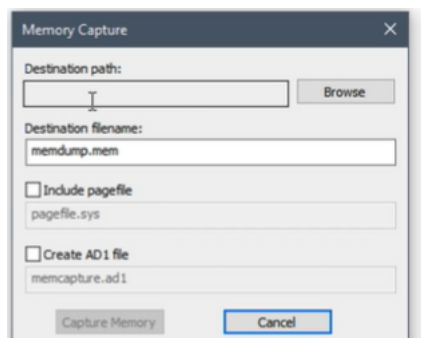
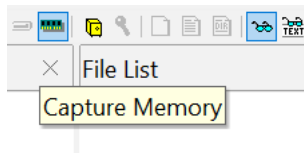


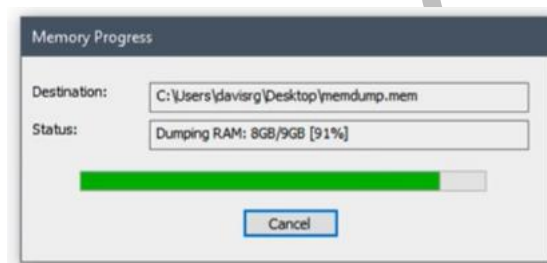
Image creation

Always obtaining volatile data:



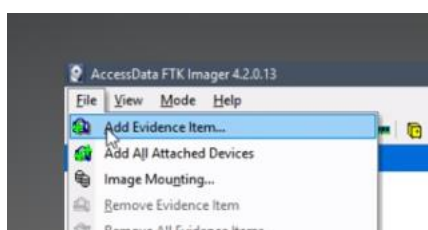
Browse must be on external drive.

Then capture memory. example



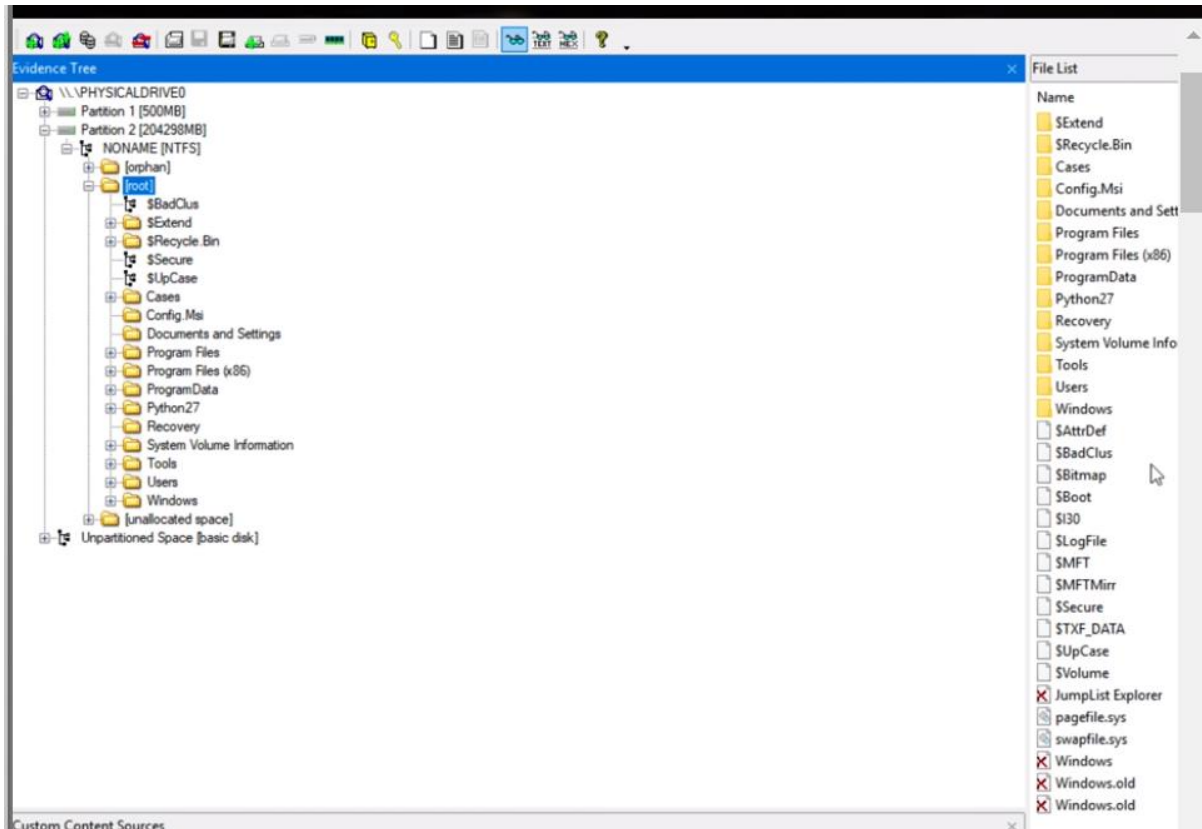
One of the least known features of FTK Imager is its capability to easily create custom content images. Custom content images contain only selected files, folders, and file types based on file extensions. You can create a custom content image from a live system, a dead system (attached to a write block), or from an image file. The process of creating a custom content image starts by using the preview feature to view and select the files you want included in your image.

Add evidence.

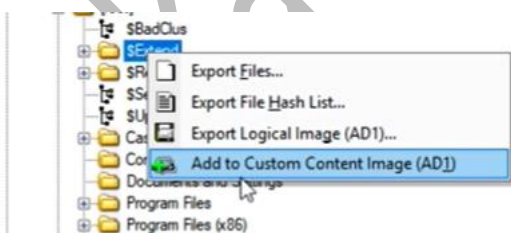


Select source → select drive → finish.

You must be interested in root folder where you get everything.

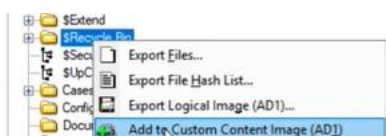


First thing to collect. **\$extend** (Which contain metadata file)



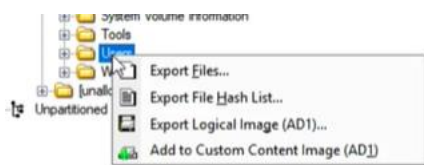
\$extend contain feature related NTFS data and metadata files

Next thing. **\$recycle bin**

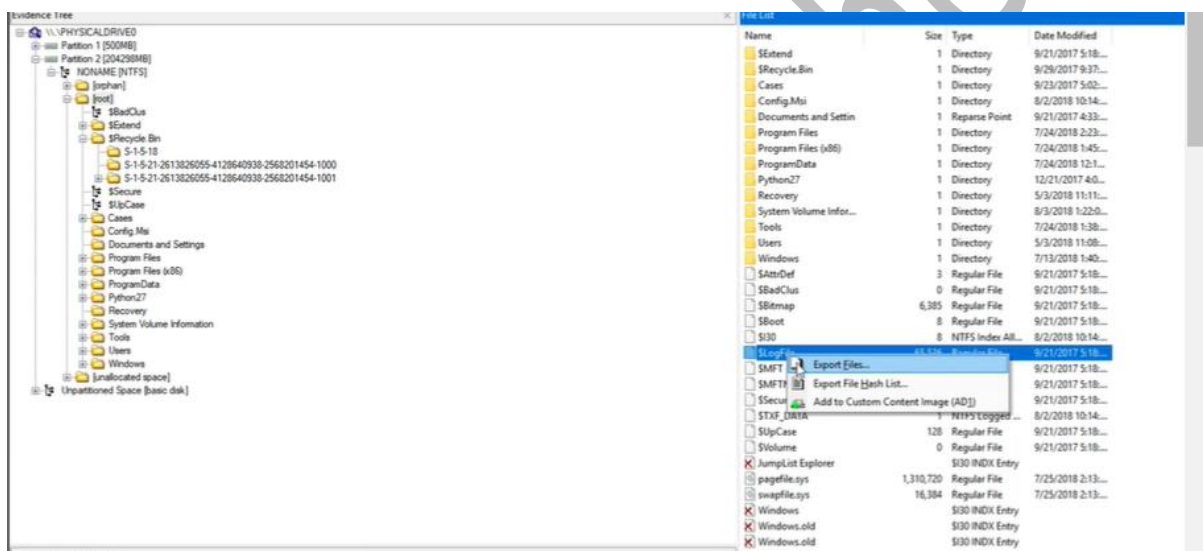


Contain series of SIDs of each user in the system which represent each user recycle bin.

Next Thing. Users (directory)



Next thing. \$log file



A log file in a file system serves as a transaction journal, recording all data related to file system activity before the activity actually occurs. Its primary purpose is to ensure the integrity of transactions in the event of a system crash or failure. By logging transactions before they are executed, the file system can roll them back or complete them once the system comes back online, thus preventing data loss or corruption.

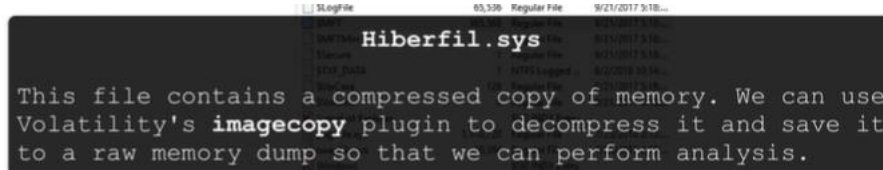
Next thing. \$MFT

\$LogFile	65,536	Regular File	9/21/2017 5:18:...
\$MFT	365,568	Regular File	9/21/2017 5:18:...
\$MFTMirr	4	Regular File	9/21/2017 5:18:...

Critical file in the entire NTFS File system it is a master file table which is basically a database than contains information about every file and directory on the system including their name there timestamps(modified, accessed, changed) there permission and much more.

Next thing. **Hiberfile.sys, Pagefile.sys, Swapfile.sys**

Hiberfile.sys: -often found on laptops and it supports hibernation when the system would suspend when battery is low for example, which contain an entire copy of RAM in the hiberfile.



```
Hiberfil.sys
This file contains a compressed copy of memory. We can use
Volatility's imagecopy plugin to decompress it and save it
to a raw memory dump so that we can perform analysis.
```



File Name	Size	Type	Modified
pagefile.sys	1,310,720	Regular File	7/25/2018 2:13:...
swapfile.sys	16,384	Regular File	7/25/2018 2:13:...

Next thing. **Program**

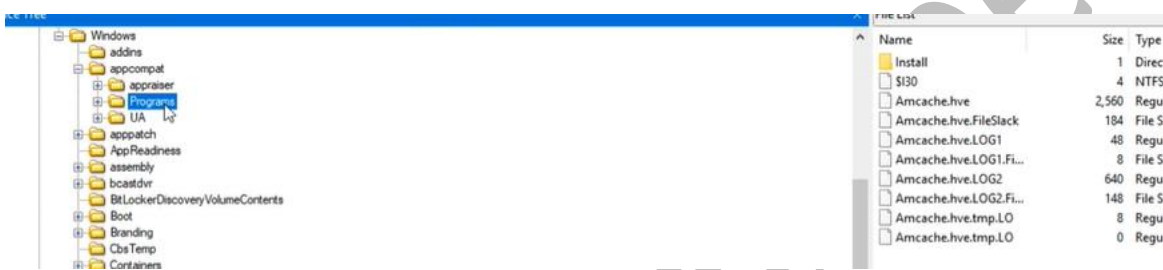
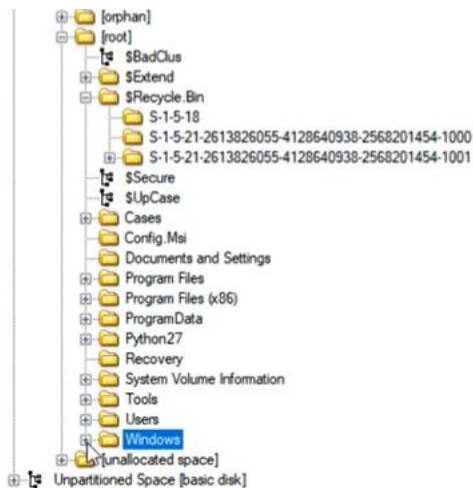
data→Microsoft→search→data→applications→windows→File: -
windows.edb



File Name	Size	Type	Modified
cubrtmp.jta	1,004	Regular File	7/24/2018 1:21:...
Windows.edb	32,768	Regular File	8/2/2018 10:14:...

Which is esc data extensible storage engine data base than pertains to windows search(any window related search history can be parsed by looking at this database)

Next thing. **Windows**→ programs →appcompat



Which contains **amcache.hive** it shows program of execution

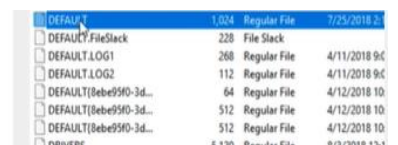
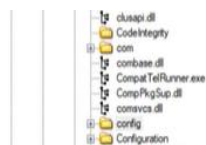
Next thing. **Windows**→**INF**→**File: -setupapi.dev.log**



Contains log file which record any kind of peripheral installation things like example we inserted USB this file not only contain evidence of that in registry but also within the setup API devlog

Next thing. **Windows**→**system32**→**config**→ **5 Five registry and 1 Folder**

1. Default



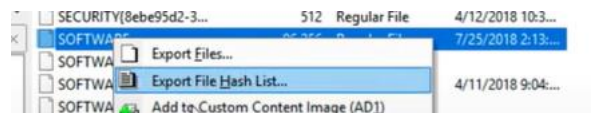
2. SAM



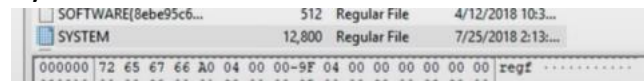
3. Security



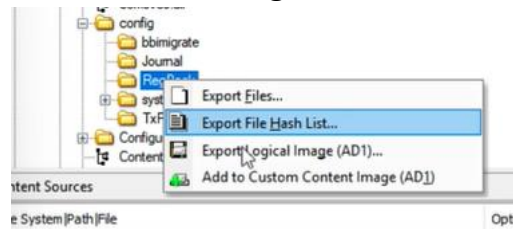
4. Software



5. System



6. Folder named Regback



RegBack every 10 days will actually create backup of registry hives so it important in case registry hives have been deleted or modified or changed

Next thing. **Windows**→**system32**→**Logfile**



Next thing. **Windows**→**sru** (Called shrum) **system 32/sru**



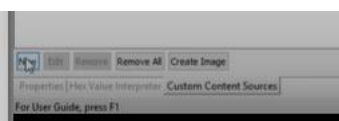
Contains things like number of bytes transferred SSIDs connected to even energy related settings all important about system

Next thing. **User.dat, usrclass.dat**

Which is every user personal registry hive. Every user contains his own registry in that.

For collecting that.

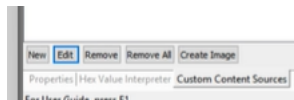
Click new.



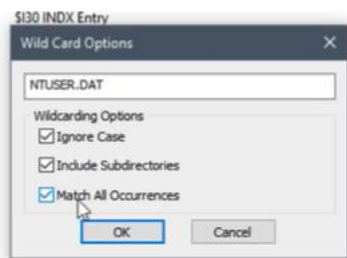
After that you will notice (*)

\\.\PHYSICALDRIVE0:Partition 2 [20429846]NONAME [NTFS][root]\Windows\System32\ruj*

Then click on edit

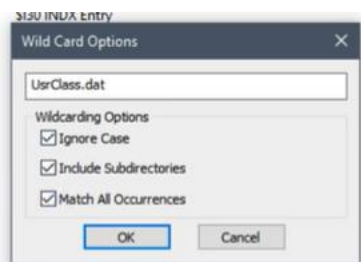


Enter NTUSER.DAT and all tick.



Another registry hive you want to collect. (USR.class.dat)

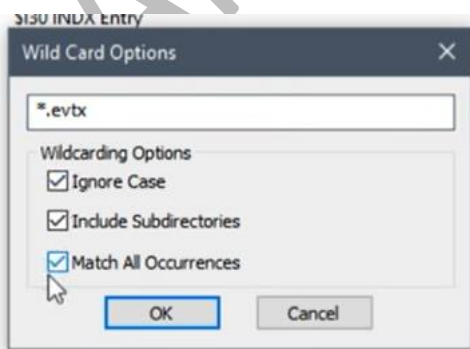
New→(*)→edit.



This will contain shell bag. This will put there to facilitate user account control in windows.

Next Thing. **Event log**

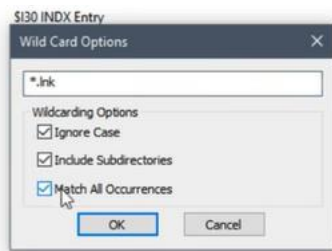
New→(*)→edit.



*.evtx

Next thing. **Lnk files**

New→(*)→edit.

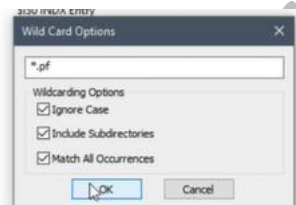


*.lnk

Next thing. **PF Files**

Prefetch file that can show us evidence of program execution like amcache

New→(*)→edit.

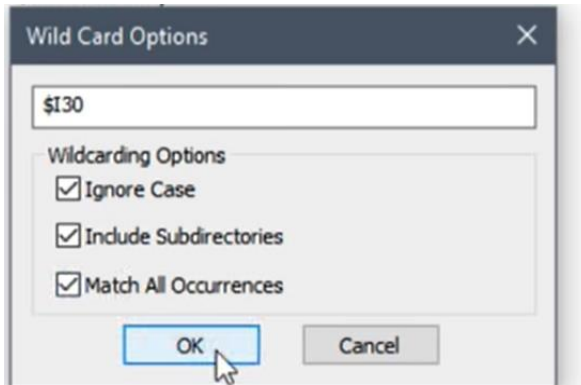


*.pf

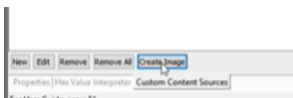
Next Thing. **\$130 file**

every directory on file system will have this file and this is basically a directory index. So this file maintain list of all files and directories that belong within given directory (We can use this to identify file that were previously deleted or overwritten)

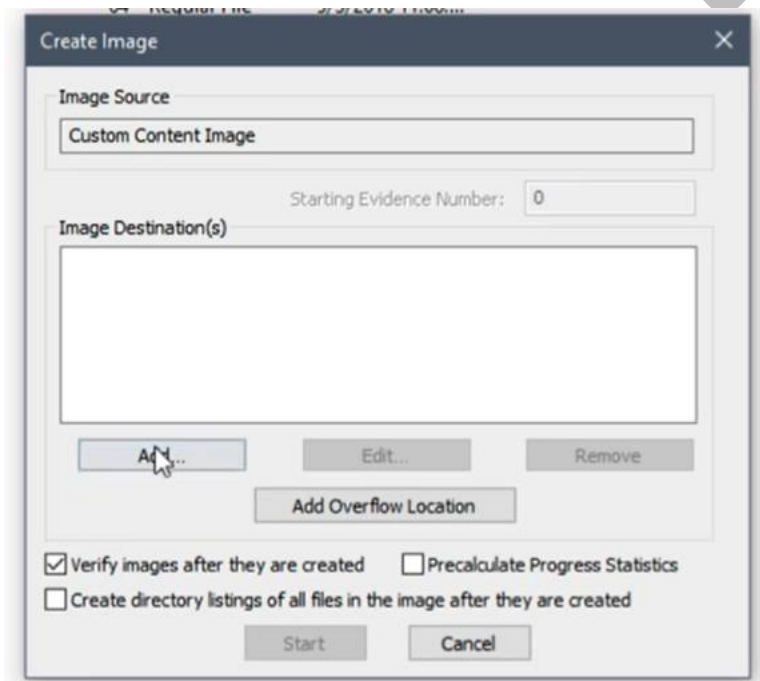
New→(*)→edit.



create image



Add destination.



Create Image

Evidence Item Information

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

< Back Next > Cancel Help

64 Regular File 5/3/2018 11:08:...

Create Image

Select Image Destination

Image Destination Folder
 Browse

Image Filename (Excluding Extension)

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

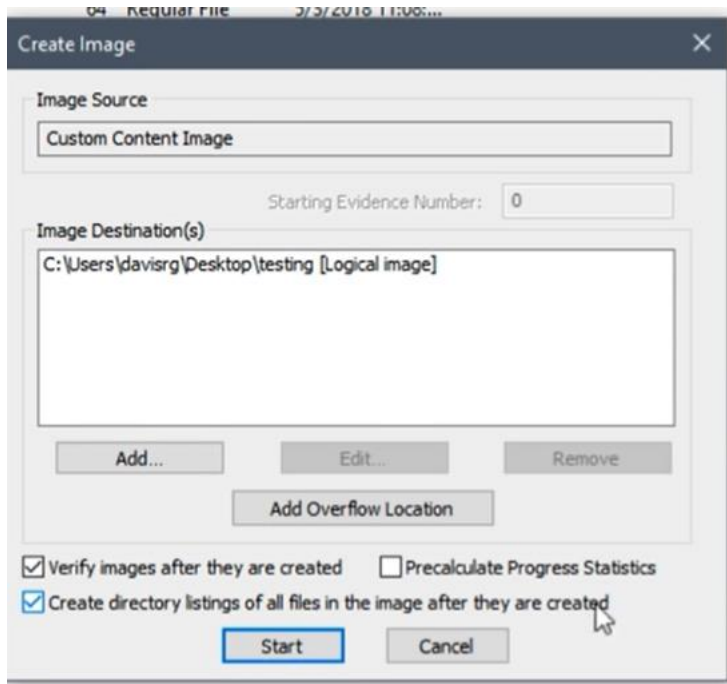
Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption

Filter by File Owner

< Back Finish Cancel Help

Check last two



Akash Cheatsheet