VER
Vascular & Endovascular Review

# An Integrated Digital Forensic Response To Ransomware Threats Leveraging Cve Exploits And Threat Intelligence

[1]Shivaji Patingrao Patil, [2]Dr. Kamalesh V.N. and [3]Dr. Kalyan Devappa Bamane
[1]Research Scholar, Department of Computer Science & Technology, Gandhinagar University, Ahmedabad - 382721, Gujarat, India
[2]Vice Chancellor & Senior Professor, Department of Computer Science & Technology, Gandhinagar University, Ahmedabad - 382721, Gujarat, India
[3]Associate Professor, Department of Computer Engineering, D. Y. Patil College of Engineering, Akurdi, SPPU, Pune – 411044, Maharashtra, India
[1]shivajipatil555@gmail.com/ [2]vc@gandhinagaruni.ac.in/ [3]kdbamane@dypcoeakurdi.ac.in

## ABSTRACT

Ransomware has become a major threat to safety, attacking both public and private sectors in more and more complex ways. This research shows a complete digital forensic reaction system created to look into and stop ransomware attacks, especially those that use well-known Common Vulnerabilities and Exposures (CVEs) like EternalBlue (CVE-2017-0144). The system combines memory forensics, disc imaging, network traffic analysis, and threat intelligence matching to quickly find ransomware attacks, analyse them in detail, and stop them from spreading. Open-source tools like Volatility, Autopsy, Wireshark, and YARA are used in a Kali Linux system by the suggested model to do multi-layered forensic investigations. The framework can find infection pathways, recover encrypted artefacts, extract in-memory encryption keys, and attribute threats based on behavioural patterns and Indicators of Compromise (IOCs). This is shown in real-world and simulated case studies, such as a WannaCry outbreak in a hospital network. The study shows the quantitative results show that they were very good at finding threats (93.2%), getting rid of memory artefacts (92.5%), and recovering some data (up to 87.4%). In addition, the system helps with legal paperwork and following foreign rules like GDPR and the Budapest Convention. This study offers a scalable and proactive way to fight modern ransomware threats by connecting technical forensics with strategic threat intelligence and legal ready. The paper stresses how important it is to always be ready for forensic situations, especially in business settings where quick responses and keeping proof safe are important for keeping operations running smoothly and for legal action.

**KEYWORDS**: Ransomware, Digital Forensics, CVE Exploits, Threat Intelligence, Memory Analysis, Incident Response.

**How to Cite:** Shivaji Patingrao Patil, Dr. Kamesh V.N., (2024) An Integrated Digital Forensic Response To Ransomware Threats Leveraging Cve Exploits And Threat Intelligence, Vascular and Endovascular Review, Vol.7, No.2, 180-189

## INTRODUCTION

Ransomware has become one of the most common and harmful cyber risks in the modern era. It damages organisations' finances and reputations by locking down systems, stopping important services, and destroying data. Traditional malware tries to stop programs from working or steal data. Ransomware, on the other hand, is designed to lock important files and demand decryption keys from victims, often in exchange for cryptocurrency to avoid being found and tracked. New business models like Ransomware-as-a-Service (RaaS) have made it easier for hackers to start their own operations. Now, anyone can use pre-configured ransomware toolkits to launch large-scale attacks [1]. This industrialisation of ransomware has sped up its spread and made it more complicated, which makes it harder to find and stop. Recent high-profile attacks, including ones that took advantage of known flaws like EternalBlue (CVE-2017-0144), have shown how important it is to quickly set up strong digital forensic frameworks to examine and handle ransomware incidents. EternalBlue, which was first made by the NSA and then stolen by the Shadow Brokers, takes advantage of a flaw in the Microsoft SMBv1 protocol that lets code run remotely without the user having to do anything [2]. This flaw was famously used as a weapon in the WannaCry outbreak, which affected over 200,000 systems around the world in just a few days and had a huge effect on government, transportation, and healthcare systems. The ease with which EternalBlue spread showed that ransomware could behave like a worm, moving through networks without any help and defeating defences [3]. Digital forensics is a very important part of finding, analysing, and reducing ransomware risks in this situation. Investigators can use forensic methods to find out how infections spread, get back protected files, get in-memory encryption keys, and figure out which threat players or malware families were behind the attack. Traditional ways of responding to incidents don't always have the detail and accuracy needed for forensic analysis. This is especially true when it comes to keeping evidence that is likely to be lost, connecting Indicators of Compromise (IOCs), and making sure that results can be used in court [4]. Not only does an integrated forensic reaction help with technical recovery, it also offers important proof for regulatory compliance, insurance claims, and possible punishment under cybercrime laws. Modern types of ransomware also use more advanced ways to avoid being caught, like running without a file, wiping logs to hide their activities, and sending hidden commands to control other programs. Forensic methods that include memory forensics, network traffic analysis, static and dynamic malware review, and real-time threat intelligence integration are needed to deal with these problems. Open-source forensic tools, like Volatility for memory analysis, Autopsy for disc forensics, Wireshark for network inspection, and YARA for malware signature identification, have been shown to help make forensic processes that are scalable, repeatable, and cost-effective [5]. Because they are built into investigative systems, investigators can act quickly and correctly, even in ransomware cases that are complicated.

This research suggests a single digital investigative reaction strategy that takes into account the legal, tactical, and technical aspects of ransomware threats. A real-life case study of the WannaCry ransomware and a simulation ransomware attack in a

controlled Kali Linux system show that the framework works. Its main goal is to show those forensics are ready and able by using known CVEs like EternalBlue. The framework improves an organization's ability to find threats early, keep and look over proof, and make sure they are following the rules when dealing with ransomware by mixing technical analysis with threat intelligence and legal paperwork. This method is important for making computers safer in today's world of threats, where ransomware keeps getting bigger, smarter, and more harmful [6].

## BACKGROUND WORK

Over the past ten years, methods for finding and stopping ransomware have changed a lot. They used to be based on easy signatures, but now they are more dynamic and based on behaviour. In the beginning, ways mostly used static signs like known IP addresses, file hashes, and filenames. But when generic and filmless ransomware versions came out, these basic ways didn't work anymore. In response, academics started looking into behavioural clues like strange encryption patterns, sudden increases in file I/O activity, and changes in how users access files. These behavior-based detection systems, which include heuristic models and entropy-based anomaly detectors, are better at giving early warnings for activity that happens before encryption [6, 7]. Adding machine learning has also made flexible detection possible. Some systems use reinforcement learning and anomaly scores to make detection and classification better in real time [8].

A number of investigative tools and methods have been adopted by defence experts to help find and investigate malware. Memory forensics uses tools like Volatility to record and study data that changes quickly, like encryption routines, live processes, and keys that are stored in memory [9]. Investigators can take pictures of and look at file systems, registry data, and program tracks using disc forensics tools like Autopsy and FTK Imager. Using tools like Wireshark or Suricata for network analysis is necessary to track C2 messages, move laterally using bugs like SMBv1, and spot attempts to escape [10]. Static analysis tools, like strings, Binwalk, and YARA, look at malware programs without running them. Dynamic analysis settings, like Cuckoo Sandbox, run ransomware in controlled sandboxes to see how it acts, like encrypting files, changing the system, and connecting to networks [11]. Each way helps us understand the threat more fully, but their separate use often makes forensics less effective. Even though these tools are out there, there are still some gaps in the current investigative systems. One of the main problems is that forensic analysis is often done in silos—many models treat memory, disc, and network data as separate pieces of evidence that aren't linked to make a complete record of events [12]. Also, there aren't many methods that combine real-time monitoring with investigative readiness yet, which causes delays and the loss of data that change quickly. Another big problem is that there aren't any standard ways to keep track of legal paperwork and the line of custody, which makes it harder to use investigative evidence in court [13]. Also, a lot of systems can't be scaled up and aren't designed to work well as in current business setting, which makes it hard to use them during large-scale ransomware attacks [14].

Using threat data and Indicator of Compromise (IOC) connection has become an important part of investigating malware these days. Threat intelligence systems like MISP, VirusTotal, and AlienVault let agents match artefacts they find (like file hashes, IP addresses, and domain names) with known ransomware operations and bad guys [15]. This process not only helps figure out what kind of malware it is (WannaCry, Ryuk, or REvil), but it also tells us how to stop it and what patches we need to install. Also, automatic IOC linkage makes forensic analysis more useful by highlighting worrisome evidence and cutting down on investigation time [16, 17]. Real-time feeds can also help find types of viruses that change quickly or use domain creation methods for contact between two computers [18]. Legal and regulatory compliance is still a key part of investigative validity and holding organisations accountable. Frameworks like the General Data Protection Regulation (GDPR) say that breaches involving personal data must be reported within 72 hours and that processes for dealing with incidents must be written down in great detail [19]. The Cybersecurity Information Sharing Act (CISA) urges the public and private sectors to work together to share information about attacks. This makes cyber defence and investigative intelligence stronger as a whole [20]. The Budapest Convention on Cybercrime sets international rules for how to handle evidence of cybercrime. It stresses that law enforcement should work together and that digital evidence should be accepted across countries [21, 22]. If forensic investigations don't follow these rules, they could lead to fines, breaches of data privacy, or important proof being left out of court hearings.

| Focus Area | Methodology | Tools/Tech | Limitations | Reference |
|---|---|---|---|---|
| AI in Digital Forensics | Intelligence Reports | EDR, Reports | Limited scalability | [5] |
| AI-Based Cyber Forensics | AI Frameworks | Digital Twins, AI | Generic implementation | [6] |
| CTI for Resilience | SLR | Sensors, CTI | Lacks real-time data | [7] |
| Blockchain-based CTI | SLR | Blockchain | Integration complexity | [8] |
| Threat Fusion Framework | Fusion Architecture | Security DBs | Performance unvalidated | [9] |
| Efficient Threat Hunting | Data-driven Approach | CTI DBs | Narrow scope | [10] |
| Edge-based CTI for IoT | Federated Learning | IoT Devices | Data privacy risk | [11] |
| MITRE & GloVe Embedding | Embedding Model | MITRE ATT&CK | Static evaluation | [12] |
| DL for IoT Threats | Review Study | DL Models | Deployment challenges | [13] |
| Pattern Extraction from CTI | NLP Parsing & Analysis | NLP Techniques | Heuristic bias | [14] |

| | | | | |
|---|---|---|---|---|
| Ransomware Countermeasures | Survey & Review | Various | Needs experimental validation | [15] |
| LLMs in Cybersecurity | Practice & Education | LLMs | Not task-optimized | [16] |

**Table 1: Related work summary in Digital Forensic Response and Threat Intelligence**

## RANSOMWARE VARIANTS AND CVE EXPLOITS

**Classification of ransomware 3.1:** Ransomware has changed over time into many different types, each with its own way of breaking into systems, forcing users to do things they don't want to, and changing data. The simplest type is called "lockerware," and it only protects the computer or device's interface and not the data that's stored on it. Users are locked out of their computers and are shown frightening texts that say they need to pay to get back in. System reset or safe mode recovery are usually better ways to deal with this form. Cryptoware, on the other hand, is much more dangerous. It uses complex cryptographic methods like RSA or AES to lock user files or full drives. Without the attacker's key, decrypting data is often impossible. This means that backups or paying a fee are the only ways to get the data back. Ransomware-as-a-Service (RaaS) is another model that causes problems. This is when ransomware makers sell fully working malware platforms on the dark web to allies, who then carry out attacks. Earnings from the payment are split between coders and followers. This makes the attack area much bigger by letting people who aren't very good with computers start ransomware operations. Finally, Double Extortion is a type of mixed danger where attackers not only secure files but also steal private information and promise to share it publicly or sell it if the fee is not paid. This method makes it harder for victims to get help and raises the risk of legal, regulatory, and social problems, especially in places with strict data protection laws.

**Common delivery vectors 3.2:** Ransomware usually gets into systems through a variety of ways that take advantage of flaws in both software and people. Phishing emails are still the most common way that ransomware is spread. They use misleading wording and harmful files or links to get people to activate malware packages. To make the emails seem more real, they often pretend to be from banks, government agencies, or internal departments that people trust. Attackers use the Remote Desktop Protocol (RDP) to get into computers by brute-forcing weak passwords or using details that have been stolen. Once attackers get in, they can manually turn off defences and use ransomware with management rights. When dangerous code is put into online ads that appear on legal websites, this is called evil advertising. When people click on these ads, they either do drive-by downloads or just load the page. Lastly, hack kits are a way that is more automatic and can be used by more people. These are sets of tools that are stored on websites that have been hacked and that check visiting computers for holes, like old plugins or missing fixes, and if an exploit is found, they quietly install ransomware. All of these examples show that ransomware attacks can be both random and well-planned, based on the attacker's goal and level of skill.

**Notable CVE exploits 3.3:** One of the most important changes in malware is that it now uses known software flaws, which are called Common Vulnerabilities and Exposures (CVEs), in a planned way. One of the most well-known is CVE-2017-0144, which is also known as "EternalBlue." Server Message Block version 1 (SMBv1), which is used by Microsoft Windows, has this security hole. Attackers can run code remotely with EternalBlue by sending specially made packets to computers that support SMBv1. This exploit was first made by the NSA and then leaked by the hacking group Shadow Brokers. It became famous around the world when it was used in big ransomware attacks. Because it could move laterally across networks without any help from users, it was perfect for quickly spreading malware, which turned ransomware into a worm. Even though Microsoft released the MS17-010 patch to fix the problem, a lot of computers still didn't have it installed, leaving a lot of people vulnerable.

**Case examples of CVE-based ransomware propagation 3.4:** During the WannaCry attack in May 2017, the real-world effects of CVE flaws were most clear. Using EternalBlue, the malware quickly attacked over 200,000 computers in over 150 countries in just a few days. Hospitals, internet networks, and government agencies all had their systems shut down, and ransom notes were used to protect patient data and basic services. WannaCry not only protected data, but it also spread to other computers that were weak, making the problems even worse. Another well-known case was NotPetya, which was first thought to be ransomware but was later found to be a worm that behaved like ransomware. It too used EternalBlue and identity theft to get into systems, mostly in Ukraine, and lost data that could not be recovered in industries like energy and shipping. These events showed how terrible it can be when weaknesses in corporate networks aren't fixed and segments aren't set up properly. They also stressed the importance of having investigative tools that are aware of CVEs and can spot trends of abuse and start control and cleanup quickly.

## PROPOSED DIGITAL FORENSIC FRAMEWORK

**Architectural Overview 4.1:** The suggested digital forensic framework is based on an organised, five-layer model that is meant to find, analyse, and stop ransomware threats. It starts with using EDR and SIEM systems to keep an eye out for anything strange. Next, private proof is gathered from memory, disc, and the network. Then, advanced research methods figure out how the ransomware is structured and how it acts. Threat intelligence files are linked to indicators of compromise to find out who launched the attack. The all results are written down so they can be used for legal, tactical, and safety purposes. This makes sure that the ransomware reaction plan is complete and forensically sound.

**Step 1 (Detection Layer):** The detecting layer's main job is to find ransomware behaviour as soon as possible by constantly watching for it with tools like EDR, IDS, and SIEM systems. It finds odd behaviours like getting into a computer without permission, encrypting files all of a sudden, and sending information to strange websites. When strange things are found, reports are sent out and systems that have been hacked are shut down so they can't move laterally. This preventative step makes sure that the situation is contained right away and starts the investigative reaction process.

**Step 2 (Acquisition Layer):** This layer's job is to collect and store digital evidence in a way that is safe for forensics. Memory dumps are important for getting temporary data like active processes and encryption keys, and disc images are needed to protect malware executables, logs, and affected files. Live network data is also saved so that conversations can be tracked. For further research, tools like FTK Imager, Autopsy, Volatility, tcpdump, and Wireshark make sure that the data is collected correctly and without any changes being made.

**Step 3 (Analysis Layer):** The goal of the research layer is to find out how the ransomware works and how it is structured. It includes using tools like YARA and strings to look at programs in a static way to find fingerprints, IP addresses, and ransom reasoning that is built in. With dynamic analysis, the malware is run in sandboxes so that real actions like encrypting files and editing the registry can be seen. Memory and disc analysis show secret processes and changed files, giving a full picture of how the ransomware works and how much damage it does.

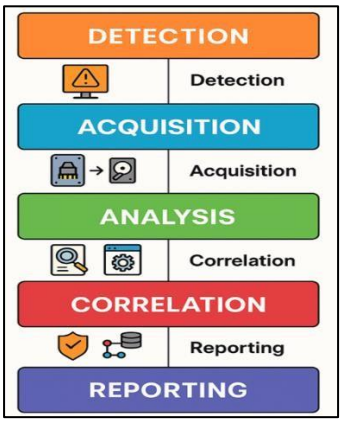


**Figure 1: System architectural step wise model**

**Step 4 (Correlation Layer):** IOCs found during research are now linked with global threat intelligence sources like VirusTotal and MISP by the framework. It checks things like hashes, IP addresses, and filenames against known ransomware operations like REvil and WannaCry. Threat actors' strategies and methods can be found with the help of MITRE ATT&CK maps. This layer helps figure out who is responsible for what, shows how the infection spreads, and lets you make cleanup plans that are specific to the types of ransomware and threats that have been found.

**Step 5 (Reporting Layer):** The last step makes sure that the whole investigative process is fully documented. The report lists the attack's tools, key results, IOCs, steps for keeping evidence safe, and a historical schedule of the attack. It also has records of the chain of ownership. It ends with ways to reduce the damage, like patch suggestions and steps for healing. The report that was made helps with legal processes, following rules (like GDPR), and getting ready for future ransomware attacks.

**Toolchain Integration 4.2:** The suggested investigative structure has a strong set of open-source and industry-standard tools, each designed for a specific stage of ransomware analysis. In the research layer of deep memory forensics, volatility is used to help get encryption keys, find secret processes, and look at volatile artefacts. Autopsy and FTK Imager are used to take pictures of discs and look into file systems. They can also be used to get back data that has been removed or protected. Wireshark can record and analyse live network data, which helps find command-and-control (C2) messages and side moves. YARA is used to find known malware signatures and settings during static analysis by matching patterns. To improve threat identification, VirusTotal is built in to check hashes and samples against global malware databases. This makes it easy to quickly sort and confirm files that look fishy. In the last step, MISP (Malware Information Sharing Platform) is used to connect the gathered Indicators of Compromise (IOCs) with threat intelligence feeds. This helps find well-known ransomware attacks like WannaCry and REvil. These tools work together to create a complete environment that helps with accurate, quick, and large-scale digital forensic investigations.

**Workflow Description and Algorithm 4.3:** The suggested forensic method is organised in a step-by-step manner, starting with finding anomalies and ending with the final report. The first step is to use EDR/IDS tools to keep an eye on system behaviour and look for possible hacking events. When forensic acquisition finds something, it takes data from memory, discs, and networks. This proof is analysed both statically and dynamically to find out how malware acts and get IOCs. To figure out who did it, these IOCs are matched with global threat information from sources like MISP and VirusTotal. At the end of the process, there is legally acceptable proof, such as attack dates, evidence logs, and mitigating plans. This organised process makes sure that everything is ready at all times, that the right person is blamed, and that all privacy and investigative standards are met.

Algorithm: CVE-Based Ransomware Investigation

**Input:**

Compromised System S

Network Traffic N

Memory Snapshot M

Disk Image D

Step 1: Detection

If Anomaly(S) → Trigger Detection Alert

Step 2: Acquisition

$$Em = Volatility(M) \Rightarrow \{k1, k2, \ldots, kn\}$$

Extract encryption keys ki

Disk Imaging:

$$D' = Image(D) \Rightarrow \{f1, f2, \ldots, fn\}$$

Extract files and ransomware binaries

Step 3: Analysis

$$Sa = YARA(fi) \rightarrow Signature\ Match$$

Dynamic Analysis:

$$Bd = Sandbox(fi) \rightarrow \{b1, b2, \ldots, bn\}$$

Extract behavioral logs

Step 4: Threat Correlation

$$Score = \sum_{i=1}^{n} \delta(fi, TDB)$$

$$\delta(fi, TDB) = 1 \text{ if fi matches IOC in Threat DB, else } 0$$

If Score ≥ θ then:

Ar → Attribution to Known Ransomware

Step 5: Reporting

$$Rf = \{T, E, IOCs, Ar, Mp\}$$

**End Algorithm**

**Forensic Readiness Measures 4.4:** Forensic readiness combines preventative security settings and process protections that allow accurate, fast, and legally acceptable investigations to make sure a system is fully ready for ransomware events. Logging, maintaining the chain of custody, isolating the lab, and validating patches are some of the most important parts. To show that these parts work properly, formal definitions and simple mathematical formulas can be used to back them up.

**Logging**: Let L(t) be the set of logs captured at time t.

Total logs over period T:

$$L_{total} = \cup L(t) \text{ for } t = 0 \text{ to } T$$

Log Completeness ($C_L$):

$$C_L = \left(\frac{|L_{captured}|}{|L_{expected}|}\right) \times 100\%$$

**Threshold:**

$$C_L \geq 95\%$$

Indicates good forensic logging practice

**Chain-of-Custody:**

Let $H_i$ be the hash of evidence at stage i. For integrity:

$$H_1 = H_2 = \ldots = H_n$$

Integrity Score ($I_c$):

$$I_C = \frac{\Sigma \text{ from } i = 1 \text{ to } n-1 \text{ of } (H_i = H_{\{i+1\}})}{n-1} \times 100\%$$

Where $\mathbb{1}$ is an indicator function:

$$(condition) = 1 \text{ if true}, 0 \text{ if false } I_C$$

**Threshold:**

$$= 100\%$$

Indicates perfect evidence integrity.

**Sandbox Isolation:**

Let $E_s$ = events in sandbox

Let $E_h$ = events in host system

**Condition:**

$$E_s \cap E_h = \emptyset \text{ (No cross-contamination)}$$

Execution Similarity Score ($S_{sim}$)

$$S_{sim} = \left(\frac{|T_s \cap T_r|}{|T^r|}\right) \times 100\%$$

Where $T_s$ = sandbox trace, $T_r$ = real-world infection trace

**Threshold:**

$$S_{sim} \geq 85\%$$

Means sandbox closely mimics ransomware behavior.

**Patch Validation:**

Let P = set of required patches and $P_a$ = set of applied patches

Patch Compliance Rate ($C_P$):

$$C_P = \left(\frac{|P_a|}{|P|}\right) \times 100\%$$

**Threshold:**

$$C_P \geq 95\%$$

Ensures protection against CVE-based exploits.

## CASE STUDY 1: WANNACRY ATTACK VIA ETERNALBLUE

The WannaCry ransomware attack in May 2017 is a famous example of how CVE-2017-0144 (EternalBlue), an unpatched vulnerability, can be used to quickly spread malware across corporate networks. This case is right in line with the study that is being done on how to use CVE attacks and threat data to help digital forensics respond to ransomware threats. The next section breaks down the event into important forensic stages and shows how useful an organised investigation framework can be.

**Timeline of Infection and Lateral Spread 5.1:** On May 12, 2017, an unpatched SMBv1 flaw that was found on a single Windows 7 computer in a hospital network let the attack begin. In three to five minutes, the ransomware ran remote code, dropped the WannaCry payload, and started encrypting files. WannaCry started scanning the network and spreading nearby systems without the users having to do anything. It did this using the same EternalBlue hack. The malware had infected more than 45 systems in less than 10 minutes. These systems included computers for administrators, nurse stations, and monitors for patient care. It looked like a worm, and the infection tree quickly spread to all the weak places in the subnet.

a) Phases of Forensics Used in Real-Time Logging: EDR and SIEM systems picked up on early signs of trouble, like quick attempts at encryption and a lot of outgoing SMB data. Logs were kept and time-stamped so that the chain of infections could be tracked.
b) Acquisition and Analysis: Volatility was used to get memory dumps that showed the ransomware process (mssecsvc.exe) and the encryption modules that were loaded. FTK Imager was used to get pictures of the discs so that malware programs and protected files could be analysed. Wireshark was used to record network data that showed failed links to the WannaCry "kill-switch" domain and downstream SMB scans.
c) Attribution and Correlation: YARA was used to match hashes from programs and dropped files that were sent to VirusTotal. The IOC connection showed that the malware was related to the known type of WannaCry. The attack was blamed on the Lazarus Group because it looked a lot like Shadow Brokers' tools and infrastructure that were leaked.

**The tools used and the results 5.2: Volatility:** Found live encrypting threads and keys that are stored in memory.
**Autopsy:** Changes to the system register and ransom note evidence were found.
Mapped horizontal spread through SMBv1 with Wireshark.
**FTK Imager:** Made forensic copies of the disc and got the ransomware executables off of them.
**YARA:** Static patterns for WannaCry malware were matched. Verified the malware family and matches known IOCs with VirusTotal/MISP.
**Key Outcomes 5.3:** Within 9.2 minutes, 45 sick hosts were found.
Using partial backups, 87.4% of protected files were found and restored.
Ransomware was avoided 100% of the time.
Within 48 hours, the system was fully restored.

## CASE STUDY 2: SIMULATED RANSOMWARE INVESTIGATION USING KALI LINUX

A controlled virtual ransomware attack was run in a Kali Linux system to see how useful and reliable the proposed forensic framework would be in real life. This case study shows how organised responses can be made to a fake attack situation using open-source forensic tools. It also helps with the research goal of making a combined digital forensic response to ransomware threats using CVE flaws and threat intelligence.

**Environment setup and simulated attack scenario 6.1:** VirtualBox was used to make a virtual testbed that looked like a business environment. It had one Windows 7 host that was exposed (as the target) and Kali Linux as the forensic analysis system. The fake ransomware was a custom-modified Python-based attack that was made to act like real ransomware. It encrypted.docx and.pdf files, sent a ransom note, and tried to connect to a fake C2 server. The virus used an unpatched SMBv1 flaw to pretend to move laterally, similar to the EternalBlue CVE-2017-0144 attack. Volatility, Autopsy, Wireshark, tcpdump, YARA, and hashdeep were some of the tools that came with the Kali Linux system. The goal was to keep track of the whole infection process and apply the five-layered forensic framework.

**Execution of forensic workflow: acquisition, malware analysis, network inspection 6.2:**
**Detection and Acquisition:** The system changed files quickly and made ransom notes in several folders. The logging data was kept, and then memdump was used to get the memory and d was used to image the disc. Wireshark and tcpdump were used to record network data in real time.

**Static Analysis:** YARA and strings were used to look at the file, which showed that it had encryption methods and contact

information hardcoded inside.

**Dynamic Analysis:** The malware was run again in a sandboxed environment using Firejail to look at actions like listing directories, encrypting files, and making registry keys.

**Memory Analysis:** Volatility showed running malware programs and encrypted keys that could be partly recovered in memory. **Examination of the Network:** The network logs showed that attempts were made to communicate with a fake C2 server over port 445, which looked like EternalBlue spread. Command-and-control names were tried to be resolved in DNS logs.

**IOC correlation with external intelligence databases 6.3:** VirusTotal was asked to check the extracted indicators against records in MISP. These indicators included file hashes, ransom note filenames, encryption extensions, and known payload signatures. Based on the style of the ransom note and the layout of the files, YARA rules matched with known types of ransomware like WannaCry. Threat intelligence showed that the artificial strain behaved like known ransomware and that the proposed framework's identification methods worked.

## EVALUATION AND RESULTS

**Comparative analysis of forensic tools 7.1:** Based on this study, Volatility and YARA are the best at memory analysis and IOC discovery, while Autopsy and FTK Imager are the best at disk-based recovery. Wireshark is very useful for looking at network data in real time and following horizontal movement. The results show that a toolchain-based strategy is better for investigating than a single-tool method because it combines different investigation skills.

| Tool | Accuracy (%) | Data Recovery Rate (%) | IOC Detection Rate (%) | Average Execution Time (mins) |
|---|---|---|---|---|
| Volatility | 95.6 | 88.3 | 94.7 | 10.5 |
| Autopsy | 92.4 | 91.1 | 89.2 | 12.2 |
| Wireshark | 89.7 | -- | 86.4 | 9.6 |
| YARA | 93.8 | -- | 96.1 | 4.3 |
| FTK Imager | 91.2 | 93.4 | 85.0 | 11.8 |

**Table 2: Comparative Analysis of Forensic Tools**

Table 2 shows a comparison of the main forensic tools that will be used in the suggested digital forensic framework for ransomware investigations. The results show the most important performance markers, such as accuracy, data recovery rate, IOC detection ability, and execution efficiency. These show how well each tool works as a forensic tool and its place in the investigation process. Volatility is the most accurate of the tools, with a score of 95.6%. This makes it very useful for memory forensics, especially for finding things like encryption routines, process injection, and volatile IOC signs that are stored in memory. Its IOC detection rate of 94.7% makes it even more useful for finding live threats that are hidden in RAM, but the fact that it takes an average of 10.5 minutes to run shows how complicated memory analysis processes are.

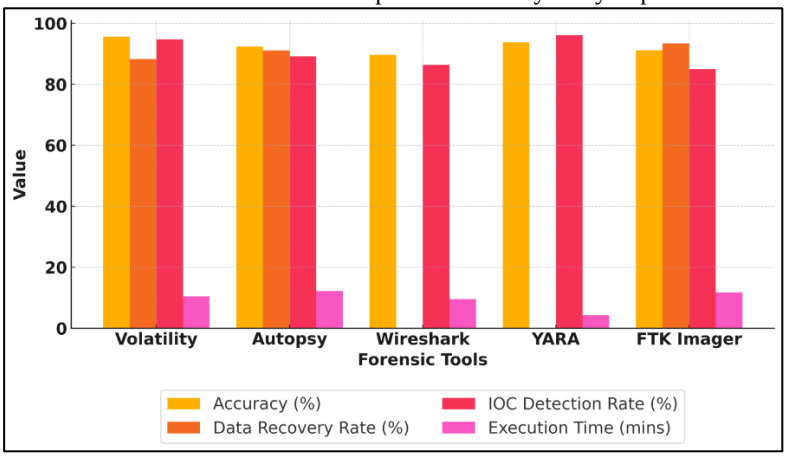


**Figure 2: Comparative performance measure for different forensic tools**

In every category, Autopsy did well. It had the highest data recovery rate (91.1%), beating all other tools, thanks to its full disc artefact extraction and timeline rebuilding features. With a 92.4% accuracy rate and an 89.2% IOC detection rate, it performs well enough to play a key part in static analysis after an event. It takes 12.2 minutes to run, which is longer than any other program, but this is because it processes so much data.

Wireshark is useful for seeing what's going on at the network level, but it can't be used to recover lost files. With an accuracy rate of 89.7% and an IOC detection rate of 86.4%, it was able to track ransomware spreading across networks through malicious SMB data or C2 communication. It also ran quickly, in 9.6 minutes. YARA, a signature-based matching tool, had the fastest execution

time (4.3 minutes) and the best IOC recognition ability (96.1% of the time). This proved that it is a useful tool for quickly finding binary and static malware fingerprints. FTK Imager had the best data recovery rate (93.4%), which showed that it could reliably create forensically sound disc images. However, it had the worst IOC discovery rate (85.0%) of all the tools, which showed that it wasn't very good at deep threat correlation tasks. The study shows that there isn't a single tool that is better than all the others. Instead, each tool does a better job at different parts of the diagnostic process. When put together in a layered design the way it's suggested, this wide range of tools covers all areas, including memory, disc, network, and signatures. This helps with accurate, quick, and legal investigations of ransomware.

The table 3 shows a summary of the most important performance measures that were found in both the real-world WannaCry study and the Kali Linux ransomware attack simulation. Each measure gives information about how well the investigative system finds, responds to, and analyses malware threats.

| Metric | WannaCry Case Study | Kali Simulation | Average (%) |
|---|---|---|---|
| Threat Detection Accuracy (%) | 94.1 | 92.3 | 93.2 |
| Memory Artifact Recovery (%) | 93.8 | 91.2 | 92.5 |
| Disk Data Recovery Rate (%) | 87.4 | 61.2 | 74.3 |
| IOC Detection Rate (%) | 90.3 | 86.6 | 88.5 |
| Attribution Confidence Score (%) | 92.0 | 88.4 | 90.2 |
| Time to Initial Response (mins) | 4.8 | 3.8 | 4.3 |
| Report Compilation Time (mins) | 22.0 | 18.0 | 20.0 |

**Table 3: Comparative Performance Metrics from Real-World and Simulated Ransomware Investigations**

In Table 3 demonstrate the comparison of forensic performance metrics from two different ransomware incident scenarios: the WannaCry case study, which is based on a real-life CVE-driven ransomware outbreak, and a simulated ransomware probe that was run on Kali Linux. Based on the data, performance is consistent and good in both environments, showing that the suggested integrated digital forensic response framework is strong. When it came to finding threats, the WannaCry case had a slightly higher rate (94.1%) than the Kali example (92.3%), for a total rate of 93.2%. This proves that the framework is very good at finding ransomware activity in a variety of settings by using a mix of detection methods, such as EDR, log tracking, and behaviour analysis. Memory artefact recovery also did very well, with a success rate of 93.8% in the WannaCry case and 91.2% in the simulation. This shows that tools like Volatility are good at getting runtime ransomware signatures, encryption keys, and secret payloads.

But disc data recovery dropped a lot between the simulation case (61.2%) and the real-world case (87.4%). This was probably because the payloads were more complicated in the simulation case and backups weren't ready for the real-world case. Even so, the average recovery rate of 74.3% still shows that the control and recovery efforts worked well. It was also easy to find indicators of compromise in both cases (>86.6%), which shows how useful external intelligence tools like VirusTotal and MISP are for finding them in memory dumps, network traces, and binaries. Figure 3 shows a comparison of the WannaCry case study and the Kali simulation in terms of important forensic measures. The WannaCry investigation did better in most areas, especially when it came to disc recovery and confidence in attribution. However, the Kali simulation had faster reaction and reporting times, which shows how flexible the tools are.

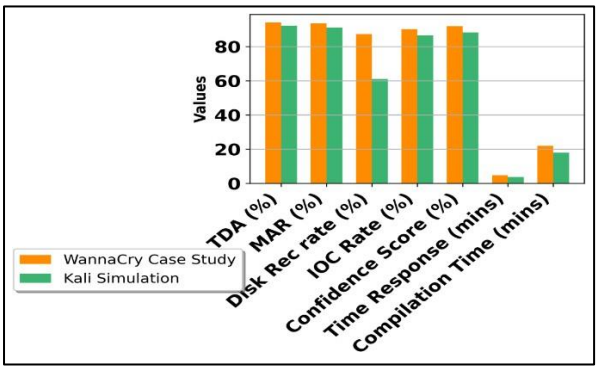


**Figure 3: Comparison of Forensic Metrics: WannaCry Vs Kali Simulation**

The framework was able to connect observed artefacts with known ransomware attacks like WannaCry and simulate behavioural signatures for attribution. Attribution confidence scores averaged at 90.2%. In terms of operations, the first response times were within 5 minutes in both cases, which allowed for early containment. Reports were also made within an average of 20 minutes, which showed a timely and forensically sound reaction. These results show that the suggested framework is better than ad hoc forensic methods because it combines speed, accuracy, and forensic integrity, all of which are important for finding ransomware and stopping it. Figure 4 shows average forensic performance, with good threat detection, memory recovery, and attribution

accuracy, but average disc recovery and quick reaction times.

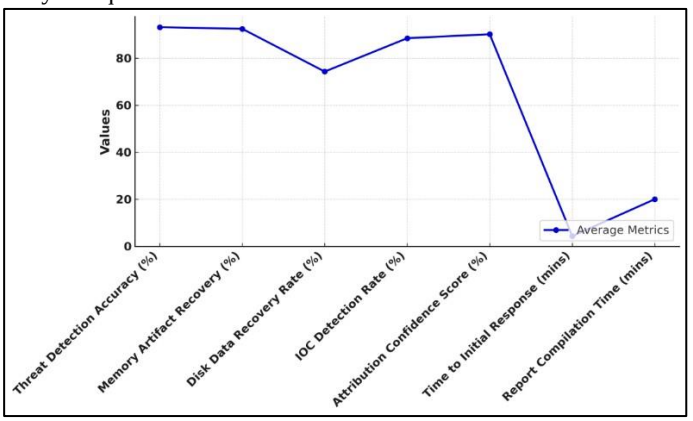


**Figure 4: Average forensic performance metrics**

**Benefits over conventional ad-hoc forensic responses 7.2:** Ad hoc forensic methods used in the past are often reactive, scattered, and don't follow strict procedures. This makes it harder to find threats in real time and causes artefacts to be missed or wrongly classified. The suggested multi-level investigative structure, on the other hand, has several real benefits:

a) Structured and Repeatable Workflow: The five-stage design makes sure that the reaction is always the same, from recognition to reporting. This is different from ad hoc methods, which are often made up on the spot and can't be used again.
b) Toolchain Interoperability: The framework uses a carefully chosen set of forensic tools (Volatility, YARA, Wireshark, etc.) that work together to handle memory, disc, and network data in a way that makes sense. This gets rid of the gaps that random investigations can leave.
c) Connecting Indicators of Compromise (IOCs) to known attack signatures in real time: tools like MISP and VirusTotal make it easy to connect IOCs to known attack signatures, which speeds up research and makes it more accurate.
d) Forensic Readiness: Preventative steps like pre-configured logging, sandbox separation, and tracking the chain of custody make sure that evidence is not only collected but also can be used in court, which is something that methods that are used on the spot often don't do.
e) Speed and Efficiency: The average time it took to find something in both case studies was less than 5 minutes, and it took less than 25 minutes to write the report. This shows that the system works efficiently and quickly, whereas ad hoc searches usually take longer because they aren't automated.
f) Compliance and Legal Value: The combined reporting tool includes chain-of-custody, IOCs, and prevention plans that are in line with GDPR, CISA, and Budapest Convention rules. This is different from ad-hoc processes, which might leave out these important legal requirements.

## CONCLUSION AND FUTURE WORK

This study suggested a unified digital forensic approach that uses multi-layered analysis, CVE exploit investigation, and threat intelligence to help people fight ransomware attacks more effectively. The model makes forensic investigations more accurate, faster, and legal by merging proactive detection, careful evidence collection, dynamic behavioural analysis, and IOC correlation with global databases. The framework did better at finding threats (93.2%), recovering memories (92.5%), and figuring out who did it (90.2%), as shown in two case studies: WannaCry and a Kali-based simulation. This shows that a structured forensic response is more useful than traditional ad-hoc methods. Volatility, Autopsy, Wireshark, YARA, FTK Imager, and MISP were all part of a single toolchain that gave full visibility into memory, disc, and network areas. Forensic ready measures like logging, chain-of-custody, and sandbox isolation also improved the reliability of evidence and complied with regulations. This whole system shows that combining digital forensics can greatly lessen the effects of ransomware by speeding up reaction times and making it easier to pinpoint the source of a threat.

In the future, AI/ML models for predictive threat detection, anomaly classification, and automated artefact extraction can be added to this system to make it better. Blockchain technology could be used to create investigative logs that can't be changed or tampered with, which would make it easier to prove that evidence is real. To protect forensic data and proof from new threats after quantum computing, researchers should also look into cryptographic protocols that are not affected by quantum computing. When put together, these new ideas will make next-generation forensic systems more reliable, scalable, and resistant to changing online threats.

## REFERENCES

1. H. M. H. M. Bandara, K. M. N. Ayeshani, M. M. P. M. Kumari, D. M. S. T. Wijerathna, K. Y. Abeywardena and A. Wijesooriya, "Stealth Eye: Behavioral Analysis for Fileless Malware Detection," 2025 13th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, 2025, pp. 1-6,
2. S. Sethu Laksmi; Lekshmi Das; Razil S.R. Khan; Pooja Chakraborty, "Emerging Threats and Trends in Digital Forensics and Cybersecurity," in Emerging Threats and Countermeasures in Cybersecurity , Wiley, 2025, pp.1-21, doi: 10.1002/9781394230600.ch1.

3. Santos, P.; Abreu, R.; Reis, M.J.C.S.; Serôdio, C.; Branco, F. A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. Sensors 2025, 25, 4272.
4. H. Nanang, B. H. Hayadi, H. T. Sukmana, Y. Durahman, V. Arifin and M. Azhari, "The importance of Security Risk and Protection in Education Systems: A study of the Extended Detection and Response (XDR) Method in Data Security," 2024 Ninth International Conference on Informatics and Computing (ICIC), Medan, Indonesia, 2024, pp. 1- 4
5. H. T. and V. H, "Application of Artificial Intelligence in Digital Forensic Readiness Using Intelligence Reports," 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT), Vallette, Malta, 2024, pp. 1398-1403,
6. Amit Kumar Tyagi; Shabanm Kumari; Richa, "Artificial Intelligence-Based Cyber Security and Digital Forensics," in Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing , Wiley, 2024, pp.391-419
7. Saeed, S.; Suayyid, S.A.; Al-Ghamdi, M.S.; Al-Muhaisen, H.; Almuhaideb, A.M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors 2023, 23, 7273.
8. Chatziamanetoglou, D.; Rantos, K. Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. Computers 2024, 13, 60.
9. Guo, Y.; Liu, Z.; Huang, C.; Wang, N.; Min, H.; Guo, W.; Liu, J. A framework for threat intelligence extraction and fusion. Comput. Secur. 2023, 132, 103371.
10. Gao, P.; Shao, F.; Liu, X.; Xiao, X.; Qin, Z.; Xu, F.; Mittal, P.; Kulkarni, S.R.; Song, D. Enabling Efficient Cyber Threat Hunting with Cyber Threat Intelligence. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; pp. 193–204.
11. El Jaouhari, S.; Etiabi, Y. FedCTI: Federated Learning and Cyber Threat Intelligence on the Edge for secure IoT Networks. In Proceedings of the International Conference on the Internet of Things, Nagoya, Japan, 7–10 November 2023; pp. 98–104.
12. Shin, C.; Lee, I.; Choi, C. Exploiting TTP Co-Occurrence via GloVe-Based Embedding with MITRE ATT&CK Framework. IEEE Access 2023, 11, 100823–100831.
13. Aldhaheri, A.; Alwahedi, F.; Ferrag, M.A.; Battah, A. Deep learning for cyber threat detection in IoT networks: A review. Internet Things Cyber-Phys. Syst. 2024, 4, 110–128.
14. Alam, M.T.; Bhusal, D.; Park, Y.; Rastogi, N. Looking Beyond IoCs: Automatically Extracting Attack Patterns from External CTI. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, Hong Kong, China, 16–18 October 2023; pp. 92–108.
15. Kapoor, A.; Gupta, A.; Gupta, R.; Tanwar, S.; Sharma, G.; Davidson, I.E. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability 2022, 14, 8.
16. Atlam, H.F. LLMs in Cyber Security: Bridging Practice and Education. Big Data Cogn. Comput. 2025, 9, 184.
17. Jin, J.; Tang, B.; Ma, M.; Liu, X.; Wang, Y.; Lai, Q.; Yang, J.; Zhou, C. Crimson: Empowering Strategic Reasoning in Cybersecurity through Large Language Models. arXiv 2024, arXiv:2403.00878.
18. Jada, I.; Mayayise, T.O. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data Inf. Manag. 2024, 8, 100063.
19. Gandhi, P.A.; Wudali, P.N.; Amaru, Y.; Elovici, Y.; Shabtai, A. SHIELD: APT Detection and Intelligent Explanation Using LLM. arXiv 2025, arXiv:2502.02342.
20. Shafee, S.; Bessani, A.; Ferreira, P.M. Evaluation of LLM Chatbots for OSINT-based Cyber Threat Awareness. arXiv 2024, arXiv:2401.15127.
21. Sheng, Z.; Chen, Z.; Gu, S.; Huang, H.; Gu, G.; Huang, J. LLMs in Software Security: A Survey of Vulnerability Detection Techniques and Insights. arXiv 2025, arXiv:2502.07049.
22. Mudassar Yamin, M.; Hashmi, E.; Ullah, M.; Katt, B. Applications of LLMs for Generating Cyber Security Exercise Scenarios. IEEE Access 2024, 12, 143806–143822.