**CREATION OF SIMULATED CASE SCENARIOS TO CONDUCT FORENSIC ANALYSIS**

*PROJECT REPORT*

*Submitted in the partial fulfilment of the requirements*

*for award of the*

**Six Months Online Certificate Course**

*In*

**Cyber Security/**

**Data Science with Python Programming/**

**Artificial Intelligence and Machine Learning**

**Course Duration: [22-01-2024 to 21-07-2024]**

By

ALURU CHANDRA MOULI

(Ht No. 2406CYS123)

Under the Esteemed Guidance

Prof. P.PENCHALAIAH

****

**DIRECTORATE OF INNOVATIVE LEARNING & TEACHING**

**(DILT)**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

(Formerly SCDE\_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)

Kukatpally, Hyderabad, Telangana State, INDIA- 500 085

**JULY 2024**

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NUMBER** | **CHAPTER NAME** | **PAGE NUMBER** |
| **1.** | **Abstract** | **3** |
| **2.** | **Introduction** | **4** |
| **3.** | **Schematic Representation** | **6** |
| **4.** | **Literature Survey** | **11** |
| **5.** | **Objectives** | **13** |
| **6.** | **Problem Statement** | **14** |
| **7.** | **Methodology** | **15** |
| **8.** | **Diagram** | **17** |
| **9.** | **Algorithms** | **22** |
| **10.** | **Implementations** | **25** |
| **11.** | **Result analysis & Conclusion** | **28** |
| **12.** | **Future Scope** | **29** |

**ABSTRACT**

This report outlines a methodical approach for developing simulated case scenarios and practical exercises aimed at honing forensic analysis proficiency using autopsy tools. Autopsy, an open-source digital forensic platform, serves as a cornerstone tool for professionals in this field. Our methodology focuses on crafting realistic case scenarios mirroring diverse digital crimes, including cyber-attacks, data breaches, and financial fraud. These scenarios are coupled with the process of leveraging autopsy tools to scrutinize digital evidence, extract pertinent insights, and draw informed conclusions. The exercises span various facets of forensic analysis such as file system examination, keyword exploration, timeline reconstruction, and data recovery.

**INTRODUCTION**

This is designed to assist forensic analysts and investigators in examining digital media thoroughly. This comprehensive application facilitates the analysis of disk images, file systems, and various digital artifacts. Autopsy offers extensive support for artifact analysis, including internet history, email records, chat logs, and multimedia files. Its modular architecture allows for easy extension with custom modules and plugins, enhancing its versatility and adaptability to diverse forensic scenarios and other storage devices. Helps in enabling forensic professionals, law enforcement agencies, and cybersecurity experts to uncover valuable evidence, build strong cases, and ultimately contribute to the pursuit of justice.

Autopsy—an open-source, digital forensics platform used by law enforcement agencies worldwide to determine how a digital device was used in a crime and recover evidence—is being enhanced with the addition of several new capabilities requested by law enforcement.

Since it was first released 15 years ago, a community has grown around Autopsy development that continues to grow and deliver law enforcement investigators the new capabilities and functionality they have identified as pressing needs. The DHS Science and Technology Directorate previously funded the development and open-source release of Autopsy modules and its stewardship continues today as part of the Cyber Security Division’s (CSD) Cyber Security Forensics project. CSD is part of the Homeland Security Advanced Research Projects Agency. Autopsy—built as an extensible platform—boasts thousands of users around the world and is downloaded an average of 4,000 times each week. It supports all types of criminal investigations—from fraud to terrorism to child exploitation. As an open-source platform, it is a cost-effective tool investigators can use to solve crimes, especially in these days of shrinking budgets. In addition to the development activity, the platform also supports the incorporation of third-party modules (either open or closed source).

The easy-to-use software system has standard forensic tool features regularly used by federal, state, and local law enforcement organizations, including disk-image analysis, hash-set analysis, indexed keyword search, registry analysis, and Android and web-artifact analysis. Additionally, Autopsy includes unique capabilities such as support for multi-user cases, automated ingest and correlation analysis.

**As part of the current Cyber Forensics project work plan, the following capabilities will be developed or enhanced within Autopsy:**

* **A New Communication Analysis Framework**— This will develop a storage framework for communications-based data and a graphical interface, making it easier for investigators to view messages from a variety of sources, visualize the messages, and see the relationships between accounts.
* **Advanced Image Analysis Functionality**— This enhancement will expand Autopsy’s existing photo and video analysis capabilities to more efficiently analyze large numbers of images stored on a device’s hard drive.
* **Advanced Timeline Visualization**— New features will be added, including integration with existing open-source parsing tools, allowing users to create events and highlight events, and filter by file type to the timeline module to more efficiently analyze activity to determine what events occurred.

Over the last several years, the Cyber Security Forensics project has transitioned the following technologies in support of law enforcement organizations nationwide.

* Tutorials on accessing and analyzing disposable mobile phones
* Previous Autopsy module enhancements
* iVe, a digital forensics tool that acquires user data from the vehicle infotainment and telematics systems of more than 10,000 vehicle makes and models

**SCHEMATIC REPRESENTATION**

**Here are several key diagrams that illustrate how digital forensics works, focusing on different aspects of the process:**

### 1. ****Digital Forensics Process Overview****

This diagram provides a high-level view of the digital forensics process, outlining the main stages from evidence collection to reporting.

Diff

Copy code

+---------------------+

| Evidence Collection |

+---------------------+

 |

 V

+---------------------+

| Evidence Preservation|

+---------------------+

 |

 V

+---------------------+

| Evidence Analysis |

+---------------------+

 |

 V

+---------------------+

| Reporting & Review |

|  |
| --- |
|  |

****Description:****

* **Evidence Collection:** Gathering digital evidence from various sources (e.g., hard drives, mobile devices).
* **Evidence Preservation:** Ensuring the evidence is preserved in its original state to maintain integrity.
* **Evidence Analysis:** Performing forensic analysis to extract and interpret relevant data.
* **Reporting & Review:** Documenting findings and preparing reports for legal or investigative purposes.

### 2. ****Digital Evidence Acquisition****

This diagram shows the process of acquiring digital evidence from a device.

diff

Copy code

+---------------------+

| Device Preparation |

+---------------------+

 |

 V

+---------------------+

| Data Imaging |

+---------------------+

 |

 V

+---------------------+

| Data Verification |

+---------------------+

****Description:****

* **Device Preparation:** Preparing the device for imaging, this may include securing and documenting the device.
* **Data Imaging:** Creating a bit-for-bit copy of the device's storage.
* **Data Verification:** Verifying that the image is an exact copy of the original data.

### 3. ****File Carving Process****

This diagram illustrates the steps involved in file carving to recover files from a disk image.

Sql

Copy code

+---------------------+

| Data Block Analysis |

+---------------------+

 |

 V

+---------------------+

| Header/Footer Search|

+---------------------+

 |

 V

+---------------------+

| File Reconstruction |

+---------------------+

****Description:****

* **Data Block Analysis:** Examining blocks of data to identify potential file fragments.
* **Header/Footer Search:** Looking for known file signatures (headers/footers) to identify file boundaries.
* **File Reconstruction:** Reconstructing complete files from identified fragments.

### 4. ****Timeline Analysis****

This diagram depicts how timeline analysis is used to correlate events from different data sources.

diff

Copy code

+---------------------+

| Extract Timestamps |

+---------------------+

 |

 V

+---------------------+

| Correlate Events |

+---------------------+

 |

 V

+---------------------+

| Build Timeline |

+---------------------+

****Description:****

* **Correlate Extract Timestamps:** Extracting timestamps from file metadata, logs, and other sources.
* **Events:** Matching events from different sources based on timestamps.
* **Build Timeline:** Constructing a chronological sequence of events.

### 5. ****Keyword Search Process****

This diagram shows the steps involved in conducting a keyword search in digital forensics.

Sql

Copy code

+---------------------+

| Define Keywords |

+---------------------+

 |

 V

+---------------------+

| Index Data |

+---------------------+

 |

 V

+---------------------+

| Search & Retrieve |

+---------------------+

 |

 V

+---------------------+

| Analyze Results |

+---------------------+

****Description:****

* **Define Keywords:** Establishing the terms or patterns to search for in the data.
* **Index Data:** Creating an index to speed up search operations.
* **Search & Retrieve:** Performing the search and retrieving matching data.
* **Analyze Results:** Reviewing and analyzing the search results to find relevant information.

### 6. ****Autopsy Tool Workflow****

This diagram illustrates the workflow of using the Autopsy tool for digital forensic analysis.

Sql

Copy code

+---------------------+

| Data Ingestion |

+---------------------+

 |

 V

+---------------------+

| Case Management |

+---------------------+

 |

 V

+---------------------+

| Analysis Modules |

+---------------------+

 |

 V

+---------------------+

| Reporting |

+---------------------+

**Description:**

* **Data Ingestion:** Importing data into Autopsy for analysis.
* **Case Management:** Organizing and managing cases within the tool.
* **Analysis Modules:** Using various analysis modules to examine and interpret the data.
* **Reporting:** Generating reports based on the analysis for documentation and presentation.

These diagrams provide a visual representation of the digital forensic process and the specific steps involved in different aspects of forensic analysis. They help to understand the workflow and methodology used in digital forensics.

 **LITERATURE SURVEY**

### Digital Forensics and Its Importance

Digital forensics encompasses a wide range of techniques and tools used to investigate digital devices and media. The primary objectives are to recover, analyze, and present data that can be used in legal proceedings. This field has grown significantly due to the rise in cybercrime, necessitating robust methods for investigating digital evidence.

#### Key Concepts in Digital Forensics

* **Data Recovery**: Techniques to retrieve deleted, corrupted, or hidden data.
* **Analysis**: Examining recovered data to reconstruct events.
* **Chain of Custody**: Ensuring evidence is preserved in its original state.
* **Legal Framework**: Understanding the legal implications and requirements of digital evidence.

### The Role of Autopsy in Digital Forensics

Autopsy is a highly regarded digital forensics tool that supports a variety of forensic tasks, including:

* **File Analysis**: Recovering and analyzing files from disk images.
* **Timeline Analysis**: Creating timelines of user activity.
* **Keyword Search**: Searching for specific terms within recovered data.
* **Hash Filtering**: Using hash values to identify known good and bad files.

#### Features of Autopsy

* **Open-Source**: Accessible and modifiable by the forensic community.
* **Modular Design**: Allows integration of additional modules to extend functionality.
* **User-Friendly Interface**: Facilitates ease of use for both novice and experienced investigators.

### Simulated Case Scenarios in Digital Forensics

Simulated case scenarios are designed to mimic real-life digital crimes, offering investigators a platform to apply theoretical knowledge in practice. These scenarios can vary from simple data recovery tasks to complex multi-device investigations. Studies have shown that hands-on experience with simulated cases enhances the learning curve and prepares investigators for real-world challenges.

#### Key Elements of Effective Simulated Scenarios

Effective simulated case scenarios should include several key elements:

1. **Realism:** Scenarios should closely resemble actual cases to provide realistic challenges.
2. **Complexity:** A range of complexity levels, from basic to advanced, ensures comprehensive skill development.
3. **Relevance:** Scenarios should cover a wide range of digital crimes, reflecting current trends and threats.

### Integration of Simulated Scenarios with Autopsy

The integration of simulated case scenarios with the Autopsy tool enhances the practical training of digital forensic investigators. Research indicates that using Autopsy in simulated environments provides a dual benefit: familiarizing investigators with the tool’s functionalities while developing their analytical and problem-solving skills.

#### Methodologies for Creating Simulated Scenarios

Several methodologies have been proposed for creating effective simulated case scenarios:

1. **Case Study Approach:** Using real-world cases as templates to create similar scenarios.
2. **Modular Approach:** Developing modular components that can be combined to form different scenarios.
3. **Scenario-based Learning:** Incorporating learning objectives into scenario development to ensure educational value.

### Evaluation of Training Effectiveness

### **The effectiveness of training using simulated scenarios in Autopsy**

* **Skill Assessment:** Pre- and post-training assessments to measure skill improvement.
* **Performance Metrics:** Analysis of accuracy, efficiency, and thoroughness in handling simulated cases.
* **Feedback Mechanisms:** Gathering feedback from trainees to continuously improve the scenarios and training methodologies.

**OBJECTIVES**

* **As part of the current Cyber Forensics project work plan, the following capabilities will be developed or enhanced within Autopsy:**
* **A New Communication Analysis Framework—This will develop a storage framework for communications-based data and a graphical interface, making it easier for investigators to view messages from a variety of sources, visualize the messages, and see the relationships between accounts.**
* **Advanced Image Analysis Functionality—This enhancement will expand Autopsy’s existing photo and video analysis capabilities to more efficiently analyze large numbers of images stored on a device’s hard drive.**
* **Advanced Timeline Visualization—new features will be added, including integration with existing open-source parsing tools, allowing users to create events and highlight events, and filter by file type to the timeline module to more efficiently analyze activity to determine what events occurred.**
* **“These enhancements will substantially increase Autopsy’s ease-of-use for law enforcement agencies,” said Megan Mahle, program manager of S&T’s Cyber Security Forensics project. “The modules we’re focusing on through our effort will add new functionalities and promote flexibility for use by each law enforcement investigator.”**

The primary objective of this project is to develop and implement realistic simulated case scenarios for training digital forensic investigators using the Autopsy tool. These scenarios aim to enhance the practical skills and analytical capabilities of investigators by providing a controlled environment that mimics real-world digital crime situations. By integrating comprehensive, relevant, and complex cases, the project seeks to bridge the gap between theoretical knowledge and practical application, ultimately preparing investigators for effective and efficient handling of digital evidence in actual investigations.

**PROBLEM STATEMENT**

Understanding the importance and usage of Autopsy tool in Digital forensic by applying simulated case scenarios.

Current training methods often lack the depth and realism necessary to simulate the complexities of actual digital forensic investigations. Many existing simulated scenarios fail to accurately reflect the range of digital crimes or the intricacies involved in forensic analysis. This shortfall in training realism and variety can lead to gaps in an investigator’s ability to handle complex cases, potentially resulting in errors, incomplete analyses, and decreased overall efficacy in forensic operations.

As digital crimes become more sophisticated and frequent, there is a growing need for digital forensic investigators who can effectively analyze and interpret complex digital evidence. Traditional training methods, which often focus more on theory than on hands-on practice, are not always sufficient to prepare investigators for the real-world challenges they will face. This gap in practical training can lead to mistakes and inefficiencies, potentially undermining the effectiveness of forensic investigations and impacting the justice process.

Although tools like Autopsy are available to aid investigations, there is a noticeable lack of realistic training scenarios where investigators can practice their skills. Existing simulated cases often do not reflect the complexity or variety of real-world digital crimes, leaving investigators underprepared.

This project seeks to fill this gap by developing a set of realistic simulated case scenarios using the Autopsy tool. The goal is to create a training environment that mirrors real-life digital crime situations, helping investigators to hone their skills and build confidence. By offering a more practical and comprehensive training experience, this project aims to improve the overall effectiveness of digital forensic investigations.

This project addresses these critical issues by designing and implementing a series of detailed and realistic simulated case scenarios, specifically tailored for use with the Autopsy tool. The objectives are to:

1. **Develop Realistic Scenarios:** Create a range of simulated digital crime cases that accurately reflect the complexity and variety of real-world incidents.
2. **Enhance Training Quality:** Use these scenarios to provide investigators with practical, hands-on experience, enabling them to apply their knowledge in a controlled yet challenging environment.
3. **Improve Tool Utilization:** Ensure that the Autopsy tool is used effectively within these scenarios to familiarize investigators with its full range of features and capabilities.

**METHODOLOGY**

# Workflow Overview and Case Analysis

**Workflow Overview**

Before diving into Autopsy and analyzing data, there are a few steps to perform; such as identifying the data source and what Autopsy actions to perform with the data source.

**Basic workflow:**

1. Create/open the case for the data source you will investigate.
2. Select the data source you wish to analyze.
3. Configure the ingest modules to extract specific artefacts from the data source.
4. Review the artefacts extracted by the ingest modules.
5. Create the report.

****Case Analysis | Create a New Case****

To prepare a new case investigation, you need to create a case file from the data source. When you start Autopsy, there will be three options. You can create a new case file using the**“New Case”** option.

 Once you click on the “New Case” option, the **Case Information**menu opens**,** where information about the case is populated.

* **Case Name**: The name you wish to give to the case
* **Base Directory**: The root directory that will store all the files specific to the case (the full path will be displayed)
* **Case Type**: Specify whether this case will be local (**Single-user**) or hosted on a server where multiple analysts can review (**Multi-user**)

**Note**: In this room, the focus is on **Single-User**. Also, the room doesn’t simulate a new case creation, and the given VM has a sample case file to practice covered Autopsy features.

The following screen is titled “**Optional Information”** and can be left blank for our purposes. In an actual forensic environment, you should fill out this information. Once you click on “Finish”, Autopsy will create a new case file from the given data source.

**Case Analysis | Open an Existing Case**

The Autopsy can also open prebuilt case files. Note that supported data sources are discussed in the next task. This part aims to show how to create/open case files with Autopsy.

**Note:** Autopsy case files have a “.aut” file extension.

**In this room, you will import a case.** To open a case, select the “Open Case” option. Navigate to the case folder (located on the desktop) and select the .aut file you wish to open. Next, Autopsy will process the case files and open the case. You can identify the name of the case at the top left corner of the Autopsy window. In the image below, the name of this case is**“Sample Case”**.

### **DIAGRAM**

This methodology ensures a comprehensive and iterative approach to developing high-quality, realistic training scenarios that effectively utilize the Autopsy tool. The following diagram outlines the methodology for creating and implementing the simulated case scenarios:

1. **Scenario Design:** The process begins with designing realistic scenarios based on a thorough needs assessment and detailed scenario documentation.
2. **Tool Integration:** Next, the Autopsy tool is configured and integrated into the scenarios, followed by testing to ensure functionality.
3. **Testing:** The scenarios are tested with pilot users to gather feedback and refine the scenarios and tool integration.
4. **Evaluation:** Finally, the effectiveness of the training is evaluated using performance metrics and outcome assessments, leading to reporting and further improvements.

**+-------------------+**

**| Scenario Design |**

**+-------------------+**

**|**

**V**

**+-------------------+**

**| Tool Integration |**

**+-------------------+**

**|**

**V**

**+-------------------+**

**| Testing |**

**+-------------------+ |**

**V**

**+-------------------+**

**| Evaluation**

 **|+-------------------+**

# **Ingest Modules**

Essentially **Ingest Modules** are Autopsy plug-ins. Each Ingest Module is designed to analyses and retrieves specific data from the drive. You can configure Autopsy to run specific modules during the source-adding stage or later by choosing the target data source available on the dashboard. By default, the Ingest Modules are configured to run on **All Files, Directories, and Unallocated Space**. You can change this setting during the module selecting step. You can track the process with the bar appearing in the lower right corner.

**The Tree Viewer has five top-level nodes:**

* **Data Sources**— all the data will be organized as you would typically see it in a normal Windows File Explorer.
* **Views** — files will be organized based on file types, MIME types, file size, etc.
* **Results** — as mentioned earlier, this is where the results from Ingest Modules will appear.
* **Tags** — will display files and/or results that have been tagged.
* **Reports** — will display reports either generated by modules or the analyst.

**Data Sources Summary**

The **Data Sources Summary**provides summarized info in nine different categories. Note that this is an overview of the total findings. If you want to dive deep into the findings and look for a specific artefact, you need to analyses each module separately using the **“Result Viewer”**shown in the previous task.

**Generate Report**

You can create a report of your findings in multiple formats, enabling you to create data sheets for your investigation case. The report provides all information listed under the “Result Viewer” pane. Reports can help you to re-investigate findings after finishing the live investigation. **However, reports don’t have additional search options, so you must manually find artefacts for the event of interest.**

**Tip:**The Autopsy tool can be heavy for systems with low resources. Therefore completing an investigation with Autopsy on low resources can be slow and painful. Especially browsing long results might end up with a system freeze. You can avoid that situation by using reports. You can use the tool for parsing the data and generating the report, then continue to analyses through the generated report without a need for Autopsy. Note that it is always easier to conduct and manage an investigation with the GUI.

# **Visualization Tools**



* **Images/Videos:**<http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/image_gallery_page.html>
* **Communications:**<http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/communications_page.html>
* **Timeline:**<http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/timeline_page.html>

**Note**: Within the attached VM, you will **NOT** be able to access with some of the visualisation tools, except for **Timeline**.

**The Timeline tool is composed of three areas:**

1. **Filters:**Narrow the events displayed based on the filter criteria
2. **Events:**The events are displayed here based on the **View Mode**
3. **Files/Contents:**Additional information on the event(s) is displayed in this area

**ALGORITHMS**

Autopsy tool utilizes various algorithms to perform critical analysis tasks. These algorithms support the recovery, examination, and interpretation of digital evidence. Here’s an overview of the key algorithms and techniques used in forensic analysis with the Autopsy tool:

### 1. ****File Carving Algorithms****

File carving is the process of recovering files from a disk image without the use of file system metadata. Autopsy uses several algorithms to identify and recover file fragments:

* **Header and Footer Identification:** Detects file types by looking for known file headers and footers. For example, JPEG files typically start with the hex signature FFD8 and end with FFD9.
* **Pattern Matching:** Uses signature databases to identify file types and recover files based on known patterns and structures.
* **Entropy-Based Carving:** Analyzes the entropy of data blocks to identify and reconstruct files, particularly useful for recovering fragmented or partially overwritten files.

### 2. ****Keyword Search Algorithms****

Keyword searches are used to locate specific terms or patterns within the digital evidence

* **Exact Match Search:** Finds exact matches of keywords or phrases within the data.
* **Regular Expression Search:** Allows for more complex searches using patterns defined by regular expressions, which can match variations and more sophisticated search criteria.

3. ****Timeline Analysis Algorithms****

Timeline analysis involves organizing events based on timestamps to reconstruct the sequence of actions:

* **File Metadata Parsing:** Extracts timestamps and metadata from file systems, such as creation, modification, and access times.
* **Event Correlation:** Combines timestamps from various sources (e.g., file metadata, system logs) to build a chronological sequence of events.
* **Gap Detection:** Identifies gaps or inconsistencies in the timeline to highlight potential areas of interest.

### 4. ****Data Extraction and Recovery Algorithms****

These algorithms are used to extract and recover data from digital media:

* **Disk Imaging:** Creates an exact copy of the disk, preserving the original data and metadata.
* **Volume Reconstruction:** Rebuilds logical volumes from physical disk images, particularly useful for complex file systems.
* **Unallocated Space Analysis:** Examines free space on the disk to recover deleted or hidden files.

### 5. ****Hashing Algorithms****

Hashing is used for data integrity verification and to detect duplicate files:

* **MD5 (Message Digest Algorithm 5):** Commonly used for generating hash values to verify file integrity and identify files.
* **SHA-1 (Secure Hash Algorithm 1):** Another hashing algorithm used for generating hash values, providing a higher degree of collision resistance compared to MD5.
* **SHA-256:** Provides a more secure hashing option, offering enhanced collision resistance and security.

### 6. ****Image and Video Analysis Algorithms****

 Involves specific techniques to extract and interpret visual data:

* **Exif Data Extraction:** Extracts metadata from image files, such as camera settings, GPS coordinates, and timestamps.
* **Steganography Detection:** Identifies hidden information embedded within image or video files, which may be used to conceal evidence.

### **7. **Database and Email Analysis Algorithms****

These algorithms are tailored for analyzing structured data and communication artifacts:

* **Database Query Parsing:** Extracts and analyzes data from database files, such as SQLite or MySQL databases.
* **Email Parsing:** Analyzes email messages, attachments, and metadata to uncover communication patterns and relevant information.

### **8. **File System Analysis Algorithms****

Autopsy performs detailed analysis of various file systems:

* **File System Metadata Analysis:** Parses file system structures to recover file entries, directories, and other metadata.
* **File System Reconstruction:** Reconstructs the logical structure of the file system from raw disk images, particularly useful for damaged or corrupted file systems.

**IMPLEMENTATION**

 Autopsy tool comes preinstalled in kali Linux so, start the Kali Virtual Machine. You will find the option ‘forensics’ in the application tab. Select ‘autopsy’ from the list of forensics tools. When you select autopsy, it will open a prompt where you see program information, the version number listed as 2.24 with the path to the Evidence Locker folder as /var/lib/autopsy and an address [***http://localhost:9999/autopsy***](http://localhost:9999/autopsy) to open it on a web browser. Click on that link and open it in your Kali web browser, you will be redirected to the home page of autopsy. This tool is running on our local web server accessing the port 9999.

# ***Create a New Case***

There will be three options on the home page: ‘OPEN CASE’, NEW CASE’, ‘and HELP’. For forensic investigation, we need to create a new case and arrange all the information and evidences. Select ‘NEW CASE’.

***Case Analysis | Create a New Case***

To prepare a new case investigation, you need to create a case file from the data source. When you start Autopsy, there will be three options. You can create a new case file using the**“New Case”** option. Once you click on the “New Case” option, the **Case Information**menu opens**,** where information about the case is populated.

* **Case Name**: The name you wish to give to the case
* **Base Directory**: The root directory that will store all the files specific to the case (the full path will be displayed)
* **Case Type**: Specify whether this case will be local (**Single-user**) or hosted on a server where multiple analysts can review (**Multi-user**)

# ***Data Sources***

Autopsy can analyze multiple disk image formats. Before diving into the data analysis step, let’s briefly cover the different data sources Autopsy can analyze. You can add data sources by using the **“Add Data Source”** button.

**Supported Disk Image Formats:**

* **Raw Single** (For example: \*.img, \*.dd, \*.raw, \*.bin)
* **Raw Split** (For example: \*.001, \*.002, \*.aa, \*.ab, etc.)
* **EnCase** (For example: \*.e01, \*.e02, etc.)
* **Virtual Machines** (For example: \*.vmdk, \*.vhd)

# ***Ingest Modules***

Essentially **Ingest Modules** are Autopsy plug-ins. Each Ingest Module is designed to analyze and retrieve specific data from the drive. You can configure Autopsy to run specific modules during the source-adding stage or later by choosing the target data source available on the dashboard. By default, the Ingest Modules are configured to run on **All Files, Directories, and Unallocated Space**. One can change this setting during the module selecting step.

***Status Area***

 Lastly, the **Status Area**is at the bottom right. When Ingest Modules run, a progress bar (along with the percentage completed) will be displayed in this area. More detailed information regarding the Ingest Modules is provided if you click on the bar.

# ***The User Interface***

Let’s look at where we can find summarized info with ease. Summarized info can help analysts decide where to focus by evaluating available artefacts. It is suggested to view the summary of the data sources before starting an investigation. Therefore you can have a general idea about the system and artefacts.

****Data Sources Summary**:**

The **Data Sources Summary**provides summarized info in nine different categories. Note that this is an overview of the total findings. If you want to dive deep into the findings and look for a specific artefact, you need to analyze each module separately using the **“Result Viewer”.**

***Generate Report***

You can create a report of your findings in multiple formats, enabling you to create data sheets for your investigation case. The report provides all information listed under the “Result Viewer” pane. Reports can help you to re-investigate findings after finishing the live investigation.

#  RESULT ANALYSIS AND CONCLUSION

#### Key Findings

1. ****Development of Test Cases:****
	* We successfully created a variety of test cases, each with its own unique set of challenges. These included scenarios such as email fraud, data breaches, malware infections, and insider threats.
	* The test cases were designed to be as realistic as possible, incorporating authentic data and conditions to closely mimic real forensic investigations.
2. ****Performance of the Autopsy Tool:****
	* ****Strengths:**** Autopsy performed admirably in several areas. It handled different file systems well, was effective at recovering deleted files, and excelled in analyzing web artifacts. The tool also generated comprehensive forensic reports that were easy to understand.
	* ****Limitations:**** However, we did notice some limitations. For instance, the tool struggled a bit with certain file types and very large datasets. These performance issues highlighted potential areas for future improvement. Additionally, while Autopsy is powerful, its efficiency could be enhanced by better integration with other forensic tools.
3. ****Application of Forensic Techniques:****
	* Throughout the project, we applied a variety of forensic techniques within the Autopsy framework. These included timeline analysis, keyword searching, hash analysis, and file carving.
	* We demonstrated how Autopsy can effectively guide investigators through the forensic process, from the initial acquisition of evidence to the final reporting stage.

#### Final Thought

* ****Practical Utility:**** The simulated test cases we developed are incredibly useful for training and education in digital forensics. They offer hands-on experience without the need for real-world data, which is often sensitive and restricted.
* ****Tool Effectiveness:**** Autopsy is a robust tool for digital forensic investigations, offering a wide range of features that meet various forensic needs. The tool's continuous updates and strong community support are significant advantages.

****FUTURE SCOPE/****RECEOMMENDATION****

* + **Tool Enhancements:** ongoing development to address the performance issues we identified, particularly with large datasets and certain file types.
	+ **Integration:** Better integration with other forensic tools and platforms would make Autopsy even more effective.
	+ **Advanced Training Modules:** Developing more advanced training modules that include complex scenarios and the use of additional forensic tools alongside Autopsy would be highly beneficial.

#### Cloud Forensics

As data moves to the cloud, forensic tools will need to handle complex cloud environments efficiently, ensuring data integrity and legal compliance.

#### Blockchain Forensics

Future tools will focus on tracing transactions and identifying fraudulent activities within blockchain networks.

#### Cybersecurity Integration

Digital forensics will integrate more with real-time cybersecurity, enabling immediate analysis during cyber attacks to preserve evidence.

#### Legal and Ethical Considerations

Advancements must ensure privacy and data protection, with clear legal frameworks for the admissibility of digital evidence in court.

**References:**

Autopsy user documentation

<https://www.hackercoolmagazine.com/digital-forensics-with-autopsy-part-1/>

<https://irfaanshakeel.medium.com/how-to-use-autopsy-for-digital-forensics-anal-4ece1ebac5c9>