**BYTEWISE FELLOWSHIP CYBERSECURITY**

**Project Title:**

**Memory Forensics Tools Comparison for Slack and Discord Desktop Applications on Windows OS  
Name: Seerat E Marryum**

**Track Cyber Security**

**Track Lead: Sir Tayyab**

**1. Introduction**

In the realm of digital forensics, memory analysis is an essential process that enables investigators to uncover transient data stored in the volatile memory (RAM) of computers. This data is particularly valuable when examining messaging applications like Slack and Discord, which often contain critical information that can aid in forensic investigations. This project focuses on comparing Autopsy and FTK Imager, two widely used tools in the forensic community, to ascertain their capabilities, identify areas for improvement, and offer insights into their practical applications.

**2. Tools Overview**

**Autopsy**

* **Type:** Forensic Analysis Platform
* **Purpose:** Primarily designed for comprehensive digital investigations, Autopsy analyzes file systems, recovers deleted files, and can be extended with plugins for memory analysis.
* **Key Features:**
  + Open source with an intuitive graphical user interface (GUI).
  + Capable of integrating with memory analysis plugins such as Volatility.
  + Focuses on file system forensics with additional memory artifact analysis capabilities.

**FTK Imager**

* **Type:** Forensic Imaging Tool
* **Purpose:** FTK Imager excels in capturing disk images and live memory for forensic examinations.
* **Key Features:**
  + A free tool with a user-friendly GUI that simplifies the memory acquisition process.
  + Supports the acquisition of live memory from Windows systems without causing disruptions.
  + Outputs memory images in formats suitable for further analysis with forensic tools.

**3. Methodology**

**Step 1: Environment Setup**

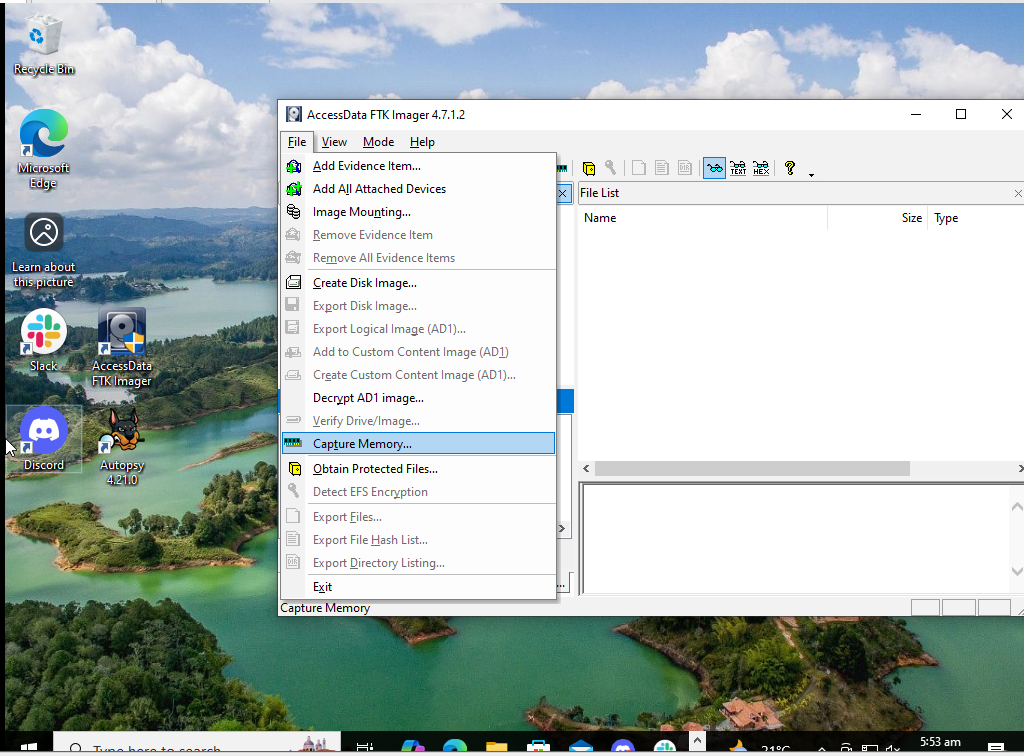
* A Windows system was prepared, with Slack and Discord installed and running.
* Both Autopsy and FTK Imager were installed for use in the project.

**Step 2: Memory Acquisition using FTK Imager**

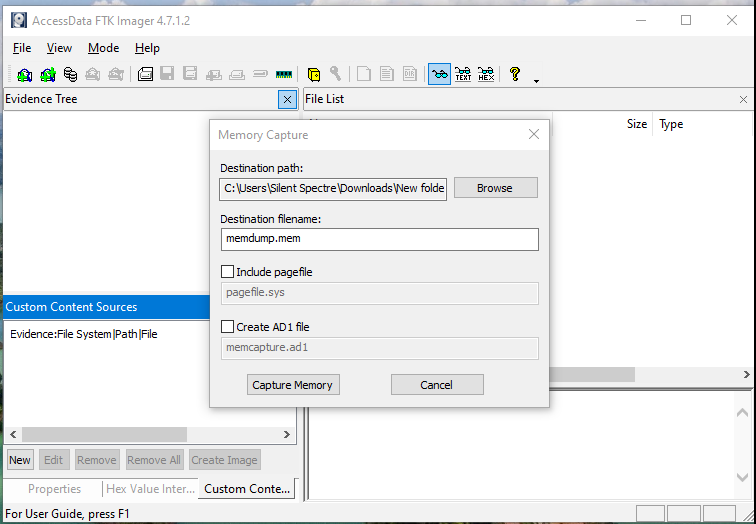
* FTK Imager was utilized to perform a live memory capture of the Windows operating system.
* The acquired memory image was saved in a raw format, ensuring compatibility for subsequent analysis.
* The focus was on obtaining real-time data while the messaging applications were actively in use.

**Step 3: Memory Analysis using Autopsy**

* Autopsy was employed to load and analyze the captured memory image.
* The analysis concentrated on extracting relevant artifacts, such as:
  + Chat histories and user interactions from Slack and Discord.
  + Session tokens and potential credentials stored in memory.

****



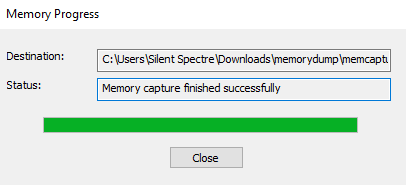
****



**A screenshot of a computer

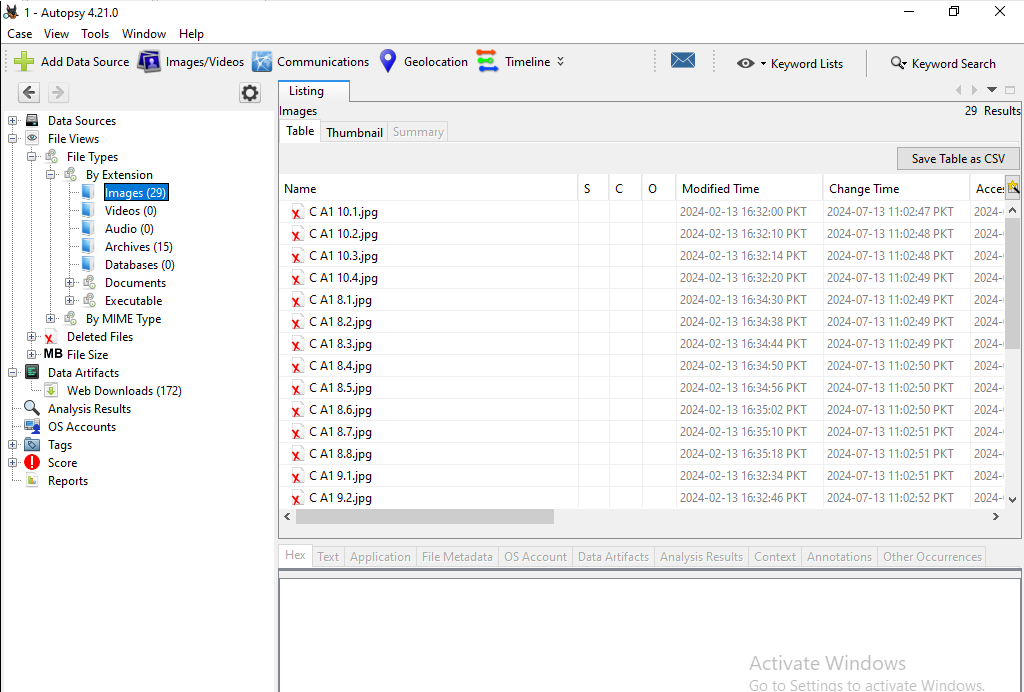
Description automatically generated**



****



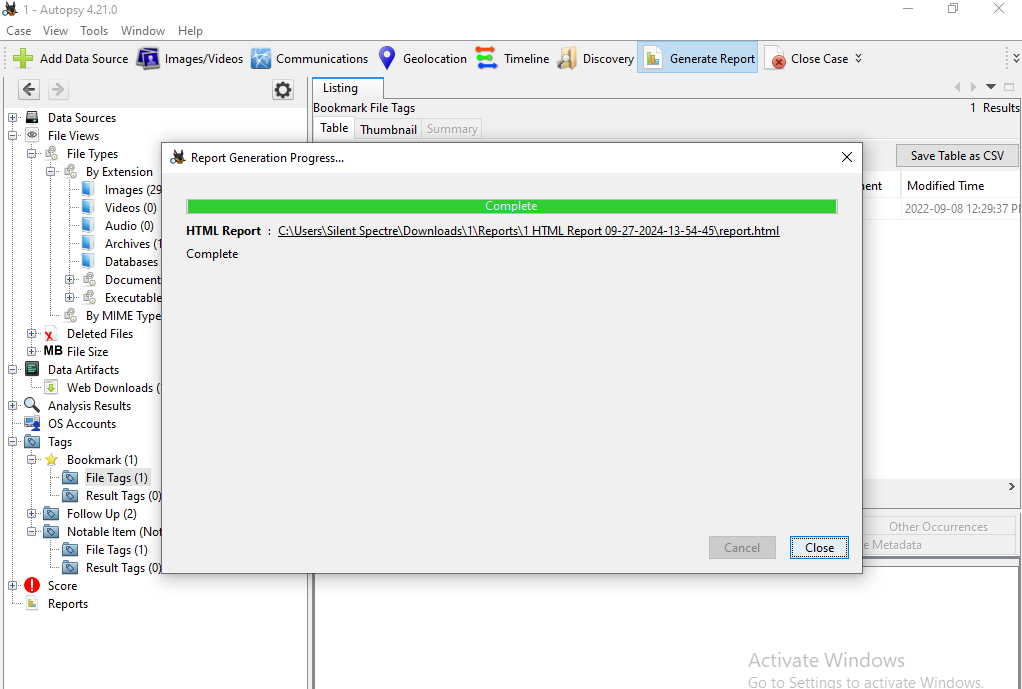
**Analyzing data:**

****

**Generating Report:**

**A screenshot of a computer

Description automatically generated**

****

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Autopsy**

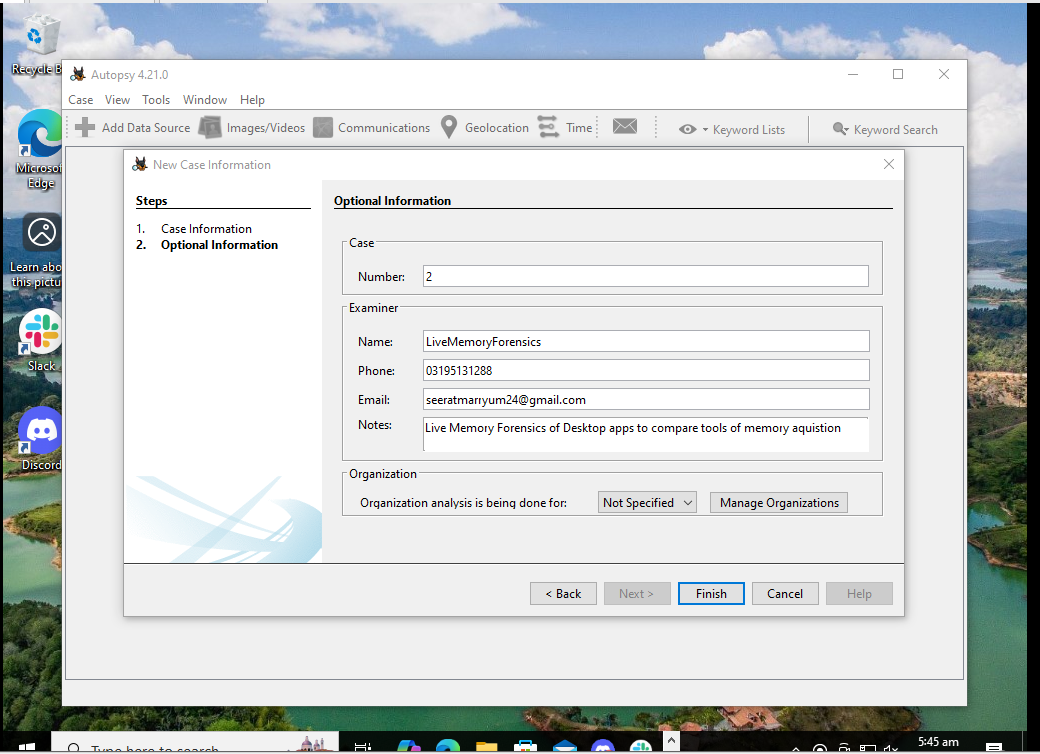
* **Analysis Results**: Autopsy demonstrated its capabilities in analyzing the memory image, identifying artifacts such as user metadata, chat logs, and session details.
* **Integration with Plugins**: By leveraging plugins like Volatility, Autopsy was able to perform deeper memory analysis, though its primary design catered more towards file system investigations.

**Procedure**:

A screenshot of a computer

Description automatically generated







**4. Results**

**FTK Imager**

* **Performance:** FTK Imager effectively captured the live memory, creating a comprehensive raw image without impacting system performance.
* **Artifacts Captured:** The tool successfully retrieved key memory artifacts, including chat histories and session data from the messaging applications.

**Autopsy**

* **Analysis Results:** Autopsy demonstrated its capabilities in analyzing the memory image, identifying artifacts such as user metadata, chat logs, and session details.
* **Integration with Plugins:** By leveraging plugins like Volatility, Autopsy was able to perform deeper memory analysis, though its primary design catered more towards file system investigations.

**5. Comparative Analysis of Tools**

| **Feature** | **FTK Imager** | **Autopsy** |
| --- | --- | --- |
| **Type** | Memory Acquisition Tool | Forensic Analysis Platform |
| **Primary Function** | Live memory and disk imaging | Disk and file system analysis |
| **Memory Acquisition** | Direct from live systems | Relies on external memory acquisition |
| **GUI** | Simple and user-friendly | Advanced interface with multiple tools |
| **Artifact Detection** | Captured relevant data effectively | Effective with additional plugins |
| **Ease of Use** | Straightforward process | More complex, requires configuration |
| **Output Formats** | Supports various formats | Compatible with multiple image formats |

**6. Advantages of Each Tool**

**FTK Imager**

* **User-Centric Design:** The intuitive interface allows users to navigate the tool with ease, even those new to memory forensics.
* **Live Acquisition:** Capable of capturing memory in real-time without disrupting ongoing processes, making it invaluable for volatile data recovery.
* **Format Versatility:** Outputs memory images in formats that are compatible with a wide range of forensic analysis tools.

**Autopsy**

* **Extensibility:** As an open-source tool, Autopsy can be enhanced through plugins, making it adaptable for various forensic tasks.
* **Comprehensive Reporting:** Offers robust reporting features that assist in documenting findings and presenting them effectively to stakeholders.
* **Community Engagement:** Active community support contributes to ongoing enhancements and a wealth of shared knowledge.

**7. Challenges and Limitations**

**FTK Imager**

* **Analysis Limitations:** While FTK Imager excels in acquisition, it lacks robust analysis capabilities, necessitating the use of other tools for deeper investigations.
* **Dependency on Plugins:** The effectiveness of memory analysis may hinge on the proper integration and configuration of external plugins.

**Autopsy**

* **Complex Configuration for Memory Analysis:** Setting up Autopsy for effective memory analysis requires additional plugins, which may complicate the process for new users.
* **Resource Consumption:** The application can be resource-intensive during analysis, which may lead to performance issues on lower-end hardware.
* **Learning Curve:** Users may face a steeper learning curve due to the advanced features and settings available in Autopsy.

**8. Recommendations for Improvement**

**FTK Imager**

* **Enhanced Analysis Features:** Integrate basic forensic analysis capabilities directly into FTK Imager to minimize reliance on additional software for comprehensive investigations.
* **Improved Documentation:** Provide more extensive documentation and tutorials to assist users in leveraging the full potential of the tool.

**Autopsy**

* **Streamlined Memory Acquisition Process:** Develop features that simplify the memory acquisition process, reducing dependency on external tools for capturing live memory.
* **Performance Enhancements:** Focus on optimizing resource usage to improve efficiency during memory analysis, making it more viable for use on less powerful machines.

**9. Conclusion**

In summary, FTK Imager and Autopsy serve distinct yet complementary roles in the domain of memory forensics. FTK Imager stands out for its straightforward memory acquisition capabilities, while Autopsy provides a comprehensive analysis framework. For practitioners in the field, using these tools in tandem can yield valuable insights into memory artifacts from messaging applications, thereby enhancing the effectiveness of digital investigations. Combining the strengths of both tools can create a robust forensic workflow, enabling deeper insights into volatile data captured from messaging applications like Slack and Discord.

**10. References**

* [**Autopsy Documentation**](https://sleuthkit.org/autopsy/docs/user-docs/4.3/)**:** The Sleuth Kit - Autopsy
* [**FTK Imager Documentation**](https://www.exterro.com/uploads/documents/FTK_7.4.2_UG.pdf)**:** AccessData - FTK Imager