Digital Forensics Using Autopsy to Analyse the Contents of a Laptop

Contents

Introduction

After downloading the latest version of Autopsy and completing the previous lab proceed with this lab.

This is an extensive lab in using Autopsy and will be a work in progress as the semester progresses.

The lab instructions serve as general guidelines as there can and should be difference in each investigation, version of Autopsy, laptop, version of windows, it is up to you to troubleshoot as you advance through the document.

Autopsy proves to be a robust, open-source tool that is ideal for beginners looking to delve into digital forensic investigations. Its user-friendly interface simplifies the complexities of forensic analysis, making it an excellent starting point for anyone interested in the field. Using this tool, users will discover how Autopsy's straightforward design helps alleviate the initial overwhelm often associated with digital investigations.

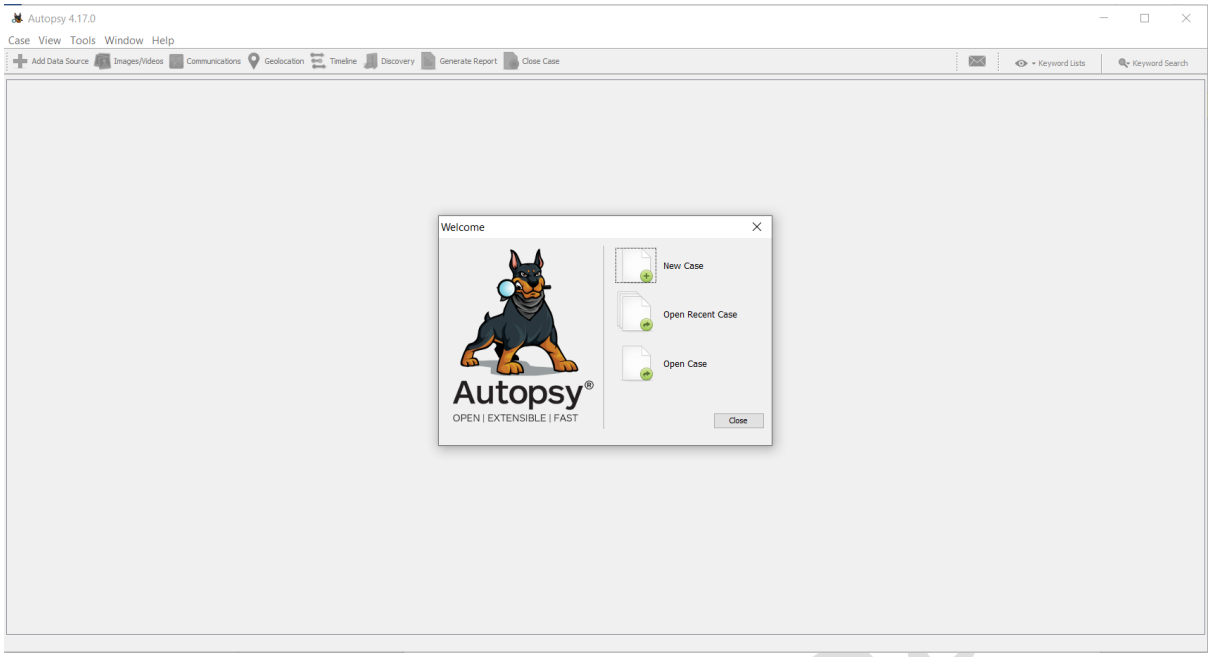
This lab provides a comprehensive overview of how to use Autopsy for forensically examining a device. By completing this lab, the user gains not only practical experience but also a deeper understanding of the tool's full potential. While the primary goal of the lab is to teach users how to create a logical image of a laptop's contents, it also emphasizes broader forensic investigation techniques. The ***skills developed in this lab with Autopsy can easily be transferred to other forensic tools***, as many of the underlying principles—such as file and directory structure—are consistent across platforms.

Autopsy serves as an excellent gateway into the world of digital forensics, offering users a versatile and adaptive learning experience. The completion of this lab allows participants to gain hands-on experience with the tool, learning how to identify and extract important files, directories, and information that could be crucial in a real-world investigation. In addition, the lab encourages self-guided exploration, giving users the freedom to experiment and explore various files and features within Autopsy, enhancing their learning experience.

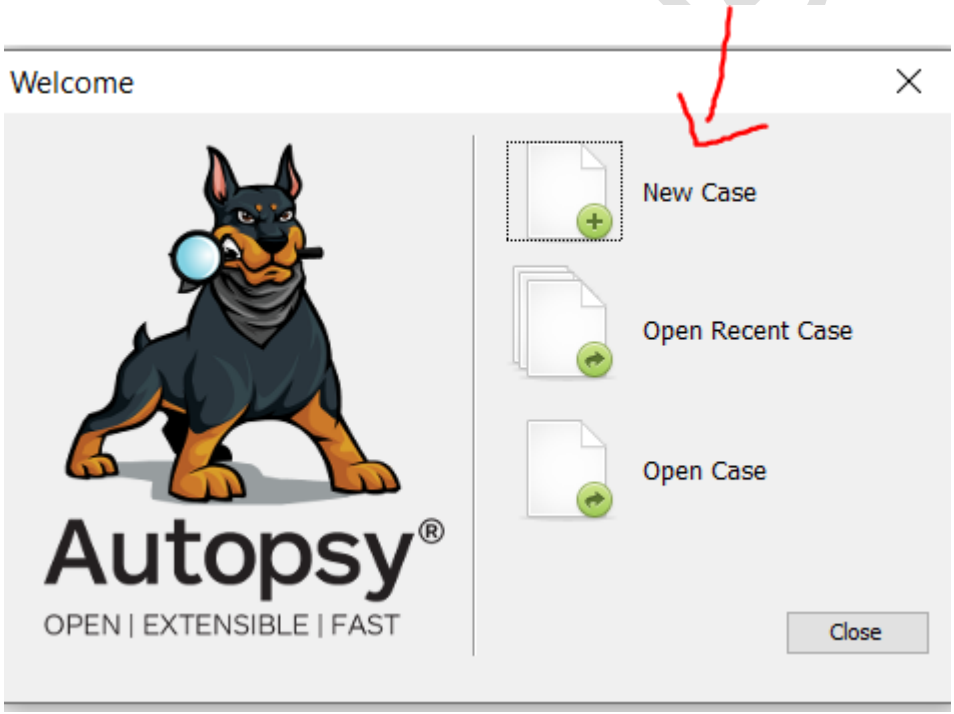
Overall, this lab tries to strike a balance between being informative and user-friendly. Its structured approach makes it accessible to readers of all levels, ensuring that even if mistakes occur, the process remains forgiving and easy to follow. The lab not only introduces users to Autopsy but also fosters a mindset of self-learning and problem-solving—skills that are invaluable in the field of digital forensics.

Imaging your own Laptop

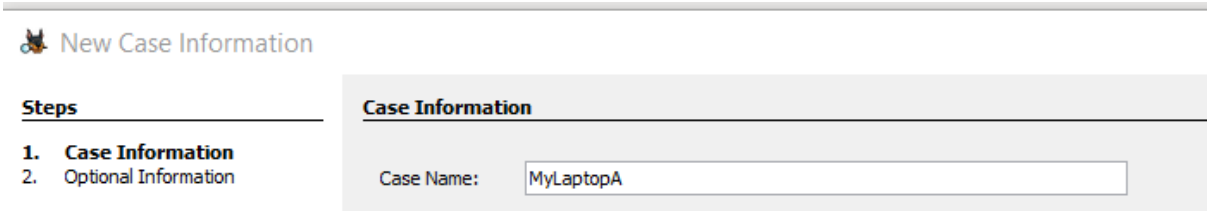
Step 1. As this is a lab, we want a tool that can quickly image the contents of the laptops local disk. As this is the case, we want to re-use autopsy in admin mode.



Step 2. Once open, as mentioned in the previous lab, select new case

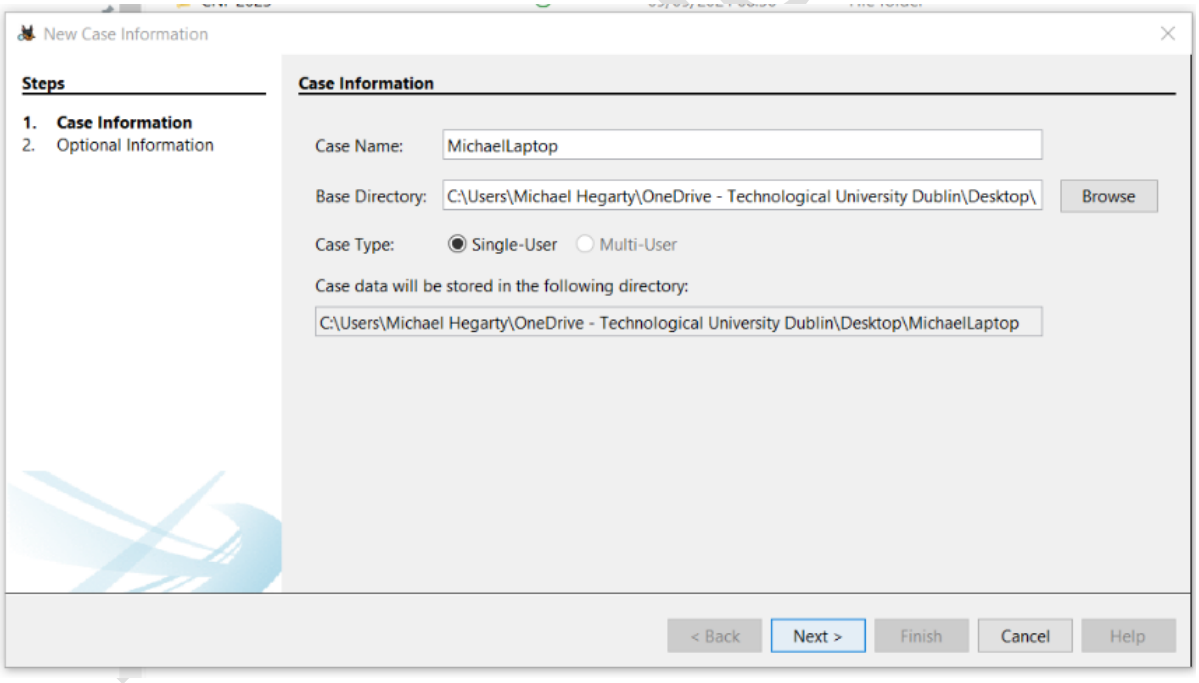


Step 3. Give the case some basic information such as a case name, in this case the name “MyLaptopA” but name it as you please.



Step 4. Assign the case a base directory to save the folder containing the case, this lab uses desktop, but feel free to place it in the most convenient spot.

Step 5. Now assign the case a type, this is quite important as later you will be asked to give user information to retain integrity. This lab is to be done by one person, so select single user (same as previous lab).



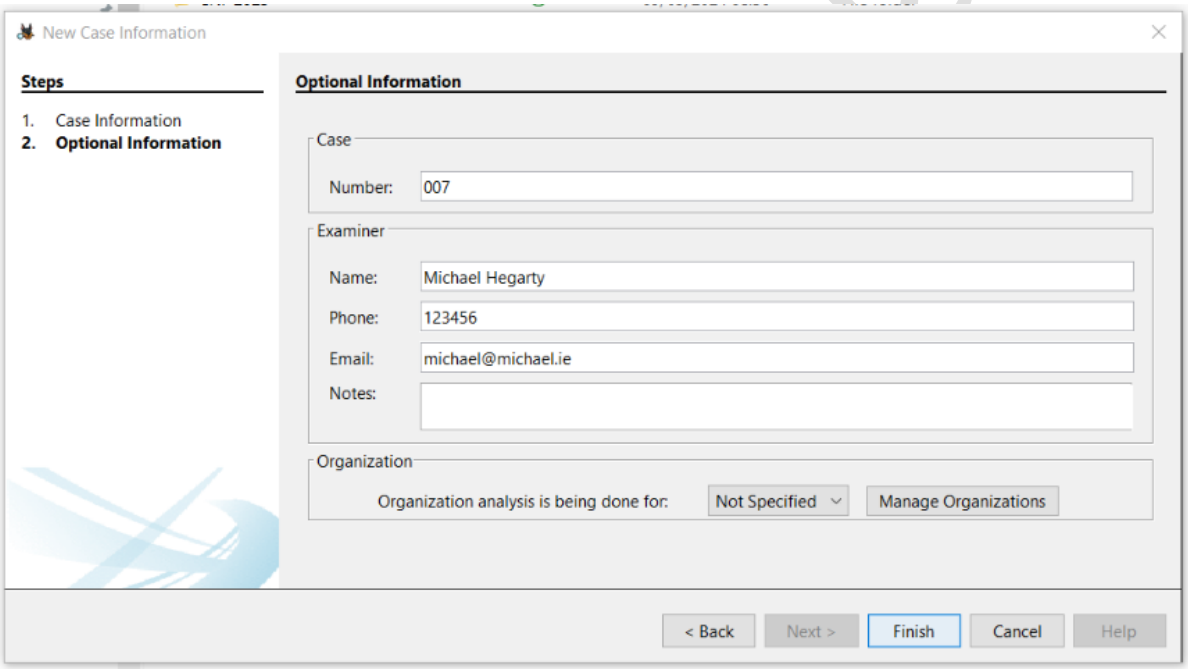
Step 6. Next the case number needs to be assigned, this is more important when a bunch of investigations are being done. I have assigned the case the number 007, but feel free to assign the case number any unassigned number.

Step 7. Assign the case some examiner information, as this is a learning lab your initials will do.

Note: *In a professional manner always give your full name.*

Step 8. Assign a Phone number, for the lab feel free to use a fake number just to make it look more professional.

Note: *During a professional investigation, always give your up-to-date phone number.*

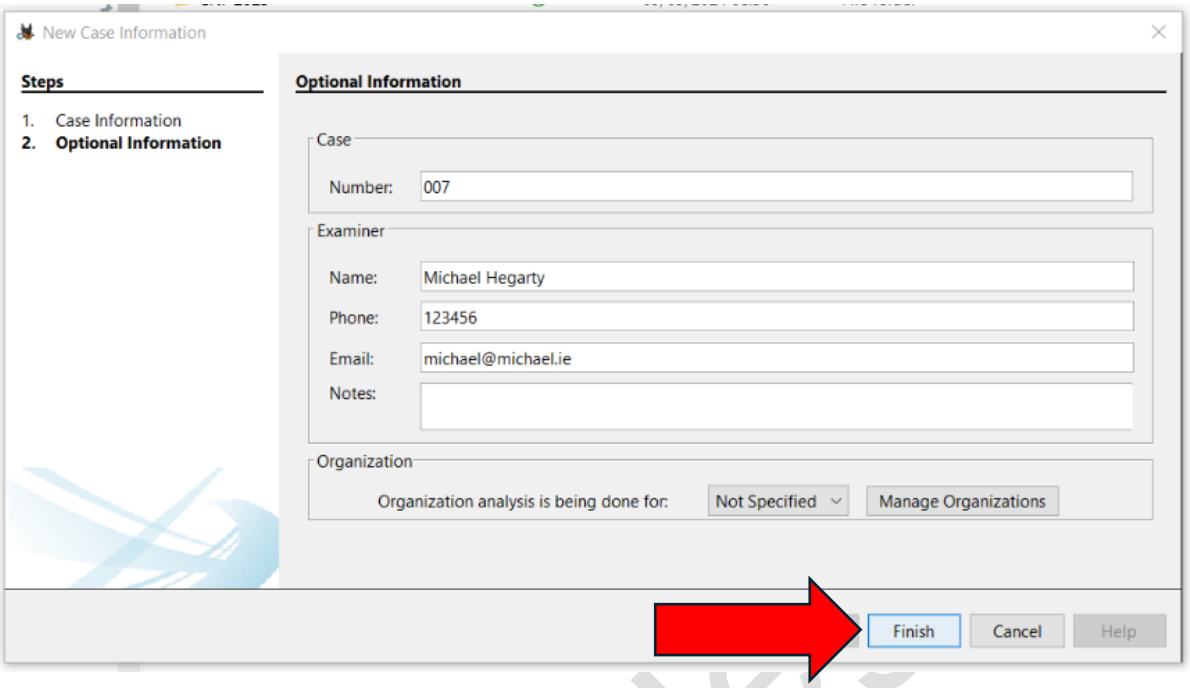


Step 9. Give the case an email address, once again for the sake of this lab, this can be a fake email to make the case more professional.

Note: *During a professional investigation, use your current up to date email, or organization assigned email.*

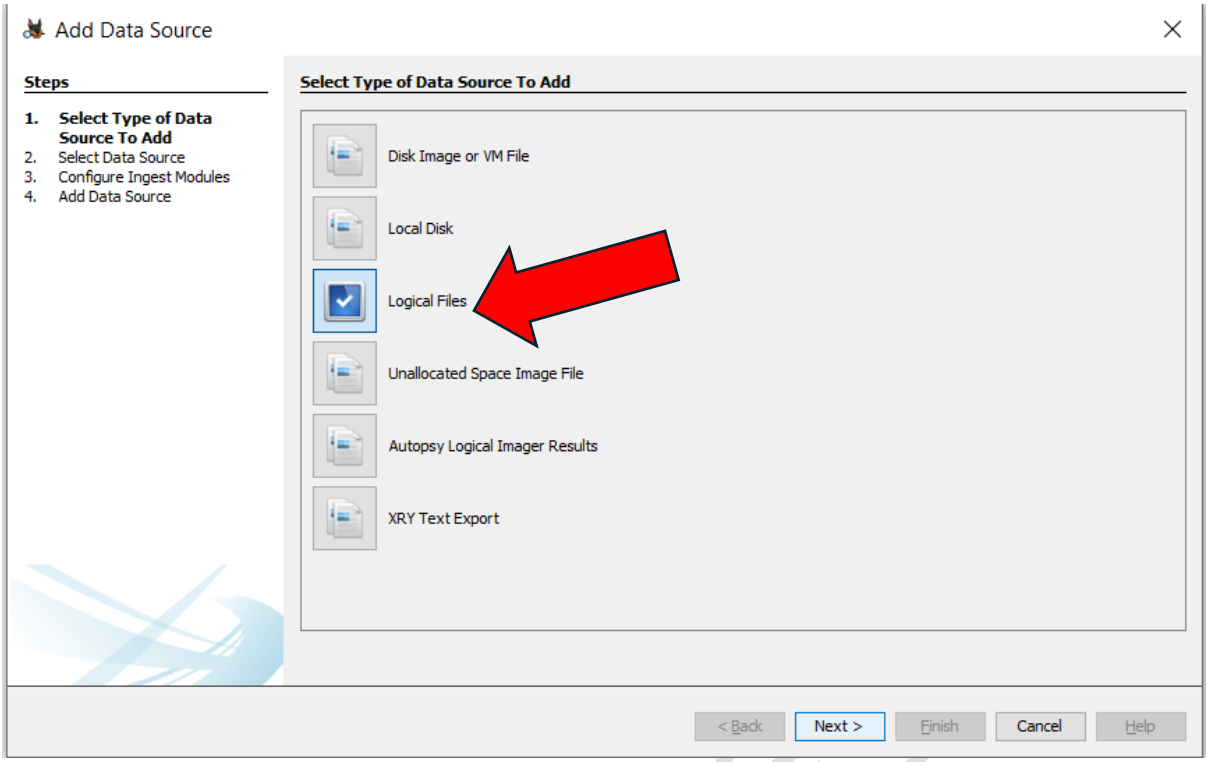
Step 9. Assign the case some important notes such as the purpose, for the sake of this lab assign the notes section the following “Lab Work”.

Step 10. Now click the finish button.

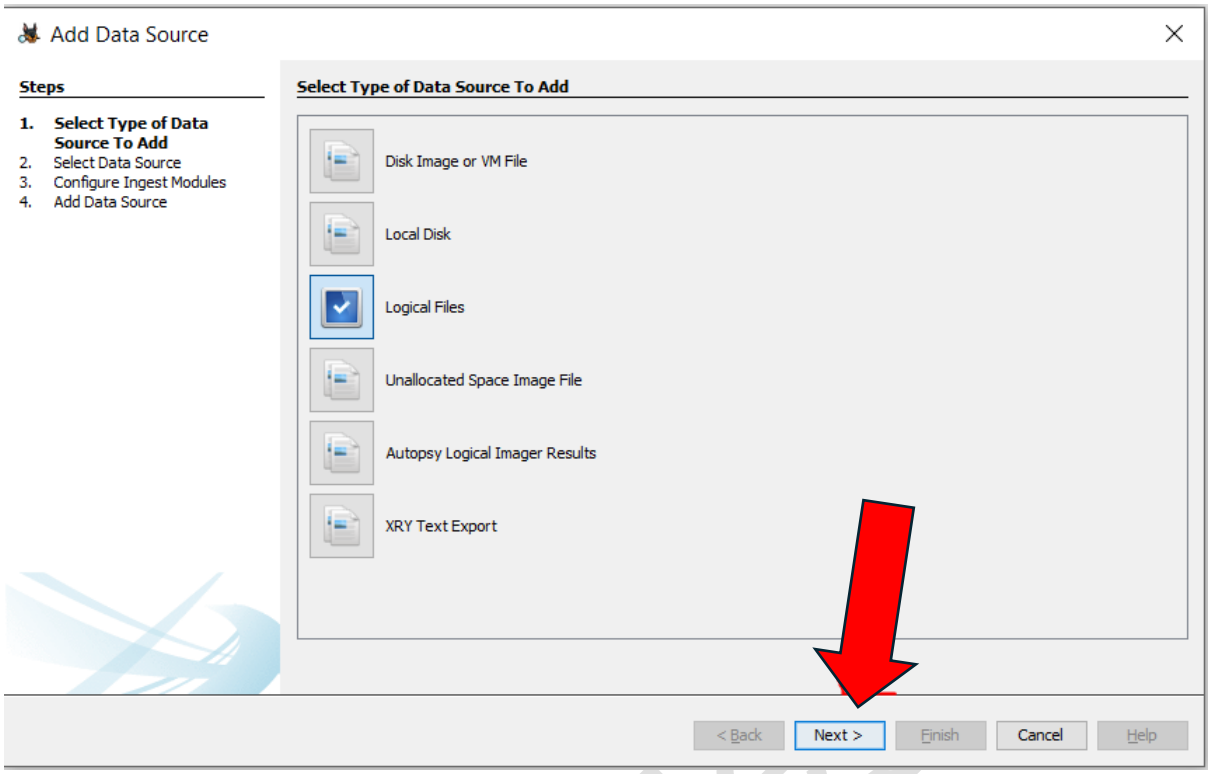


Step 11. Next, you will see options, these options allow for a data source to be added, for today we will be using logical files.

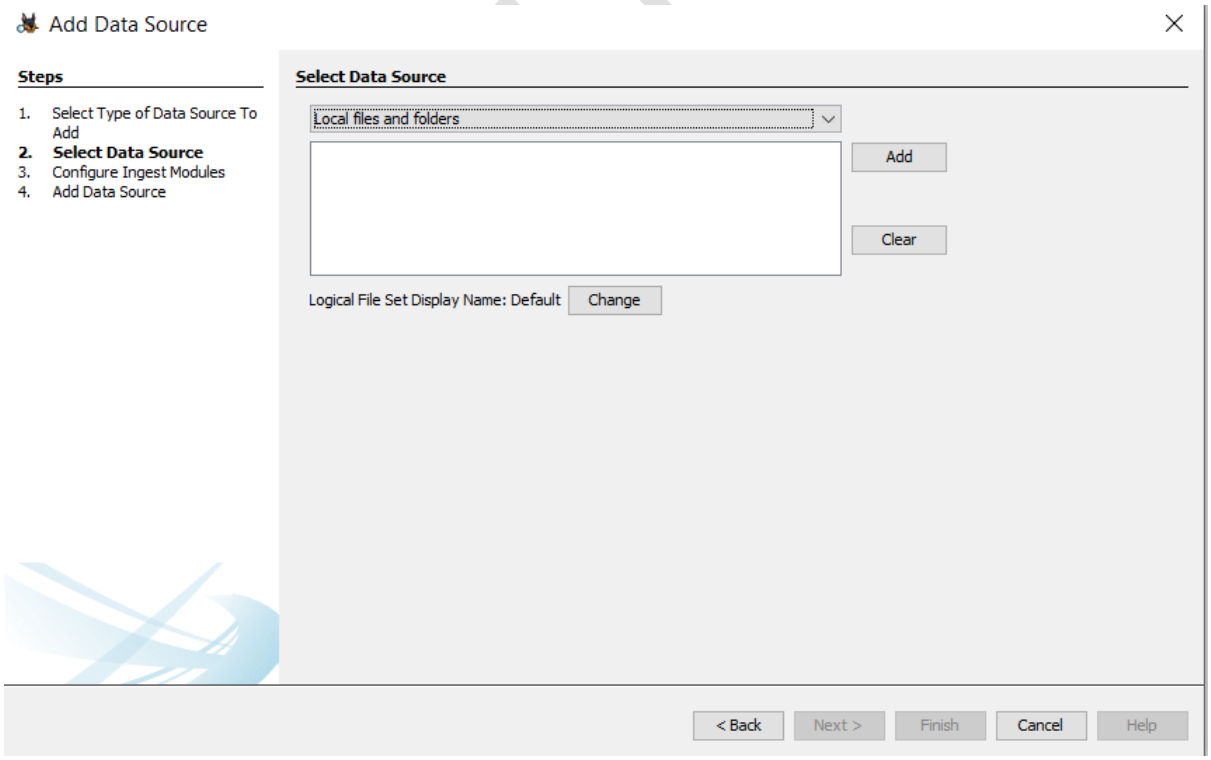
Note*: Although autopsy allows for a wide range of different data sources to be added*



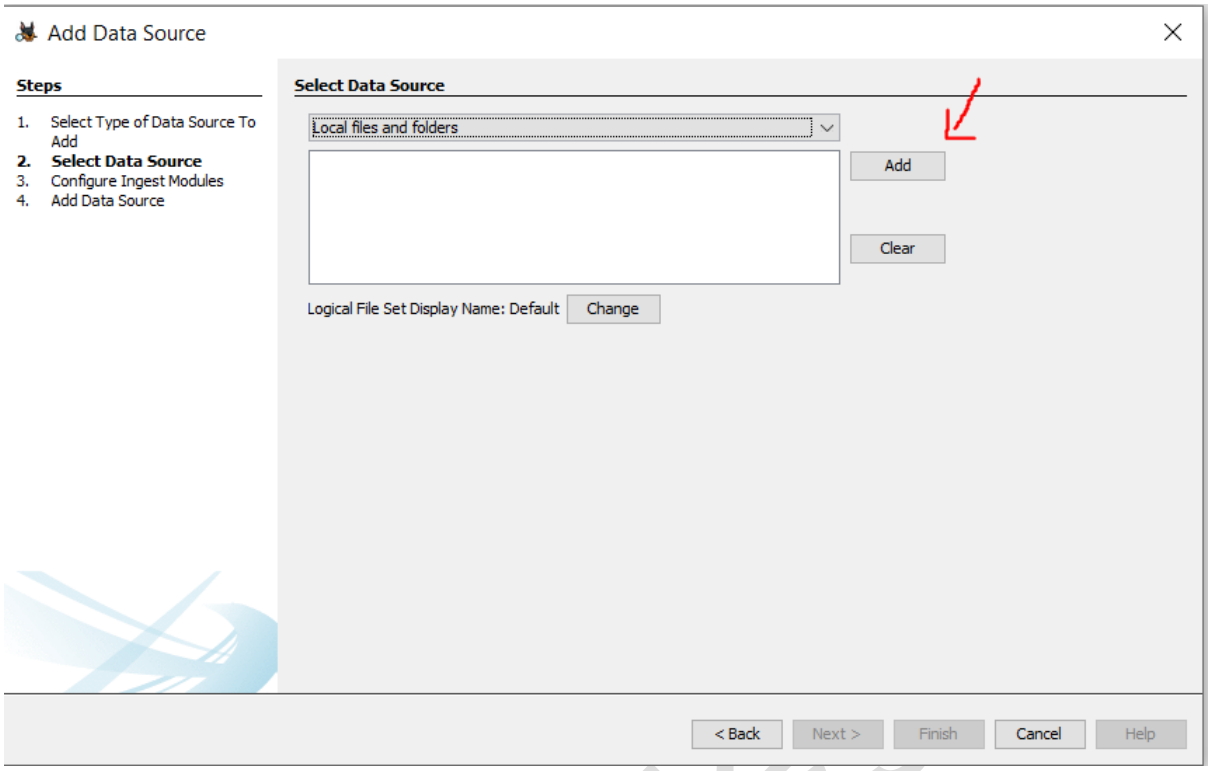
Step 12. Once selected, press the next button.



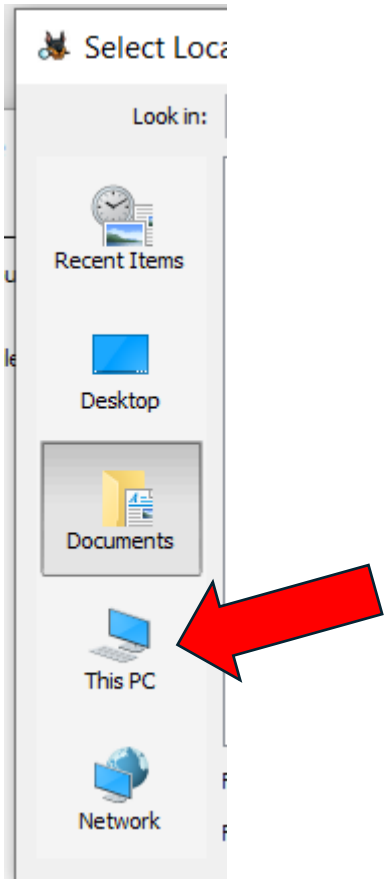
Step 13. Now you will see the following:



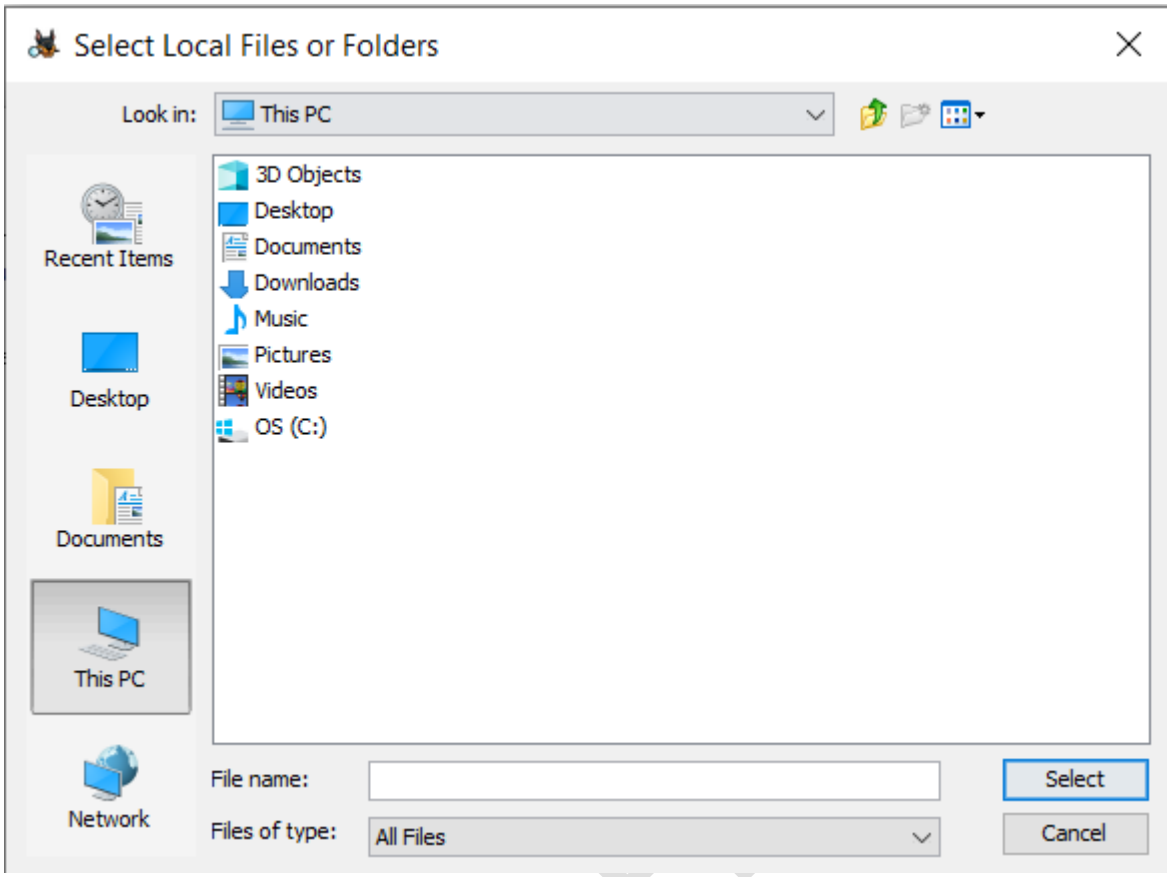
Step 14. Now that you see the select data sources section, please press on the add button to add a specific file or folder.



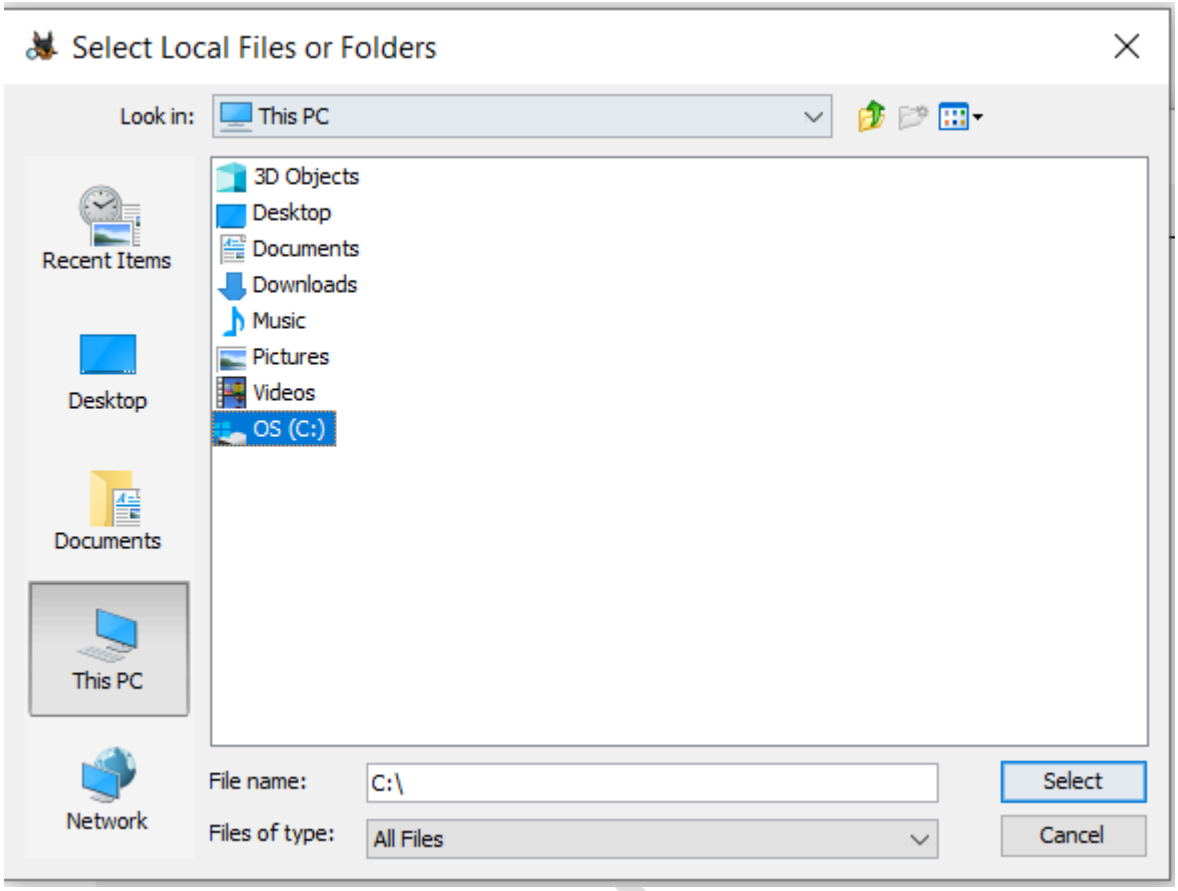
Step 15. Once selected, you will see a range of options



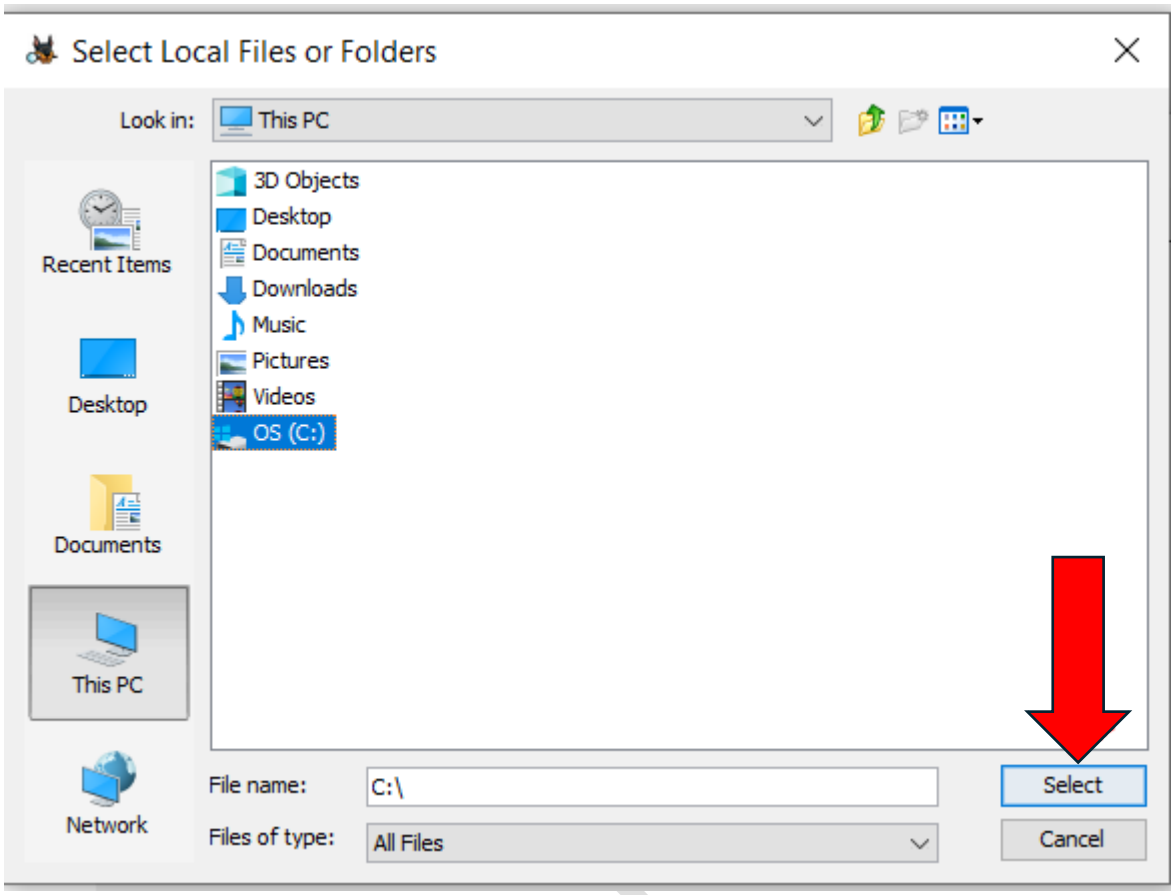
Step 16. I suggest you select “this pc”



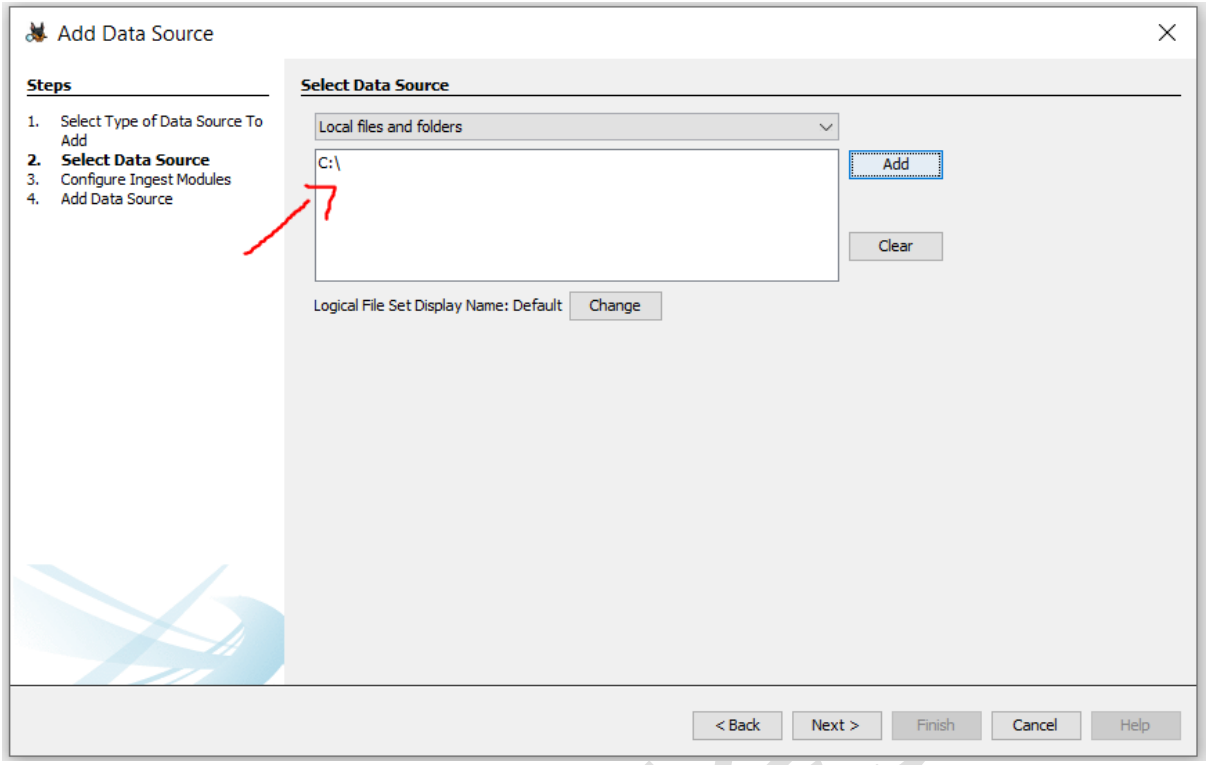
Step 17. Once inside the “this pc” option, you will see some basic directories, for this lab we will be using the OS (C:)



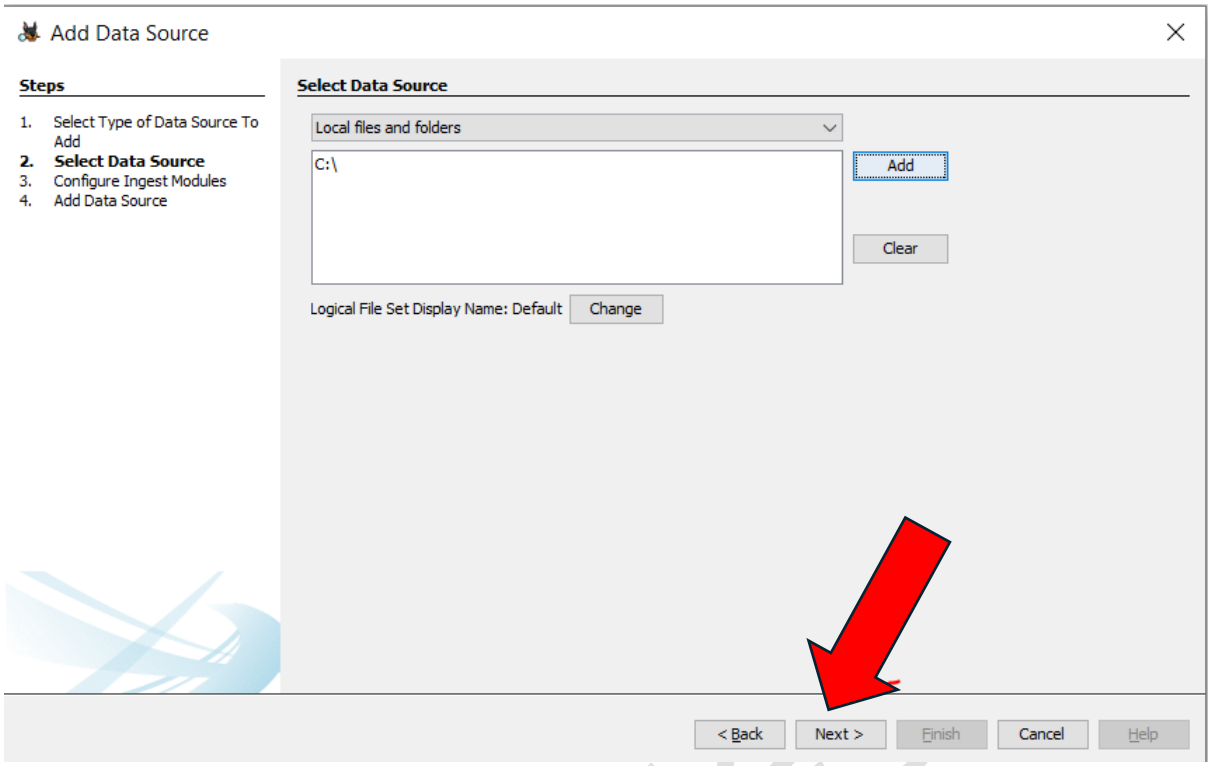
Step 18. Click select



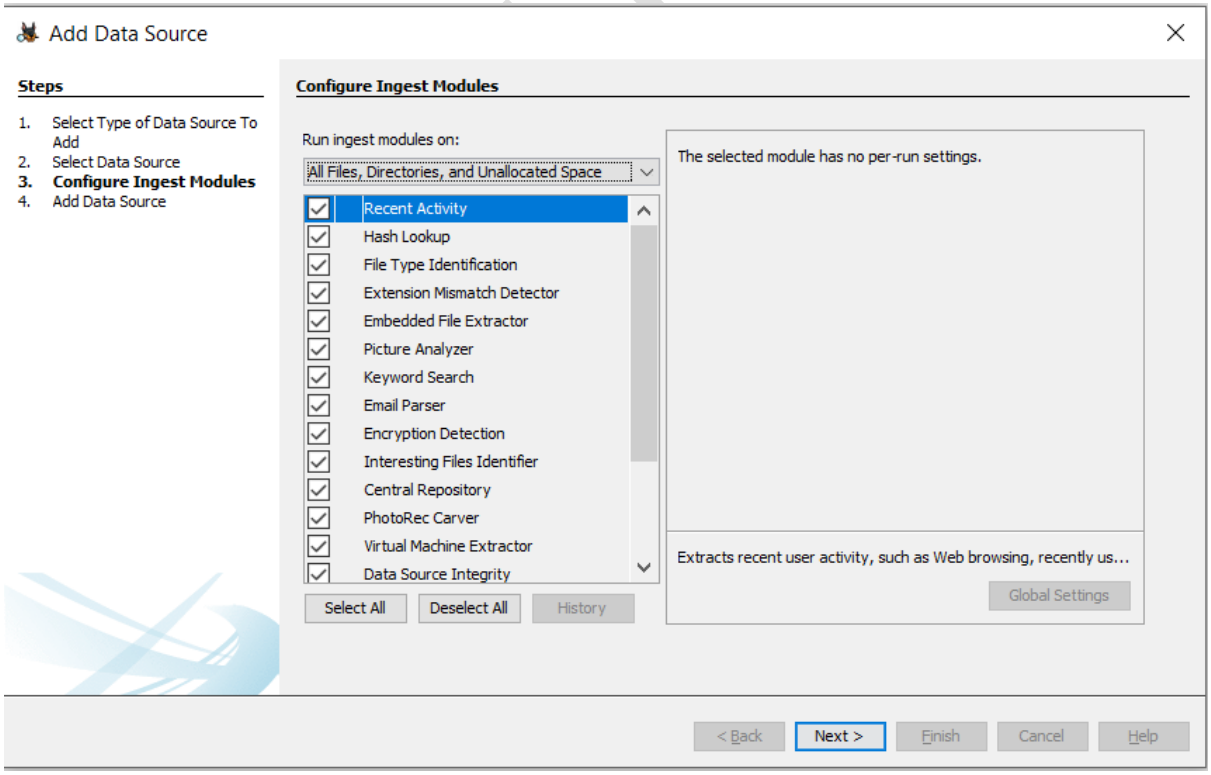
Step 19. You should now see the C:\ added to the chosen files and folders.



Step 20. If you want to you can add more files and folders to find more information, but for this lab the C:\ will provide more than enough data. Click the next button.



Step 21. Now you will see a selection of places to ingest data from.

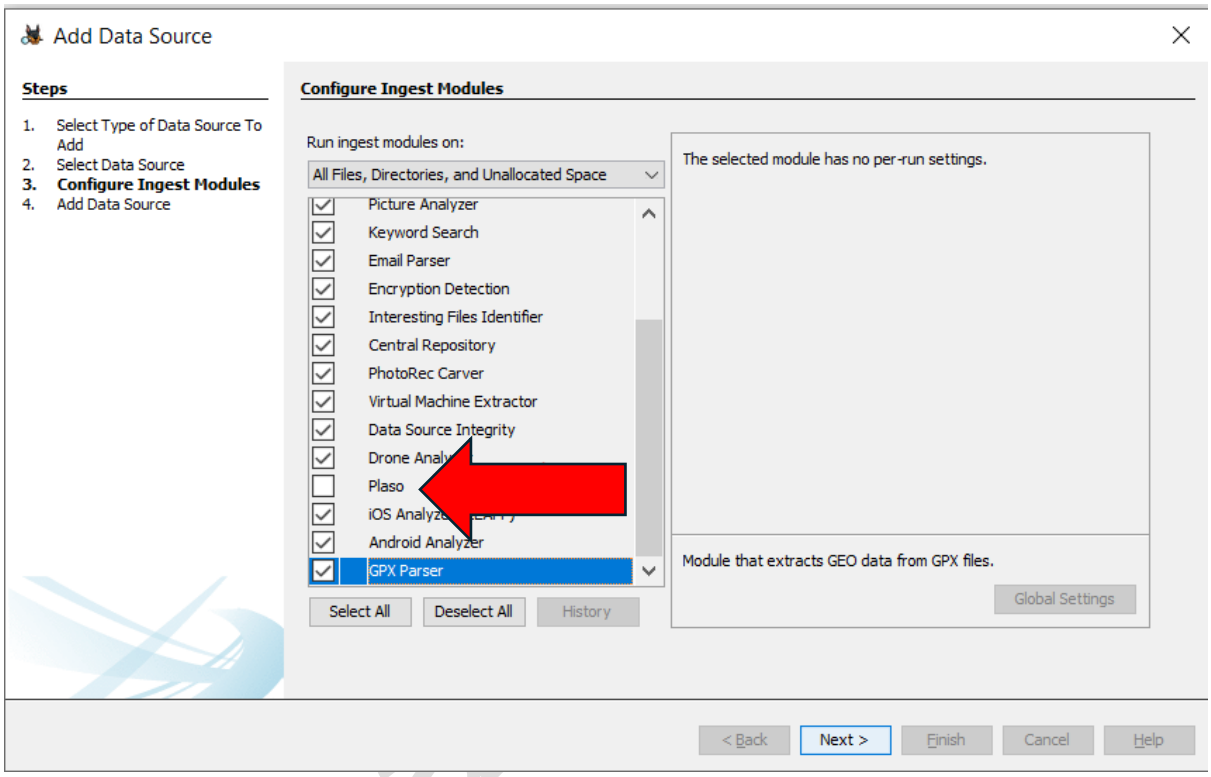


1. Recent Activity – Will view your recent activity, such as viewing a website

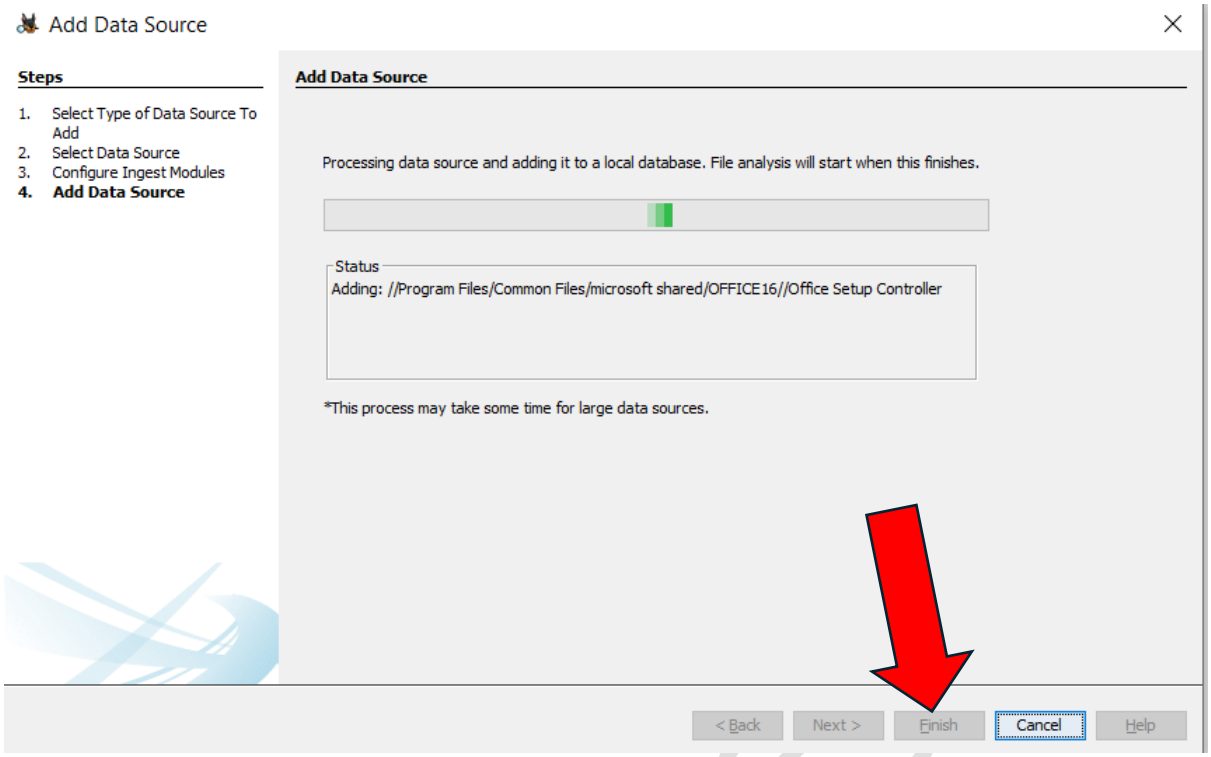
2. Hash Lookup – Will identify known hashes that are being used
3. File type Identification – Will match files on your laptop based on signatures
4. Extension Mismatch Detector – Flags files that have a bad extension due to the file type
5. Embedded file Extractor – Embedded files such as .docs will be extracted
6. Picture Analyzer – Will analyse pictures and retrieve information such as metadata
7. Keyword Search – Allows users to index files through the use of keywords
8. Email Parser – Populates a dashboard through parsing mbox and pst files
9. Encryption Detection – Looks for files based on the entropy used
10. Interesting Files Identifier -Any file with an interesting rule set will be identified
11. Central Repository – Allows for the repository to be saved so it can be examined at a later time
12. PhotoRec Carver -Unallocated space will be subject to examination by PhotoRec
13. Virtual Machine Extractor – Virtual machine files will be extracted and added
14. Data Source Integrity – Can be used to calculate and validate hashes files
15. Drone Analyzer – Any files generated by the use of drones will be examined
16. Plaso – Plaso will be ran against data sources
17. iOS Analyzer – LEAPP is used to analyse logical acquisitions
18. Android Analyzer - Android data will be extracted

19. GPX Parser – Finds GEO data in GPX files and extracts it

Step 22. We want every option ticked **except for plaso, scroll down until you see Plaso and deselect it.**



Step 23. Wait **patiently** for the data source to be added and hit “finish” once highlighted.

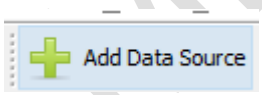


Understanding the tools

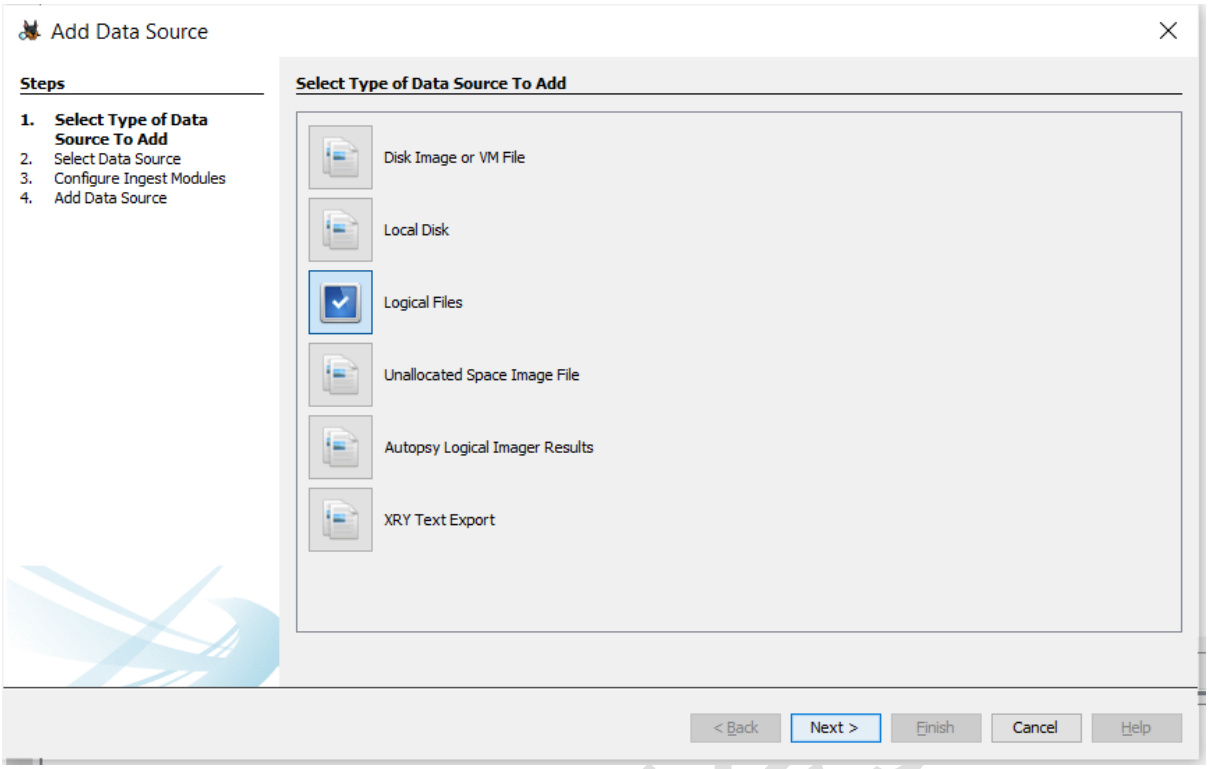
Step 1. Locate the tools at the top of Gui

Add data source

Step 1. Navigate to the add data source



Step 2. Notice the same section as used at the start

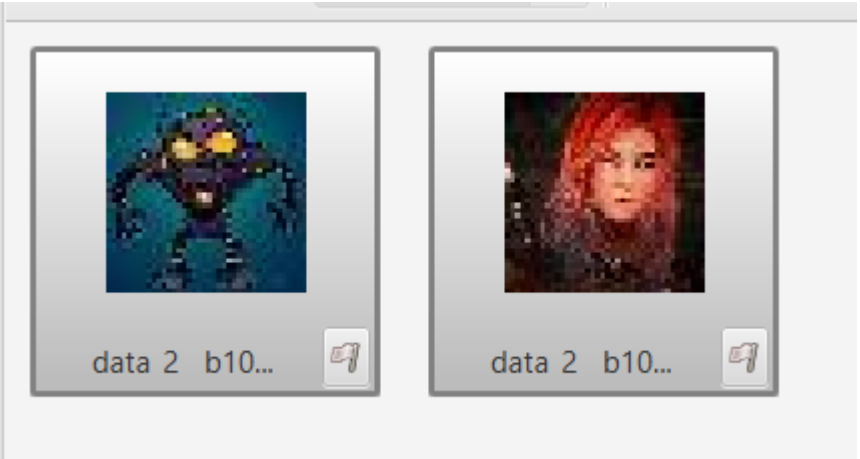


Note: This will allow an investigator to add any more data sources should they appear over the course of the investigation.

Images/videos

Step 1. Navigate to the images and videos tools

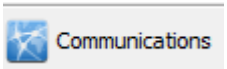
Step 2. Look at the GUI displaying the images in one convenient space



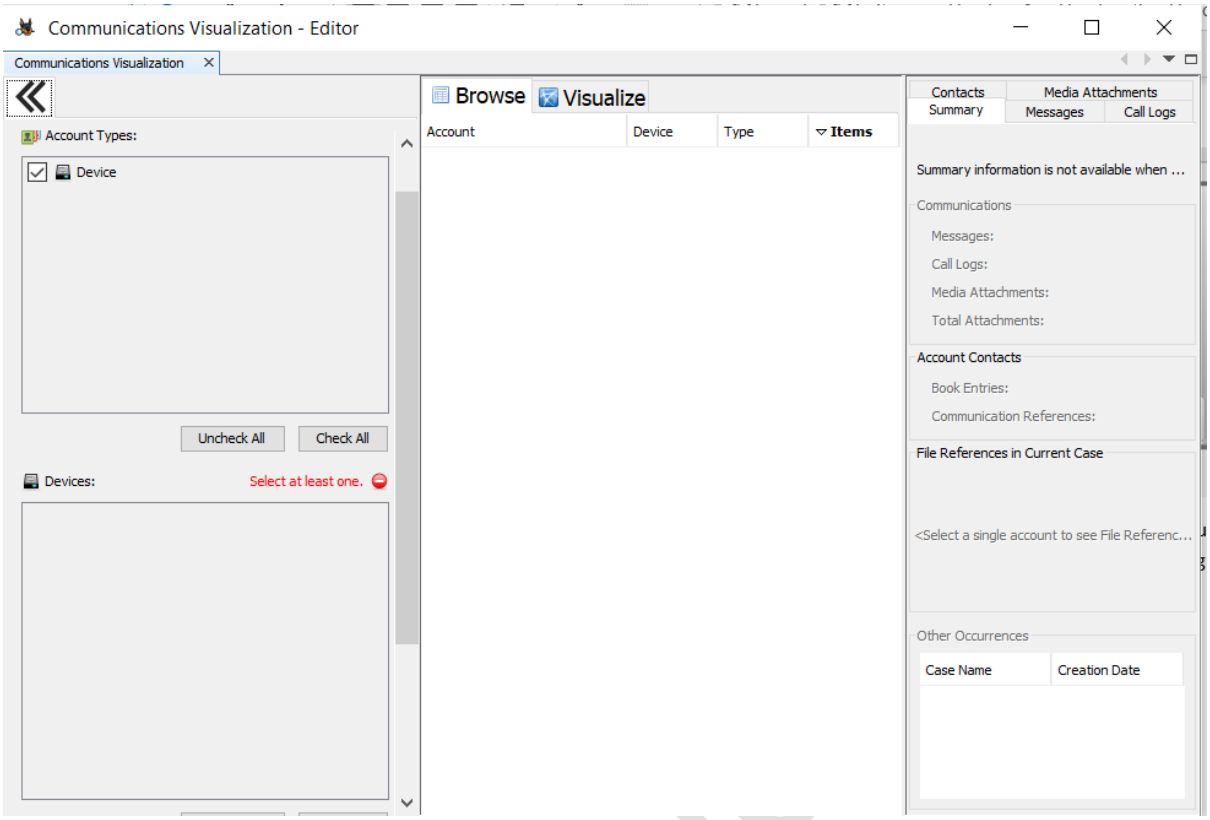
Note: *This can help an investigator use visual skills to find a picture of interest and identify any distortions to the image that may suggest steganography among other things.*

Communications

Step 1. Navigate to the communications tool



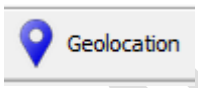
Step 2. Notice the GUI for the communications tool



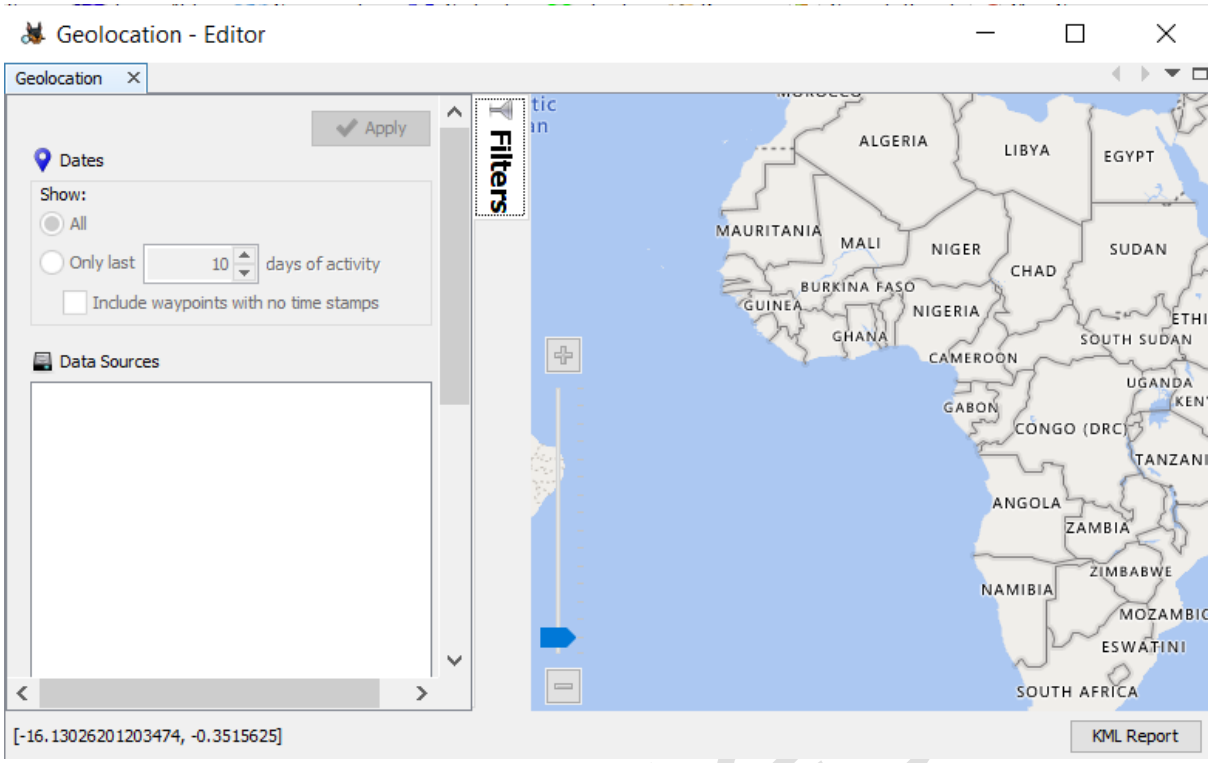
Note: *This can help an investigator visually see communications between two parties, this allows an investigator to build a picture.*

Geolocation

Step 1. Navigate to the geolocation tool



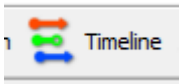
Step 2. Notice the Geolocations GUI.



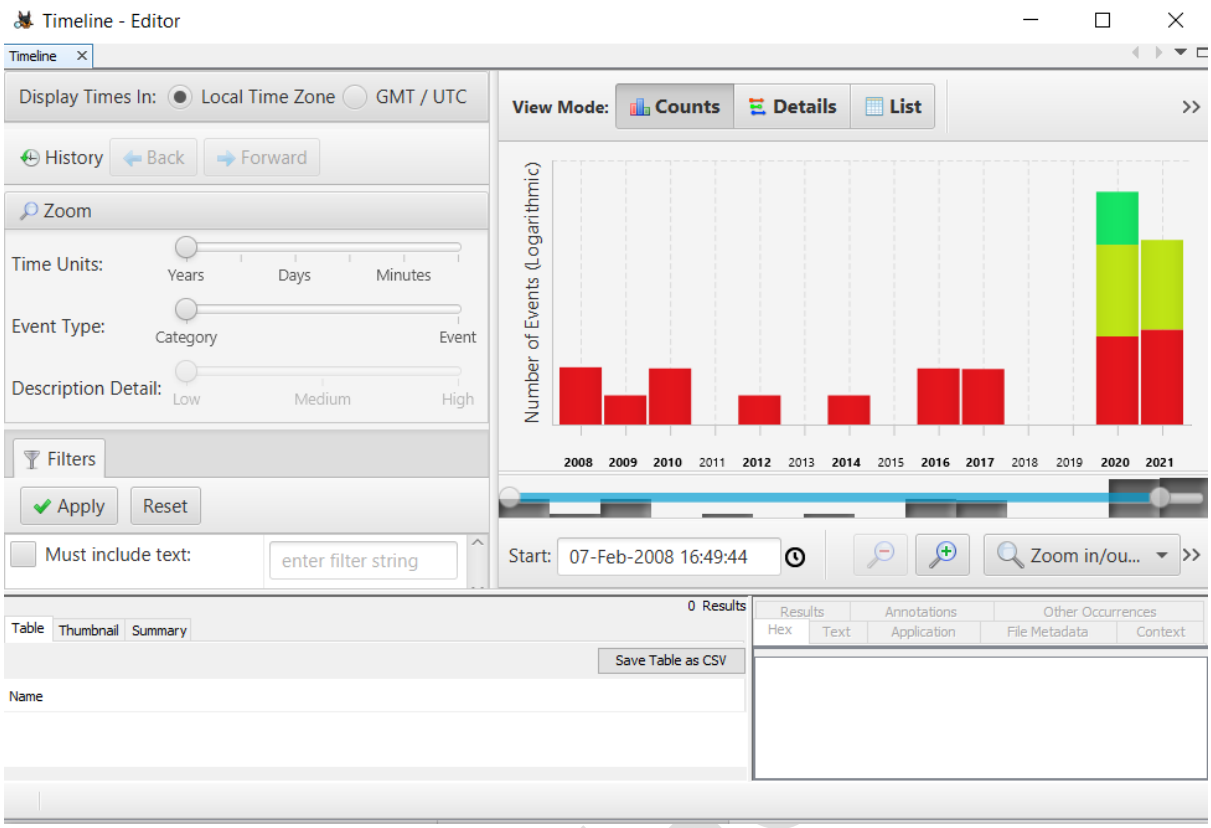
Note: *This will generate geolocations should any artifact have it on. This can help an investigator clear or incriminate a defendant.*

Timeline

Step 1. Navigate to the timeline tool



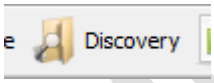
Step 2. Notice the timeline GUI generating a timeline of events



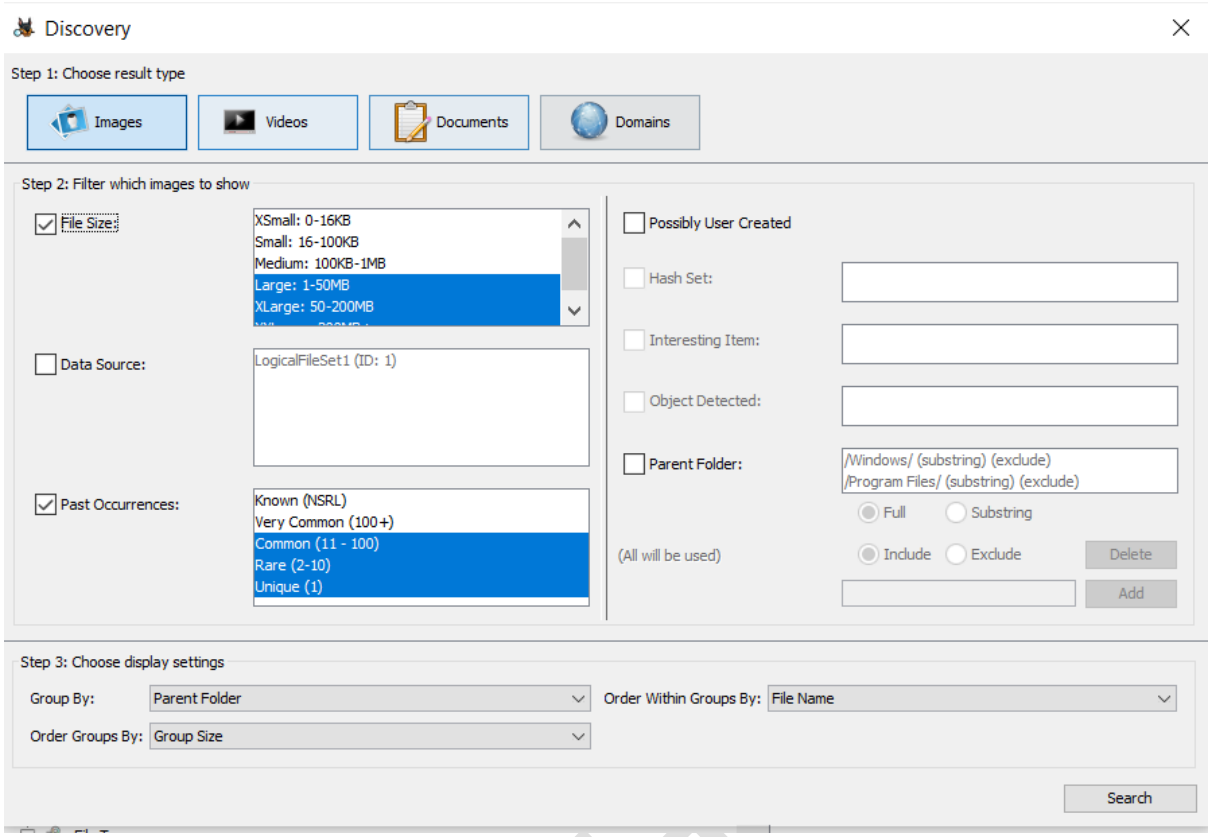
Note: *This allows an investigator to have visual representation of a timeline of events that occurred on the system.*

Discovery

Step 1. Navigate to the discovery tool



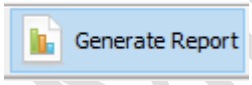
Step 2. Notice the Discovery GUI tool



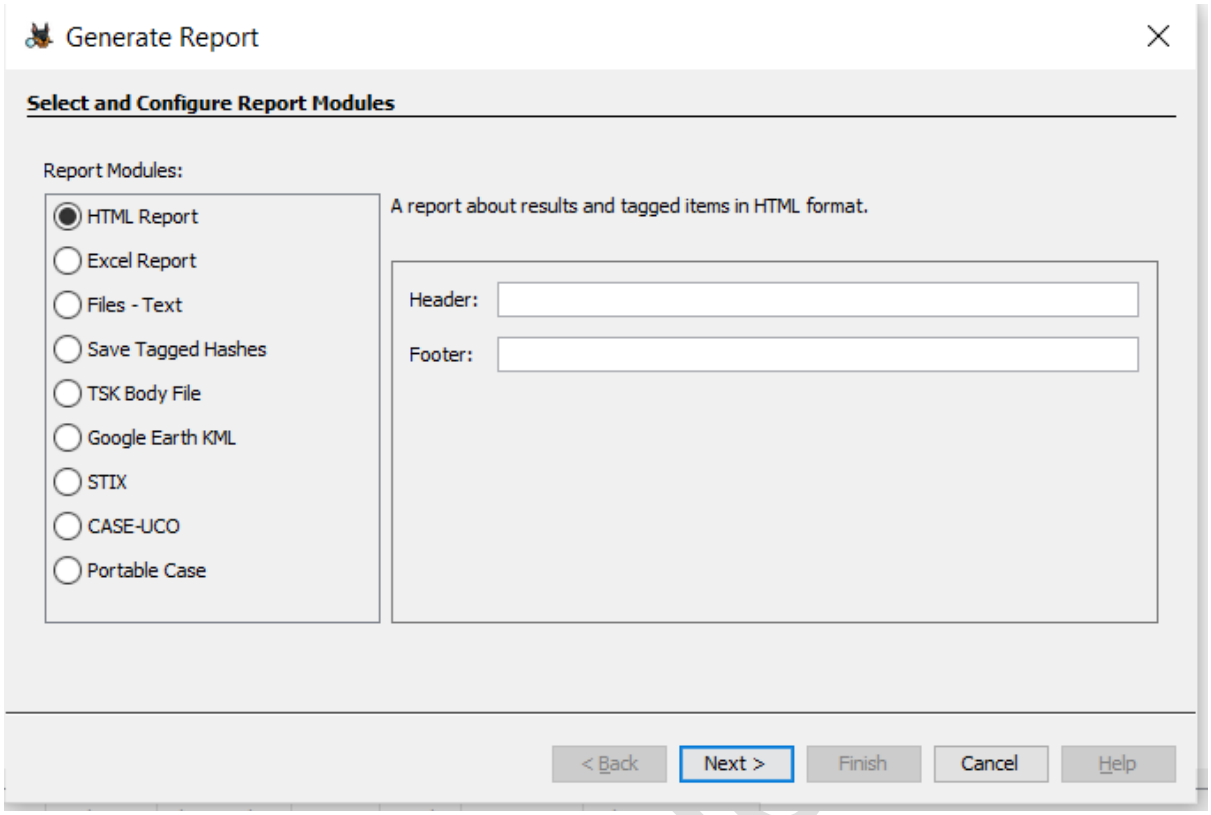
Note: *This allows an investigator to discover potentially missed images, videos, documents and domains. Which can help with performing a thorough investigation*

Generate Report

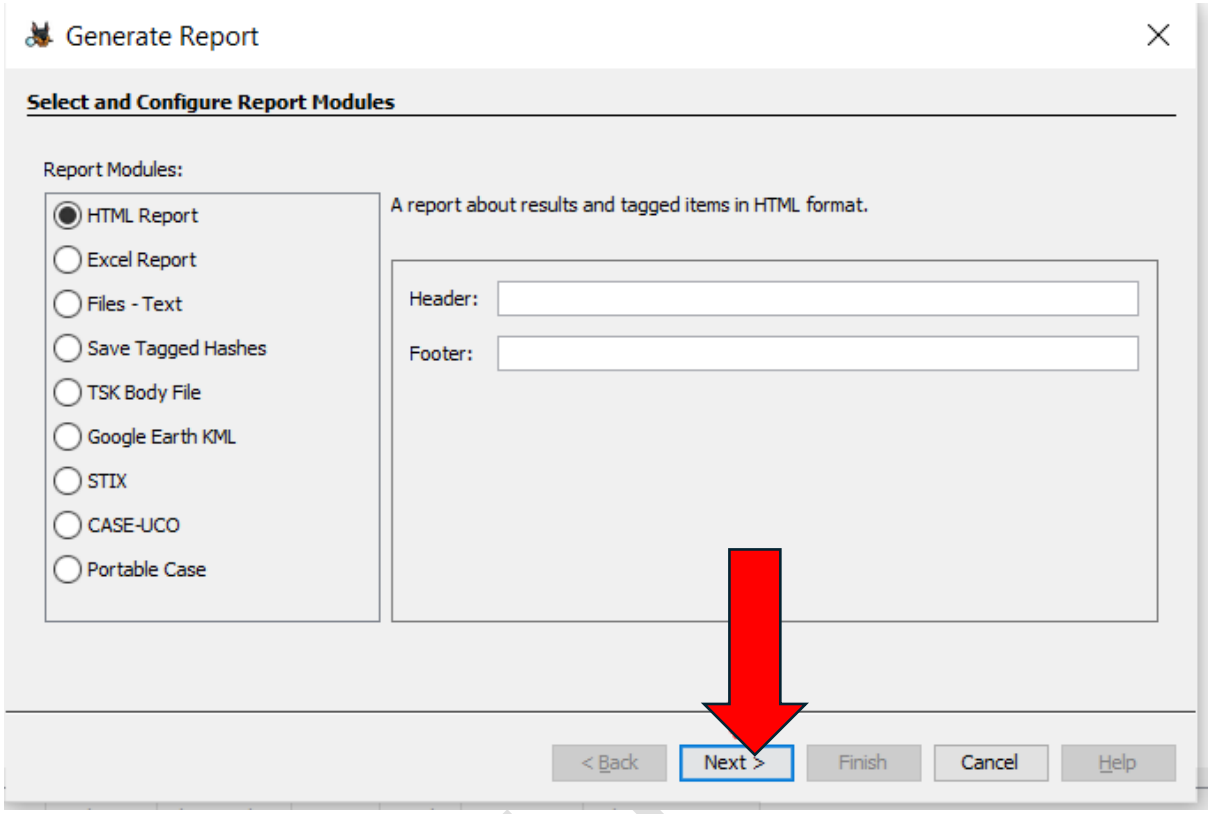
Step 1. Navigate to the generate report tool



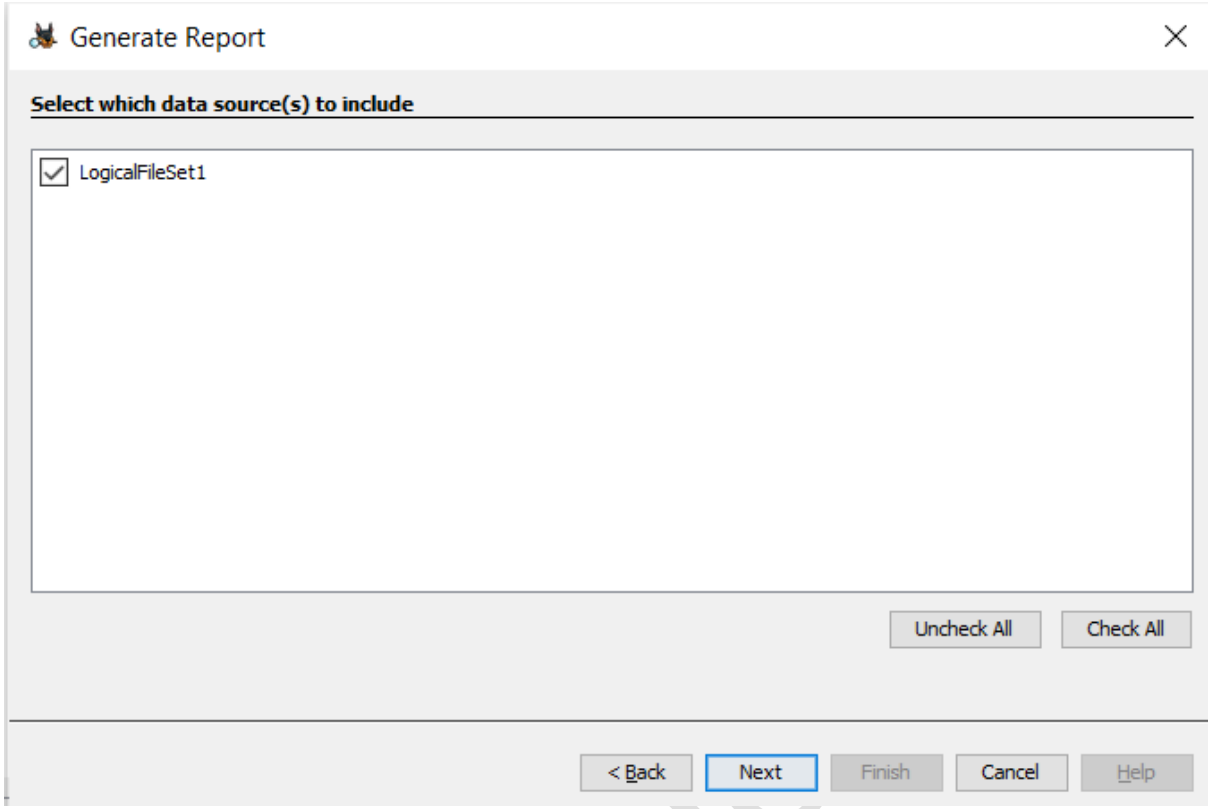
Step 2. Notice the GUI.


Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in HTML format.
Header:
Footer:
< Back
Next >
Finish
Cancel
Help

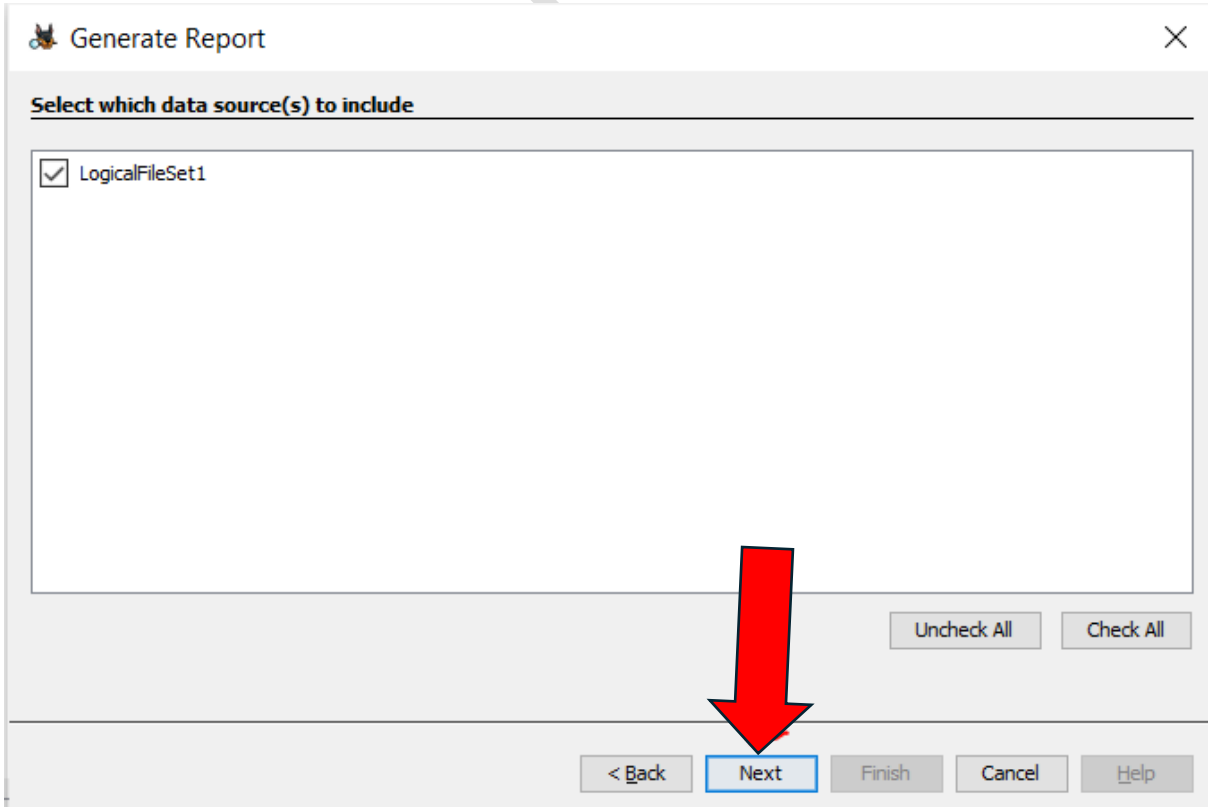
Step 3. Choose the report module. In this case HTML report and hit next



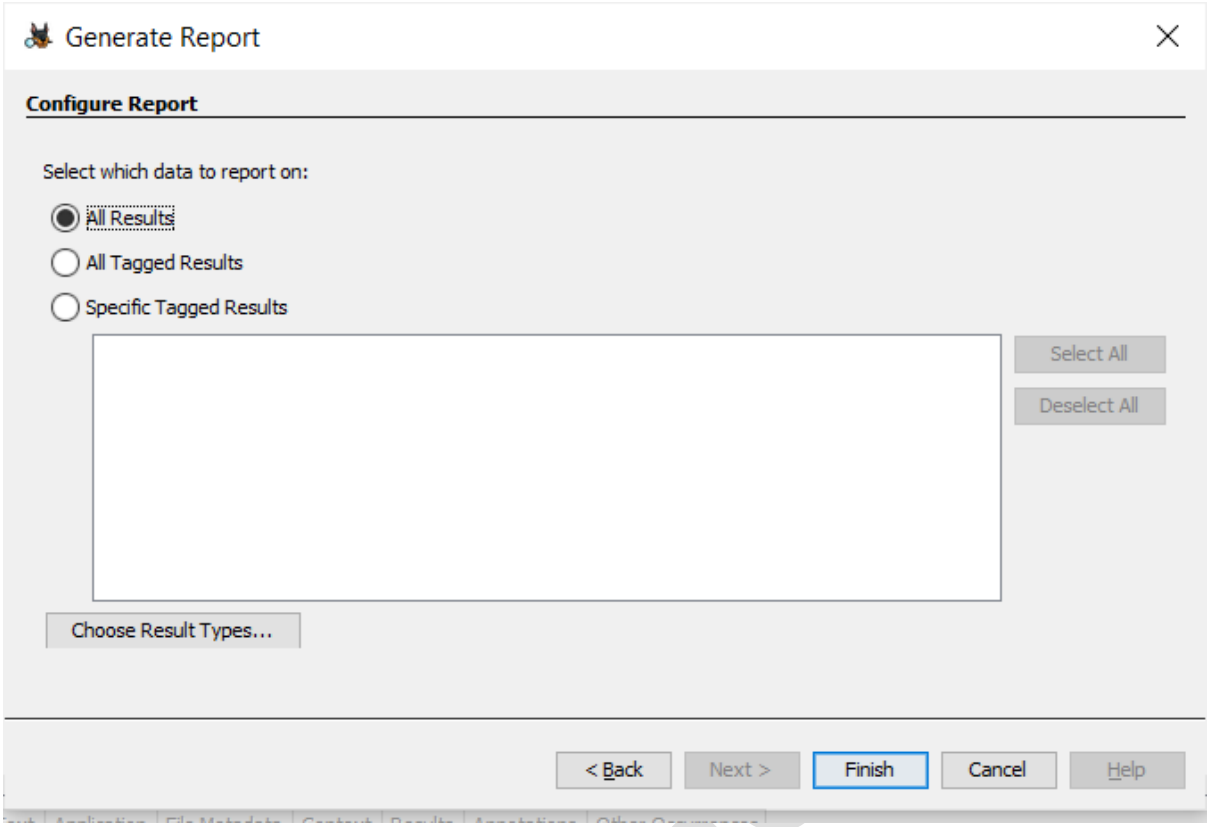
Step 4. Select data sources, in this case only one data source is used, in an investigation it could be multiple



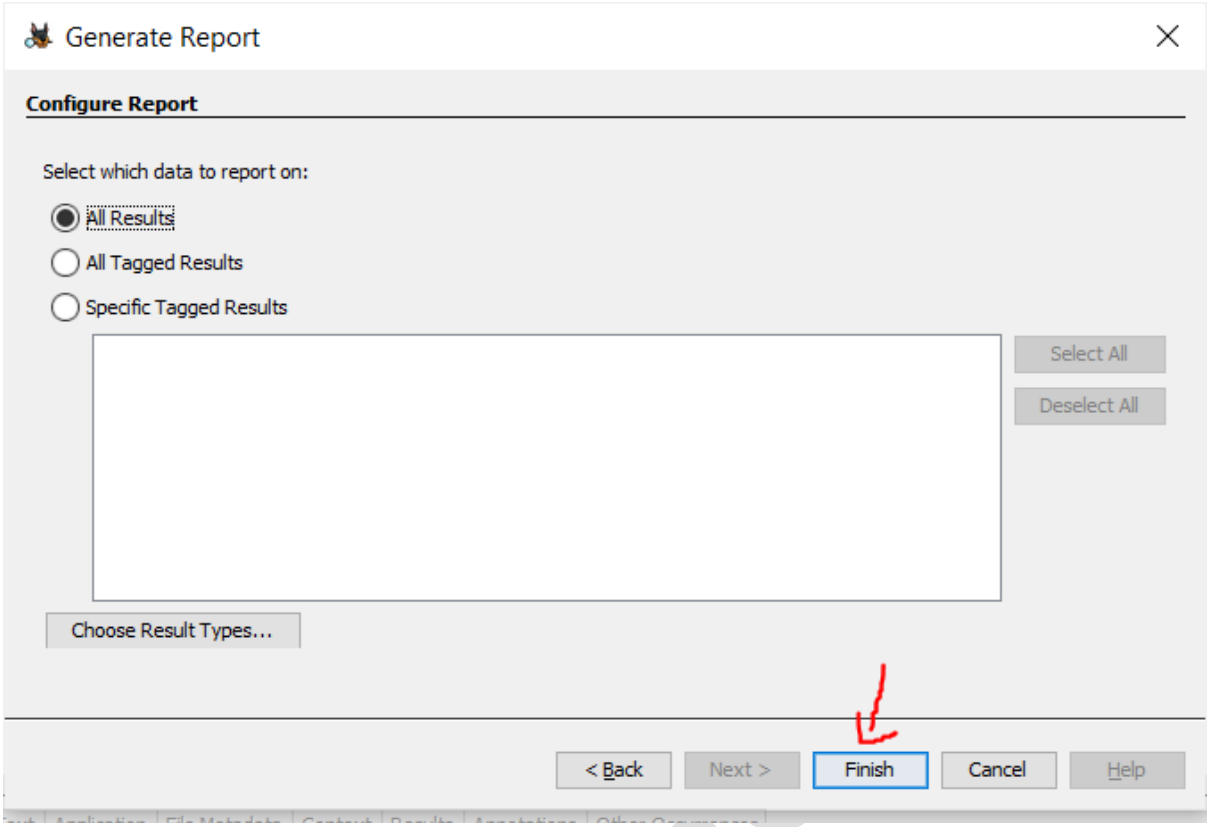
Step 5. Hit next



Step 6. Select the configure report options. Choose “all results”



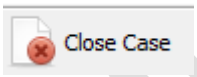
Step 7. Click finish



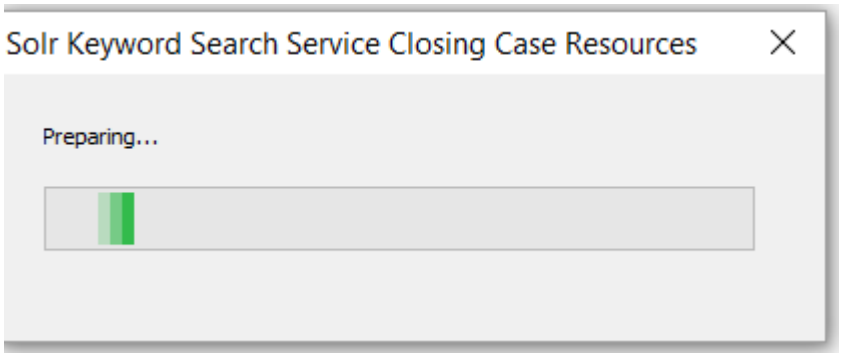
Step 8. Visit the Interesting findings section of the lab to see how to view the report.

Close Case

Step 1. Navigate to the close case tool



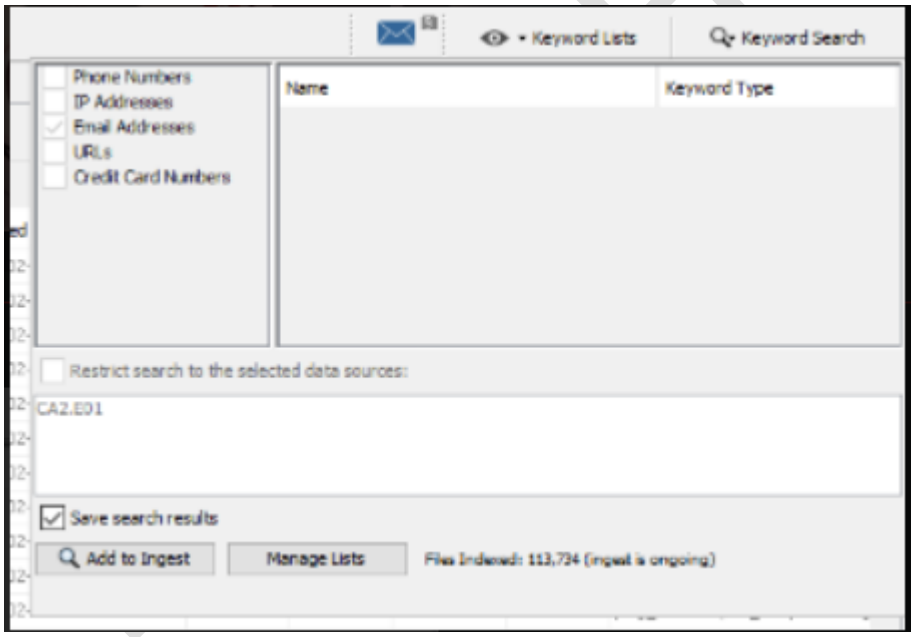
Step 2. Select close case to safely close the open case and return to the home page



Keyword Lists

Step 1. Navigate to keyword lists tool

Step 2. Open the keyword lists to see the options

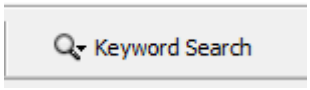


Step 3. Notice all the options available in creating a list, such as the key searches. Select each box of information relevant to what is needed which will then search for hits.

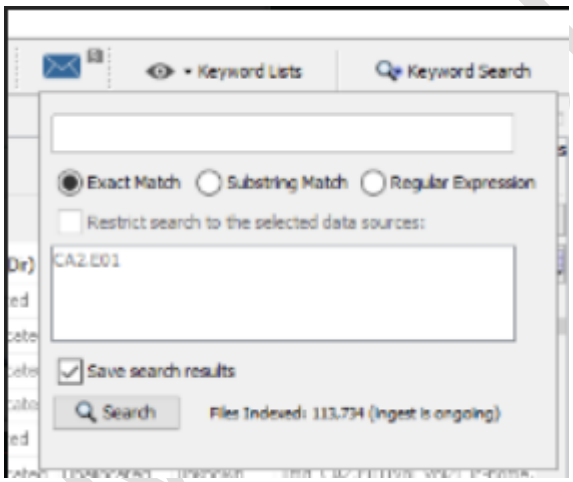
Note: *This can help an investigator quickly hit the relevant pieces of information, should the relevant information be known.*

Keyword Search

Step 1. Navigate to the keyword search tool



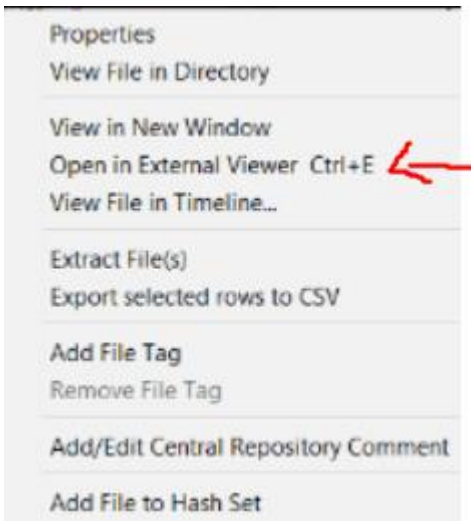
Step 2. Notice the available options for searching which allows the investigator to search for an exact match of the keyword, a substring match or regular expression



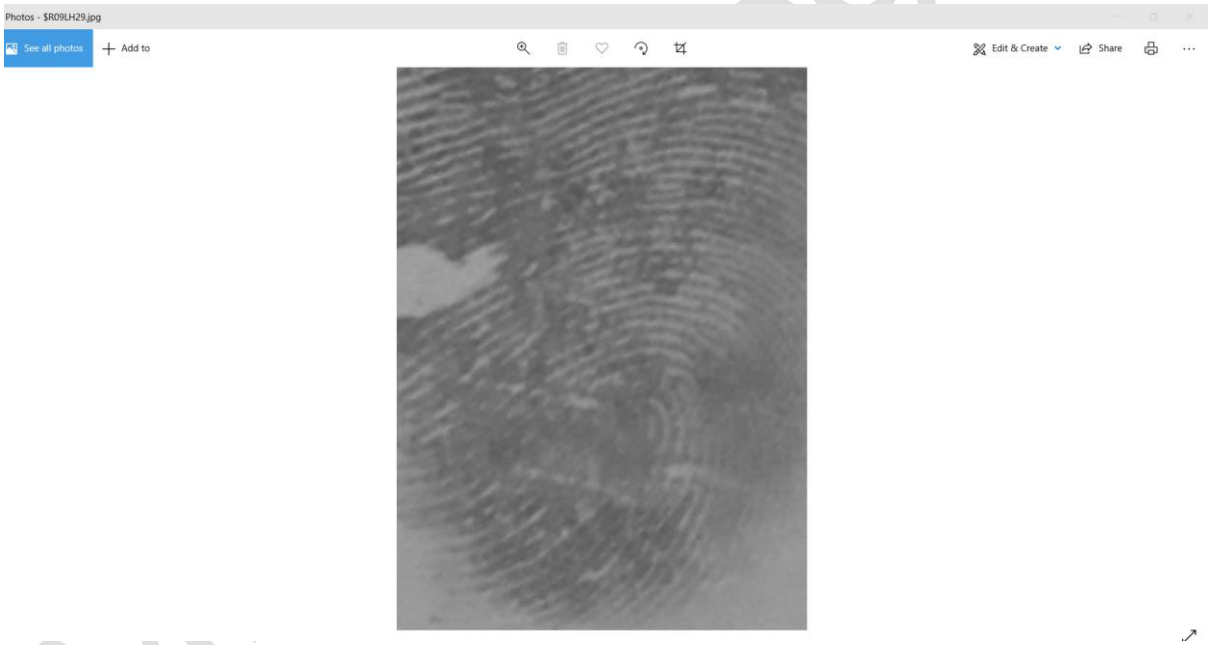
Step 3. Visit the interesting findings section of the lab to see results of a specific search

External viewer

Step 1. Right click on an image and select “external viewer”

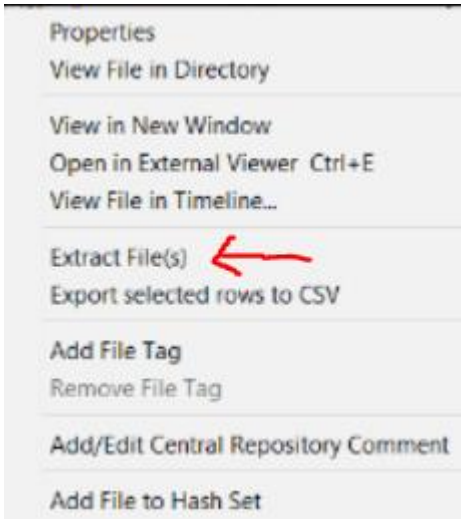


Step 2. Once selected the image will be opened on a related image software such as photos

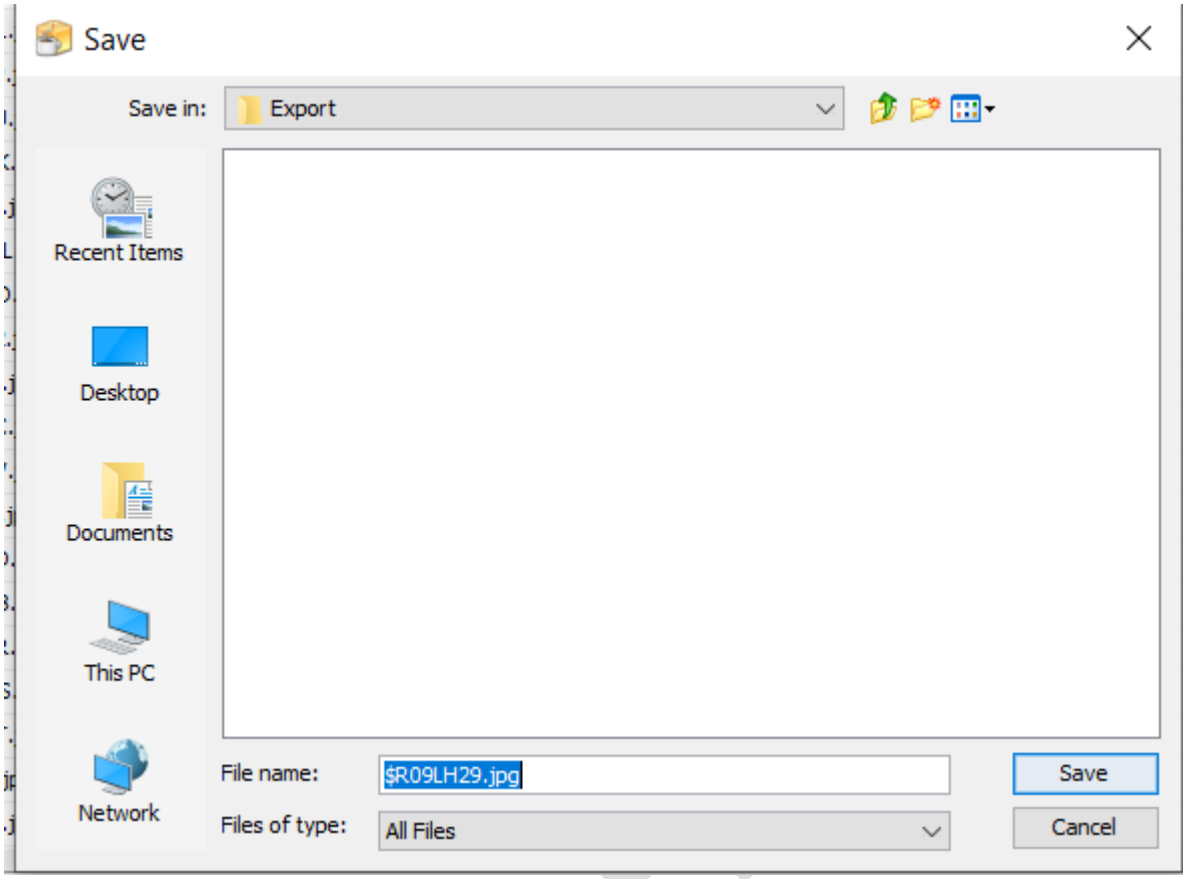


Extraction

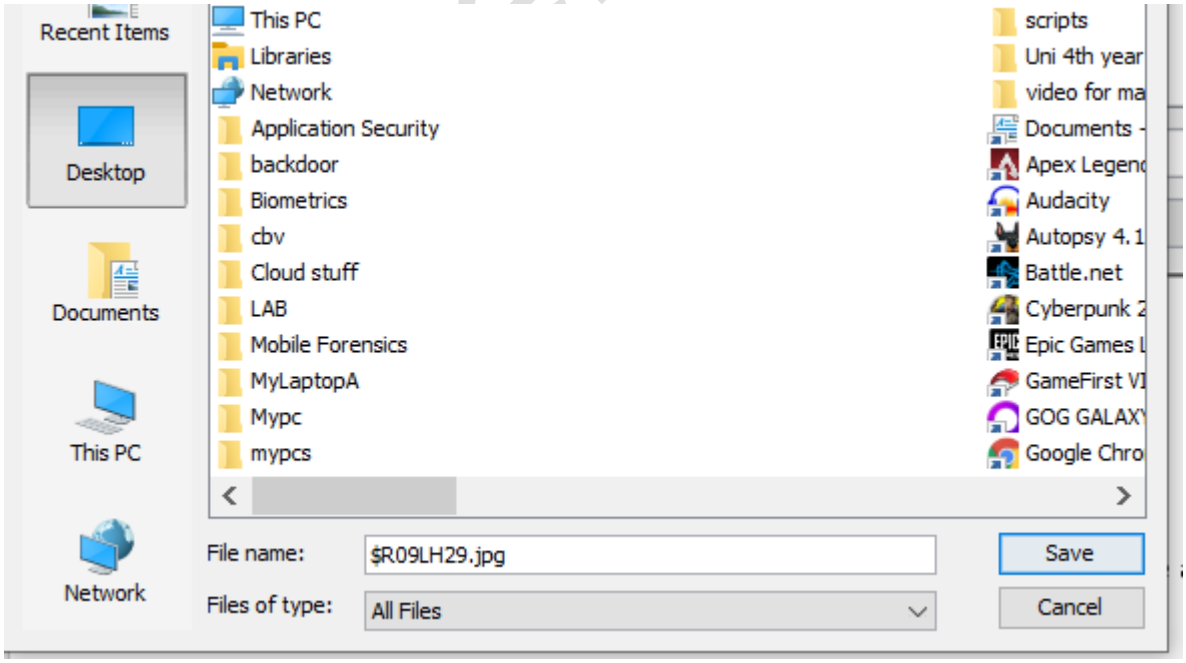
Step 1. Right click on an image and select “extract files”



Step 2. Select the extract destination



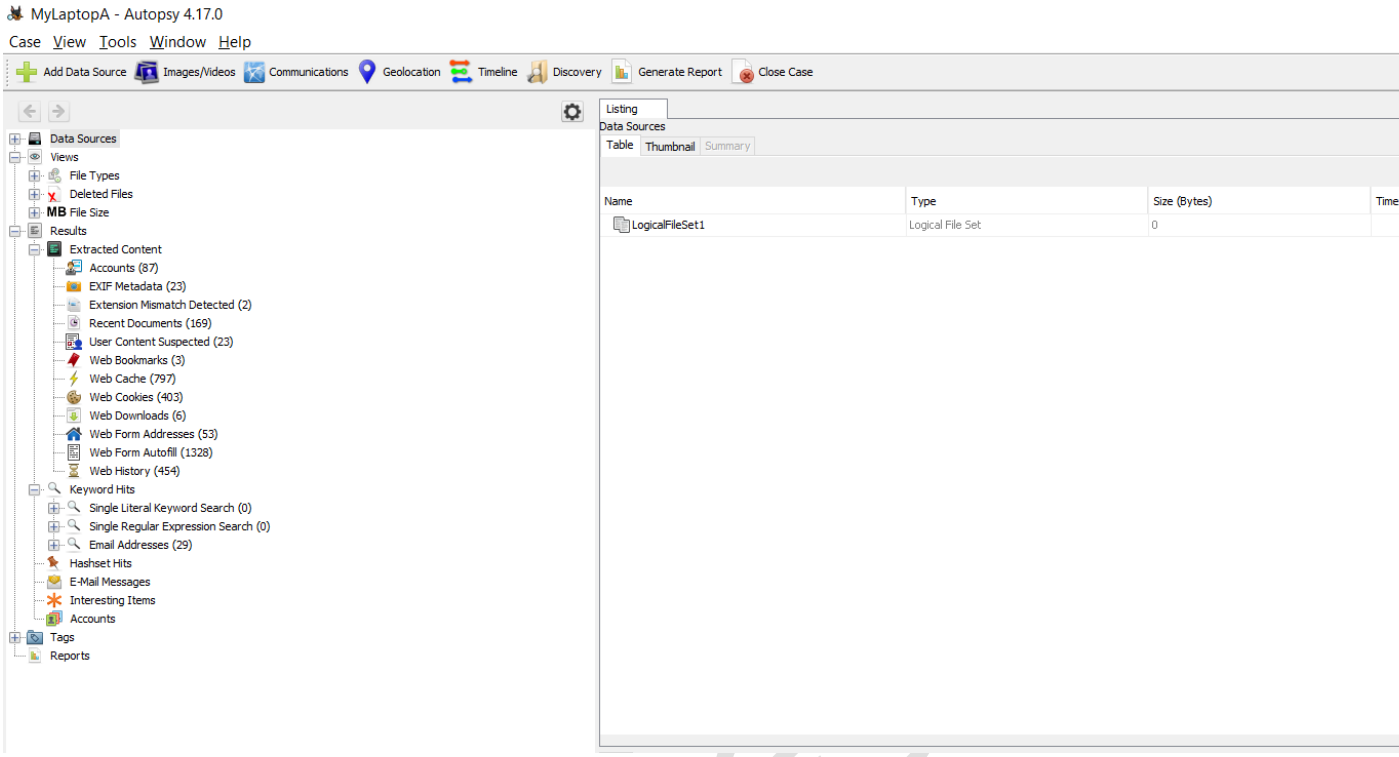
Step 3. Save the file



Step 4. Notice the file has been saved and is viewable from the save location

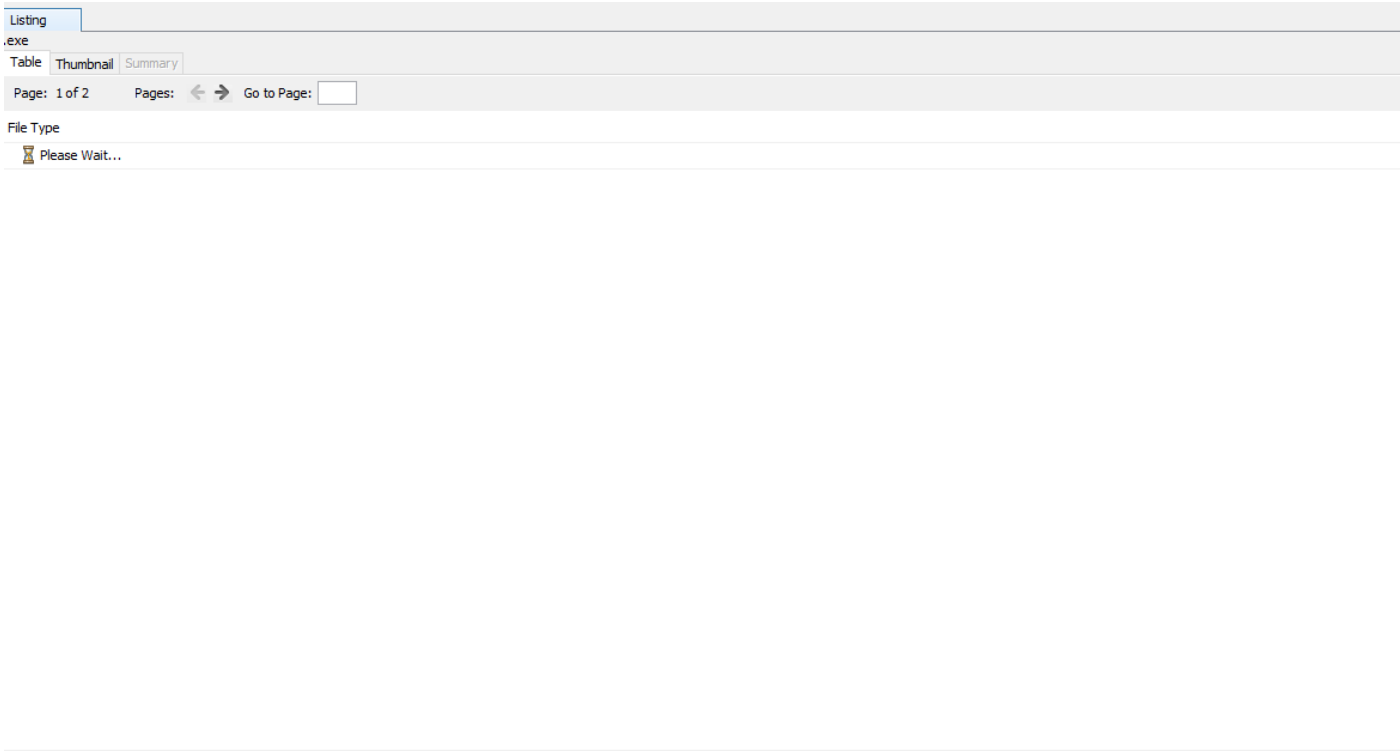
Lab – Starting to load content

Step 1 – Now that the Setup has been completed, you will see a bunch of options, which may look overwhelming at first

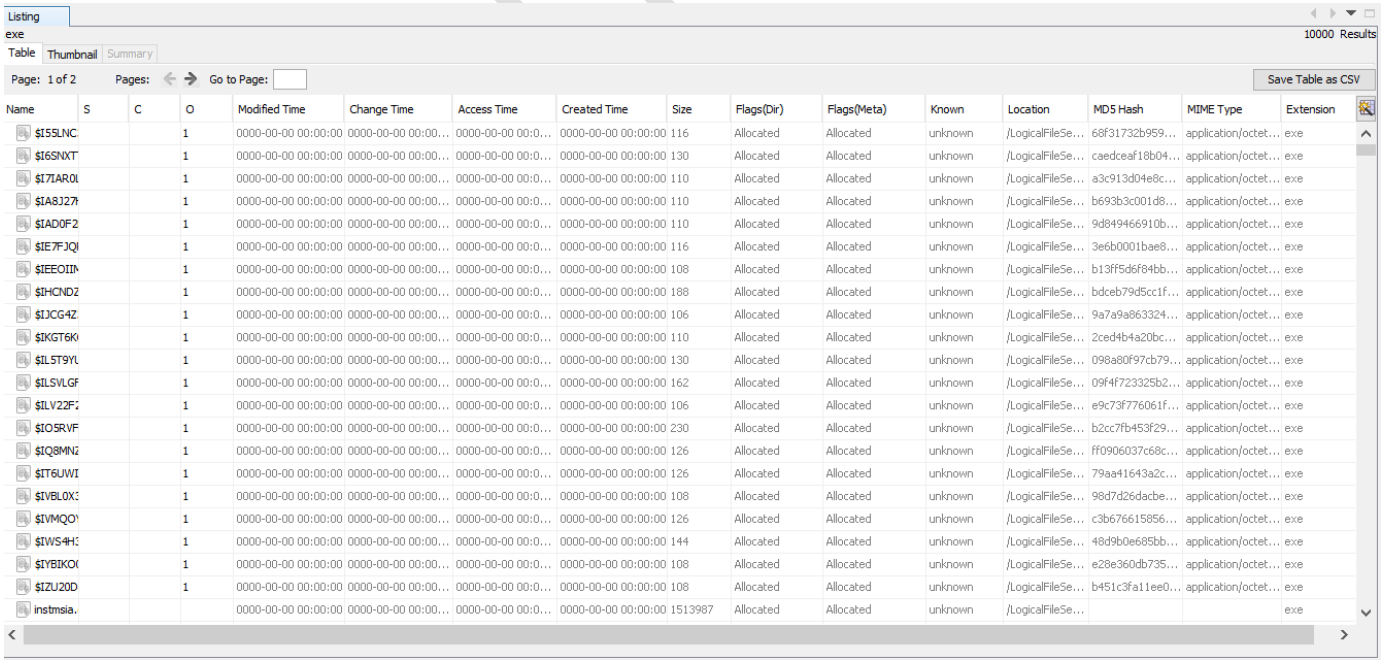


Step 2. Click into each option available so that the files are all loaded for when we surf the content

Note: *What you see before the content of a specific category has loaded*



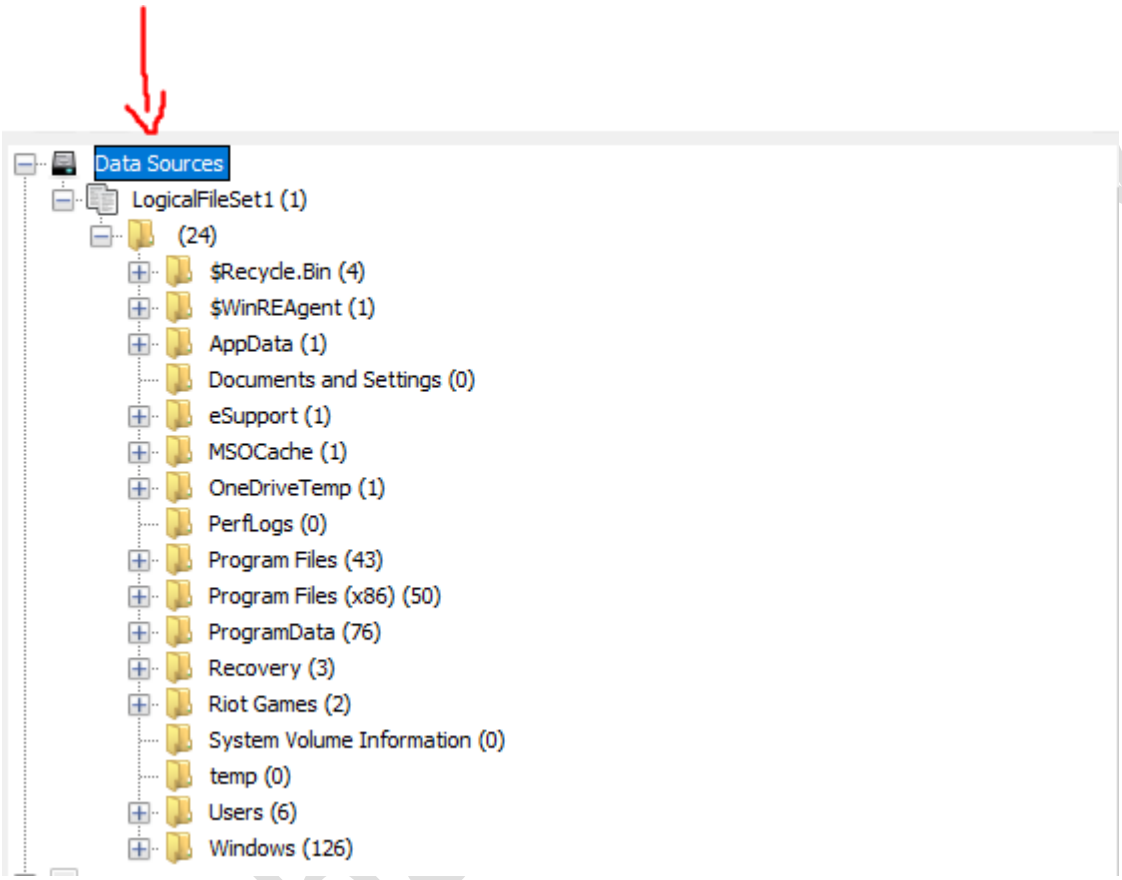
Note: *<u>An example</u> of what you will see after the field has populated*



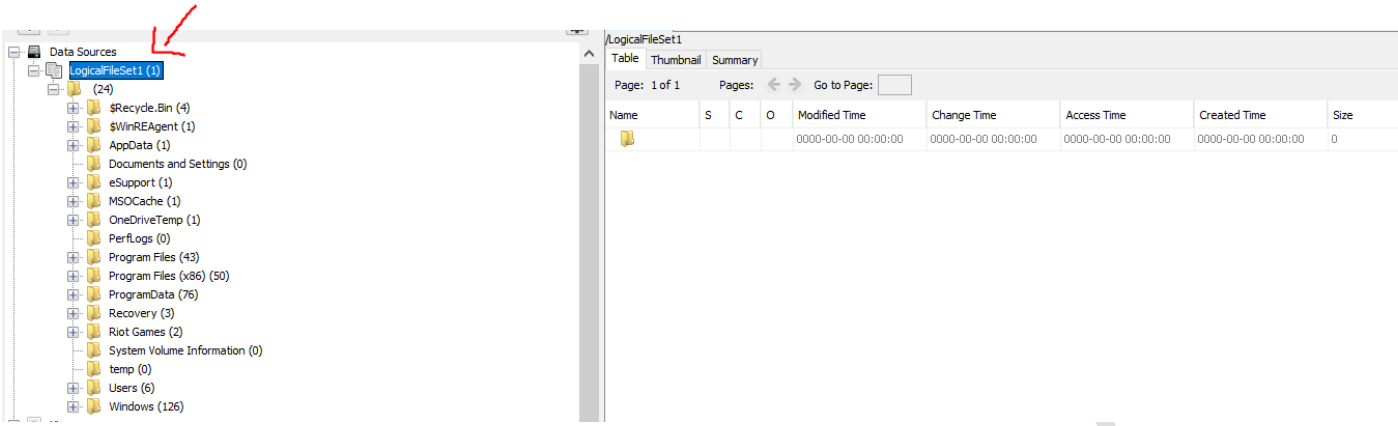
Lab – Learning the directories and files being found

Data sources – LogicalFileSet1

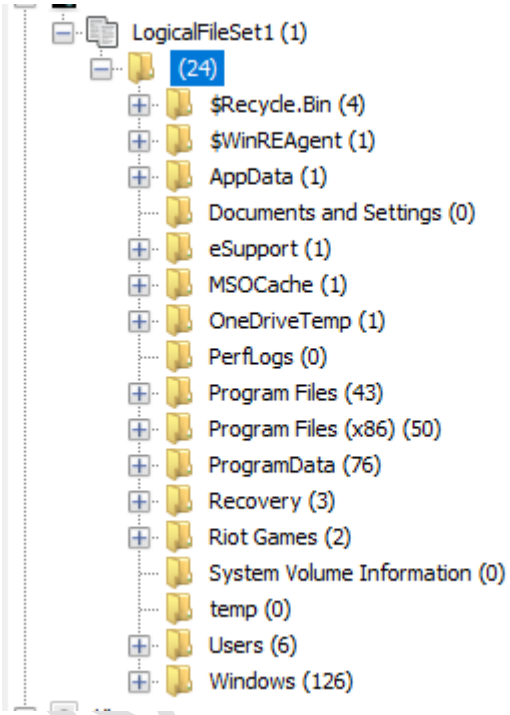
Step 1. Firstly, acknowledge the data sources section



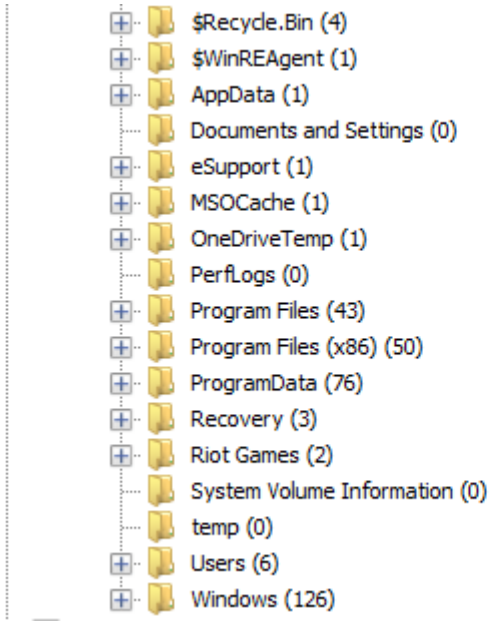
Step 2. Within the data sources section, you will see the LogicalFileSet, which will contain a lot of interesting directories



Step 3. Inside the LogicalFileSet1 you will see several directories, this number will be completely based on the contents of your laptop, in this case we have 24 directories.

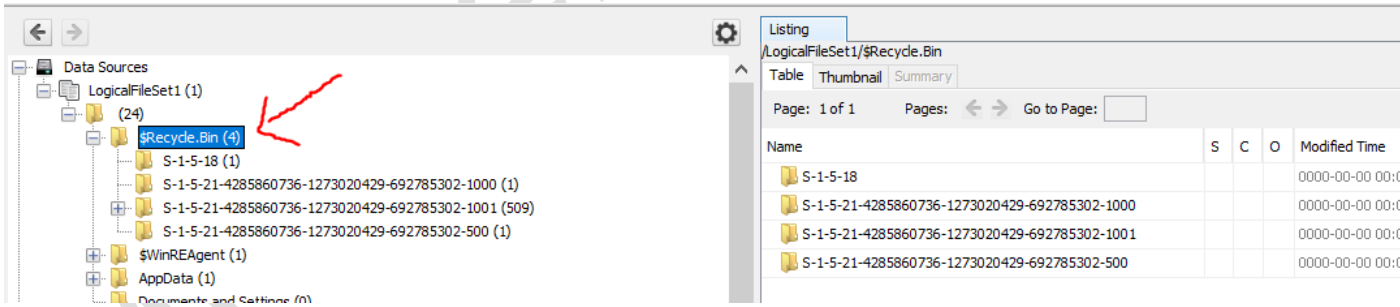


Step 4. Just under the 24 directories, you can see the directories autopsy has found relevant to the contents of your laptop. These directories will also have sub directories

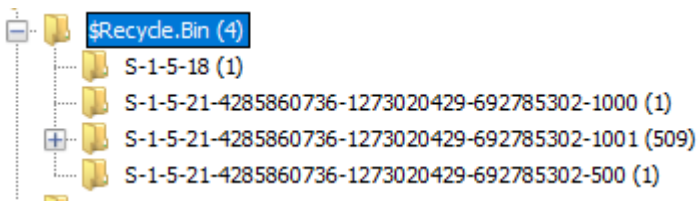


Recycle bin

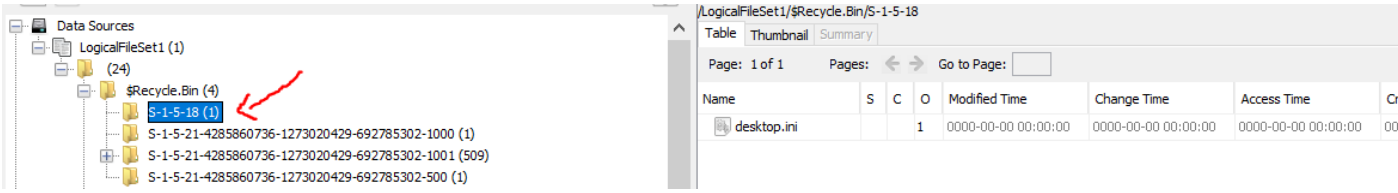
Step 1. Notice that the first directory in the LogicalFileSet is the Recycle Bin



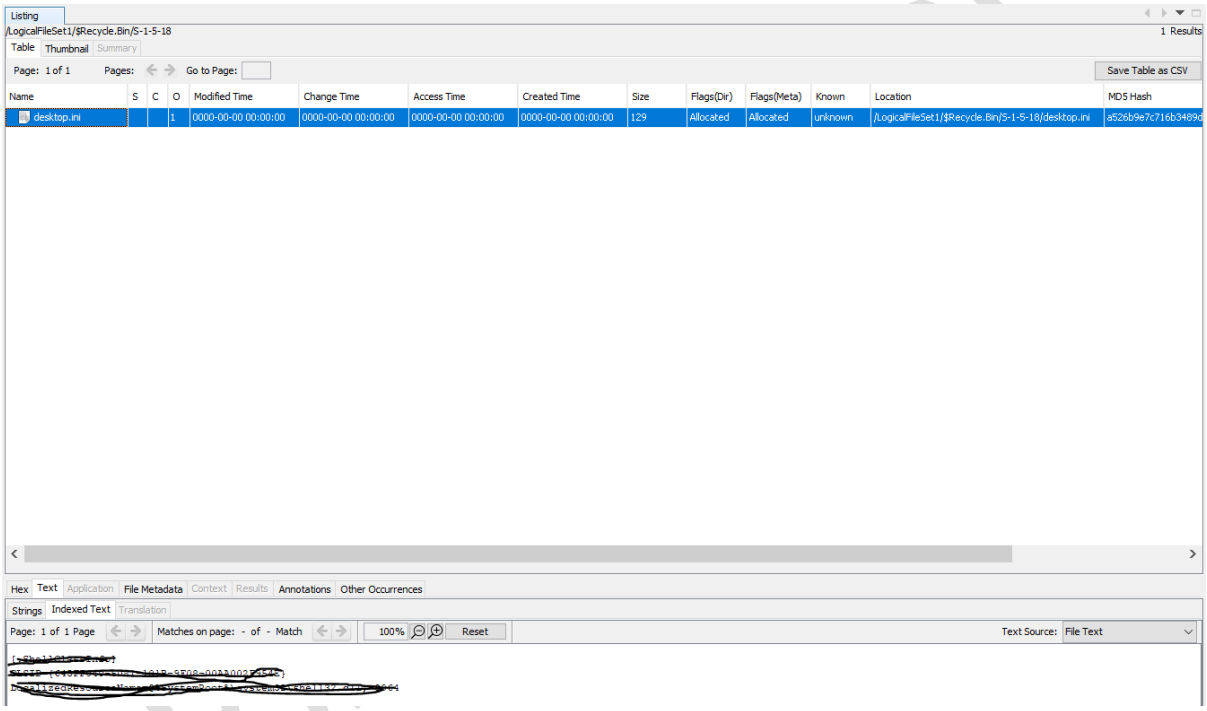
Step 2. Inside this directory notice the remnants of your recycle bin



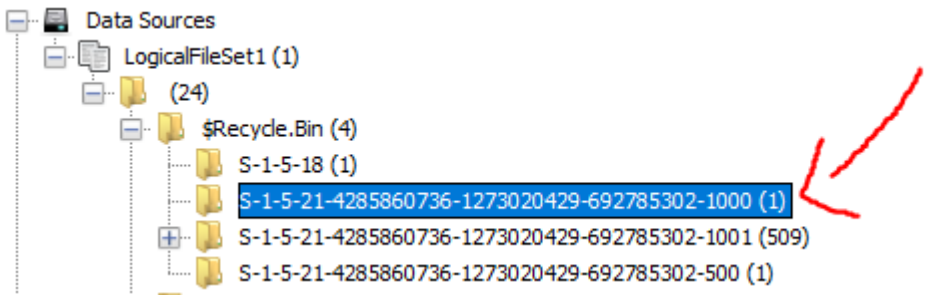
Step 3. Start analysing the contents of the recycle bin. In this case the directory being examined is S-1-5-18



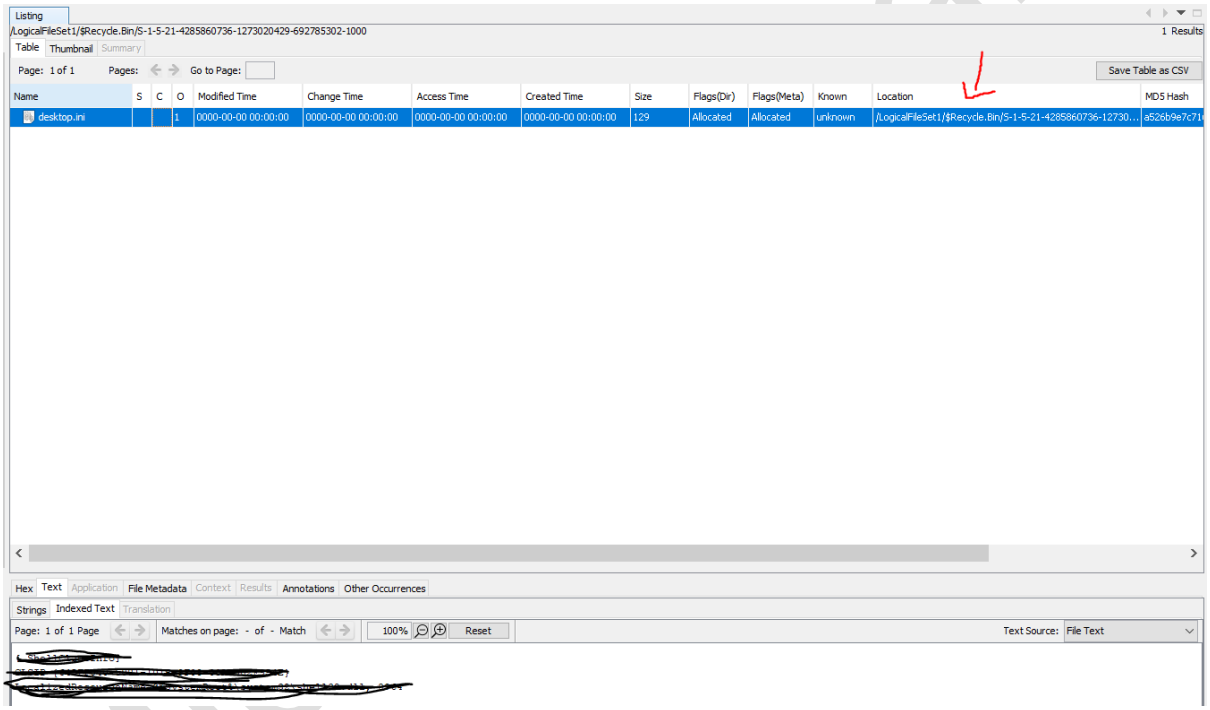
Step 4. Notice inside this directory is a file called desktop.ini. Examine the contents of the file.



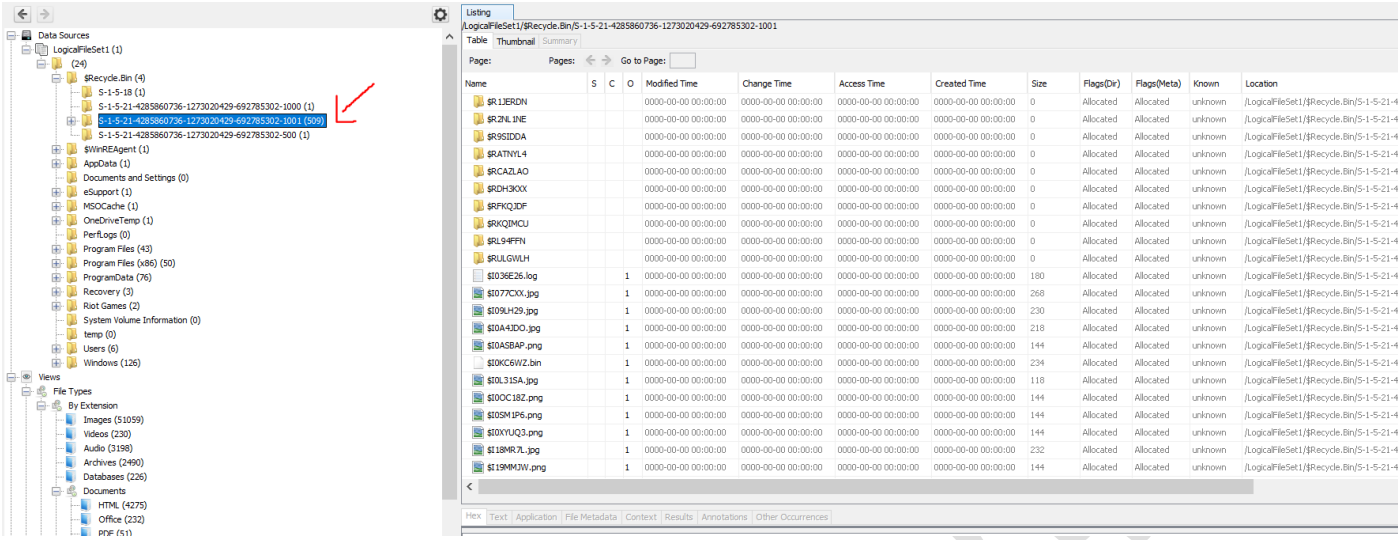
Step 5. Start analysing the contents of the S-1-5-21-4285860736-1273020429-692785302-1000



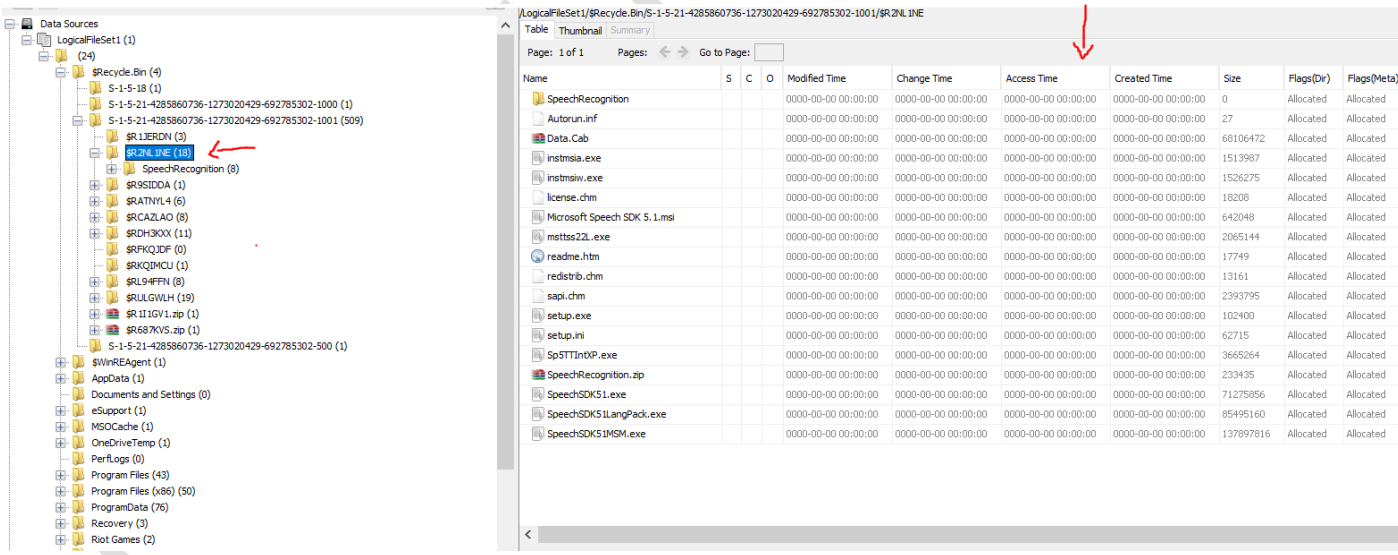
Step 6. Inside S-1-5-21-4285860736-1273020429-692785302-1000 file is the same desktop.ini file. Notice only the location of the file has changed



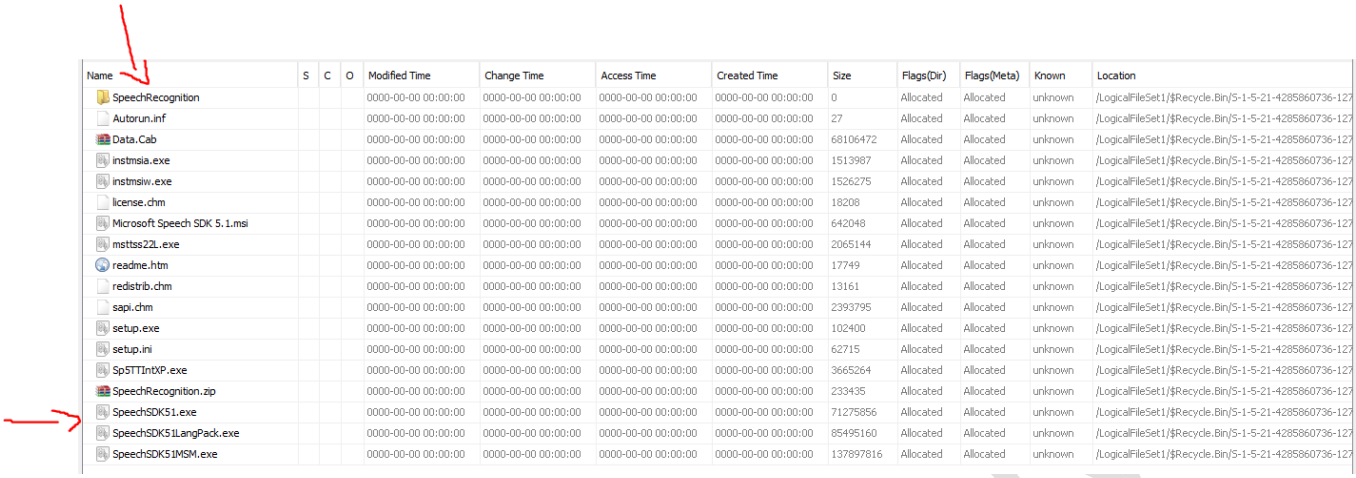
Step 7. Start analysing the contents of the S-1-5-21-4285860736-1273020429-692785302-1001 directory



Step 8. Notice the contents of the recycle bin, on this laptop there has been a directory called $Sr2nL1NE, for the sake of time lets choose this directory and examine the contents.

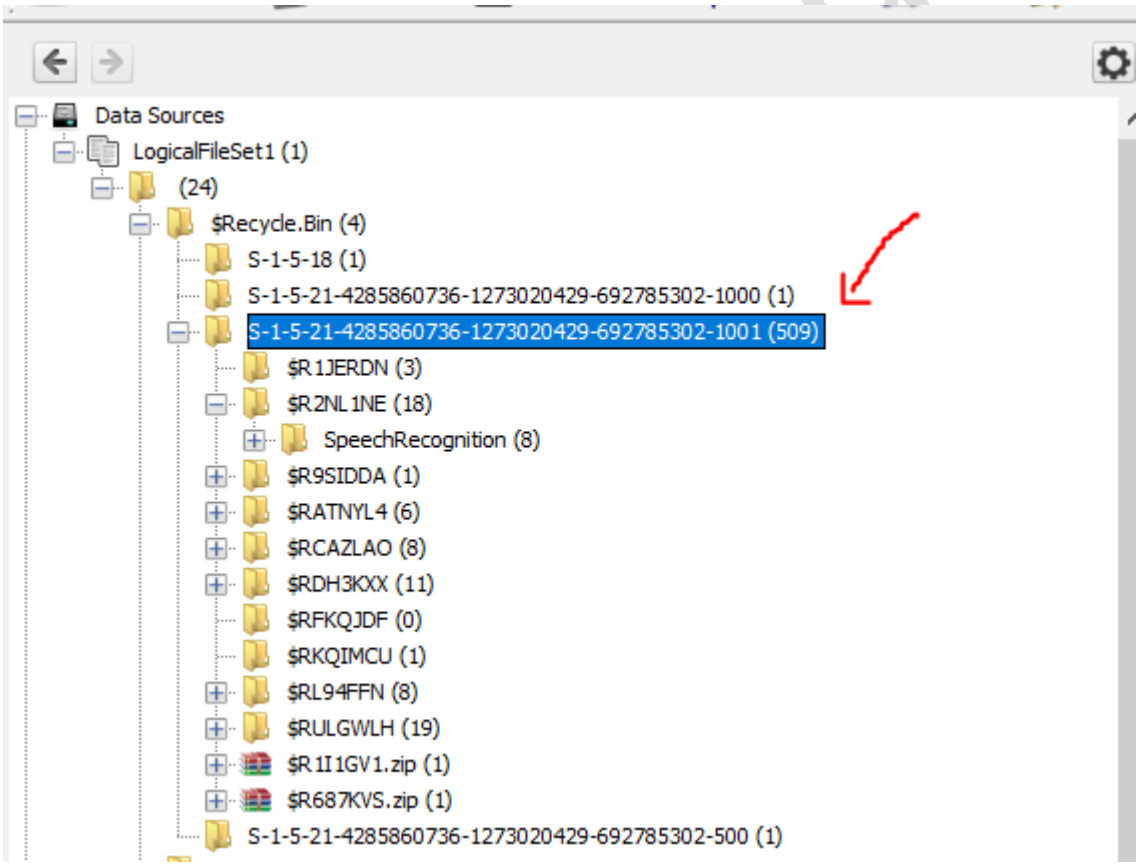


Step 9. Notice the amount of SpeechRecognition related data, during an investigation it would be safe to assume that biometric data is being held on the laptop being examined.



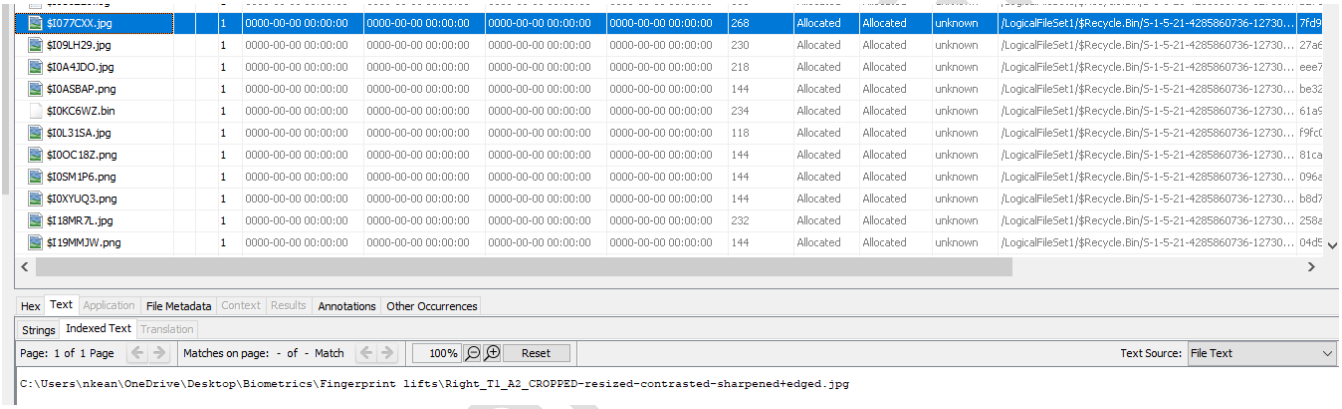
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
SpeechRecognition				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
Autorun.inf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	27	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
Data.Cab				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	68106472	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
instmsia.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1513987	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
instmsiw.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1526275	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
license.chm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18208	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
Microsoft Speech SDK 5.1.msi				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	642048	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
msttss22L.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2065144	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
readme.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17749	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
redistrib.chm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13161	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
sapi.chm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2393795	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
setup.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	102400	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
setup.ini				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	62715	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
Sp5TTIntXP.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3665264	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
SpeechRecognition.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	233435	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
SpeechSDK51.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71275856	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
SpeechSDK51LangPack.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	85495160	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127
SpeechSDK51MSM.exe				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	137897816	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-21-4285860736-127

Step 10. Going back to the main directory and reanalysing the contents

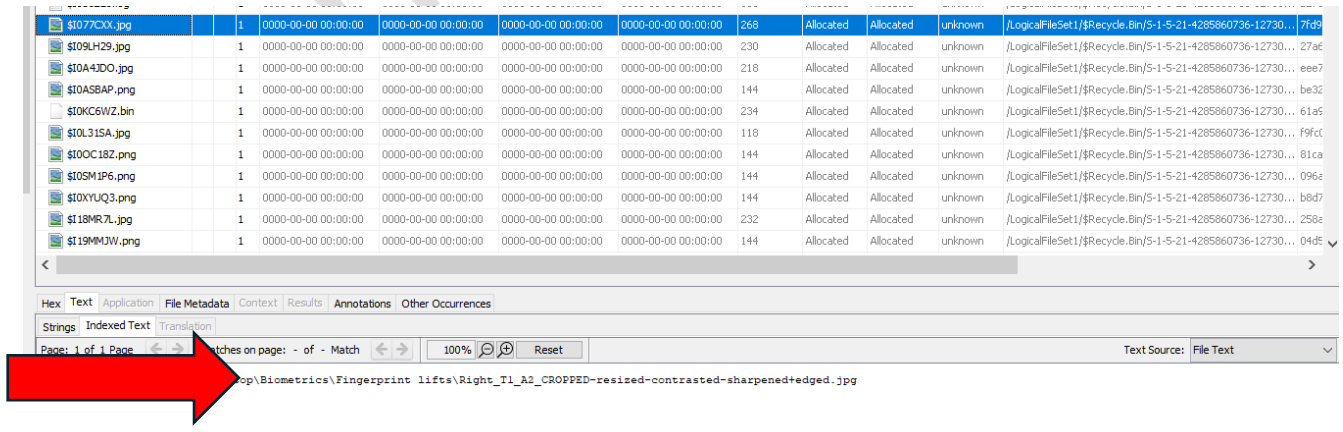


Step 11. Select an image held within the directory to see the contents.

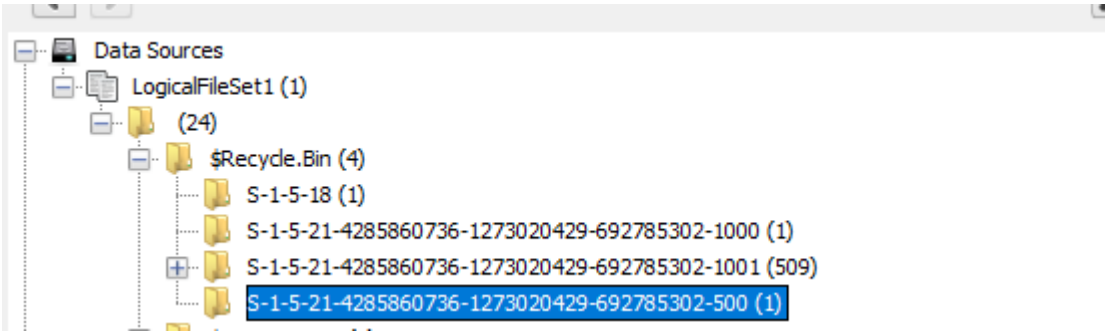
Step 12. Analyse the contents of the selected image



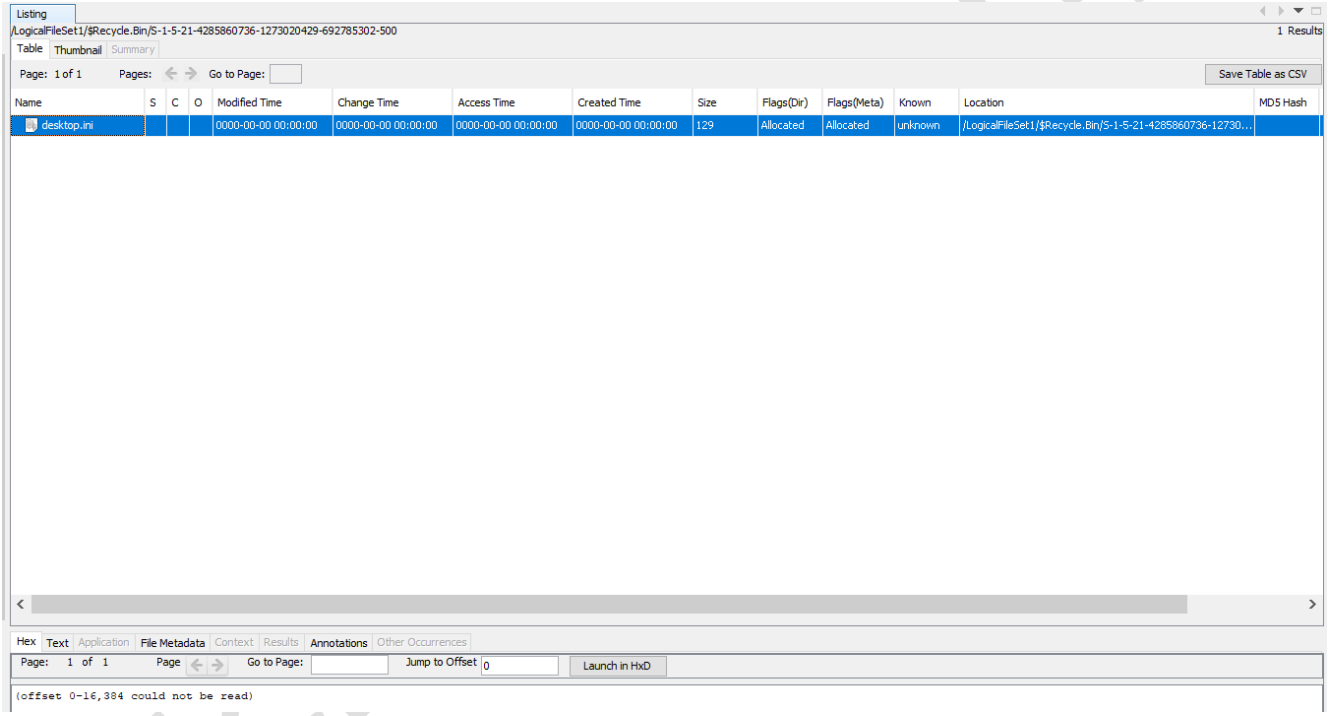
Step 13. Notice more information containing biometric data has been confirmed, which during a case would confirm your suspicion.



Step 14. Lastly start analysing the contents of the last S-1-5-21-4285860736-1273020429-692785302-500 directory

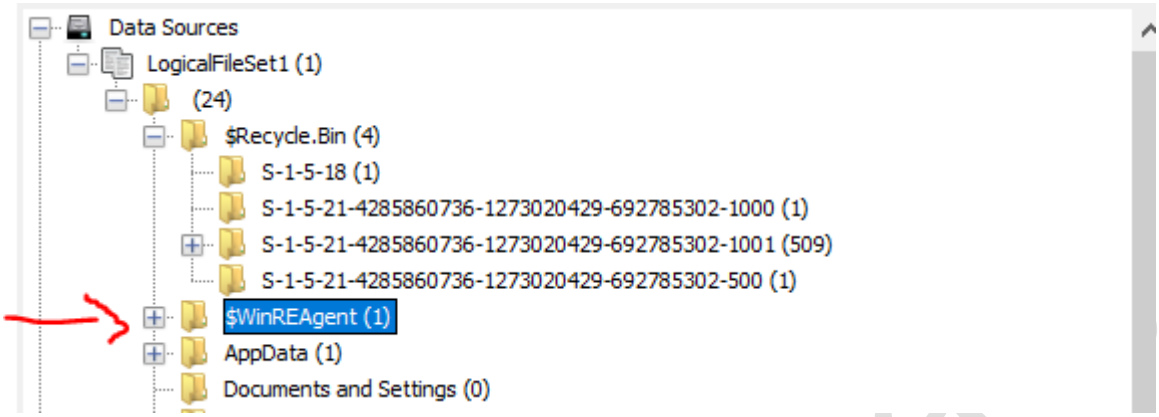


Step 15. Inside this directory is another desktop.ini file, this time round the file could not be read.

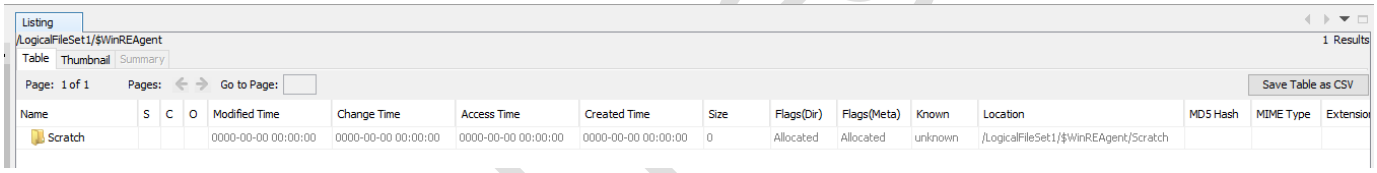


WinREAgent

Step 1. Notice the 2nd directory inside the LogicalFileSet is WinREAgent



Step 2. Inside this directory is a sub-directory called scratch

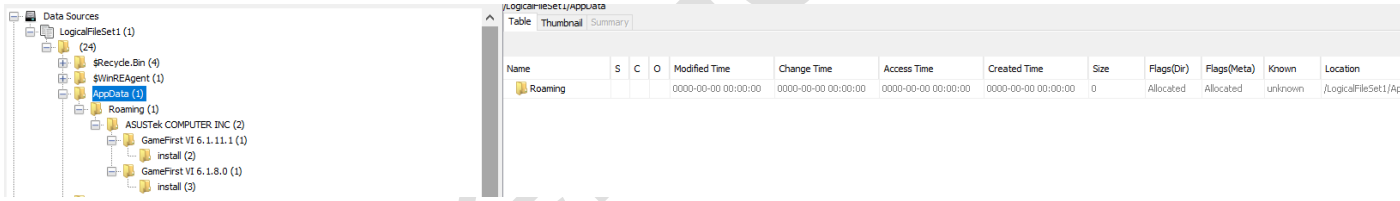


Step 3. Analyse the contents of the scratch directory

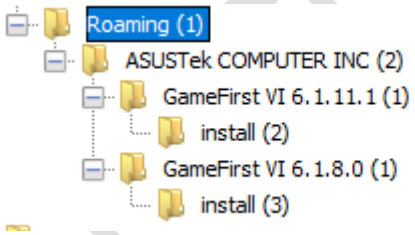
Step 4. Notice that some subdirectories will be found containing no data.

App Data

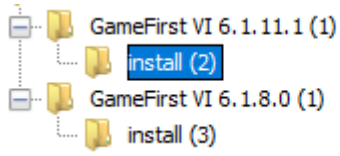
Step 1. Notice that autopsy also returns appdata in the logicalfileset



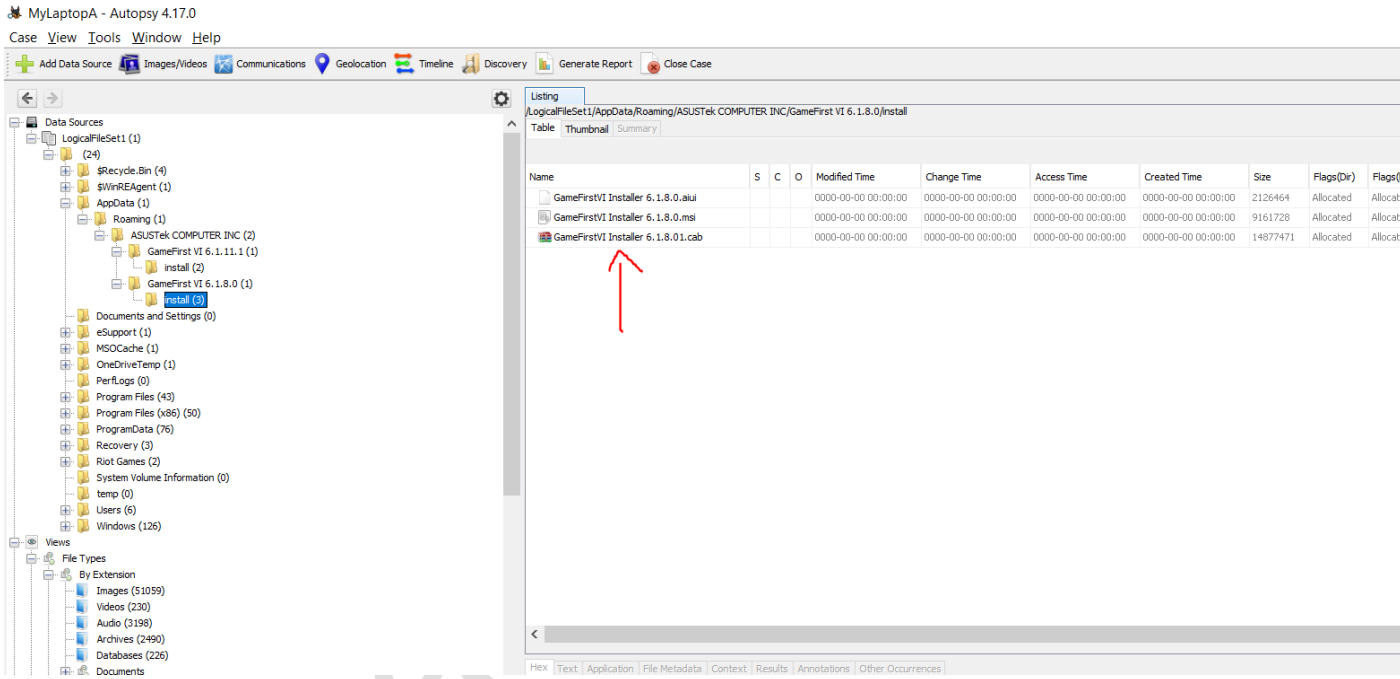
Step 2. You will be able to see a subdirectory called roaming, selecting this directory will open up gamefirst directories.



Step 3. Select on these GameFirst directories in order to see install subdirectories.



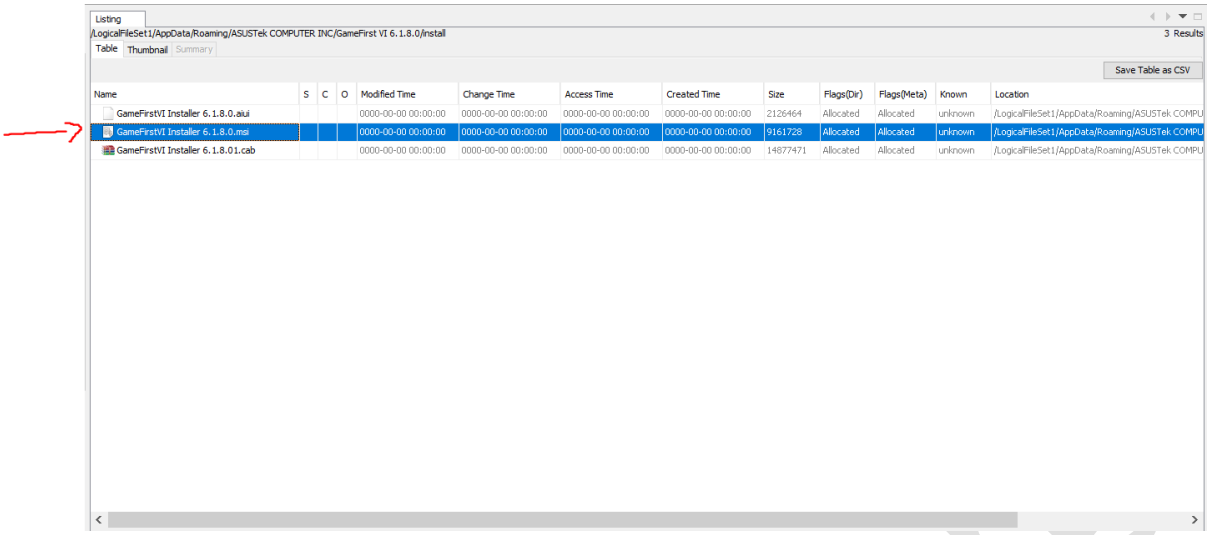
Step 4. Inside these install directories is some .cab files, these are of interest as they contain compressed data, which is used in during important window updates such as software installations



Step 5. Investigate the .cab file, you should find compressed data that is important to software installations, such as license agreements.

```
.. .LicenseAgree
ment.rtf.......h
...dP.. .Privacy
Policy.rtf..*m..
Ak....O.. .Syste
m.Management.Aut
```

Step 6. You will also notice an MSI file, this file will contain install information

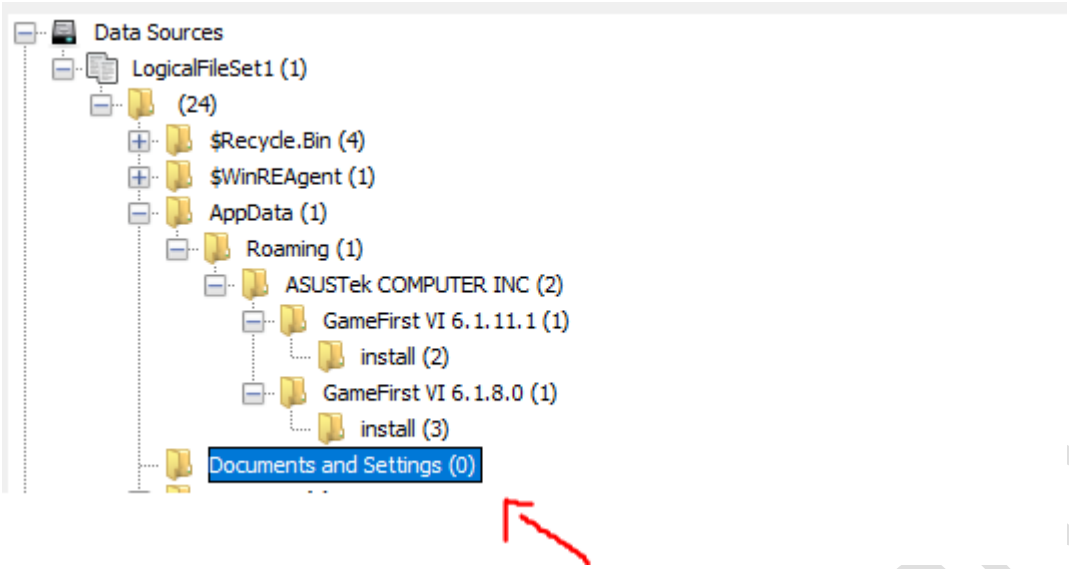


Step 7. Investigate the .msi file and see what you find, if you look hard enough you can see filewall exception information.

```
I_FirewallExcept
ionFirewallExcep
tionThe ID of th
e Firewall rule.
DisplayNameThe d
isplay name of t
he Firewall rule
```

Documents and Settings

Step 1. Notice the next directory of interest is the documents and Settings directory.

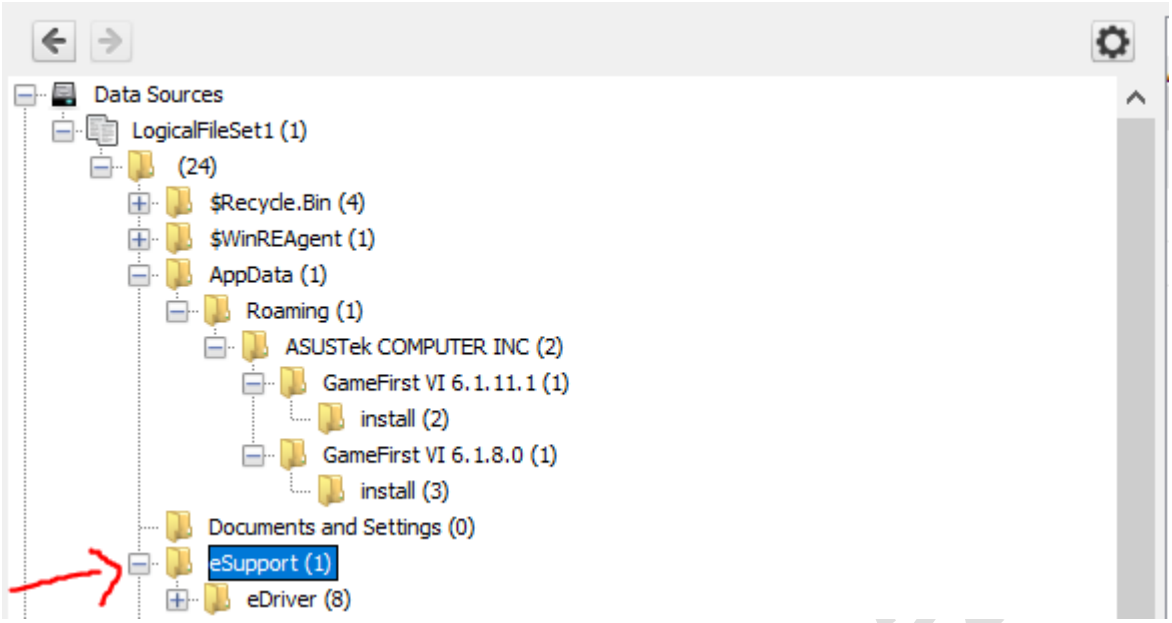


Step 2. The findings will differ from person to person, in this case the directory is empty, if your directory has been filled, it will contain important document locations as well as important settings information.

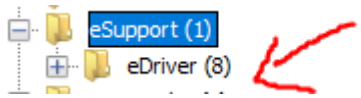
Esupport

Step 1. Notice the next directory on the list is esupport, this directory will change based on the brand of laptop you use but will contain manual and driver information, during this lab an ASUS laptop is being used

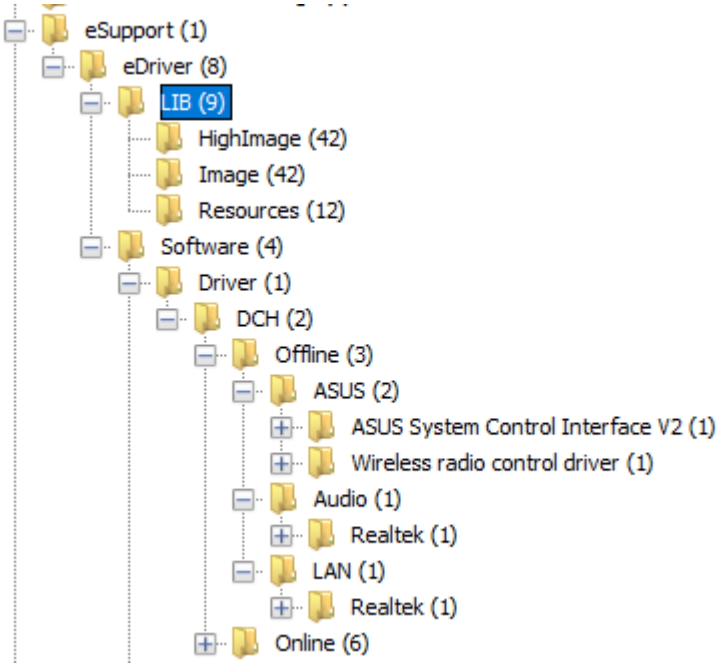
Note: *Follow along as the contents of the directory will, in most cases, be the same*



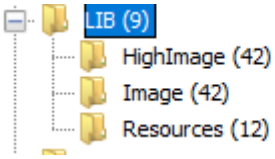
Step 2. As the laptop being used is an ASUS laptop, autopsy has found an ESupport directory, inside this directory is a subdirectory called eDriver.



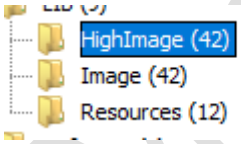
Step 3. Expand the directories of the driver directory



Step 4. Notice a lot of subdirectories have appeared, this looks more intimidating than it is so take it bit by bit. Start at your lib directory.



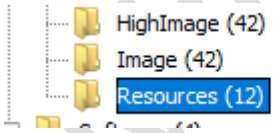
Step 5. Notice the subdirectories found within this directory, suggesting the lib directory contains resources such as images.



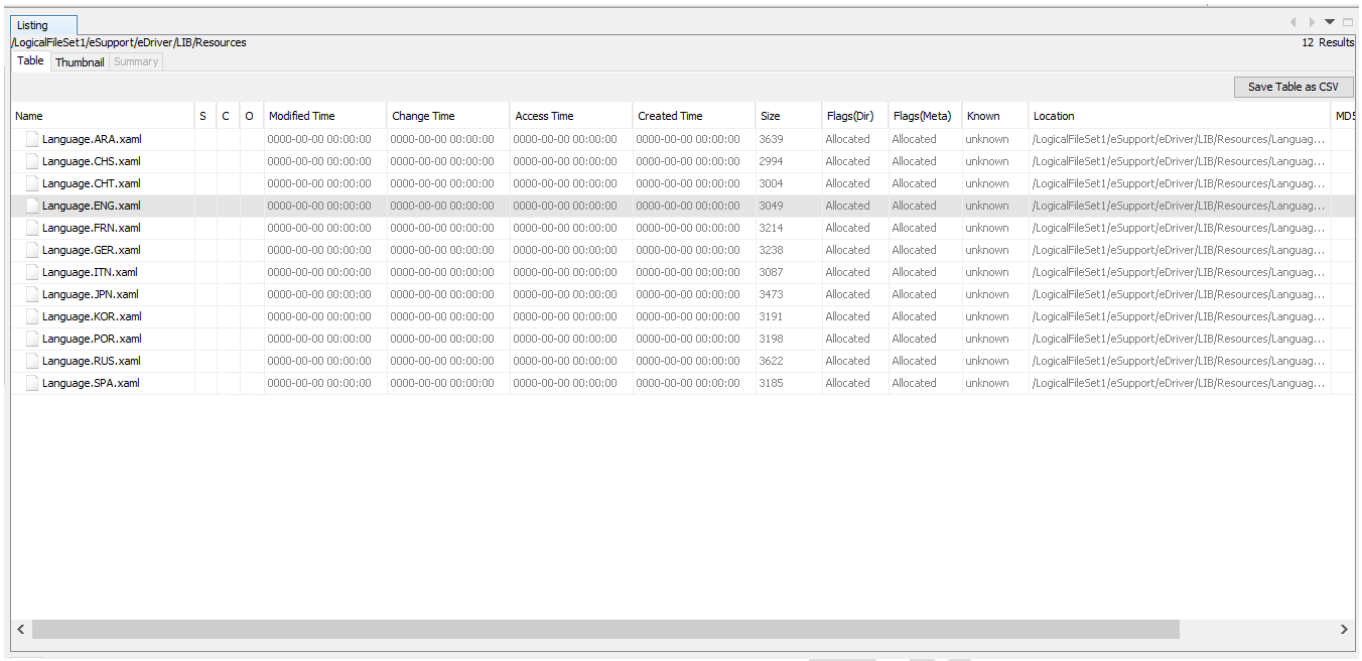
Step 6. Investigate both highimage and image, one is a high-resolution image and the other is a low-quality image. Can you tell the difference?

Note: *The first image is from the highimage section, the second image is from the image section*

Step 7. Investigate the contents of the resources directory.

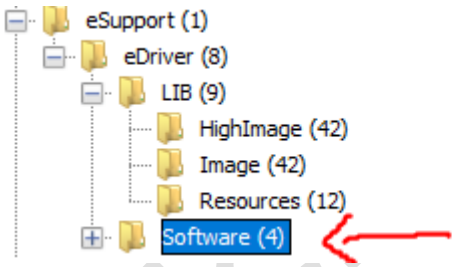


Step 8. Have you been able to determine what files this directory contains? If not, the resources directory contains your different language options.

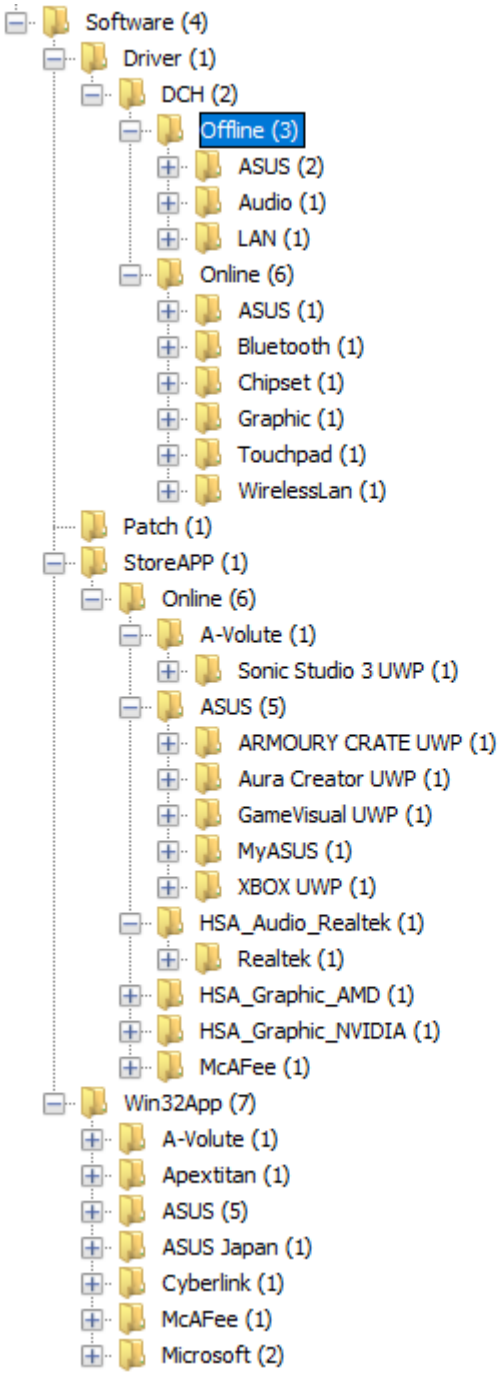


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Language.ARA.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3639	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.CHS.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2994	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.CHT.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3004	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.ENG.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3049	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.FRN.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3214	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.GER.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3238	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.ITN.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3087	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.JPN.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3473	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.KOR.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3191	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.POR.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3198	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.RUS.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3622	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...
Language.SPA.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3185	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/LIB/Resources/Languag...

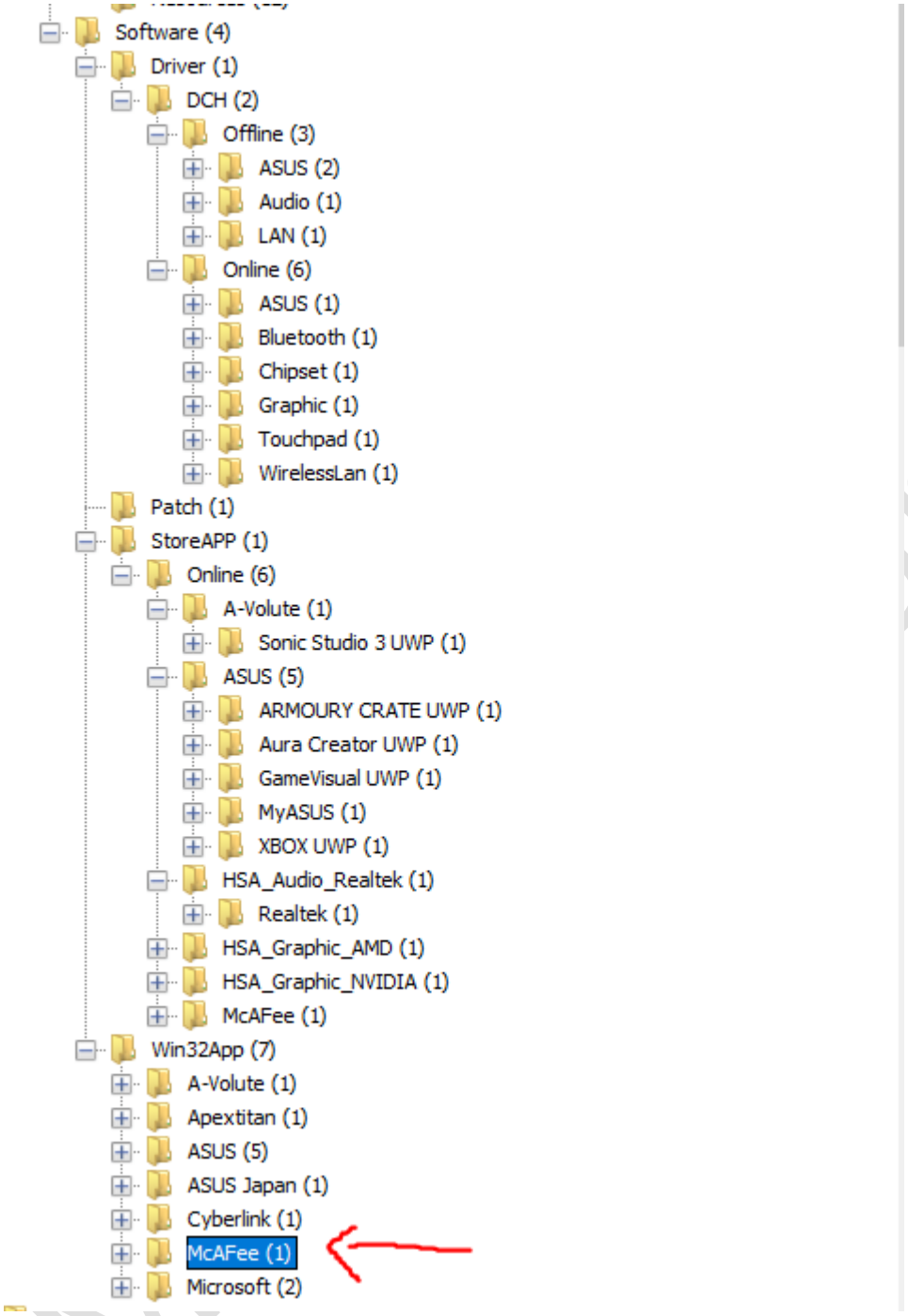
Step 9. Now on to the software portion of the subdirectories



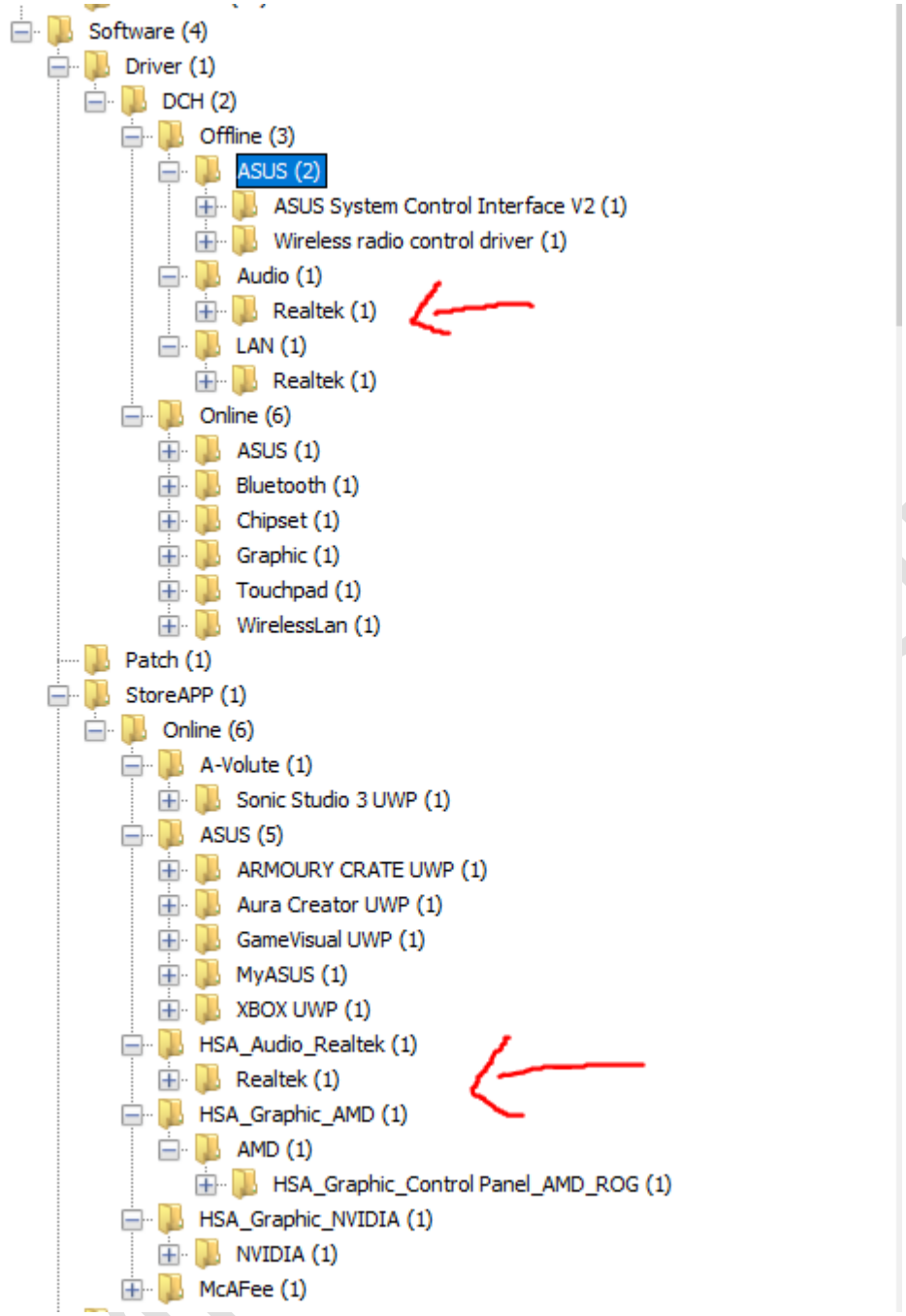
Step 10. Look at all the software directories your laptop has returned. In the case of an ASUS laptop, the following was returned



Step 11. This looks quite intimidating but is quite basic, autopsy has returned software information. This can help an investigator get more information on the software on the laptop. Such as firewalls.

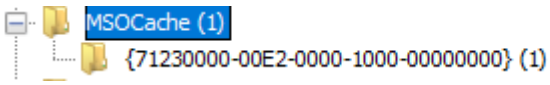


Step 12. Investigate around, you will find software specifics for the components being used such as graphics card, brands used for audio and a lot of cool and interesting things

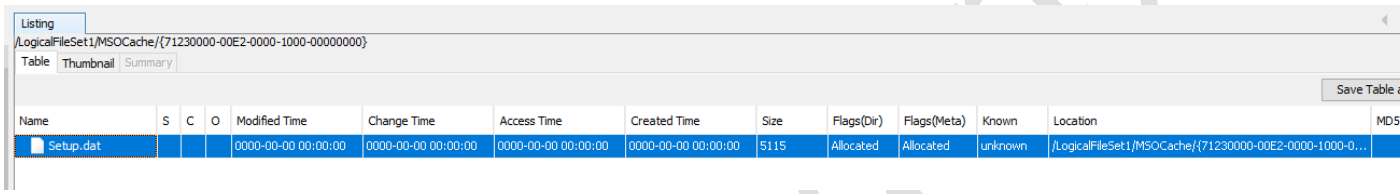


MSOCache

Step 1. The next subdirectory of the LogicalFileSet1 directory is MSOCache. This directory is put into your root directory after downloading Microsoft office and is used solely to download other components on to Microsoft office.

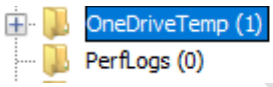


Step 2. Most laptop users will have Microsoft office, as this is the case the common finding of the typical user who has not downloaded additional features in a setup file, which is used to install the components later down the line.

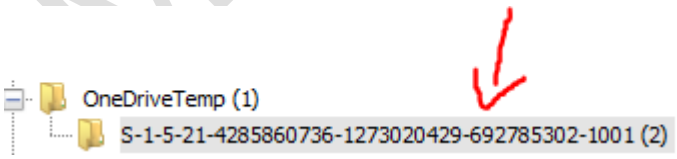


OnedriveTemp

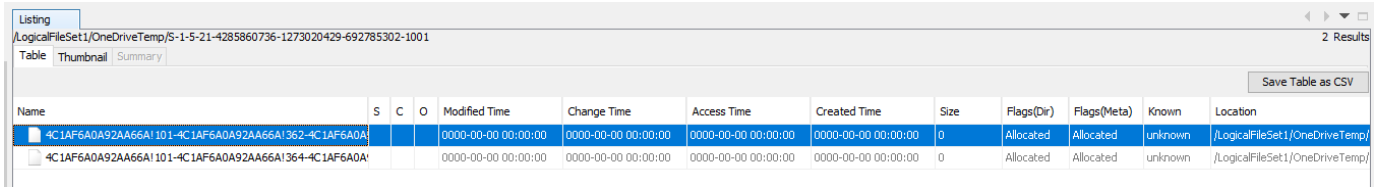
Step 1. The next directory found on the LogicalFileSet is OneDriveTemp, this directory forces itself into an existent state on your root.



Step 2. Investigate the contents of your OneDriveTemp, this will keep files related to OneDrive.

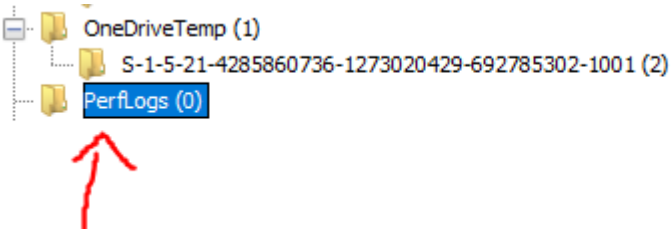


Step 3. Investigate the contents of the found directory, this will reveal two files related to OneDrive



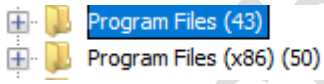
PerfLogs

Step 1. The next of the directories is PerfLogs, this will contain information relating to performance logs, and will often be empty.

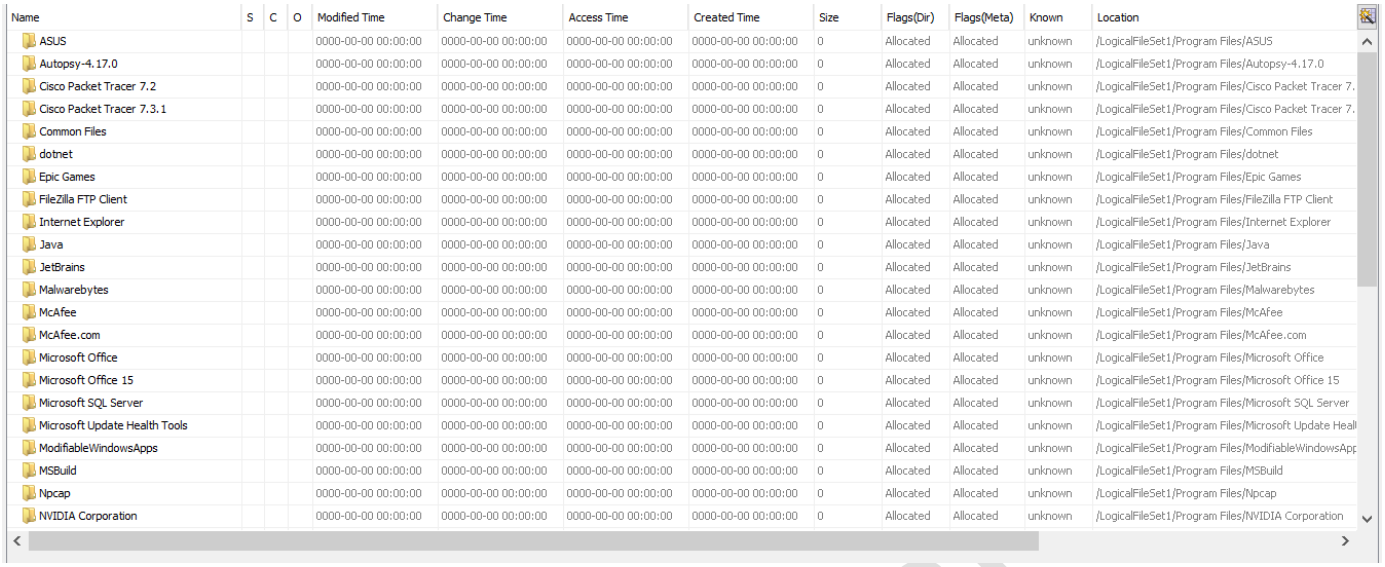


Program Files/x86

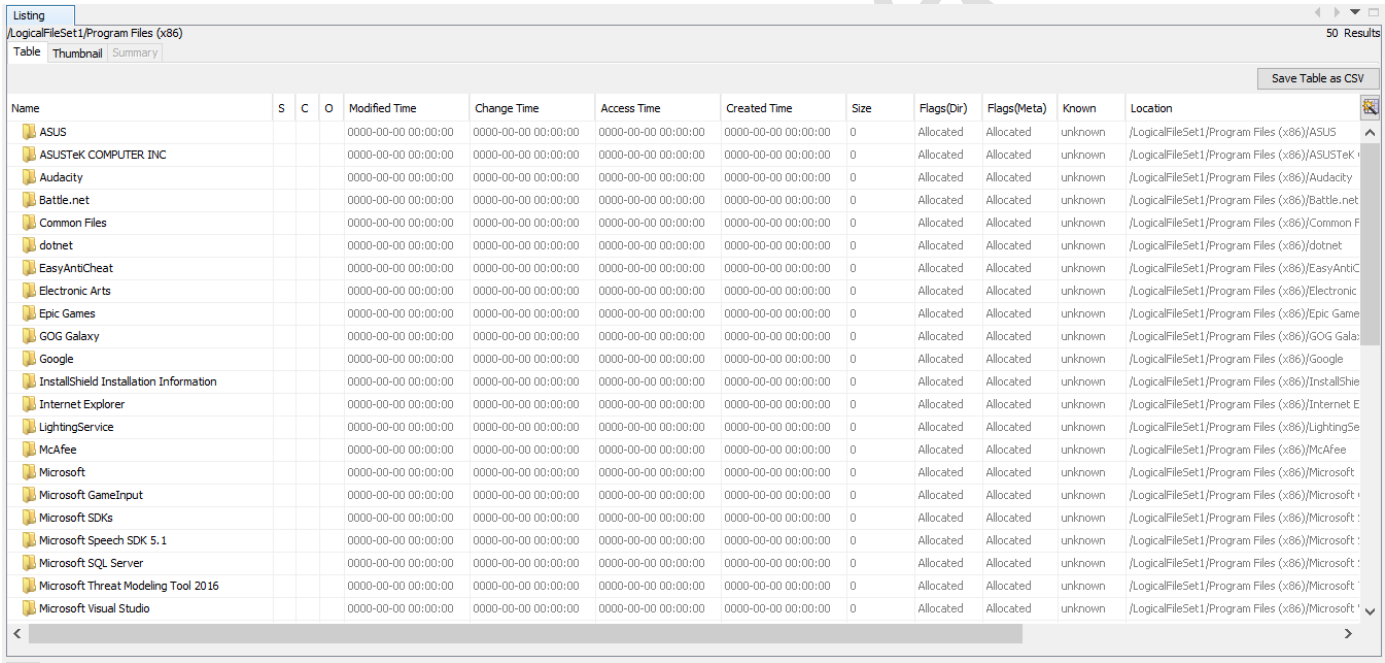
Step 1. Notice the next two directories of the LogicalFileSet directory, the program files, these directories contain programs that are unrelated to the system. One of which are your 32-bit programs, the other, 64-bit. Although this is often randomised in which file the program is set.



Step 2. Investigate the contents of these directories, you will find many programs.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ASUS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/ASUS
Autopsy-4.17.0				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Autopsy-4.17.0
Cisco Packet Tracer 7.2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Cisco Packet Tracer 7.
Cisco Packet Tracer 7.3.1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Cisco Packet Tracer 7.
Common Files				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Common Files
dotnet				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/dotnet
Epic Games				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Epic Games
FileZilla FTP Client				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/FileZilla FTP Client
Internet Explorer				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Internet Explorer
Java				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Java
JetBrains				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/JetBrains
Malwarebytes				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Malwarebytes
McAfee				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/McAfee
McAfee.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/McAfee.com
Microsoft Office				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Microsoft Office
Microsoft Office 15				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Microsoft Office 15
Microsoft SQL Server				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Microsoft SQL Server
Microsoft Update Health Tools				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Microsoft Update Healt
ModifiableWindowsApps				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/ModifiableWindowsApp
MSBuild				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/MSBuild
Npcap				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Npcap
NVIDIA Corporation				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/NVIDIA Corporation



Listing

/LogicalFileSet1/Program Files (x86)

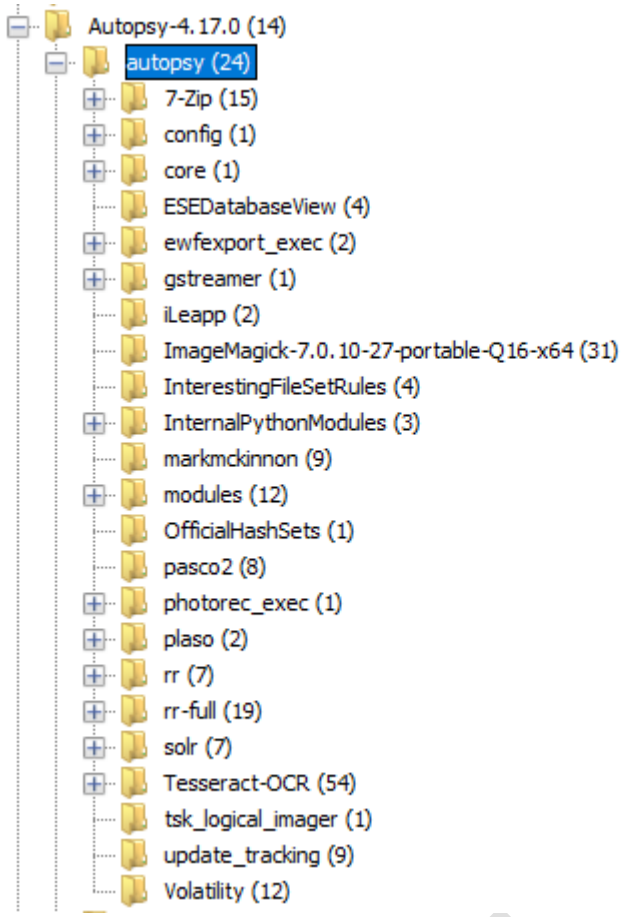
50 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ASUS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/ASUS
ASUSTeK COMPUTER INC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/ASUSTeK
Audacity				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Audacity
Battle.net				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Battle.net
Common Files				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Common F
dotnet				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/dotnet
EasyAntiCheat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/EasyAntiC
Electronic Arts				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Electronic
Epic Games				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Epic Game
GOG Galaxy				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/GOG Gala
Google				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Google
InstallShield Installation Information				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/InstallShie
Internet Explorer				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Internet E
LightingService				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/LightingSe
McAfee				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/McAfee
Microsoft				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft GameInput				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft SDKs				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft Speech SDK 5.1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft SQL Server				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft Threat Modeling Tool 2016				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft
Microsoft Visual Studio				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft

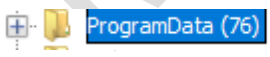
Step 3. Choose a program at random and investigate the contents of the programs directory, this is where you will find more information about the programs configurations, modules and more.



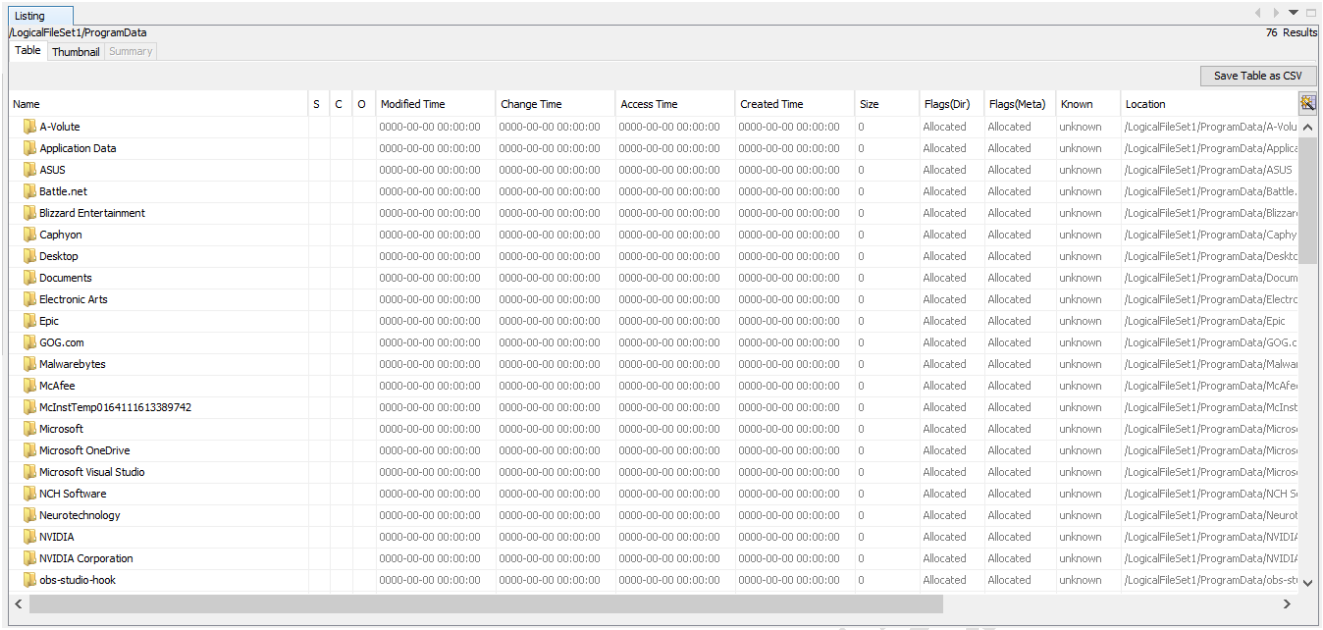
Note: *Investigating these program directories can be quite time consuming.*

ProgramData

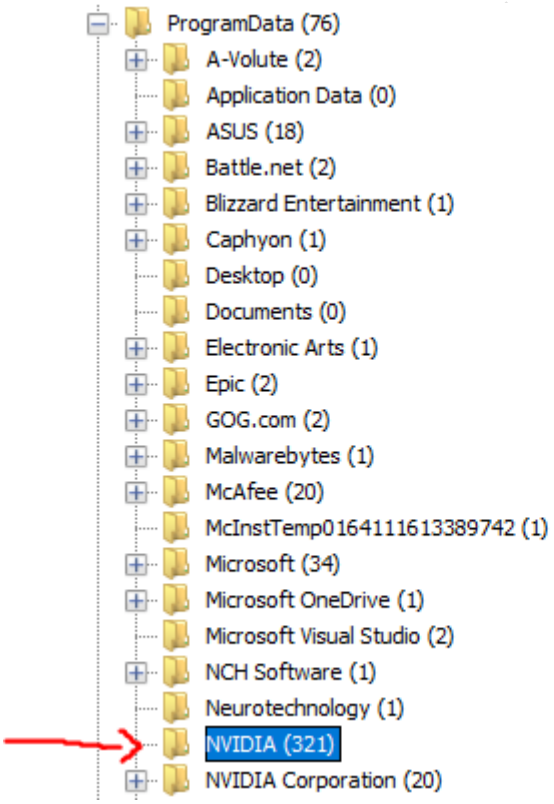
Step 1. Notice the next directory ProgramData, this will contain data from programs, this data can be stored in several places depending on the specifications of the program.



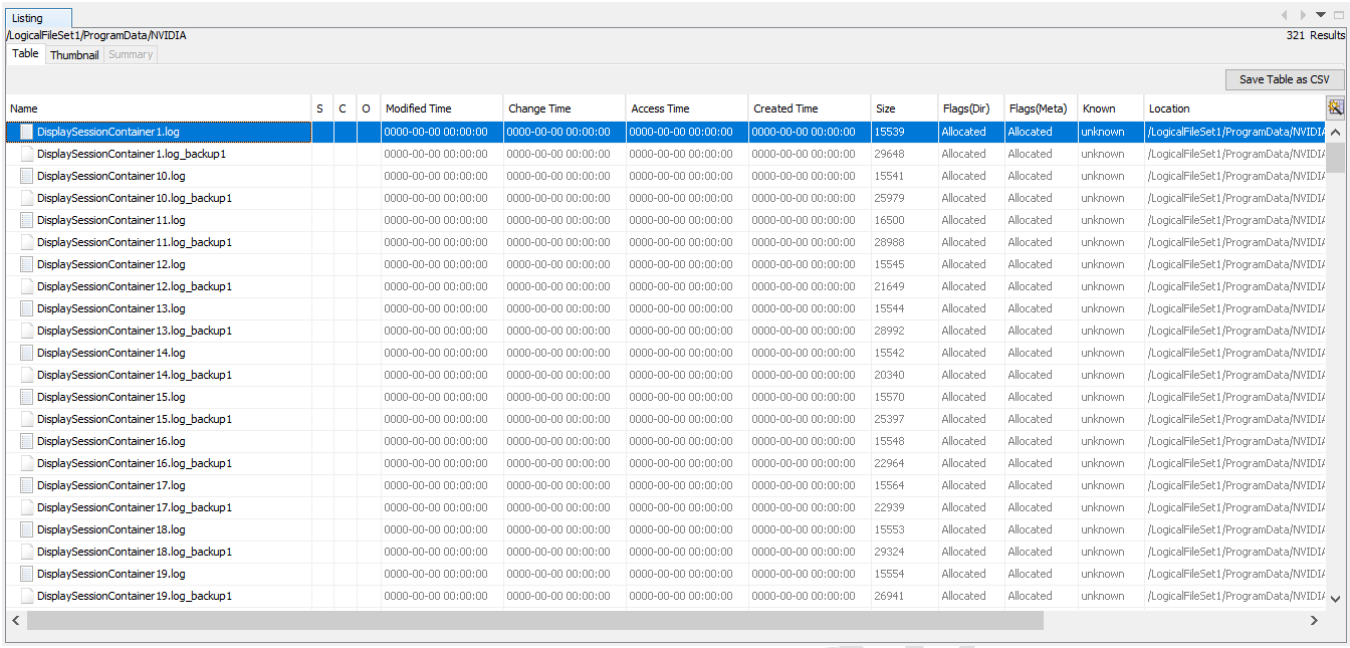
Step 2. Investigate the contents of the ProgramData directory



Step 3. Once again choose a directory at random and investigate its contents. Each will contain different data. In this case the directory being examined is the NVIDIA directory.



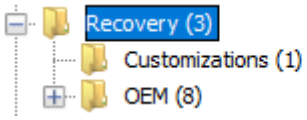
Step 4. This directory contains log data, as well as backups for those logs. These logs keep track of NVIDIA related actions.



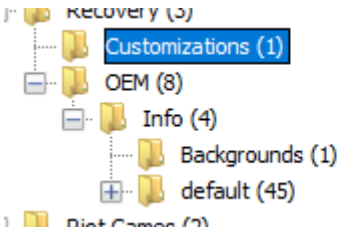
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
DisplaySessionContainer 1.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15539	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 1.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29648	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 10.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15541	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 10.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25979	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 11.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16500	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 11.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	28988	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 12.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15545	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 12.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	21649	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 13.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15544	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 13.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	28992	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 14.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15542	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 14.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20340	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 15.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15570	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 15.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25397	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 16.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15548	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 16.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22964	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 17.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15564	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 17.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	22939	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 18.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15553	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 18.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29324	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 19.log				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15554	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA
DisplaySessionContainer 19.log_backup1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26941	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA

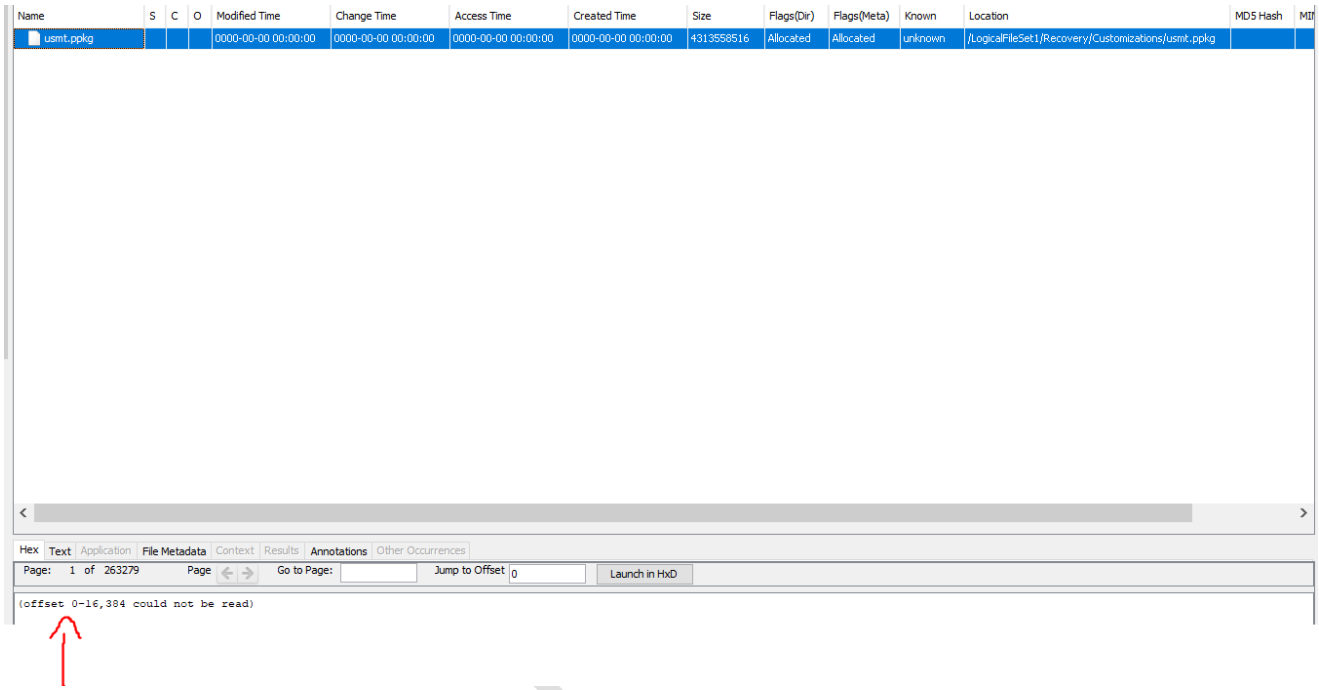
Recovery

Step 1. Notice the next directory “recovery” this directory contains recovery information for your laptop.

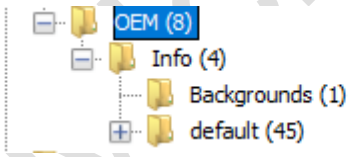


Step 2. Investigate the contents of the customization subdirectory, this information will and should not be read by autopsy.

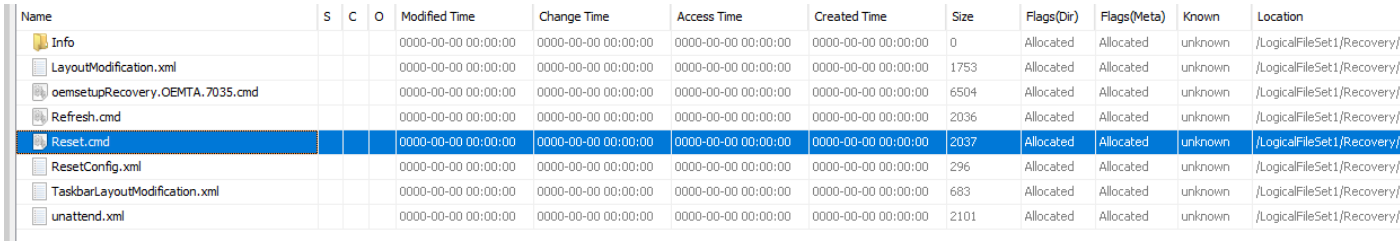




Step 3. Investigate the contents of the OEM(original equipment manager) subdirectory.

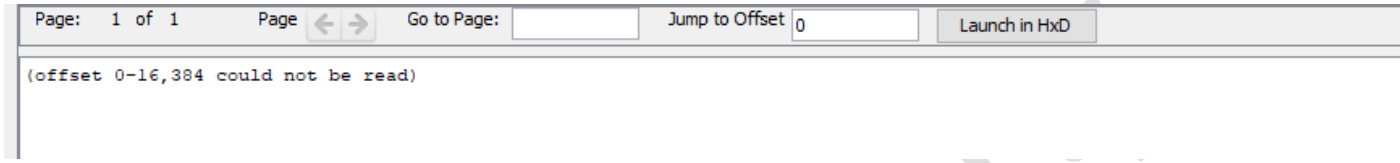


Step 4. Notice the high amount of recovery files.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
LayoutModification.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1753	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
oemsetupRecovery.OEMTA.7035.cmd				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6504	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
Refresh.cmd				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2036	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
Reset.cmd				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2037	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
ResetConfig.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	296	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
TaskbarLayoutModification.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	683	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/
unattend.xml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2101	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/

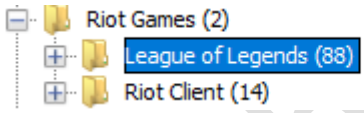
Step 5. Notice that these files will also be unreadable.



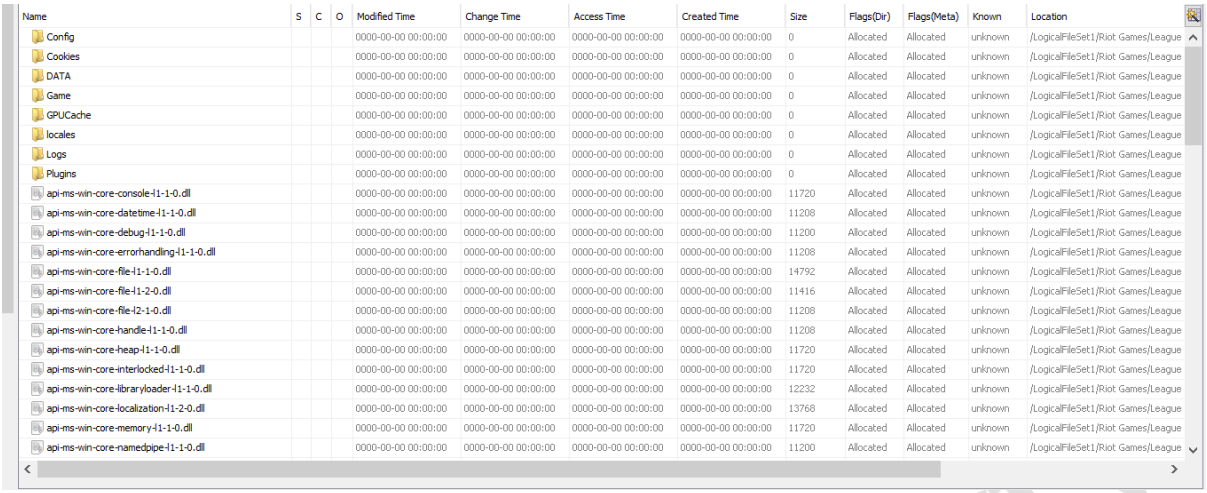
Riot Games

Step 1. Notice the next subdirectory, a familiar sounding directory “Riot Games” for all you league of legend gamers.

Step 2. Investigate the contents of the riot games directory.



Step 3. Notice the two subdirectories, these directories will contain cookies, logs, plugins and more.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Config				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
Cookies				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
DATA				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
Game				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
GPUCache				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
locales				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
Logs				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
Plugins				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-console-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11720	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-datetime-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11208	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-debug-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11200	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-errorhandling-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11208	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-file-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14792	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-file-l1-2-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11416	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-file-l2-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11208	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-handle-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11208	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-heap-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11720	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-interlocked-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11720	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-libraryloader-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12232	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-localization-l1-2-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13768	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-memory-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11720	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League
api-ms-win-core-namedpipe-l1-1-0.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11200	Allocated	Allocated	unknown	/LogicalFileSet1/Riot Games/League

System Volume Information

Step 1. Notice the next directory, system volume information, this data is used during a system restore.

Note: *Expect this directory to be empty unless the laptop has had a system restore performed.*

Temp

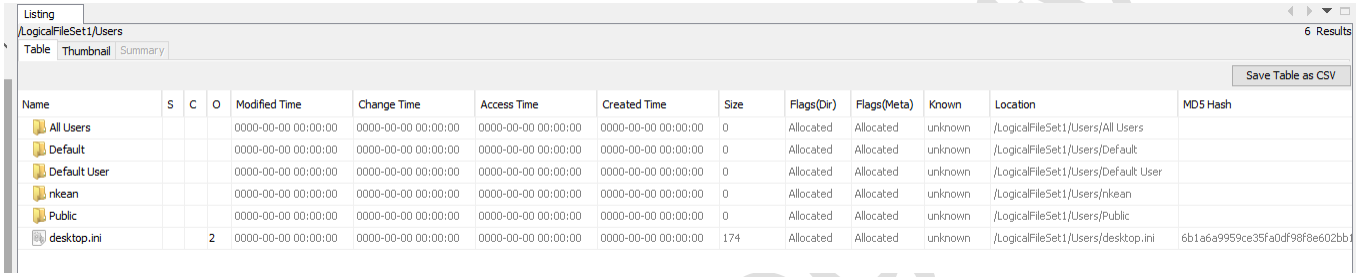
Step 1. Notice the next directory, temp, this folder contains temporary files.

Note: *As the laptop owner you want this directory empty, although during an investigation a person might try being clever by hiding files in this directory.*

Users

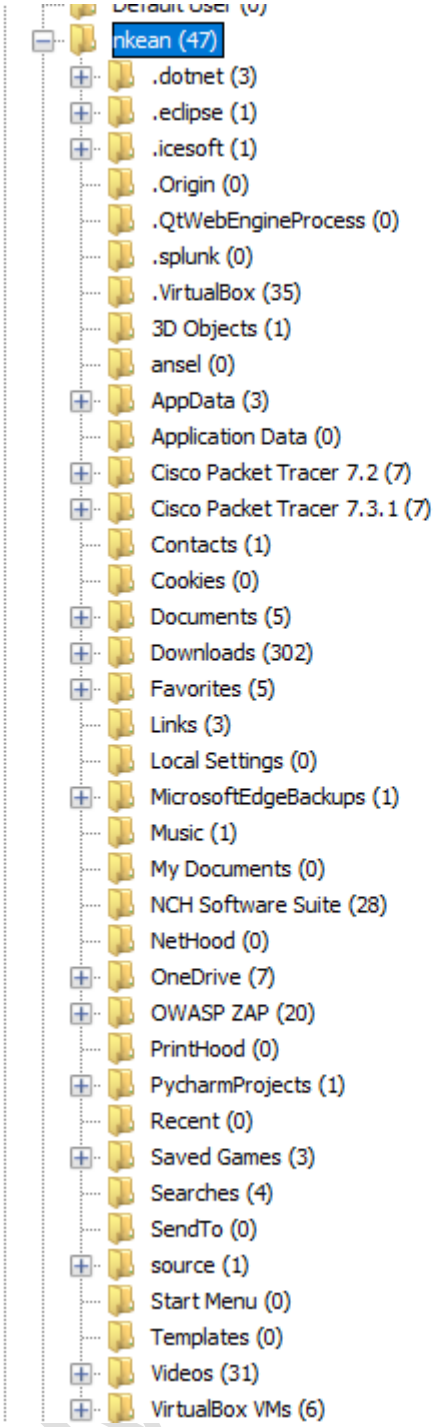
Step 1. The next directory is users, this directory contains all the users on the laptop, or the device being examined.

Step 2. Examine the contents of the Users directory.

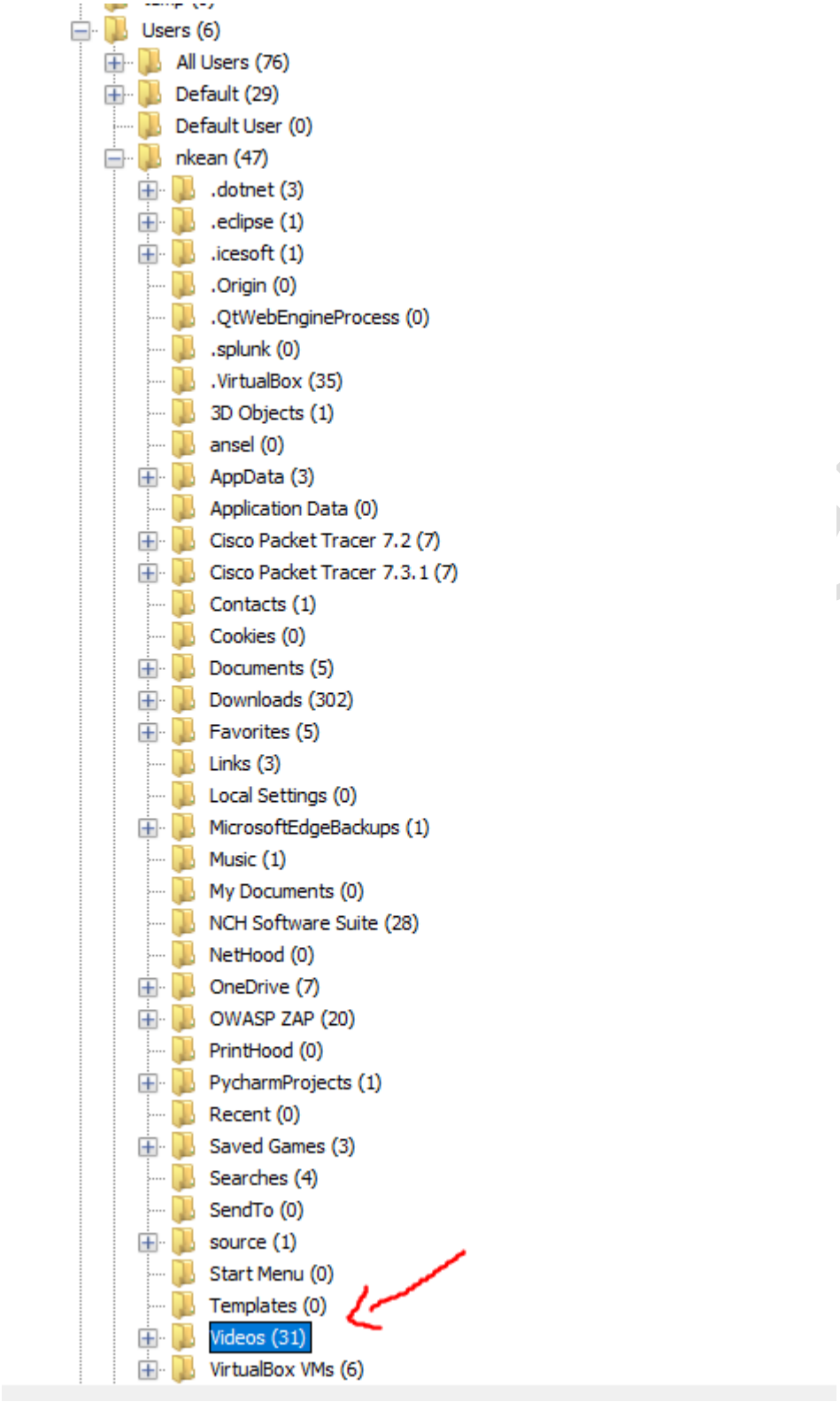


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
All Users				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Users/All Users	
Default				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Users/Default	
Default User				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Users/Default User	
nkean				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean	
Public				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/Users/Public	
desktop.ini			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	174	Allocated	Allocated	unknown	/LogicalFileSet1/Users/desktop.ini	6b1a6a9959ce35fa0df98f8e602bb1

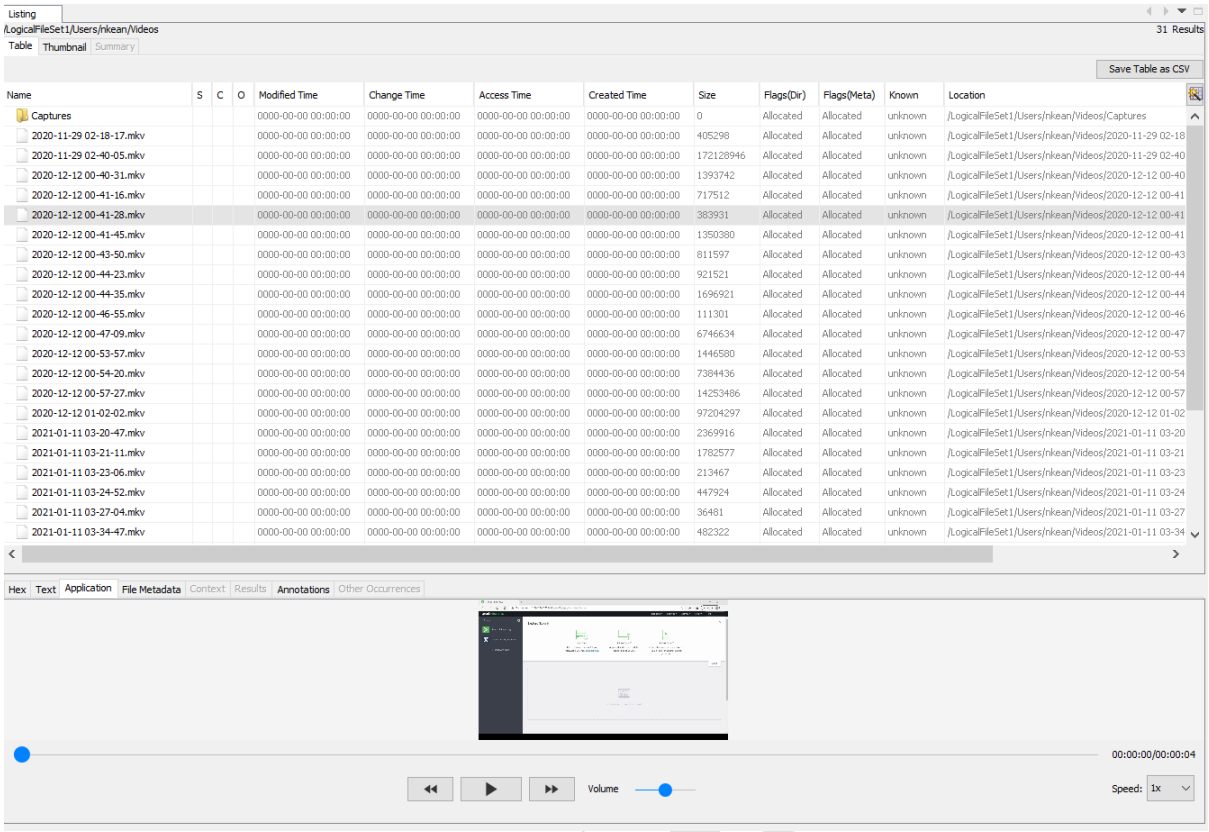
Step 3. Choose a user and investigate the contents.



Step 4. Notice the overall directories of the user you have selected; this will contain data found on the user. A good example is found in the videos.



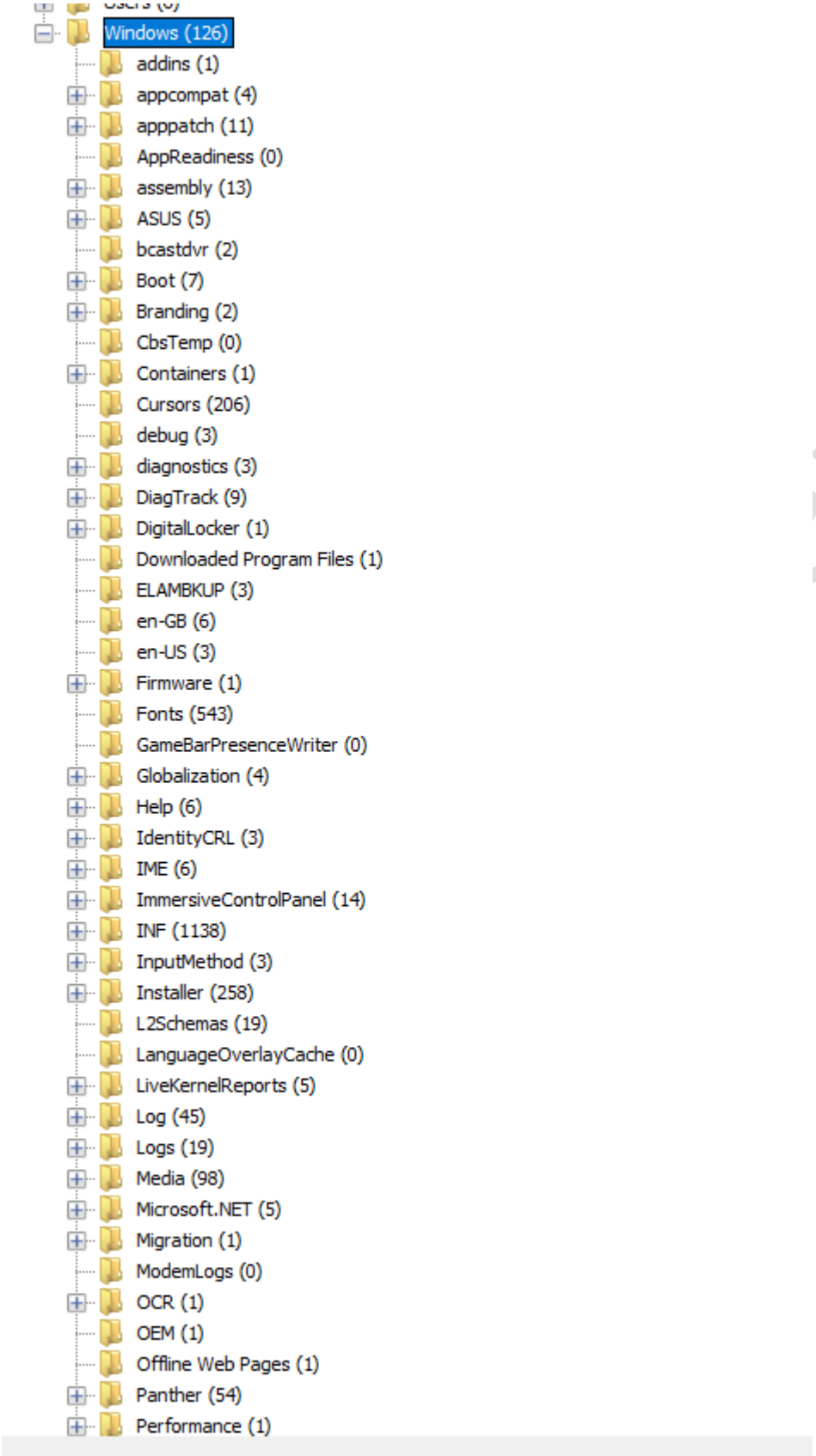
Step 5. Investigate the contents of your videos. Videos and pictures can be more incriminating than any form of text. A picture tells a thousand words. This makes this section invaluable



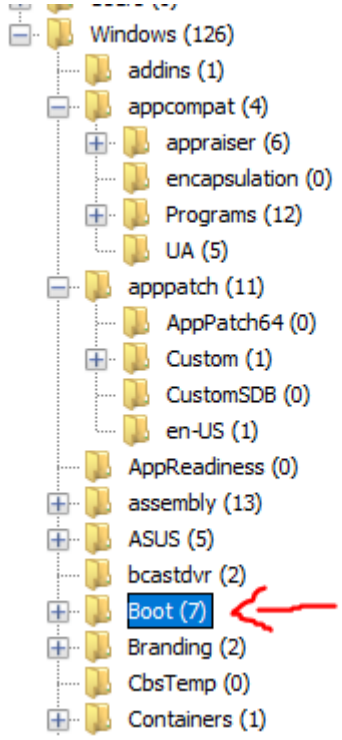
Windows

Step 1. Last of the directories found is the windows subdirectory, this directory contains a lot of interesting data

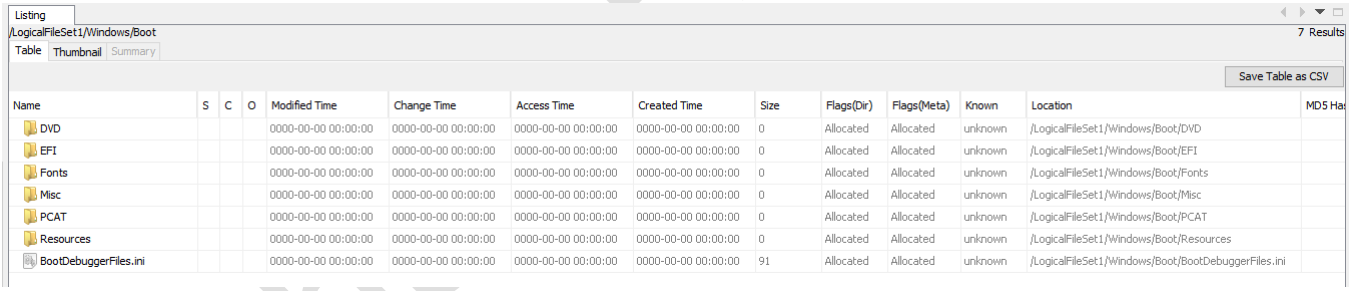
Step 2. Investigate the contents of the directory



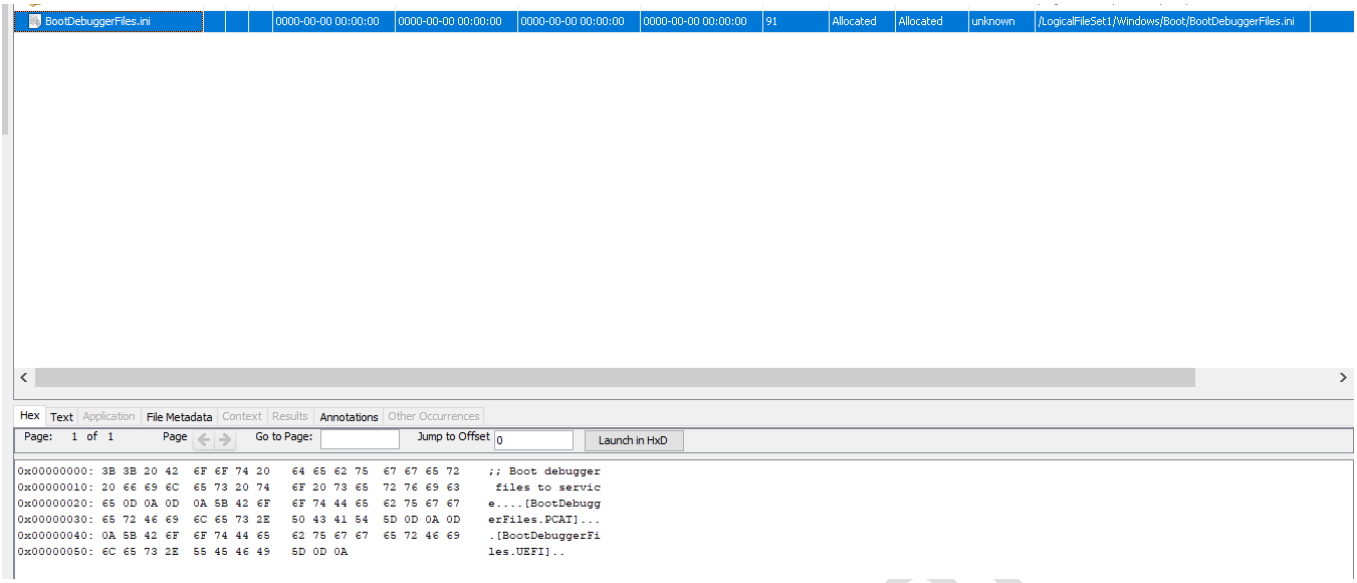
Step 3. Choose a subdirectory at random and investigate its contents. In this case the directory chosen is “boot”



Step 4. Investigate the contents of the chosen directory, in this case boot.



Step 5. Notice that the boot directory contains information relation to the boot, investigate the bootdebuggerfile.



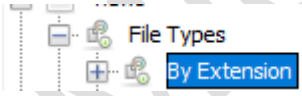
Views – File types

Autopsy also splits files based on the file type it uses.

Step 1. Navigate to views

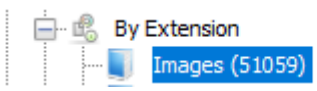
Extension

Step 1. Navigate to by extension.

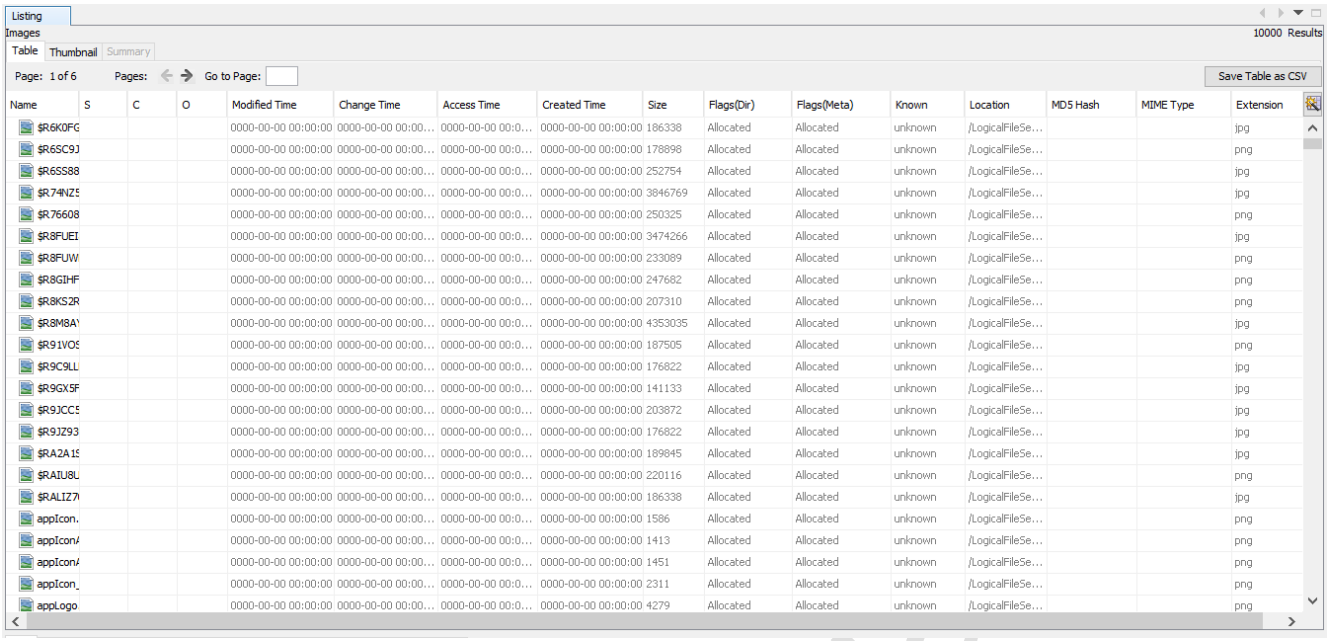


Images

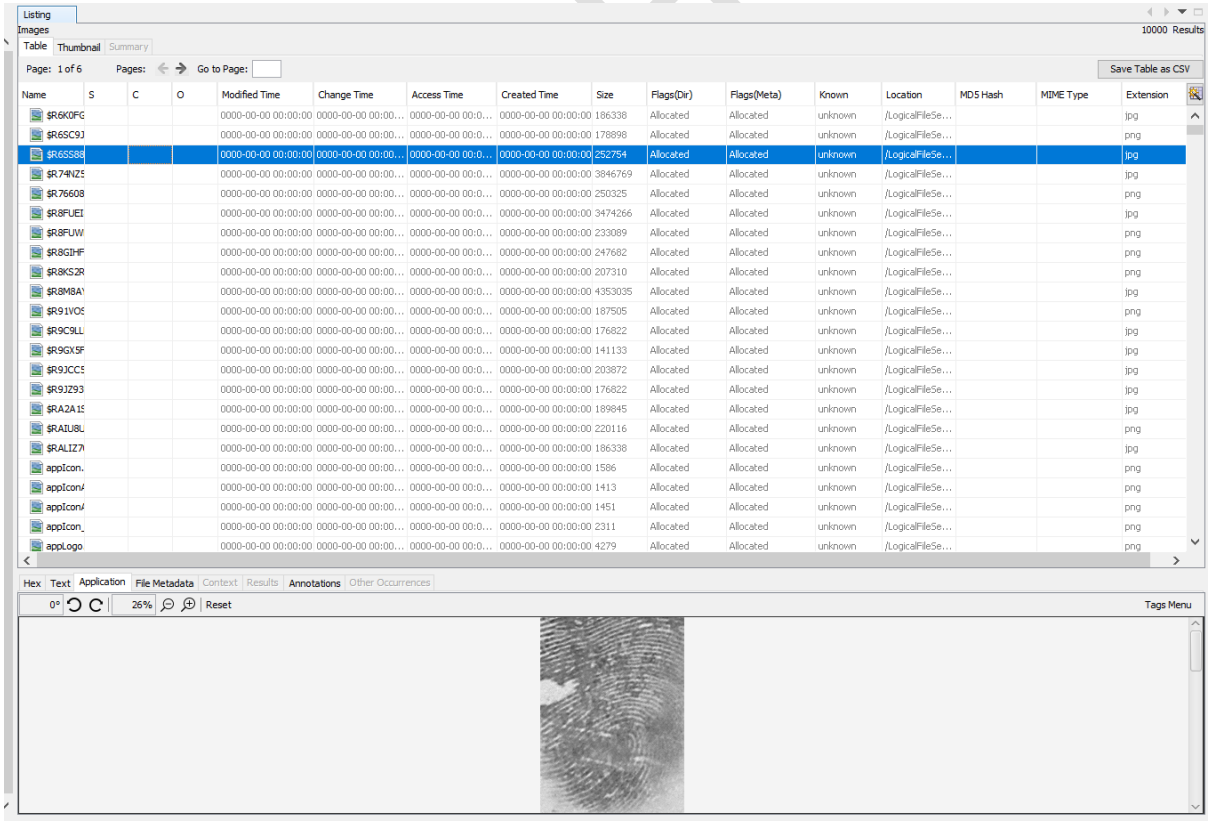
Step 1. Navigate to images



Step 2. Investigate the images found



Step 3. Choose an image at random and see what happens. The image chosen is a biometric fingerprint.

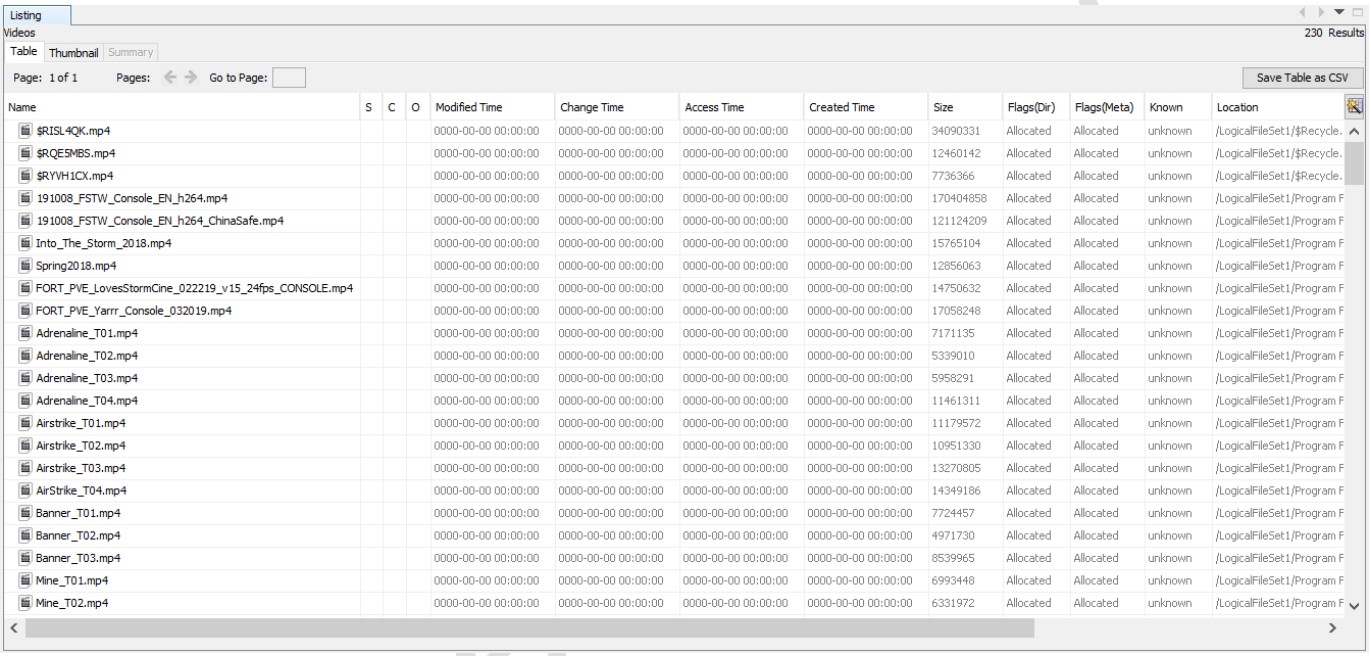


Q. Did the image you chose load?

Video

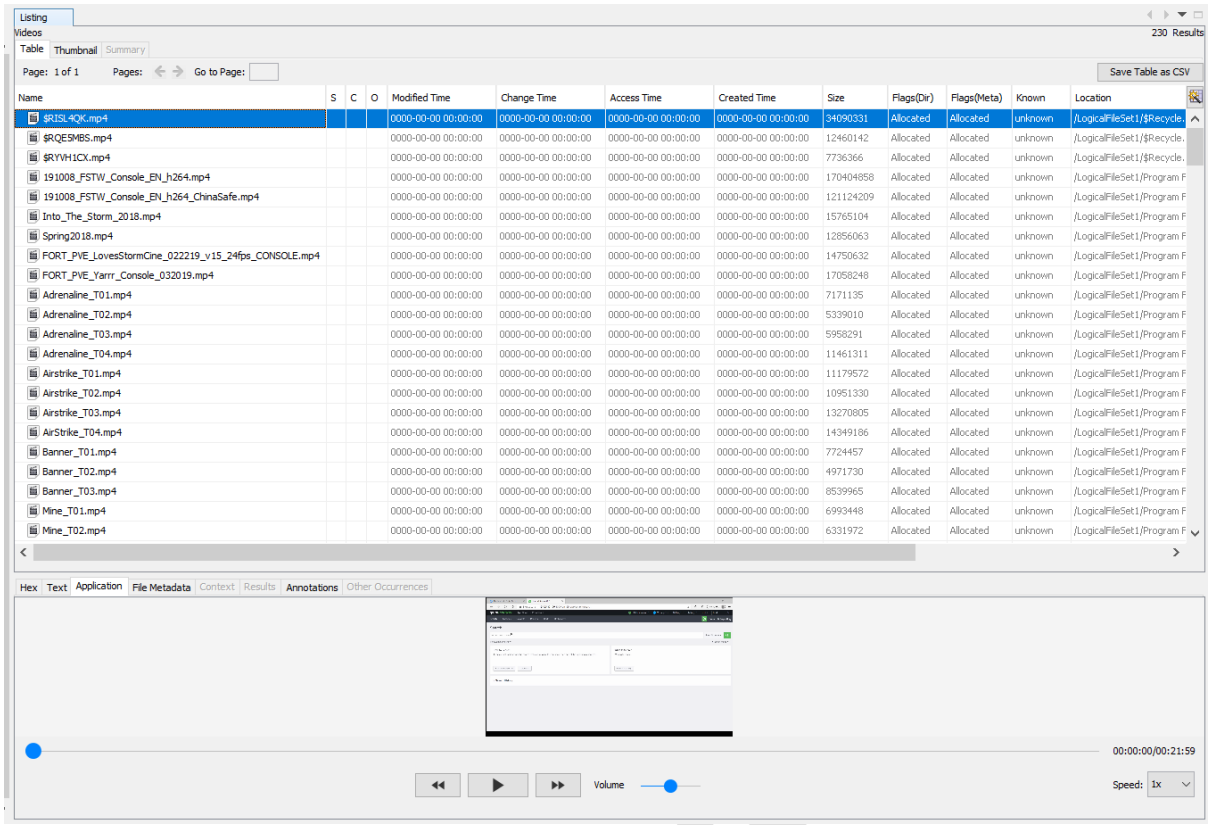
Step 1. Navigate to videos.

Step 2. Investigate the videos found



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
$RISL4QK.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	34090331	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
$RQE5MBS.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12460142	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
$RYVH1CX.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7736366	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
191008_FSTW_Console_EN_h264.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	170404858	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
191008_FSTW_Console_EN_h264_ChinaSafe.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	121124209	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Into_The_Storm_2018.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15765104	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Spring2018.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12856063	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
FORT_PVE_LovesStormCine_022219_v15_24fps_CONSOLE.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14750632	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
FORT_PVE_Yarrr_Console_032019.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17058248	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Adrenaline_T01.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7171135	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Adrenaline_T02.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5339010	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Adrenaline_T03.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5958291	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Adrenaline_T04.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11461311	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Airstrike_T01.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11179572	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Airstrike_T02.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	10951330	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Airstrike_T03.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13270805	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
AirStrike_T04.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14349186	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Banner_T01.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7724457	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Banner_T02.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4971730	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Banner_T03.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8539965	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Mine_T01.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6993448	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
Mine_T02.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6331972	Allocated	Allocated	unknown	/LogicalFileSet1/Program F

Step 3. Choose a video at random.

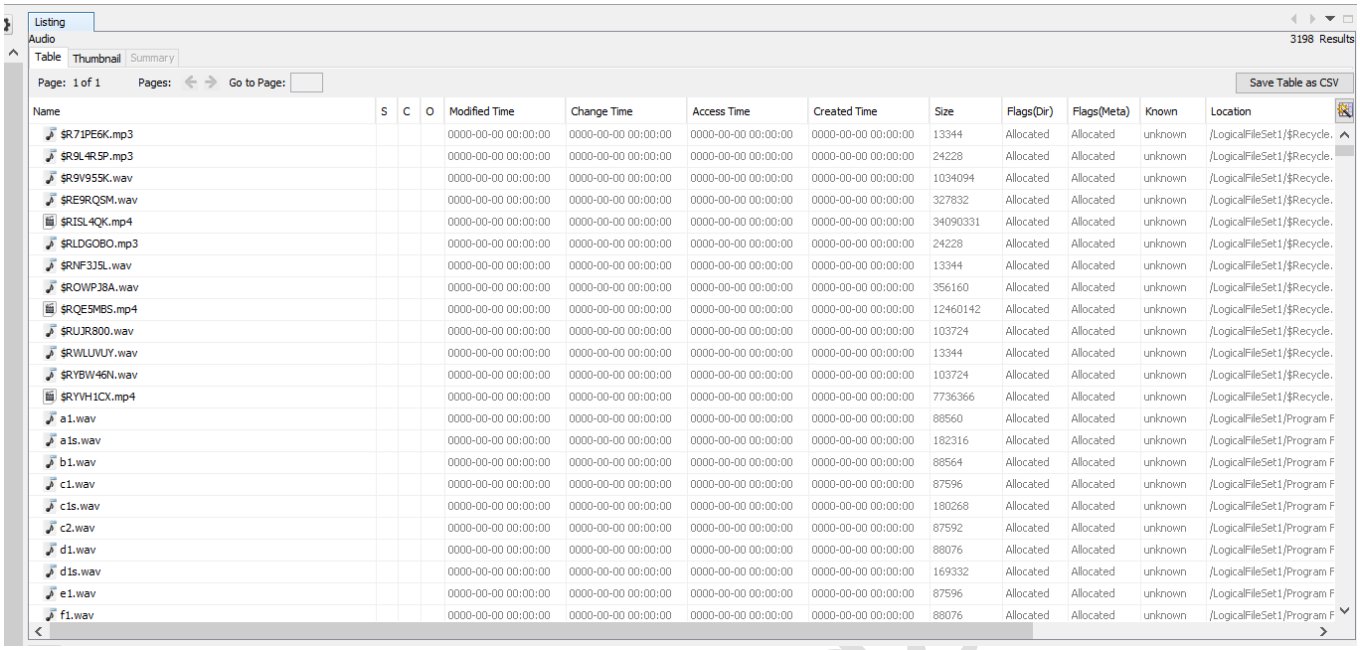


Q. What kind of functionality has the video got?

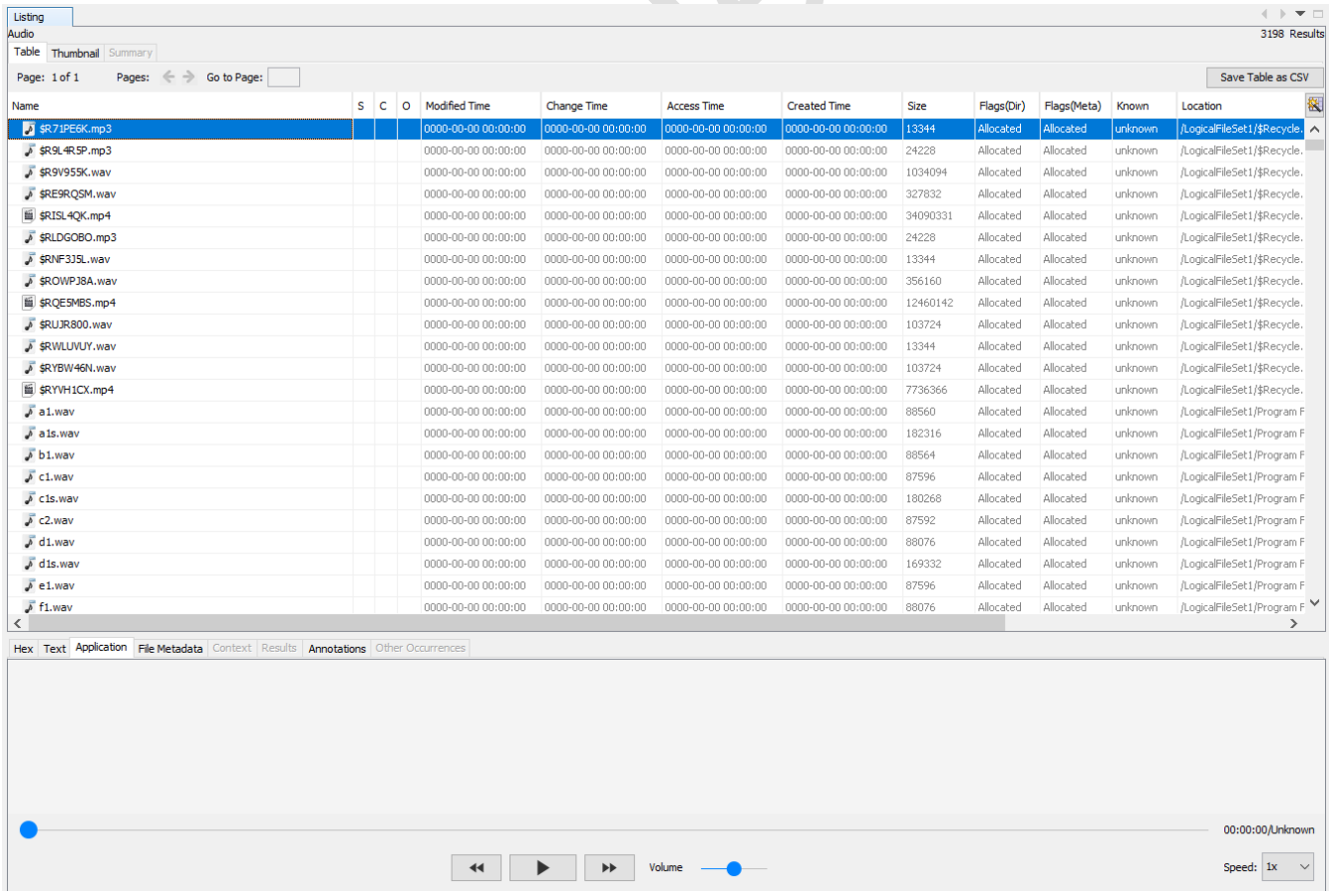
Audio

Step 1. Navigate to Audio

Step 2. Investigate the audio files found.



Step 3. Choose an audio file.

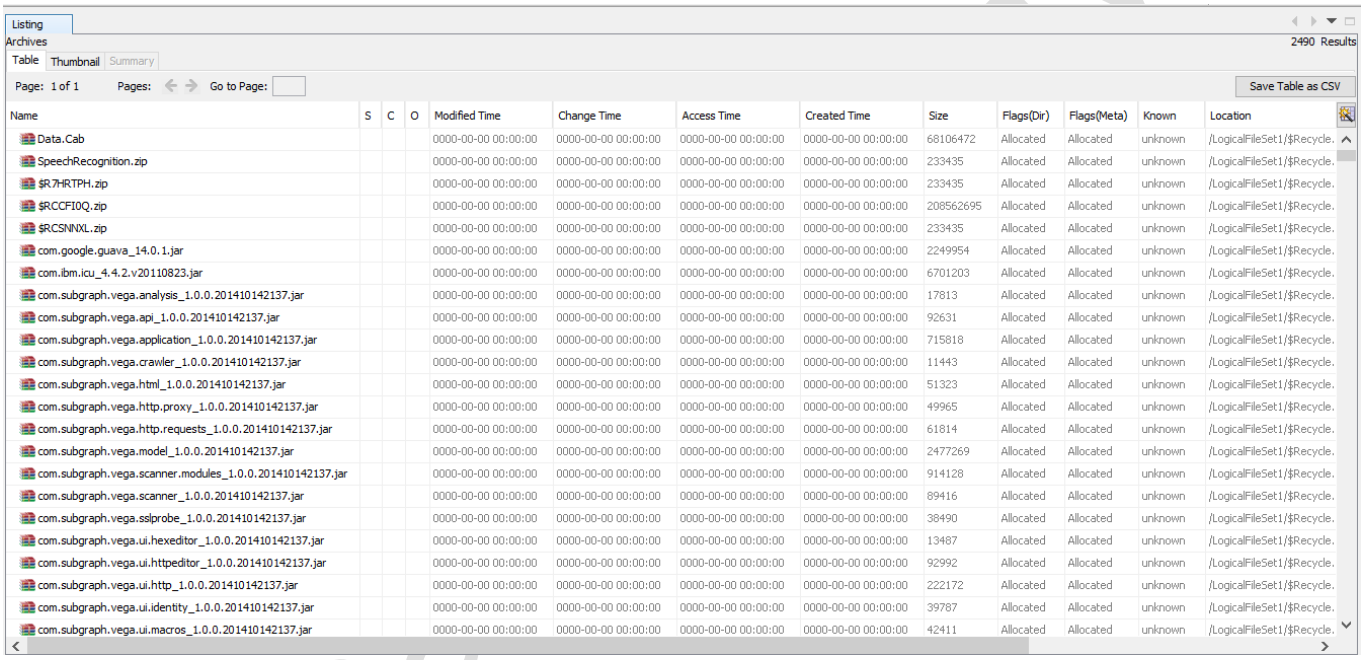


Q. What functionality does the audio file have that the video file may not or vice versa?

Archives

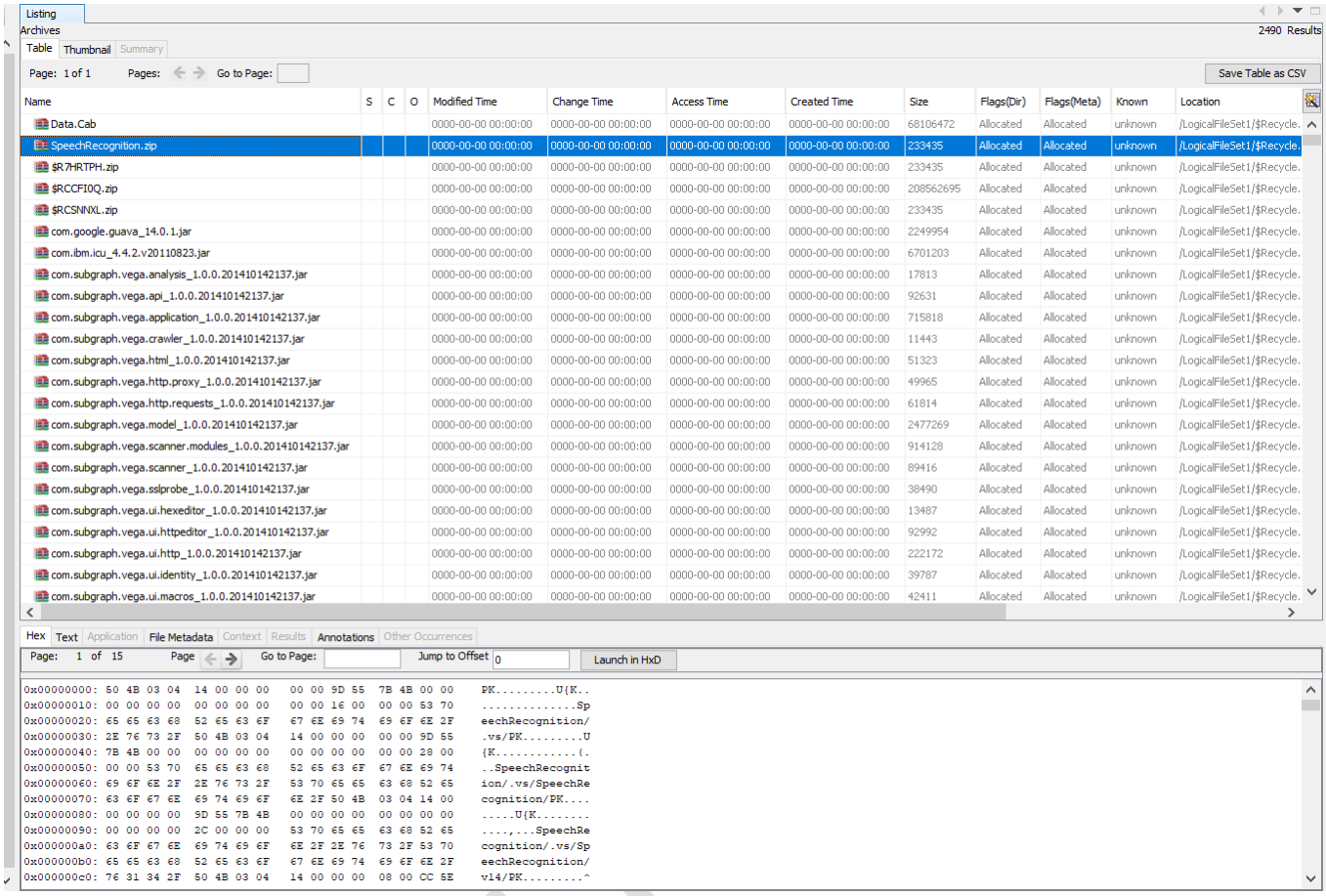
Step 1. Navigate to archives

Step 2. Investigate the archive files



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Data.Cab				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	68106472	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
SpeechRecognition.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	233435	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
$R7HRTPH.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	233435	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
$RCCFI0Q.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	208562695	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
$RCSNNXL.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	233435	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.google.guava_14.0.1.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2249954	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.ibm.icu_4.4.2.v20110823.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6701203	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.analysis_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17813	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.api_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	92631	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.application_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	715818	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.crawler_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	11443	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.html_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51323	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.http.proxy_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49965	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.http.requests_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61814	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.model_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2477269	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.scanner.modules_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	914128	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.scanner_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	89416	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.sslprobe_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	38490	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.ui.hexeditor_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13487	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.ui.httpeditor_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	92992	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.ui.http_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	222172	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.ui.identity_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	39787	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.
com.subgraph.vega.ui.macros_1.0.0.201410142137.jar				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42411	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.

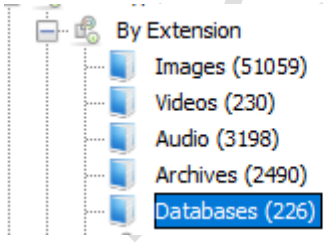
Step 3. Choose an archive file to investigate.



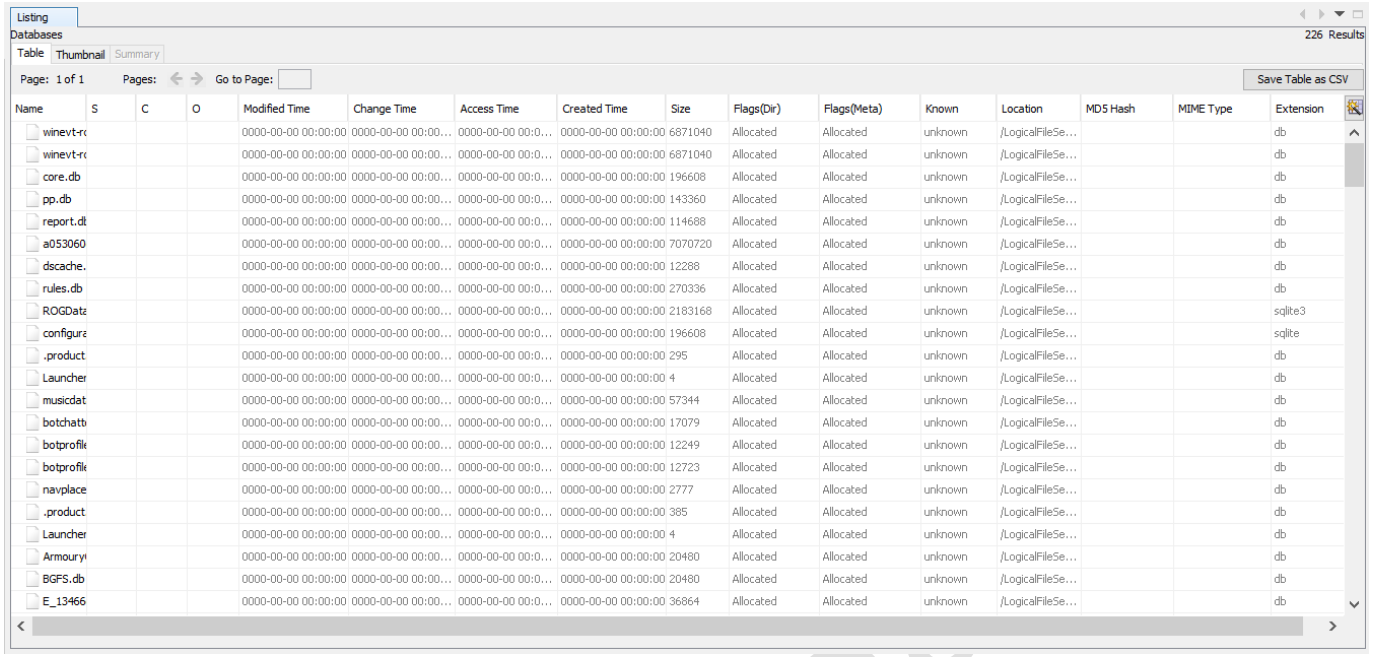
Q. Are archive files of any use to a forensic investigation?

Databases

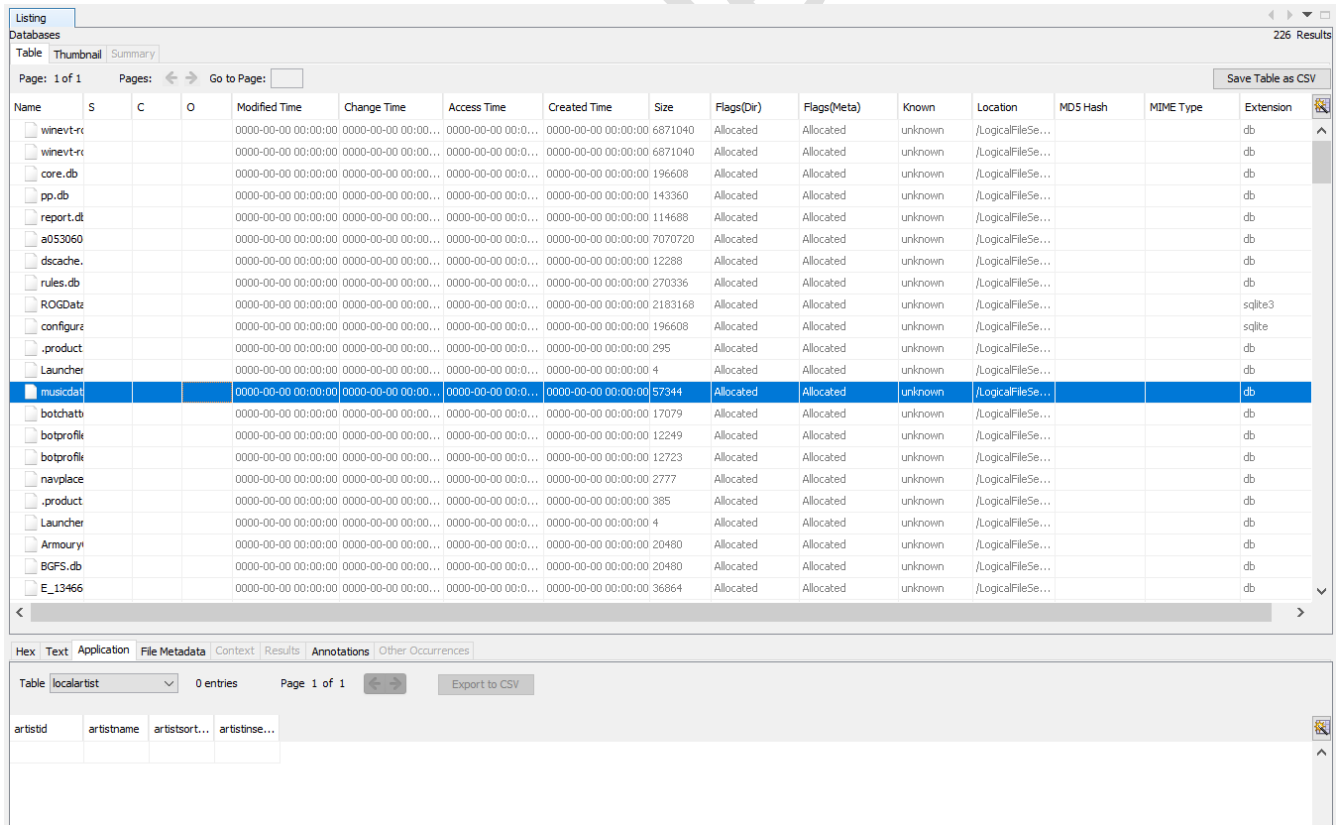
Step 1. Navigate to Databases



Step 2. Investigate the contents of the databases extension



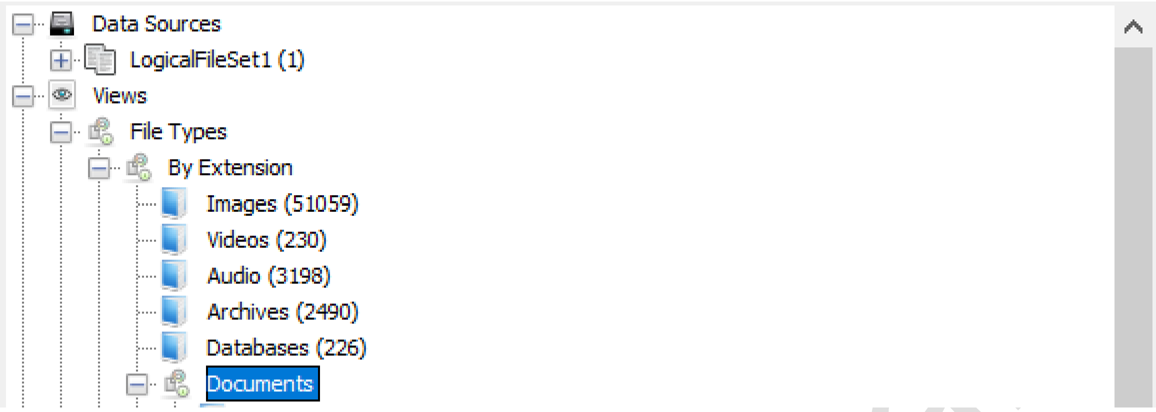
Step 3. Choose a file to investigate.



Q. If the database chosen is updated without re-imaging the logical files, would this file update?

Documents

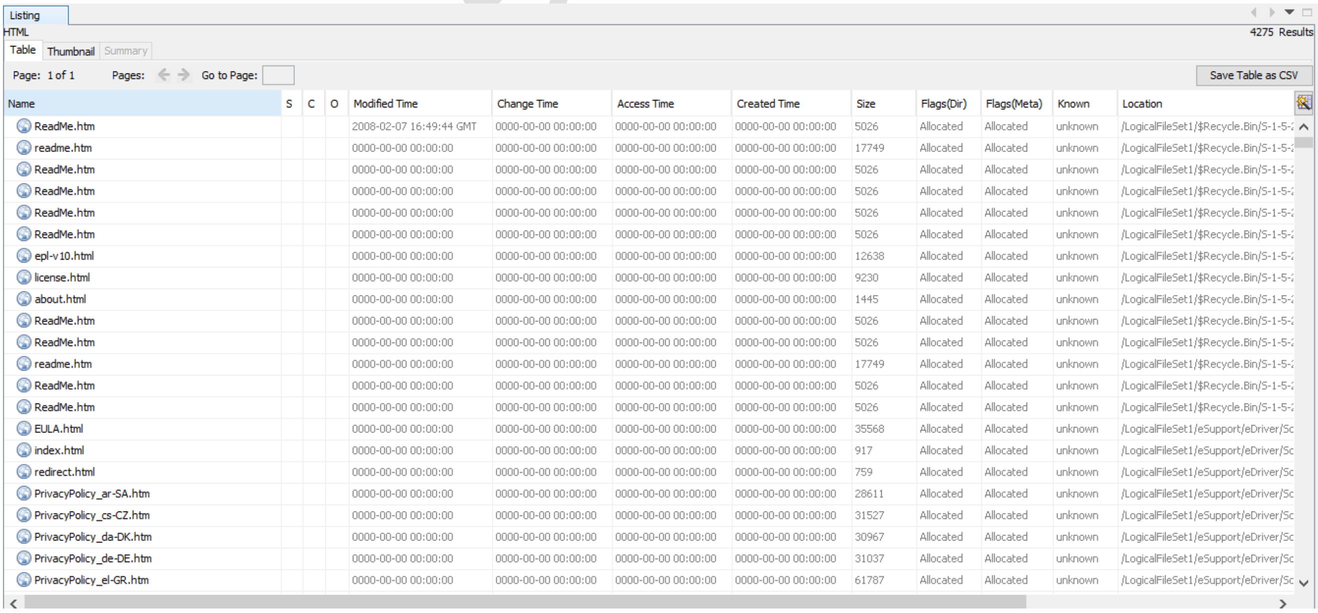
Step 1. Navigate to documents.



HTML

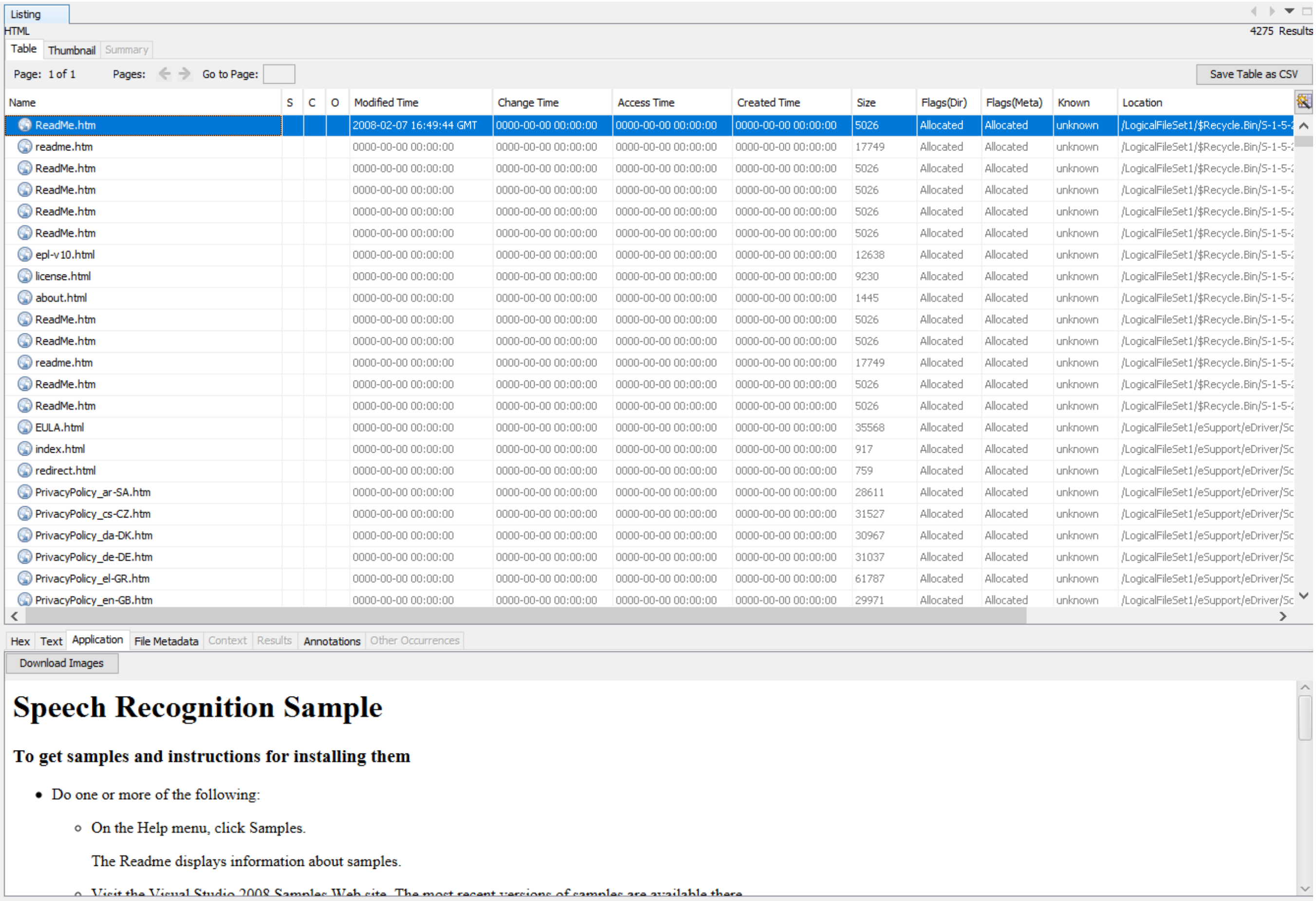
Step 1. Navigate to HTML

Step 2. Investigate the findings of HTML


Listing
HTML
4275 Results
Table Thumbnail Summary
Page: 1 of 1 Pages: Go to Page:
Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ReadMe.htm				2008-02-07 16:49:44 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
readme.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17749	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
epl-v10.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12638	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
license.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9230	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
about.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1445	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
readme.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17749	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
ReadMe.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5026	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-
EULA.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	35568	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
index.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	917	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
redirect.html				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	759	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
PrivacyPolicy_ar-SA.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	28611	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
PrivacyPolicy_cs-CZ.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31527	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
PrivacyPolicy_da-DK.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	30967	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
PrivacyPolicy_de-DE.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31037	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc
PrivacyPolicy_el-GR.htm				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61787	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc

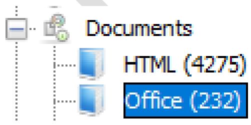
Step 3. Choose a html file to investigate



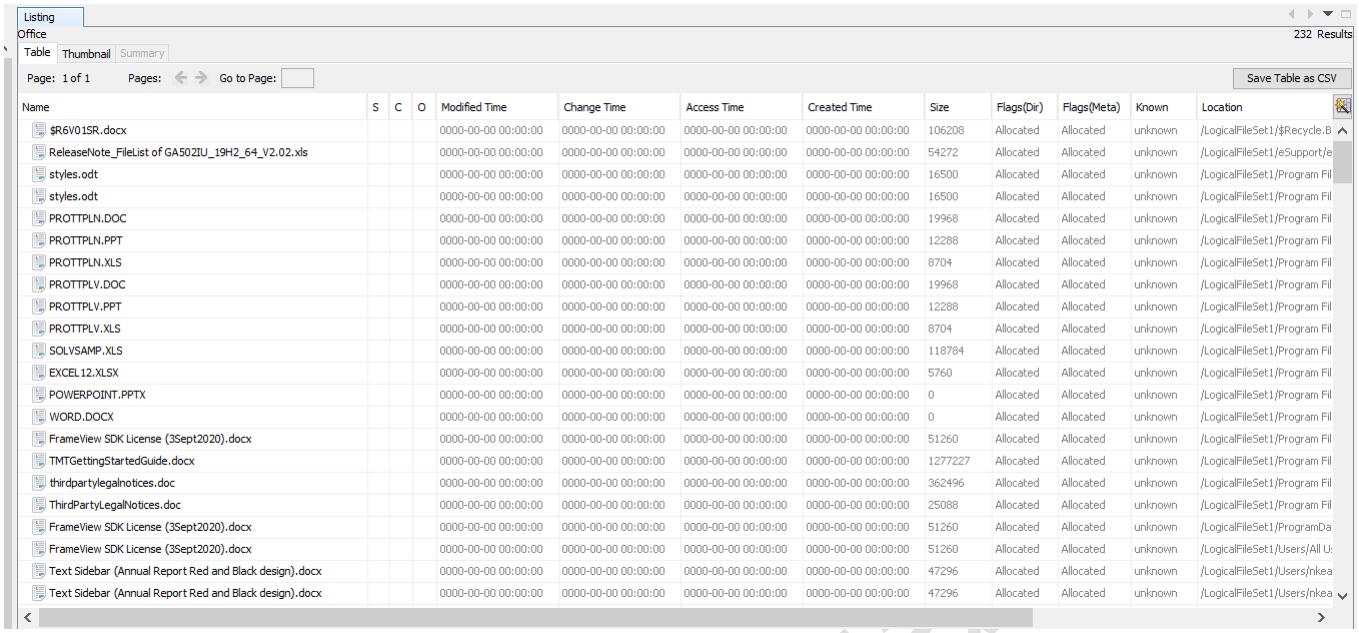
Q. Will all HTML files be readable? If not, why?

Office

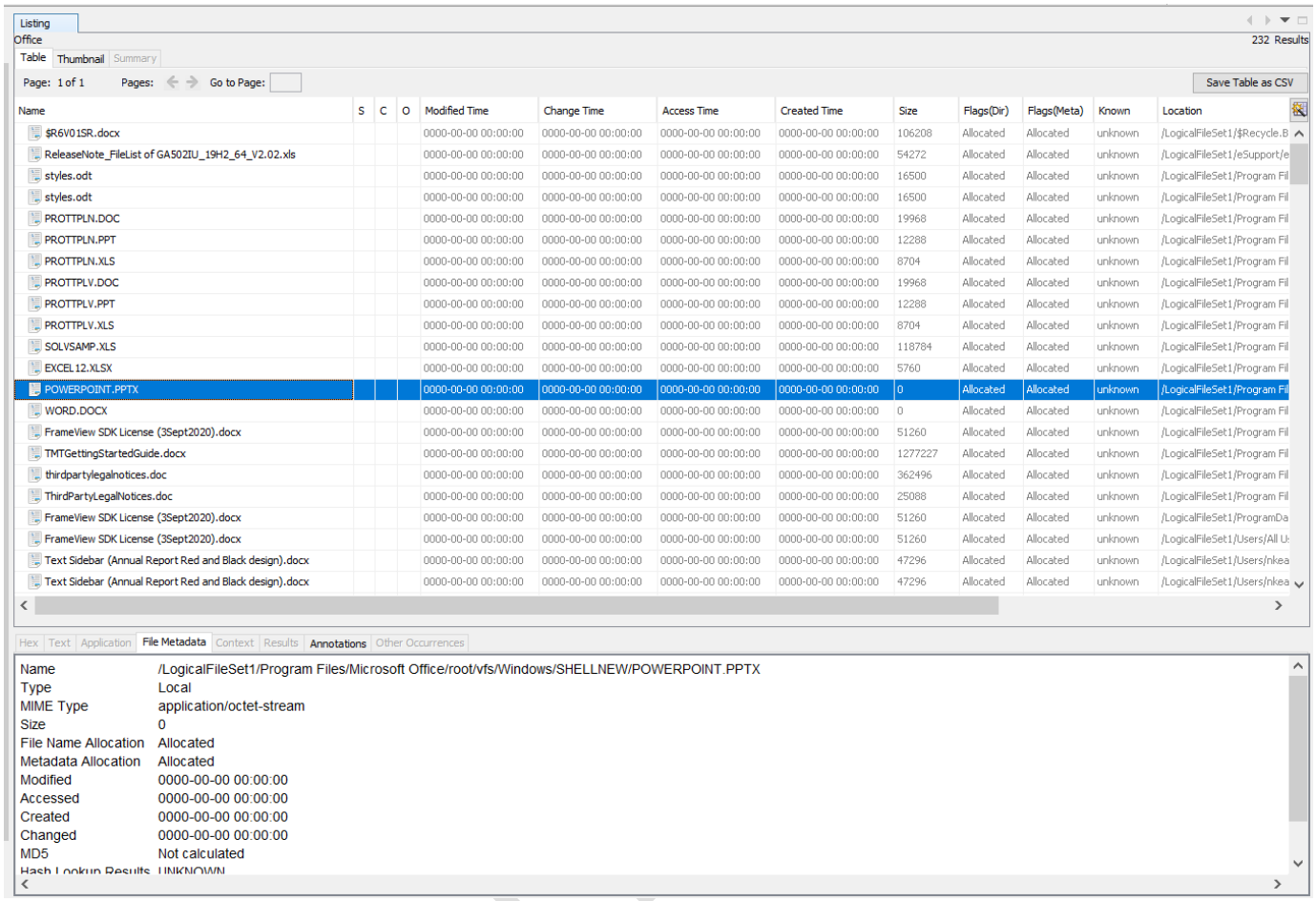
Step 1. Navigate to Office



Step 2. Investigate the contents of Office.



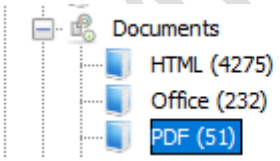
Step 3. Choose a file to investigate



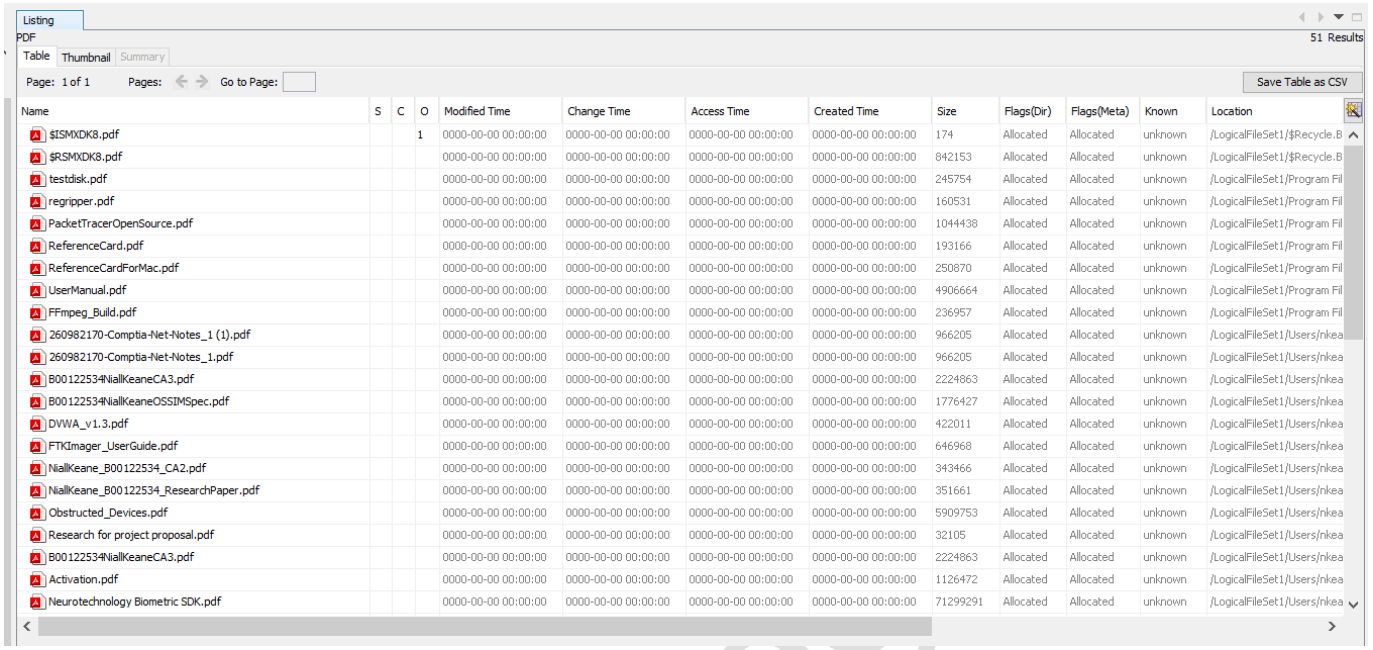
Q. The file chosen for the lab is a PowerPoint, can you determine the other file types?

PDF

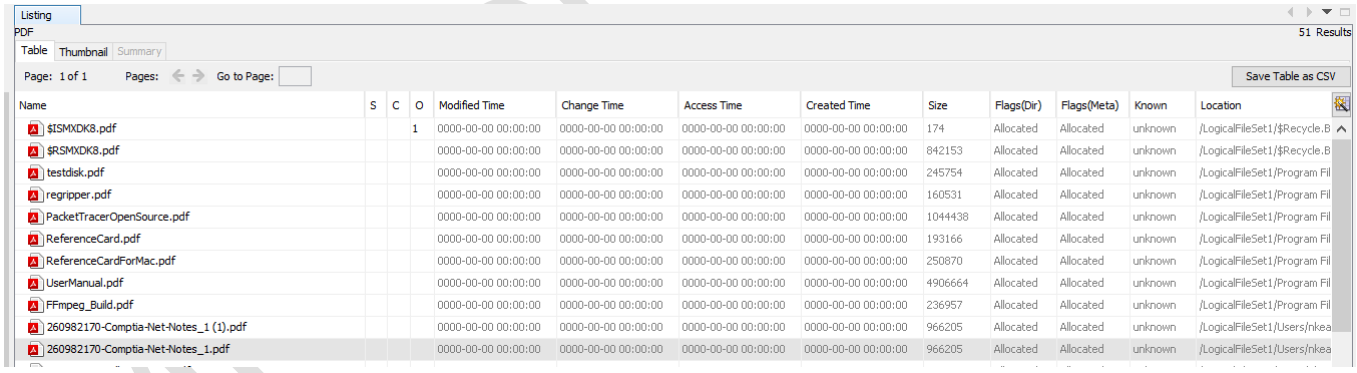
Step 1. Navigate to PDF

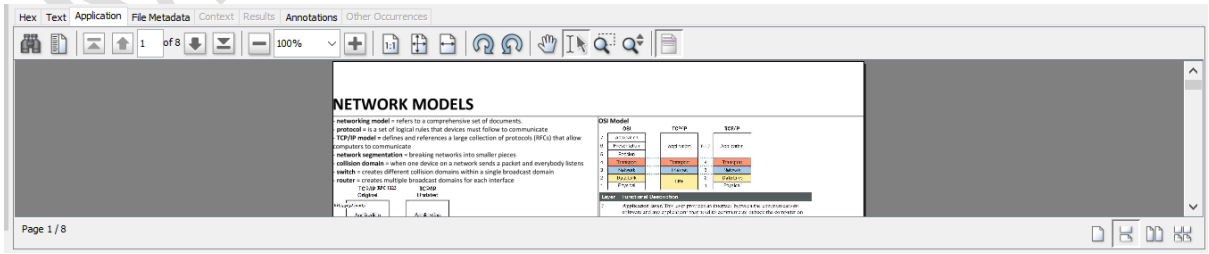


Step 2. Investigate the contents of the pdf documents.



Step 3. Choose a pdf to investigate.

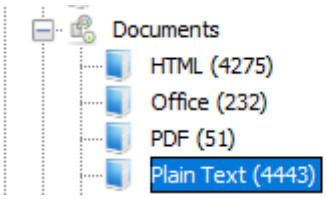




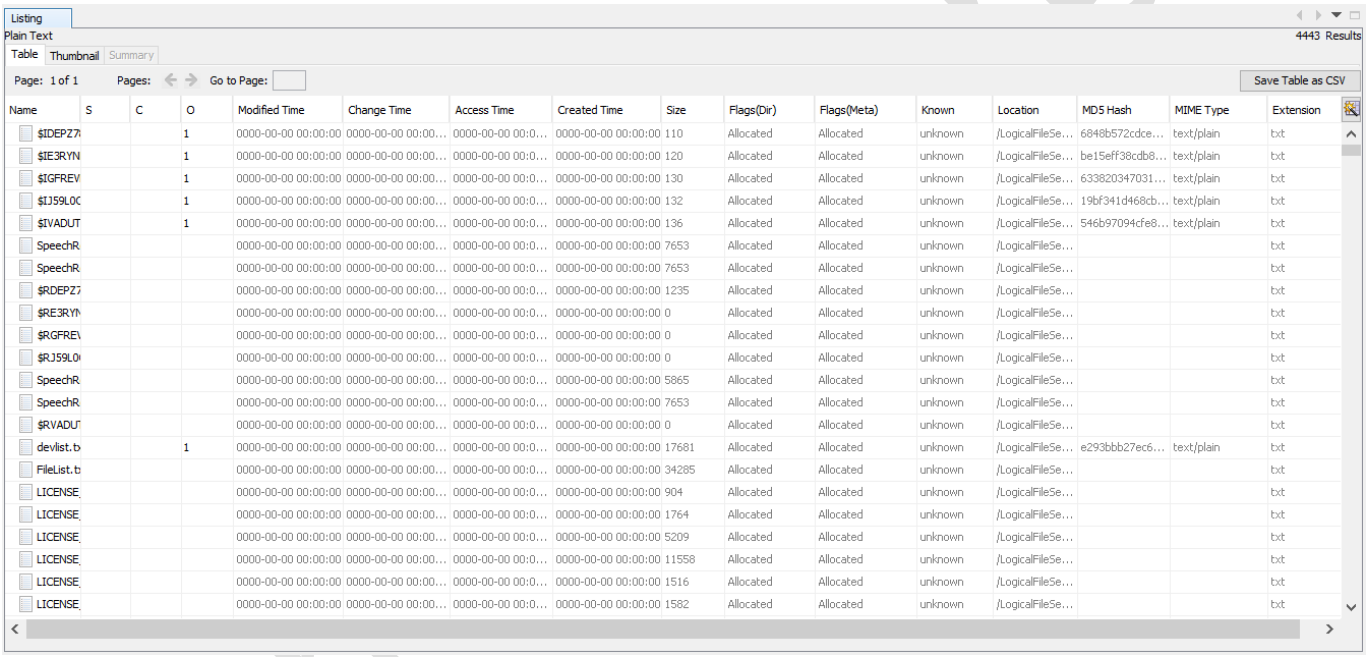
Q. Were all pdfs readable? If not, why?

Plain Text

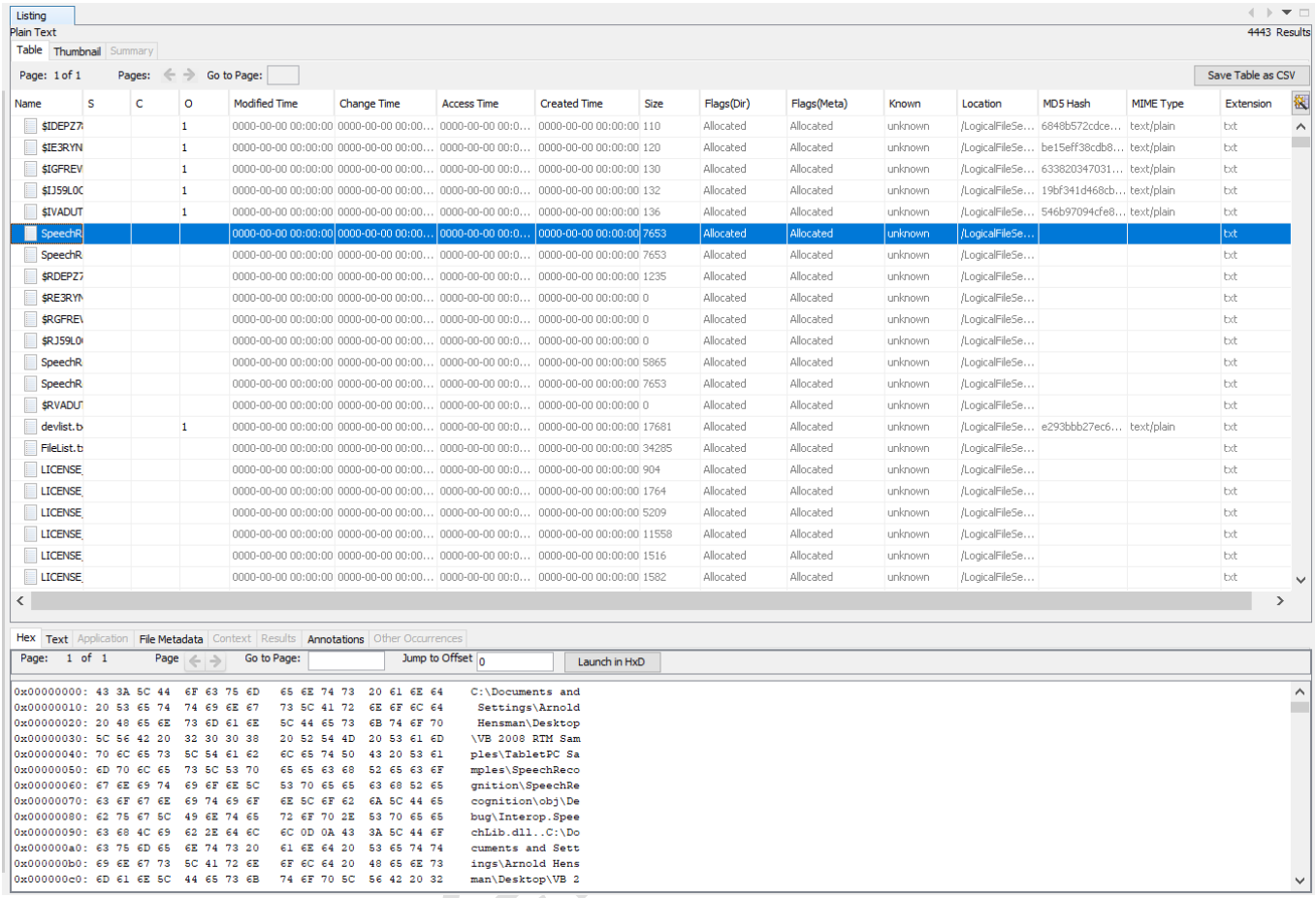
Step 1. Navigate to Plain Text.



Step 2. Investigate the contents of Plain Text



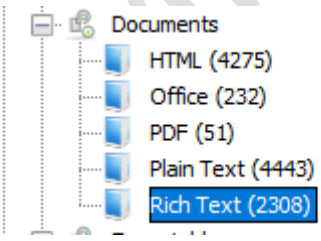
Step 3. Choose a plain text file to investigate.



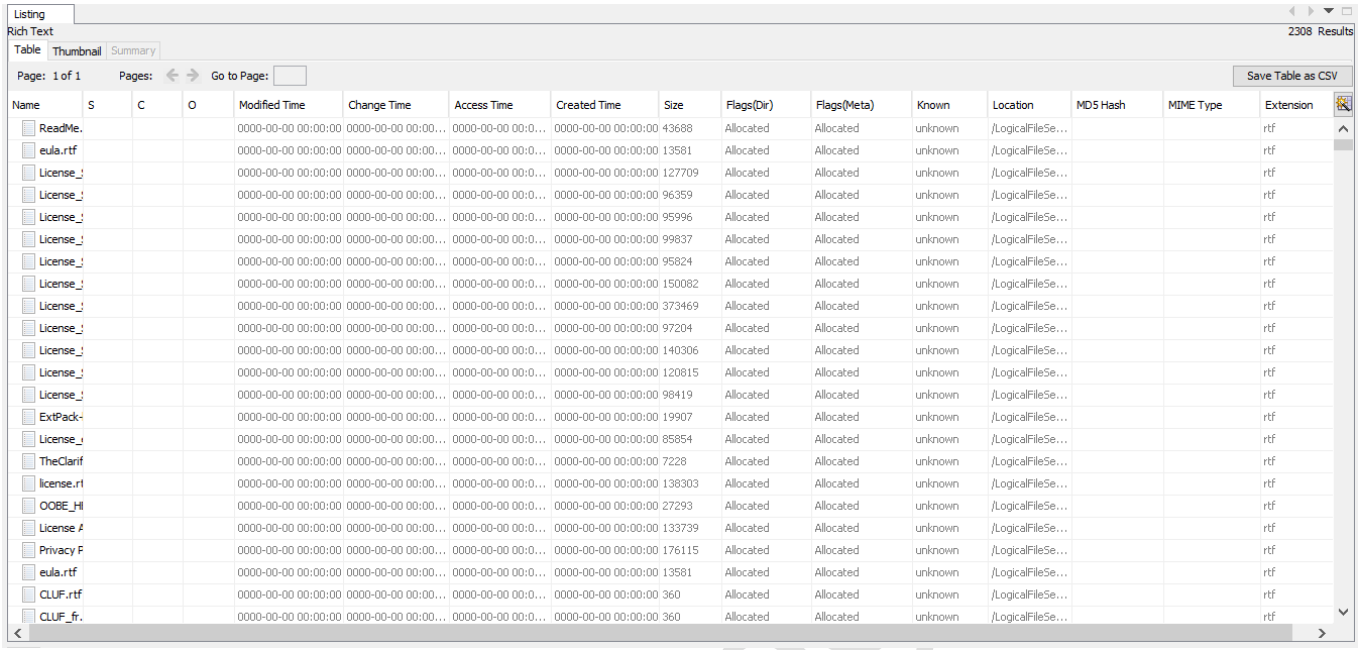
Q. Are all files written in plain text? If not, why?

Rich Text

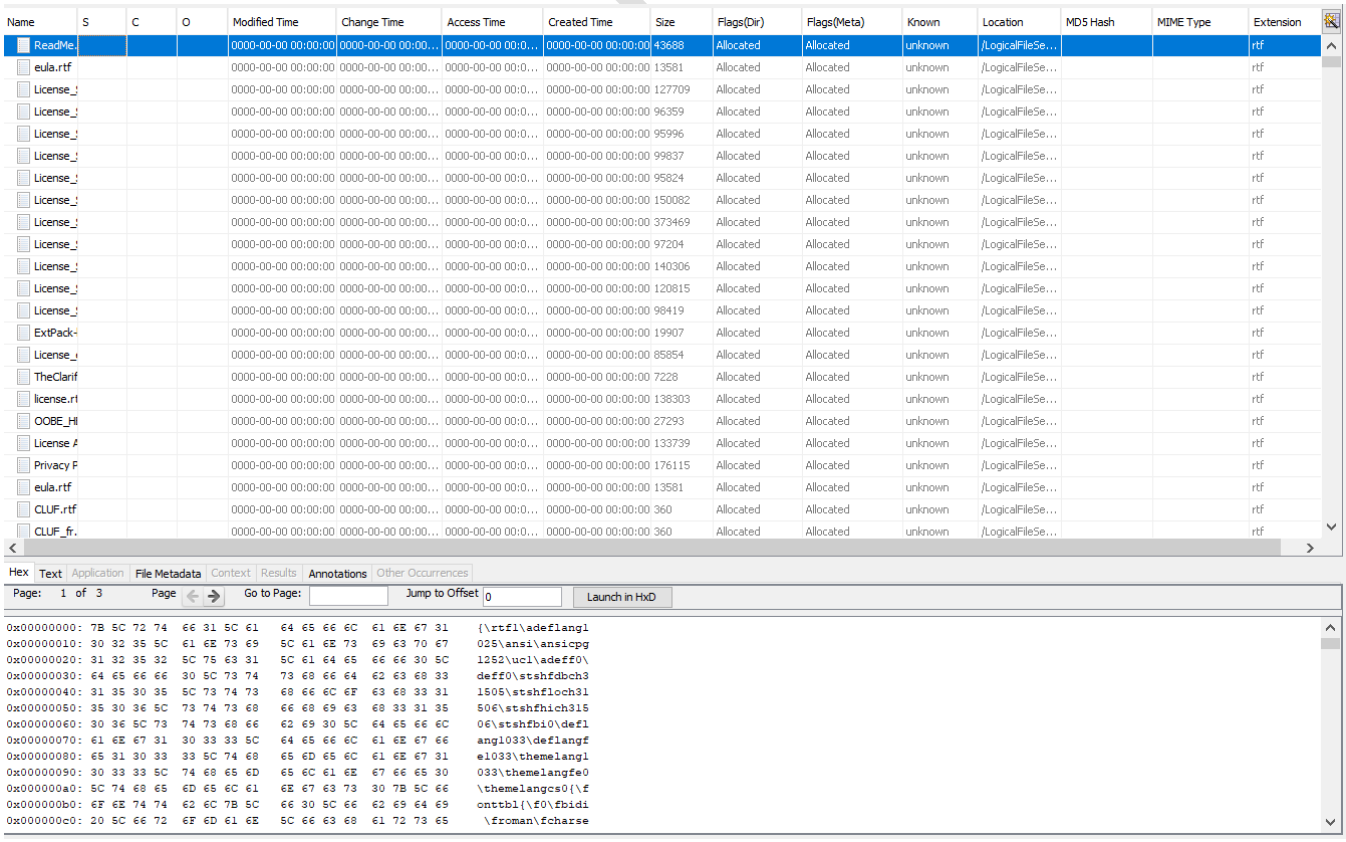
Step 1. Navigate to Rich text



Step 2. Investigate the contents of rich text



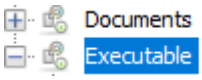
Step 3. Choose a rich text file to investigate.



Q. Why is the file not readable?

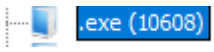
Executable

Step 1. Navigate to executable

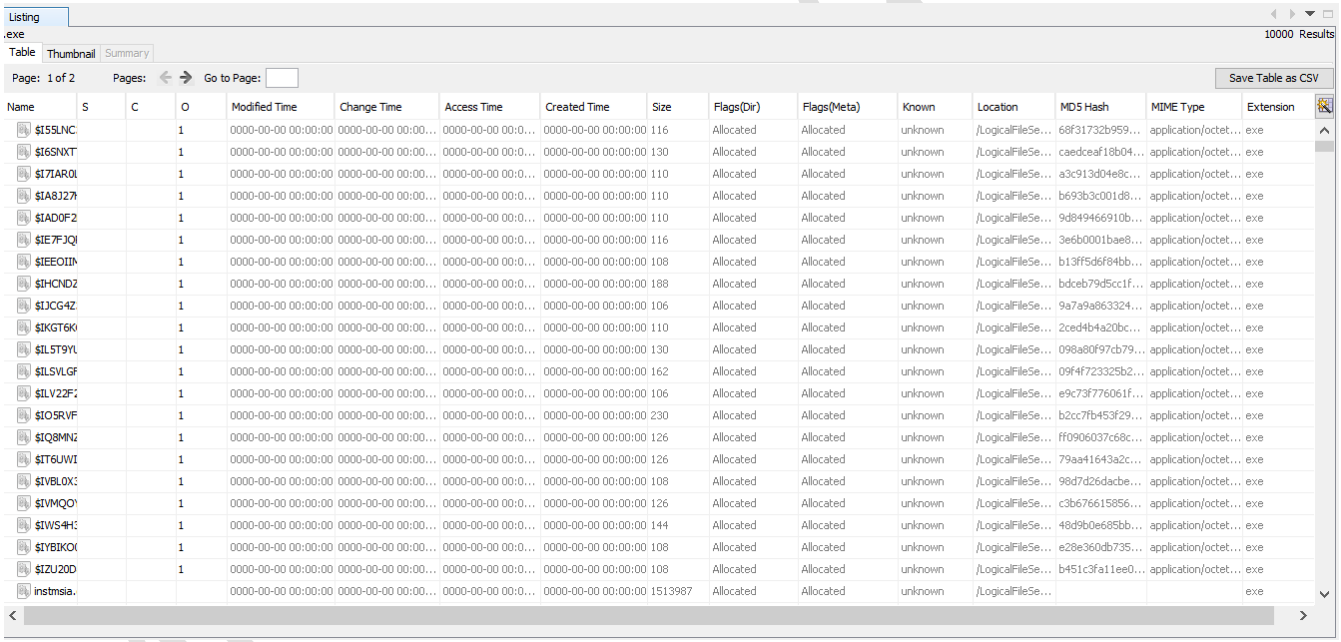


.Exe

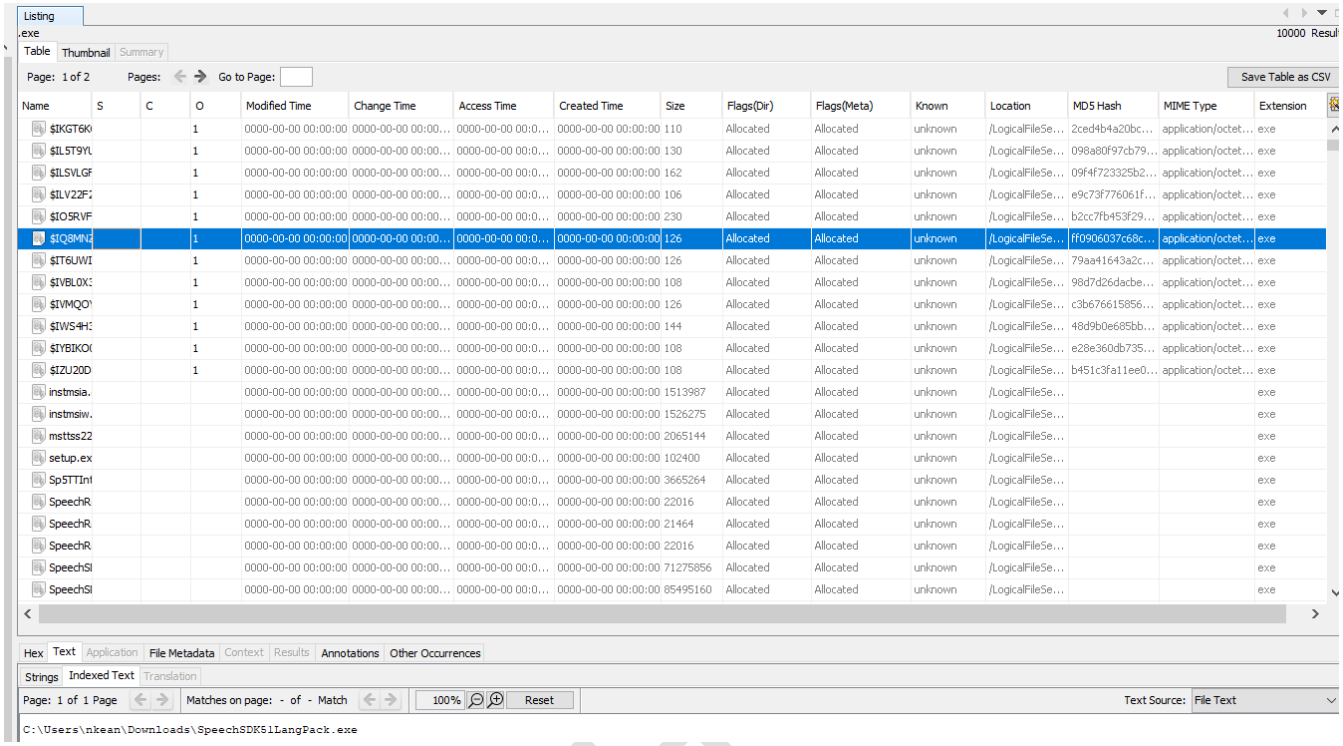
Step 1. Navigate to .exe



Step 2. Investigate the contents of .exe



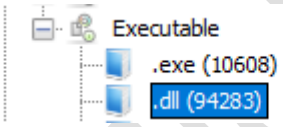
Step 3. Choose a .exe file to investigate



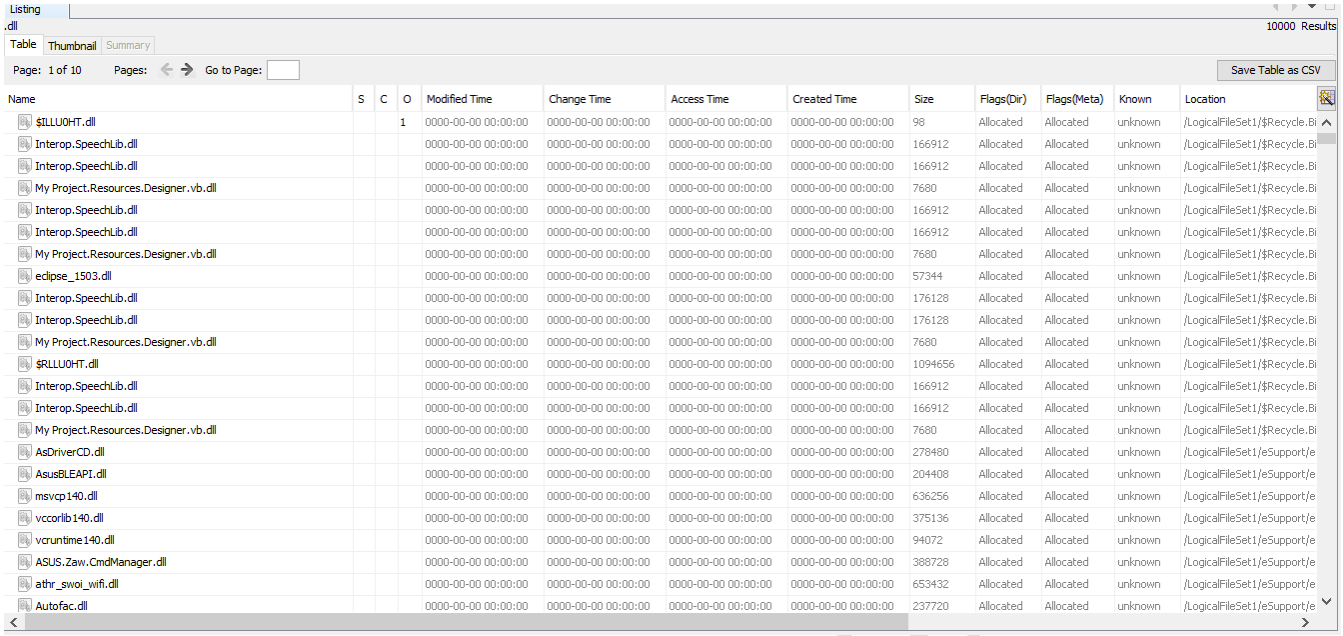
Q. What do you think this will execute based on the text?

.DLL

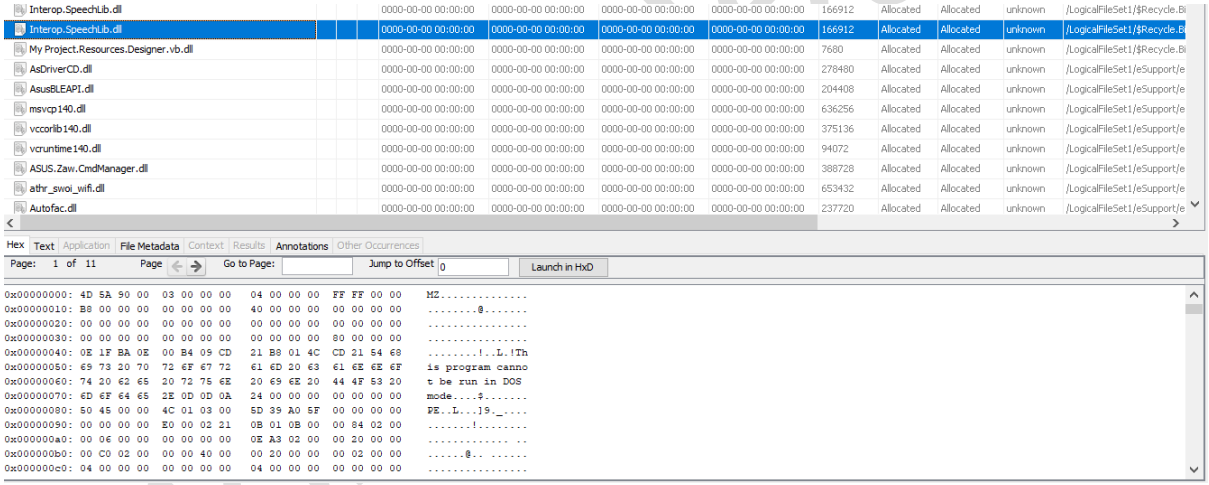
Step 1. Navigate to .dll



Step 2. Examine the contents of .dll



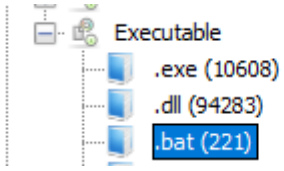
Step 3. Choose a file to investigate.



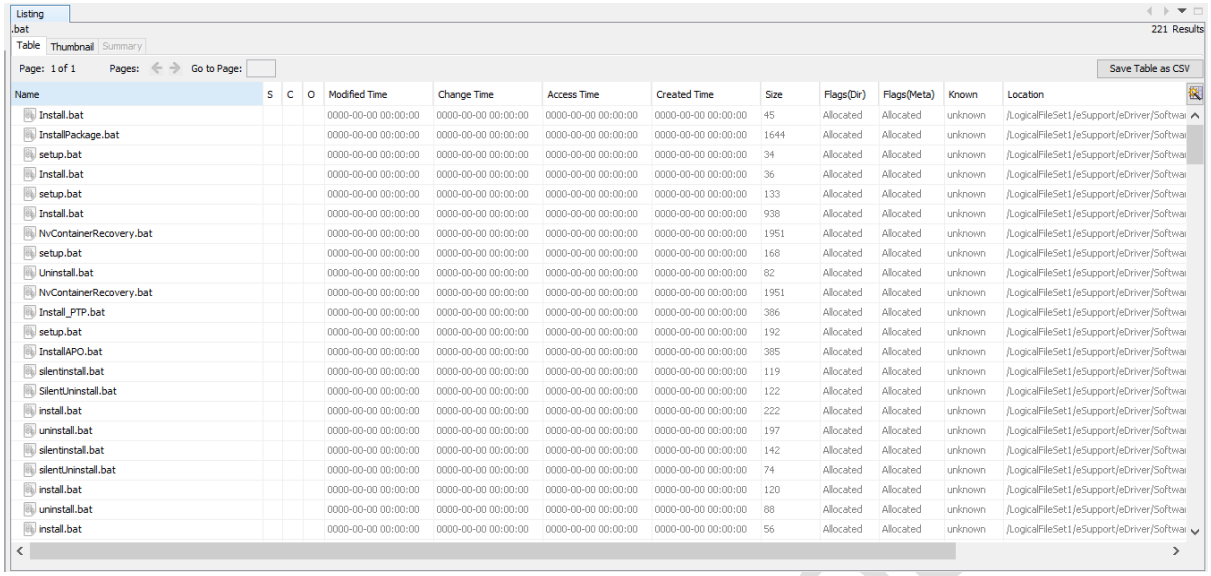
Q. What is the purpose of .dll files?

.Bat

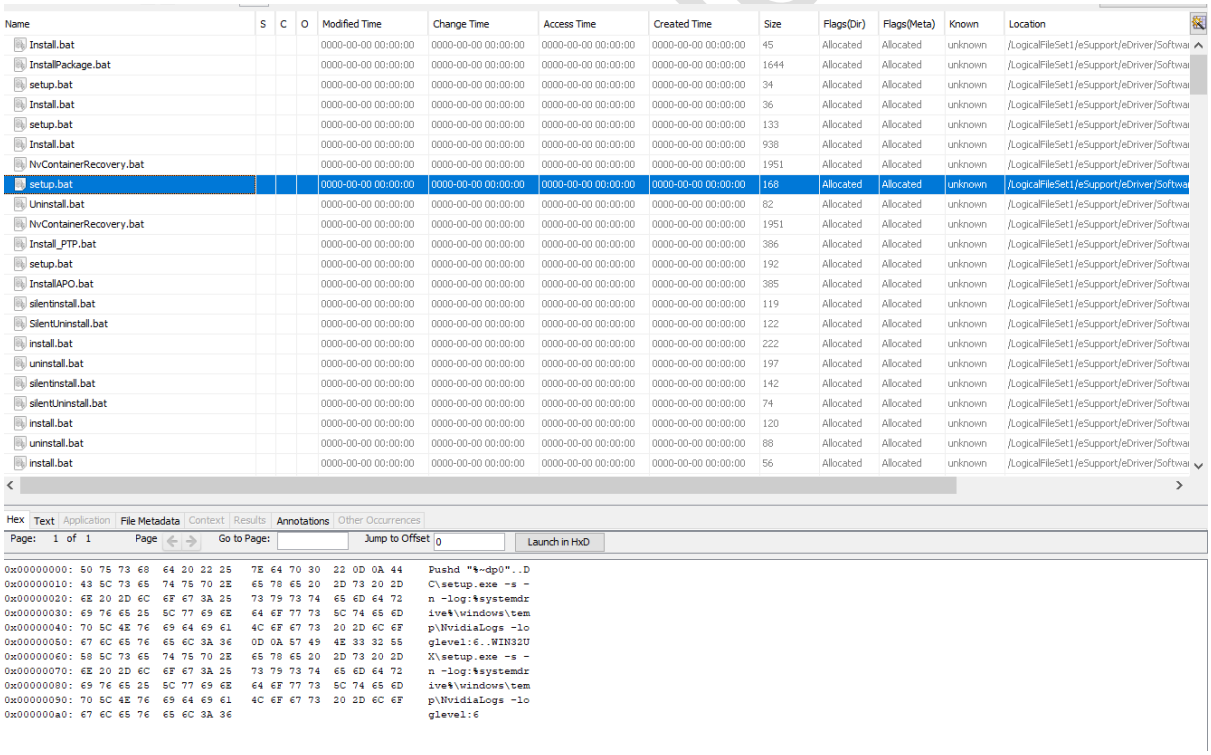
Step 1. Navigate to .bat



Step 2. Investigate the contents of .bat



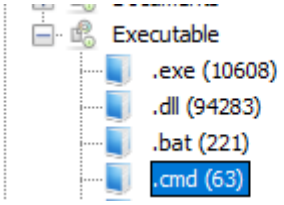
Step 3. Choose a .bat file to examine



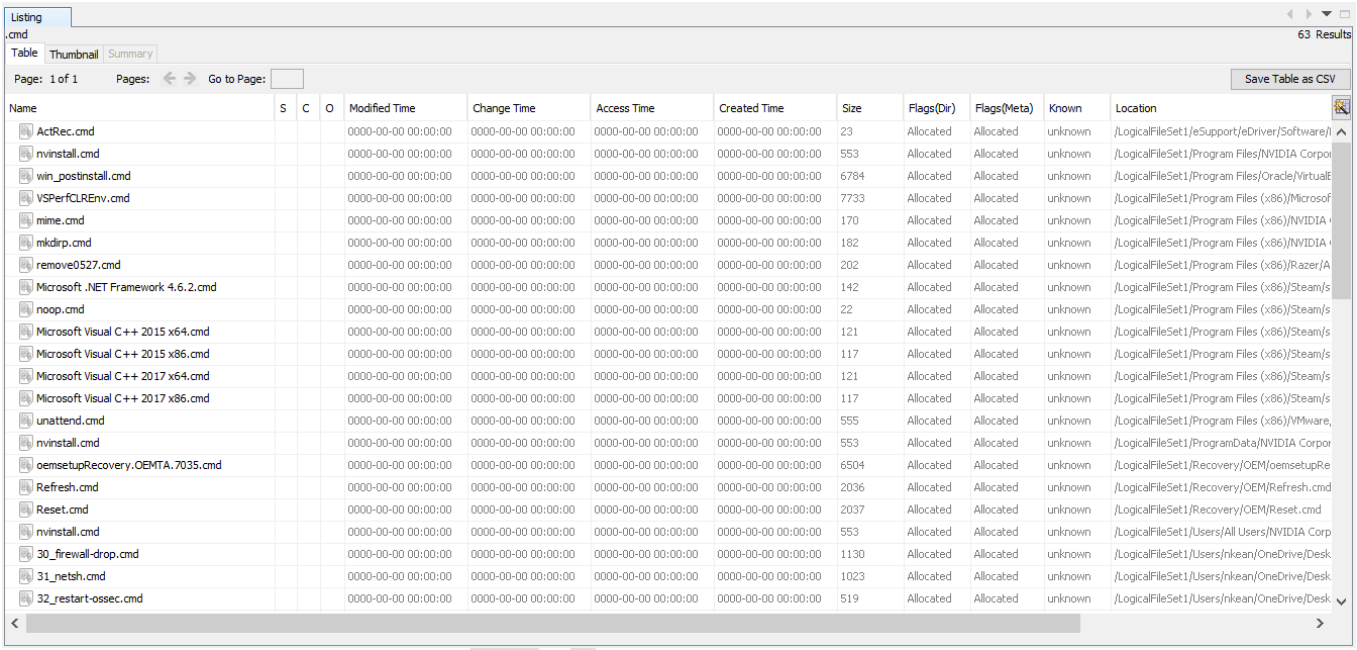
Q. What are .bat files?

.CMD

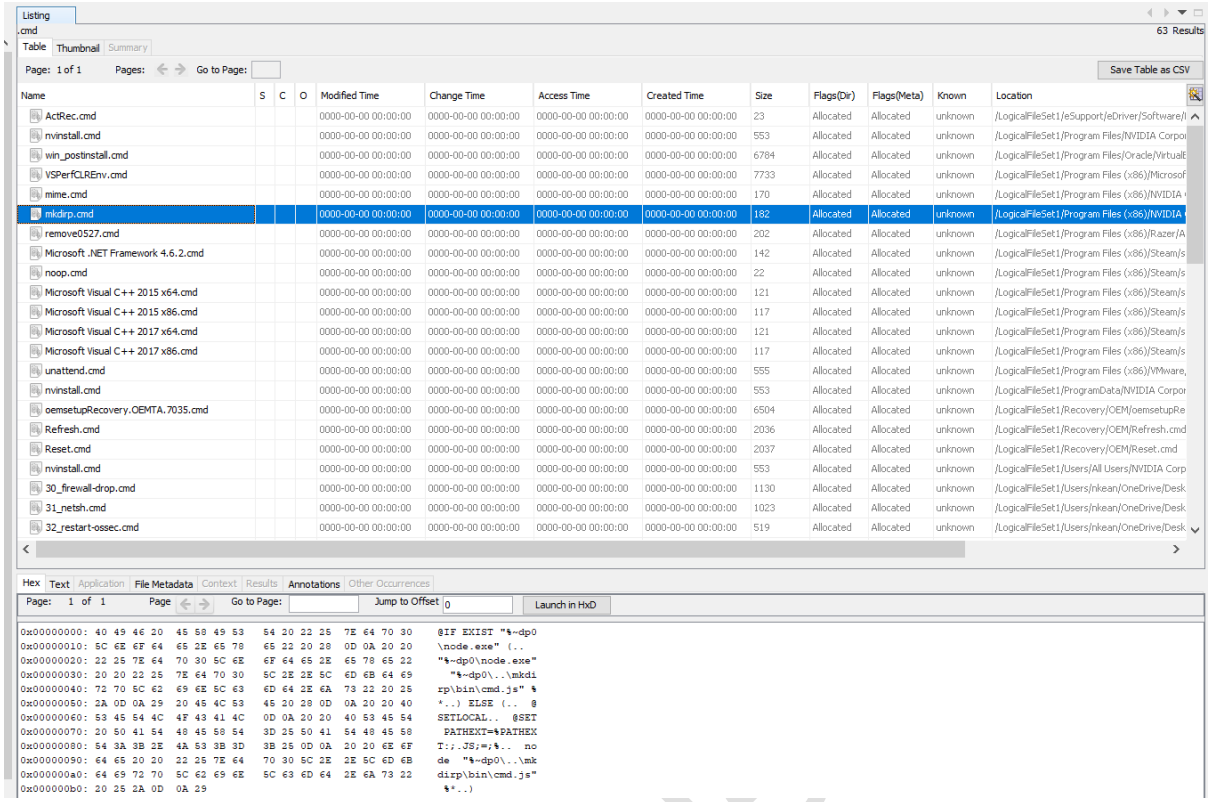
Step 1. Navigate to .CMD



Step 2. Investigate the contents of .cmd



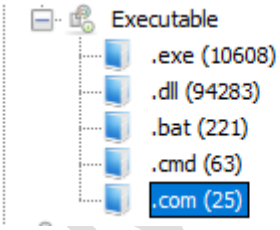
Step 3. Choose a .cmd file to investigate



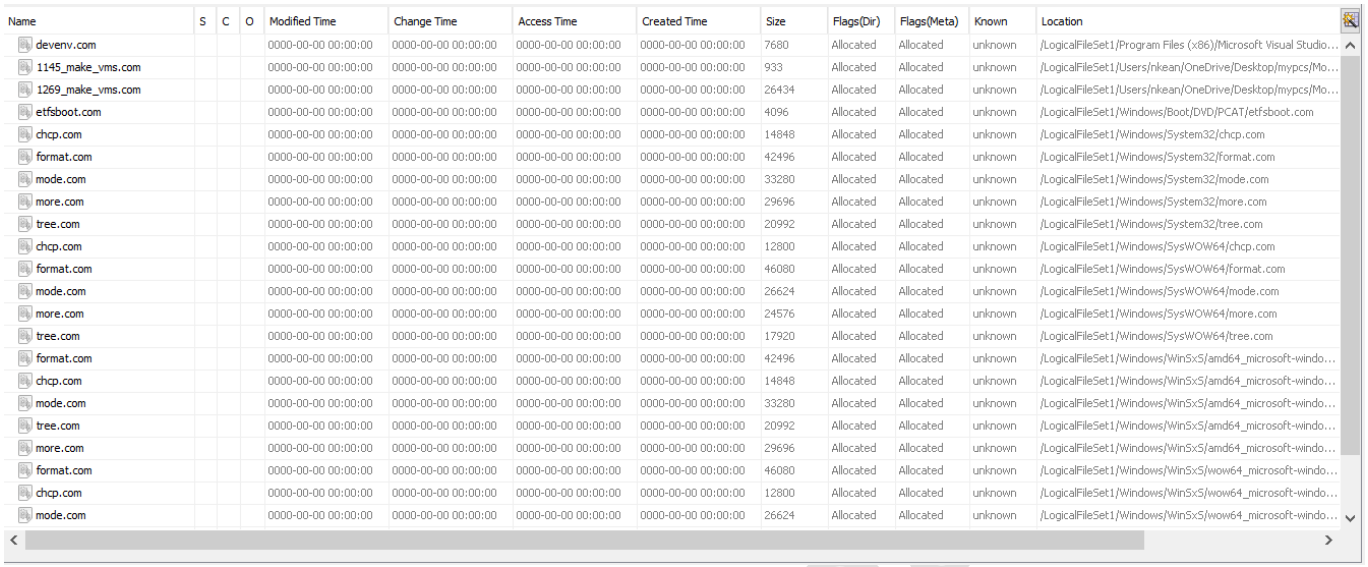
Q. What could a forensic investigator do with captured cmd actions from the user?

.com

Step 1. Navigate to .com

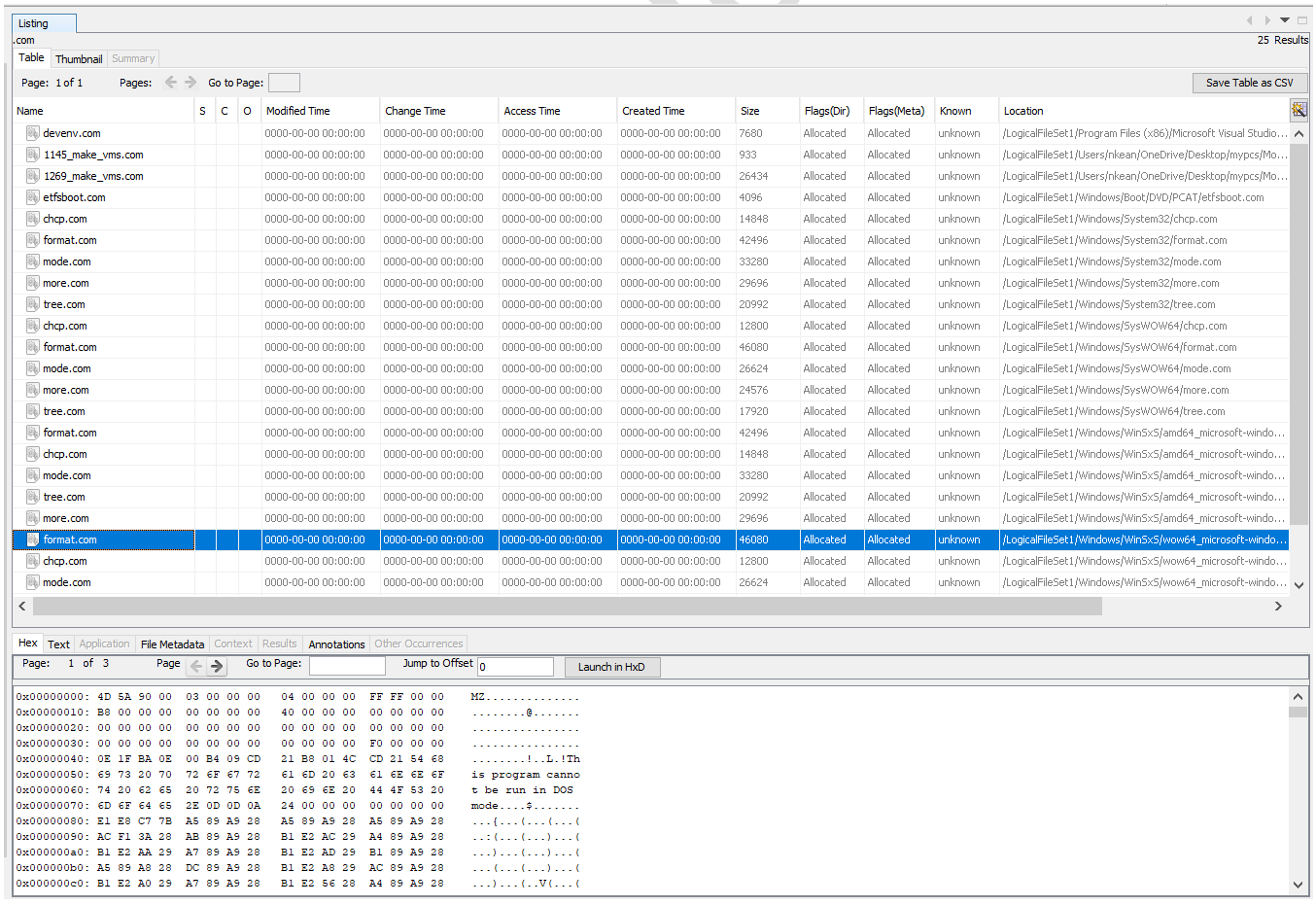


Step 2. Investigate the contents of .com



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
devenv.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7680	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft Visual Studio...
1145_make_vms.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	933	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop/mypcs/Mo...
1269_make_vms.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26434	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop/mypcs/Mo...
etfsboot.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/Boot/DVD/PCAT/etfsboot.com
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14848	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/chcp.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42496	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/format.com
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33280	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/mode.com
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29696	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/more.com
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20992	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/tree.com
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12800	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/chcp.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	46080	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/format.com
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26624	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/mode.com
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24576	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/more.com
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/tree.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42496	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14848	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33280	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20992	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29696	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	46080	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12800	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26624	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...

Step 3. Choose a .com file to investigate.



Listing

.com — 25 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
devenv.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7680	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft Visual Studio...
1145_make_vms.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	933	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop/mypcs/Mo...
1269_make_vms.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26434	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop/mypcs/Mo...
etfsboot.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/Boot/DVD/PCAT/etfsboot.com
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14848	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/chcp.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42496	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/format.com
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33280	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/mode.com
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29696	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/more.com
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20992	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/System32/tree.com
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12800	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/chcp.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	46080	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/format.com
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26624	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/mode.com
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24576	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/more.com
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/SysWOW64/tree.com
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	42496	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14848	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	33280	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
tree.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20992	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
more.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29696	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/amd64_microsoft-windo...
format.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	46080	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...
chcp.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12800	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...
mode.com				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	26624	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Page: 1 of 3 Page Go to Page: Jump to Offset 0 Launch in HxD

```
0x00000000: 4D 5A 90 00  03 00 00 00   04 00 00 00  FF FF 00 00    MZ..............
0x00000010: B8 00 00 00  00 00 00 00   40 00 00 00  00 00 00 00    ........@.......
0x00000020: 00 00 00 00  00 00 00 00   00 00 00 00  00 00 00 00    ................
0x00000030: 00 00 00 00  00 00 00 00   00 00 00 00  F0 00 00 00    ................
0x00000040: 0E 1F BA 0E  00 B4 09 CD   21 B8 01 4C  CD 21 54 68    ........!..L.!Th
0x00000050: 69 73 20 70  72 6F 67 72   61 6D 20 63  61 6E 6E 6F    is program canno
0x00000060: 74 20 62 65  20 72 75 6E   20 69 6E 20  44 4F 53 20    t be run in DOS
0x00000070: 6D 6F 64 65  2E 0D 0D 0A   24 00 00 00  00 00 00 00    mode....$.......
0x00000080: E1 E8 C7 7B  A5 89 A9 28   A5 89 A9 28  A5 89 A9 28    ...{...(...(...(
0x00000090: AC F1 3A 28  AB 89 A9 28   B1 E2 AC 29  A4 89 A9 28    ..:(...(...)...(
0x000000a0: B1 E2 AA 29  A7 89 A9 28   B1 E2 AD 29  B1 89 A9 28    ...)...(...)...(
0x000000b0: A5 89 A8 28  DC 89 A9 28   B1 E2 A8 29  AC 89 A9 28    ...(...(...)...(
0x000000c0: B1 E2 A0 29  A7 89 A9 28   B1 E2 56 28  A4 89 A9 28    ...)...(..V(...(
```

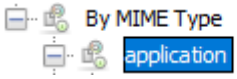
Q. What is the purpose of these files?

Mime Type

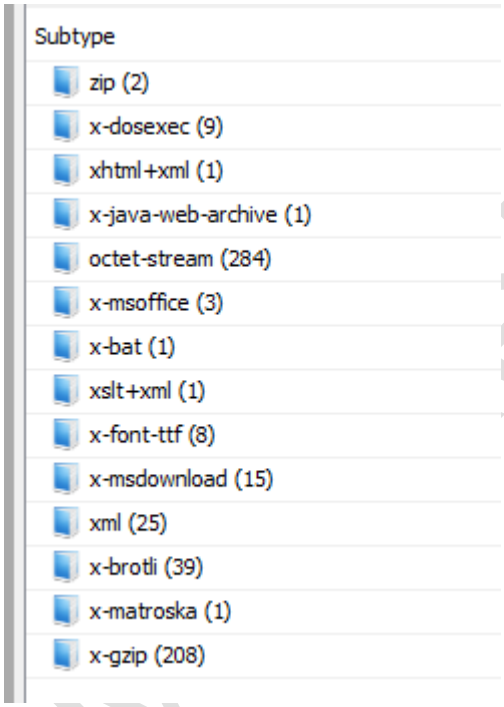
Step 1. Navigate to “By Mime type”

Application

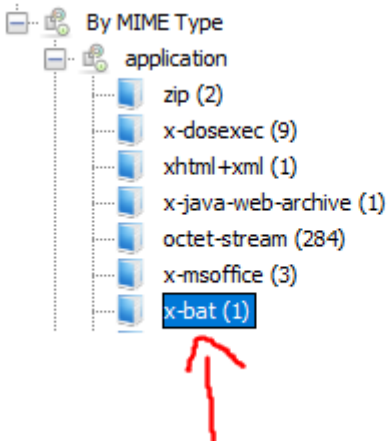
Step 1. Navigate to application



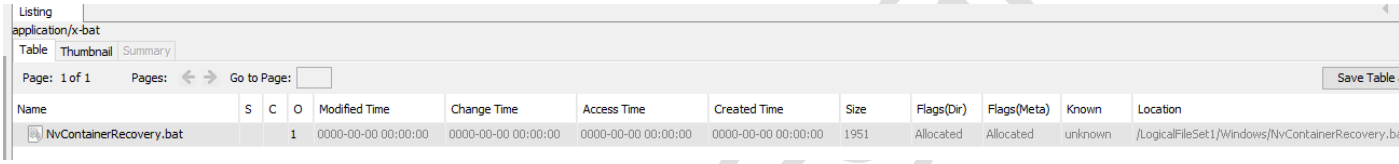
Step 2. Investigate the contents of the application directory



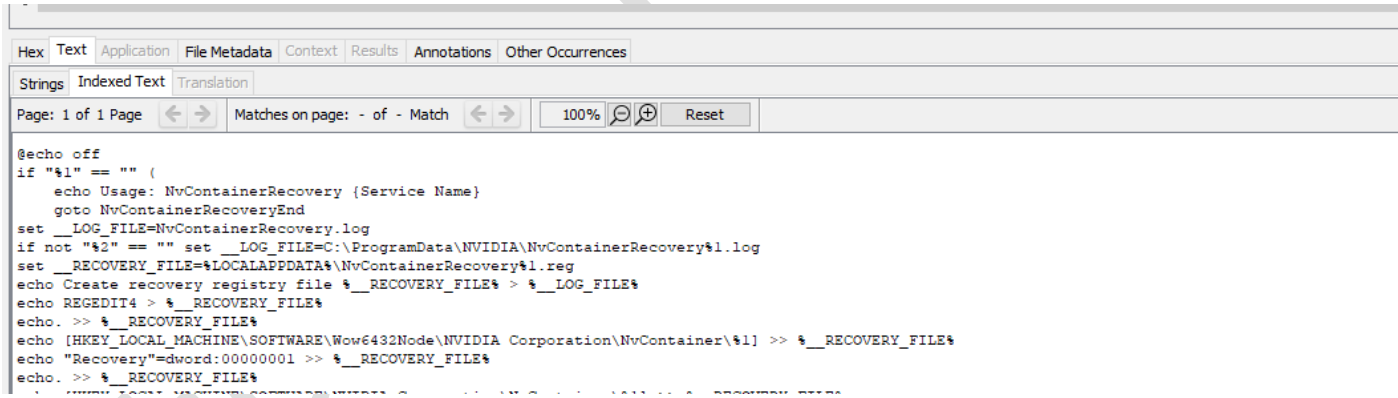
Step 3. Much of these files contain similar information to findings discussed above, but if you notice the file called “x-bat”



Step 4. Investigate the contents of x-bat



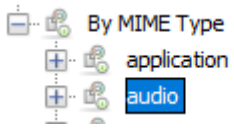
Step 5. Examine the contents of nocontainerecovery



Q. What is the purpose of the file?

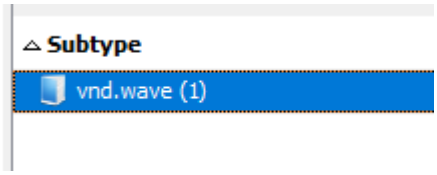
Audio

Step 1. Navigate to Audio

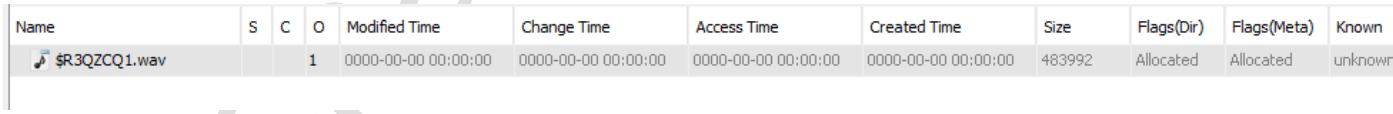


Step 2. Examine the contents of the audio directory

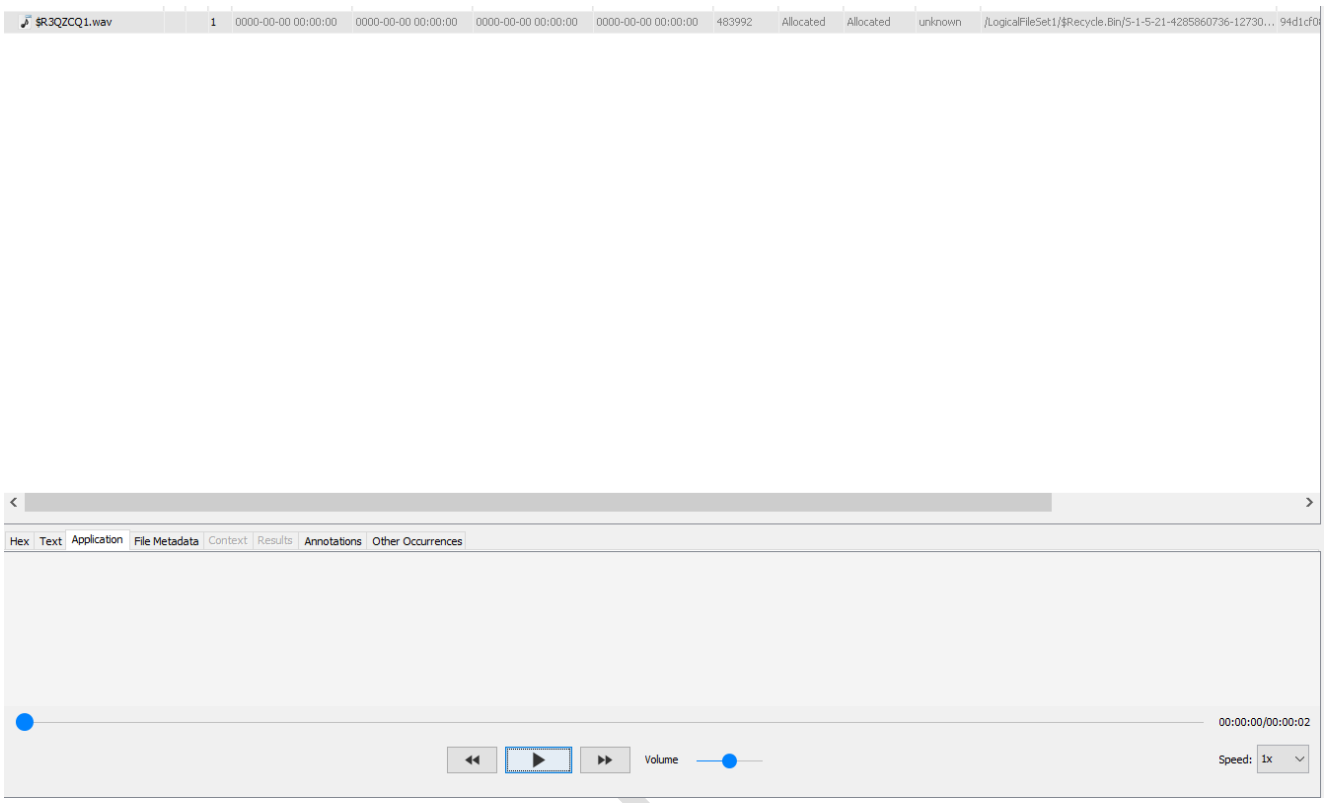
Step 3. Investigate the audio file found on your laptop.



Step 4. Further investigation of something harmless can reveal something quite malicious.



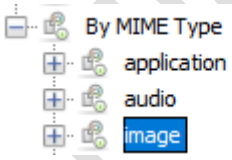
Step 5. Investigate the hidden audio file if you have found one.



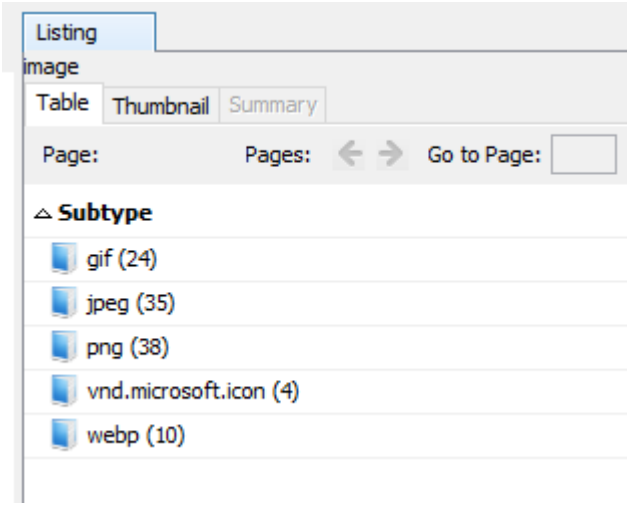
Q. If you found an audio file following the instructions, why do you think it, or they were there?

Image

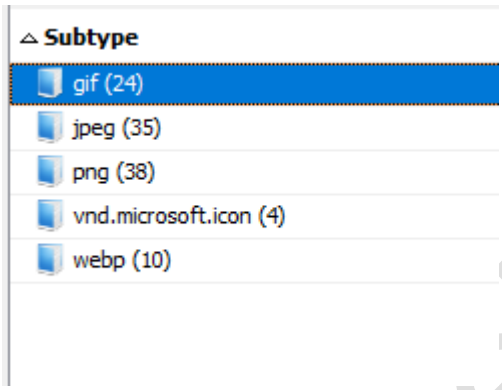
Step 1. Navigate to Image



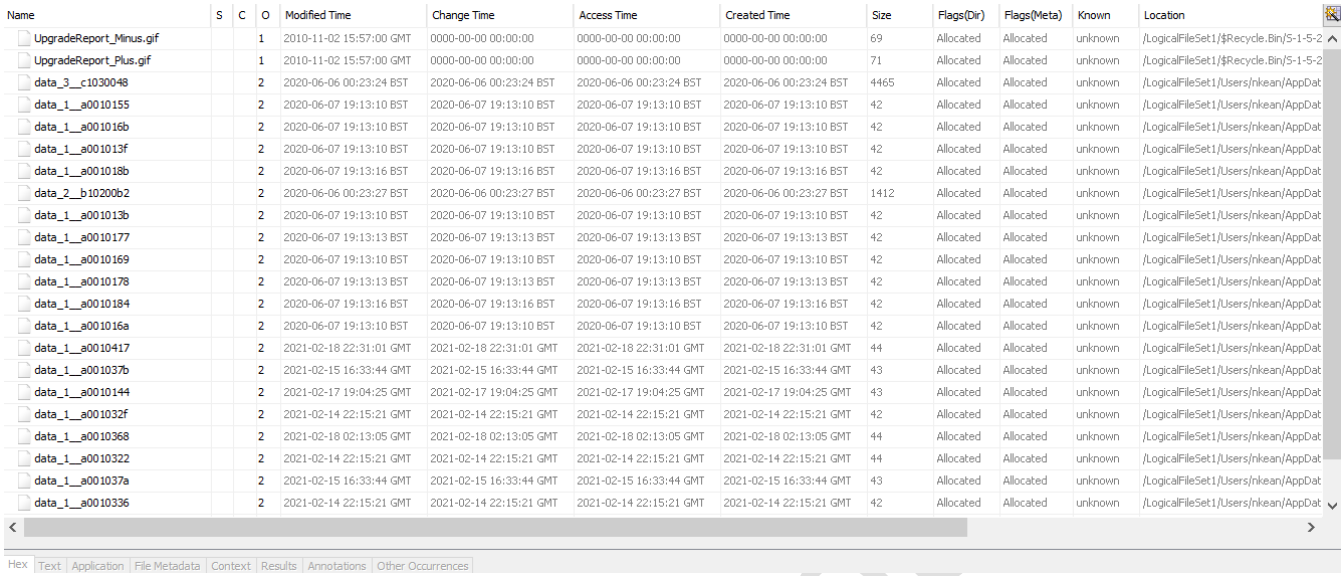
Step 2. Investigate the contents of the image directory.



Step 3. Choose your preferred image type to investigate, in this case gif



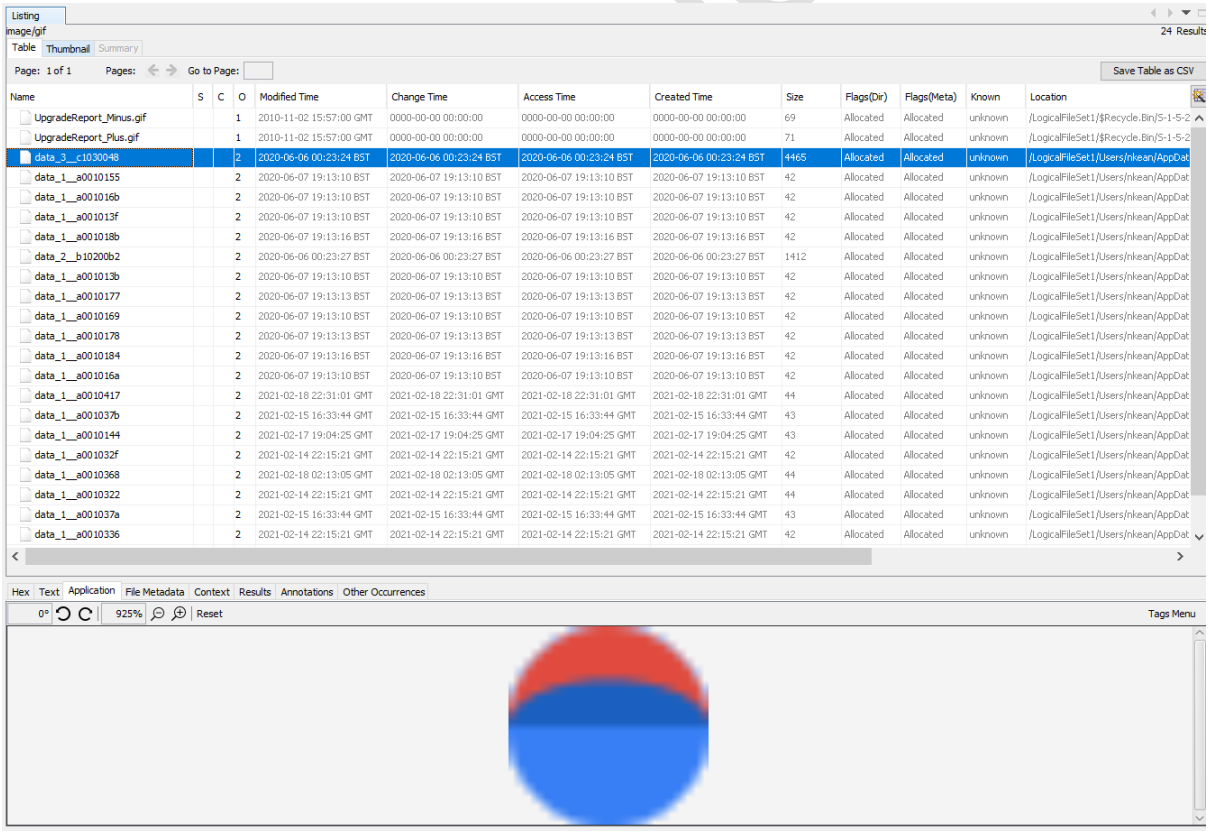
Step 4. Examine the contents of your chosen image type



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
UpgradeReport_Minus.gif			1	2010-11-02 15:57:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	69	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-2
UpgradeReport_Plus.gif			1	2010-11-02 15:57:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-2
data_3__c1030048			2	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	4465	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010155			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001016b			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001013f			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001018b			2	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_2__b10200b2			2	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	1412	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001013b			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010177			2	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010169			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010178			2	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010184			2	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001016a			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010417			2	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001037b			2	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010144			2	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001032f			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010368			2	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010322			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001037a			2	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010336			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Step 5. Select an image inside your chosen type to investigate.



Listing
image/gif
24 Results
Table | Thumbnail | Summary
Page: 1 of 1 Pages: Go to Page: Save Table as CSV

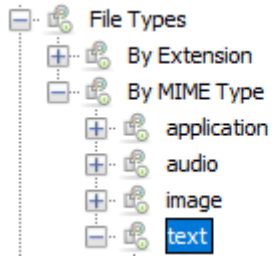
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
UpgradeReport_Minus.gif			1	2010-11-02 15:57:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	69	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-2
UpgradeReport_Plus.gif			1	2010-11-02 15:57:00 GMT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	71	Allocated	Allocated	unknown	/LogicalFileSet1/$Recycle.Bin/S-1-5-2
data_3__c1030048			2	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	2020-06-06 00:23:24 BST	4465	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010155			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001016b			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001013f			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001018b			2	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_2__b10200b2			2	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	2020-06-06 00:23:27 BST	1412	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001013b			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010177			2	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010169			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010178			2	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	2020-06-07 19:13:13 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010184			2	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	2020-06-07 19:13:16 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001016a			2	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	2020-06-07 19:13:10 BST	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010417			2	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	2021-02-18 22:31:01 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001037b			2	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010144			2	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	2021-02-17 19:04:25 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001032f			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010368			2	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	2021-02-18 02:13:05 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010322			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	44	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a001037a			2	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	2021-02-15 16:33:44 GMT	43	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat
data_1__a0010336			2	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	2021-02-14 22:15:21 GMT	42	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/AppDat

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences
0° 925% Reset Tags Menu

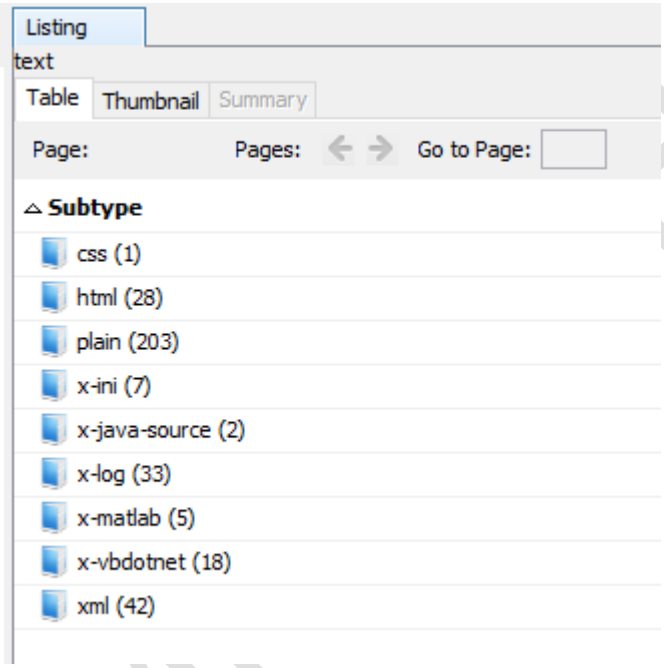
Q. If you chose to follow the gif path, you may have noticed not every picture loaded, why is this the case?

Text

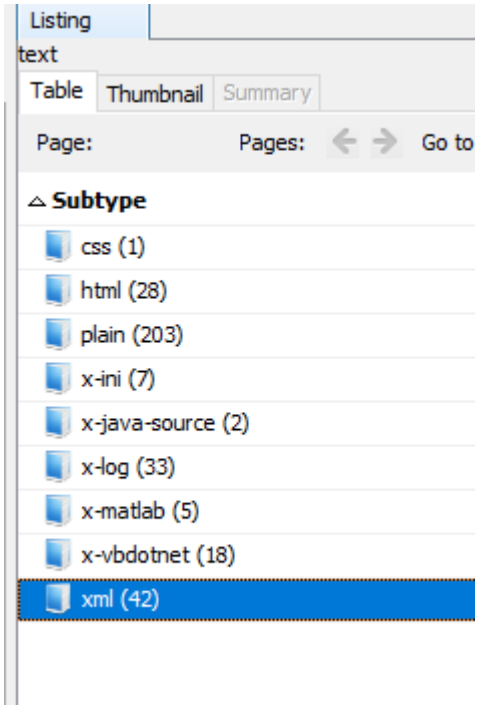
Step 1. Navigate to text



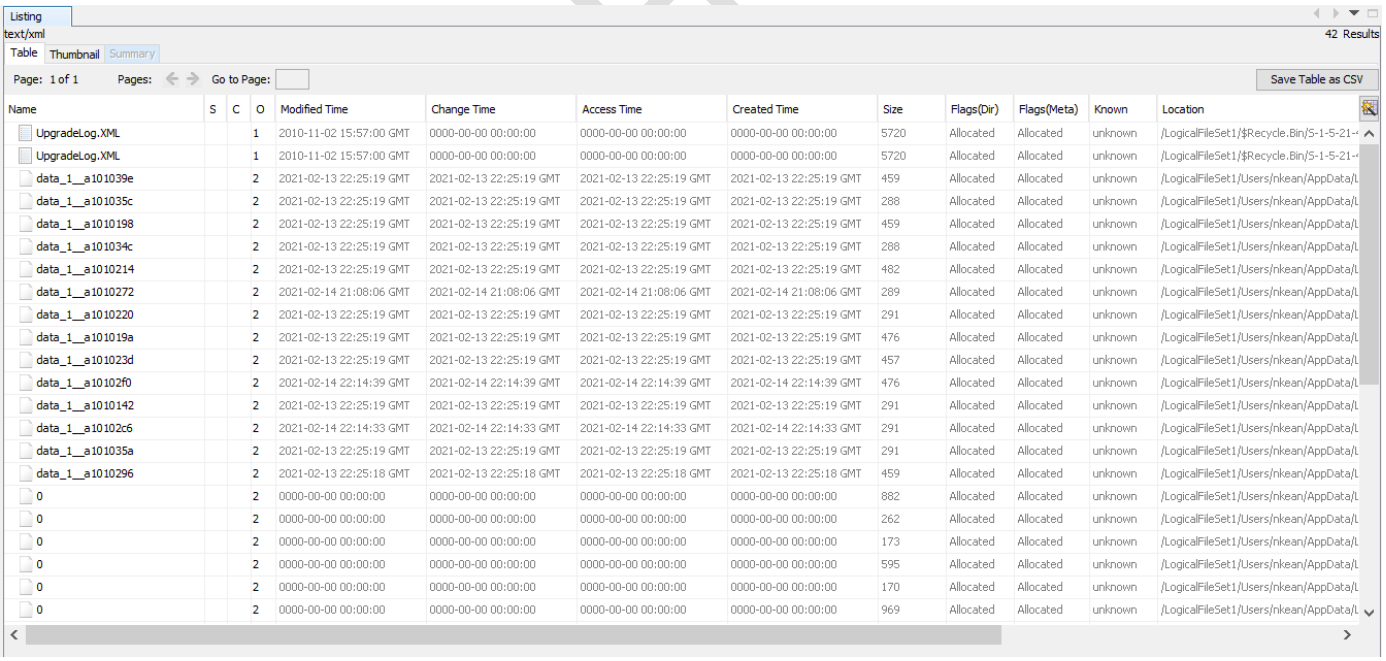
Step 2. Examine the contents of the text directory



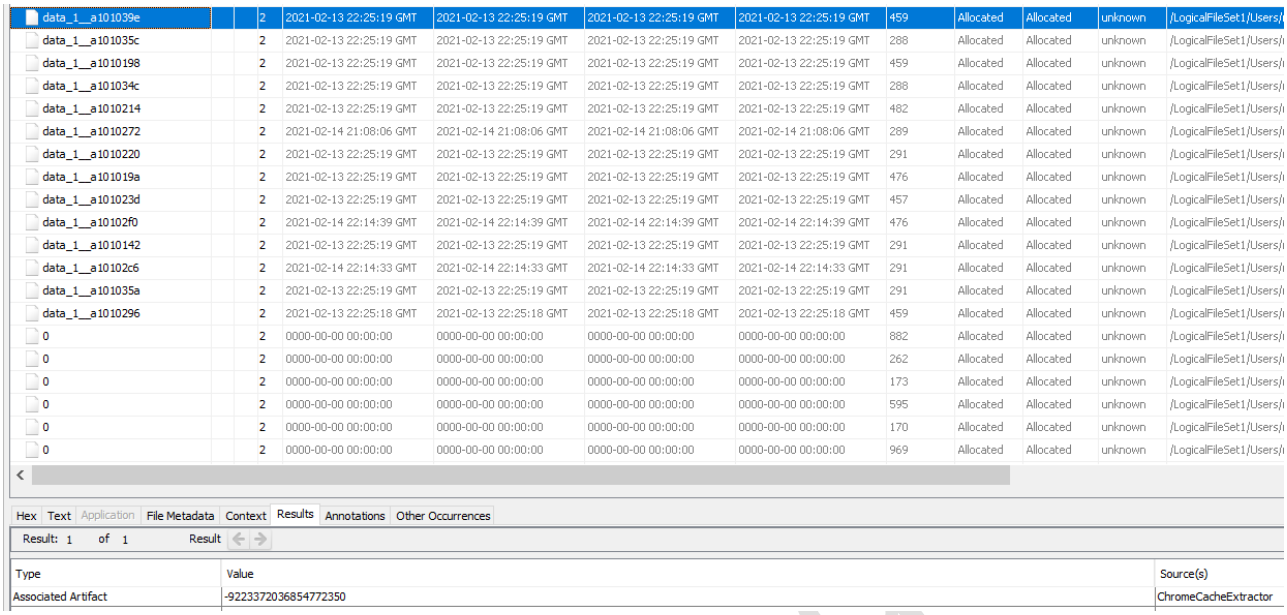
Step 3. Choose your preferred text choice to investigate, in this case xml was chosen



Step 4. Examine the contents of the xml directory



Step 5. Choose a file to investigate



data_1__a101039e			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	459	Allocated	Allocated	unknown
data_1__a101035c			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	288	Allocated	Allocated	unknown
data_1__a1010198			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	459	Allocated	Allocated	unknown
data_1__a101034c			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	288	Allocated	Allocated	unknown
data_1__a1010214			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	482	Allocated	Allocated	unknown
data_1__a1010272			2	2021-02-14 21:08:06 GMT	2021-02-14 21:08:06 GMT	2021-02-14 21:08:06 GMT	2021-02-14 21:08:06 GMT	289	Allocated	Allocated	unknown
data_1__a1010220			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	291	Allocated	Allocated	unknown
data_1__a101019a			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	476	Allocated	Allocated	unknown
data_1__a101023d			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	457	Allocated	Allocated	unknown
data_1__a10102f0			2	2021-02-14 22:14:39 GMT	2021-02-14 22:14:39 GMT	2021-02-14 22:14:39 GMT	2021-02-14 22:14:39 GMT	476	Allocated	Allocated	unknown
data_1__a1010142			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	291	Allocated	Allocated	unknown
data_1__a10102c6			2	2021-02-14 22:14:33 GMT	2021-02-14 22:14:33 GMT	2021-02-14 22:14:33 GMT	2021-02-14 22:14:33 GMT	291	Allocated	Allocated	unknown
data_1__a101035a			2	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	2021-02-13 22:25:19 GMT	291	Allocated	Allocated	unknown
data_1__a1010296			2	2021-02-13 22:25:18 GMT	2021-02-13 22:25:18 GMT	2021-02-13 22:25:18 GMT	2021-02-13 22:25:18 GMT	459	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	882	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	262	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	173	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	595	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	170	Allocated	Allocated	unknown
0			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	969	Allocated	Allocated	unknown

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

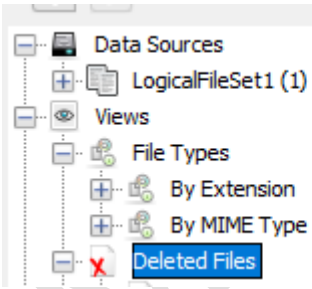
Result: 1 of 1 Result

Type	Value	Source(s)
Associated Artifact	-9223372036854772350	ChromeCacheExtractor

Q. What is the purpose of these data tables?

Deleted Files

Step 1. Navigate to Deleted files, this section will contain any deleted files on your system

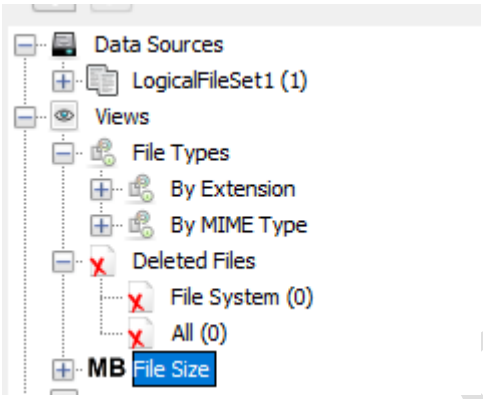


Step 2. Notice that the file system and all files start with 0 deleted files.

Task. Being able to reproduce the means in which criminals can try hide or delete information is an essential part of the forensic process. Create a worthless/test file, delete it and reimage the laptop.

File size

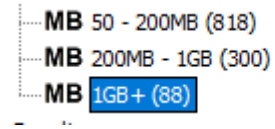
Step 1. Navigate to file size, this section splits files based on the size of said file



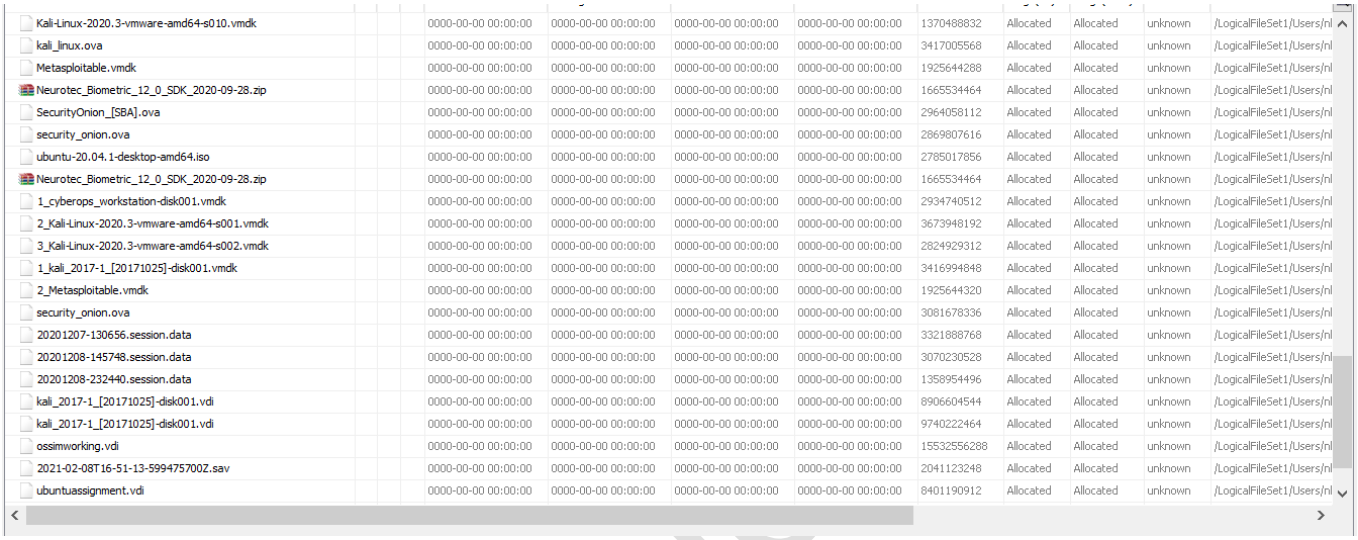
Step 2. Examine the contents of file size

Q. What files would you expect to see in each?

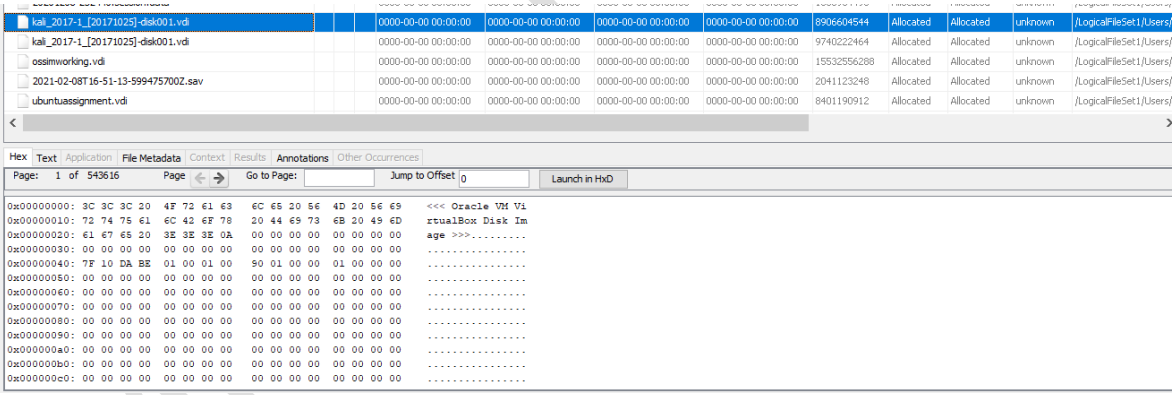
Step 3. Choose the file size in which you would like to investigate, in this case, 1gb+



Step 4. Examine the contents of the chosen file size.



Step 5. Choose a file to investigate



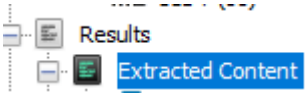
Q. What interesting information can be seen about the vm?

Lab – Examining Results

Step 1. Navigate to results

Extracted Content

Step 1. Navigate to extracted content

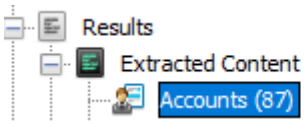


Step 2. Examine the extracted content

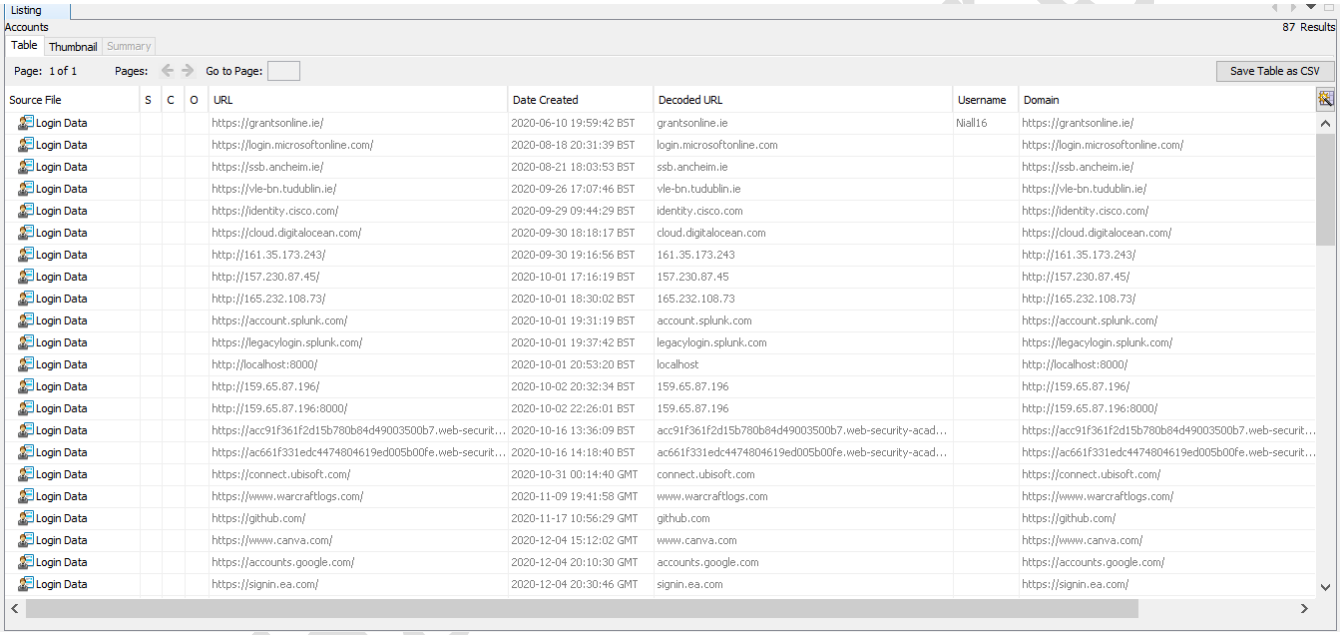
Artifact Type	Child Count
Accounts (87)	87
EXIF Metadata (23)	23
Extension Mismatch Detected (2)	2
Recent Documents (169)	169
User Content Suspected (23)	23
Web Bookmarks (3)	3
Web Cache (797)	797
Web Cookies (403)	403
Web Downloads (6)	6
Web Form Addresses (53)	53
Web Form Autofill (1328)	1328
Web History (454)	454

Accounts

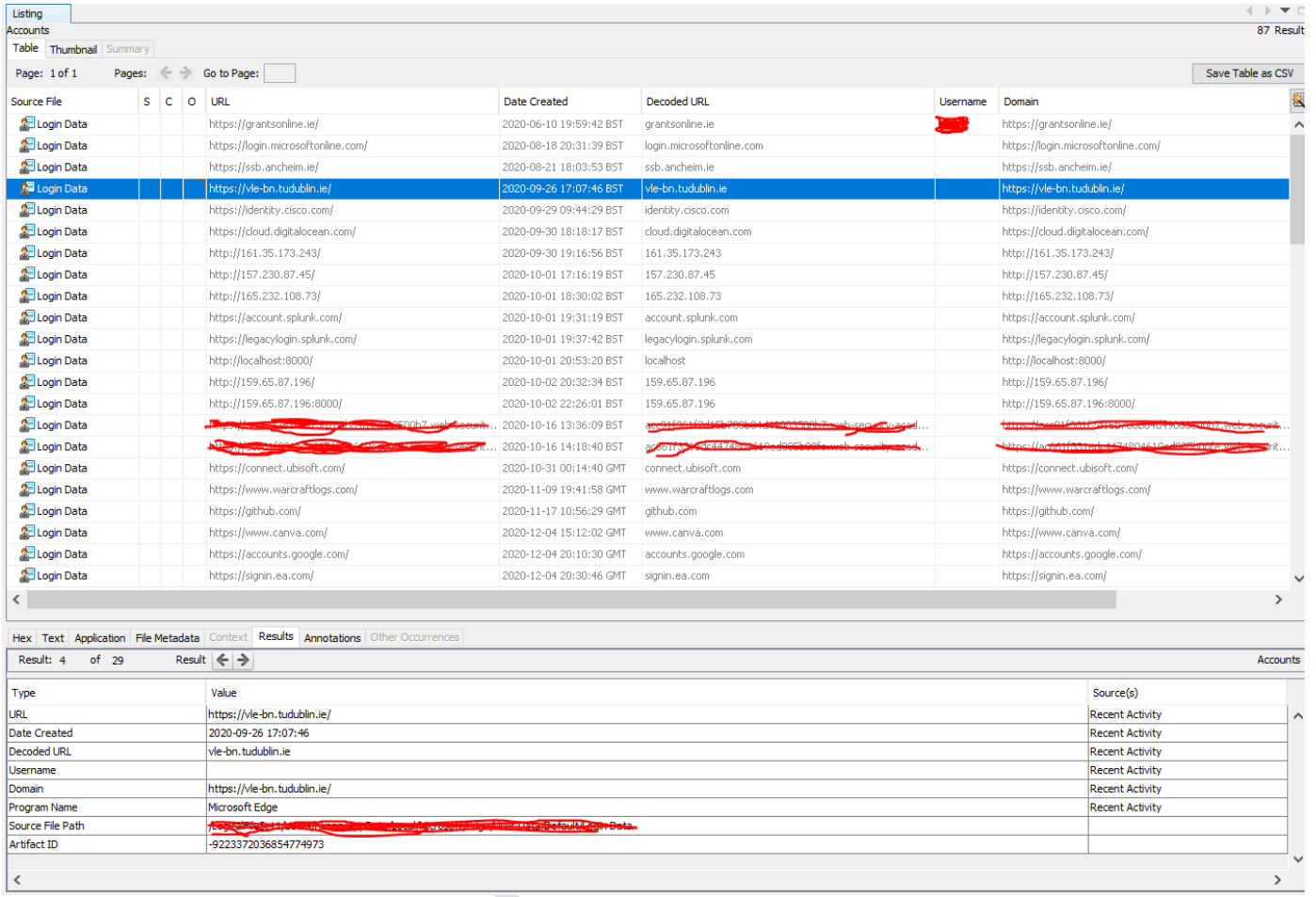
Step 1. Navigate to accounts, this will contain any captured accounts, without login information.



Step 2. Examine the contents of accounts



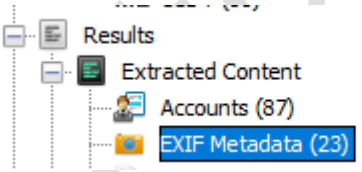
Step 3. Notice the information being displayed, this can help investigators hugely during an investigation. Choose a file to examine.



Note: Some options are removed due to autopsy being a bit too powerful

EXIF metadata

Step 1. Navigate to EXIF metadata



Step 2. Examine the contents of EXIF Metadata

Listing

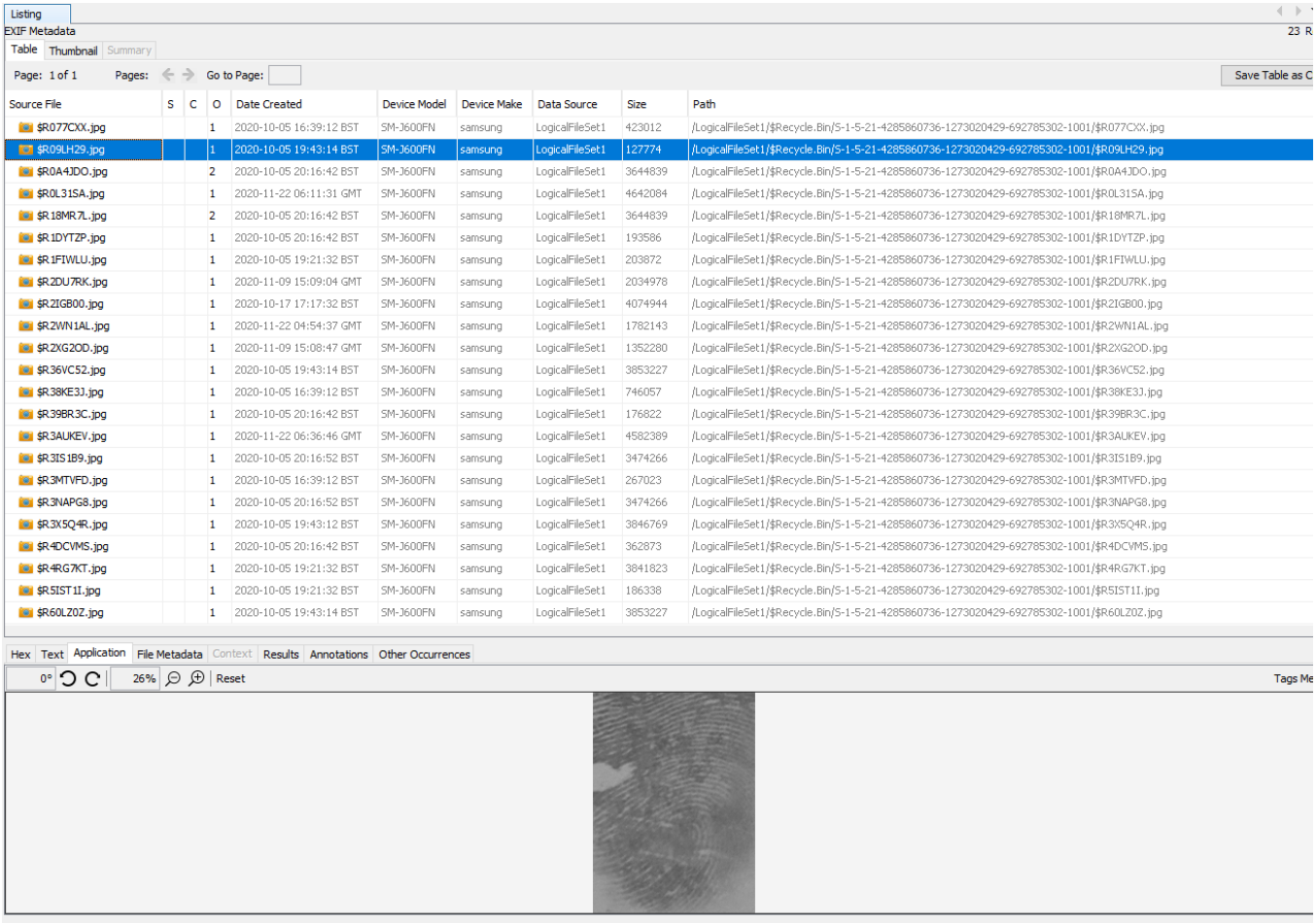
EXIF Metadata

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page:

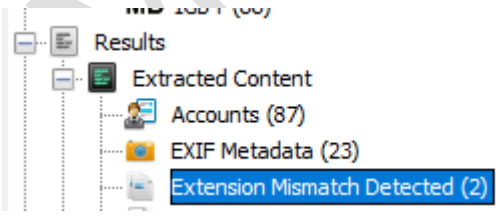
Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size
$R077CXX.jpg			1	2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	423012
$R09LH29.jpg			1	2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	127774
$R0A4JDO.jpg			2	2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	3644839
$R0L31SA.jpg			1	2020-11-22 06:11:31 GMT	SM-J600FN	samsung	LogicalFileSet1	4642084
$R18MR7L.jpg			2	2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	3644839
$R1DYTZP.jpg			1	2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	193586
$R1FIWLU.jpg			1	2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	203872
$R2DU7RK.jpg			1	2020-11-09 15:09:04 GMT	SM-J600FN	samsung	LogicalFileSet1	2034978
$R2IGB00.jpg			1	2020-10-17 17:17:32 BST	SM-J600FN	samsung	LogicalFileSet1	4074944
$R2WN1AL.jpg			1	2020-11-22 04:54:37 GMT	SM-J600FN	samsung	LogicalFileSet1	1782143
$R2XG2OD.jpg			1	2020-11-09 15:08:47 GMT	SM-J600FN	samsung	LogicalFileSet1	1352280
$R36VC52.jpg			1	2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	3853227
$R38KE3J.jpg			1	2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	746057
$R39BR3C.jpg			1	2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	176822
$R3AUKEV.jpg			1	2020-11-22 06:36:46 GMT	SM-J600FN	samsung	LogicalFileSet1	4582389
$R3IS1B9.jpg			1	2020-10-05 20:16:52 BST	SM-J600FN	samsung	LogicalFileSet1	3474266
$R3MTVFD.jpg			1	2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	267023
$R3NAPG8.jpg			1	2020-10-05 20:16:52 BST	SM-J600FN	samsung	LogicalFileSet1	3474266
$R3X5Q4R.jpg			1	2020-10-05 19:43:12 BST	SM-J600FN	samsung	LogicalFileSet1	3846769
$R4DCVMS.jpg			1	2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	362873
$R4RG7KT.jpg			1	2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	3841823
$R5IST1I.jpg			1	2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	186338
$R60LZ0Z.jpg			1	2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	3853227

Step 3. Choose a file to investigate

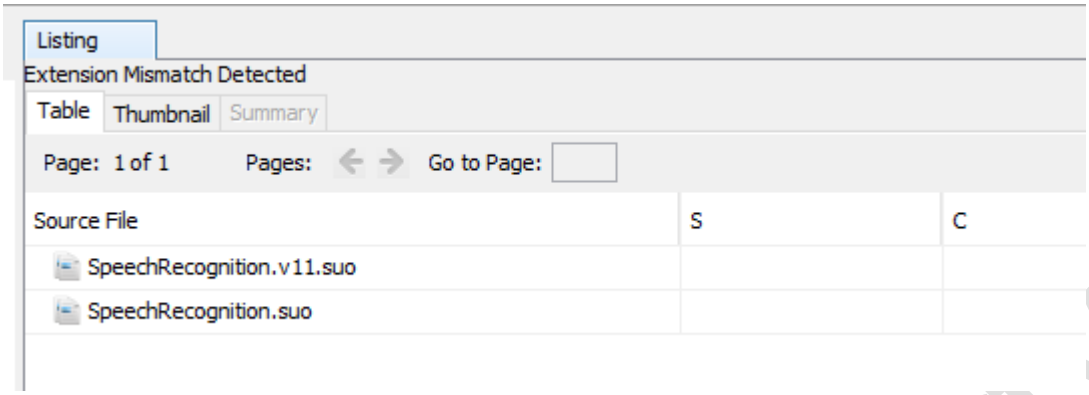


Extension Mismatch detected

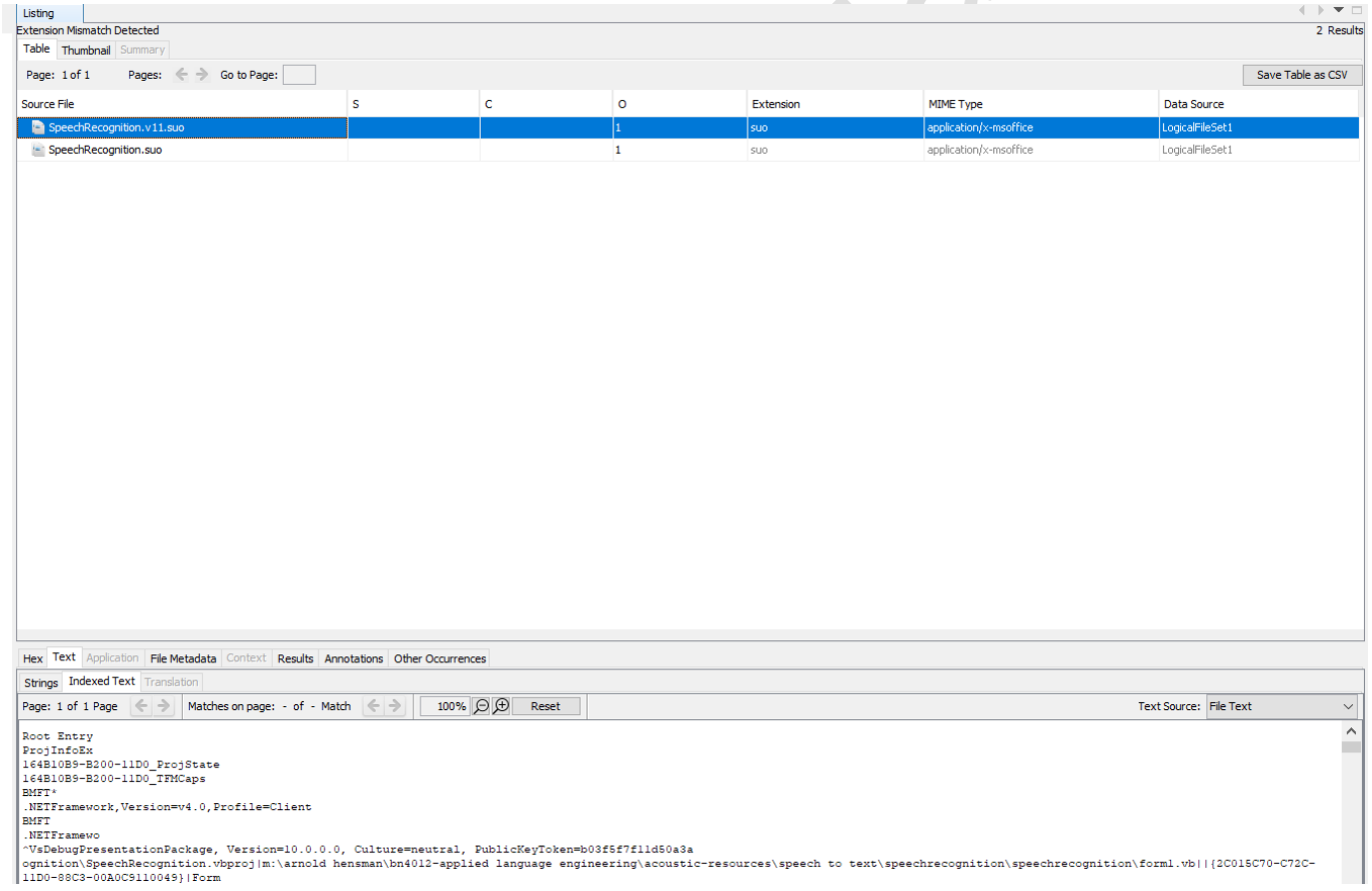
Step 1. Navigate to Extension Mismatch detected



Step 2. Examine the contents of extension mismatch detected

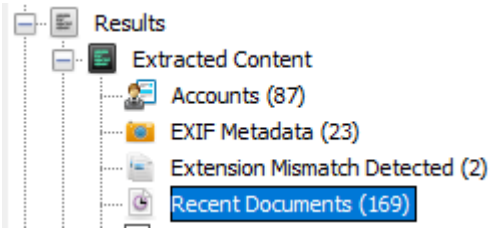


Step 3. Choose a file to investigate

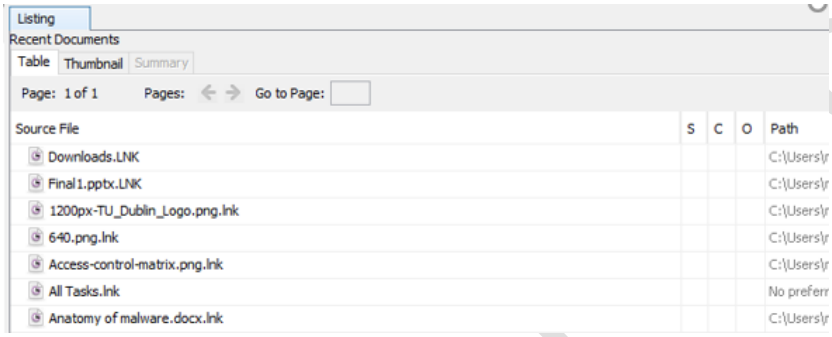


Recent Documents

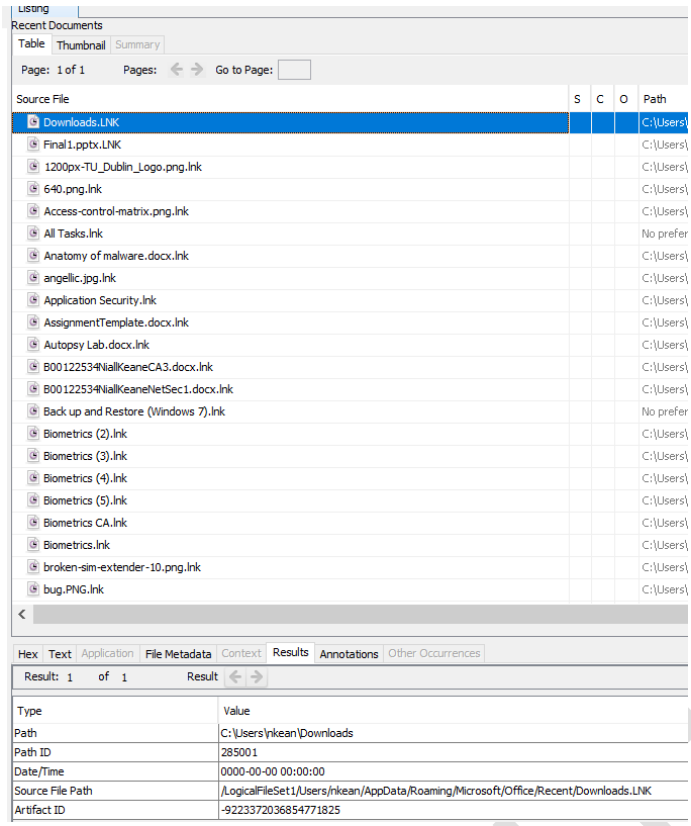
Step 1. Navigate to the recent documents, are the most recent documents opened by the user before imaging occurred



Step 2. Examine the contents of Recent documents

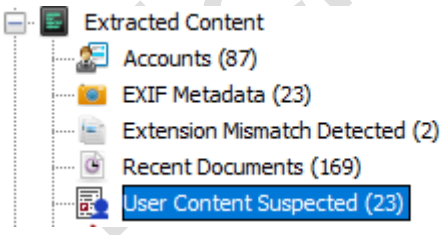


Step 3. Choose a file to investigate

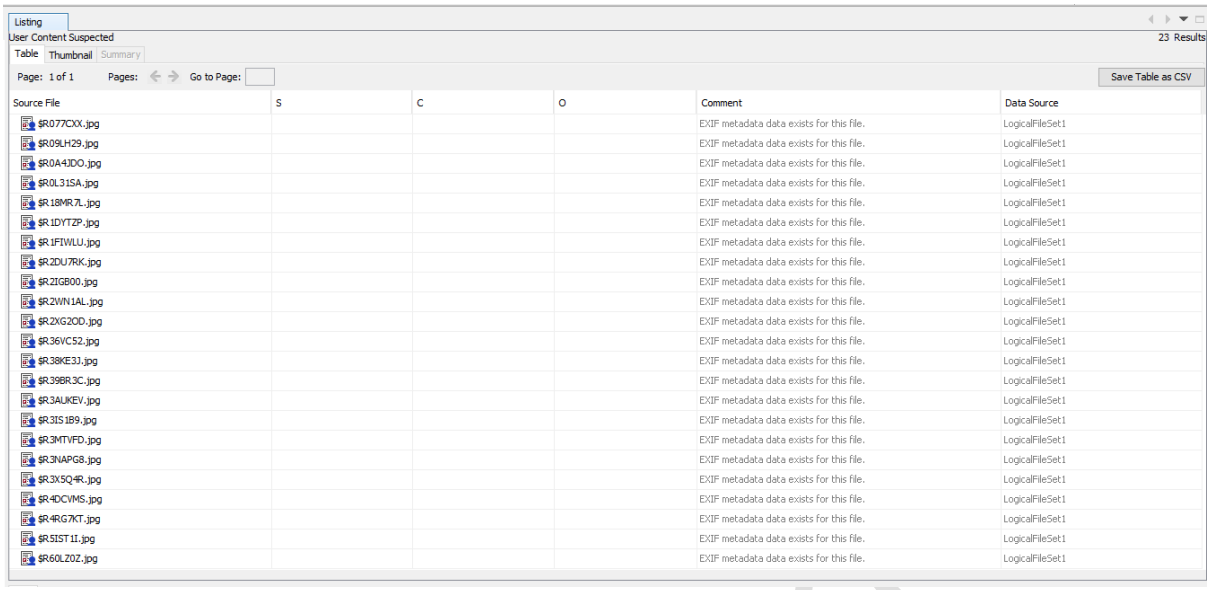


User Content Suspected

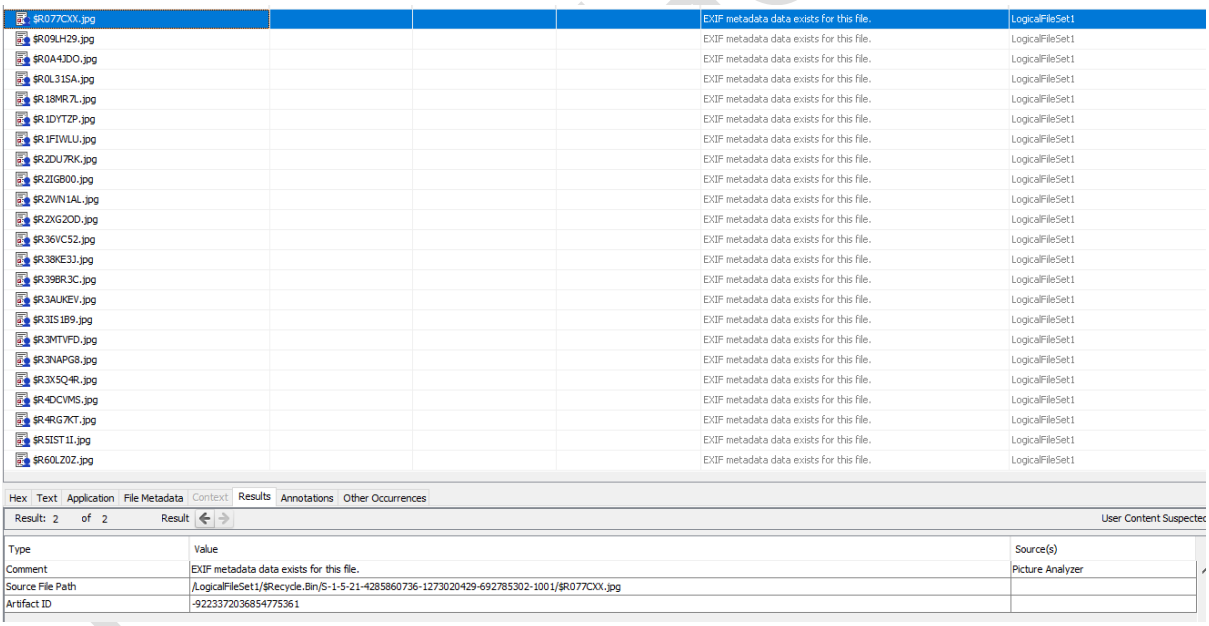
Step 1. Navigate to user content suspected



Step 2. Examine user content suspected

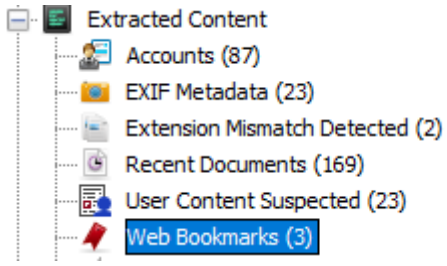


Step 3. Choose a file to investigate

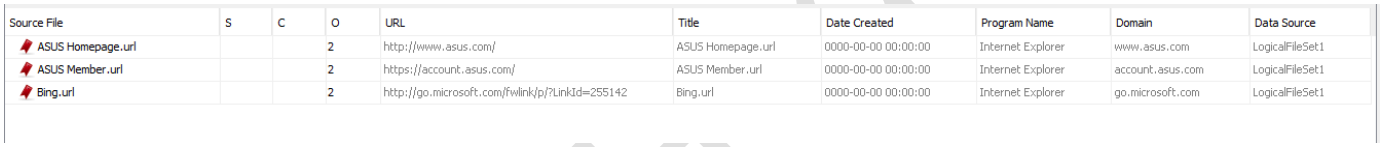


Web Bookmarks

Step 1. Navigate to web bookmarks

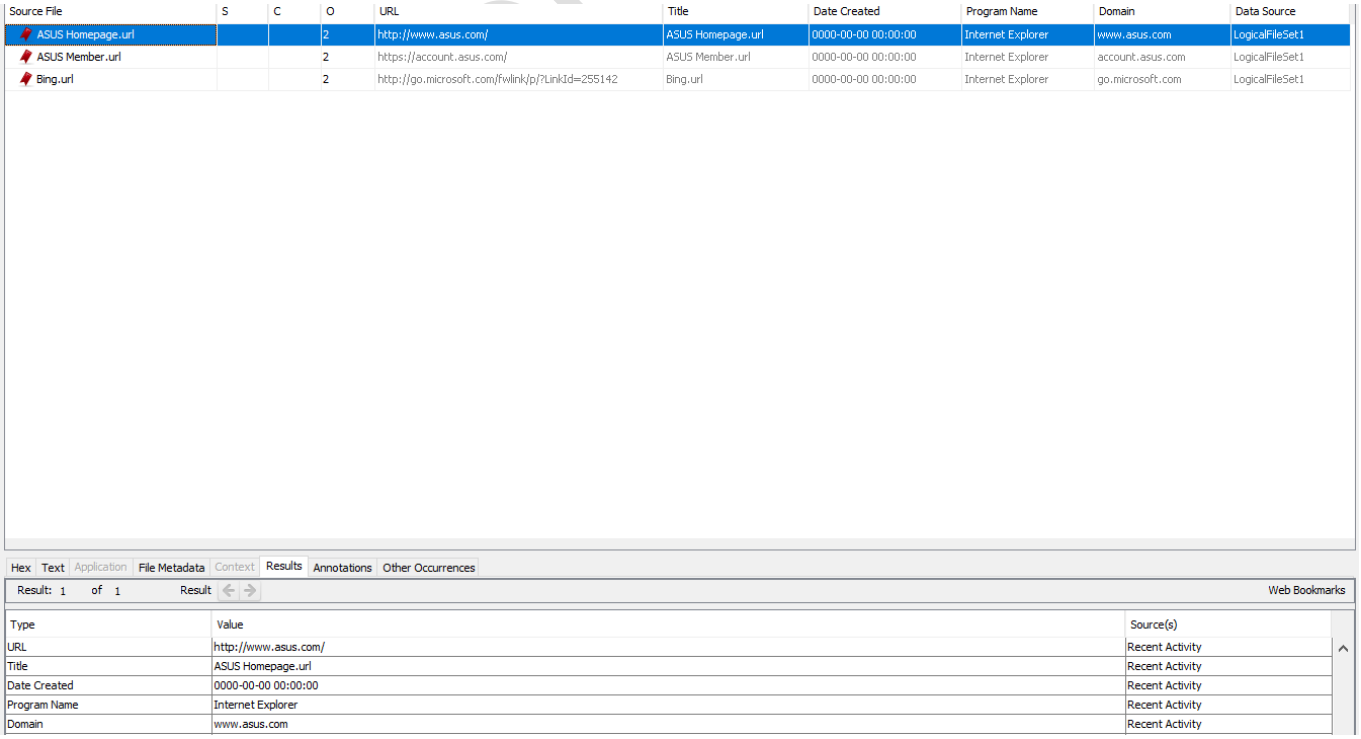


Step 2. Examine the contents of web bookmarks



Source File	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source
ASUS Homepage.url			2	http://www.asus.com/	ASUS Homepage.url	0000-00-00 00:00:00	Internet Explorer	www.asus.com	LogicalFileSet1
ASUS Member.url			2	https://account.asus.com/	ASUS Member.url	0000-00-00 00:00:00	Internet Explorer	account.asus.com	LogicalFileSet1
Bing.url			2	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	0000-00-00 00:00:00	Internet Explorer	go.microsoft.com	LogicalFileSet1

Step 3. Choose a file to examine



Source File	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source
ASUS Homepage.url			2	http://www.asus.com/	ASUS Homepage.url	0000-00-00 00:00:00	Internet Explorer	www.asus.com	LogicalFileSet1
ASUS Member.url			2	https://account.asus.com/	ASUS Member.url	0000-00-00 00:00:00	Internet Explorer	account.asus.com	LogicalFileSet1
Bing.url			2	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	0000-00-00 00:00:00	Internet Explorer	go.microsoft.com	LogicalFileSet1

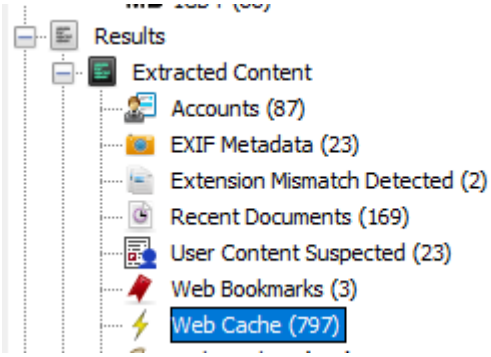
Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 1 of 1 Result — Web Bookmarks

Type	Value	Source(s)
URL	http://www.asus.com/	Recent Activity
Title	ASUS Homepage.url	Recent Activity
Date Created	0000-00-00 00:00:00	Recent Activity
Program Name	Internet Explorer	Recent Activity
Domain	www.asus.com	Recent Activity

Web Cache

Step 1. Navigate to Web cache



Step 2. Examine the contents of the web cache, this saves previously visited websites.

data_1				https://www.origin.com/views/ogd.html	www.origin.com	2021-02-18 22:31:00 GMT	date : Thu, 18 Feb
data_1				https://api1.origin.com/avatar/user/1008187446646/avat...	api1.origin.com	2021-02-13 22:25:19 GMT	date : Thu, 18 Feb
data_1				https://api1.origin.com/ecommerce2/offerUpdatedDate?of...	api1.origin.com	2021-02-18 22:31:01 GMT	x-origin-currenttim
data_1				https://data3.origin.com/asset/content/dam/originx/web/a...	data3.origin.com	2021-02-13 22:25:17 GMT	date : Sun, 14 Feb
data_1				https://www.origin.com/bower_components/origin-compon...	www.origin.com	2021-02-18 22:30:05 GMT	date : Thu, 18 Feb

Step 3. Choose a cached web site to investigate

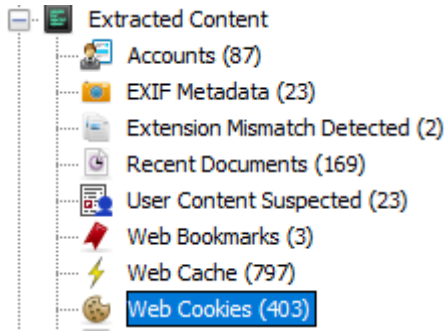
Result: 24 of 516 Result

Type	Value	Source(s)
URL	https://data3.origin.com/asset/content/dam/originx/web/app/games/apex/apex/F2P/myHome/season8/Apex_S8_home_merch_en_ww_v1.jpg/6c93fec4-53d7-4aeb-8014-e0441861c2	ChromeCacheExtractor
Domain	data3.origin.com	ChromeCacheExtractor
Date Created	2021-02-15 16:33:46	ChromeCacheExtractor
Headers	date : Wed, 17 Feb 2021 19:04:27 GMT last-modified : Tue, 02 Feb 2021 17:51:44 GMT server : nginx content-length : 327645 x-origin-ops : bgcegQjnKyl/hRpNbjUGEFe69bMbudavAHLJ1f8BvK4=%0A	ChromeCacheExtractor

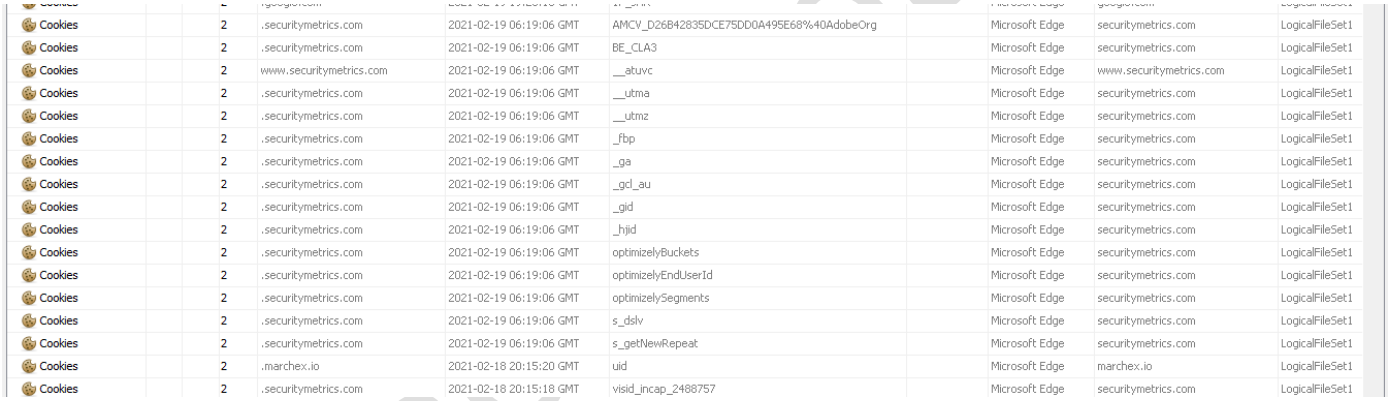
Q. What could a forensic investigator use web caches to find evidence of?

Web Cookies

Step 1. Navigate to Web Cookies

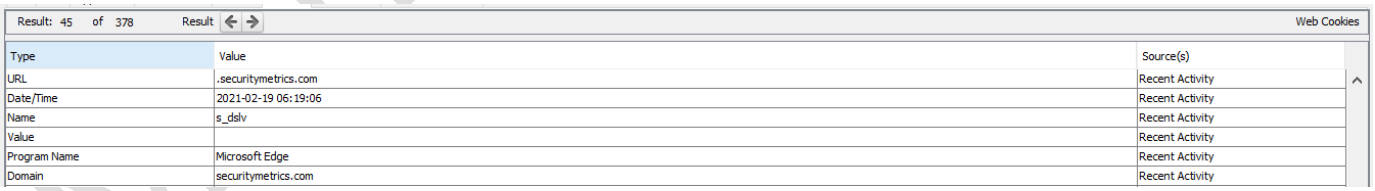


Step 2. Examine the contents of web cookies



Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	AMCV_D26B42835DCE75DD0A495E68%40AdobeOrg	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	BE_CLA3	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	www.securitymetrics.com	2021-02-19 06:19:06 GMT	__atuvc	Microsoft Edge	www.securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	__utma	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	__utmz	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	_fbp	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	_ga	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	_gcl_au	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	_gid	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	_hjid	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	optimizelyBuckets	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	optimizelyEndUserId	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	optimizelySegments	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	s_dslv	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-19 06:19:06 GMT	s_getNewRepeat	Microsoft Edge	securitymetrics.com	LogicalFileSet1
Cookies	2	.marchex.io	2021-02-18 20:15:20 GMT	uid	Microsoft Edge	marchex.io	LogicalFileSet1
Cookies	2	.securitymetrics.com	2021-02-18 20:15:18 GMT	visid_incap_2488757	Microsoft Edge	securitymetrics.com	LogicalFileSet1

Step 3. Investigate the contents of web cookies



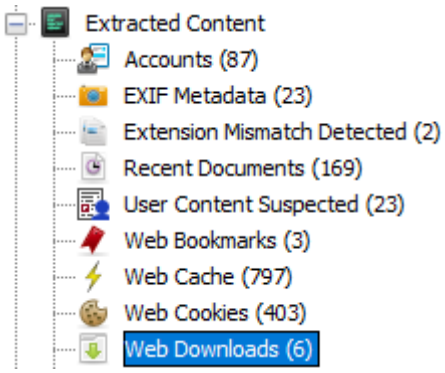
Result: 45 of 378 Result — Web Cookies

Type	Value	Source(s)
URL	.securitymetrics.com	Recent Activity
Date/Time	2021-02-19 06:19:06	Recent Activity
Name	s_dslv	Recent Activity
Value		Recent Activity
Program Name	Microsoft Edge	Recent Activity
Domain	securitymetrics.com	Recent Activity

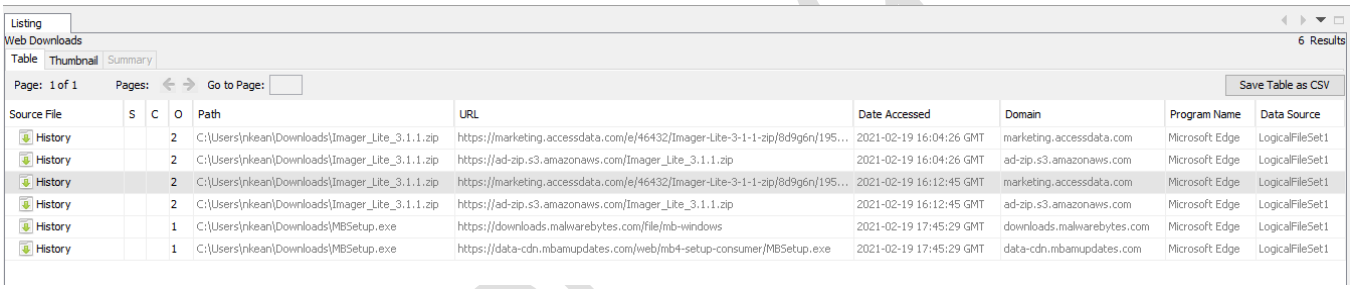
Q. How could an investigator use cookies to find evidence?

Web Downloads

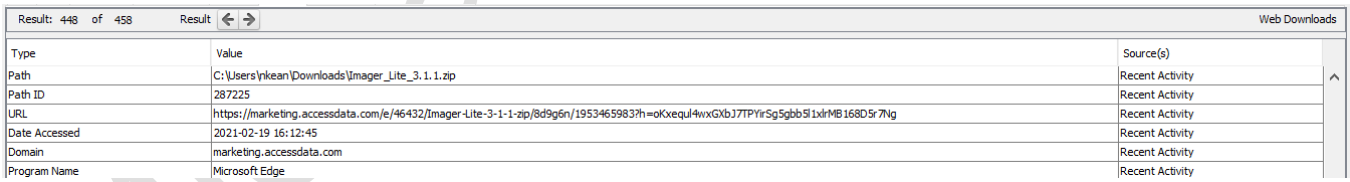
Step 1. Navigate to web downloads



Step 2. View the contents of the web downloads

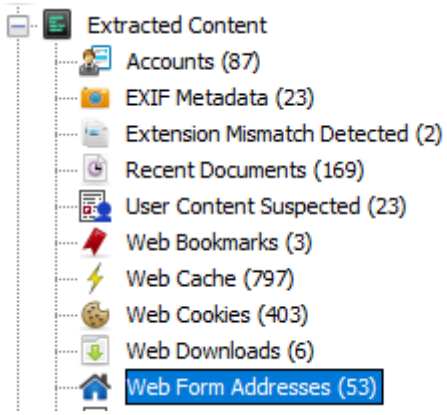


Step 3. Choose a web download to investigate

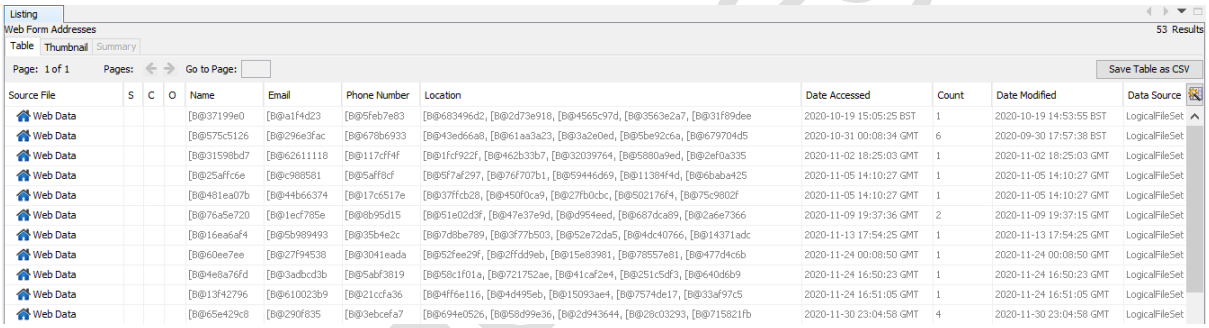


Web Form Addresses

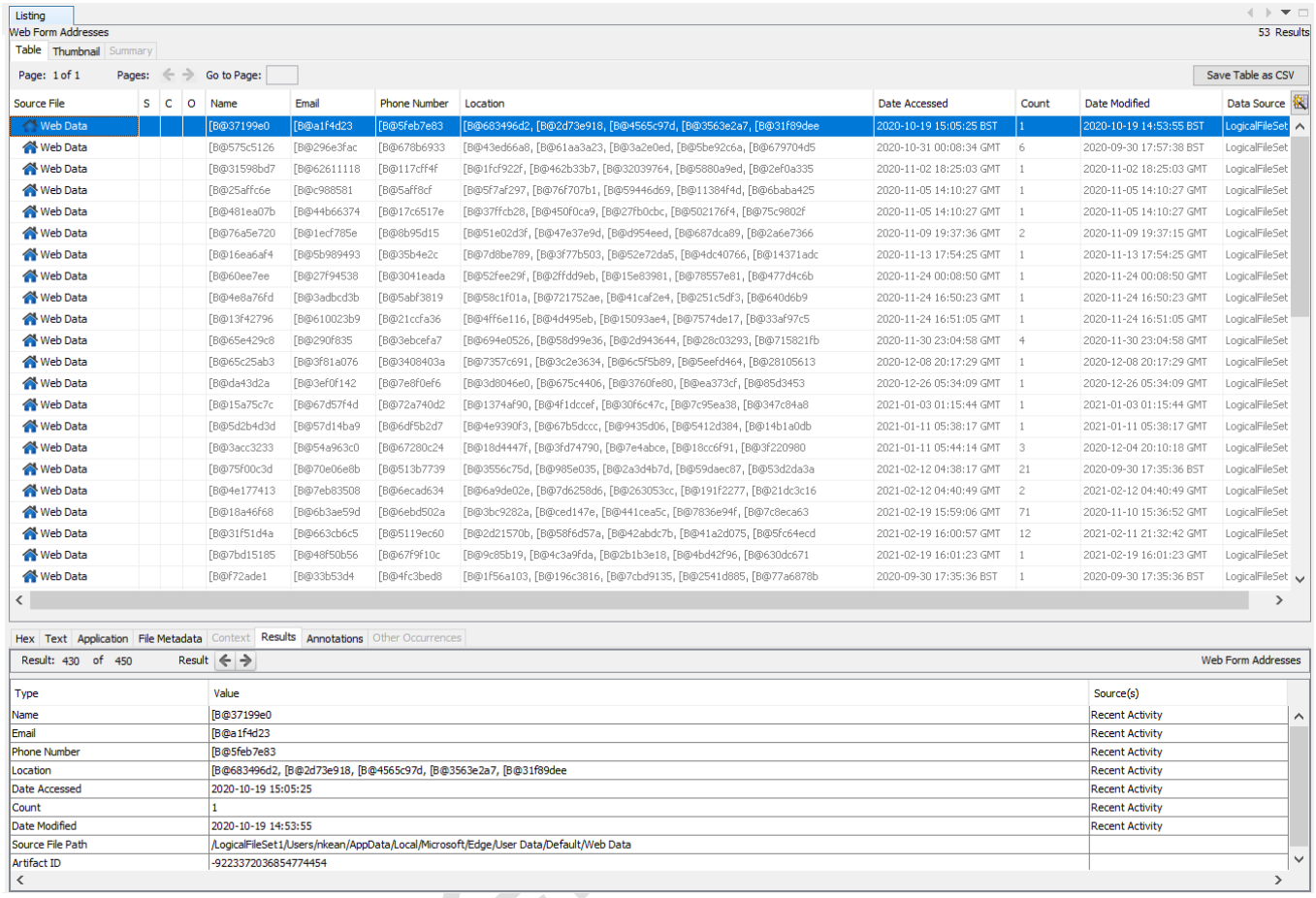
Step 1. Navigate to Web Form Addresses



Step 2. Examine the contents of web form addresses



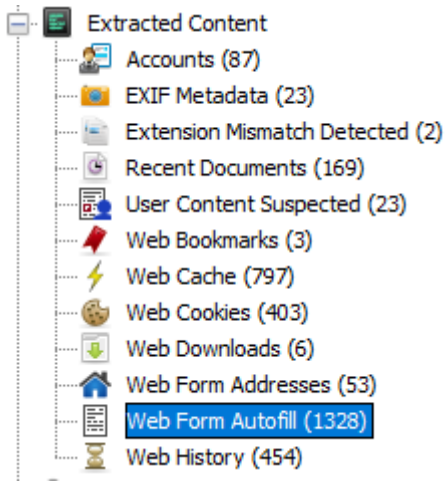
Step 3. Choose a web form address to investigate



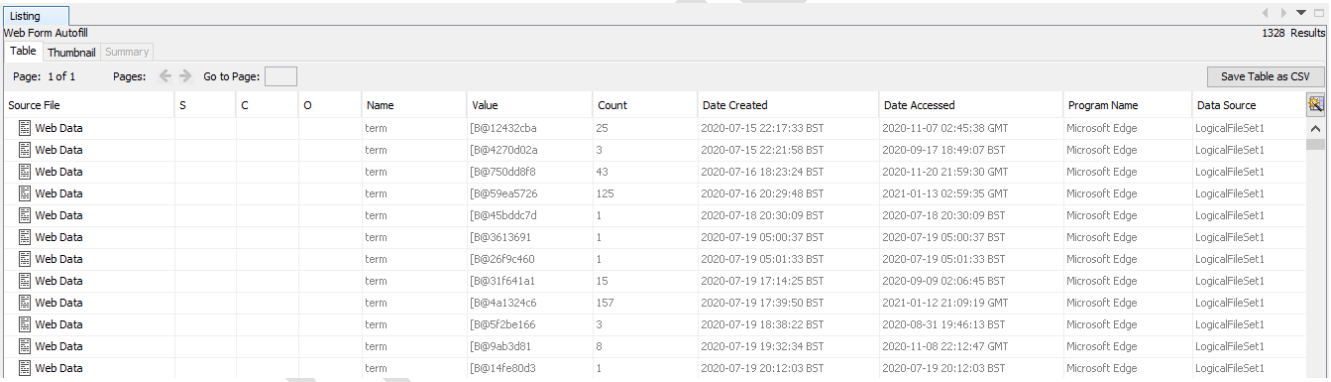
Q. What do you think these web form addresses show us?

Web form Autofill

Step 1. Navigate to web form autofill

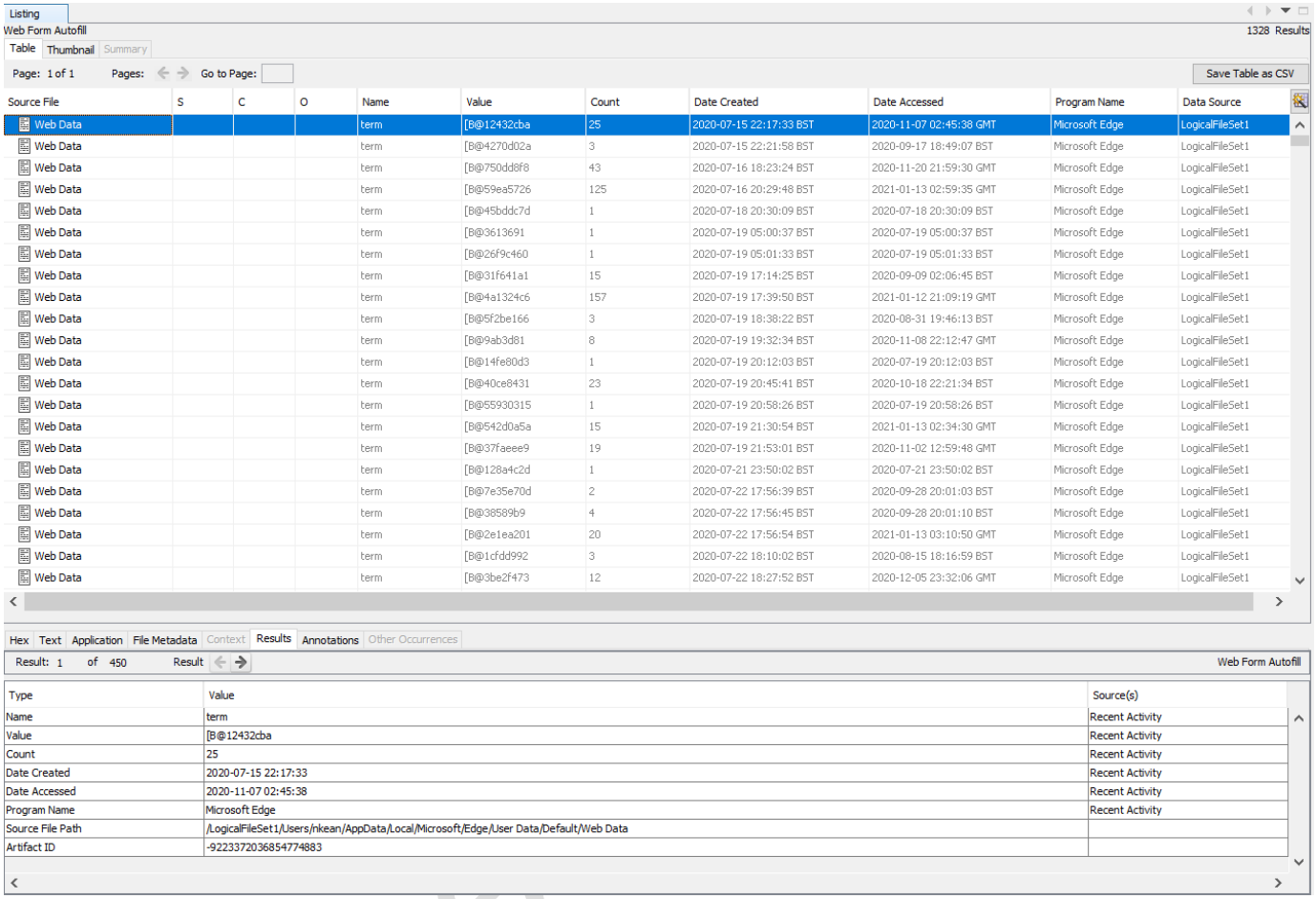


Step 2. Examine the contents of web form autofill



Source File	S	C	O	Name	Value	Count	Date Created	Date Accessed	Program Name	Data Source
Web Data				term	[B@12432cba	25	2020-07-15 22:17:33 BST	2020-11-07 02:45:38 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@4270d02a	3	2020-07-15 22:21:58 BST	2020-09-17 18:49:07 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@750dd8f8	43	2020-07-16 18:23:24 BST	2020-11-20 21:59:30 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@59ea5726	125	2020-07-16 20:29:48 BST	2021-01-13 02:59:35 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@45bddc7d	1	2020-07-18 20:30:09 BST	2020-07-18 20:30:09 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@3613691	1	2020-07-19 05:00:37 BST	2020-07-19 05:00:37 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@26f9c460	1	2020-07-19 05:01:33 BST	2020-07-19 05:01:33 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@31f641a1	15	2020-07-19 17:14:25 BST	2020-09-09 02:06:45 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@4a1324c6	157	2020-07-19 17:39:50 BST	2021-01-12 21:09:19 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@5f2be166	3	2020-07-19 18:38:22 BST	2020-08-31 19:46:13 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@9ab3d81	8	2020-07-19 19:32:34 BST	2020-11-08 22:12:47 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@14fe80d3	1	2020-07-19 20:12:03 BST	2020-07-19 20:12:03 BST	Microsoft Edge	LogicalFileSet1

Step 3. Choose a web form autofill to investigate



Listing

Web Form Autofill — 1328 Results

Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Source File	S	C	O	Name	Value	Count	Date Created	Date Accessed	Program Name	Data Source
Web Data				term	[B@12432cba	25	2020-07-15 22:17:33 BST	2020-11-07 02:45:38 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@4270d02a	3	2020-07-15 22:21:58 BST	2020-09-17 18:49:07 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@750dd8f8	43	2020-07-16 18:23:24 BST	2020-11-20 21:59:30 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@59ea5726	125	2020-07-16 20:29:48 BST	2021-01-13 02:59:35 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@45bddc7d	1	2020-07-18 20:30:09 BST	2020-07-18 20:30:09 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@3613691	1	2020-07-19 05:00:37 BST	2020-07-19 05:00:37 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@26f9c460	1	2020-07-19 05:01:33 BST	2020-07-19 05:01:33 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@31f641a1	15	2020-07-19 17:14:25 BST	2020-09-09 02:06:45 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@4a1324c6	157	2020-07-19 17:39:50 BST	2021-01-12 21:09:19 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@5f2be166	3	2020-07-19 18:38:22 BST	2020-08-31 19:46:13 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@9ab3d81	8	2020-07-19 19:32:34 BST	2020-11-08 22:12:47 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@14fe80d3	1	2020-07-19 20:12:03 BST	2020-07-19 20:12:03 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@40ce8431	23	2020-07-19 20:45:41 BST	2020-10-18 22:21:34 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@55930315	1	2020-07-19 20:58:26 BST	2020-07-19 20:58:26 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@542d0a5a	15	2020-07-19 21:30:54 BST	2021-01-13 02:34:30 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@37faeee9	19	2020-07-19 21:53:01 BST	2020-11-02 12:59:48 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@128a4c2d	1	2020-07-21 23:50:02 BST	2020-07-21 23:50:02 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@7e35e70d	2	2020-07-22 17:56:39 BST	2020-09-28 20:01:03 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@38589b9	4	2020-07-22 17:56:45 BST	2020-09-28 20:01:10 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@2e1ea201	20	2020-07-22 17:56:54 BST	2021-01-13 03:10:50 GMT	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@1cfdd992	3	2020-07-22 18:10:02 BST	2020-08-15 18:16:59 BST	Microsoft Edge	LogicalFileSet1
Web Data				term	[B@3be2f473	12	2020-07-22 18:27:52 BST	2020-12-05 23:32:06 GMT	Microsoft Edge	LogicalFileSet1

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

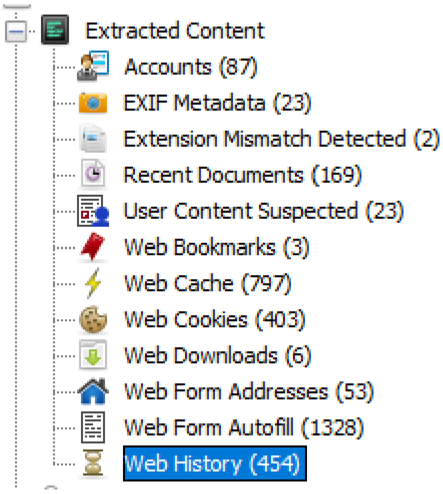
Result: 1 of 450 Result — Web Form Autofill

Type	Value	Source(s)
Name	term	Recent Activity
Value	[B@12432cba	Recent Activity
Count	25	Recent Activity
Date Created	2020-07-15 22:17:33	Recent Activity
Date Accessed	2020-11-07 02:45:38	Recent Activity
Program Name	Microsoft Edge	Recent Activity
Source File Path	/LogicalFileSet1/Users/nkean/AppData/Local/Microsoft/Edge/User Data/Default/Web Data	
Artifact ID	-9223372036854774883	

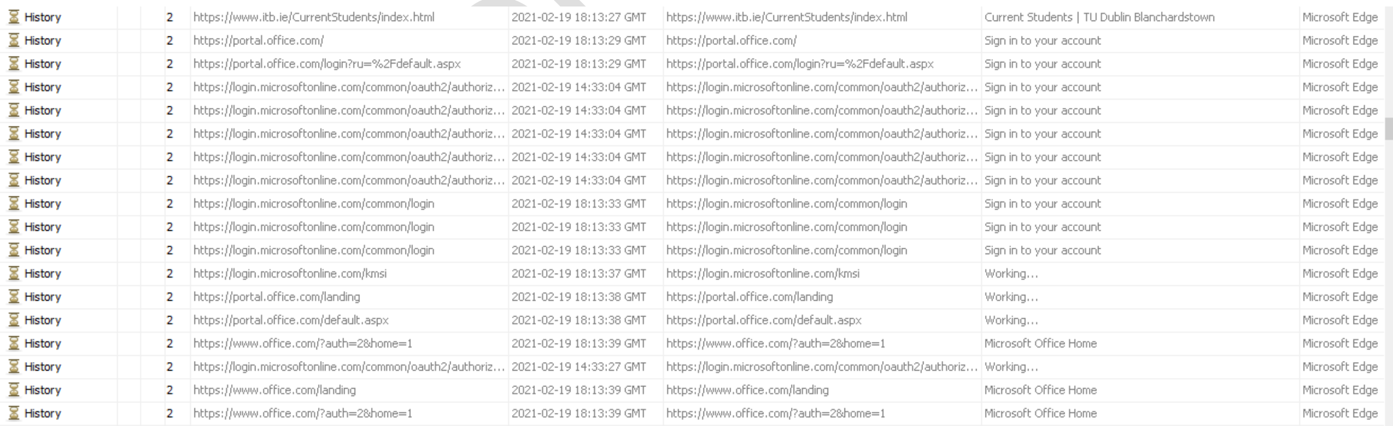
Q. What can we learn from these web form autofill's?

Web History

Step 1. Next is the interesting one... navigate to web history. This is often the first thing checked depending on the investigation.

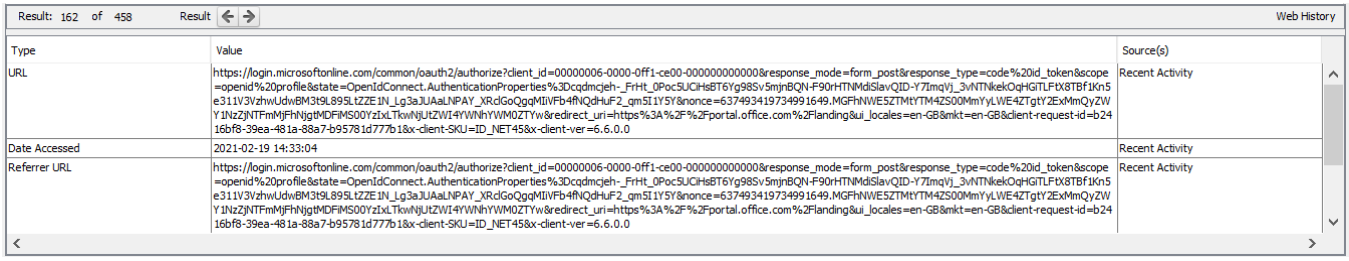


Step 2. Examine the contents of the web history



History		2	https://www.itb.ie/CurrentStudents/index.html	2021-02-19 18:13:27 GMT	https://www.itb.ie/CurrentStudents/index.html	Current Students | TU Dublin Blanchardstown	Microsoft Edge
History		2	https://portal.office.com/	2021-02-19 18:13:29 GMT	https://portal.office.com/	Sign in to your account	Microsoft Edge
History		2	https://portal.office.com/login?ru=%2Fdefault.aspx	2021-02-19 18:13:29 GMT	https://portal.office.com/login?ru=%2Fdefault.aspx	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:04 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:04 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:04 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:04 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:04 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/login	2021-02-19 18:13:33 GMT	https://login.microsoftonline.com/common/login	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/login	2021-02-19 18:13:33 GMT	https://login.microsoftonline.com/common/login	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/common/login	2021-02-19 18:13:33 GMT	https://login.microsoftonline.com/common/login	Sign in to your account	Microsoft Edge
History		2	https://login.microsoftonline.com/kmsi	2021-02-19 18:13:37 GMT	https://login.microsoftonline.com/kmsi	Working...	Microsoft Edge
History		2	https://portal.office.com/landing	2021-02-19 18:13:38 GMT	https://portal.office.com/landing	Working...	Microsoft Edge
History		2	https://portal.office.com/default.aspx	2021-02-19 18:13:38 GMT	https://portal.office.com/default.aspx	Working...	Microsoft Edge
History		2	https://www.office.com/?auth=2&home=1	2021-02-19 18:13:39 GMT	https://www.office.com/?auth=2&home=1	Microsoft Office Home	Microsoft Edge
History		2	https://login.microsoftonline.com/common/oauth2/authoriz...	2021-02-19 14:33:27 GMT	https://login.microsoftonline.com/common/oauth2/authoriz...	Working...	Microsoft Edge
History		2	https://www.office.com/landing	2021-02-19 18:13:39 GMT	https://www.office.com/landing	Microsoft Office Home	Microsoft Edge
History		2	https://www.office.com/?auth=2&home=1	2021-02-19 18:13:39 GMT	https://www.office.com/?auth=2&home=1	Microsoft Office Home	Microsoft Edge

Step 3. Choose one of the history options and investigate the findings



Result: 162 of 458 Result Web History

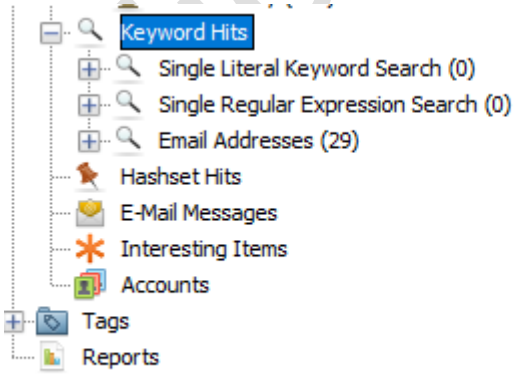
Type	Value	Source(s)
URL	https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3Dcqdmcjeh-_FrHt_0Poc5UCiHsBT6Yg98Sv5mjnBQN-F90rHTNMdiSlavQID-Y7ImqVj_3vNTNkekOqHGiTLFtX8TBf1Kn5e311V3VzhwUdwBM3t9L895LtZZE1N_Lg3aJUAaLNPAY_XRclGoQgqMIiVFb4fNQdHuF2_qm5I1Y5Y&nonce=637493419734991649.MGFhNWE5ZTMtYTM4ZS00MmYyLWE4ZTgtY2ExMmQyZWY1NzZjNTFmMjFhNjgtMDFiMS00YzIxLTkwNjUtZWI4YWNhYWM0ZTYw&redirect_uri=https%3A%2F%2Fportal.office.com%2Flanding&ui_locales=en-GB&mkt=en-GB&client-request-id=b2416bf8-39ea-481a-88a7-b95781d777b1&x-client-SKU=ID_NET45&x-client-ver=6.6.0.0	Recent Activity
Date Accessed	2021-02-19 14:33:04	Recent Activity
Referrer URL	https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code%20id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3Dcqdmcjeh-_FrHt_0Poc5UCiHsBT6Yg98Sv5mjnBQN-F90rHTNMdiSlavQID-Y7ImqVj_3vNTNkekOqHGiTLFtX8TBf1Kn5e311V3VzhwUdwBM3t9L895LtZZE1N_Lg3aJUAaLNPAY_XRclGoQgqMIiVFb4fNQdHuF2_qm5I1Y5Y&nonce=637493419734991649.MGFhNWE5ZTMtYTM4ZS00MmYyLWE4ZTgtY2ExMmQyZWY1NzZjNTFmMjFhNjgtMDFiMS00YzIxLTkwNjUtZWI4YWNhYWM0ZTYw&redirect_uri=https%3A%2F%2Fportal.office.com%2Flanding&ui_locales=en-GB&mkt=en-GB&client-request-id=b2416bf8-39ea-481a-88a7-b95781d777b1&x-client-SKU=ID_NET45&x-client-ver=6.6.0.0	Recent Activity

Q. Can you determine what the above history is in relation to?

Interesting findings

Emails

The following screenshot shows the interesting findings section, these are often findings populated by the investigator themselves, such as a generated report.



Step 1. Visit email addresses.

Email Addresses (29)

Step 2. Examine the contents of email addresses

(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4} (29)

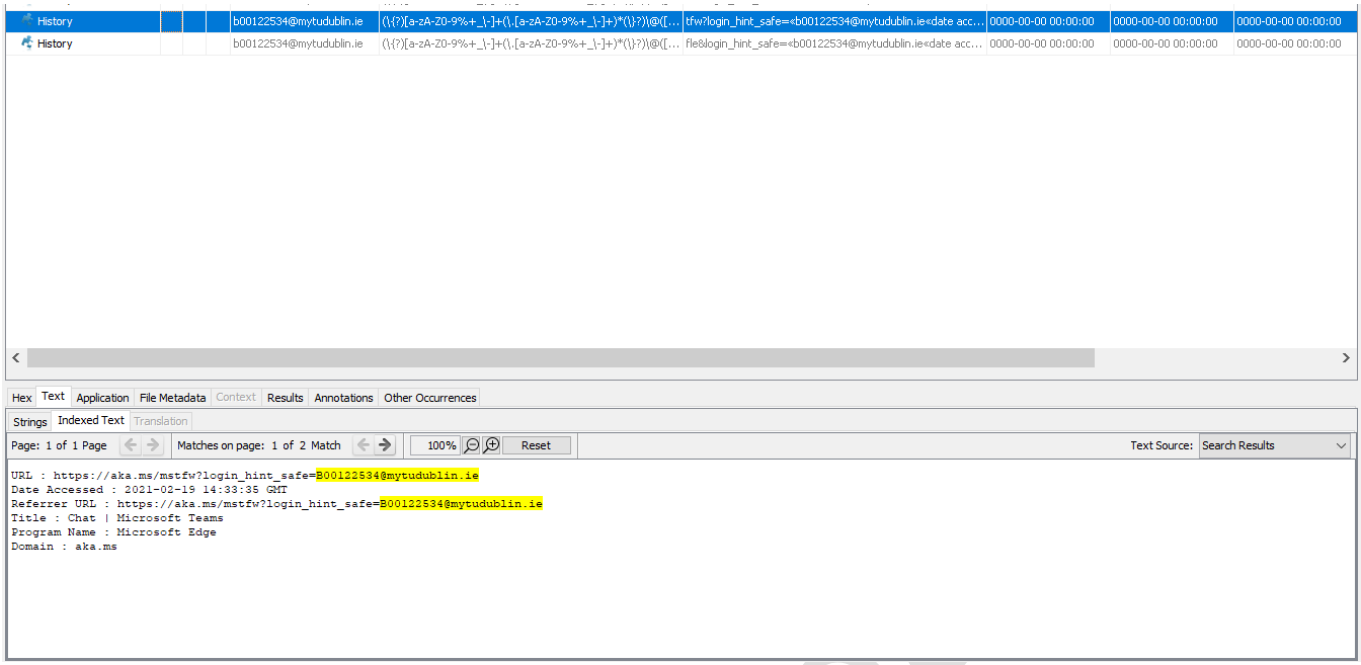
Step 3. If you investigate further, you will find emails associated with the system

534@mytudublin.ie (9)

Step 4. Further investigation of the email address returns the following information

0			2	b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	coveryemail" value="«b00122534@mytudublin.ie«"/34) inp…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	fle&login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
MEMORY.DMP			1	b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	a_scopewa_username«b00122534@mytudublin.ie«vi01fmf…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	tfw?login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	fle&login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	fle&login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	fle&login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	tfw?login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History				b00122534@mytudublin.ie	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([…	fle&login_hint_safe=«b00122534@mytudublin.ie«date acc…	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

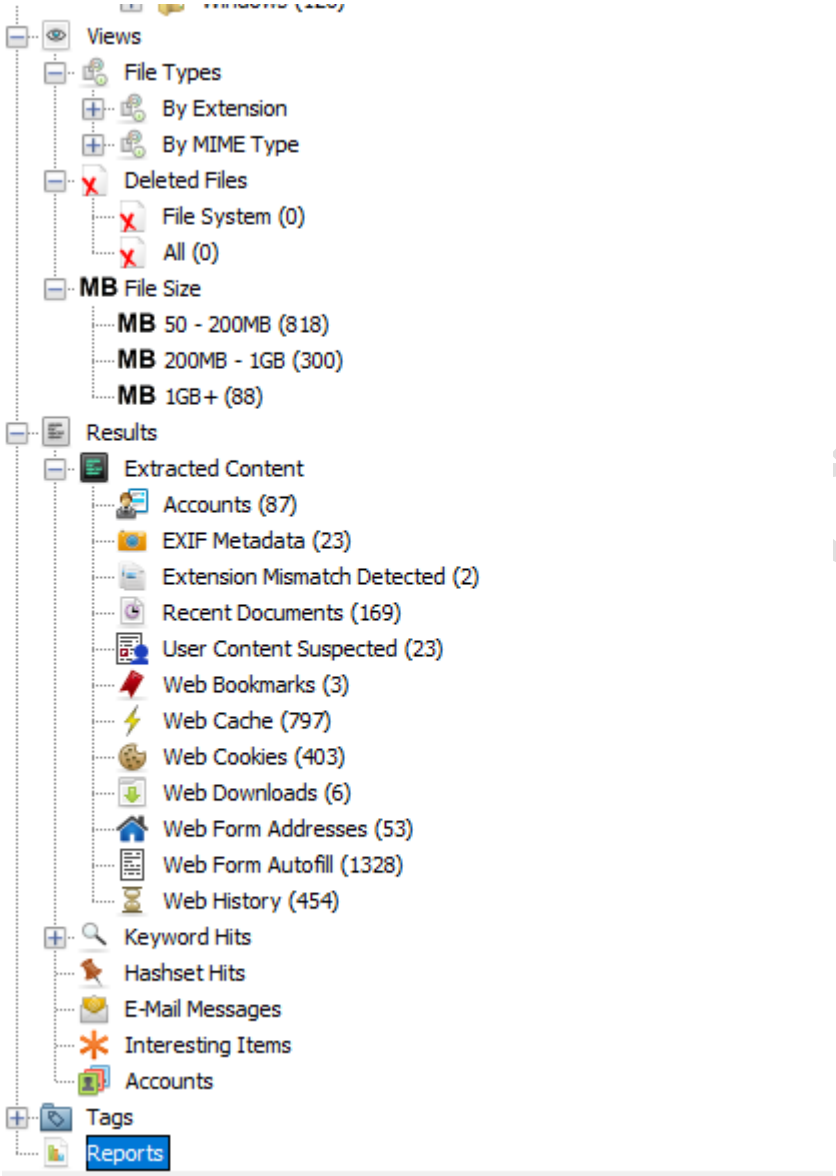
Step 5. Choose one of the files associated with the email you chose to examine. Investigate this file.



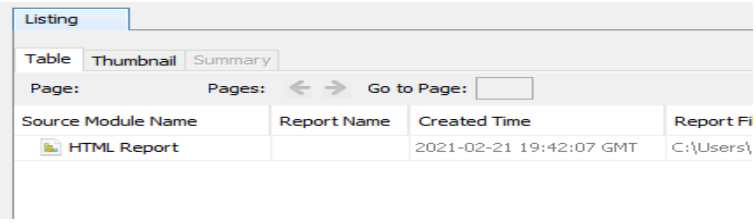
Q. Is this a sign of communication between the email address given? If so, what was the program used for this communication?

Reports

Step 1. Navigate to the reports section



Step 2. View the contents of reports which was populated at the start of the lab.

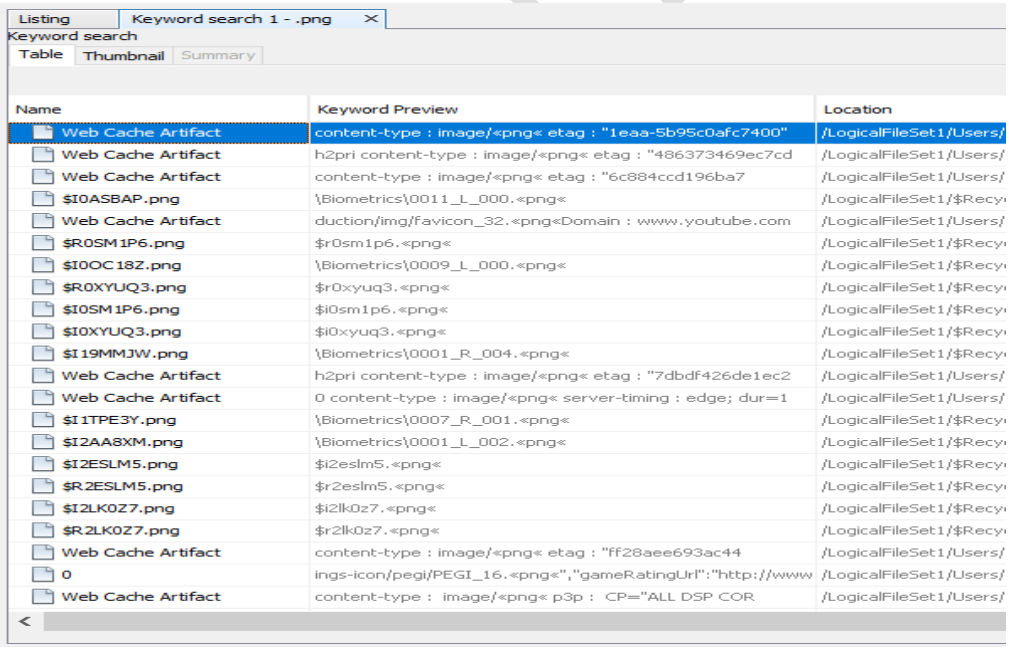


Step 3. Right click the file to open the report

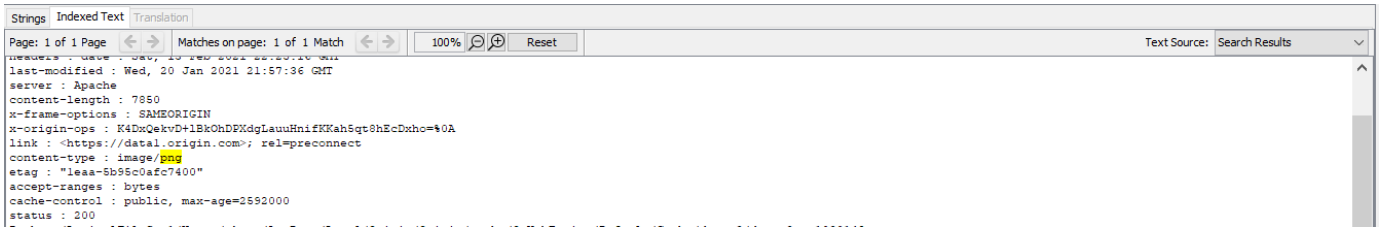
Step 4. Select any text editor such as notepad ++ to view the contents.

Keyword hits

Step 1. Based on the tools learned about earlier in the tools section, the keywords that hit a finding will return to the findings section under “keywords hit”



Step 2. Investigate the contents of one of the files



Q. Based on the above screenshots can you determine the keyword used to get these results?

References

Autopsy. (2021). Autopsy | Digital Forensics. [online] Available at: https://www.autopsy.com/.