint.com/get_filea_metadata_exif_tool/

5. PDFid

This forensic tool is used in pdf files. The tool scans pdf files for specific keywords, which allows you to identify executable codes when opened. The suspicious files are then analyzed with the pdf-parser tool.

Getting help:

```
C:\Users\squidward\Desktop\Tools\pdfid_v0_2_8>python pdfid.py -h
Usage: pdfid.py [options] [pdf-file|zip-file|url|@file] ...
Tool to test a PDF file

Arguments:
pdf-file and zip-file can be a single file, several files, and/or @file
@file: run PDFiD on each file listed in the text file specified
wildcards are supported

Source code put in the public domain by Didier Stevens, no Copyright
Use at your own risk
https://DidierStevens.com

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -s, --scan            scan the given directory
  -a, --all             display all the names
  -e, --extra           display extra data, like dates
  -f, --force           force the scan of the file, even without proper %PDF
                        header
  -d, --disarm          disable JavaScript and auto launch
  -p PLUGINS, --plugins=PLUGINS
                        plugins to load (separate plugins with a comma , ;
                        @file supported)
  -c, --csv             output csv data when using plugins
  -m MINIMUMSCORE, --minimumscore=MINIMUMSCORE
                        minimum score for plugin results output
  -v, --verbose         verbose (will also raise catched exceptions)
  -S SELECT, --select=SELECT
                        selection expression
  -n, --nozero          supress output for counts equal to zero
  -o OUTPUT, --output=OUTPUT
                        output to log file
  --pluginoptions=PLUGINOPTIONS
                        options for the plugin
  -l, --literalfilenames
                        take filenames literally, no wildcard matching
  --recursedir          Recurse directories (wildcards and here files (@...)
                        allowed)

C:\Users\squidward\Desktop\Tools\pdfid_v0_2_8>
```

Usage:

Python pdfid.py [options] pdf-file|zip-file|url

```
C:\Users\squidward\Desktop\Tools\pdfid_v0_2_8>python pdfid.py "C:\Users\squidward\Downloads\module\Lab 5\Linda.pdf"
PDFiD 0.2.8 C:\Users\squidward\Downloads\module\Lab 5\Linda.pdf
 PDF Header: %PDF-1.6
 obj                   582
 endobj                582
 stream                 54
 endstream              54
 xref                    1
 trailer                 1
 startxref               1
 /Page                   3
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                   12
 /Colors > 2^24          0

C:\Users\squidward\Desktop\Tools\pdfid_v0_2_8>
```

6. Strings

Strings allows you to find valuable information on any file you feed it.

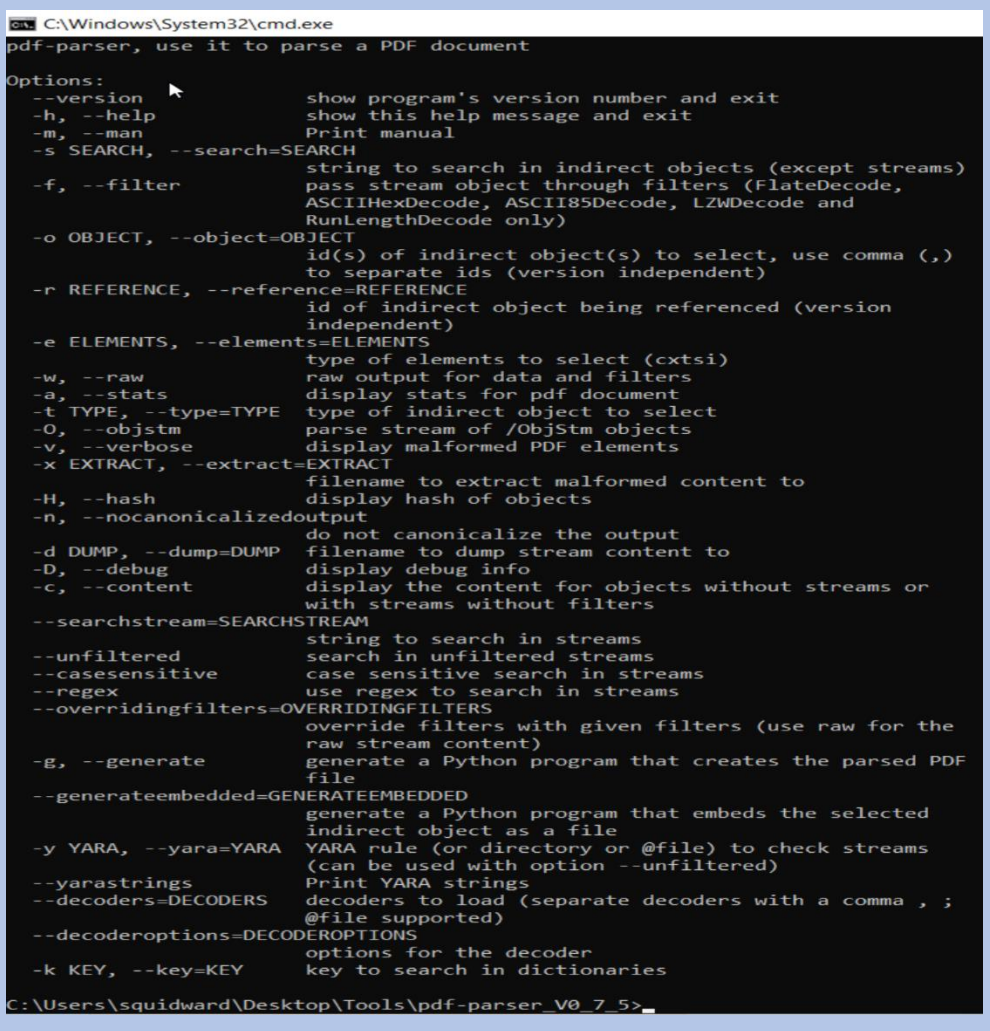
Command syntax:

Strings.exe <File>

7. PDFparcer

This tool is one of the most important forensic tools for pdf files. pdf-parser parses a pdf document and distinguishes the important elements utilized during its analysis, and this tool does not render that pdf document.

Getting Help:



Usage:

python pdf-parser.py [options] pdf-file|zip-file|url

Disks Viewer/Repairing:

1. FTK imager (Viewing)

FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.

To Download FTK Imager, Visit https://www.exterro.com/ftk-imager

Visit the page, click on “Download FTK Imager” and complete the form with any info.

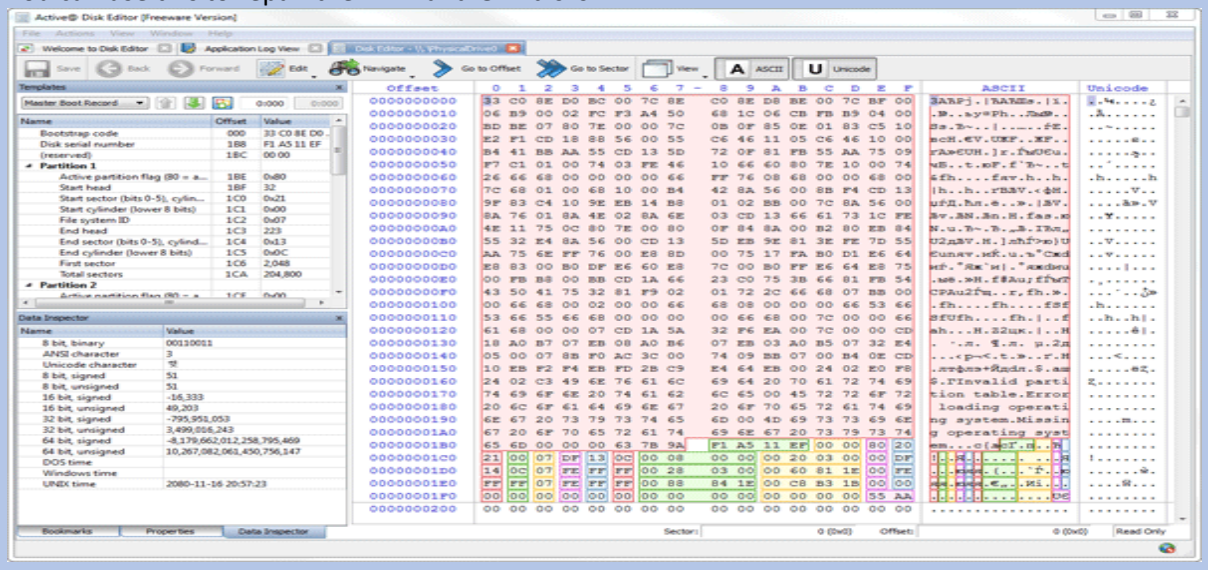
And to learn how to use FTK Imager, visit https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/

2. Active Disk Editor (Repairing)

Active Disk Editor uses a simple, low-level disk viewer which displays information in binary and text modes at the same time. You can use this view to analyze the contents of data storage structure elements such as:

- Hard disk drives
- SSD & USB Disks
- Partitions & Volumes
- Files

You can use this to repair the MBR and GPT disks.



Data Recovering/Carving Tools:

1- PhotoRec

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures from digital camera memory.

It can recover lost files from:

- FAT
- NTFS
- exFAT
- ext2/ext3/ext4 filesystem
- HFS+

To Download PhotoRec and learn how to use it, visit website:
https://recoverit.wondershare.com/photo-recovery/how-to-use-photorec.html

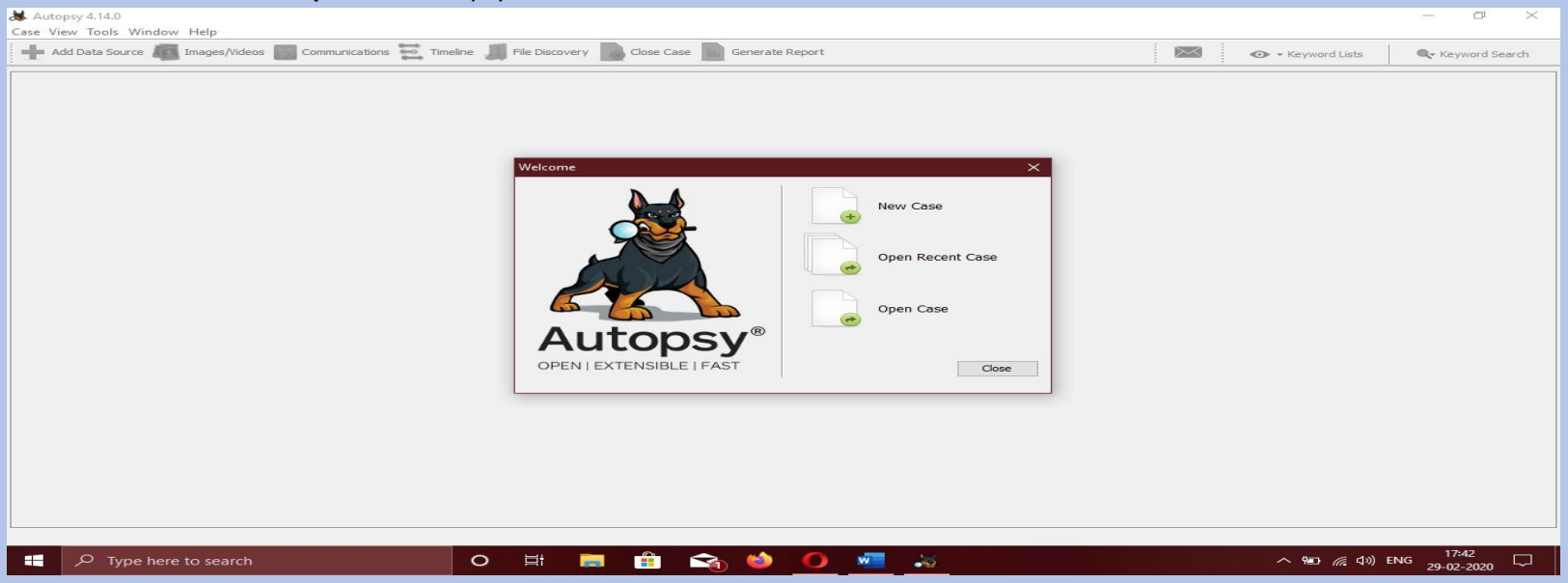
2- Autopsy For Windows

It is a free to use and quite efficient tool for hard drive investigation with features like multi-user cases, timeline analysis, registry analysis, keyword search, email analysis, media playback, EXIF analysis and malicious file detection.

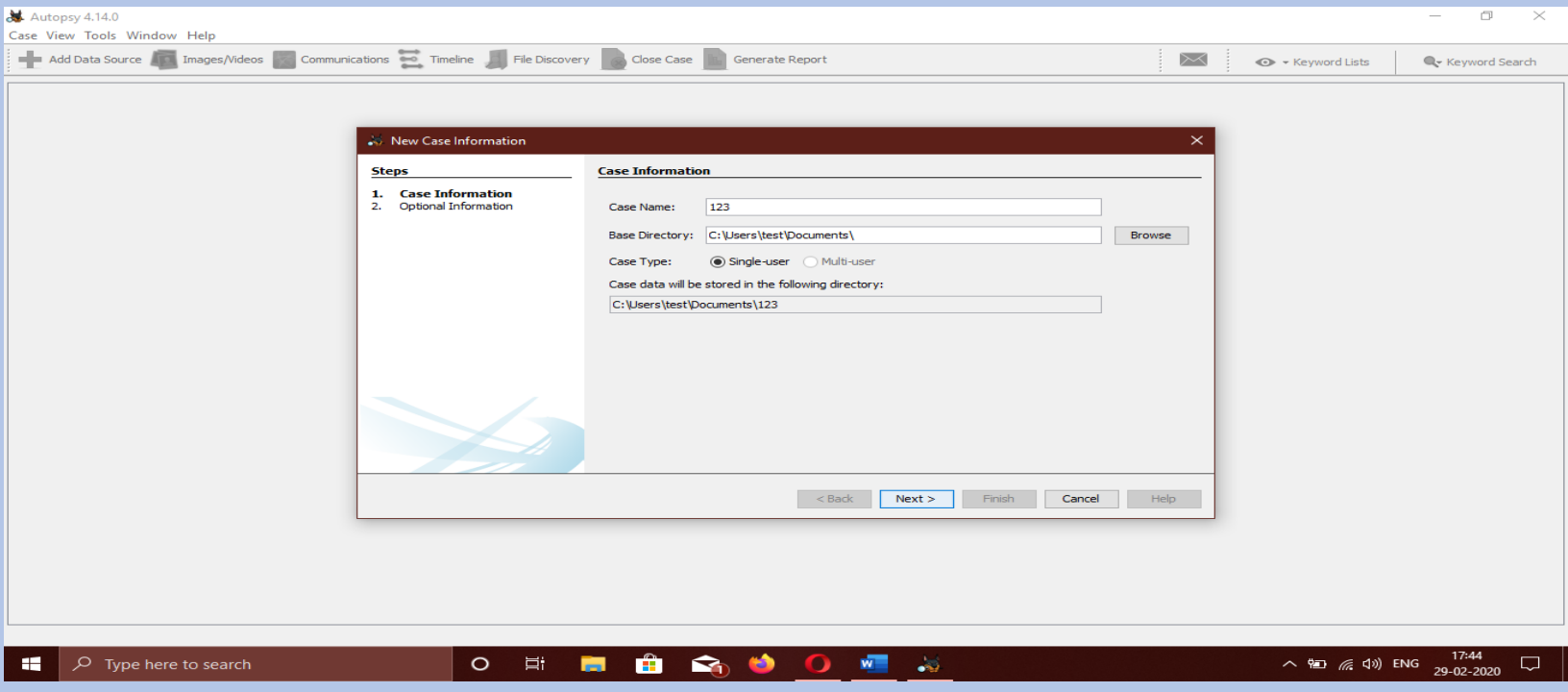
Download here: www.sleuthkit.org/autopsy/

Usage:

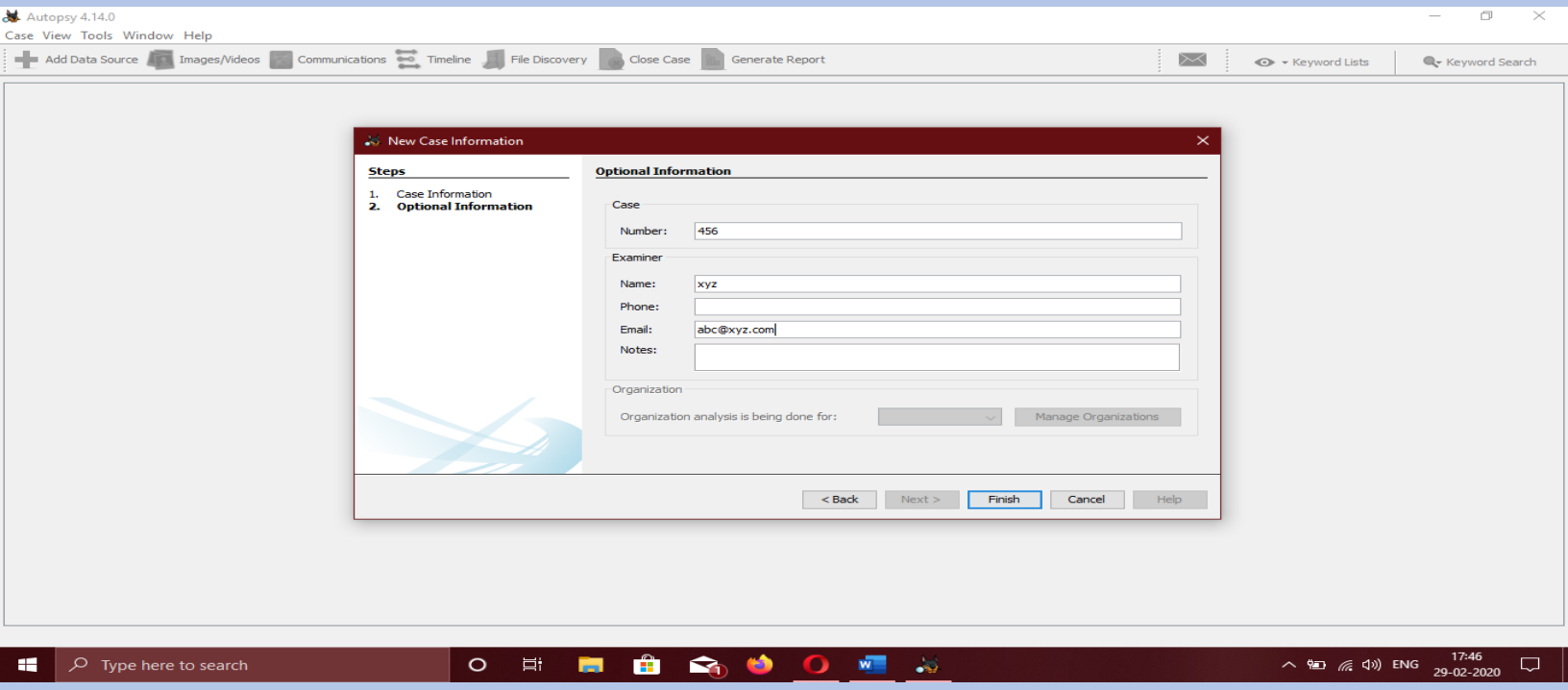
- **Step 1:** Run Autopsy and select “New Case”



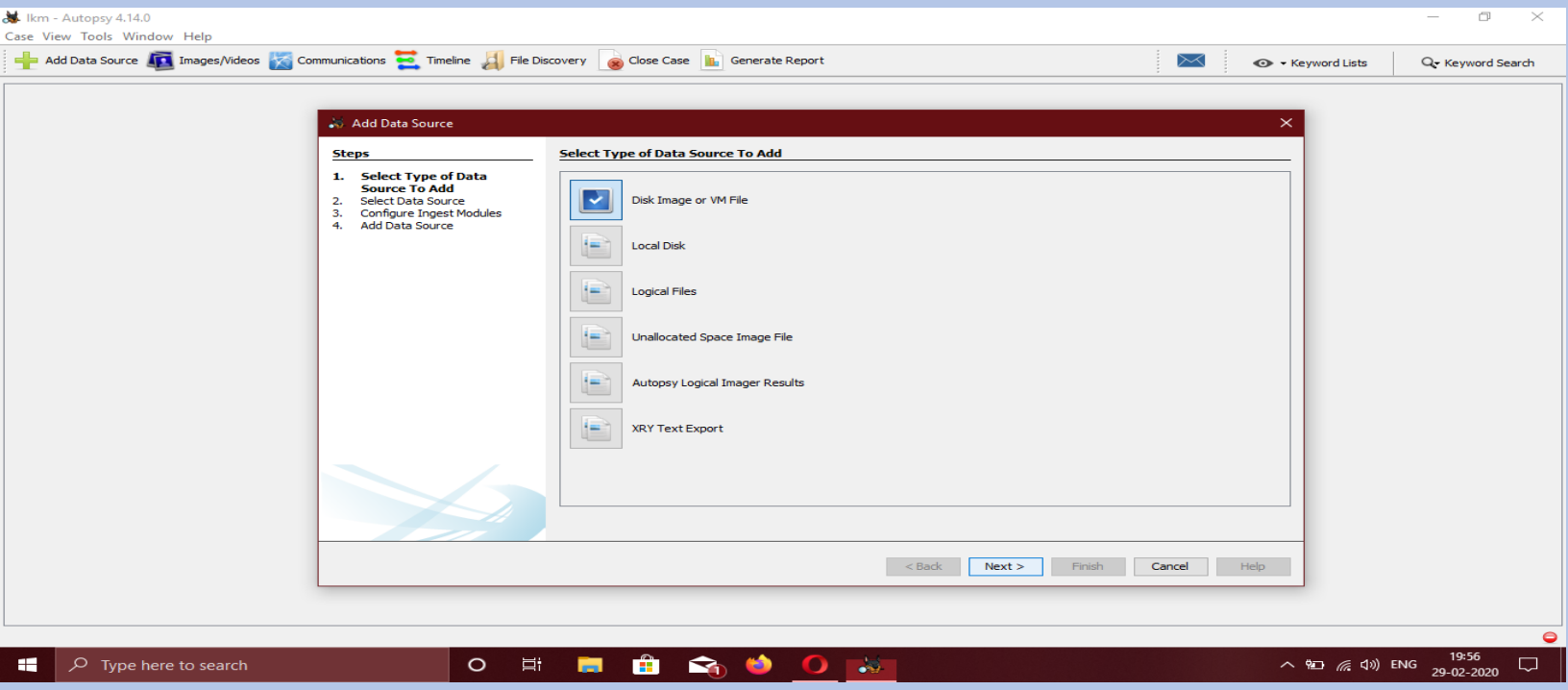
- **Step 2:** Provide the “Case Name” and the “Directory” to store the case file. Click on “Next”.



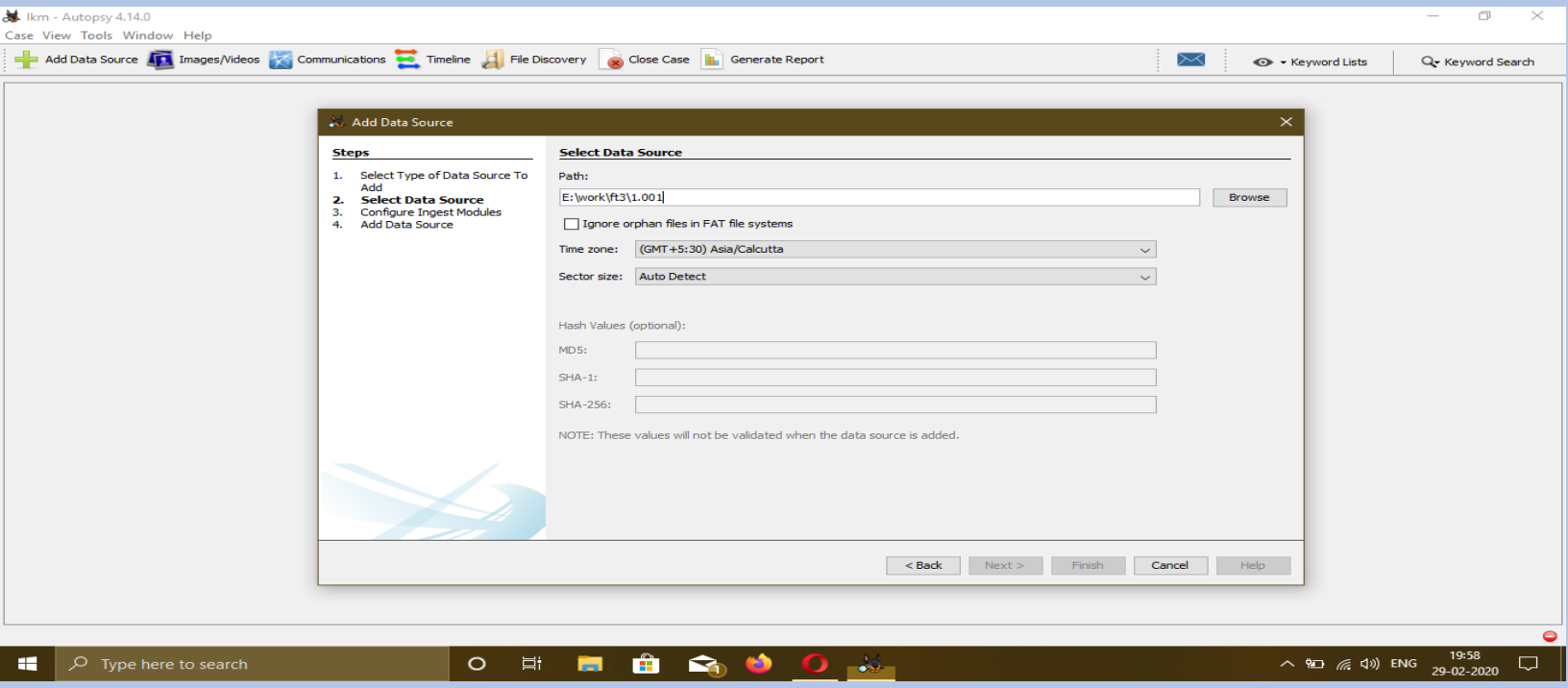
- **Step 3:** Add “Case Number” and examiner’s details, then click on “Finish”.



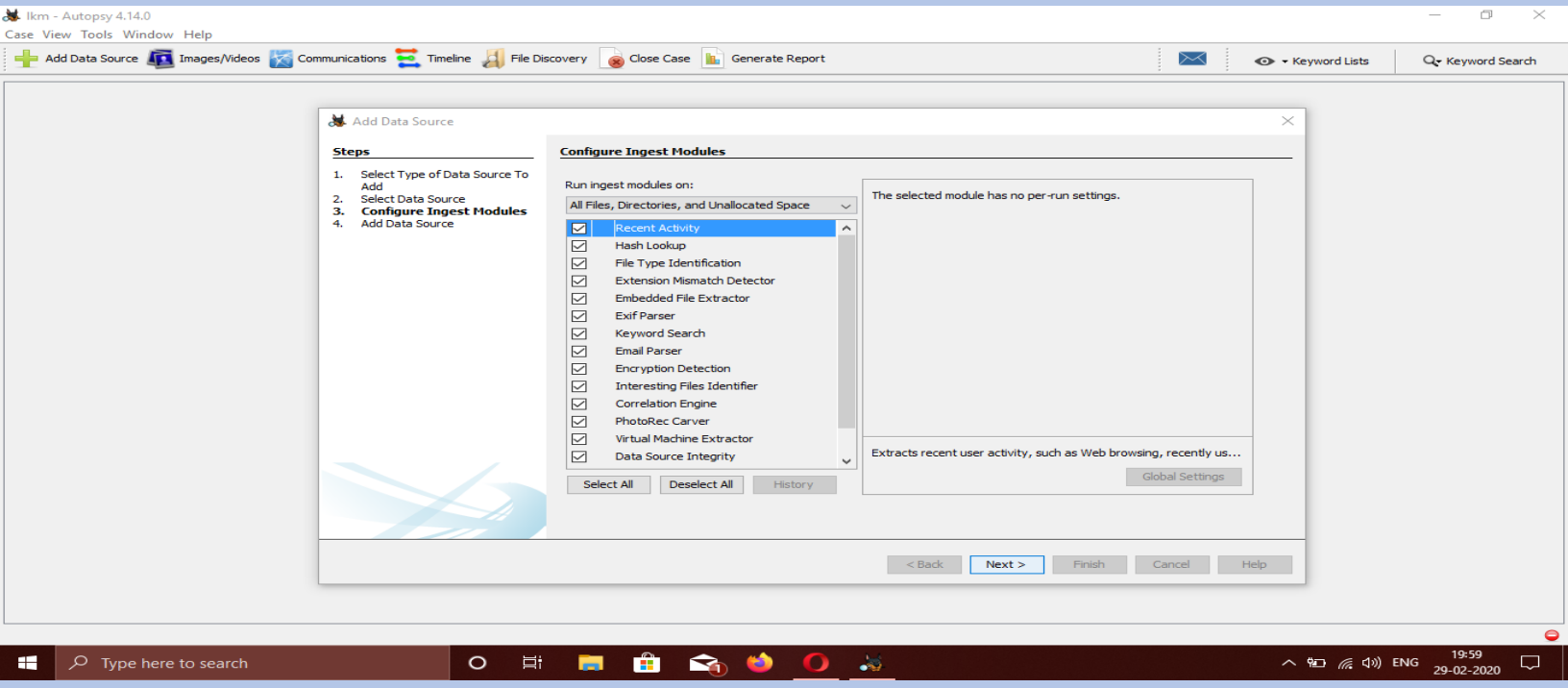
- **Step 4:** Choose the required data source type, in the case “Disk Image” and click on “Next”.



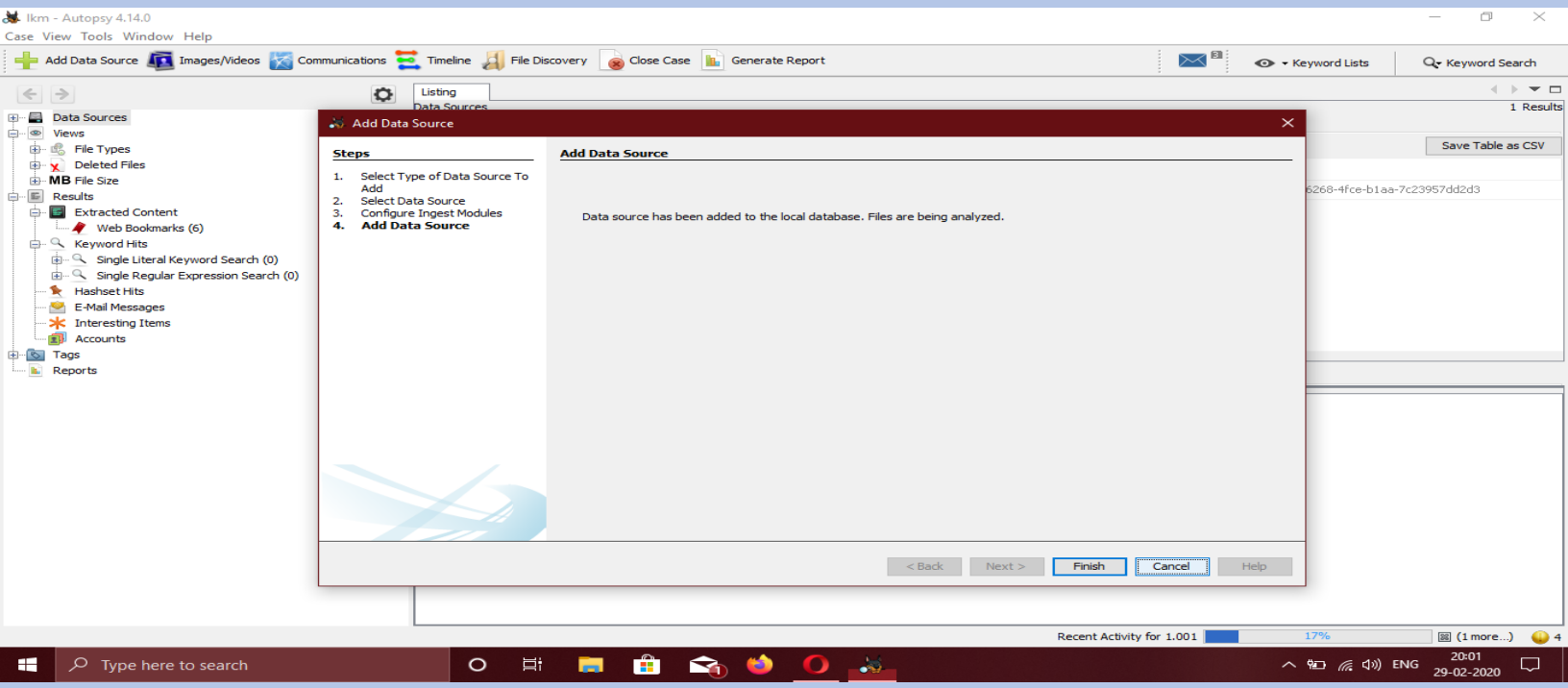
- **Step 5:** Give path of the data source and click on “Next”.



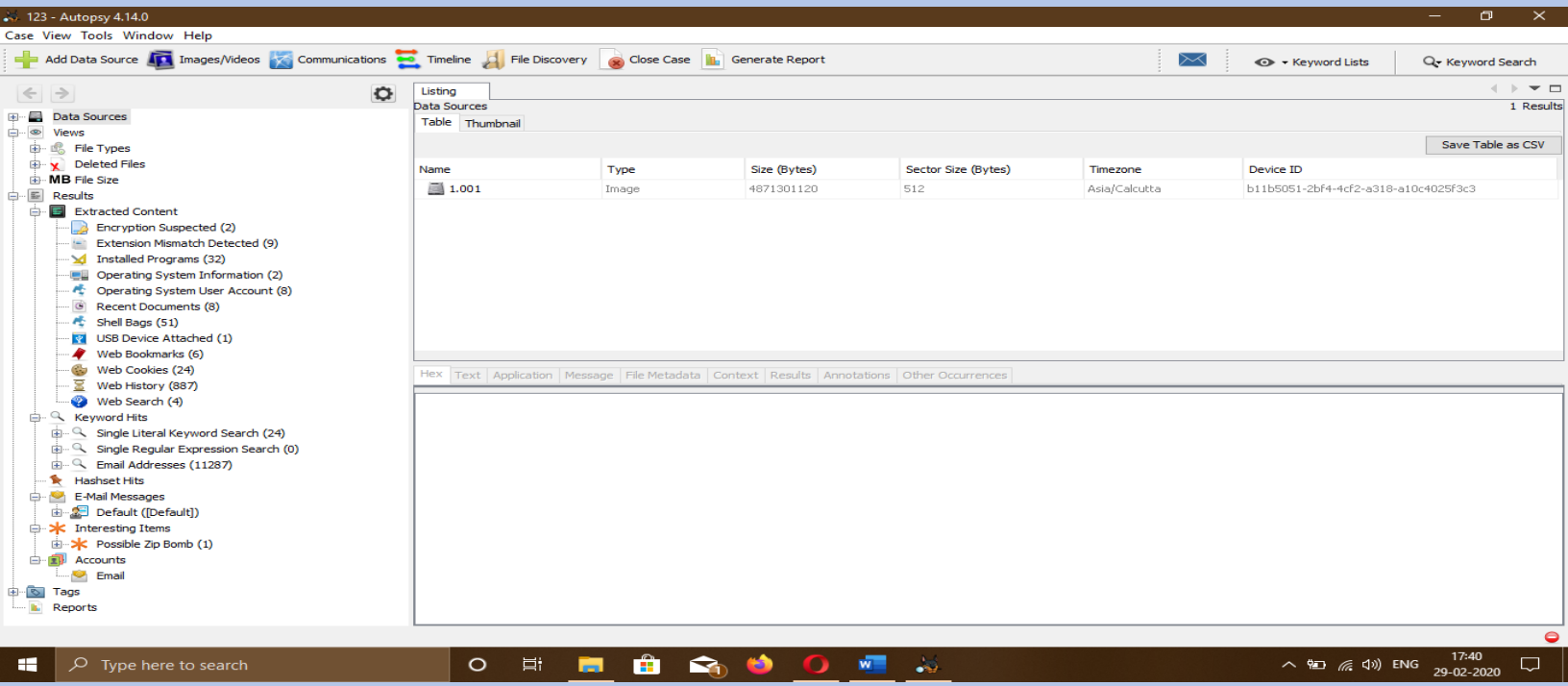
- **Step 6:** Select the required modules and click on “Next”.



- **Step 7:** After the data source has been added, click on “Finish”.



- **Step 8:** You can begin investigating once the “Analysis and Integrity check” is complete.



For more examples on how to use the program, visit the following website:

https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d

3- Foremost

This is a Linux Forensic Tool and is used for carving disks for wanted files such as pictures and documents.

This is the command used in linux:

Foremost -o <output dir> -i <disk image path>

4- Scalpel

scalpel is a fast file carver that reads a database of header and footer definitions and extracts matching files from a set of image files or raw device files.

scalpel is filesystem-independent and will carve files from FAT16, FAT32, exFAT, NTFS, Ext2, Ext3, Ext4, JFS, XFS, ReiserFS, raw partitions, etc.

scalpel is a complete rewrite of the Foremost 0.69 file carver and is useful for both digital forensics investigations and file recovery.

To Install, type:

Sudo apt install scalpel

To get help on how to use, type:

Scalpel -h

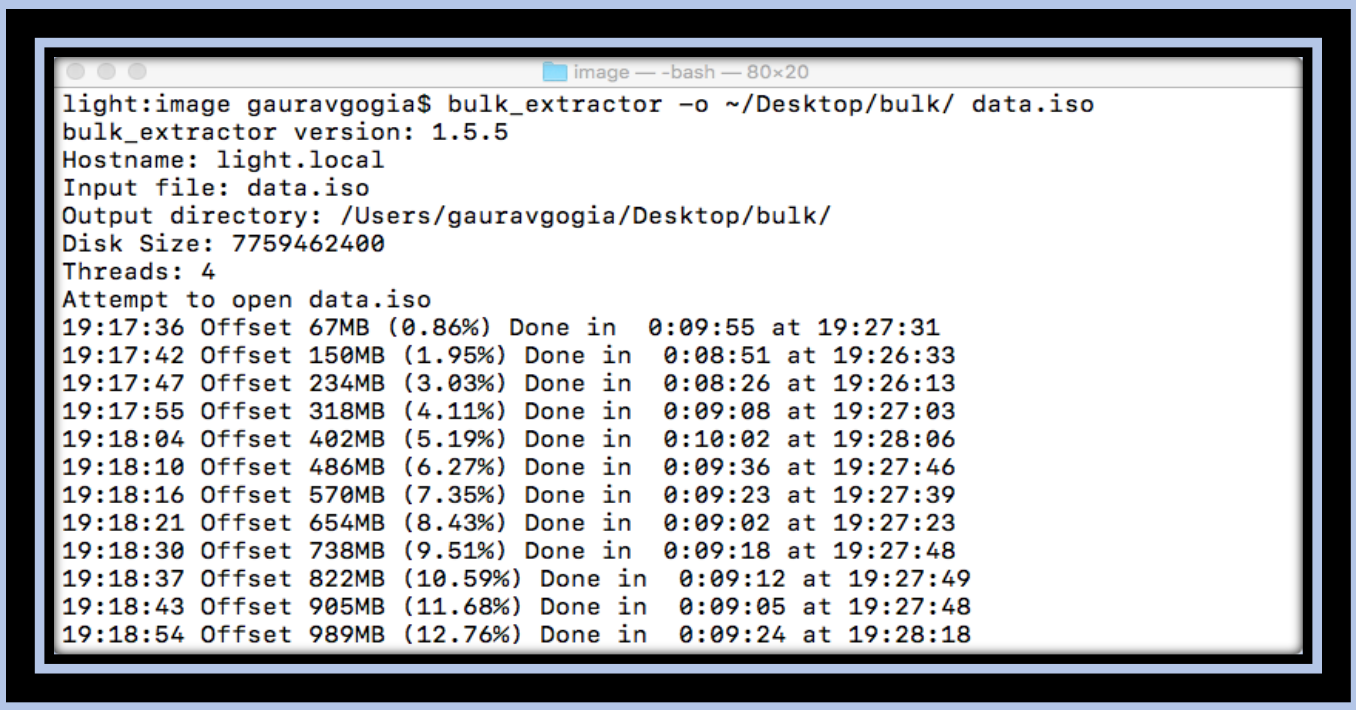
5- Bulk extractor

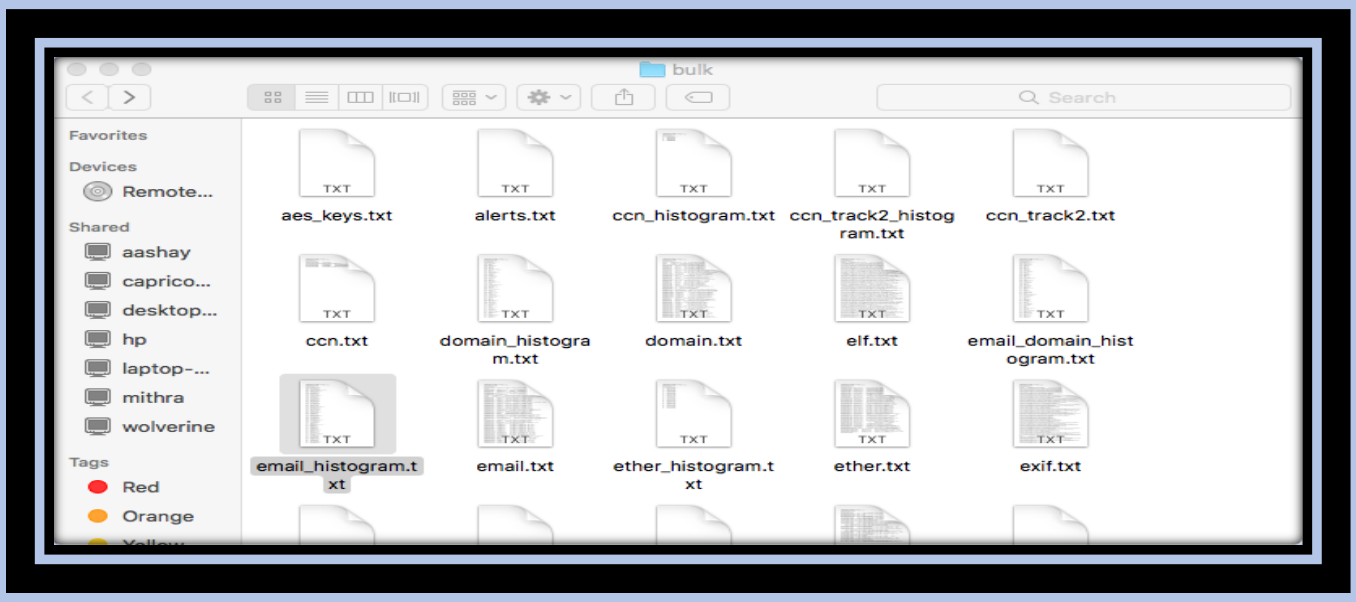
A data recovery and suspicious text extraction tool. Uses disk image as input.

This is the command used in linux:

bulk_extractor -o <output dir> <disk image path>

Usage:

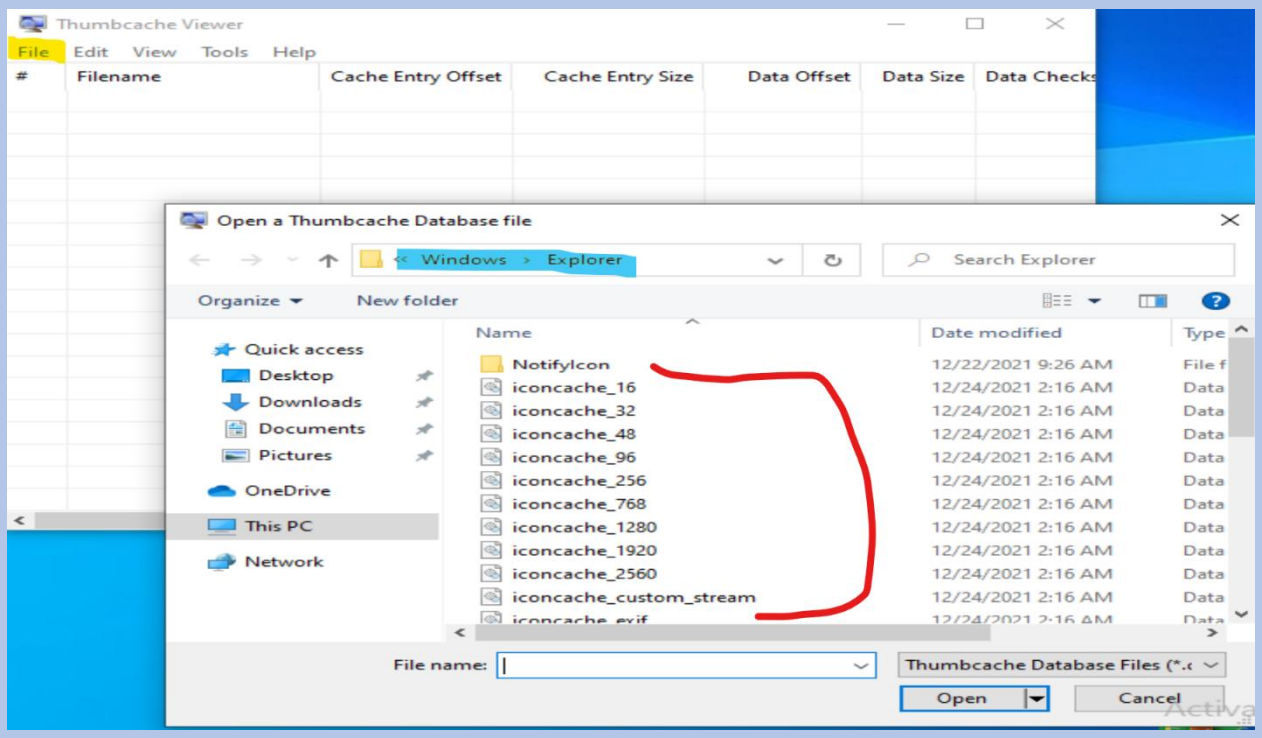




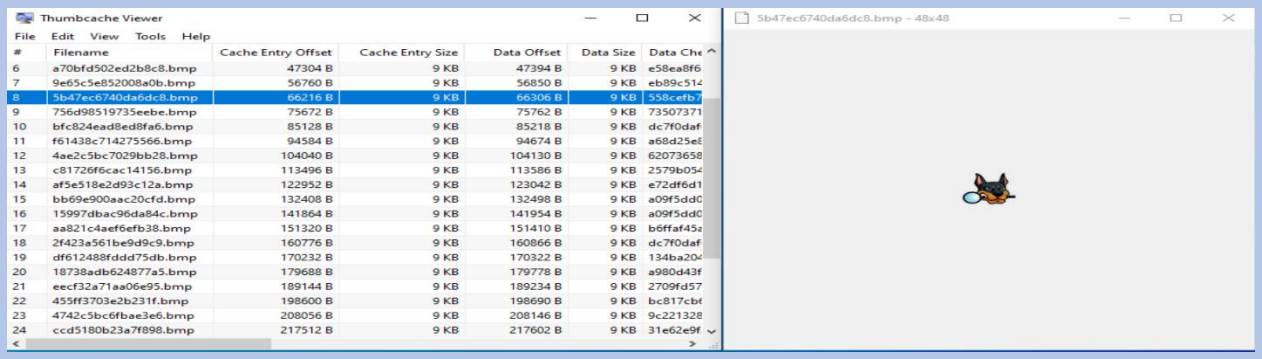
6- Thumbcache viewer

Windows saves it's thumbcache in the following directory:
C:\Users\Win\AppData\Local\Microsoft\Windows\Explorer

- Now we open Thumbcache-viewer and go to (File → open → [Directory] → select any iconcache file)



- Now we can view the thumbnails saved by windows.



The iconcache_16 files are the smallest icons and the iconcache_2560 are the largest.

7- LECmd.exe

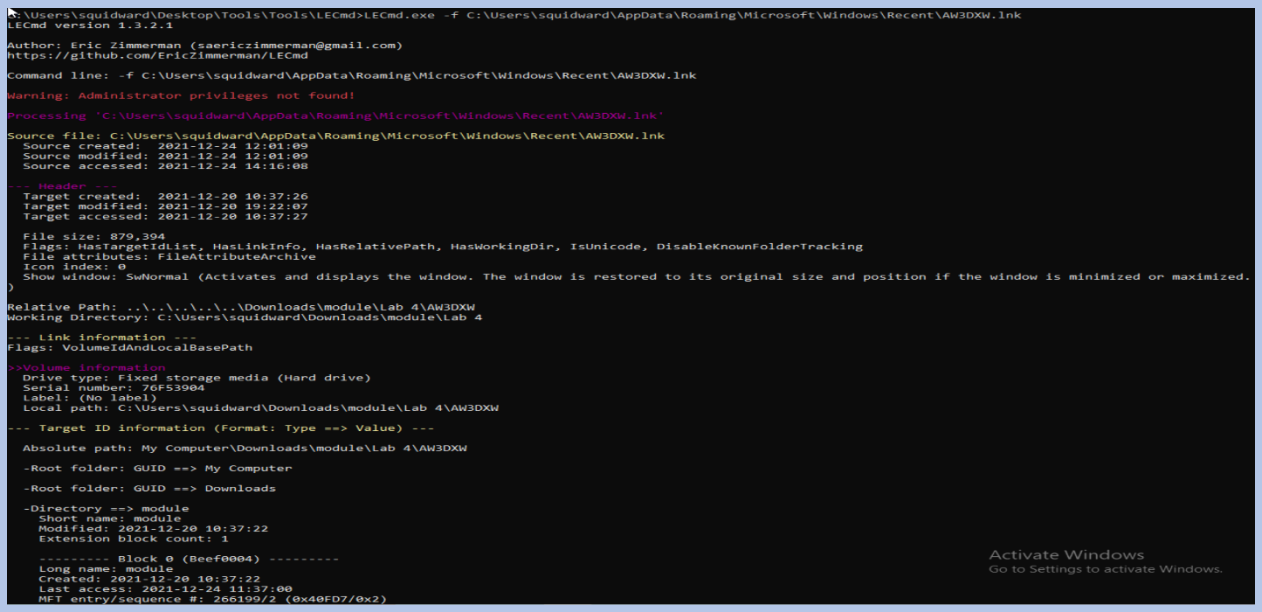
When we get asked what the last created file was, we can scan the following directory to gain some information to answer our question. **Used to scan LNK files.**

All the lnk files are stored here →
C:\Users\<Name>\Windows\AppData\Roaming\Microsoft\windows\Recent Items

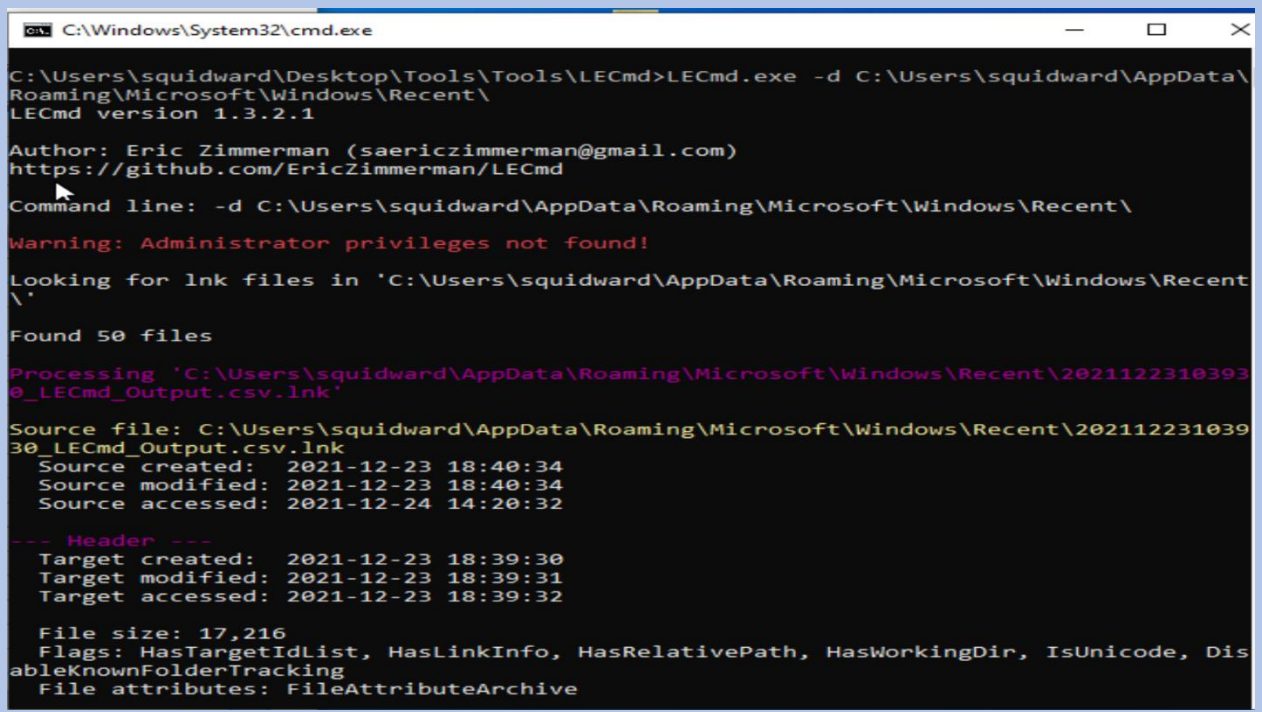
Usage:

- After we access the directory, we open LECmd.exe via cmd and use the following commands.

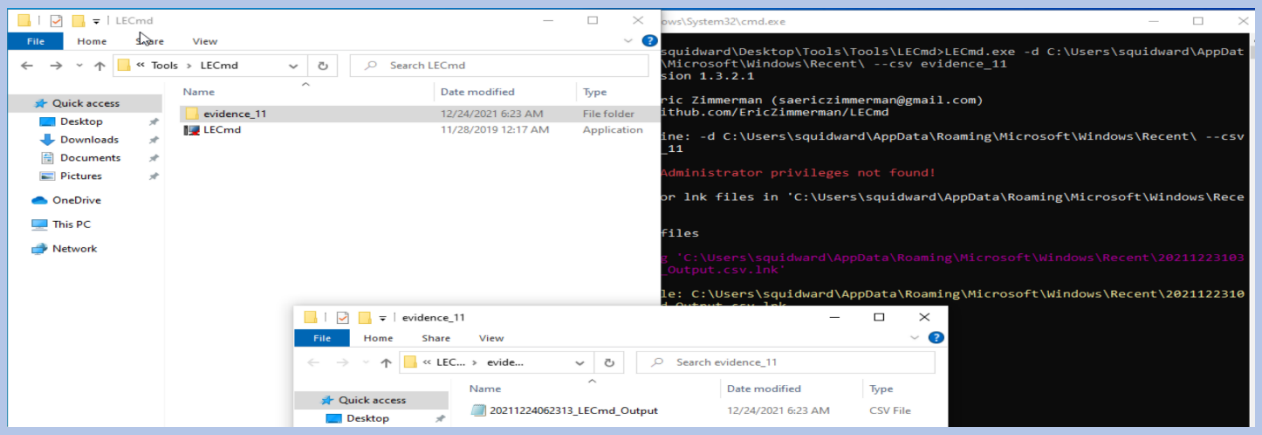
LECmd.exe -f <File-Name> → This command scans the file and prints out results to the terminal.



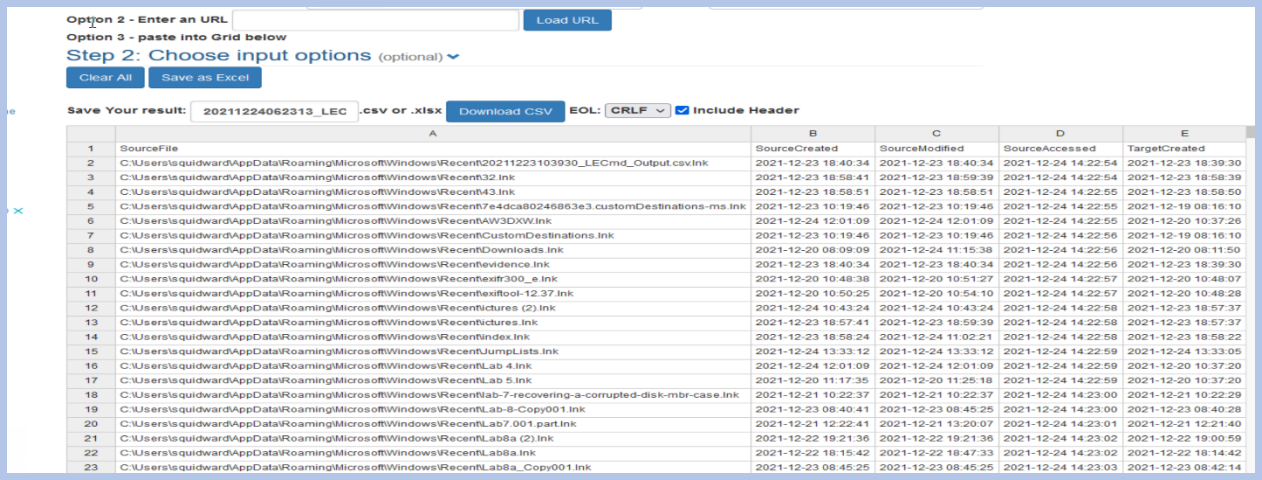
LECmd.exe -d <Directory> → This command scans the directory and prints out results to the terminal.



LECmd.exe -f <File-Name> --csv <output_name>



We saved our results to a new file called “evidence_11” in a CSV format which we can open using Excel sheet which will organize our information the way we need.



	A	B	C	D	E
1	SourceFile	SourceCreated	SourceModified	SourceAccessed	TargetCreated
2	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\20211223103930_LECmd_Output.csv.lnk	2021-12-23 18:40:34	2021-12-23 18:40:34	2021-12-24 14:22:54	2021-12-23 18:39:30
3	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\32.lnk	2021-12-23 18:58:41	2021-12-23 18:59:39	2021-12-24 14:22:54	2021-12-23 18:58:39
4	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\43.lnk	2021-12-23 18:58:51	2021-12-23 18:58:51	2021-12-24 14:22:55	2021-12-23 18:58:50
5	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\7e4dca80246863e3.customDestinations-ms.lnk	2021-12-23 10:19:46	2021-12-23 10:19:46	2021-12-24 14:22:55	2021-12-19 08:16:10
6	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\AW3DXW.lnk	2021-12-24 12:01:09	2021-12-24 12:01:09	2021-12-24 14:22:55	2021-12-20 10:37:26
7	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations.lnk	2021-12-23 10:19:46	2021-12-23 10:19:46	2021-12-24 14:22:56	2021-12-19 08:16:10
8	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Downloads.lnk	2021-12-20 08:09:09	2021-12-24 11:15:38	2021-12-24 14:22:56	2021-12-20 08:11:50
9	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\evidence.lnk	2021-12-23 18:40:34	2021-12-23 18:40:34	2021-12-24 14:22:56	2021-12-23 18:39:30
10	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\exifr300_e.lnk	2021-12-20 10:48:38	2021-12-20 10:51:27	2021-12-24 14:22:57	2021-12-20 10:48:07
11	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\exiftool-12.37.lnk	2021-12-20 10:50:25	2021-12-20 10:54:10	2021-12-24 14:22:57	2021-12-20 10:48:28
12	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\ictures (2).lnk	2021-12-24 10:43:24	2021-12-24 10:43:24	2021-12-24 14:22:58	2021-12-23 18:57:37
13	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\ictures.lnk	2021-12-23 18:57:41	2021-12-23 18:59:39	2021-12-24 14:22:58	2021-12-23 18:57:37
14	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\ndex.lnk	2021-12-23 18:58:24	2021-12-24 11:02:21	2021-12-24 14:22:58	2021-12-23 18:58:22
15	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\JumpLists.lnk	2021-12-24 13:33:12	2021-12-24 13:33:12	2021-12-24 14:22:59	2021-12-24 13:33:05
16	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab 4.lnk	2021-12-24 12:01:09	2021-12-24 12:01:09	2021-12-24 14:22:59	2021-12-20 10:37:20
17	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab 5.lnk	2021-12-20 11:17:35	2021-12-20 11:25:18	2021-12-24 14:22:59	2021-12-20 10:37:20
18	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\lab-7-recovering-a-corrupted-disk-mbr-case.lnk	2021-12-21 10:22:37	2021-12-21 10:22:37	2021-12-24 14:23:00	2021-12-21 10:22:29
19	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab-8-Copy001.lnk	2021-12-23 08:40:41	2021-12-23 08:45:25	2021-12-24 14:23:00	2021-12-23 08:40:28
20	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab7.001.part.lnk	2021-12-21 12:22:41	2021-12-21 13:20:07	2021-12-24 14:23:01	2021-12-21 12:21:40
21	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab8a (2).lnk	2021-12-22 19:21:36	2021-12-22 19:21:36	2021-12-24 14:23:02	2021-12-22 19:00:59
22	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab8a.lnk	2021-12-22 18:15:42	2021-12-22 18:47:33	2021-12-24 14:23:02	2021-12-22 18:14:42
23	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\Lab8a_Copy001.lnk	2021-12-23 08:45:25	2021-12-23 08:45:25	2021-12-24 14:23:03	2021-12-23 08:42:14

8- Shadowcopyview.exe

ShadowCopyView is simple tool for Windows 10/8/7/Vista that lists the snapshots of your hard drive created by the 'Volume Shadow Copy' service of Windows.

Every snapshot contains an older version of your files and folders from the date that the snapshot was created, you can browse the older version of your files and folders, and optionally copy them into a folder on your disk.

To download and learn more on how to use ShadowCopyView.exe, visit the website:

https://www.nirsoft.net/utils/shadow_copy_view.html

9- JumpList Explorer

Jump Lists are a windows feature introduced with Windows 7. They contain information about recently accessed applications and files.

There are two types of Jump lists created in Windows,

- Automatic-Destinations-MS → Which are jump lists created automatically when the users opens a files or an application. → Location: `C:\Users\<Name>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`

- Custom-Destinations-MS → As their name indicated these are custom made jump lists, created when the users pin a file or an application to the taskbar. → Location: `C:\Users\<Name>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations`

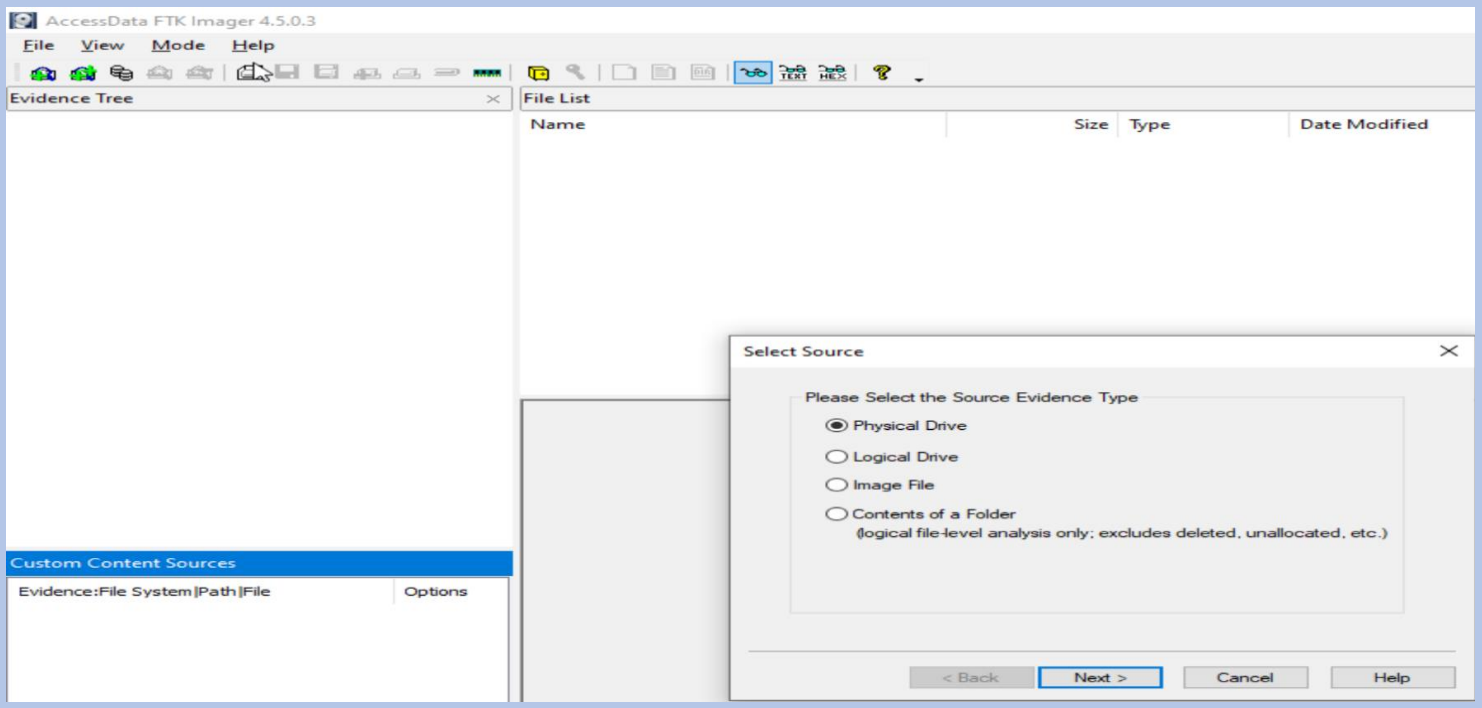
To get information from these files, we can use the following tool:

JumpList Explorer by Eric Zimmerman, Download here:

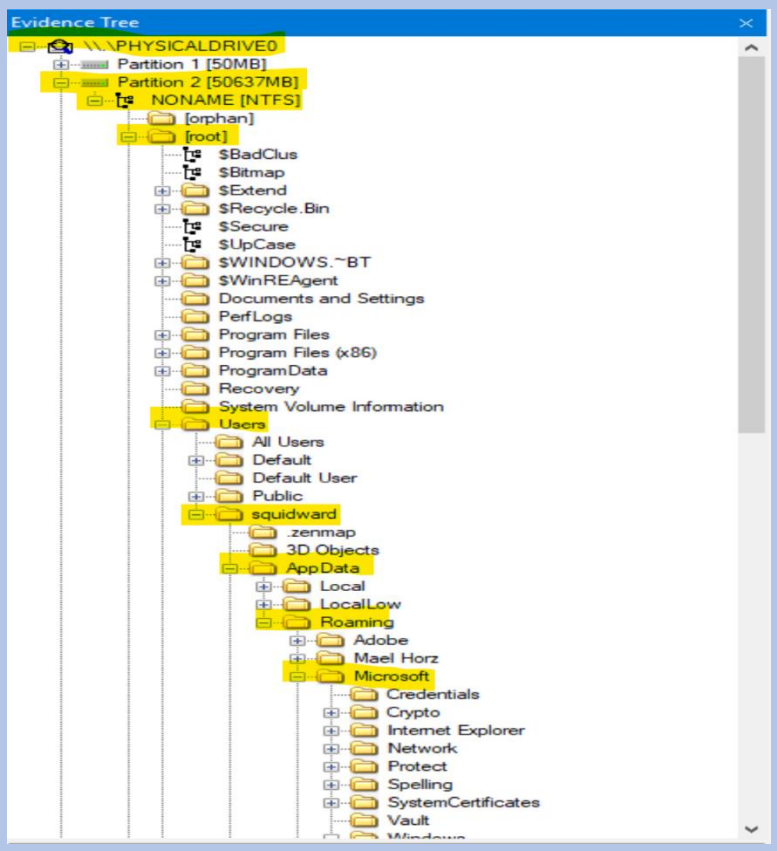
https://ericzimmerman.github.io/#!index.md

Usage:

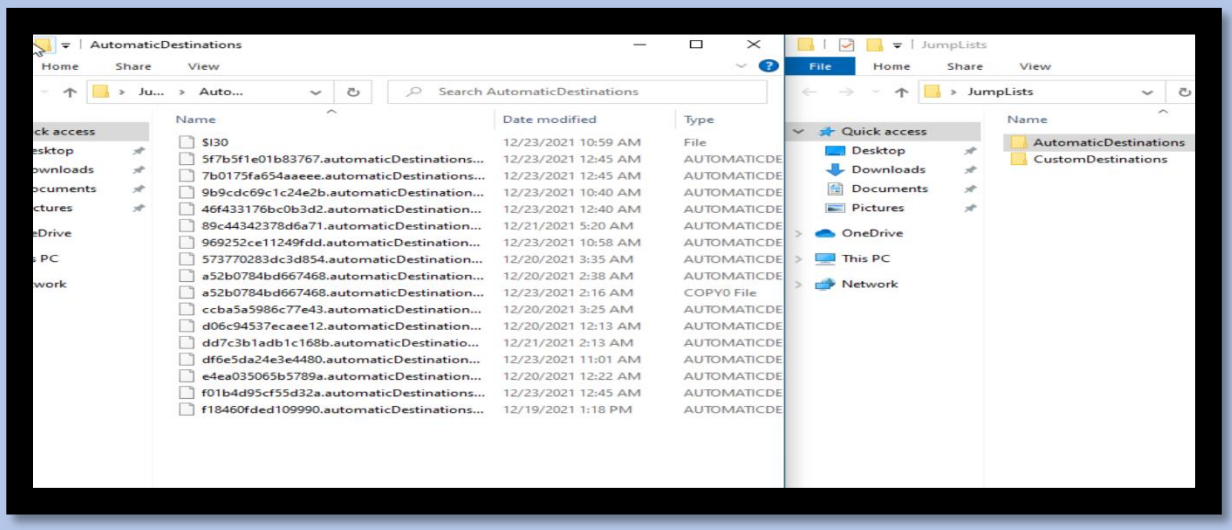
- **Step 1:** Open up FTK imager and select a hard disk to scan.



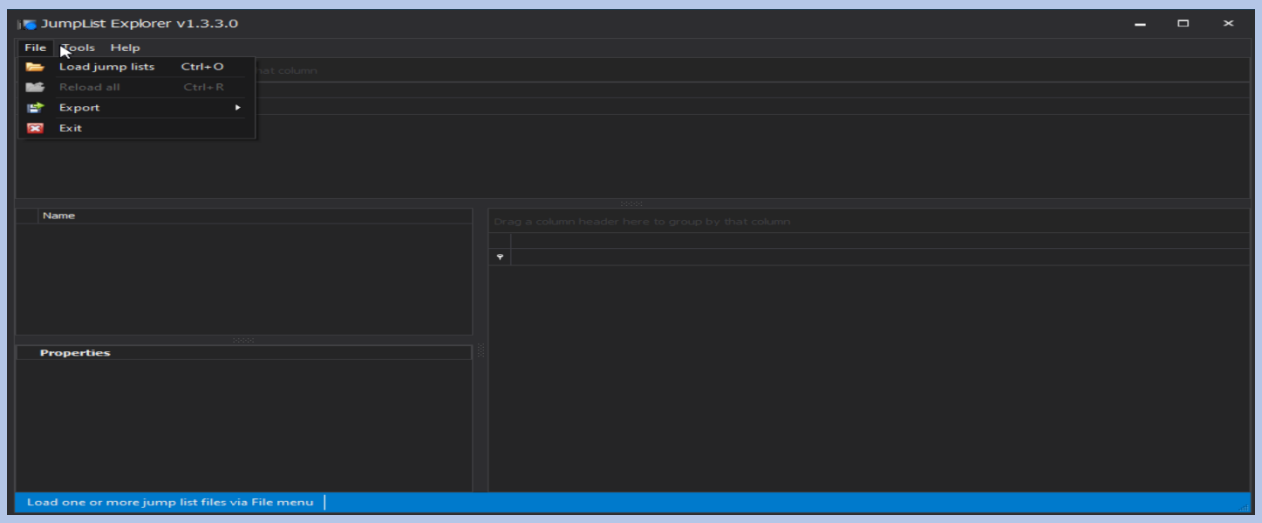
Now we go to the automatic and custom destinations so we can save them for later use. We can find them in this directory:
`C:\Users\<Name>\AppData\Roaming\Microsoft\Windows\Recent\`



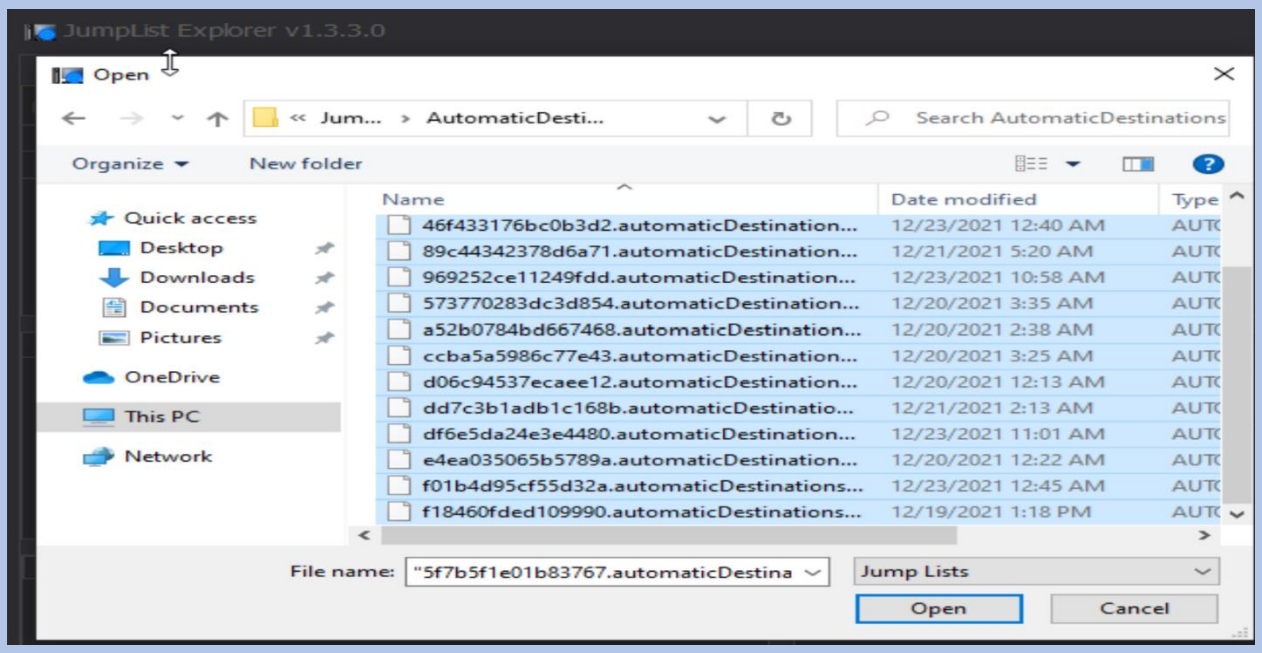
- **Step 2:** Now we create a file in the Desktop, and export both “Automatic-Destination” and “Custom-Destination” to the created file, so we can use it later via JumpList explorer.



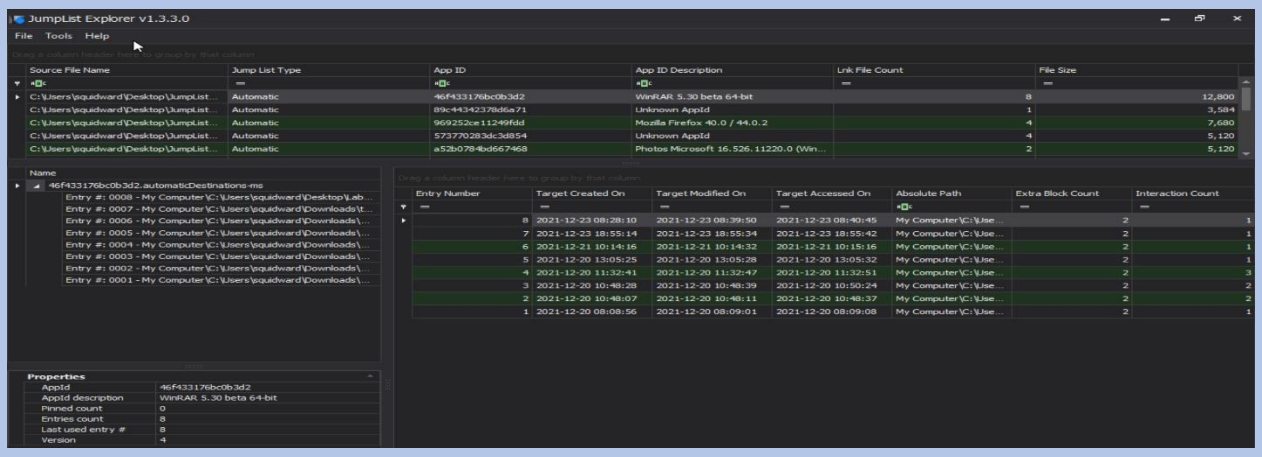
- **Step 3:** Now we open the files via JumpList Explorer.



- **Step 4:** Then we open the Automatic-Destination Folder and select everything inside it.



- **Step 5:** Now we can examine the Automatic-Destination files and see what recent actions took place in a machine.



10- RBCmd.exe

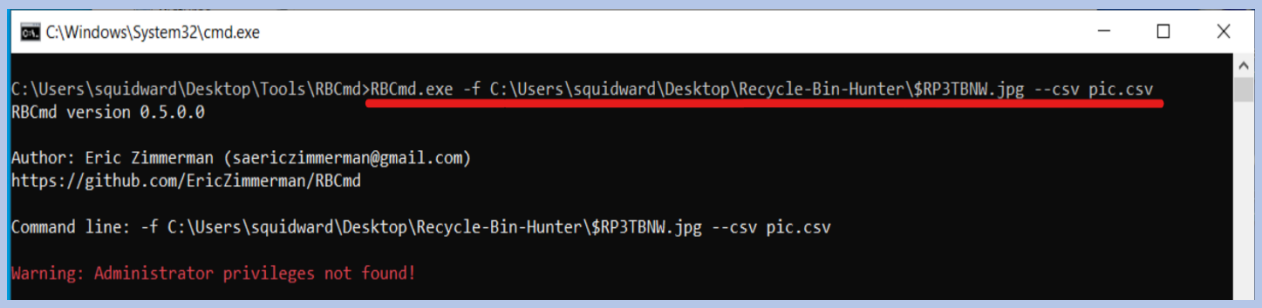
This is a Windows Recycle Bin artifact parser tool.

Usage:

```
RBCmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RBCmd

        d               Directory to recursively process. Either this or -f is required
        f               File to process. Either this or -d is required
        q               Only show the filename being processed vs all output. Useful to speed up exporting to json and/or csv

        csv             Directory to save CSV formatted results to. Be sure to include the full path in double quotes
        csvf            File name to save CSV formatted results to. When present, overrides default name

        dt              The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for options.
                        Default is: yyyy-MM-dd HH:mm:ss

        debug           Show debug information during processing
        trace           Show trace information during processing


Examples: RBCmd.exe -f "C:\Temp\INFO2"
          RBCmd.exe -f "C:\Temp\$I3VPA17" --csv "D:\csvOutput"
          RBCmd.exe -d "C:\Temp" --csv "c:\temp"

          Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
```

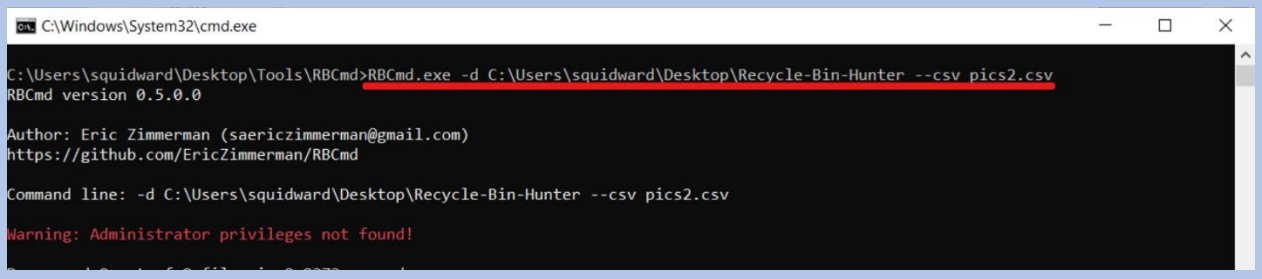
To scan a file, use this command:

- RBCmd.exe -f <FileName> --csv <output.csv>



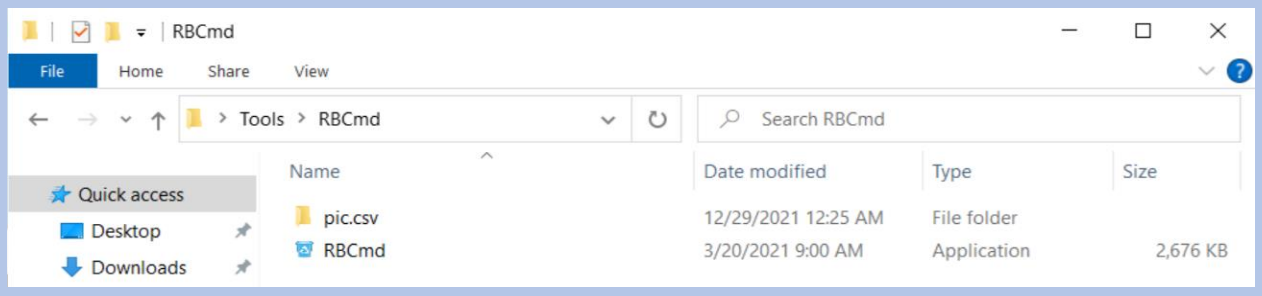
To scan a directory, use this command:

- RBCmd.exe -d <directory of files> --csv <output.csv>



To save output as csv file, use this command when scanning files or directories.

- --csv <output.csv> , This will save the output to the tool directory.



11- Registry Explorer

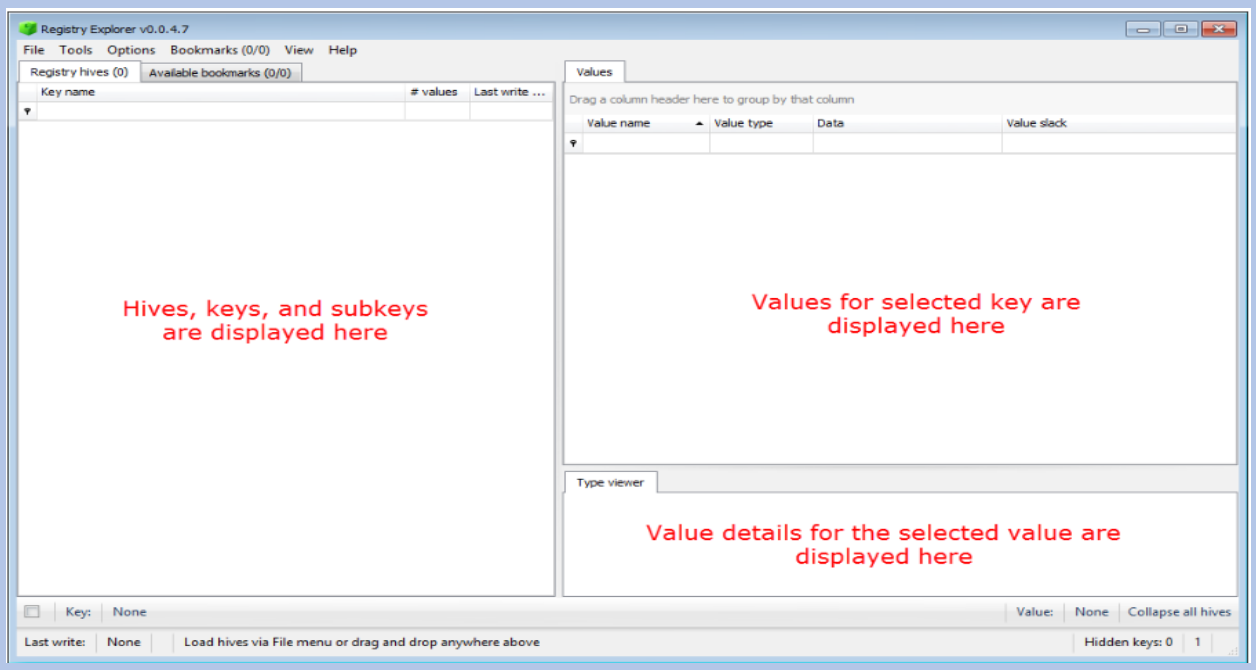
Registry Explorer is a GUI based tool used to view the contents of offline Registry Hives. It has the ability to load multiple hives at once, search across all loaded hives using strings or regular expressions, exporting of data, and much more.

We can use it to view contents of the following hives:

SECURITY, SOFTWARE, SYSTEM, and SAM

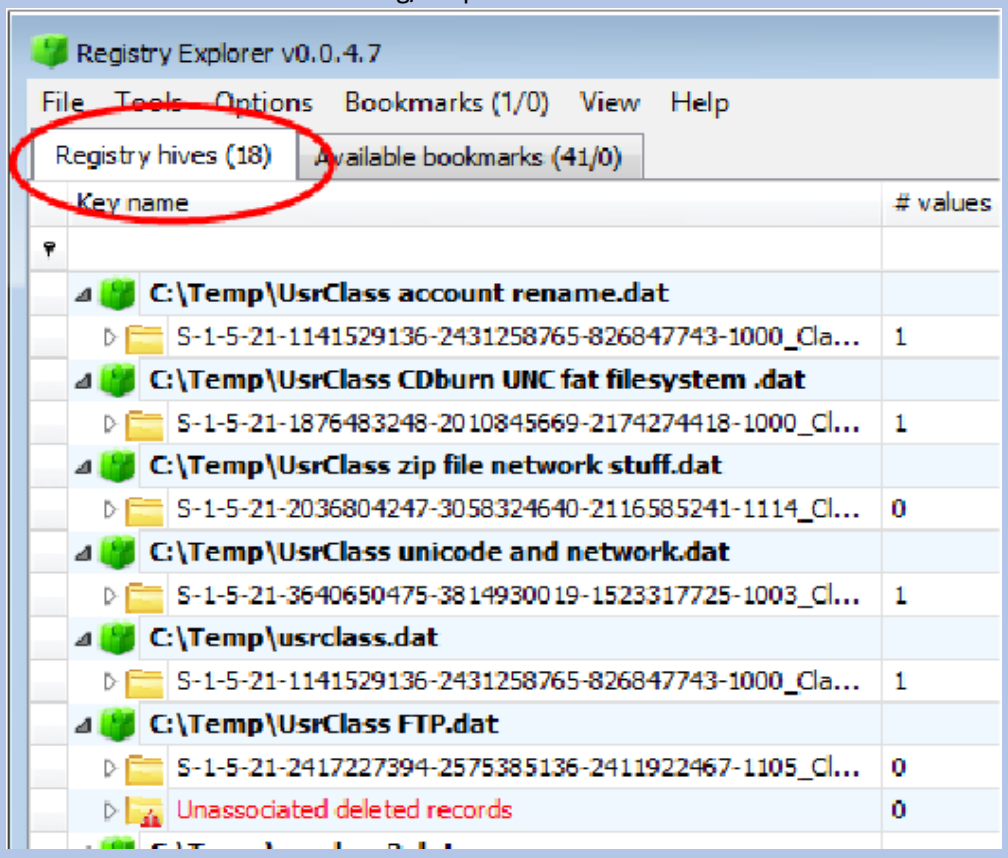
Getting Started:

After starting Registry Explorer, the main interface is displayed.



Loading Hives:

To load Hives such as (Security,Software,System,etc), go to **(File)**, then select **(load hive)** or you can select one or more hives and drag/drop them onto the main interface.



As you can see, we loaded 18 hives without any problems.

Projects:

Projects allow you to load one or more hives into Registry Explorer and save the currently loaded hives into a project file.

This allows you quickly load the same hives for a particular case quickly vs having to load a bunch of hives individually.

You can also drag and drop Registry Explorer project files (.re_proj) just like you would a registry hive.

References:

To learn more about the usage of the program, visit the website below, it will open a pdf file written by the creator himself, it explains every feature the program has.

Author/ Eric Zimmerman

https://www.oit.va.gov/Services/TRM/files/RegistryExplorerManual.pdf

To download tool:

https://ericzimmerman.github.io/#!index.md

12- Shellbag Explorer

Shellbags are a set of Windows Registry Keys located in **NTUser.dat** and **USRClass.dat** registry hives that maintain view, icon, position, and size of folders when using Windows Explorer.

With Shellbag, you can find timestamps and other useful information which provide context into what has happened. You can also learn the history of any data that was in the system before it was deleted.

Shellbags Location in the Registry:

- HKCU\Software\Microsoft\Windows\Shell\Bags
- HKCU\Software\Microsoft\Windows\Shell\BagMRU (Ntuser.dat)
- HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags

Under NTUSER.DAT:

- HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU

Under USRCLASS.DAT:

- HKCU\software\Classes\Local\Settings\Software\Microsoft\Windows\Shell\BagMRU
- HKCU\software\Classes\Local\Settings\Software\Microsoft\Windows\Shell\Bags

Recommended Tools:

- ShellBags Explorer
- RegRipper
- RegEdit

You can use any tools you feel comfortable with, but I recommend Shellbags Explorer as it has a lot of great features that helps with investigating.

To learn more on how to use the (Shellbags Explorer), visit the following website: https://shehackske.medium.com/windows-shellbags-part-1-9aae3cfaf17

13- Amcacheparser (AmCache)

The **Amcache.hve** file is a registry file that stores the information of executed applications.

It is considered **(Evidence of Execution)**

This file can contain:

- Execution path
- First executed time
- Deleted time
- First installation

Location:

\%SystemRoot%\AppCompat\Programs\Amcache.hve

How can we use it?

Amcache.hve records the recent processes that were run and lists the path of the files that's executed which can then be used to find the executed program.

It also records the programs SHA1 so it can be researched with databases like **VirusTotal** for easy identification.

14- AppCompatCacheParser (ShimCache)

ShimCache (aka Application Compatibility Cache), allows Windows to track executable files and scripts that may require special compatibility settings to properly run.

It is considered **(Evidence of Existence)**

These files can contain:

- The executable or script file names and full paths
- The standard information last modified date
- The size of the binary
- Finally, whether the file actually ran on the system or just browsed through explorer.exe

Locations:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache

How can we use it?

The **Shimcache** tracks metadata such as the **full file path**, **last modified date**, and **file size** but only contains the information prior to the system's last startup, as current entries are stored only in memory

The events in **Shimcache.hve** are listed in chronological order with the most recent event first and can be used in timelines to recreate and determine malicious activities.

Shimcache can be investigated using **ShimCacheParser.py**, by Mandiant:

https://github.com/mandiant/ShimCacheParser

List of Resources:

- DD -- http://www.chrysocome.net/dd
- Dcode -- https://www.digital-detective.net/dcode/
- OfficeMalScanner -- http://www.reconstructer.org/main.html
- Exiftool -- https://github.com/exiftool/exiftool – By Phil Harvey
- PDFparser and PDFid -- https://blog.didierstevens.com/programs/pdf-tools/ -- by Didier Stevens
- AmcacheParser – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- AppCompatCacheparser (Shimcache) – https://github.com/mandiant/ShimCacheParser Zimmerman
- JumpList Explorer – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- LECmd – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- PECmd – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- RBCmd – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- Registry Explorer/RECmd – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- Shellbags Explorer – https://ericzimmerman.github.io/#!index.md – By Eric Zimmerman
- ShadowCopyView.exe -- https://www.nirsoft.net/utils/shadow_copy_view.html
- Autopsy for Windows -- www.sleuthkit.org/autopsy/
- PhotoRec -- https://recoverit.wondershare.com/photo-recovery/how-to-use-photorec.html