International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 22, Issue 5 (May 2026), PP 229-234

WannaCry Ransomware Attack: A Digital Forensic Investigation and Analysis

Amrita Bhardwaj[1] Khushi Chennuri[2] Kalpesh Dandekar[3] Shrushti Deshmukh[4] Vidya Gupta[5]
K.C. College of Engineering & Management Studies & Research

Abstract
The WannaCry ransomware attack, which occurred in May 2017, is considered one of the most significant global cyber incidents, affecting over 300,000 systems across more than 150 countries. The attack exploited a vulnerability in the Windows Server Message Block (SMB) protocol using the EternalBlue exploit (CVE-2017-0144), allowing it to spread rapidly across unpatched systems. This paper presents a digital forensic investigation of the WannaCry attack, focusing on its propagation, execution, and impact. The study analyzes various forensic artifacts including malware executables, encrypted files, system logs, and registry changes to understand the behavior of the ransomware.
A structured forensic methodology is applied using tools such as FTK Imager, Autopsy, Volatility, and Wireshark for evidence collection and analysis. The investigation reconstructs the attack timeline and examines how the ransomware encrypted data and attempted to disable recovery mechanisms. The findings highlight the importance of timely security updates, proper network configuration, and effective incident response strategies. This study provides a comprehensive understanding of ransomware behavior and offers insights into improving digital forensic investigations and cybersecurity practices.
Keywords*: WannaCry; Ransomware; Digital Forensics; EternalBlue; SMB Exploit; Encryption; Memory Forensics; Kill Switch; Incident Response*

Date of Submission: 03-05-2026 Date of acceptance: 13-05-2026

I. Introduction

The rapid expansion of digital infrastructure and interconnected systems has significantly increased the frequency and impact of cyberattacks worldwide. Among these, ransomware has emerged as one of the most critical cybersecurity threats, targeting individuals, organizations, and critical infrastructure. Ransomware is a type of malicious software that encrypts user data and demands payment, typically in cryptocurrency, for its recovery. Over the past decade, ransomware attacks have evolved in complexity, scale, and impact, making them a major concern in the field of cybersecurity [1].

One of the most prominent examples of such attacks is the WannaCry ransomware outbreak that occurred in May 2017. This attack affected more than 300,000 computers across over 150 countries, disrupting services in sectors such as healthcare, transportation, and finance [2]. WannaCry exploited a vulnerability in the Microsoft Windows Server Message Block (SMB) protocol using the EternalBlue exploit (CVE-2017-0144), which was originally developed by the National Security Agency (NSA) and later leaked publicly [3]. Despite the availability of security patches prior to the attack, many systems remained unpatched, allowing the malware to spread rapidly. A distinguishing feature of WannaCry was its worm-like propagation capability, which enabled it to spread automatically across networks without requiring user interaction. Once inside a system, the ransomware encrypted files and displayed a ransom note demanding payment in Bitcoin. Additionally, the malware attempted to delete shadow copies of files to prevent recovery, thereby increasing the likelihood of victims paying the ransom [4]. The widespread impact of WannaCry highlighted the vulnerabilities in existing cybersecurity practices and the need for stronger defensive mechanisms.

Digital forensics plays a crucial role in analyzing and investigating such cyber incidents. By collecting and examining digital evidence such as system logs, memory data, file artifacts, and network traces, investigators can reconstruct the sequence of events and understand the behavior of malware. In the case of WannaCry, forensic analysis helps identify how the attack was initiated, how it propagated across networks, and what artifacts were left behind during execution [5]. This paper presents a comprehensive digital forensic investigation of the WannaCry ransomware attack. It focuses on analyzing the attack methodology, identifying forensic evidence, and understanding the overall impact of the incident. The remainder of this paper is organized as follows: (Section 2) presents a review of existing literature related to ransomware and digital forensics. (Section 3) describes the

methodology used for evidence collection and analysis. (Section 4) discusses the WannaCry case study in detail. (Section 5) presents the results and analysis, followed by discussion in (Section 6). Finally, (Section 7) and (Section 8) provide recommendations and conclusion respectively.

II. Literature Review

Several studies have analyzed ransomware attacks and digital forensic techniques to understand their behavior, impact, and investigation methods. Early research highlights that ransomware primarily relies on exploiting system vulnerabilities and weak security practices. Studies on WannaCry confirm that the attack leveraged the EternalBlue exploit to target unpatched Windows systems, enabling rapid propagation across networks [2][3].

Research in digital forensics emphasizes the importance of collecting and analyzing multiple sources of evidence such as system logs, memory data, and network traffic. According to forensic guidelines, artifacts such as executable files, registry entries, and event logs play a crucial role in identifying malware behavior and reconstructing attack timelines [5]. Memory forensics studies also show that volatile data can reveal running processes, network connections, and hidden malware components, which are essential during ransomware investigations.

Several cybersecurity analyses have focused on ransomware behavior and impact. Reports indicate that WannaCry created encrypted files with specific extensions and attempted to delete shadow copies using system commands, making data recovery difficult [4]. Other studies highlight that ransomware attacks often use built-in system utilities to avoid detection, making forensic analysis more challenging.

Recent research also explores advanced techniques such as machine learning and anomaly detection for identifying cyber threats. These approaches analyze large datasets of system logs and network activity to detect unusual patterns that may indicate ransomware activity. However, such techniques require high-quality data and may produce false positives, limiting their effectiveness in real-world scenarios.

Despite the availability of research on ransomware and digital forensics, there is a lack of studies that combine real-world case analysis with detailed forensic investigation. Most existing work focuses either on attack mechanisms or detection techniques, but does not provide a complete forensic reconstruction of incidents like WannaCry. This creates a gap in understanding how digital evidence can be systematically used to investigate and analyze large-scale ransomware attacks.

Ref.	Year	Focus Area	Methods	Key Findings	Limitations
[2]	2017	WannaCry Attack Analysis	Analysis of global incident reports, malware behavior study, network propagation analysis	Identified that WannaCry used SMB vulnerability (EternalBlue) for rapid worm-like spreading across unpatched systems	Focused mainly on attack spread; lacked detailed forensic evidence analysis
[3]	2017	Vulnerability Exploitation (EternalBlue)	Technical analysis of SMB protocol weakness, exploit behavior, and patch impact evaluation	Demonstrated how unpatched systems were highly vulnerable and enabled large-scale exploitation	Limited to vulnerability analysis; did not include post-attack forensic investigation
[4]	2017	Ransomware Behavior Analysis	File system analysis, process monitoring, and system command tracking	Showed encryption techniques, creation of ransom notes, and use of commands to delete shadow copies to prevent recovery	Did not provide complete timeline reconstruction or real-world forensic case correlation
[5]	2006	Digital Forensic Framework	Standard forensic procedures including evidence acquisition, preservation, and analysis (NIST guidelines)	Highlighted importance of maintaining chain of custody, log analysis, and multi-source evidence correlation	General guidelines; not specifically focused on ransomware or modern cyberattacks
[6]	2020	AI-based Threat Detection	Machine learning models and anomaly detection techniques on system logs and network data	Demonstrated improved detection of abnormal behavior and potential ransomware activities using AI techniques	Requires large datasets, high computational resources, and may produce false positives in real environments

Table 1. *Comparison of Related Studies on Ransomware and Digital Forensics*

III. Methodology

The forensic methodology adopted in this study follows a structured approach to investigate the WannaCry ransomware attack. The objective is to collect, preserve, and analyze digital evidence in order to reconstruct the attack sequence and understand its behavior. The methodology is based on standard digital forensic practices and guidelines [5].

The investigation process involves the following steps:

- **Incident Identification:** Identify affected systems and determine the scope of the attack, including infected devices, encrypted files, and network involvement.
- **Evidence Collection:**

Acquire digital evidence from compromised systems, including disk images, memory dumps, system logs, and network traffic data. Tools such as FTK Imager are used for disk imaging, while memory acquisition tools are used to capture volatile data.

- **Evidence Preservation:**
  Ensure integrity of collected data by generating hash values (MD5, SHA256) and maintaining proper chain of custody. All evidence is handled in a secure and controlled environment.
- **Analysis:**
  Analyze collected data using forensic tools. Autopsy is used for file system analysis, Volatility for memory forensics, and Wireshark for network traffic analysis. Windows Event Logs and registry entries are examined to identify malicious activity.
- **Timeline Reconstruction:**
  Correlate data from different sources to reconstruct the sequence of events, including infection time, file encryption process, and system changes.
- **Validation:**
  Cross-verify findings using multiple tools and techniques to ensure accuracy and reliability of the investigation.

Tool/Stage	Data Source	Purpose	Legal/Ethical Considerations
Disk Imaging (FTK Imager)	Hard disk, storage media	Create forensic image of system for analysis without altering original data	Must use write-blocker; ensure data integrity and maintain chain of custody
Memory Forensics (Volatility)	RAM (volatile memory)	Identify running processes, malware traces, and network connections	Must be captured carefully to avoid data alteration
File System Analysis (Autopsy)	Disk image files	Recover deleted files, identify encrypted data, analyze file structure	Ensure analysis is performed on duplicate image, not original
Network Analysis (Wireshark)	Network traffic (PCAP files)	Detect suspicious communication and propagation behavior	Requires proper authorization for capturing network data
Log Analysis (Event Viewer)	Windows system and security logs	Identify system events, malware execution, and suspicious activities	Logs must be preserved and accessed securely
Timeline Correlation	Timestamps from all sources	Reconstruct sequence of attack events	Requires accurate time synchronization across systems

Table 2. Methodology and Forensic Tools Used

Investigation Workflow

The investigation begins with identifying affected systems and collecting relevant evidence from multiple sources. The collected data is preserved and analyzed using forensic tools to detect malware behavior and system changes. Finally, the results are correlated to reconstruct the attack timeline and validate findings.

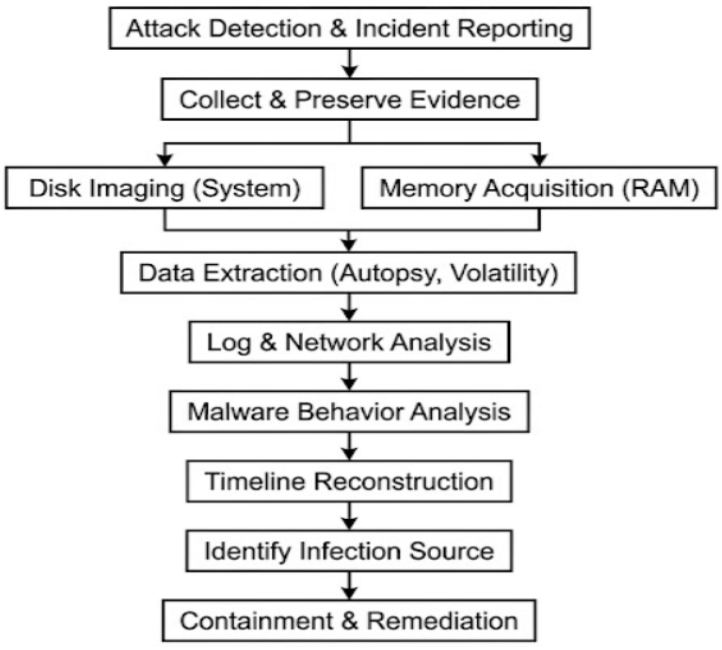

Figure 1: Investigative workflow for WannaCry ransomware (forensic evidence collection, analysis, and incident response).

IV. Case Study - WannaCry Ransomware Attack (May 2017)

A large-scale global cyber incident in May 2017 illustrates the forensic methodology discussed above. The WannaCry ransomware attack rapidly spread across more than 150 countries, infecting over 300,000 systems and causing widespread disruption in sectors such as healthcare, transportation, and business operations [2]. Many organizations experienced sudden system shutdowns, encrypted files, and loss of access to critical data.

Incident Summary:

The attack began on May 12, 2017, when multiple systems across different regions started showing ransomware messages. Investigation revealed that WannaCry exploited a vulnerability in the Windows SMB protocol using the EternalBlue exploit [3]. Systems that had not installed the required security updates were automatically targeted.

Once a system was compromised, the malware executed the ransomware payload and began encrypting user files. At the same time, it scanned the network for other vulnerable machines and propagated without user interaction. The ransomware displayed a message demanding Bitcoin payment for file recovery. In addition, the malware executed system commands to delete shadow copies, reducing the possibility of restoring files [4]. The attack continued spreading until a kill-switch domain embedded in the malware was discovered, which helped limit further infections.

Forensic Findings:

The reconstruction of the attack is based on analysis of system logs, file activity, and network behavior. The following log snippets illustrate the sequence of events:

System Log (Infected Machine):

2017-05-12 08:45 | Suspicious SMB connection detected on port 445
2017-05-12 08:47 | Execution of unknown file WanaDecryptor.exe
2017-05-12 08:48 | Multiple file modification and encryption events observed

File Activity Log:

Encrypted files created with extension .WCRY
Ransom note files generated in system directories
High volume of file access and modification within short duration

Command Execution Log:

cmd.exe /c vssadmin delete shadows /all /quiet
cmd.exe /c wmic shadowcopy delete

Network Activity Log:

Continuous scanning of IP addresses over port 445 (SMB)
Multiple outbound connection attempts indicating worm propagation

These logs confirm that the attack began with SMB exploitation, followed by execution of the ransomware, rapid file encryption, and lateral spread across the network. The presence of system commands aimed at deleting backup data further supports the intent to prevent recovery.The correlation of system, file, and network logs clearly establishes the sequence of the attack. Unlike traditional malware, WannaCry demonstrated automated propagation and large-scale impact within a very short time. The timeline derived from these artifacts highlights how quickly the infection spread and how critical timely patching and monitoring are in preventing such incidents.

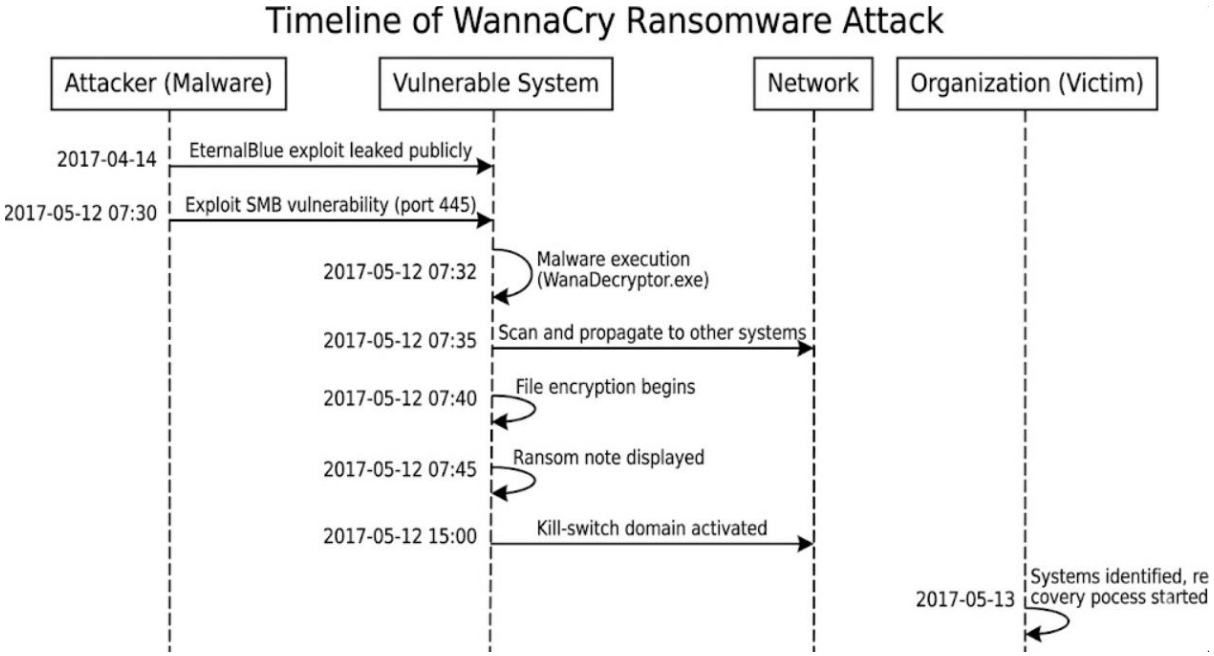

Figure 2: Timeline of the WannaCry ransomware attack showing propagation, encryption, and containment events.

Outcome:

System logs, network activity, and malware artifacts were key evidence in investigating the WannaCry attack. Analysis confirmed that the EternalBlue exploit was used to infect unpatched systems, followed by rapid propagation and file encryption [3]. The discovery of the kill-switch domain helped slow down the spread of the attack [2].

The incident highlighted major security gaps such as delayed patching and weak network protection. It demonstrates how a single vulnerability can lead to large-scale global impact and emphasizes the importance of proper monitoring and timely updates.

5. Results and Analysis

The forensic analysis of the WannaCry attack shows that it followed a structured sequence of exploitation, execution, encryption, and rapid propagation. The use of the EternalBlue exploit enabled the malware to spread automatically across unpatched systems, which significantly increased the scale and speed of the attack [3].

File system analysis confirmed that a large number of user files were encrypted and ransom notes were generated across multiple directories. In addition, system commands were executed to delete shadow copies, reducing the chances of data recovery [4]. This indicates that the attack was designed not only to encrypt data but also to prevent restoration.

Network analysis revealed continuous scanning of systems over SMB ports, confirming the worm-like behavior of the malware. The presence of abnormal network traffic and repeated connection attempts further supports how the attack propagated across networks.

The discovery of the kill-switch domain played a crucial role in slowing down the spread of the attack [2]. Overall, the findings highlight that delayed patching and weak network security were key factors that contributed to the widespread impact of the WannaCry incident.

V. Discussion

The WannaCry attack highlights how a combination of technical vulnerabilities and weak security practices can lead to large-scale cyber incidents. Unlike traditional attacks, WannaCry did not rely on user interaction, but instead used an automated propagation mechanism, making it more dangerous and difficult to control. One key observation is the heavy reliance on outdated systems and delayed patch management. Many organizations failed to apply available security updates, which allowed the malware to exploit known vulnerabilities. This shows that even basic security negligence can result in severe consequences.

Another important aspect is the limitation of traditional security measures. Since WannaCry used legitimate system tools and network protocols, it was able to bypass simple detection mechanisms. This makes forensic analysis essential in identifying hidden activities and reconstructing the attack.From a forensic perspective, the investigation required correlation of multiple data sources such as system logs, file activity, and

network traffic. This highlights the importance of maintaining proper logs and having forensic readiness in place before an incident occurs.

However, challenges still exist. Collecting volatile data such as memory contents is difficult, and delays in response can lead to loss of important evidence. Additionally, analyzing large volumes of data requires expertise and proper tools, which may not always be available.

Overall, the WannaCry case demonstrates that effective cybersecurity requires not only prevention but also strong investigation capabilities and coordinated response strategies.

VI. Recommendations

To prevent and mitigate ransomware attacks like WannaCry, organizations should adopt strong cybersecurity and forensic practices.

- **Regular Patch Management:**
  Ensure timely installation of security updates to fix known vulnerabilities such as those exploited by WannaCry.
- **Network Security and Segmentation:**
  Restrict unnecessary network access and isolate critical systems to prevent rapid spread of malware across networks.
- **Advanced Threat Detection:**
  Use modern security tools to monitor unusual system behavior, network activity, and unauthorized file modifications.
- **Regular Data Backups:**
  Maintain secure and offline backups of important data to enable recovery without paying ransom.
- **Employee Awareness:**
  Train users about cybersecurity risks and safe practices to reduce the chances of system compromise.
- **Forensic Readiness:**
  Maintain proper logging systems and prepare incident response plans to support effective investigation and evidence collection.

VII. Conclusion

The WannaCry ransomware attack demonstrated how a single vulnerability can lead to a large-scale global cyber incident when combined with weak security practices. The forensic investigation clearly showed how the attack exploited unpatched systems, spread rapidly across networks, and encrypted critical data.

The analysis of system logs, file activity, and network behavior helped reconstruct the attack sequence and confirm the presence of ransomware. This highlights the importance of digital forensics in understanding and responding to cyber incidents.

Overall, the study emphasizes the need for timely patch management, strong network security, and effective incident response strategies. By adopting proper cybersecurity measures and maintaining forensic readiness, organizations can better protect themselves against similar attacks in the future.

References

[1] Microsoft, “WannaCry ransomware attack – Lessons learned,” Microsoft Security Blog, June 2017.
[2] US-CERT, “Alert (TA17-132A): Indicators Associated with WannaCry Ransomware,” United States Computer Emergency Readiness Team, 2017.
[3] Symantec Security Response, “WannaCry: Ransomware attacks show strong links to Lazarus group,” 2017.
[4] Check Point Research, “WannaCry Ransomware – Technical Analysis Report,” 2017.
[5] NIST, “Guide to Integrating Forensic Techniques into Incident Response (SP 800-86),” National Institute of Standards and Technology, 2006.
[6] Kaspersky Lab, “WannaCry ransomware used in widespread attacks all over the world,” Securelist Blog, 2017.
[7] Europol, “WannaCry ransomware cyber attack,” European Cybercrime Centre Report, 2017.
[8] MalwareTech (Marcus Hutchins), “WannaCry Kill Switch Analysis,” 2017.