**Project Report on Computer RAM Capturing and Analysis**

**Performed By: Dhrumit Asari**

**Under The Guid**

**Date: Jan 28TH,2025 – Jan 30TH,2025**

**1. Introduction**

**1.1 Objective**

This project aims to capture and analyse a computer system's volatile memory (RAM) using forensic tools, namely FTK Imager for acquisition and Autopsy for forensic analysis.

**1.2 Importance of RAM Analysis**

RAM analysis is crucial in digital forensics as it contains valuable information such as:

* Running processes
* Open network connections
* Encryption keys
* Cached files and data
* Malware footprints

**1.3 Tools Used**

* **FTK Imager**: Used for RAM acquisition
* **Autopsy**: Used for forensic analysis of the captured memory

**2. RAM Capturing Using FTK Imager**

**2.1 Installation and Setup**

1. Download and install FTK Imager from the official website.
2. Open FTK Imager with administrator privileges.

**2.2 Capturing RAM**

1. Launch FTK Imager.
2. Click on **"File" → "Capture Memory"**.
3. Select the destination folder for saving the captured RAM image.
4. Enable options to capture the page file and dump compressed memory.
5. Click **"Capture Memory"** and wait for the process to complete.
6. The captured memory file (e.g., memory.dmp) will be saved for further analysis.

**3. Analysis of Captured RAM Using Autopsy**

**3.1 Importing Memory Dump into Autopsy**

1. Open **Autopsy** and create a new case.
2. Select **"Add Data Source"** and choose **"RAM Image"**.
3. Upload the memory dump file captured using FTK Imager.

**3.2 Analyzing the RAM Dump**

1. **Searching for Running Processes:**
   * Identify active processes at the time of capture.
   * Detect suspicious processes linked to malware or unauthorized access.
2. **Extracting Network Connections:**
   * Identify live network sessions and suspicious connections.
3. **Recovering Cached Files & Passwords:**
   * Extract sensitive files and credentials stored in RAM.
4. **Detecting Malicious Activities:**
   * Scan for indicators of compromise (IOCs) like malware footprints, injected DLLs, and suspicious scripts.

**4. Observations and Findings**

**4.1 Key Findings**

* List any unusual or suspicious activities found.
* Highlight extracted artifacts such as passwords, network details, or malware.
* Provide screenshots of important forensic evidence.

**4.2 Challenges Faced**

* Issues in acquiring memory due to antivirus interference.
* Large RAM dump file size affecting processing speed.
* Difficulty in interpreting raw memory structures.

**5. Conclusion and Recommendations**

**5.1 Summary**

This project successfully demonstrated RAM acquisition using FTK Imager and its forensic analysis using Autopsy. The captured memory contained valuable artifacts like running processes, network connections, and potential security threats.

**5.2 Recommendations**

* Use volatile memory analysis in incident response scenarios.
* Employ advanced forensic tools like Volatility for deeper analysis.
* Automate RAM forensics using scripts for efficiency.
* Regularly update forensic tools to stay ahead of evolving cyber threats.

**6. References**

1. FTK Imager User Guide – AccessData
2. Autopsy Forensic Suite Documentation
3. Digital Forensic Analysis Techniques and Best Practices
4. Video References:
   * [RAM Capturing and Analysis Tutorial 1](https://youtu.be/Qi5yLXC0v54)
   * [RAM Capturing and Analysis Tutorial 2](https://youtu.be/Fw9lF5eLjlM)

**Prepared by:**  
**Dhrumit Asari**  
MSc Cyber Forensics, NFSU Gandhinagar