



**National Forensic
Sciences University**

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

PROJECT REPORT

ON

**“Ransomware Forensics”
(Petya)**

Submitted To

**School of Cyber Security & Digital Forensics,
National Forensic Sciences University**

For partial fulfilment for the award of degree

MASTER OF SCIENCE

In

DIGITAL FORENSICS AND INFORMATION SECURITY

Submitted By

Jay K. Bhalodiya

012200300003014

Under the Supervision of

Dr. Nilay Mistry

**National Forensic Sciences University,
Gandhinagar Campus, Gandhinagar – 382009, Gujarat, India.**

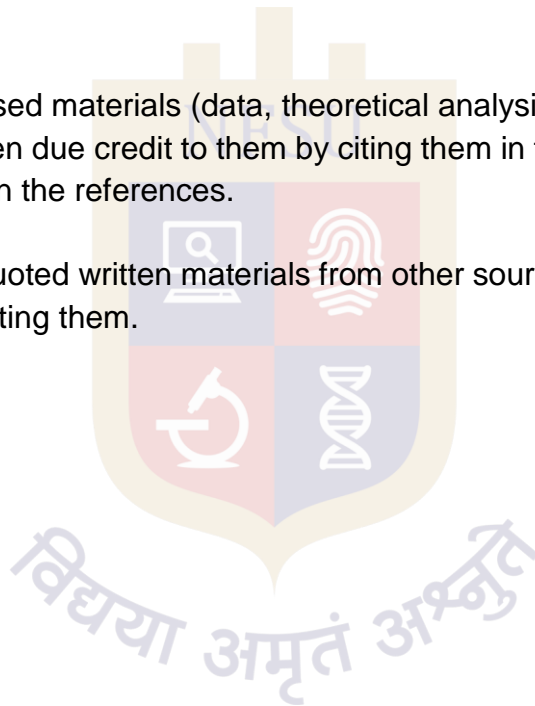
DECLARATION

I certify that,

- a) The work contained in the thesis is original and has been done by myself under the supervision of my supervisor.
- b) The work has not been submitted to any other Institute for any degree or diploma.
- c) I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.
- d) Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.
- e) Whenever I have quoted written materials from other sources and due credit is given to the sources by citing them.

Date:

Place:



(Jay K. Bhalodiya)

Enroll. No.: 012200300003014

**School of Cyber Security & Digital Forensics,
National Forensic Sciences University,
Gandhinagar Campus, Gandhinagar, Gujarat, India.**

CERTIFICATE

This is to certify that the work contained in the thesis entitled “**Ransomware Forensics**” submitted by **Jay K. Bhalodiya (Enroll. No.: 012200300003014)** for the award of the degree of **Master of Science in Digital Forensics and Information Security** to the **National Forensic Sciences University, Gandhinagar Campus**, is a record of bonafide research works carried out by him under my direct supervision and guidance.

I considered that the thesis has reached the standards and fulfilling the requirements of the rules and regulations relating to the nature of the degree. The contents embodied in the thesis have not been submitted for the award of any other degree or diploma in this or any other university.

Date:

Place:

Prof. Nilay Mistry
Assistant Professor,
School of Cyber Security & Digital Forensics,
National Forensic Sciences University,
Gandhinagar Campus, Gandhinagar, Gujarat, India.



ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my guide **Dr. Nilay Mistry** sir for continuous support and motivation that helped to diversify the road-map for the project as well as our dean **Dr. Naveen Kumar Chaudhary** sir who gave me the golden opportunity to do this wonderful project on the topic **Ransomware Forensics**, which also helped me in doing a lot of Research and I came to know about so many new things related to Digital Forensic.

Secondly, I would also like to thank my parents and friends who helped me a lot in finishing this project within the limited time.

I am making this project not only for marks but to also increase my knowledge and skill.

With Sincere Regards,

(Jay K. Bhalodiya)

Enroll. No.: 012200300003014

School of Cyber Security & Digital Forensics,
National Forensic Sciences University,
Gandhinagar Campus, Gandhinagar, Gujarat, India.

ABSTRACT

In this era of Digital World, attackers are waiting to infect user's machine with various types of malicious software. One such malicious software which became infamous for encrypting user's data and then demanding Ransom (in bit coins) to decrypt the data is known as Ransomware. As most of the time the files are being decrypted once the ransom is paid, while sometimes the attacker may not do the same, it makes the examination of these malicious software really important. This project is about how to examine the HDD of a user once it is infected by some Ransomware. During this Project work, tools like Guymager, Autopsy & Digital Forensic Framework (DFF) were used for further analysis and extract the file if file will not extract from autopsy.

the cyber threats have reached a new level of menace and maturity. One of the major threats in this cyber world nowadays is ransomware attack which had affected millions of computers. Ransomware locks the valuable data with often unbreakable encryption codes making it inaccessible for both organization and consumers, thus demanding heavy ransom to decrypt the data. In this paper, advanced and improved version of the Petya ransomware has been introduced which has a reduced anti-virus detection of 33% which actually was 71% with the original version. System behavior is also monitored during the attack and analysis of this behavior is performed and described. Along with the behavioral analysis two mitigation strategies have also been proposed to defend the systems from the ransomware attack. This multi-layered approach for the security of the system will minimize the rate of infection as cybercriminals continue to refine their tactics, making it difficult for the organization's complacent development.

In the recent past, there has been an exponential increase in the cyber-attack. One of the most dangerous attacks in this cyber-attack is the ransomware attack which not only corrupt and encrypts the data but also steals the information from the system which can be very dangerous. One of the major ransomware attacks in recent past is the Petya ransomware attack. Methodology and threats due to Petya ransomware are discussed. Awareness and Mitigation for this are also discussed.

LIST OF FIGURES

<u>No.</u>	<u>DESCRIPTION</u>	<u>PAGE NO.</u>
1	Fig. 3.1: Virus total Report of Petya.zip	13
2	Fig 3.2: Virus Total Report of files inside Petya.zip.	14
3	Fig 4.2.1 Infecting TM with Petya	18
4	Fig.6.1: Phony check disk Display.	19
5	Fig 6.2: Red screen with Skull.	19
6	Fig.6.3: Ransom Note.	20
7	Fig. 6.4: Petya-Ransom site.	21
8	Fig. 7.2.1: Taking image of HDD	21
9	Fig:8.1: Failure in adding Image in Encase	22
10	Fig.8.2.1: Autopsy in windows	23
11	Fig 8.2.1.1: Adding New case in Autopsy	24
12	Fig.8.2.1.2: Adding New host in Autopsy.	24
13	Fig. 8.2.1.3: opening a case resource.	25
14	Fig. 8.2.1.4: Verifying the case details	25
15	Fig. 8.2.1.5: Autopsy displaying directories of the Image File Fig. 8.2.1.6: Autopsy displaying thumbnail of the Image File.	26
16	Fig. 8.2.1.7: Browsing through the Directories. Fig. 8.2.1.8: Browsing through the thumbnails.	27
17	Fig. 8.2.1.9: autopsy displaying clear preview of image file.	28
18	Fig. 8.2.1.10: autopsy displaying all deleted files.	28
19	Fig. 8.2.1.11: autopsy displaying carved files of. vmdk.	29
20	Fig. 8.2.1.12: autopsy displaying clear preview carved files of. vmdk.	29
21	Fig. 8.2.1.13: autopsy filter data as per geolocation.	30
22	Fig. 8.2.1.14: extracting image in autopsy.	31
23	Fig. 8.2.1.15: selecting path for extracting an image.	31
24	Fig. 8.3.1.1: DFF launched	34

25	Fig. 8.3.1.2: adding file in DFF.	35
26	Fig. 8.3.1.3: Image file listing “Logical files”	36
27	Fig. 8.3.1.4: confirmation for applying modules.	36
28	Fig 8.3.1.5: listing all partition.	37
29	Fig. 8.3.1.6: confirmation for applying modules	37
30	Fig. 8.3.1.7: listing of “FAT” and “unallocated” particles	38
31	Fig. 8.3.1.9: content of [root] folder in partition 1. Fig. 8.3.1.9: content of [root] folder in partition 1.	39



LIST OF ABBREVIATION

Abbreviation	Description
DFF	Digital Forensic Framework
Gb	Gigabyte
HDD	Hard Dick Drive
Kb	Kilobyte
Mb	Megabyte
MBR	Master Boot Record
MD5	Media Digest 5
MFT	Master File Table
OS	Operating system
Tb	Terabyte
TM	Target Machine

TABLE OF CONTENTS

DECLARATION	2
CERTIFICATE	3
ACKNOWLEDGMENT	4
ABSTRACT	5
LIST OF FIGURES.....	6
LIST OF ABBREVIATION	8
1. INTRODUCTION	10
1.1 OVERVIEW	10
1.2 SCOPE	11
1.3 AIM AND OBJECTIVE	12
1.4 PURPOSE	
2. LITERATURE REVIEW	
3. SAMPLE INFORMSTION	14
4. MACHINE INFORMATION	16
4.1 DETAIL OF TM	16
4.2 PREPARING THE TM.....	17
5. INFECTING THE MACHINE	18
6. WORKING OF PETYA RANSOMWARE.....	19
7. IMAGING.....	22
7.1 BOOTING THE TM	22
7.2 TAKING IMAGE	22
8. TOOLS AND TECHNOLOGY	23
8.1 ENCASE	23
8.2 AUTOPSY.....	24
8.2.1 WORKING AND FINDING.....	24
8.2.2 RESULT OF AUTOPSY	33
8.3 DFF	35
8.3.1 WORKINH AND FINDING.....	35
9. CONCLUSIONS.....	41
10. FUTURE WORK.....	42
11. REFERENCE LINKS.....	43

1.Introduction

1.1 Overview

Ransomware is computer malware that installs covertly on a victim's device (e.g., computer, smartphone, wearable device) and that either mounts the crypto viral extortion attack from cryptovirology that holds the victim's data hostage, until a ransom is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key. Ransomware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file.

The first known malware extortion attack, the "AIDS Trojan" written by Joseph Popp in 1989, had a design failure so severe it was not necessary to pay the extortionist at all. Its payload hid the files on the hard drive and encrypted only their names, and displayed a message claiming that the user's license to use a certain piece of software had expired. The user was asked to pay US\$189 to "PC Cyborg Corporation" in order to obtain a repair tool even though the decryption key could be extracted from the code of the Trojan. The Trojan was also known as "PC Cyborg". Popp was declared mentally unfit to stand trial for his actions, but he promised to donate the profits from the malware to fund AIDS research.

In this Project report we will see how Petya Ransomware works and prevent the user from accessing the files on the machine. To do so a standalone machine was infected intentionally by the Petya ransomware and then the Forensic Analysis was done on that System

1.2 Scope

The project should include immediate incident response activities, such as identifying and containing the Petya ransomware infection, isolating affected systems, and preserving evidence for analysis.

I will examine the Petya Ransomware which encrypts the MBR and MFT sectors of an HDD and denies access to the full system. I will infect a virtual machine with the Petya Ransomware and would perform the forensic analysis of the image file of the system by using the software's such as EnCase, Autopsy and DFF (if autopsy fails to extract the data). Project Scope is to try to find out more information regarding working of Petya ransomware and retrieving the files hijacked.

It involves assessing the impact of the Petya ransomware attack. This includes identifying the extent of data encryption, determining which systems and files were affected, and evaluating any additional damage caused to the targeted organization's infrastructure or operations.

The project should encompass the collection and preservation of forensic data from compromised systems. This includes acquiring system logs, memory dumps, network traffic captures, and other relevant artifacts that can provide insights into the attack timeline, attacker activity, and potential indicators of compromise (IOCs).

1.3 Aims and Objective

The primary objective is to conduct a detailed analysis of the Petya ransomware attack. This includes understanding the attack vectors, propagation methods, and the specific variant of Petya ransomware involved. The goal is to gain insights into how the attack occurred, the scope of the compromise, and any unique characteristics of the ransomware variant.

An important objective is to recover encrypted data and restore affected systems to a functional state. This involves leveraging available backups, ensuring the removal of the ransomware, and implementing measures to prevent re-infection. The goal is to minimize downtime and restore normal operations as quickly as possible.

The project aims to derive lessons from the incident and provide recommendations for enhancing the organization's security posture. This may include identifying vulnerabilities or weaknesses exploited by the ransomware, suggesting improvements in security controls, and developing incident response plans to better prepare for future attacks.

1.4 Purpose

The project purpose to gain a comprehensive understanding of the Petya ransomware attack. By analyzing the attack's characteristics, propagation methods, and impact, the project helps in understanding how the attack occurred and the techniques employed by the ransomware.

Identifying the threat actors responsible for the Petya ransomware attack is another crucial purpose of the forensic project. By analyzing indicators of compromise (IOCs), command-and-control infrastructure, and any available threat intelligence, the project seeks to establish potential attribution. Attribution helps with legal actions, intelligence sharing, and developing countermeasures against future attacks.

The project seeks to assess the impact of the Petya ransomware attack on the targeted organization. This includes evaluating the extent of data encryption, determining which systems and files were affected, and identifying any additional damage caused by the attack. Understanding the impact helps in prioritizing recovery efforts and implementing appropriate mitigation strategies.



2.Literature Review

“RANSOMWARE IN INDUSTRIAL CONTROL SYSTEMS. WHAT COMES AFTER WANNACRY AND PETYA GLOBAL ATTACKS?” [1]

Author: Marcelo Ayres Branquinho

The analysis of WannaCrypt0r and Not Petya malware reveals they both exploited the Eternal Blue security vulnerability. Eternal Blue was part of a leaked hacking tool collection by the Shadow Brokers group, claimed to be stolen from the NSA. These attacks indicate a concerning trend where powerful ransomware exploits target critical industrial control systems. To combat upcoming attacks, critical infrastructures must invest in cybersecurity and strengthen defenses according to established frameworks such as IEC-62433.

“Digital Forensic Readiness Framework for Ransomware Investigation” [2]

Author: Avinash Singh

This study introduces a digital forensic readiness framework for ransomware investigations, enabling the collection of near real-time evidence. However, the implementation may face challenges due to modern OS security mechanisms that limit access to process information. Despite this, the framework has the potential to gather more evidential information compared to post-mortem forensics. The study provides a preliminary investigation into the Windows 10 OS, supporting the framework's effectiveness. Future work aims to develop a reliable and faster data discovery method, along with a contextual trigger mechanism for data collection. The framework enhances legal prosecution, protects against ransom payments, and improves understanding of ransomware behavior at a granular level.

“The Evolution of Ransomware Variants” [3]

Author: Veronica Drake

Our work, throughout its analysis of ransoms such as; WannaCry, Petya and Crisis led to many key findings and determined that despite the increasing obstinance of ransomware, numerous issues exist within ransomware which drastically reduce the overall effectivity of each variant.

“Behavior Based Ransomware Detection” [4]*Author: Christopher J. W. Chew and Vimal Kumar*

The threat of ransomware is ever increasing and evolving as attackers continuously create new and unique strains. Signature based detection is unable to keep up with this pace of ransomware development. In this paper we showed that behavior-based approaches can be the way forward. We implemented some simple detection methods and tested them against some well-known ransomware samples. Our preliminary investigation has shown promise and we can see that their implementation is not very resource intensive as signature based detection methods generally are.

“Analysis of Ransomware on Windows platform” [5]*Author: Adel Hamdan Mohammad*

In conclusion, the study demonstrates the impact of selected ransomware families on the Windows platform through experiments conducted using virtual environments and a sandbox. The findings reveal that most ransomware types exhibit similar behavior, affecting the file system and registry entities. The study suggests that monitoring system files and registry activities can be an effective defense against ransomware. Additionally, it is noted that Windows 10 shows better resilience against ransomware compared to Windows 7. The recommended approach includes regular data backups, updating the Windows operating system, and installing antivirus software to monitor system file activity. The author proposes future work on incorporating machine learning methods to enhance system file activity monitoring.

“Advanced Petya Ransomware Mitigation strategies” [6]*Author: JS Aidan, U Garg*

In this cyber era, the cyber threats have reached a new level of menace and maturity. One of the major threat in this cyber world nowadays is ransomware attack which had affected millions of computers. Ransomware locks the valuable data with often unbreakable encryption codes making it inaccessible for both organization and consumers, thus demanding heavy ransom to decrypt the data. In this paper, advanced and improved version of the Petya ransomware has been introduced which has a reduced anti-virus detection of 33% which actually was 71% with the original version.

“What petya/notpetya ransomware is and what is remediation are”[7]

Ransomware attacks have been growing worldwide since they appeared around 2012. The idea of ransomware attacks is, encrypting and locking the files on a computer until the ransom is paid. These attacks usually enter the system by using Trojans, which has malicious programs that run a payload that encrypts and locks the files. The basic goal of this type of attack is getting money, so hackers usually unlock the files when they receive the money, but really there is no guarantee of that. Ransomware attacks have various versions such as Reveton, CryptoWall, WannaCry, and Petya.

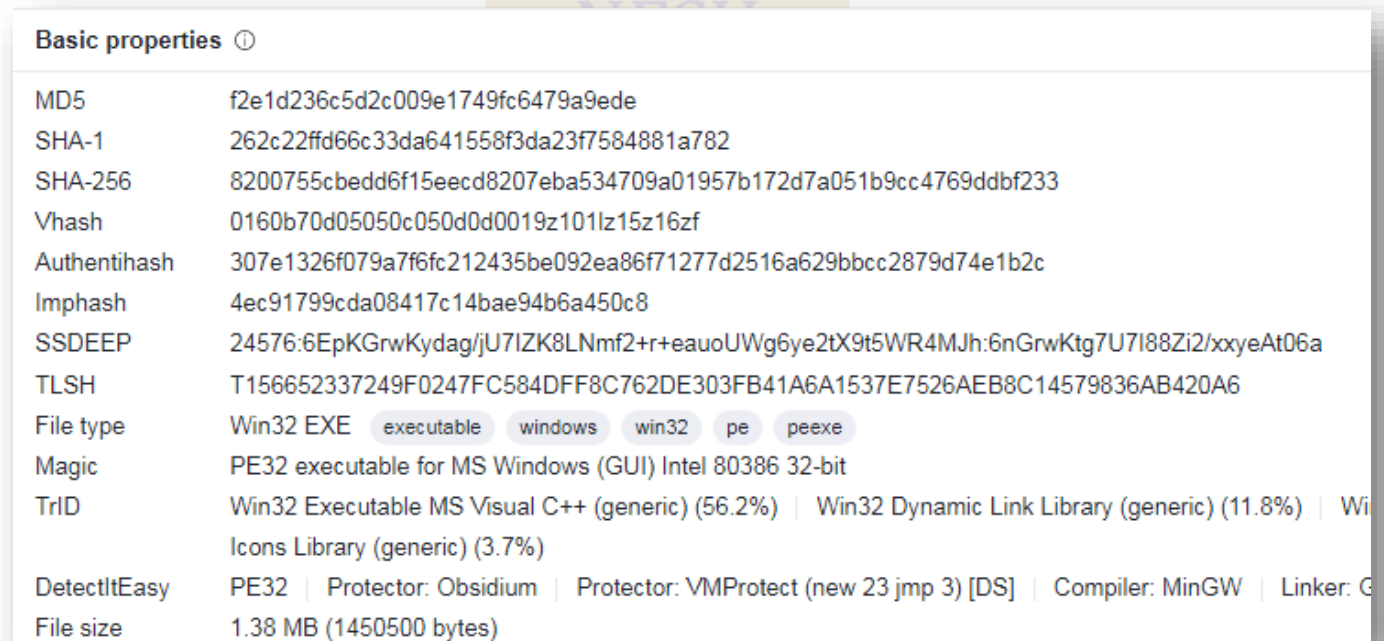
Eternal Blue Vulnerability [8]

MR GUPTA, YP KOLI

Many organizations have experienced the damage caused by cyberattacks exploiting Windows vulnerabilities. For operational reasons, the parameters of Windows are still used, especially in the enterprise management system (ICS). In this case, attackers can torture them to spread the disease. Specifically, the vulnerability in MS17-010 was used in attacks to spread malware such as WannaCry ransomware and other malware. Many systems for example, electronic newspapers, payment centres and car manufacturers are used around the world and there is a security vulnerability in Windows that causes serious problems. Since tools like Eternal Blue or Eternal Romance are published on the internet, attackers can easily exploit these vulnerabilities. This tool attacks legitimate processes running on Windows systems. It can be difficult for employees to see the signs of a struggle. Attacks can be mitigated using security updates; however, security updates are sometimes difficult to implement due to their long lifetime and stringent requirements. There are many ways to identify attacks that cause vulnerabilities, such as intrusion detection systems (IDS), but they are sometimes difficult to use because they require prior service. In this research, we propose a method to identify the attack that exploited the vulnerability in MS17-010 by analyzing Windows built-in event Logs. This method can detect attacks against almost all supported versions of Windows. It can also be easily integrated into the production environment as it only uses the standard Windows operating system. Keywords: Eternal Blue, Vulnerability, Ransomware, attacks, malware

3. Sample Information

- After searching various source, the malware sample was taken from the project guide.
- Malware sample was compressed and was isolated from the system in a zip file protected by the password “infected”
- MD5 value of the file was “f2e1d236c5d2c009e1749fc6479a9ede”
- Virus total report of .zip file



The image shows a VirusTotal report for a file named petya.zip. The report is titled 'Basic properties' and lists various hashes and file information. The MD5 hash is f2e1d236c5d2c009e1749fc6479a9ede. The SHA-1 hash is 262c22ffd66c33da641558f3da23f7584881a782. The SHA-256 hash is 8200755cbdd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddb233. The Vhash is 0160b70d05050c050d0d0019z101lz15z16zf. The Authentihash is 307e1326f079a7f6fc212435be092ea86f71277d2516a629bbcc2879d74e1b2c. The Imphash is 4ec91799cda08417c14bae94b6a450c8. The SSDEEP is 24576:6EpKGrwKydag/jU7IZK8LNmf2+r+eaoUWg6ye2tX9t5WR4MJh:6nGrwKtg7U7I88Zi2/xxyeAt06a. The TLSH is T156652337249F0247FC584DFF8C762DE303FB41A6A1537E7526AEB8C14579836AB420A6. The File type is Win32 EXE, with tags for executable, windows, win32, pe, and peexe. The Magic is PE32 executable for MS Windows (GUI) Intel 80386 32-bit. The TrID is Win32 Executable MS Visual C++ (generic) (56.2%) | Win32 Dynamic Link Library (generic) (11.8%) | Win32 Icons Library (generic) (3.7%). The DetectItEasy is PE32 | Protector: Obsidium | Protector: VMProtect (new 23 jmp 3) [DS] | Compiler: MinGW | Linker: G. The File size is 1.38 MB (1450500 bytes).

Basic properties ⓘ	
MD5	f2e1d236c5d2c009e1749fc6479a9ede
SHA-1	262c22ffd66c33da641558f3da23f7584881a782
SHA-256	8200755cbdd6f15eecd8207eba534709a01957b172d7a051b9cc4769ddb233
Vhash	0160b70d05050c050d0d0019z101lz15z16zf
Authentihash	307e1326f079a7f6fc212435be092ea86f71277d2516a629bbcc2879d74e1b2c
Imphash	4ec91799cda08417c14bae94b6a450c8
SSDEEP	24576:6EpKGrwKydag/jU7IZK8LNmf2+r+eaoUWg6ye2tX9t5WR4MJh:6nGrwKtg7U7I88Zi2/xxyeAt06a
TLSH	T156652337249F0247FC584DFF8C762DE303FB41A6A1537E7526AEB8C14579836AB420A6
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (56.2%) Win32 Dynamic Link Library (generic) (11.8%) Win32 Icons Library (generic) (3.7%)
DetectItEasy	PE32 Protector: Obsidium Protector: VMProtect (new 23 jmp 3) [DS] Compiler: MinGW Linker: G
File size	1.38 MB (1450500 bytes)

Figure 3.1 virus total report of petya.zip

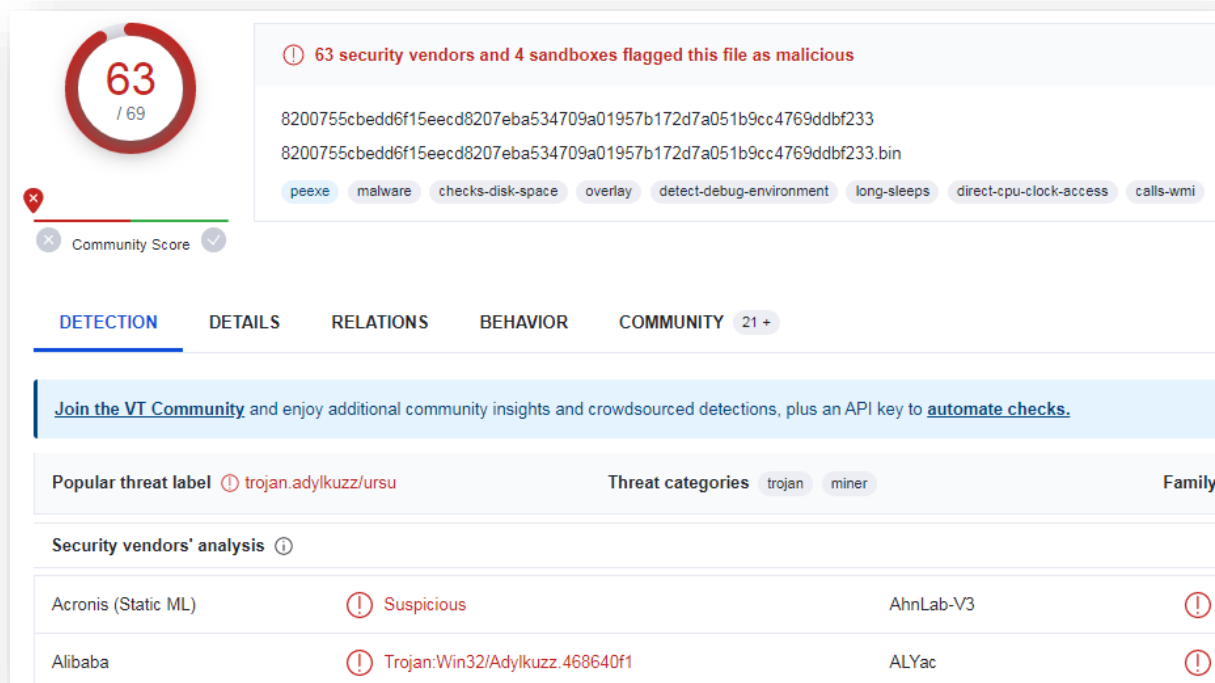


Figure 3.2 Virus total Report of File Inside .Zip file

4. Machine Information

4.1 Details of TM

- A physical machine running windows 7 OS was selected as a TM.
- The TM was having a 370gb HDD with some sample test data in it
- Set the virtual machine's display resolution to match your host system or adjust it as needed. Windows 7 typically supports resolutions starting from 800 x 600 pixels.
- Configure the virtual machine's network adapter to use the appropriate network settings, such as NAT (Network Address Translation) or bridged mode, depending on your networking requirements.
- A modern processor with virtualization support, such as Intel VT-x or AMD-V, is recommended for better performance. Multiple cores or threads can also help improve the virtual machine's responsiveness.
- Most virtualization software provides virtual graphics adapters that support the Windows 7 display requirements. However, advanced graphics features like hardware

4.2 Preparing the TM

- The TM had Windows 7 as using in a virtual machine.
- Some sample data was added to the HDD (370 GB) to assist the examination after infecting the machine with Ransomware.
- Data include image, videos and pdf.
- All the data must be completely download.
- After the preparation, infection of VM take place

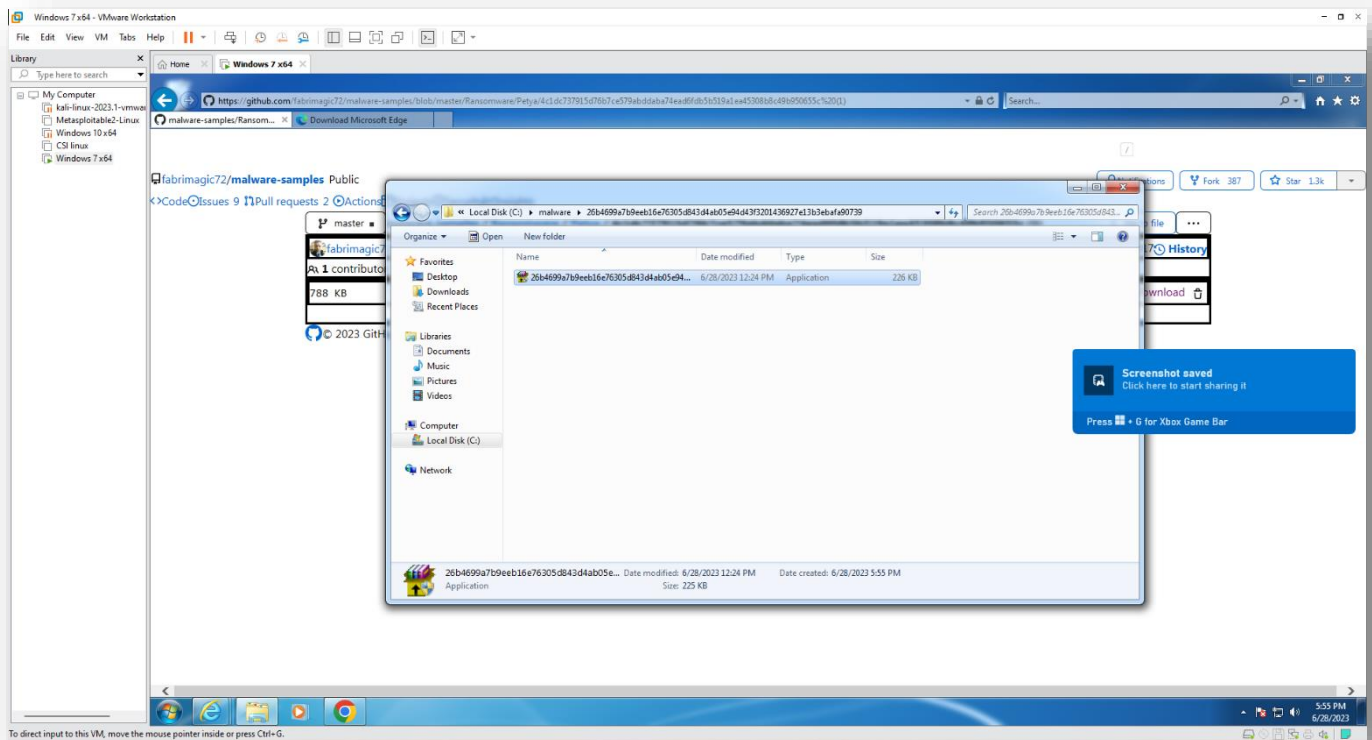
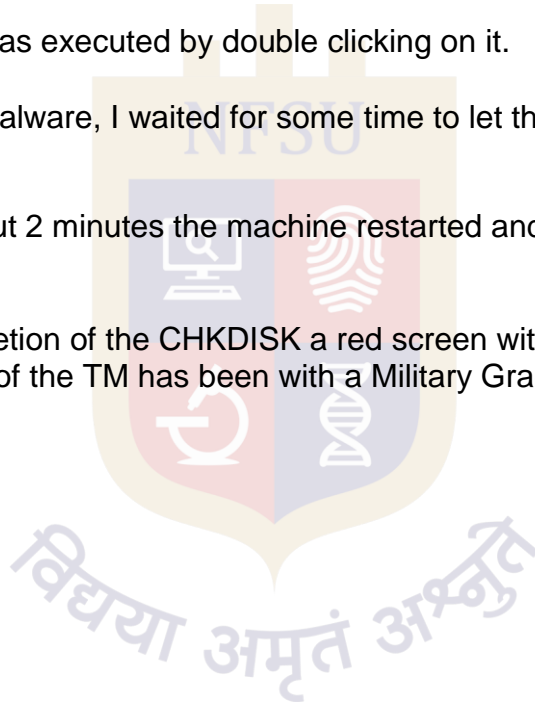


Figure 4.2.1 Infecting TM with Petya

5. Infecting the Machine

- The Ransomware sample was introduced into the TM by using a Pen Drive.
- The contents of .zip file were extracted on the Desktop of the TM.
- A file named "Petya.bin" was extracted from the zip file using the password "infected".
- The file "Petya.bin" was executed by double clicking on it.
- After executing the malware, I waited for some time to let the ransomware start its Encryption.
- After waiting for about 2 minutes the machine restarted and the screen displayed the CHKDISK message.
- Right after the completion of the CHKDISK a red screen with a skull was displayed stating that the HDD of the TM has been with a Military Grade Encryption.



6. Working of the Petya ransomware

- When Petya ransomware is executed, it replaces the boot drive's MBR with a malicious loader. The malware forces Windows to reboot and displays a phony check disk (CHKDSK) operation to the victim while the malware executes in the background and encrypts the MBR.

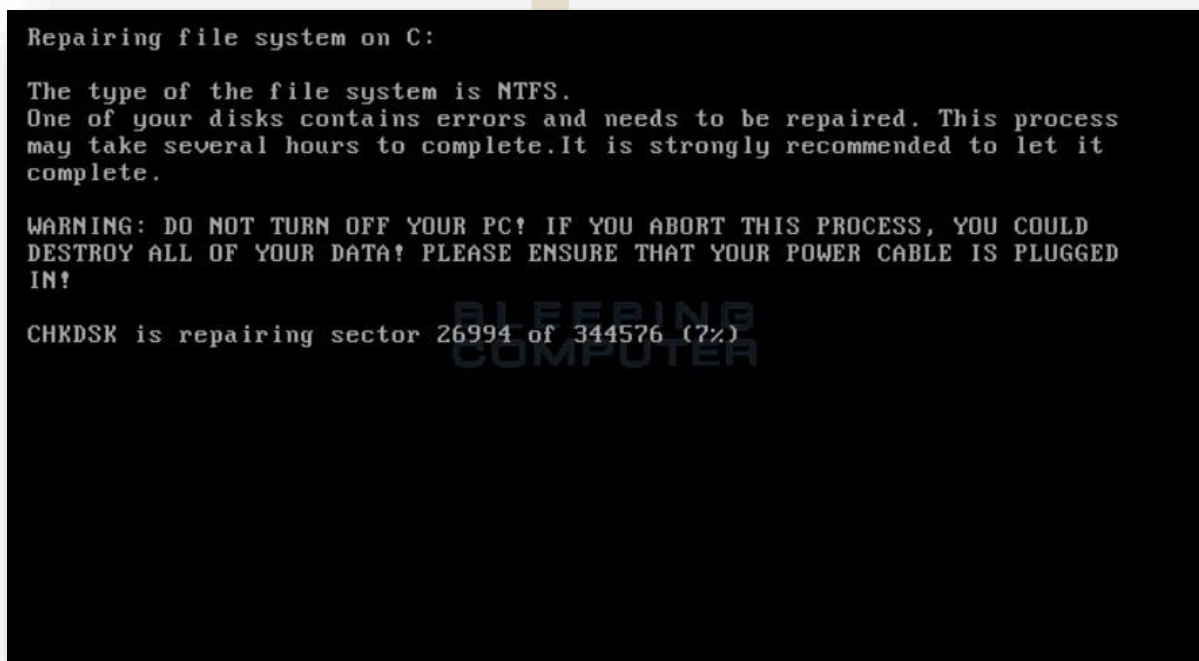


Figure 6.1 Phony check disk Display

- Once the MFT is corrupted, or encrypted in this case, the computer does not know where files are located, or if they even
- Exist, and thus they are not accessible. The victim will then see a ransom note displayed before
- Windows boots explaining that the hard drive is encrypted and provides the victim with directions on how to download Tor in order to access the attacker's payment website and how to pay the ransom in Bitcoin.

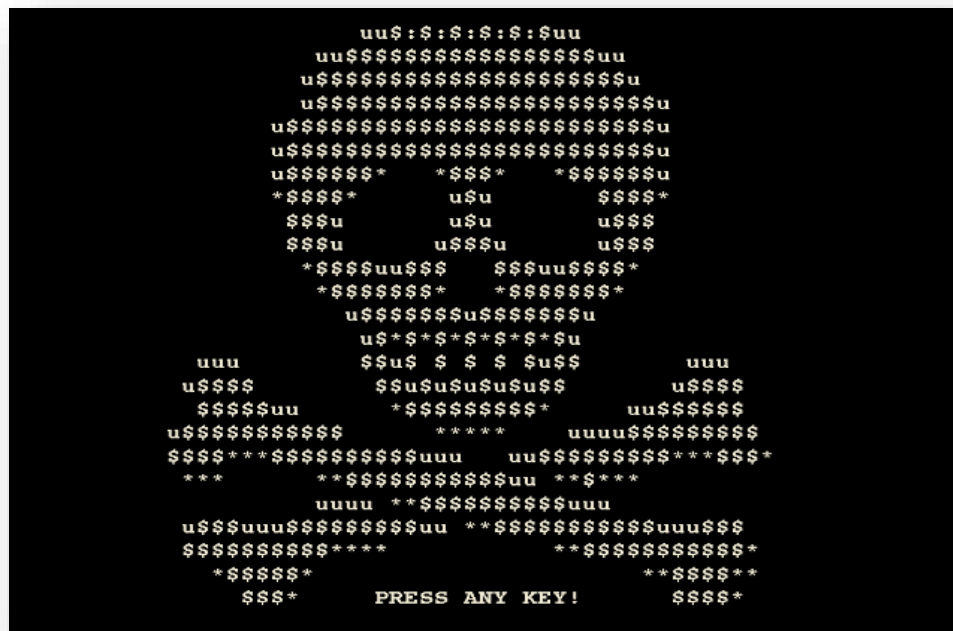


Figure 6.2 screen with skull.

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/GFCsUs>
<http://petya5koahtsf7sv.onion/GFCsUs>

3. Enter your personal decryption code there:

3bPCQ7-cU6Ca j-v5GAP8-GvsHr5-9yb6fF-9cfffN-Nz4czH-qxvsSy-42PyLG-YxTFxz-Yput66-gBXo79-Xy2U9m-r9B8tu-K33K2V

If you already purchased your key, please enter it below.

Key: _

Figure 6.3 Ransom Note

- Once the victim downloads the Tor browser as shown in first step, they can access the "onion" webpage of Petya ransomware. These web pages show how to obtain a decryption key and how to pay for it



Figure 6.4 Petya-Ransom site

- If the victim pays the ransom as demanded they will be provided with a key which might decrypt the MBR and MFT of the HDD, but there are chances that the key might fail to decrypt the HDD or that the key might not be provided to the victim.
- This may lead to complete data loss of the victim.

7. Imaging

7.1: Booting the TM

- A bootable Pen Drive with Kali Linux was prepared using Rufus Software.
- The TM was booted using the Live Kali Linux OS.

7.2 Taking Image

- "Guymager"- a preinstalled software of Kali OS was used to take the image of the 370 GB.

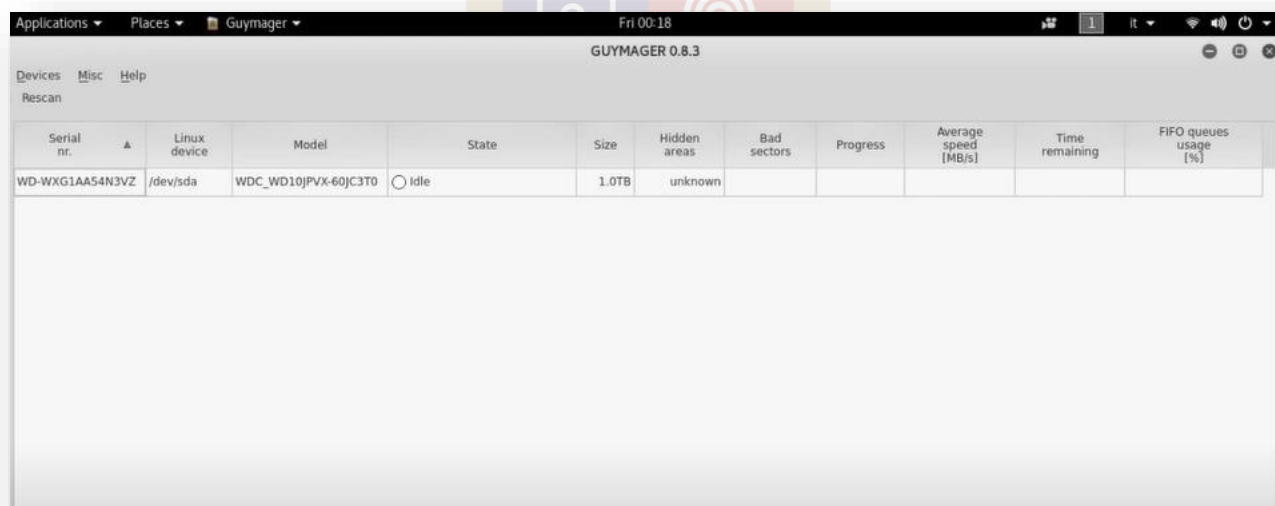


Figure 7.2.1 taking image of HDD.

- Image file was created in ".dd" format and after creation the MD5 Hash value was calculated of both the original HDD and Image file, then compared and verified.

8. Tools and Technology

8.1 Encase

- Initially I tried to add and process the Image file in Encase.
- But Windows Defender detected the malicious content of the image file and thus Encase was unable to access it.

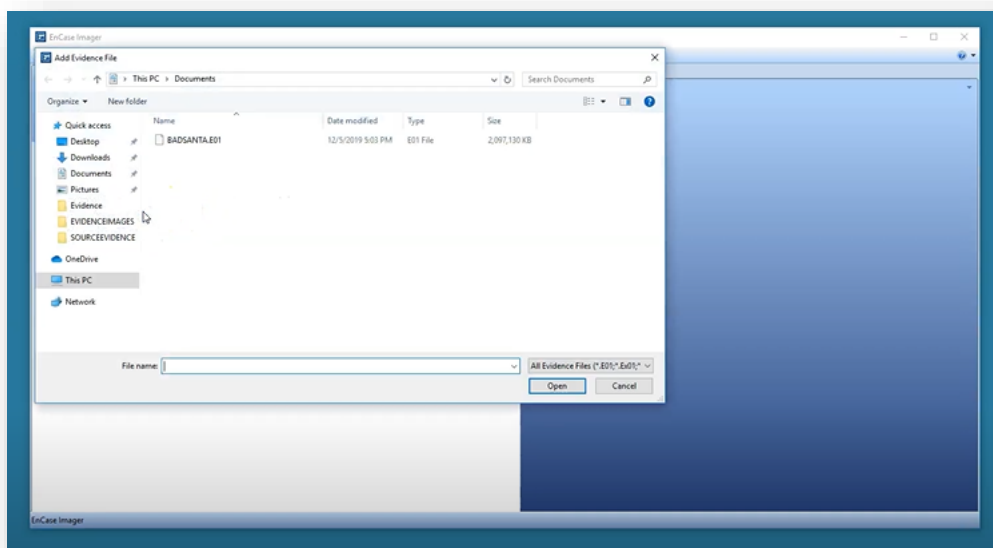


Figure 8.1 failure in adding image in Encase.

- It was possible to add the image file in EnCase by disabling the windows defender, but processing the image containing the malicious content might had infected the host machine as well as the network on which EnCase was running.
- Thus, the idea of analyzing the Image file in EnCase was dropped and further analysis was done by booting the machine in Live Kali Linux OS.

8.2 Autopsy:

8.2.1 Working and finding

- As windows defender was able to detect the malicious content inside the image file, we decided to boot the machine using Live Kali Linux for further analysis either we can use virtual machine as TM.
- We can use .vmdk file for further analysis
- Autopsy version 4.20 was installed in the windows.
- Autopsy version 4.20 was launched.



Figure 8.2.1 Autopsy in windows

- A new case was created in autopsy with name “case 1”



Figure 8.2.1.1 Adding New case in Autopsy

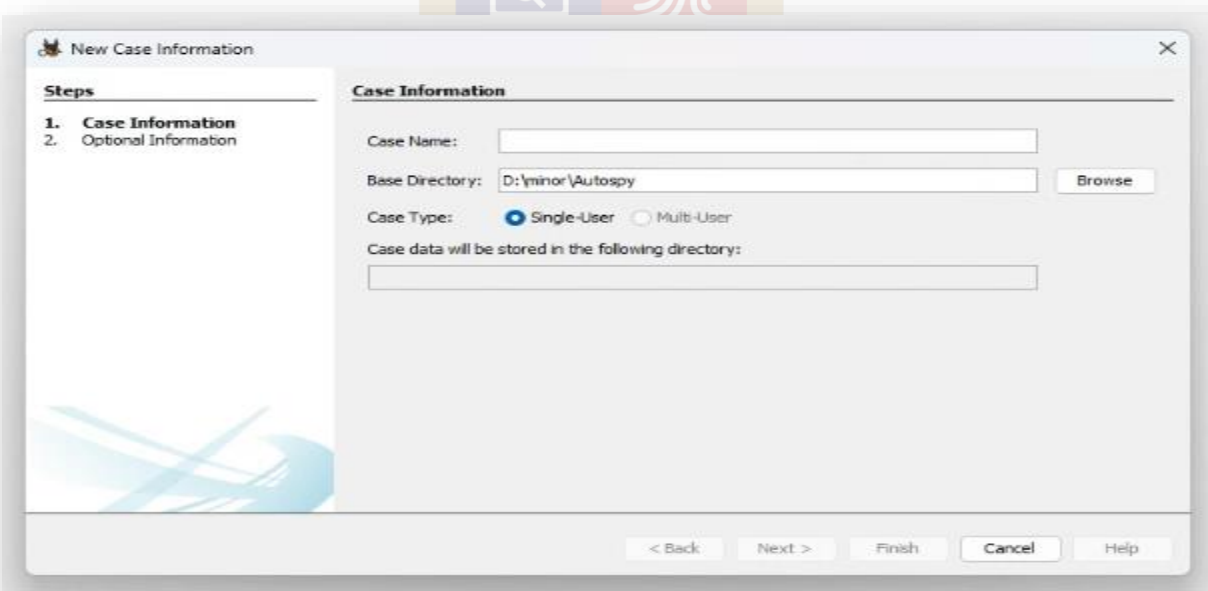


Figure 8.2.1.2 adding a new case info. In autopsy

- Then image resource is opening in an autopsy

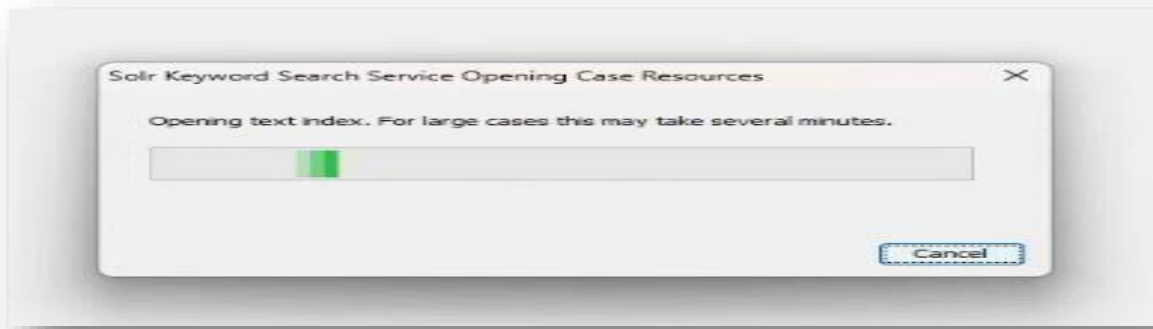


Figure 8.2.1.3 opening a case resource

- Then we have to verify the case details.

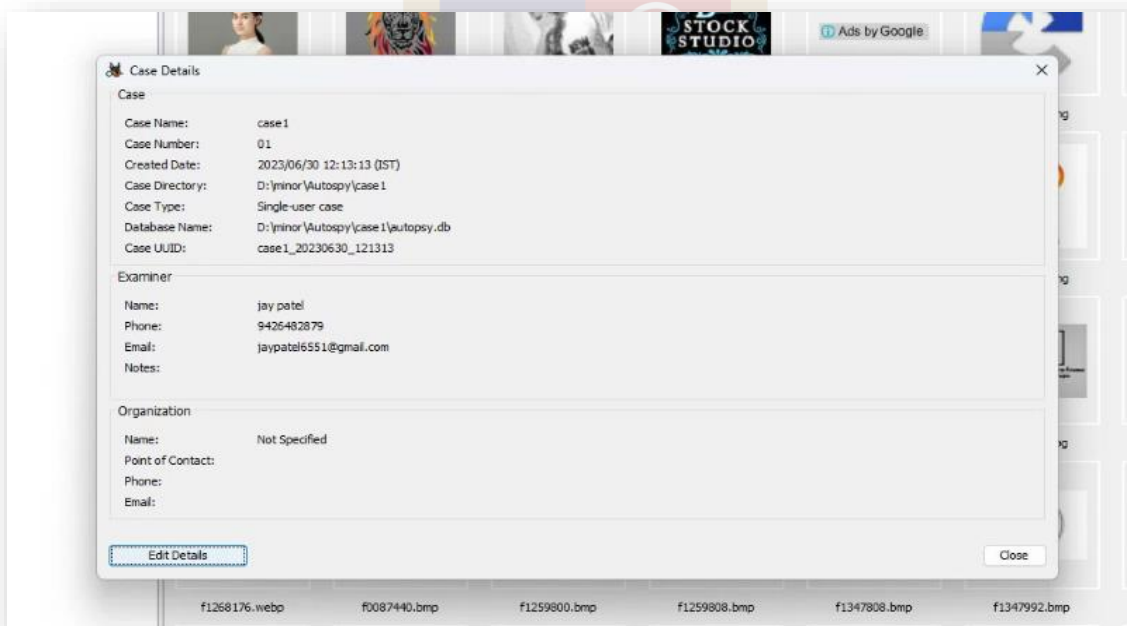


Figure 8.2.1.4 verifying the case details.

- As soon as we verify the image file details. Autopsy starts calculating the MD5 of the image file and display all the partition on the image file.

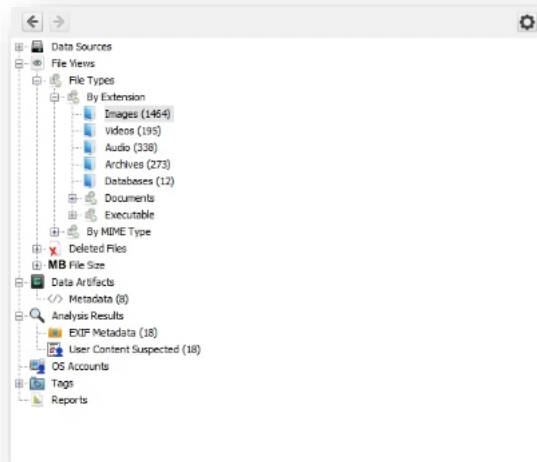


Figure 8.2.1.5 Autopsy displaying directories of image file(.vmdk)

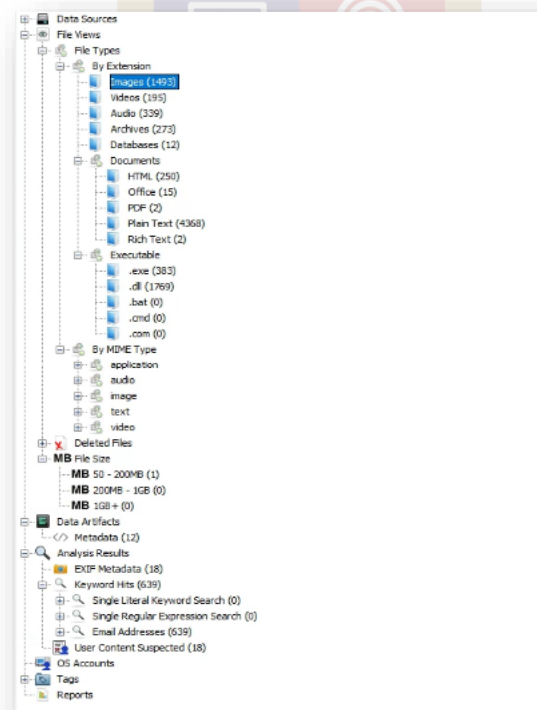


Figure 8.2.1.6 Autopsy displaying directories of the image file or .vmdk file

- Data Sources**

 - File Views
 - File Types
 - By Extension
 - Images (3048)
 - Videos (440)
 - Audio (522)
 - Archives (757)
 - Desktops (58)
 - Documents
 - Executable
 - By MIME Type
 - Deleted Files
 - MB File Size
 - Data Artifacts
 - Metadata (1390)
 - Analysis Results
 - Encryption Detected (2)
 - OS Metadata (5)
 - Keyword Hits (6303)
 - User Content Suspected (55)
 - OS Accounts
 - Tags
 - Reports

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Di)	Flags(Meta)	Known
eq_vldsr_thumb_1	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1214	Allocated	Allocated	unknown
eq_vldsr_thumb_1	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1214	Allocated	Allocated	unknown
flag.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1210	Allocated	Allocated	unknown
pause_colormap.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1310	Allocated	Allocated	unknown
pause_down.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2062	Allocated	Allocated	unknown
pause_hover.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2054	Allocated	Allocated	unknown
pause_up.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2046	Allocated	Allocated	unknown
player_disable.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9836	Allocated	Allocated	unknown
player_down.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9248	Allocated	Allocated	unknown
player_hover.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9002	Allocated	Allocated	unknown
player_map.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2620	Allocated	Allocated	unknown
player_up.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8832	Allocated	Allocated	unknown
pl_b.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1162	Allocated	Allocated	unknown
pl_b1.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1190	Allocated	Allocated	unknown
pl_b1.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1190	Allocated	Allocated	unknown
pl_b1.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4278	Allocated	Allocated	unknown
pl_r.bmp	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4278	Allocated	Allocated	unknown
pl_restoremin_b1img	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1190	Allocated	Allocated	unknown
pl_restoremin_b1img	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1286	Allocated	Allocated	unknown
pl_restoremin_b1img	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1318	Allocated	Allocated	unknown
pl_restoremin_b1img	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1318	Allocated	Allocated	unknown
pl_restoremin_b1img	1			2010-11-04 18:05:36...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00				

8.2.1.7 browsing through the

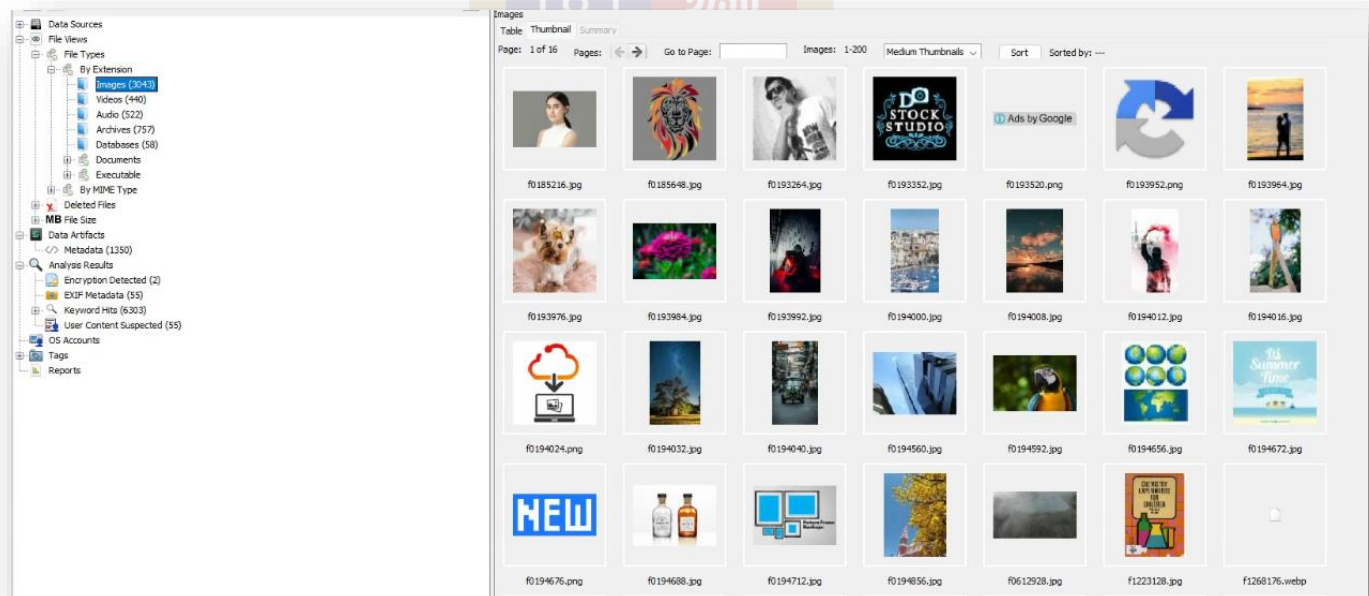


Figure 8.2.1.8 browsing through the directories with thumbnail.

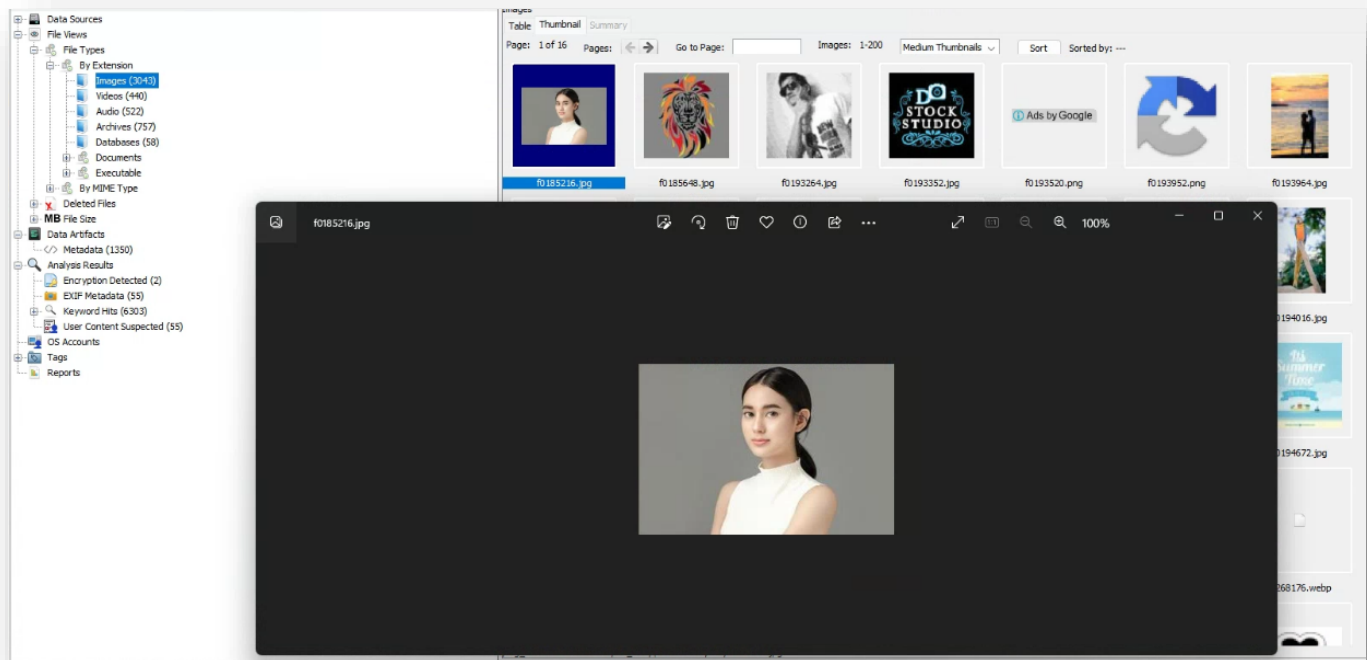


Figure 8.2.1.9 Autopsy displaying clear preview of image file.

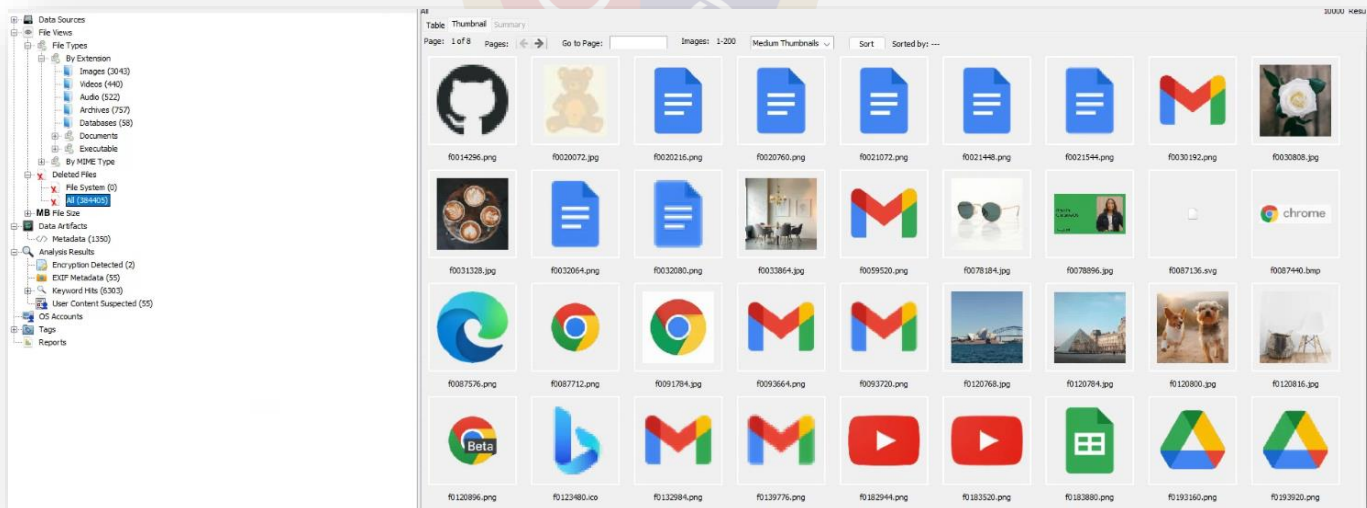


Figure 8.2.1.10 Autopsy displaying all deleted files.

Add Data Source

Add Images/Videos

Communications

Geolocation

Timeline

Discovery

Generate Report

Close Case ?

193 Results

Save Table as CSV

Listing

img_windows_7_x64_vmdk\vol_ysd2\SCarvedFiles

TableThumbnailSummary

Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MDS Hash	SHA-256 Hash	HQME Type	Extension
1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
10				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
100				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
101				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
102				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
103				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
104				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
105				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
106				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
107				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
108				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
109				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
11				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
110				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
111				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
112				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
113				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
114				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
115				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
116				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
117				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
118				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
119				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
12				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
120				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
121				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
122				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
123				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
124				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
125				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
126				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				
127				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown				

Figure 8.2.1.11 Autopsy showing carved files of the. vmdk

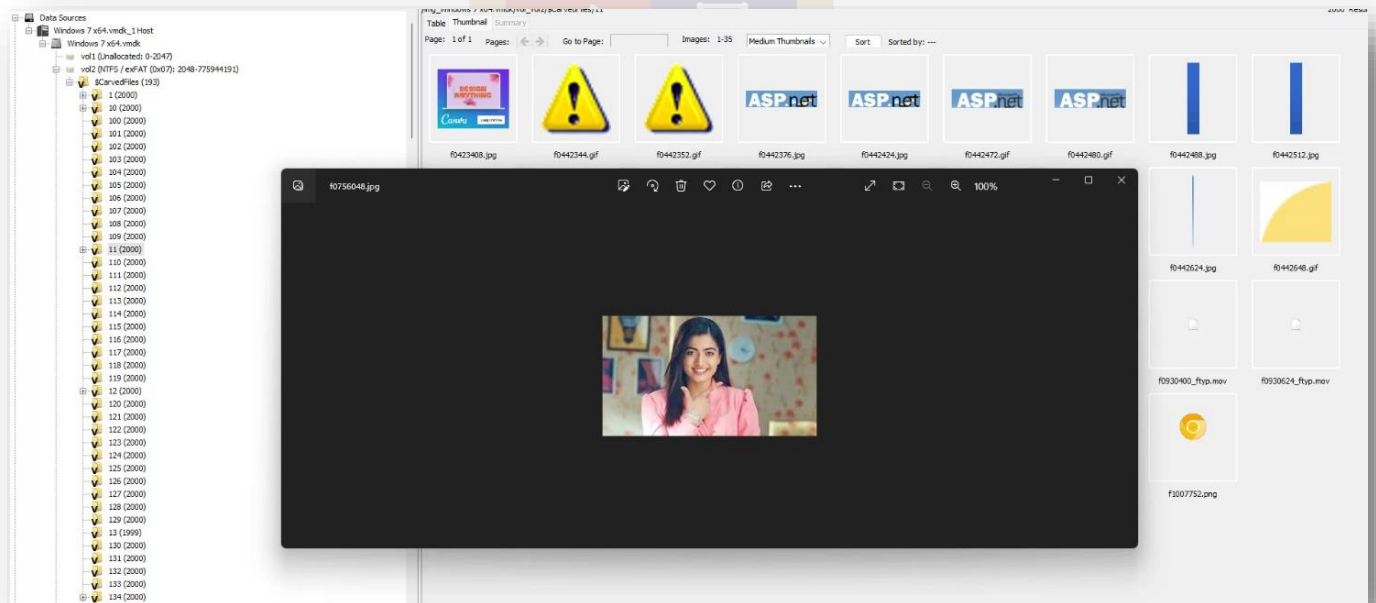


Figure 8.2.1.12 Autopsy displaying clear preview of carved files of the .vmdk

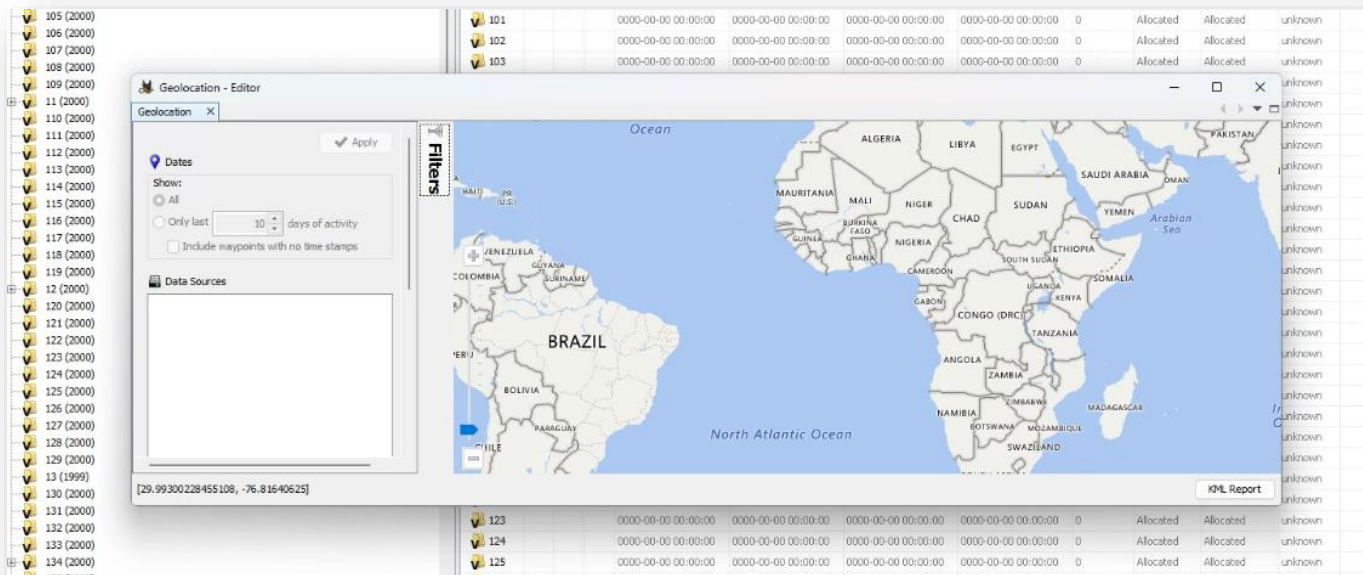


Figure 8.2.1.13 Autopsy filter the data as per the geolocation.

- Now we can try extract the data through Autopsy and save that data to the specific location in host machine. With the analyzing the data and view the main work is extraction of all files.
- If extraction of that data is successful then we can recover all the data from encrypted HDD file and there is no need of decryption key to recover data and no need to pay the “ransomware”.
- Here we are using TM as a window 7 in a virtual machine and .vmdk file is using as image for the analysis and try to recover/extract data from it.

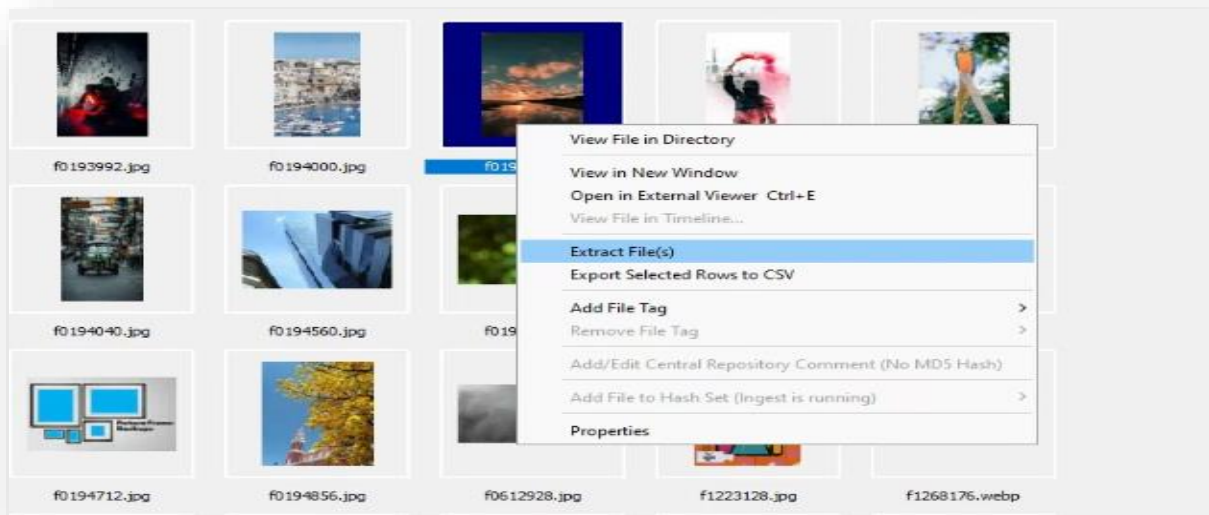


Figure 8.2.1.14 Extracting image from Autopsy

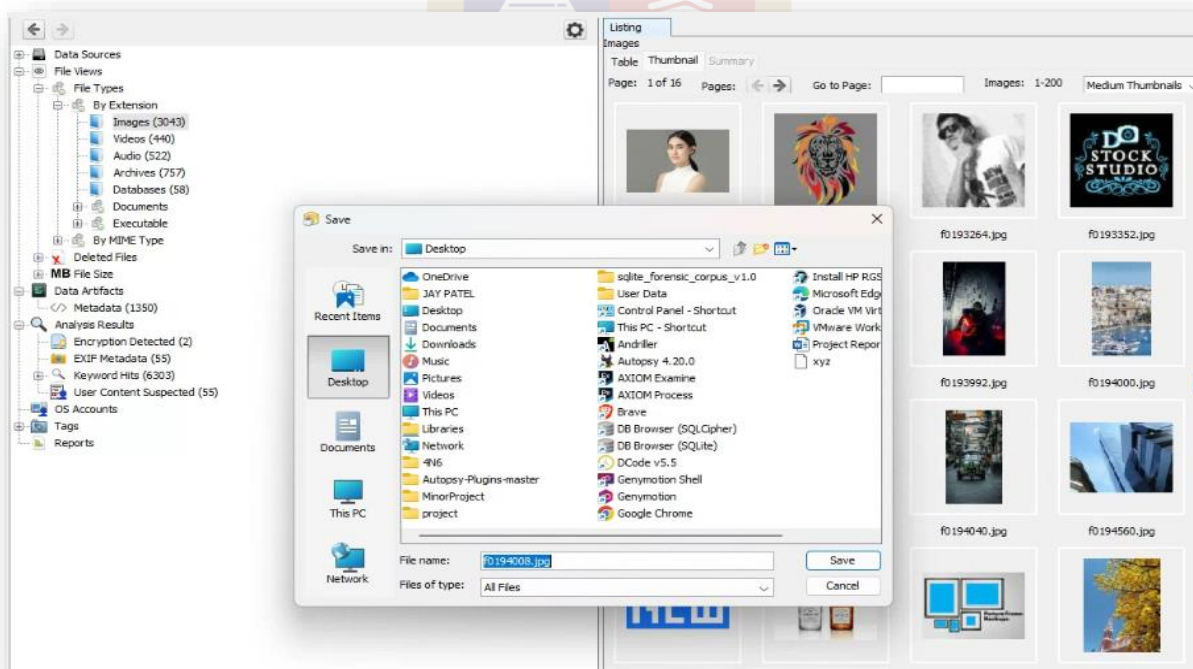
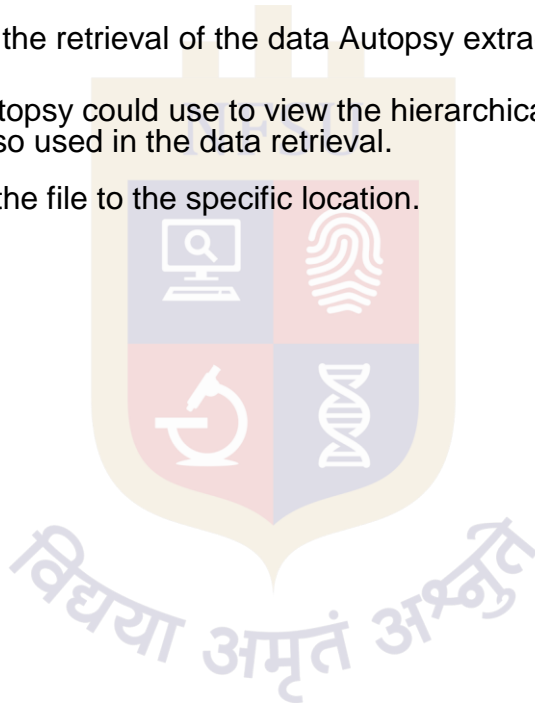


Figure 8.2.1.15 selecting path for extracting an image

8.2.2 Result of Autopsy

- A proper hierarchical structure of all the partitions, directories and files was created.
- Most of the Files present on the .vmdk file of the infected system were discovered by using Autopsy.
- Autopsy also retrieve the deleted data.
- Autopsy displaying carved file with the clear preview.
- But when it comes to the retrieval of the data Autopsy extracts data.
- It can be said that Autopsy could use to view the hierarchical structure of hijacked data but it can't be also used in the data retrieval.
- Autopsy also extract the file to the specific location.



8.3 Digital Forensic Framework

- digital forensic framework refers to a structured and systematic approach used in the field of digital forensics to investigate and analyze digital evidence. It provides a set of guidelines, processes, and tools that help forensic examiners collect, preserve, analyze, and present evidence in a consistent and reliable manner. A well-defined framework ensures that digital forensic investigations adhere to best practices, maintain the integrity of evidence, and produce accurate and admissible findings.
- Digital forensic frameworks are designed to guide investigators in a structured and repeatable manner, promoting consistency, reliability, and defensibility of forensic findings. These frameworks are dynamic and continually evolving to keep pace with advancements in technology, changes in legal requirements, and emerging investigative challenges. Various frameworks exist, such as the National Institute of Standards and Technology (NIST) framework, the Digital Investigation Framework (DIF), and the Scientific Working Group on Digital Evidence (SWGDE) guidelines, each providing a structured approach to digital forensic investigations.
- Digital Forensics Framework (DFF) was a computer forensics open-source software. It is used by professionals and non-experts to collect, preserve and reveal digital evidence without compromising systems and data.
- Here we are using DFF for further analysis and extraction of evidence. Infected we recover the image and other data from the Autopsy version 4.20. DFF is a framework for digital forensic which is used in Kali to examine and acquisition of the data.
- We are using DFF for exploring the framework and analysis and examine data. We get the success to recover the data from Autopsy. Purpose of using DFF is just to explore

8.3.1 Working and Finding

- DFF was launched inside Live Kali OS

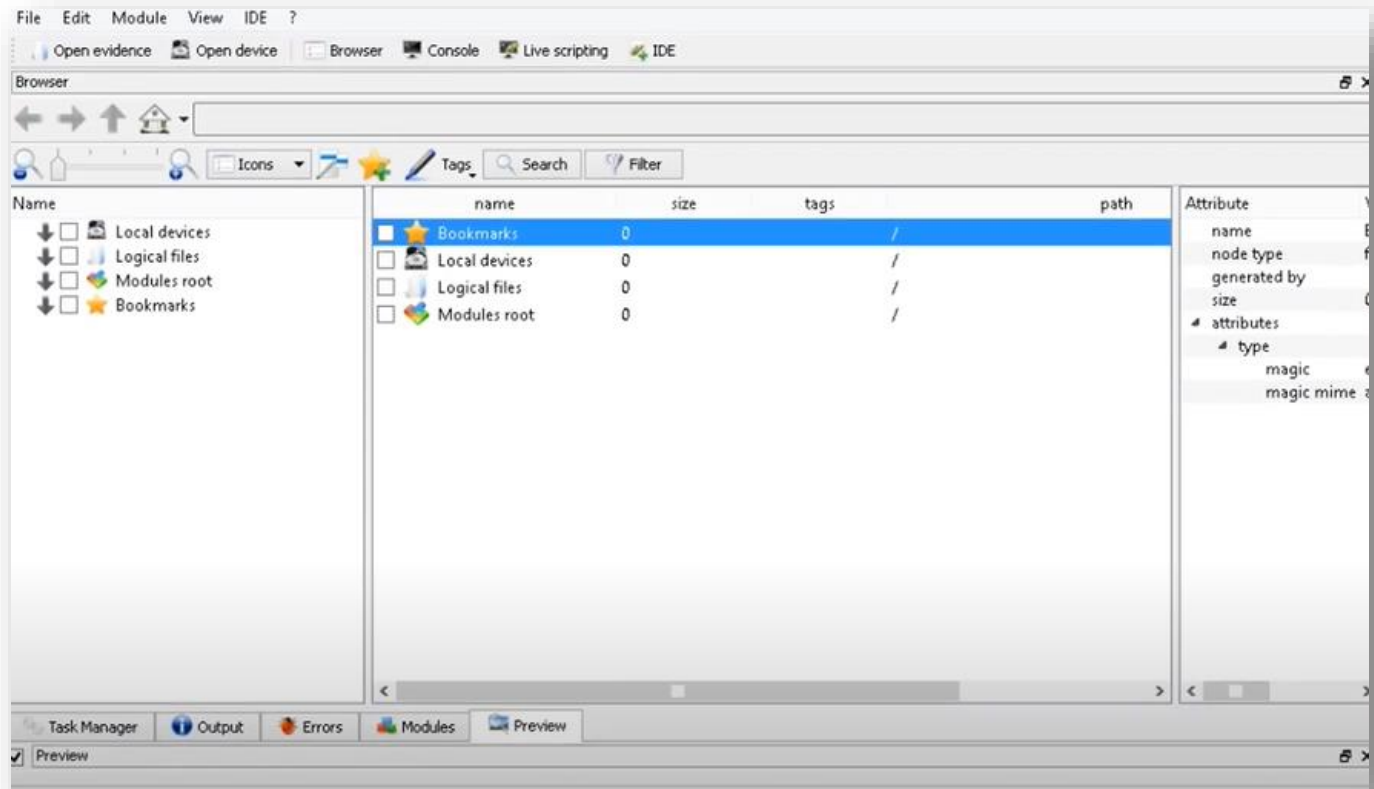


Figure 8.3.1.1 DFF launched in live kali

- Choose option open Evidence to add image file in DFF

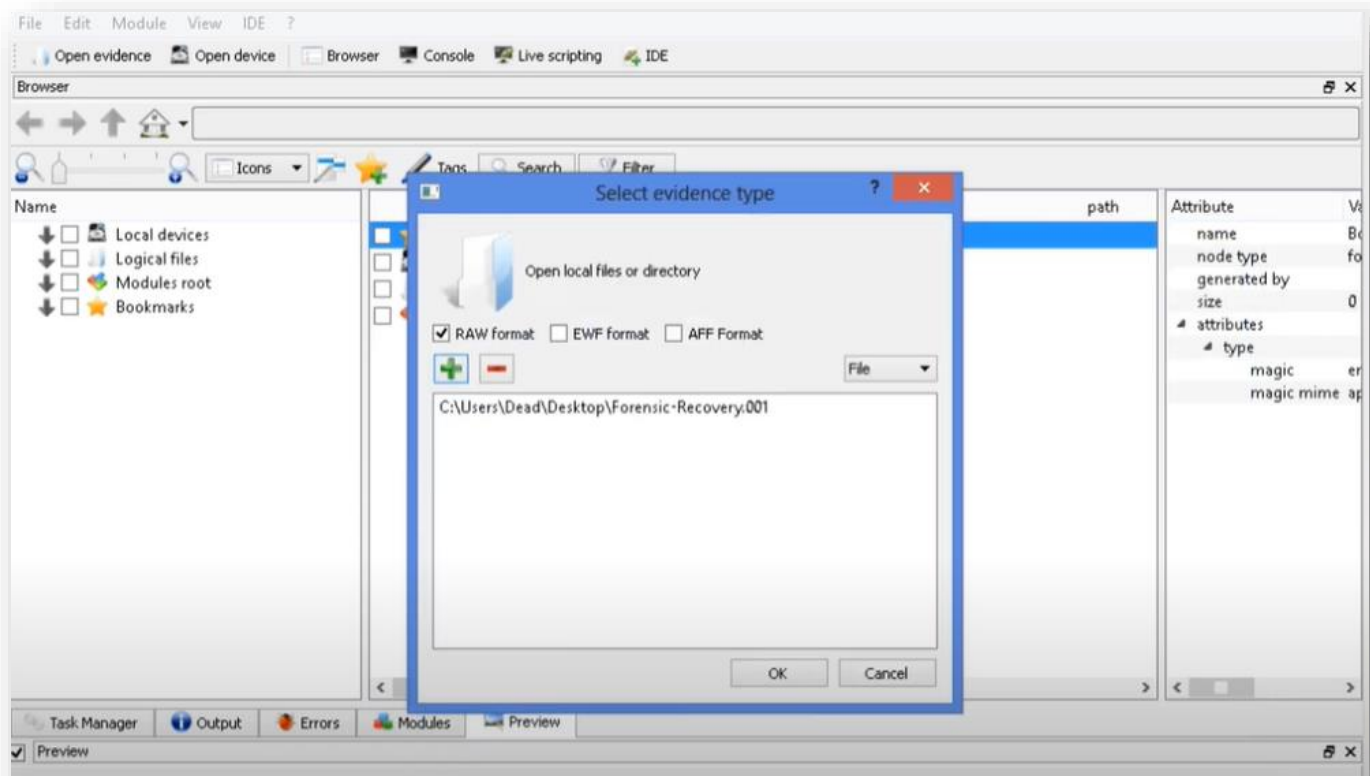


Figure 8.3.1.2 Adding image file in DFF

- The image file gets added under the section of “Logical Files”

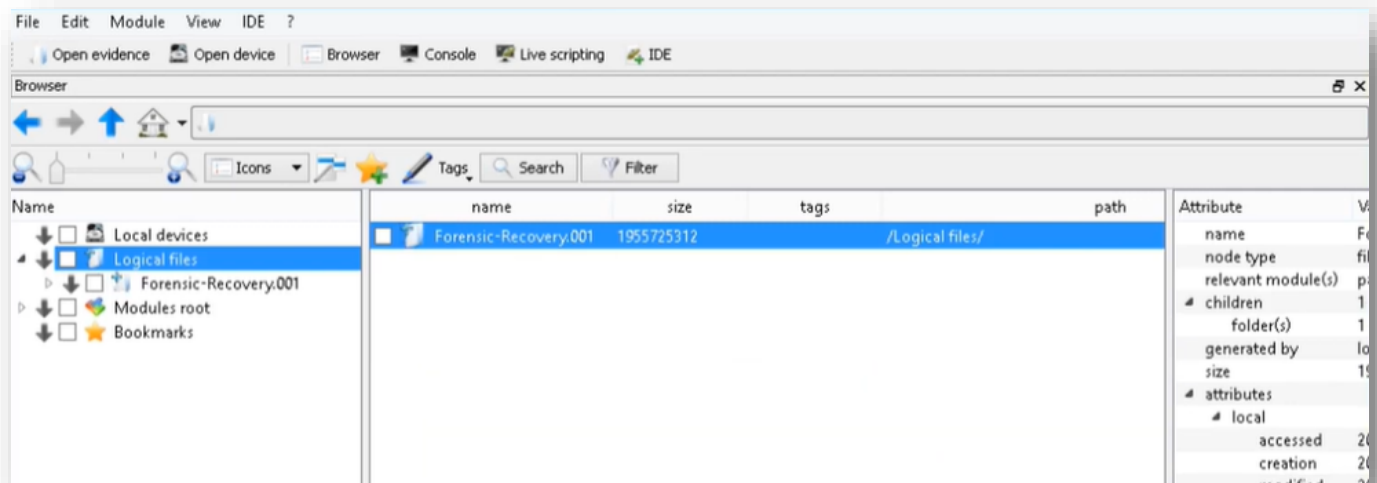


Figure 8.3.1.3 Image file listing in “Logical Files”

- Double click on the file to apply the Module Partitions on it. It would ask for the confirmation, click “yes”. After applying the Module Partitions, all the partitions present in the image file will be listed under the image file.

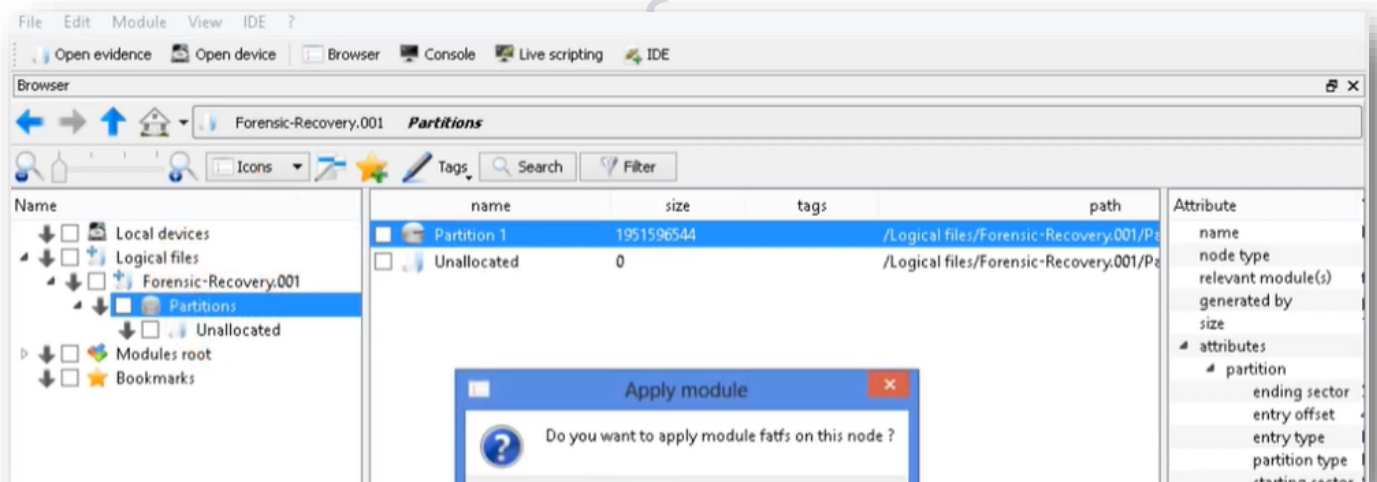


Figure 8.3.1.4 confirmation for applying Module Partition

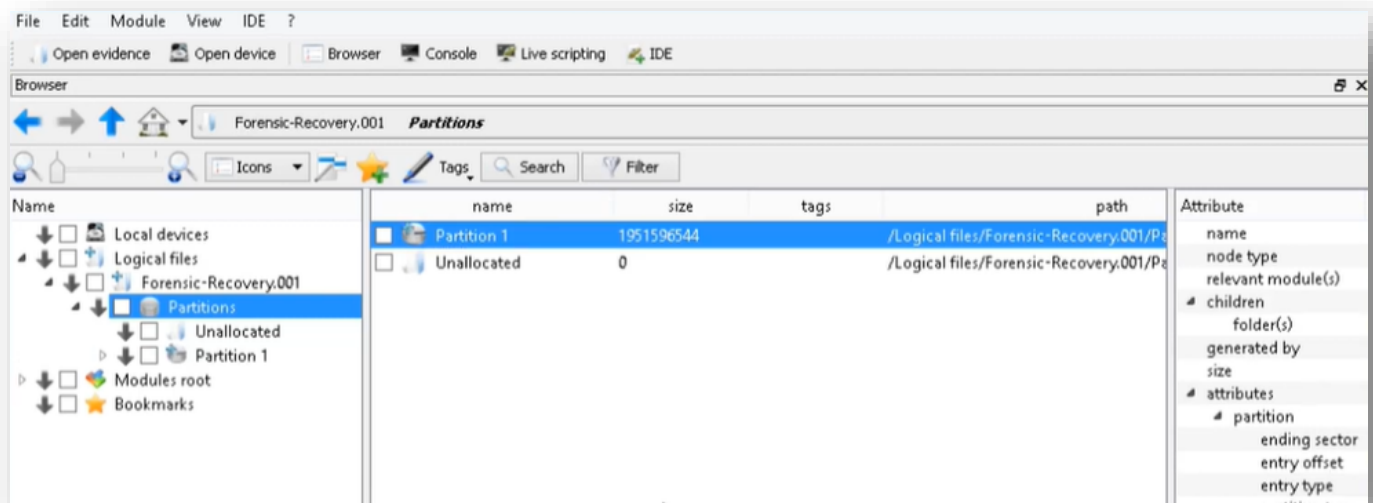


Figure 8.3.1.5 Listing of all partition present in the Image

- Double click on every Partition to apply the Module NTFS on it. It would ask for the confirmation, click "Yes". After applying the Module NTFS, all the Partitions will have "NTFS" and "NTFS" Unallocated" folders listed in it.

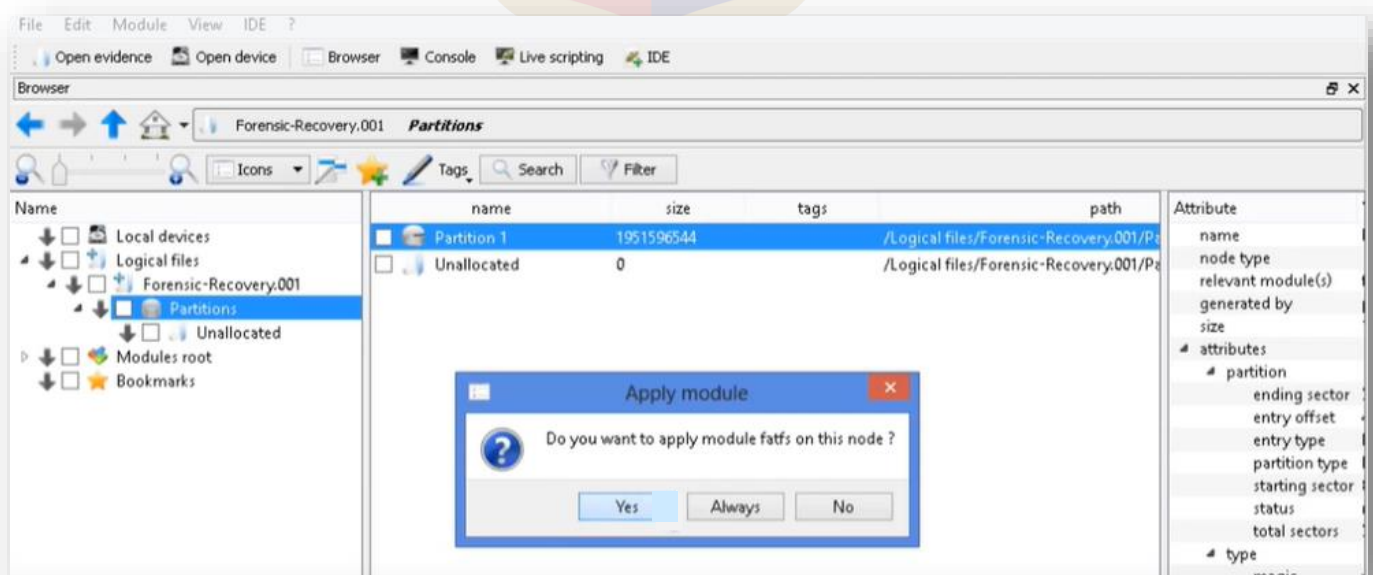


Figure 8.3.1.6 confirmation for applying Module NTFS.

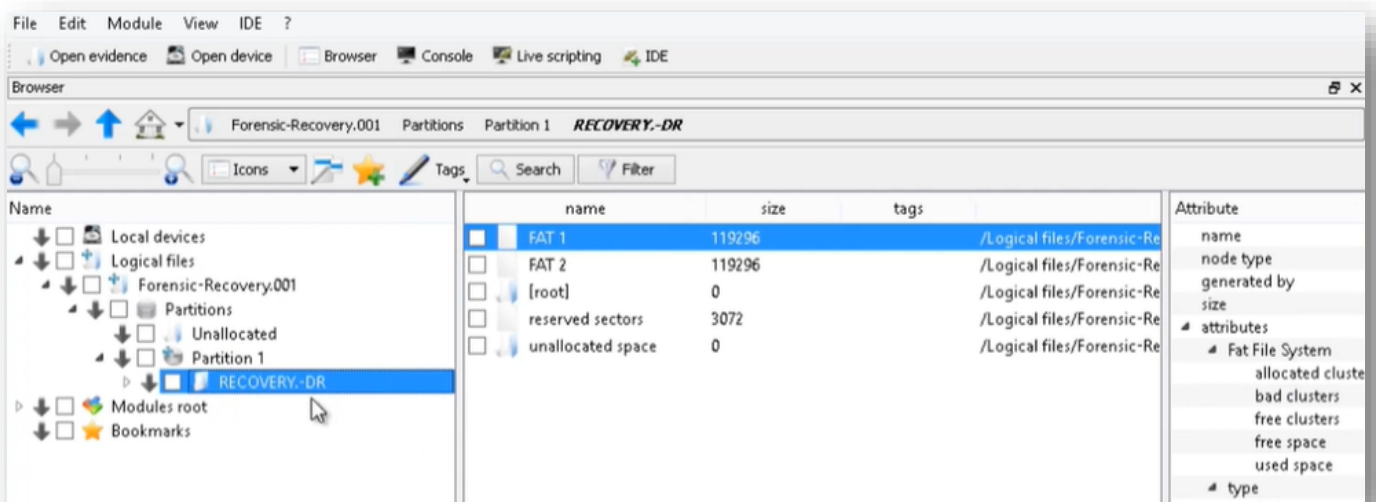


Figure 8.3.1.7 Listing of “FAT” and “unallocated” in Partition.

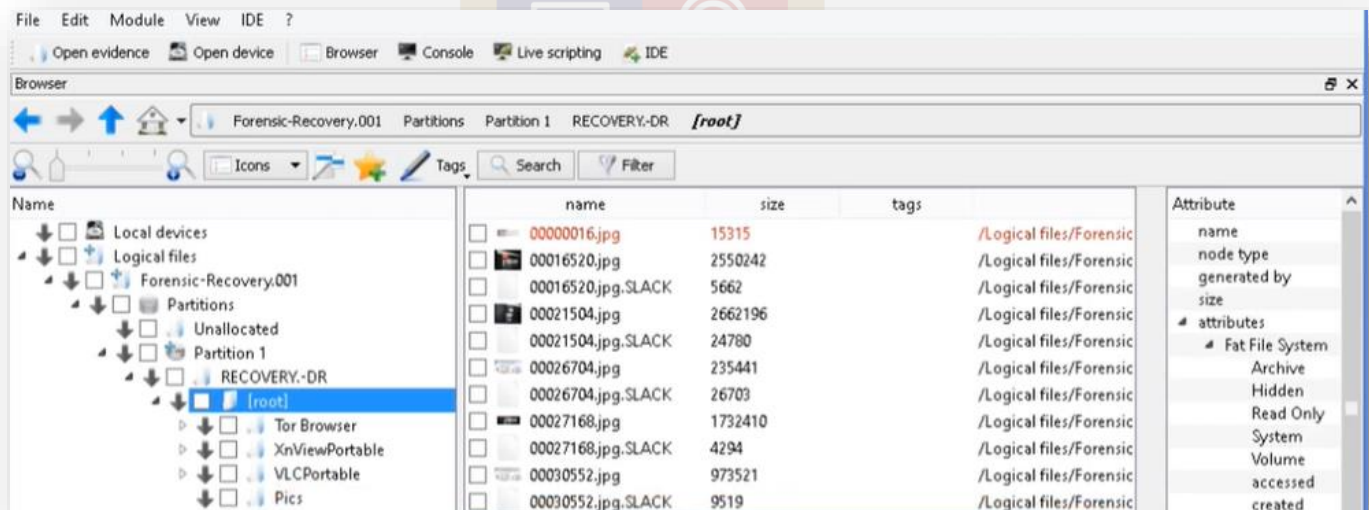


Figure 8.3.1.8 Content of “[root]” Folder in Partition 1.

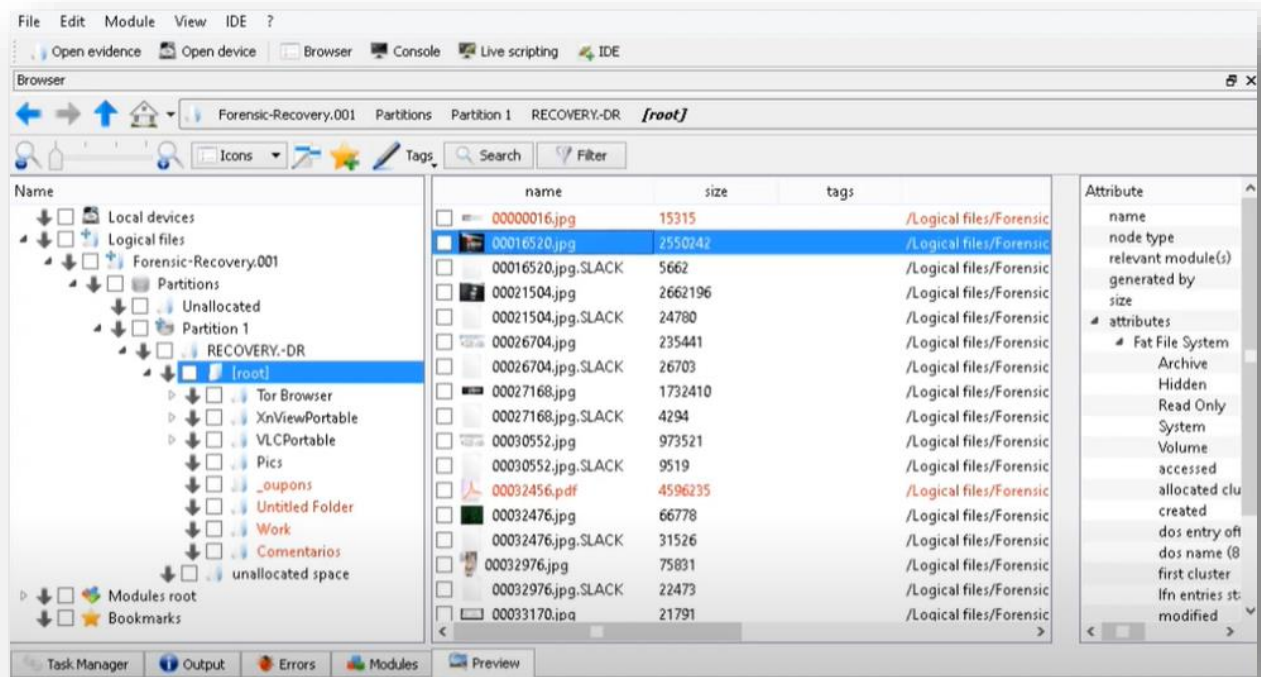


Figure 8.3.1.9 Content of "[root]" Folder in Partition 1.

9. Conclusion

During this Project work it was found that Petya ransomware encrypts/corrupts only the MBR or MFT of the system and the data files in the HDD/.vmdk remains intact. These data files can be retrieved by using the Autopsy software very easily without actually paying the Ransom demanded by the attacker.

Autopsy version 4.20 is used to Extracting the data for encrypted file. NotPetya utilized the Eternal Blue exploit, originally developed by the NSA and later leaked, to rapidly spread within networks. This contributed to its widespread impact and highlights the importance of timely patching and vulnerability management.



10.Future Work

Analysis of various other Ransomwares can be done to find a way to retrieve the data encrypted by them in decrypted form by using tools like and Autopsy.

Such Tools can also be used in future to analyze the working of the new ransomwares and finding new information about retrieval of the data Hijacked by the same.



11. Reference Links.


- <http://www.vinransomware.com/petya-ransomware>
- <https://blog.avast.com/inside-petya-and-mischa-ransomware>
- <https://blog.gdatasoftware.com/2016/03/28213-ransomware-petya-encrypts-hard-drives>
- <https://threatpost.com/petya-ransomware-encrypts-master-file-table/117024/>
- <https://www.virustotal.com/en/file/33ca487a65d38bad82dccfa0d076bad071466e4183562d0b1ad1a2e954667fe9/analysis/>
- <https://heimdalsecurity.com/blog/what-is-ransomware-protection/>
- [http://wiki.sleuthkit.org/index.php?title=The Sleuth Kit](http://wiki.sleuthkit.org/index.php?title=The_Sleuth_Kit)
- <https://www.sleuthkit.org/sleuthkit/docs.php> <http://tools.kali.org/forensics/df>
- [https://en.wikipedia.org/wiki/Digital Forensics Framework](https://en.wikipedia.org/wiki/Digital_Forensics_Framework)
- <http://www.arxsys.fr/>
- [SAFE17030FU1.pdf \(witpress.com\) \[1\]](#)
- [Microsoft Word - Avinash DFR RansomwareInvestigationv5-1.docm \(up.ac.za\) \[2\]](#)
- [The Title of the Paper Goes Here, in Title Case and Title Style \(researchgate.net\) \[3\]](#)
- [Behaviour Based Ransomware Detection.pdf \(waikato.ac.nz\) \[4\]](#)
- [Analysis-of-Ransomware-on-Windows-platform.pdf \(researchgate.net\) \[5\]](#)
- [https://ieeexplore.ieee.org/abstract/document/8703323/ \[6\]](https://ieeexplore.ieee.org/abstract/document/8703323/)
- [https://link.springer.com/chapter/10.1007/978-3-319-77028-4_15 \[7\]](https://link.springer.com/chapter/10.1007/978-3-319-77028-4_15)
- [https://www.researchgate.net/profile/Manoj-Gupta-35/publication/371470741 Eternal Blue Vulnerability/links/6484b55c79a722376524](https://www.researchgate.net/profile/Manoj-Gupta-35/publication/371470741_Eternal_Blue_Vulnerability/links/6484b55c79a722376524)

c949/Eternal-Blue-Vulnerability.pdf [8]

12.Plagarisiom Report

xyz.pdf

Ransomware Forensics (Petya) 012200300003014

 **National Forensic Sciences University**
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

PROJECT REPORT
ON
"Ransomware Forensics"
(Petya)

Submitted To
School of Cyber Security & Digital Forensics,
National Forensic Sciences University

For partial fulfilment for the award of degree
MASTER OF SCIENCE
In
DIGITAL FORENSICS AND INFORMATION SECURITY

Submitted By
Jay K. Bhalodiya
012200300003014

Under the Supervision of
Dr. Nilay Mistry

Share

Submission Details Help

Top sources All Sources

56 Similarity Exclusions

8%
Overall Similarity

1	srjis.com	2%
2	tekifumapixin.weebly.com	1%
3	www.nfsu.ac.in	<1%
4	yourbegininfo.blogspot.com	<1%
5	baadalsg.inflibnet.ac.in	<1%
6	link.springer.com	<1%
7	www.ijraset.com	<1%
8	docs.nopsema.gov.au	<1%
9	www.netkom.com	<1%
10	docslib.org	<1%

Page 1 of 44

