



## OPEN SOURCE TECHNOLOGIES (INT 301) CA3

Submitted to  
Dr.Rajeshwar sharma  
Lovely Professional University Phagwara,  
Punjab , India.

Submitted by  
Name : Somisetty Teja  
Reg\_No :11904182  
Roll:14  
Section:KE009

# **Investigation of signs of malicious activity through memory and file analysis using RedLine tool**

## **INTRODUCTION**

Now a days computer network attacks have become more frequent, it immediately affects legacy and loss for individuals or businesses. The timely response to the situation is the responsibility of the incident response team and lessen the damage. Following the incident, it is used to assess the damage caused, the financial losses, and the lessons learned to prevent similar incidents in the future. The branch of computer forensics employed under similar circumstances is memory forensics, sometimes known as RAM forensics. The Memory is filled with data that can be used to piece together the occurrence. This can be accomplished by employing software to take a image of the compromised device, which is then analysed on the investigator's device using memory forensic software. The investigator's job is to record and analyse the memory image of the compromised system, look for threats and vulnerabilities, and follow the malfunctioning process to determine where the incident originated and report it to the affected organisation or person. The software can record changes made to running processes' registry keys, as well as user activity in event logs and surfing history. In order to provide the necessary results, the investigation must delve deeply into the artefacts and analyse a tremendous amount of data. Memory forensics are also employed by organisations on a regular basis to monitor each employee's log and check for insiders.

## Objectives:

The primary objective of investigating the signs of malicious activity through memory and file analysis using Redline tool is to identify and mitigate potential security threats to an organization's computer network.

1. Identifying and analyzing malicious processes running in memory: Redline allows for the creation of memory dumps, which can be analyzed to identify any malicious processes running on a system. By analyzing the memory dumps, it's possible to identify the behavior of the process and determine if it's part of a larger malware infection.
2. Identifying signs of lateral movement: Malware can often move laterally through a network, infecting other systems as it goes. By analyzing memory and file artifacts on multiple systems, it's possible to identify signs of lateral movement and determine how far the infection has spread.
3. Generating reports for further analysis: Redline can generate reports that summarize the results of the analysis. These reports can be used to further investigate potential security threats or to share information with other members of the security team.

Overall, the objective of using Redline tool for memory and file analysis is to detect and mitigate potential security threats to an organization's computer network before they can cause significant damage.

## Description:

Investigating the signs of malicious activity through memory and file analysis using Redline tool involves a detailed analysis of the computer system's memory and file artifacts to identify any suspicious behavior or activity that may indicate the presence of malware.

1. Collecting data: Redline tool is used to collect data from the computer system, including memory dumps and file artifacts.
2. Analyzing memory dumps: The memory dumps are analyzed using Redline's memory analysis capabilities to identify any malicious processes running on the system. This analysis can include examining running processes, network connections, and loaded modules to determine if they are part of a larger malware infection.
3. Analyzing file artifacts: Redline can also analyze file artifacts on the system, including executable files, DLLs, and registry keys, to identify any signs of malicious activity. This analysis may include examining file names, file types, digital signatures, and other attributes.
4. Identifying indicators of compromise: Redline can identify indicators of compromise (IOCs) based on the analysis of memory and file artifacts. These IOCs may include IP addresses, domain names, file hashes, and other data points that indicate a system has been compromised.
5. Generating reports: Redline can generate reports that summarize the results of the analysis, including any identified IOCs and suspicious behavior. These reports can be used to further investigate potential security threats or to share information with other members of the security team.

By investigating the signs of malicious activity through memory and file analysis using Redline tool, organizations can detect and mitigate potential security threats to their computer networks, reducing the risk of data breaches and other cybersecurity incidents.

## Scope :

Redline is a free memory and file analysis tool developed by FireEye that is designed to help investigators identify and understand the behavior of malicious software on a compromised system. Redline offers a wide range of capabilities for memory and file analysis, and can be used to investigate a variety of signs of malicious activity.

**Suspicious network activity:** Redline can be used to analyze network traffic captured on a compromised system and identify any suspicious connections or data transfers. This can help investigators identify the IP addresses, domains, or URLs associated with the malicious activity.

**Persistence mechanisms:** Malicious software often uses persistence mechanisms to ensure that it remains active on a compromised system even after a reboot. Redline can help investigators identify these persistence mechanisms, such as registry keys or scheduled tasks, and understand how they are being used to maintain the malware's presence on the system.

**Malicious processes:** Redline can be used to analyze running processes on a compromised system and identify any processes that are associated with malicious activity. This can help investigators understand how the malware is operating on the system and what actions it is taking.

**File and registry changes:** Malicious software often makes changes to files and registry keys on a compromised system. Redline can help investigators identify these changes and understand how they are related to the malware's behavior.

**Memory analysis:** Redline can be used to perform memory analysis on a compromised system and identify any suspicious processes or code that are running in memory. This can help investigators identify malware that is designed to evade detection by traditional antivirus software.

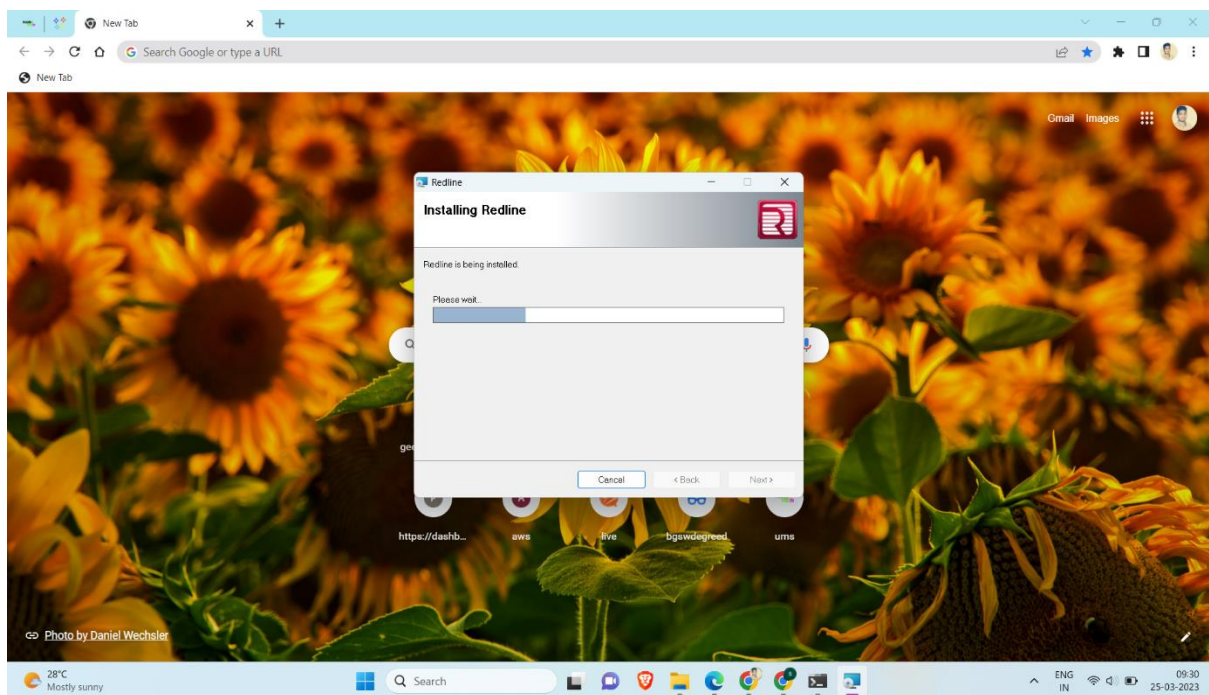
Overall, Redline provides a powerful set of tools for investigating signs of malicious activity through memory and file analysis. By leveraging the capabilities of Redline, investigators can gain a deeper understanding of the behavior of malware on a compromised system and identify the tools and tactics used by attackers.

# Steps involved in investigate the signs of malicious activity Through memory and file analysis using redline tool

**Step 1:** Firstly we have to goto the fireeye.com website to download and install the redline tool.

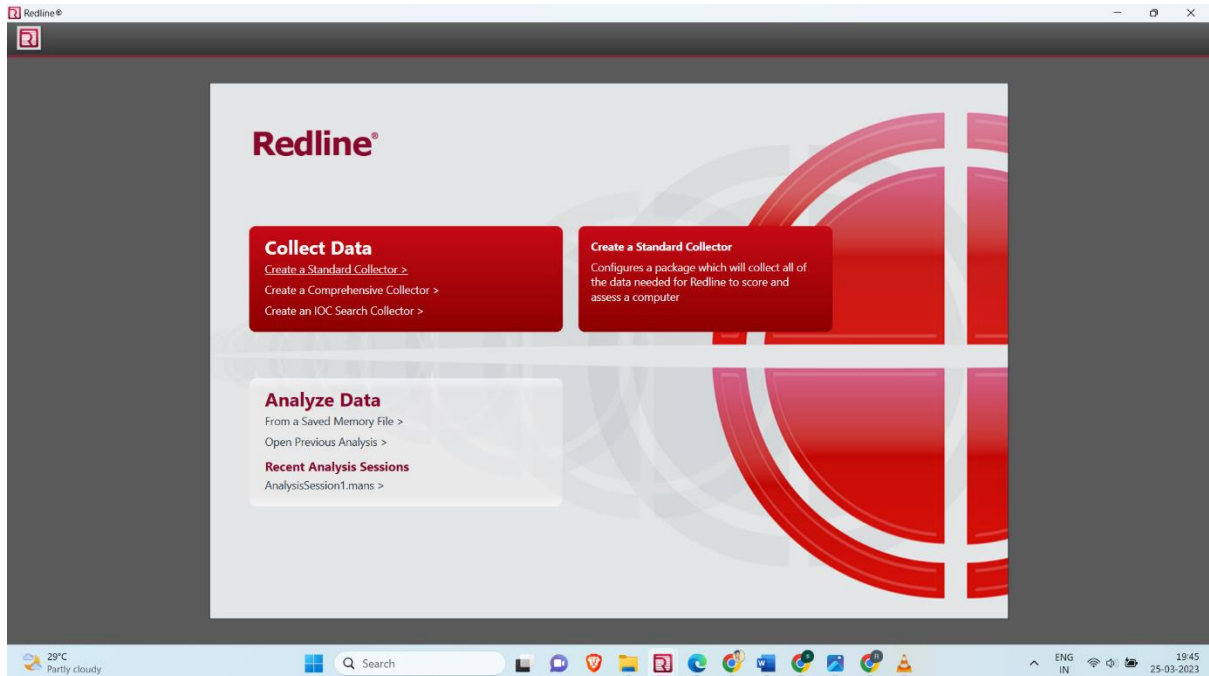
**Step 2:** Extract the downloaded archive the file.

**Step 3:** Install the extract file.



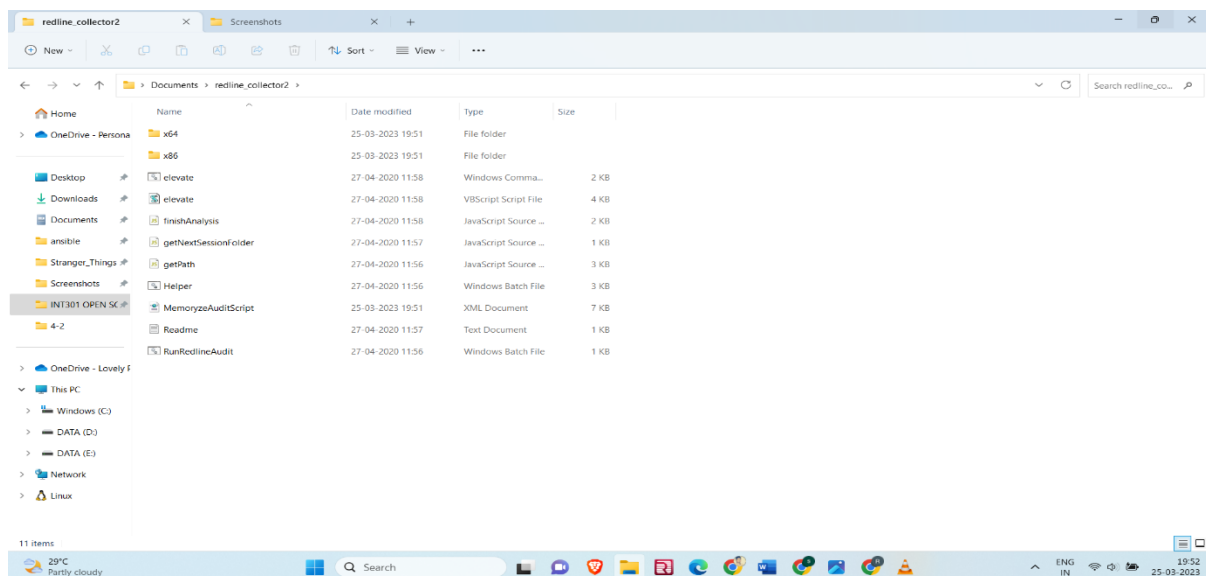
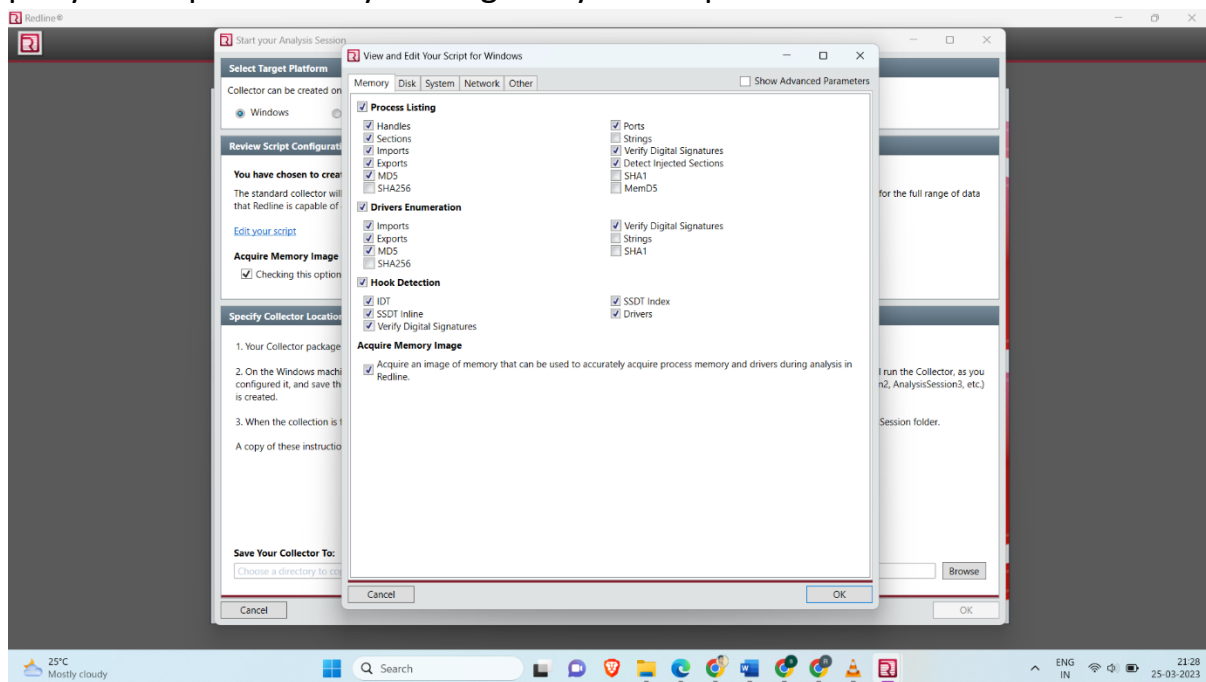
## Investigating signs of malicious activity through memory analysis.

**Step 4:** Once RedLine is launched, click on "Collect" to create a new collection.



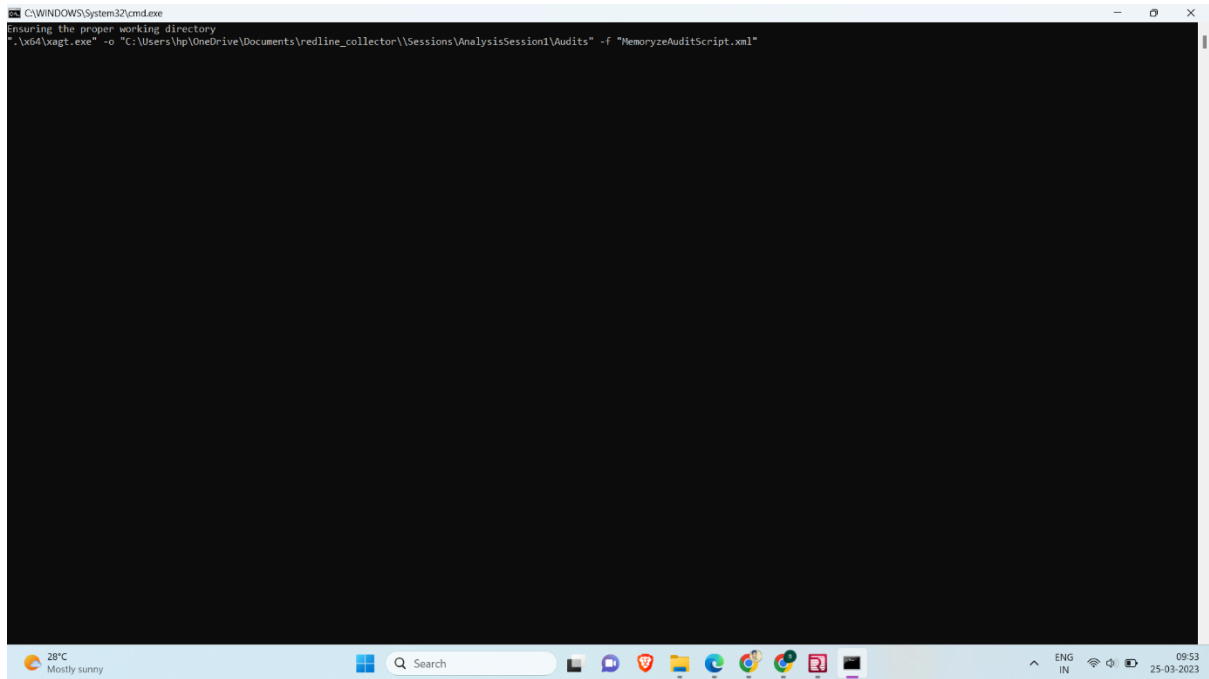
**Step 5:** After the launching of RedLine tool select the target platform as windows and then select "Memory" as the collection type and then choose the empty folder to store the analysis and remaining reports and then goto the file location. And you can also edit memory , disk , system, network and others as

per your requirements by clicking edit your script.

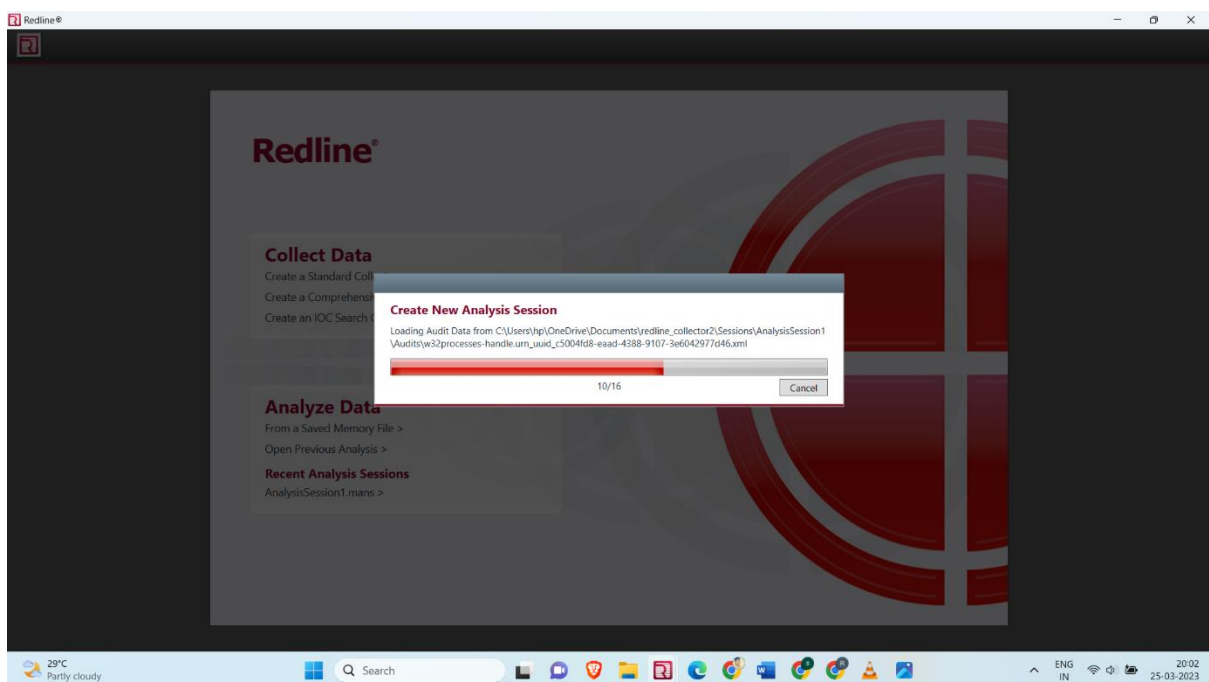


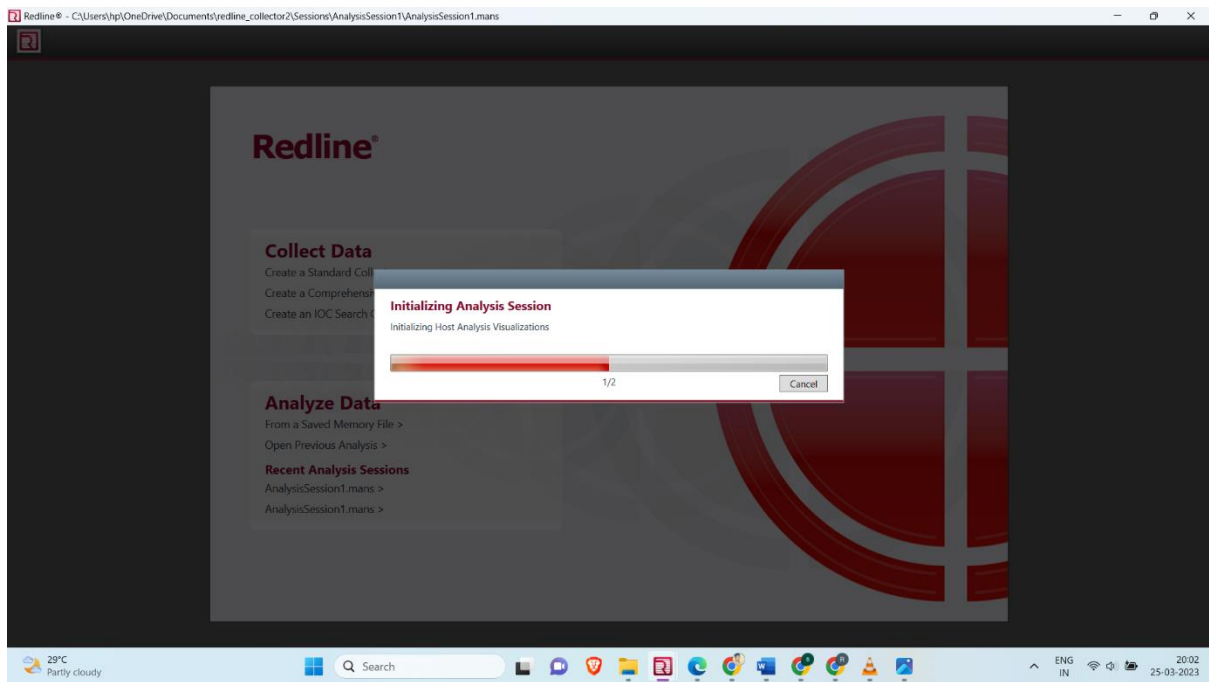
**Step 5:** After going to the file location and then double click on the file name called RunRedLineAudit and the it redirect to the command promt.



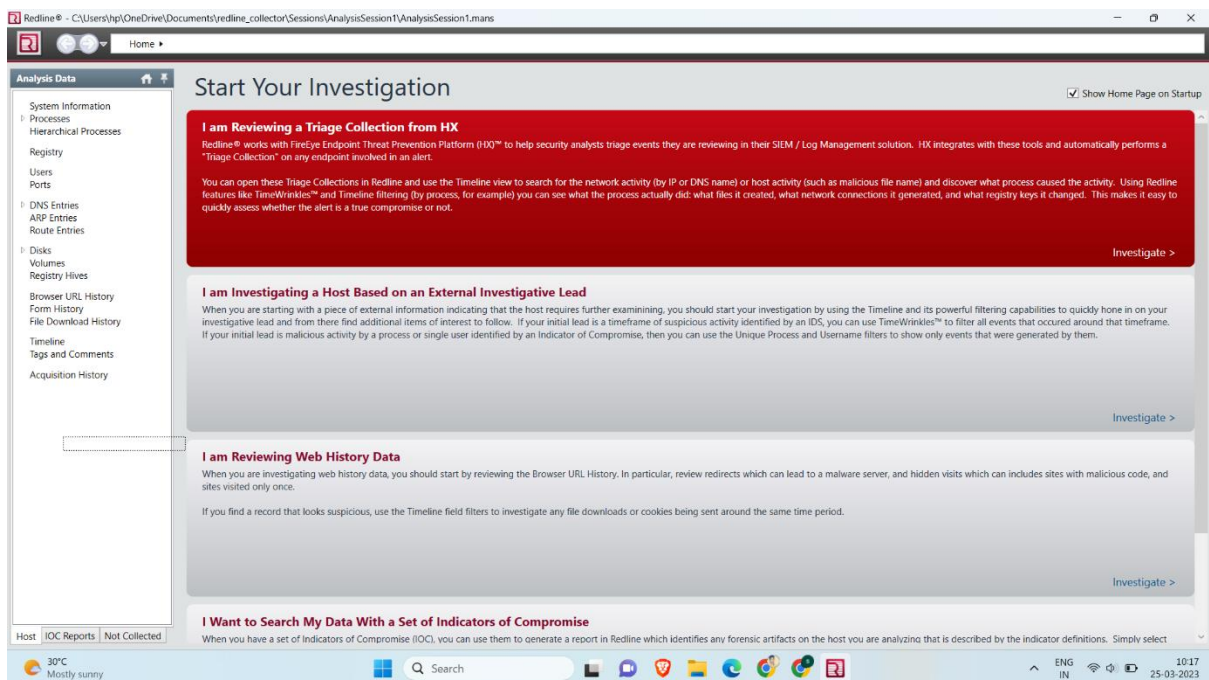


**Step 6:** After that goto the redline tool and then form Analyze data select the Open previous Analysis and then choose the file called AnalysisSession1 which present the file called Sessions And then it will create and initializing the session.





**Step 7:** Then after we will land on the analysis data page here we will find different analysis modules provided by RedLine to investigate the memory for signs of malicious activity.



**Step 8:** Here in first module you can investigate the trigger modules. The Triage Summary is a high-level view of the triage data.

**Redline®** - C:\Users\hpl\OneDrive\Documents\redline\_collector\Sessions\AnalysisSession1\AnalysisSession1.mans

Home

**Analysis Data**

- System Information
- Processes
- Hierarchical Processes
- Registry
- Users
- Ports
- DNS Entries
- ARP Entries
- Route Entries
- Disks
- Volumes
- Registry Hives
- Browser URL History
- Form History
- File Download History
- Timeline
- Tags and Comments
- Acquisition History

**Start Your Investigation**

☒ Show Home Page on Startup

**I am Reviewing a Triage Collection from HX**

Redline® works with FireEye Endpoint Threat Prevention Platform (ETP) to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.

You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.

[Investigate >](#)

**I am Investigating a Host Based on an External Investigative Lead**

When you are starting with a piece of external information indicating that the host requires further examining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWinkles™ to filter all events that occurred around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

[Investigate >](#)

**I am Reviewing Web History Data**

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

[Investigate >](#)

**I Want to Search My Data With a Set of Indicators of Compromise**

When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select

Host | IOC Reports | Not Collected

30°C Mostly sunny

Search

ENG IN 10:17 25-03-2023

**Redline®** - C:\Users\hpl\OneDrive\Documents\redline\_collector2\Sessions\AnalysisSession1\AnalysisSession1.mans

Home

**Analysis Data**

- System Information
- Processes
- Hierarchical Processes
- Timeline
- Tags and Comments
- Acquisition History

**Timeline Configuration**

☐ Show All ☐ Deselect All

**Files:**

- ☐ Created
- ☐ Accessed
- ☒ Modified
- ☒ Changed
- ☒ FilenameCreated
- ☒ FilenameAccessed
- ☒ FilenameModified
- ☒ FilenameChanged

**Processes:**

- ☒ StartTime

**Registry:**

- ☒ Modified

**Event Logs:**

- ☒ GenTime
- ☐ WriteTime

**Tasks:**

- ☒ NextRunTime
- ☒ MostRecentRunTime
- ☒ CreationDate
- ☐ Trigger/Begin
- ☐ Trigger/End

**User Accounts:**

- ☒ LastLogin

**System Information:**

- ☒ SystemDate
- ☐ InstallDate
- ☐ NetworkInfo/DHCPLeaseExpires
- ☐ NetworkInfo/DHCPLeaseObtained

**Ports:**

- ☒ CreationTime

Fields: TimeCrunches™ 0 Users Processes

Enter string to find here...

In All Fields Clear Column Filters Prev Next

Y	Timestamp	Field	Y	Summary
	2022-10-12 19:14:59Z	System/InstallDate		Machine: KANDUKURISAIBAB Domain: WORKGROUP OS: Windows 10 Home Single Language 22H2
	2023-03-24 11:58:32Z	Process/StartTime		Name: Secure System PID: 108 Path: Args:
	2023-03-24 11:58:32Z	Process/StartTime		Name: Registry PID: 156 Path: Args:
	2023-03-24 11:58:32Z	Process/StartTime		Name: Secure System PID: 108 Path: Args:
	2023-03-24 11:58:32Z	Process/StartTime		Name: Registry PID: 156 Path: Args:
	2023-03-24 11:58:32Z	Process/StartTime		Name: smss.exe PID: 600 Path: Args:
	2023-03-24 11:58:39Z	Process/StartTime		Name: System PID: 4 Path: Args:
	2023-03-24 11:58:39Z	Process/StartTime		Name: System PID: 4 Path: Args:
	2023-03-24 11:58:39Z	Process/StartTime		Name: smss.exe PID: 600 Path: Args:
	2023-03-24 11:58:47Z	Process/StartTime		Name: csrss.exe PID: 1000 Path: Args:
	2023-03-24 11:58:47Z	Process/StartTime		Name: csrss.exe PID: 1000 Path: Args:
	2023-03-24 11:58:50Z	Process/StartTime		Name: wininit.exe PID: 688 Path: Args:
	2023-03-24 11:58:50Z	Process/StartTime		Name: services.exe PID: 1048 Path: Args:
	2023-03-24 11:58:50Z	Process/StartTime		Name: lsass.exe PID: 1080 Path: Args:
	2023-03-24 11:58:50Z	Process/StartTime		Name: lsass.exe PID: 1108 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: svchost.exe PID: 1216 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: fontdrvhost.exe PID: 1252 Path: C:\WINDOWS\system32 Args: "fontd
	2023-03-24 11:58:50Z	Process/StartTime		Name: WUDFHost.exe PID: 1308 Path: C:\Windows\system32 Args: "C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: svchost.exe PID: 1392 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: svchost.exe PID: 1436 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: lsass.exe PID: 1080 Path: Args:
	2023-03-24 11:58:50Z	Process/StartTime		Name: lsass.exe PID: 1108 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: svchost.exe PID: 1216 Path: C:\WINDOWS\system32 Args: C:\WI
	2023-03-24 11:58:50Z	Process/StartTime		Name: fontdrvhost.exe PID: 1252 Path: C:\WINDOWS\system32 Args: "fontd

586 Items

25°C Mostly cloudy

Search

ENG IN 21:30 25-03-2023

Step 9: In the same way you can investigate I am Investigating a Host Based on an External Investigative lead here you can here you can investigate host related problems.

The screenshot displays the Redline application interface. The top section, titled "Start Your Investigation", contains three main guides:

- I am Reviewing a Triage Collection from HX**: Explains how Redline works with FireEye Endpoint Threat Prevention Platform (ETP) to help security analysts triage events. It mentions that HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.
- I am Investigating a Host Based on an External Investigative Lead**: Provides instructions on how to start an investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on an investigative lead and find additional items of interest.
- I am Reviewing Web History Data**: Advises on reviewing Browser URL History, particularly focusing on redirects and hidden visits to sites with malicious code.

Below these guides is a section titled "I Want to Search My Data With a Set of Indicators of Compromise", which explains how to use IOC reports to generate a report in Redline.

The bottom section of the interface shows the "Timeline" view. On the left, there is a sidebar with "Analysis Data" and "Timeline Configuration". The "Timeline Configuration" panel includes checkboxes for various filters such as "Files", "Processes", "Registry", "Event Logs", "Tasks", "User Accounts", "System Information", and "Ports". The main area displays a table of events with columns for "Timestamp", "Field", "Summary", and "Args". The table lists various system events, including process starts, registry changes, and file operations, with details like machine name, domain, OS, and process path.

Step 10 : In the same way you can investigate I am reviewing web history data in this you can investigate url history and review redirects and many in this.

Redline - C:\Users\hp\OneDrive\Documents\redline\_collector2\Sessions\AnalysisSession1\AnalysisSession1.mars

Home

### Start Your Investigation

☒ Show Home Page on Startup

[Investigate >](#)

**I am Investigating a Host Based on an External Investigative Lead**

When you are starting with a piece of external information indicating that the host requires further examining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWinkles™ to filter all events that occurred around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

[Investigate >](#)

**I am Reviewing Web History Data**

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

[Investigate >](#)

**I Want to Search My Data With a Set of Indicators of Compromise**

When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select 'Create a New IOC Report' and specify the location on disk that contains your indicator. When the report is finished you will find it underneath the IOC Reports tab to the left. For more information on IOCs visit <http://www.openioc.org>

[Investigate >](#)

Host | IOC Reports | Not Collected

25°C Mostly cloudy

Search

ENG IN 21:41 25-03-2023

Redline - C:\Users\hp\OneDrive\Documents\redline\_collector2\Sessions\AnalysisSession1\AnalysisSession1.mars

Home | Host | System Information

### System Information

**Machine Information**

Machine Name:	KANDUKURISABAB
Host Name:	KANDUKURISABABU
System Date:	2023-03-25 04:22:52Z
Time Zone DST:	India Daylight Time
Time Zone Standard:	India Standard Time
Processor Identity:	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz
Processor Type:	Multiprocessor Free
Primary Network Adapter MAC:	c0-e4-34-7b-92-6d
Total Physical Memory:	7,809 Gigabytes
Available Physical Memory:	1,962 Gigabytes
Drives:	c,d,e,f,k
Uptime:	16:24:20
Containment State:	normal
Clock Skew:	00:00:00
State Agent Status:	monitoring_disabled

**BIOS Information**

BIOS Date String:	02/03/2021
BIOS Version:	Insyde F36
BIOS Type:	Unknown

**Operating System Information**

Operating System:	Windows 10 Home Single Language 22H2
Product Name:	Windows 10 Home Single Language
Patch Level:	Not Available
OS Build:	22H2
Product ID:	00327-35176-67707-AAOEM
System directory:	C:\WINDOWS\system32
Install Date:	2022-10-12 19:14:59Z
Operating System Bitness:	64-bit

**User Information**

Registered Owner:	hp
Registered Organization:	HP
Domain:	WORKGROUP

Host | IOC Reports | Not Collected

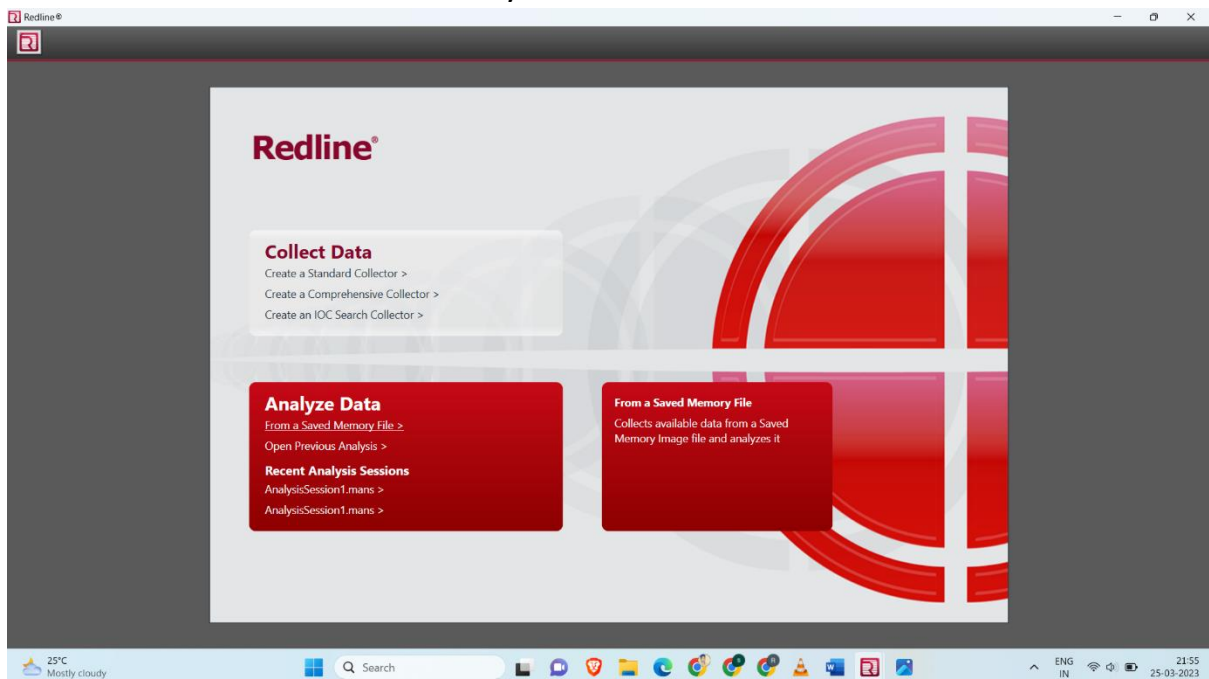
30°C Partly sunny

Search

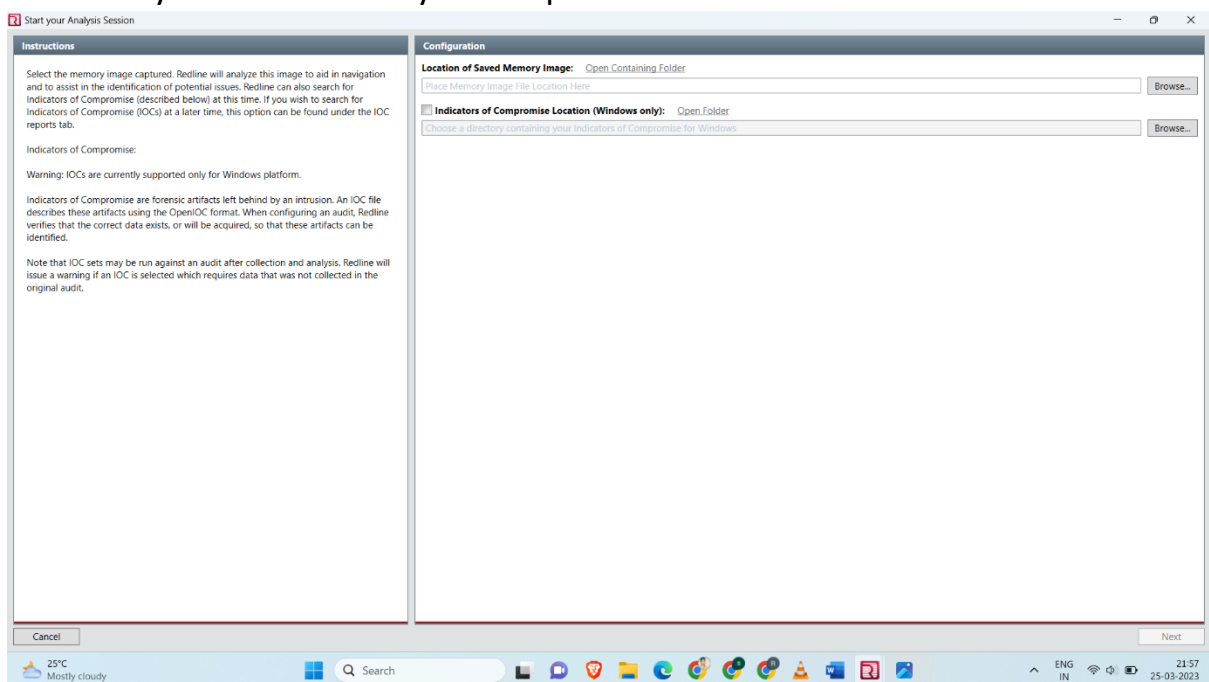
ENG IN 11:28 25-03-2023

## Investigating signs of malicious activity through file analysis

Step 11: Open the redline tool in main tab you can see analyze data and then click on the from a saved memory file.

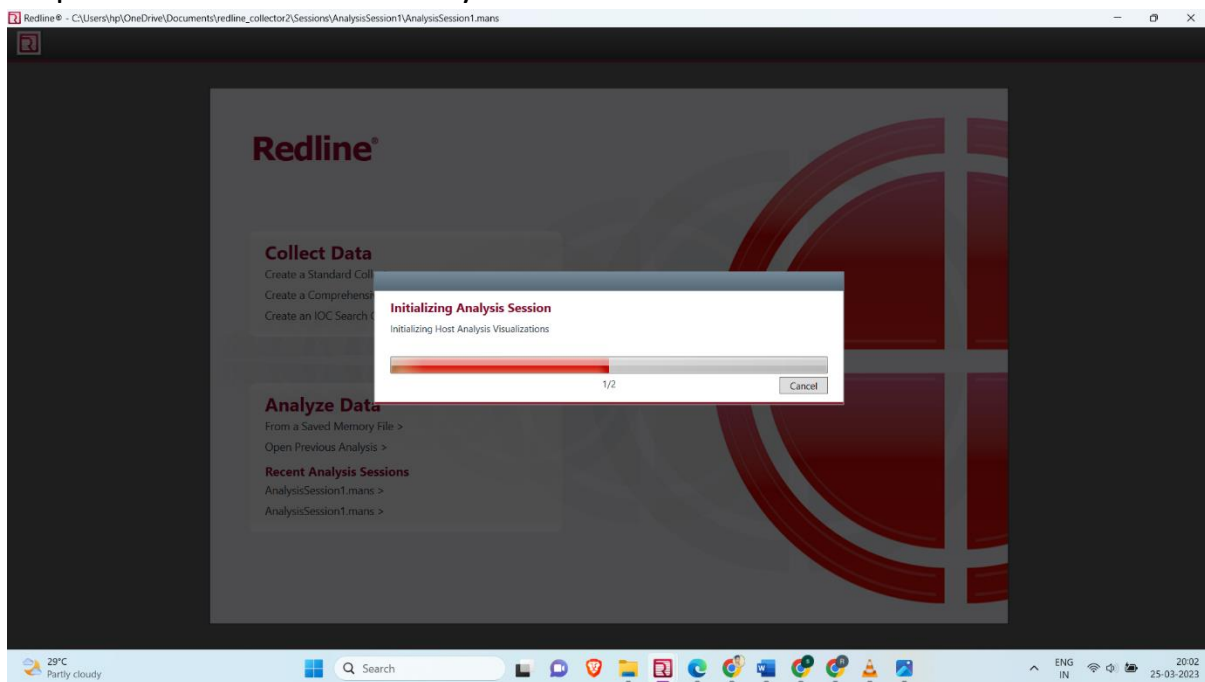


Step 12 : After that select the folder where image present and then click on Next and you can also edit your script .

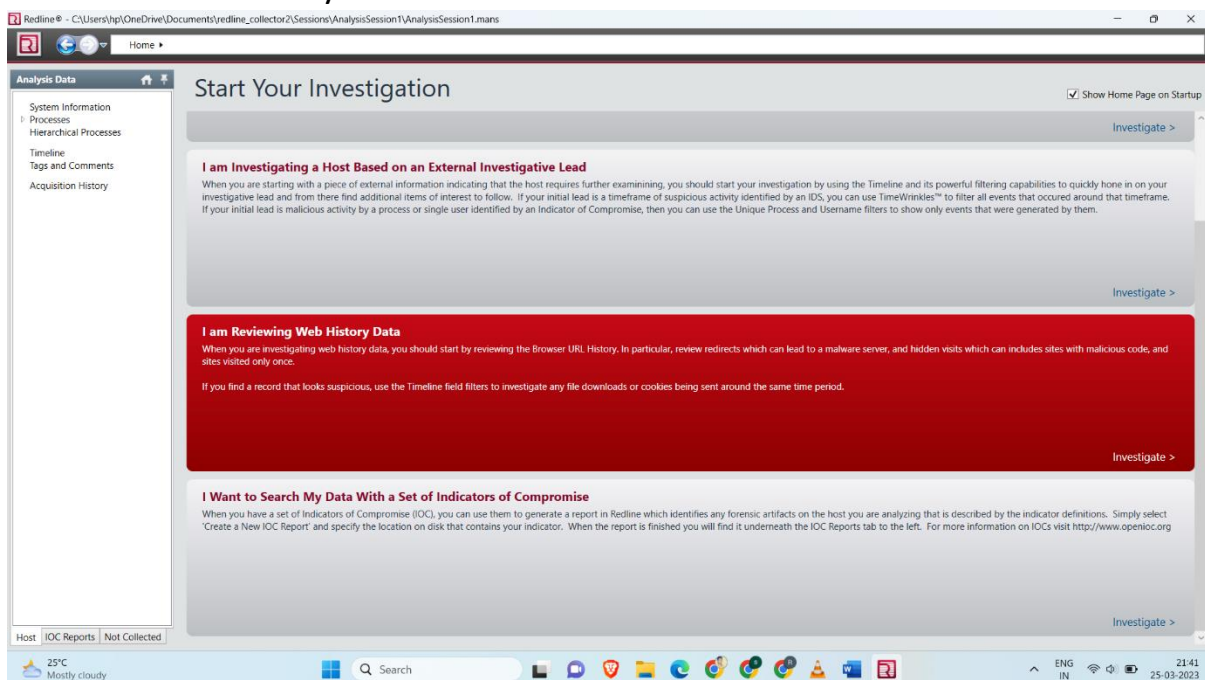




Step 13 : After that it will analyze and then initialize.



Step 14 : In the same way like memory analysis we Use the different analysis modules provided by RedLine to investigate the file for signs of malicious activity. For example, you can use the "Strings" module to search for known malicious strings in the file or the "PE Headers" module to view information about the file's binary structure.



Here we can analyse using different modules which is same as memory analysis.

**Conclusion:** Investigating the signs of malicious activity through memory and file analysis using Redline tool can provide valuable insights into potential security breaches and help identify the source of the attack. Redline tool is a powerful tool that enables the analysis of system memory and file artifacts to detect and investigate malicious activity. By analyzing the system's memory and file artifacts, Redline can identify suspicious processes, network connections, registry modifications, and other indicators of compromise. Redline tool can be an effective tool for investigating signs of malicious activity through memory and file analysis, and can help organizations improve their overall security posture by identifying and mitigating potential threats.

## References:

FireEye Redline User Guide:

[https://fireeye.market/assets/apps/211364/documents/877936\\_en.pdf](https://fireeye.market/assets/apps/211364/documents/877936_en.pdf)

ScienceDirect:

<https://www.sciencedirect.com/topics/computer-science/memory-forensics>