Parul University

FACULTY OF ENGINEERING AND TECHNOLOGY

BACHELOR OF TECHNOLOGY

REVERSE ENGINEERING AND MALWARE ANALYSIS LABORATORY (303105389)

6th SEMESTER

COMPUTER SCIENCE & ENGINEERING DEPARTMENT
Cyber Security

Laboratory Manual

Session:2025-26

CERTIFICATE

This is to certify that Mr./Ms. **TUTA JEEVITH SWARUP** with enrollment no **2303031260232** has successfully completed his/her laboratory experiments in the **Reverse Engineering and Malware Analysis (303105390)** from the department of COMPUTER SCIENCE & ENGINEERING during the academic year **2025-2026**.

Date of Submission:..... Staff In charge:.....

Head Of Department:.....

Practical Assessment Table

Sr. No.	Practical Title	Page No.		Marks (10)	Sign
		From	To		
1.	Lab Setup for Reverse Engineering and Malware Analysis				
2.	Static Analysis Techniques				
3.	Dynamic Analysis Techniques				
4.	Malware Obfuscation and Packing Techniques				
5.	Code Analysis and Disassembly				
6.	Malware Persistence and Anti-Analysis Techniques				
7.	Network Analysis and Traffic Inspection				
8.	Memory Analysis and Malware Behavior				
9.	Advanced Malware Analysis Techniques				
10.	Incident Response and Forensics				

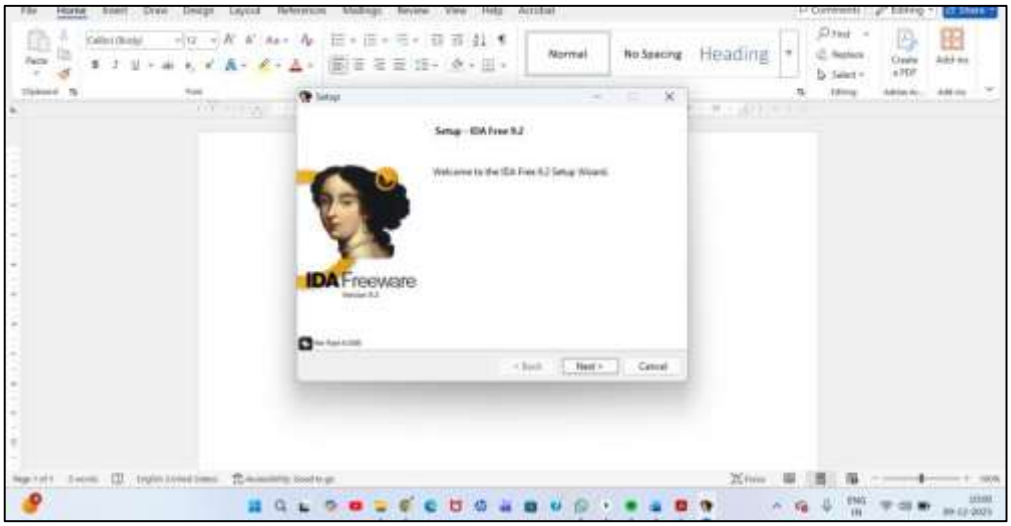
PRACTICAL 1

Aim:- Lab Setup for Reverse Engineering and Malware Analysis.

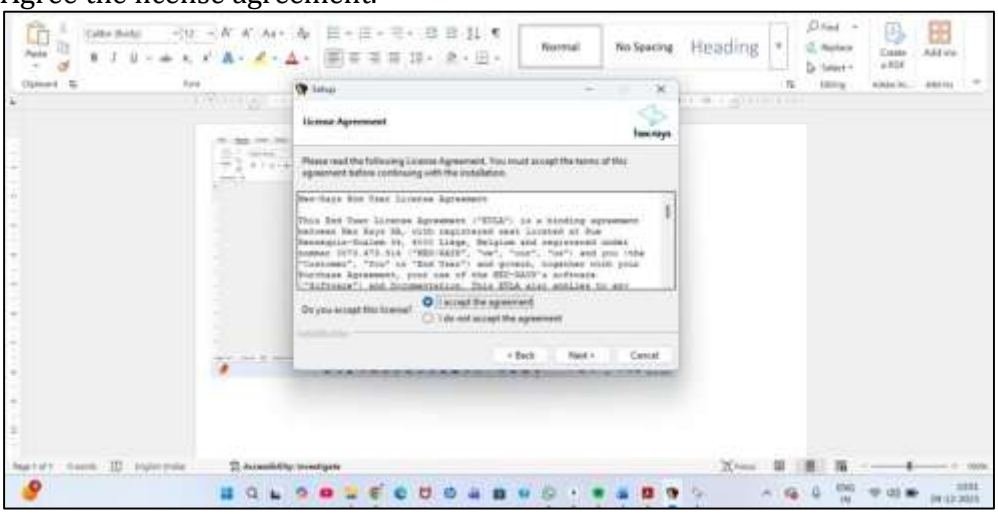
Tools:-

1) **IDA FREE:- IDA Free** is a free software tool used to study and understand executable programs. It changes compiled files into assembly language so that we can see how a program works without running it. It is mainly used in cybersecurity and malware analysis, but it has fewer features than the paid IDA Pro version.

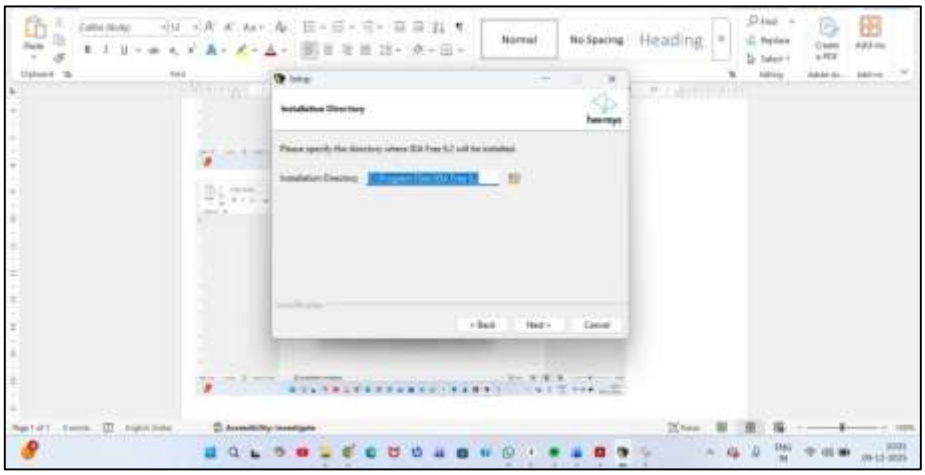
- Open browser and search IDA Freeware download, and then download it.
- Setup the downloaded file.
- The setup dialogue box will appear , select next.



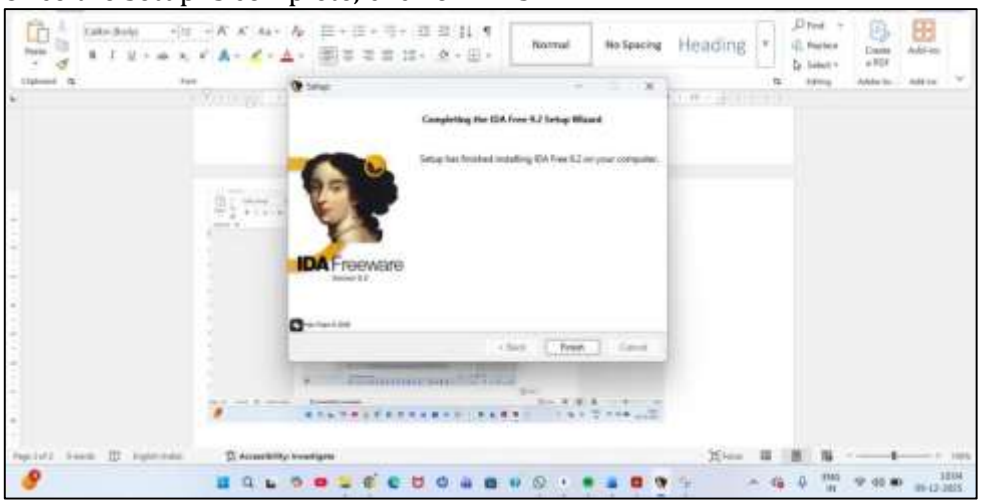
- Agree the license agreement.



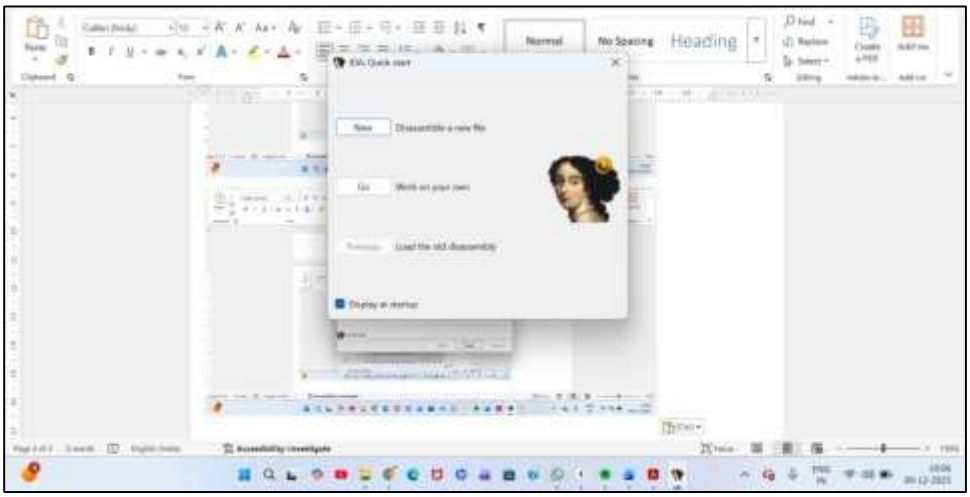
- Choose file location for the software.

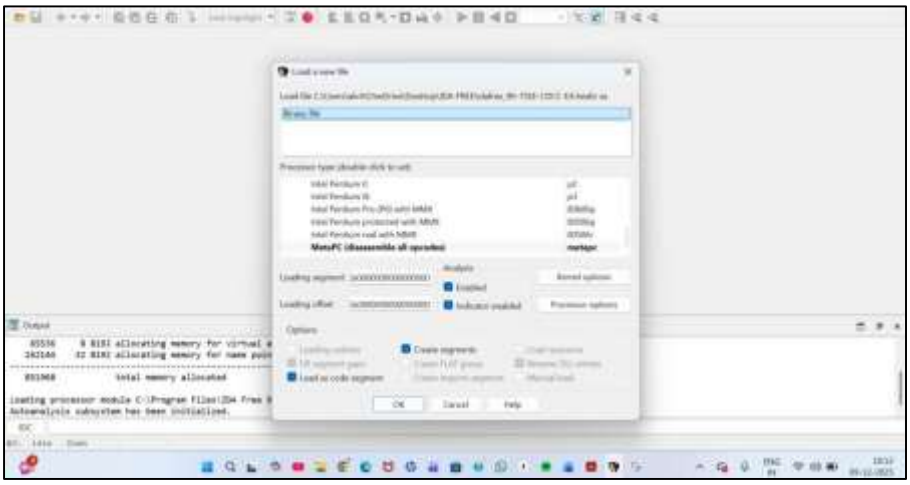


- Once the setup is complete, click on finish.



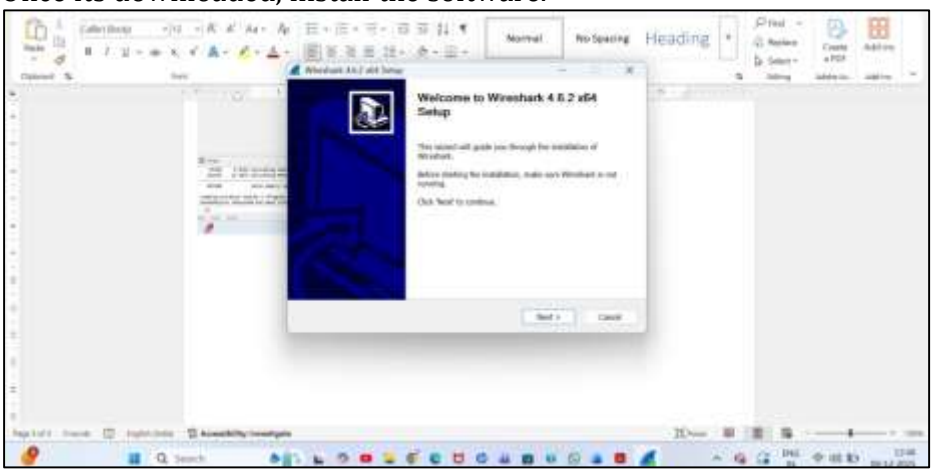
- Launch IDA Freeware.



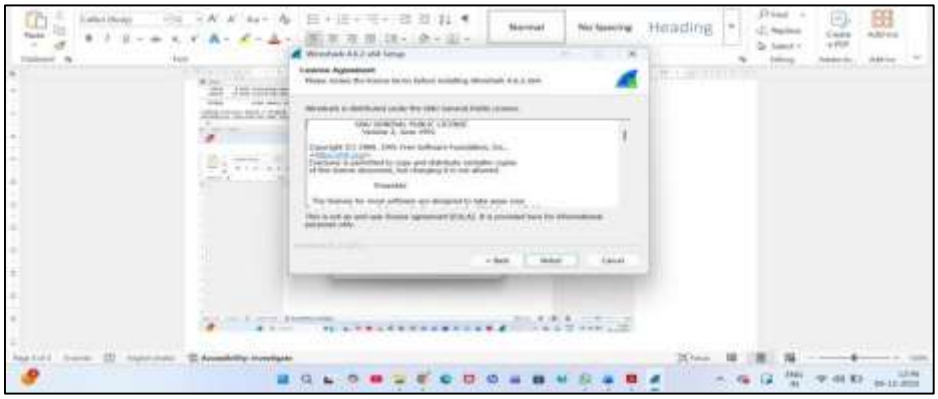


2) **WIRESHARK:** Wireshark is a free and open-source network analysis tool used to capture and examine data packets traveling over a network. It helps users see how data is sent and received between devices in real time, which is useful for network troubleshooting, monitoring, and security analysis.

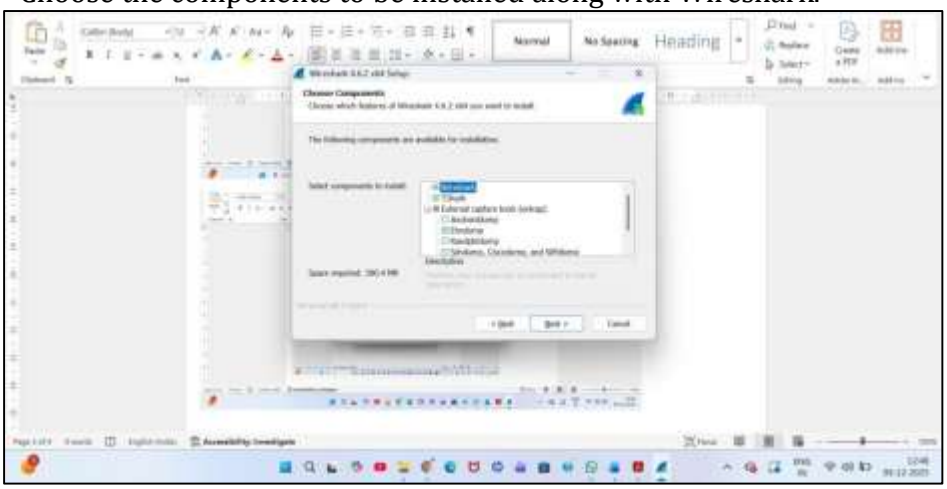
- Open browser and search for wireshark download.
- Once its downloaded, install the software.

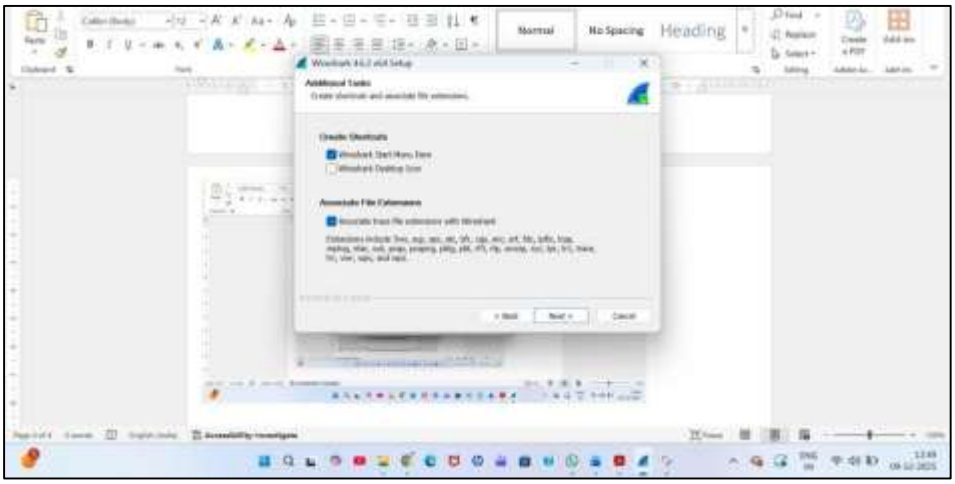


- Agree the license agreement by clicking on noted.



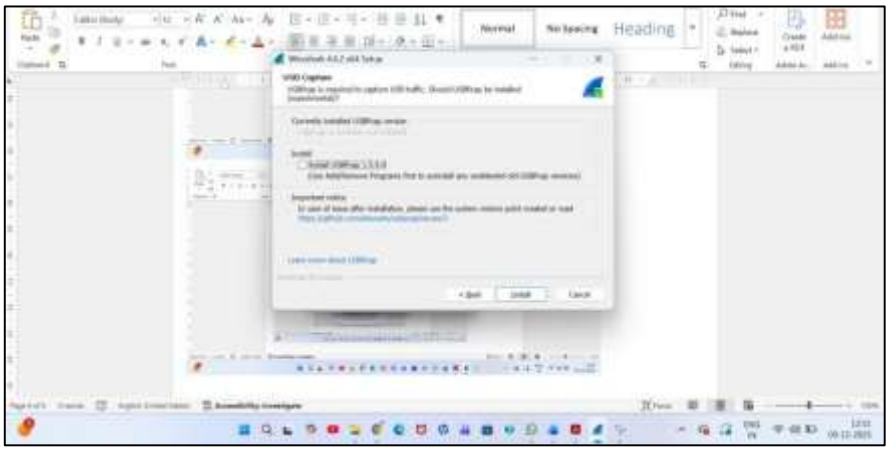
- Choose the components to be installed along with Wireshark.

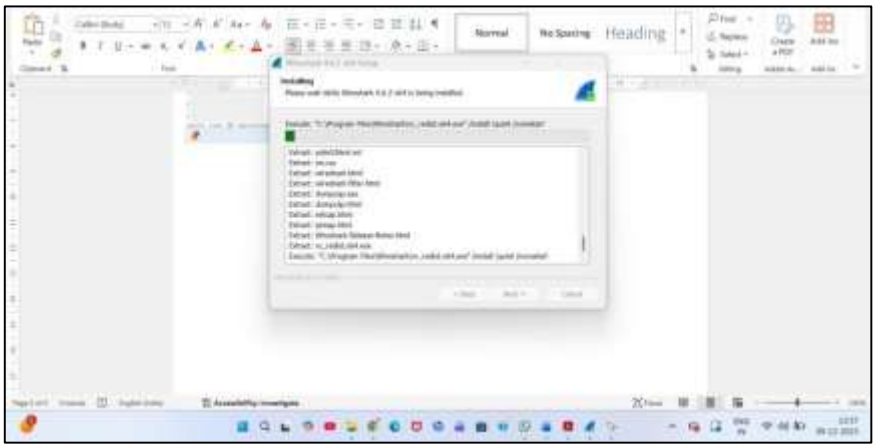


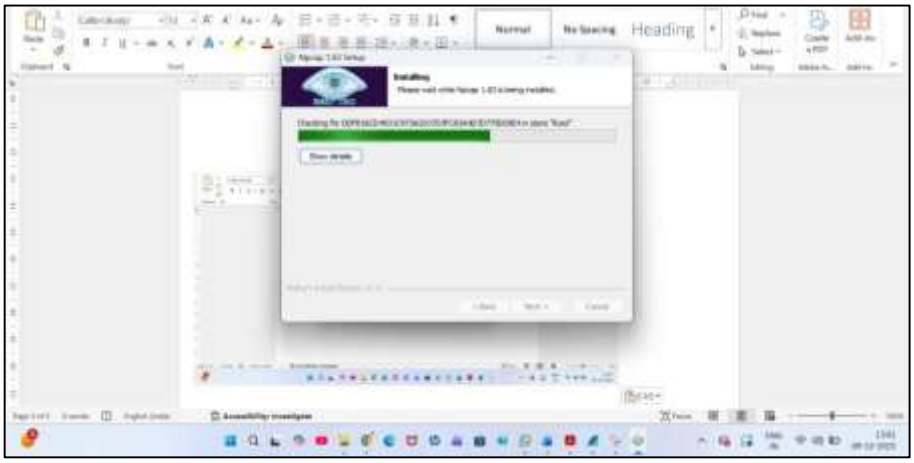


- Choose the location for installation of wireshark.

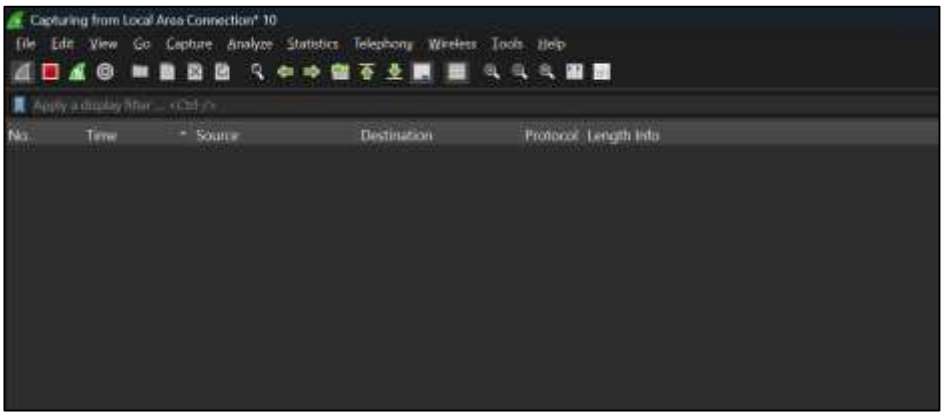
- Once the installation is complete, click on next and further complete the setup.





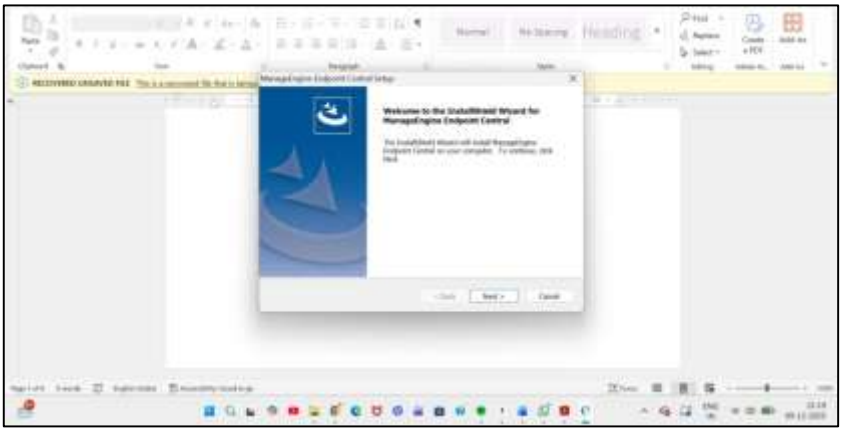


- Launch wireshark

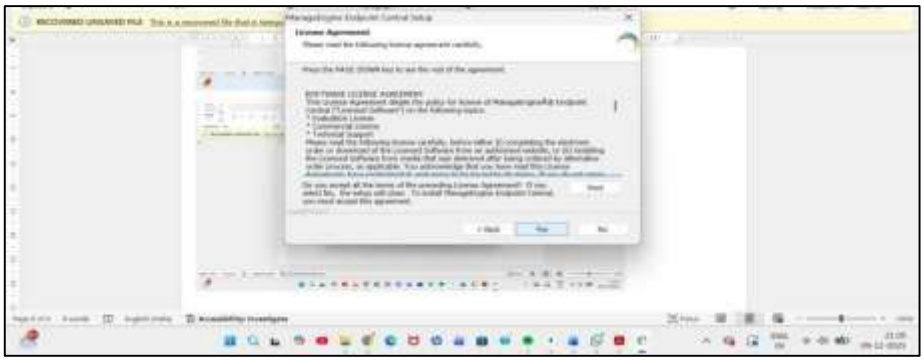


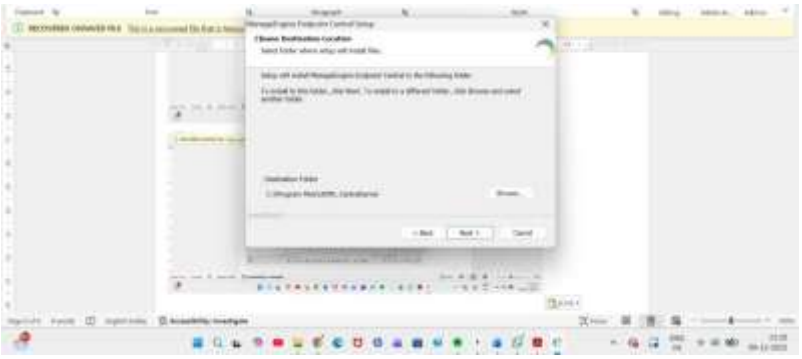
3) **PROCESS MONITOR:** Process Monitor is a Windows tool used to monitor system-level activities and capture the real-time runtime behavior of processes. It provides detailed information about file system access, registry changes, and process activity, making it useful for digital forensics, malware analysis, and system troubleshooting.

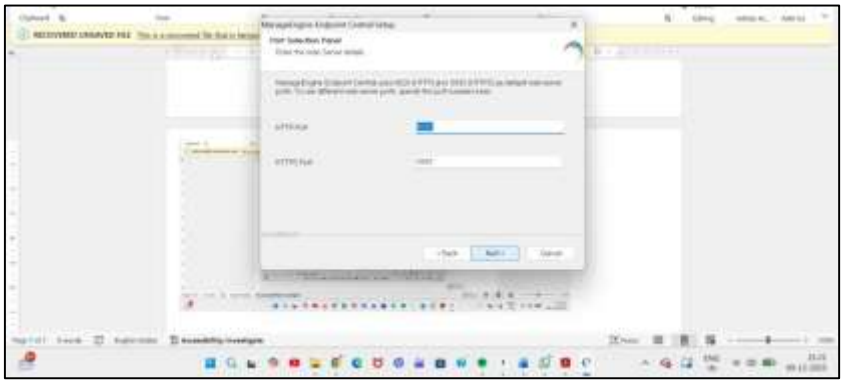
- Open browser and search for process monitor .
- Once its downloaded, install the software.

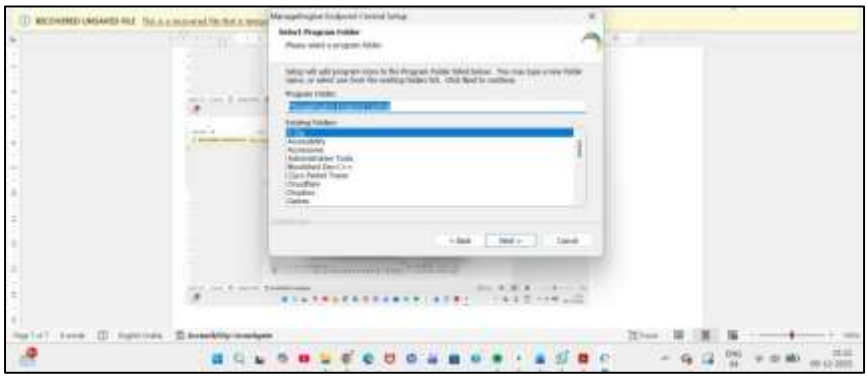


- Agree the license agreement by clicking on noted.



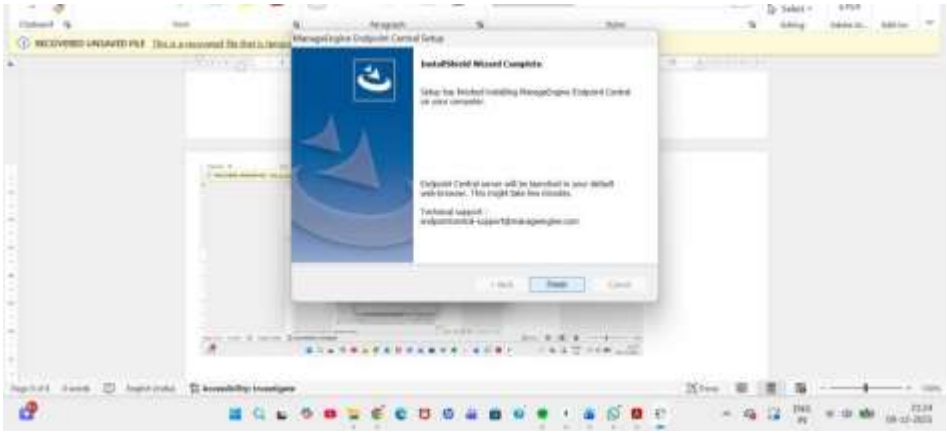







ManageEngine Endpoint Central Setup
Installing
C:\...\data2.cab
Cancel

- Launch process monitor.

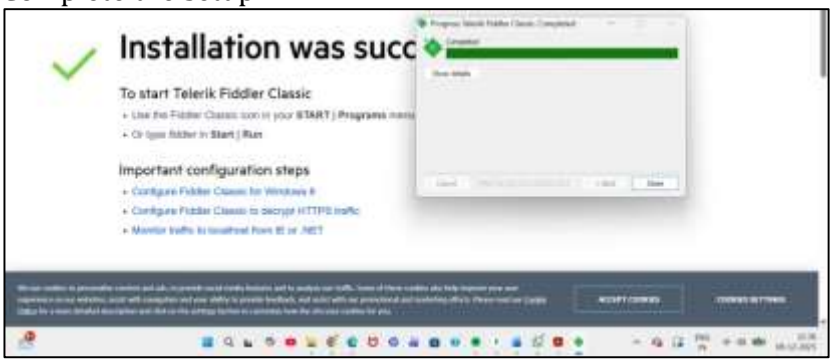


4) **FIDDLER:** Fiddler is a web debugging and traffic analysis tool used to capture, inspect, and analyze HTTP and HTTPS network traffic between a client (such as a web browser or application) and a server. It helps security analysts and forensic investigators understand how data is transmitted over the network and detect suspicious, malicious, or unauthorized communication.

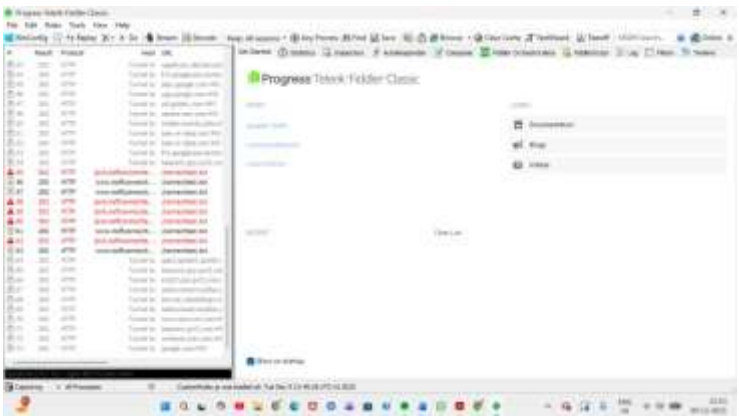
- Open browser and search for Fiddler download and then download it.
- Upon downloading, install it firstly by agreeing the license agreement.

- Choose installation options.

- Complete the setup.



- Launch Fiddler.



CONCLUSION:- The lab setup required for performing practical exercises in **reverse engineering and malware analysis** has been **successfully completed**, ensuring a safe and functional environment for hands-on analysis and learning.

PRACTICAL 2

Aim:- Static Analysis Techniques
- File format analysis (PE, ELF, etc.)
- Identifying and extracting resources from executables.

Strings analysis and identifying suspicious patterns

THEORY : What is Ransomware?

- Ransomware is malicious software that affects your device by encrypting your files and data or locking your system. After the successful setup of ransomware into the system, attackers demand ransom in exchange for decryption code.

The main objective of ransomware is –

(1) to get unauthorized access to the system and encrypt it.
(2) to get financial greed from the victims' ransom. Ransomware Analysis Technique:

Tools Used For Ransomware Analysis:

- CFF Explore
- Pestudio
- PEid
- Hex Editor
- Hash calc
- ExeInfo
- Process Monitor
- Process Explorer
- Process Hacker
- Fidller
- Regshot
- Wireshark
- Procmon
- CRSTATIC

STATIC ANALYSIS:

- It is collecting information about the malicious application without running it. The objective of static analysis is to collect as much metadata as possible like strings, and PE Header. Static analysis can be fast by examining the features of an executable ransomware code and matching it to a previously observed malicious code. For analysis, there is no need to click on the sample file just drag and drop the sample file to the selected tool. The malicious code is easily and quickly analyzed. The entire static analysis has been done on windows 10 in VMWare for safety purposes. For Static analysis, we used various tools using the FlareVm package and extract as much as information possible and extract the information that seems valuable for further analysis.

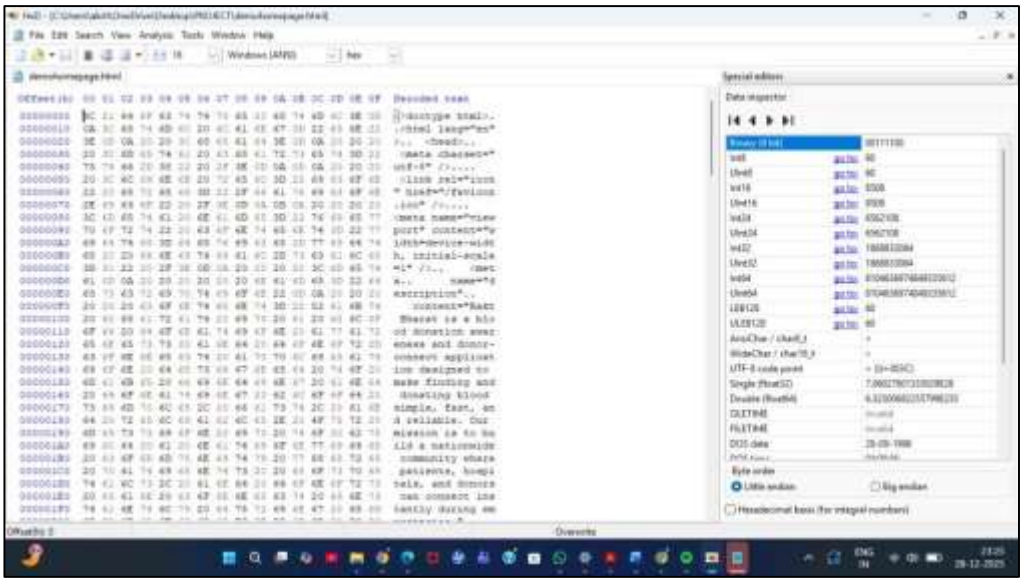
- Static analysis is a step-by-step procedure that elaborates as under

Step 1 : File Identification:-

- Any unknown file could be an executable file or not. Starting analysis of any ransomware sample by identifying its file type. It could be a portable executable or not. Executables are encoded instruction that gives the computer to perform the indicated tasks. EXE is a PE format used for windows, ELF is used for Linux, and Mach-OS used for MacOS and IOS.

- For identification of file type, we can use the tools like-

- Hex Editor(HxD)
- Pestudio
- CFF Explorer



The used sample is a Portable Executable file confirmed by results from hex editor-

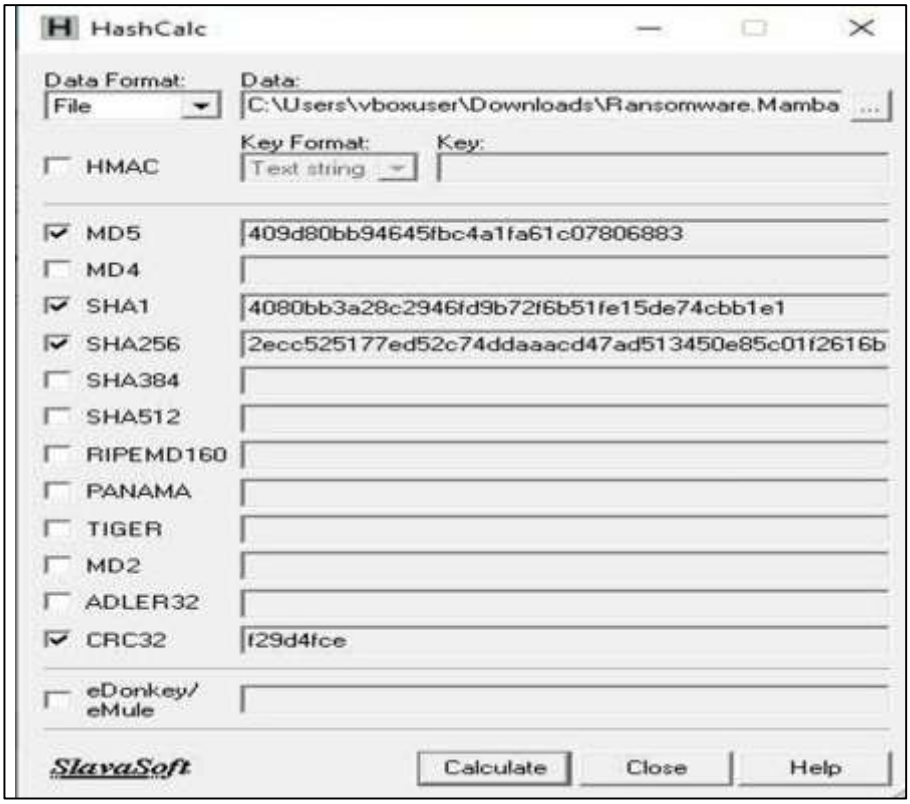
- In first two bytes we can see 4D 5A and in decode text MZ which represented that file is PE(Portable executable).
- This program cannot be run in DOS mode' which is also denoted PE file.
- PE header starts from 50 45 of binary offsets.

Step 2 : Malware Hashing:

- Malware hashing is a process of generating a unique fingerprint of a file. For performing any digital analysis, hashing is a crucial part. Hashes are also crucial in cryptography to verify whether or not data has been altered. Any bit flip could theoretically result in a different hash value being calculated. All data files used as evidence in court are instantly hashed to demonstrate their integrity. The hash value is like a fingerprint for any file. In

malware hashing, we can generate the cryptographic hash value of malware files by using tools like Hashcalc and Hash my files.

- Hash values could be in form of different Hashing algorithms like MD5, SHA 1, SHA256, SHA512, CR2C, etc.



Here we used MD5, SHA 1, and SHA 256.

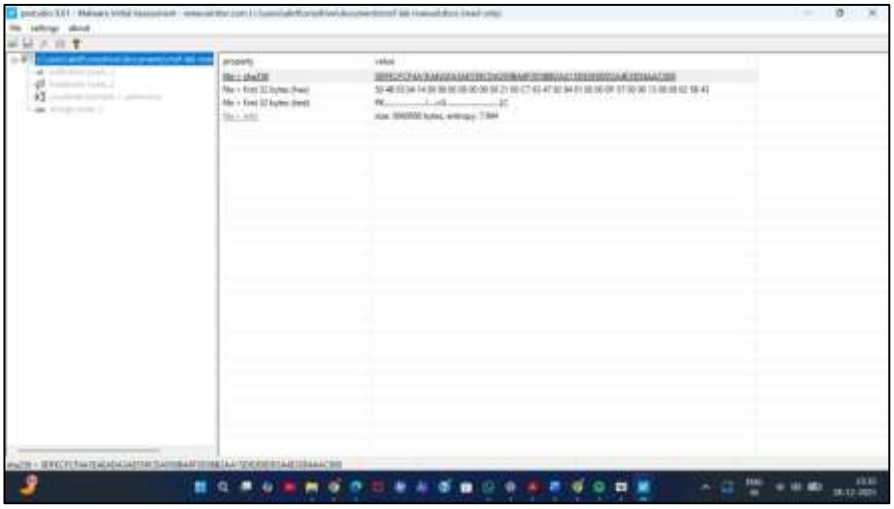
These hash values are useful for an investigation the Investigator can get information on whether the sample was previously analyzed or not by searching these hash values on websites like virus total and hybrid analysis.

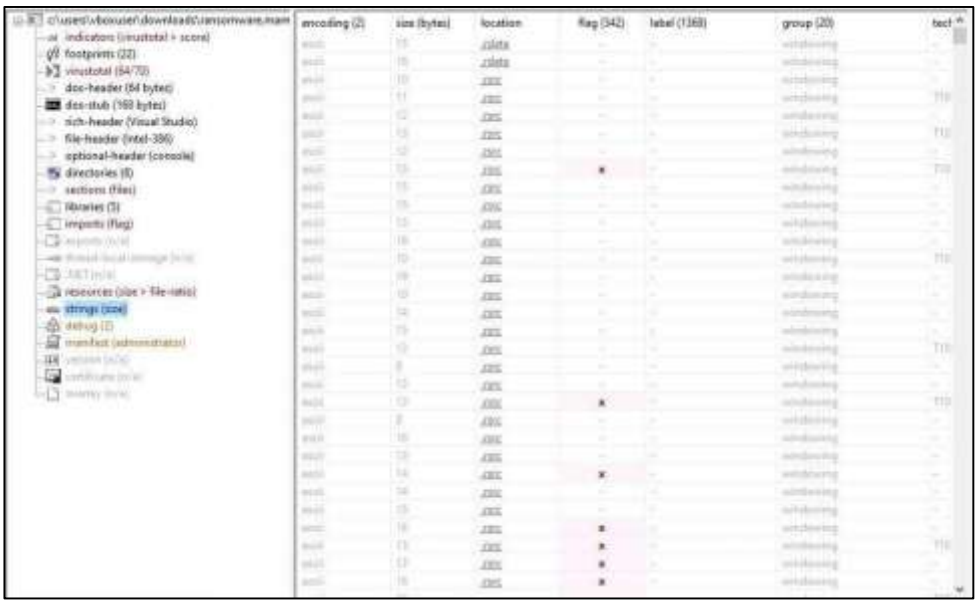
Step 3 : String Analysis:-

- String analysis is the process of extracting readable characters and words from the sample file. String analysis gives a glimpse of what ransomware can do to the system. Strings are in form of ASCII and Unicode-printable sequences of characters lodged within a file. Extracting strings can give clues about the program functionality and indicators associated with a suspect binary. For example, if malware creates a file, the filename is stored as a string in the binary. Or, if malware resolves a domain name controlled by the attacker, then the domain name is stored as a string. Strings extracted from the binary can contain references to filenames, URLs, domain names, IP addresses, attack commands, registry

keys, and so on. Although strings do not give a clear picture of the purpose and capability of a file, they can give a hint about what malware is capable of doing 22,35,73.

For string analysis, we can use the tools like Pe studio, Detect it Easy, Peid.





- In the above picture, we can see that the red flags indicate some malicious strings which could be dangerous. The extracted attributes from strings are listed below.

Sr. no.	Malicious Strings
1.	CryptReleaseContext
2.	CryptAcquireContext
3.	CryptGetHashParam
4.	CryptCreateHash
5.	CryptDestroyHash
6.	GetUserObjectInformation
7.	SetDefaultDllDirectories
8.	GlobalAddAtom
9.	GetProcessWindowStation
10.	GetCursorPos
11.	SetCursorPor
12.	Hooking
13.	Execution Through API
14.	Process Injection

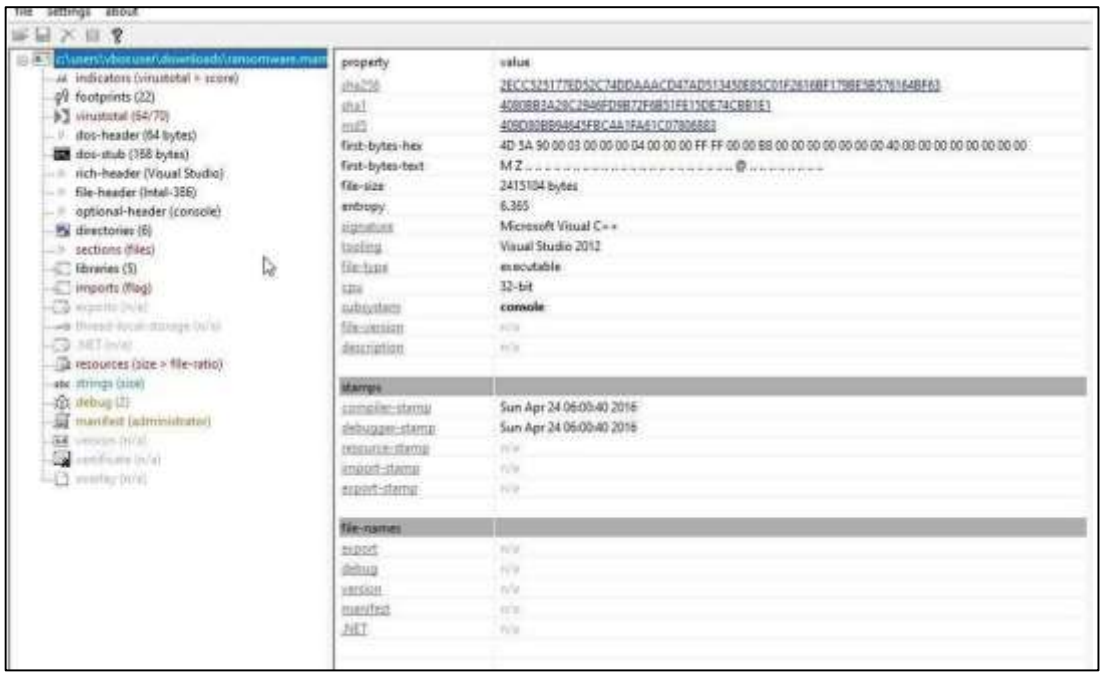
Step 4 : Packers: -

- Packers are used to compress the content of the Malware file. Packers can encrypt, compress or simply change the format of a malware file to make it look like something else entirely. Tools like UPX And EXE Info are used to pack or unpack the file. If the sample file is packed first we have to unpack it using UPX.

Step 5 : PE Header Analysis:-

- The Portable Executable (PE) file header contains the metadata about the executable file itself. At its bare minimum, it comprises the following: a DOS stub, a signature, the architecture of the file's code, a time stamp, a pointer, and various flags. PE Headers gives more Information about the functionality of the ransomware and ransomware interactions with the operating system. PE Header contains library and sections. PE Header contains all

instructions which are needed to run a particular program. So by analyzing the PE Header we can extract the important attributes and can know about the file functionality. Tools like Pe studio, CFF explorer, and Detect it easy are utilized to analyze PE Headers**.**



- We can analyze the dos header, dos stub, file header, optional header, directories, sections, library, overlay, etc. We analyze the sample file in the tool and detects it easy, we then found that the overlay was packed with the important instruction of the file that could be stored in the overlay.

Conclusion: Static analysis was successfully carried out by performing **file format analysis** and **systematically identifying and extracting important data from executable files**. This approach helped in understanding the internal structure, characteristics, and potential behavior of the executables **without executing them**, making the analysis safe and effective.

PRACTICAL 3

Aim:- Dynamic Analysis Techniques.
Setting up virtual environments for malware analysis
Process monitoring and hooking techniques
Behavioral analysis and monitoring system interactions

THEORY:

What is Ransomware?

- Ransomware is malicious software that affects your device by encrypting your files and data or locking your system. After the successful setup of ransomware into the system, attackers demand ransom in exchange for decryption code.

The main objective of ransomware is:-
(1) to get unauthorized access to the system and encrypt it.
(2) to get financial greed from the victims' ransom.

Ransomware Analysis Technique:

Tools Used For Ransomware Analysis:

- CFF Explore
- Pestudio
- PEid
- Hex Editor
- Hash calc
- ExeInfo
- Process Monitor
- Process Explorer
- Process Hacker
- Fidller
- Regshot
- Wireshark
- Procmon
- CRSTATIC

DYNAMIC ANALYSIS:

- Dynamic analysis is also called behavioral-based analysis. Malicious code was executed in a controlled and monitored environment, Sandbox is the best example of a safe environment. All actions were captured for analysis while running it. This type of analysis is less prone to evasiveness, and encrypted code can be analyzed. Malicious action must be part of the process to achieve its objective. Encrypted code is decrypted before the malware can perform its action. One of the setup behaviors of ransomware is environment mapping. If the analysis was performed using a virtual machine, which can cut costs and resources, the ransomware may discover this and prevent itself from exhibiting all its behaviors.

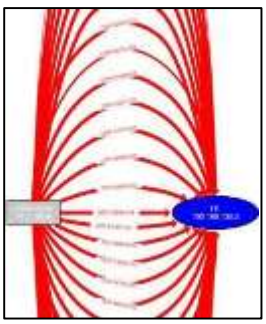
Registry Operations:

- A central structured database termed the Windows registry is used to hold required data to set up the system for one or more users, software, or physical devices. The System, Software, Security, and SAM registry are the four main registry files. Different data can be found under the tags in each registry file. File system folders and the Windows registry both have comparable organizational structures. Each registry holds a wealth of data that can be used in forensic investigations. The below-listed tools are employed to analyze the windows registry:

  - RegRipper.
  - ShellBags Explorer.
  - AmcacheParser.
  - AppCompatCacheParser.
  - JLECmd.
  - RecentFileCacheParser.
  - Computer Account Forensic Artifact Extractor (cafae)
  - Yet Another Registry Utility (yaru)

For this work we used Procmon and Regshot for registry analysis.

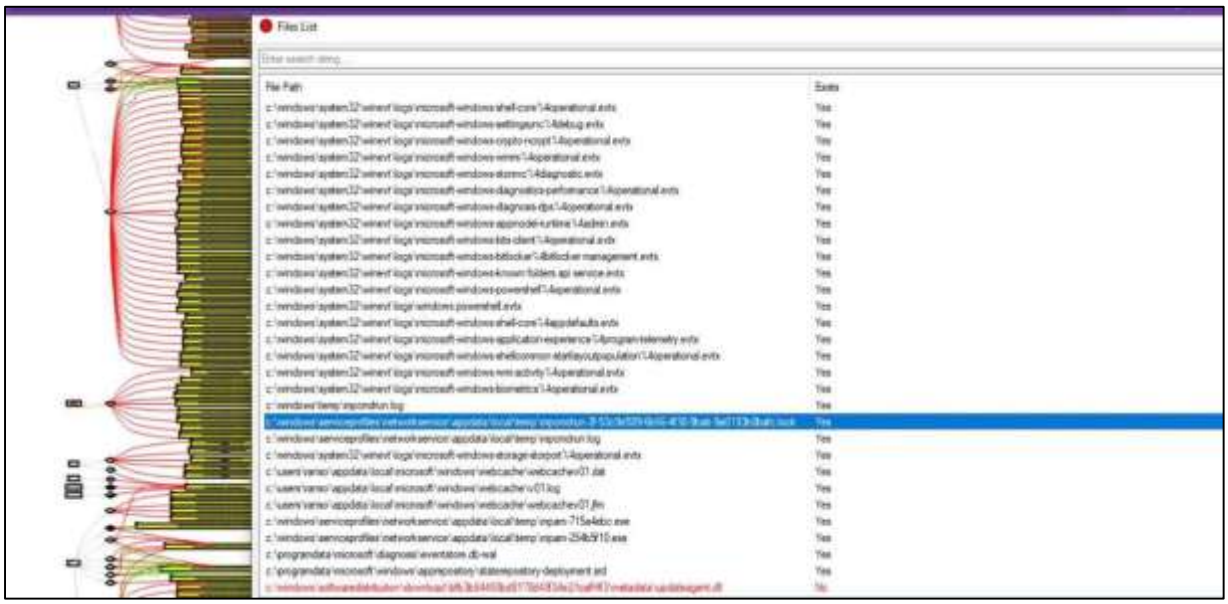
Suspicious keywords find out from the registry file which is listed below as shown in the above picture ”Bitlocker Drive Encryption” ”Bitlocker Data RecoveryAgent” “Document Encryption” “Windows Hello Key Encryption” etc. This Keywords or tags are not commonly present in every file.



A network monitoring solution should be able to detect activity indicative of ransomware attacks via insecure protocols. Our Sample file attempted to connect to a server using TCP and UDP packets caught by procmon and fiddler even while the network was disabled. Our malware's main objective is to establish a connection with a command and control server (C & C). C&C servers usually reside on trustworthy cloud providers, have brief lifespans, and use automated domain generation techniques to evade detection by law enforcement.

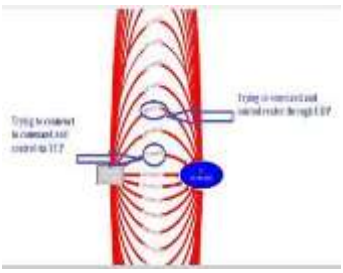
File Directory Operation:

- Crypto ransomware encrypts computer files in a number of methods. Demanding a ransom for the decryption key after encryption It begins by capturing screenshots of all currently running programs before searching for common file extensions. Add the arbitrary character at the end of each file name after that. finally, it replaces the previous ones. because it is difficult to discern the original file type from file names other than that. The observation in procmon file directories the finding of.Lock file extension which is not common for other files. A lock file is a file used by various operating systems and programs to lock a resource, such as a file or a device.

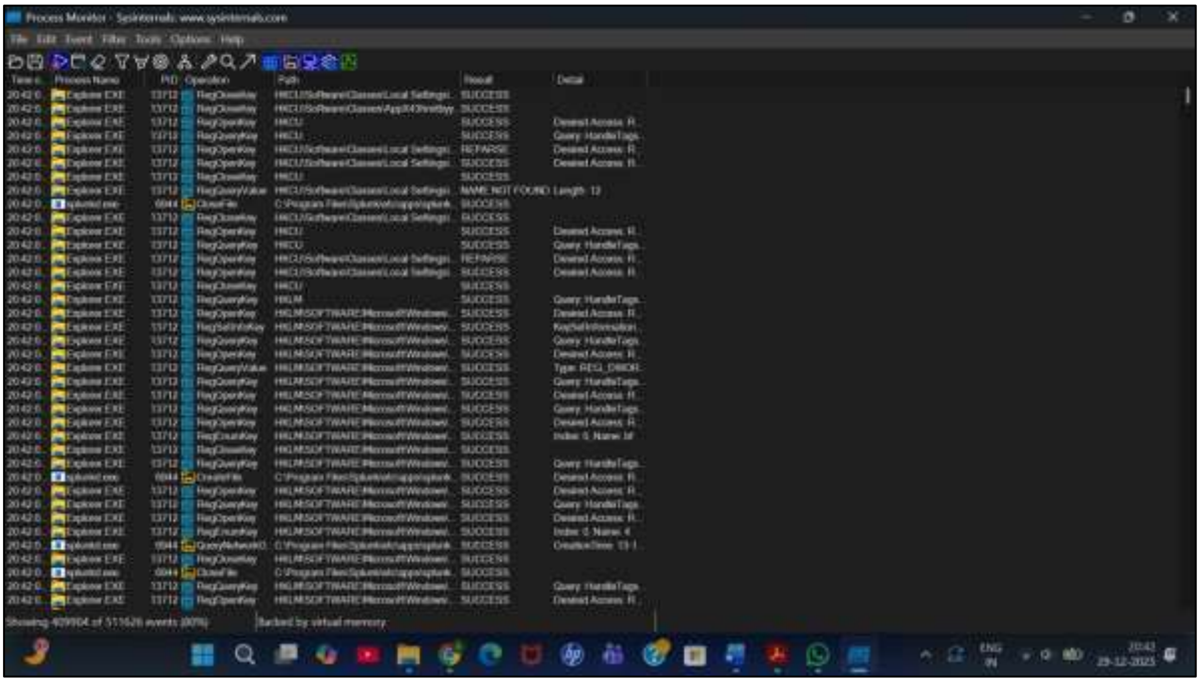


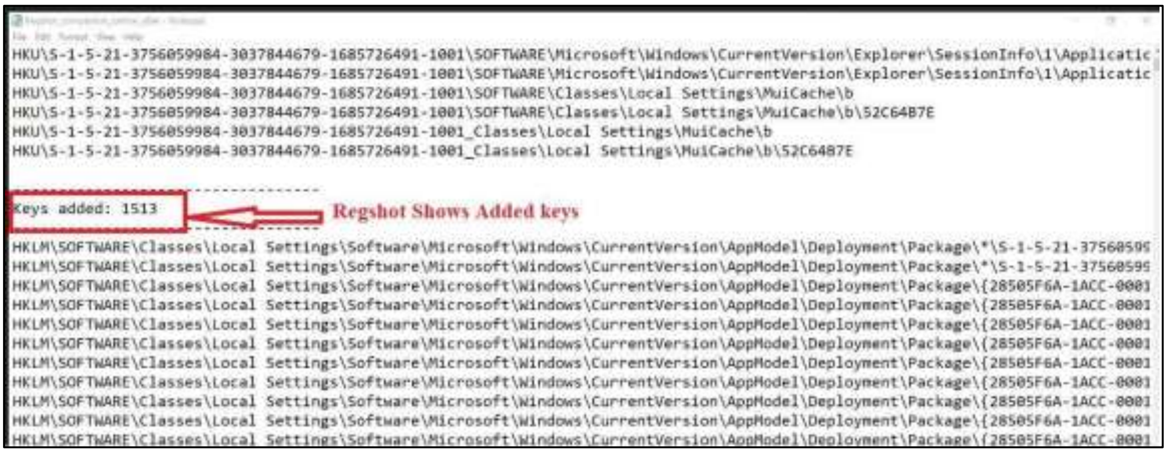
OBSERVATION:

- I have included a few screenshots from our research below, which demonstrate the features and functioning of the sample file:
- In below picture shows the Ransomware sample trying to connect with the C&C center via UDP and TCP servers even though Network is turned off.

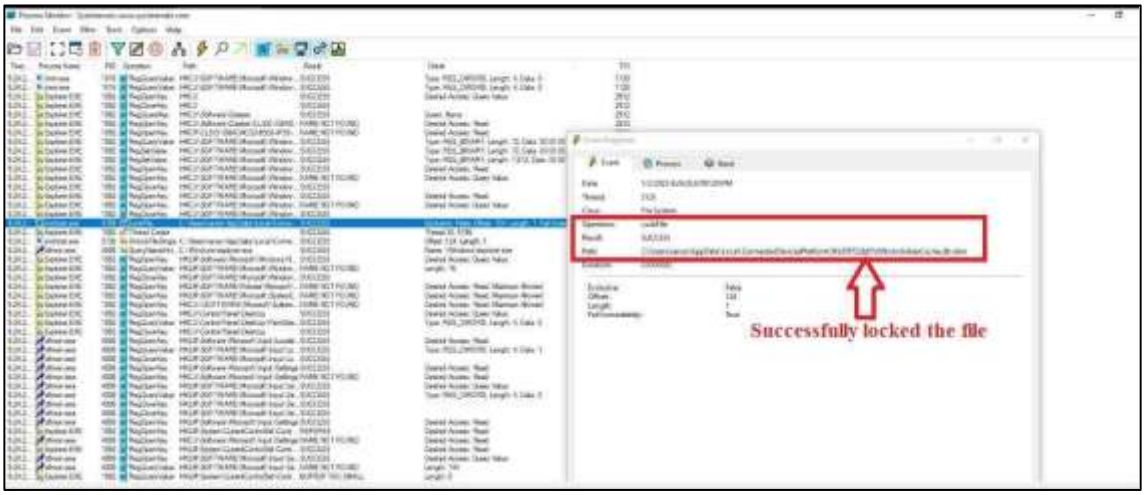


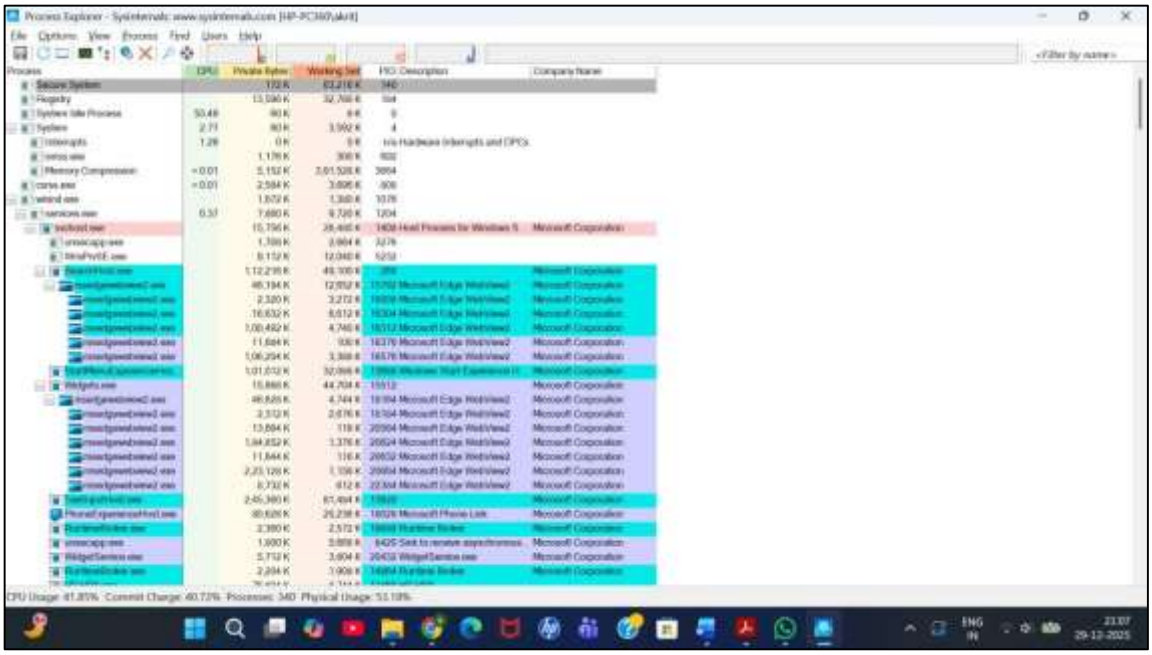
- The below picture shows the running activity while ransomware is executed. The log creates a thread is could be suspicious activity successfully performed by Ransomware.





- The registry files created by Regshot show the alteration of keys by comparing these two pictures.





RESULT AND DISCUSSION:

Sr no.	Analysis Technique	Analysis Tool	Applications	Result
1.	Dynamic Analysis	Process Explore	System monitoring tool, information about running process, DLL dependencies, performance graphs	Display the running process.
2.	Dynamic Analysis	Process Monitor	Real time data capturing, detailed information about system activity, monitor registry, process and network activity.	Shows all running process and its status. Oper of locked file.

3.	Dynamic Analysis	Process Hacker	Process priority control, view network activity, edit system service.	Shows all running process and status
4.	Dynamic Analysis	ProcDot	Display interactions betweens processes, system calls, registry access, analyze system behaviour	Shows the TCP and UDP connections, flowchart of network activity.lock exten in path of temp file.
5.	Dynamic Analysis	Autorun	System Configuration Utility	
6.	Dynamic Analysis	Wireshark	Network protocol analyzer	Shows network activity
7.	Dynamic Analysis	Regshot	Export registry changes, tresting software installation, save registry snapshots	Creat snapshot of a registry for further analysis. Find the changes in keys.
8.	Dynamic Analysis	Fiddler	Inspect incoming and outgoing data	Shows network activity.

CONCLUSION:- Dynamic analysis allows safe observation of malware behavior in real time using isolated virtual environments. Process monitoring and behavioral analysis help identify malicious activities and system interactions, enabling effective detection, understanding, and mitigation of malware threats.