**A close-up of a logo

Description automatically generated**

**Title of the project:**

**Ransomware Forensics**

**Group Members:**

**Bhudev Nevaniya (100848467)**

**Maisha Khatoon (100899259)**

**Shreeraj Shah(100848468)**

Contents

[Capstone Project Report- Ransomware Forensics 2](#_Toc141824742)

[Introduction 2](#_Toc141824743)

[Scope 3](#_Toc141824744)

[Objectives 3](#_Toc141824745)

[Methodology 4](#_Toc141824746)

[Computer Analyzed Evidence 5](#_Toc141824747)

[Detailed Description of Evidence 5](#_Toc141824748)

[Relevant Findings 6](#_Toc141824749)

[Supporting Details 7](#_Toc141824750)

[Challenges 8](#_Toc141824751)

[Assumptions 8](#_Toc141824752)

[Additional Report Sections 9](#_Toc141824753)

[Conclusions 9](#_Toc141824754)

# Capstone Project Report- Ransomware Forensics

## Introduction

Cyber dangers threaten people and companies in today's linked, technology-driven society. Ransomware is one of the most dangerous and costly cybercrimes. Ransomware encrypts or locks victims' files until they pay a ransom. Cybercrime has cost millions of people and companies money, data, and key operations.

This paper analyzes a simulated ransomware attack caused by a victim clicking a malicious email link. This simulation is entirely instructional and regulated. The main goal is to investigate ransomware attacks, discover weaknesses, and develop better defenses.

The ransomware assault simulation is based on real-world techniques used by thieves to spread their destructive payload. The recipient of the email is tricked into opening the malicious attachment or clicking the malicious link. Adhering to ethical principles and legal concerns, the decision to utilize a simulated assault guarantees that no real damage is done to any systems or data.

The inquiry will look at everything from the ransomware's distribution method to the malicious link to the victim's encrypted files and the effects on their computer. For effective cybersecurity defenses, it is essential to get a thorough understanding of the attack chain and strategies used by ransomware.

The importance of this simulation rests in the practical experience and insight obtained from responding to ransomware attacks in a simulated environment. We may better prepare for actual cyber-attacks and establish suitable ways to limit risks if we investigate the ransomware's methods and tactics in a controlled setting.

Our goal is to improve our awareness of the ransomware environment and our capacity to defend against such cybercrimes as we go into the specifics of this simulated assault and undertake a detailed investigation. Our efforts to prevent ransomware and safeguard people and businesses from falling prey to these harmful schemes are strengthened by the dissemination of our discoveries and insights to the broader cybersecurity community.

## Scope

This inquiry will examine all aspects of a fictitious ransomware assault that begins when a target clicks on a malicious link in an email. The purpose of the probe is to learn as much as possible about the ransomware's inner workings, from how it was spread through email to the effect of locking people out of their systems with an unsolvable command prompt.

The study will look at the ransomware's email distribution chain to better understand how it reached its victims. To do so, we need to analyze the malicious email in detail, dissecting its content and structure to determine how the victim is duped into clicking on the link.

**System Impact:** The infiltration procedure of the ransomware will be carefully analyzed once the victim has clicked on the infected link. Changes to the system's configuration and settings, alterations to crucial system files, and the installation of permanent access points will be the primary areas of inquiry. One of the most distinguishing features of ransomware is the encryption techniques it employs to lock the victim's data. The investigation will investigate the ransomware's encryption methods in detail, examining things like the algorithm's robustness, the key's length, and the ransomware's ability to generate unique keys for each victim.

**Targeted Files:** Depending on the ransomware version, certain files may be specifically targeted because of their high value to the victim. File types targeted for encryption by the ransomware and the criteria utilized by the malware to make that determination are both within the purview of this analysis. Following encryption, ransomware often presents the victim with a ransom letter or a demand for cash in return for the decryption key. The research will look at what the ransomware does after encryption, such as the message it leaves behind, how much it demands in exchange for decryption, and how it wants to be paid.

Win Hex, a forensic tool WinHex, which has powerful features for examining disk images, files, and system architecture, is the major forensic program utilized for this investigation. The system, encrypted files, and other artifacts affected by the ransomware may be studied in detail. We want to learn more about the ransomware's assault chain and how it affected the victim's system and data by doing this indepth analysis. By learning from this simulation, we can better understand the methods used by ransomware and create defenses that are both more effective and harder to breach. Our investigation will be precise and comprehensive thanks to WinHex, our principal forensic tool, adding credence to the results reported in this report.

## Objectives

The primary objectives of our investigation are outlined as follows:

**Identify the Ransomware Variant:** The inquiry relies heavily on determining the ransomware strain in question. Each variety has its own distinct traits, habits, and ways of spreading. We can learn more about the variant's inner workings and vulnerabilities if we locate it. The ransom message, ransomware binary, and the infected system's behavior will all need to be thoroughly analyzed.

**Analyze the Encryption Techniques**: Most ransomware uses formidable encryption methods to permanently lock the data of its victims. Our goal is to investigate various encryption methods to find flaws in the encryption implementation that may be exploited to restore lost data, as well as to get a better understanding of the encryption strength and key generation process.

**Understand the Command Prompt’s Role:** This ransomware's tactic is to launch a command prompt that the victim has no way of closing on their own. Our goal is to figure out how these fits into the larger assault. The ransomware's persistence mechanisms, for example, or how it prevents people from fixing the problem, may need to be investigated.

**Identify the Types of Files Targeted**: The ransomware's tactics and its intentions may be uncovered by learning which files it encrypts. To do this, it may be necessary to examine the encrypted files in detail, looking for patterns in the filename extensions, the modifications done, and the categories of data that were encrypted.

**Make Extensive Notes on Your Evidence and Results:** We will keep careful records of everything we do throughout the investigation, from collecting evidence to analyzing it to drawing conclusions. Protecting the investigation, preparing for any legal action, and learning more about ransomware attacks all depend on achieving this goal. In addition to aiding in the fight against ransomware, this material may be used as a reference for the cybersecurity community at large.

## Methodology

**Simulation Setup:** We simulate ransomware attacks in a controlled, isolated setting. A test machine gets infected by a synthetic email with a malicious link. To avoid unwanted effects, the test system is securely segregated from the production environment.

**Data Collection:** The compromised test machine collects essential data during the ransomware assault. This involves capturing the ransom message, detecting encrypted files, and collecting system logs that reveal the ransomware's operations. Data collecting is careful to preserve original evidence. We utilize forensically sound procedures to avoid data contamination and manipulation, enabling accurate analysis and authorized usage.

**WinHex Analysis:** We use WinHex to analyze the ransomware's effects on the system. This program lets us analyze the evidence, notably encrypted file headers and extensions. We can identify ransomware encrypted files by examining file headers. This study helps determine the attack's breadth and vital data affected.

**Command Prompt Analysis:** Ransomware opens a helpless command prompt. The command prompts logs, and ransomware's leftover commands help us understand its activities. This analysis reveals the ransomware's orders and how they limit the user's ability to address the problem.

**Ransomware Characteristics:** We identified the ransomware strain through WinHex and command prompt log analysis. We can identify the version by matching our results to ransomware signatures and behavior patterns. Understanding the ransomware variant's traits helps us understand its functioning, motives, and decryption approaches.

We hope to accurately analyze the simulated ransomware attack using this rigorous technique. This analysis will help us understand ransomware forensics and improve defensive measures and incident response. Ethical procedures also keep this simulation informative and safe for actual systems and data.

## Computer Analyzed Evidence

**Malicious URL/Attachment Analysis:** If the ransomware was spread by a malicious link or attachment in the email, the URL or attachment was studied to understand its operation and detect relevant attack indications.

**Digital Signatures and Hash Values:** The ransomware's components, such as the executable file or malware payload, may be inspected for known malware signatures to identify the variation.

**Memory Analysis (if applicable):** Memory analysis may detect process injections or malicious programs. This investigation shows how ransomware avoids detection.

**Registry Entries and Persistence techniques:** The ransomware's persistence techniques may be examined.

Investigators learn about the ransomware attack's method, its effects on the affected machine, and possible remedies by scrutinizing and recording computer data. This comprehensive research helps create effective countermeasures, improve cybersecurity, and prepare for real-world ransomware attacks.

## Detailed Description of Evidence

**Ransome note:** The ransom letter placed on the victim's computer is a crucial piece of evidence. A text file of this kind will often be found on the user's desktop or in encrypted-file directories. The message is the attackers' means of contact, and it explains how the victim may pay the ransom and get the decryption key to unlock their data. Information like the ransom amount, the preferred mode of payment (often digital currencies like Bitcoin), the deadline for payment, and the potential repercussions of not paying may all be included in the ransom letter. It often shows a special ID that the victim must give in the ransom transaction for the criminals to keep track of the money.

The ransom letter may include information beyond just payment instructions. This information might be used to help identify the specific ransomware strain. The ransomware's name, the perpetrators' contact information, and any allusions to the malware's unique techniques and traits are all examples. We are documenting and preserving the contents of the ransom letter as part of our inquiry. To better understand the ransomware variant's behavior and develop decryption solutions, it might be helpful to trace its origins and examine its characteristics.

**Encrypted Files:** One important part of the inquiry is figuring out how the ransomware affected the victim's files. The principal effect of a ransomware attack is encrypted data that is unavailable to the victim until they pay the ransom demanded by the cybercriminals. To see what modifications were made to the files during encryption, we utilize the forensics application WinHex to analyze the encrypted files. There is a lot of information that can be gleaned about the ransomware's preferences for various file types from the encrypted files' headers and extensions.

We want to learn more about the ransomware's intended victims by examining the encrypted data. To have the most possible effect on the victim's operations and enhance the possibility that they would comply with the ransom demands, certain ransomware versions may target file extensions, such as documents, photos, or databases. Data recovery without paying the ransom is also analyzed by analyzing the ransomware's encryption strength and algorithm. Decryption tools or other approaches to recover encrypted data may or may not be successful, thus this examination is essential.

**System Logs:** The ransomware's activity on the victim's machine may be deduced from the command prompt logs. By using a command prompt to carry out its instructions, ransomware creates a paper trail that may be used to assess the full extent of the assault.

By poring through the system logs, we can reconstruct the steps the ransomware used to obstruct the user's access to their files. Understanding the ransomware's tactic of limiting the user's independence in resolving the problem is made easier by this study.

The ransomware's post-encryption activity, such as establishing persistence, disabling security systems, and interfering with system parameters to thwart recovery efforts, may be deduced by analyzing the instructions it executes. The impacts of the ransomware assault may be lessened with the use of these insights, which aid in the creation of efficient countermeasures and incident response methods.

There is careful documentation and preservation of the ransom letter, encrypted information, and system logs throughout the inquiry. Taken together, these traces of the assault can provide light on the ransomware's inner workings, strategy, and vulnerabilities.

## Relevant Findings

**Ransomware Variant Identification:** The precise ransomware variant responsible for the assault may be identified by careful research and comparison with known malware signatures and behavior patterns. This discovery is critical for comprehending the nature and goals of the attackers, and for figuring out what decryption techniques or freely accessible tools may be used to restore the encrypted material. If the discovered ransomware strain is one that has been extensively studied and for which decryption tools already exist, for instance, victims may be able to retrieve their data without having to pay the demanded sum. On the other hand, victims may have a tougher time recovering their data if the version is new or overly complex, and no known decryption techniques exist.

**Decryption Complexity:** The complexity and security of the ransomware's encryption algorithm may be evaluated by careful examination of the method it uses to encrypt data. This discovery is critical for appreciating the challenge of unlocking the data without the decryption key. Developing decryption tools or finding exploits in ransomware's implementation may be possible if the encryption is insufficient or incorrect. However, if the encryption is strong and well done, recovering the data without the decryption key may be impossible, forcing victims to seriously contemplate paying the ransom.

**Unique Decryption Key Generation:** To decrypt the data, ransomware normally generates a unique decryption key for each victim. The decryption keys may be determined by analyzing the ransom message and the ransomware's activity. By gaining insight into how decryption keys are generated, we can assess the complexity of the attackers and the likelihood of uncovering trends or flaws that might lead to the creation of a decryption tool.

**Ransomware Communication Channel:** The ransomware's interaction channel with the attackers is another important discovery. During the ransom negotiation process, victims may contact the attackers using the details provided in the ransom letter or a special identification. To effectively respond to an issue, businesses or law enforcement must first understand the communication route. It may help victims choose the best course of action by revealing details about the attackers' demands, payment terms, and potential for bargaining.

## Supporting Details

**File Headers and Extensions:** With WinHex, a robust forensics program, we may inspect the encrypted files' headers and extensions by delving into their binary structure. If you want to know what kinds of files the ransomware is after, you need to know their file headers and extensions.

**File Headers Analysis:** Analysis of File Headers File headers are discrete sections at a file's beginning that include crucial metadata and information about the file's type and structure. These headers may be modified as part of the ransomware's attack technique throughout the encryption process.

**Identifying File Types:** The original file type, before being encrypted by the ransomware, may be identified by inspecting the file headers. The sorts of files that the ransomware encrypts may be determined with the use of this data. This study reveals the ransomware's affinity for certain file kinds, such as documents, photos, videos, or executables, by examining the file headers associated with each.

**Extension of the File .bat:** The.bat file extension designates a batch file, a kind of script file common to Windows operating systems. The instructions in a batch file may be run in sequence, much like a script. Encrypted files with the.bat extension is exceedingly rare in the context of a ransomware assault, since malware often renames encrypted files with its own unique extension.

**Possible Indicators:** The usage of the.bat file extension in encrypted files may be an indicator that the ransomware is trying to fool people into believing that they are safe batch scripts. This strategy takes use of the fact that most people are already acquainted with the.bat file format, making them more likely to unwittingly open the encrypted files.

**Deceptive Tactics:** Using.bat file extensions, ransomware may try to trick victims into executing the malicious payload when they open or run encrypted files thinking they are safe scripts. This highlights the need for a comprehensive study to uncover such misleading methods used by ransomware.

## Challenges

**Attribution:** Finding the hackers who launched the ransomware assault and tracking them down is a difficult problem. Cybercriminals will frequently go to great lengths to cover their trails, making it impossible to pinpoint who exactly was responsible for an assault. It may be difficult for investigators to track individuals down if they utilize anonymizing technologies like Tor to conceal their IP addresses and route their conversations via many proxy servers. As an added layer of complexity, attackers may use botnets, or networks of hacked computers, as intermediates, or leave false digital breadcrumbs for investigators to follow. Communication with victims using throwaway email accounts or false identities further complicates the attribution procedure.

**Decryption Complexity:** An enormous obstacle lies in identifying and localizing the hackers responsible for the ransomware assault. When cybercriminals launch an attack, it may be difficult to determine who is responsible because of the measures they take to cover their traces. They could employ anonymizing technologies like Tor to prevent investigators from tracking their online activity by masking their IP addresses and redirecting their traffic via a series of proxy sites. In addition, attackers may use methods like exploiting hacked computers as intermediates (botnets) or leaving false digital breadcrumbs for investigators to follow. The attribution procedure is further complicated by disposable email accounts or false identities when communicating with victims.

**Ransom Payment Anonymity:** Ransoms are often demanded by cybercriminals in the form of cryptocurrency like Bitcoin due to the high degree of anonymity they provide. Attempts to identify and capture the culprits are complicated by the usage of cryptocurrencies, which makes it difficult to track the movement of money. Due to blockchain's decentralized structure, tracking cryptocurrency transactions may be challenging for law enforcement.

**Legal and Ethical Considerations:** Investigations into ransomware require negotiating intricate legal and ethical waters. Digital evidence, privacy, and chain of custody are all subject to stringent restrictions that law enforcement and private investigators must follow. It might be difficult to collect evidence in a reliable and acceptable way in court.

## Assumptions

It is assumed that no actual people will be harmed in this simulation, nor will any actual industrial processes be used. The scope of the inquiry is confined to the space designated for the simulation's instructional use. The inquiry is based on the premise that no unauthorized users get access to the simulated environment, systems, networks, or data. No attempts are made to infiltrate or compromise any external systems; all activity is contained inside the authorized test system.

Assumption of Consent and Legality Conducting the simulation with the informed consent of all participants and in accordance with all relevant laws, regulations, and ethical standards. By asking for permission beforehand, you can make sure everyone involved understands the scope of the study and gives their full consent. The scope of the simulation is limited to the parameters of the agreed-upon study, and no extraneous actions are taken. All actions done inside the simulation will be restricted to achieving the predetermined goals. Protecting confidential information and conducting a thorough inquiry are both presumptions made by the investigator. To protect individuals' privacy and security, all sensitive information utilized in the simulation has been anonymized or hidden.

## Additional Report Sections

To forestall future ransomware attacks and fortify system security in general, we recommend taking the measures outlined in the Mitigation Recommendations section. These suggestions stem from the investigation's results and new understandings. The major objective is to assist businesses and people in strengthening their cybersecurity and reducing their vulnerability to ransomware attacks.

**Regular Data Backups:** Drive home the significance of routinely making copies of your most important data and keeping those copies safely kept and apart from your production environment. In a successful ransom attack, this procedure allows businesses to recover data without paying the demanded ransom.

**User Awareness and Training:** Employees and users should be educated about ransomware, phishing, and safe computing behaviors via cybersecurity awareness training. Remind people to take caution when accessing attachments in emails or clicking on links in messages.

**Endpoint Security Solutions:** Antivirus and anti-malware software are only the beginning of the endpoint security solutions you will need to identify and prevent ransomware infestations. The newest ransomware variations may be avoided by keeping security software up to date.

**Email Filtering and Web Security:** Protect yourself against phishing and ransomware by using email filtering tools to eliminate potentially harmful files and links. Prevent visitors from visiting harmful websites by using web security measures.

**Detection and Isolation:** Describe the processes for detecting and confirming a ransomware attack. Once detected, promptly isolate the infected system to prevent further spreading and notify the incident response team.

**Evidence Preservation:** Encourage keeping all digital evidence from the ransomware attack in case it becomes necessary to use it in a lawsuit. Chain of custody must be maintained when collecting data such as logs, screenshots, and the ransom letter.

**Recovery and Restoration:** Give explicit instructions on how to restore compromised systems and data from safe archives. Insist that backups be checked for errors before any restorations are started.

The knowledge that has been given helps create a proactive cybersecurity strategy, which makes it possible to identify ransomware assaults, react to them efficiently, and recover from them successfully.

## Conclusions

We learned a lot about ransomware and its effects from the simulated assault. We identified the ransomware version, understood its encryption methods, and analyzed its effect on the test system. This information may strengthen cybersecurity protection measures.

Ransomware version Identification: We now understand the ransomware version that caused the simulated attack better. Knowing the variation helps cybersecurity experts keep aware, current on ransomware trends, and apply tailored defensive measures to avoid attacks and identify indications of compromise.

Encryption Techniques Understanding: Modern ransomware variations are sophisticated and complicated, as shown by their encryption techniques. This highlights the need of data backup and encryption strength assessment in deciding the possibility of alternate recovery options without paying the ransom.

Impact on the Infected System: The examination revealed the ransomware's effects. The ransom message and file extension alterations demonstrate the attack's purpose to keep important data hostage. These results emphasize the need for strong endpoint security and safe backups to prevent data loss and business interruptions. This analysis emphasizes the need for ransomware prevention. Data backups, network segmentation, and user awareness training help lower the organization's ransomware risk.

Effective Incident Response: The simulated ransomware investigation highlighted the need for a well-defined incident response strategy. In real life, a quick and effective reaction is needed to confine the assault, reduce its effects, and start recovery. Incident response requires evidence preservation and stakeholder communication.

Continuous Improvement: This inquiry offers cybersecurity practice improvement. The simulation may help firms improve their security, defense, and incident response policies. This simulated ransomware assault has improved our understanding of ransomware's processes and effects. Understanding the ransomware version, encryption methods, and system consequences helps us prevent and react to genuine events. This underlines the necessity for proactive cybersecurity and strong incident response to protect enterprises from ransomware's ever-changing threat environment. This simulation will help strengthen future defenses against ransomware and other cybersecurity threats.