International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

An Integrated Ethical Hacking and Digital Forensics Framework for Automated Cyberattack Detection and Evidence Analysis

Ramya P
Assistant Professor JAIN COLLEGE(AUTONOMOUS), No.15,Vasavi Temple Road, VV Puram, Bangalore - 560004 Ph. No.: 8618848287

Email: ramya2624@gmail.com ORCID ID **0009-0009-7284-0790**

Abstract - The increasing sophistication of cyberattacks has created a growing need for security approaches that combine proactive vulnerability assessment with reliable digital forensic investigation. This research proposes an integrated framework that connects ethical hacking techniques with automated cyber-forensic analysis to improve the detection, investigation, and understanding of cybersecurity incidents. The proposed approach uses controlled penetration testing to identify vulnerabilities and simulate realistic attack scenarios across networked systems. Security events generated during these activities are subsequently collected and correlated with digital evidence, including network traffic, system logs, authentication records, and endpoint artifacts. An automated evidence-analysis layer is introduced to classify suspicious activities, reconstruct attack timelines, and identify relationships between vulnerabilities and observed attack behaviors. The framework also incorporates evidence integrity mechanisms to support reliable forensic analysis and maintain traceability throughout the investigation process. Experimental evaluation can be conducted using controlled datasets and simulated cyberattack scenarios, with performance assessed using detection accuracy, forensic analysis time, evidence integrity, and attack reconstruction effectiveness. The proposed framework aims to reduce the separation between penetration testing and post-incident investigation, enabling security teams to transform ethical hacking results into actionable forensic intelligence. The research can contribute toward developing more efficient, systematic, and evidence-driven cybersecurity defense mechanisms for modern organizations.

Keywords - Ethical Hacking, Digital Forensics, Cyberattack Detection, Evidence Analysis

1. INTRODUCTION

The rapid expansion of cloud computing, interconnected networks, Internet-connected devices, remote-access technologies, and digital services has significantly increased the attack surface of modern organizations. Cyberattacks have consequently become more complex, requiring organizations to adopt security mechanisms capable of both preventing attacks and investigating incidents after they occur.

Ethical hacking and penetration testing provide a proactive mechanism for identifying vulnerabilities before malicious attackers exploit them. Penetration testing systematically evaluates networks, applications, systems, and other assets by simulating authorized attacks. Recent literature describes penetration testing as an important component of cybersecurity because it can expose exploitable weaknesses and provide actionable information for improving security controls.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Digital forensics, in contrast, primarily focuses on the identification, acquisition, preservation, examination, and interpretation of digital evidence following a security incident. However, forensic investigations increasingly face difficulties because evidence can be distributed across endpoints, networks, cloud services, mobile devices, and other platforms. A major review by Casino et al. identified evidence acquisition and preprocessing as recurring challenges in digital forensics, together with procedural, reporting, presentation, and ethical concerns.

Traditionally, penetration testing and digital forensics have been treated as relatively separate activities. Penetration testers identify vulnerabilities and demonstrate attack paths, while forensic investigators analyze evidence after an incident. This separation can result in the loss of valuable relationships between known vulnerabilities, attack techniques, system events, and forensic artifacts.

This research therefore proposes an **Integrated Ethical Hacking and Digital Forensics Framework (IEH-DFF)** that connects vulnerability discovery, controlled attack simulation, security-event collection, automated evidence analysis, attack reconstruction, and forensic reporting.

2. RESEARCH PROBLEM

Conventional cybersecurity practices frequently generate large quantities of security information from different sources. Penetration testing may produce vulnerability reports, while security monitoring systems generate network logs, authentication records, alerts, and endpoint events. Digital forensic investigators must subsequently correlate these heterogeneous sources manually or through partially integrated tools.

This creates several challenges:

1. Difficulty correlating vulnerabilities with actual attack behaviors.
2. Large volumes of heterogeneous forensic evidence.
3. Time-consuming manual investigation.
4. Difficulty reconstructing complete attack timelines.
5. Potential loss or alteration of evidence.
6. Challenges in validating the authenticity of digital artifacts.
7. Limited integration between proactive security assessment and incident investigation.

Digital forensic research has also identified evidence acquisition, preprocessing, authentication, anti-forensic techniques, and increasingly complex digital environments as important challenges.

Therefore, an integrated approach is required in which the results of ethical hacking can become useful contextual information during forensic investigation.

3. OBJECTIVES OF THE RESEARCH

The primary objective is to design an integrated framework connecting ethical hacking and digital forensics for automated cyberattack detection and evidence analysis.

The specific objectives are:

- To identify vulnerabilities through controlled ethical hacking and penetration testing.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- To simulate authorized cyberattack scenarios.
- To collect network, system, authentication, and endpoint evidence.
- To automatically correlate attack events with forensic artifacts.
- To reconstruct attack timelines from heterogeneous evidence.
- To identify relationships between vulnerabilities and observed attack behavior.
- To maintain the integrity and traceability of collected evidence.
- To reduce the time required for forensic analysis.
- To provide structured forensic intelligence for incident response.

4. RESEARCH QUESTIONS

The study addresses the following research questions:

RQ1: How can ethical hacking results be integrated with digital forensic evidence?

RQ2: How can automated evidence correlation improve cyberattack detection?

RQ3: How can heterogeneous forensic artifacts be used to reconstruct attack timelines?

RQ4: How can evidence-integrity mechanisms improve the reliability and traceability of automated forensic analysis?

RQ5: What performance measures can be used to evaluate an integrated ethical hacking and digital forensics framework?

5. LITERATURE REVIEW

5.1 Ethical Hacking and Penetration Testing

Ethical hacking involves authorized security testing designed to identify weaknesses before they are exploited by malicious actors. Penetration testing generally follows a structured process involving reconnaissance, vulnerability identification, controlled exploitation, analysis, and reporting.

The 2024 review *Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools* examined research-informed ethical hacking tools and their role in supporting security testing. The article emphasizes the diversity of tools and approaches available for ethical hacking and penetration testing.

Similarly, Selvamurugan et al. describe penetration testing as a systematic evaluation of systems, networks, or applications for exploitable vulnerabilities and emphasize its role in identifying security weaknesses through controlled attacker behavior.

However, penetration testing alone does not necessarily provide sufficient information for reconstructing an actual security incident. This creates an opportunity to connect penetration-test results with forensic evidence.

5.2 Digital Forensics

Digital forensics involves the systematic investigation of digital artifacts to determine what happened during a security incident. Relevant evidence may include:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Network packets
- Firewall logs
- Authentication records
- Operating-system logs
- File-system artifacts
- Memory artifacts
- Browser artifacts
- Application logs
- Cloud records
- Endpoint security alerts

5.3 Artificial Intelligence and Digital Forensics

Automation and artificial intelligence have increasingly been considered for digital forensic investigation. Fähndrich et al. conducted a structured literature review of digital forensics and strong AI, indicating growing research interest in applying AI-based techniques to forensic processes.

Automated analysis can potentially support:

- Evidence classification
- Anomaly identification
- Event correlation
- Timeline construction
- Artifact prioritization
- Pattern recognition
- Suspicious-activity detection

Nevertheless, automated forensic systems must be designed carefully because incorrect classification or unexplained automated conclusions can affect the reliability of an investigation.

5.4 Digital Evidence Integrity

The usefulness of digital evidence depends not only on its availability but also on its authenticity and integrity. Research has examined methods for authenticating digital artifacts and detecting evidence manipulation. Neale's systematic review, for example, examines techniques for authenticating digital artifacts.

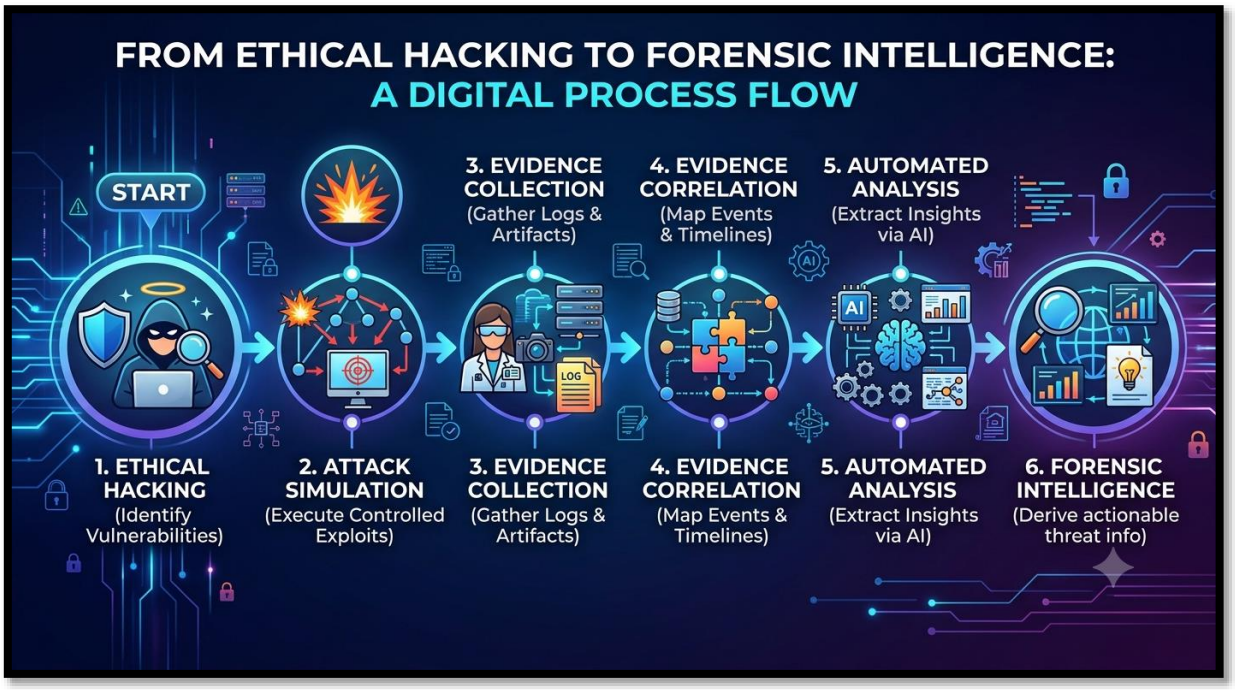
Consequently, the proposed framework incorporates hashing, timestamps, provenance information, and controlled evidence handling into the analysis process.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

6. PROPOSED INTEGRATED FRAMEWORK

The proposed framework consists of six major layers:



6.1 Layer 1: Asset and Vulnerability Identification

The first layer identifies the systems and assets that will be assessed. Ethical hackers perform authorized vulnerability assessment and penetration testing.

The output includes:

- Identified vulnerabilities
- Vulnerability severity
- Affected assets
- Potential attack paths
- Attack techniques used during testing

The vulnerability information becomes contextual information for later forensic analysis.

6.2 Layer 2: Controlled Attack Simulation

Authorized penetration tests are performed within a controlled environment.

Possible scenarios include:

- Unauthorized login attempts
- Credential attacks

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Web-application attacks
- Privilege escalation
- Malware execution simulation
- Suspicious file creation
- Network reconnaissance
- Lateral movement simulation

The objective is not merely to demonstrate that a vulnerability exists but also to generate observable security events that can subsequently be studied.

6.3 Layer 3: Evidence Collection

The framework collects evidence from multiple sources.

Evidence Source	Examples of Evidence
Network	Packets, flows, IP addresses, ports
Authentication	Login attempts, successful logins, failed authentication
Operating System	Event logs, processes, system events
Endpoint	Files, registry artifacts, process activity
Application	Web and application logs
Security Tools	IDS/IPS and EDR alerts
Cloud	Access records and activity logs

Evidence should be collected according to an established forensic procedure so that the original artifacts are preserved and their provenance can be tracked.

6.4 Layer 4: Evidence Preprocessing and Integrity Verification

Collected evidence is normalized before analysis.

The preprocessing stage can include:

1. Removal of duplicate records.
2. Conversion into a common event format.
3. Timestamp normalization.
4. Extraction of relevant attributes.
5. Hash generation.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

6. Metadata preservation.
7. Evidence-source identification.

A cryptographic hash can be generated for each evidence object:

$$H_i = Hash(E_i)$$

where:

- E_i= evidence object i
- H_i= integrity hash of evidence object i

During later analysis, the hash can be recalculated and compared with the stored value.

6.5 Layer 5: Automated Evidence Correlation

This is the central component of the proposed framework.

The correlation engine receives:

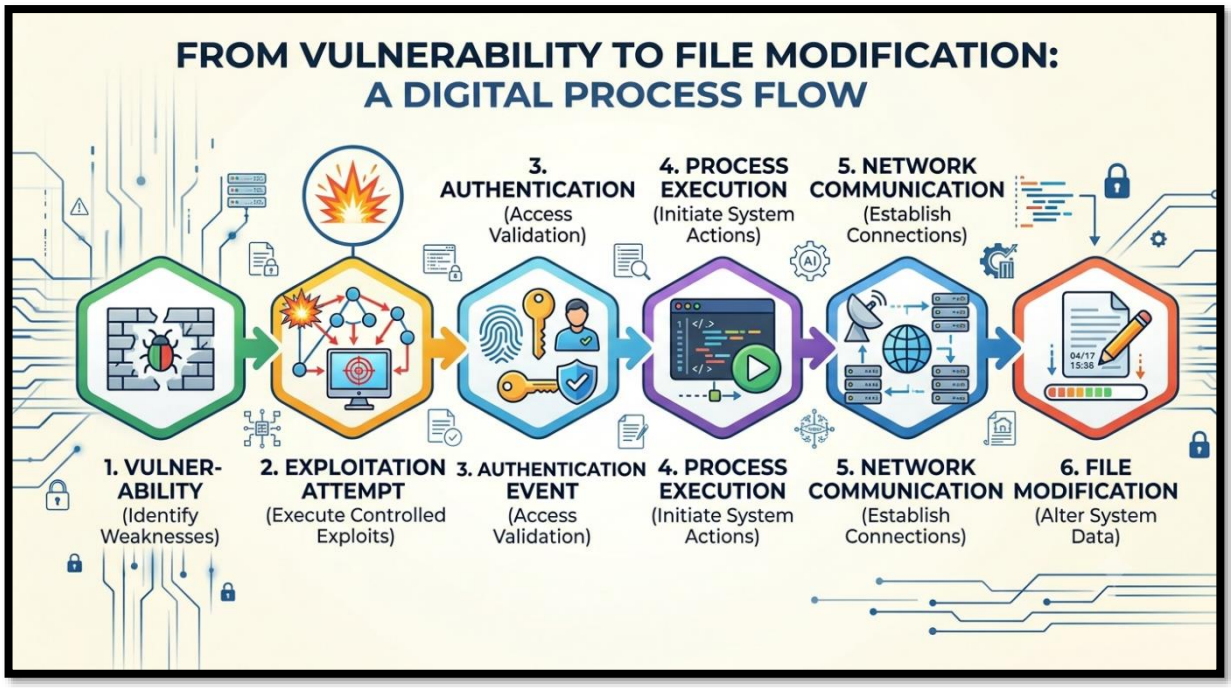
- Penetration-testing results
- Vulnerability information
- Network events
- Authentication events
- Endpoint artifacts
- Security alerts

The system searches for relationships among these sources.

For example:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026



This relationship can provide a more complete representation of an attack than an isolated security alert.

A correlation score can be conceptually represented as:

$$C = w_1V + w_2T + w_3N + w_4A + w_5E$$

where:

- V= vulnerability relationship
- T= temporal relationship
- N= network relationship
- A= authentication relationship
- E= endpoint relationship
- $w_1, \dots, w_5$= weighting factors

The formula represents a conceptual model rather than a claimed experimentally validated scoring system.

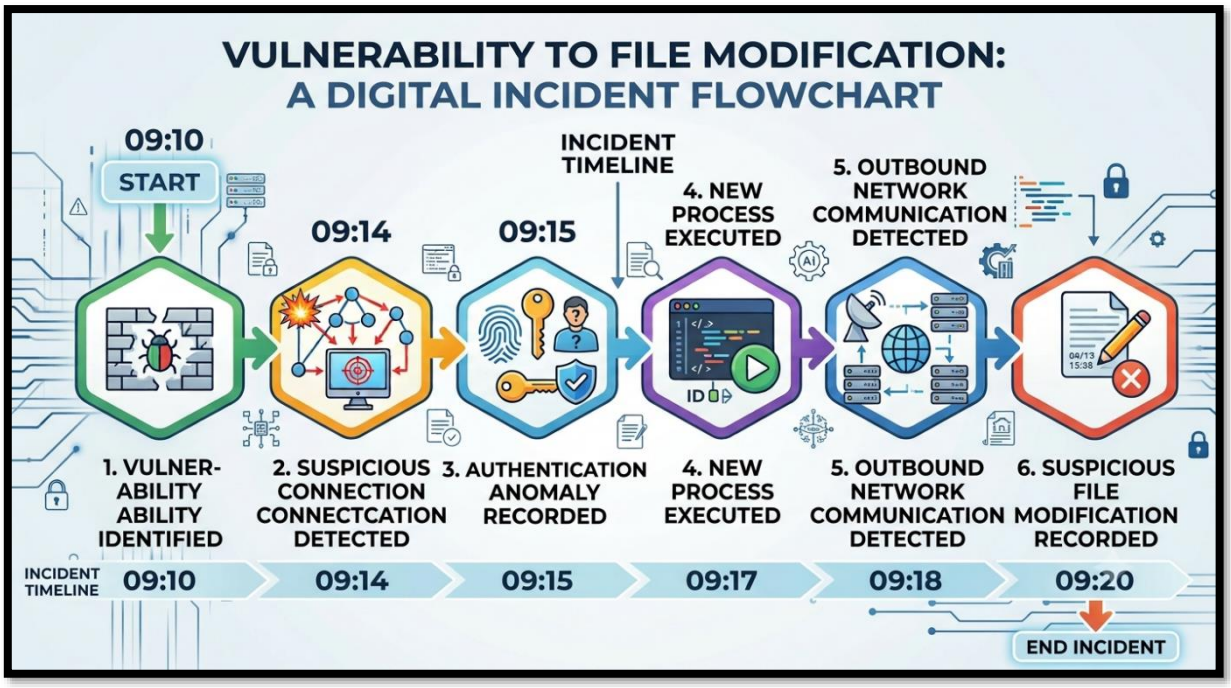
6.6 Layer 6: Attack Timeline Reconstruction

After correlation, the framework reconstructs the sequence of events.

For example:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026



The resulting timeline allows investigators to examine the relationship between the tested vulnerability and subsequent system behavior.

Timestamp interpretation is particularly important because manipulated or inconsistent timestamps can affect forensic reconstruction. Research has specifically investigated timestamp tampering and the reliability of artifacts used in event reconstruction.

7. AUTOMATED DETECTION MECHANISM

The proposed framework can incorporate rule-based analysis and machine-learning-based classification.

Rule-Based Detection

Rules can identify known relationships, such as:

- Multiple failed logins followed by successful authentication.
- Exploitation activity followed by process creation.
- Vulnerability exploitation followed by unusual network traffic.
- Suspicious file creation followed by outbound communication.

Machine-Learning-Based Detection

A supervised classifier can be trained using labeled attack and normal events.

Possible features include:

- Number of authentication failures
- Connection frequency
- Destination-port patterns

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Process execution frequency
- File modifications
- User-account changes
- Network-flow characteristics
- Temporal relationships between events

A general classification function can be represented as:

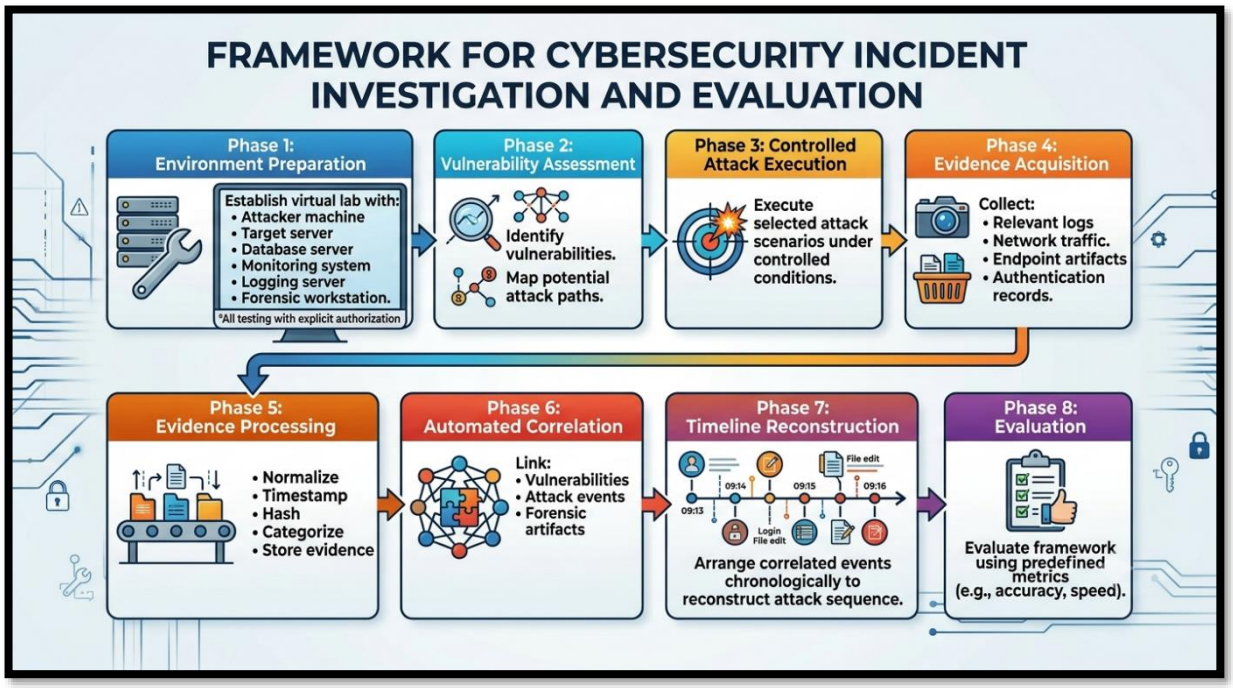
$$Y = f(X_1, X_2, \ldots, X_n)$$

where $X_1, \ldots, X_n$ represent extracted security-event features and Y represents the predicted event category.

The model should support human investigators rather than replace forensic judgment.

8. PROPOSED METHODOLOGY

The research can follow a controlled experimental methodology.



9. EVALUATION METRICS

The proposed framework can be evaluated using the following measures.

9.1 Detection Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

9.2 Precision

$$Precision = \frac{TP}{TP + FP}$$

Precision indicates how many detected events are actually relevant security events.

9.3 Recall

$$Recall = \frac{TP}{TP + FN}$$

Recall measures the ability to identify relevant attack events.

9.4 F1-Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

9.5 Forensic Analysis Time

The time required to move from evidence acquisition to an actionable incident timeline can be compared between conventional analysis and the proposed automated approach.

9.6 Evidence Integrity

Evidence integrity can be evaluated by comparing stored cryptographic hashes with hashes generated during subsequent verification.

9.7 Attack Reconstruction Effectiveness

The reconstructed timeline can be compared with the known sequence of events generated during the controlled experiment.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

10. EXPECTED RESULTS AND DISCUSSION

Because the proposed framework is presented as a research design rather than a report of a completed laboratory experiment, numerical performance values should not be claimed without conducting the proposed experiments.

The expected contribution is that integrating penetration-testing information with forensic evidence can provide additional context during incident investigation. A vulnerability discovered during ethical hacking can become a reference point for interpreting subsequent security events.

For example, if penetration testing identifies a vulnerable service and the forensic system subsequently detects an unusual connection to that service followed by authentication anomalies and process execution, the combined evidence may provide a stronger investigative context than any individual event.

Automation may also reduce repetitive evidence-processing activities. Instead of requiring investigators to manually inspect every event, the framework can prioritize events according to temporal relationships, vulnerability context, source reliability, and suspicious behavior.

However, automation introduces its own challenges. Incorrect event correlation may generate false associations, while incomplete logging can result in missing portions of an attack timeline. Therefore, automated results should remain traceable to the original evidence.

11. EVIDENCE INTEGRITY AND CHAIN OF CUSTODY

An important feature of the framework is the preservation of evidence integrity.

Each evidence object should contain metadata such as:

Attribute	**Purpose**
Evidence ID	Unique identification
Source	Identifies originating system
Timestamp	Establishes acquisition time
Hash	Supports integrity verification
Collector	Identifies collection process
Location	Identifies storage location
Access history	Maintains traceability

The framework can maintain a chain-of-custody record for each artifact.

For example:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

$$Evidence \rightarrow Hash \rightarrow Storage \rightarrow Analysis \rightarrow Report$$

This approach helps establish traceability from the original evidence to the final forensic finding.

Research on digital evidence authentication and tampering demonstrates why the reliability of artifacts must be considered during forensic investigation.

12. ADVANTAGES OF THE PROPOSED FRAMEWORK

The integrated approach offers several potential advantages.

12.1 Proactive and Reactive Security Integration

Ethical hacking identifies weaknesses before or during controlled testing, while digital forensics analyzes evidence associated with security events.

12.2 Improved Event Correlation

The framework links vulnerability information with observed system behavior.

12.3 Reduced Investigation Time

Automated preprocessing and correlation can reduce repetitive manual investigation tasks.

12.4 Better Attack Reconstruction

Combining network, authentication, endpoint, and vulnerability information can provide a more comprehensive timeline.

12.5 Evidence Traceability

Hashing and provenance metadata provide mechanisms for monitoring evidence integrity.

12.6 Actionable Security Intelligence

The output of forensic analysis can be fed back into vulnerability management and penetration-testing activities.

13. LIMITATIONS

Several limitations should be considered.

First, the quality of automated analysis depends on the quality and completeness of collected evidence. Missing logs may prevent accurate reconstruction.

Second, different systems use different timestamp formats and time sources, creating synchronization challenges.

Third, encrypted communications may restrict the visibility of network-level information.

Fourth, sophisticated attackers may attempt anti-forensic activities such as modifying, deleting, or obscuring evidence.

Fifth, machine-learning approaches require representative datasets. A model trained only on limited attack scenarios may not generalize to previously unseen environments.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Finally, forensic automation should not be treated as an unquestionable source of truth. Human investigators must validate important findings against the underlying evidence.

14. FUTURE SCOPE

Future research can extend the framework in several directions.

14.1 AI-Based Evidence Analysis

Machine-learning and deep-learning techniques can be investigated for automated event classification and anomaly detection.

14.2 Large Language Models

Large language models could assist investigators in summarizing correlated evidence and generating preliminary incident reports, provided that outputs remain linked to verifiable source evidence.

14.3 MITRE ATT&CK Integration

The framework can map observed behaviors to standardized adversary tactics and techniques, improving attack characterization.

14.4 Cloud Forensics

Future implementations can incorporate evidence from cloud platforms, container environments, and serverless systems.

14.5 IoT Forensics

The framework can be extended to IoT environments where heterogeneous devices produce large quantities of distributed evidence.

14.6 Real-Time Forensic Analysis

Future versions can investigate near-real-time collection and correlation for faster incident detection.

14.7 Explainable Automated Forensics

Automated conclusions should provide the evidence and reasoning chain supporting each finding, enabling investigators to validate system-generated conclusions.

15. CONCLUSION

This research proposes an **Integrated Ethical Hacking and Digital Forensics Framework for Automated Cyberattack Detection and Evidence Analysis**. The framework addresses the gap between proactive vulnerability assessment and post-incident forensic investigation by connecting penetration-testing results with network, authentication, endpoint, and system evidence.

The proposed architecture consists of vulnerability identification, controlled attack simulation, evidence collection, preprocessing, integrity verification, automated evidence correlation, attack timeline reconstruction, and forensic reporting. This integration provides a systematic method for transforming ethical-hacking observations into contextual forensic intelligence.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Existing research indicates that both penetration testing and digital forensics face challenges related to increasingly sophisticated attacks, heterogeneous environments, evidence acquisition, artifact authentication, and automation. The proposed framework addresses these issues conceptually by establishing a continuous relationship between vulnerability discovery and evidence-based investigation.

The proposed evaluation methodology provides measurable criteria including detection accuracy, precision, recall, F1-score, forensic analysis time, evidence integrity, and attack reconstruction effectiveness. Actual numerical results should be obtained through implementation and controlled experimentation rather than assumed.

Overall, the framework provides a foundation for future research into automated, evidence-driven cybersecurity operations in which ethical hacking, continuous monitoring, digital forensics, and intelligent analysis operate as interconnected components of an integrated security lifecycle.

REFERENCES

[1] Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Böröcz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access, 10*, 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059

[2] Selvamurugan, A., Selvamurugan, C., Parthiban, K. G., et al. (2026). Ethical hacking and penetration testing in cyber security. In *Ethical Hacking and Penetration Testing in Cybersecurity* (pp. 145–186). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3536-0.ch006

[3] *Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools*. (2024). *Journal of Cybersecurity and Privacy*, *4*(3), 410–448. https://doi.org/10.3390/jcp4030021

[4] Fähndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. *Forensic Science International: Digital Investigation, 46*, 301617. https://doi.org/10.1016/j.fsidi.2023.301617

[5] Neale, C. (2023). Fool me once: A systematic review of techniques to authenticate digital artefacts. *Forensic Science International: Digital Investigation*, *45*, 301516. https://doi.org/10.1016/j.fsidi.2023.301516

[6] Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, Y. (2022). The case for zero trust digital forensics. *Forensic Science International: Digital Investigation, 40*, 301352. https://doi.org/10.1016/j.fsidi.2022.301352.

[7] Breitinger, F., Hilgert, J.-N., Hargreaves, C., Sheppard, J., Overdorf, R., & Scanlon, M. (2024). DFRWS EU 10-year review and future directions in digital forensic research. *Forensic Science International: Digital Investigation, 48*, 301685. https://doi.org/10.1016/j.fsidi.2023.301685.

[8] Mohamed, A., & Khalid, C. (2019). Detection of timestamps tampering in NTFS using machine learning. *Procedia Computer Science, 160*, 778–784. https://doi.org/10.1016/j.procs.2019.11.011.

[9] Palmbach, D., & Breitinger, F. (2020). Artifacts for detecting timestamp manipulation in NTFS on Windows and their reliability. *Forensic Science International: Digital Investigation, 32*, 300920. https://doi.org/10.1016/j.fsidi.2020.300920.

[10] Schneider, J., Wolf, J., & Freiling, F. C. (2020). Tampering with digital evidence is hard: The case of main memory images. *Forensic Science International: Digital Investigation, 32*, 300924. https://doi.org/10.1016/j.fsidi.2020.300924

(This work is licensed under a Creative Commons Attribution 4.0 International License.)