

# **ATM Malware Analysis**

Thesis submitted in partial fulfilment  
of the requirements of the degree of  
**Masters in Science with Specialization in  
Cybersecurity**

by

**Anshveer Chhabra**

**Roll Number - 06**

**G.R. Number - 3509468**

Under the Supervision of

**Prof. Sagar Mehta**



**April 2023**

**Nagindas Khandwala College(Autonomous)  
Malad, Mumbai 400064**



## **CERTIFICATE**

This is to certify that the dissertation entitled **“ATM Malware Analysis”** is a bonafide work of **“Anshveer Chhabra”** (Roll No: 06 and G.R. No: 3509468) submitted to the Nagindas Khandwala College(Autonomous),Mumbai in partial fulfillment of the requirement for the award of the degree of **“Masters in Science with Specialization in Cybersecurity”**.

**(Prof. Sagar Mehta)**

Internal-Examiner

External Examiner



## Supervisor's Certificate

This is to certify that the dissertation entitled “**ATM Malware Analysis**” submitted by **Anshveer Chhabra, Roll No: 06** and **G.R. No: 3509468**, is a record of original work carried out by him/her under my supervision and guidance in partial fulfillment of the requirements of the degree of **Masters in Science with Specialization in Cybersecurity** at Nagindas Khandwala College(Autonomous), Mumbai 400064 . Neither this dissertation nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

**(Prof. Sagar Mehta)**

Internal Examiner



## Declaration of Originality

I, **Anshveer Chhabra**, Roll No: 06 and G.R. No: 3509468, hereby declare that this dissertation entitled “**ATM Malware Analysis**” presents my original work carried out as a Master Student of Nagindas Khandwala College(Autonomous), Mumbai 400064. To the best of my knowledge, this dissertation contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of Nagindas Khandwala College(Autonomous), Mumbai or any other institution. Works of other authors cited in this dissertation have been duly acknowledged under the sections “Reference” or “Bibliography”. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I am fully aware that in case of any non-compliance detected in future, the Academic Council of Nagindas Khandwala College(Autonomous), Mumbai may withdraw the degree awarded to me on the basis of the present dissertation.

**Date:**

**Place:**

**Anshveer Chhabra**

SIDR SOLUTIONS & TECHNOLOGIES PVT LTD  
49, ADITYA ESTATE, Behind Evershine Mall,  
Mindspace, Malad West, Mumbai-400064  
GSTIN: 27AAZCS1256J1ZO : PAN NO:AAZCS1256J  
CIN NO: U74999MH2017PTC298942



Mr. AnshveerChhabra  
Mumbai

Dear Anshveer,

We are glad to offer you an internship in our organization for a period of 6 months starting October 17, 2022.

The following will be the terms of contract :

1. You will be paid a stipend of Rs. 5000/- per month.
2. Working Hours - Working days will be from Monday to Friday. The working hours for your profile will be from 10 am till 6 pm. However, if there is urgent work that needs to be done and completed on Saturday/Sunday, you will need to be in office.
3. In case you are absent from work and have not informed management you will have loss of pay for those days.
4. During your period of engagement with the company, you will have to maintain complete secrecy on projects you will be working on, about clients and their company. Sharing of confidential information outside the company will be considered as a criminal offence.
5. You should be available to travel outside Mumbai for any company related work. The expenses will be borne by the company.
6. During your tenure with SIDR, you will not be allowed to take up any other employment.

If you agree with these terms and conditions, request you to kindly sign the duplicate copy of this letter.

Best Regards,

A handwritten signature in blue ink, appearing to read "K. Krishna Kumar", followed by a stylized flourish.

Krishna Kumar  
Director

# **Abstract**

Over the years, ATM thefts have been undertaken in a variety of ways: from blowing up safes to gluing on skimmers and attaching fake keypads to installing malware executables. In particular, the use of malware in attacking ATMs has seen considerable adoption among cybercriminals, and one of the primary factors contributing to its sustained use is the fact that many of the targeted machines still use outdated operating systems. Such systems no longer receive critical security updates, so in the most basic sense, system vulnerabilities are not addressed, let alone resolved. Among cybercriminals who use malware to attack and steal cash from ATMs, gaining physical access has become perhaps the most common approach [1].

This project is done to identify the malware in a ATM system and analyzing the malware using several tools. Malware analysis has become really important nowadays and can be adopted to prevent the system from malware attacks.

<b>Table of Contents</b>		
<b>CHAPTER 1 :</b>	<b>INTRODUCTION</b>	<b>1-3</b>
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Objective	3
<b>CHAPTER 2 :</b>	<b>LITERATURE SURVEY</b>	<b>4</b>
<b>CHAPTER 3 :</b>	<b>METHEDOLOGY</b>	<b>5-18</b>
	3.1 Introduction	5
	3.2 Requirements: Hardware and Software	6
	3.3 Methodology	7
<b>CHAPTER 4 :</b>	<b>CONCLUSION</b>	<b>19</b>
<b>CHAPTER 5 :</b>	<b>REFERENCES</b>	<b>20</b>

## **CHAPTER 1 : INTRODUCTION**

### **1.1 INTRODUCTION**

Nowadays, Internet becomes an essential part of the daily life of many people. Several services are available and growing daily on the internet. These services are being used by an increasing number of people. One example of an Internet business service is online banking or advertising. Similar to the real world, there are those online who wish to harm others by taking advantage of honest users whenever money is involved. These individuals achieve their objectives with the aid of malicious software such as malware. Security suppliers, including makers of antivirus software, offer detection and analysis techniques to shield authorized users from a variety of dangers.. Various online tools can dynamically analyze the malware and detect it, the tools use cloud computing hence they are more efficient and safer. The main idea of this project is to identify the malware or a malicious file, perform the analysis and then finally prepare a report and submit it to the concerned authorities.



## 1.2 PROBLEM STATEMENT

Trojans, viruses, worms, and ransomware are the four main categories of malware. Every major operating system, including those from Apple, Android, and Windows, is exposed to malware. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- For monetary benefit, i.e., to enable the user to make money through theft, fraud, advertising, or ransom.
- For intellectual advantage, which results in the disclosure of information (such passwords, extortion demands, or top-secret data) to the malware owner or the general public.
- Investigate the infected user's local network.
- Steal sensitive data.

The purpose of this project is to focus on eliminating all of the above points by removing the malware itself from the system. Our main aim is to first identify the malware, because if we are not able to detect it, then it is of no use. Cybercriminals will keep on increasing, and so will the malware attacks that they conduct for their own greed and money. To avoid this problem and protect the system from malware attacks, a complete malware analysis is required.

### **1.3 OBJECTIVE**

The growing dependency on digital systems, which accelerated immensely during the COVID-19 pandemic, also led to a massive increase in malware and particularly ransomware-related incidents in recent years [2]. To avoid and mitigate the chances of the system getting affected with the malware, malware analysis is performed and it is really important. The objective of this project is to determine the capability of malware, detect it, and contain it. It also helps in determining identifiable patterns that can be used to cure and prevent future infections. The goal of malware analysis is to gain an understanding of how a specific piece of malware functions so that defenses can be built to protect an organization's network. There are two key questions that must be answered. The first: is there a malware in the system? The second: what exactly does this malware do and when it was created? Here are some key benefits of this process: Identifying the Malware, Identifying the source of the attack, Determining the damage from a security threat, Deleting the malicious file and Reporting the malware.

## CHAPTER 2 : LITERATURE SURVEY

The research articles on malware analysis listed a number of methods and procedures that might be used to find and examine malware. There are two fundamental approaches of analysing malware: static and dynamic. Most research conclude that dynamic analysis is far more accurate and effective than static analysis. Some papers provide an overview of various malware analysis techniques and tools, including static analysis, dynamic analysis, and hybrid analysis, while others provide an industry perspective on malware analysis, including the challenges faced by organisations in detecting and mitigating malware. The authors also discuss the challenges and limitations of each technique and suggest future research directions. One of the paper presents a study of automated dynamic malware analysis using Cuckoo Sandbox, an open-source software package and implementation of MALPRACTICE, a tool for practical malware analysis. The authors evaluate the effectiveness of Cuckoo Sandbox in identifying malware behavior and compare it with other approaches and even demonstrates the effectiveness of their tool in identifying malware behavior and detecting anti-analysis techniques.

Malware Detection using Machine Learning Techniques: A Survey by Sanket S. Shinde et al. (2020) - This paper provides an overview of the machine learning techniques used in malware detection, including feature extraction, feature selection, and classification algorithms. The authors also discuss the challenges and limitations of these techniques and suggest future research directions. A Framework for Automated Malware Analysis and Classification by Wei Hu et al. (2014) - This paper proposes a framework for automated malware analysis and classification using a combination of static and dynamic analysis techniques. The authors evaluate the effectiveness of their framework and discuss the challenges and limitations of automated malware analysis.

## **CHAPTER 3 : METHEDOLOGY**

### **3.1 INTRODUCTION**

Malware is a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network. Cybercriminals typically use it to extract data that they can leverage over victims for financial gain. That data can range from financial data, to healthcare records, to personal emails and passwords—the possibilities of what sort of information can be compromised have become endless [3]. Generally malware is categorized into following categories:

**Virus:** It is a program that attaches itself to other programs in order to infect that program and perform some unwanted function

**Trojan:** Trojan makes copies of themselves and steals information. It is standalone malicious program that does attempt to infect other computers in a completely automatic manner without help from outside forces like other programs.

**Worms:** A worm is self replicated malware computer program which uses computer and network resources without authenticated user permission. In the network, it consumes the network bandwidth.

**Spyware:** It is installed without a user's knowledge in order to report the behaviour of the user to the attacker.

Malware Analysis is the practice of determining and analyzing suspicious files on endpoints and within networks using dynamic analysis, static analysis, or full reverse engineering [4]. A strong Malware Analysis practice aids in the analysis, detection, and mitigation of potential threats. Malware Analysis can help organizations identify malicious objects used in advanced, targeted, and zero-day attacks [4]. Malware Analysis is important because it helps security operations teams rapidly detect and prevent malicious objects from gaining persistence and causing destruction within the organization [4].

## **3.2 REQUIREMENTS**

### **Hardware Used:-**

Laptop

Tableau

External HDD

Pendrive

### **Software and Tools Used:-**

AccessData FTK

OSForensics

Comodo Cleaning Essential (CCE)

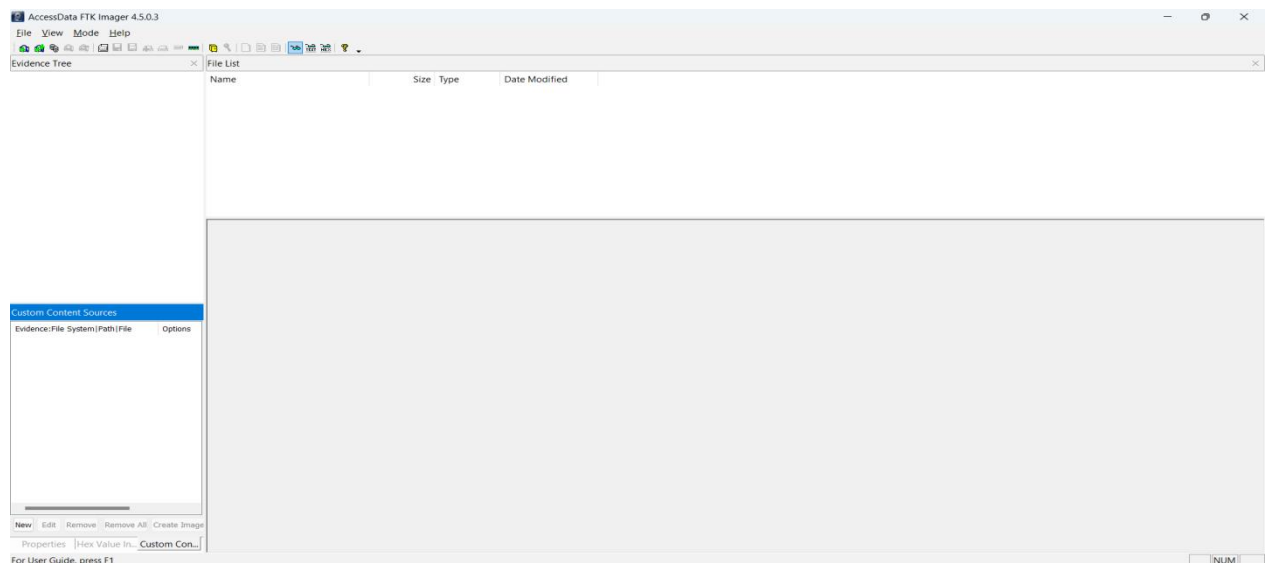
Virus Total

### 3.3 METHEDOLOGY

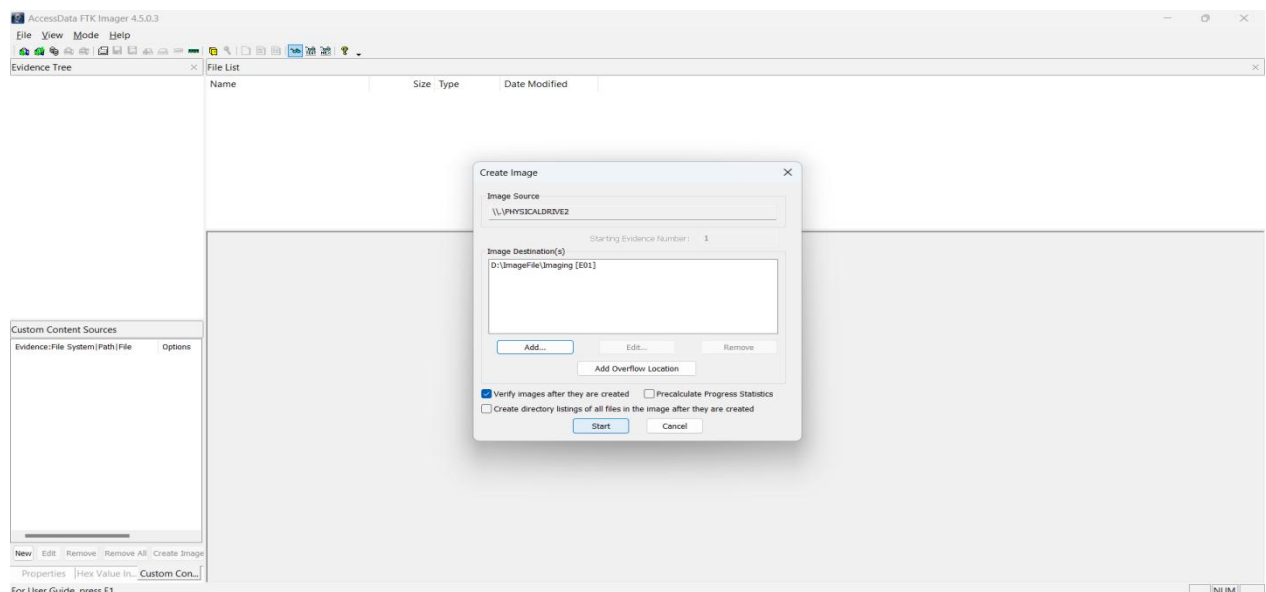
#### Imaging of the Hard Disk Drive using AccessData FTK Imger

FTK® Imager can create perfect copies, or forensic images of computer data without making changes to the original evidence. The forensic image is identical in every way to the original, including file slack and unallocated space or drive free space. This allows you to store the original media away, safe from harm while the investigation proceeds using the image [5].

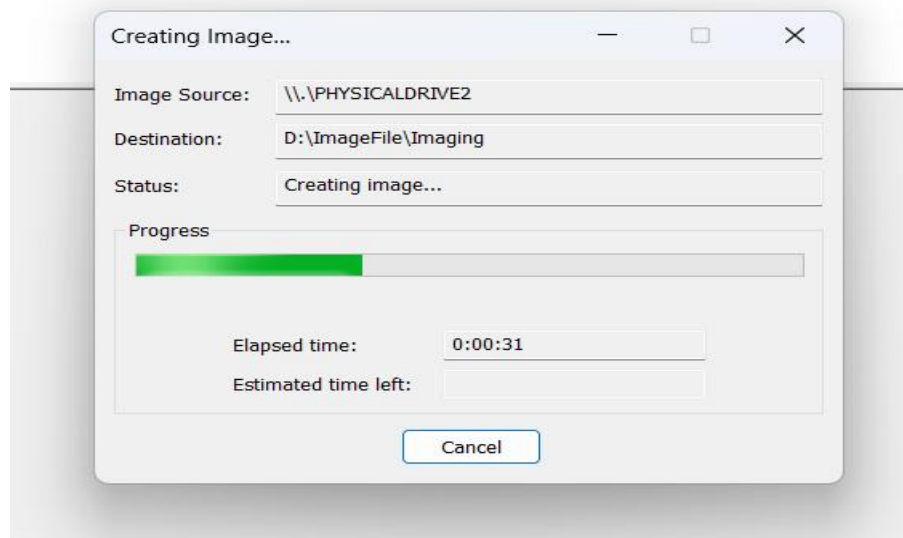
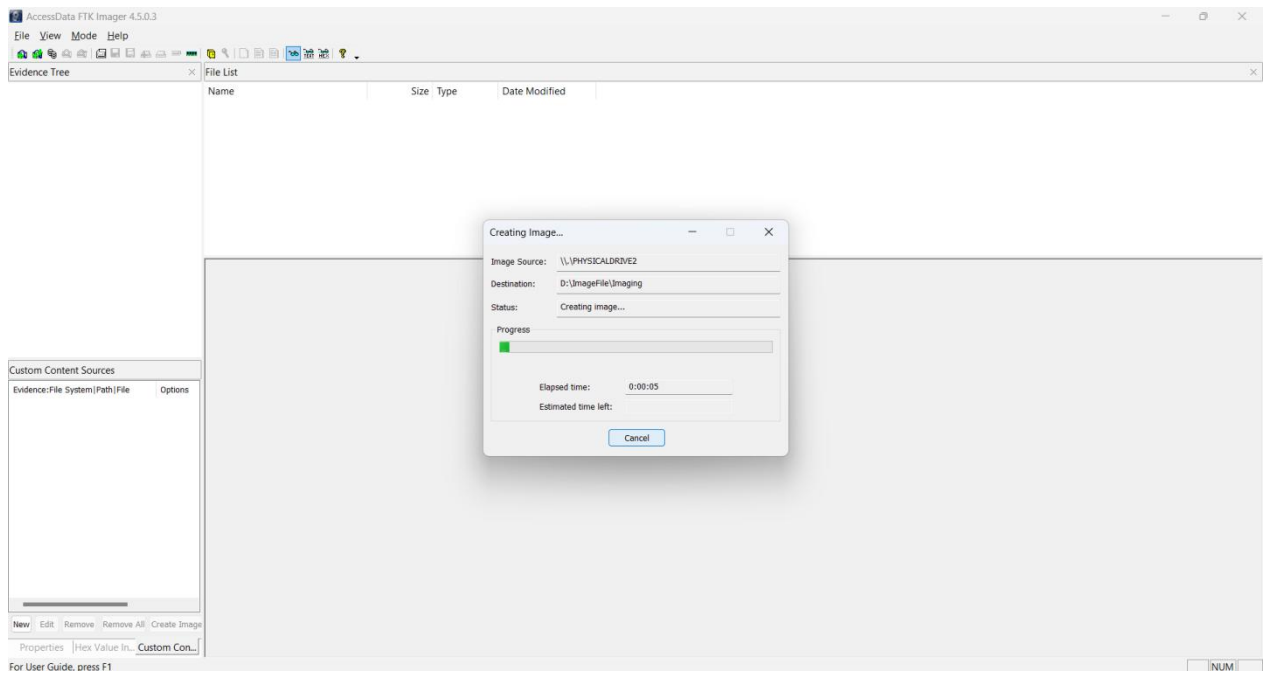
➤ Firstly, to the the imaging of the the HDD, I have used AccessData FTK Imager.



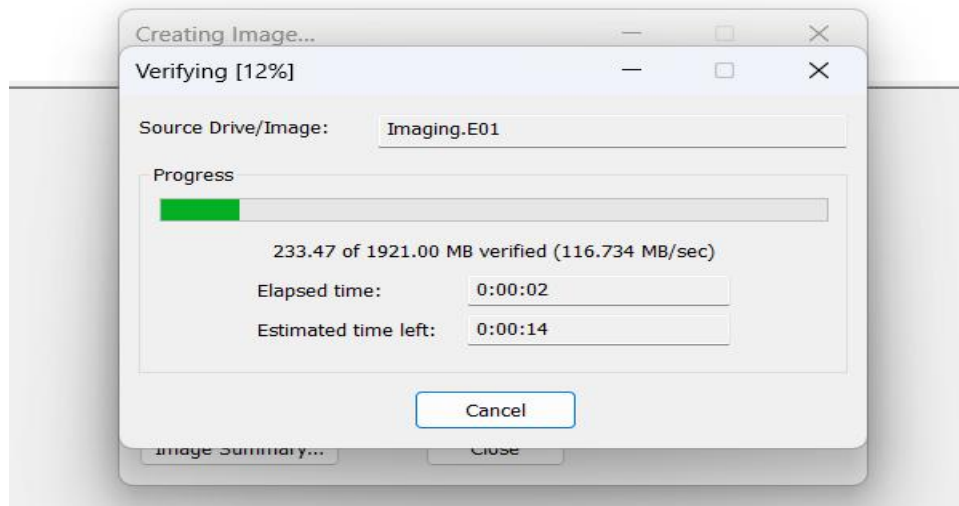
➤ Here, I have added the Source and the Destination Folder of the Image.



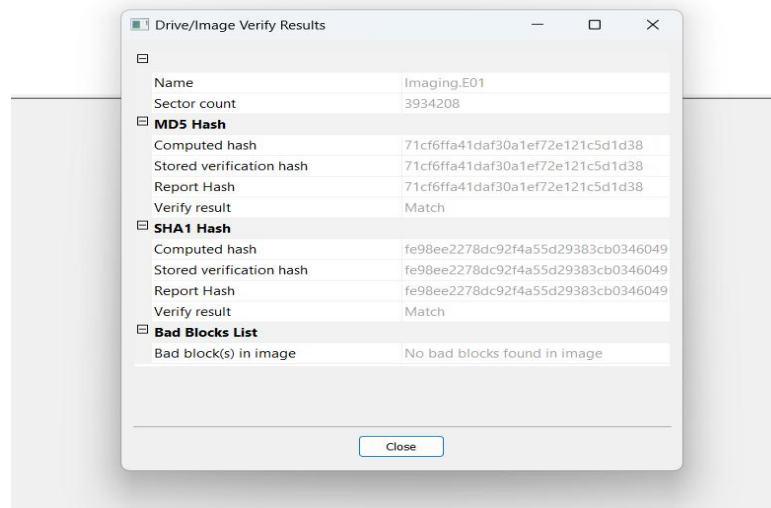
- Imaging has been started.



- After the imaging is done, it then verifies the image created.

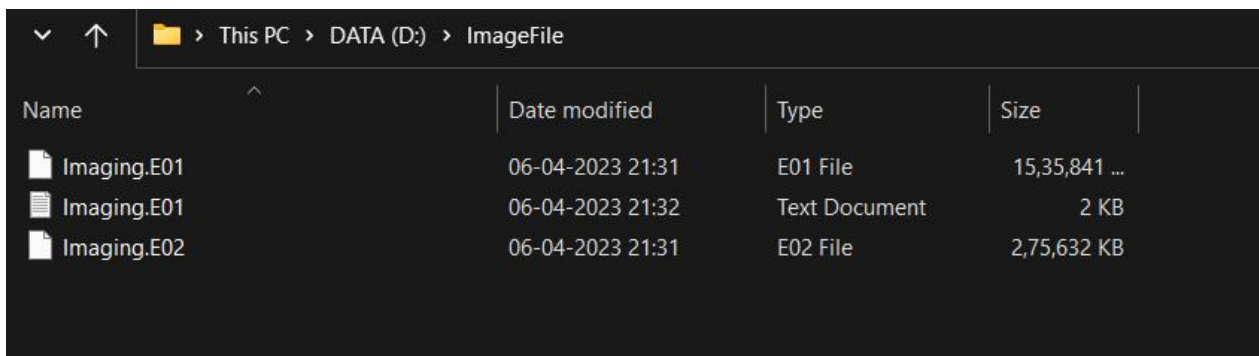


- After Verification, here I have got the results.





- The Image file is created successfully.

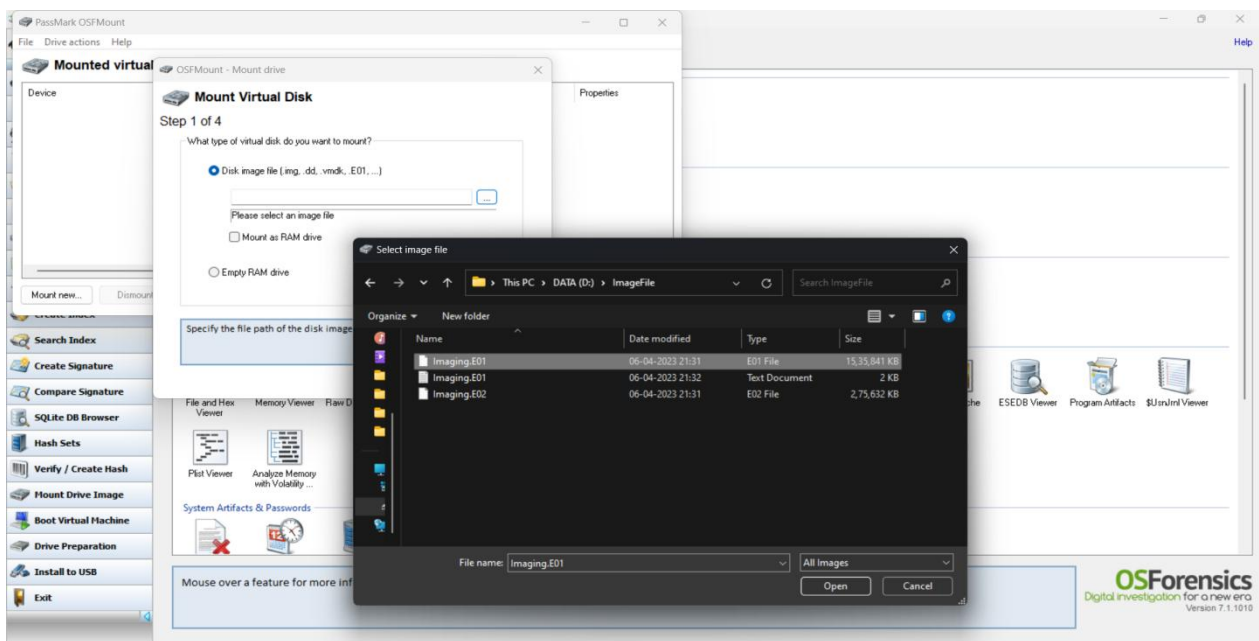


Name	Date modified	Type	Size
Imaging.E01	06-04-2023 21:31	E01 File	15,35,841 ...
Imaging.E01	06-04-2023 21:32	Text Document	2 KB
Imaging.E02	06-04-2023 21:31	E02 File	2,75,632 KB

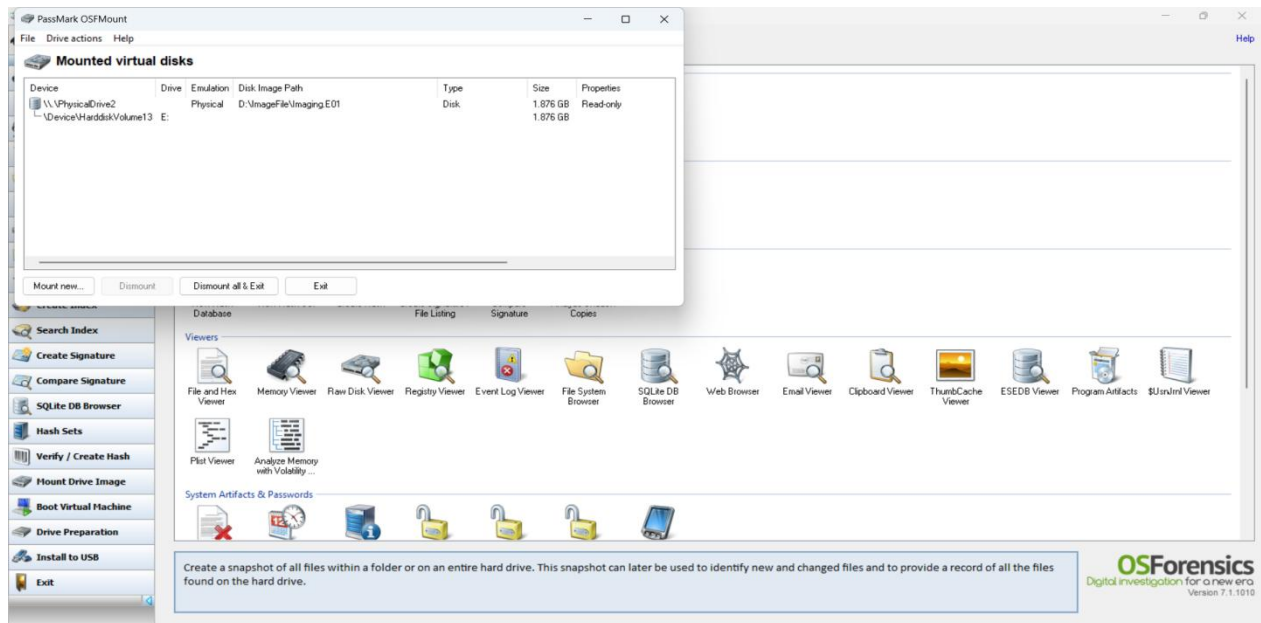
## Mounting the Image File using OSForensics

OSForensics lets you extract forensic evidence from computers quickly with high performance file searches and indexing. Identify suspicious files and activity with hash matching, drive signature comparisons, e-mails, memory and binary data. OSFMount allows you to mount local disk image files in Windows as a physical disk or a logical drive letter [6].

- Here I have used OSForensics to mount the image file.



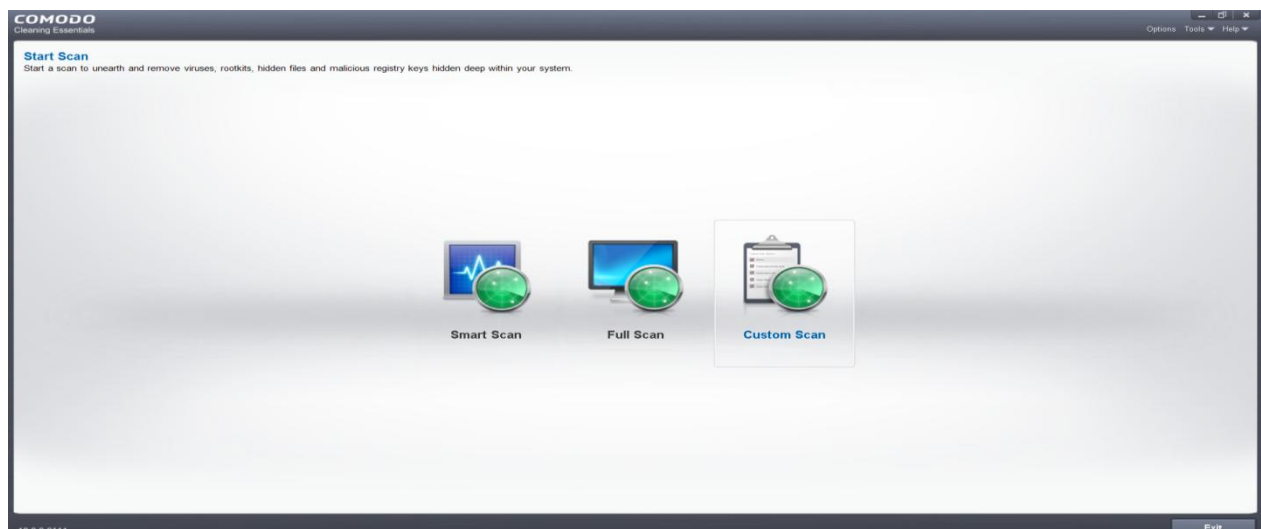
- The image file has been mounted.



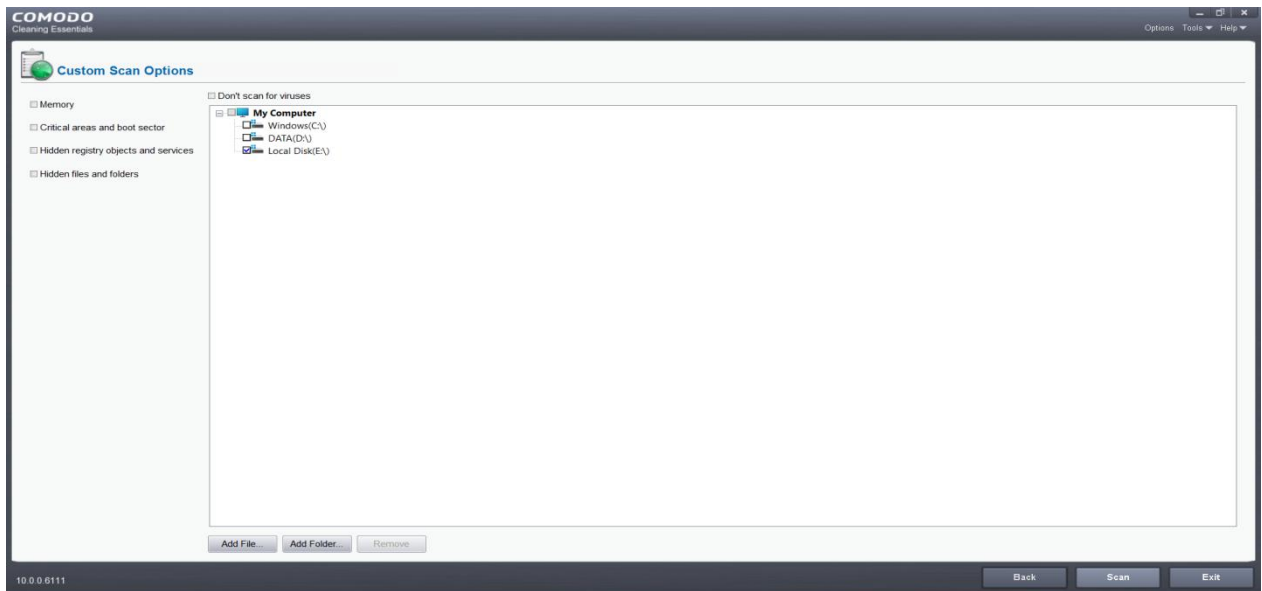
## Detecting Malware and Malicious Files using Comodo Cleaning Essentials (CCE).

Comodo Cleaning Essentials (CCE) is a set of computer security tools designed to help users identify and remove malware and unsafe processes from infected computers. CCE is a lightweight, portable application which requires no installation and can be run directly from removable media such as a USB key, CD or DVD [7].

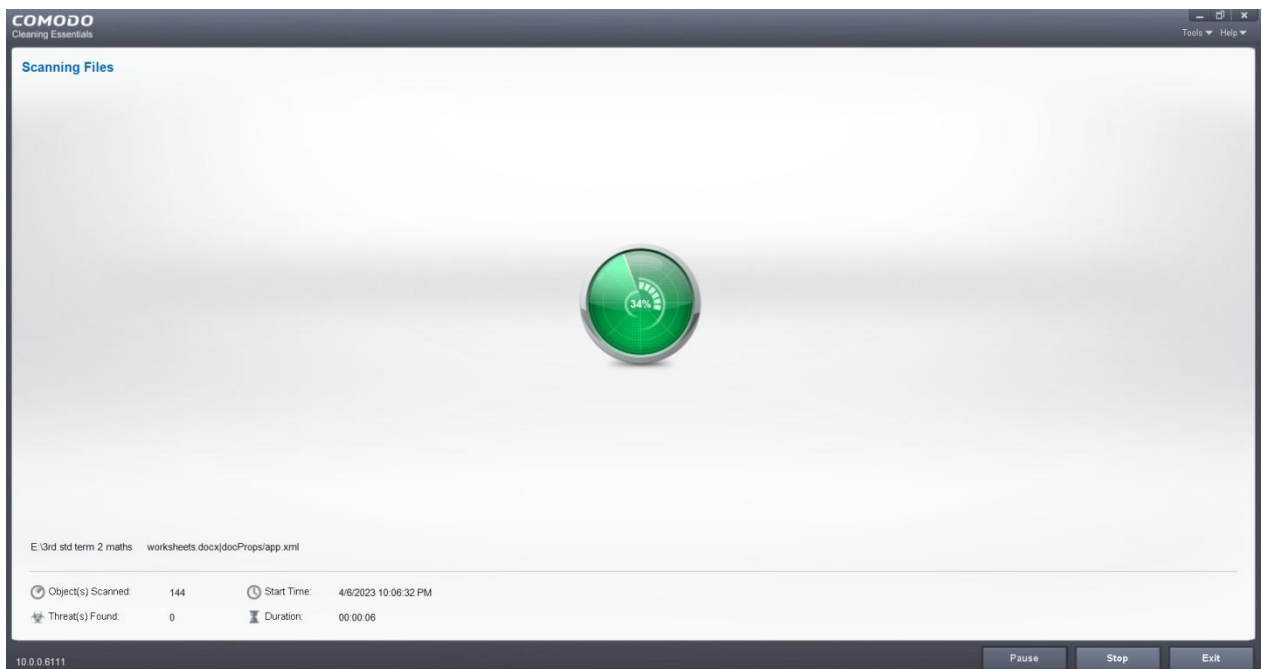
- After mounting the image file, here I have used CCE to check for any Malware or Malicious files present in that system.



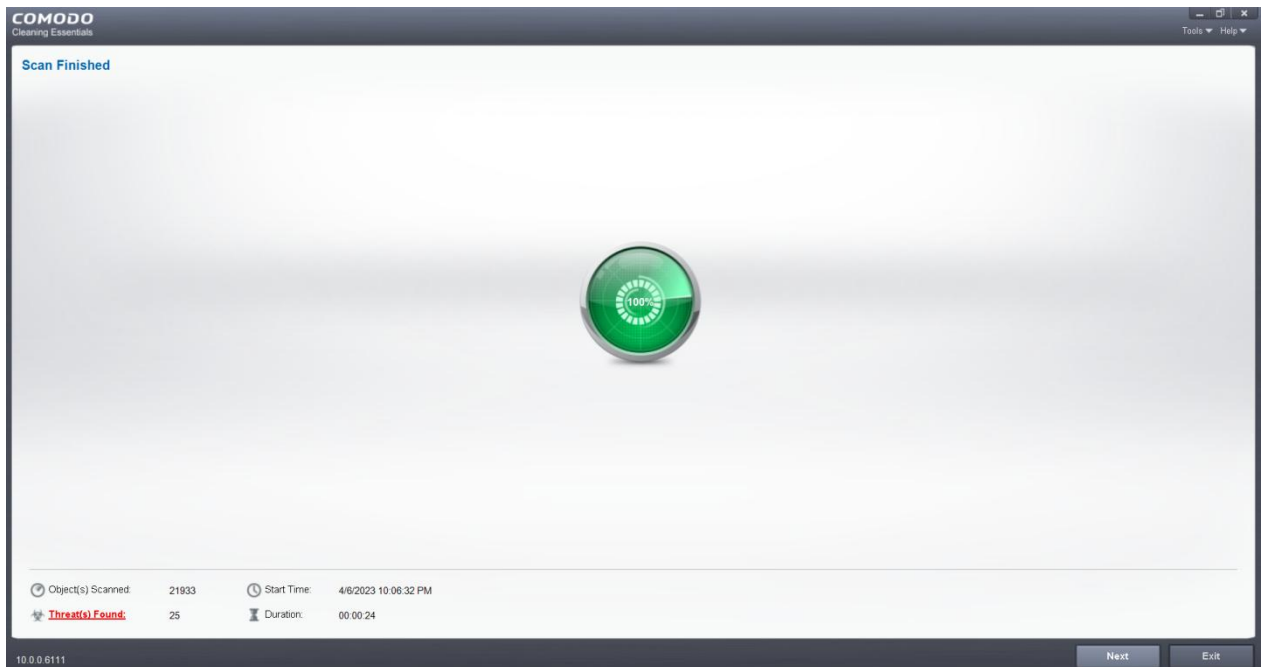
- I have selected the drive that I want to scan to detect the malware or any Malicious File(if any).



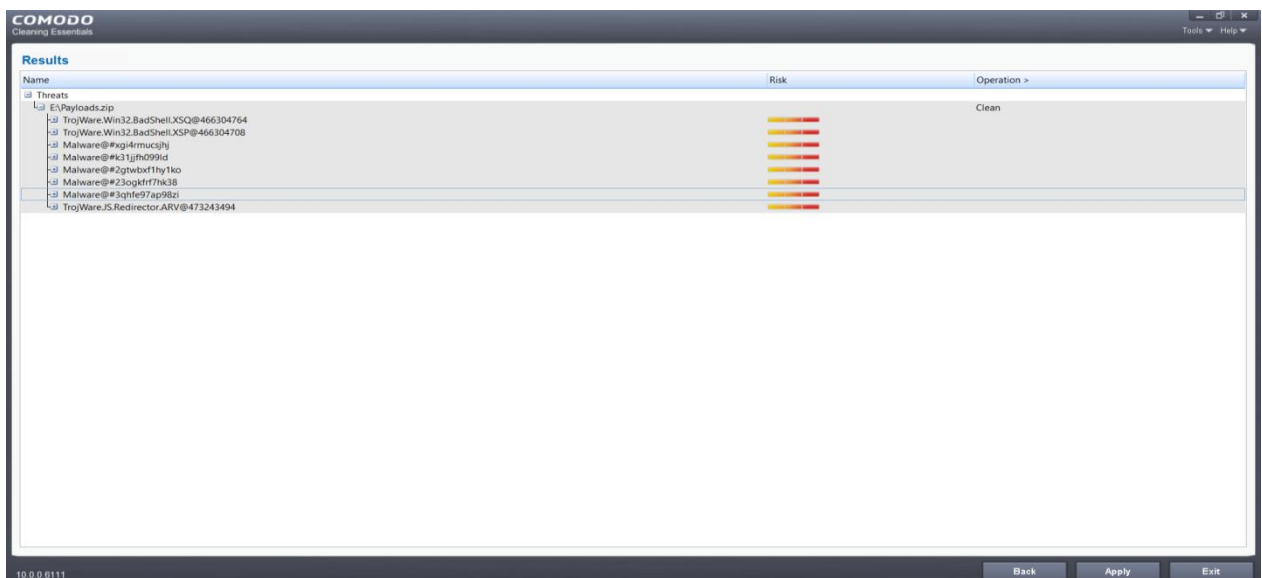
- After Selecting the drive that we want to scan, CCE will start scanning the selected drive.



- After the scanning is finished, we will come to know the malware files that are present.



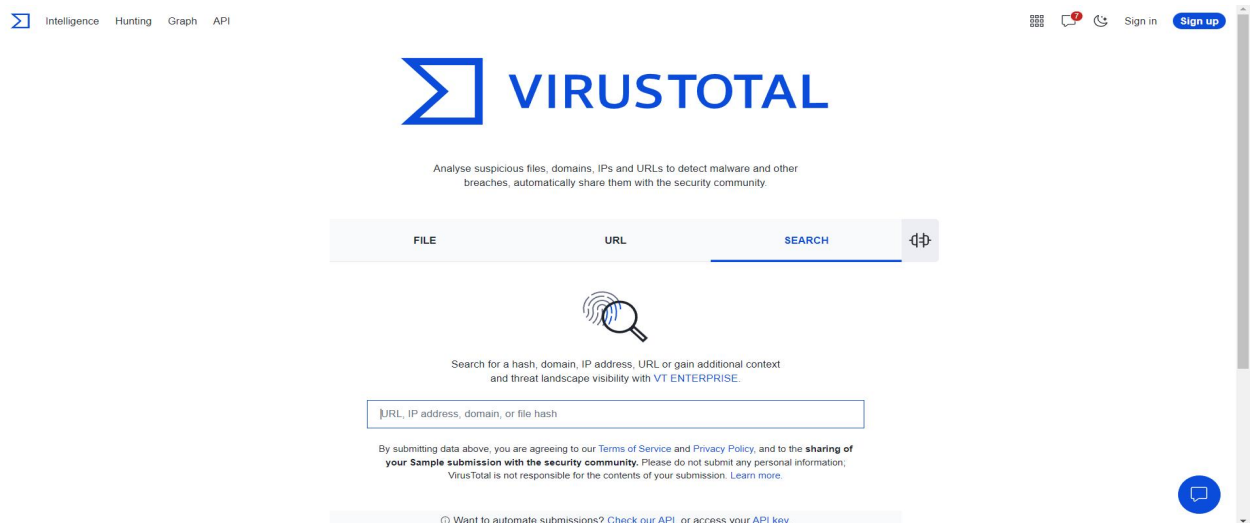
- These are the results of the scan conducted. Here we can clearly see the Malware and Malicious files that are present in the drive.



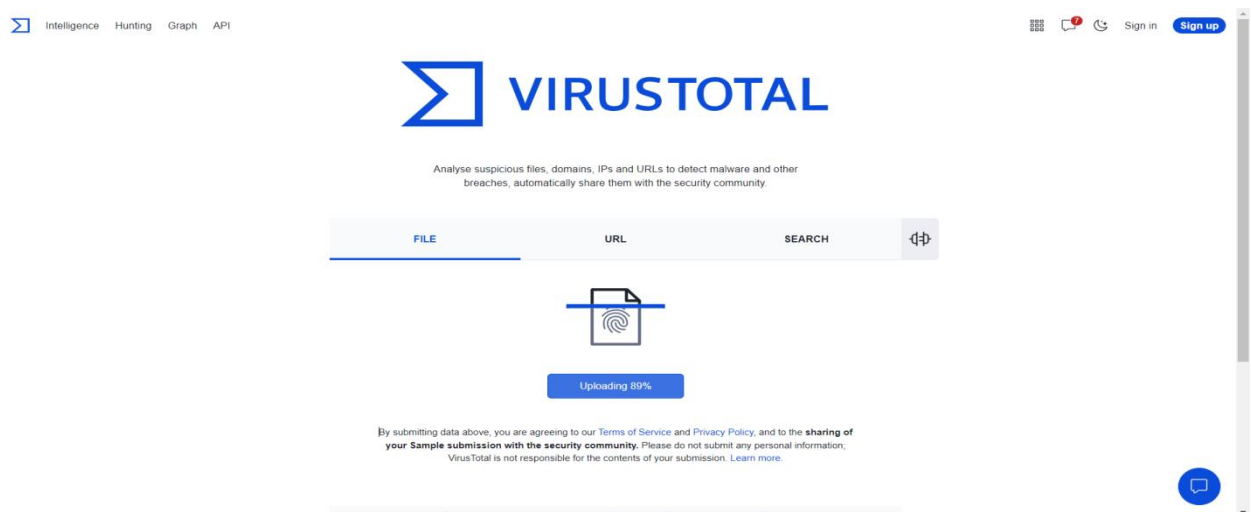
## Inspecting the Malware on Virus Total

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal. VirusTotal offers a number of file submission methods, including the primary public web interface, desktop uploaders, browser extensions and a programmatic API [8].

- After getting the malware, I have used Virus Total to inspect the malware.



- I have added the malware to the Virus Total or we can even take the hash value of the file and upload it.



- Here, Virus Total is showing me that out of 63 Security vendors 52 vendors have detected the file as malicious file.

**52 / 63** Community Score

52 security vendors and no sandboxes flagged this file as malicious

File: b7efb199b6b3c5525bb63e8e0495f8af30c225de02bac3d3e6fe19f695d12446  
 Payloads: zip  
 Size: 6.96 MB  
 Date: 2023-04-06 16:40:05 UTC  
 Uploaded: 1 minute ago

Threat categories: trojan, virus, downloader  
 Family labels: eicar, test, file

Security vendors' analysis	Threat categories	Family labels
AhniLab-V3	Virus/EICAR_Test_File	Trojan/JS_Redirector.aah
Arcabit	Generic.IQYDownloader.2.09899068 [m...]	JSP.CVE-2022-29464-A [Exp]
Avast-Mobile	Eicar	JSP.CVE-2022-29464-A [Exp]
Avira (no cloud)	SPR/RemoteShell.LFJA	Win32.Test.Eicar.a
BitDefender	Generic.IQYDownloader.2.09899068	EICAR-Test-File (not A Virus)

- At last I have selected the Clean operation to be performed to clean out the malware.

**COMODO Cleaning Essentials**

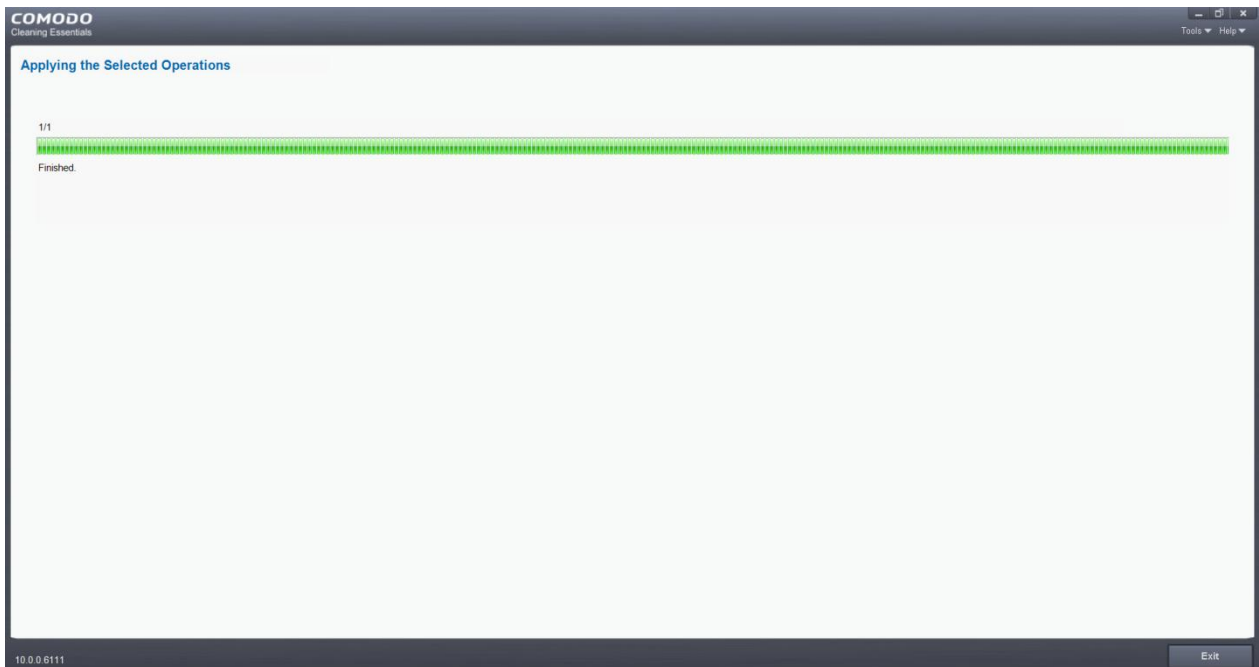
**Results**

Name	Risk	Operation
Threats		
E:\Payloads.zip		Clean
TrojWare.Win32.BadShell.XSQ@466304764	High	Clean
TrojWare.Win32.BadShell.XSP@466304708	High	Clean
Malware@#mj4rmucslj	High	Clean
Malware@#k31jfh099ld	High	Clean
Malware@#2gtwbt1hy1ko	High	Clean
Malware@#23ogkrf1hk38	High	Clean
Malware@#3qhye97ap98zi	High	Clean
TrojWare.JS.Redirector.ARV@473243494	High	Clean

10.0.0.6111

Buttons: Back, Apply, Exit

- CCE i.e. Comodo Cleaning Essentials deletes the malware.



- After doing all this I have to prepare a report and send it to the concerned authorities. Few Screenshots of the report have been added.

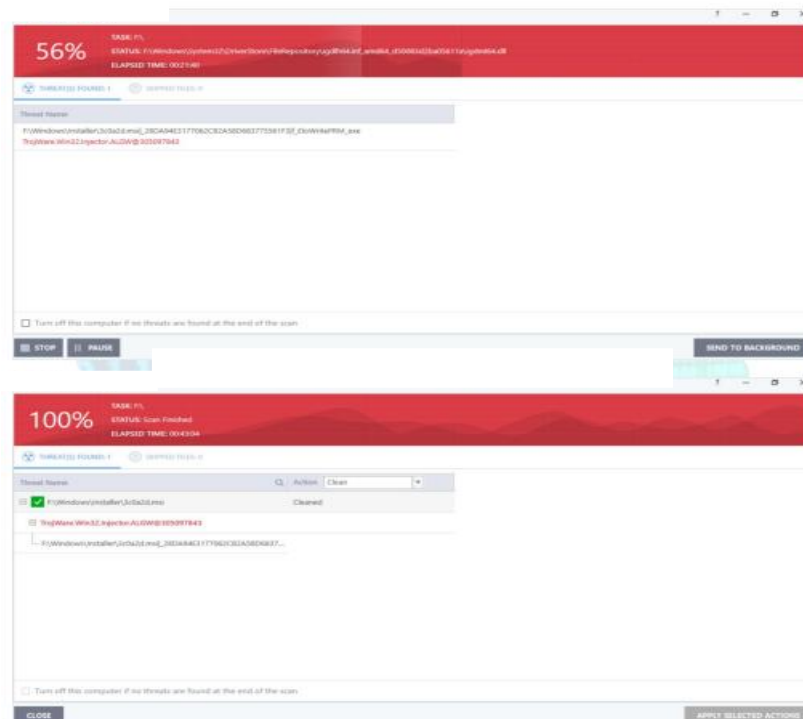


# TABLE OF CONTENT

SCOPE .....	3
TOOLS USED .....	3
IDENTIFICATION OF SN: ZA4A7VF2 .....	4
Operational Parameters, Hash Information, Verify Information .....	4
MALWARE ANALYSIS OF SN: ZA4A7VF2 .....	5
Method 1 : Scanning with Comodo Cleaning Essentials (CCE) .....	5
Method 2 : Scanning With Xcitium - Advanced Anti-Malware Software .....	6
Method 3 : Analysing Suspicious file with Virus Total .....	7
Method 4: Analysing Suspicious File with Any.Run .....	8
Method 5: Analyzing Using OSForensics .....	9

## Method 2 : Scanning With Xcitium - Advanced Anti-Malware Software

Using “Xcitium – Advanced Anti-Malware” Software, malware analysis was carried out.



**Observation :** Malicious file was found after scanning.  
**File name:** 3c0a2d.msi



**Observations:** No registry files found on hard disk image.

## **RECOMMENDATIONS**

- 1) Every 3 months the drive should be thoroughly scanned to prevent malicious activity.
- 2) Anti-malware software should be installed on the system.
- 3) Xcitium is a highly recommendable anti-malware software.

Page 15 of 16

---

**Malware Analysis conducted by:**

Anshveer Chhabra

## **CHAPTER 4 : CONCLUSION**

In conclusion, malware analysis is an important area of study in cybersecurity as it allows organizations and security professionals to detect and mitigate malicious software before it can cause harm to computer systems and networks. However, malware authors continuously evolve their tactics to evade detection, making malware analysis a constantly evolving field that requires ongoing research and development. Effective malware analysis requires collaboration among security professionals, adoption of best practices, and automation of analysis wherever possible. Overall, malware analysis plays a crucial role in defending against cyber threats and protecting digital assets.

## CHAPTER 5 : REFERENCES

1. <https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/shift-in-atm-malware-landscape-to-network-based-attacks>
2. <https://subscription.packtpub.com/book/security/9781803240244/2/ch02lv11sec03/why-malware-analysis>
3. <https://www.mcafee.com/en-in/antivirus/malware.html>
4. <https://www.vmware.com/topics/glossary/content/malware-analysis.html>
5. <https://www.exterro.com/ftk-imager>
6. <https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/shift-in-atm-malware-landscape-to-network-based-attacks>
7. [https://help.comodo.com/topic-457-1-979-14367-.html#:~:text=Comodo%20Cleaning%20Essentials%20\(CCE\)%20is,USB%20key%2C%20CD%20or%20DVD.](https://help.comodo.com/topic-457-1-979-14367-.html#:~:text=Comodo%20Cleaning%20Essentials%20(CCE)%20is,USB%20key%2C%20CD%20or%20DVD.)
8. <https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works>