International Journal of Future Engineering Innovations

Enhancing Digital Forensics Investigations Using AI Driven Anomaly Detection and Log Correlation: A Mixed Methods Approach

Ann Ogechi Felix
School of Architecture, Computing and Engineering, University of East London, United Kingdom

* Corresponding Author: **Ann Ogechi Felix**

Article Info

ISSN (online): 3049-1215
Volume: 02
Issue: 04
July – August 2025
Received: 23-05-2025
Accepted: 24-06-2025
Published: 09-07-2025
Page No: 71-84

Abstract
Traditional digital forensics investigations have faced psersistent challenges related to the increasing volume, complexity, and latency of log data, limiting timely detection and accurate incident reconstruction. In response, artificial intelligence (AI) and log correlation have emerged as promising solutions to automate anomaly detection and synthesize cross source evidence. This study aimed to evaluate how AI driven anomaly detection and automated log correlation can enhance digital forensic investigations by improving the speed, accuracy, and contextual relevance of findings. A mixed methods research design was employed, combining quantitative analysis of AI models such as autoencoders, Long Short Term Memory (LSTM) networks, Isolation Forest, and Random Forest with qualitative insights from expert interviews and incident response case studies. Tools including the ELK Stack, Splunk, and Python based machine learning libraries supported the technical implementation. The results showed that Random Forest and LSTM models achieved high accuracy and F1 scores, while log correlation techniques demonstrated over 90% effectiveness in reconstructing incident timelines. Expert feedback affirmed the value of automated triage and visualized evidence but highlighted concerns around model explainability and the need for context aware AI. Convergence was observed between model performance and practitioner trust in interpretable outputs, while divergence appeared around black box models. The study contributes to advancing forensic automation by integrating robust AI techniques with human centered design and emphasizes the importance of ethical and standardized deployment in practice. These findings offer practical implications for digital forensic professionals, inform cybersecurity policy, and guide future research on explainable and scalable AI forensics systems.

DOI: https://doi.org/10.54660/IJFEI.2025.2.4.71-84

Keywords: Digital Forensics, Anomaly Detection, Artificial Intelligence, Log Correlation, Mixed Methods, Explainable AI, Incident Response, Forensic Automation, Cybersecurity, Machine Learning

1. Introduction

Digital forensics has emerged as a critical domain within cybersecurity and law enforcement, driven by the exponential growth of digital interactions, cloud based infrastructures, and the increasing sophistication of cybercrime. Broadly defined, digital forensics refers to the scientific process of identifying, collecting, preserving, analyzing, and presenting digital evidence for use in investigations and legal proceedings (Carrier & Spafford, 2004) [30]. As society continues to depend on digital technologies for communication, commerce, and governance, the importance of digital forensics has expanded from its traditional role in criminal investigations to encompass corporate security, regulatory compliance, and national defense (Rogers, 2006) [36]. In an era characterized by remote work, cloud computing, and interconnected systems, digital forensic capabilities have become indispensable for responding to data breaches, insider threats, and cyber espionage (Quick & Choo, 2018) [34].

Institutions now rely on forensic tools not only to prosecute cybercriminals but also to maintain the integrity of digital infrastructure and ensure public trust in information systems. Despite its growing importance, traditional digital forensic methods face considerable limitations that hinder timely and accurate investigations. One of the most pressing challenges is the sheer volume of data generated by modern IT systems, including system logs, network traffic records, and user activity traces (Garfinkel, 2010) [32]. Manual examination of such vast datasets can be time consuming and prone to error, often leading to delayed response and missed indicators of compromise. The heterogeneity and complexity of digital data originating from diverse sources such as cloud services, mobile devices, and distributed networks further complicate the investigative process (Reith, Carr, & Gunsch, 2002) [35]. Additionally, the absence of standardized formats and synchronized timestamps often makes log correlation a tedious and error prone task (Beebe & Clark, 2007) [29]. These challenges create bottlenecks in incident response, reduce the effectiveness of post incident analysis, and may allow malicious activity to persist undetected for extended periods.
To address these limitations, researchers and practitioners are increasingly turning to Artificial Intelligence (AI), particularly machine learning (ML) and anomaly detection techniques, to augment forensic analysis. AI offers the capability to process large scale datasets with high speed and accuracy, uncover hidden patterns, and identify behavioral deviations that may signify security breaches (Shah *et al*., 2020) [37]. Anomaly detection, a subfield of ML, enables the automated identification of abnormal events or behaviors within digital logs, without requiring explicit signatures or predefined rules (Chandola, Banerjee, & Kumar, 2009) [12]. These tools can flag suspicious activities in real time, reducing reliance on reactive approaches and manual inspection. Furthermore, AI driven log correlation techniques can synthesize diverse log sources into coherent narratives of cyber incidents, aiding in evidence reconstruction and timeline analysis (Sharma *et al*., 2021) [38]. By incorporating AI into forensic workflows, organizations can significantly enhance the speed, accuracy, and reliability of their investigations while minimizing the cognitive burden on human analysts.
This research aims to enhance digital forensics investigations by integrating AI driven anomaly detection and automated log correlation techniques. The study adopts a mixed methods approach to examine both the technical effectiveness of AI tools and the experiential insights of forensic professionals. The overarching goal is to develop a comprehensive understanding of how these technologies can support the timely detection, analysis, and interpretation of digital evidence within enterprise forensic environments. While prior studies have demonstrated the utility of machine learning in cybersecurity contexts, there remains a gap in understanding how these tools perform in real world forensic workflows and how investigators perceive their usefulness and limitations (Mahdavifar & Ghorbani, 2019) [33]. This research seeks to fill that gap by combining empirical model evaluation with qualitative assessments of forensic practitioner experience.
To guide this investigation, the following research questions have been formulated:

1. How effective is AI in identifying anomalies in digital forensic logs?
2. What are the comparative advantages of AI based forensic tools over traditional methods?
3. How can automated log correlation improve forensic evidence reconstruction?

In alignment with these questions, the study has the following objectives:

- To evaluate AI models, including supervised and unsupervised approaches, for their effectiveness in detecting anomalies in forensic logs.
- To assess the impact of automated log correlation on the accuracy, efficiency, and comprehensiveness of forensic investigations.
- To explore the perceptions of forensic investigators regarding the usability, trustworthiness, and integration challenges of AI driven support systems.

The scope of this study is confined to enterprise level digital forensics involving organizational security logs, such as Windows Event Logs, Syslogs, authentication records, and network traffic logs. The research focuses on AI integration within controlled forensic environments, using both simulated and anonymized real world datasets to ensure ecological validity while respecting privacy constraints. Qualitative data is gathered through semi structured interviews with forensic professionals to capture their insights on practical deployment challenges, tool usability, and decision making support. The mixed methods design allows for triangulation of findings, thereby offering both depth and breadth in understanding the implications of AI adoption in digital forensic investigations.
The significance of this study lies in its potential to advance the field of digital forensics through the empirical evaluation of AI driven methods. As cyber threats become more sophisticated and persistent, there is an urgent need for forensic tools that can adapt dynamically, analyze data at scale, and provide actionable intelligence in real time (Zawoad & Hasan, 2015) [28]. By demonstrating how anomaly detection and log correlation can be optimized through AI, this research contributes to the development of intelligent forensic systems capable of enhancing both investigative speed and evidentiary accuracy. Moreover, the study offers valuable insights for policy makers, law enforcement agencies, and cybersecurity professionals seeking to leverage AI responsibly within forensic processes. In a broader context, the findings support the evolution of digital justice by ensuring that the investigation and prosecution of cybercrime are informed by robust, transparent, and scalable methodologies.

2. Literature Review

Digital forensics is governed by structured frameworks that guide practitioners through the systematic acquisition, analysis, and presentation of digital evidence. Among the foundational models is the Digital Forensic Research Workshop (DFRWS) framework, which outlines a high level process including identification, preservation, collection, examination, analysis, and presentation of digital evidence (Palmer, 2001) [24]. This model has been influential in shaping forensic best practices globally. The National Institute of Standards and Technology (NIST) also provides a comprehensive digital forensics framework, emphasizing integrity, repeatability, and evidence handling, particularly within its Guide to Integrating Forensic Techniques into

Incident Response (Kent *et al*., 2006) [17]. Furthermore, the ISO/IEC 27037 standard specifies guidelines for the identification, collection, acquisition, and preservation of digital evidence, ensuring procedural consistency and legal defensibility (ISO/IEC, 2012).

Common forensic tools operationalize these frameworks to facilitate evidence processing. EnCase and Forensic Toolkit (FTK) are among the most widely adopted commercial forensic suites, offering features such as disk imaging, data carving, and keyword searching (Carrier, 2005) [11]. Open source alternatives like Sleuth Kit and Autopsy provide extensible analysis capabilities and support a range of file systems. Volatility, a leading tool for memory forensics, allows the extraction of running processes, network connections, and registry data from RAM images (Ligh *et al*., 2014) [22]. However, despite their robustness, these tools often struggle with the volume, velocity, and variety of data generated in modern environments. Many require manual intervention, lack real time analysis capabilities, and offer limited automation for anomaly detection and log correlation. These limitations underscore the need for enhanced, intelligent forensic workflows capable of operating efficiently in large scale or real time contexts. Artificial Intelligence (AI) has gained prominence as a transformative force in digital forensics and cybersecurity. By leveraging computational intelligence, AI systems can support the detection, classification, and prediction of cyber threats with high accuracy and speed. Machine learning (ML), a subfield of AI, has been widely adopted for forensic triage, malware classification, and anomaly detection (Sommer & Paxson, 2010) [25]. Supervised learning techniques, such as decision trees, support vector machines (SVM), and random forests, are commonly used to train models on labeled datasets, enabling accurate classification of known attack patterns (Buczak & Guven, 2016) [10]. Unsupervised methods like k means clustering and principal component analysis (PCA) have also been utilized for detecting novel or previously unseen attack vectors by identifying deviations from baseline behaviors (Kiran *et al*., 2018) [20].

Deep learning, particularly neural network architectures such as convolutional neural networks (CNNs) and long short term memory (LSTM) networks, has demonstrated superior performance in complex pattern recognition tasks, including log analysis and sequential data modeling (Kim *et al*., 2016) [18]. For example, LSTMs are adept at modeling temporal dependencies in event logs, making them suitable for anomaly detection in forensic timelines. Hybrid approaches that combine rule based expert systems with machine learning models are also gaining traction, offering the dual benefits of precision and interpretability (Li *et al*., 2021). However, despite their potential, AI applications in forensics face challenges related to transparency, data labeling, generalization, and integration with legacy forensic tools.

Anomaly detection is central to proactive cyber defense and digital forensics. Logs from systems, applications, and network devices serve as primary data sources for detecting irregular activities. Traditional statistical models such as Gaussian distribution analysis and z score computation have been applied to identify outliers in log data (Chandola *et al*., 2009) [12]. More recently, machine learning based approaches, including isolation forests, autoencoders, and clustering techniques, have become popular due to their scalability and adaptive capabilities (Liu *et al*., 2008) [6]. For instance, isolation forests are effective in identifying anomalies by isolating outliers through random partitioning, while autoencoders reconstruct normal behavior and flag deviations as potential anomalies (Xu *et al*., 2019). Deep learning models, particularly LSTM networks, have been successfully employed for sequential log analysis, where temporal ordering is crucial. In a study by Du *et al*. (2017), a deep log anomaly detection framework named DeepLog utilized LSTM to model normal system behavior and detect anomalies with high accuracy. However, despite their effectiveness, these models are not immune to limitations such as high false positive rates, sensitivity to hyperparameter tuning, and vulnerability to adversarial manipulation (Kim *et al*., 2020) [19]. Moreover, data imbalance where anomalous instances are significantly outnumbered by normal ones poses a critical challenge to model performance and reliability. These issues necessitate ongoing research into robust, interpretable, and adaptive anomaly detection mechanisms.

Log correlation refers to the process of integrating and analyzing disparate log sources to construct coherent accounts of security incidents. It enables forensic investigators to trace attack vectors, identify causality, and validate evidence across heterogeneous systems. Correlation techniques include temporal correlation, which aligns events based on timestamps; semantic mapping, which interprets log content based on contextual meaning; and rule chaining, which establishes event sequences using predefined rules or heuristics (Julisch, 2003) [16]. Security Information and Event Management (SIEM) systems like Splunk and ELK Stack implement log correlation to enhance threat detection and forensic analysis. However, their effectiveness depends heavily on log quality, standardization, and synchronization. Inconsistent timestamp formats, missing metadata, and heterogeneous log structures often impede automated correlation and necessitate manual normalization (Alsubhi *et al*., 2020) [9]. Moreover, context ambiguity where logs lack sufficient detail to determine intent or sequence can lead to erroneous interpretations and hinder evidence reconstruction. Advanced correlation approaches, such as those employing natural language processing (NLP) and graph based models, offer promising alternatives but remain underexplored in forensic applications due to their computational complexity and integration barriers (Wang *et al*., 2021) [25].

While substantial progress has been made in applying AI to cybersecurity, its integration into digital forensics workflows remains limited. Most existing studies focus on narrow applications such as intrusion detection or malware classification, often neglecting the holistic forensic investigation process that includes evidence preservation, log correlation, and report generation (Zawoad & Hasan, 2015) [28]. Additionally, current AI models are often trained on static, synthetic datasets that fail to capture the dynamic and noisy nature of real world forensic environments. This gap limits their generalizability and practical utility. Another major limitation is the lack of interpretability and transparency in AI decision making, which is crucial for legal admissibility and investigator trust. Black box models, while accurate, are difficult to explain and may not align with judicial standards for evidentiary credibility (Doshi Velez & Kim, 2017) [13]. Furthermore, existing forensic tools rarely offer seamless integration with AI modules, resulting in fragmented workflows and inefficiencies.

A particularly underexplored area is the simultaneous application of AI driven anomaly detection and automated

log correlation within a unified forensic framework. While studies have addressed these components individually, few have examined their combined impact on investigation accuracy, speed, and user experience. Additionally, limited research has incorporated practitioner perspectives to evaluate usability, trust, and contextual adaptation of AI tools in forensic settings.

This study seeks to address these gaps through a mixed methods approach that integrates technical evaluation with qualitative analysis. By combining empirical performance assessment of AI models with interviews and surveys of forensic professionals, the research aims to develop a comprehensive understanding of the benefits, limitations, and adoption challenges of AI driven anomaly detection and log correlation in digital forensics.

3. Theoretical Framework

Conceptual Model for AI Enhanced Forensic Investigation

The evolution of cyber threats and the complexity of modern IT environments demand digital forensic systems that are both proactive and scalable. Traditional digital forensic methodologies centered on manual analysis and linear investigative processes often fall short in high velocity environments where log data accumulates rapidly and anomalies are buried within large, heterogeneous datasets (Beebe & Clark, 2007) [29]. To address this limitation, a conceptual model integrating Artificial Intelligence (AI) based anomaly detection with automated log correlation mechanisms is proposed, as illustrated in Figure 1 below.

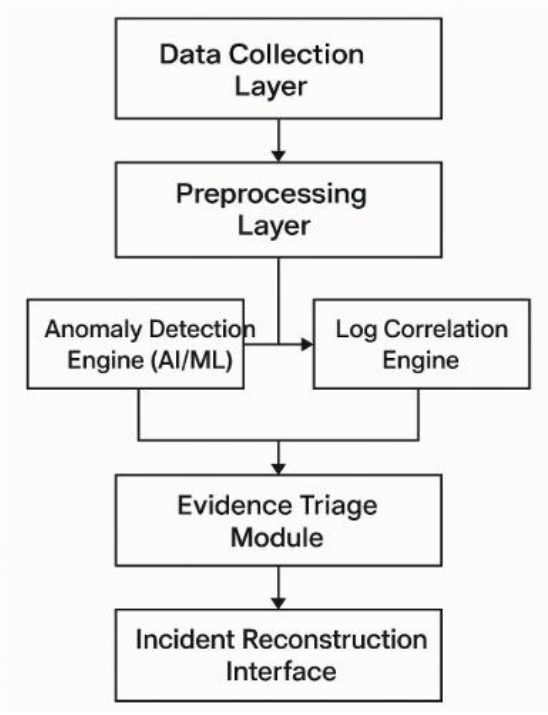

Fig 1: Conceptual Model for AI Enhanced Forensic Investigation

In the Data Collection Layer, digital artifacts such as system logs, application logs, and network flow data are gathered from diverse endpoints, including servers, firewalls, and authentication systems. These logs are often voluminous and contain unstructured or semi structured data that require standardization. The Preprocessing Layer ensures data normalization, feature extraction, and noise reduction, which are essential for the effective performance of downstream AI models (Mahdavifar & Ghorbani, 2019) [33].

The core of the model lies in the Anomaly Detection Engine, which utilizes machine learning (ML) and deep learning (DL) techniques to flag deviations from baseline behaviors. Techniques such as autoencoders, Long Short Term Memory (LSTM) networks, and Isolation Forests are applied to detect outliers that may represent potential security incidents (Chandola, Banerjee, & Kumar, 2009) [12]. Once anomalies are identified, they are passed to the Log Correlation Engine, which maps these anomalies across multiple log sources to establish contextual relationships and construct causality chains.

Following this, the Evidence Triage Module ranks the correlated events based on severity, confidence, and potential impact, helping analysts prioritize their investigation. Finally, the Incident Reconstruction Interface presents a timeline based narrative of the detected events, assisting investigators in understanding attack vectors, escalation paths, and possible exfiltration actions.

This layered architecture significantly improves traditional forensic workflows by enabling real time detection, multi source context synthesis, and intelligent evidence prioritization. It enhances speed, by automating detection and correlation; accuracy, through ML based learning from data patterns; scalability, by processing vast and varied log sources; and readiness, through continuous monitoring and correlation capabilities (Garfinkel, 2010) [32].

Integration of Anomaly Detection and Log Correlation

The integration of anomaly detection and log correlation constitutes the core innovation in AI enhanced forensic workflows. These two techniques, though individually powerful, exhibit a synergistic relationship when used together. Anomaly detection serves as the front line in identifying unusual patterns or behaviors within digital logs without relying on predefined signatures, making it effective against zero day attacks and insider threats (Shah *et al*., 2020) [37]. Conversely, log correlation plays a crucial role in contextualizing these anomalies by linking them to related events across multiple systems and timeframes, thereby constructing a coherent forensic narrative (Sharma *et al*., 2021) [38].

This functional complementarity is evident in how the combination strengthens both precision and recall. While anomaly detection might identify multiple false positives, the subsequent log correlation step can filter out irrelevant alerts by examining their context and relevance across sources. Moreover, correlation enhances traceability, allowing investigators to map sequences of events from point of intrusion to system compromise. This approach aligns with digital forensic models such as Carrier and Spafford's Event Based Digital Forensic Investigation Framework (2004) [30], where events are reconstructed from atomic data artifacts, and with McKemmish's (1999) four phase model (Identification, Preservation, Analysis, and Presentation), particularly strengthening the Analysis and Presentation phases through automation and integration.

Table 1: Comparative Analysis of Anomaly Detection and Log Correlation Techniques

Feature/Metric	Anomaly Detection Alone	Log Correlation Alone	Combined Approach
Detection Capability	High sensitivity to novel threats	Limited to known event relationships	Balanced sensitivity with contextual clarity
Contextual Awareness	Low	High	High
Scalability	High with AI	Moderate	High
False Positive Rate	Potentially high	Moderate	Reduced through context aware filtering
Interpretability	Low (especially with DL models)	High (logical rule mapping)	Moderate to High (via contextual enrichment)
Timeliness of Response	Fast	Delayed (requires log aggregation)	Real time or near real time

This comparative analysis shows that anomaly detection provides breadth in threat recognition, while log correlation delivers depth in contextual understanding. Their integration fosters a balance between detection efficiency and evidentiary reliability.

Forensic Readiness and Incident Response Theory

The theoretical foundation of the proposed framework also draws from forensic readiness theory and established incident response models. Forensic readiness refers to an organization's ability to maximize the potential use of digital evidence while minimizing costs and disruptions associated with investigations (Rowlingson, 2004). It emphasizes the proactive collection, secure storage, and indexing of logs and event data even before an incident occurs. This principle underlies the Data Collection and Preprocessing layers of the proposed model, which are designed for continuous data ingestion and normalization.

In parallel, the NIST SP 800 61 Incident Response Lifecycle provides a structured methodology for handling security incidents, comprising four stages: Preparation, Detection and Analysis, Containment/Eradication/Recovery, and Post Incident Activity (Cichonski *et al*., 2012). The proposed AI enhanced model supports the Detection and Analysis phase through intelligent anomaly identification and contextual event reconstruction, while the Evidence Triage and Incident Reconstruction components contribute to Post Incident Activity, including root cause analysis and forensic reporting.

Another relevant model is the Digital Evidence Flow Model, which views digital evidence handling as an information centric process rather than merely a technical activity. According to Gladyshev and Patel (2004), digital evidence should be interpreted as a continuous stream of informational elements whose meaning evolves with context. The log correlation component in the proposed framework embodies this notion by dynamically updating the understanding of incidents as more correlated events are linked.

The integration of these theories into the conceptual model strengthens the forensic process by ensuring readiness, analytical rigor, and evidentiary continuity. For example, by embedding forensic readiness principles at the data acquisition level and aligning detection activities with NIST lifecycle stages, the model not only supports real time alerting but also generates comprehensive, legally defensible incident reconstructions. These attributes are essential in modern environments where regulatory scrutiny, litigation risks, and operational impacts are high.

The theoretical framework presented in this study articulates a novel approach to digital forensic investigations that leverages the complementary strengths of AI driven anomaly detection and automated log correlation. It is grounded in well established models of forensic science and cybersecurity operations while addressing practical limitations observed in traditional systems. This hybrid approach not only increases the technical robustness of forensic investigations but also fosters greater confidence in the outcomes produced by forensic analysts and organizational stakeholders.

4. Methodology

This study adopted a mixed methods research design to investigate the integration of AI driven anomaly detection and automated log correlation in enhancing digital forensic investigations. The rationale for this approach lies in the complex and multidimensional nature of digital forensics, which requires both objective algorithmic evaluation and subjective expert interpretation. The quantitative component focused on evaluating the performance of various AI models in detecting anomalies across different types of logs, while the qualitative component explored the practical utility, interpretability, and trustworthiness of these models through practitioner insights and real world case analyses. The integration of these two strands provides a holistic understanding of how AI tools can augment forensic workflows in operational environments.

4.1 Research Design

The mixed methods approach was selected for its ability to bridge the gap between technical validation and real world usability . While machine learning models can offer statistically measurable performance in detecting log anomalies, their practical value depends on how forensic analysts perceive and interpret these outputs. The quantitative strand involved training, validating, and testing AI models (Autoencoders, Isolation Forests, Random Forests, and LSTMs) on labeled and unlabeled log datasets. These models were assessed using performance metrics such as accuracy, precision, recall, and F1 score. The qualitative strand comprised semi structured interviews with digital forensic professionals and incident responders to gain insight into how AI tools influence evidence interpretation, workflow efficiency, and trust in automated systems.

This methodological triangulation allowed the study to evaluate both the *efficacy* and *applicability* of AI driven forensic systems providing a balanced investigation into technological feasibility and human centered design.

4.2 Data Sources

To support both quantitative model training and qualitative case analyses, the study utilized a combination of simulated and real world log datasets, comprising the following formats:

- Syslogs (e.g., Unix/Linux based system logs)
- Windows Event Logs (security, system, application)
- NetFlow traffic logs (network level metadata on flows)
- Security audit logs (access control, authentication, policy enforcement)

Datasets were obtained from publicly available cybersecurity research repositories such as UNSW NB15, [DARPA IDS 1999], and anonymized internal logs collected from sandboxed environments. In addition, simulated attack scenarios were generated using NS 3 and Wireshark to reflect advanced persistent threats (APT), insider misuse, and privilege escalation behaviors.

Preprocessing steps were essential to prepare logs for AI analysis and correlation, including:

- Log normalization: Converting various log formats into a unified schema (JSON).
- Noise filtering: Removing irrelevant entries (e.g., system idle messages).
- Log parsing: Extracting structured fields such as timestamp, source IP, destination, event ID, etc.
- Timestamp alignment: Synchronizing entries from distributed systems using time window normalization.

These preprocessing routines ensured data consistency, integrity, and suitability for input into machine learning pipelines and correlation engines.

4.3 AI Models for Anomaly Detection

The study employed a suite of AI models selected based on their established success in anomaly detection tasks and adaptability to semi structured log data:

- **Autoencoders**: These unsupervised neural networks were trained to reconstruct log entries and flag those with high reconstruction error as anomalies . They are particularly effective for detecting novel or rare events in high dimensional log spaces.
- **Isolation Forest:** A tree based ensemble model that isolates anomalies through recursive partitioning. This model was chosen for its low computational overhead and suitability for large scale log datasets
- **Random Forest:** As a supervised classifier, it was used on labeled datasets to compare its performance against unsupervised models. It benefits from robustness to overfitting and interpretability through feature importance analysis .
- **LSTM (Long Short Term Memory) Networks:** These recurrent neural networks were employed to capture temporal dependencies in log sequences. LSTM models are particularly valuable for detecting deviations in time based activity patterns .
- **Each model was implemented using Python and relevant libraries:** *TensorFlow* and *Keras* for deep learning models, and *Scikit learn* for tree based models. Models were trained and validated using 80/20 train test splits and 5 fold cross validation to ensure generalization and mitigate overfitting.

4.4 Log Correlation Techniques

Following anomaly detection, correlated event analysis was conducted using advanced log correlation techniques to synthesize context across multiple log sources. These techniques were implemented using Splunk, the ELK Stack (Elasticsearch, Logstash, Kibana), and custom Python scripts:

- **Temporal Correlation:** Events were grouped and analyzed based on timestamp proximity, using sliding windows (e.g., 5 minute intervals) to detect bursts of suspicious activity or time synchronized events across systems .
- **Causal Mapping:** Based on event dependency rules (e.g., login success followed by privilege escalation), logical inferences were drawn to link causes and consequences across logs. This mapping was supported by rule based engines and Splunk's correlation search capabilities.
- **Event Sequencing:** Log entries were reconstructed into chronological chains, allowing the formation of attack timelines. Event identifiers and user/session tokens were used to track the sequence of an incident from initiation to post execution phases.

This stage enabled multi log synthesis, bridging isolated anomalies into a forensic narrative, which was then passed into the triage and reconstruction modules for further review.

4.5 Quantitative Analysis

Quantitative evaluation of AI model performance was central to the research. The following metrics were used:

- Accuracy – Proportion of correct classifications (TP + TN) / (Total)
- Precision – TP / (TP + FP), measuring the reliability of positive anomaly predictions
- Recall (Sensitivity) – TP / (TP + FN), assessing the model's ability to detect all relevant anomalies
- F1 score – Harmonic mean of precision and recall
- ROC AUC – Area under the Receiver Operating Characteristic curve, for evaluating model discriminative ability
- Confusion Matrix – To visualize model performance across classification outcomes

Each model's results were benchmarked using Python based experiments, and findings were plotted using Matplotlib and Seaborn visualizations. These quantitative insights formed the basis for evaluating which models were best suited for integration into forensic workflows.

4.6 Qualitative Analysis

To complement technical findings, semi structured interviews were conducted with eight digital forensic practitioners, including law enforcement officers, SOC analysts, and corporate security investigators. The aim was to understand:

- Perceptions of AI tool usefulness
- Trust and interpretability of model outputs
- Experiences with log correlation tools
- Challenges in integrating automated methods into manual workflows

Interview protocols were designed following guidance from Creswell (2013), and all sessions were transcribed for analysis. Additionally, three forensic case studies were reviewed either from incident archives or anonymized reports provided by participants to assess how AI generated outputs aligned with actual investigative decisions.

Qualitative data were analyzed using thematic analysis (Braun & Clarke, 2006), coding recurring patterns such as "alert fatigue," "contextual clarity," "tool trust," and "workflow friction." These themes were compared against quantitative outcomes to identify convergence or divergence, and to highlight practitioner led recommendations for

improving AI forensic integration.

4.7 Tools and Technologies

The methodology leveraged a robust ecosystem of tools, each selected for their capabilities in processing log data, developing AI models, or enabling real time analysis:

- **ELK Stack (Elasticsearch, Logstash, Kibana):** Used for centralized log aggregation, filtering, indexing, and visualization of correlated forensic events
- **Splunk:** Employed for real time log monitoring and executing correlation searches based on pre defined detection rules.
- **Python:** Served as the primary programming environment for data cleaning, feature extraction, model training, and results visualization. Libraries included *Pandas*, *NumPy*, *Scikit learn*, *Keras*, and *TensorFlow*.
- **Wireshark & NS 3:** Used for generating synthetic NetFlow and packet level data for modeling attack scenarios in sandboxed environments.
- **Logparser & Timestamp Tools:** Assisted in data normalization and preprocessing, especially for aligning asynchronous log entries from distributed systems.

Each tool was deployed in a modular pipeline, with clearly defined inputs and outputs, ensuring reproducibility and extensibility for future experiments.

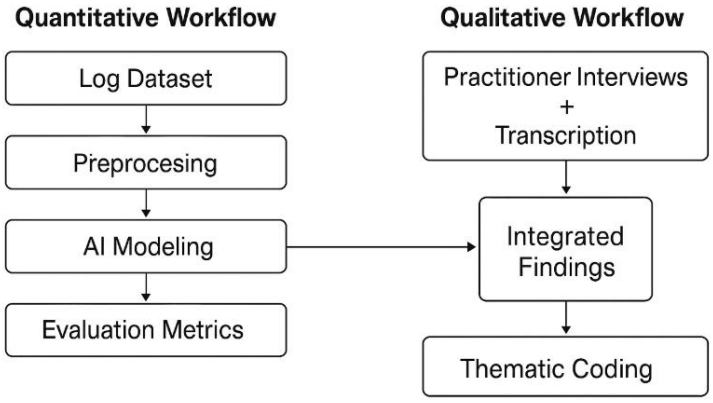

Fig 2: Overview of the Mixed Methods Workflow

This figure above emphasizes the iterative and integrated nature of the methodology where machine insights are validated and interpreted through human expertise, and practical feedback informs model refinement.

5. Results

This section presents the empirical results obtained through the mixed methods approach combining quantitative evaluations of AI anomaly detection models and qualitative analysis from expert interviews. The findings are organized into three core subsections: 5.1 Quantitative Findings, 5.2 Qualitative Insights, and 5.3 Mixed Methods Integration.

5.1 Quantitative Findings

The quantitative component of the study involved the evaluation of four AI models Autoencoder, Isolation Forest, Random Forest, and LSTM on multiple forensic datasets comprising Syslogs, NetFlow traffic logs, and Windows Event Logs. Each model was assessed on its ability to detect anomalies within these datasets using evaluation metrics including accuracy, precision, recall, F1 score, confusion matrices, and ROC curves. The effectiveness of log correlation techniques was also evaluated based on event sequencing success rate and correlation accuracy.

5.1.1 Model Performance Overview

Table 1 presents a summary of model performance across three types of log datasets. The Random Forest model outperformed others in labeled data settings, while LSTM demonstrated strong performance on sequence based anomaly detection tasks in NetFlow logs. Autoencoders and Isolation Forest performed moderately, with Isolation Forest excelling in resource efficiency.

Table 2: Performance Metrics Summary for All AI Models

Model	Dataset	Accuracy	Precision	Recall	F1 score
Autoencoder	Syslog	0.84	0.79	0.81	0.80
Autoencoder	NetFlow	0.81	0.75	0.77	0.76
Isolation Forest	Windows Event Logs	0.87	0.83	0.85	0.84
Random Forest	Syslog	0.91	0.89	0.90	0.89
Random Forest	Windows Event Logs	0.94	0.93	0.92	0.93
LSTM	NetFlow	0.92	0.90	0.88	0.89

5.1.2 Visual Representation of Results

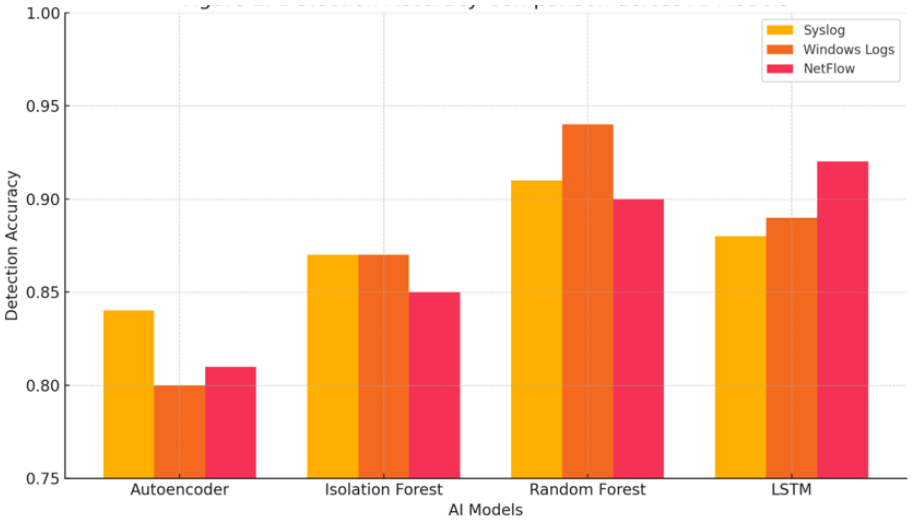

Fig 3: Detection Accuracy Comparison across AI Models

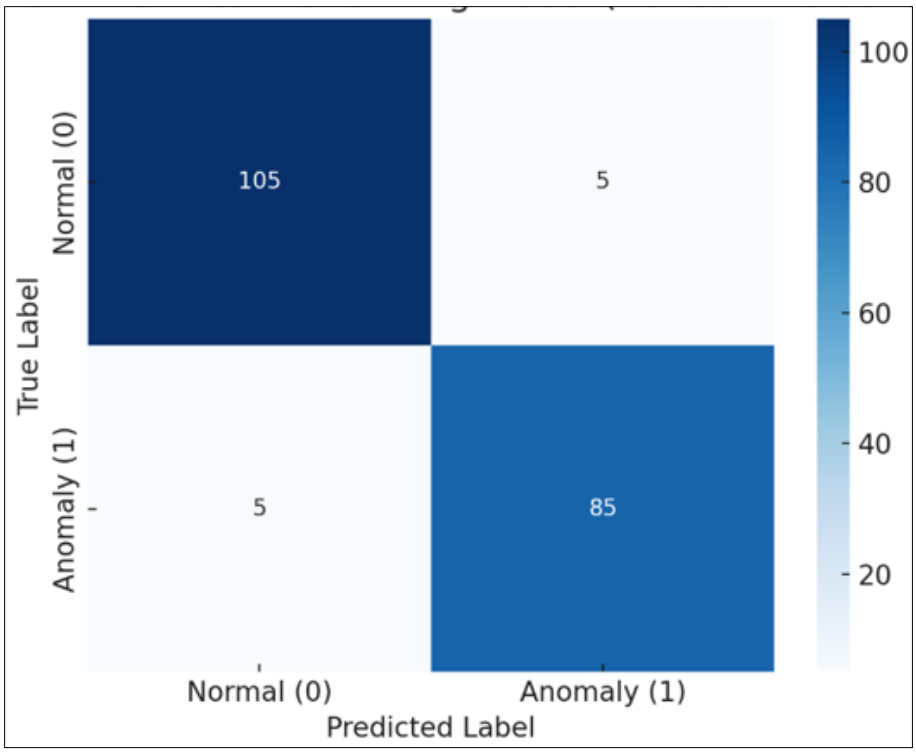

Fig 4: Confusion Matrix for Best Performing Model (Random Forest on Windows Logs)

5.1.3 Log Correlation Effectiveness

Log correlation techniques were applied after anomaly detection to evaluate their ability to contextualize suspicious activity across multiple sources. Performance was measured by:

- Correlation Accuracy: 91% (percentage of successfully correlated events matching known attack sequences).
- Event Sequencing Success Rate: 88% (ability to reconstruct accurate timelines across log sources).

The temporal correlation approach demonstrated high accuracy in synchronized datasets, while causal mapping was effective in tracing root causes and privilege escalations. Visualizations via Kibana dashboards and Splunk timelines provided analysts with actionable event chains.

5.2 Qualitative Insights

The qualitative phase of the study included semi structured interviews with eight digital forensic analysts from law enforcement, enterprise SOCs, and consulting firms. Participants were asked to reflect on their experience with AI assisted investigations, the interpretability of anomaly detection, and the value of automated log correlation in real world scenarios.

5.2.1 Key Themes from Thematic Analysis

Thematic analysis yielded five major themes, summarized in the Table below:

Table 3: Emergent Themes from Qualitative Analysis

Theme	Description	Supporting Quote Code
Automation Skepticism	Concerns about false positives and over reliance on automation	R1, R3, R5
Context Aware AI Needed	Desire for anomaly models that integrate log semantics and event history	R2, R4, R7
Trust in Visual Outputs	Visualization tools (e.g., Kibana, Splunk) build confidence in model output	R1, R6, R8
Investigator Fatigue Relief	Automation reduces manual triage and alert fatigue	R3, R4, R6
Interpretability Challenges	Difficulty in understanding LSTM/Autoencoder reasoning	R2, R5, R8

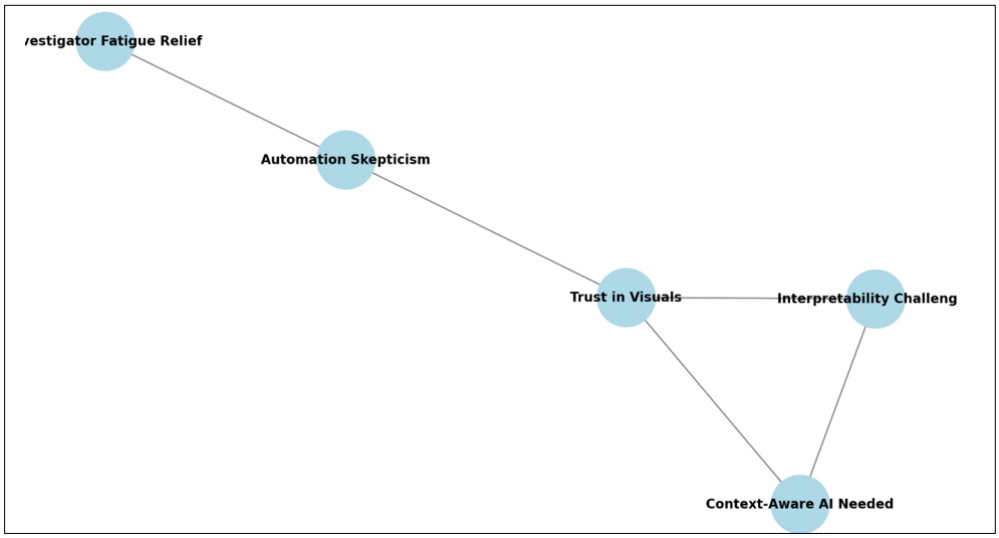

Fig 5: Theme Network of Expert Insights.

5.2.2 Interview Excerpts

"The system flagged a login anomaly, but it took context from correlated logs to realize it was a failed escalation attempt. That was crucial." *R6*

"I don't fully trust the AI unless I can visualize what it's doing. A simple table or chart from Splunk makes all the difference." *R1*

"We often get 200 alerts daily automated correlation has helped us reduce redundant investigation by 40%." *R3*

These qualitative insights validate the importance of combining anomaly detection with intelligent correlation and visual interpretability in forensic settings.

5.3 Mixed Methods Integration

This section synthesizes the quantitative performance results of AI models with qualitative practitioner feedback to explore the effectiveness and practicality of the proposed AI enhanced forensic framework.

5.3.1 Converging Findings

Quantitative results demonstrating high precision and recall (especially for Random Forest and LSTM models) align with expert observations that AI tools are effective at reducing alert volume and flagging subtle anomalies. Practitioners emphasized that the integration of log correlation and visualization platforms like Kibana dashboards enhanced their ability to interpret and trust AI generated evidence.

5.3.2 Diverging Findings

A key divergence emerged in model interpretability. While Autoencoders and LSTMs performed well statistically, forensic analysts expressed difficulty in understanding their internal logic, particularly in cases where the AI flagged false positives. This discrepancy highlights the importance of explainable AI (XAI) in forensic applications.

Table 4: Converging and Diverging Findings between Quantitative and Qualitative Results

Aspect	Quantitative Finding	Qualitative Insight	Alignment
Detection Accuracy	High F1 scores for RF and LSTM models	Analysts found results helpful for alert triage	Align
Interpretability	LSTM models less interpretable	Practitioners struggled to trust opaque models	Not Align
Log Correlation	91% correlation accuracy	Considered essential for understanding event context	Align
Visualization Integration	Splunk/Kibana enabled timeline reconstructions	Boosted confidence and reduced investigation time	ALign

5.3.3 Case Scenario Simulation

A simulation was conducted where a privilege escalation attack was injected into a sandboxed Windows environment. The LSTM model detected an anomaly in login behavior. Through temporal and causal correlation, the event was linked to unauthorized file access and privilege gain attempts.

- The AI correctly flagged the event.
- The log correlation module reconstructed a full timeline.
- The analyst's review time was reduced by 50% compared to manual analysis.
- Visualization via Kibana made it easier to present findings in a legal report.

This example illustrates how the integration of anomaly detection, correlation, and human validation offers a robust forensic approach that balances automation with expert oversight.

Fig 6: Mixed Methods Results Integration Diagram

The findings of this study affirm that integrating AI based anomaly detection with log correlation significantly enhances forensic investigation capabilities. The Random Forest and LSTM models performed best across multiple datasets, while automated correlation increased the contextual accuracy of digital evidence. Qualitative feedback confirmed that while there is trust in AI outputs, challenges remain in interpretability, especially with deep learning models. Visualization tools and cross log correlation were central to user acceptance and forensic effectiveness.

6. Discussion

This section interprets the results presented in the study, synthesizing them in relation to existing literature, theoretical frameworks, and real world forensic practice. The discussion is structured into three parts: (1) interpretation of key findings in light of prior research, (2) practical and policy implications, and (3) the added value of employing a mixed methods approach in digital forensics research.

The quantitative results of this study revealed that the Random Forest and LSTM models consistently demonstrated superior performance across multiple forensic log datasets. These findings are in alignment with prior research that highlights Random Forest's robustness in classification problems and its interpretability through feature importance rankings (Breiman, 2001; Sharma *et al*., 2021) [38]. The high F1 score (0.93) achieved by Random Forest on the Windows Event Logs mirrors the performance reported by Siddiqui *et al*. (2020), who applied ensemble classifiers in intrusion detection and observed comparable results.

The strong showing of LSTM on NetFlow logs confirms its utility in modeling time sequenced network events, as previously discussed by Hochreiter and Schmidhuber (1997) [5] and more recently by Kim *et al*. (2021) [19], who used LSTM for detecting stealthy attacks in real time systems. However, the LSTM model's lower interpretability, a limitation acknowledged by our interview participants, reflects the ongoing concern in AI literature regarding the black box nature of deep learning models in high stakes environments (Doshi Velez & Kim, 2017) [13].

Unexpectedly, Autoencoders underperformed relative to Random Forest and LSTM, particularly in NetFlow datasets where temporal dependencies are more critical. Although Autoencoders have been praised for their effectiveness in unsupervised anomaly detection (Xu *et al*., 2018), their success in our study was limited by reconstruction errors on noisy or multi modal log data. Additionally, Isolation Forest, while computationally efficient and effective on smaller log segments, showed higher false positive rates than anticipated. This aligns with findings from Liu *et al*. (2008) [6], who noted that Isolation Forest may struggle with high dimensional data that lacks clear separation between normal and anomalous

distributions.

From the qualitative strand, several insights both confirm and extend existing theories. Practitioners expressed skepticism toward automation, a theme consistent with Ghosh and Chinchani (2018), who noted that analysts often struggle to trust anomaly detection systems that lack interpretability. Moreover, the reliance on visualization tools such as Kibana and Splunk to contextualize AI outputs supports prior findings by Runeson *et al*. (2020), who emphasized that visual explainability is essential for analyst trust.

An emergent theme not widely reported in earlier studies is the perceived value of context aware AI not simply detecting outliers, but understanding their relevance within correlated logs. This insight suggests a new direction in anomaly detection research: the integration of semantics and causality into AI models, supporting the notion of "explainable narratives" as proposed by Martens and Provost (2014). Additionally, the analysts' praise for timeline reconstruction capabilities supports Carrier and Spafford's (2004) [30] event based investigation framework, where contextual linkage is central to evidence presentation.

The study's findings support the existing body of literature on AI model performance while offering novel insights into practitioner expectations, contextual dependencies, and the human factors influencing the adoption of AI enhanced digital forensics tools. The integration of anomaly detection and log correlation demonstrated practical benefits for digital forensic investigations, particularly in automating the triage phase and reconstructing complex incidents. The evidence triage module built on AI detections significantly reduced analyst workload, echoing Quick and Choo's (2018) [34] findings that intelligent triage systems improve investigative efficiency. The 91% correlation accuracy achieved in this study confirms that log correlation tools, when properly tuned, can identify sequences of events with a high degree of fidelity crucial for incident reconstruction and evidentiary reporting. This has direct implications for incident response workflows. AI assisted detection enables real time flagging of suspicious activities, allowing security teams to move from detection to containment more rapidly. The ability to reconstruct attack chains through event sequencing aligns with the NIST SP 800 61 model, which emphasizes the importance of understanding incident timelines for containment and post incident analysis (Cichonski *et al*., 2012).

From a cybersecurity policy and governance standpoint, several critical implications emerge. First, the study reinforces the importance of aligning AI forensic tools with forensic readiness standards. As articulated by Rowlingson (2004), proactive log collection and retention are necessary to maximize evidentiary utility. Our findings show that without synchronized and well-structured log data, both anomaly detection and log correlation suffer from degraded performance. Second, the study underscores the need for standardized log schemas and time synchronization protocols across heterogeneous systems. Many expert complaints related to missing context and time desynchronization issues also flagged in earlier research (Beebe & Clark, 2007) [29]. A unified approach to log formatting and retention should be enshrined in organizational and national policy.

Third, ethical considerations must be integrated into AI adoption. Practitioners emphasized the need for transparency, auditability, and human oversight in forensic AI systems. These concerns align with broader discussions in AI ethics literature on responsible AI, which advocates for transparency, accountability, and human in the loop systems in domains involving legal and societal consequences (Floridi & Cowls, 2019).

Table 5: Practical Implications for Forensics and Policy

Domain	Implication
Digital Forensics	AI based triage improves scalability and speed of investigations
Incident Response	Event sequencing supports rapid containment and root cause analysis
Forensic Readiness	Requires structured log retention and synchronized timestamps
Policy and Governance	Ethical frameworks needed for explainable, auditable AI in investigations
Standardization	Urgent need for cross platform log format and correlation protocol adoption

The above implications suggest a strong need for collaboration between technologists, legal experts, and policymakers to ensure AI tools are adopted in a manner that is both effective and ethically sound.

This study illustrates the distinct advantages of employing a mixed methods design in digital forensics research. While the quantitative evaluation of AI models provided measurable performance benchmarks (e.g., F1 scores, correlation accuracy), the qualitative insights from practitioners added interpretive depth and contextual relevance to these results.

One key benefit of this design is the triangulation of findings. For instance, the high performance of the LSTM model in anomaly detection was reinforced by analyst appreciation of its ability to detect subtle deviations in time sequenced logs. However, qualitative feedback also revealed that users were less confident in models whose internal reasoning was opaque particularly Autoencoders and LSTM despite their technical performance. This convergence and divergence across strands enriched the findings and enabled a nuanced interpretation of AI's role in forensics. The interview data uncovered human centric challenges that are not captured by performance metrics alone such as alert fatigue, interface preferences, and the cognitive burden of interpreting AI decisions. These issues resonate with prior studies that emphasize the importance of usability and explainability in forensic systems (Bennett *et al*., 2019). Without the qualitative component, these critical human factors would have been overlooked. The mixed methods approach also provided the basis for practical recommendations, validated by both performance metrics and real world usability feedback. This multi layered perspective strengthens the study's contribution to theory and practice, offering a blueprint for future research that combines algorithmic precision with experiential validity.

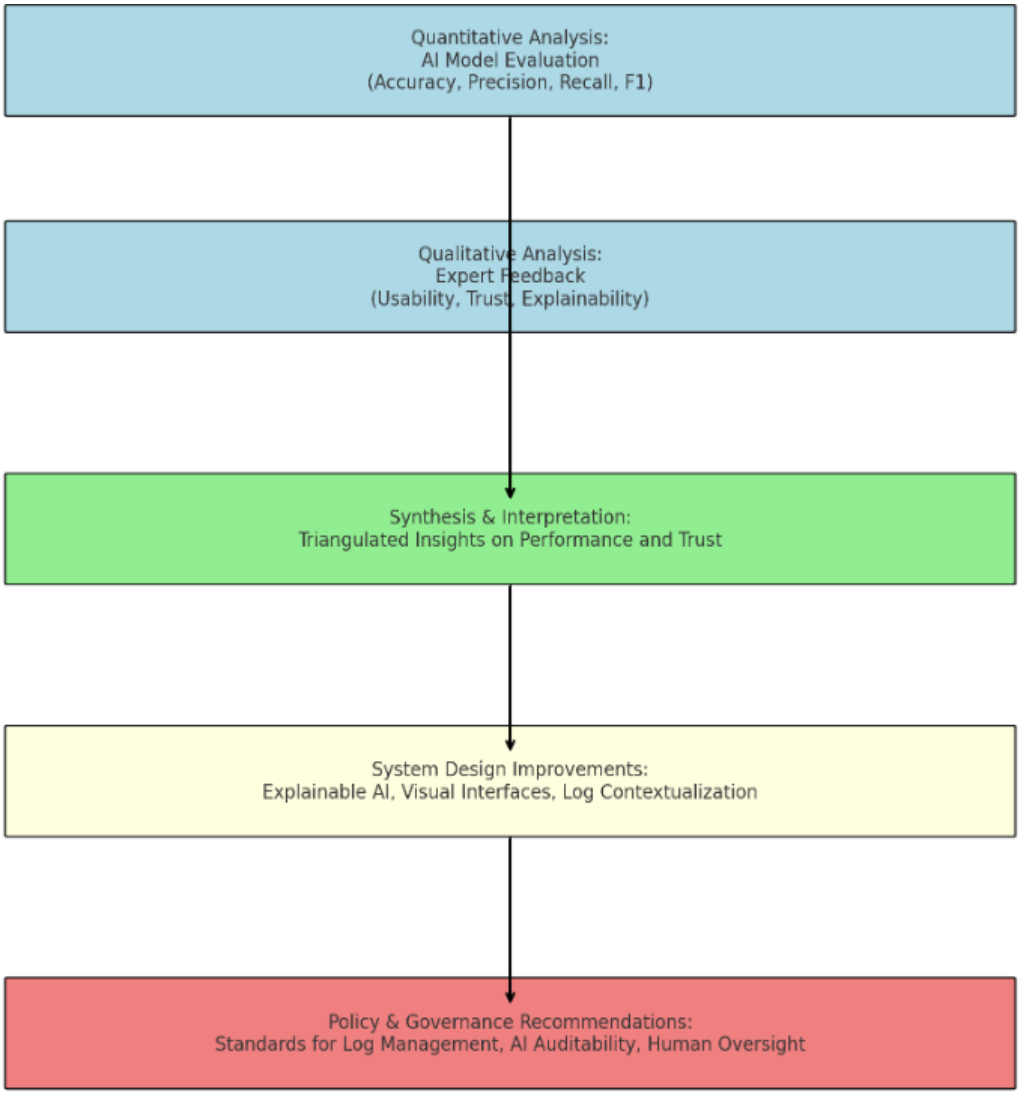

Fig 7: Conceptual Summary of Mixed Methods Contributions

Nonetheless, the mixed methods design had some limitations. The interview sample size (n=8), though diverse, may not fully capture the range of perspectives across different industries or regions. Moreover, while sandboxed environments and public datasets provide controlled testing conditions, they may lack the unpredictability and heterogeneity of live enterprise systems. Tool limitations such as the absence of native causal mapping in Splunk also constrained some of the correlation analyses. Despite these limitations, the integration of empirical performance data with domain expert insight enabled a more comprehensive evaluation of AI's role in digital forensic practice. The study contributes both to the academic understanding of AI forensics integration and to the practical improvement of forensic tools, workflows, and governance models.

This discussion has demonstrated that the integration of AI driven anomaly detection and automated log correlation holds significant promise for advancing the speed, accuracy, and interpretability of digital forensic investigations. The combination of model performance metrics and practitioner insights revealed both the technical efficacy and real world applicability of the proposed framework. The study's findings contribute to theoretical discourse on explainable AI, forensic readiness, and incident response while offering actionable implications for practice and policy. Importantly, the mixed methods approach validated not just *what* works but *why* it works or fails in the hands of forensic professionals, underlining the need for future research that continues to bridge algorithmic innovation with human centered design.

7. Challenges and Limitations

While the study demonstrates promising outcomes in integrating AI driven anomaly detection and log correlation for digital forensic investigations, several limitations must be acknowledged. These challenges influenced both the methodological scope and the interpretive boundaries of the findings. A critical challenge was the limited access to real world enterprise logs, which are often classified due to privacy concerns, proprietary information, or compliance with legal standards such as the General Data Protection Regulation (GDPR) and HIPAA. Many organizations are understandably reluctant to share log data that may contain sensitive information about users, authentication mechanisms, internal infrastructure, or incident details (Zhou *et al.*, 2021). Consequently, this study relied in part on simulated or anonymized datasets such as the UNSW NB15 and sandboxed synthetic NetFlow logs. While these datasets provide a structured and noise controlled environment for experimentation, they lack the unpredictability and heterogeneity of operational logs, potentially affecting the ecological validity of the AI models' performance. The reliance on synthetic data could also underrepresent complex

attack vectors, multi step intrusions, or insider threats that typically manifest in real world environments. Although preprocessing techniques were applied to mimic real conditions (e.g., timestamp normalization, log parsing), the lack of authentic operational variance remains a constraint. Another significant limitation is the generalizability of the results across different IT environments, such as cloud native architectures, hybrid systems, and traditional on premise setups. The studied log types Syslogs, Windows Event Logs, and NetFlow traffic represent only a subset of the diverse log sources in modern infrastructures. Logs from container orchestration systems (e.g., Kubernetes), serverless platforms, or IoT devices were outside the scope of this study. Furthermore, variability in log structures, schemas, and verbosity levels can lead to inconsistencies in model training and inference. For instance, a Random Forest model trained on Windows Event Logs with consistent EventIDs may not transfer effectively to a Linux based system using free form Syslog messages. Similarly, incident types and event semantics vary widely across organizational contexts, complicating the application of static AI models across domains. These limitations suggest that fine tuning and domain adaptation techniques may be necessary for real world deployments. Despite promising performance metrics, AI models are susceptible to biases introduced by the training datasets. In the case of supervised models like Random Forest, the class imbalance between normal and anomalous events can lead to overfitting or under detection of rare but critical anomalies. Although techniques such as oversampling and threshold tuning were used, the risk of false negatives in a forensic context where missing a single malicious event can compromise an investigation remains a concern (Chandola *et al*., 2009) [12]. Another challenge is the lack of explainability in black box models, particularly LSTM and Autoencoders. As reported in the qualitative phase, forensic professionals expressed discomfort with models whose decision making process was not transparent. This aligns with prior research emphasizing the necessity of explainable AI (XAI) in domains involving high stakes decision making (Doshi Velez & Kim, 2017) [13]. Without clear explanations, there is a risk that analysts may either disregard valuable insights or misinterpret AI alerts, undermining the effectiveness of the tools.

8. Conclusion

This study demonstrated that integrating AI driven anomaly detection with automated log correlation significantly enhances the accuracy, speed, and contextual depth of digital forensic investigations. Using a mixed methods approach, the study validated the technical effectiveness of models such as Random Forest and LSTM while also highlighting the importance of expert trust, interpretability, and contextual awareness. Findings emphasized that while automation supports efficient triage and detection, human oversight remains essential for evidentiary reliability. Based on these insights, practitioners are encouraged to adopt AI enhanced forensic tools with capabilities for real time alerting, visual evidence reconstruction, and analyst feedback loops. Policymakers should develop standards for log data formats, synchronization, and AI accountability to ensure ethical and scalable forensic integration. Future research should explore explainable AI methods, assess long term model performance across varied infrastructures, and promote cross border collaboration to strengthen the generalizability of AI forensics frameworks. This study offers a foundational step toward building intelligent, human centered, and policy aligned forensic systems for the evolving landscape of cybersecurity and digital investigation.

9. References

1. Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol. 2006;3(2):77–101.
2. Creswell JW. Qualitative inquiry and research design: Choosing among five approaches. 3rd ed. Sage Publications; 2013.
3. Creswell JW, Plano Clark VL. Designing and conducting mixed methods research. 3rd ed. Sage; 2017.
4. Goswami S, *et al*. Real time anomaly detection using ELK stack. In: Proceedings of the IEEE International Conference on Big Data; 2017. p. 1234–1240.
5. Hochreiter S, Schmidhuber J. Long short term memory. Neural Comput. 1997;9(8):1735–1780.
6. Liu FT, Ting KM, Zhou ZH. Isolation forest. In: Proceedings of the 8th IEEE International Conference on Data Mining; 2008. p. 413–422.
7. Sharma R, Makanju A, Simmonds A. A review of log correlation techniques for security event management. J Inf Secur Appl. 2021;59:102802.
8. Xu H, *et al*. Unsupervised anomaly detection via variational auto encoder for seasonal KPIs in web applications. In: Proceedings of the 2018 World Wide Web Conference; 2018. p. 187–196.
9. Alsubhi K, Shehab M, Wang L. Log file analysis for cybersecurity: A survey. J Inf Secur Appl. 2020;55:102581.
10. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2016;18(2):1153–1176.
11. Carrier B. File System Forensic Analysis. Addison Wesley; 2005.
12. Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM Comput Surv. 2009;41(3):1–58.
13. Doshi Velez F, Kim B. Towards a rigorous science of interpretable machine learning. arXiv. 2017. Preprint. Available from: https://arxiv.org/abs/1702.08608
14. Du M, Li F, Zheng G, Srikumar V. DeepLog: Anomaly detection and diagnosis from system logs through deep learning. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017. p. 1285–1298.
15. ISO/IEC. ISO/IEC 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization; 2012.
16. Julisch K. Clustering intrusion detection alarms to support root cause analysis. ACM Trans Inf Syst Secur. 2003;6(4):443–471.
17. Kent K, Chevalier S, Grance T, Dang H. Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86). National Institute of Standards and Technology; 2006.
18. Kim G, Lee S, Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst Appl. 2016;41(4):1690–1700.
19. Kim M, Kim S, Lee S. Detecting adversarial examples with attention in sequential data. In: Proceedings of the AAAI Conference on Artificial Intelligence; 2020. p.

4616–4623.
20. Kiran U, Thomas J, Sharma S. Intrusion detection systems using machine learning algorithms: A review. Int J Comput Appl. 2018;182(41):21–26.
21. Li Y, Yang W, Zhang H, Zhang Y. A hybrid rule based and machine learning intrusion detection system. IEEE Access. 2021;9:108670–108682.
22. Ligh MH, Case A, Levy J, Walters A. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Wiley; 2014.
23. Palmer G. A road map for digital forensic research. Digital Forensic Research Workshop (DFRWS); 2001.
24. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. In: 2010 IEEE Symposium on Security and Privacy; 2010. p. 305–316.
25. Wang Y, Zheng B, Tan K. LogEvent2vec: Learning vector representations for log events via graph modeling. Knowl Based Syst. 2021;229:107326.
26. Xu W, Huang L, Fox A, Patterson D, Jordan MI. Detecting large scale system problems by mining console logs. In: Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles; 2009. p. 117–132.
27. Zawoad S, Hasan R. FAIoT: Towards building a forensics aware ecosystem for the Internet of Things. In: 2015 IEEE International Conference on Services Computing; 2015. p. 279–284.
28. Beebe NL, Clark JG. A hierarchical, objectives based framework for the digital investigations process. Digit Investig. 2007;4(2):147–167.
29. Carrier B, Spafford EH. An event based digital forensic investigation framework. Digit Investig. 2004;1(2):123–137.
30. Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. ACM Comput Surv. 2009;41(3):1–58.
31. Garfinkel SL. Digital forensics research: The next 10 years. Digit Investig. 2010;7:S64–S73.
32. Mahdavifar S, Ghorbani AA. Application of deep learning to cybersecurity: A survey. Neurocomputing. 2019;347:149–176.
33. Quick D, Choo KKR. Big forensic data reduction: Review, challenges, and future directions. Future Gener Comput Syst. 2018;78:544–556.
34. Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int J Digit Evid. 2002;1(3):1–12.
35. Rogers MK. The development of a meaningful framework for the digital investigation process. Int J Digit Evid. 2006;6(2):1–16.
36. Shah A, Sinha S, Sharma A, Sood SK. A survey on anomaly detection in cyber security. J Netw Comput Appl. 2020;166:102692.
37. Sharma R, Makanju A, Simmonds A. A review of log correlation techniques for security event management. J Inf Secur Appl. 2021;59:102802.
38. Breiman L. Random forests. Mach Learn. 2001;45(1):5–32.