Acquire and Analyze the volatile data of RAM

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

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

1. Introduction

1.1 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.

1.2 Description of the project

The acquisition and analysis of 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 contents of 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 analysis of 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 in general 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.

2. 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.

3. 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.

4. 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.

2. System Description:

2.1 Target System Description:

1. **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.

2. **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.

3. **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.

4. **Analysis Tools:** Tools for analysis of acquired volatile data. These can include instruments such as Volatility, Rekall and Redline.

5. **Storage Media:** A storage medium that stores acquired volatile data. It can be a hard disk or a USB flash drive.

6. **Chain of custody:** A written record of data ownership to ensure its integrity is maintained.

7. **Reporting:** Documentation and reporting of analysis results, including any conclusions drawn from unstable data.

8. **Compliance Requirements:** Any regulatory or legal requirements to retrieve and analyze volatile RAM data, such as privacy or security regulations.

2.2 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.

2.3 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 RAM should be able to access and extract all relevant data stored in RAM.

2. **Data Preservation:** To enable correct analysis, data obtained from RAM should be preserved in a way that maintains its integrity.

3. **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.

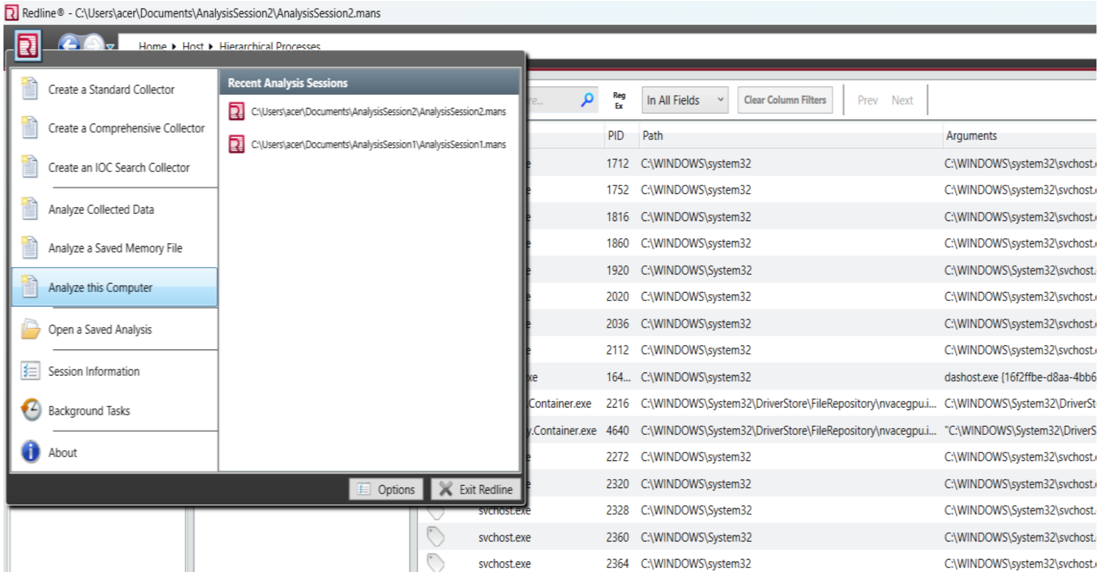
3. **Reliability and robustness:** The tools and techniques used to acquire and analyze the data should be reliable and robust, to minimize the risk of errors or failures.

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.

3. Analysis Report:

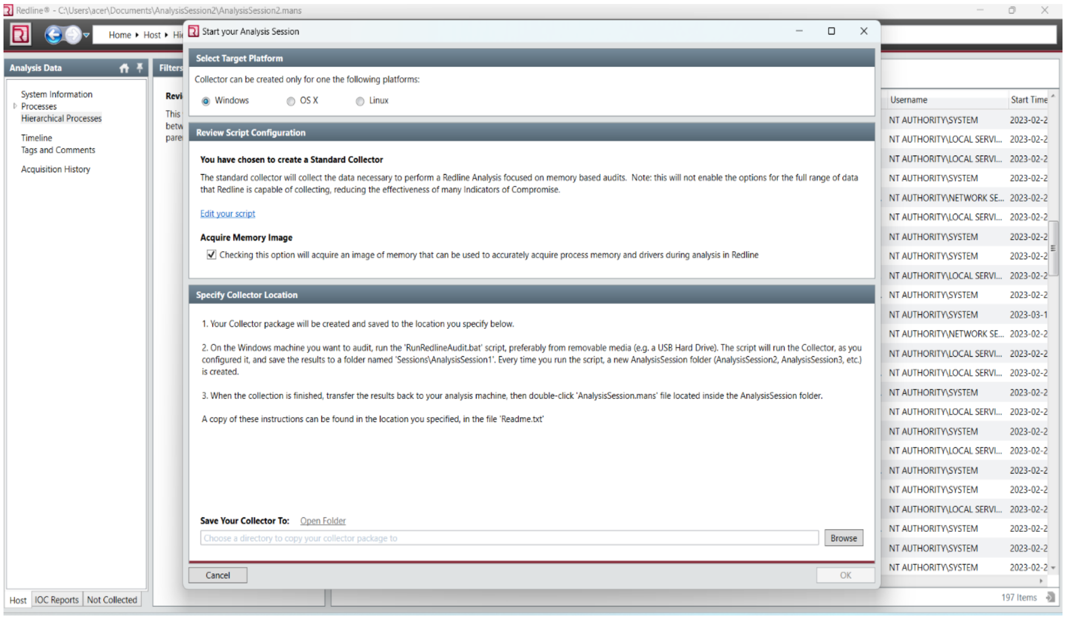
3.1 Steps for Acquire and Analysis volatile data of RAM in a machine:

Acquire memory Image file:


Redline® - C:\Users\acer\Documents\AnalysisSession2\AnalysisSession2.mans
Home ▸ Host ▸ Hierarchical Processes
Create a Standard Collector
Create a Comprehensive Collector
Create an IOC Search Collector
Analyze Collected Data
Analyze a Saved Memory File
Analyze this Computer
Open a Saved Analysis
Session Information
Background Tasks
About
Recent Analysis Sessions
C:\Users\acer\Documents\AnalysisSession2\AnalysisSession2.mans
C:\Users\acer\Documents\AnalysisSession1\AnalysisSession1.mans
Options
Exit Redline
Reg Ex
In All Fields
Clear Column Filters
Prev
Next

	PID	Path	Arguments
e	1712	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	1752	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	1816	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	1860	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	1920	C:\WINDOWS\System32	C:\WINDOWS\System32\svchost.
e	2020	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	2036	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	2112	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
xe	164...	C:\WINDOWS\system32	dashost.exe {16f2ffbe-d8aa-4bb6
Container.exe	2216	C:\WINDOWS\System32\DriverStore\FileRepository\nvacegpu.i...	C:\WINDOWS\System32\DriverSt
y.Container.exe	4640	C:\WINDOWS\System32\DriverStore\FileRepository\nvacegpu.i...	"C:\WINDOWS\System32\DriverS
e	2272	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
e	2320	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.
svchost.exe	2328	C:\WINDOWS\System32	C:\WINDOWS\System32\svchost.
svchost.exe	2360	C:\WINDOWS\System32	C:\WINDOWS\System32\svchost.
svchost.exe	2364	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.

Creating Memory File:



Redline® - C:\Users\acer\Documents\AnalysisSession2\AnalysisSession2.mans

Start your Analysis Session

Select Target Platform

Collector can be created only for one the following platforms:

● Windows ○ OS X ○ Linux

Review Script Configuration

You have chosen to create a Standard Collector

The standard collector will collect the data necessary to perform a Redline Analysis focused on memory based audits. Note: this will not enable the options for the full range of data that Redline is capable of collecting, reducing the effectiveness of many Indicators of Compromise.

Edit your script

Acquire Memory Image

☑ Checking this option will acquire an image of memory that can be used to accurately acquire process memory and drivers during analysis in Redline

Specify Collector Location

1. Your Collector package will be created and saved to the location you specify below.

2. On the Windows machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.

3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.

A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'

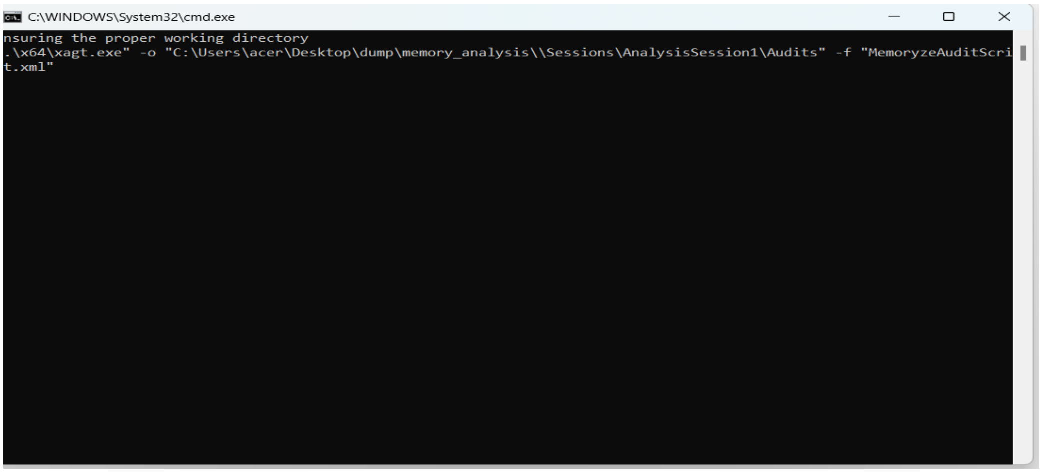
Save Your Collector To: Open Folder

Choose a directory to copy your collector package to

Username	Start Time
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\NETWORK SE...	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\SYSTEM	2023-03-1
NT AUTHORITY\NETWORK SE...	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\LOCAL SERVI...	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2
NT AUTHORITY\SYSTEM	2023-02-2

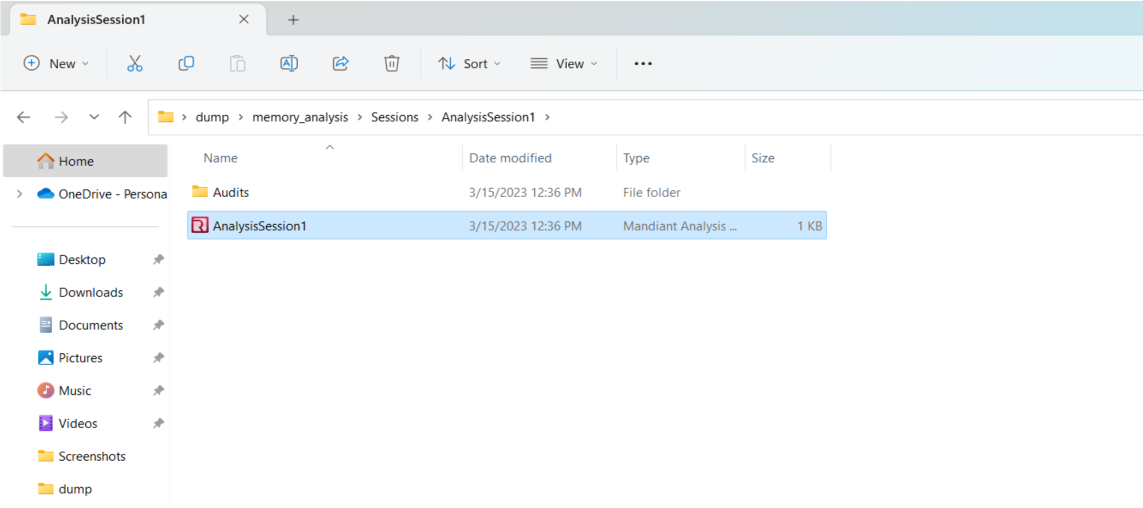
197 Items

Memory Analysis file created:



C:\WINDOWS\System32\cmd.exe

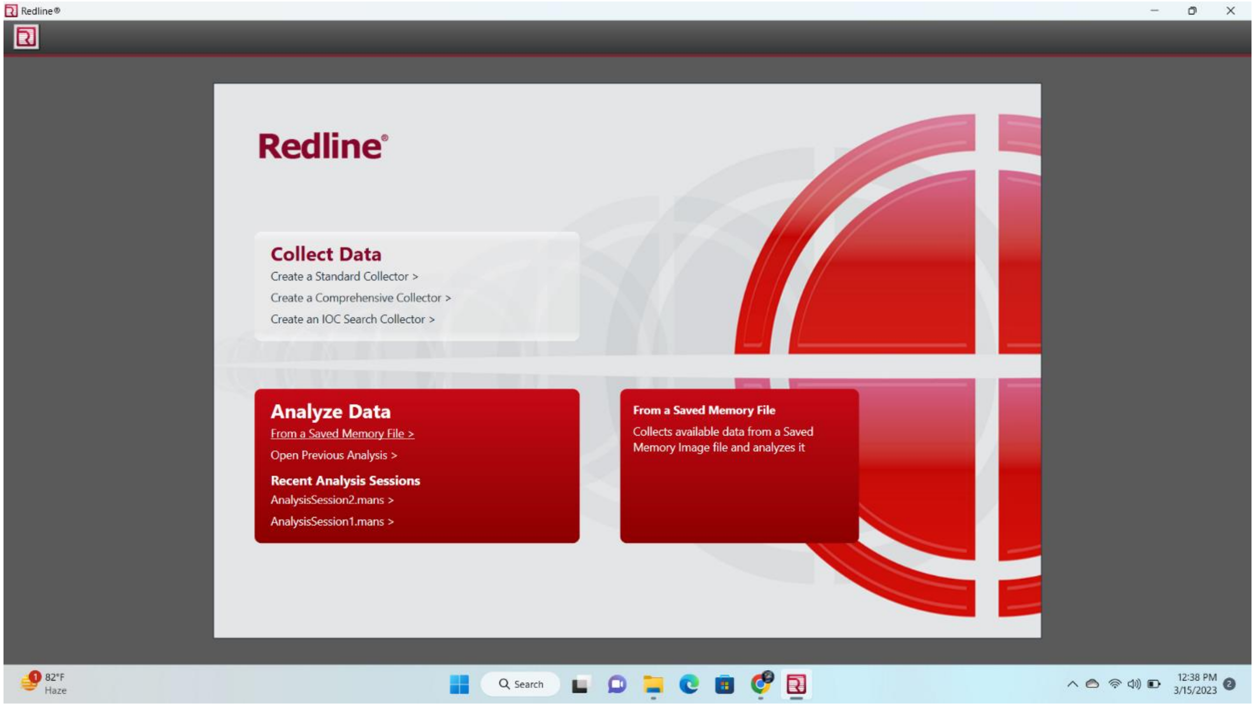
```
nsuring the proper working directory
.\x64\xagt.exe" -o "C:\Users\acer\Desktop\dump\memory_analysis\\Sessions\AnalysisSession1\Audits" -f "MemoryzeAuditScri
t.xml"
```



Name	Date modified	Type	Size
Audits	3/15/2023 12:36 PM	File folder	
AnalysisSession1	3/15/2023 12:36 PM	Mandiant Analysis ...	1 KB

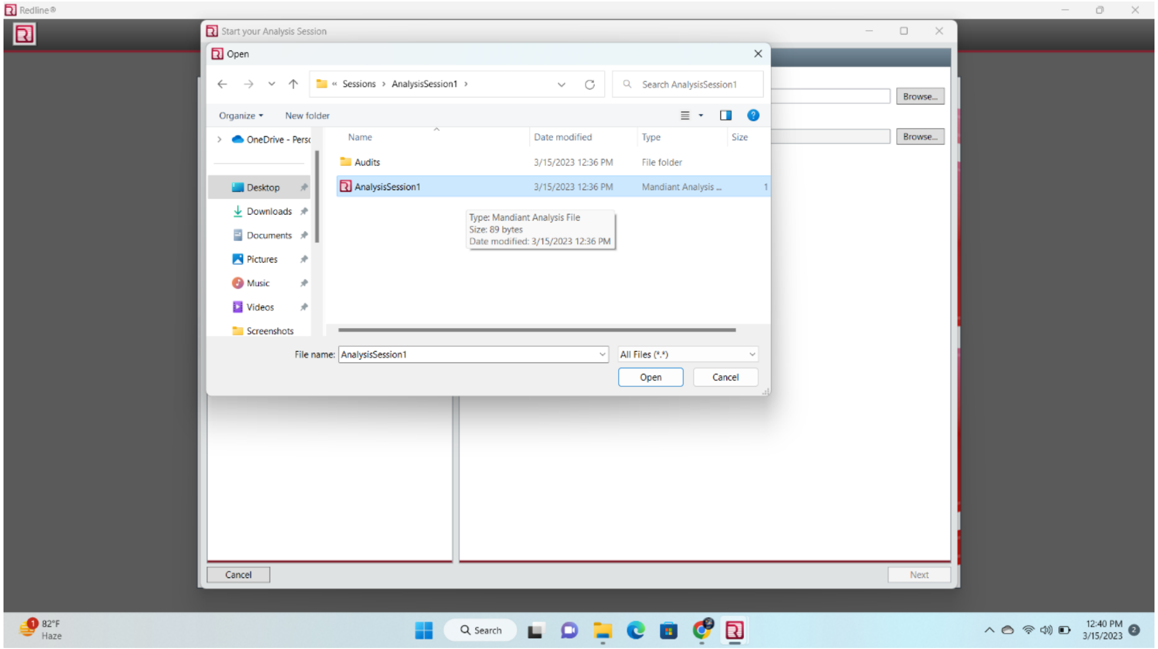
Analyzing Memory File Using Redline Tool:

Click on from a send memory file option:



Collects available data from a Saved Memory Image file and analyzes it

Select the memory file from folder:



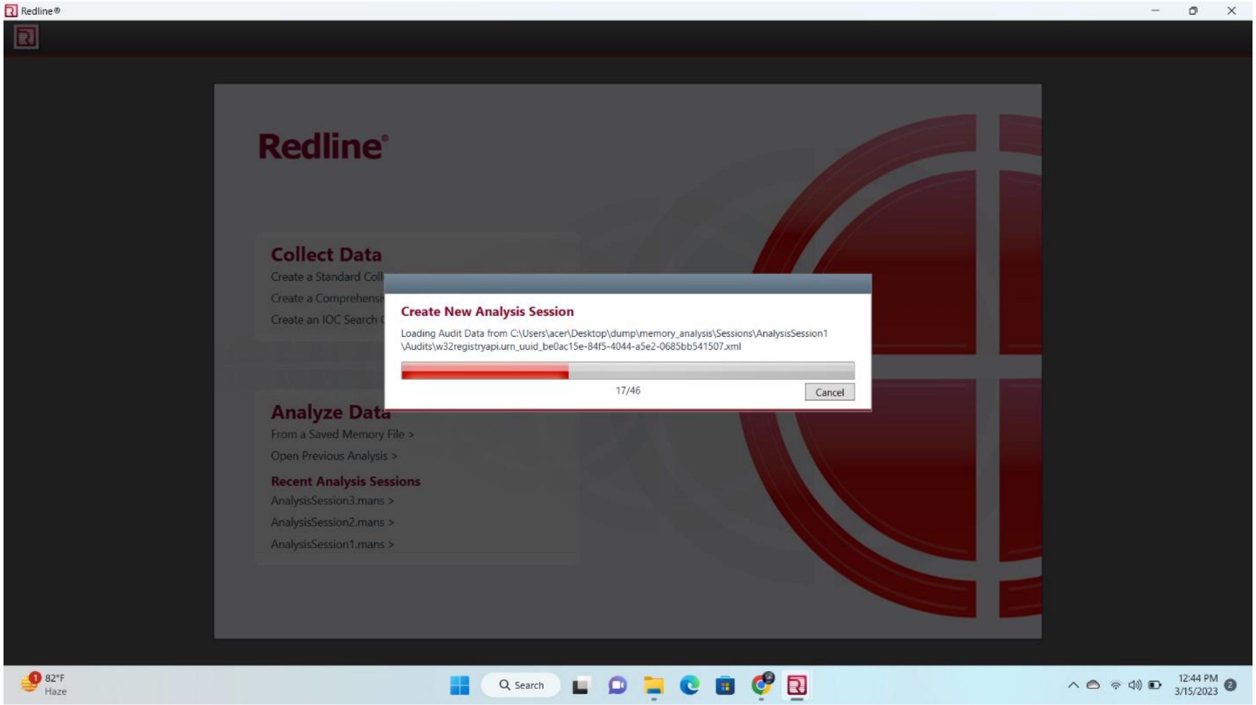
Name	Date modified	Type	Size
Audits	3/15/2023 12:36 PM	File folder	
AnalysisSession1	3/15/2023 12:36 PM	Mandiant Analysis ...	1

Type: Mandiant Analysis File
Size: 89 bytes
Date modified: 3/15/2023 12:36 PM

File name: AnalysisSession1

All Files (*.*)

Analyzing Data:

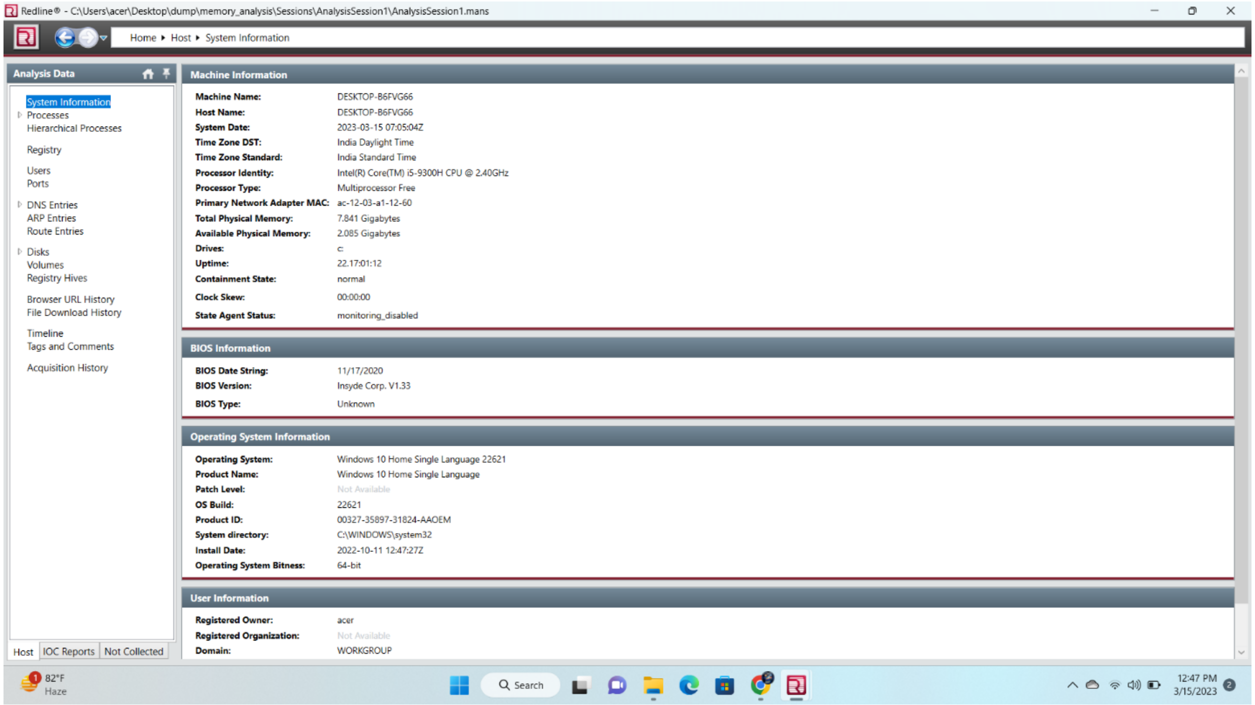


Create New Analysis Session

Loading Audit Data from C:\Users\acer\Desktop\dump\memory_analysis\Sessions\AnalysisSession1
\Audits\w32registryapi.urn_uuid_be0ac15e-84f5-4044-a5e2-0685bb541507.xml

17/46

System Information:


Redline® - C:\Users\acer\Desktop\dump\memory_analysis\Sessions\AnalysisSession1\AnalysisSession1.mans

Machine Information

Machine Name:	DESKTOP-B6FVG66
Host Name:	DESKTOP-B6FVG66
System Date:	2023-03-15 07:05:04Z
Time Zone DST:	India Daylight Time
Time Zone Standard:	India Standard Time
Processor Identity:	Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz
Processor Type:	Multiprocessor Free
Primary Network Adapter MAC:	ac-12-03-a1-12-60
Total Physical Memory:	7.841 Gigabytes
Available Physical Memory:	2.085 Gigabytes
Drives:	c:
Uptime:	22.17:01:12
Containment State:	normal
Clock Skew:	00:00:00
State Agent Status:	monitoring_disabled

BIOS Information

BIOS Date String:	11/17/2020
BIOS Version:	Insyde Corp. V1.33
BIOS Type:	Unknown

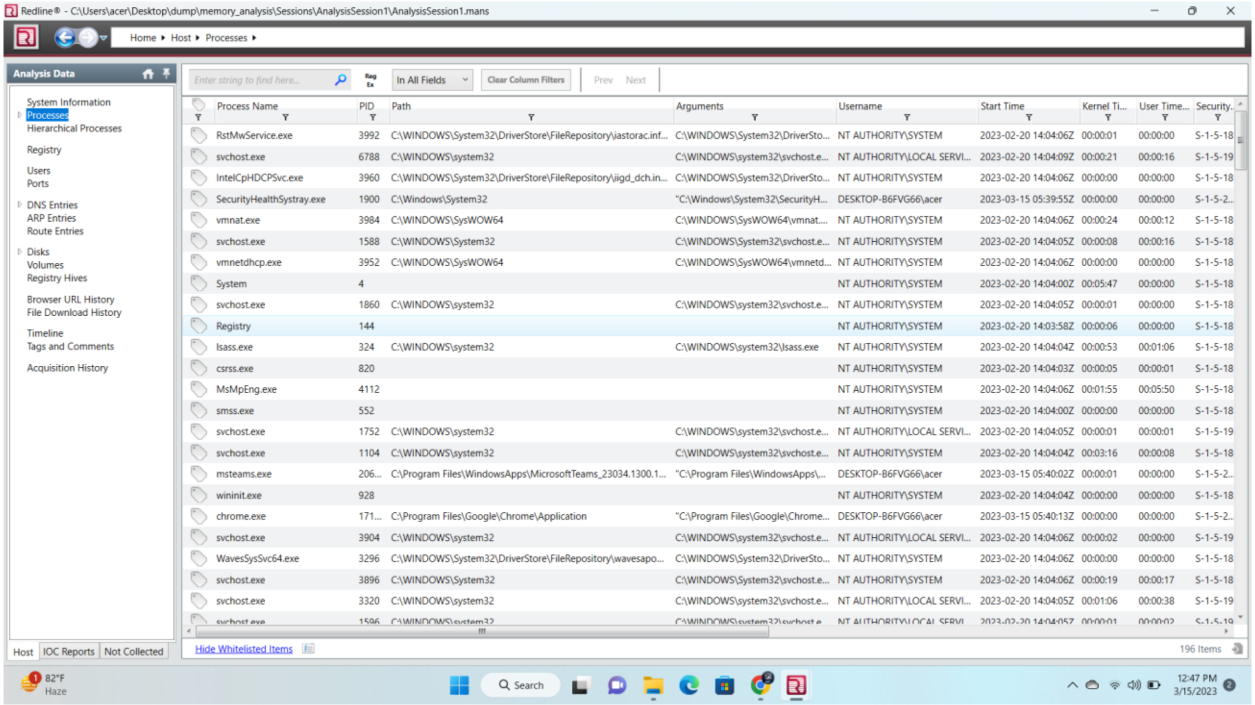
Operating System Information

Operating System:	Windows 10 Home Single Language 22621
Product Name:	Windows 10 Home Single Language
Patch Level:	Not Available
OS Build:	22621
Product ID:	00327-35897-31824-AAOEM
System directory:	C:\WINDOWS\system32
Install Date:	2022-10-11 12:47:27Z
Operating System Bitness:	64-bit

User Information

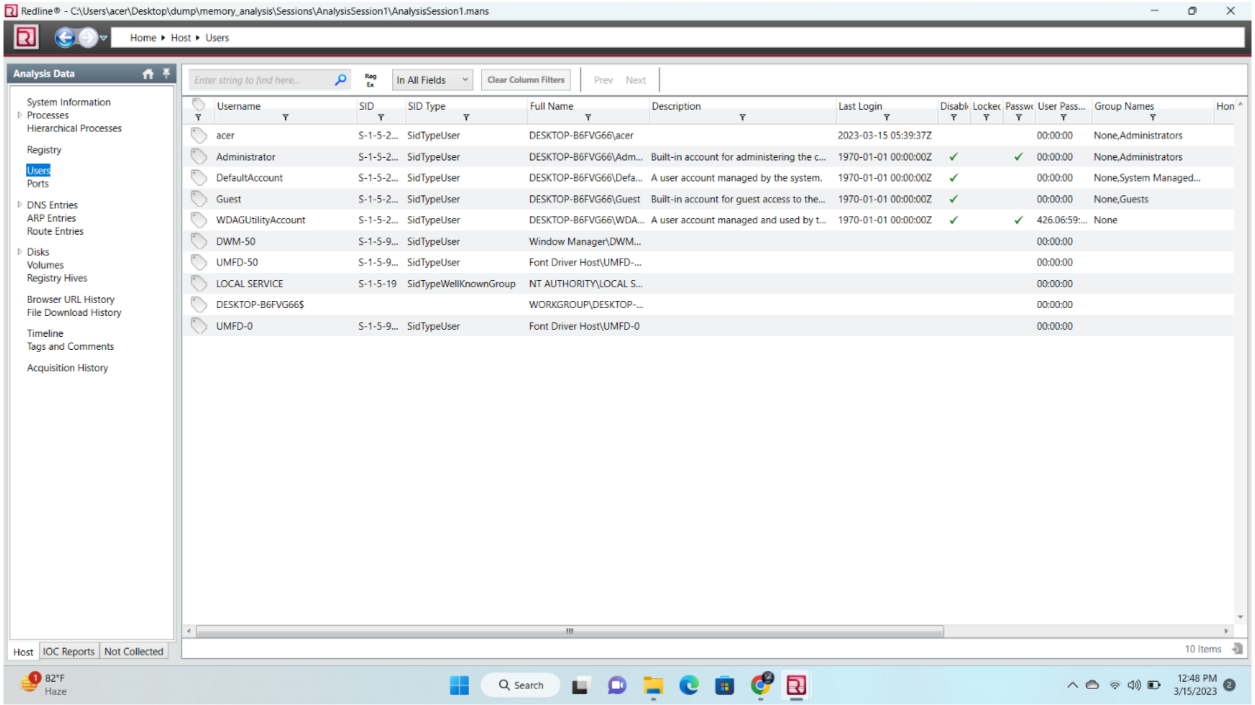
Registered Owner:	acer
Registered Organization:	Not Available
Domain:	WORKGROUP

Process Details:



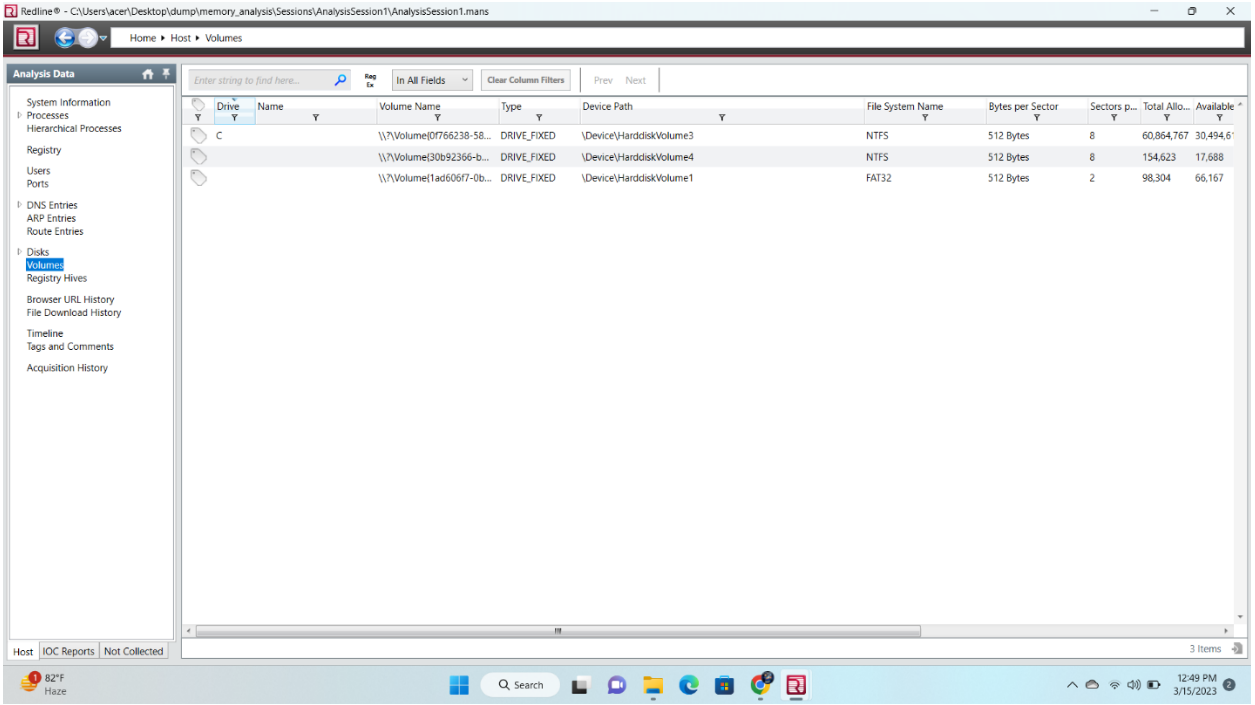
Process Name	PID	Path	Arguments	Username	Start Time	Kernel Ti...	User Time...	Security...
RstMwService.exe	3992	C:\WINDOWS\System32\DriverStore\FileRepository\iastorac.inf...	C:\WINDOWS\System32\DriverSto...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:01	00:00:00	S-1-5-18
svchost.exe	6788	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\LOCAL SERVI...	2023-02-20 14:04:09Z	00:00:21	00:00:16	S-1-5-19
IntelCpHDCPSvc.exe	3960	C:\WINDOWS\System32\DriverStore\FileRepository\iigd_dch.in...	C:\WINDOWS\System32\DriverSto...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:00	00:00:00	S-1-5-18
SecurityHealthSystray.exe	1900	C:\Windows\System32	"C:\Windows\System32\SecurityH...	DESKTOP-B6FVG66\acer	2023-03-15 05:39:55Z	00:00:00	00:00:00	S-1-5-2...
vmnat.exe	3984	C:\WINDOWS\SysWOW64	C:\WINDOWS\SysWOW64\vmnat....	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:24	00:00:12	S-1-5-18
svchost.exe	1588	C:\WINDOWS\System32	C:\WINDOWS\System32\svchost.e...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:05Z	00:00:08	00:00:16	S-1-5-18
vmnetdhcp.exe	3952	C:\WINDOWS\SysWOW64	C:\WINDOWS\SysWOW64\vmnetd...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:00	00:00:00	S-1-5-18
System	4			NT AUTHORITY\SYSTEM	2023-02-20 14:04:00Z	00:05:47	00:00:00	S-1-5-18
svchost.exe	1860	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:05Z	00:00:01	00:00:00	S-1-5-18
Registry	144			NT AUTHORITY\SYSTEM	2023-02-20 14:03:58Z	00:00:06	00:00:00	S-1-5-18
lsass.exe	324	C:\WINDOWS\system32	C:\WINDOWS\system32\lsass.exe	NT AUTHORITY\SYSTEM	2023-02-20 14:04:04Z	00:00:53	00:01:06	S-1-5-18
csrss.exe	820			NT AUTHORITY\SYSTEM	2023-02-20 14:04:03Z	00:00:05	00:00:01	S-1-5-18
MsMpEng.exe	4112			NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:01:55	00:05:50	S-1-5-18
smss.exe	552			NT AUTHORITY\SYSTEM	2023-02-20 14:04:00Z	00:00:00	00:00:00	S-1-5-18
svchost.exe	1752	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\LOCAL SERVI...	2023-02-20 14:04:05Z	00:00:01	00:00:01	S-1-5-19
svchost.exe	1104	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:04Z	00:03:16	00:00:08	S-1-5-18
msteams.exe	206...	C:\Program Files\WindowsApps\MicrosoftTeams_23034.1300.1...	"C:\Program Files\WindowsApps\...	DESKTOP-B6FVG66\acer	2023-03-15 05:40:02Z	00:00:01	00:00:00	S-1-5-2...
wininit.exe	928			NT AUTHORITY\SYSTEM	2023-02-20 14:04:04Z	00:00:00	00:00:00	S-1-5-18
chrome.exe	171...	C:\Program Files\Google\Chrome\Application	"C:\Program Files\Google\Chrome...	DESKTOP-B6FVG66\acer	2023-03-15 05:40:13Z	00:00:00	00:00:00	S-1-5-2...
svchost.exe	3904	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\LOCAL SERVI...	2023-02-20 14:04:06Z	00:00:02	00:00:00	S-1-5-19
WavesSysSvc64.exe	3296	C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo...	C:\WINDOWS\System32\DriverSto...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:00	00:00:00	S-1-5-18
svchost.exe	3896	C:\WINDOWS\System32	C:\WINDOWS\System32\svchost.e...	NT AUTHORITY\SYSTEM	2023-02-20 14:04:06Z	00:00:19	00:00:17	S-1-5-18
svchost.exe	3320	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e...	NT AUTHORITY\LOCAL SERVI...	2023-02-20 14:04:05Z	00:01:06	00:00:38	S-1-5-19
svchost.exe	1596	C:\WINDOWS\system32	C:\WINDOWS\system32\svchost.e	NT AUTHORITY\LOCAL SERVI	2023-02-20 14:04:05Z	00:00:01	00:00:02	S-1-5-19

Users Details:



Username	SID	SID Type	Full Name	Description	Last Login	Disabl	Lockec	Passw	User Pass...	Group Names	Hon
acer	S-1-5-2...	SidTypeUser	DESKTOP-B6FVG66\acer		2023-03-15 05:39:37Z				00:00:00	None,Administrators	
Administrator	S-1-5-2...	SidTypeUser	DESKTOP-B6FVG66\Adm...	Built-in account for administering the c...	1970-01-01 00:00:00Z	✓		✓	00:00:00	None,Administrators	
DefaultAccount	S-1-5-2...	SidTypeUser	DESKTOP-B6FVG66\Defa...	A user account managed by the system.	1970-01-01 00:00:00Z	✓			00:00:00	None,System Managed...	
Guest	S-1-5-2...	SidTypeUser	DESKTOP-B6FVG66\Guest	Built-in account for guest access to the...	1970-01-01 00:00:00Z	✓			00:00:00	None,Guests	
WDAGUtilityAccount	S-1-5-2...	SidTypeUser	DESKTOP-B6FVG66\WDA...	A user account managed and used by t...	1970-01-01 00:00:00Z	✓		✓	426.06:59:...	None	
DWM-50	S-1-5-9...	SidTypeUser	Window Manager\DWM...						00:00:00		
UMFD-50	S-1-5-9...	SidTypeUser	Font Driver Host\UMFD-...						00:00:00		
LOCAL SERVICE	S-1-5-19	SidTypeWellKnownGroup	NT AUTHORITY\LOCAL S...						00:00:00		
DESKTOP-B6FVG66$			WORKGROUP\DESKTOP-...						00:00:00		
UMFD-0	S-1-5-9...	SidTypeUser	Font Driver Host\UMFD-0						00:00:00		

Volume Details:



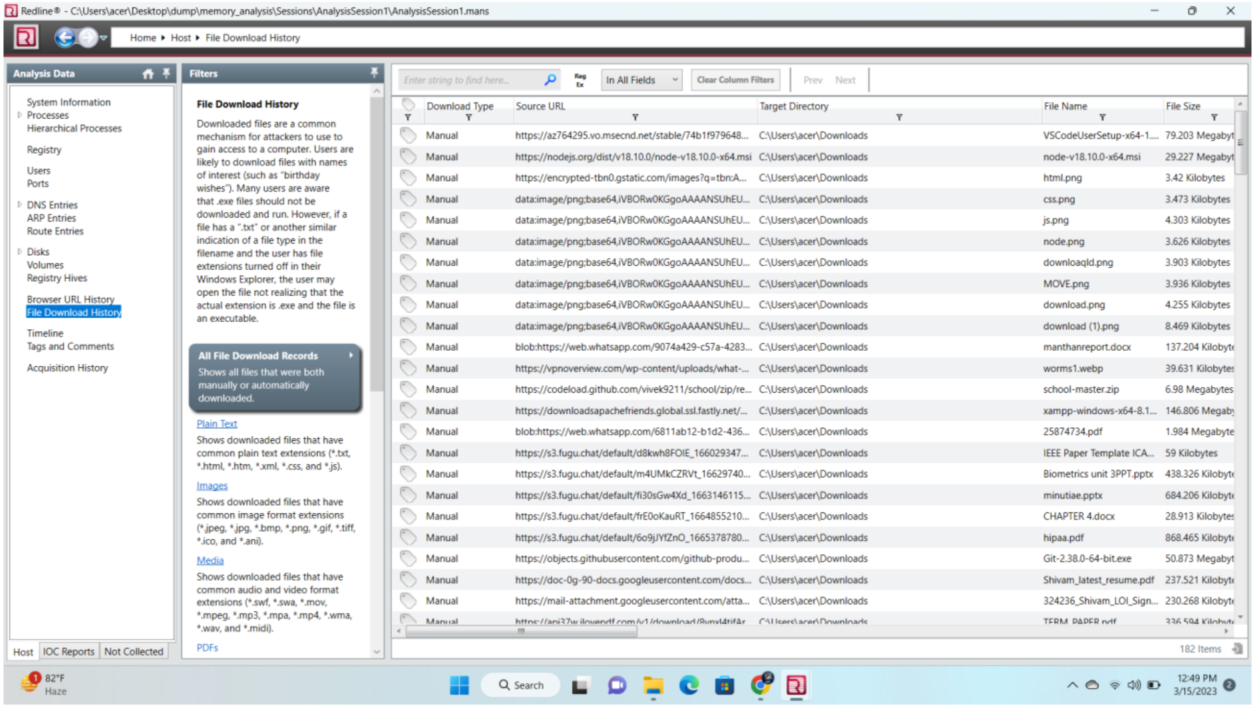
Redline® - C:\Users\acer\Desktop\dump\memory_analysis\Sessions\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ Volumes

Drive	Name	Volume Name	Type	Device Path	File System Name	Bytes per Sector	Sectors p...	Total Allo...	Available
C		\\?\Volume{0f766238-58...	DRIVE_FIXED	\Device\HarddiskVolume3	NTFS	512 Bytes	8	60,864,767	30,494,6
		\\?\Volume{30b92366-b...	DRIVE_FIXED	\Device\HarddiskVolume4	NTFS	512 Bytes	8	154,623	17,688
		\\?\Volume{1ad606f7-0b...	DRIVE_FIXED	\Device\HarddiskVolume1	FAT32	512 Bytes	2	98,304	66,167

3 Items

Download History Details:



Redline® - C:\Users\acer\Desktop\dump\memory_analysis\Sessions\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ File Download History

File Download History

Downloaded files are a common mechanism for attackers to use to gain access to a computer. Users are likely to download files with names of interest (such as "birthday wishes"). Many users are aware that .exe files should not be downloaded and run. However, if a file has a ".txt" or another similar indication of a file type in the filename and the user has file extensions turned off in their Windows Explorer, the user may open the file not realizing that the actual extension is .exe and the file is an executable.

All File Download Records
Shows all files that were both manually or automatically downloaded.

Plain Text
Shows downloaded files that have common plain text extensions (*.txt, *.html, *.htm, *.xml, *.css, and *.js).

Images
Shows downloaded files that have common image format extensions (*.jpeg, *.jpg, *.bmp, *.png, *.gif, *.tiff, *.ico, and *.ani).

Media
Shows downloaded files that have common audio and video format extensions (*.swf, *.swa, *.mov, *.mpeg, *.mp3, *.mpa, *.mp4, *.wma, *.wav, and *.midi).

PDFs

Download Type	Source URL	Target Directory	File Name	File Size
Manual	https://az764295.vo.msecnd.net/stable/74b1f979648...	C:\Users\acer\Downloads	VSCodeUserSetup-x64-1....	79.203 Megabyt
Manual	https://nodejs.org/dist/v18.10.0/node-v18.10.0-x64.msi	C:\Users\acer\Downloads	node-v18.10.0-x64.msi	29.227 Megabyt
Manual	https://encrypted-tbn0.gstatic.com/images?q=tbn:A...	C:\Users\acer\Downloads	html.png	3.42 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	css.png	3.473 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	js.png	4.303 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	node.png	3.626 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	downloaqld.png	3.903 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	MOVE.png	3.936 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	download.png	4.255 Kilobytes
Manual	data:image/png;base64,iVBORw0KGgoAAAANSUhEU...	C:\Users\acer\Downloads	download (1).png	8.469 Kilobytes
Manual	blob:https://web.whatsapp.com/9074a429-c57a-4283...	C:\Users\acer\Downloads	manthanreport.docx	137.204 Kilobyte
Manual	https://vpnoverview.com/wp-content/uploads/what-...	C:\Users\acer\Downloads	worms1.webp	39.631 Kilobytes
Manual	https://codeload.github.com/vivek9211/school/zip/re...	C:\Users\acer\Downloads	school-master.zip	6.98 Megabytes
Manual	https://downloadsapachefriends.global.ssl.fastly.net/...	C:\Users\acer\Downloads	xampp-windows-x64-8.1...	146.806 Megaby
Manual	blob:https://web.whatsapp.com/6811ab12-b1d2-436...	C:\Users\acer\Downloads	25874734.pdf	1.984 Megabyte
Manual	https://s3.fugu.chat/default/d8kwh8FOIE_166029347...	C:\Users\acer\Downloads	IEEE Paper Template ICA...	59 Kilobytes
Manual	https://s3.fugu.chat/default/m4UMkCZRVt_16629740...	C:\Users\acer\Downloads	Biometrics unit 3PPT.pptx	438.326 Kilobyte
Manual	https://s3.fugu.chat/default/fi30sGw4Xd_1663146115...	C:\Users\acer\Downloads	minutiae.pptx	684.206 Kilobyte
Manual	https://s3.fugu.chat/default/frE0oKauRT_1664855210...	C:\Users\acer\Downloads	CHAPTER 4.docx	28.913 Kilobytes
Manual	https://s3.fugu.chat/default/6o9jJYfZnO_1665378780...	C:\Users\acer\Downloads	hipaa.pdf	868.465 Kilobyte
Manual	https://objects.githubusercontent.com/github-produ...	C:\Users\acer\Downloads	Git-2.38.0-64-bit.exe	50.873 Megabyt
Manual	https://doc-0g-90-docs.googleusercontent.com/docs...	C:\Users\acer\Downloads	Shivam_latest_resume.pdf	237.521 Kilobyte
Manual	https://mail-attachment.googleusercontent.com/atta...	C:\Users\acer\Downloads	324236_Shivam_LOI_Sign...	230.268 Kilobyte
Manual	https://api37w.ilovepdf.com/v1/download/8vnxl4tifAr	C:\Users\acer\Downloads	TERM_PAPER.pdf	336.594 Kilobyte

182 Items

4. References

1. Burdach, M. (2005, July 9). An Introduction to Windows memory forensic. Retrieved October 25, 2008, from http://forensic.seccure.net/
2. Guidance Software. (2008). Computer Forensics. Retrieved March 3, 2009, from http://www.guidancesoftware.com/
3. https://fireeye.market.com