CYBER TRIAGE TOOL TO STREAMLINE DIGITAL FORENSIC INVESTIGATION

Mrs. .S.Kanmani
Assistant Professor/ Department of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India
kanmani.s@srec.ac.in

C.Unus
UG student / Department of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India
unus.2205153@srec.ac.in

C.Vishal
UG student / Department of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India
vishal.2205159@srec.ac.in

M.Rathina seelan
UG student / Department of Information Technology
Sri Ramakrishna Engineering College
Coimbatore, India
rathinam.2205169@srec.ac.in

Abstract— This tool focuses on streamlining digital forensic investigations by prioritizing and analyzing digital evidence efficiently. Traditional forensic processes are often time-consuming and require handling large volumes of data. The proposed Cyber Triage Tool enables quick identification of critical evidence, reducing investigation time. It follows structured forensic guidelines inspired by NIST digital forensic frameworks. Users can upload system data, logs, and evidence sources, after which the system evaluates and prioritizes them based on severity and relevance. The frontend is developed using HTML, CSS, and Bootstrap, while the backend uses Node.js. Data is stored in a lightweight database system. The tool provides dashboards, real-time insights, and automated report generation. It is especially useful for small organizations, educational institutions, and initial forensic analysis scenarios.

I.Introduction

With the rapid increase in cybercrimes, digital forensic investigation has become a critical process in identifying, analyzing, and preventing cyber incidents. However, traditional forensic methods are often slow, complex, and require significant manual effort. Investigators must analyze large volumes of digital data such as logs, system files, and network traces, making it difficult to quickly identify relevant evidence.

Delays in investigation can lead to loss of crucial evidence, increased damage, and difficulty in tracking attackers. Manual processes also introduce errors and inconsistencies, especially when handling multiple cases simultaneously.

To address these challenges, a Cyber Triage Tool is proposed. The tool acts as a first-level forensic analysis system that quickly scans, filters, and prioritizes digital evidence. Instead of analyzing everything, it highlights the most critical data based on predefined rules and severity scores.

The system provides a structured approach where evidence is collected, categorized, and scored based on its importance. Visual dashboards and automated reports help investigators make faster decisions. The lightweight design ensures that the tool is accessible and easy to deploy in resource-constrained environments.

II. Literature Review

Existing research in digital forensics highlights the importance of efficient evidence handling and prioritization. Frameworks such as NIST digital forensic guidelines provide structured approaches for evidence collection, preservation, analysis, and reporting.

Many tools focus on deep forensic analysis but lack quick triage capabilities. Recent studies emphasize the need for automated triage systems that can reduce investigation time by identifying high-priority evidence early in the process.

Some modern forensic tools incorporate automation and machine learning for anomaly detection. However, they are often complex and expensive, making them less accessible for smaller organizations and academic use.
The proposed system bridges this gap by providing a lightweight, rule-based triage mechanism that is simple, cost-effective, and efficient.

III. System Architecture

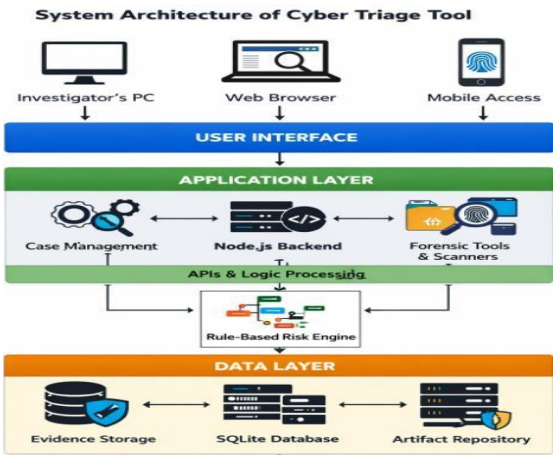

Fig 1 Flow Chart

The Cyber Triage Tool follows a three-tier architecture

consisting of the presentation layer, application layer, and data layer.
The frontend is developed using HTML, CSS, and Bootstrap, providing a user-friendly interface for uploading and analyzing evidence. Users can input logs, files, and system data through structured forms.

The backend is implemented using Node.js, which handles processing, rule-based evaluation, and API communication. The system analyzes uploaded data and assigns priority scores based on predefined criteria such as severity, frequency, and impact.
The database stores evidence details, analysis results, and reports. A lightweight database ensures fast performance and easy deployment.

The workflow begins with evidence collection, followed by preprocessing and analysis. The system then assigns priority levels such as low, medium, and high. Results are displayed through dashboards and can be exported as reports.
runs locally - the design doesn't lock you in. Bigger needs later? Shifting to a heavy-duty database stays possible.

The core component of the architecture is the rule-based risk engine, which performs the primary analysis of the uploaded data. Instead of relying on a traditional database system, the tool processes data dynamically using predefined rules. The rule-based engine evaluates the evidence based on factors such as severity, frequency, and potential impact, and assigns priority levels such as low, medium, and high. This approach helps in quickly identifying critical evidence that requires immediate attention.

The final output is presented through dashboards and structured reports, enabling investigators to make faster and more informed decisions during digital forensic investigations. This architecture ensures efficiency, simplicity, and rapid triage capability in handling cyber incidents.

The application layer is implemented using a Node.js backend, which acts as the central controller of the system. It manages request handling, input validation, and communication between the frontend and the processing modules. This layer ensures smooth data flow and efficient execution of operations. It also includes modules such as case management and forensic input handling, which organize and preprocess the collected data before analysis.

The core of the system is the rule-based risk engine, which replaces the need for complex databases and heavy analytical tools. This engine applies predefined logical rules to evaluate the uploaded evidence based on parameters such as severity, frequency, and potential impact.

IV. Novelty

The main novelty of the Cyber Triage Tool lies in its ability to simplify digital forensic investigations through rapid triage. Unlike traditional tools that focus on deep analysis, this system prioritizes speed and efficiency.

It introduces a rule-based scoring mechanism to quickly identify critical evidence. The lightweight architecture ensures accessibility for small-scale environments. The integration of dashboards and automated reporting enhances usability and decision-making.

The proposed Cyber Triage Tool introduces a lightweight and efficient approach to digital forensic investigation by focusing on rapid evidence prioritization rather than complex and time-consuming analysis. Unlike traditional forensic tools that rely on heavy data storage and extensive processing, this system eliminates the need for a database and instead uses a rule-based risk engine for dynamic analysis. This significantly reduces system complexity and improves processing speed, making it suitable for quick triage in real-time scenarios.

A key novelty of the system lies in the implementation of a rule-based decision engine that evaluates digital evidence based on predefined parameters such as severity, frequency, and impact. This approach ensures consistent and explainable results without requiring advanced machine learning models, making the system more transparent and easier to understand for investigators.

Another unique aspect is its focus on accessibility and simplicity. The tool is built using lightweight web technologies and a Node.js backend, allowing it to be easily deployed in resource-constrained environments such as small organizations and educational institutions. The integration of real-time dashboards and automated report generation further enhances usability by enabling quick decision-making during investigations.

The tool is built using lightweight web technologies and a Node.js backend, allowing it to be easily deployed in resource-constrained environments such as small organizations and educational institutions. The integration of real-time dashboards and automated report generation further enhances usability by enabling quick decision-making during investigations.

A key innovative aspect of this system is the use of a rule-based risk engine instead of traditional database-driven or machine learning-based approaches. The engine applies predefined logical rules to evaluate incoming evidence dynamically, eliminating the need for complex model training or large-scale data storage.

V. Results and Discussions

The proposed Cyber Triage Tool was evaluated using multiple simulated digital forensic scenarios involving system logs, suspicious activity records, and sample evidence files.

The primary objective of testing was to analyze the efficiency of the rule-based risk engine in identifying and prioritizing critical evidence. During experimentation, different types of inputs with varying severity levels were provided to the system, and the results demonstrated that the tool was able to accurately classify and prioritize evidence into low, medium, and high categories based on predefined rules.

The performance of the system showed a significant improvement in reducing the time required for initial forensic analysis when compared to traditional manual methods. Instead of analyzing all available data, the tool filtered and highlighted only the most relevant and high-risk evidence.

This triage-based approach enabled faster decision-making and reduced the workload on investigators. The rule-based engine consistently produced stable and predictable outputs, ensuring reliability and eliminating ambiguity in the evaluation process.

Fig 2 Login Page

Fig 3 Scanning

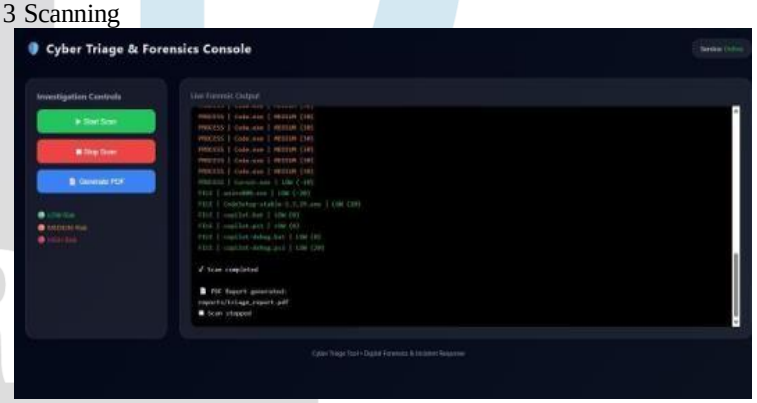

Fig 4 Report generation

During testing, the system successfully processed various inputs and classified them into different priority levels such as low, medium, and high. The rule-based engine applied predefined criteria including severity, frequency, and potential impact to evaluate each piece of evidence. The results showed that the classification was consistent and aligned with expected outcomes, demonstrating the reliability of the rule-based approach in forensic triage.

one of the major observations was the significant reduction in investigation time. Unlike traditional forensic methods that require analyzing large volumes of data manually, the proposed system quickly filtered out irrelevant information and highlighted only the most important evidence. This triage mechanism helped in reducing the workload on investigators and enabled faster decision-making during the initial stages of analysis.

The system also demonstrated efficient real-time processing capabilities. As soon as the data was uploaded, the backend processed it instantly and displayed the results on the dashboard without noticeable delay. The dynamic updates ensured that investigators always had access to the latest analysis results. This feature improved the overall usability and responsiveness of the system.

VI. Merits and Demerits

The proposed Cyber Triage Tool offers several advantages in improving the efficiency of digital forensic investigations. One of the major merits is its ability to perform rapid triage of digital evidence. Instead of analyzing all available data, the system quickly identifies and prioritizes critical evidence, helping investigators focus on the most important aspects of a case.

Another key advantage of the system is its lightweight architecture. Since the tool does not rely on a traditional database, it reduces system complexity and resource usage. This makes it easy to deploy and operate even in environments with limited computational resources, such as small organizations or educational institutions.

The use of a rule-based risk engine is also a significant strength of the system. It ensures consistent and explainable results by applying predefined logical rules for analysis. Unlike complex machine learning models, this approach is transparent and easier to understand, which is important in forensic investigations where clarity and justification are required.

The system also enhances usability through a simple and interactive user interface. Investigators can easily upload data, view results, and generate reports without requiring advanced technical knowledge. understanding of analysis results.

Another merit is the real-time processing capability of the system. The tool analyzes data instantly and updates results dynamically, allowing investigators to make quick decisions. This reduces delays in the investigation process and improves overall response time during cyber incidents.

Despite these advantages, the system has certain limitations. One of the major demerits is the absence of a database, which prevents long-term storage and historical analysis of forensic data. This limits the system's ability to track previous cases and perform trend analysis.

Another limitation is the dependency on predefined rules in the rule-based engine. While this ensures consistency, it may not be flexible enough to handle new or unknown types of cyber threats. Updating the rules manually is required to adapt to evolving attack patterns.

The system also lacks advanced forensic features such as deep file analysis, automated evidence collection, and integration with external security tools. These features are commonly found in high-end forensic tools and could enhance the system's overall capability.

Overall, while the Cyber Triage Tool has some limitations, its merits such as speed, simplicity, and efficiency make it highly suitable for initial forensic triage.
It serves as a practical solution for quickly identifying critical evidence and supporting faster decision-making in digital forensic investigations.

VII. Applications

The Cyber Triage Tool can be widely used in the field of cybersecurity incident response, where rapid identification of critical evidence is essential. During cyberattacks such as malware infections or unauthorized access, the tool helps investigators quickly analyze logs and prioritize suspicious activities, enabling faster containment and mitigation of threats.

In small and medium-sized organizations, the tool provides an affordable solution for handling digital forensic investigations. Many such organizations lack access to advanced and expensive forensic tools. This system offers a lightweight and cost-effective alternative that can be easily deployed without requiring high-end infrastructure.

Educational institutions can use the Cyber Triage Tool as a practical learning platform for students studying cybersecurity and digital forensics. It allows students to understand how evidence is collected, analyzed, and prioritized in real-world scenarios, bridging the gap between theoretical concepts and practical implementation.

The tool can also be applied in academic research projects related to cyber forensics and incident analysis. Researchers can use it to simulate different attack scenarios and study how evidence is classified and prioritized based on rule-based approaches.

In law enforcement agencies, the system can assist in the initial stages of digital investigations. Officers can use the tool to perform quick triage of seized digital devices, helping them identify relevant evidence before conducting detailed forensic analysis using advanced tools.

The Cyber Triage Tool is also useful in corporate environments where continuous monitoring of systems is required. IT security teams can use the tool to analyze system logs and detect potential threats early, reducing the risk of data breaches and system failures.

Another important application is in incident response teams that handle multiple cases simultaneously. The tool helps in organizing and prioritizing evidence from different cases, allowing teams to focus on high-priority incidents and manage their workload more effectively.

The system can be used as a preliminary screening tool before performing deep forensic analysis. By filtering and prioritizing data, it reduces the amount of information that needs to be examined in detail, saving both time and effort for investigators.

The Cyber Triage Tool can also be applied in cybersecurity training and awareness programs. It can be used to demonstrate how cyber incidents are analyzed and how decision-making is performed based on evidence prioritization.

References

[1] C. Hargreaves, S. Quick, and L. Scanlon, "DFPulse: The 2024 digital forensic practitioner survey," *Forensic Science International: Digital Investigation*, vol. 49, 2024.

[2] N. R. Roy, A. P. Singh, P. Kumar, and A. Kaul, Eds., *Cyber Security and Digital Forensics*, in *Proc. ReDCySec 2024*, Singapore: Springer, 2025.

[3] S. Goel, E. Uzun, and M. Xie, Eds., *Digital Forensics and Cyber Crime*, in *Lecture Notes in Computer Science*, Springer, 2025.

[4] Z. H. Zamil, "AI-driven digital evidence triage in digital forensics: A comprehensive review," in *Proc. 13th Int. Symp. Digital Forensics and Security (ISDFS)*, 2025.

[5] K.-K. R. Choo, T. Holt, and M. Levi, Eds., *Advances in Digital Forensics*, in *Proc. DFRWS 2025*, *Forensic Science International: Digital Investigation*, 2025.