LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

CA-3

Topic: Q: 31: Install a RedLine tool and investigate the signs of malicious activity through memory and file analysis.

Github link: [Mritunjay-maker/OpenSourceCA3: This is the repository for the Redline tool analysis. (github.com)]

Submitted by:
Mritunjay Jha
Section: KE059
Reg no: 11906046
Roll no: 14

After the installation of the Redline tool in the pc, Open it to analyze the file for malocius activities

Redline is a free forensic tool developed by Mandiant, a cybersecurity company that is now part of FireEye. The tool is used for analyzing volatile system data, such as memory and network activity, in order to detect and investigate security threats.

Redline provides a comprehensive set of features for collecting and analyzing system data, including memory analysis, file analysis, registry analysis, and network analysis. It can be used to identify indicators of compromise (IOCs) and other signs of malicious activity on a system, as well as to gather intelligence and insights into an attack.

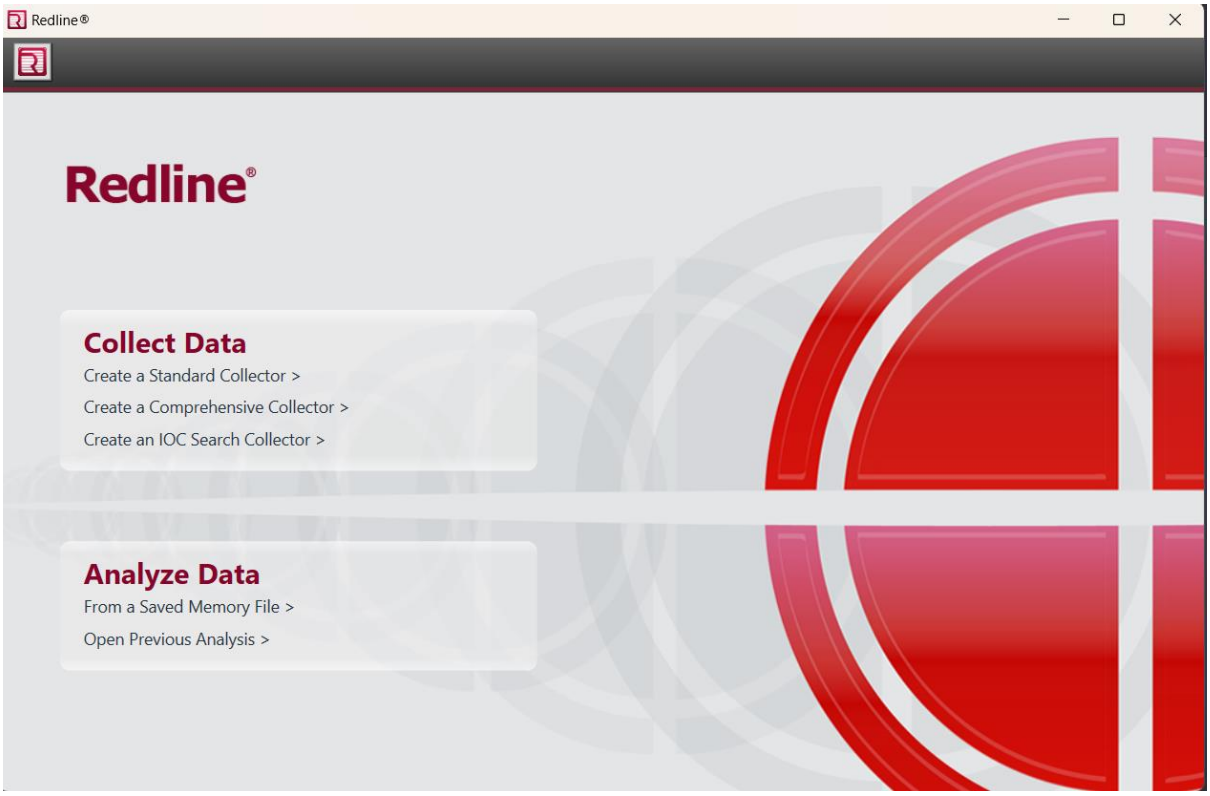
Redline is designed to be user-friendly and flexible, with customizable analysis options and a powerful reporting engine that allows users to generate detailed reports on their findings. It is used by security professionals, incident responders, and other IT professionals to investigate security incidents, perform forensic analysis, and improve overall security posture.

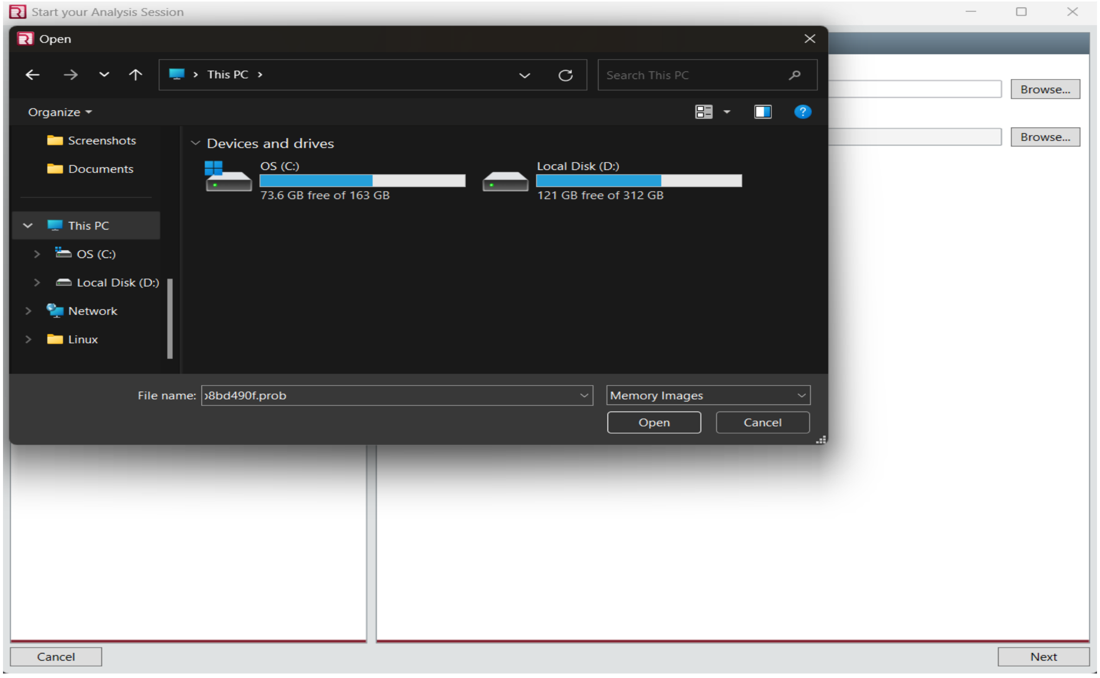
The process Involved are as follows:

1. After installation of the redline tool, launch the tool and select "analyze data (from a saved memory file)" from the main menu.
2. Choose the system you want to analyze and configure the analysis options according to your needs.

3. Select the memory analysis option and configure the settings. This will allow RedLine to capture volatile system data, including process and network activity, from the system's memory.
4. Select the file analysis option and configure the settings. This will allow RedLine to scan the system for malicious files and analyze their behavior.
5. Start the analysis and wait for it to complete. This may take some time, depending on the size of the system and the amount of data being analyzed.
6. Once the analysis is complete, review the results and look for signs of malicious activity, such as unusual network connections, suspicious processes, or malicious files.
7. Use the built-in tools in RedLine to further investigate any suspicious activity and gather additional information about the threat.
8. Take appropriate action to contain and remediate any threats detected by RedLine, such as quarantining infected files or blocking malicious network traffic.

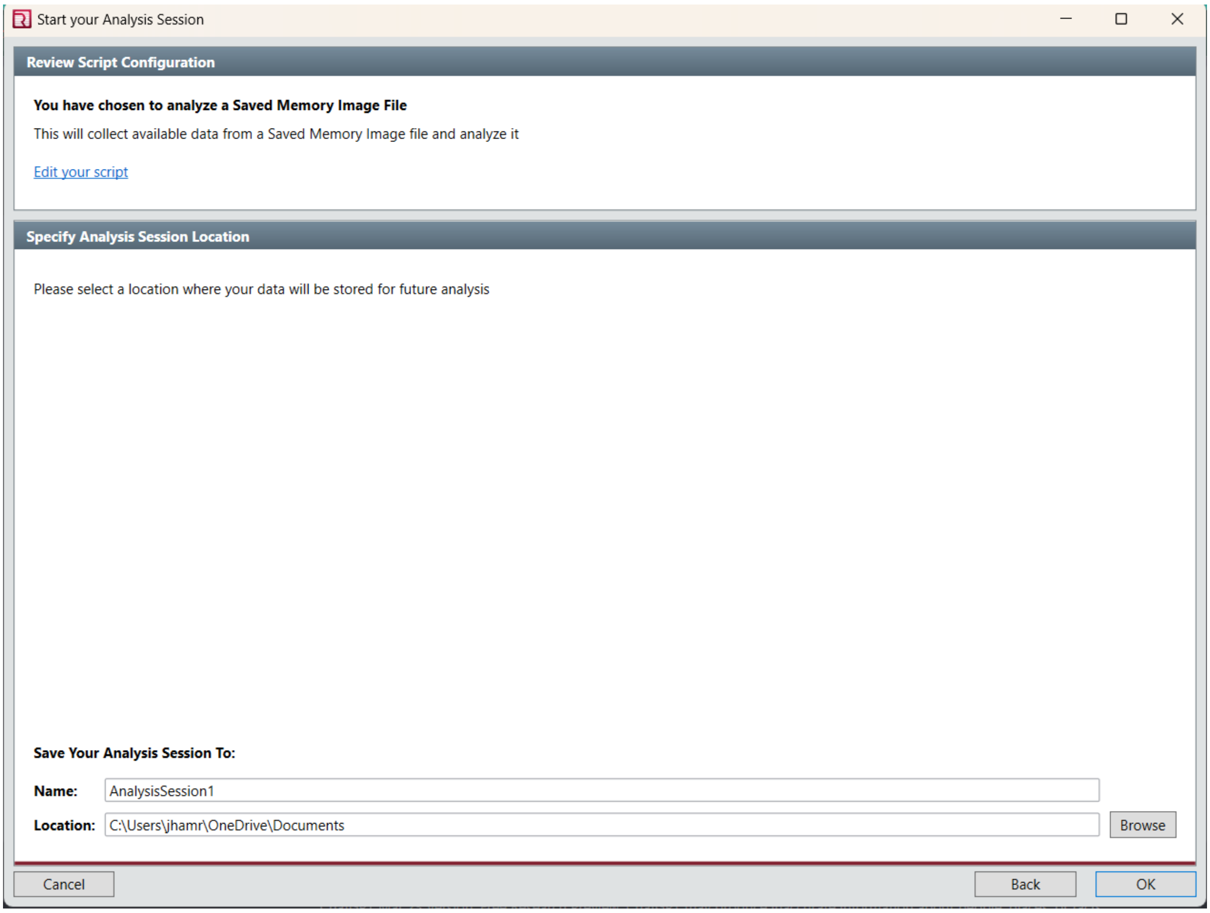
The home page looks like this:


Redline®
Redline®
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >



File name: ›8bd490f.prob

Memory Images



Review Script Configuration

You have chosen to analyze a Saved Memory Image File

This will collect available data from a Saved Memory Image file and analyze it

Edit your script

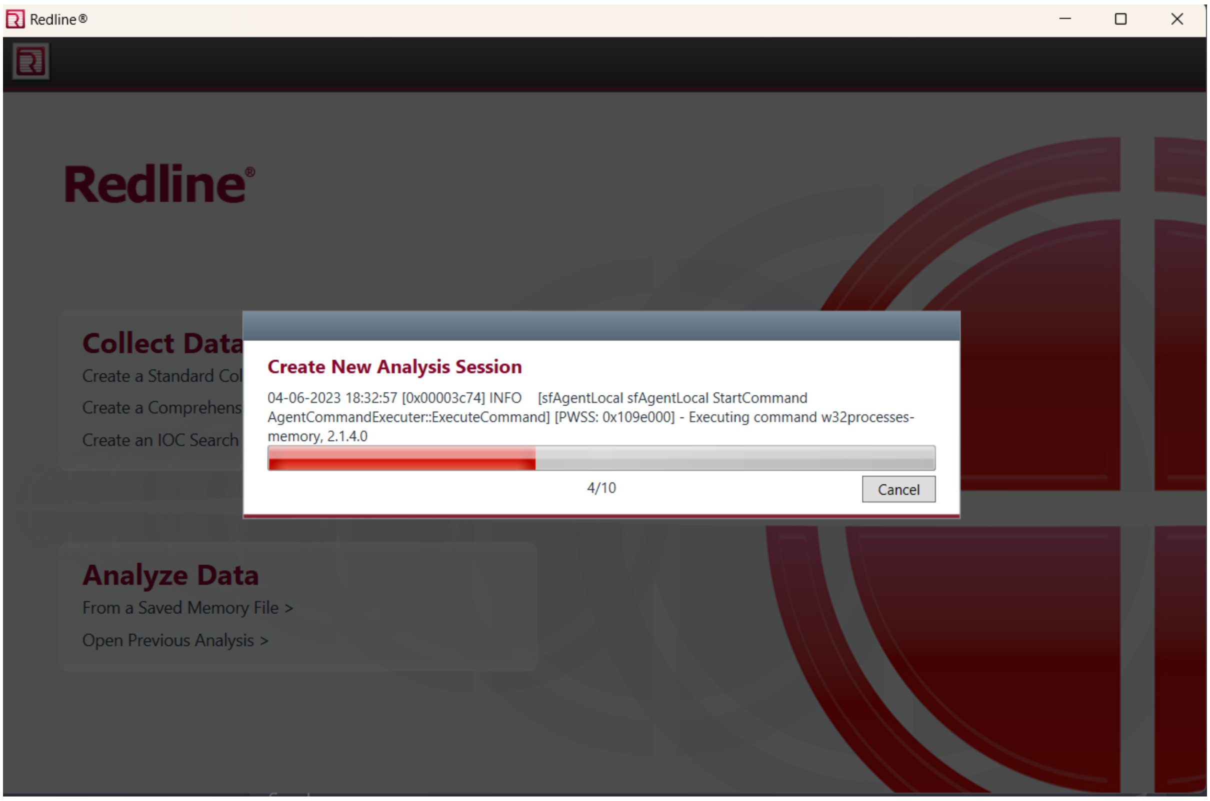
Specify Analysis Session Location

Please select a location where your data will be stored for future analysis

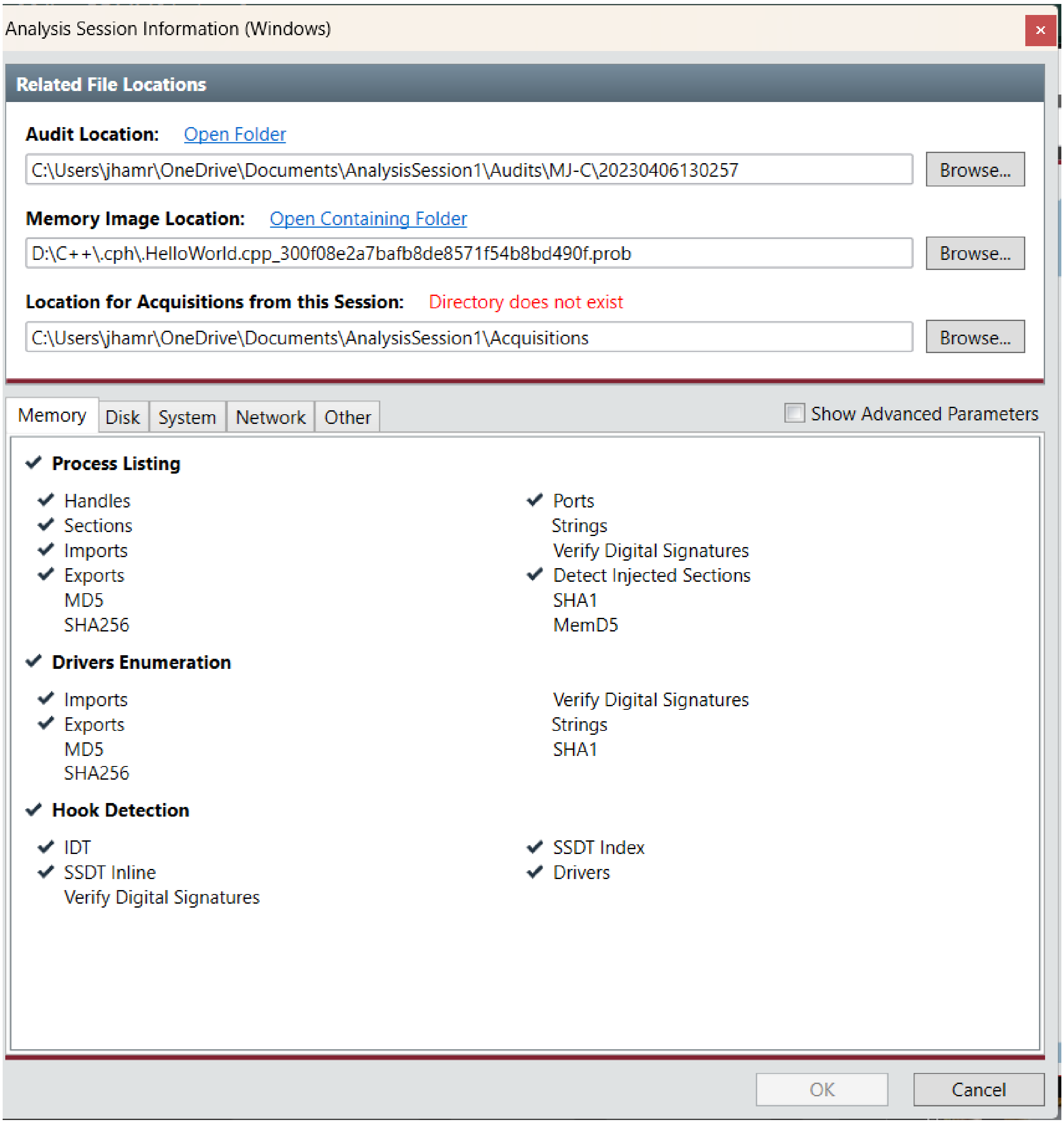
Save Your Analysis Session To:

Name: AnalysisSession1

Location: C:\Users\jhamr\OneDrive\Documents



```
04-06-2023 18:32:57 [0x00003c74] INFO    [sfAgentLocal sfAgentLocal StartCommand
AgentCommandExecuter::ExecuteCommand] [PWSS: 0x109e000] - Executing command w32processes-
memory, 2.1.4.0
```



Analysis Session Information (Windows)

Related File Locations

Audit Location: Open Folder

C:\Users\jhamr\OneDrive\Documents\AnalysisSession1\Audits\MJ-C\20230406130257

Memory Image Location: Open Containing Folder

D:\C++\.cph\.HelloWorld.cpp_300f08e2a7bafb8de8571f54b8bd490f.prob

Location for Acquisitions from this Session: Directory does not exist

C:\Users\jhamr\OneDrive\Documents\AnalysisSession1\Acquisitions

□ Show Advanced Parameters

✓ **Process Listing**

- ✓ Handles
- ✓ Sections
- ✓ Imports
- ✓ Exports
- MD5
- SHA256
- ✓ Ports
- Strings
- Verify Digital Signatures
- ✓ Detect Injected Sections
- SHA1
- MemD5

✓ **Drivers Enumeration**

- ✓ Imports
- ✓ Exports
- MD5
- SHA256
- Verify Digital Signatures
- Strings
- SHA1

✓ **Hook Detection**

- ✓ IDT
- ✓ SSDT Inline
- Verify Digital Signatures
- ✓ SSDT Index
- ✓ Drivers