International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

ForenSift: Gen-AI powered Integrated Digital Forensics and Incident Response Platform Using LangChain Framework

Amruta Patil[1], Pushkar Deore [2], Pratik Patil[3], Akhilesh Talekar[4], Manisha Mali[5]

[1,2,3,4,5]Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India

Abstract

ForenSift brings innovation to the domain of Digital Forensics and Incident Response using Generative AI and the LangChain framework to combat the significant surge in the complexity and volume of digital evidence discovered in cybersecurity investigations. ForenSift deals with key issues in cybersecurity investigation work, specifically time constraints and the need for deep analysis of huge datasets. We have proposed an integrated solution that would automate key parts of the DFIR workflow that ranges from evidence collection, artifact management, anomaly detection, to report generation. ForenSift architecture is based on a strong, evidence-preserving workflow, integrating fully with existing forensic tools but introducing AI-driven analysis capabilities. We have focused on utilisation of Large Language Models (LLMs) together with multi-agent systems at the platform level to notably enhance efficacy and accuracy in DFIR procedures. Concluding, we elaborate on how ForenSift may revolutionize DFIR as it is scalable, combining AI-driven analysis with human expertise. They indicate future possible improvements to be applied in the hybrid system, such as adding a quantum computing machine and blockchain technology to further increase processing speed and maintain data security. This research contributes to the emerging field of AI-enabled cybersecurity by proposing a well-rounded framework that addresses the emerging needs of digital forensic investigations in an increasingly complex threat landscape.

Keywords Digital Forensics, Incident Reporting, Automation, Artifact Management, LangChain, LLM, Ollama, Digital Forensics Investigations

Introduction

The growing pace of cybercrimes, coupled with increasingly complex digital technologies, highlights the need for robust digital forensics and incident response (DFIR) services across the cybersecurity landscape. This perspective is useful in understanding that DFIR (as a practice) is critical for organizations to respond promptly to security breaches, manage and control cyberattacks, and maintain the integrity of digital infrastructure. Yet the threat landscape has changed greatly, and we now face more advanced persistent threats (APTs), sophisticated malware, insider attacks, and massive data breaches that result in huge volumes of digital evidence. Traditional DFIR methodologies — characterized by manual, time-

consuming data acquisition and image creation processes that expose them to human error — are ill-suited to the increasing scale and complexity of digital forensic data.

In the current rapidly evolving cyber threat landscape creative solutions are required to quickly process and analyse large quantities of digital evidence while retaining high levels of accuracy and timeliness. Enter ForenSift, which uses the rich capabilities of generative Artificial Intelligence (Gen AI) to entirely transform DFIR practices in response to these constraints. The platform is designed to automate and improve every part of the digital forensic investigation process including evidence acquisition, artifact organisation, anomaly detection and detailed incident reporting.

Using the LangChain framework empowers ForenSift to use modern LLMs trained on current datasets, and offers its innovative generative power towards leveraging an intelligent and adaptive digital evidence handling mechanism. The platform's capabilities that have developed overtime are intuitive, scalable and helpful for investigators who are used for the interrogation of vast datasets (structures), logging, or even finding new ways to detect anomalies in patterns are also more efficient than conventional methods. This level of automation can in turn contribute to cutting time spent on investigations as well and improve general forensic analysis accuracy by reducing the possibility of human error.

Related Work

Digital Forensics and Incident Response (DFIR) is an extensive and often lengthy process where security analysts might have to review security logs, evaluate the risk assessment of the alarms, and—in many cases—eliminate noise [1]. That is, it has become quite a dilemma to implement this particular method in today's constantly shifting threat landscape. Essentially, it is imperative to hasten these tasks as investigators cannot afford to wait for efficiency of clerkly forms in a world of fast-evolving cyber threats [1][2]. Computerization of otherwise repetitive activities like record collection, report writing, and artifact management is vital so as to enable the human intelligence and reasoning power of security analysts and investigators to carry out investigation, rather than doing errands. As presently understood, the methodologies of Generative Artificial Intelligence (GenAI) seem to be capable of having a prominent impact on different aspects of society, particularly in the field of Digital Forensics [3]. A common application of generative AI, particularly Large Language Models (LLMs), fits well in automating such procurements and especially where the input is in natural language or free text [1]. By incorporating the LLMs, it is possible to find potential deviations from the norms, improve the processing of incidents, and facilitate the dynamics of repeated security-related tasks [4], thereby significantly reducing the number of time-consuming processes for representatives of the cyber security industry [5]. This paper [6] examines the implications of large language models for cybersecurity tasks, while underlining the requirements of realistic evaluation for determining the true aspects of potential risks and capabilities of AI. Addition to LLMs, Retrieval Augmented Generation (RAG) techniques enhance their performance by incorporating supplementary data as well [7], making them even more valuable for automating the DFIR processes. Not only does this approach increase investigation efficiency but it has the potential for increasing traceability and mitigating technical and judicial challenges currently experienced by law enforcement entities [8], thereby allowing human intelligence to focus on other aspects of cybersecurity investigations.

Research shows that traditional IRPs and SOPs are deficient in handling novel and dynamic form of threats because of their rigid documentation-based approach [9]. It has been suggested that the application of LLMs by means of "SMART" models will increase speed and accuracy by minimizing the role of man-made intervention [9]. Comparisons of several LLMs like ChatGPT and Llama have shown differences

including varying levels of performance in tasks like case comprehension and report writing [10]. Real-world examples of AI integration in DFIR are best portrayed in frameworks which use advance LLMs such as Llama and StarCoder and specialised agents for NLP and task management [11]. The prospect of using AI is also mentioned in the areas of creating and enforcing policies so as to counter the lack of cyber police personnel [12]. The implementation of discrete time analysis together with AI-based analysis of cyber incidences represents additional approaches to investigating digital evidence in chronological way [13]. Assessment of multiple LLMs in different operating systems and architectures, have provided useful insights on the LLMs' efficiency in various aspects of DFIR [14] and the ethical considerations that accompany enhancements of LLMs with system-level task execution features have also been investigated [15]. Researchers have examined the ability of AI for both malware detection and creation, with token-based LLM operations presented as a challenge in various previous studies [16]. New opportunities such as CRUSH (Cybersecurity Research using Universal LLMs and Semantic Hypernetworks) has been suggested for design and optimization of Threat Intelligence Graphs (TIGs) [17]. Moreover, the need to identify line patterns or templates of unstructured textual event logs has been highlighted for good analysis of event logs and security monitoring [18]. Although LLMs hold much promise in application to tasks such as writing systematic reviews and network meta-analyses, there is a limitation with regard to ensuring consistency across multiple queries due to its continuous learning nature [19]. In cloud forensics, a framework for tools using the open-source tools like Python, Docker, and Azure is developed for overcoming challenges identified by NIST [25]. Digital evidence, patterns, and anomalies also need to be visualized. The knowledge graph and simple trees can be included in the proposed model, which is way beyond simple forensic cases [26].

As our proposed work targets at the implementation of automatic processes in DFIR, there are several advancements in related fields, which we used to adopt lessons on the applicability of AI in cybersecurity. RAGLog [20] introduces a state-of-the-art paradigm in log anomaly detection by integrating Retrieval Augmented Generation models with LLMs. Unlike all the methods of traditional log parsing, this technique depends on zero-shot classification to detect anomalies in raw logs that may enhance security system performance through unsupervised clustering and vector embeddings. The CyberMetric benchmark dataset [21] was used to great benefit in assessing the strengths and weaknesses of LLMs across various security domains. This presents how advanced models like GPT-4 can potentially be better than humans for certain tasks, at the same time indicating areas for improvement. BreachSeek [22] is one representation of the effectiveness of AI-driven platforms for pen testing. With LangChain-powered LLMs, it is possible to simulate and execute exploits with very minimal human interaction. Excellent results are achieved with the application of LLMs in constructing Enterprise Knowledge Graphs of Threat Intelligence Graphs [23], even reporting up to 99% recall in detecting malicious scripts. Specialized tools such as SecKnowledge and CyberPal.AI [24] truly show the efficiency of fine-tuning LLMs on domain-specific cybersecurity datasets, showing the efficiency of CyberPal.AI over baseline models by 24% in threat investigation tasks.

While those solutions had substantial progress in the application of LLMs to most areas in cybersecurity, including threat detection, anomaly analysis, penetration testing, and knowledge graph construction, our project is somewhat unique because we're focusing more on automation in the area of the DFIR process where comprehensive AI-driven solutions have still not been completed. Based on the related works and their successful implementation of LLMs in some particular cyber security operations, we are geared

towards making an innovative solution that integrates some of the required approaches as ways of bridging gaps within the current AI-based cybersecurity tools in providing unique needs for DFIR.

Proposed System

The core of the design of ForenSift lies within an overarching, rigid workflow regarding evidence preservation. This solution is centered on automating key tasks, cataloging and tracking artifacts, and safeguarding integrity of case-related evidence.

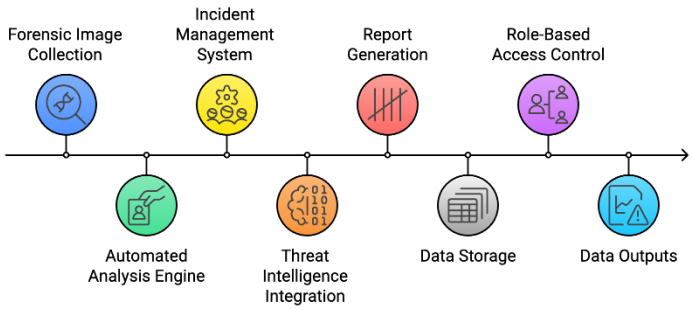

Fig. 1. Data Flow in DFIR tool.

In order to preserve the integrity of case files, the platform creates cryptographic hashes of all ingested artifacts automatically, logs all interactions with the evidence and also maintains detailed audit trails. From the creation of forensic images on the original equipment to management, this translates directly into being able to carry out investigations without corrupting or in any way compromising the integrity of your original evidence.

Forensift integrates with virtually all CLI-based forensic tools available on Kali Linux to further improve its analytical capabilities. ForenSift will then automatically run specialized forensic tools, data carving utilities, as well as analysis scripts by AI agents who will have aptly selected and applied the tools for the type of artifact and specific necessities of the investigation in question.

An easily customisable alerting mechanism, and a complex role-based notification system complements the analytical functionalities offered by the platform. Alerts can be configured with trigger definitions that will alert, for example, when certain types of artifacts are discovered, or when there is a recognized pattern of malware, thus ensuring the prompt attention to critical discoveries. It provides user-role-specific messages tailored to be aimed at the analyst, incident responder, or to management and, therefore, aids in giving transparent communication and assistance towards the smooth integration of team members.

Forensift comes with an advanced reporting module that uses natural language processing to produce human-understandable reports. The work automatically aggregates results of a variety of tools for analysis, summarizes the main discoveries, and represents their findings in a structured manner, tailored for specific audiences. As it were, reports can appear with technical details for the convenience of forensic analysts or in an executive summary for the management.

Among the most distinctive features of Forensift is its ability to automatically create in-depth timelines of events. In effect, the system constructs a chronological representation built from the timestamps of different artifacts and log files, which gives the investigators a deep understanding and prime insight into events, efficacy of cause and effect, and critical moments in the cycle of an incident.

Methodology

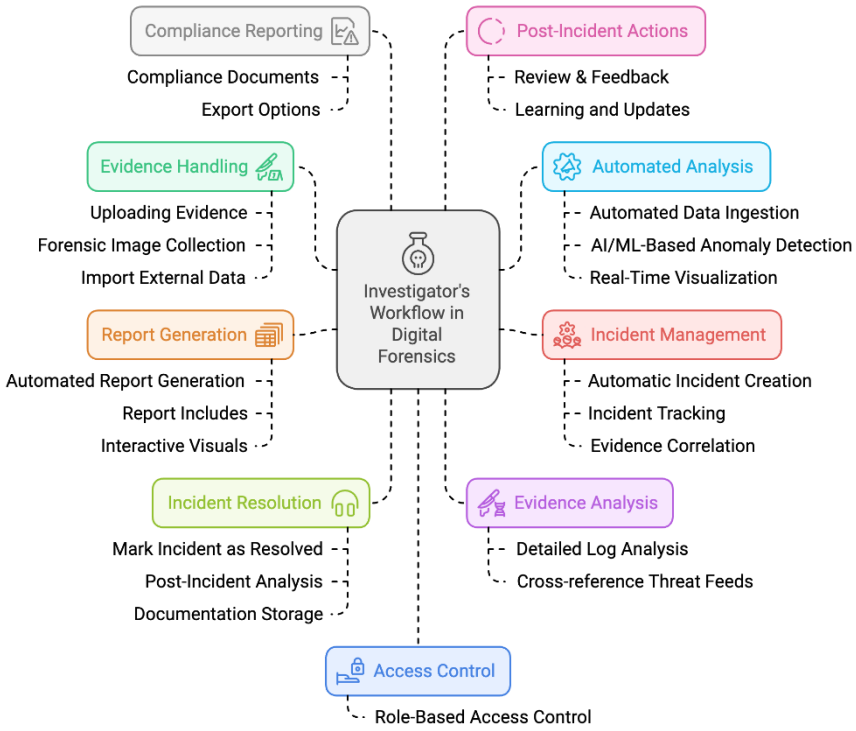

Fig. 2. Investigation Workflow in DFIR tool.

Architecture is founded on an interactive web interface and manifests as a central hub to be used in the management of forensic cases. This includes the management of artifacts, case summaries, and also automated workflow management.

The automated data collection: It automatically collects data from forensic formats holding RAW disk images. Thus, it would seamlessly integrate with the current disk imaging tools. When using disk imaging tools, one ensures that many pieces of evidence can be processed without much human involvement that minimizes the possibilities of errors when extracting the data.

Artifact Automation This system automatically identifies, catalogues and stores artifacts. It classifies different artifacts; it also includes integrity checking processes to ensure that there is data integrity during the whole process of an investigation. This same mechanism then utilizes the same process in safeguarding the chain of custody when dealing with digital evidence - it then frequently becomes a legal requirement for most forensic investigations.

Advanced Case Management: The project methodology highlights a workflow in preserving evidence that is especially designed to secure artefacts, do legal preservation, and facilitate easy retrieval. This aspect of the methodology is very crucial since it ensures the integrity and completeness of the data, which is very crucial for court proceedings or incident reports. In addition, the feature of generating timelines that is integrated into the tool is another automated entity that compiles timelines from evidence collected, hence enhancing event correlation and understanding of incidents.

AI/ML Integration: Artificial Intelligence and Machine Learning form the core of the system that detects Indicators of Compromise (IoCs). Algorithms of Artificial Intelligence have been used for the injection of pattern recognition, detection of anomalous behaviour, scoring of alarms, and differentiation of high priority against low priority events. This also brings a reduction in the overload to the cognition of

investigators, where investigators focus only on high-risk areas. The scoring system thus forms an intelligent filter, thereby sifting through massive databases to select the most relevant events.

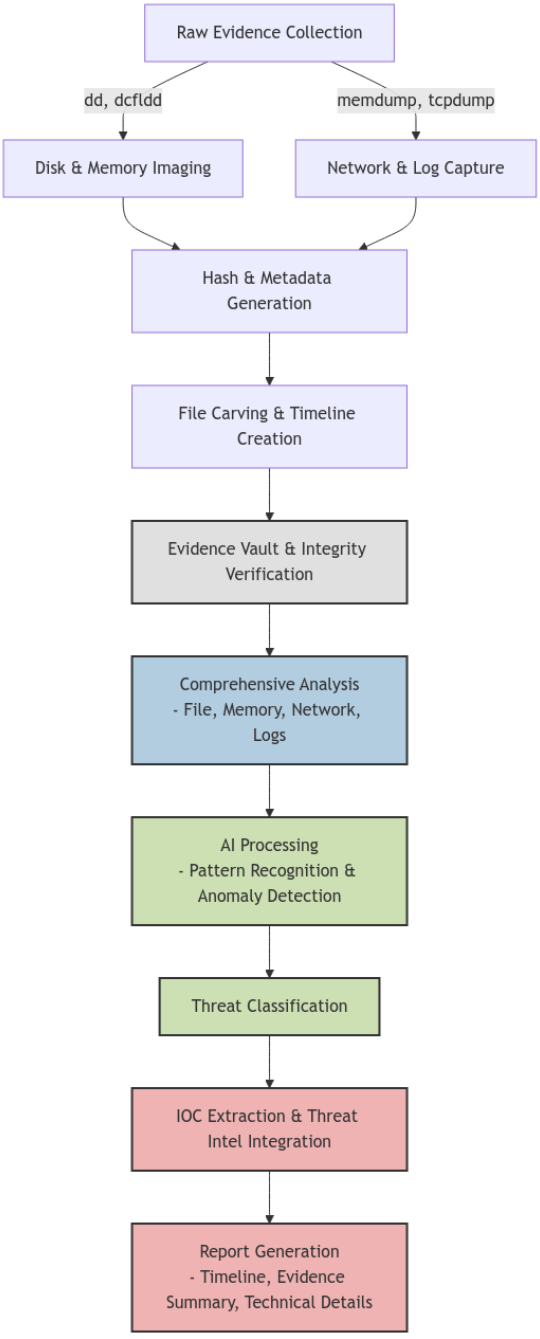

Fig. 3. Evidence Workflow in DFIR tool.

Visualization and Reporting: Reporting encompasses a huge percentage of the forensic investigations. The system adopted methodology is purely reporting-oriented, holding multiple views and graphical visualizations in terms of analysing case data. The views support the event analysis, which can be exported into different formats- PDF, JSON, and CSV. It enables the investigators to understand how incidents would come out much more speedily with graphical summaries and interactive timelines thus accelerating the whole process of deciding.

Security and Compliance: This design is all set with security in mind, including compliance such as the view of role-based notification, which will allow users to be updated on cases based on roles that will significantly reduce chances of unauthorized access; only the right people will handle sensitive operations. Integration of Kali Linux adds on extra security measures through the package of AI-based forensic tools that heighten the data recovery, analytical, and visual processes.

Scalability and Future Scope Scalability and Future Scope The long-term vision of this project would be integrating quantum computing along with blockchain technology. It is supposed to improve the speed combined with security in data processing. There are volumes of datasets that could be processed with real-time quantum computing. Blockchain would form immutable records of forensic data. It will expand the scope of the tool with the integration and processing of IoT forensics, cloud-native forensics, and Edge Computing for the management of the heterogeneous nature of connected devices along with real-time forensic requirements.

Emphasis on automated processes, AI-driven analysis, and secure evidence handling has established the project as an all-around answer to the modern digital forensic scenario in which manual methods are woefully inadequate in addressing complexity and scale of cyber incidents.

Conclusion

ForenSift is a paradigm shift in digital forensics and incident response, using the power of generative AI to address increasing dimensions in cybersecurity investigations, with large language models and multi-agent systems joined together with a number of specialised forensic tools by ForenSift significantly improving the efficiency and effectiveness of processes in DFIR. Our findings reveal that it accelerates the analysis of large volumes of digital evidence while also enhancing the accuracy in anomaly detection and completeness in incident reporting. These features provide exact answers to two of the current challenges facing modern cybersecurity practitioners-insufficient investigation due to pressure on time.

Preliminary results suggest that Gen AI-powered platforms like Forensift are likely to play a great deal in cybersecurity investigations in the years to come. As we continue to perfect and expand Forensift, we'll look toward a future where AI systems and human expertise blend in perfect harmony- one that will considerably enhance the effectiveness with which we can identify and investigate cyber threats.

References

1. “Automating the Cybersecurity Triage Process : A Comparative study on the performance of large language models - University of Twente Student Theses.” https://purl.utwente.nl/essays/100966
2. M. Ruzickova, I. Dzhalladova, O. Kaminsky, O. Bartash, and A. Pavlov, ‘AI and LLM Models to Analyze and Identify Cybersecurity Incidents’.
3. A. Nikolakopoulos et al., "Large Language Models in Modern Forensic Investigations: Harnessing the Power of Generative Artificial Intelligence in Crime Resolution and Suspect Identification," 2024 5th International Conference in Electronic Engineering, Information Technology & Education (EEITE), Chania, Greece, 2024, pp. 1-5, doi: 10.1109/EEITE61750.2024.10654427
4. M. Hassanin and N. Moustafa, “A Comprehensive overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions,” arXiv (Cornell University), May 2024, doi: 10.48550/arxiv.2405.14487.
5. S. R. Rahmani, ‘Integrating Large Language Models into Cybersecurity Incident Response: Enhancing Threat Detection and Analysis’, University of Applied Sciences Technikum Wien, 2024

6. "Considerations for evaluating large language models for cybersecurity tasks," SEI Digital Library, Feb. 20, 2024.https://insights.sei.cmu.edu/library/considerations-for-evaluating-large-language-models-for-cybersecurity-tasks/
7. N. Capodieci, C. Sanchez-Adames, J. Harris and U. Tatar, "The Impact of Generative AI and LLMs on the Cybersecurity Profession," 2024 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2024, pp. 448-453, doi: 10.1109/SIEDS61124.2024.10534674.
8. Wickramasekara, F. Breitinger, and M. Scanlon, "Exploring the potential of large language models for improving digital forensic investigation efficiency," arXiv (Cornell University), Feb. 2024, doi: 10.48550/arxiv.2402.19366
9. S. Hays and J. White, "Employing LLMs for incident response planning and review," arXiv.org, Mar. 02, 2024. https://arxiv.org/abs/2403.01271
10. G. Michelet and F. Breitinger, "ChatGPT, Llama, can you write my report? An experiment on assisted digital forensics reports written using (local) large language models," Forensic Science International Digital Investigation, vol. 48, p. 301683, Mar. 2024, doi: 10.1016/j.fsidi.2023.301683
11. "A framework for integrated digital forensic investigation employing AutoGen AI agents," IEEE Conference Publication | IEEE Xplore, Apr. 29, 2024. https://ieeexplore.ieee.org/abstract/document/10527235/
12. H. Dubravova, J. Cap, K. Holubova, and L. Hribnak, "Artificial intelligence as an innovative element of support in policing," Procedia Computer Science, vol. 237, pp. 237–244, Jan. 2024, doi: 10.1016/j.procs.2024.05.101
13. F. Y. Loumachi and M. C. Ghanem, "Advancing cyber incident timeline analysis through rule based AI and large language models," arXiv.org, Sep. 04, 2024. https://arxiv.org/abs/2409.02572
14. F. T. O. Technology and F. and C. Technology, "Evaluation of LLM agents for the SOC Tier 1 Analyst Triage process," UTUPub, Jun. 20, 2024. https://urn.fi/URN:NBN:fi-fe2024062457864
15. Giovanni Cimmino. Large Language Models in Cybersecurity: Digital Defense and Ethical Challenge. TechRxiv. August 20, 2024
16. J. Al-Karaki, M. A.-Z. Khan, and M. Omar, "Exploring LLMs for Malware Detection: review, framework design, and countermeasure approaches," arXiv.org, Sep. 11, 2024. https://arxiv.org/abs/2409.07587
17. M. Sewak, V. Emani, and A. Naresh, 'CRUSH: Cybersecurity Research using Universal LLMs and Semantic Hypernetworks', in EKG-LLM@ CIKM, 2023
18. R. Vaarandi and H. Bahsi, "Using Large Language Models for Template Detection from Security Event Logs," arXiv.org, Sep. 08, 2024. https://arxiv.org/abs/2409.05045
19. T. Reason, E. Benbow, J. Langham, A. Gimblett, S. L. Klijn, and B. Malcolm, "Artificial intelligence to Automate Network Meta-Analyses: Four case studies to evaluate the potential application of large language models," PharmacoEconomics - Open, Feb. 2024, doi: 10.1007/s41669-024-00476-9
20. "RAGLog: Log Anomaly Detection using Retrieval Augmented Generation," IEEE Conference Publication | IEEE Xplore, May 14, 2024. https://ieeexplore.ieee.org/abstract/document/10607047/
21. N. Tihanyi, M. A. Ferrag, R. Jain, T. Bisztray and M. Debbah, "CyberMetric: A Benchmark Dataset based on Retrieval-Augmented Generation for Evaluating LLMs in Cybersecurity Knowledge," 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom, 2024, pp. 296-302, doi: 10.1109/CSR61664.2024.10679494

22. Alshehri, A. Alshehri, A. Almalki, M. Bamardouf, and A. Akbar, "BreachSeek: a Multi-Agent automated penetration tester," arXiv.org, Aug. 31, 2024. https://arxiv.org/abs/2409.03789
23. "Evaluating the usability of LLMs in threat intelligence enrichment." https://arxiv.org/html/2409.15072v1
24. M. Levi, Y. Alluouche, D. Ohayon, and A. Puzanov, "CyberPal.AI: Empowering LLMs with Expert-Driven Cybersecurity Instructions," arXiv (Cornell University), Aug. 2024, doi: 10.48550/arxiv.2408.09304.
25. T. C. da Silva, 'Open-Source Framework for Digital Forensics Investigations', 2024.
26. Ogundiran, "A Goal-Oriented Visualization Approach to Digital Forensics Evidence Presentation - ProQuest." https://www.proquest.com/openview/d78875db38a8606bbf65f1adf680c8df/1?pq-origsite=gscholar&cbl=18750&diss=y