Michael Hegarty

Forensics

Forensics Analysis using Autopsy

Lab Title: Exploring Digital Forensics with Autopsy

Introduction:

In this lab, you will explore the powerful open-source forensic tool, Autopsy, and learn how to install and use it for digital investigations. Autopsy, along with the Sleuth Kit, is a versatile platform that allows you to analyse disk images, perform in-depth file system analysis, and extract valuable insights from various sources.

Lab Objectives:

1. **Install Autopsy:** Learn how to download and install the latest version of Autopsy on your system.
2. **Overview of Autopsy:** Familiarize yourself with the features and capabilities of Autopsy.
3. **Perform Forensic Analysis:** Analyse a disk image using Autopsy to extract valuable information, such as file attributes, system events, and web artifacts.
4. **Compare Findings:** Compare the results obtained from Autopsy with those from the previous FTK lab, highlighting the strengths and weaknesses of each tool.

Autopsy Features:

Autopsy offers a wide range of features that aid in digital forensic investigations, including:

- **Timeline Analysis:** Visualize system events to identify suspicious activities.
- **Keyword Search:** Extract and search for specific terms and patterns within files.
- **Web Artifacts:** Recover web activity data to understand user actions.
- **Registry Analysis:** Identify recently accessed documents and USB devices.
- **Email Analysis:** Parse MBOX format messages for email investigations.
- **EXIF Data Extraction:** Extract geolocation and camera information from image files.
- **File Type Sorting:** Group files by type for quick identification.
- **Media Playback:** View images and videos within the application.
- **Thumbnail Viewer:** Quickly preview images with thumbnail support.
- **File System Analysis:** Support for various file systems, including NTFS, FAT, HFS+, and more.
- **Hash Set Filtering:** Identify known good and bad files using hash sets.
- **Tagging:** Tag files and add comments for categorization.
- **Unicode Strings Extraction:** Extract strings from unallocated space in multiple languages.
- **File Type Detection:** Identify file types based on signatures and extensions.

- **Interesting Files Module:** Flag files and folders based on names and paths.
- **Android Support:** Extract data from Android devices, including SMS, call logs, and more.

Lab Procedure:

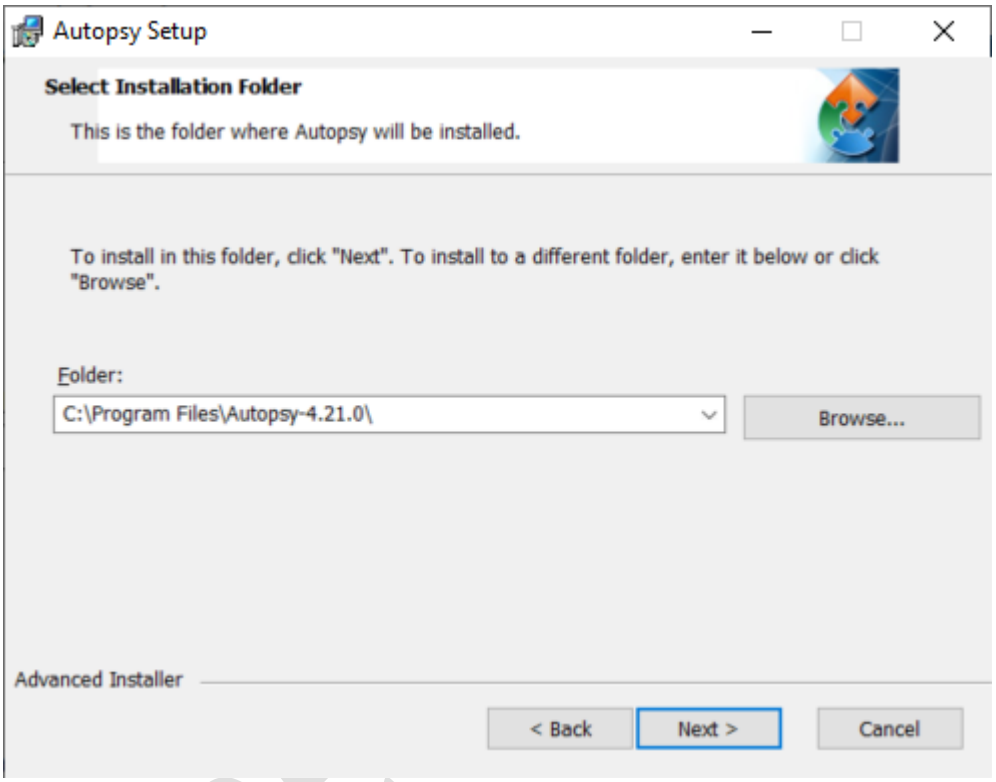
1. **Installation of Autopsy:**
    - Visit the official Autopsy website (http://www.sleuthkit.org/autopsy).
    - Download the latest version of Autopsy for your operating system (Windows, Linux, OS X, etc.).
    - Follow the installation instructions provided for your specific OS.
    - Launch Autopsy after successful installation.
2. **Getting to Know Autopsy:**
    - Familiarize yourself with the Autopsy interface and its various modules.
    - Explore the main features, including Timeline Analysis, Keyword Search, Web Artifacts, and more.
3. **Analysing a Disk Image:**
    - Load a disk image for analysis in Autopsy.
    - Utilize Autopsy's features to extract information, investigate system events, and uncover relevant evidence.
4. **Comparing Findings:**
    - Refer to the results of the previous FTK lab.
    - Highlight the differences in findings between FTK and Autopsy.
    - Assess the strengths and weaknesses of each tool for specific forensic tasks.
5. **Document Your Analysis:**
    - Record your observations, findings, and any notable insights.
    - Compile a comprehensive report, including screenshots and a comparison of findings from both labs.
    -

Conclusion:

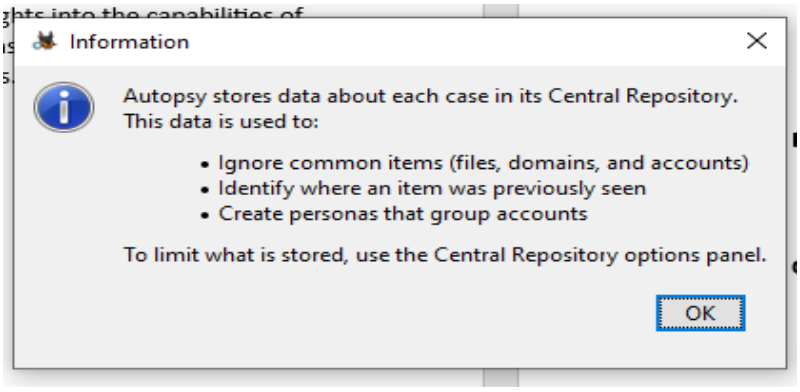
This lab provides you with hands-on experience in using Autopsy for digital forensic investigations. By comparing the results with the previous FTK lab, you will gain valuable insights into the capabilities of each tool and their suitability for specific tasks. Understanding the strengths and weaknesses of different forensic tools is essential for a successful career in digital forensics.

Installing Autopsy and Starting a New Case: (Please note that some installs will vary, this is a guide)

1. **Run the Autopsy MSI File:**
    - Locate the Autopsy MSI file that you downloaded from the official website.
    - Double-click the MSI file to initiate the installation process.

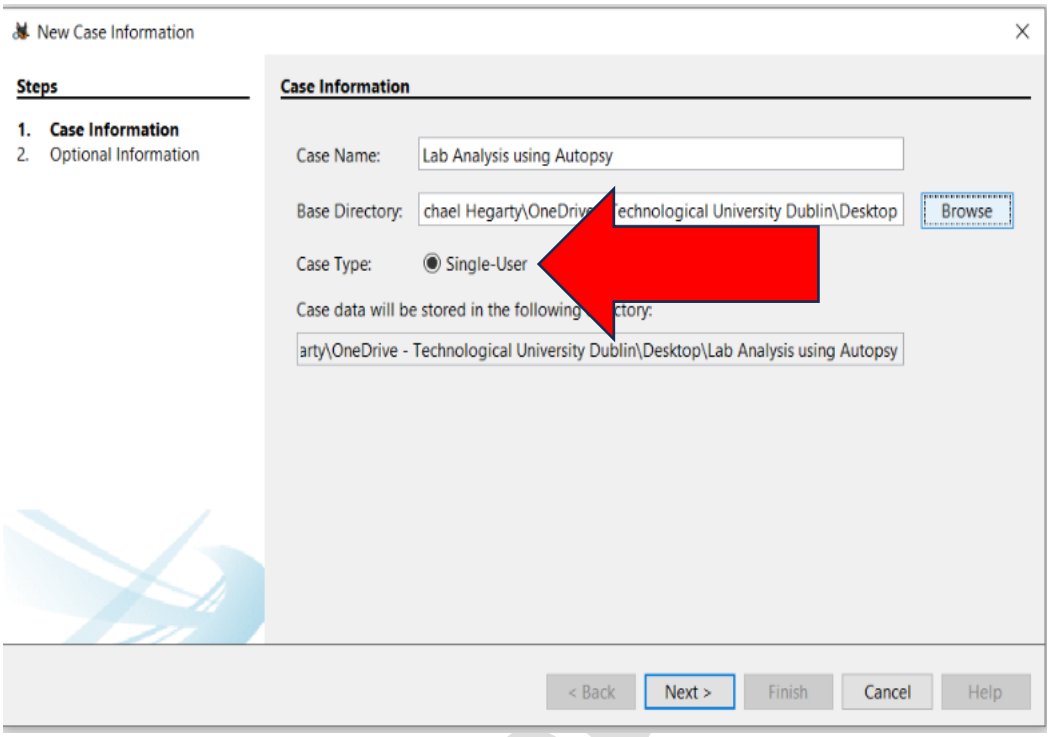


2. **User Account Control (UAC) Prompt:**
    - If Windows prompts you with a User Account Control (UAC) dialog, click "Yes" to allow the installation to proceed.
3. **Default Installation Settings:**
    - The installation wizard will appear. Stay with the default installation settings, which are usually fine for most users.
    - Click "Next" to continue.

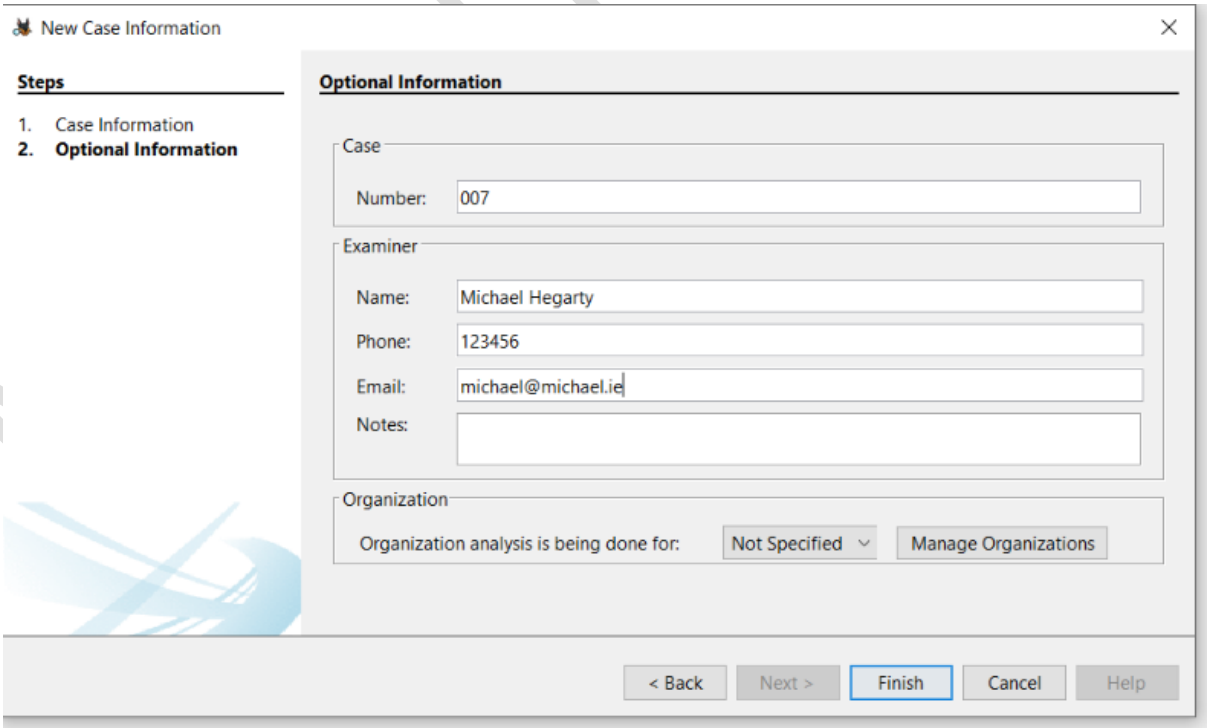


4. **Complete Installation:**
    - Follow the on-screen instructions and click "Next" to proceed through the installation steps.
    - When the installation is complete, click the "Finish" button to exit the installation wizard.
5. **Launch Autopsy:**
    - After installation, you can start Autopsy by double-clicking the Autopsy icon that is created on your desktop.
6. **Creating a New Case:**
    - Once Autopsy is launched, follow these steps to start a new case:
        - In the Autopsy interface, click on "File" in the top menu bar.
        - Select "Create New Case" from the drop-down menu.

7. **Case Creation Details:**
    - A new window will open for case creation. Provide the necessary details for your case, including the case name, examiner's name, case number, and case description.
    - Ensure you choose an appropriate directory to save the case files.
    - Click "Create Case" to initiate the case setup.
    - **Choose: Single-User Installation**



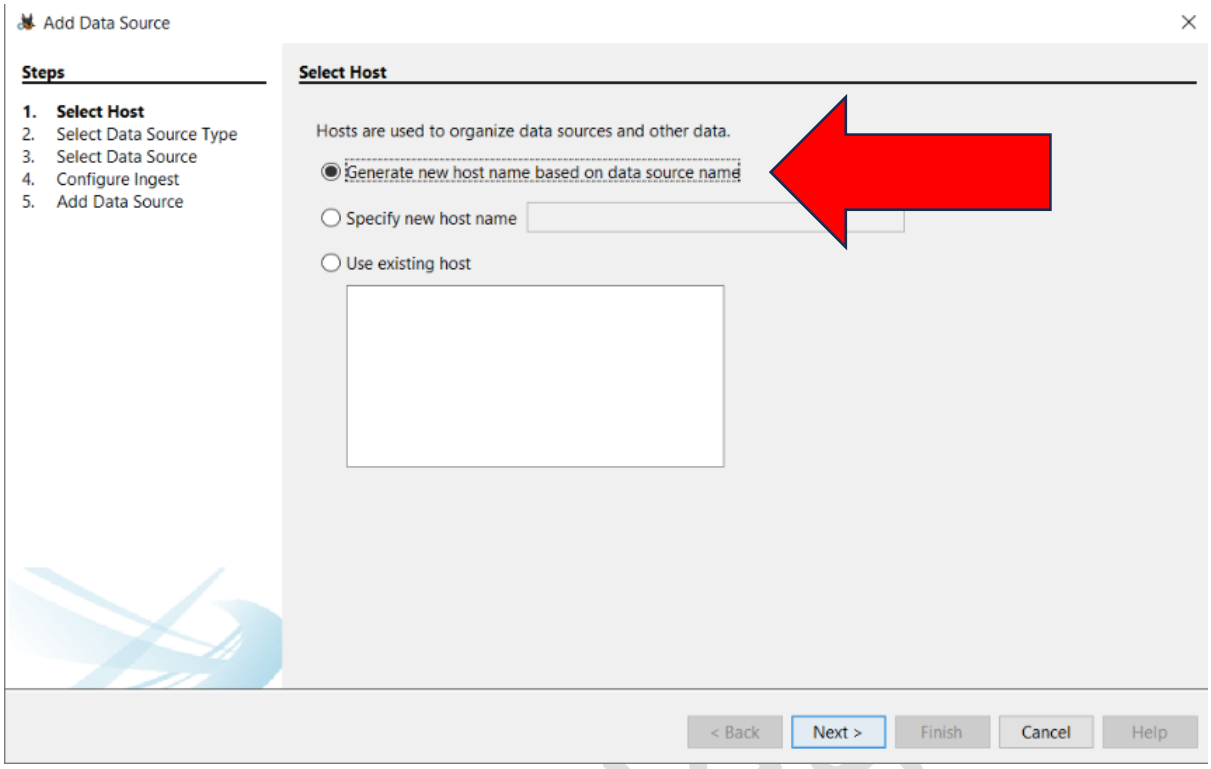
8. **Case Created:**
    - Autopsy will now create the case with the specified details, and you will be ready to start your analysis within this case.

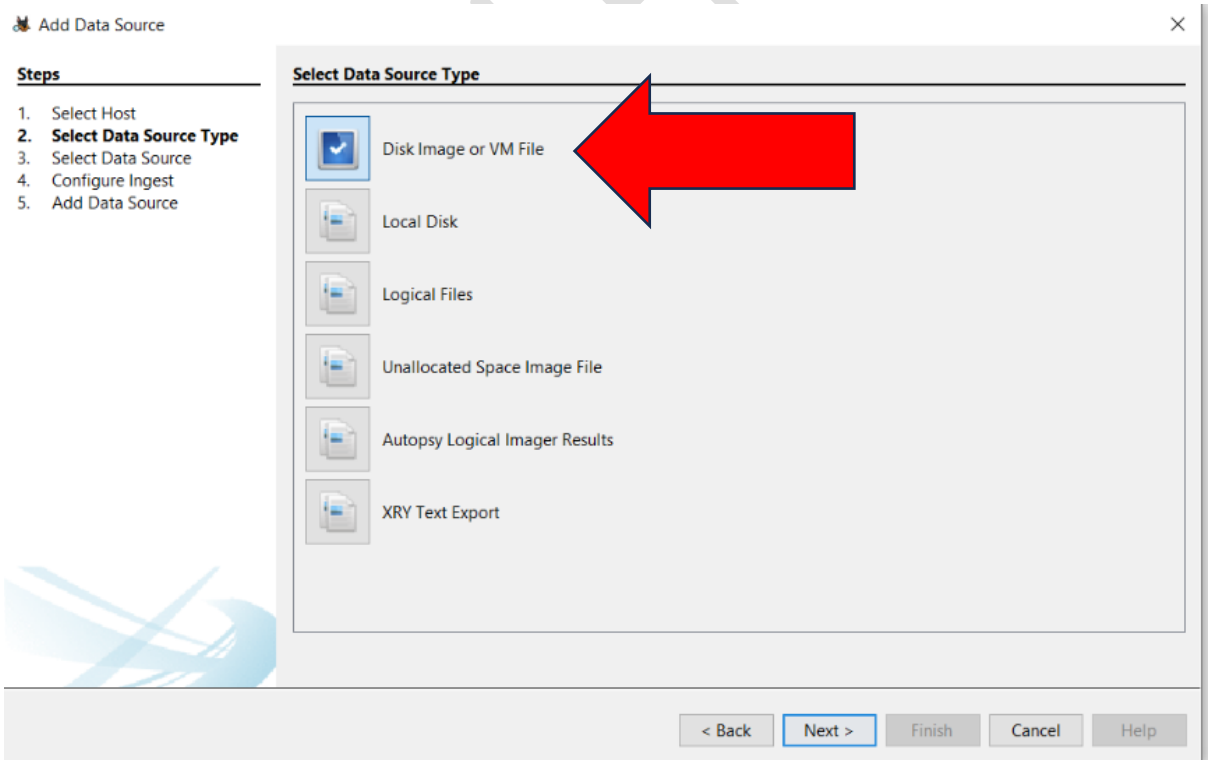


By following these steps, you will successfully install Autopsy and create a new case, allowing you to begin the analysis of the memory stick discovered.

Verify Image Integrity:

1. **Checksum Verification:**
    - Before adding the image file to Autopsy, you should verify its integrity by comparing its checksum with the provided checksum value.
    - Locate the checksum value provided with the image file. This may be an **MD5**, SHA-1, or SHA-256 checksum.
    - Utilize a checksum verification tool or command-line utility to calculate the checksum of the received image file.
    - Compare the calculated checksum with the provided checksum value. They should match.
2. **Cross-Check with the Provider:**
    - If the calculated checksum matches the provided checksum, it's a good indication that the image file hasn't been tampered with during transmission.
    - To further ensure the integrity of the image, you can cross-check with the provider to confirm that the checksum matches their records.
3. **Validation Procedures:**
    - Some digital forensic tools, including Autopsy, may include validation procedures during the import process. These procedures can automatically verify the integrity of the image file. Be sure to enable this option if available.
4. **Secure Backup:**
    - It's a best practice to create a *secure backup of the original image file* before adding it to your case. This ensures that you have an unaltered copy in case any issues arise during analysis.


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

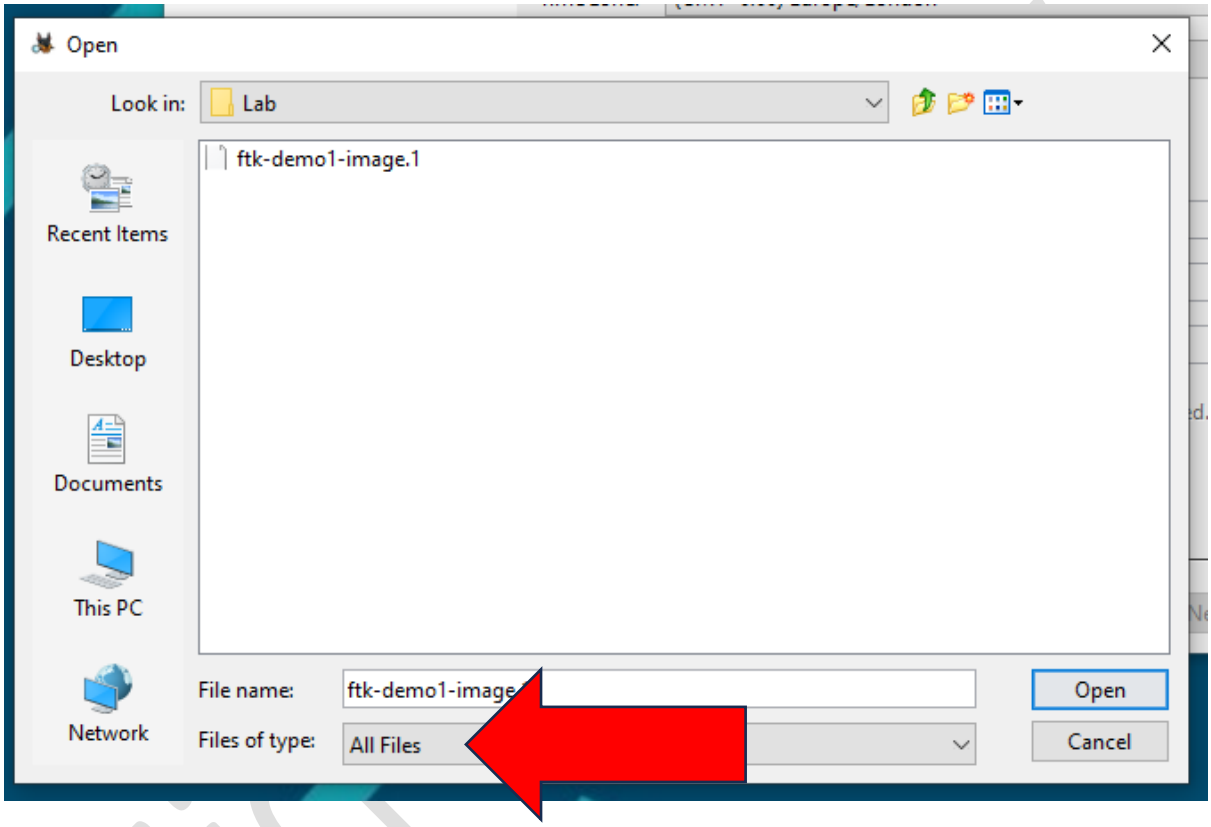
Adding a Data Source:

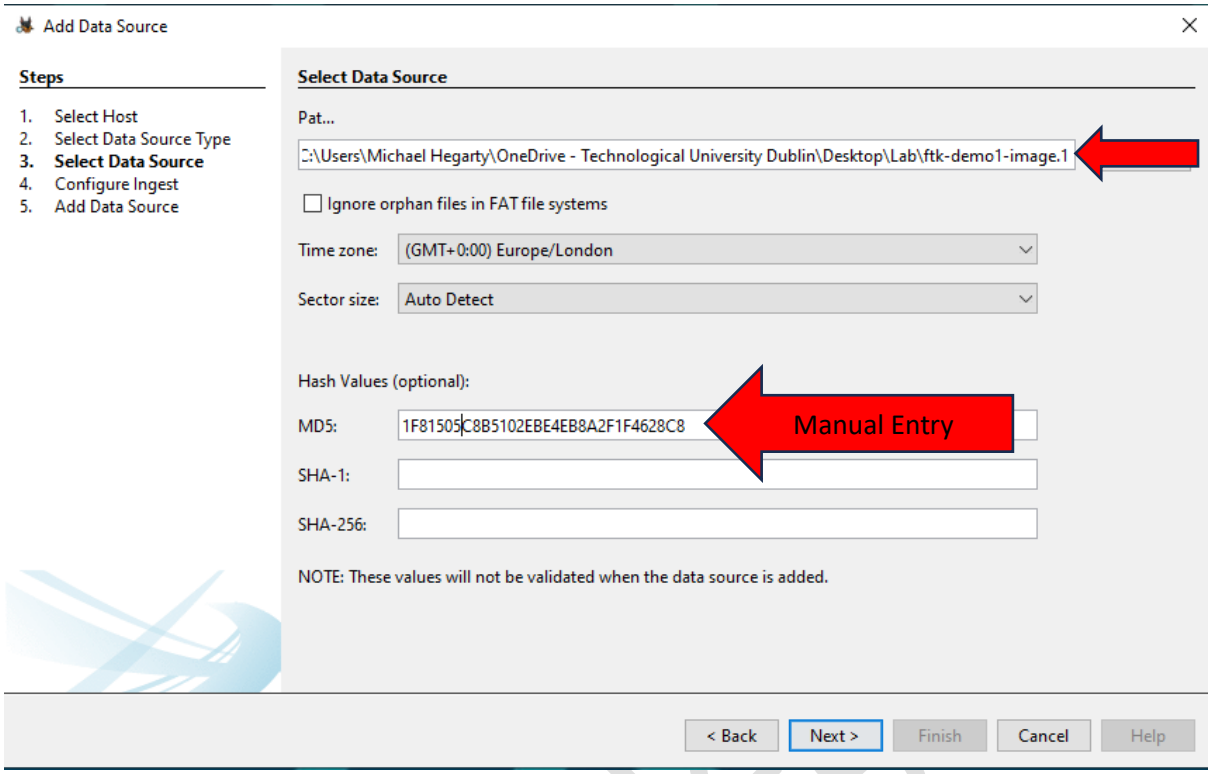
1. **Access the Add Data Source Wizard:**
    - After creating your case, the Add Data Source Wizard will start automatically. If it does not, you can manually start it by either going to the "File" menu or using the toolbar.
2. **Choose the Data Source Type:**
    - In the Add Data Source Wizard, you need to specify the type of input data source to add. You have several options:
        - *Image: If you want to analyse a disk image, select this option.*
        - Local Disk: Choose this option to analyse a local disk drive.
        - Logical Files and Folders: Select this option if you want to analyse specific files or folders on your system.
3. **Select the Appropriate Data Source:**
    - Depending on your selection:
        - For local disks: Autopsy will display a drop-down menu with detected disk drives. Choose the relevant disk you want to analyse.
            - Note: Running Autopsy as an Administrator may be necessary to detect all disks, especially on Windows 8.
        - For logical files and folders: Use the "Add" button to select one or more files or folders on your system that you want to add to the case. If you select a folder, its contents will be recursively added to the case.
4. **Providing the Image File Location:**
    - In this case, you will supply the location of the image file received for the lab.
    - Click "Browse" or a similar button to navigate to the location of the image file.
    - *The image file you will be using for this lab can be found in the lab folder from the previous week's lab. It is named "ftk-demo1-image.1."*
5. **Confirm and Add Data Source:**
    - Review your selection and ensure that you have chosen the correct data source for your case.
    - Click "Add" or a similar button to add the selected data source to your case.
6. **Data Source Added:**
    - Autopsy will add the chosen data source to your case, making it available for analysis within the Autopsy platform.

By following these steps, you will successfully add the relevant data source to your case in Autopsy, allowing you to begin the forensic analysis of the provided image file or other data sources.

Please note that running Autopsy as an Administrator may be necessary for detecting all disk drives, especially on certain Windows versions like Windows 8.

If you cannot view the file choose the "All Files" option (See screenshot below)





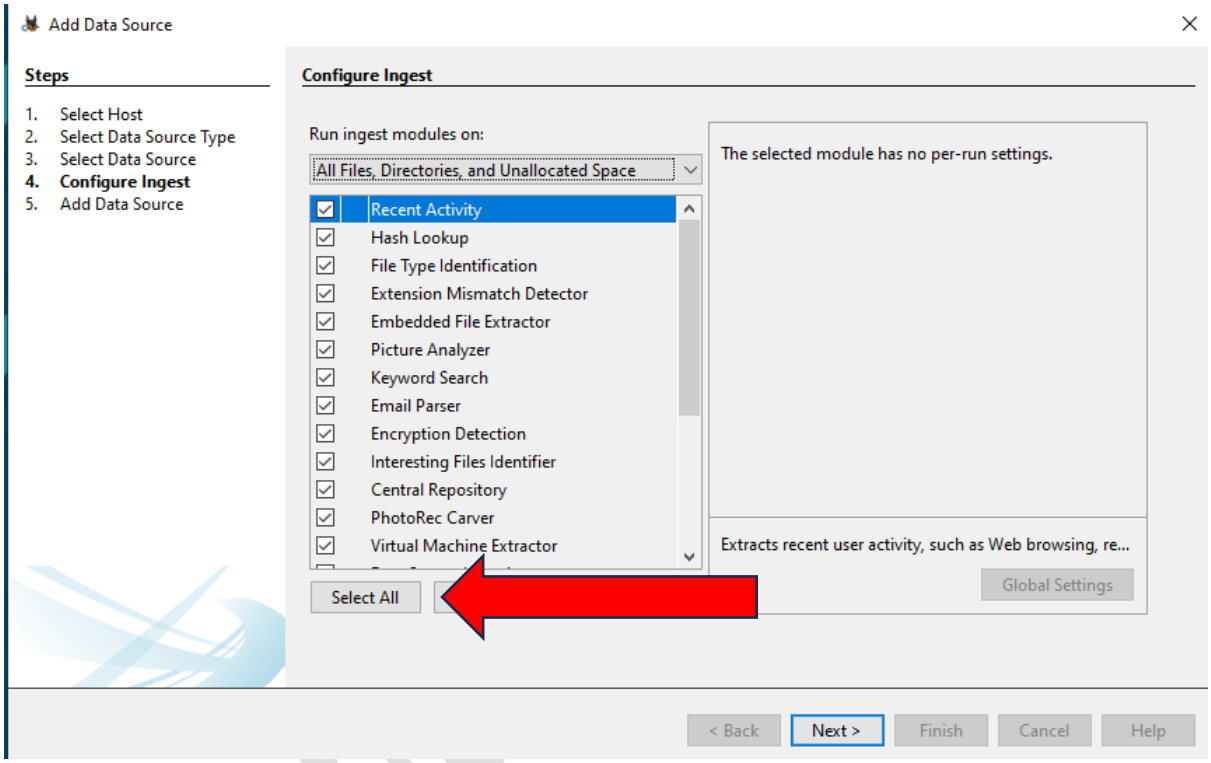
When adding the image to your case in Autopsy, you will be presented with options that can streamline the analysis process, including the discovery of deleted files. These options allow you to control the duration of the analysis. Since the image provided for this lab is relatively small, it is advisable to select all available options to ensure a thorough examination of the data.

Selecting Analysis Options:

1. **Access the Analysis Options:**
    - While adding the image to your case, you will come across a set of analysis options in the wizard. These options can enhance the efficiency of your analysis.
2. **Discovering Deleted Files:**
    - One of the key options presented in the wizard is related to the discovery of deleted files. Enabling this option will instruct Autopsy to search for and recover deleted files within the image.
3. **Control Analysis Duration:**
    - Autopsy offers options to fine-tune the analysis process. These options can be used to manage the duration of the analysis, especially on larger datasets.
4. **"Select All" for Faster Analysis:**

- Given that the image provided for this lab is relatively small, it is recommended to select all available options. This ensures a comprehensive analysis that covers deleted files and various forensic artifacts within the image.

By choosing to "Select All" for the analysis options, you optimize the examination process, making it more efficient while still maintaining a thorough and comprehensive analysis of the image.



Autopsy welcomes you with a user-friendly graphical interface (UI) that simplifies the forensic analysis process. To initiate your analysis, all procedures start from the left-hand tree view. Here's an overview of the key elements you'll encounter:

Data Sources:

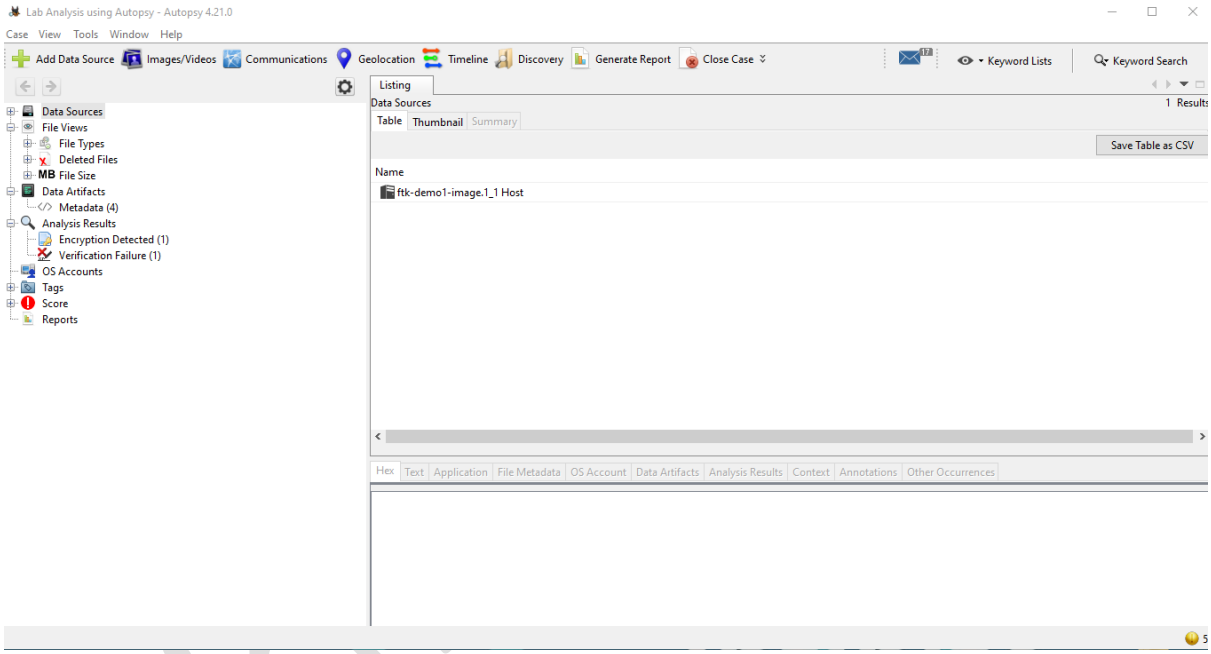
- The "Data Sources" section provides a comprehensive overview of the image and displays all the data contained within the case. It serves as the central point for managing and navigating through your analysis.

Image Nodes:

- Under the "Data Sources" section, you'll find individual image nodes. These nodes represent the file system structure of the local disks or disk image contained within the case. Each node

corresponds to a specific aspect of the data, enabling you to explore and analyse the content in a structured manner.

This tree-based approach in Autopsy simplifies your analysis workflow, allowing you to navigate through the data systematically and access various aspects of the case. Whether you're examining the file system structure, uncovering deleted files, or exploring other forensic artifacts, Autopsy's UI provides a user-friendly experience to aid in your investigative tasks.



On the right-hand side of Autopsy's interface, you'll find the "LogicalFileSet" nodes. These nodes are responsible for displaying the logical files contained within a specific folder or location within the image or case.

Key features of the "LogicalFileSet" nodes include:

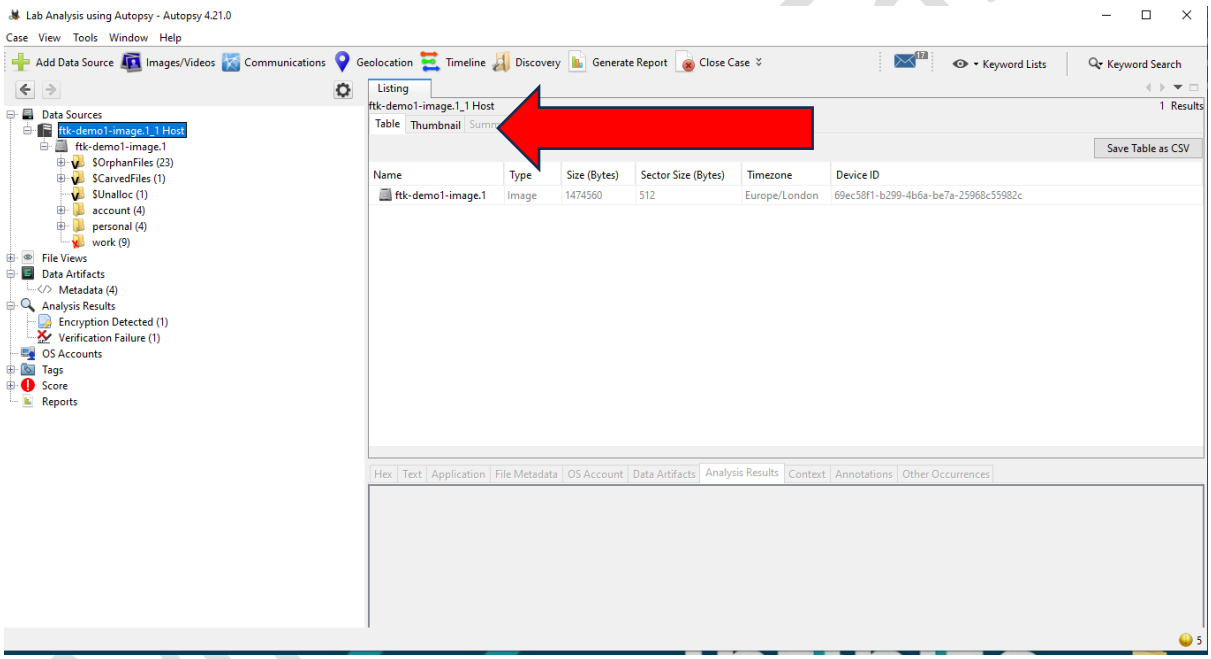
1. Displaying Logical Files: Each "LogicalFileSet" node represents a folder or location within the case. These nodes display the logical files contained within that specific folder.

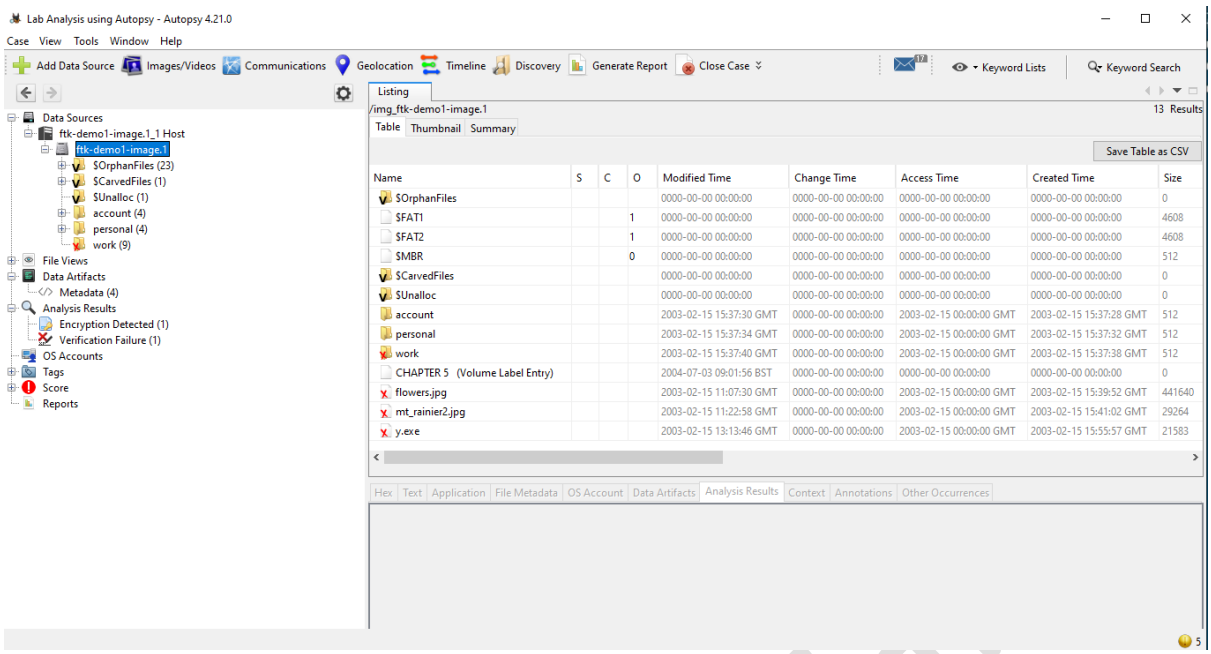
2. View Options: Autopsy provides you with flexibility in how you view these logical files. You can choose between two primary view options:

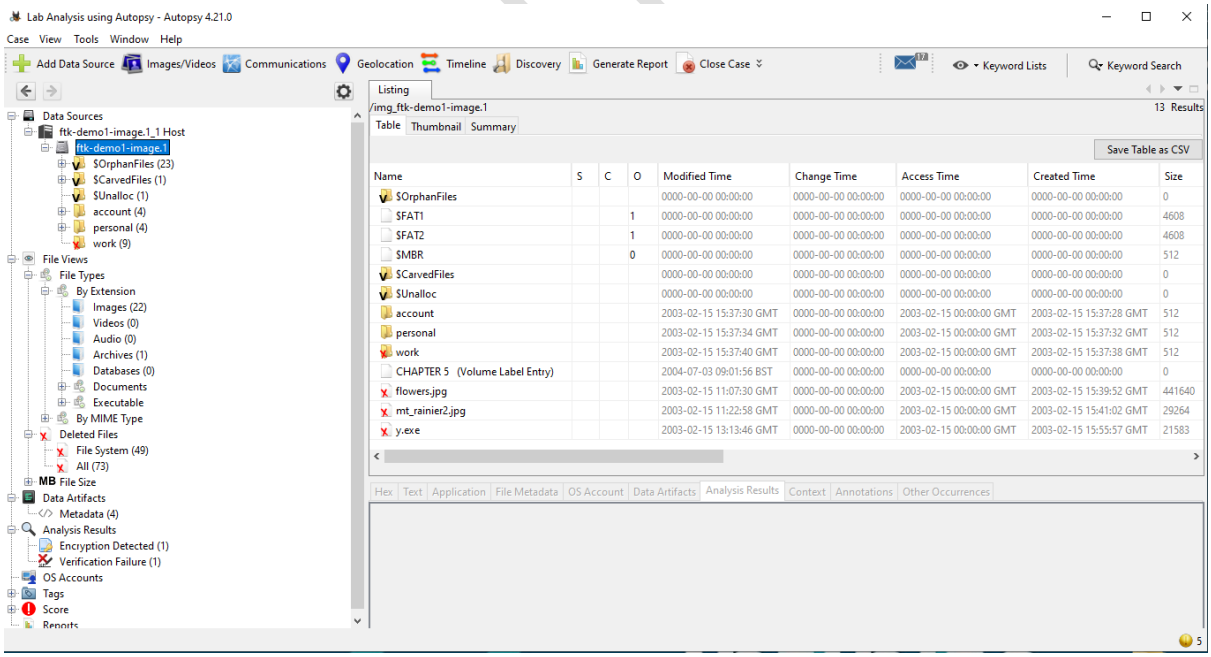
- **Table View:** This view presents the logical files in a structured table format, allowing you to access information such as file names, sizes, timestamps, and other file attributes.
- **Thumbnail View:** In this view, you can see thumbnail representations of image files, which can be particularly useful for quickly identifying visual content.

By offering both table and thumbnail views, Autopsy allows you to choose the display format that best suits your analysis needs. Whether you need a detailed file attribute overview or visual identification of images, Autopsy accommodates various analysis preferences.

These features make it easier for digital forensic investigators to explore and assess the logical files within the specified folders or locations, aiding in the comprehensive examination of the case's data.







In Autopsy, the "Views" option provides a convenient way to filter and display files of known format types, such as images, documents, PDFs, and HTML files. For instance, if you are specifically interested in locating media files like images and videos within the disk image, follow these steps:

1. Access the "Views" Section:

- On the left-hand tree view within Autopsy, navigate to the "Views" section. This section allows you to focus on specific types of files.

2. File Types Subsection:

- Within the "Views" section, locate the "File Types" subsection. This is where you can refine your search for files of a particular format.

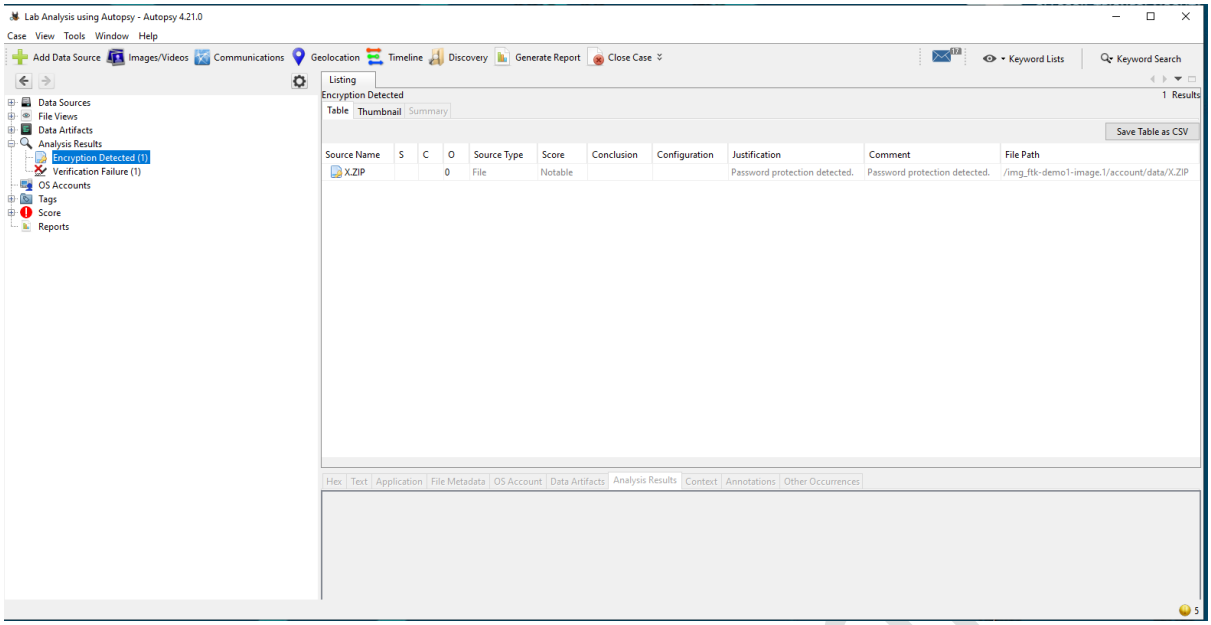
3. Select Images:

- Under the "File Types" subsection, select the category that corresponds to your desired file format, such as "Images" for media files like images and videos.

4. Thumbnail View:

- After selecting the relevant category (e.g., "Images"), you can use the thumbnail view option in the upper right-hand corner. This allows you to view thumbnails of all images that match the selected format.

By following these steps, you can quickly and efficiently filter files to display only those of a known format type, making it easier to examine and identify specific types of files, like images and videos, within the disk image. This feature streamlines the analysis process by focusing your attention on the file types most relevant to your investigation.



Question 1: How many images are viewable in thumbnail mode?

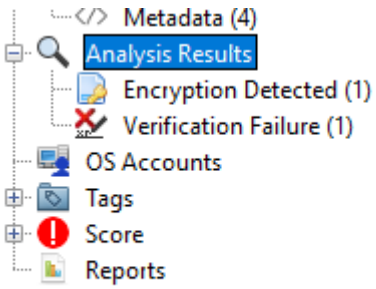
To answer this question, follow these steps:

1. In Autopsy, go to the "Views" section on the left-hand tree view.
2. Under "File Types," select the category "Images."
3. Use the thumbnail view option in the upper right to display the images in thumbnail mode.
4. Count the number of viewable images in thumbnail mode. This will be your answer to Question 1.

Question 2: Investigating the image _AF6.JPG using alternative options. What are your findings?

To investigate the image "_AF6.JPG" and report your findings, follow these steps:

1. In Autopsy, navigate to the "File Types" section under the "Views" section on the left-hand tree view.
2. Select the "Images" category to filter images.
3. Locate the image "_AF6.JPG" within the list of images.
4. Right-click on the image "_AF6.JPG" and explore the available options.
5. You can try alternative views, such as hex view, or use image analysis tools to examine the image for hidden or encrypted data.
6. Carefully document your findings, including any hidden or embedded information within the image



Question 3: What happens when you try to unzip the encrypted folder? Screen shot and detail the steps you took.

In Autopsy, the "Results" node displays the output from the ingest modules that were selected during the initial analysis. It has come to your attention that there is an encrypted file present in the results.

To extract the encrypted file for further analysis and explore additional options, follow these steps:

1. In the "Results" node, identify the encrypted file you want to extract.
2. Right-click on the file in the directory listings pane.
3. From the context menu, choose the option to extract the file to a desired folder. This action will save a copy of the file to the specified location.

This extraction process allows you to obtain a separate copy of the encrypted file, which can be further examined using encryption analysis tools or decryption techniques.

Additionally, explore the other options available in the context menu when right-clicking on a file. These options may include actions like viewing, analysing, or tagging the file, depending on your analysis needs. Autopsy provides a range of tools and features to facilitate comprehensive forensic analysis and examination of digital evidence.

The "Results" view in Autopsy includes a valuable feature that allows you to tag or bookmark files for future reference. This feature is especially useful when you want to highlight files that you consider important during your forensic analysis. To tag or bookmark a file, follow these steps:

1. Identify the file you want to tag or bookmark within the "Results" view.
2. Right-click on the file.
3. From the context menu, select the option to "Add Tag to File" and then choose "Bookmark."

By tagging and bookmarking files in this manner, you can create a quick reference list of significant files for future analysis or reporting.

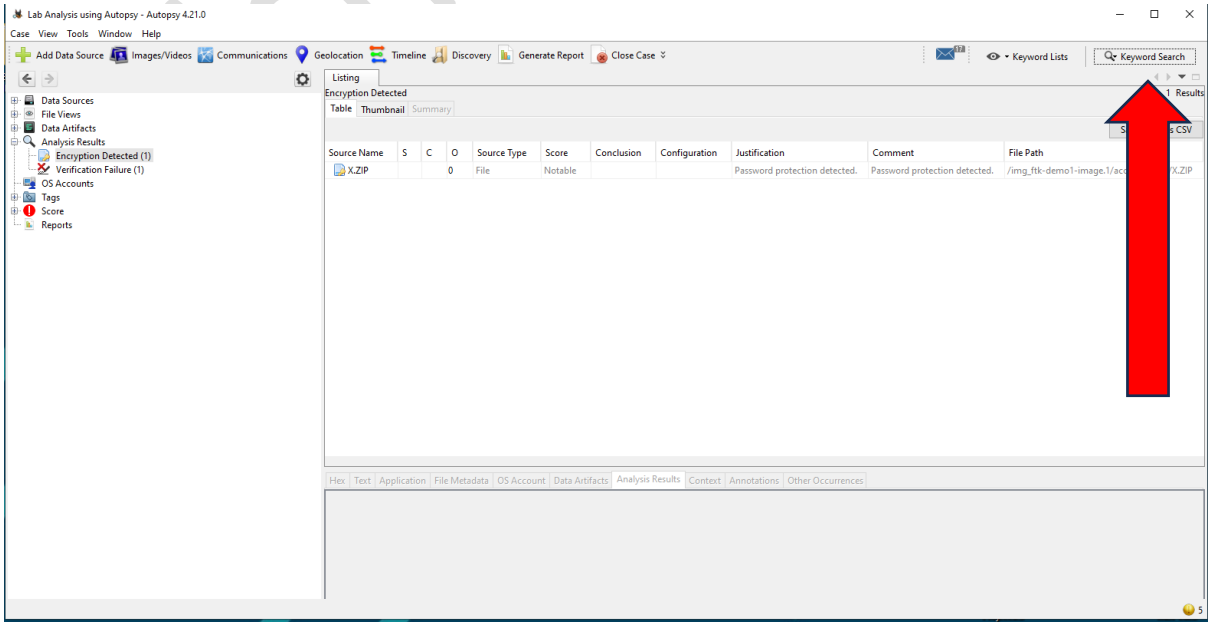
While examining a small image like the one in this lab, you may not need to tag many files. However, on larger storage devices (e.g., 500 GB or larger), the volume of data can be extensive, and tagging becomes essential to keep track of important findings. This practice helps maintain organization and aids in creating comprehensive reports. Autopsy also provides the capability to include tagged files and their details in the generated reports, further streamlining the documentation process.

To search for an exact match of the word "password" located throughout the image using the keyword search feature in Autopsy, follow these steps:

1. In Autopsy, access the "Keyword Search" feature. You can typically find this in the toolbar or menu options.
2. In the keyword search interface, enter the word "password" as the search term. Make sure to select the option for an exact match to ensure precise results.
3. Initiate the keyword search by clicking the search or find button, usually represented by a magnifying glass icon.
4. Autopsy will scan the image for any instances of the word "password."
5. Review the search results to identify any locations where the word "password" is found.

If any matches are discovered, you can further investigate the context in which "password" appears and determine if it is related to unlocking the encrypted zip folder. This search can be instrumental in finding potential password clues or hints within the image.

Carefully document your findings, as this information may be crucial in decrypting the encrypted folder and uncovering its contents.



Question 4, follow the instructions to determine how many files contain the word "password" and assess their relevance to the case:

1. Perform a keyword search for the term "password" throughout the image using Autopsy, as described in the previous text.
2. After the search is complete, take note of the number of files that contain the word "password."
3. Review the context and content of these files to assess their relevance to the case. Look for any clues or hints that may suggest which, if any, of these passwords could potentially open the encrypted folder.

The number of files containing the word "password" and their relevance to the case can provide insights into potential password options for unlocking the encrypted folder. Be sure to document your findings and any indications of the relevance of these passwords in your report.

Question 5 determine how many text files (.txt) can be found throughout the image, follow these steps:

1. In Autopsy, navigate to the "File Types" section under the "Views" tree on the left-hand side.
2. Look for the category or file type corresponding to text files, typically denoted as ".txt" or "Text."
3. Count the number of text files that are available within the image.
4. If you have located multiple text files, consider organizing them by their created time. This can help establish the chronological order of events that took place, providing a clearer timeline for your analysis.

Organizing text files by created time is particularly useful when dealing with a substantial number of text files, as it aids in identifying the sequence of events and understanding the context of the information contained within these files. Be sure to document your findings and any notable details related to these text files in your report.

Question 6 determine how we know that George has been using Outlook Express to send messages, we can rely on file extensions, which provide important clues about the software used. Follow these steps to identify the evidence:

1. Within the "File Types" section in Autopsy, locate the file extensions related to email messages, which are typically associated with specific email clients like Outlook Express. Common file extensions for email messages include .eml and .msg.
2. Search for files with these email-related file extensions within the image.
3. Once you've identified files with .eml or .msg extensions, this is an indicator that George has been using Outlook Express to send messages. These file extensions are specific to email messages generated by Outlook Express and are used to store individual email messages.

By recognizing the presence of .eml or .msg files in the image, you can conclude that George has utilized Outlook Express for sending messages. This evidence is crucial for your investigation and can help shed light on his email communications. Document this finding in your report for future reference.

Question 7 generate a report based on the facts uncovered during your investigation using Autopsy, follow these steps:

1. Review all the evidence you've collected and the key files you've tagged in Autopsy. Ensure that you have thoroughly documented your findings, including information related to the encrypted folder, passwords, email messages, and any other relevant data.
2. Utilize the built-in report feature in Autopsy to create an Excel report of the key evidence you've tagged. You can access the reporting feature within Autopsy. Refer to the additional information available at the provided link (http://sleuthkit.org/autopsy/docs/user-docs/4.17.0/reporting_page.html) for guidance on generating a report.
3. In your MS Word document, compile a comprehensive report that presents all the facts uncovered during your investigation. The report should be written in a professional and organized manner, including an executive summary, findings, analysis, and conclusions.
4. Ensure that your report follows a structured format, providing a clear overview of the case, the evidence collected, and the significance of each piece of evidence.
5. Add the Excel spreadsheet report generated in Autopsy to the end of your MS Word document.
6. Remember to maintain professionalism and impartiality in your report, as Steve Billings may use it for potential criminal proceedings. Be thorough and objective in presenting the facts you've uncovered.

Your final report should serve as a comprehensive document that presents all the necessary information in a clear and organized manner, aiding in Steve Billings' decision-making and any potential legal actions.

Question 8 confirm and validate the findings from FTK in last week's lab using Autopsy, perform the following steps:

1. First, ensure that you have access to the findings and evidence collected in FTK during the previous lab.
2. In Autopsy, review the findings from the current lab, which may include evidence related to George and Martha's case, email messages, tagged files, and the encrypted folder.
3. Compare the evidence and findings in Autopsy with the results obtained in FTK from the previous lab.
4. Look for consistencies and differences between the two sets of findings. Determine whether the evidence uncovered in Autopsy aligns with the evidence discovered in FTK.
5. Assess whether the evidence supports or corroborates the findings from both tools, reinforcing the conclusions drawn in the FTK lab.
6. Document any new insights or additional information uncovered in Autopsy that may complement the FTK findings.

By comparing the findings from both tools, you can verify the accuracy and reliability of your forensic analysis. If the evidence in Autopsy confirms and validates the findings from FTK, it strengthens the overall case and provides a more comprehensive view of the investigation. Document your comparative analysis in your final report to provide a holistic view of the case.

Place all your answer and report in one MS Word document and upload to moodle

"It is essential to maintain academic integrity and avoid any form of plagiarism or unauthorized sharing of answers or findings. Any suspected violations of academic honesty can lead to serious consequences, including being brought before the university's plagiarism committee. To ensure your work is original and adheres to ethical standards, always properly cite, and reference your sources and follow the institution's guidelines on academic integrity and honesty".