**Name – Shubham Verma**

**Roll no. – 14**

**Reg no – 11905678**

**Section – KE016**

**Project – Investigate malicious activity in redline tool**

1. **Introduction**

**1.1 Objective**

By installing RedLine, security teams can conduct memory and file analysis to identify signs of malicious activity, such as file tampering, unauthorized access, privilege escalation, and other indicators of compromise. RedLine provides deep visibility into the system's memory and file system, allowing security teams to quickly identify anomalous activity and respond to it in real-time.

**1.2 Description**

Memory analysis is a valuable malware detection approach since many advanced threats only exist in memory and leave no traces on disc. Memory analysis is used by Redline to identify operating processes, loaded modules, open handles, and network connections. This information can be used by analysts to identify unusual behaviour, such as programmes that have no corresponding executable, processes that use suspect network connections, or processes that are put into memory from non-standard places.

Another key tool for detecting malicious activity is file analysis. Redline can execute file analysis on a system to identify newly produced, updated, or deleted files. Analysts can utilise this data to identify suspicious files, such as executables created in a temporary location or files changed to incorporate malicious code.

**1.3 Scope**

The scope of investigating signs of malicious activity through memory and file analysis by Redline tool can vary depending on the specific needs and requirements of the investigation. However, in general, Redline can be used to investigate a wide range of security incidents and threats on Windows systems, including:

1. Infections caused by malware: Redline can be used to detect indicators of compromise (IOCs) linked with known malware families, such as file hashes, network connections, and process names.
2. Advanced persistent threats (APTs): Redline is especially good at detecting APTs that only exist in memory, such as fileless malware and rootkits. It can also detect network connections to APT command-and-control servers.
3. Insider risks: By examining file and process activity on a system, Redline can be used to analyse potential insider threats. It can detect suspicious files created or updated by a user, as well as processes initiated by a user account but not normally linked with that account.

Overall, the scope of investigating signs of malicious activity through memory and file analysis by Redline tool is quite broad, as it can be used to investigate a wide range of security incidents and threats on Windows systems. By leveraging memory and file analysis, Redline provides valuable insights into the behavior of a system and can help security analysts identify potential security incidents and respond to them quickly and effectively.

1. **System Description**

**2.1 Target system description**

It is a windows-based system which is saved vulnerable to attack. Redline tool can be installed on the target system itself or a separate system that has to the target system’s memory and file artifacts.The tool can collect data from the target system, including memory dumps, process information, file information, and network connection information.

In addition to examining compromised systems, Redline can be used to proactively detect vulnerabilities and potential security threats on Windows-based systems. This can assist firms in taking proactive steps to secure their systems and avoid potential security problems from occurring.

In summary, The utility can be installed on the target system or on a separate system with memory and file artifact access to the target system. It is critical for effective inquiry to have a good understanding of the target system's design and usual behaviour.

**2.2 Assumption and Dependencies**

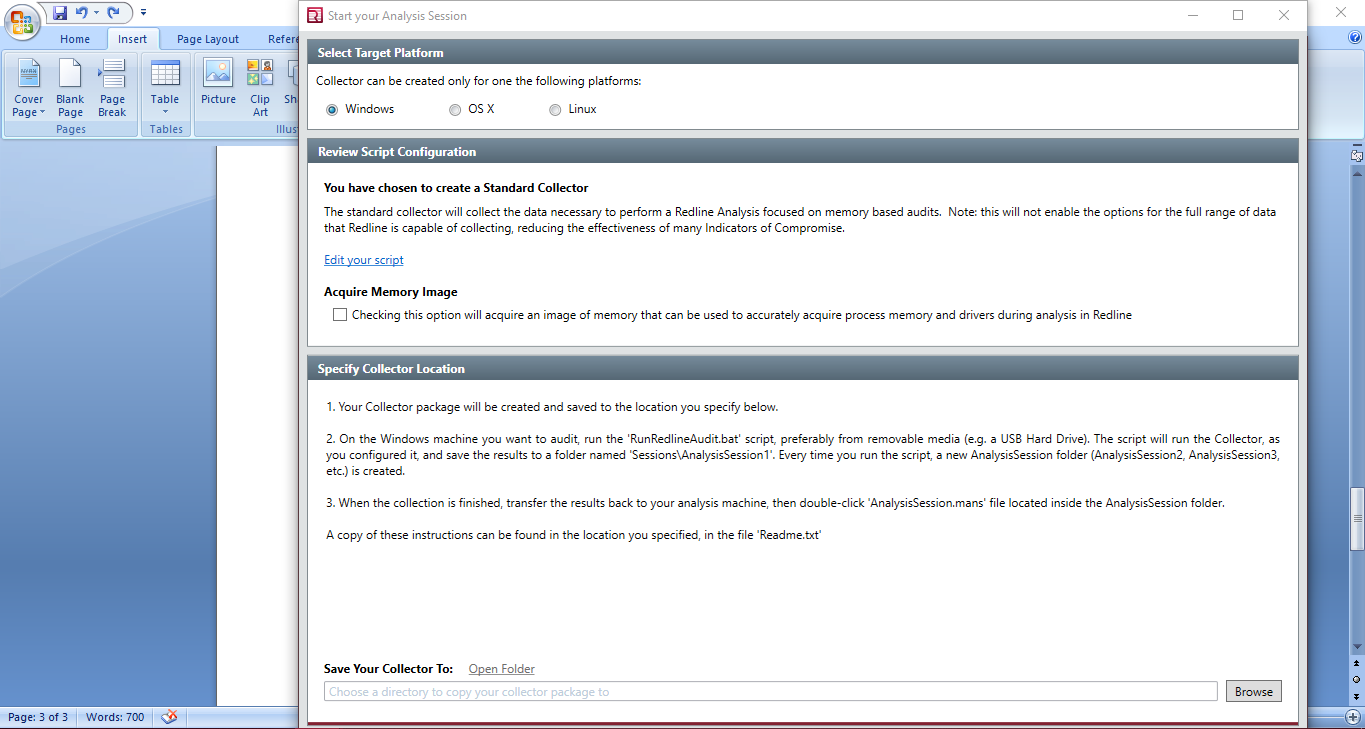
1. The investigation assumes that the Redline tool is an effective tool for evaluating memory and file artefacts associated with malicious activity. This means that the tool can detect symptoms of compromise as well as provide useful analysis and interpretation of the data it collects.
2. Dependence on the Redline tool: The investigation relies on the Redline tool to perform memory and file analysis. The utility may have restrictions, such as only analysing Windows systems or having problems with particular types of malware.
3. External Dependencies: The investigation may also depend on external factors, such as the availability of threat intelligence feeds or access to a sandbox environment for testing malware samples. These dependencies may impact the effectiveness of the investigation and the accuracy of the results obtained using Redline tool.
4. **Analysis Report**

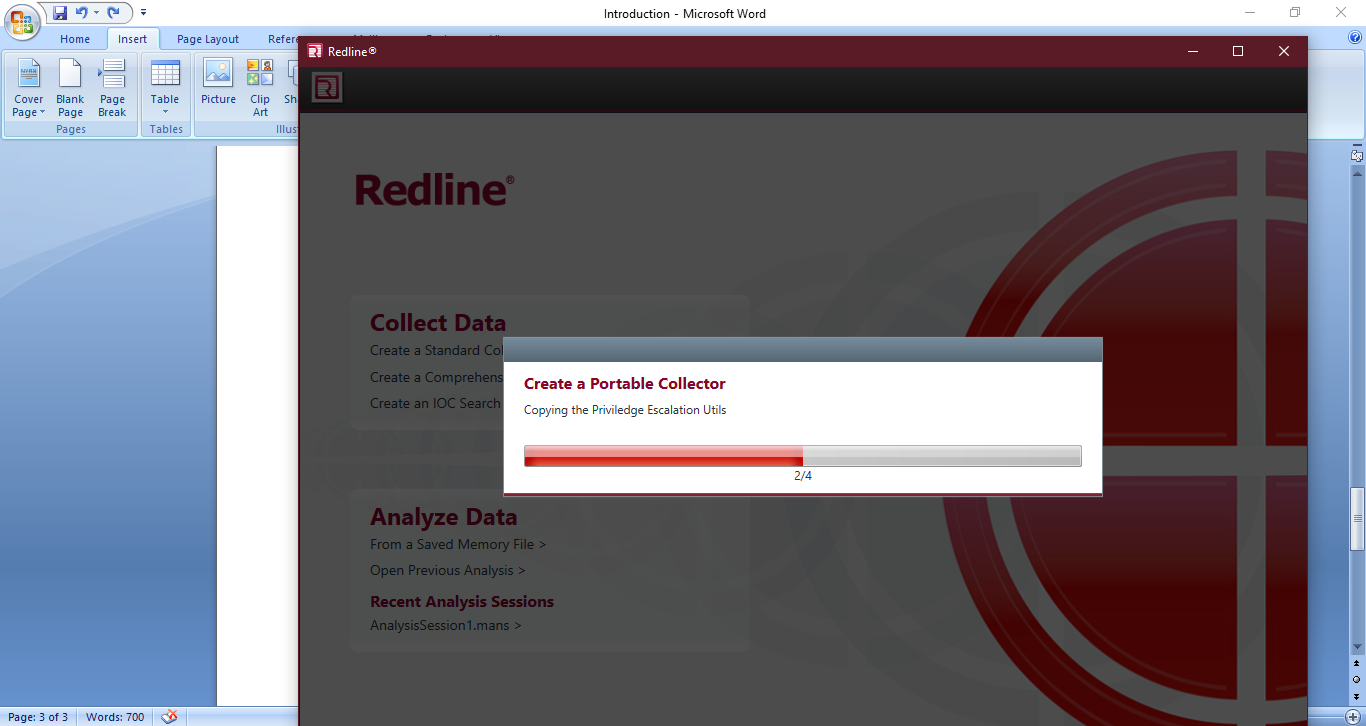
**Step 1.** First I downloaded redline tool.

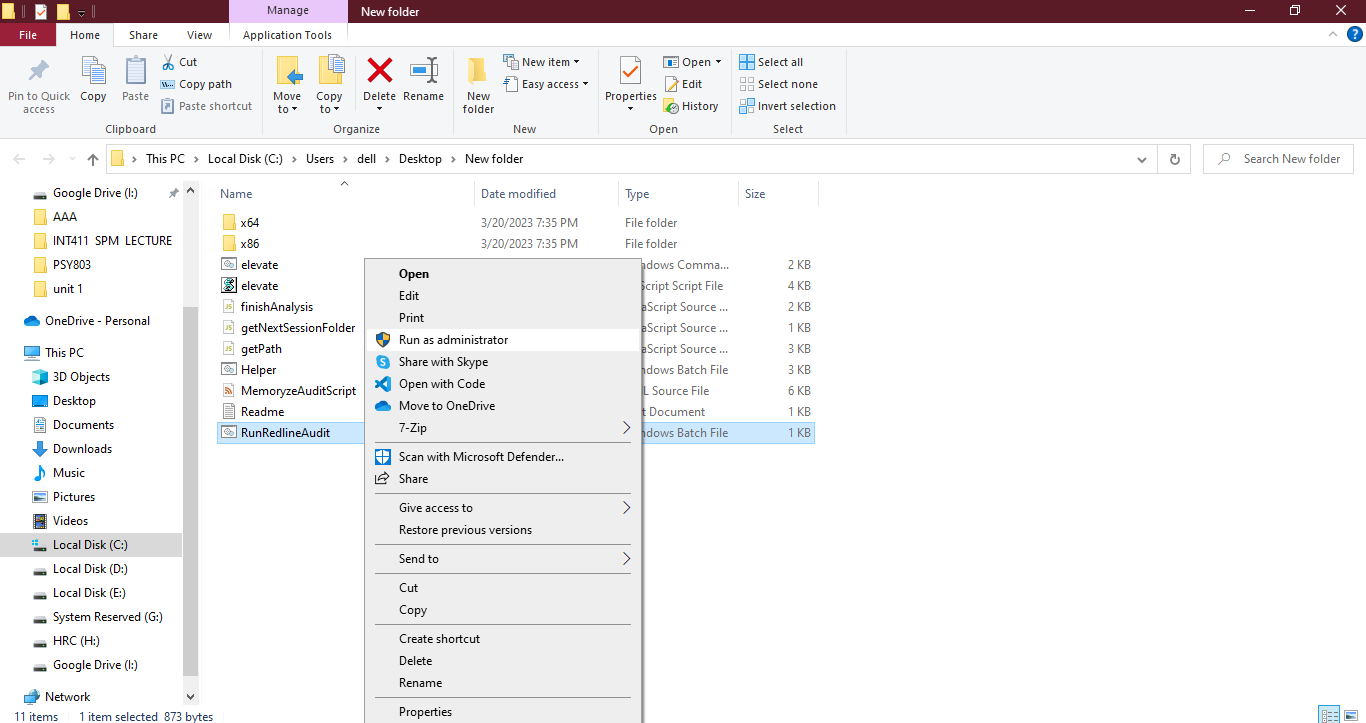
**Step 2.** Create a empty folder.

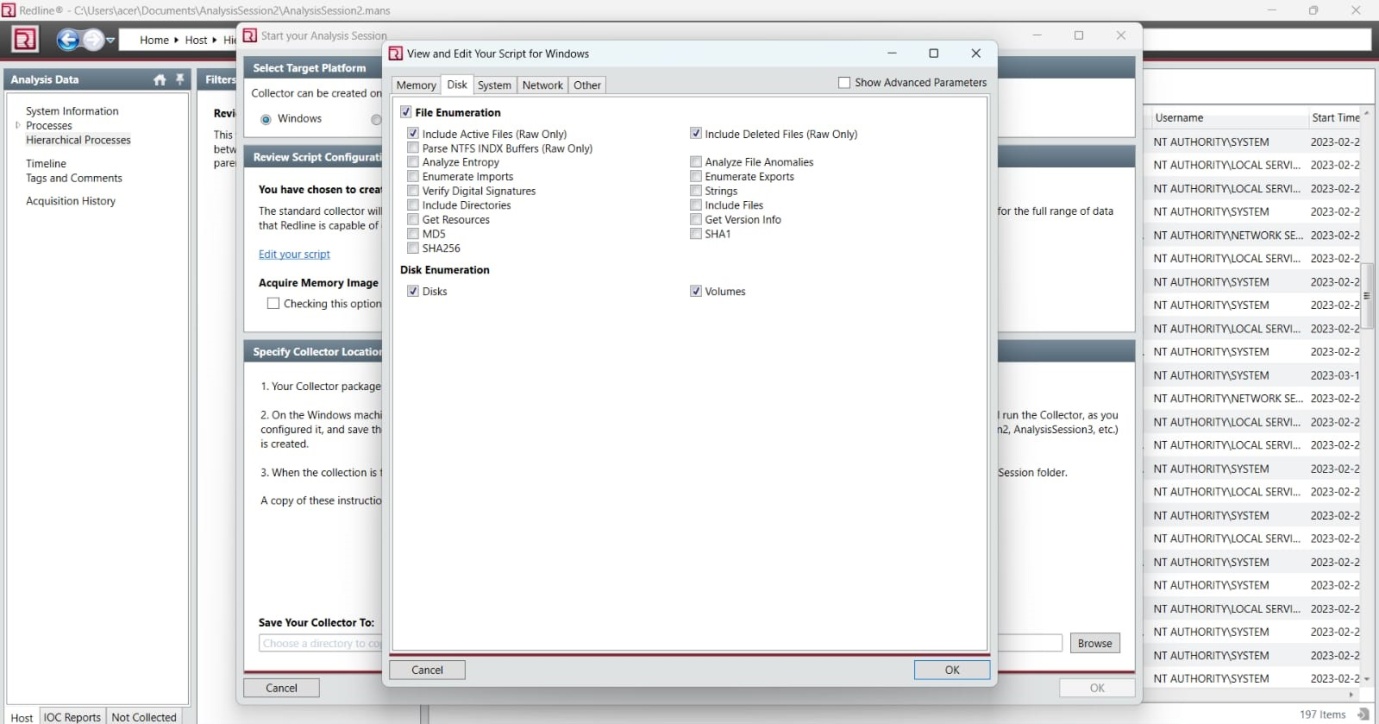
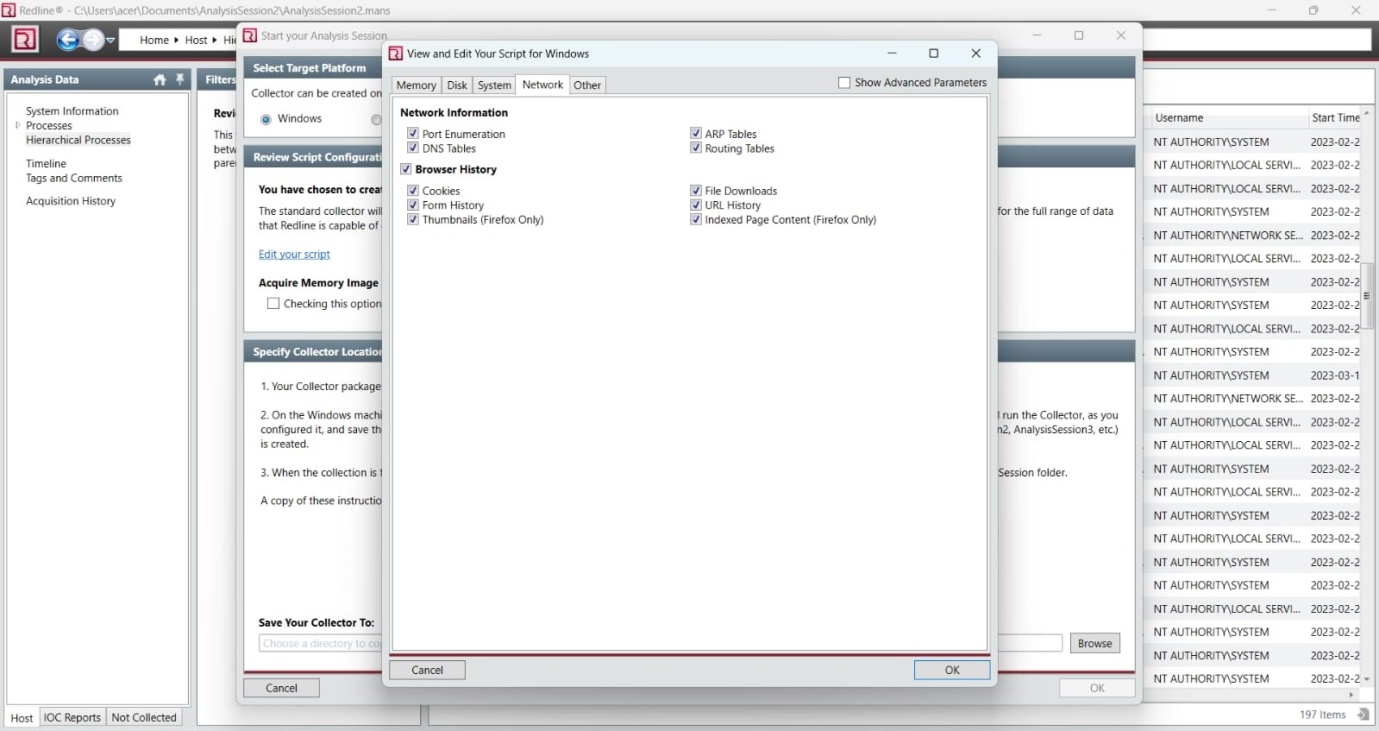
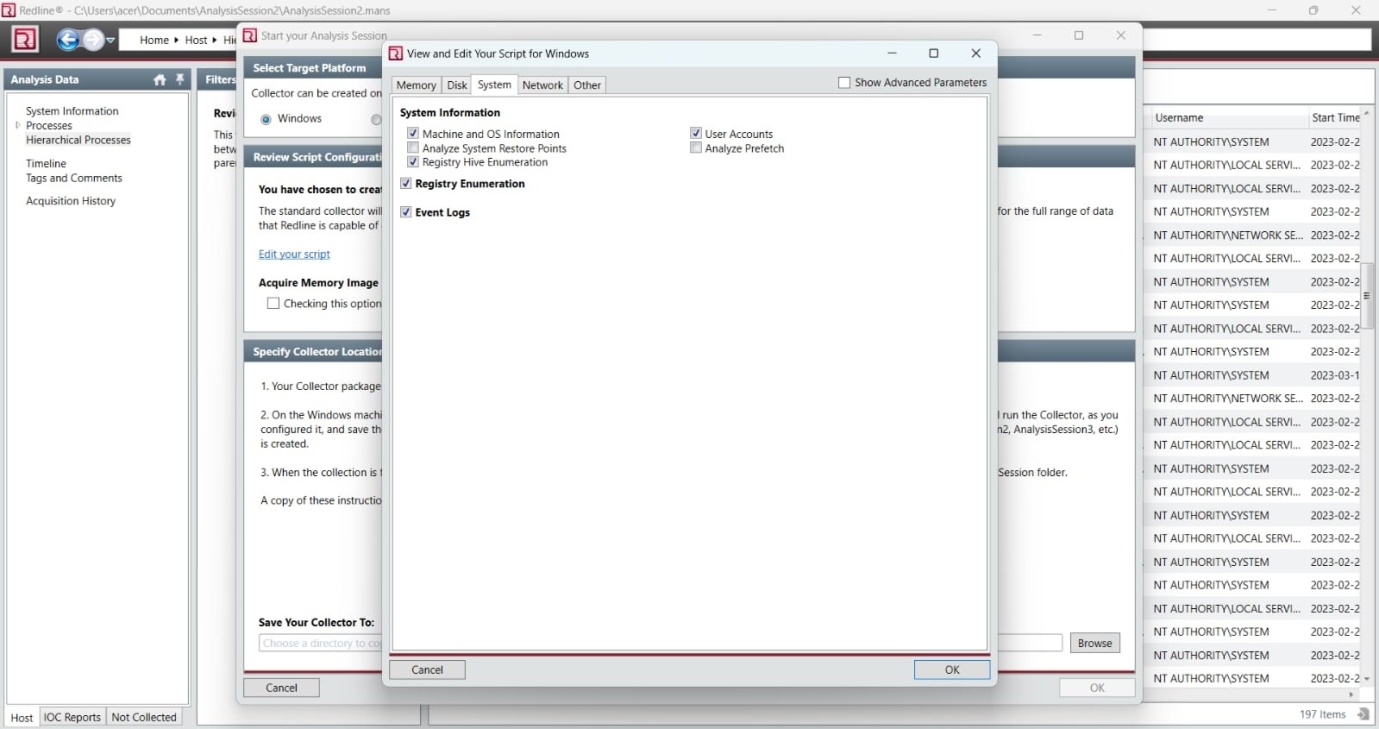
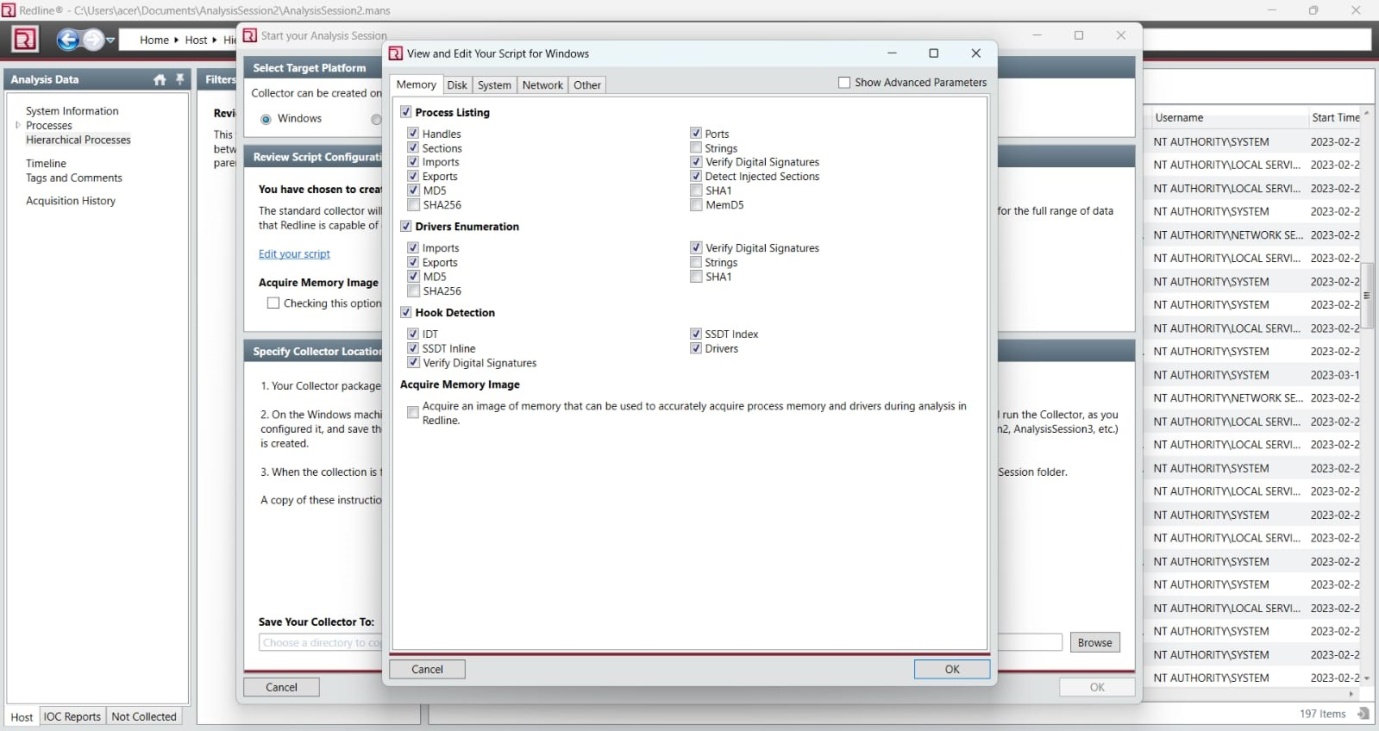
**Step3.** Collect the data.

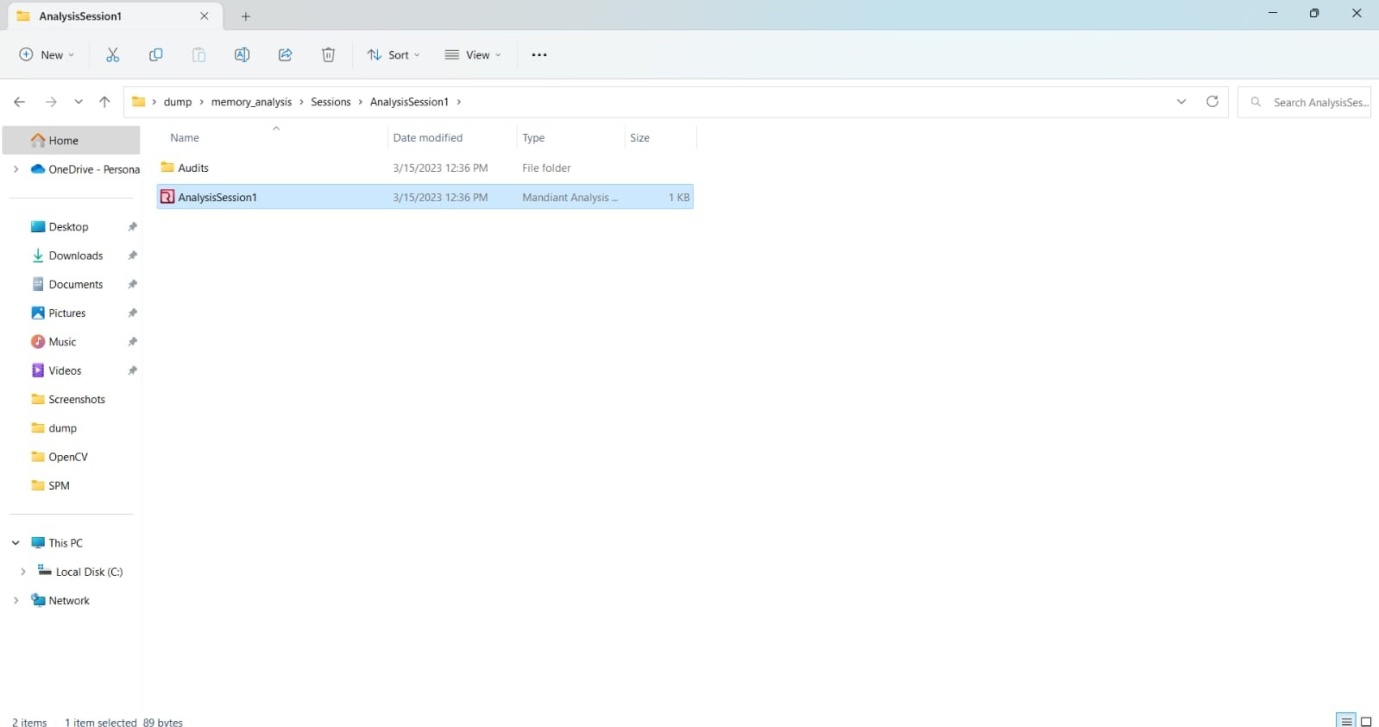
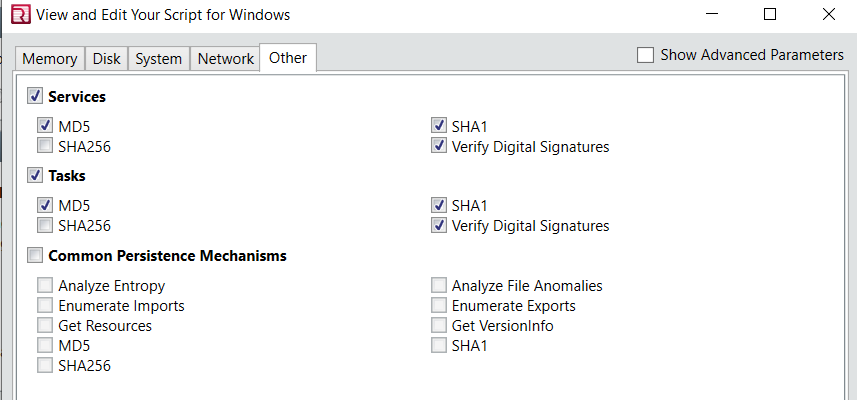
**Step4.** Check the malicious activity

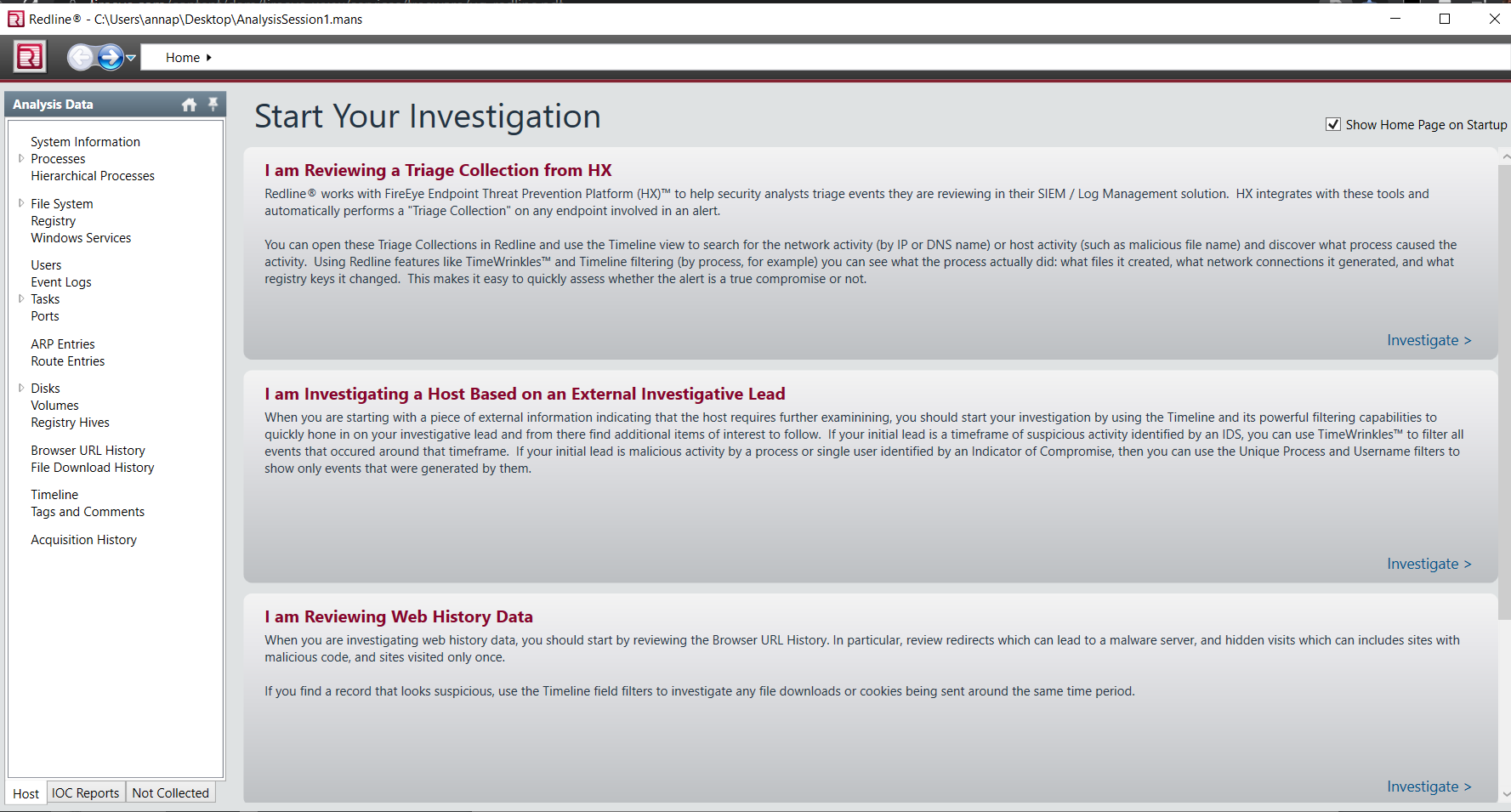
****

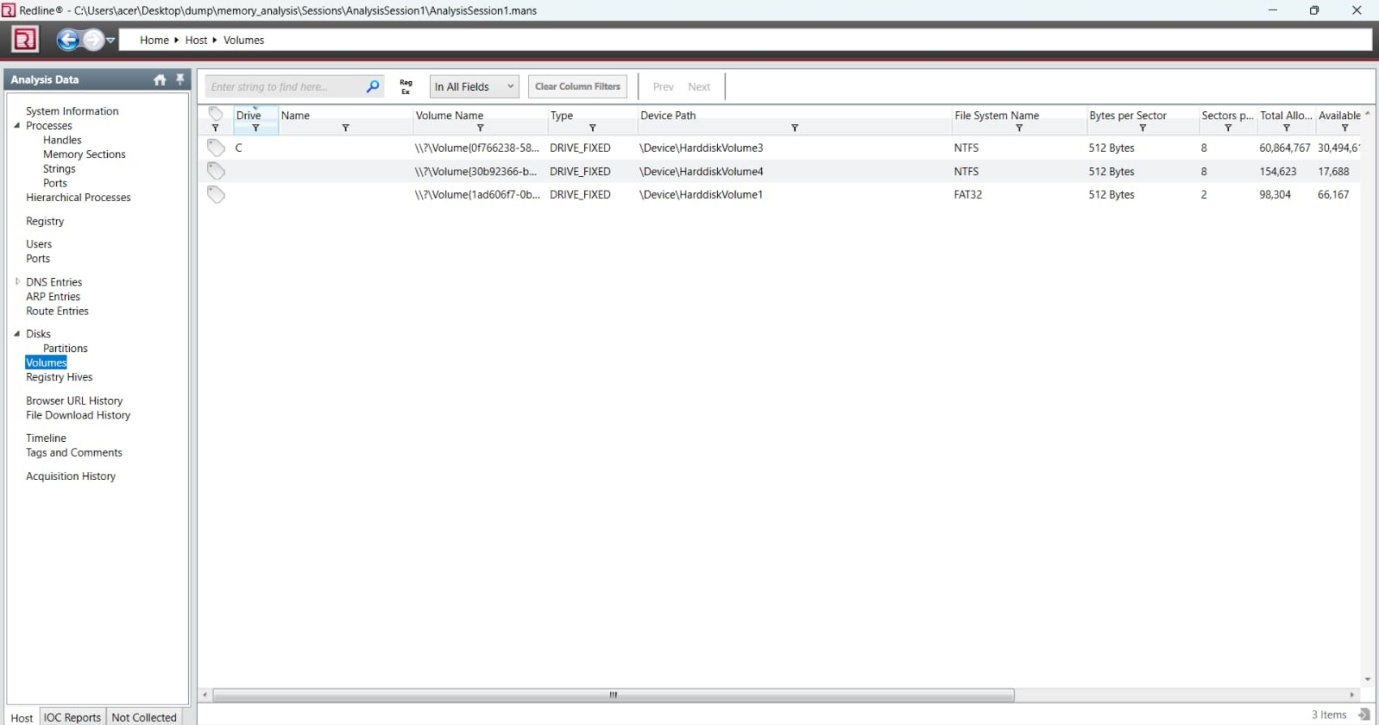
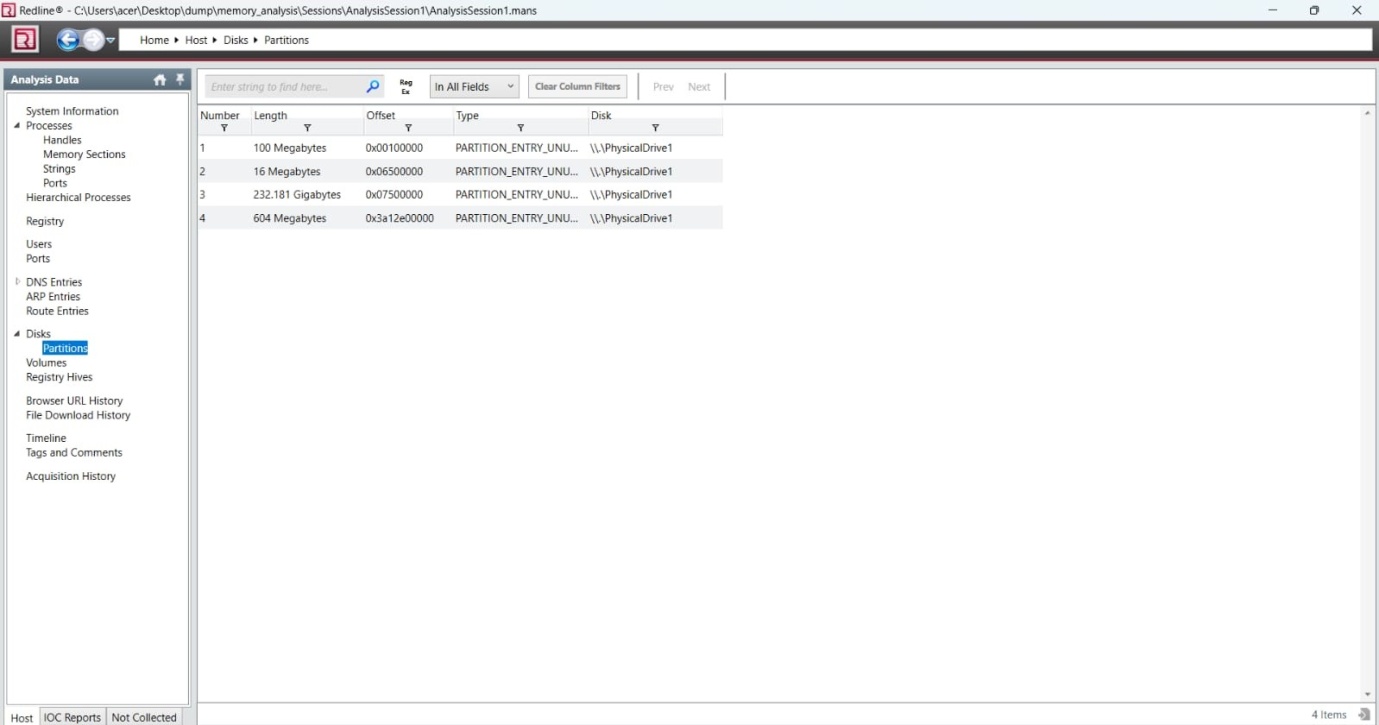
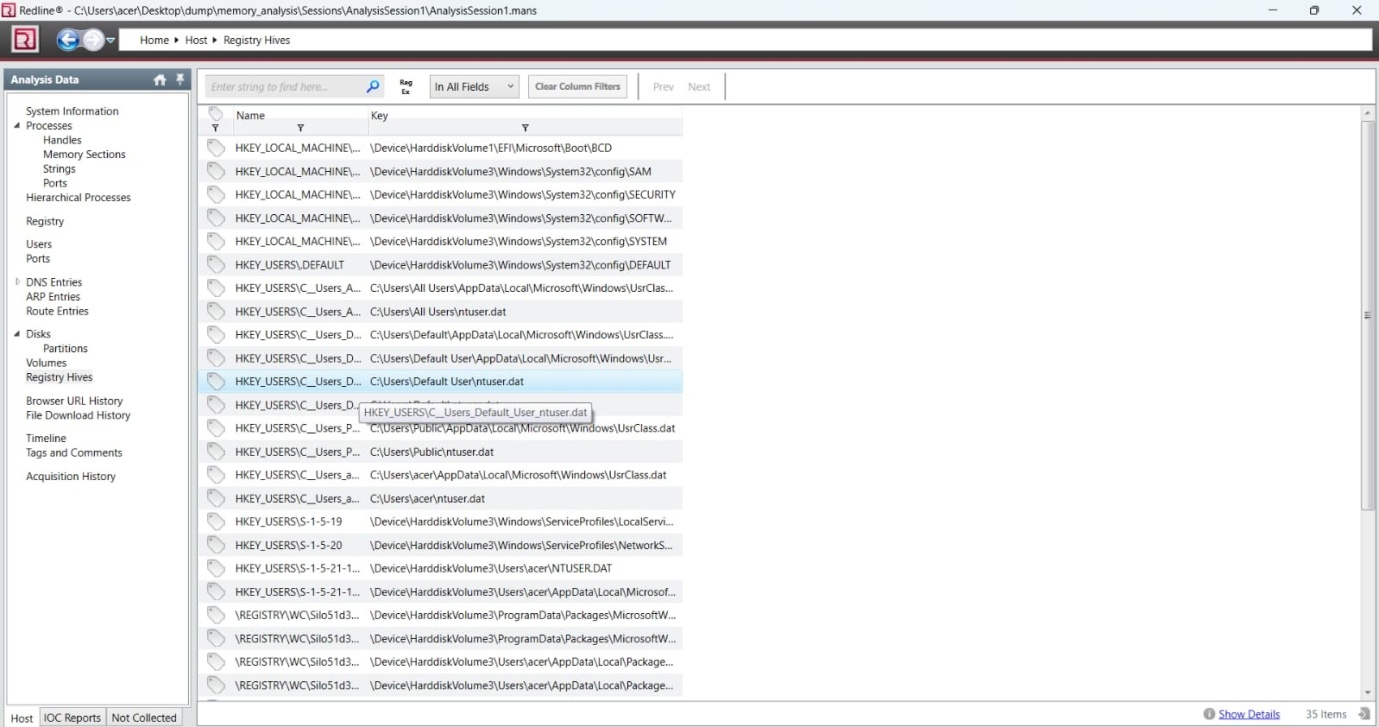
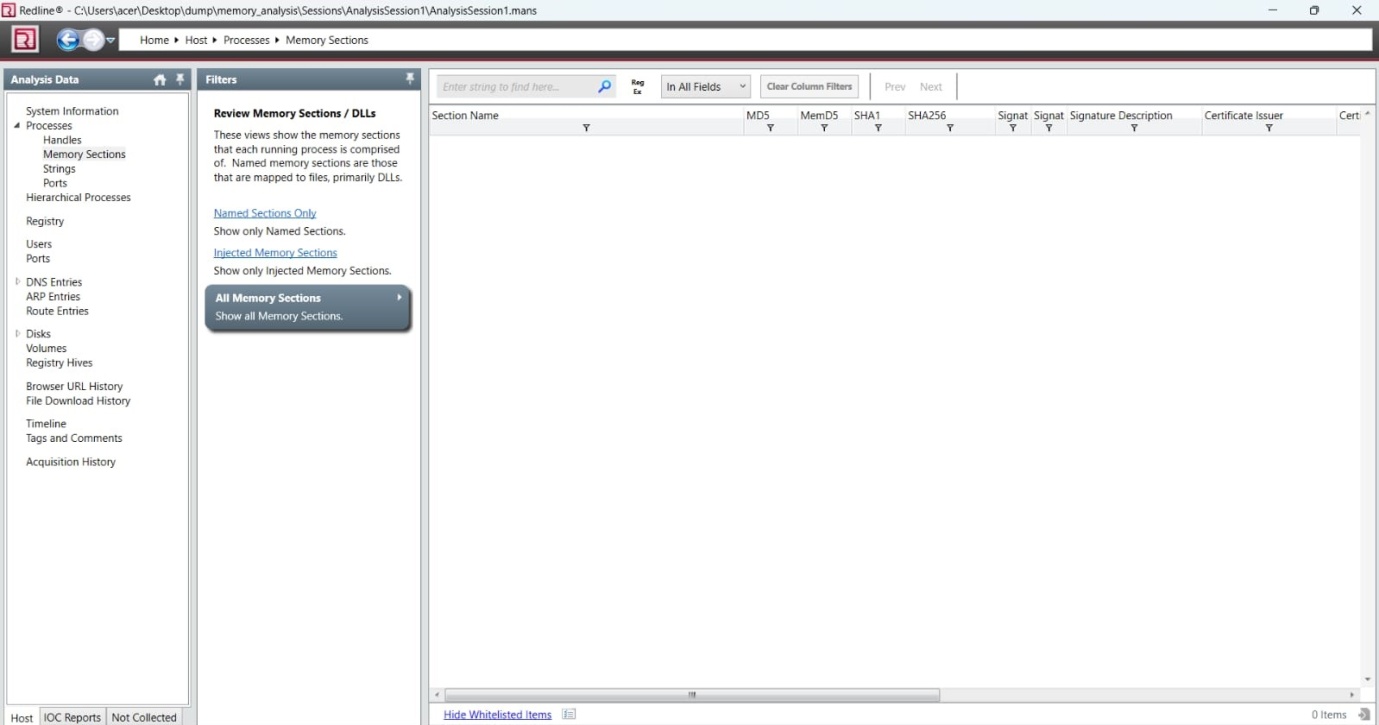
****

****









**References**

I have seen Youtube for downloading the tool.

Take the help of internet.

Help the website TrackHack me.

**Github link is :**

**Thank You**