**Acquire and Analyze the volatile data of RAM**

**Name:** Shivam Verma **Roll No.**: 47

**Reg. No:** 11905604 **Section:** KE016

1. **Introduction**
   1. **Objective of project**

Capturing and analyzing volatile data in RAM (random access memory) is important for digital forensics and incident response investigations. RAM is volatile memory, which means that its contents are lost when the computer is

turned off or restarted.

Therefore, capturing and analyzing volatile data in RAM allows investigators to capture valuable information that can be lost when a computer is shut down or restarted. This information can include running processes, network connections, open files, and other system activity that can provide valuable

Clues about what is happening on your system.

Additionally, volatile data in RAM may contain sensitive information such as login credentials, encryption keys, and other data that may be useful for investigations. In general, capturing and analyzing volatile data in RAM is an important step in a forensic investigation, as it can provide valuable information that might otherwise not be available, such as by examining a hard drive.

* 1. **Description of the project**

The acquisition and analysisof volatile RAM (Random Access Memory) data is an important aspect of digital forensics. Volatile data **is** information stored in a computer's RAM that is lost when the computer is turned off or restarted. This data can include running processes, network connections, open files, and other system information that can be crucial in a forensic investigation.  
  
Obtaining volatile data involves taking a snapshot of the current state of RAM. This can be done using a variety of tools and techniques, including:

**Live Scanning:** In this approach,a forensic analyst accesses a running

system and retrieves volatile data in real time. This can be done using the tools such as task manager or process explorer on window or top or ps on Linux.

**Memory Dump:** This involves creating a copy of the contentsof RAM and saving it to a file for later analysis. This can be done using specialized tools like

FTK Imager or WinHex.

Once the volatile data has been obtained**,** the next step is to analyze it for evidence of malicious activity or other relevant information. This may include checking running processes, network connections, open files, and other system information to identify any unusual or suspicious activity.  
Some common analysis techniques used in volatile data analysis include:  
  
**Timeline** **analysis**: This involves creating a timeline of events from volatile data

To identify patterns or anomalies.

**Memory** **Forensics:** This involves the analysisof memory dump files to identify specific artifacts, such as malicious code or network connections.  
  
**Pattern** **Matching:** This involves comparing volatile data **to** known patterns of

malicious activity to identify any matches.

Obtaining and analyzing volatile data from RAM ingeneral is an important part

of digital forensics and can provide valuable information for forensic investigations.

**1.3 Scope of the project:**

1. **Cybercrime Investigation:**

Cybercriminals often use techniques such as malware, rootkits and others advanced persistent threats to carry out their activities. Hidden in system volatile memory. Capturing and analyzing volatile memory. Capturing and analyzing volatile data in RAM can help investigators identify such activity and determine the extent of damage caused.

1. **Incident Response:**

During a cyber incident, capturing and analyzing volatile data in RAM can help investigators determine the scope and severity of the attack and take appropriate measures to contain the incident and prevent further damage.

1. **Recovery of Lost Data:**

The acquisition and analysis of volatile data in RAM can help to recover the lost data. For example if a user close the window without saved the document we can restored that documents.

1. **Identification of Malware:**

If a malware is not in hardware still it can be detected in volatile memory. The acquisition and analysis of volatile data in RAM can help identify such malwares.

1. **System Description:**
   1. **Target System Description:**
2. **Acquisition device:** A device capable of capturing volatile data from the target system’s RAM. It can be a hardware device such as a memory-gathering tool or a software tool that can create a memory dump.
3. **Target System Information:** Details about the target system, such as operating system, processor type, and memory type. This information helps determine the appropriate collection tools and methods.
4. **Get Method:** The method used to obtain volatile data from the target system’s RAM. This can be done using a variety of techniques, such as live analysis or creating memory dumps.
5. **Analysis Tools:** Tools for analysis of acquired volatile data. These can include instruments such as Volatility, Rekall and Redline.
6. **Storage Media:** A storage medium that stores acquired volatile data. It can be a hard disk or a USB flash drive.
7. **Chain of custody:** A written record of data ownership to ensure its integrity is maintained.
8. **Reporting:** Documentation and reporting of analysis results, including any conclusions drawn from unstable data.
9. **Compliance Requirements:** Any regulatory or legal requirements to retrieve and analyze volatile RAM data, such as privacy or security regulations.

* 1. **Assumptions and Dependencies:**

**Assumptions:**

1. The system is still running and operational.
2. The data in the RAM has not been tampered with or modified.
3. The acquisition tool and method used are appropriate for the system’s hardware and operating system.
4. The analysis tools used are capable of detecting any relevant information in the volatile data.
5. The analysts performing the analysis have the necessary skills and expertise to interpret the volatile data accurately.

**Dependencies:**

1. The acquisition and analysis process may be affected by the system’s CPU speed, available memory, and other system resources.
2. The volatility of the data may change depending on the activity on the system.
3. The quality of the analysis may be dependent on the quality of the acquired volatile data.
4. The analysis may depend on the specific context and understanding of the system under investigation, such as software installed or user behavior.
5. Legal and regulatory requirements may impact the acquisition and analysis process.
   1. **Functional and Non-Functional dependencies:**

**Functional Dependencies:**

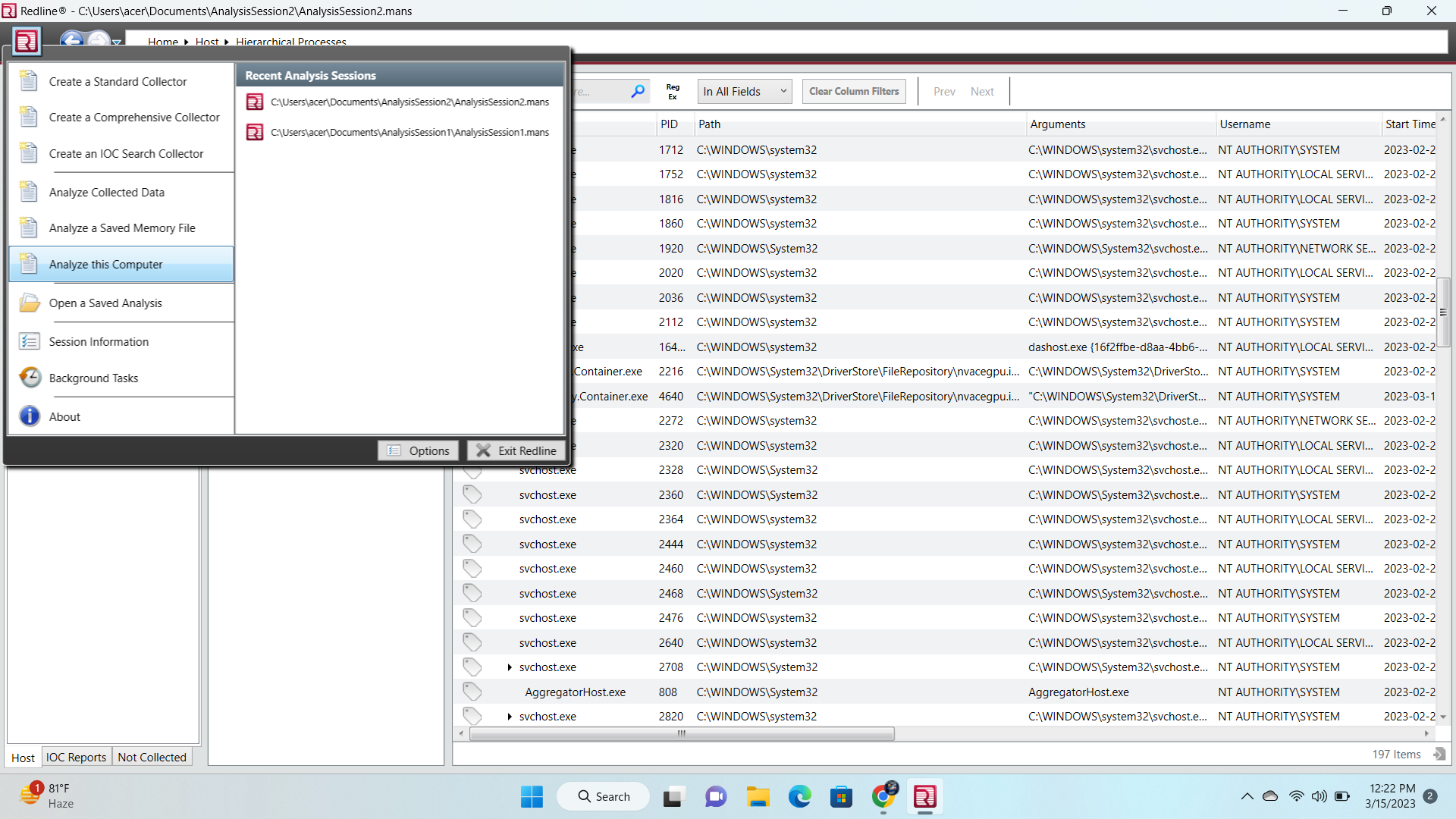
1. **Ability to access and extract data from RAM:**

The methods and tools used to retrieve volatile data from RAMshould be able to access and extract all relevant data stored in RAM.

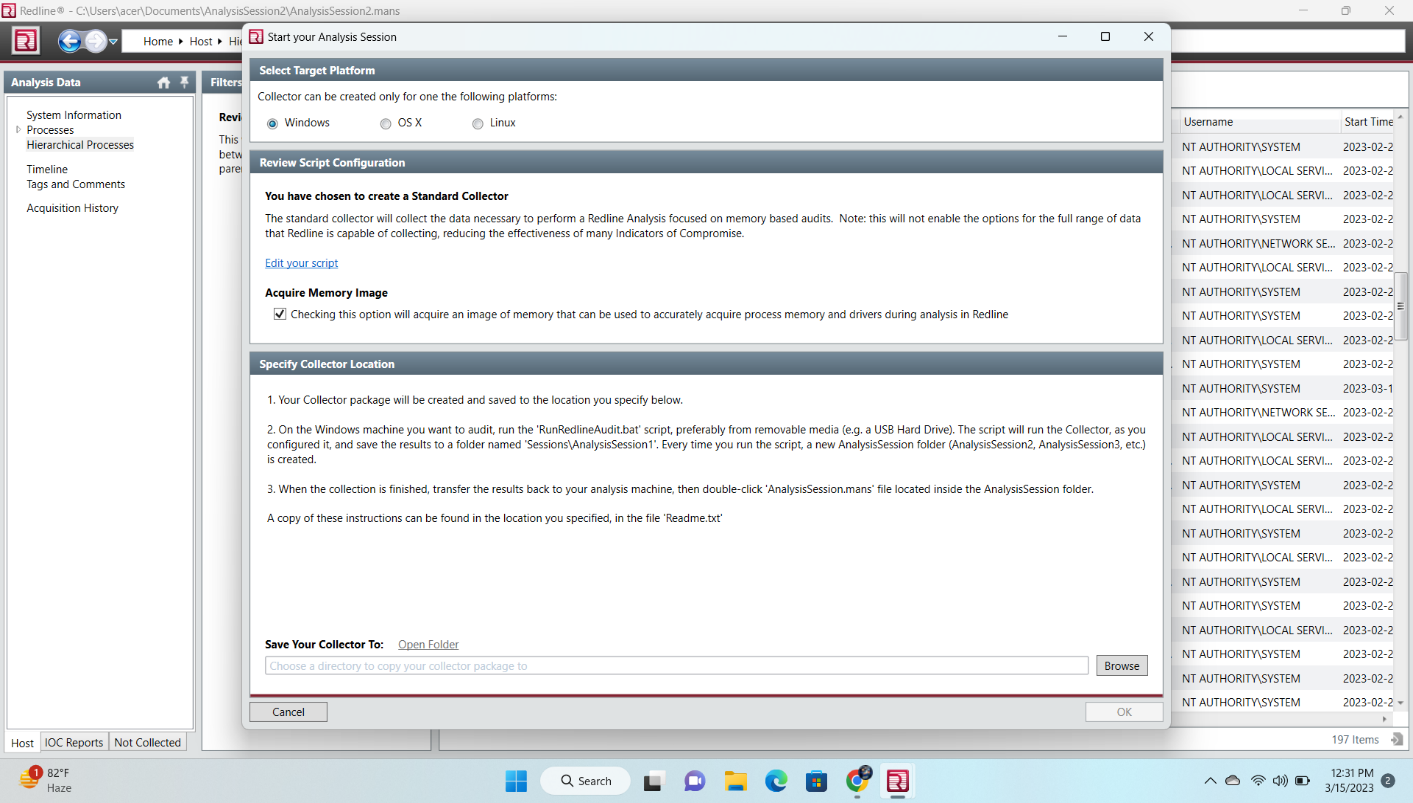
1. **Data Preservation:** To enable correct analysis, data obtained from RAM should be preserved in a way that maintains its integrity.
2. **Data Analysis:** The methods and tools used to evaluate the volatile data should be able to locate essential details such as running programs, network connections, and user activity.

**Non-Functional Dependencies:**

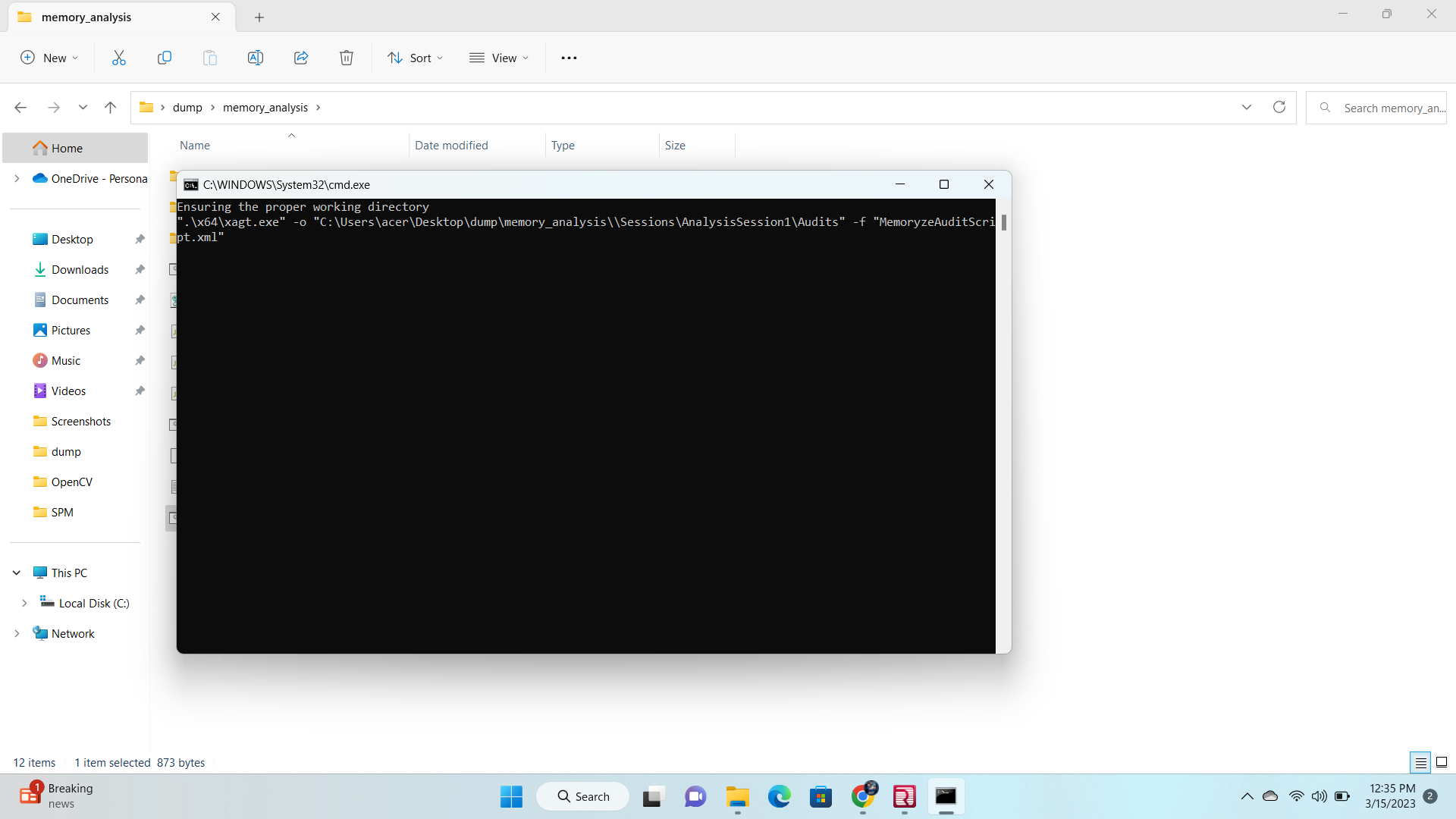
1. **Speed and efficiency:** Acquiring and analyzing volatile data from RAM needs to be done quickly and efficiently to minimize the risk of data loss.
2. **Accuracy and completeness:** The tools and techniques used to acquire and analyze the data should be accurate and complete, to ensure that all relevant information is captured and analyzed.
3. **Reliability and robustness:** The tools and techniques used to acquire and analyze the data should be reliable and robust, to minimize the risk of errors or failures.
4. **Compatibility and interoperability:** The tools and techniques used to acquire and analyze the data should be compatible with a variety of hardware and software configurations, and should be able to work seamlessly with other forensic tools and processes.
5. **Analysis Report:**
   1. **Steps for Acquire and Analysis volatile data of RAM in a machine:**

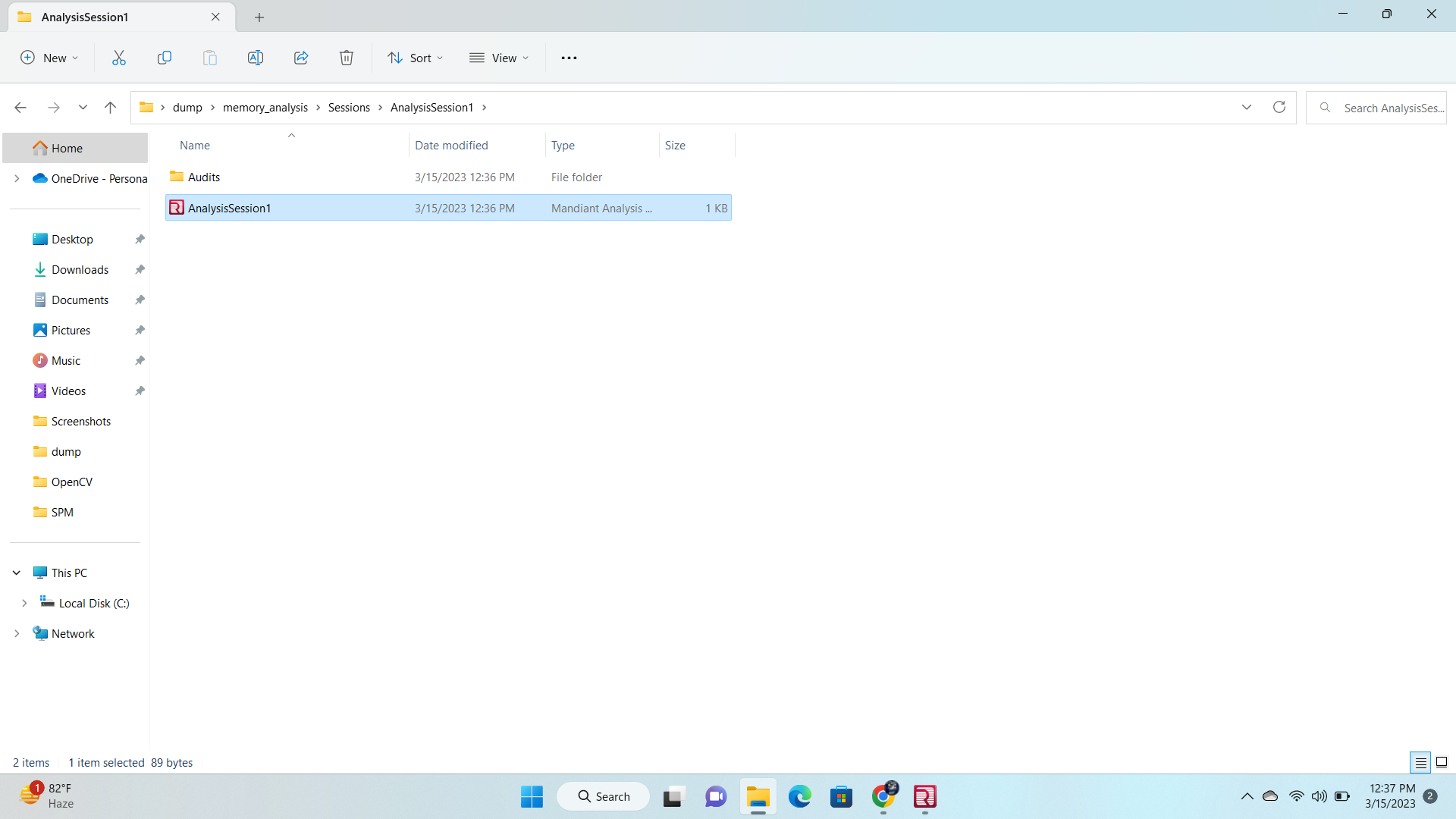
**Acquire memory Image file:**

**Creating Memory File:**



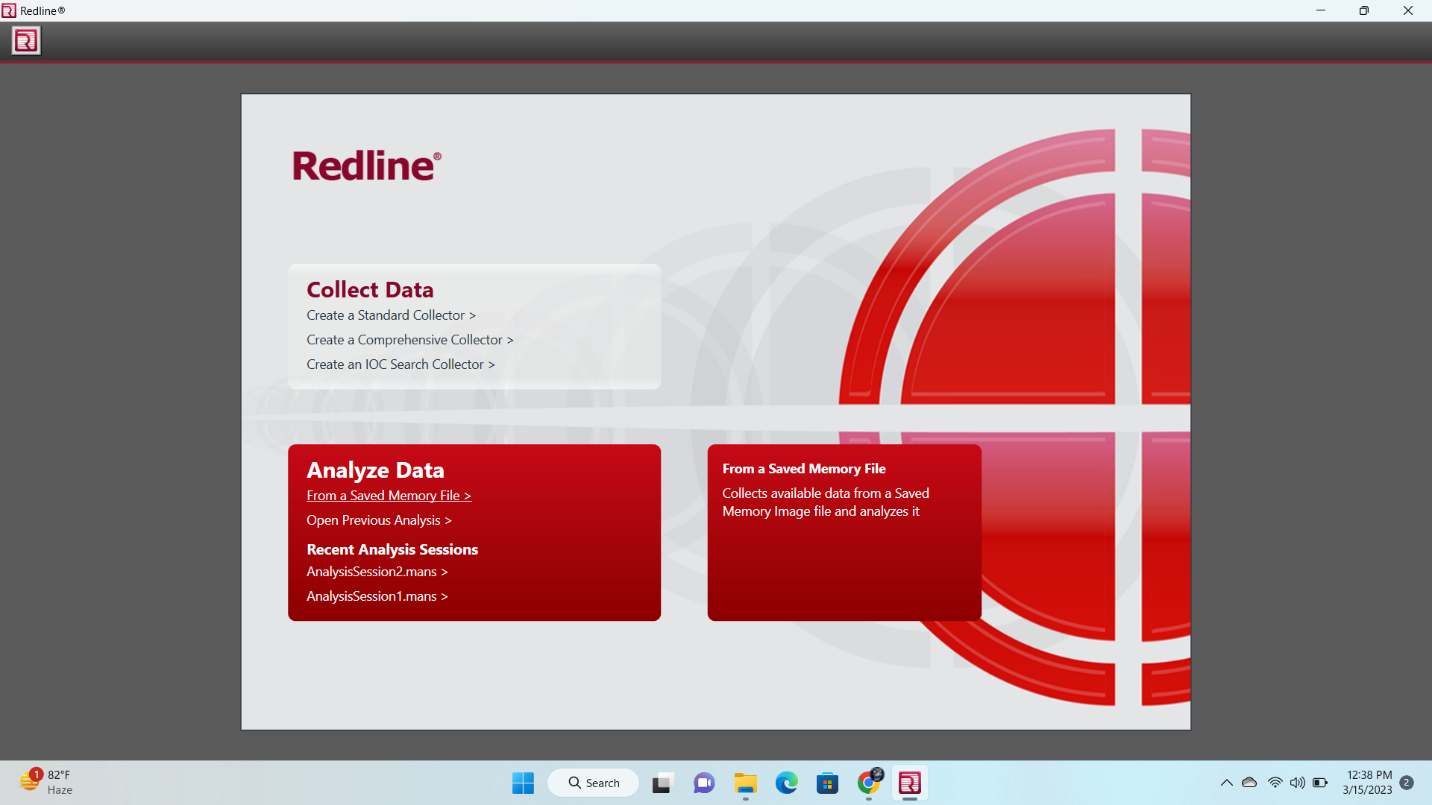
**Memory Analysis file created:**



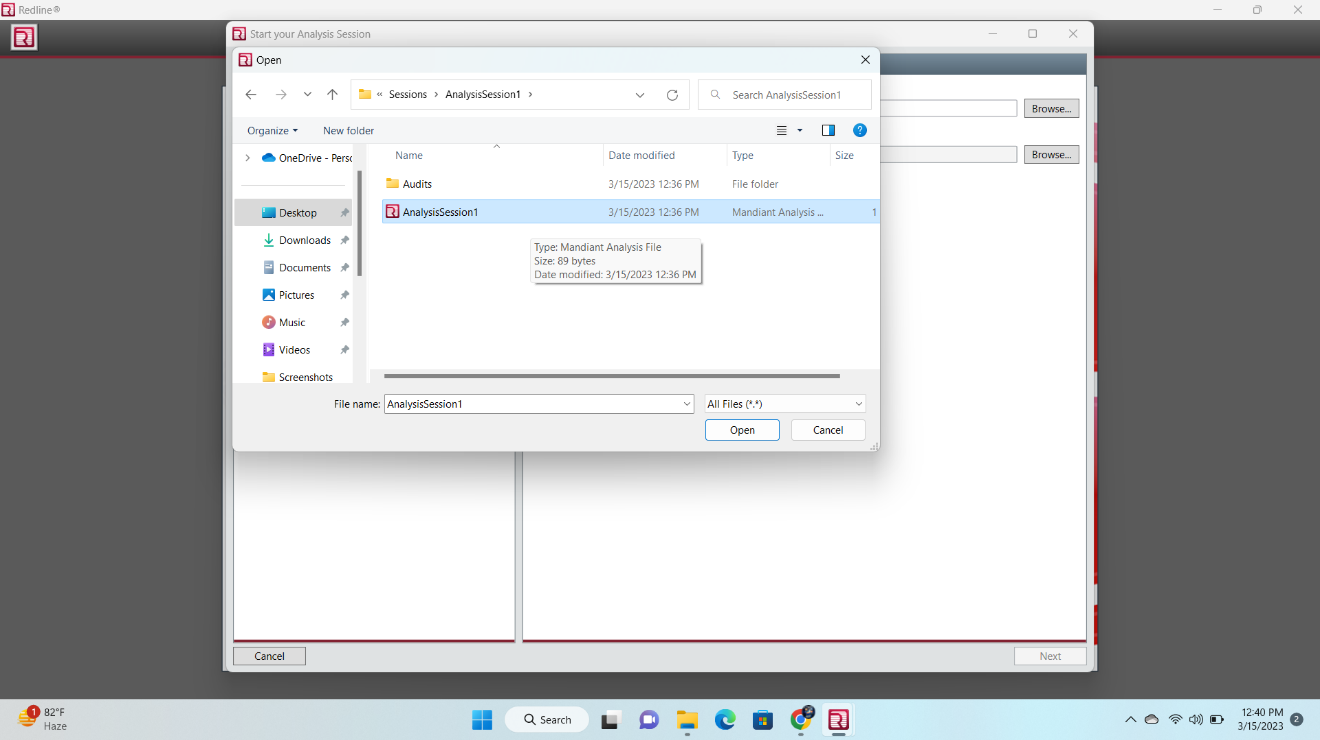
****

**Analyzing Memory File Using Redline Tool:**

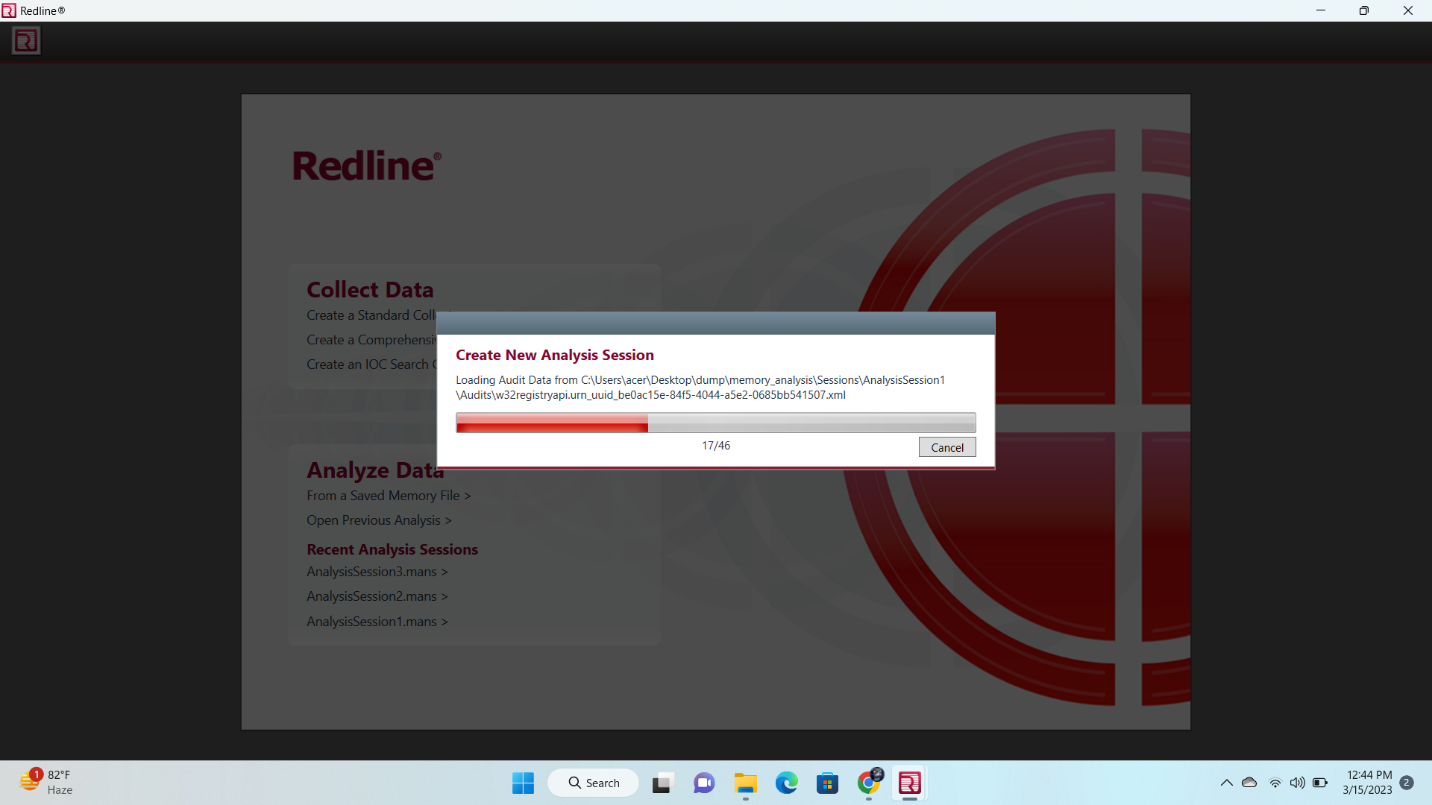
**Click on from a send memory file option:**

****

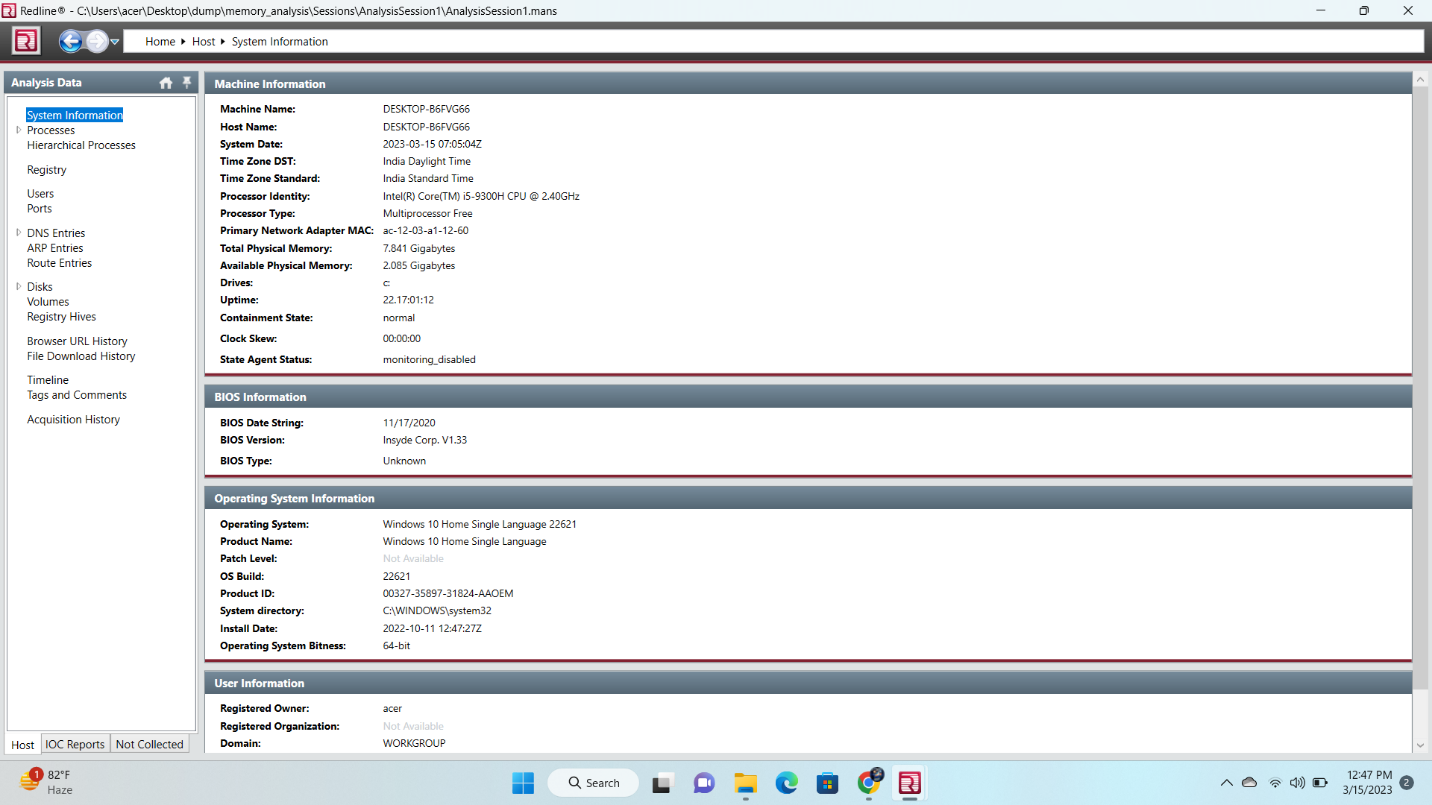
**Select the memory file from folder:**

****

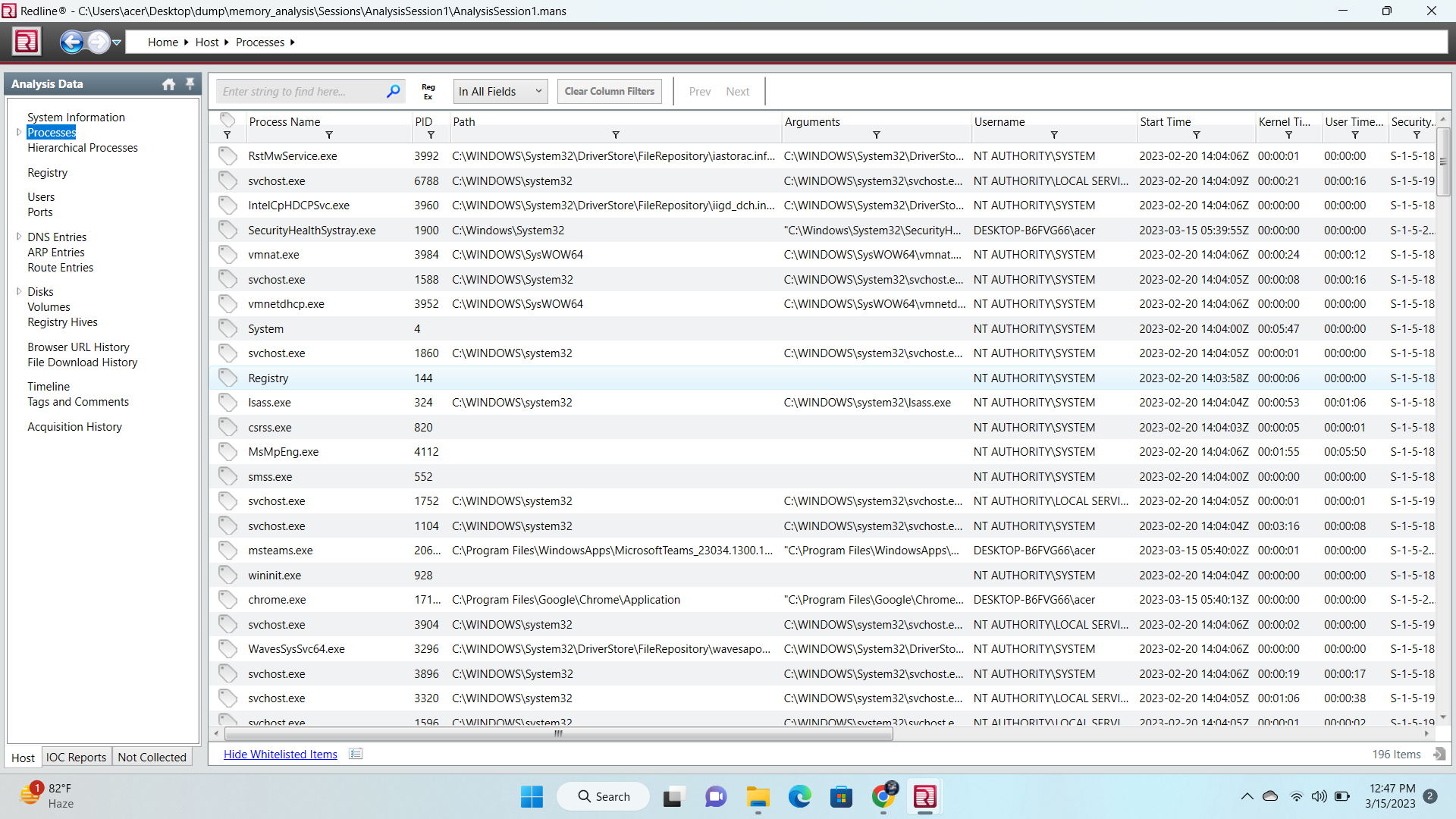
**Analyzing Data:**

****

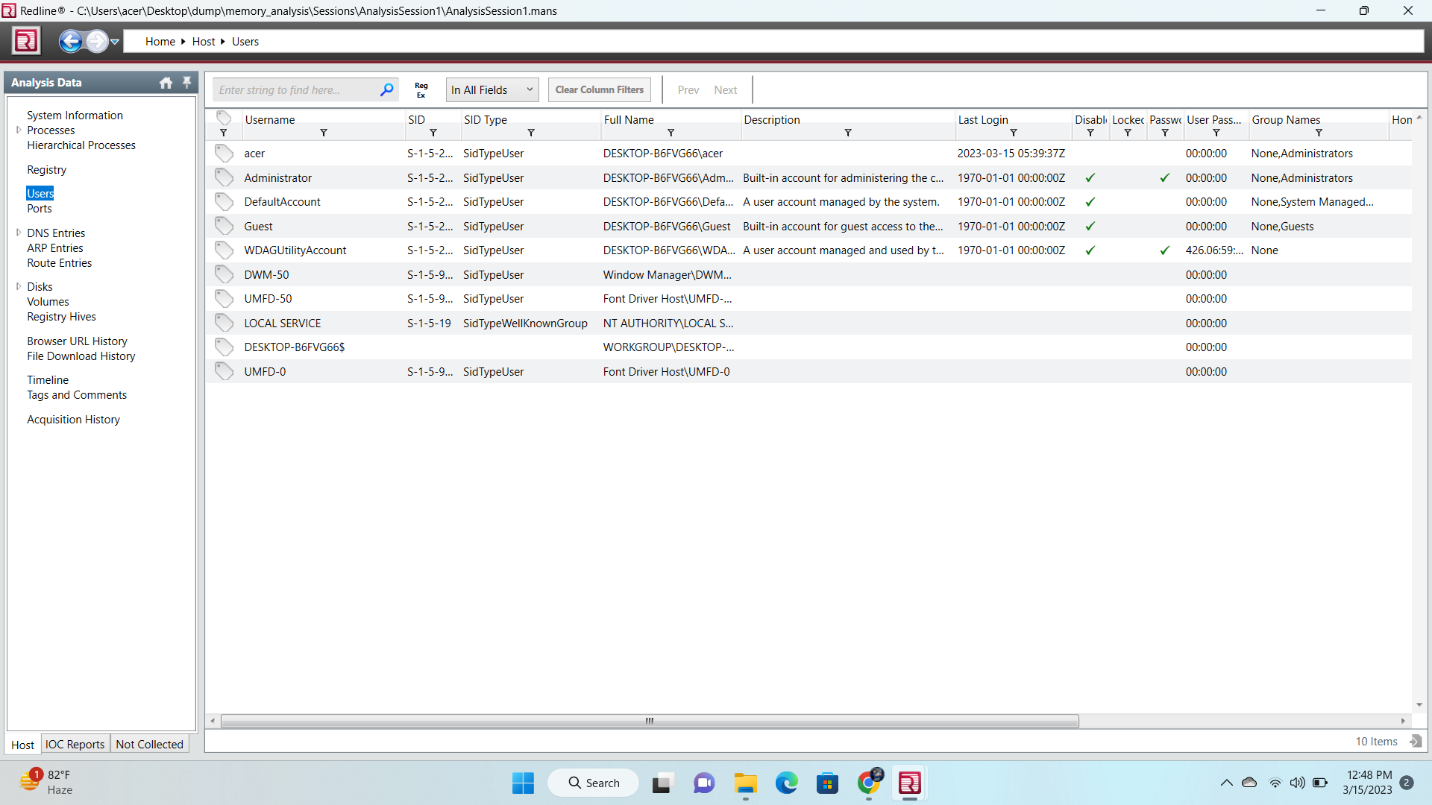
**System Information:**

****

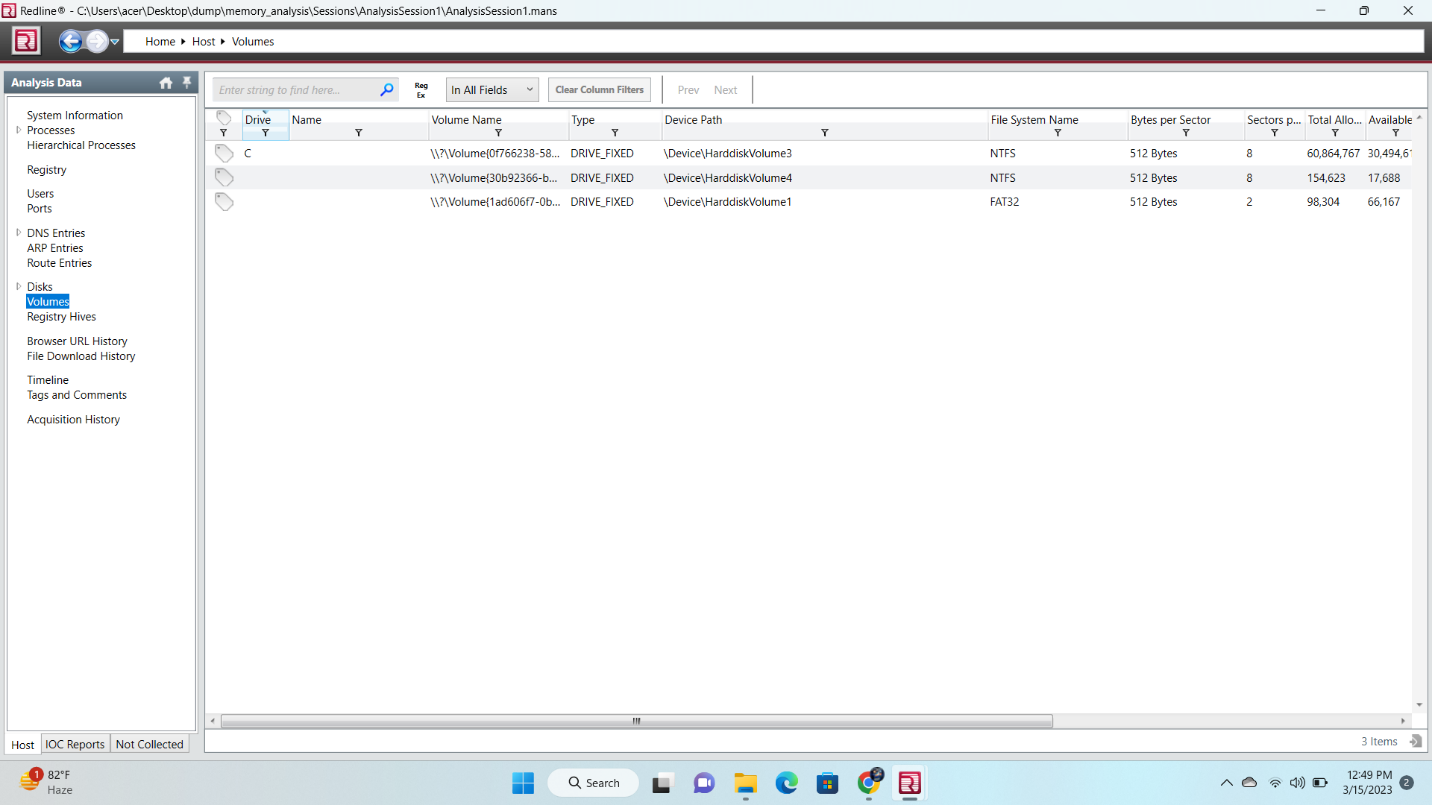
**Process Details:**

****

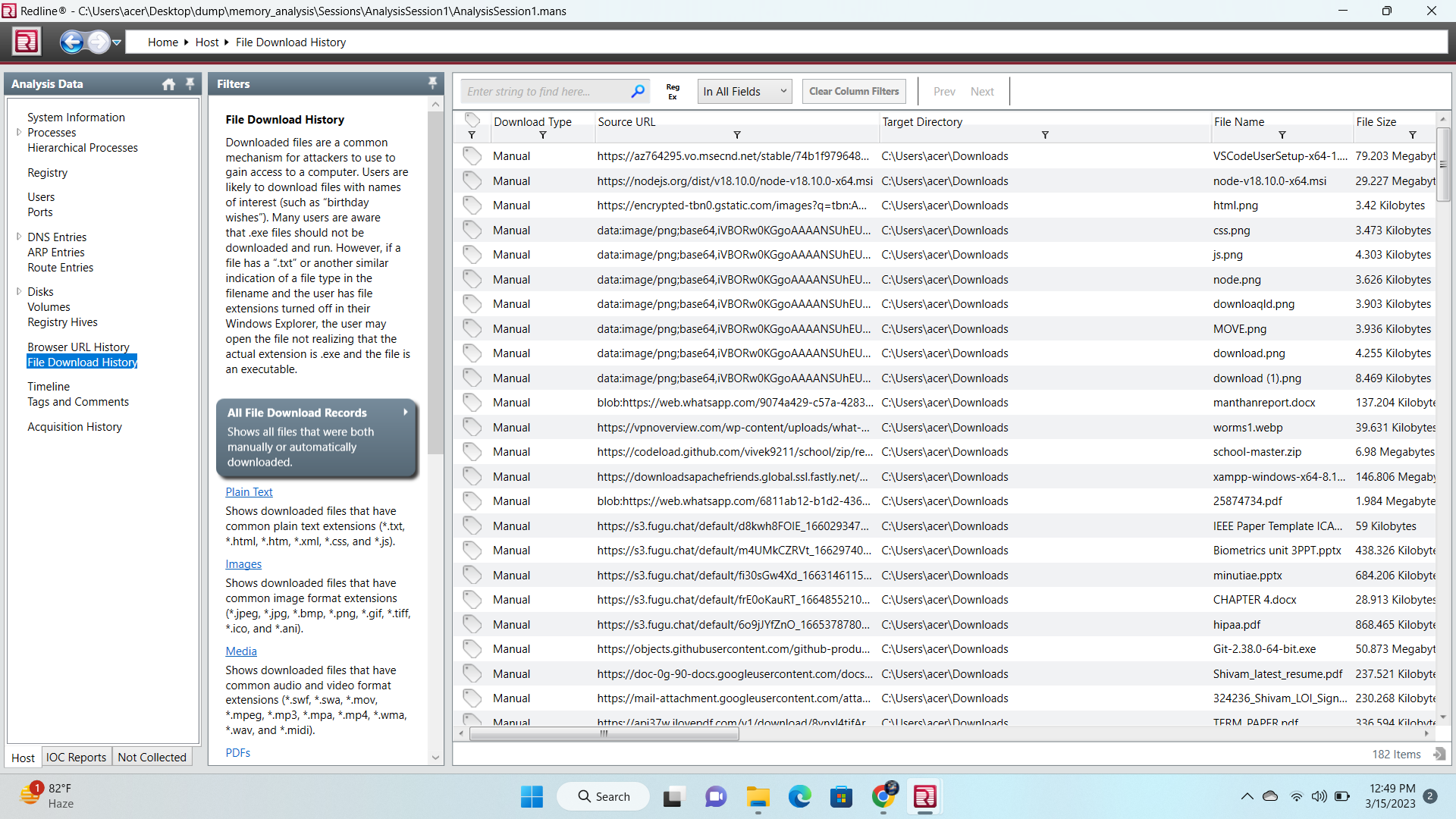
**Users Details:**

****

**Volume Details:**

****

**Download History Details:**

****

1. **References**
2. Burdach, M. (2005, July 9). An Introduction to Windows memory

forensic. Retrieved October 25, 2008, from <http://forensic.seccure.net/>

1. Guidance Software. (2008). Computer Forensics. Retrieved March 3, 2009, from <http://www.guidancesoftware.com/>
2. <https://fireeye.market.com>