

# ***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 Baldwin / www.reconstructor.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" scan
+-----+
|          OfficeMalScanner v0.62           |
| Frank Baldwin / www.reconstructor.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" scan brute
+-----+
|          OfficeMalScanner v0.62          |
| Frank Baldwin / www.reconstructor.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: SE              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: 119D41299878      adc [ebp+789B2941h], ebx
00000260: 7669            jo $+68h
00000262: FF09            dec [ecx]
00000264: 225988          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, EFn
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              cwd
0000027F: 37              add
00000280: B883516544CF      mov eax, [ebx-30BB9AAFh]
00000286: C49AE185D411      les ebx, [edx+1D485E1h]
0000028C: B9085DC509      mov ecx, 09C55D08h
00000291: 24AC5882          sub cl, [eax+ebx*2+02h]
00000295: 754E            jnz $+50h
00000297: 5A              pop edx
00000298: C70DC744042B91FFFEC7    invalid
000002A2: 2806            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.

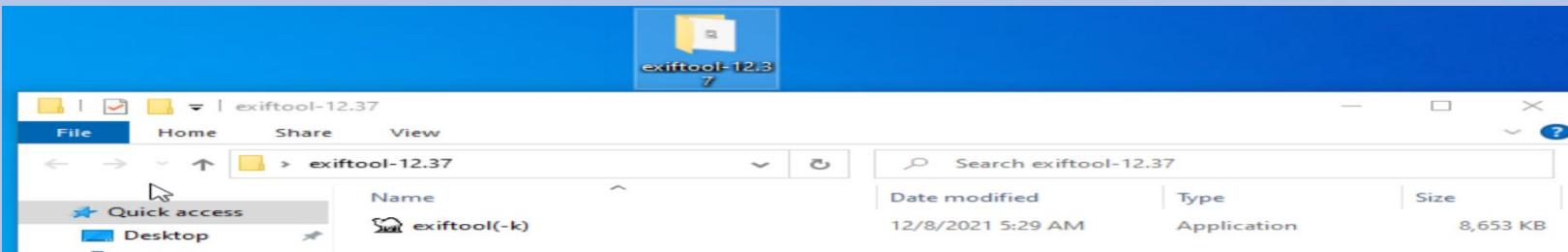
### Getting Help:

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

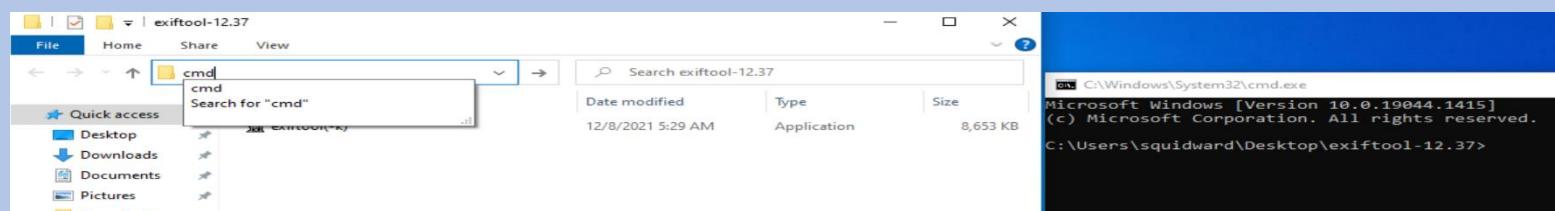
- Exiftool -h

### Usage:

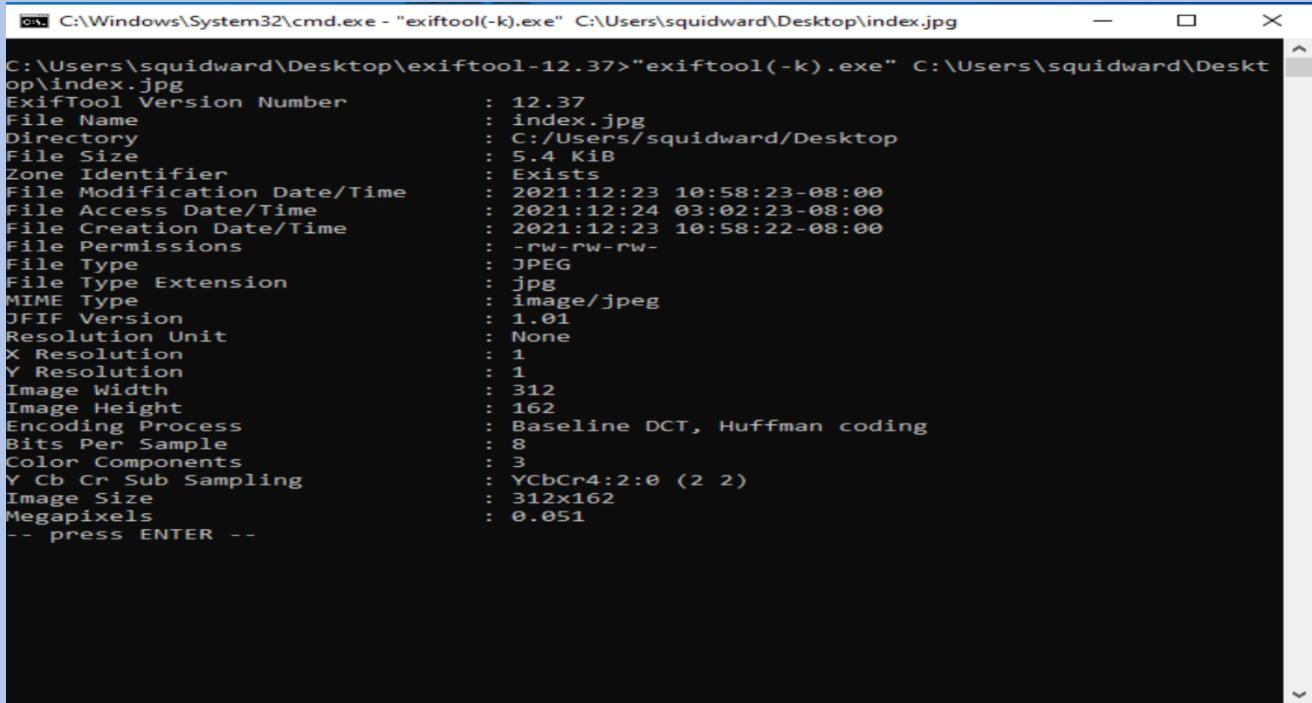
- Find the exif-tool file



- 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.



```
C:\Windows\System32\cmd.exe - "exiftool(-k).exe" C:\Users\squidward\Desktop\index.jpg
C:\Users\squidward\Desktop\exiftool-12.37>"exiftool(-k).exe" C:\Users\squidward\Desktop\index.jpg
ExifTool Version Number      : 12.37
File Name                   : index.jpg
Directory                   : C:/Users/squidward/Desktop
File Size                   : 5.4 Kib
Zone Identifier             : Exists
File Modification Date/Time : 2021:12:23 10:58:23-08:00
File Access Date/Time       : 2021:12:24 03:02:23-08:00
File Creation Date/Time    : 2021:12:23 10:58:22-08:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
Image Width                  : 312
Image Height                  : 162
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
YCbCr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                   : 312x162
Megapixels                   : 0.051
-- press ENTER --
```

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/](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 caught 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. PDFparser

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:

```
C:\Windows\System32\cmd.exe
pdf-parser, use it to parse a PDF document

Options:
  --version      show program's version number and exit
  -h, --help      show this help message and exit
  -m, --man       Print manual
  -s SEARCH, --search=SEARCH
                  string to search in indirect objects (except streams)
  -f, --filter    pass stream object through filters (FlateDecode,
                  ASCIIHexDecode, ASCII85Decode, LZWDecode and
                  RunLengthDecode only)
  -o OBJECT, --object=OBJECT
                  id(s) of indirect object(s) to select, use comma (,) to
                  separate ids (version independent)
  -r REFERENCE, --reference=REFERENCE
                  id of indirect object being referenced (version
                  independent)
  -e ELEMENTS, --elements=ELEMENTS
                  type of elements to select (cxtsi)
  -w, --raw        raw output for data and filters
  -a, --stats     display stats for pdf document
  -t TYPE, --type=TYPE type of indirect object to select
  -O, --objstm   parse stream of /ObjStm objects
  -v, --verbose    display malformed PDF elements
  -x EXTRACT, --extract=EXTRACT
                  filename to extract malformed content to
  -H, --hash      display hash of objects
  -n, --nocanonicalizedoutput
                  do not canonicalize the output
  -d DUMP, --dump=DUMP filename to dump stream content to
  -D, --debug     display debug info
  -c, --content   display the content for objects without streams or
                  with streams without filters
  --searchstream=SEARCHSTREAM
                  string to search in streams
  --unfiltered    search in unfiltered streams
  --casesensitive case sensitive search in streams
  --regex         use regex to search in streams
  --overridingfilters=OVERRIDINGFILTERS
                  override filters with given filters (use raw for the
                  raw stream content)
  -g, --generate   generate a Python program that creates the parsed PDF
                  file
  --generateembedded=GENERATEEMBEDDED
                  generate a Python program that embeds the selected
                  indirect object as a file
  -y YARA, --yara=YARA YARA rule (or directory or @file) to check streams
                  (can be used with option --unfiltered)
  --yarastrings   Print YARA strings
  --decoders=DECODERS decoders to load (separate decoders with a comma , ;
                  @file supported)
  --decoderoptions=DECODEROPTIONS
                  options for the decoder
  -k KEY, --key=KEY key to search in dictionaries
```

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.

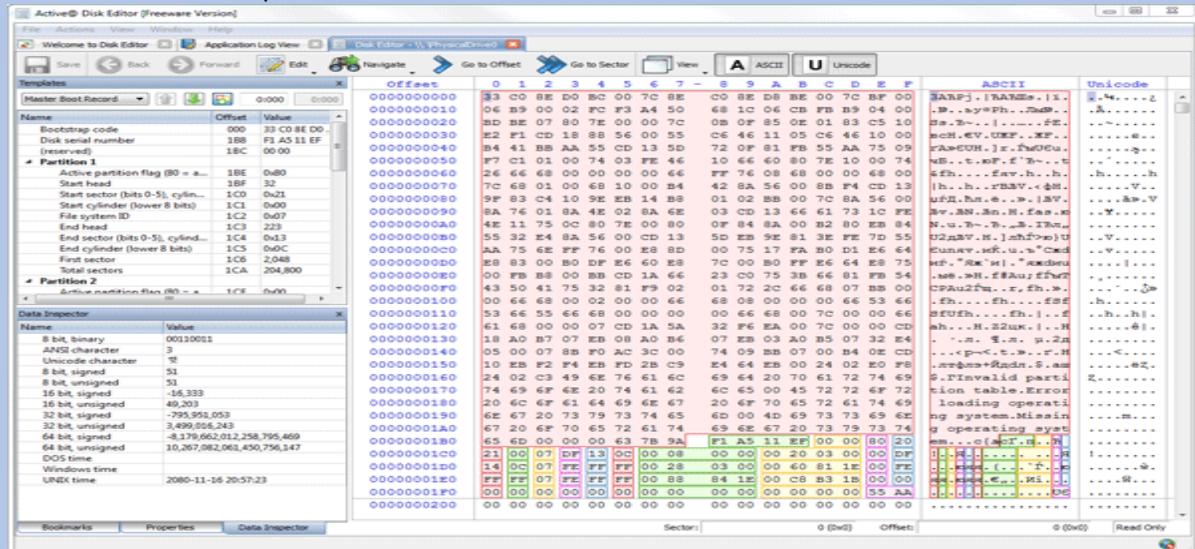
And to learn how to use FTK Imager, visit <https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/>

### 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.

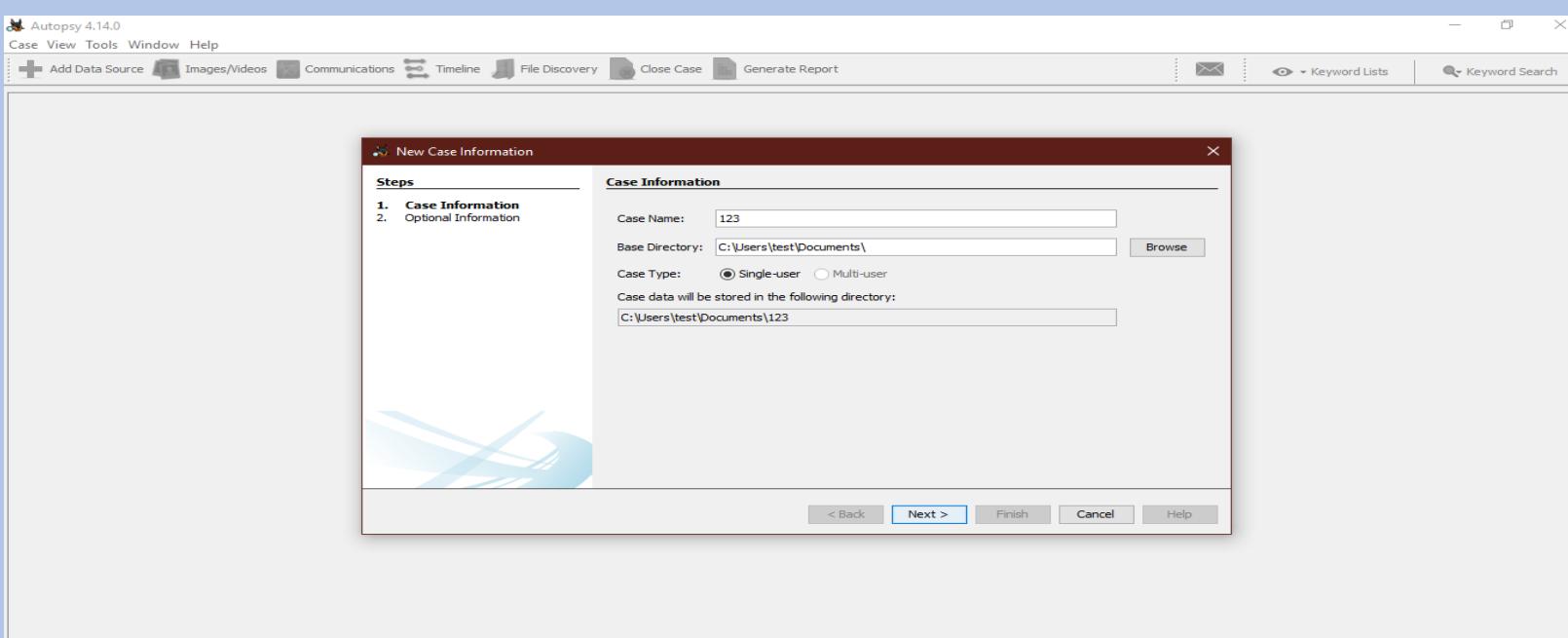
Download here: [www.sleuthkit.org/autopsy/](http://www.sleuthkit.org/autopsy/)

**Usage:**

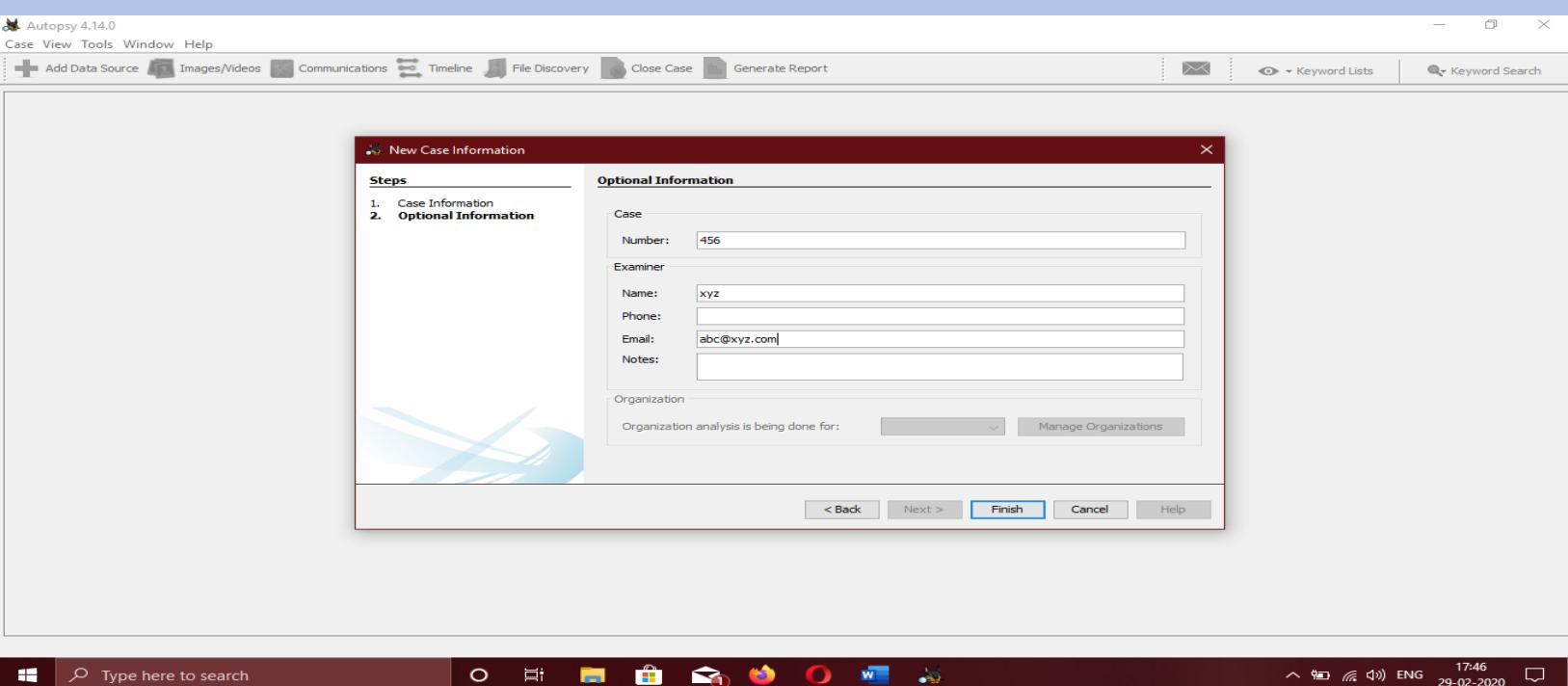
- **Step 1:** Run Autopsy and select “New Case”



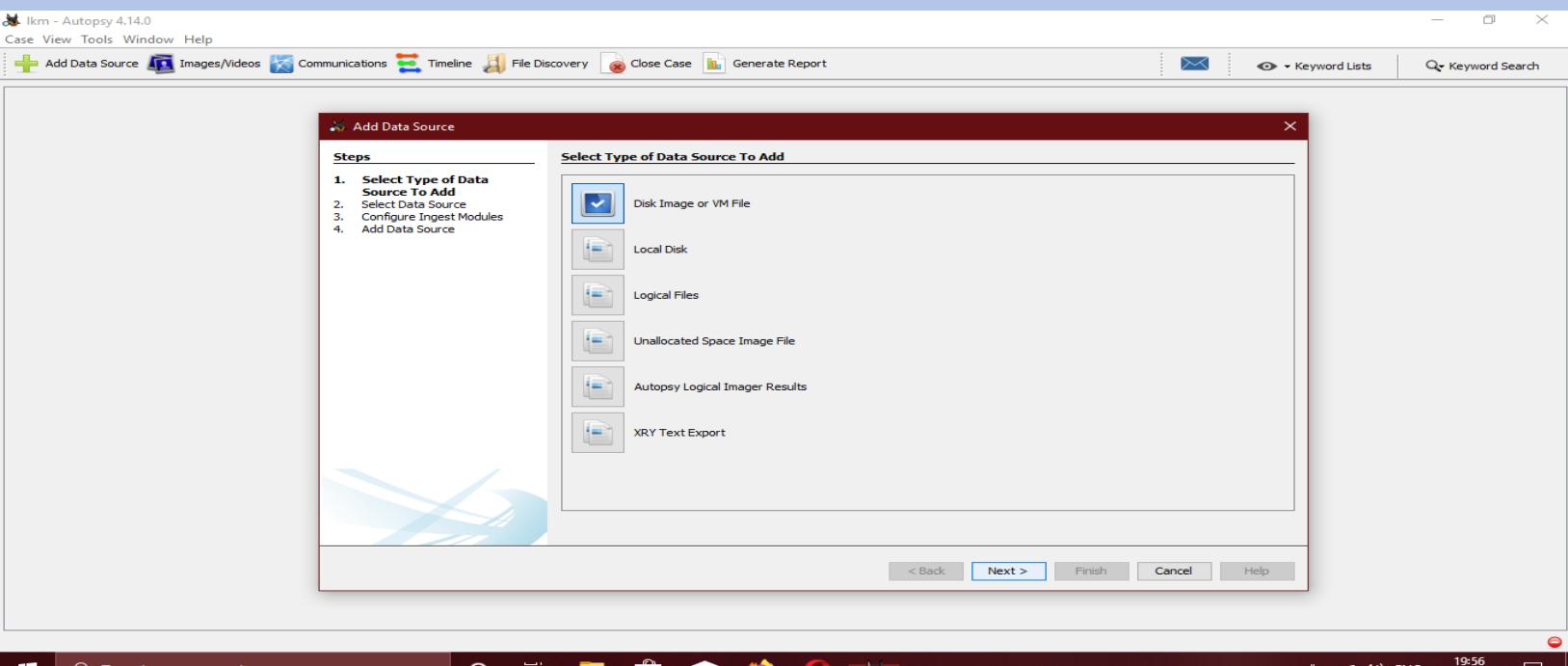
- **Step 2:** Provide the “Case Name” and the “Directory” to store the case file. Click on “Next”.



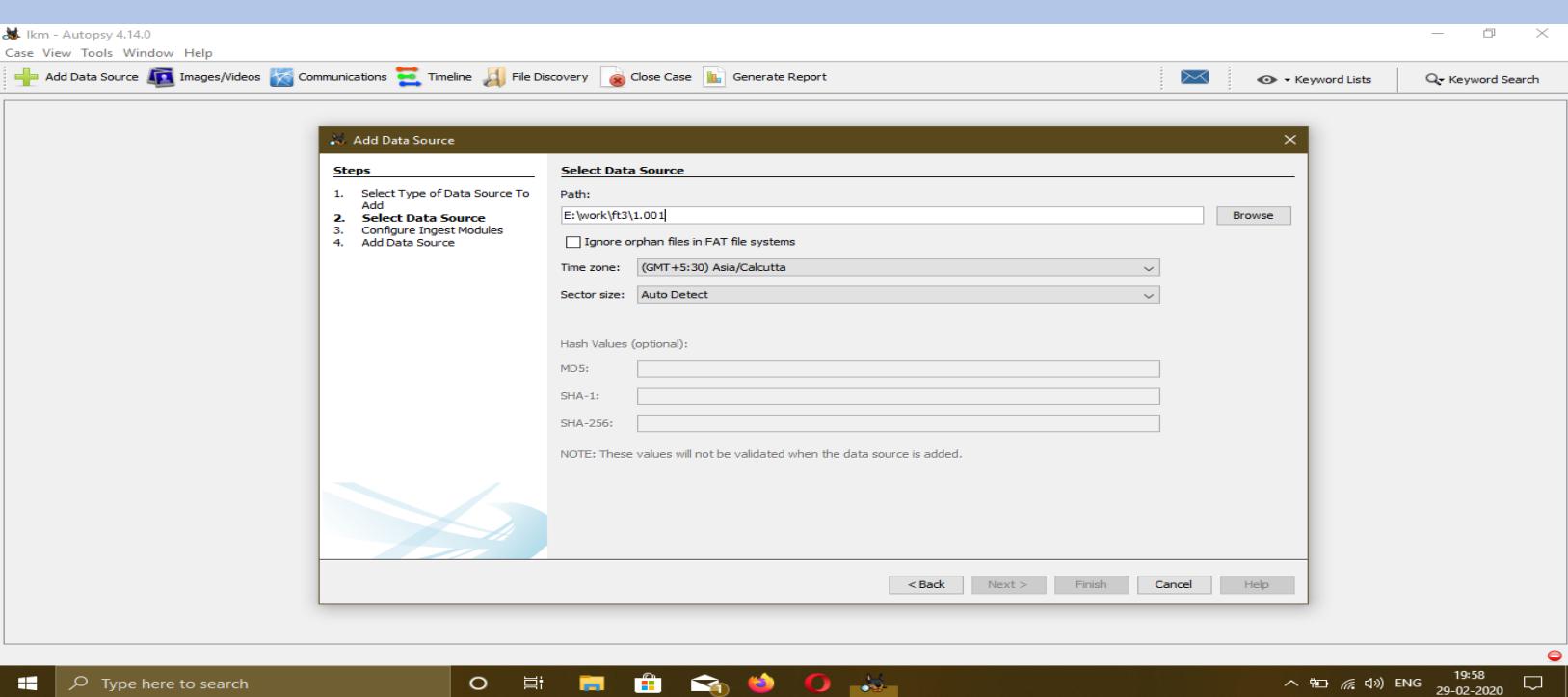
- **Step 3:** Add “Case Number” and examiner’s details, then click on “Finish”.



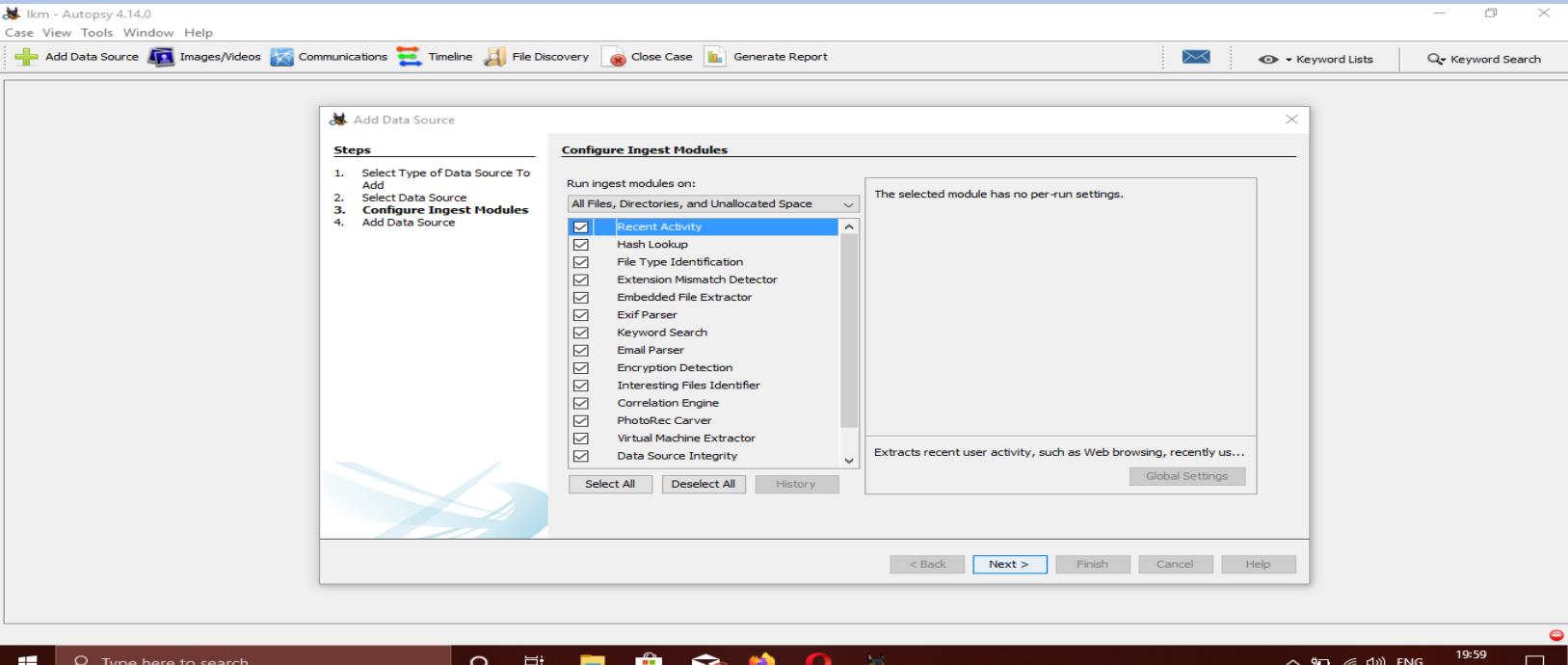
- **Step 4:** Choose the required data source type, in the case “Disk Image” and click on “Next”.



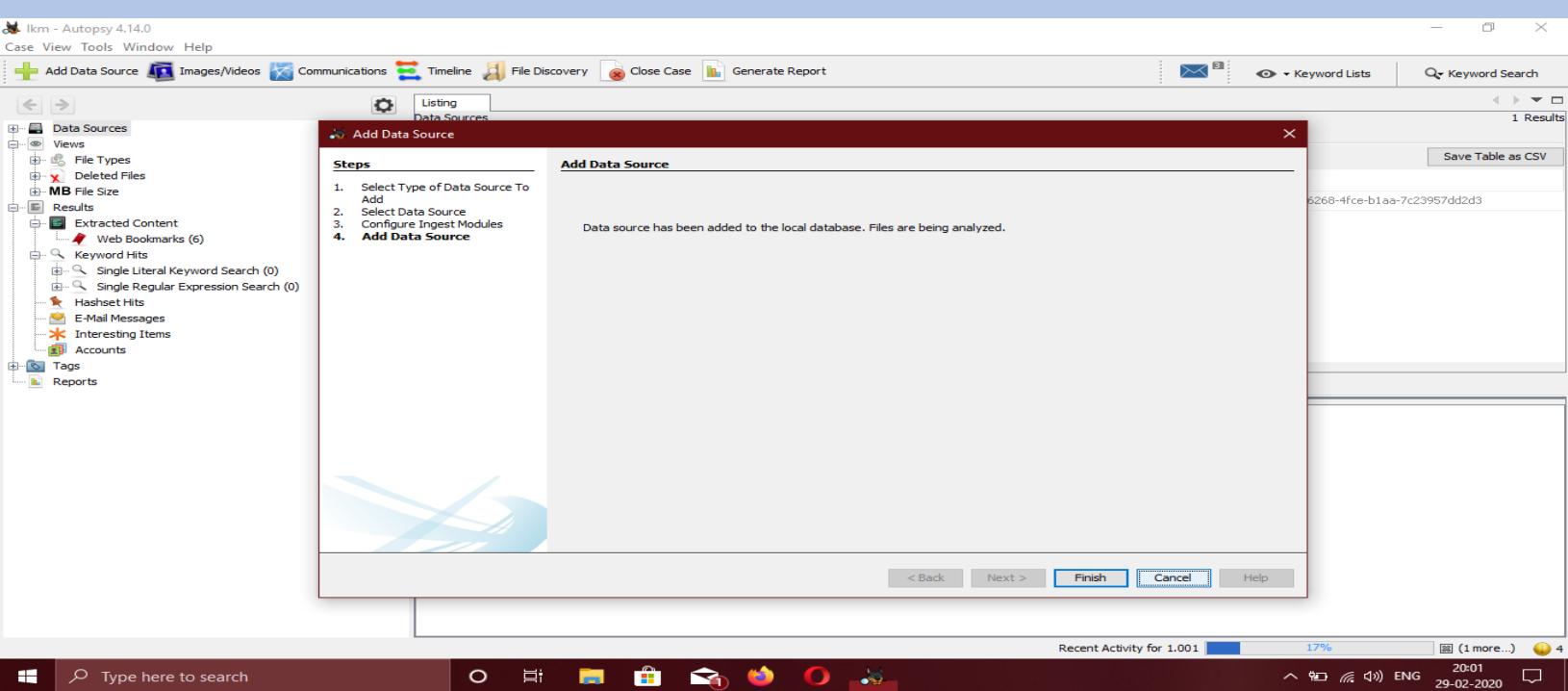
- **Step 5:** Give path of the data source and click on “Next”.



- **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.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
1.001	Image	4871301120	512	Asia/Calcutta	b11b5051-2bf4-4cf2-a318-a10c4025f3c3

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
```

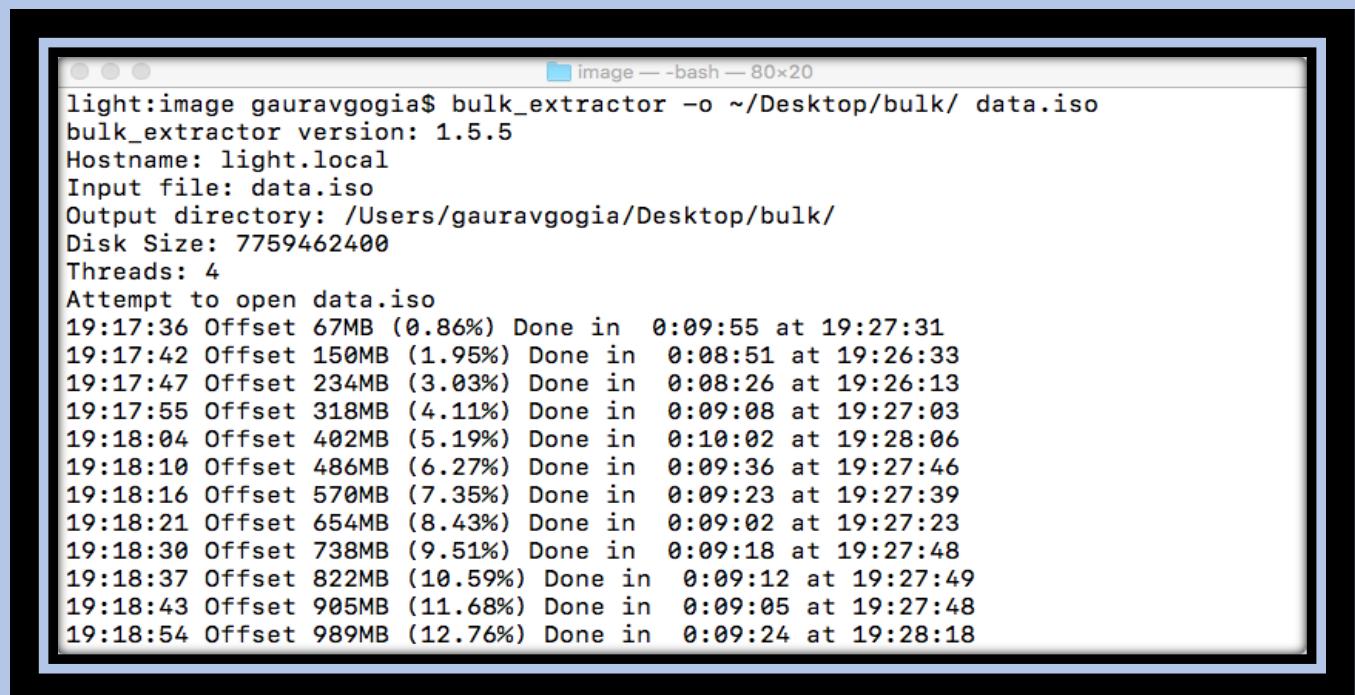
### 5- Bulk extractor

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

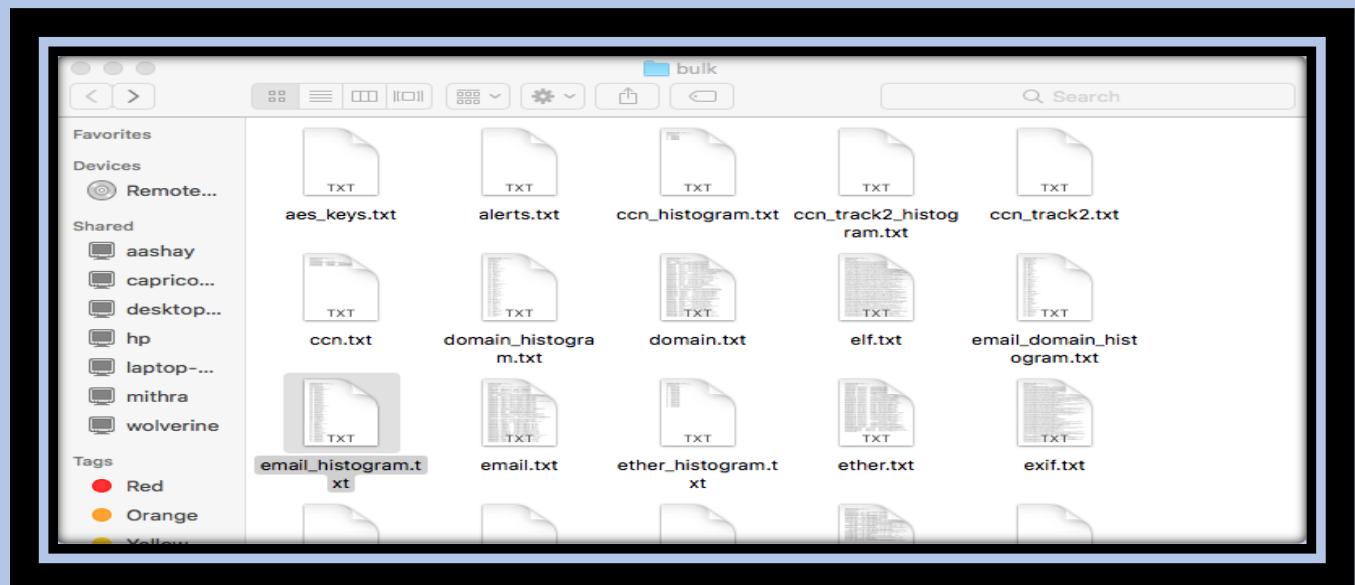
This is the command used in linux:

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

Usage:



```
light:image gauravgogia$ bulk_extractor -o ~/Desktop/bulk/ data.iso
bulk_extractor version: 1.5.5
Hostname: light.local
Input file: data.iso
Output directory: /Users/gauravgogia/Desktop/bulk/
Disk Size: 7759462400
Threads: 4
Attempt to open data.iso
19:17:36 Offset 67MB (0.86%) Done in 0:09:55 at 19:27:31
19:17:42 Offset 150MB (1.95%) Done in 0:08:51 at 19:26:33
19:17:47 Offset 234MB (3.03%) Done in 0:08:26 at 19:26:13
19:17:55 Offset 318MB (4.11%) Done in 0:09:08 at 19:27:03
19:18:04 Offset 402MB (5.19%) Done in 0:10:02 at 19:28:06
19:18:10 Offset 486MB (6.27%) Done in 0:09:36 at 19:27:46
19:18:16 Offset 570MB (7.35%) Done in 0:09:23 at 19:27:39
19:18:21 Offset 654MB (8.43%) Done in 0:09:02 at 19:27:23
19:18:30 Offset 738MB (9.51%) Done in 0:09:18 at 19:27:48
19:18:37 Offset 822MB (10.59%) Done in 0:09:12 at 19:27:49
19:18:43 Offset 905MB (11.68%) Done in 0:09:05 at 19:27:48
19:18:54 Offset 989MB (12.76%) Done in 0:09:24 at 19:28:18
```

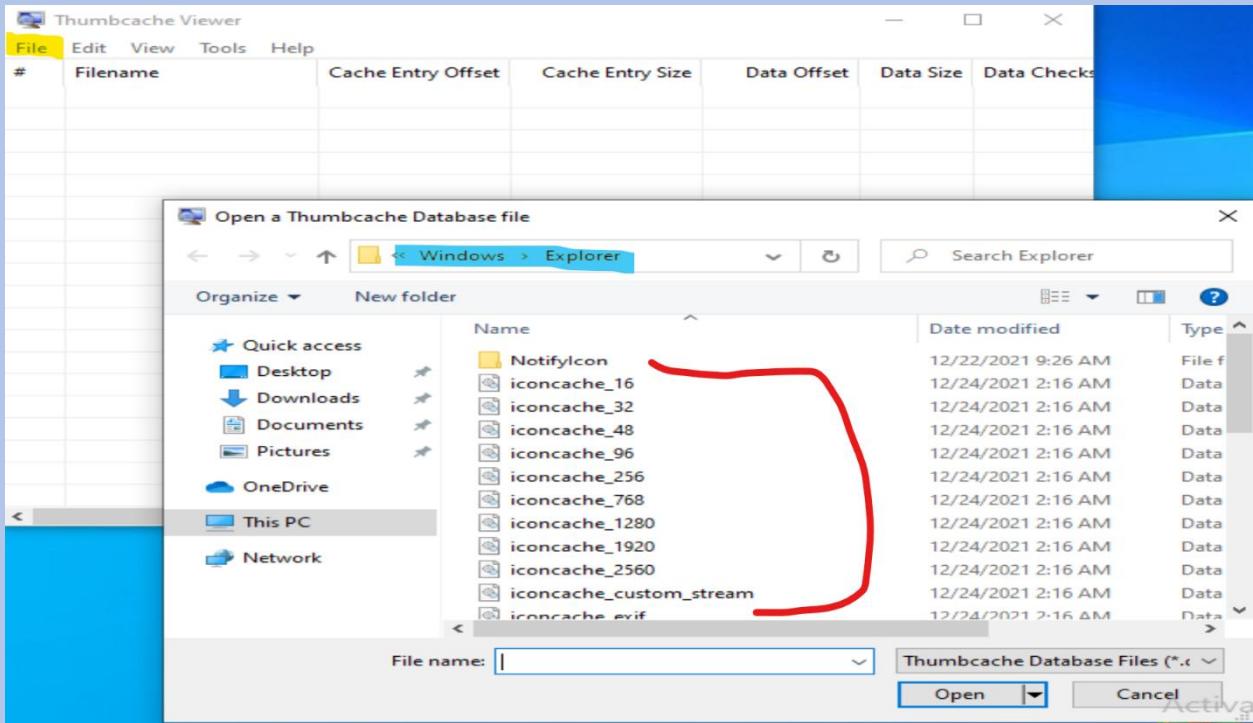


## 6- Thumbcache viewer

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 screenshot shows the 'Thumbcache Viewer' application with a list of thumbnail files. A small icon preview is visible next to the entry for file 8.

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checks
6	a70fdf502ed2b8c8.bmp	47304 B	9 KB	47394 B	9 KB	e58a8f86
7	9e65ce852008a0b.bmp	56760 B	9 KB	56850 B	9 KB	eb89c514
8	5b47ec6740da6dc8.bmp	66216 B	9 KB	66306 B	9 KB	558cefb7
9	756d98519735eebe.bmp	75672 B	9 KB	75762 B	9 KB	73507371
10	bfc824ead8ed8fa6.bmp	85128 B	9 KB	85218 B	9 KB	dc7f0daf
11	f61438c714275566.bmp	94584 B	9 KB	94674 B	9 KB	a68d25e8
12	4ae2c5bc7029bb28.bmp	104040 B	9 KB	104130 B	9 KB	62073658
13	c81720f6cac14156.bmp	113496 B	9 KB	113586 B	9 KB	2579b054
14	af5e518e2d93c12a.bmp	122952 B	9 KB	123042 B	9 KB	e72df6d1
15	bb69e900a0ac20cf0.bmp	132408 B	9 KB	132498 B	9 KB	a095ddd0
16	15997dbac96da84c.bmp	141864 B	9 KB	141954 B	9 KB	a095dd00
17	aa821c4eff6efb38.bmp	151320 B	9 KB	151410 B	9 KB	b6ffaf45a
18	2f423a561be9d9c9.bmp	160776 B	9 KB	160866 B	9 KB	dc7f0daf
19	df612488fd7d75db.bmp	170232 B	9 KB	170322 B	9 KB	134ba204
20	18738ad624877a5.bmp	179688 B	9 KB	179778 B	9 KB	a980d43f
21	eef32a71aa06e95.bmp	189144 B	9 KB	189234 B	9 KB	2709fd57
22	455f3703e2b231f.bmp	198600 B	9 KB	198690 B	9 KB	bc817cbf
23	4742c5bc6fbae3e6.bmp	208056 B	9 KB	208146 B	9 KB	9c221328
24	cccd5180b23a7f898.bmp	217512 B	9 KB	217602 B	9 KB	31e62e9f

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.

```
C:\Users\squidward\Desktop\Tools\Tools\LECmd>LECmd.exe -f C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\AW3DXW.lnk
LECmd version 1.3.2.1
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
Command line: -f C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\AW3DXW.lnk
Warning: Administrator privileges not found!
Processing 'C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\AW3DXW.lnk'
Source file: C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\AW3DXW.lnk
  Source created: 2021-12-24 12:01:09
  Source modified: 2021-12-24 14:16:09
  Source accessed: 2021-12-24 14:16:08
--- Header ---
  Target created: 2021-12-20 10:37:26
  Target modified: 2021-12-20 19:22:07
  Target accessed: 2021-12-20 10:37:27
  File size: 829,394
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir,IsUnicode, DisableKnownFolderTracking
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SWNormal (Activates and displays the window. The window is restored to its original size and position if the window is minimized or maximized.)
)
Relative Path: .....\..\..\..\..\..\Downloads\module\Lab 4\AW3DXW
Working Directory: C:\Users\squidward\Downloads\module\Lab 4
--- Link information ---
Flags: VolumeIdAndLocalBasePath
>>Volume Information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 76F53904
  Label: (No label)
  Local path: C:\Users\squidward\Downloads\module\Lab 4\AW3DXW
--- Target ID information (Format: Type ==> Value) ---
  Absolute path: My Computer\Downloads\module\Lab 4\AW3DXW
  -Root folder: GUID ==> My Computer
  -Root folder: GUID ==> Downloads
  -Directory ==> module
    -Short name: module
    -Modified: 2021-12-20 10:37:22
    -Extension block count: 1
      ----- Block 0 (0x00000000) -----
      Long name: module
      Created: 2021-12-20 10:37:22
      Last modified: 2021-12-24 11:37:00
      MFT entry/sequence #: 266199/2 (0x40FD7/0x2)

----- Activate Windows -----
Go to Settings to activate Windows.

-----
```

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

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

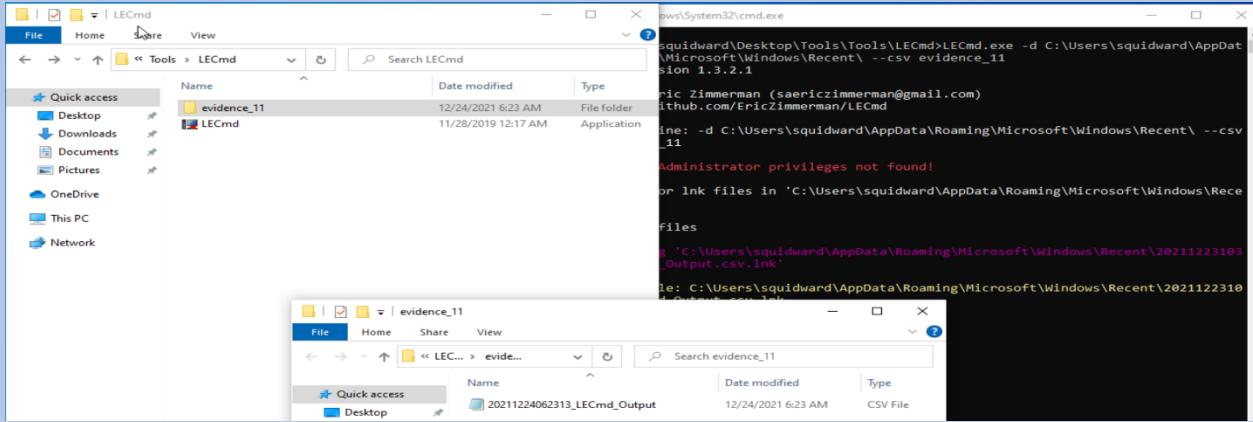
C:\Users\squidward\Desktop\Tools\Tools\LECmd>LECmd.exe -d C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\
LECmd version 1.3.2.1
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/LECmd
Command line: -d C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\
Warning: Administrator privileges not found!
Looking for lnk files in 'C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\'

Found 50 files

Processing 'C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\2021122310393
0_LECmd_Output.csv.lnk'

Source file: C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\202112231039
30_LECmd_Output.csv.lnk
  Source created: 2021-12-23 18:40:34
  Source modified: 2021-12-23 18:40:34
  Source accessed: 2021-12-24 14:20:32
--- Header ---
  Target created: 2021-12-23 18:39:30
  Target modified: 2021-12-23 18:39:31
  Target accessed: 2021-12-23 18:39:32
  File size: 17,216
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir,IsUnicode, Dis
ableKnownFolderTracking
  File attributes: FileAttributeArchive
```

**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.

Option 2 - Enter an URL					Load URL																																																																																																																																															
Option 3 - paste Into Grid below																																																																																																																																																				
Step 2: Choose input options (optional)																																																																																																																																																				
<a href="#">Clear All</a> <a href="#">Save as Excel</a>																																																																																																																																																				
Save Your result: <a href="#">20211224062313_LEC .csv or .xlsx</a> <a href="#">Download CSV</a> EOL: CRLF <input checked="" type="checkbox"/> Include Header																																																																																																																																																				
<table border="1"> <thead> <tr> <th>A</th><th>B</th><th>C</th><th>D</th><th>E</th></tr> </thead> <tbody> <tr><td>1</td><td>SourceFile</td><td>SourceCreated</td><td>SourceLastModified</td><td>SourceAccessed</td><td>TargetCreated</td></tr> <tr><td>2</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\20211223103930..._LECmd_Output.csv.Ink</td><td>2021-12-23 18:40:34</td><td>2021-12-23 18:40:34</td><td>2021-12-24 14:22:54</td><td>2021-12-23 18:39:30</td></tr> <tr><td>3</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent32.Ink</td><td>2021-12-23 18:58:41</td><td>2021-12-23 18:59:39</td><td>2021-12-24 14:22:54</td><td>2021-12-23 18:58:39</td></tr> <tr><td>4</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent43.Ink</td><td>2021-12-23 18:58:51</td><td>2021-12-23 18:58:51</td><td>2021-12-24 14:22:55</td><td>2021-12-23 18:58:50</td></tr> <tr><td>5</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\7e4dc80246863e3:customDestinations-ms.Ink</td><td>2021-12-23 10:19:46</td><td>2021-12-23 10:19:46</td><td>2021-12-24 14:22:55</td><td>2021-12-19 08:16:10</td></tr> <tr><td>6</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentAV3DXW.Ink</td><td>2021-12-24 12:01:09</td><td>2021-12-22 12:01:09</td><td>2021-12-24 14:22:55</td><td>2021-12-20 10:37:26</td></tr> <tr><td>7</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentCustomDestinations.Ink</td><td>2021-12-23 10:19:46</td><td>2021-12-23 10:19:46</td><td>2021-12-24 14:22:56</td><td>2021-12-19 08:16:10</td></tr> <tr><td>8</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentDownloads.Ink</td><td>2021-12-20 08:09:09</td><td>2021-12-22 11:15:38</td><td>2021-12-24 14:22:56</td><td>2021-12-20 08:11:50</td></tr> <tr><td>9</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentEvidence.Ink</td><td>2021-12-23 18:40:34</td><td>2021-12-23 18:40:34</td><td>2021-12-24 14:22:56</td><td>2021-12-23 18:39:30</td></tr> <tr><td>10</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recentexitfile300_e.Ink</td><td>2021-12-20 10:48:38</td><td>2021-12-20 10:51:27</td><td>2021-12-24 14:22:57</td><td>2021-12-20 10:48:07</td></tr> <tr><td>11</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recentexitfile12..37.Ink</td><td>2021-12-20 10:50:25</td><td>2021-12-20 10:54:10</td><td>2021-12-24 14:22:57</td><td>2021-12-20 10:48:28</td></tr> <tr><td>12</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentPictures.(2).Ink</td><td>2021-12-24 10:43:24</td><td>2021-12-24 10:43:24</td><td>2021-12-24 14:22:58</td><td>2021-12-23 18:57:37</td></tr> <tr><td>13</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentPictures.Ink</td><td>2021-12-23 18:57:41</td><td>2021-12-23 18:59:39</td><td>2021-12-24 14:22:58</td><td>2021-12-23 18:57:37</td></tr> <tr><td>14</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentIndex.Ink</td><td>2021-12-23 18:58:24</td><td>2021-12-24 11:02:21</td><td>2021-12-24 14:22:58</td><td>2021-12-23 18:58:22</td></tr> <tr><td>15</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentJumpLists.Ink</td><td>2021-12-24 13:33:12</td><td>2021-12-24 13:33:12</td><td>2021-12-24 14:22:59</td><td>2021-12-24 13:33:05</td></tr> <tr><td>16</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab.4.Ink</td><td>2021-12-24 12:01:09</td><td>2021-12-24 12:01:09</td><td>2021-12-24 14:22:59</td><td>2021-12-20 10:37:20</td></tr> <tr><td>17</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab.5.Ink</td><td>2021-12-20 11:17:35</td><td>2021-12-20 11:25:18</td><td>2021-12-24 14:22:59</td><td>2021-12-20 10:37:20</td></tr> <tr><td>18</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab-7-recovering-a-corrupted-disk-mbr-case.Ink</td><td>2021-12-21 10:22:37</td><td>2021-12-21 10:22:37</td><td>2021-12-24 14:23:00</td><td>2021-12-21 10:22:29</td></tr> <tr><td>19</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab.8-Copy001.Ink</td><td>2021-12-23 08:40:41</td><td>2021-12-23 08:45:25</td><td>2021-12-24 14:23:00</td><td>2021-12-23 08:40:28</td></tr> <tr><td>20</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab.001.part.Ink</td><td>2021-12-21 12:22:41</td><td>2021-12-21 13:20:07</td><td>2021-12-24 14:23:01</td><td>2021-12-21 12:21:40</td></tr> <tr><td>21</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab8a.Ink</td><td>2021-12-22 19:21:36</td><td>2021-12-22 19:21:36</td><td>2021-12-24 14:23:02</td><td>2021-12-22 19:00:59</td></tr> <tr><td>22</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab8a.Ink</td><td>2021-12-22 18:15:42</td><td>2021-12-22 18:47:33</td><td>2021-12-24 14:23:02</td><td>2021-12-22 18:14:42</td></tr> <tr><td>23</td><td>C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentLab8a_Copy001.Ink</td><td>2021-12-23 08:45:25</td><td>2021-12-23 08:45:25</td><td>2021-12-24 14:23:03</td><td>2021-12-23 08:42:14</td></tr> </tbody> </table>					A	B	C	D	E	1	SourceFile	SourceCreated	SourceLastModified	SourceAccessed	TargetCreated	2	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\20211223103930..._LECmd_Output.csv.Ink	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\Recent32.Ink	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\Recent43.Ink	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\7e4dc80246863e3:customDestinations-ms.Ink	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\RecentAV3DXW.Ink	2021-12-24 12:01:09	2021-12-22 12:01:09	2021-12-24 14:22:55	2021-12-20 10:37:26	7	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentCustomDestinations.Ink	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\RecentDownloads.Ink	2021-12-20 08:09:09	2021-12-22 11:15:38	2021-12-24 14:22:56	2021-12-20 08:11:50	9	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentEvidence.Ink	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\Recentexitfile300_e.Ink	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\Recentexitfile12..37.Ink	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\RecentPictures.(2).Ink	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\RecentPictures.Ink	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\RecentIndex.Ink	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\RecentJumpLists.Ink	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\RecentLab.4.Ink	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\RecentLab.5.Ink	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\RecentLab-7-recovering-a-corrupted-disk-mbr-case.Ink	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\RecentLab.8-Copy001.Ink	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\RecentLab.001.part.Ink	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\RecentLab8a.Ink	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\RecentLab8a.Ink	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\RecentLab8a_Copy001.Ink	2021-12-23 08:45:25	2021-12-23 08:45:25	2021-12-24 14:23:03	2021-12-23 08:42:14	
A	B	C	D	E																																																																																																																																																
1	SourceFile	SourceCreated	SourceLastModified	SourceAccessed	TargetCreated																																																																																																																																															
2	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\Recent\20211223103930..._LECmd_Output.csv.Ink	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\Recent32.Ink	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\Recent43.Ink	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\7e4dc80246863e3:customDestinations-ms.Ink	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\RecentAV3DXW.Ink	2021-12-24 12:01:09	2021-12-22 12:01:09	2021-12-24 14:22:55	2021-12-20 10:37:26																																																																																																																																															
7	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentCustomDestinations.Ink	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\RecentDownloads.Ink	2021-12-20 08:09:09	2021-12-22 11:15:38	2021-12-24 14:22:56	2021-12-20 08:11:50																																																																																																																																															
9	C:\Users\squidward\AppData\Roaming\Microsoft\Windows\RecentEvidence.Ink	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\Recentexitfile300_e.Ink	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\Recentexitfile12..37.Ink	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\RecentPictures.(2).Ink	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\RecentPictures.Ink	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\RecentIndex.Ink	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\RecentJumpLists.Ink	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\RecentLab.4.Ink	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\RecentLab.5.Ink	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\RecentLab-7-recovering-a-corrupted-disk-mbr-case.Ink	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\RecentLab.8-Copy001.Ink	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\RecentLab.001.part.Ink	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\RecentLab8a.Ink	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\RecentLab8a.Ink	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\RecentLab8a_Copy001.Ink	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/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](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 file 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

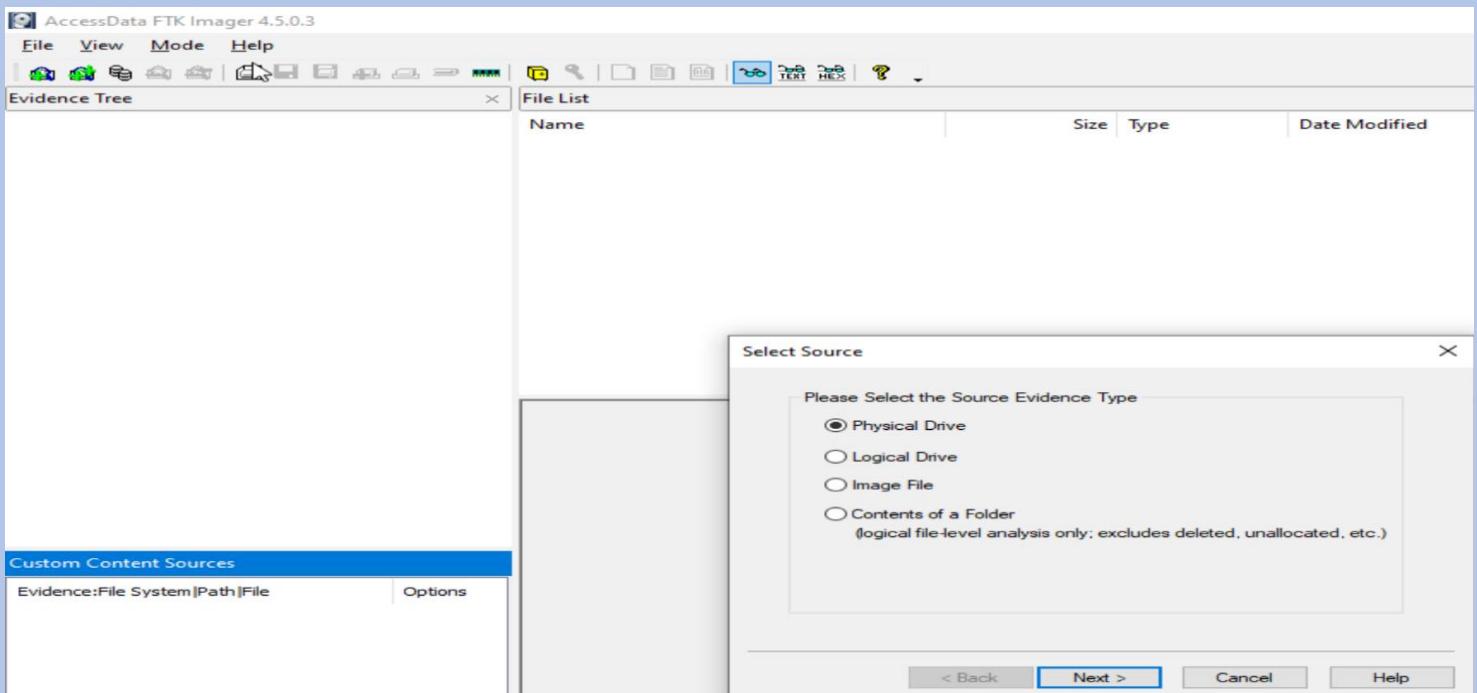
To get information from these files, we can use the following tool:

[JumpList Explorer](#) by Eric Zimmerman, Download here:

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

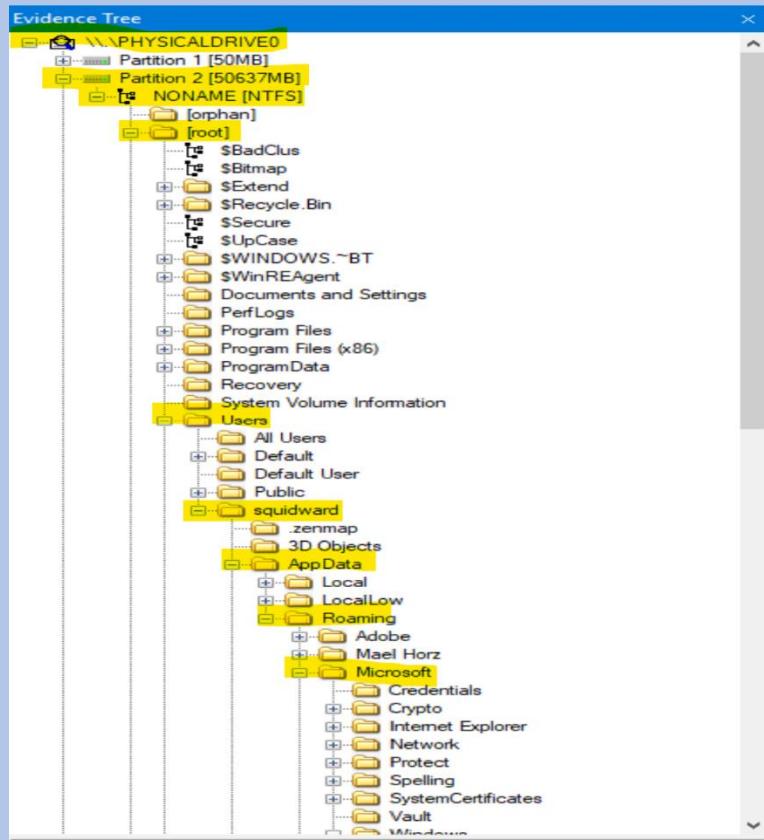
### Usage:

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

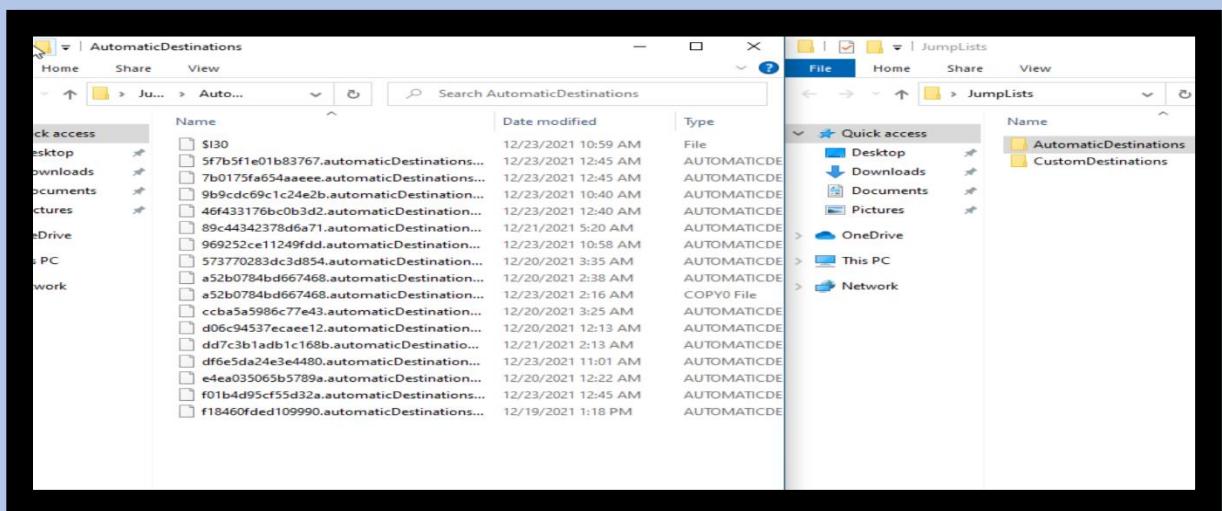


Now we go to the automatic and custom destinations so we can save them for later use. We can find them in this directory:

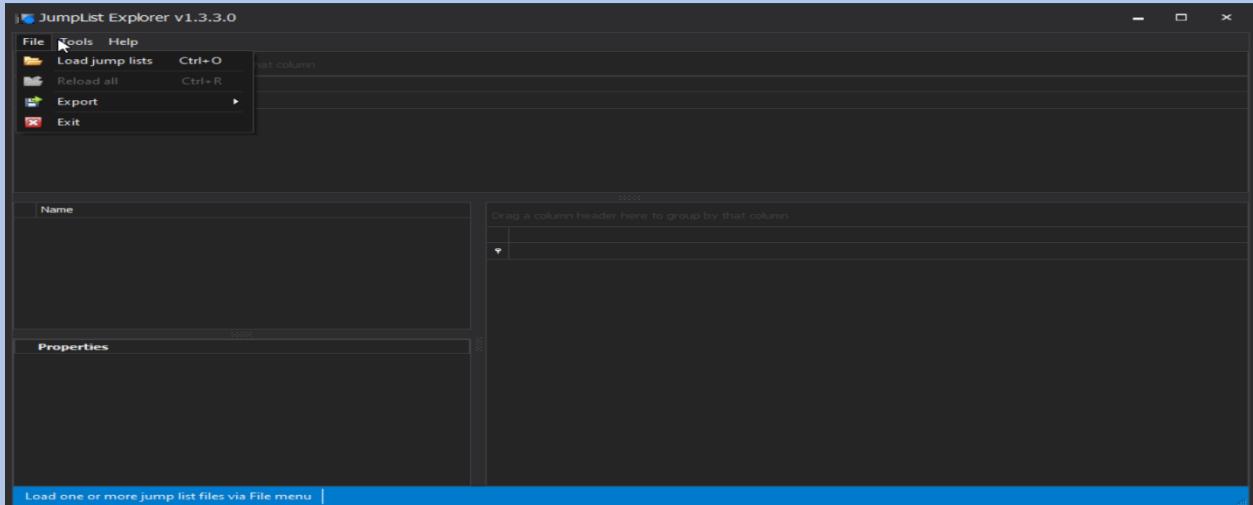
C:\Users\<Name>\AppData\Roaming\Microsoft\Windows\Recent\



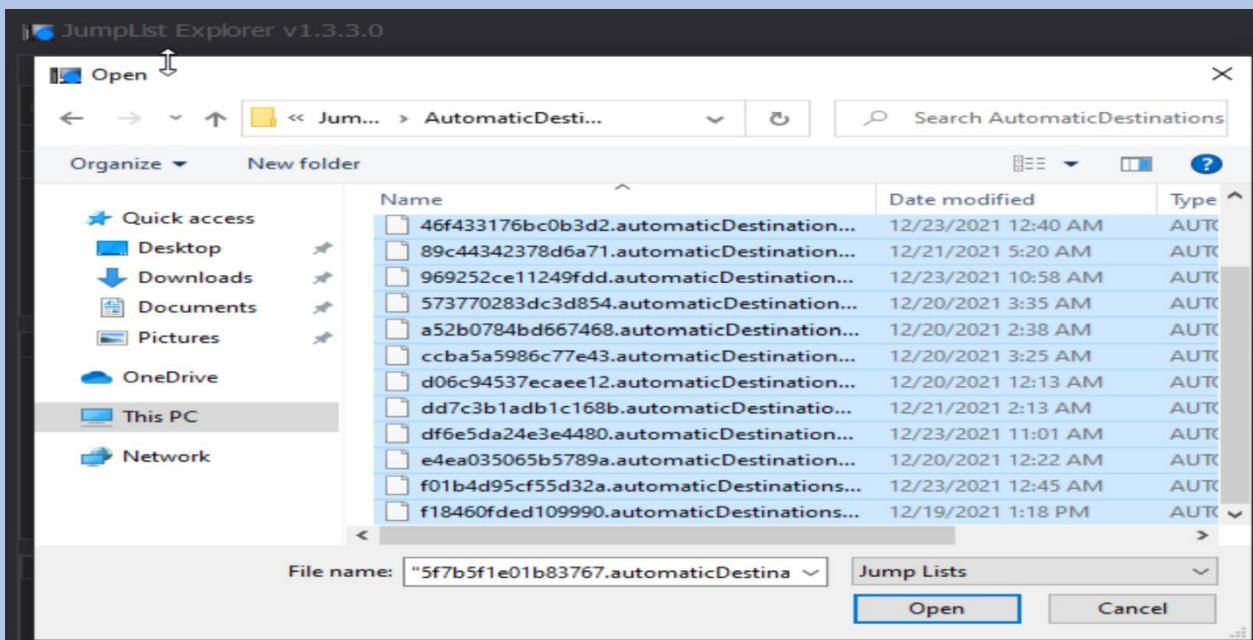
- **Step 2:** Now we create a file in the Desktop, and export both “Automatic-Destination” and “Custom-Destination” to the created file, so we can use it later via JumpList explorer.



- **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.

The screenshot shows the JumpList Explorer application interface. On the left, there's a tree view under 'Source File Name' showing several jump lists, with one expanded to show its entries. The main area contains two tables. The top table has columns: 'Source File Name', 'Jump List Type', 'App ID', 'App ID Description', 'Link File Count', and 'File Size'. The bottom table has columns: 'Entry Number', 'Target Created On', 'Target Modified On', 'Target Accessed On', 'Absolute Path', 'Extra Block Count', and 'Interaction Count'. Both tables have a header row with sorting icons.

## 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\INFO02"
          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
```

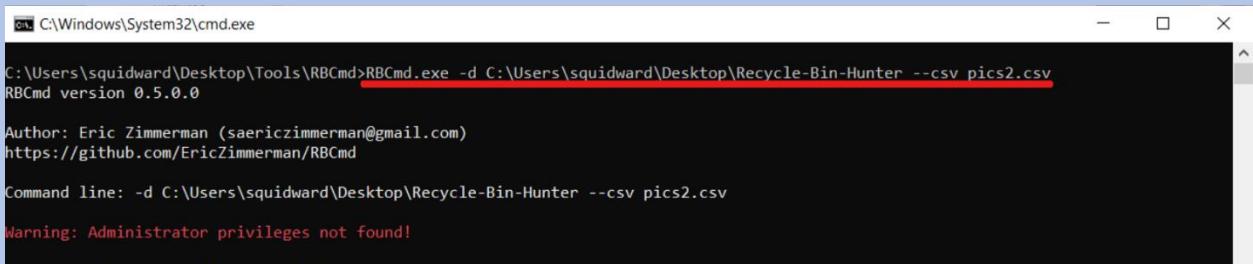
To scan a file, use this command:

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

The screenshot shows a Windows Command Prompt window with the title 'C:\Windows\System32\cmd.exe'. The command entered is 'RBCmd.exe -f C:\Users\squidward\Desktop\Recycle-Bin-Hunter\RP3TBNW.jpg --csv pic.csv'. Below the command, the output shows the RBCmd version (0.5.0.0), author information (Eric Zimmerman), and a warning message: 'Warning: Administrator privileges not found!'. The command line and output text are highlighted in yellow and cyan respectively.

**To scan a directory, use this command:**

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



```
C:\Windows\System32\cmd.exe
C:\Users\squidward\Desktop\Tools\RBCmd>RBCmd.exe -d C:\Users\squidward\Desktop\Recycle-Bin-Hunter --csv pics2.csv
RBCmd version 0.5.0.0

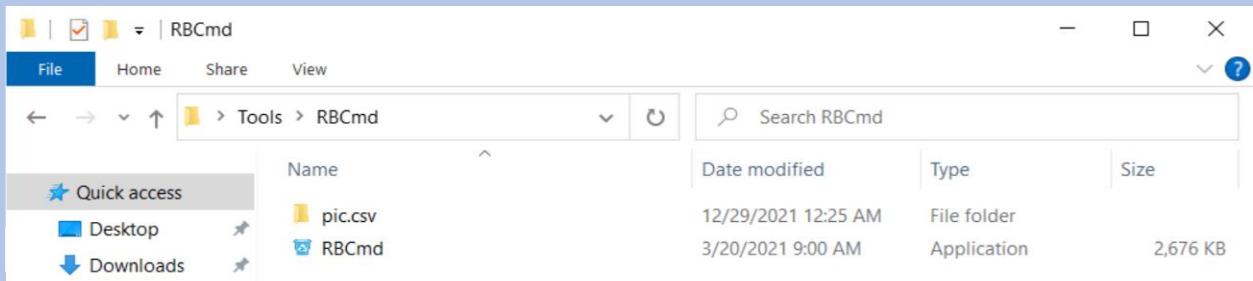
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RBCmd

Command line: -d C:\Users\squidward\Desktop\Recycle-Bin-Hunter --csv pics2.csv

Warning: Administrator privileges not found!
```

**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

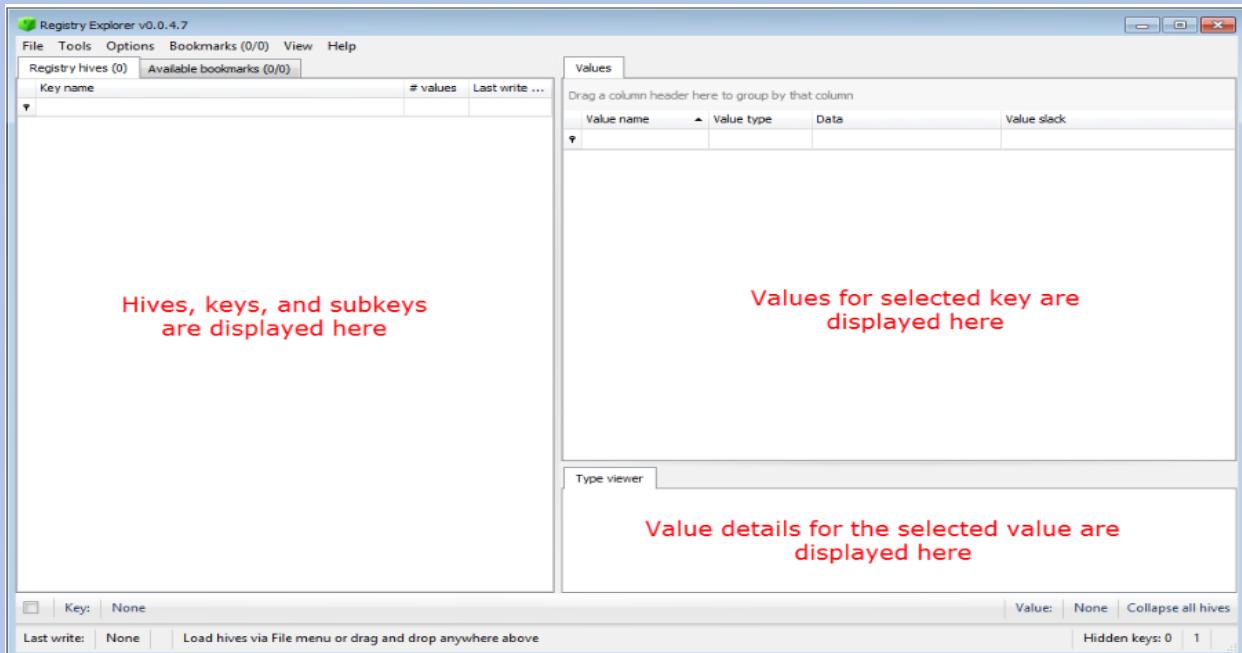
**Registry Explorer** is a GUI based tool used to view the contents of offline Registry Hives. It has the ability to load multiple hives at once, search across all loaded hives using strings or regular expressions, exporting of data, and much more.

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.

File Tools Options Bookmarks (1/0) View Help

Registry hives (18) Available bookmarks (41/0)

Key name	# values
C:\Temp\UsrClass account rename.dat	
S-1-5-21-1141529136-2431258765-826847743-1000_Cla...	1
C:\Temp\UsrClass CDburn UNC fat filesystem .dat	
S-1-5-21-1876483248-2010845669-2174274418-1000_Cl...	1
C:\Temp\UsrClass zip file network stuff.dat	
S-1-5-21-2036804247-3058324640-2116585241-1114_Cl...	0
C:\Temp\UsrClass unicode and network.dat	
S-1-5-21-3640650475-3814930019-1523317725-1003_Cl...	1
C:\Temp\usrclass.dat	
S-1-5-21-1141529136-2431258765-826847743-1000_Cla...	1
C:\Temp\UsrClass FTP.dat	
S-1-5-21-2417227394-2575385136-2411922467-1105_Cl...	0
Unassociated deleted records	0

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\**

### **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](https://www.nirsoft.net/utils/shadow_copy_view.html)
- Autopsy for Windows -- [www.sleuthkit.org/autopsy/](http://www.sleuthkit.org/autopsy/)
- PhotoRec -- <https://recoverit.wondershare.com/photo-recovery/how-to-use-photorec.html>