



Digital Forensics

Using Autopsy to

Analyse the

Contents of a Laptop

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Contents

Introduction	3
Imaging your own Laptop	4
Understanding the tools	20
Lab – Starting to load content	37
Lab – Examining Results	110
Interesting findings	128
Emails	128
Reports	131
Keyword hits	132

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

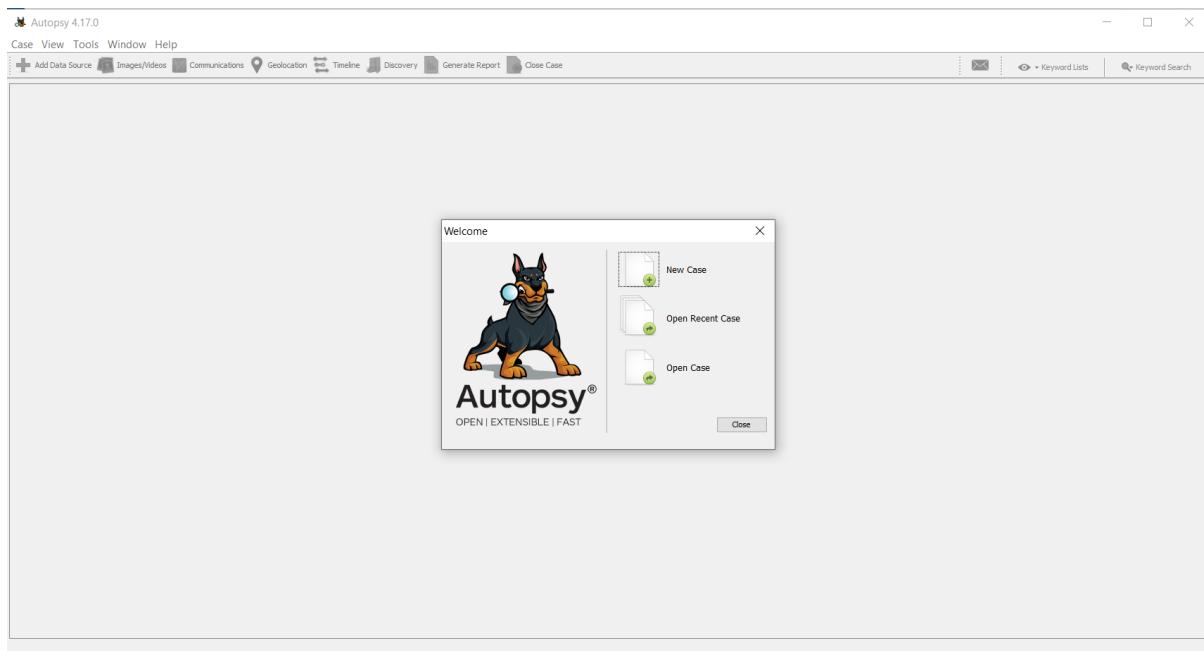
Autopsy serves as an excellent gateway into the world of digital forensics, offering users a versatile and adaptive learning experience. The completion of this lab allows participants to gain hands-on experience with the tool, learning how to identify and extract important files, directories, and information 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.

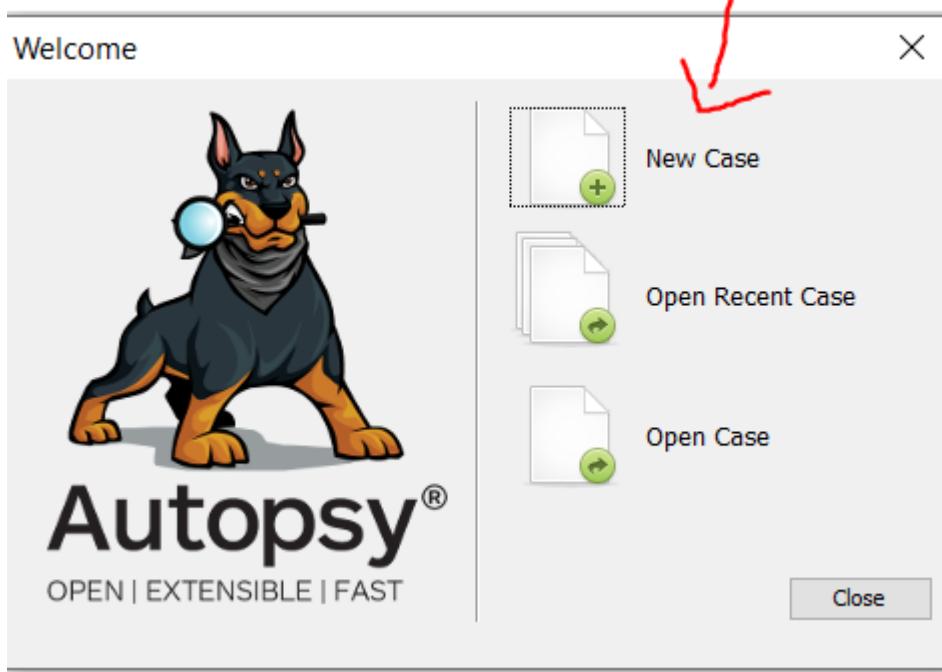
Imaging your own Laptop

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: MyLaptopA

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).

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: MichaelLaptop

Base Directory: C:\Users\Michael Hegarty\OneDrive - Technological University Dublin\Desktop\

Case Type: Single-User Multi-User

Case data will be stored in the following directory:
C:\Users\Michael Hegarty\OneDrive - Technological University Dublin\Desktop\MichaelLaptop

< Back

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.

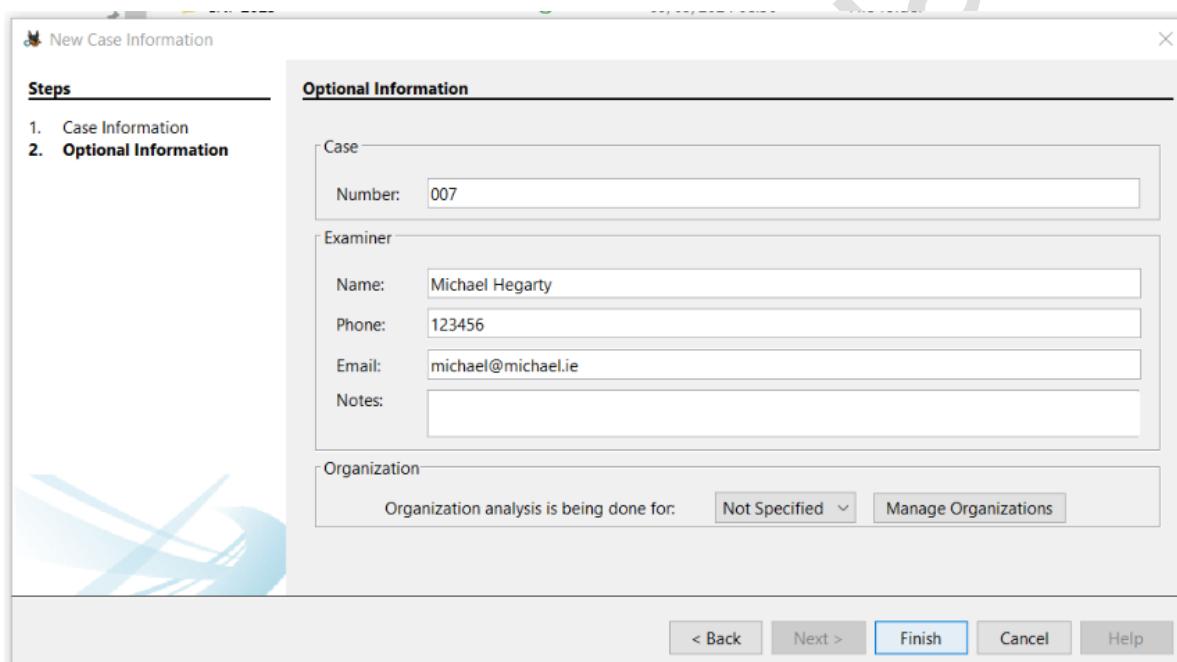
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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.*



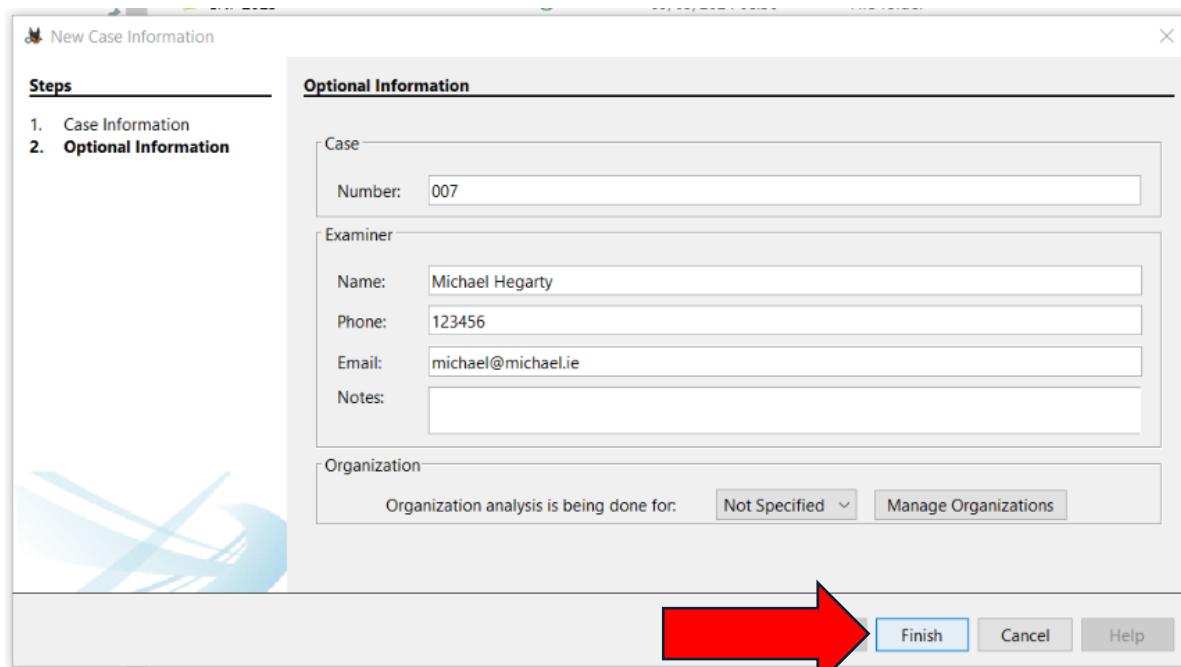
Step 9. Give the case an email address, once again for the sake of this lab, this can be a fake email to make the case more professional.

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”.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

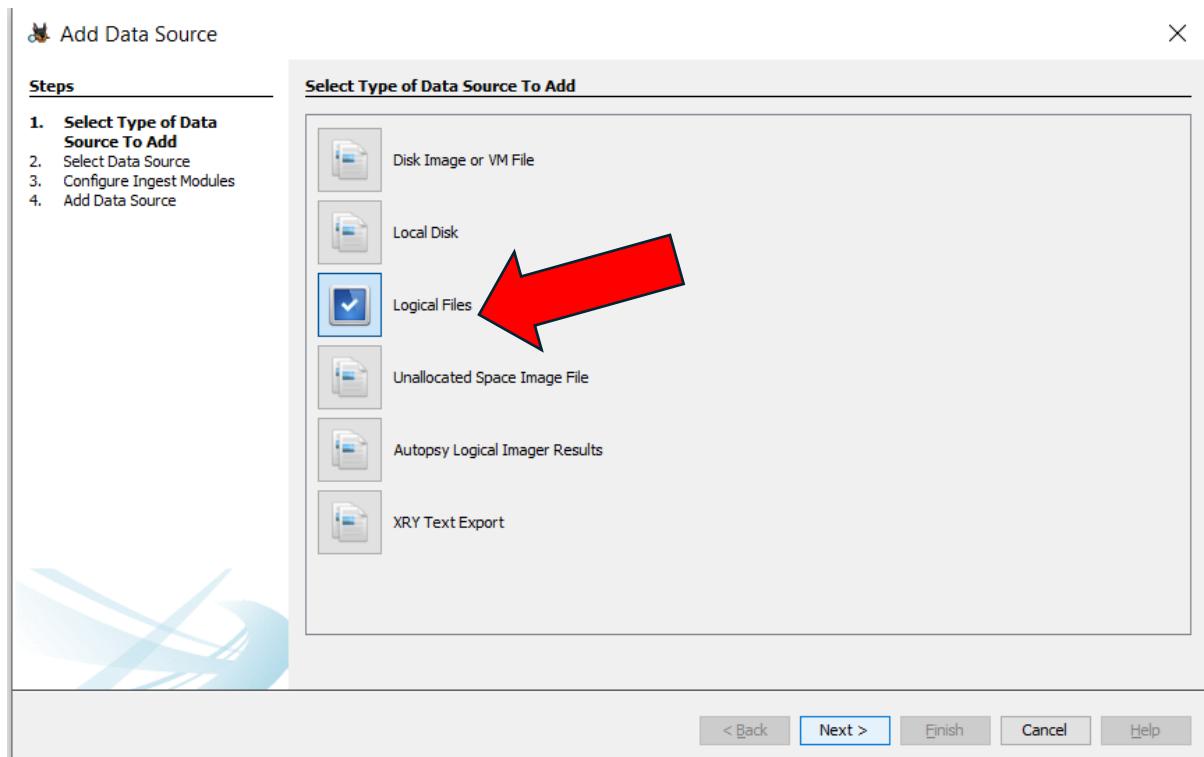
Step 10. Now click the finish button.



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.

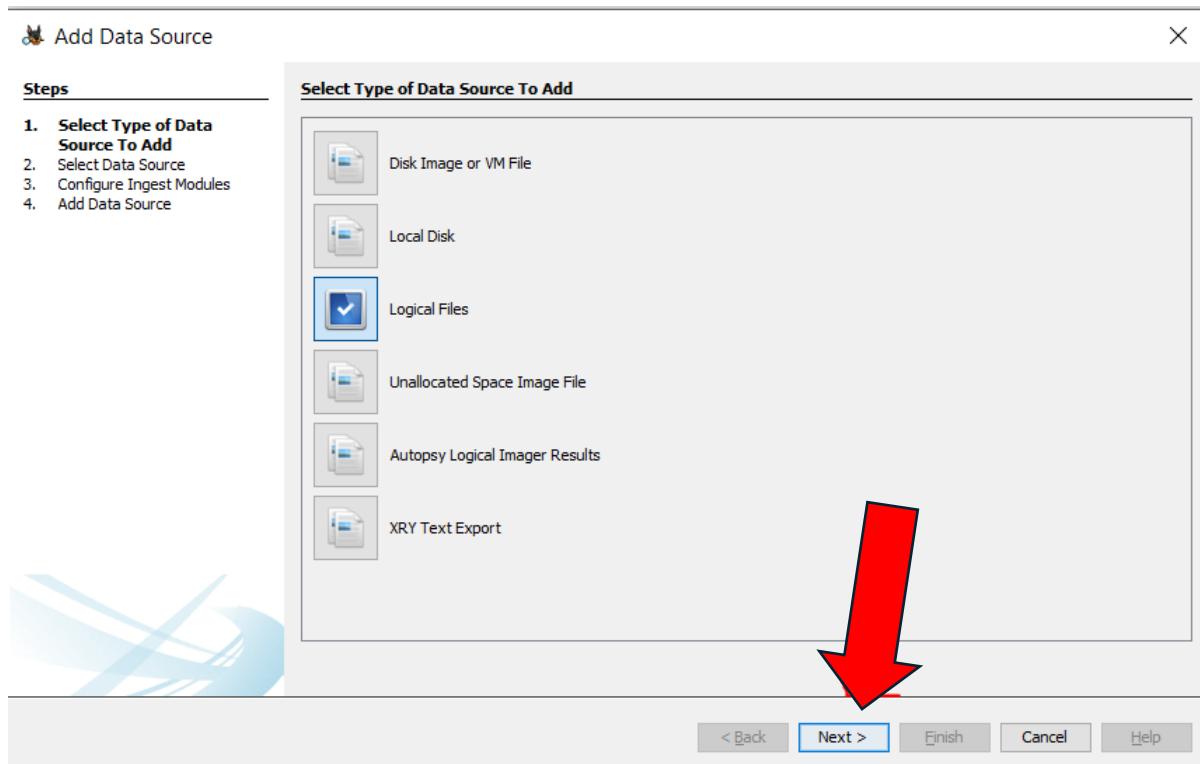
Note: *Although autopsy allows for a wide range of different data sources to be added*

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

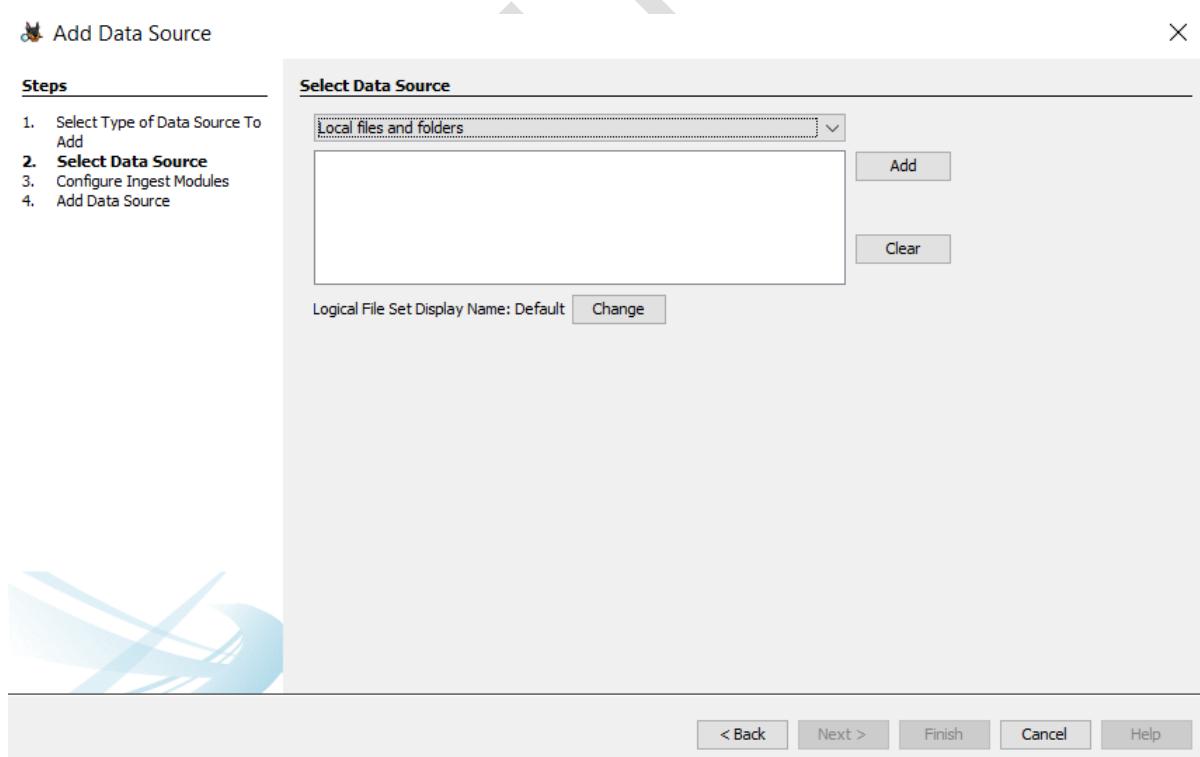


Step 12. Once selected, press the next button.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

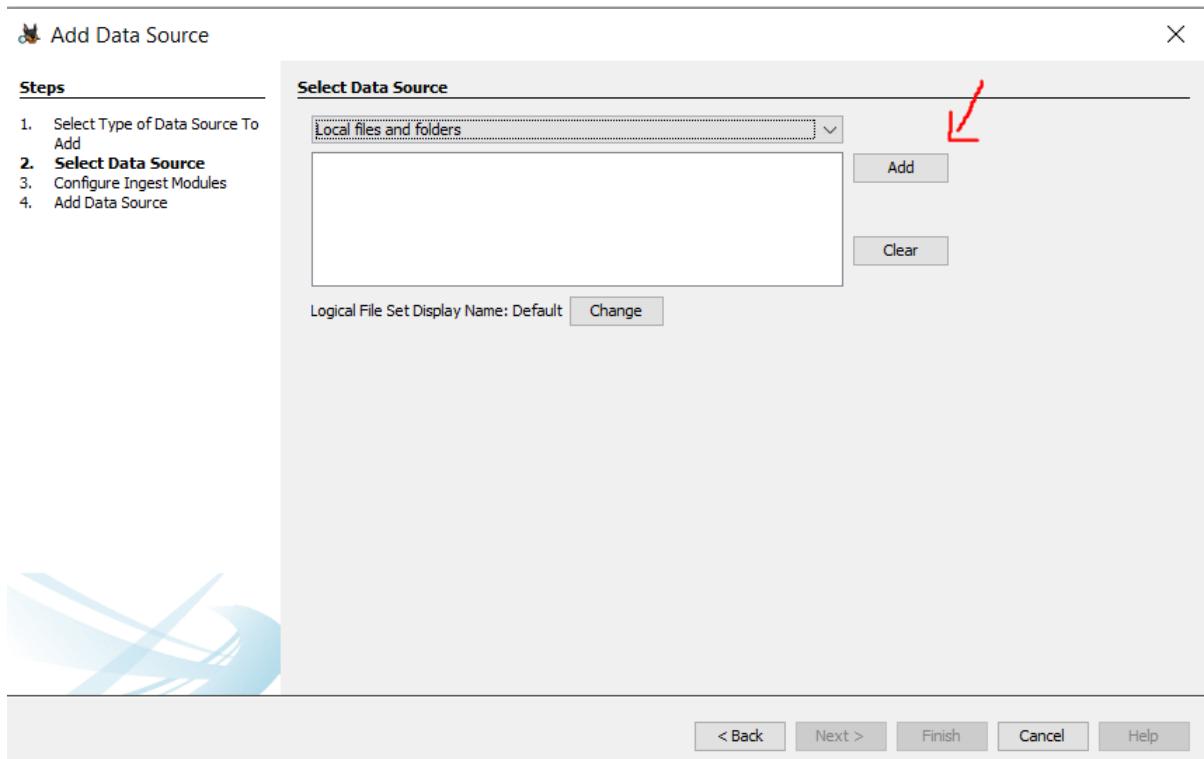


Step 13. Now you will see the following:



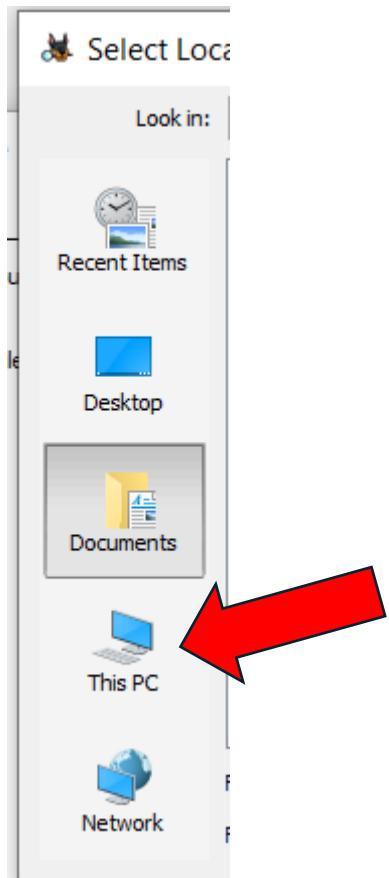
Step 14. Now that you see the select data sources section, please press on the add button to add a specific file or folder.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



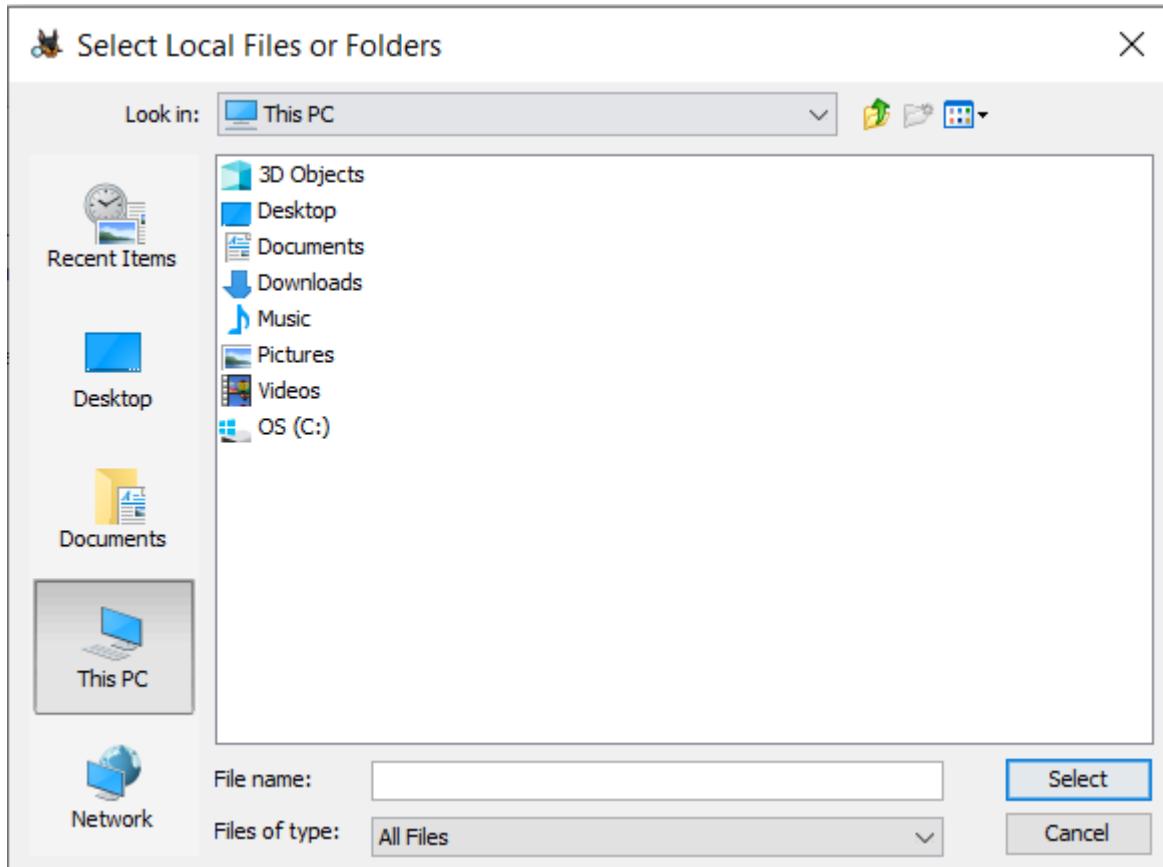
Step 15. Once selected, you will see a range of options

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



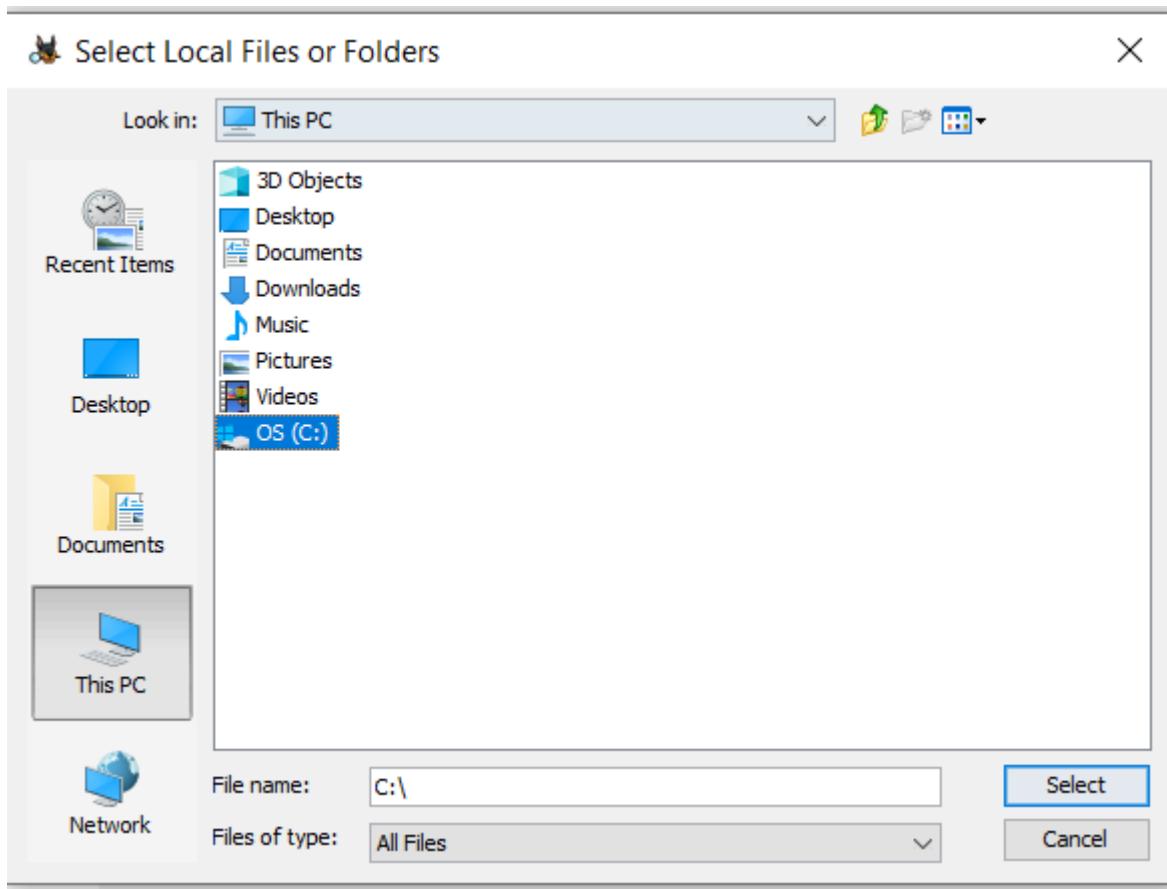
Step 16. I suggest you select “this pc”

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



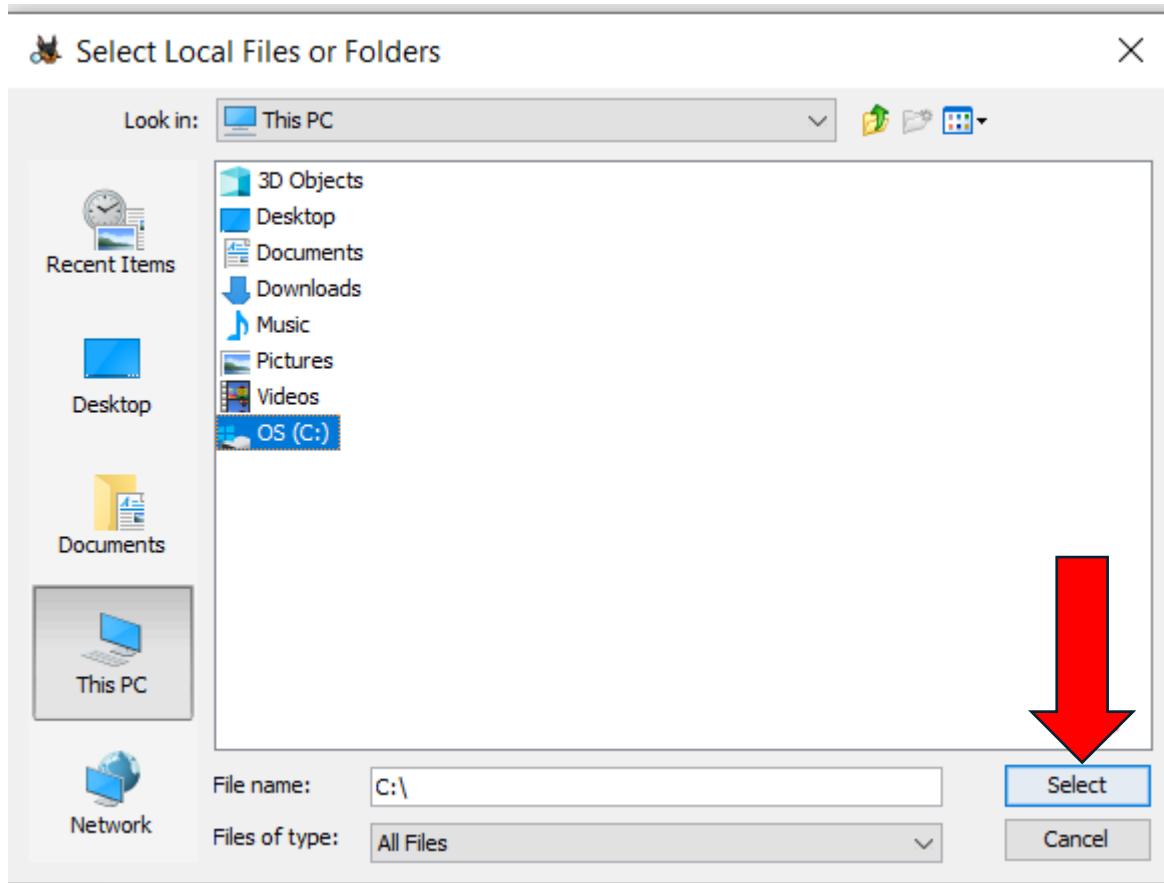
Step 17. Once inside the “this pc” option, you will see some basic directories, for this lab we will be using the OS (C:)

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



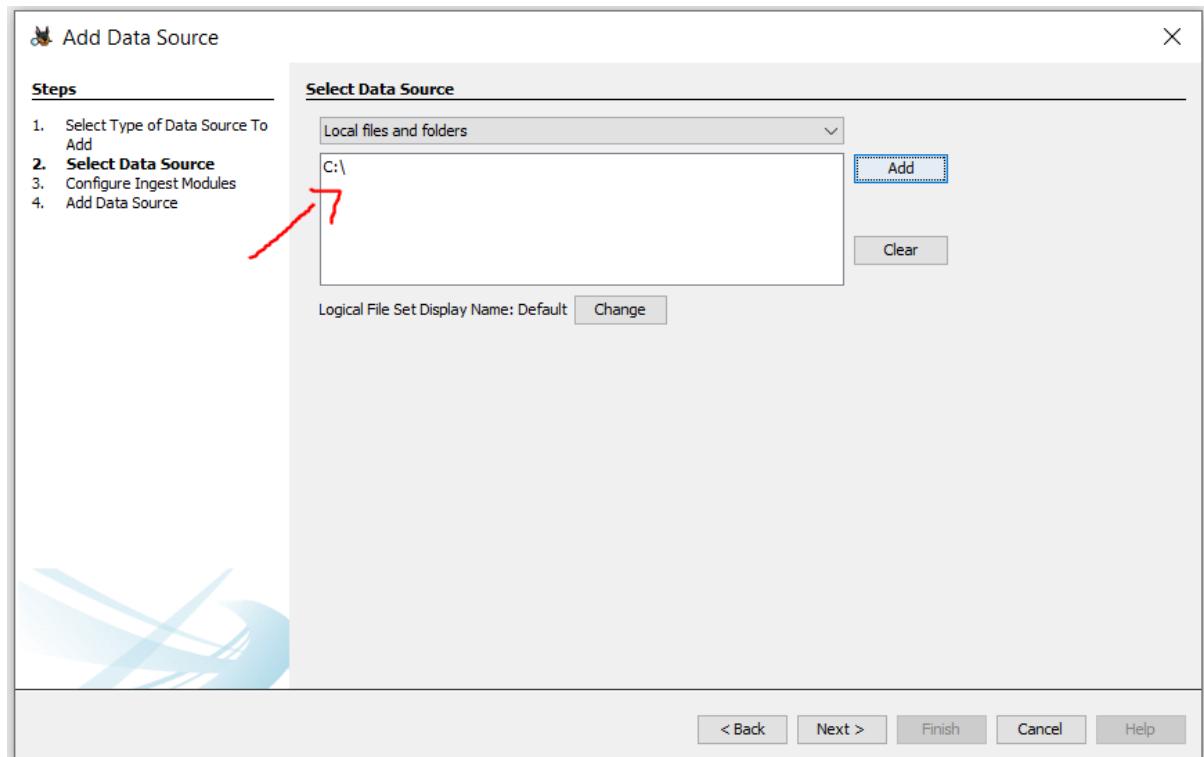
Step 18. Click select

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



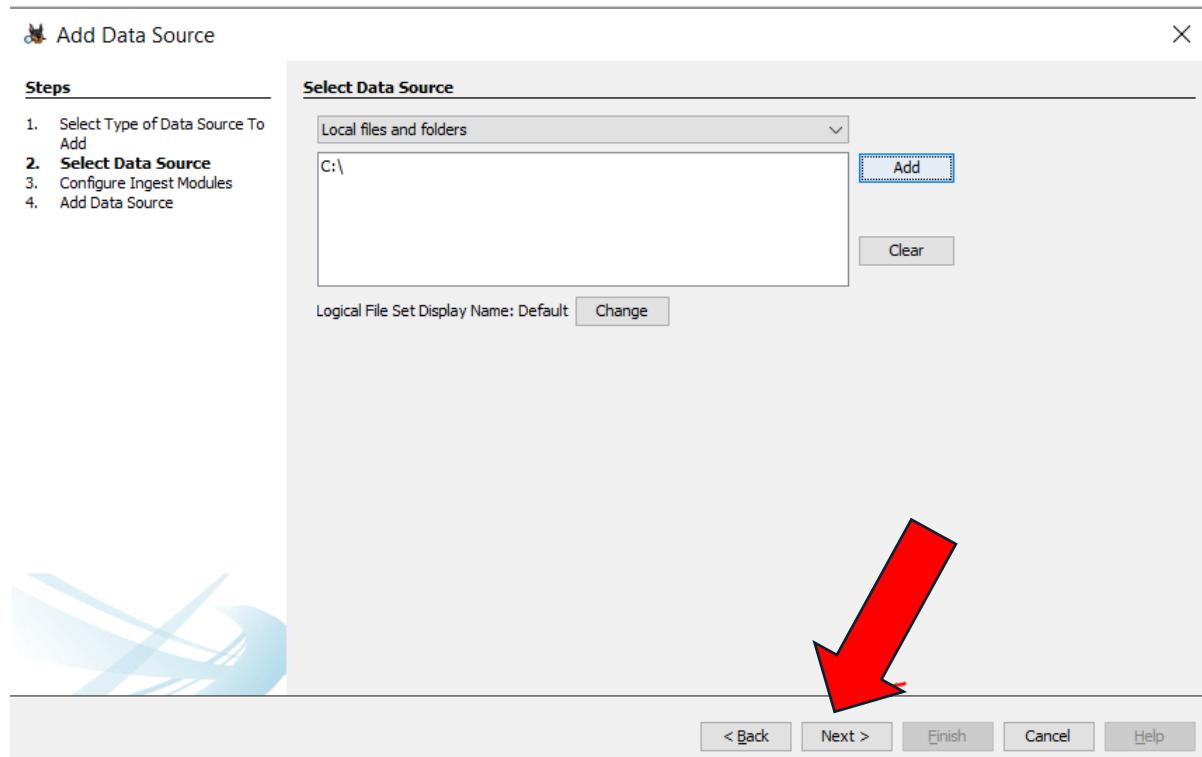
Step 19. You should now see the C:\ added to the chosen files and folders.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

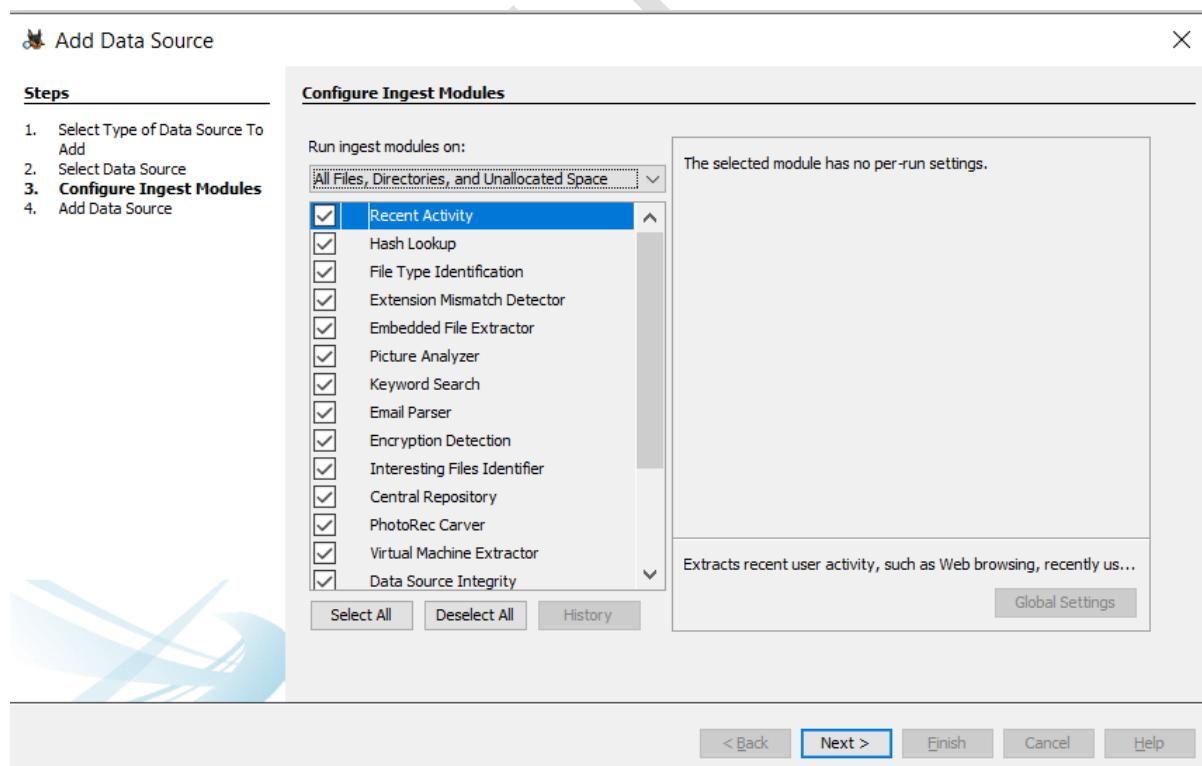


Step 20. If you want to you can add more files and folders to find more information, but for this lab the C:\ will provide more than enough data. Click the next button.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

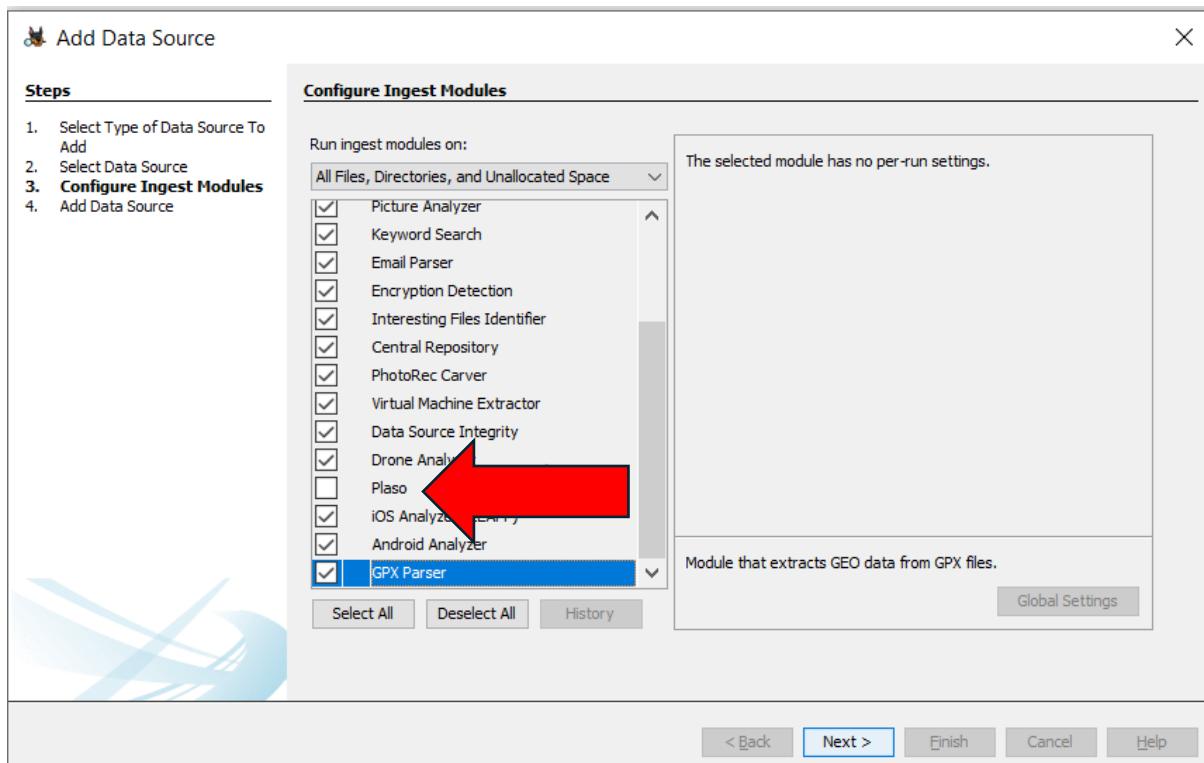
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

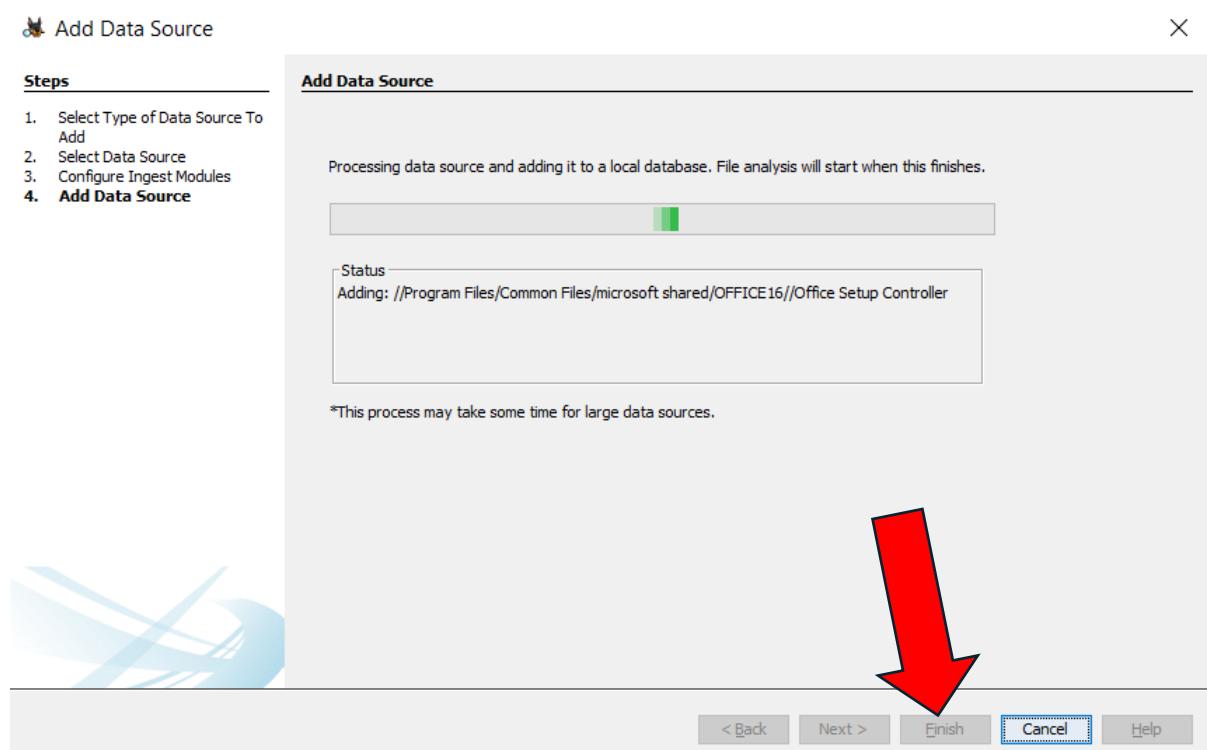
19. GPX Parser – Finds GEO data in GPX files and extracts it

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



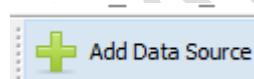
Understanding the tools

Step 1. Locate the tools at the top of Gui



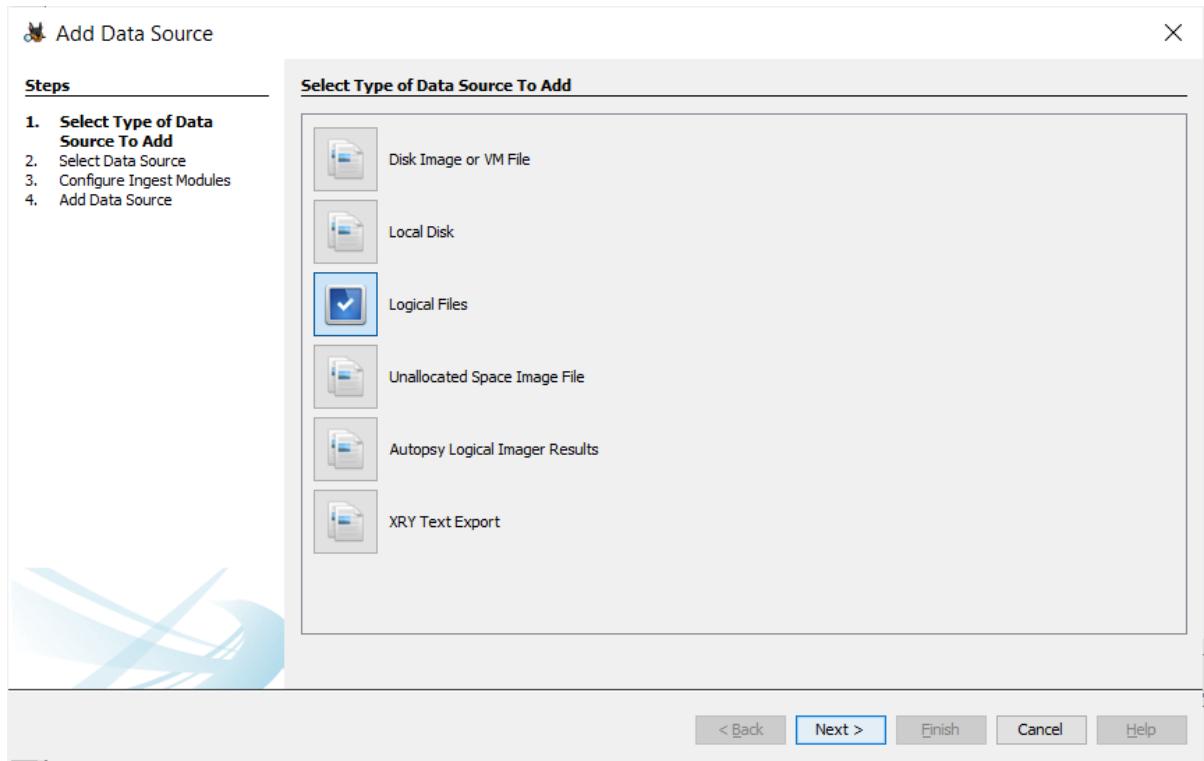
Add data source

Step 1. Navigate to the add data source



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

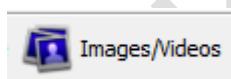
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

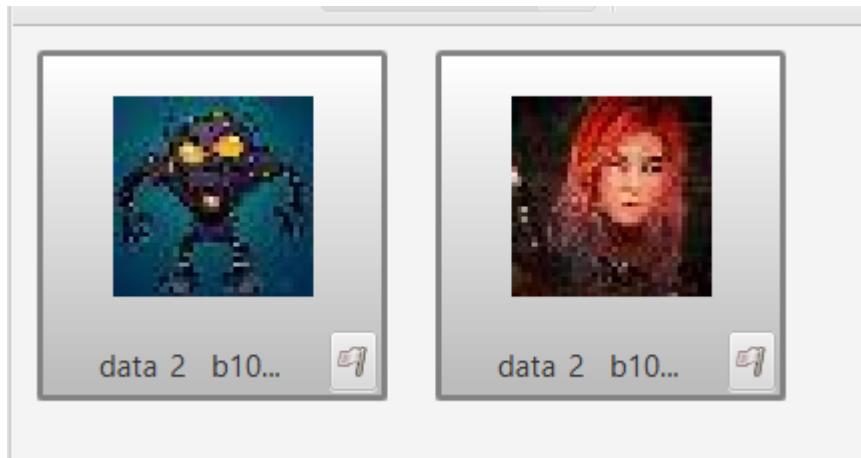
Images/videos

Step 1. Navigate to the images and videos tools



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

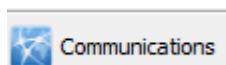
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.*

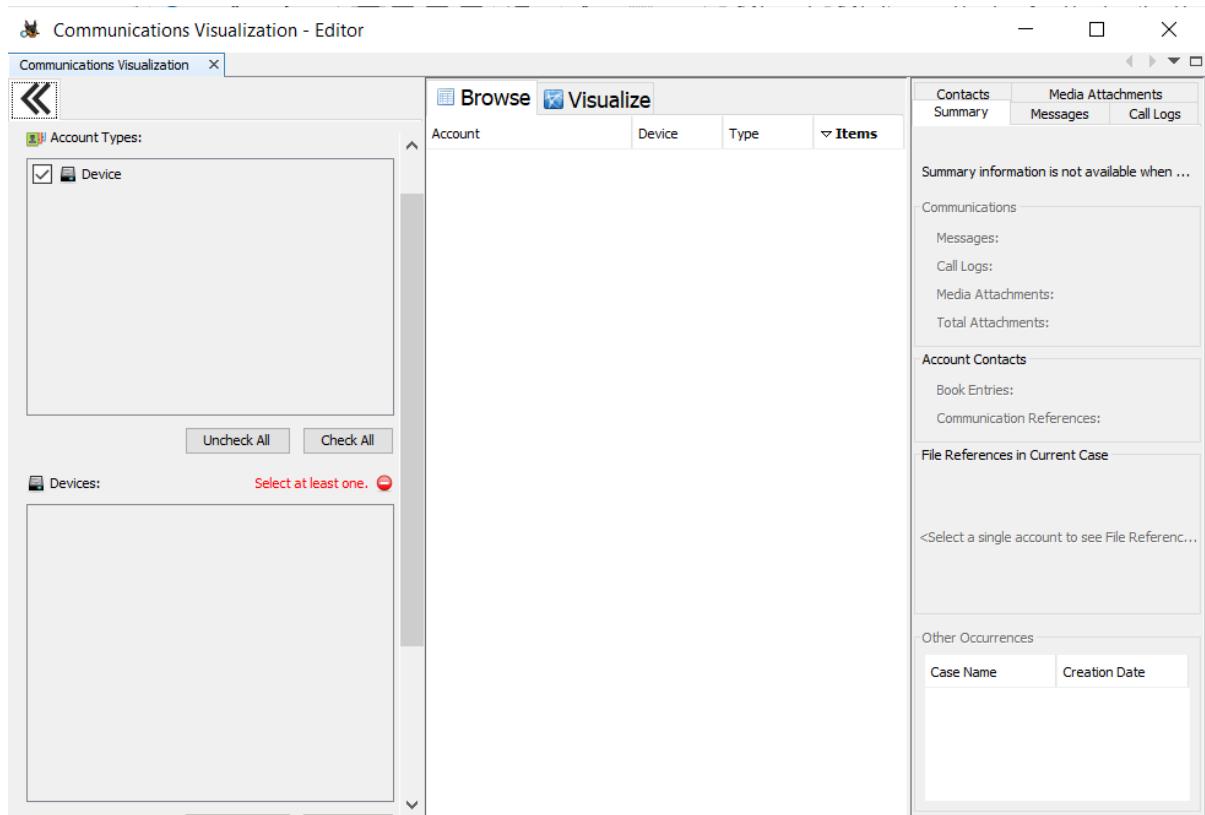
Communications

Step 1. Navigate to the communications tool



Step 2. Notice the GUI for the communications tool

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

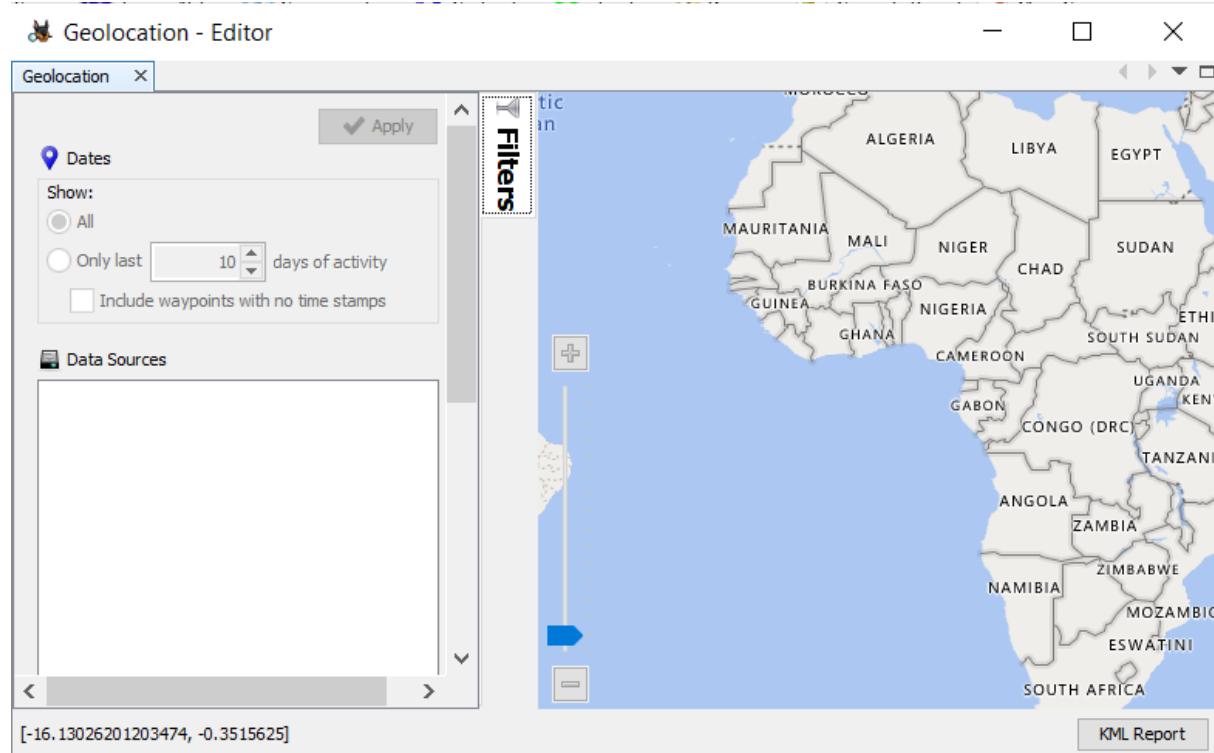
Geolocation

Step 1. Navigate to the geolocation tool



Step 2. Notice the Geolocations GUI.

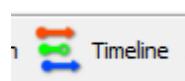
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

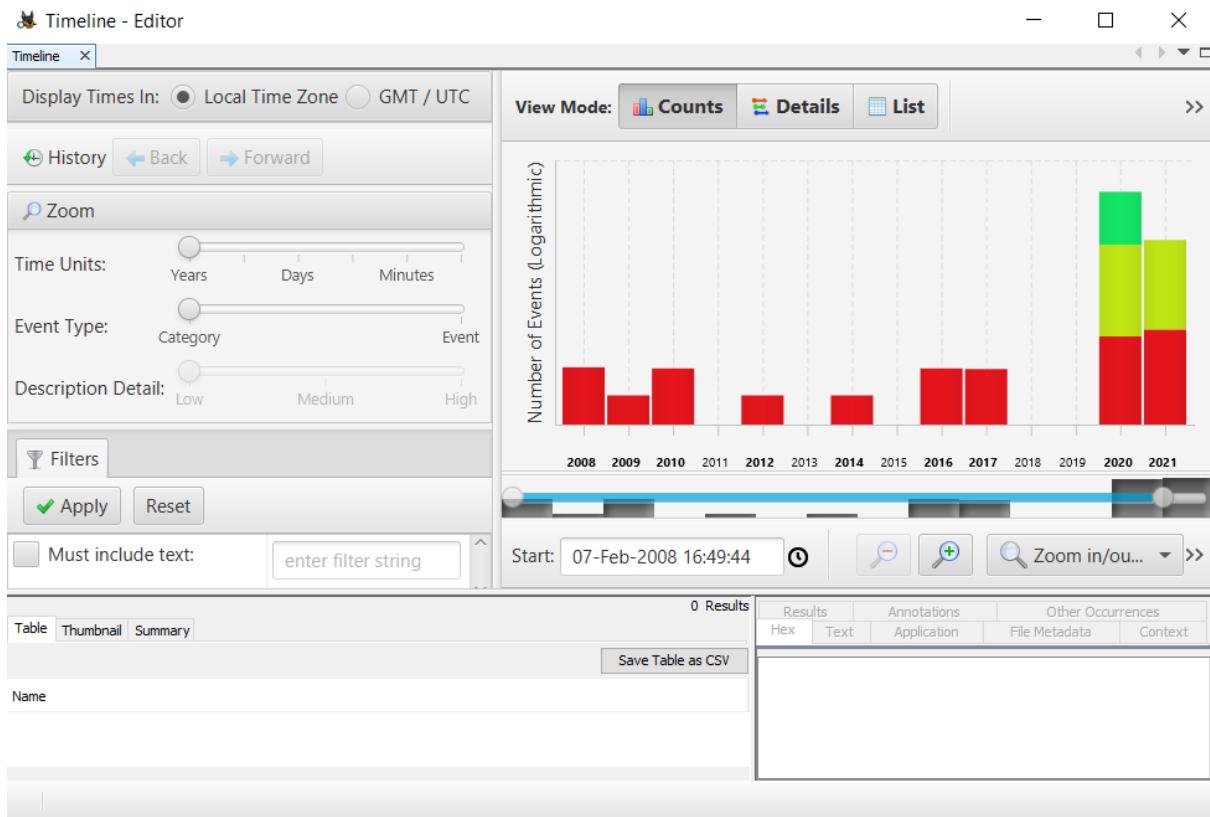
Timeline

Step 1. Navigate to the timeline tool



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

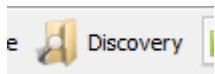
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the 'Discovery' module in Autopsy. It has three tabs at the top: 'Images' (selected), 'Videos', and 'Documents'. Below is 'Step 1: Choose result type' with four categories: 'Images', 'Videos', 'Documents', and 'Domains'. Under 'Step 2: Filter which images to show', there are several filter options:

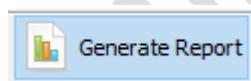
- File Size:** A dropdown menu with options: XSmall: 0-16KB, Small: 16-100KB, Medium: 100KB-1MB, Large: 1-50MB, XLarge: 50-200MB, and XXLarge: 200+MB. 'Large' is selected.
- Data Source:** A dropdown menu showing 'LogicalFileSet1 (ID: 1)'.
- Past Occurrences:** A dropdown menu with options: Known (NSRL), Very Common (100+), Common (11 - 100), Rare (2-10), and Unique (1). 'Common (11 - 100)' is selected.
- Filter Options:** Includes checkboxes for 'Possibly User Created', 'Hash Set', 'Interesting Item', 'Object Detected', and 'Parent Folder'. The 'Parent Folder' field contains '/Windows/ (substring) (exclude) /Program Files/ (substring) (exclude)'. Below it are radio buttons for 'Full', 'Substring', 'Include', and 'Exclude', with 'Include' selected. There are 'Delete' and 'Add' buttons.

Step 3: Choose display settings includes dropdown menus for 'Group By' (set to 'Parent Folder'), 'Order Within Groups By' (set to 'File Name'), and 'Order Groups By' (set to 'Group Size'). A 'Search' button is also present.

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

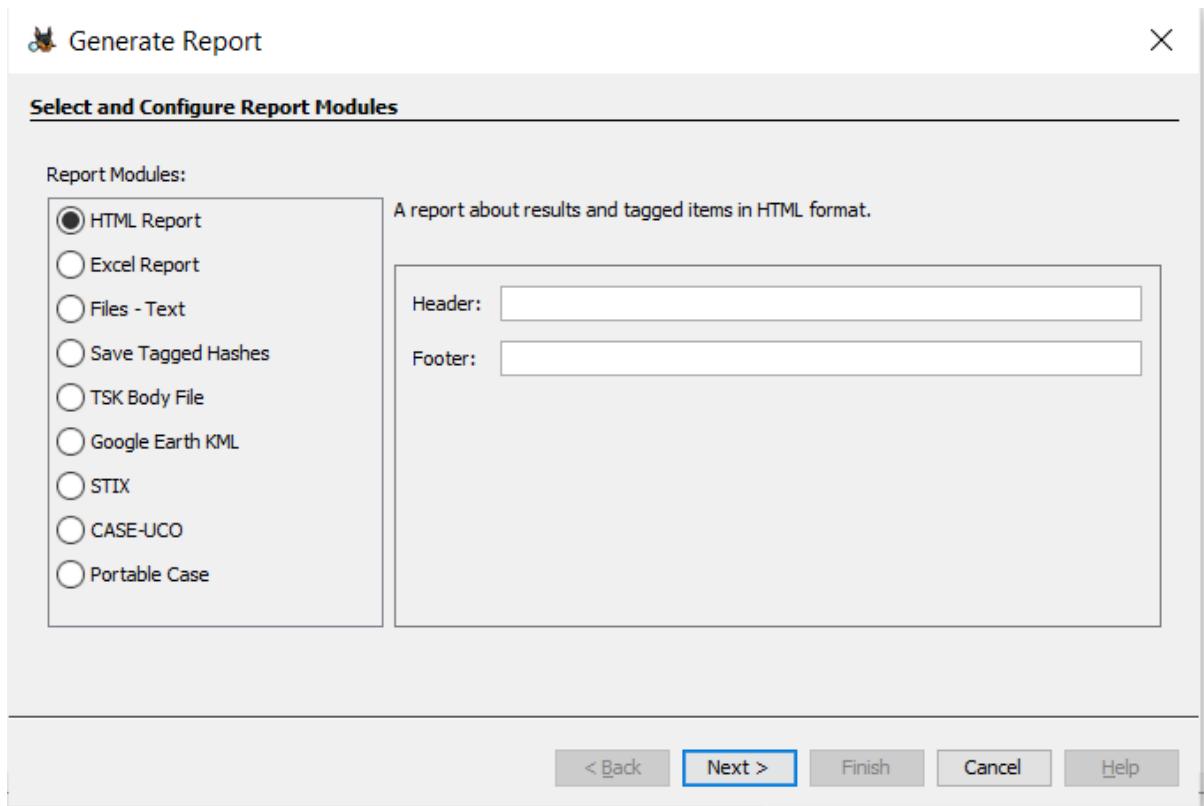
Generate Report

Step 1. Navigate to the generate report tool



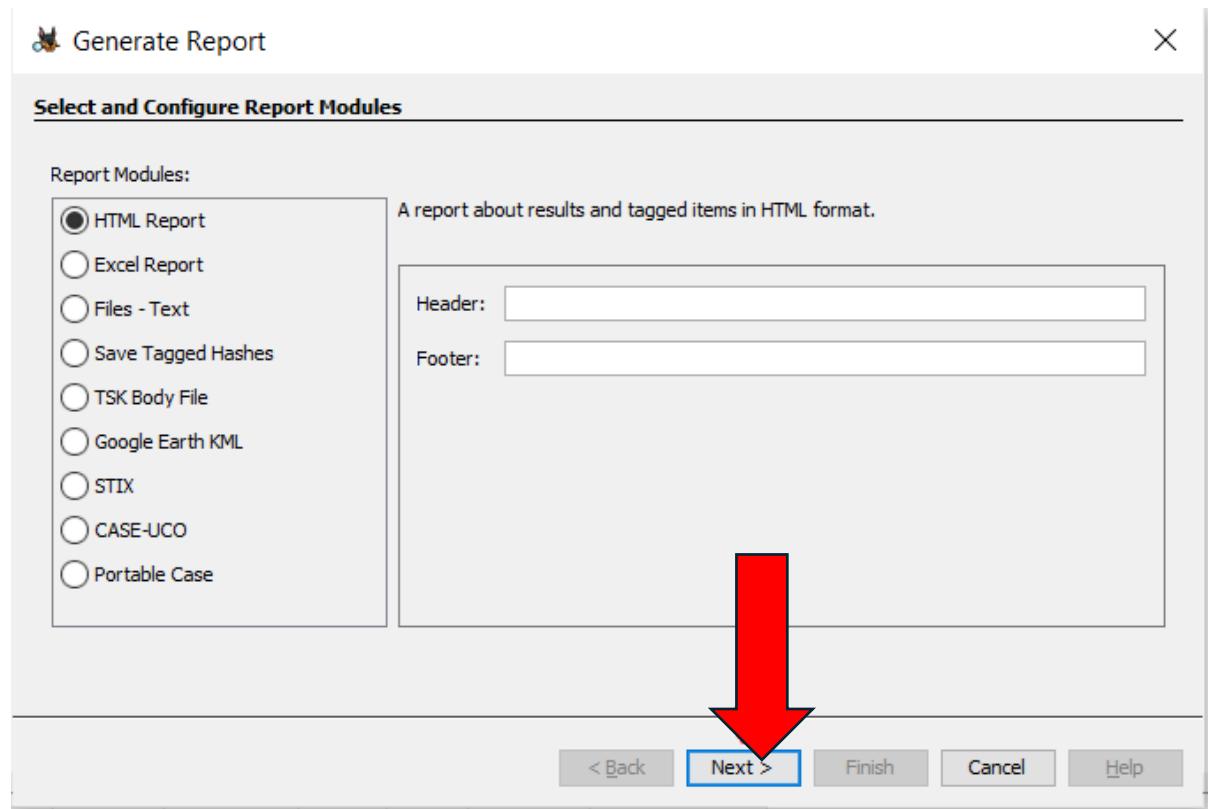
Step 2. Notice the GUI.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



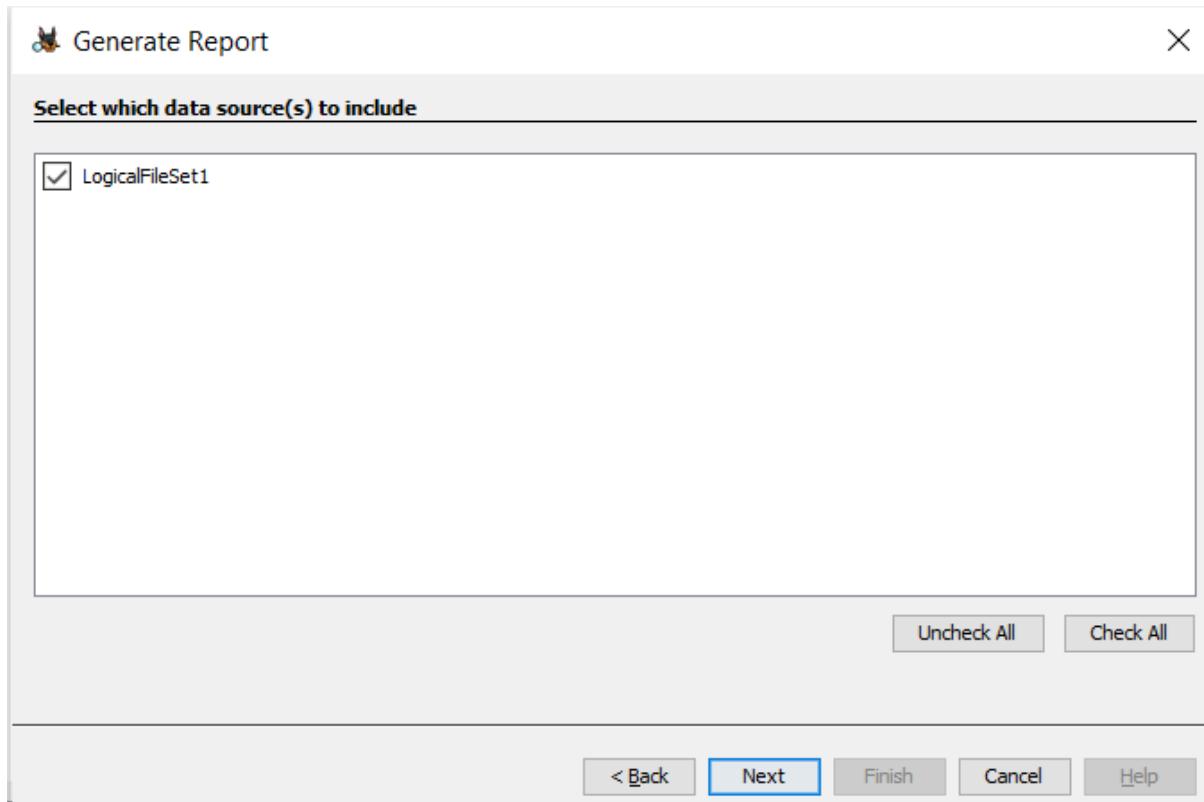
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

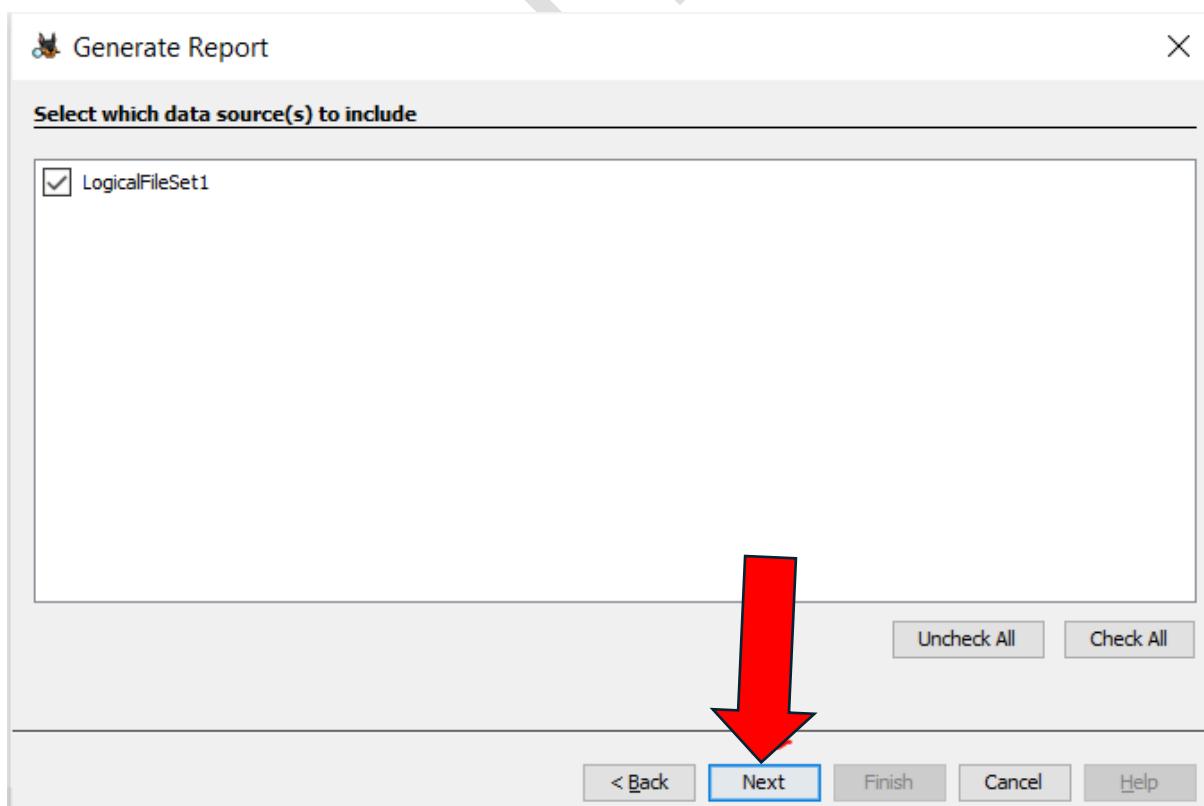


Step 4. Select data sources, in this case only one data source is used, in an investigation it could be multiple

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

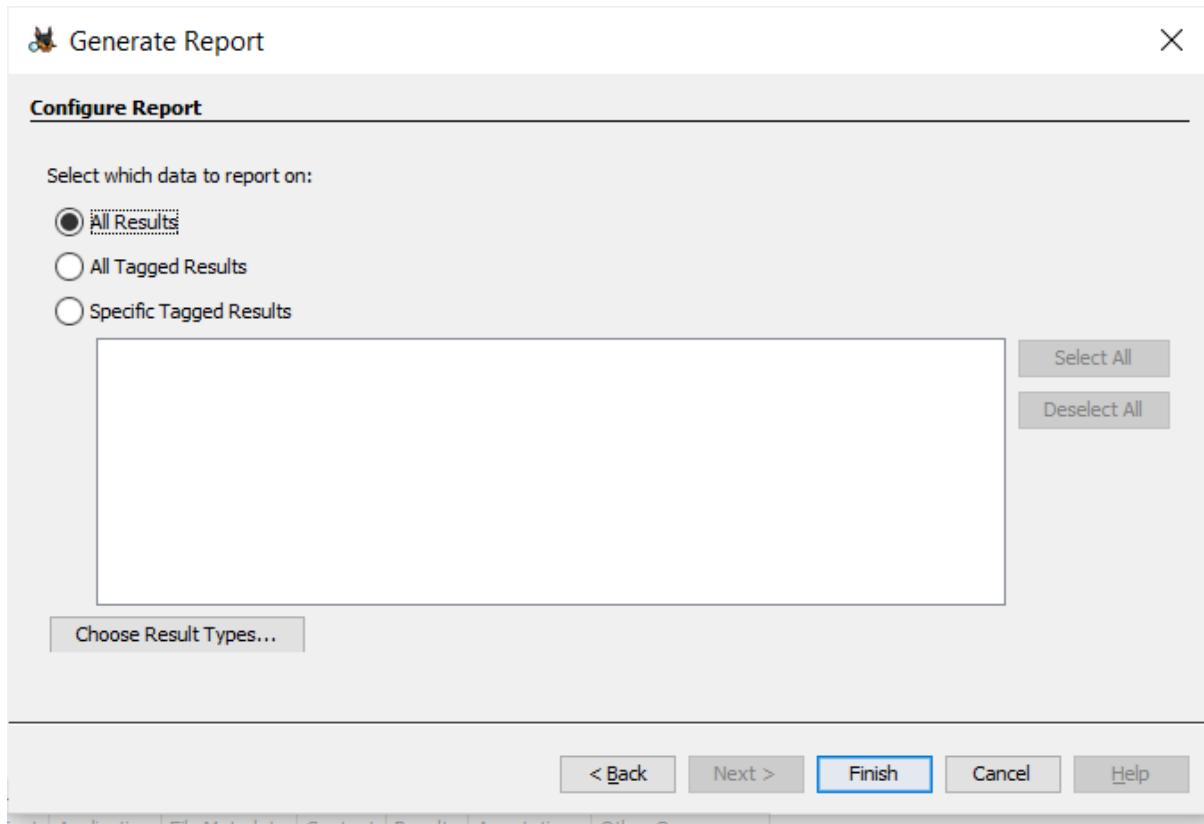


Step 5. Hit next



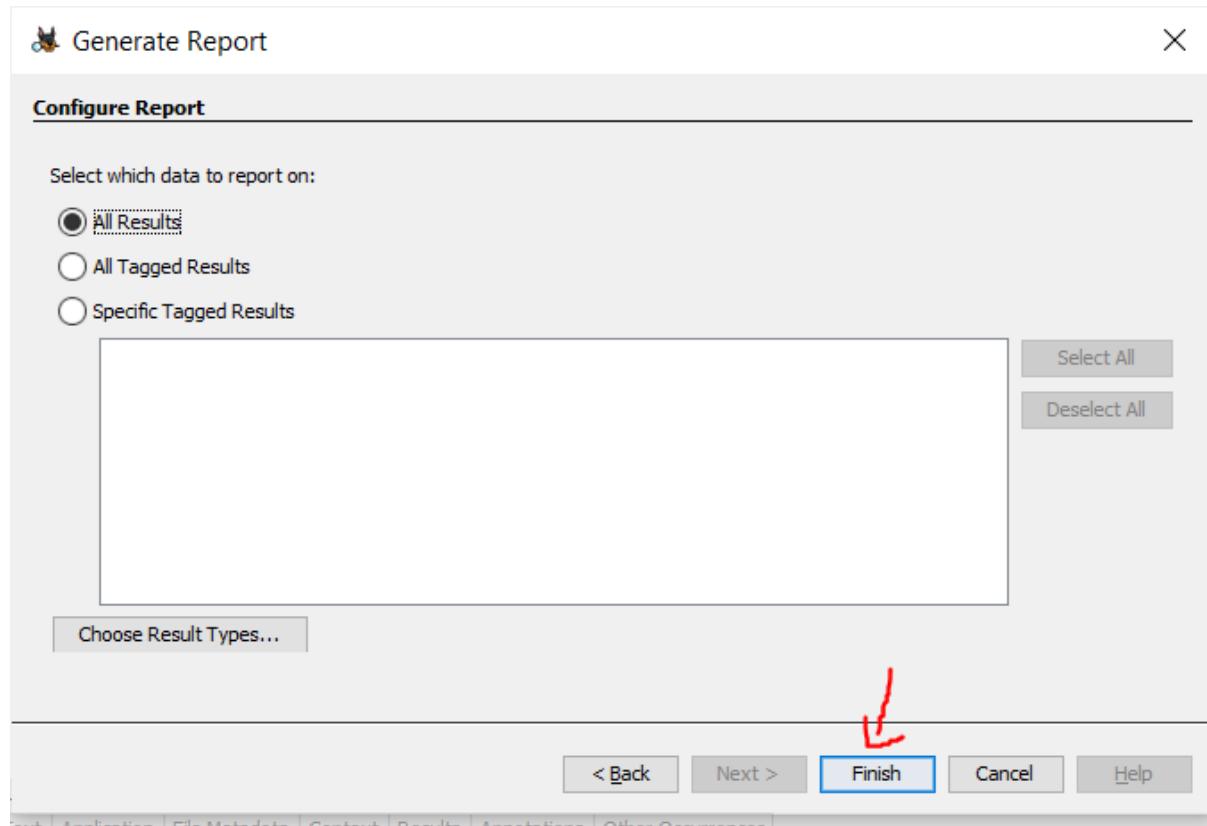
Step 6. Select the configure report options. Choose “all results”

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Step 7. Click finish

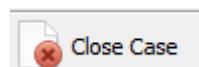
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

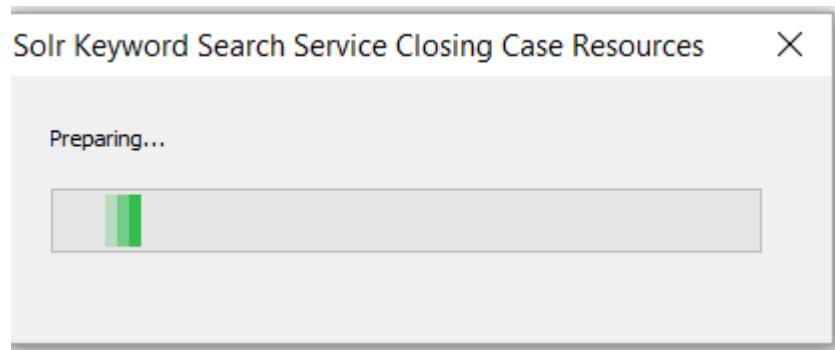
Close Case

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Keyword Lists

Step 1. Navigate to keyword lists tool



Step 2. Open the keyword lists to see the options

A screenshot of the "Keyword Lists" tool interface. The sidebar shows "Email Addresses" is selected. The main area displays a table with columns "Name" and "Keyword Type". There are checkboxes for "Restrict search to the selected data sources" and "Save search results". Buttons for "Add to Ingest" and "Manage Lists" are at the bottom, along with a status message "File Indexing: 113,734 (ingest is ongoing)".

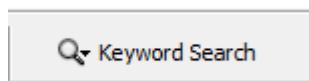
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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.

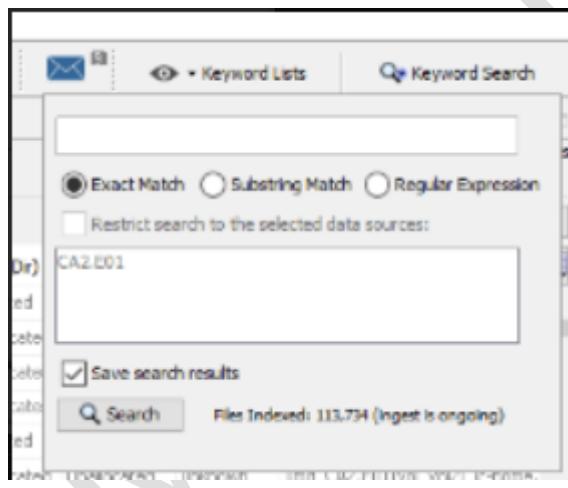
Note: *This can help an investigator quickly hit the relevant pieces of information, should the relevant information be known.*

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

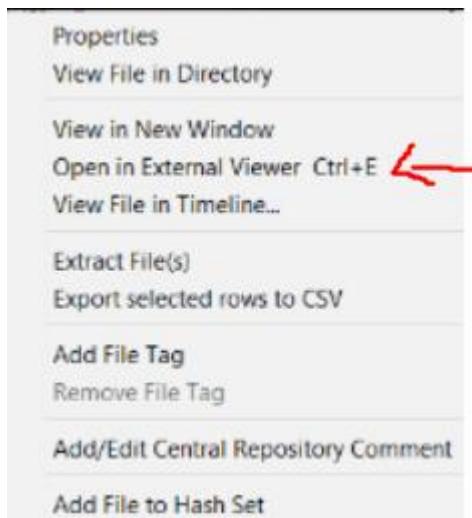


Step 3. Visit the interesting findings section of the lab to see results of a specific search

External viewer

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



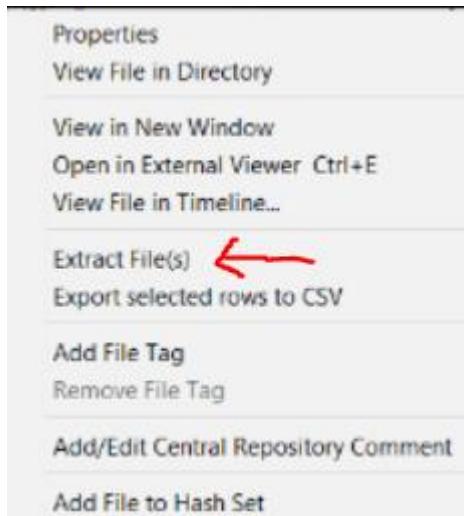
Step 2. Once selected the image will be opened on a related image software such as photos



Extraction

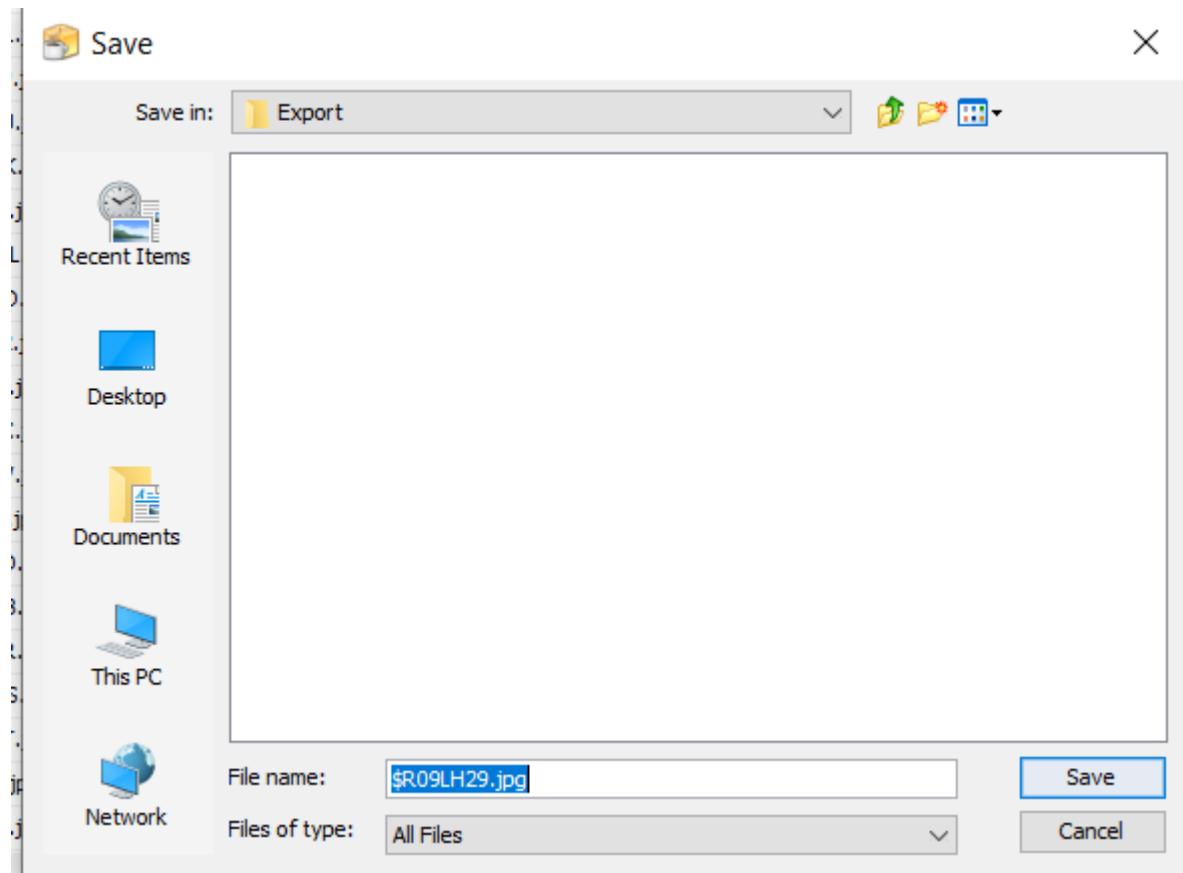
Step 1. Right click on an image and select “extract files”

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

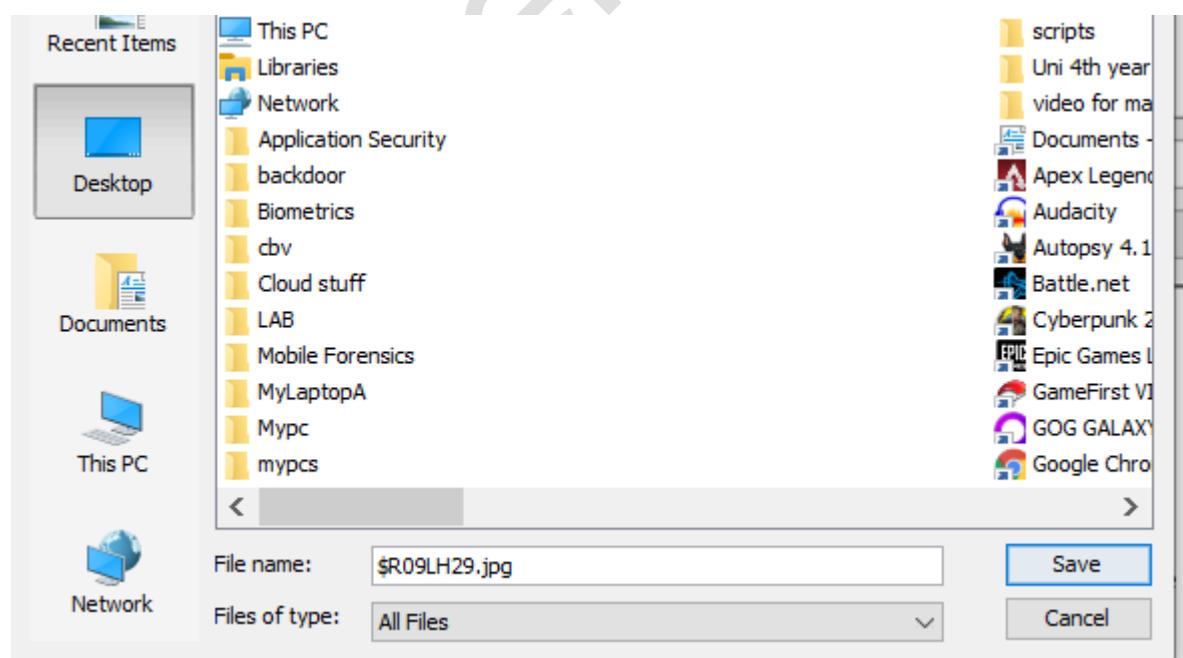


Step 2. Select the extract destination

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

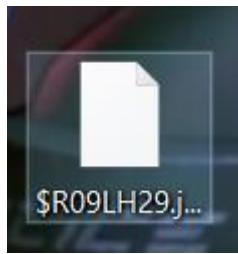


Step 3. Save the file



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

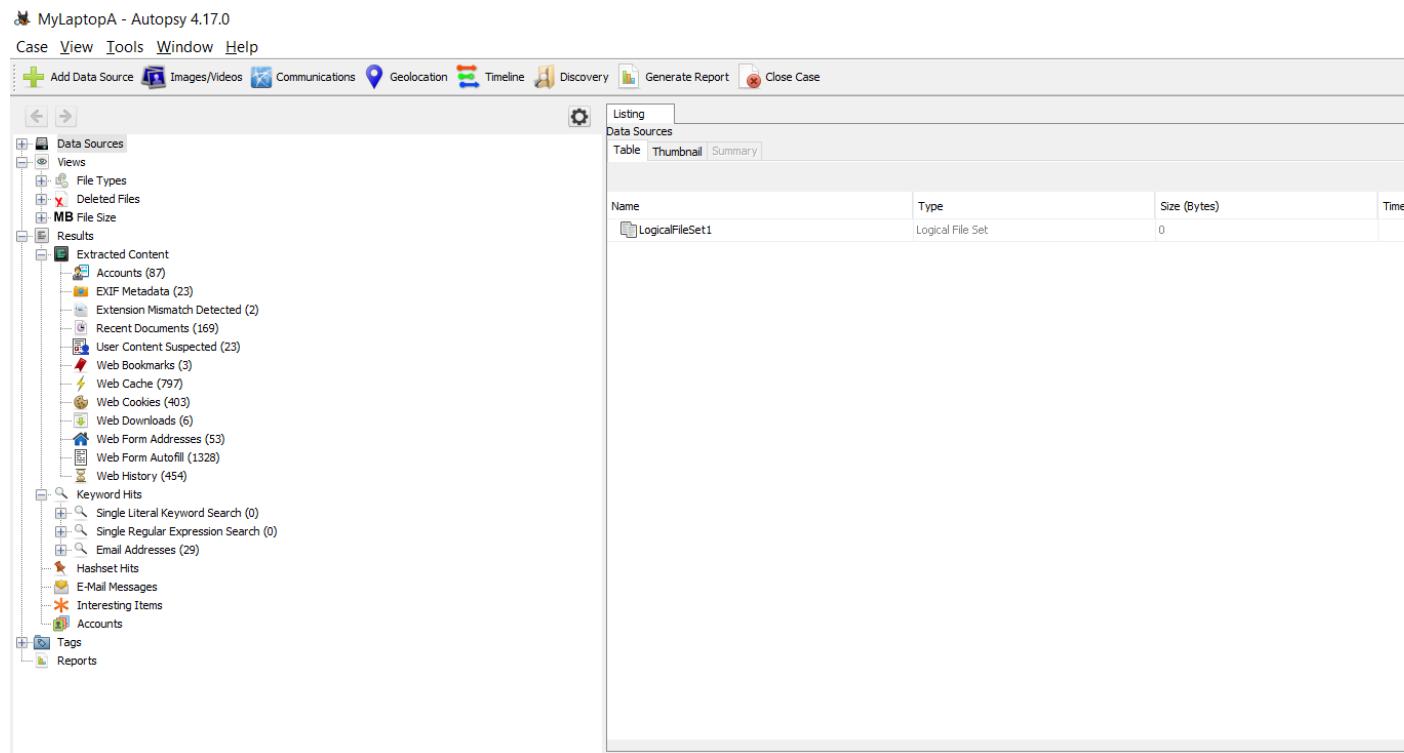
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

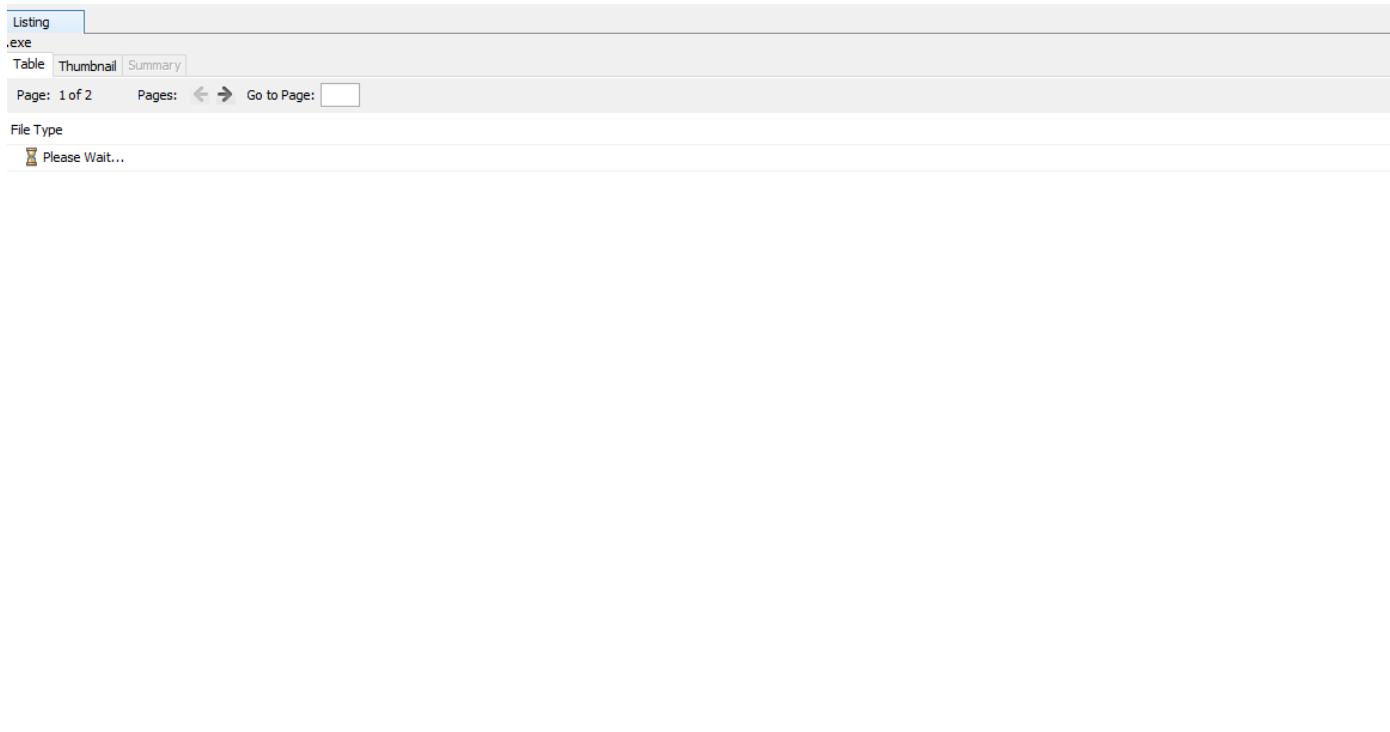
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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*

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



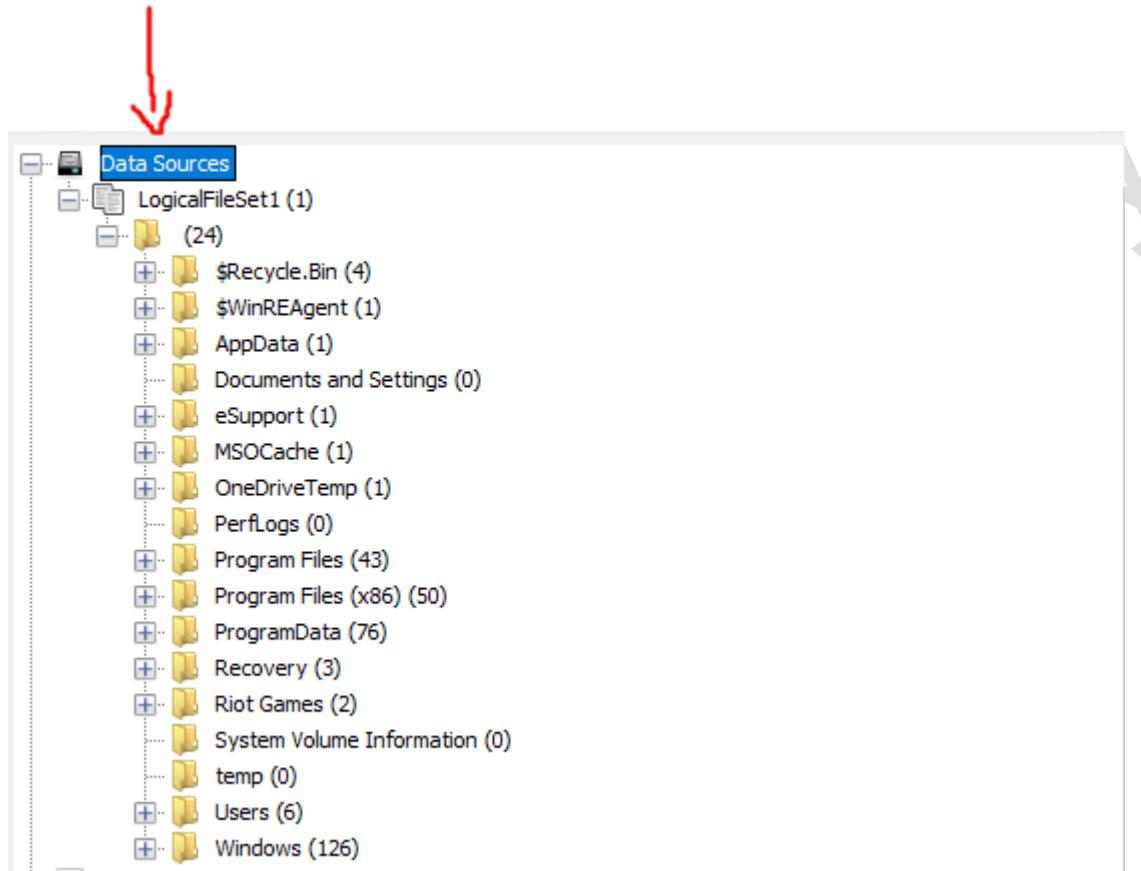
Note: An example of what you will see after the field has populated

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	MIME Type	Extension
\$_\$15LNC-			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 116		Allocated	Allocated	unknown	/LogicalFile5e...	e6f31732b595...	application/octet...	exe
\$_\$16SNXT			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 130		Allocated	Allocated	unknown	/LogicalFile5e...	cædcef18b04...	application/octet...	exe
\$_\$171AR01			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 110		Allocated	Allocated	unknown	/LogicalFile5e...	a3c913d04e8c...	application/octet...	exe
\$_\$1A8J27#			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 110		Allocated	Allocated	unknown	/LogicalFile5e...	b693b3c001d8...	application/octet...	exe
\$_\$1AD0F2			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 110		Allocated	Allocated	unknown	/LogicalFile5e...	9d849466910b...	application/octet...	exe
\$_\$1E7FJQI			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 116		Allocated	Allocated	unknown	/LogicalFile5e...	3eb0001bae8...	application/octet...	exe
\$_\$EEEOIN			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 108		Allocated	Allocated	unknown	/LogicalFile5e...	b13ff5def84bb...	application/octet...	exe
\$_\$HCHND2			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 188		Allocated	Allocated	unknown	/LogicalFile5e...	bdecbe79d5cc1...	application/octet...	exe
\$_\$JCG4Z			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 106		Allocated	Allocated	unknown	/LogicalFile5e...	9a7a9a86324...	application/octet...	exe
\$_\$KGT6K1			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 110		Allocated	Allocated	unknown	/LogicalFile5e...	2ced4b4a20bc...	application/octet...	exe
\$_\$L5T9Y1			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 130		Allocated	Allocated	unknown	/LogicalFile5e...	098a80f97cb79...	application/octet...	exe
\$_\$LSVLGF			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 162		Allocated	Allocated	unknown	/LogicalFile5e...	09f4f723325b2...	application/octet...	exe
\$_\$LV2F2#			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 106		Allocated	Allocated	unknown	/LogicalFile5e...	e9c73f776061f...	application/octet...	exe
\$_\$SRVVF			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 230		Allocated	Allocated	unknown	/LogicalFile5e...	b2cc7fb53f29...	application/octet...	exe
\$_\$Q8MN#			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 126		Allocated	Allocated	unknown	/LogicalFile5e...	ff0906037c68c...	application/octet...	exe
\$_\$T6UWI			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 126		Allocated	Allocated	unknown	/LogicalFile5e...	79aa41643a2c...	application/octet...	exe
\$_\$VBL0X:			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 108		Allocated	Allocated	unknown	/LogicalFile5e...	98d7d26dacbe...	application/octet...	exe
\$_\$VMQO\			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 126		Allocated	Allocated	unknown	/LogicalFile5e...	c3b676615856...	application/octet...	exe
\$_\$WS4H:			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 144		Allocated	Allocated	unknown	/LogicalFile5e...	489b0e685b...	application/octet...	exe
\$_\$YB1K0\			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 108		Allocated	Allocated	unknown	/LogicalFile5e...	e28e360db735...	application/octet...	exe
\$_\$ZU20D			1	0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00 108		Allocated	Allocated	unknown	/LogicalFile5e...	b451c3fa1ee0...	application/octet...	exe
instmsia.				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	/LogicalFile5e...			exe

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

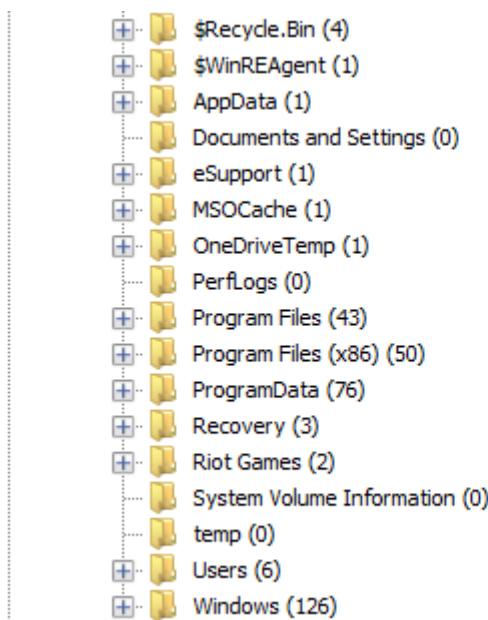
The screenshot shows the Autopsy digital forensics tool's interface. On the left, the 'Data Sources' pane is open, displaying a tree structure under 'LogicalFileSet1 (1)'. A red arrow points to the 'LogicalFileSet1 (1)' node. The tree lists 24 directories, including '\$Recycle.Bin (4)', '\$WinREAgent (1)', 'AppData (1)', 'Documents and Settings (0)', 'eSupport (1)', 'MSOCache (1)', 'OneDriveTemp (1)', 'PerfLogs (0)', 'Program Files (43)', 'Program Files (x86) (50)', 'ProgramData (76)', 'Recovery (3)', 'Riot Games (2)', 'System Volume Information (0)', 'temp (0)', 'Users (6)', and 'Windows (126)'. To the right, a table titled 'LogicalFileSet1' is displayed with one row of data. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, and Size. The single row shows a file named 'LogicalFileSet1' with all values set to 0000-00-00 00:00:00.

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.

This screenshot shows the same Autopsy interface as above, but with the 'LogicalFileSet1 (1)' node expanded. The expanded tree view shows the 24 individual directory entries listed under the main node. A large grey arrow points from the text in Step 4 towards this expanded tree view.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Recycle bin

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

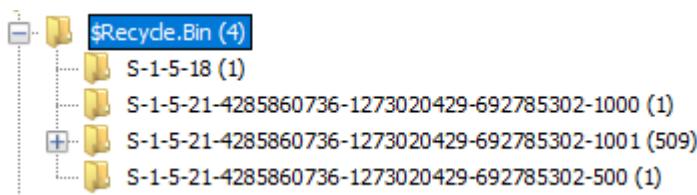
Data Sources

- LogicalFileSet1 (1)
 - (24)
 - \$Recycle.Bin (4) (1) (1)
 - S-1-5-18 (1)
 - S-1-5-21-4285860736-1273020429-692785302-1000 (1)
 - S-1-5-21-4285860736-1273020429-692785302-1001 (509)
 - S-1-5-21-4285860736-1273020429-692785302-500 (1)
 - \$WinREAgent (1)
 - AppData (1)
 - Documents and Settings (0)

Listing /LogicalFileSet1/\$Recycle.Bin

Name	S	C	O	Modified Time
S-1-5-18				0000-00-00 00:00:00
S-1-5-21-4285860736-1273020429-692785302-1000				0000-00-00 00:00:00
S-1-5-21-4285860736-1273020429-692785302-1001				0000-00-00 00:00:00
S-1-5-21-4285860736-1273020429-692785302-500				0000-00-00 00:00:00

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



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

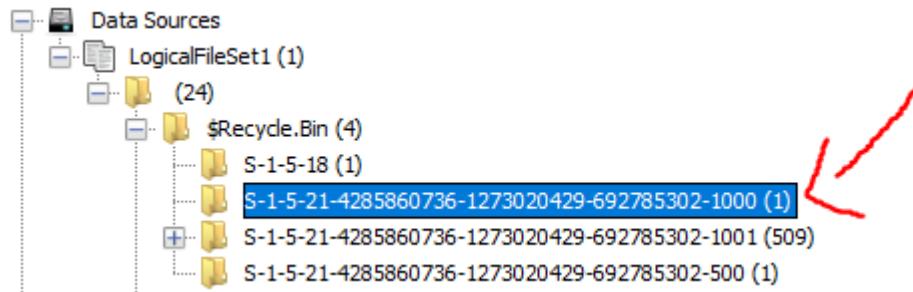
The screenshot shows the Autopsy digital forensics tool's interface. On the left, the 'Data Sources' pane displays a tree structure of logical file sets and their contents. A red arrow points to the 'S-1-5-18 (1)' folder under the '\$Recycle.Bin' directory. On the right, the 'LogicalFileSet1/\$Recycle.Bin/S-1-5-18' pane shows a 'Summary' table with one result. The table has columns for Name, S, C, O, Modified Time, Change Time, and Access Time. The single entry is 'desktop.ini'.

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

This screenshot shows the detailed view of the 'desktop.ini' file within the Autopsy interface. The top part is a 'Summary' table with one row for 'desktop.ini'. The bottom part is a 'Text' editor window showing the file's contents. The file is mostly blank with some very small, illegible text at the top. The 'Text' tab is selected, and the 'File Metadata' tab is visible above it.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

The screenshot shows the 'File Metadata' view in Autopsy. A red arrow points to the row for 'desktop.ini' in the table. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The 'Known' column for 'desktop.ini' is marked as 'Unknown'. The 'Location' column shows the full path: '/LogicalFileSet1/\$Recycle.Bin/S-1-5-21-4285860736-12730...'. The MD5 hash is listed as 'a52cb9e7c71'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
desktop.ini			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	129	Allocated	Allocated	Unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-21-4285860736-12730...	a52cb9e7c71

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

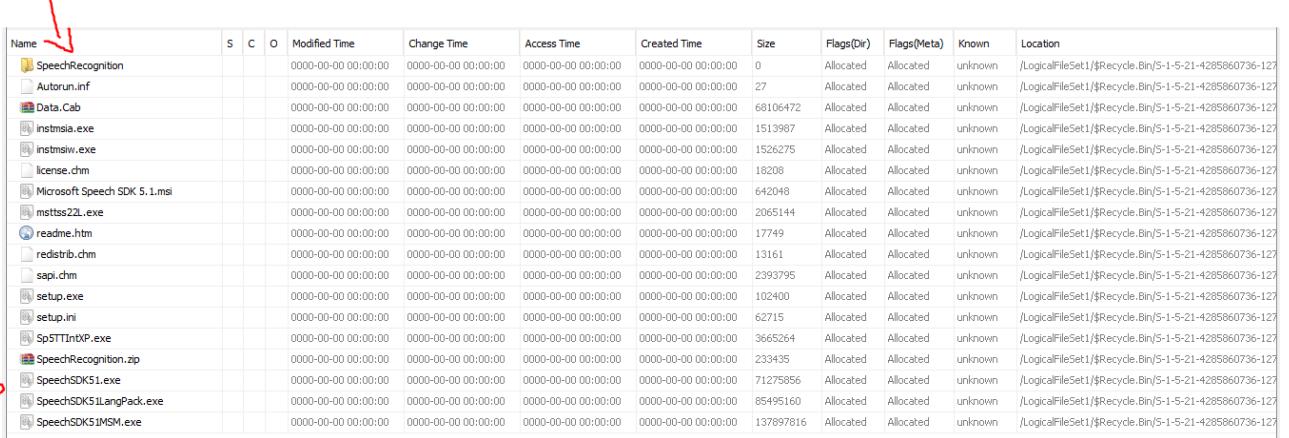
The screenshot shows the Autopsy tool's file listing interface. The left sidebar shows 'Data Sources' with 'LogicalFileSet1 (1)' selected, containing a folder named '(24)'. Inside '(24)' is a folder '\$Recycle.Bin (4)'. Within '\$Recycle.Bin (4)' are several sub-folders, including 'S-1-5-18 (1)', 'S-1-5-21-4285860736-1273020429-692785302-1000 (1)', and '\$R2NL1NE (18)'. A red arrow points to the '\$R2NL1NE (18)' folder. The main pane displays a table titled 'Listing' with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists numerous files, including SR13ERDN, \$R2NL1NE, SR95IDDA, SRATNLY4, SRCAZLAO, SRDH30XX, SRFKQUDF, SRKQIMCU, SR95FFN, SRULGWHL, \$T03E2E6.log, \$T077C0X.jpg, \$T09H29.jpg, \$T0A43D0.jpg, \$T0A5ABP.png, \$T0K6C6V2.bn, \$T0L31A.jpg, \$T0LC18Z.png, \$T0SM1P6.png, \$T0XVUQ3.png, \$T18MR2L.jpg, and \$T19HMJW.png. The 'Known' column indicates that most files are 'Allocated'.

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.

The screenshot shows the Autopsy tool's file listing interface. The left sidebar shows 'Data Sources' with 'LogicalFileSet1 (1)' selected, containing a folder named '(24)'. Inside '(24)' is a folder '\$Recycle.Bin (4)'. Within '\$Recycle.Bin (4)' are several sub-folders, including 'S-1-5-18 (1)', 'S-1-5-21-4285860736-1273020429-692785302-1000 (1)', and '\$R2NL1NE (18)'. A red arrow points to the '\$R2NL1NE (18)' folder. The main pane displays a table titled 'Listing' with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). The table lists files related to SpeechRecognition, such as Autorun.inf, Data.Cab, instmsia.exe, instmsiw.exe, license.chm, Microsoft Speech SDK 5.1.msi, msttsc2l.exe, readme.htm, redistrib.chm, sapi.chm, setup.exe, setup.ini, SpTTInkXP.exe, SpeechRecognition.zip, SpeechSDK51.exe, SpeechSDK5LangPack.exe, and SpeechSDK5IMSM.exe. The 'Known' column indicates that all files are 'Allocated'.

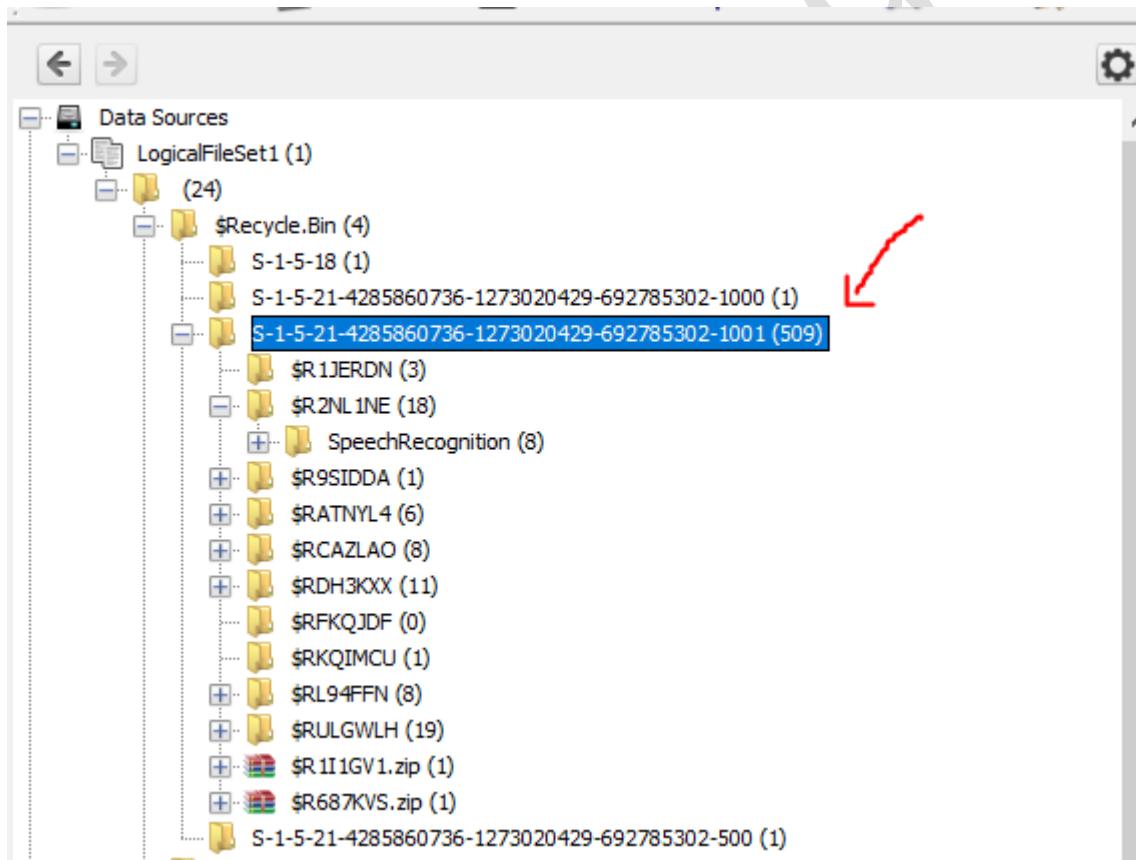
Step 9. Notice the amount of SpeechRecognition related data, during an investigation it would be safe to assume that biometric data is being held on the laptop being examined.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
SpeedRecognition				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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
mstss22.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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
SpTTTIntXP.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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127
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/5-1-5-21-4285860736-127

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	MD5
\$R1JERDN				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$R2NLINIE				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$R95IDDA				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RATNyl4				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RC2LAQO				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RDH3KXX				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RPKQJDF				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RKQJIMU				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RUL94FTN				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$RULGWHL				2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730...	40e5...
\$_T035E26.log	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	180	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... b27e	
\$_T077CXX.jpg	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	268	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 7fd...	
\$_T09LH29.jpg	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	230	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 27af	
\$_T0A4JDO.jpg	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	218	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... eee0	
\$_T0ASAP.png	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... be32	
\$_T0KC6W2.bin	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	234	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 61a5	
\$_T0L31SA.jpg	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	118	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 19c...	
\$_T0OC18Z.png	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 81ca	
\$_T0SM1P6.png	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 09e6	
\$_T0XYUQ3.png	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... b6d7	
\$_T18M97L2.jpg	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	232	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 2584	
\$_T19M4JWJV.png	1			2000-00-00 00:00:00	2000-00-00 00:01:00	2000-00-00 00:00:00	2000-00-00 00:00:00	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-1-21-4285860736-12730... 04e5	

Step 12. Analyse the contents of the selected image

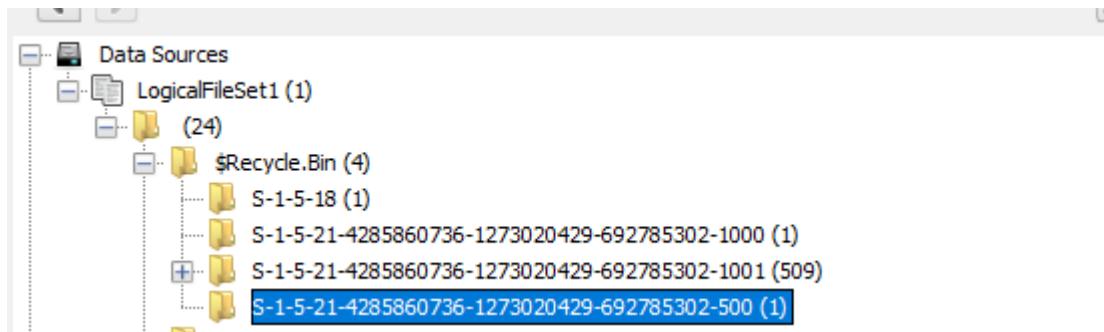
File Path	File ID	File Size	Creation Time	Last Access Time	Last Write Time	File Type	Allocation Status	File Size (Allocated)	File Hash	Notes
C:\Users\knean\OneDrive\Desktop\Biometrics\Fingerprint lifts\Right_T1_A2_CROPPED-resized-contrasted-sharpened+edged.jpg	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	268	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 7fd9
C:\09LH29.jpg	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	230	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 27a6
C:\D0A41D0.jpg	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	218	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... eee?
C:\00ASBAP.png	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... be32
C:\00KCG6WZ.bin	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	234	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 61a5
C:\00L31SA.jpg	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	118	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... f9fc
C:\00OC18Z.png	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 81ca
C:\00SM1P6.png	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 096e
C:\00XYUQ3.png	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... b8d7
C:\118MK7-.jpg	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	232	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 258e
C:\119MMJW.png	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$5-1-5-21-4285860736-12730... 04d5

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

	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	268	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...7fd9	
	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	230	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...27e6	
	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	218	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...eee7	
	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...be32	
	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	234	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...61a5	
	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	118	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...f9fc	
	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...81ca	
	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...096e	
	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...b8d7	
	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	232	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...258a	
	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	144	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin\$1-5-21-4285860736-12730...04de	

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



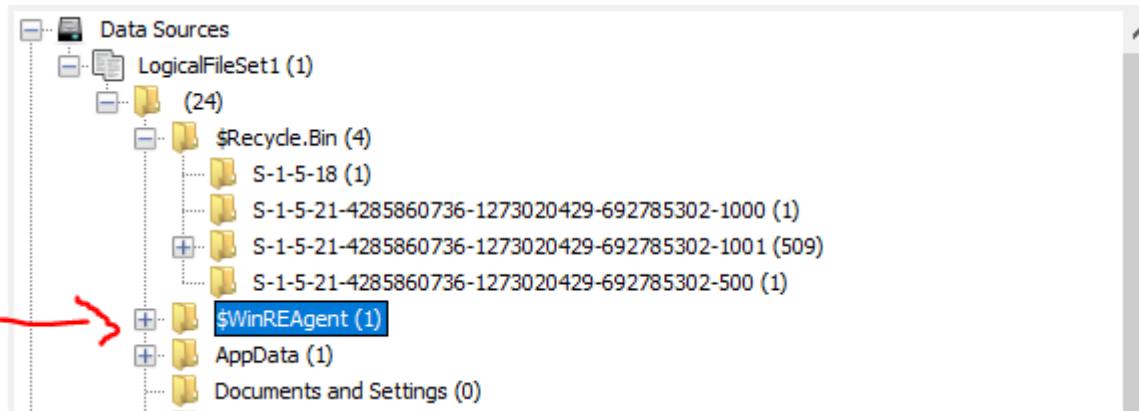
Step 15. Inside this directory is another desktop.ini file, this time round the file could not be read.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
desktop.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	129	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-21-4285860736-1273020429-692785302-500/desktop.ini	

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

WinREAgent

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



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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	MIME Type	Extension
Scratch				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/\$WinREAgent/Scratch			

Step 3. Analyse the contents of the scratch directory



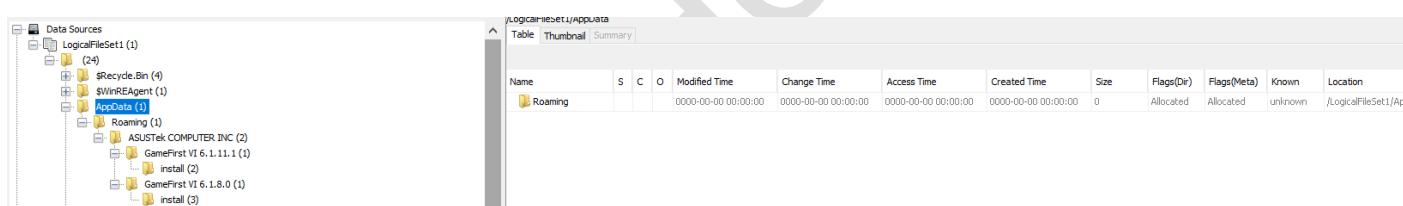
Step 4. Notice that some subdirectories will be found containing no data.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

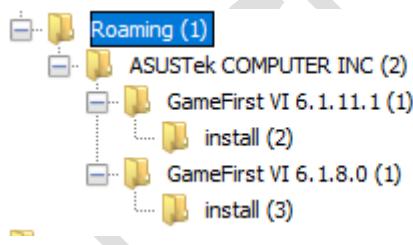


App Data

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

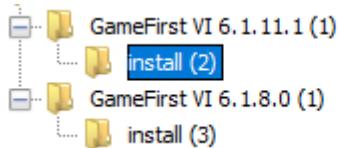


Step 2. You will be able to see a subdirectory called roaming, selecting this directory will open up gamefirst directories.



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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

The screenshot shows the MyLaptopA - Autopsy 4.17.0 interface. The left sidebar displays a tree view of data sources, including LogicalFileSet1 (1) which contains 24 items. One item under LogicalFileSet1 is highlighted: GameFirst VI Installer 6.1.8.0.1.cab. A red arrow points from the status bar at the bottom to this file entry. The main pane shows a table listing files from the GameFirst VI 6.1.8.0\install folder. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags. The table data is as follows:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
GameFirstVI Installer 6.1.8.0.aiul				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2126464	Allocated	Allocated
GameFirstVI Installer 6.1.8.0.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	9161728	Allocated	Allocated
GameFirstVI Installer 6.1.8.0.1.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	14977471	Allocated	Allocated

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
GameFirstVI Installer 6.1.8.0.aui				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2126464	Allocated	Allocated	unknown	/LogicalFileSet1/AppData/Roaming/ASUSTek COMPUTER INC/GameFirst VI 6.1.8.0/install
GameFirstVI Installer 6.1.8.0.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	9161728	Allocated	Allocated	unknown	/LogicalFileSet1/AppData/Roaming/ASUSTek COMPUTER INC/GameFirst VI 6.1.8.0/install
GameFirstVI Installer 6.1.8.01.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	14677471	Allocated	Allocated	unknown	/LogicalFileSet1/AppData/Roaming/ASUSTek COMPUTER INC/GameFirst VI 6.1.8.0/install

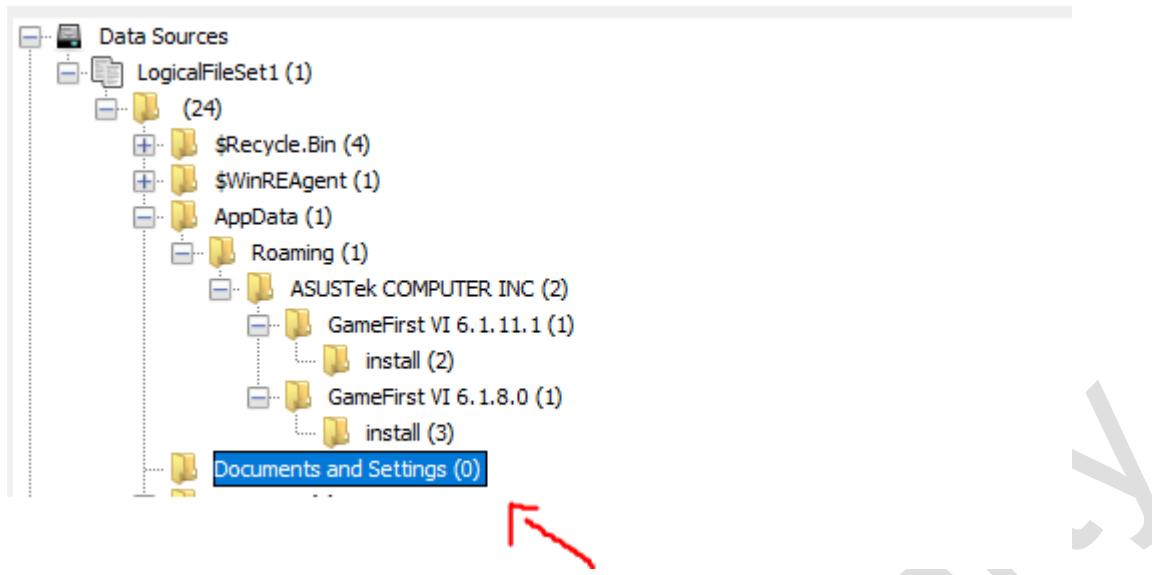
Step 7. Investigate the .msi file and see what you find, if you look hard enough you can see firewall exception information.

```
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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



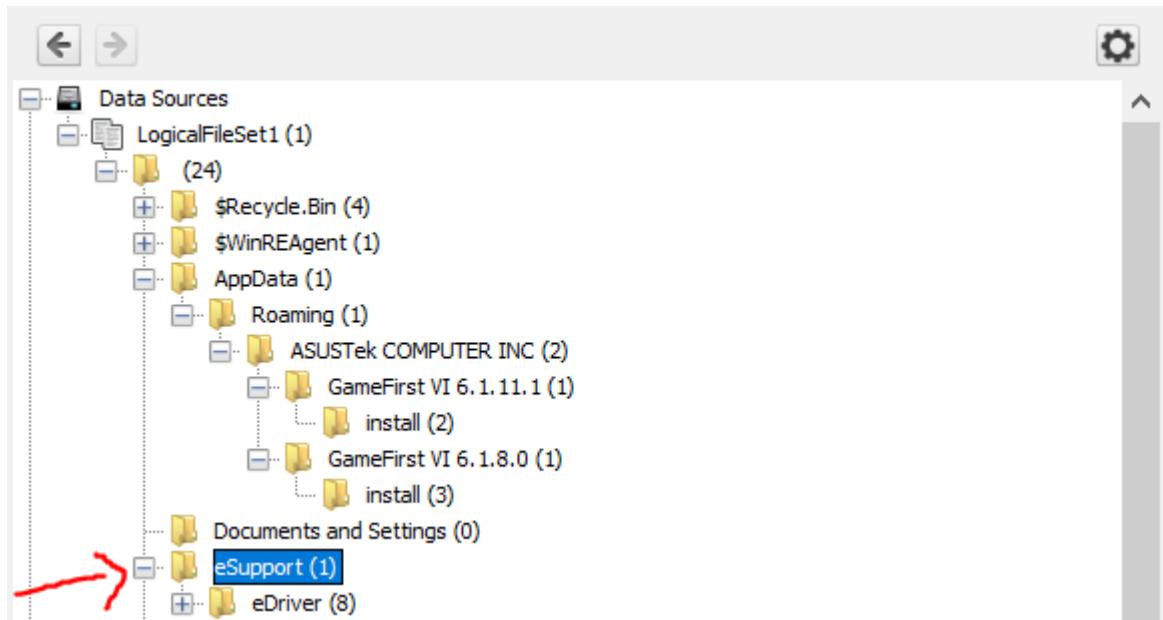
Step 2. The findings will differ from person to person, in this case the directory is empty, if your directory has been filled, it will contain important document locations as well as important settings information.

Esupport

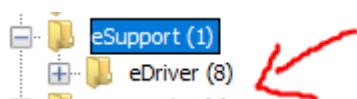
Step 1. Notice the next directory on the list is esupport, this directory will change based on the brand of laptop you use but will contain manual and driver information, during this lab an ASUS laptop is being used

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

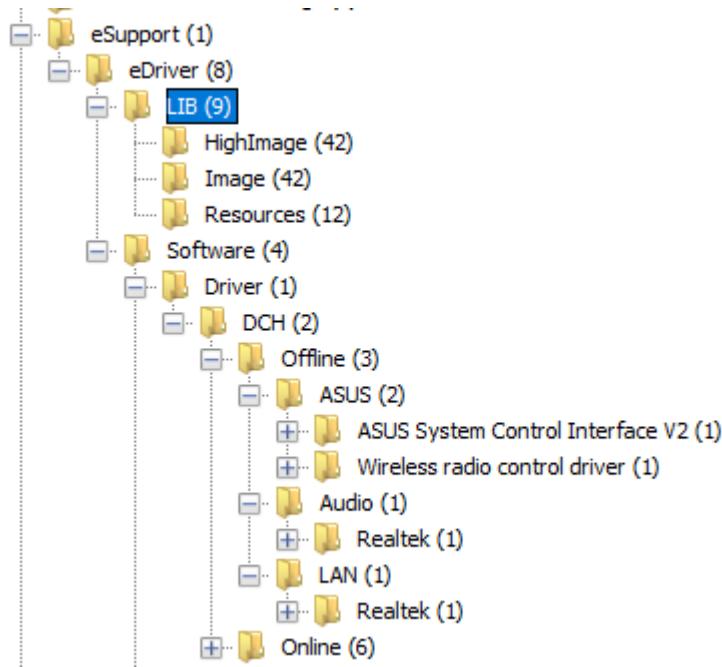


Step 2. As the laptop being used is an ASUS laptop, autopsy has found an eSupport directory, inside this directory is a subdirectory called eDriver.

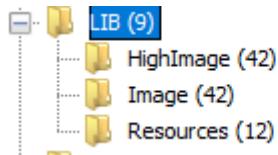


Step 3. Expand the directories of the driver directory

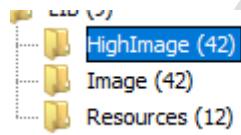
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.



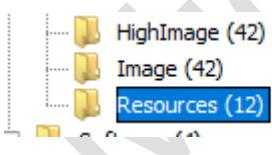
Step 6. Investigate both highimage and image, one is a high-resolution image and the other is a low-quality image. Can you tell the difference?

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.

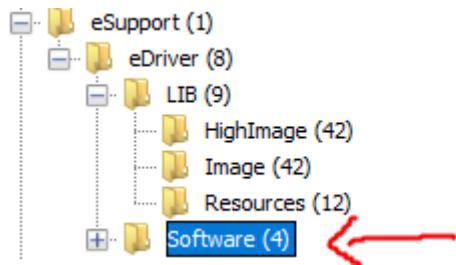


Step 8. Have you been able to determine what files this directory contains? If not, the resources directory contains your different language options.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

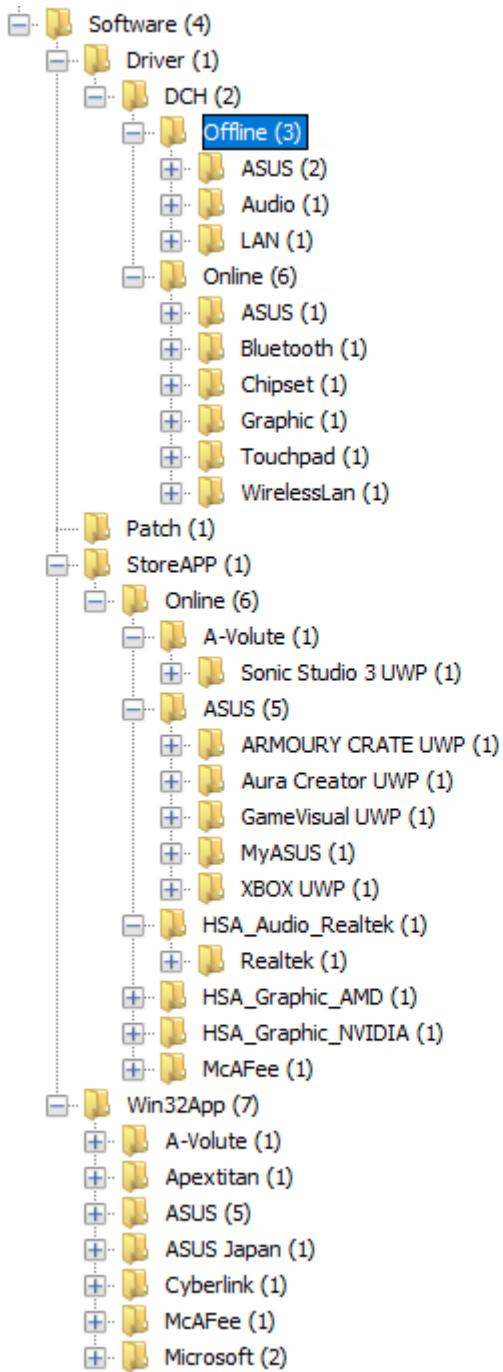
Listing /LogicalFileSet1/eSupport/eDriver/LIB/Resources												12 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Language.ARA.xaml				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3639	Allocated	Allocated	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.FRН.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



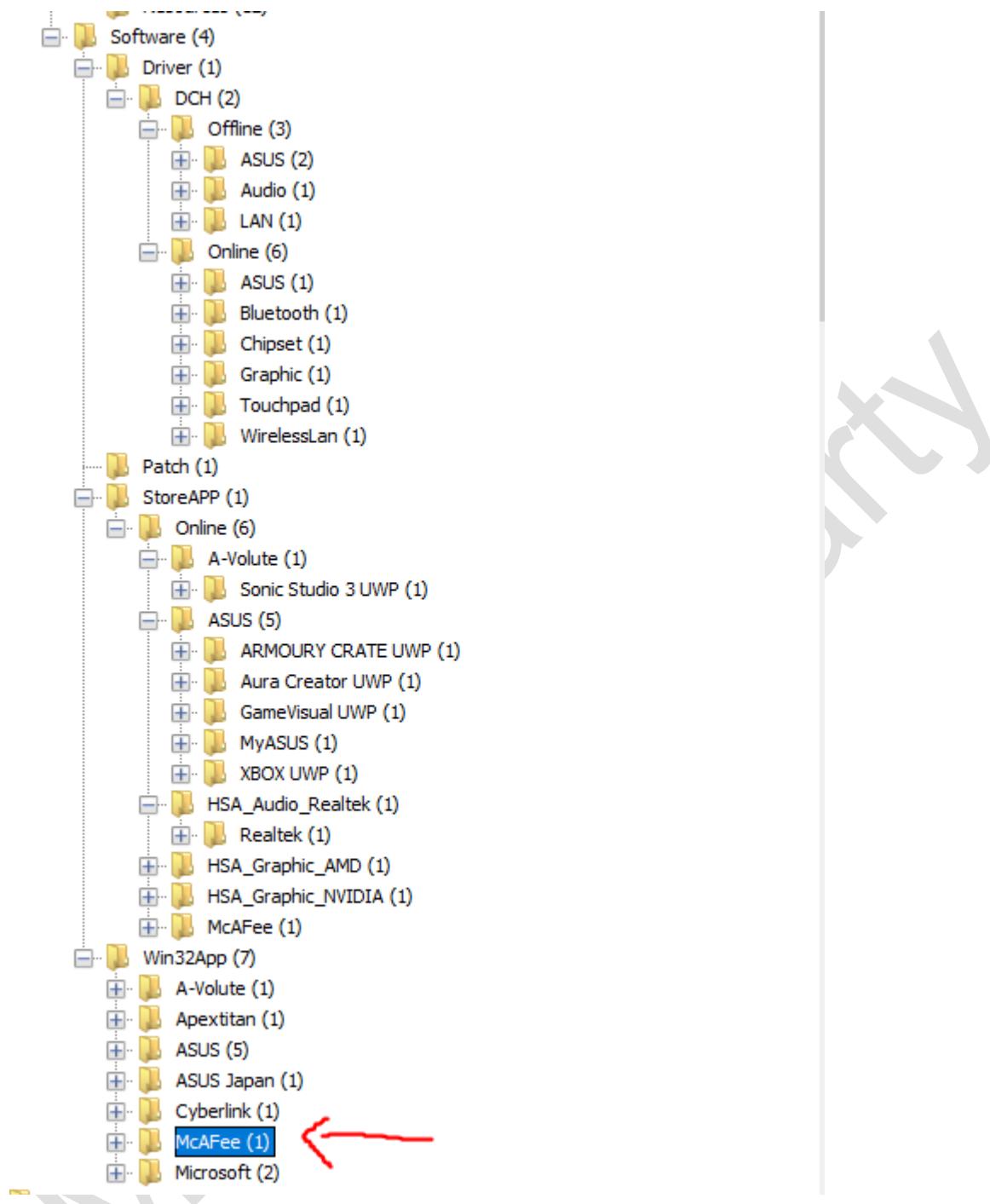
Step 10. Look at all the software directories your laptop has returned. In the case of an ASUS laptop, the following was returned

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



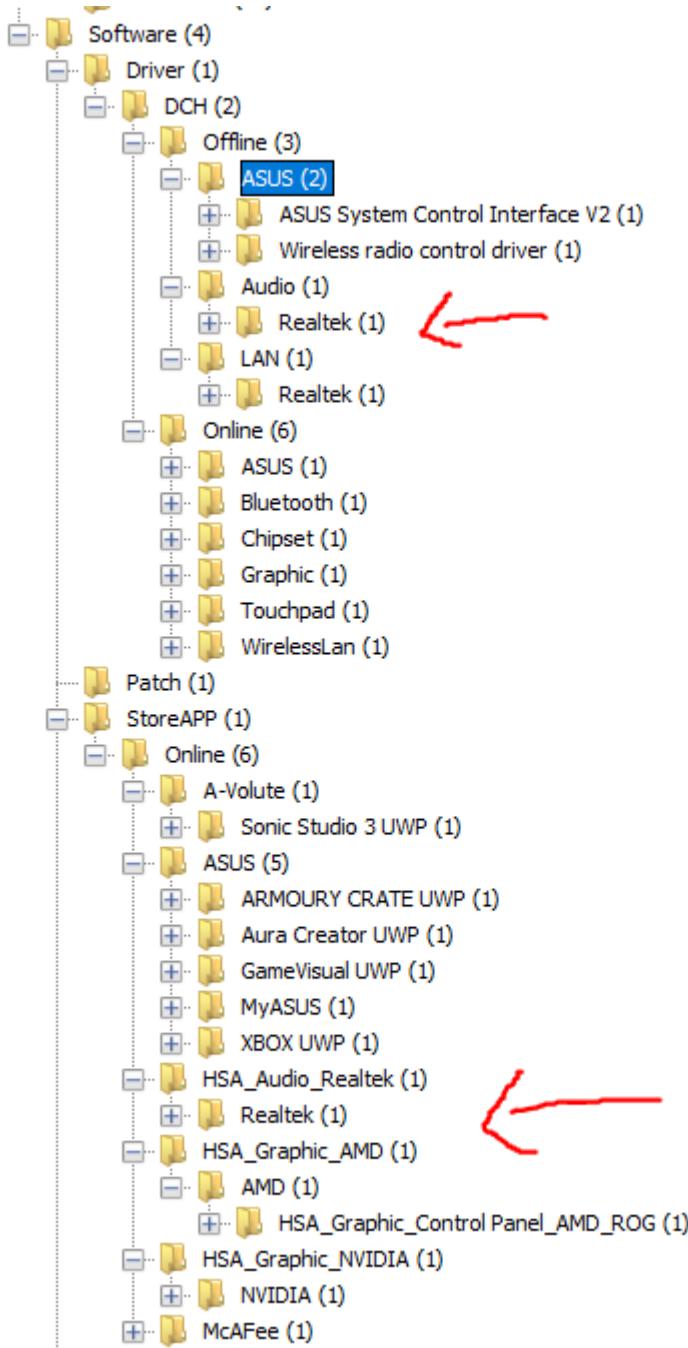
Step 11. This looks quite intimidating but is quite basic, autopsy has returned software information. This can help an investigator get more information on the software on the laptop. Such as firewalls.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

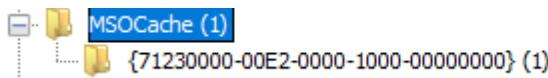
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

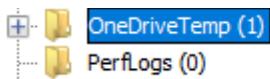


Step 2. Most laptop users will have Microsoft office, as this is the case the common finding of the typical user who has not downloaded additional features in a setup file, which is used to install the components later down the line.

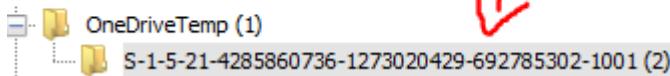
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Setup.dat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5115	Allocated	Allocated	unknown	/LogicalFileSet1/MSOCache/{71230000-00E2-0000-1000-00000000}

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.



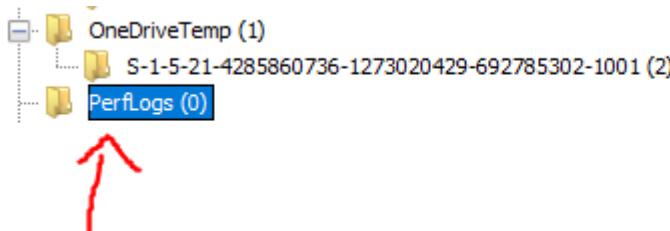
Step 3. Investigate the contents of the found directory, this will reveal two files related to OneDrive

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
4C1AF6A0A92AA66A!101-4C1AF6A0A92AA66A!362-4C1AF6A0A				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/OneDriveTemp/
4C1AF6A0A92AA66A!101-4C1AF6A0A92AA66A!364-4C1AF6A0A!				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/OneDriveTemp/

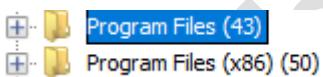
PerfLogs

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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 Health Tools
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/ModifiableWindowsApps
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

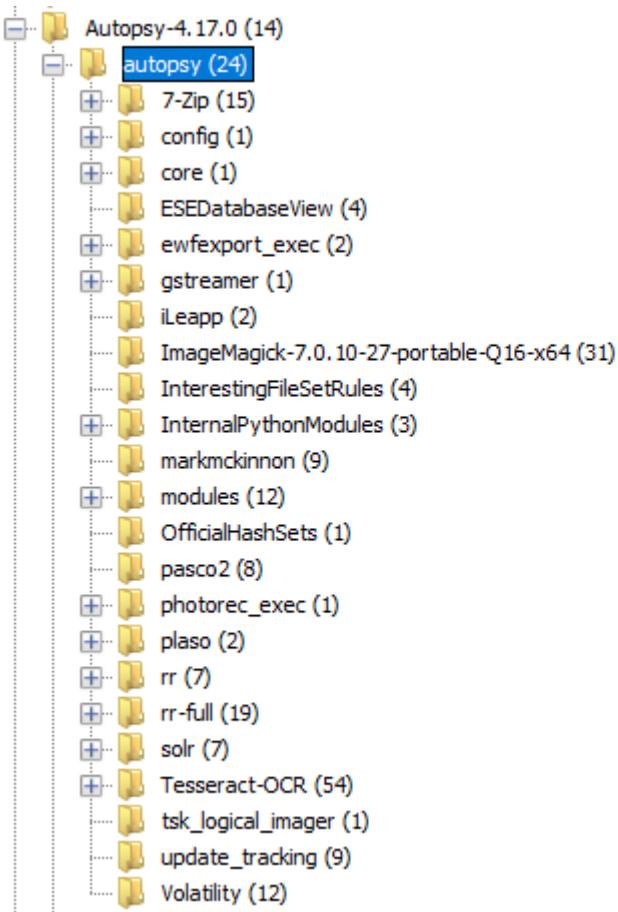
Listing /LogicalFileSet1/Program Files (x86) 50 Results

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 COMPUTER INC
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 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 (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)/EasyAntiCheat
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 Arts
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 Games
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 Galaxy
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)/InstallShield Installation Information
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 Explorer
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)/LightingService
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 GameInput
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 SDKs
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 Speech SDK 5.1
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 SQL Server
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 Threat Modeling Tool 2016
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 Visual Studio

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.

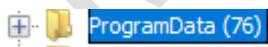
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.

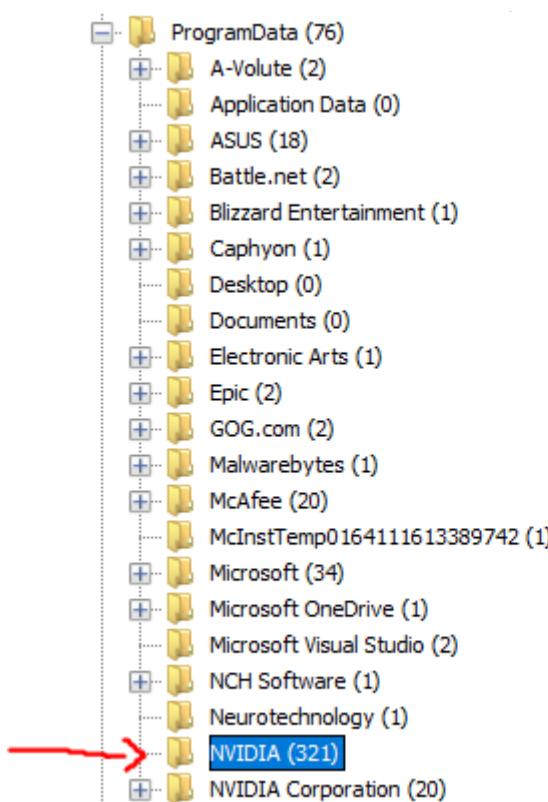


Step 2. Investigate the contents of the ProgramData directory

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
A-Volute				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/ProgramData/A-Volu
Application 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/ProgramData/Applic
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/ProgramData/ASUS
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/ProgramData/Battle.
Blizzard Entertainment				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/ProgramData/Blizzar
Caphyon				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/ProgramData/Caphy
Desktop				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/ProgramData/Desktop
Documents				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/ProgramData/Docum
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/ProgramData/Electrc
Epic				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/ProgramData/Epic
GOG.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/ProgramData/GOG.c
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/ProgramData/Malwar
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/ProgramData/McAfe
McInstTemp0164111613389742				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/ProgramData/McInst
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/ProgramData/Micros
Microsoft OneDrive				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/ProgramData/Micros
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/ProgramData/Micros
NCH Software				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/ProgramData/NCH Si
Neurotechnology				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/ProgramData/Neurol
NVIDIA				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/ProgramData/NVIDI
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/ProgramData/NVIDI/
obs-studio-hook				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/ProgramData/obs-st

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.



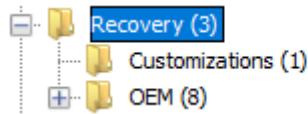
Step 4. This directory contains log data, as well as backups for those logs. These logs keep track of NVIDIA related actions.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
DisplaySessionContainer1.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/NVIDI/
DisplaySessionContainer1.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/NVIDI/
DisplaySessionContainer10.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/NVIDI/
DisplaySessionContainer10.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/NVIDI/
DisplaySessionContainer11.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/NVIDI/
DisplaySessionContainer11.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/NVIDI/
DisplaySessionContainer12.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/NVIDI/
DisplaySessionContainer12.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/NVIDI/
DisplaySessionContainer13.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/NVIDI/
DisplaySessionContainer13.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/NVIDI/
DisplaySessionContainer14.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/NVIDI/
DisplaySessionContainer14.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/NVIDI/
DisplaySessionContainer15.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/NVIDI/
DisplaySessionContainer15.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/NVIDI/
DisplaySessionContainer16.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/NVIDI/
DisplaySessionContainer16.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/NVIDI/
DisplaySessionContainer17.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/NVIDI/
DisplaySessionContainer17.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/NVIDI/
DisplaySessionContainer18.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/NVIDI/
DisplaySessionContainer18.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/NVIDI/
DisplaySessionContainer19.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/NVIDI/
DisplaySessionContainer19.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/NVIDI/

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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy file browser interface. The left pane displays a tree view of the file system:

- Recovery (2)
 - Customizations (1)
 - OEM (8)
 - Info (4)
 - Backgrounds (1)
 - default (45)
 - Dist Cache (2)

The right pane shows a table of file metadata for a file named "usmt.pkg" located in the "Customizations" directory:

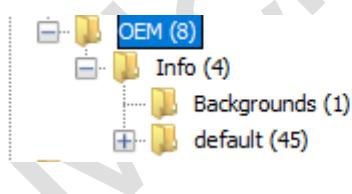
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	MD
usmt.pkg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4313558516	Allocated	Allocated	unknown	/LogicalFileSet1/Recovery/Customizations/usmt.pkg		

Below the table are navigation and search controls:

 - Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences
 - Page: 1 of 263279 | Page: < > | Go to Page: [] | Jump to Offset: [] | Launch in HxD

A red arrow points from the "OEM (8)" folder in the tree view to the "OEM (8)" folder in the table below.

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

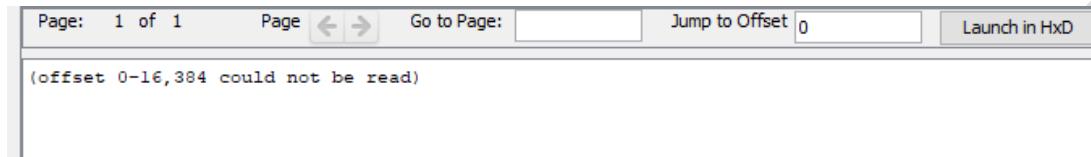


Step 4. Notice the high amount of recovery files.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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.

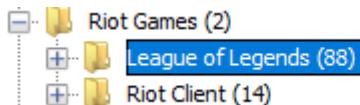


Riot Games

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.



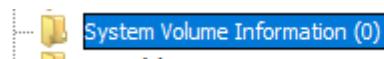
Step 3. Notice the two subdirectories, these directories will contain cookies, logs, plugins and more.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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-1!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-1!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-1!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-1!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-1!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-1!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-1!2-1.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-1!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-1!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-1!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-1!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-1!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-1!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-1!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.*

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Users

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



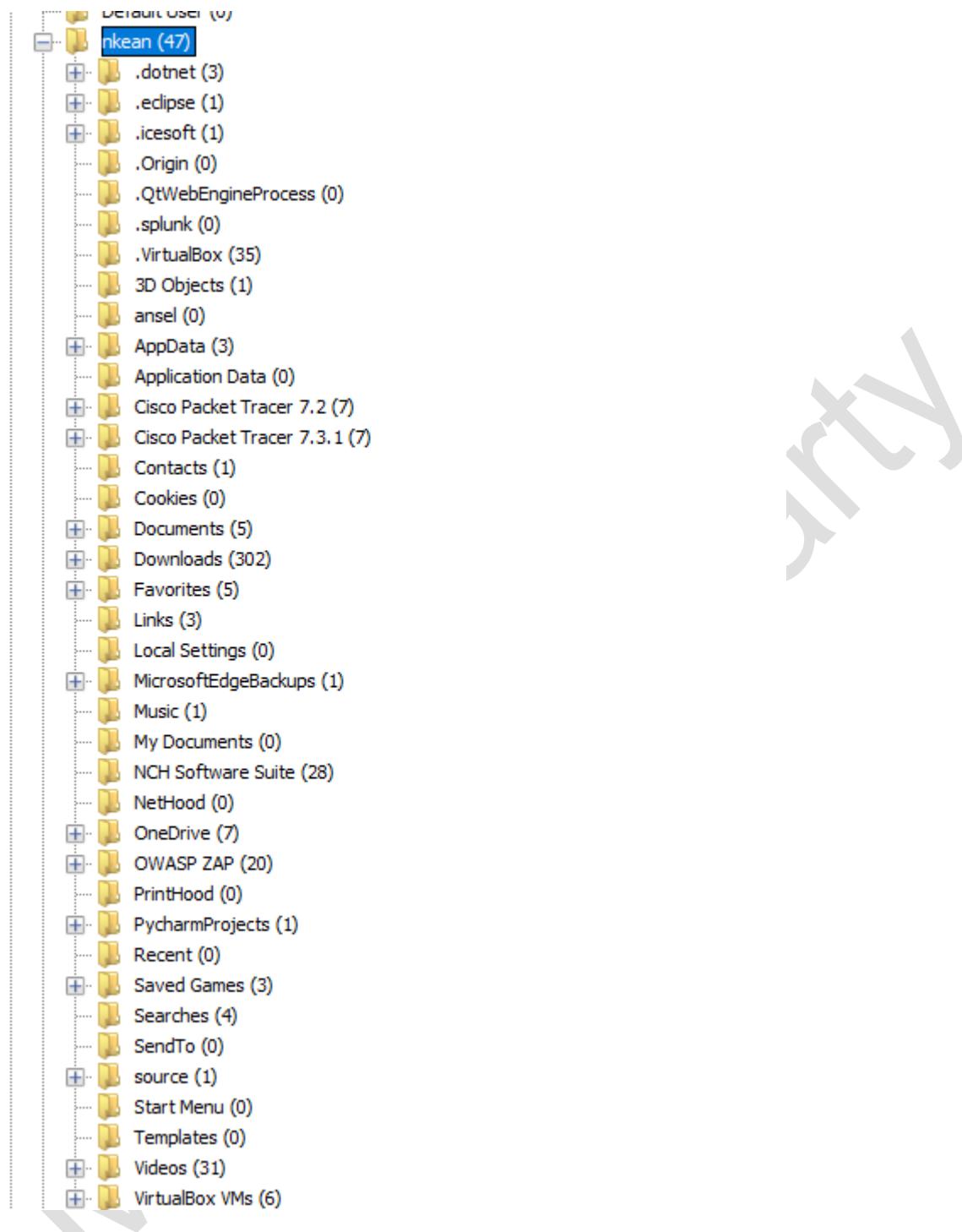
Step 2. Examine the contents of the Users directory.

A screenshot of the Autopsy interface showing a table of files in the 'LogicalFileSet1\Users' directory. The table has 14 columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, Location, and MD5 Hash. There are 6 results listed.

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

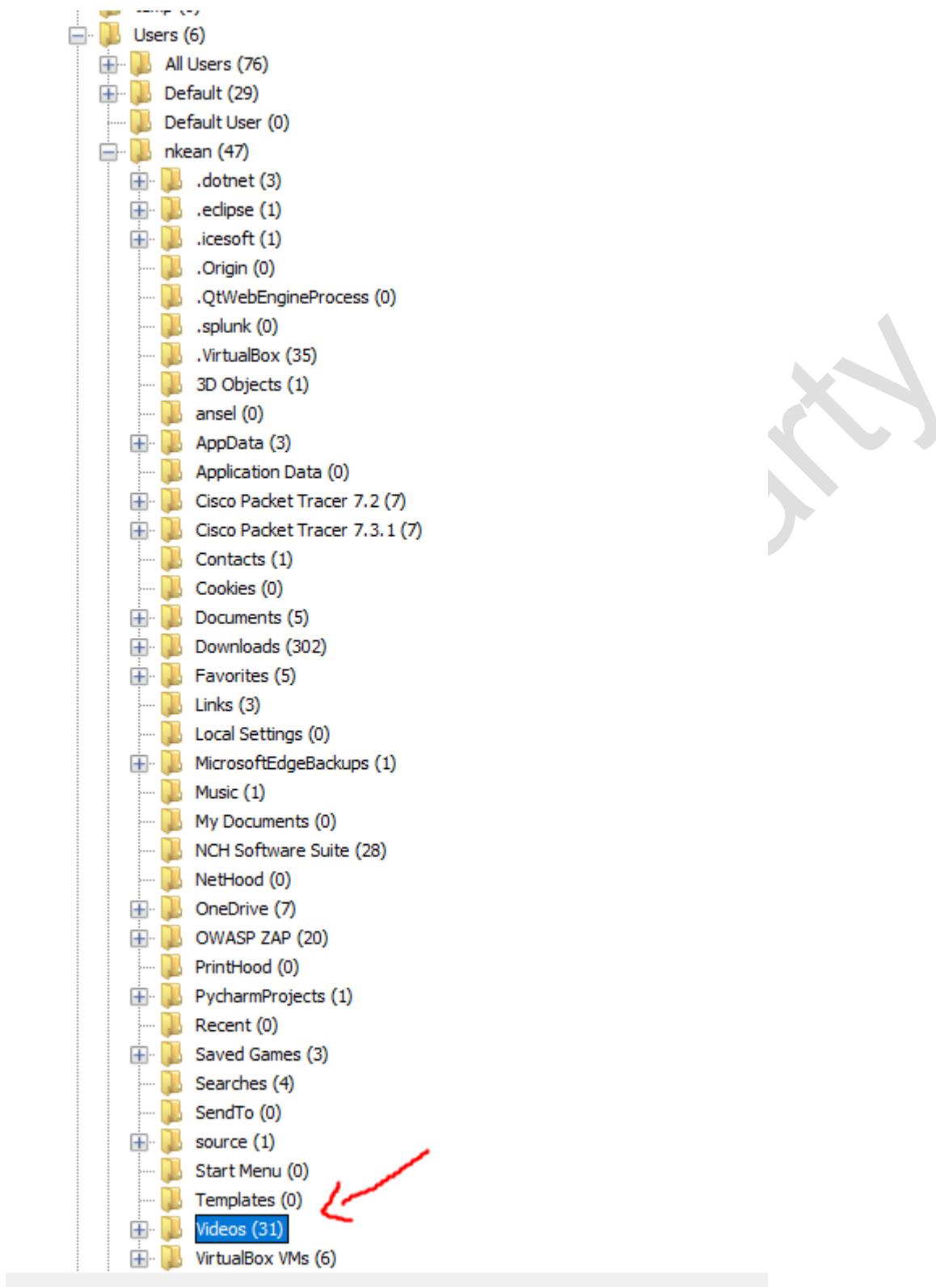
Step 3. Choose a user and investigate the contents.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs for 'Listing', 'LogicalFileSet1/Users/nkean/Videos', 'Table', 'Thumbnail', and 'Summary'. A 'Save Table as CSV' button is also visible. The main area is a table with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists numerous video files (mkv format) from the specified directory. Below the table, there's a preview pane with tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Application' tab is selected, showing a thumbnail of a video player interface with a play button and some video frames. Below the preview are playback controls (rewind, forward, volume, speed), with the speed set to 1x.

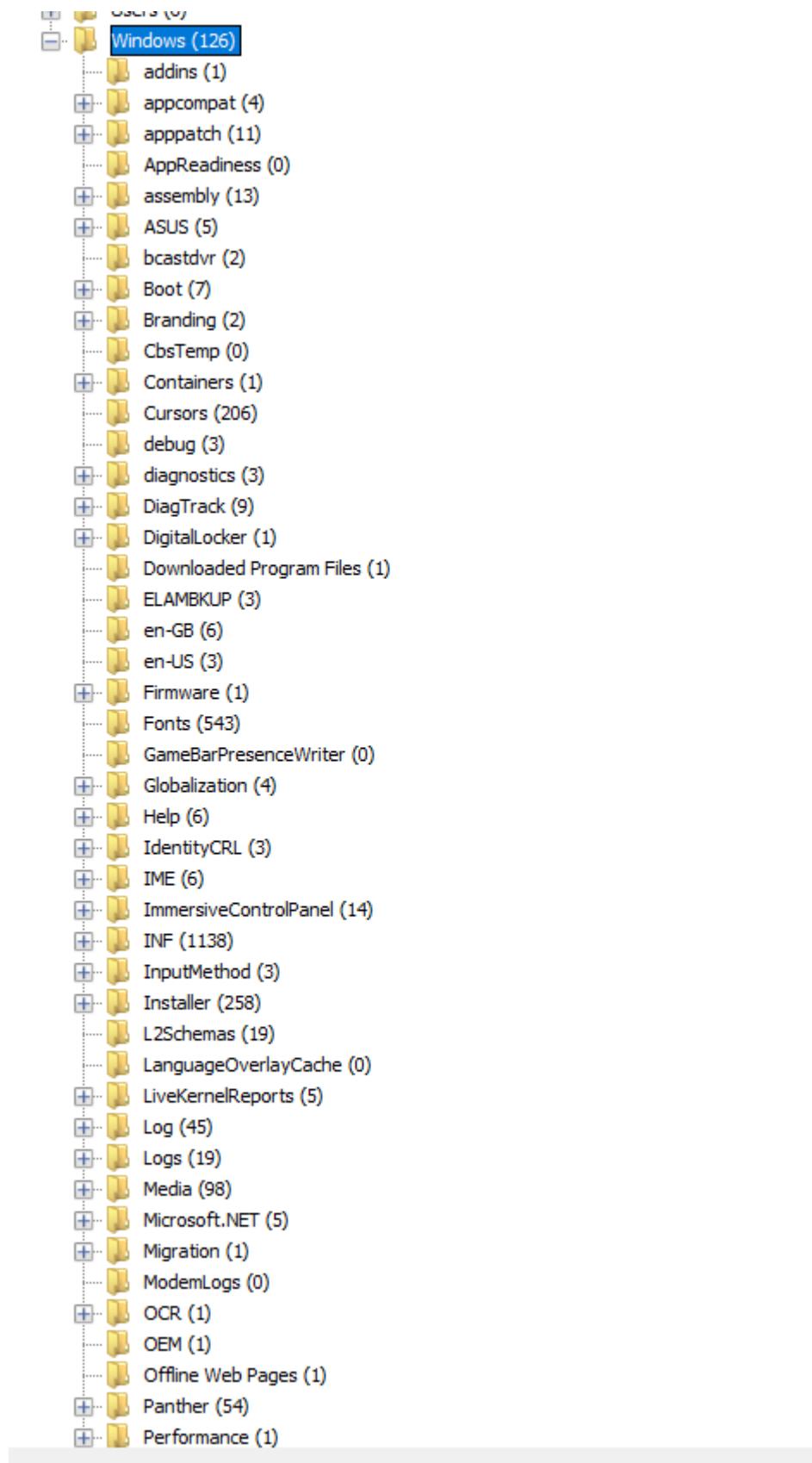
Windows

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



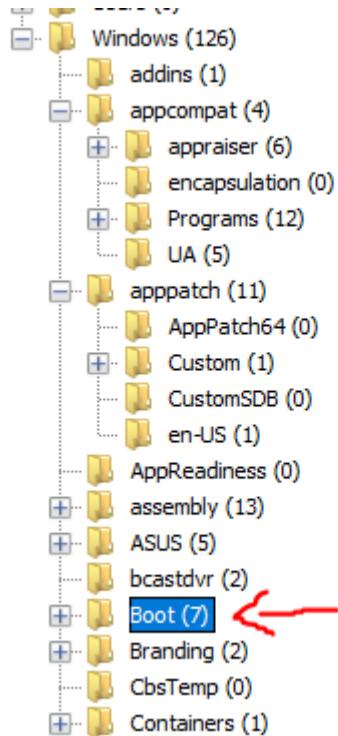
Step 2. Investigate the contents of the directory

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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

Listing /LogicalFileSet1/Windows/Boot											7 Results			
		S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
	DVD				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/Windows/Boot/DVD	
	EFI				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/Windows/Boot/EFI	
	Fonts				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/Windows/Boot/Fonts	
	Misc				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/Windows/Boot/Misc	
	PCAT				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/Windows/Boot/PCAT	
	Resources				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/Windows/Boot/Resources	
	BootDebuggerFiles.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	91	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/Boot/BootDebuggerFiles.ini	

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface with a file viewer window. The file path is /LogicalFileSet1/Windows/Boot/BootDebuggerFiles.ini. The file is 91 bytes long and is entirely allocated. The file content is displayed in hex and ASCII format. The hex dump shows the raw binary data, and the ASCII dump shows the text content, which includes boot debugger files and service files.

0x00000000: 3B 3B 20 42 6F 6F 74 20	64 65 62 75 67 67 65 72	;; Boot debugger
0x00000010: 20 66 69 6C 65 73 20 74	6F 20 73 65 72 76 69 63	files to servic
0x00000020: 65 0D 0A 0D 0A 5B 42 6F	6F 74 44 65 62 75 67 67	e....[BootDebugg
0x00000030: 65 72 46 69 6C 65 73 2E	50 43 41 54 5D 0D 0A 0D	erFiles.PCAT]...
0x00000040: 0A 5B 42 6F 6F 74 44 65	62 75 67 67 65 72 46 69	.[BootDebuggerFi
0x00000050: 6C 65 73 2E 55 45 46 49	5D 0D 0A	les.UEFI]..

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Listing Images															10000 Results
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	MIME Type	Extension
\$R6K0FG				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 186338	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R6SC9J				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 178989	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R6SS88				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 252754	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R74NZ5				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 3846769	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R76608				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 250325	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R8FUEI				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 3474266	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R8FUW				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 23309	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R8GIF				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 247682	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R8KS2R				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 207310	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R8M8A1				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 4353035	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R91VOS				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 187505	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$R9C9LU				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 176822	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R9GX5F				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 141133	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R9JCC5				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 203872	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$R9JZ93				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 176822	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$RA2A1S				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 189845	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
\$RA1U8L				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 220116	Allocated	Allocated	unknown	/LogicalFileSe...			png	
\$RALIZ7I				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 186338	Allocated	Allocated	unknown	/LogicalFileSe...			jpg	
appIcon.				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 1586	Allocated	Allocated	unknown	/LogicalFileSe...			png	
appIcon/				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 1413	Allocated	Allocated	unknown	/LogicalFileSe...			png	
appIcon_				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 1451	Allocated	Allocated	unknown	/LogicalFileSe...			png	
appLogo				0000-00-00 00:00:00 0000-00-00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 00:00:00...	0000-00-00 00:00:00 4279	Allocated	Allocated	unknown	/LogicalFileSe...			png	

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

Autopsy screenshot showing the file listing interface. A specific file, \$R6SS88, is selected and highlighted in blue. The file details show it is a 252754 byte image file located at /LogicalFileSe... with a known extension of jpg. The main pane displays the image itself, which is a grayscale biometric fingerprint.

Q. Did the image you chose load?

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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..
\$RVH1CX.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
Intro_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_Yarr_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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs for 'Listing', 'Videos', and 'Summary'. Below it, a table lists various files found on the system. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. Many files are MP4 format, such as '\$RISL_40K.mp4', '\$RQE5MBS.mp4', '\$RVH1CX.mp4', and '191008_FSTW_Console_EN_h264.mp4'. The 'Known' column shows 'unknown' for most files, and the 'Location' column shows paths like '/LogicalFileSet1/\$Recycle...' and '/LogicalFileSet1/Program F'. At the bottom of the table, there are buttons for 'Save Table as CSV' and 'Print'. Below the table is a video player interface. It has tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Application' tab is selected. A video frame from a file named '191008_FSTW_Console_EN_h264.mp4' is displayed. Below the frame are controls for 'Back', 'Play', 'Forward', 'Volume' (set to 1x), and a timestamp '00:00:00/00:21:59'.

Q. What kind of functionality has the video got?

Audio

Step 1. Navigate to Audio



Step 2. Investigate the audio files found.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
\$R71PE6K.mp3				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13344	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$R9L4RSP.mp3				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24228	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$R9V955K.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1034094	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$RE9RQSM.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	327832	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$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.
\$RLDGBO.mp3				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	24228	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$RNFI35L.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13344	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$ROWP38A.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	356160	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.
\$RUJR800.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	103724	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$RWLUUVUY.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	13344	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.
\$RYBW46N.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	103724	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.
a1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88560	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
a1s.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	182316	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
b1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88564	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
c1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	87596	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
c1s.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	180268	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
c2.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	87592	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
d1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88076	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
d1s.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	169332	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
e1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	87596	Allocated	Allocated	unknown	/LogicalFileSet1/Program F
f1.wav				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88076	Allocated	Allocated	unknown	/LogicalFileSet1/Program F

Step 3. Choose an audio file.

The screenshot shows the Autopsy digital forensics tool interface. A specific audio file, '\$R71PE6K.mp3', is selected in the list, highlighted with a blue selection bar. Below the list, there is a media player interface showing playback controls (rewind, play, fast forward), a volume slider set to 1x speed, and a timestamp of '00:00:00/Unknown'. The bottom navigation bar includes links for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Archives

Step 1. Navigate to archives



Step 2. Investigate the archive files

Listing Archives												
Table		Thumbnail		Summary								
Page: 1 of 1		Pages:		Go to Page: []								
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	6810472	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..
\$R7HRPH.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..
\$RCCEFDQ.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..
\$RCSENNXL.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.sprobe_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.hpeditor_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.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.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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs for 'Listing', 'Archives', 'Table' (which is selected), 'Thumbnail', and 'Summary'. Below that is a search bar with 'Page: 1 of 1' and 'Pages: < > Go to Page: []'. On the right, there are buttons for 'Save Table as CSV' and a magnifying glass icon. The main area displays a table of file metadata:

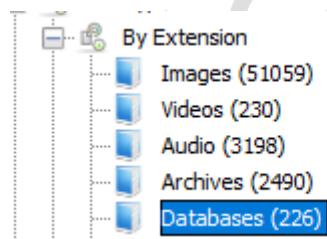
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Data.Cab				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	68106472	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle..
SpeechRecognition.zip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	233495	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..

Below the table is a hex dump of a file, showing bytes from 0x00000000 to 0x000000c0. The dump shows various file headers and data structures, including 'PK.....U(K..', '.....Sp', 'eechRecognition/...', '...vs/PK.....U', '...K.....(K.....', '.SpeechRecognit', 'ion/.vs/SpeechRe', 'ognition/PK....', '.....UI(K.....', '.....SpeechRe', 'ognition/.vs/Sp', 'eechRecognition/...', 'v14/PK.....^', and '7E 31 34 2F 50 4B 03 04 14 00 00 08 00 CC SE'.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Listing Databases														226 Results	
Table		Thumbnail		Summary										Save Table as CSV	
Page: 1 of 1		Pages: < > Go to Page: []													
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	MIME Type	Extension
winevt.rcc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6871040	Allocated	Allocated	unknown	/LogicalFileSe...		db	
winevt.rcc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6871040	Allocated	Allocated	unknown	/LogicalFileSe...		db	
core.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	196608	Allocated	Allocated	unknown	/LogicalFileSe...		db	
pp.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	143360	Allocated	Allocated	unknown	/LogicalFileSe...		db	
report.dtl				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	116868	Allocated	Allocated	unknown	/LogicalFileSe...		db	
a053060				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7070720	Allocated	Allocated	unknown	/LogicalFileSe...		db	
dscache.				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSe...		db	
rules.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	270336	Allocated	Allocated	unknown	/LogicalFileSe...		db	
ROGData				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2183168	Allocated	Allocated	unknown	/LogicalFileSe...		sqlite3	
configur2				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	196608	Allocated	Allocated	unknown	/LogicalFileSe...		sqlite	
.product				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	295	Allocated	Allocated	unknown	/LogicalFileSe...		db	
Launcher				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4	Allocated	Allocated	unknown	/LogicalFileSe...		db	
musicdat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Allocated	Allocated	unknown	/LogicalFileSe...		db	
botchatt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17079	Allocated	Allocated	unknown	/LogicalFileSe...		db	
botprofile				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12249	Allocated	Allocated	unknown	/LogicalFileSe...		db	
botprofl				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12723	Allocated	Allocated	unknown	/LogicalFileSe...		db	
navplace				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2777	Allocated	Allocated	unknown	/LogicalFileSe...		db	
.product				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	385	Allocated	Allocated	unknown	/LogicalFileSe...		db	
Launcher				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4	Allocated	Allocated	unknown	/LogicalFileSe...		db	
Armoury!				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Allocated	Allocated	unknown	/LogicalFileSe...		db	
BGFS.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Allocated	Allocated	unknown	/LogicalFileSe...		db	
E_13466				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	36864	Allocated	Allocated	unknown	/LogicalFileSe...		db	

Step 3. Choose a file to investigate.

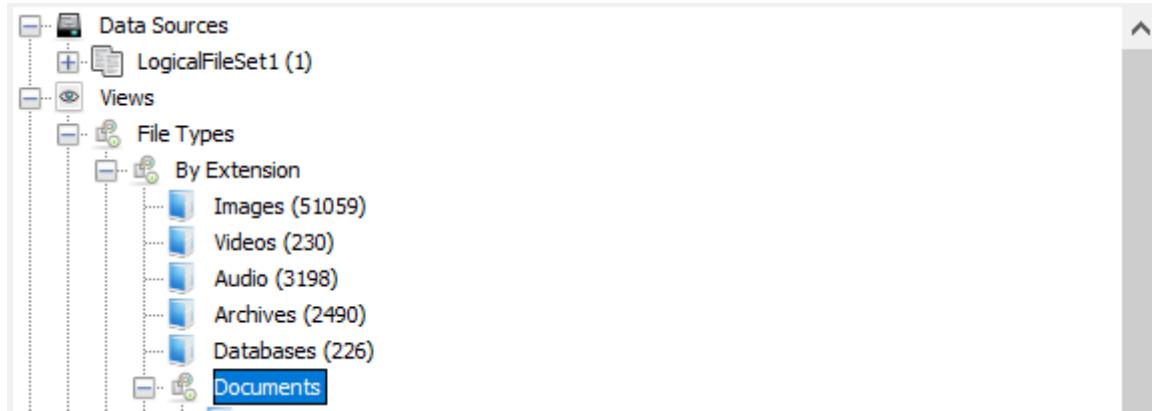
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	MIME Type	Extension	
winevt-rx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6871040	Allocated	Allocated	unknown	/LogicalFileSe...		db		
winevt-rx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6871040	Allocated	Allocated	unknown	/LogicalFileSe...		db		
core.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	196608	Allocated	Allocated	unknown	/LogicalFileSe...		db		
pp.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	143360	Allocated	Allocated	unknown	/LogicalFileSe...		db		
report.dt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	114688	Allocated	Allocated	unknown	/LogicalFileSe...		db		
a053060				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7070720	Allocated	Allocated	unknown	/LogicalFileSe...		db		
dscache.				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSe...		db		
rules.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	270336	Allocated	Allocated	unknown	/LogicalFileSe...		db		
ROGData				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2183168	Allocated	Allocated	unknown	/LogicalFileSe...		sqlite3		
configur				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	196608	Allocated	Allocated	unknown	/LogicalFileSe...		sqlite		
.product				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	295	Allocated	Allocated	unknown	/LogicalFileSe...		db		
Launcher				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4	Allocated	Allocated	unknown	/LogicalFileSe...		db		
musicdat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	57344	Allocated	Allocated	unknown	/LogicalFileSe...		db		
botchatb				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17079	Allocated	Allocated	unknown	/LogicalFileSe...		db		
botprofile				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12249	Allocated	Allocated	unknown	/LogicalFileSe...		db		
botproflik				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12723	Allocated	Allocated	unknown	/LogicalFileSe...		db		
navplace				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2777	Allocated	Allocated	unknown	/LogicalFileSe...		db		
.product				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	385	Allocated	Allocated	unknown	/LogicalFileSe...		db		
Launcher				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4	Allocated	Allocated	unknown	/LogicalFileSe...		db		
Armoury!				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20490	Allocated	Allocated	unknown	/LogicalFileSe...		db		
BGFS.db				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Allocated	Allocated	unknown	/LogicalFileSe...		db		
E_13466				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	36864	Allocated	Allocated	unknown	/LogicalFileSe...		db		

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Documents

Step 1. Navigate to documents.



HTML

Step 1. Navigate to HTML



Step 2. Investigate the findings of HTML

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-
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	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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 3. Choose a html file to investigate

Listing [HTML](#)

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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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/5-1-5-
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
PrivacyPolicy_en-GB.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	29971	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Sc

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

Office

Step 1. Navigate to Office



Step 2. Investigate the contents of Office.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
SR6V01SR.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	106208	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B
ReleaseNote_FileList of GA502IU_19H2_64_V2.02.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	54272	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
styles.odt				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/Program Fil
PROTTPLN.DOC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLN.PPT				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLN.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8704	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.DOC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.PPT				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8704	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
SOLVSAMP.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	118784	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
EXCEL12.XLSX				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5760	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
POWERPOINT.PPTX				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 Fil
WORD.DOCX				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 Fil
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
TMTGettingStartedGuide.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1277227	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
thirdpartylegalnotices.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	362496	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ThirdPartyLegalNotices.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25088	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Program Da
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Users/All U
Text Sidebar (Annual Report Red and Black design).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	47296	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkeea
Text Sidebar (Annual Report Red and Black design).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	47296	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkeea

Step 3. Choose a file to investigate

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface with a file listing and a detailed file metadata view.

File Listing: A table showing 232 results. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The file `POWERPOINT.PPTX` is selected and highlighted in blue.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
\$R6V01SR.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	106208	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B&e5upport/e
ReleaseNote_FileList of GA502IU_19H2_64_V2.02.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	54272	Allocated	Allocated	unknown	/LogicalFileSet1/e5upport/e
styles.odt				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/Program Fil
styles.odt				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/Program Fil
PROTTPLN.DOC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLN.PPT				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLN.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8704	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.DOC				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	19968	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.PPT				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	12288	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PROTTPLV.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8704	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
SOLVSAMP.XLS				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	118784	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
EXCEL 12.XLSX				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5760	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
POWERPOINT.PPTX				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 Fil
WORD.DOCX				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 Fil
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
TMTGettingStartedGuide.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1277227	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
thirdpartylegalnotices.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	362496	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ThirdPartyLegalNotices.doc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	25088	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Program Da
FrameView SDK License (3Sept2020).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51260	Allocated	Allocated	unknown	/LogicalFileSet1/Users/All U
Text Sidebar (Annual Report Red and Black design).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	47296	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkea
Text Sidebar (Annual Report Red and Black design).docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	47296	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkea

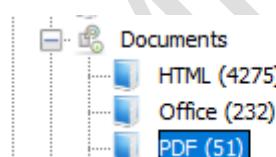
File Metadata: A detailed view of the selected file `POWERPOINT.PPTX`.

Name	/LogicalFileSet1/Program Files/Microsoft Office/root/vfs/Windows/SHELLNEW/POWERPOINT.PPTX
Type	Local
MIME Type	application/octet-stream
Size	0
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	0000-00-00 00:00:00
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
MD5	Not calculated

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

PDF

Step 1. Navigate to PDF



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 2. Investigate the contents of the pdf documents.

Listing												
PDF												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
\$1SMXDK8.pdf				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	174	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B
\$RSMXDK8.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842153	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B
testdisk.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	245754	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
regripper.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	160531	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PacketTracerOpenSource.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1044438	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ReferenceCard.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	193166	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ReferenceCardForMac.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	250870	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
UserManual.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4906664	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
FFmpeg_Build.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	236957	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
260982170-Comptia-Net-Notes_1 (1).pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	966205	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
260982170-Comptia-Net-Notes_1.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	966205	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
B00122534NialKearneCA3.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2224863	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
B00122534NialKearneOSSIMSpec.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1776427	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
DWVA_v1.3.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	422011	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
FTKImager_UserGuide.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	646968	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
NialKearne_B00122534_C42.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	343466	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
NialKearne_B00122534_ResearchPaper.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	351661	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
Obstructed_Devices.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5909753	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
Research for project proposal.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32105	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
B00122534NialKearneCA3.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2224863	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
Activation.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1126472	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
Neurotechnology Biometric SDK.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7129921	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil

Step 3. Choose a pdf to investigate.

Listing												
PDF												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
\$1SMXDK8.pdf				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	174	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B
\$RSMXDK8.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	842153	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.B
testdisk.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	245754	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
regripper.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	160531	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
PacketTracerOpenSource.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1044438	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ReferenceCard.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	193166	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
ReferenceCardForMac.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	250870	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
UserManual.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4906664	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
FFmpeg_Build.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	236957	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
260982170-Comptia-Net-Notes_1 (1).pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	966205	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil
260982170-Comptia-Net-Notes_1.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	966205	Allocated	Allocated	unknown	/LogicalFileSet1/Program Fil

Hex Text Application File Metadata Context Results Annotations Other Occurrences

NETWOK MODELS

networking model = refers to a comprehensive set of documents, protocol = is a set of logical rules that devices must follow to communicate, TCP/IP = a set of protocols that references a large collection of protocols (ICMP) that allow computers to communicate

network segmentation = breaking networks into smaller subnets collision domain = all stations on a segment can receive a packet and everybody listens switch = creates different collision domains within a single broadcast domain router = creates multiple broadcast domains for each interface

Layer 2: Data Link Layer

Layer 3: Network Layer

Layer 4: Transport Layer

Layer 5: Session Layer

Layer 6: Presentation Layer

Layer 7: Application Layer

Page 1 / 8

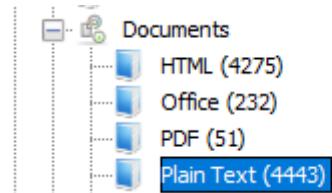
Detailed description: This screenshot shows the 'File Metadata' tab in the Autopsy application. It displays a table of file metadata for various PDF files. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. The table lists files such as \$1SMXDK8.pdf, \$RSMXDK8.pdf, testdisk.pdf, regripper.pdf, PacketTracerOpenSource.pdf, ReferenceCard.pdf, ReferenceCardForMac.pdf, UserManual.pdf, FFmpeg_Build.pdf, 260982170-Comptia-Net-Notes_1 (1).pdf, 260982170-Comptia-Net-Notes_1.pdf, and B00122534NialKearneCA3.pdf. The 'Known' column indicates that most files are unknown, while others are allocated or have specific flags like 'Allocated'. The 'Location' column shows paths like /LogicalFileSet1/\$Recycle.B and /LogicalFileSet1/Program Fil. Below the table, there is a detailed description of networking models, specifically mentioning TCP/IP, network segmentation, switches, routers, and layers 2 through 7 of the OSI model. A legend at the bottom identifies the layers: Layer 2 (Data Link Layer), Layer 3 (Network Layer), Layer 4 (Transport Layer), Layer 5 (Session Layer), Layer 6 (Presentation Layer), and Layer 7 (Application Layer).

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Plain Text

Step 1. Navigate to Plain Text.



Step 2. Investigate the contents of Plain Text

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	MIME Type	Extension
\$_DEPZ7		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	110	Allocated	Allocated	unknown	/LogicalFileSe...	6848b572cdce...	text/plain	.txt
\$_IE3RYN		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	120	Allocated	Allocated	unknown	/LogicalFileSe...	be15eff38cdb8...	text/plain	.txt
\$_GFRREV	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	130	Allocated	Allocated	unknown	/LogicalFileSe...	633820347031...	text/plain	.txt
\$_J59LOC	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	132	Allocated	Allocated	unknown	/LogicalFileSe...	19bf341d468cb...	text/plain	.txt
\$_IVADUT	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	136	Allocated	Allocated	unknown	/LogicalFileSe...	546b97094cf8e...	text/plain	.txt
SpeechR				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	7653	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
SpeechR				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	7653	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
\$_RDEPZ7				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	1235	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
\$_RESRYN				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	/LogicalFileSe...			.txt
\$_RGFRREV				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	/LogicalFileSe...			.txt
\$_J59L0				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	/LogicalFileSe...			.txt
SpeechR				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	5865	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
SpeechR				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	7653	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
\$_RVADU				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	/LogicalFileSe...			.txt
devlist.b	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	17681	Allocated	Allocated	unknown	/LogicalFileSe...	e293bbb27ec6...	text/plain	.txt
FileList.b				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	34285	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	904	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	1764	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	5209	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	11558	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	1516	Allocated	Allocated	unknown	/LogicalFileSe...			.txt
LICENSE,				0000-00-00 00:00:00	0000-00-00 00:00:00...	0000-00-00 00:00:00...	0000-00-00 00:00:00	1582	Allocated	Allocated	unknown	/LogicalFileSe...			.txt

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

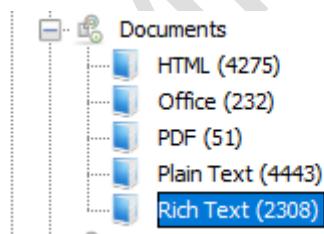
Step 3. Choose a plain text file to investigate.

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs like 'Listing', 'Thumbnail', and 'Summary'. Below it, a table displays 4443 results. The columns include Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, Location, MD5 Hash, MIME Type, and Extension. A specific file named 'SpeechR' is highlighted in blue. Below the table is a 'Hex' tab showing a hex dump of the file content, with the first few bytes being 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 followed by file metadata and context information.

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

Rich Text

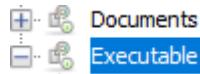
Step 1. Navigate to Rich text



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Executable

Step 1. Navigate to executable



.Exe

Step 1. Navigate to .exe



Step 2. Investigate the contents of .exe

Listing																	Save Table as CSV	
.exe																		
Table																	Thumbnail	
Page:	1	of	2	Pages:	<	>	Go to Page:											
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	MIME Type	Extension			
\$_\$5LNc.	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	116	Allocated	Allocated	unknown	/LogicalFileSe...	68f31732b959...	application/octet...	exe			
\$_\$6SNXT	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	130	Allocated	Allocated	unknown	/LogicalFileSe...	caedceaf18b04...	application/octet...	exe			
\$_\$77IAR0L	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	110	Allocated	Allocated	unknown	/LogicalFileSe...	a3c913d04e8c...	application/octet...	exe			
\$_\$A8J27	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	110	Allocated	Allocated	unknown	/LogicalFileSe...	b693b3c01d8...	application/octet...	exe			
\$_\$AD0F2	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	110	Allocated	Allocated	unknown	/LogicalFileSe...	9d849466910b...	application/octet...	exe			
\$_\$E7FJQJ	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	116	Allocated	Allocated	unknown	/LogicalFileSe...	3e6b0001bae8...	application/octet...	exe			
\$_\$EOQII	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	108	Allocated	Allocated	unknown	/LogicalFileSe...	b13ff5d6f84bb...	application/octet...	exe			
\$_\$HCND2	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	188	Allocated	Allocated	unknown	/LogicalFileSe...	bdceb79d5cc1f...	application/octet...	exe			
\$_\$JCG4Z	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	106	Allocated	Allocated	unknown	/LogicalFileSe...	9479a9863324...	application/octet...	exe			
\$_\$KGT6K	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	110	Allocated	Allocated	unknown	/LogicalFileSe...	2ced4b4a20bc...	application/octet...	exe			
\$_\$L5T9YU	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	130	Allocated	Allocated	unknown	/LogicalFileSe...	098a80f97cb79...	application/octet...	exe			
\$_\$LSVLGF	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	162	Allocated	Allocated	unknown	/LogicalFileSe...	094ff723325b2...	application/octet...	exe			
\$_\$LV2F2	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	106	Allocated	Allocated	unknown	/LogicalFileSe...	e9c73f776061f...	application/octet...	exe			
\$_\$OSR VF	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	230	Allocated	Allocated	unknown	/LogicalFileSe...	b2cc7fb453f29...	application/octet...	exe			
\$_\$Q8MN2	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	126	Allocated	Allocated	unknown	/LogicalFileSe...	ff0906037c68c...	application/octet...	exe			
\$_\$T6UW1	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	126	Allocated	Allocated	unknown	/LogicalFileSe...	79aa41643a2c...	application/octet...	exe			
\$_\$VBL0X	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	108	Allocated	Allocated	unknown	/LogicalFileSe...	98d7d26dace...	application/octet...	exe			
\$_\$VMQOY	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	126	Allocated	Allocated	unknown	/LogicalFileSe...	c3b67615856...	application/octet...	exe			
\$_\$WS4H:	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	144	Allocated	Allocated	unknown	/LogicalFileSe...	48d9b0e685bb...	application/octet...	exe			
\$_\$YB1OK	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	108	Allocated	Allocated	unknown	/LogicalFileSe...	e28e360db735...	application/octet...	exe			
\$_\$ZU20D	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...	0000-00-00 00:00:00...	0000-00-00 00:00:00...	108	Allocated	Allocated	unknown	/LogicalFileSe...	b451c3fa11e0...	application/octet...	exe			
instmsia.				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	/LogicalFileSe...			exe			

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

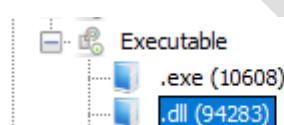
Step 3. Choose a .exe file to investigate

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	MIME Type	Extension
\$IKGT6K	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 110	Allocated	Allocated	unknown	/LogicalFileSe...	2ced4b4a20bc...	application/octet... exe					
\$IL5T9YL	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 130	Allocated	Allocated	unknown	/LogicalFileSe...	098a80f97cb79...	application/octet... exe					
\$LSVLGF	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 162	Allocated	Allocated	unknown	/LogicalFileSe...	09f4f723325b2...	application/octet... exe					
\$ILV22F	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 106	Allocated	Allocated	unknown	/LogicalFileSe...	e9c73f77601f...	application/octet... exe					
\$DSRVRF	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 230	Allocated	Allocated	unknown	/LogicalFileSe...	b2cc7fb453f29...	application/octet... exe					
\$IQ8MNQ	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 126	Allocated	Allocated	unknown	/LogicalFileSe...	ff0906037c66c...	application/octet... exe					
\$IT6UWI	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 126	Allocated	Allocated	unknown	/LogicalFileSe...	79aa41643a2c...	application/octet... exe					
\$IVBLOX:	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 108	Allocated	Allocated	unknown	/LogicalFileSe...	98d7d26dcbe...	application/octet... exe					
\$IVMQO!	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 126	Allocated	Allocated	unknown	/LogicalFileSe...	c3b676615856...	application/octet... exe					
\$IVWS4H:	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 144	Allocated	Allocated	unknown	/LogicalFileSe...	48d9b0e665bb...	application/octet... exe					
\$IVBIKO!	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 108	Allocated	Allocated	unknown	/LogicalFileSe...	e28e360db735...	application/octet... exe					
\$IZU20D	1	0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 108	Allocated	Allocated	unknown	/LogicalFileSe...	b451c3fa1ee0...	application/octet... exe					
instmsia.		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 1513987	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
instmsiw.		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 1526275	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
msttss22		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 2065144	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
setup.exe		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 102400	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpTTInI		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 3665264	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpeechR		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 22016	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpeechR		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 21464	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpeechR		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 22016	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpeechSI		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 71275886	Allocated	Allocated	unknown	/LogicalFileSe...		exe					
SpeechSI		0000-00-00 00:00:00 0000-00-00 00:00...	0000-00-00 00:00:00 00:00...	0000-00-00 00:00:00 85495160	Allocated	Allocated	unknown	/LogicalFileSe...		exe					

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
\$ILLUOH.dll			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	98	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
My Project.Resources.Designer.vb.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	7680	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
My Project.Resources.Designer.vb.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	7680	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
eclipse_1503.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	57344	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	176128	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	176128	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
My Project.Resources.Designer.vb.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	7680	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
\$RLLUOH.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	1094656	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
My Project.Resources.Designer.vb.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	7680	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
AsDriverCD.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	278480	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
AsusBLEAPI.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	204408	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
msvcp140.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	636256	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
vccorlib140.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	375136	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
vruntime140.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	94072	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
ASUS.Zaw.CmdManager.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	388728	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
athr_swoi_wifi.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	653432	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
Autofac.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	237720	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e

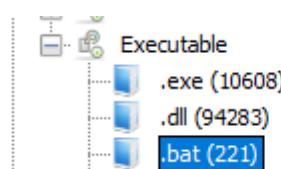
Step 3. Choose a file to investigate.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
Interop.SpeechLib.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	166912	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
My Project.Resources.Designer.vb.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	7680	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.BI
AsDriverCD.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	278480	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
AsusBLEAPI.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	204408	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
msvcp140.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	636256	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
vccorlib140.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	375136	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
vruntime140.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	94072	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
ASUS.Zaw.CmdManager.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	388728	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
athr_swoi_wifi.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	653432	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e
Autofac.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	237720	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/e

Q. What is the purpose of .dll files?

.Bat

Step 1. Navigate to .bat



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 2. Investigate the contents of .bat

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
InstallPackage.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1644	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	34	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	36	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	133	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	938	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
NvContainerRecovery.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1951	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	168	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	82	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
NvContainerRecovery.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1951	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install_PTP.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	386	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
InstallAPO.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	385	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentInstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
SilentUninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	222	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	197	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentInstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	142	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentUninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	74	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	120	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	56	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software

Step 3. Choose a .bat file to examine

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	45	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
InstallPackage.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1644	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	34	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	36	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	133	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	938	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
NvContainerRecovery.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1951	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	168	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	82	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
NvContainerRecovery.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1951	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
Install_PTP.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	386	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
setup.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	192	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
InstallAPO.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	385	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentInstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	119	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
SilentUninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	122	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	222	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	197	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentInstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	142	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
silentUninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	74	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	120	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
uninstall.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	88	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software
install.bat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	56	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Page: 1 of 1 Page Go to Page: Jump to Offset: 0 Launch in HexD

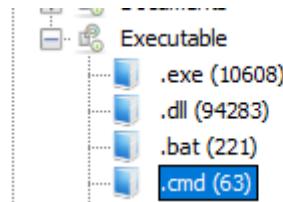
0x00000000: F0 75 73 69 64 20 32 35 7E 64 70 30 22 0D 0A 44 Pushd "\$_dp" .. D
0x00000010: 43 6C 73 65 74 75 70 2E 65 78 65 20 2D 73 20 2D C:\setup.exe -s -
0x00000020: EE 20 2D 6C 6F 67 3A 25 73 79 73 74 65 ED 64 72 n-log\sysmon
0x00000030: E9 76 65 2B 6C 77 69 6E 64 6F 77 73 5C 74 65 6D iev\windows\item
0x00000040: 70 5C 42 76 69 65 61 4C 6F 67 73 20 2D 6C 6F p\NvidiaLogs -lo
0x00000050: E7 6C 65 76 65 62 3A 36 0D 0A 57 49 4E 33 32 55 glevel:6..WIN32U
0x00000060: 58 6C 73 65 74 75 70 2E 67 85 20 2D 73 20 2D X\setup.exe -s -
0x00000070: EE 20 2D 6C 6F 67 3A 25 73 79 73 74 65 ED 64 72 n-log\sysmon
0x00000080: E9 76 65 25 6C 77 69 6E 64 6F 77 73 5C 74 65 6D iev\windows\item
0x00000090: 70 5C 42 76 69 65 61 4C 6F 67 73 20 2D 6C 6F p\NvidiaLogs -lo
0x000000a0: E7 6C 65 76 65 6C 3A 36 glevel:6

Q. What are .bat files?

.CMD

Step 1. Navigate to .CMD

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Step 2. Investigate the contents of .cmd

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ActRec.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	23	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software/
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/NVIDIA Corp/
win_postinstall.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	6784	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Oracle/Virtual
VSPerfCLREnv.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	7733	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsoft/
mime.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	170	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/NVIDIA/
mkdirp.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	182	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/NVIDIA/
remove0527.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	202	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Razer/A
Microsoft .NET Framework 4.6.2.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	142	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
noop.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	22	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
Microsoft Visual C++ 2015 x64.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	121	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
Microsoft Visual C++ 2015 x86.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	117	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
Microsoft Visual C++ 2017 x64.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	121	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
Microsoft Visual C++ 2017 x86.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	117	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/s
unattend.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	555	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/VMware,
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/ProgramData/NVIDIA Corpor
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/OEM/oemsetupRe
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/OEM/Refresh.cmd
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/OEM/Reset.cmd
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/Users/All Users/NVIDIA Corp
30_firewall-drop.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	1130	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop
31_netsh.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	1023	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop
32_restart-ossec.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	519	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nkean/OneDrive/Desktop

Step 3. Choose a .cmd file to investigate

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

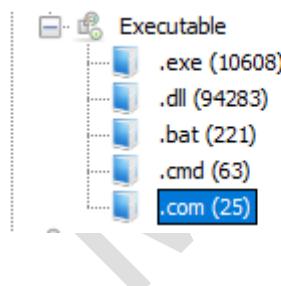
The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs like 'Listing', 'Thumbnail', and 'Summary'. Below it is a table of file entries with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), Known, and Location. A specific file, 'nidkrp.cmd', is selected and highlighted in blue. The bottom half of the screen shows a hex editor with tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The 'Hex' tab is active, displaying binary code. The status bar at the bottom shows 'Page: 1 of 1' and 'Jump to Offset 0'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
ActRec.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	23	Allocated	Allocated	unknown	/LogicalFileSet1/eSupport/eDriver/Software/I
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/NVIDIA Corpor
win_postinstall.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	6784	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files/Virtual
VSPerfCLREnv.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	7733	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Microsof
mime.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	170	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/NVIDIA
nidkrp.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	182	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/NVIDIA
remove0527.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	202	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Razer/A
Microsoft .NET Framework 4.6.2.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	142	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
noop.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	22	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
Microsoft Visual C++ 2015 x64.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	121	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
Microsoft Visual C++ 2015 x86.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	117	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
Microsoft Visual C++ 2017 x64.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	121	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
Microsoft Visual C++ 2017 x86.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	117	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Steam/S
unattend.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	555	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/Vmware,
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/Program Files (x86)/NVIDIA Corpor
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/OEM/oemsetupRe
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/OEM/refresh.cmd
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/OEM/reset.cmd
nvinstall.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	553	Allocated	Allocated	unknown	/LogicalFileSet1/Users/NVIDIA Corp
30_firewall-drop.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	1130	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nikean/OneDrive/Desktop
31_nethsh.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	1023	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nikean/OneDrive/Desktop
32_restart-ossec.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	519	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nikean/OneDrive/Desktop

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

.com

Step 1. Navigate to .com



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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/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	12800	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	26624	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/WinSxS/wow64_microsoft-windo...

Step 3. Choose a .com file to investigate.

Listing												
.com												
Table Thumbnail Summary												
Page:	1 of 1	Pages:	←	→	Go to Page:	<input type="text"/>						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
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:	<input type="text"/>	Jump to Offset	<input type="text"/> Launch in HxD
0x00000000: 4D 5A 00 00 03 00 00 00 04 00 00 FF 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 00 00 00 00							
0x00000040: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 E8!..L!Tn							
0x00000050: E9 73 20 70 72 6F 67 72 E1 ED 20 E3 61 E6 E6 E9 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: ED 6F 64 65 3E 0D 0D OA 24 00 00 00 00 00 00 mode....@.....							
0x00000080: E1 E8 C7 7B A5 A9 A5 A8 A5 A9 A9 A8 ..{...({...({							
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 A8 28 DC 89 A9 28 B1 E2 A9 29 AC 89 A9 28 ..){...({...({...({							
0x000000C0: B1 E2 A9 29 A7 89 A9 28 B1 E2 SE 28 A4 89 A9 28 ..){...({...({...({							

Q. What is the purpose of these files?

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Mime Type

Step 1. Navigate to “By Mime type”

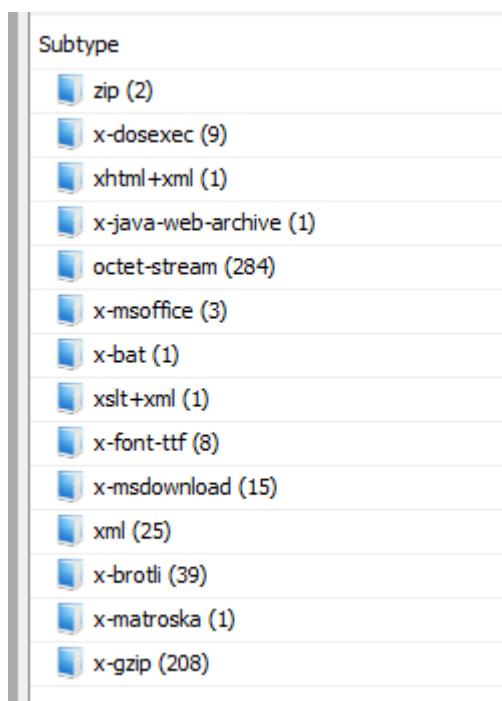


Application

Step 1. Navigate to application

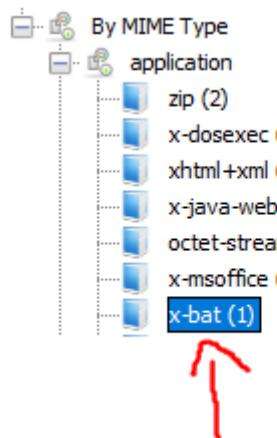


Step 2. Investigate the contents of the application directory



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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Step 4. Investigate the contents of x-bat

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
NvContainerRecovery.bat	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	0000-00-00 00:00:00	0000-00-00 00:00:00	1951	Allocated	Allocated	unknown	/LogicalFileSet1/Windows/NvContainerRecovery.bat

Step 5. Examine the contents of nocontainerecovery

```
Hex Text Application File Metadata Context Results Annotations Other Occurrences
Strings Indexed Text Translation
Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% ⚡ ⚡ Reset
Echo off
if "%1" == "" (
    echo Usage: NvContainerRecovery (Service Name)
    goto NvContainerRecoveryEnd
)
set _LOG_FILE=NvContainerRecovery.log
if not "%2" == "" set _RECOVERY_FILE=%LOCALAPPDATA%\NVIDIA\NvContainerRecovery%1.reg
echo Create recovery registry file %__RECOVERY_FILE% > %__LOG_FILE%
echo REGEDIT4 > %__RECOVERY_FILE%
echo. >> %__RECOVERY_FILE%
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NVIDIA Corporation\NvContainer\%1] >> %__RECOVERY_FILE%
echo "Recovery"=dword:00000001 >> %__RECOVERY_FILE%
echo. >> %__RECOVERY_FILE%
```

Q. What is the purpose of the file?

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Audio

Step 1. Navigate to Audio



Step 2. Examine the contents of the audio directory

A screenshot of the 'Listing' view in Autopsy. It shows a table with one result: 'vnd.wave (1)'. The table has columns for Page, Pages, Go to Page, Subtype, and a preview icon. A 'Save Table as CSV' button is visible in the top right.

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

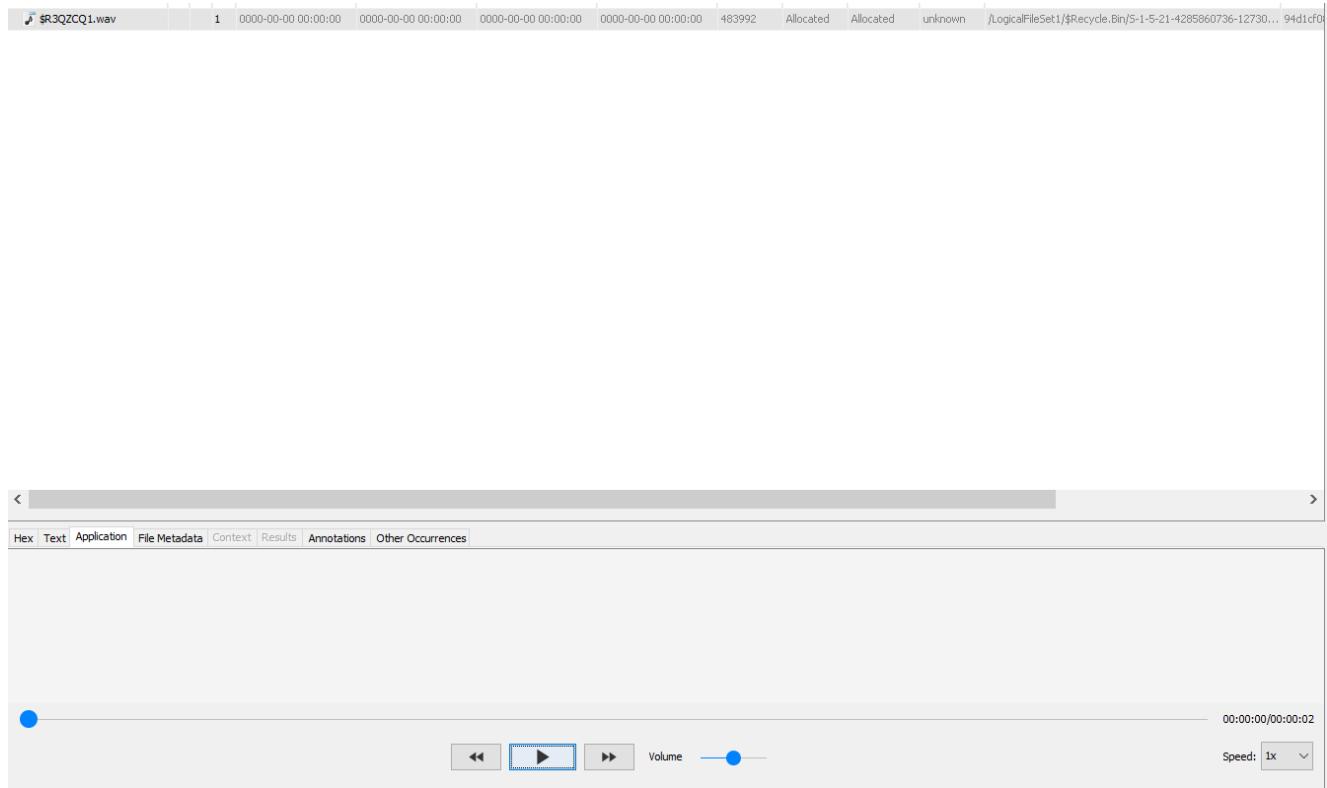
A screenshot of the 'Subtype' view in Autopsy. It shows a single item: 'vnd.wave (1)', which is highlighted with a blue selection bar.

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
\$R3QZCQ1.wav		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	483992	Allocated	Allocated	unknown

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

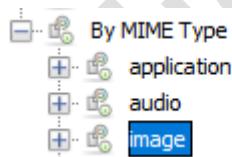
Step 5. Investigate the hidden audio file if you have found one.



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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the 'image' section of the Autopsy software. At the top, there are tabs for 'Listing' (which is selected), 'Table', 'Thumbnail', and 'Summary'. Below the tabs are buttons for 'Page:', 'Pages:', 'Go to Page:', and a search input field. A section titled 'Subtype' is expanded, showing a list of file types with their counts: gif (24), jpeg (35), png (38), vnd.microsoft.icon (4), and webp (10). Each item has a small thumbnail icon next to it.

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

The screenshot shows the same 'image' section as before, but with the 'gif' option highlighted by a blue selection bar. The other subtypes (jpeg, png, vnd.microsoft.icon, webp) are visible below it.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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				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/5-1-5-2
UpgradeReport_Plus.gif				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/5-1-5
data_3_c1030048				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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				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

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

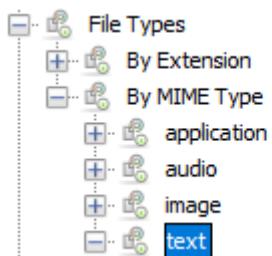
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
UpgradeReport_Minus.gif	1			2010-11-02 15:57:00 GMT	2000-00-00 00:00:00	0000-00-00 00:00:00	2000-00-00 00:00:00	69	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-2
UpgradeReport_Plus.gif	1			2010-11-02 15:57:00 GMT	2000-00-00 00:00:00	0000-00-00 00:00:00	2000-00-00 00:00:00	71	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-2
data_3_a01304b	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_a0010166	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_b1020b2	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

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Text

Step 1. Navigate to text



Step 2. Examine the contents of the text directory

A screenshot of a digital forensics interface showing a 'Listing' for the 'text' directory. The interface includes a header with tabs for 'Table' (selected), 'Thumbnail', and 'Summary', and controls for 'Page:' and 'Go to Page:'. Below this is a section titled 'Subtype' with a triangle icon. A list of subtypes is shown with icons and counts: css (1), html (28), plain (203), x-ini (7), x-java-source (2), x-log (33), x-matlab (5), x-vbdotnet (18), and xml (42).

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy software interface with the following details:

- Listing** tab selected.
- text** filter applied.
- Table** view selected.
- Pages:** Page 1 of 1, Pages: < > Go to.
- Subtype** section expanded, showing categories: css (1), html (28), plain (203), x-ini (7), x-java-source (2), x-log (33), x-matlab (5), x-vbdotnet (18), and **xml (42)** (selected).

Step 4. Examine the contents of the xml directory

The screenshot shows a detailed listing of XML files in the XML directory:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
UpgradeLog.XML			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	5720	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-21-
UpgradeLog.XML			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	5720	Allocated	Allocated	unknown	/LogicalFileSet1/\$Recycle.Bin/S-1-5-21-
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
data_1_a101034			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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L
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	/LogicalFileSet1/Users/nkean/AppData/L

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

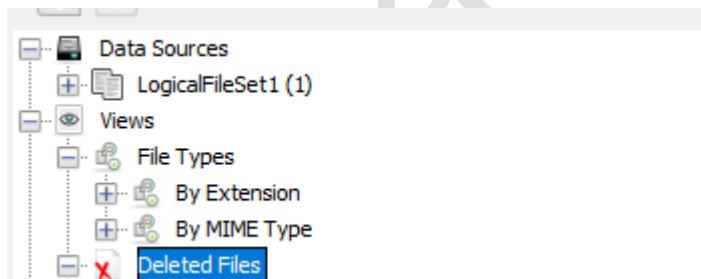
Step 5. Choose a file to investigate

	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	/LogicalFileSet1/Users/	
	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	288	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	459	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	288	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	data_1_a101034	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	/LogicalFileSet1/Users/i
	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	289	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	291	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	476	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	457	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	476	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	291	Allocated	Allocated	unknown	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	data_1_a101026	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	data_1_a1010295	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i
	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	/LogicalFileSet1/Users/i

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.

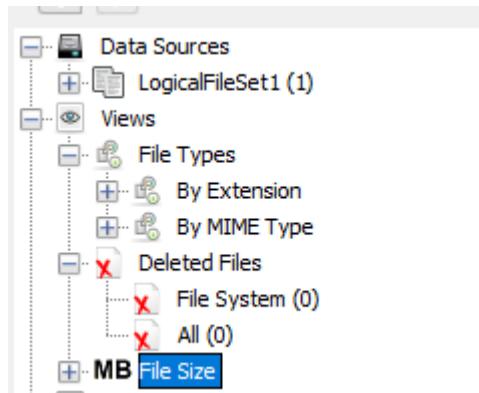
Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



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 reimagine 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

Size Range
MB 50 - 200MB (818)
MB 200MB - 1GB (300)
MB 1GB+ (88)

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+

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

- **MB 50 - 200MB (818)**
- **MB 200MB - 1GB (300)**
- **MB 1GB + (88)**

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

		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1370488832	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	Kali-Linux-2020.3-vmware-amd64-s010.vmdk									
□	kali_linux.ova	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3417005568	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	Metasploitable.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1925644288	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
■	Neurotec_Biometric_12_0_SDK_2020-09-28.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	1665534464	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	SecurityOnion_[SBA].ova	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2964058112	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	security_onion.ova	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2869807616	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	ubuntu-20.04.1-desktop-amd64.iso	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2785017856	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
■	Neurotec_Biometric_12_0_SDK_2020-09-28.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	1665534464	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	1_cyberops_workstation-disk001.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2934740512	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	2_Kali-Linux-2020.3-vmware-amd64-s001.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3673948192	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	3_Kali-Linux-2020.3-vmware-amd64-s002.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2824929312	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	1_kali_2017-1_[20171025]-disk001.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3416994848	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	2_Metasploitable.vmdk	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1925644320	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	security_onion.ova	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3081678336	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	20201207-130656.session.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	3321888768	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	20201208-145748.session.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	3070230528	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	20201208-232440.session.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	1358954496	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	kali_2017-1_[20171025]-disk001.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8906604544	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	kali_2017-1_[20171025]-disk001.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9740222464	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	ossimworking.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15532556288	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	2021-02-08T16-51-13-599475700Z.sav	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2041123248	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl
□	ubuntuassignment.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8401190912	Allocated	Allocated	unknown	/LogicalFileSet1/Users/nl

Step 5. Choose a file to investigate

		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8906604544	Allocated	Allocated	unknown	/LogicalFileSet1/Users/
■	kali_2017-1_[20171025]-disk001.vdi									
□	kali_2017-1_[20171025]-disk001.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9740222464	Allocated	Allocated	unknown	/LogicalFileSet1/Users/
□	ossimworking.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	15532556288	Allocated	Allocated	unknown	/LogicalFileSet1/Users/
□	2021-02-08T16-51-13-599475700Z.sav	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2041123248	Allocated	Allocated	unknown	/LogicalFileSet1/Users/
□	ubuntuassignment.vdi	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8401190912	Allocated	Allocated	unknown	/LogicalFileSet1/Users/

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

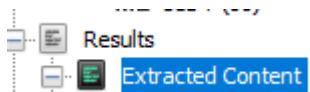
Lab – Examining Results

Step 1. Navigate to results



Extracted Content

Step 1. Navigate to extracted content



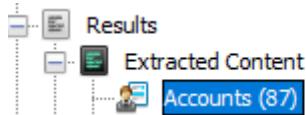
Step 2. Examine the extracted content

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Accounts

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



Step 2. Examine the contents of accounts

A screenshot of the Autopsy interface showing a table of extracted account data. The table has columns for 'Source File', 'S', 'C', 'O', 'URL', 'Date Created', 'Decoded URL', 'Username', and 'Domain'. The data shows various login attempts from different sources and domains, such as grantsonline.ie, login.microsoftonline.com, and various Cisco and Microsoft services. The table contains 87 results.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs like 'Listing', 'Accounts', 'Table', 'Thumbnail', and 'Summary'. Below that is a search bar and a page navigation section. A large table lists various URLs with their creation dates, decoded URLs, and associated accounts. One row is highlighted in blue. At the bottom, there's a detailed view of a selected item, showing its type, value, and source(s).

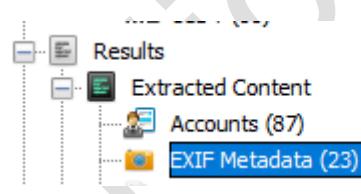
Source File	S	C	O	URL	Date Created	Decoded URL	Username	Domain
Login Data				https://grantsonline.ie/	2020-06-10 19:59:42 BST	grantsonline.ie	[REDACTED]	https://grantsonline.ie/
Login Data				https://login.microsoftonline.com/	2020-08-18 20:31:39 BST	login.microsoftonline.com		https://login.microsoftonline.com/
Login Data				https://ssb.ancheim.ie/	2020-08-21 18:03:53 BST	ssb.ancheim.ie		https://ssb.ancheim.ie/
Login Data				https://vle.bn.tudublin.ie/	2020-09-26 17:07:46 BST	vle.bn.tudublin.ie		https://vle.bn.tudublin.ie/
Login Data				https://identity.cisco.com/	2020-09-29 09:44:29 BST	identity.cisco.com		https://identity.cisco.com/
Login Data				https://cloud.digitalocean.com/	2020-09-30 18:18:17 BST	cloud.digitalocean.com		https://cloud.digitalocean.com/
Login Data				http://161.35.173.243/	2020-09-30 19:16:56 BST	161.35.173.243		http://161.35.173.243/
Login Data				http://157.230.87.45/	2020-10-01 17:16:19 BST	157.230.87.45		http://157.230.87.45/
Login Data				http://165.232.108.73/	2020-10-01 18:30:02 BST	165.232.108.73		http://165.232.108.73/
Login Data				https://account.splunk.com/	2020-10-01 19:31:19 BST	account.splunk.com		https://account.splunk.com/
Login Data				https://legacylogin.splunk.com/	2020-10-01 19:37:42 BST	legacylogin.splunk.com		https://legacylogin.splunk.com/
Login Data				http://localhost:8000/	2020-10-01 20:53:20 BST	localhost		http://localhost:8000/
Login Data				http://159.65.87.196/	2020-10-02 20:32:34 BST	159.65.87.196		http://159.65.87.196/
Login Data				http://159.65.87.196:8000/	2020-10-02 22:26:01 BST	159.65.87.196		http://159.65.87.196:8000/
Login Data				[REDACTED]	2020-10-16 13:36:09 BST	[REDACTED]		[REDACTED]
Login Data				[REDACTED]	2020-10-16 14:18:40 BST	[REDACTED]		[REDACTED]
Login Data				https://connect.ubisoft.com/	2020-10-31 00:14:40 GMT	connect.ubisoft.com		https://connect.ubisoft.com/
Login Data				https://www.warcraftlogs.com/	2020-11-09 19:41:58 GMT	www.warcraftlogs.com		https://www.warcraftlogs.com/
Login Data				https://github.com/	2020-11-17 10:56:29 GMT	github.com		https://github.com/
Login Data				https://www.canva.com/	2020-12-04 15:12:02 GMT	www.canva.com		https://www.canva.com/
Login Data				https://accounts.google.com/	2020-12-04 20:10:30 GMT	accounts.google.com		https://accounts.google.com/
Login Data				https://signin.ea.com/	2020-12-04 20:30:46 GMT	signin.ea.com		https://signin.ea.com/

Below the table, there's a detailed view of the selected item (vle.bn.tudublin.ie) with fields for Type, Value, and Source(s). The Value is https://vle.bn.tudublin.ie/. The Source(s) column shows 'Recent Activity' for each field.

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

EXIF Metadata								
Table Thumbnail Summary								
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
⌚ \$R1DYT2P.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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 3. Choose a file to investigate

The screenshot shows the Autopsy interface. At the top, there's a navigation bar with tabs like 'Listing', 'EXIF Metadata', 'Table' (which is selected), and 'Summary'. Below the navigation bar is a search bar with 'Page: 1 of 1' and 'Pages: < > Go to Page: []'. On the right side, there's a 'Save Table as CSV' button. The main area is a table with columns: Source File, S, C, O, Date Created, Device Model, Device Make, Data Source, Size, and Path. The table lists numerous files, many of which have their paths highlighted in blue. Below the table is a toolbar with buttons for 'Hex', 'Text', 'Application', 'File Metadata', 'Context', 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab is selected. In the bottom right corner, there's a preview pane showing a grayscale image of a fingerprint.

Source File	S	C	O	Date Created	Device Model	Device Make	Data Source	Size	Path
\$R077C0X.jpg	1			2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	423012	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R077C0X.jpg
\$R09LH29.jpg	1			2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	127774	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R09LH29.jpg
\$R0A4JDO.jpg	2			2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	3644839	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R0A4JDO.jpg
\$R0L31SA.jpg	1			2020-11-22 06:11:31 GMT	SM-J600FN	samsung	LogicalFileSet1	4642084	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R0L31SA.jpg
\$R18MR7L.jpg	2			2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	3644839	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R18MR7L.jpg
\$R1DYT2P.jpg	1			2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	193586	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R1DYT2P.jpg
\$R1FIWLU.jpg	1			2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	203872	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R1FIWLU.jpg
\$R2DU7RK.jpg	1			2020-11-09 15:09:04 GMT	SM-J600FN	samsung	LogicalFileSet1	2034978	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R2DU7RK.jpg
\$R2IGB00.jpg	1			2020-10-17 17:17:32 BST	SM-J600FN	samsung	LogicalFileSet1	4074944	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R2IGB00.jpg
\$R2WN1AL.jpg	1			2020-11-22 04:54:37 GMT	SM-J600FN	samsung	LogicalFileSet1	1782143	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R2WN1AL.jpg
\$R2XG20D.jpg	1			2020-11-09 15:08:47 GMT	SM-J600FN	samsung	LogicalFileSet1	1352280	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R2XG20D.jpg
\$R36VC52.jpg	1			2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	3853227	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R36VC52.jpg
\$R38KE3J.jpg	1			2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	746057	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R38KE3J.jpg
\$R39BR3C.jpg	1			2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	176822	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R39BR3C.jpg
\$R3AUKEV.jpg	1			2020-11-22 06:36:46 GMT	SM-J600FN	samsung	LogicalFileSet1	4582389	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R3AUKEV.jpg
\$R3IS1B9.jpg	1			2020-10-05 20:16:52 BST	SM-J600FN	samsung	LogicalFileSet1	3474266	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R3IS1B9.jpg
\$R3MTVFD.jpg	1			2020-10-05 16:39:12 BST	SM-J600FN	samsung	LogicalFileSet1	267023	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R3MTVFD.jpg
\$R3NAPG8.jpg	1			2020-10-05 20:16:52 BST	SM-J600FN	samsung	LogicalFileSet1	3474266	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R3NAPG8.jpg
\$R3X5Q4R.jpg	1			2020-10-05 19:43:12 BST	SM-J600FN	samsung	LogicalFileSet1	3846769	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R3X5Q4R.jpg
\$R4DCVM5.jpg	1			2020-10-05 20:16:42 BST	SM-J600FN	samsung	LogicalFileSet1	362873	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R4DCVM5.jpg
\$R4RG7KT.jpg	1			2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	3841823	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R4RG7KT.jpg
\$R51ST1I.jpg	1			2020-10-05 19:21:32 BST	SM-J600FN	samsung	LogicalFileSet1	186338	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R51ST1I.jpg
\$R60LZ0Z.jpg	1			2020-10-05 19:43:14 BST	SM-J600FN	samsung	LogicalFileSet1	3853227	/LogicalFileSet1/\$Recycle.Bin/5-1-5-21-4285860736-1273020429-692785302-1001/\$R60LZ0Z.jpg

Extension Mismatch detected

Step 1. Navigate to Extension Mismatch detected

The screenshot shows the 'Results' tree view in Autopsy. The tree has a single expanded node labeled 'Extracted Content'. Under 'Extracted Content', there are three sub-nodes: 'Accounts (87)', 'EXIF Metadata (23)', and 'Extension Mismatch Detected (2)'. The 'Extension Mismatch Detected' node is highlighted with a blue selection bar at the bottom of its list item.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 2. Examine the contents of extension mismatch detected

The screenshot shows the 'Listing' tab of the Autopsy interface. At the top, it says 'Extension Mismatch Detected'. Below that is a table with three columns: 'Source File', 'S', and 'C'. Under 'Source File', there are two entries: 'SpeechRecognition.v11.suo' and 'SpeechRecognition.suo'. The 'S' column contains the letter 'S' for both entries, and the 'C' column is empty.

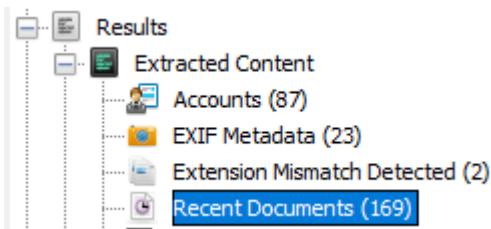
Step 3. Choose a file to investigate

This screenshot shows a more detailed view of the 'SpeechRecognition.v11.suo' file from the previous step. The table now includes additional columns: 'O', 'Extension', 'MIME Type', and 'Data Source'. The 'SpeechRecognition.v11.suo' entry has 'O' as '1', 'Extension' as 'suo', 'MIME Type' as 'application/x-msoffice', and 'Data Source' as 'LogicalFileSet1'. The 'SpeechRecognition.suo' entry has 'O' as '1', 'Extension' as 'suo', 'MIME Type' as 'application/x-msoffice', and 'Data Source' as 'LogicalFileSet1'. Below the table, there's a 'Hex' tab showing raw file data, which includes strings like 'Root Entry', 'ProjInfoEx', and '144B10B9-B200-11D0_ProjState'.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

Source File	S	C	O	Path
Downloads.LNK				C:\Users\
Final1.pptx.LNK				C:\Users\
1200px-TU_Dublin_Logo.png.Lnk				C:\Users\
640.png.Lnk				C:\Users\
Access-control-matrix.png.Lnk				C:\Users\
All Tasks.lnk				No preferr
Anatomy of malware.docx.lnk				C:\Users\

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

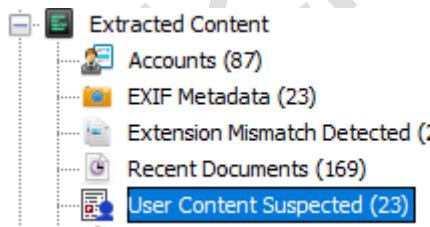
Step 3. Choose a file to investigate

The screenshot shows the Autopsy digital forensics tool's interface. At the top, there's a navigation bar with tabs for 'Listing', 'Recent Documents', 'Table', 'Thumbnail', and 'Summary'. Below this is a search bar with 'Page: 1 of 1' and 'Pages: < > Go to Page: []'. A table lists various files under 'Source File' with columns for 'S', 'C', 'O', and 'Path'. The first file, 'Downloads.LNK', is selected and highlighted in blue. The path for this file is listed as 'C:\Users\'. Below the table, there's a 'Results' tab with sub-tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'Context' (which is selected), 'Results', 'Annotations', and 'Other Occurrences'. The 'Results' tab shows 'Result: 1 of 1' and a 'Result' button with arrows. Underneath, a table provides detailed information about the selected file:

Type	Value
Path	C:\Users\nkean\Downloads
Path ID	285001
Date/Time	0000-00-00 00:00:00
Source File Path	/LogicalFileSet1/Users/nkean/AppData/Roaming/Microsoft/Office/Recent/Downloads.LNK
Artifact ID	-9223372036854771825

User Content Suspected

Step 1. Navigate to user content suspected



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 2. Examine user content suspected

Source File	S	C	O	Comment	Data Source
SR077CXX.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR09H129.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR0A41D00.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR0L31SA.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR18M7L.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR1DYT2Z.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR1FWLUL.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR2DU7RK.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR2IGB00.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR2WNV1AL.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR2XG2D0.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR36VC52.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR38KE33.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR39BR3C.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR3AUKEV.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR3IS1B9.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR3MTVFD.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR3NAPG8.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR3XS04F4.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR4DCVMS.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR4RG7K7.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR51ST1I.jpg				EXIF metadata data exists for this file.	LogicalFileSet1
SR60LZ0Z.jpg				EXIF metadata data exists for this file.	LogicalFileSet1

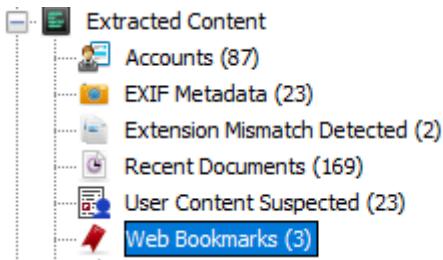
Step 3. Choose a file to investigate

File	Content	Properties	Details	Actions
SR077CXX.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR09LH29.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR0A4JDO.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR0L31SA.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR18MR7L.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR1DYTPZ.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR1FIWLU.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR2DURK.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR2JGB00.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR2WN1AL.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR2XG2D0.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR36VC52.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR38KE33.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR39BR3C.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR3AUKEV.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR3IS1B9J.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR3MTVFD.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR3NAPG8.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR3X5Q4R.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR4DCVMS.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR4RG7X7.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR51ST1I.jpg			EXIF metadata data exists for this file.	LogicalFileSet1
SR60LZDZ.jpg			EXIF metadata data exists for this file.	LogicalFileSet1

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

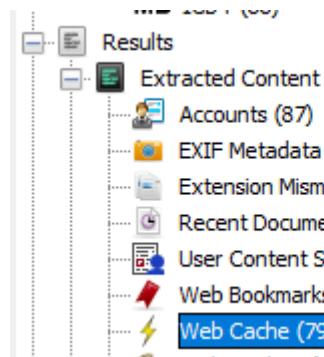
Below the table, there is a detailed examination of the first row (ASUS Homepage.url). The interface shows tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The Results tab is selected, displaying the following details:

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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/avatar...	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

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/6c93fec4-53d7-4ae8-8014-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/hRpNbJUGEFe69bMbdavAHLJ1f8BvK4=%0A	ChromeCacheExtractor

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Web Cookies

Step 1. Navigate to Web Cookies



Step 2. Examine the contents of web cookies

Cookie	Program	Date/Time Created	Value	Program Name	Program	Source(s)	Logical File Set
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

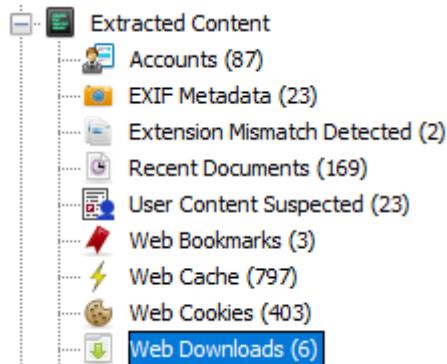
Type	Value	Source(s)
URL	.securitymetrics.com	Recent Activity
Date/Time	2021-02-19 06:19:06	Recent Activity
Name	s_dslv	Recent Activity
Value		Recent Activity
Program Name	Microsoft Edge	Recent Activity
Domain	securitymetrics.com	Recent Activity

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Web Downloads

Step 1. Navigate to web downloads



Step 2. View the contents of the web downloads

Web Downloads									
Source File	S	C	O	Path	URL	Date Accessed	Domain	Program Name	Data Source
History	2			C:\Users\nkean\Downloads\Imager_Lite_3.1.1.zip	https://marketing.accessdata.com/e/46432/Imager-Lite-3-1-1-zip/8d9g6n/195...	2021-02-19 16:04:26 GMT	marketing.accessdata.com	Microsoft Edge	LogicalFileSet1
History	2			C:\Users\nkean\Downloads\Imager_Lite_3.1.1.zip	https://ad-zip.s3.amazonaws.com/Imager_Lite_3.1.1.zip	2021-02-19 16:04:26 GMT	ad-zip.s3.amazonaws.com	Microsoft Edge	LogicalFileSet1
History	2			C:\Users\nkean\Downloads\Imager_Lite_3.1.1.zip	https://marketing.accessdata.com/e/46432/Imager-Lite-3-1-1-zip/8d9g6n/195...	2021-02-19 16:12:45 GMT	marketing.accessdata.com	Microsoft Edge	LogicalFileSet1
History	2			C:\Users\nkean\Downloads\Imager_Lite_3.1.1.zip	https://ad-zip.s3.amazonaws.com/Imager_Lite_3.1.1.zip	2021-02-19 16:12:45 GMT	ad-zip.s3.amazonaws.com	Microsoft Edge	LogicalFileSet1
History	1			C:\Users\nkean\Downloads\MBSetup.exe	https://downloads.malwarebytes.com/file/mbs-windows	2021-02-19 17:45:29 GMT	downloads.malwarebytes.com	Microsoft Edge	LogicalFileSet1
History	1			C:\Users\nkean\Downloads\MBSetup.exe	https://data-cdn.mbamupdates.com/web/mbs-setup-consumer/MBSetup.exe	2021-02-19 17:45:29 GMT	data-cdn.mbamupdates.com	Microsoft Edge	LogicalFileSet1

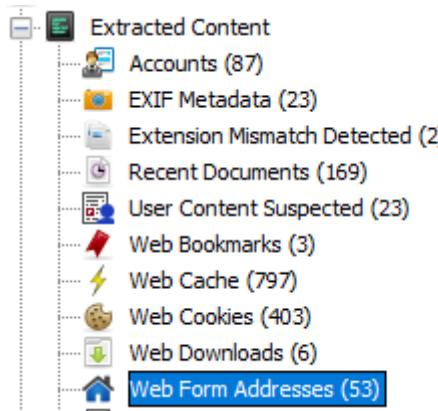
Step 3. Choose a web download to investigate

Result: 448 of 458		Result
Type	Value	Source(s)
Path	C:\Users\nkean\Downloads\Imager_Lite_3.1.1.zip	Recent Activity
Path ID	287225	Recent Activity
URL	https://marketing.accessdata.com/e/46432/Imager-Lite-3-1-1-zip/8d9g6n/1953465983?h=oKxequI4wxGxbJ7TPYirSg5gb5l1xlrMB168D5r7Ng	Recent Activity
Date Accessed	2021-02-19 16:12:45	Recent Activity
Domain	marketing.accessdata.com	Recent Activity
Program Name	Microsoft Edge	Recent Activity

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Web Form Addresses

Step 1. Navigate to Web Form Addresses



Step 2. Examine the contents of web form addresses

Source File	S	C	O	Name	Email	Phone Number	Location	Date Accessed	Count	Date Modified	Data Source
Web Data	[B@37199e0]			[B@a1f4d23]	[B@5feb7e83]		[B@663496d2, [B@2d73e918, [B@4565c97d, [B@3563e2a7, [B@31f89dee	2020-10-19 15:05:25 BST	1	2020-10-19 14:53:55 BST	LogicalFileSet
Web Data	[B@575c5126]			[B@29697ac]	[B@4786933]		[B@43ed66a8, [B@61aa3a23, [B@3ae2e0d, [B@5be92c6a, [B@679704d5	2020-10-31 00:08:34 GMT	6	2020-09-30 17:57:38 BST	LogicalFileSet
Web Data	[B@31598bd7]			[B@62611118]	[B@117cff4f]		[B@1fcf922f, [B@462b33b7, [B@32039764, [B@5880a9ed, [B@2ef0a335	2020-11-02 18:25:03 GMT	1	2020-11-02 18:25:03 GMT	LogicalFileSet
Web Data	[B@25af1c6c]			[B@985801]	[B@5aff0d7]		[B@9f7af297, [B@76f707b1, [B@59446d69, [B@11384f4d, [B@6bab425	2020-11-05 14:10:27 GMT	1	2020-11-05 14:10:27 GMT	LogicalFileSet
Web Data	[B@491ea07b]			[B@44666374]	[B@17c517e]		[B@37ffdc2b, [B@450f0ca9, [B@27fb0cb, [B@5021764, [B@75c9802f	2020-11-05 14:10:27 GMT	1	2020-11-05 14:10:27 GMT	LogicalFileSet
Web Data	[B@76a5e720]			[B@1ecf785e]	[B@6b95d15]		[B@51e02d3f, [B@47e37e9d, [B@d954eed, [B@657dca9, [B@2a6e7366	2020-11-09 19:37:36 GMT	2	2020-11-09 19:37:15 GMT	LogicalFileSet
Web Data	[B@16eaa5a4]			[B@5b899493]	[B@35bfe2e]		[B@7d8be789, [B@3f77b503, [B@62e72a5, [B@4dd0766, [B@14371adc	2020-11-13 17:54:25 GMT	1	2020-11-13 17:54:25 GMT	LogicalFileSet
Web Data	[B@60ee7ee]			[B@2794530]	[B@3041ead4]		[B@52fee29f, [B@2ffd9ab, [B@15e03981, [B@70557e01, [B@477d4c6b	2020-11-24 00:08:50 GMT	1	2020-11-24 00:08:50 GMT	LogicalFileSet
Web Data	[B@4ea876fd]			[B@3abdcd3b]	[B@5ab3819]		[B@95e1f01a, [B@721752e, [B@41cf2e4, [B@251cd5f3, [B@640dd6b9	2020-11-24 16:50:23 GMT	1	2020-11-24 16:50:23 GMT	LogicalFileSet
Web Data	[B@134f2796]			[B@610023b9]	[B@21cfa5]		[B@4ff6e116, [B@4d4959eb, [B@15093e4, [B@7574de17, [B@33497c5	2020-11-24 16:51:05 GMT	1	2020-11-24 16:51:05 GMT	LogicalFileSet
Web Data	[B@65e429c8]			[B@290f835]	[B@3ebcef7]		[B@694e0526, [B@58d99e36, [B@2d943644, [B@2803293, [B@715821fb	2020-11-30 23:04:58 GMT	4	2020-11-30 23:04:58 GMT	LogicalFileSet

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 3. Choose a web form address to investigate

Web Form Addresses											53 Results
Source File	S	C	O	Name	Email	Phone Number	Location	Date Accessed	Count	Date Modified	Data Source
Web Data				[B@37199e0]	[B@a1fd23]	[B@5feb7e83]	[B@683496d2, [B@2d73e918, [B@4565c97d, [B@3563e2a7, [B@31f89dee	2020-10-19 15:05:25 BST	1	2020-10-19 14:53:55 BST	LogicalFileSet
Web Data				[B@575c5126]	[B@296e3fac]	[B@678b6933]	[B@43ed66a8, [B@61aa3a23, [B@3a2e0ed, [B@5be92c6a, [B@679704d5	2020-10-31 00:08:34 GMT	6	2020-09-30 17:57:38 BST	LogicalFileSet
Web Data				[B@1598bd7]	[B@62611118]	[B@117cf4f]	[B@1fc922f, [B@462b33d7, [B@32039764, [B@5880a9ed, [B@2ef0a335	2020-11-02 18:25:03 GMT	1	2020-11-02 18:25:03 GMT	LogicalFileSet
Web Data				[B@25affcc8e]	[B@988581]	[B@5aff8cf]	[B@5f7af297, [B@76f707b1, [B@594f6d69, [B@11384f4d, [B@6babaa25	2020-11-05 14:10:27 GMT	1	2020-11-05 14:10:27 GMT	LogicalFileSet
Web Data				[B@481ea07b]	[B@44b66374]	[B@17c6517e]	[B@37ffcb2, [B@450f0ca9, [B@27ff0cbc, [B@502176f4, [B@75c9802f	2020-11-05 14:10:27 GMT	1	2020-11-05 14:10:27 GMT	LogicalFileSet
Web Data				[B@76a5e720]	[B@1ec785e]	[B@6b95d15]	[B@51e02d3f, [B@47e37e9d, [B@d954eed, [B@687da89, [B@246e7366	2020-11-09 19:37:36 GMT	2	2020-11-09 19:37:15 GMT	LogicalFileSet
Web Data				[B@16ea6fa4]	[B@5b989493]	[B@35b4e2c]	[B@7d6be789, [B@3f77b503, [B@52e72d5, [B@4dc40766, [B@14371adc	2020-11-13 17:54:25 GMT	1	2020-11-13 17:54:25 GMT	LogicalFileSet
Web Data				[B@2794538]	[B@301e4ead]	[B@52fe2e2f, [B@2ffd9eb, [B@15e83981, [B@78557e61, [B@477d4c6b	2020-11-24 00:08:50 GMT	1	2020-11-24 00:08:50 GMT	LogicalFileSet	
Web Data				[B@4e8a76fd]	[B@3abdc3b]	[B@5abf3819]	[B@5c1f01a, [B@721752ae, [B@41caf2e4, [B@251c5df3, [B@64d6b9	2020-11-24 16:50:23 GMT	1	2020-11-24 16:50:23 GMT	LogicalFileSet
Web Data				[B@13f42796]	[B@610023b9]	[B@21ccfa36]	[B@4ff6e116, [B@4d495eb, [B@15093a4e, [B@7574de17, [B@33af97c5	2020-11-24 16:51:05 GMT	1	2020-11-24 16:51:05 GMT	LogicalFileSet
Web Data				[B@65e429c8]	[B@290f835]	[B@3ebcfe7]	[B@694e0526, [B@58d99e36, [B@2d943644, [B@28c03293, [B@715821fb	2020-11-30 23:04:58 GMT	4	2020-11-30 23:04:58 GMT	LogicalFileSet
Web Data				[B@65c25ab3]	[B@3f81a076]	[B@3408403a]	[B@7357c691, [B@3c2e3634, [B@6c5f5b89, [B@5effd464, [B@28105613	2020-12-08 20:17:29 GMT	1	2020-12-08 20:17:29 GMT	LogicalFileSet
Web Data				[B@d43d2a]	[B@3ef0f142]	[B@7e80f0e6]	[B@3d80460, [B@675c406, [B@3760fe80, [B@e4373df, [B@85d3453	2020-12-26 05:34:09 GMT	1	2020-12-26 05:34:09 GMT	LogicalFileSet
Web Data				[B@15a75c7c]	[B@67d57f4d]	[B@72a740d2]	[B@1374a90, [B@4f1dccef, [B@30f6c47c, [B@7c9eaa38, [B@347c8a8	2021-01-03 01:15:44 GMT	1	2021-01-03 01:15:44 GMT	LogicalFileSet
Web Data				[B@5d24043d]	[B@57d14ba9]	[B@6df5b2d7]	[B@4e9390f3, [B@67b5dcc, [B@9435d06, [B@5412d384, [B@14b1a0db	2021-01-11 05:38:17 GMT	1	2021-01-11 05:38:17 GMT	LogicalFileSet
Web Data				[B@3acc3233]	[B@54a963c0]	[B@67280c24]	[B@18d4447f, [B@3fd74790, [B@7e4abe, [B@18cc6f91, [B@3f220980	2021-01-11 05:44:14 GMT	3	2020-12-04 20:10:18 GMT	LogicalFileSet
Web Data				[B@75f00c3d]	[B@70e06eb8]	[B@513b7739]	[B@3556c75d, [B@985e035, [B@2a3d4b7d, [B@59deec67, [B@53d2da3a	2021-02-12 04:38:17 GMT	21	2020-09-30 17:35:36 BST	LogicalFileSet
Web Data				[B@e177413]	[B@7e83508]	[B@649de02e, [B@7d256d6, [B@263053cc, [B@19f12277, [B@21dc3c16	2021-02-12 04:40:49 GMT	2	2021-02-12 04:40:49 GMT	LogicalFileSet	
Web Data				[B@18a46f68]	[B@6b3ae59d]	[B@6ebd502a]	[B@3b9282a, [B@ced147e, [B@441cea5c, [B@7836e94f, [B@7c8eca63	2021-02-19 15:59:06 GMT	71	2020-11-10 15:36:52 GMT	LogicalFileSet
Web Data				[B@31f51da4]	[B@663bc6c5]	[B@5119ec60]	[B@2d21570b, [B@58f6d57a, [B@42abd7b, [B@41a2d075, [B@5fc64ecd	2021-02-19 16:00:57 GMT	12	2021-02-11 21:32:42 GMT	LogicalFileSet
Web Data				[B@7bd15185]	[B@4f50b56]	[B@67f910c]	[B@9c65b19, [B@4c3a9fda, [B@2b1b3e18, [B@4bd42f96, [B@630dc671	2021-02-19 16:01:23 GMT	1	2021-02-19 16:01:23 GMT	LogicalFileSet
Web Data				[B@f72ade1]	[B@33b5d4]	[B@4fc3bed8]	[B@1f56a103, [B@196c3816, [B@7cd9135, [B@2541d885, [B@77a6878b	2020-09-30 17:35:36 BST	1	2020-09-30 17:35:36 BST	LogicalFileSet

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences	Web Form Addresses
Result: 430 of 450	Result							
Type	Value							Source(s)

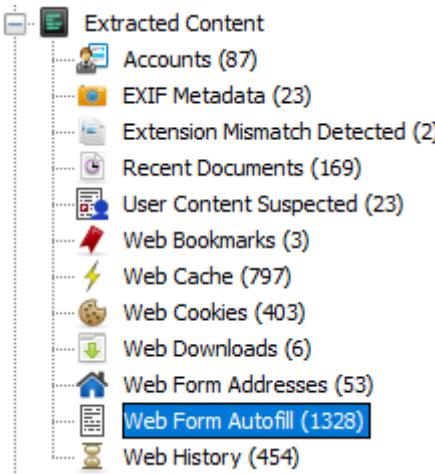
Name	[B@37199e0]							Recent Activity
Email	[B@a1fd23]							Recent Activity
Phone Number	[B@5feb7e83]							Recent Activity
Location	[B@683496d2, [B@2d73e918, [B@4565c97d, [B@3563e2a7, [B@31f89dee							Recent Activity
Date Accessed	2020-10-19 15:05:25							Recent Activity
Count	1							Recent Activity
Date Modified	2020-10-19 14:53:55							Recent Activity
Source File Path	/LogicalFileSet1/Users/nkean/AppData/Local/Microsoft/Edge/User Data/Default/Web Data							
Artifact ID	-9223372036854774454							

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Web form Autocomplete

Step 1. Navigate to web form autocomplete



Step 2. Examine the contents of web form autocomplete

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@59ae5726	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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Step 3. Choose a web form autofill to investigate

The screenshot shows the Autopsy digital forensics tool interface. At the top, there's a navigation bar with tabs like 'Listing', 'Web Form Autofill' (which is selected), 'Thumbnail', and 'Summary'. Below the navigation is a search bar with 'Page: 1 of 1' and 'Pages: < > Go to Page: []'. On the right side, there's a 'Save Table as CSV' button.

The main area displays a table of 'Web Data' entries. The columns include: Source File, S, C, O, Name, Value, Count, Date Created, Date Accessed, Program Name, and Data Source. The 'Value' column contains entries like '[B@12432cba]', '[B@4270d02a]', etc. The 'Count' column shows values such as 25, 3, 43, 125, 1, 1, 15, 157, 3, 8, 1, 23, 1, 15, 19, 1, 2, 4, 20, 3, and 12. The 'Date Created' and 'Date Accessed' columns show dates ranging from 2020-07-15 to 2021-01-13. The 'Program Name' column consistently lists 'Microsoft Edge'. The 'Data Source' column is labeled 'LogicalFileSet1' for all entries.

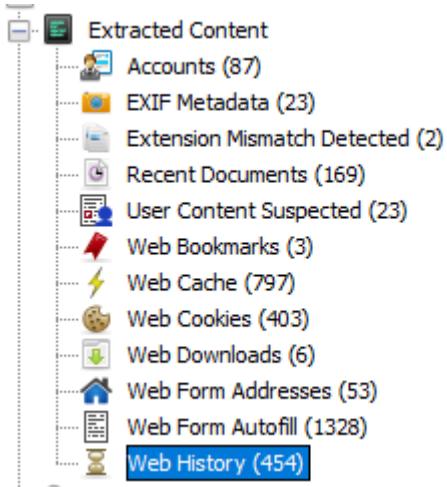
Below the table, there's a 'Hex Text Application File Metadata Context Results Annotations Other Occurrences' toolbar. The 'Results' tab is selected, showing 'Result: 1 of 450'. To the right of the results table, there's a 'Web Form Autofill' section with a table showing details for the first result. The columns here are Type, Value, and Source(s). The rows correspond to the fields in the main table: Name (term), Value ([B@12432cba]), Count (25), Date Created (2020-07-15 22:17:33), Date Accessed (2020-11-07 02:45:38), Program Name (Microsoft Edge), Source File Path (/LogicalFileSet1/Users/nkearn/AppData/Local/Microsoft/Edge/User Data/Default/Web Data), and Artifact ID (-9223372036854774883).

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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/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	

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

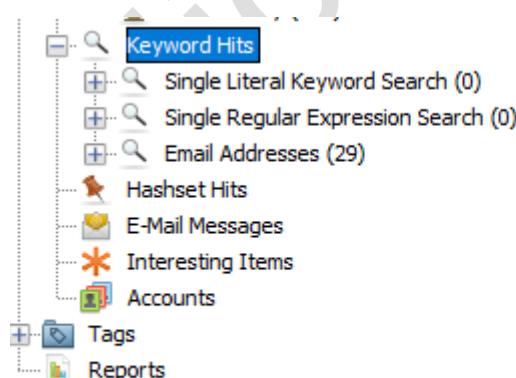
Result: 162 of 458		Result	Web History
Type	Value	Source(s)	
URL	https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000006-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code%20id_token&scope=&openid%20profile&state=OpenIdConnect.AuthenticationProperties%3Dcdqmcgeh_FHt_0PoCUCHsBt61g985v5mnbQN-F90hHTNmldSlavQJD-Y7ImqVj_3vNTNekOqHGTLFx8TBfKn5e311V3zhwUdwBM39L895LZZE_IN_Lg3aJUAalNPAY_XRclgoQggM1Fb4RNQdhUf2_gmS1Y5Y&nonce=d3749319734991649.MGFHNWE5ZTMYT4Z500mMyLWE42Tgt2ExMnQyZWY1NzJNTmFhJggMDFMS001zxlTkWnjUzW14VWhhWM02TYw&redirect_uri=https%3A%2F%2Fportal.office.com%2flanding&ui_locales=en-GB&mkt=en-GB&client-request-id=b2416bf8-39ea-481a-88a7-b95781d777b18x-client-SKU=ID_.NET45&x-client-ver=6.6.0.0	Recent Activity	Recent Activity
Date Accessed	2021-02-19 14:33:04	Recent Activity	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%3Dcdqmcgeh_FHt_0PoCUCHsBt61g985v5mnbQN-F90hHTNmldSlavQJD-Y7ImqVj_3vNTNekOqHGTLFx8TBfKn5e311V3zhwUdwBM39L895LZZE_IN_Lg3aJUAalNPAY_XRclgoQggM1Fb4RNQdhUf2_gmS1Y5Y&nonce=d3749319734991649.MGFHNWE5ZTMYT4Z500mMyLWE42Tgt2ExMnQyZWY1NzJNTmFhJggMDFMS001zxlTkWnjUzW14VWhhWM02TYw&redirect_uri=https%3A%2F%2Fportal.office.com%2flanding&ui_locales=en-GB&mkt=en-GB&client-request-id=b2416bf8-39ea-481a-88a7-b95781d777b18x-client-SKU=ID_.NET45&x-client-ver=6.6.0.0	Recent Activity	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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop



Step 2. Examine the contents of email addresses

④ `(\{?\})[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%_\.]+)*(\?\})@(\... coveremail" value=" 00122534@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%_\.]+)*(\?\})@(\... &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_scopeuser_name= b00122534@mytudublin.ie &ui... 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%_\.]+)*(\?\})@(\... &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%_\.]+)*(\?\})@(\... &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%_\.]+)*(\?\})@(\... &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%_\.]+)*(\?\})@(\... &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%_\.]+)*(\?\})@(\... &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%_\.]+)*(\?\})@(\... &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.

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

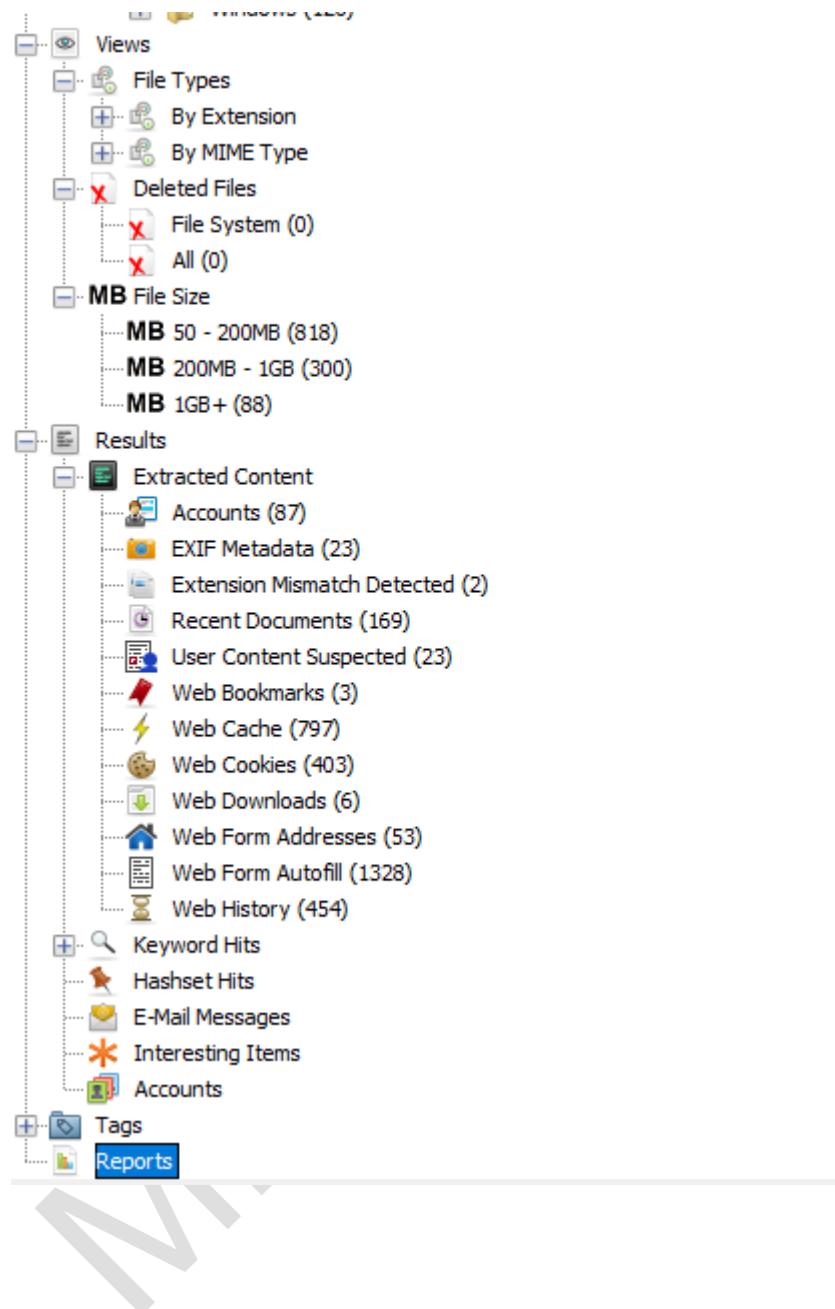
History		b00122534@mytudublin.ie	(\{\?%\}[a-zA-Z0-9%+_\-]+)([a-zA-Z0-9%+_\-]+)*(\?%)@([...)	tfw?login_hint_safe=b00122534@mytudublin.ie<date acc...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
History		b00122534@mytudublin.ie	(\{\?%\}[a-zA-Z0-9%+_\-]+)([a-zA-Z0-9%+_\-]+)*(\?%)@([...)	tfw?login_hint_safe=b00122534@mytudublin.ie<date acc...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

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

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Reports

Step 1. Navigate to the reports section



Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

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

Listing			
Table	Thumbnail	Summary	
Page: 1 Pages: < > Go to Page: []			
Source Module Name	Report Name	Created Time	Report Fi
HTML Report		2021-02-21 19:42:07 GMT	C:\Users\

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”

Listing Keyword search 1 - .png X		
Table	Thumbnail	Summary
Name	Keyword Preview	Location
Web Cache Artifact	content-type : image/*png* etag : "1eaa-5b95c0afc7400"	/LogicalFileSet1/Users/
Web Cache Artifact	h2pri content-type : image/*png* etag : "486373469ec7cd	/LogicalFileSet1/Users/
Web Cache Artifact	content-type : image/*png* etag : "6c884cccd196ba7	/LogicalFileSet1/Users/
\$IOASBAP.png	\Biometrics\0011_L_000.*png*	/LogicalFileSet1/\$Recy
Web Cache Artifact	duction/img/favicon_32.*png*Domain : www.youtube.com	/LogicalFileSet1/Users/
\$R0SM1P6.png	\$r0sm1p6.*png*	/LogicalFileSet1/\$Recy
\$IOOC18Z.png	\Biometrics\0009_L_000.*png*	/LogicalFileSet1/\$Recy
\$R0XYUQ3.png	\$r0xyuq3.*png*	/LogicalFileSet1/\$Recy
\$IOSM1P6.png	\$iosm1p6.*png*	/LogicalFileSet1/\$Recy
\$IOXYUQ3.png	\$ioxyuq3.*png*	/LogicalFileSet1/\$Recy
\$19MMJW.png	\Biometrics\0001_R_004.*png*	/LogicalFileSet1/\$Recy
Web Cache Artifact	h2pri content-type : image/*png* etag : "7dbdf426de1ec2	/LogicalFileSet1/Users/
Web Cache Artifact	O content-type : image/*png* server-timing : edge; dur=1	/LogicalFileSet1/Users/
\$I1TPE3Y.png	\Biometrics\0007_R_001.*png*	/LogicalFileSet1/\$Recy
\$I2AA8XM.png	\Biometrics\0001_L_002.*png*	/LogicalFileSet1/\$Recy
\$I2ESLM5.png	\$i2eslm5.*png*	/LogicalFileSet1/\$Recy
\$R2ESLM5.png	\$r2eslm5.*png*	/LogicalFileSet1/\$Recy
\$I2LK0Z7.png	\$i2lk0z7.*png*	/LogicalFileSet1/\$Recy
\$R2LK0Z7.png	\$r2lk0z7.*png*	/LogicalFileSet1/\$Recy
Web Cache Artifact	content-type : image/*png* etag : "ff28aae693ac44	/LogicalFileSet1/Users/
0	ings-icon/peg1/PEGI_16.*png*","gameRatingUrl":"http://www	/LogicalFileSet1/Users/
Web Cache Artifact	content-type : image/*png* p3p : CP="ALL DSP COR	/LogicalFileSet1/Users/

Step 2. Investigate the contents of one of the files

Digital Forensics – Using Autopsy to Analyse the Contents of a Laptop

Page: 1 of 1 Page Matches on page: 1 of 1 Match 100% Reset Text Source: Search Results

newer : Sat, 19 Feb 2022 02:27:11 GMT
last-modified : Wed, 20 Jan 2021 21:57:36 GMT
server : Apache
content-length : 7850
x-frame-options : SAMEORIGIN
x-origin-ops : K4IxQekvD+1BkOhDPKdgLauuHnifKKahSqt8hEcDxho=%0A
link : <https://data1.origin.com>, rel=preconnect
content-type : image/png
etag : "1eaa-5b5c0acf7400"
accept-ranges : bytes
cache-control : public, max-age=2592000
status : 200

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/>.