An LLM-driven Approach to Gain Cybercrime Insights with Evidence Networks

Honghe Zhou[1], *Weifeng Xu*[2], *Josh Dehlinger*[1], *Suranjan Chakraborty*[1], *Lin Deng*[1]
[1]*Towson University, Maryland, USA*
[2]*University of Baltimore, Maryland, USA*

Abstract

We have developed an automated approach for gaining criminal insights with digital evidence networks. This thrust will harness Large Language Models (LLMs) to learn patterns and relationships within forensic artifacts, automatically constructing Forensic Intelligence Graphs (FIGs). These FIGs will graphically represent evidence entities and their interrelations as extracted from mobile devices, while also providing an intelligence-driven approach to the analysis of forensic data. Our preliminary empirical study indicates that the LLM-reconstructed FIG can reveal all suspects' scenarios, achieving 91.67% coverage of evidence entities and 93.75% coverage of evidence relationships for a given Android device.

1 Introduction

Digital forensics is crucial in the fight against cybercrime, yet investigators grapple with substantial hurdles in sorting through the vast digital data on computing devices [1] [2] [3]. Currently, investigators heavily rely on manual processes to identify and analyze pertinent evidence from mobile devices. This approach is characterized by its ***labor-intensive nature and susceptibility to errors***, mainly due to the wide array of evidence types typically scatted all over modern devices.

This research aims at revolutionizing digital forensics by harnessing the capabilities of Large Language Models (LLMs) to automate digital evidence discovery by addressing two critical **Research Questions (RQs)**: RQ1) Can LLMs automatically identify various forms of evidence stored in different file types, such as system logs, system configurations, and databases, from mobile devices? RQ2) Can LLMs reconstruct suspects' behavior and reveal valuable insights?

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

2 Proposed LLM-driven Approach

The approach leverages LLMs to learn patterns and relationships within forensic artifacts, automatically constructing Forensic Intelligence Graphs (FIGs), which present digital forensic evidence with knowledge graphs [4]. We selected gpt-4-turbo as the supporting LLM for our approach. A FIG is defined as a graph $G = (V, E)$, where V is a set of nodes representing evidence entities, such as a person's name, address, and phone number. E is a set of edges, where each edge $e \in E$ represents a relationship between two evidence entities. Each edge e has a label that describes the relationship between the connected evidence entities. Examples of such relationships include: **"owns"**: indicating ownership, e.g., a person owns a phone number. **"lives-in"**: indicating residency, e.g., a person lives in an address. Thus, FIGs can effectively represent complex forensic scenarios by mapping entities and their interconnections through labeled edges.

Key activities are shown in Figure 1: **i) Convert raw data into plain text**: involves examining the evidence on mobile devices' Embedded MultiMediaCard (eMMC) [5,6]. eMMCs contain potential evidence entities, including deleted, hidden, and fragmented data, stored in binary format [7] [8] [9]. Raw data from eMMCs is extracted and converted into standardized text, enabling LLMs to identify evidence entities and their relationships. **ii) Discover evidence and its relationships**: involves creating and testing LLM prompts to extract evidence from text files line-by-line. This approach leverages the structured nature of records in mobile devices, such as system logs and chat histories. An example prompt for retrieving personal information from a test file is shown below:

> **LLM prompt for discovering evidence and its relationships:** Act as an experienced digital forensic investigator. Identify evidence entities, including personal information like names, addresses, and phone numbers, from the given text. Describe any relationships among entities.

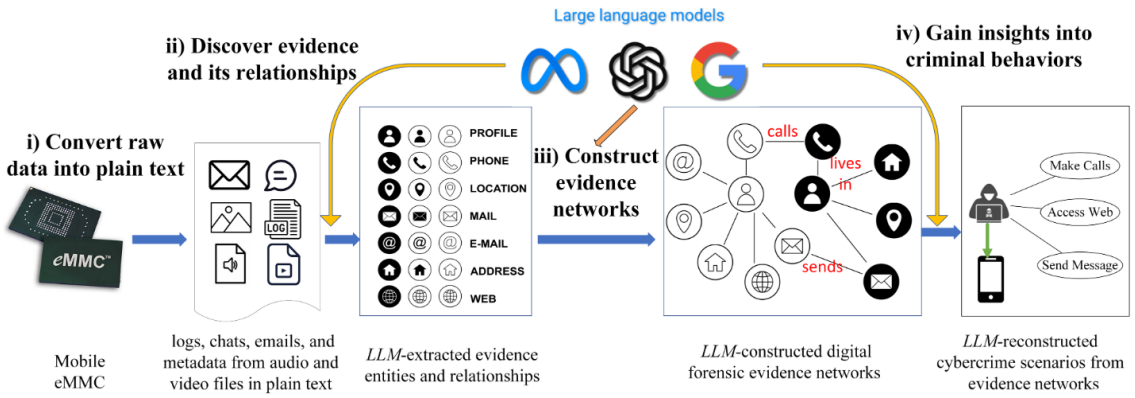

Figure 1: An LLM-driven approach for gaining cybercrime insights with evidence networks. Four key activities include: i) converting raw data into plain text, ii) discovering evidence and its relationships, iii) constructing evidence networks, and iv) gaining insights into criminal behaviors.

Desired output format:
Person's Name: `<person names>`
Address: `<mailing address>`
Phone number: `<phone number>`
Relationship: `<phone number>` ->(relationship description) `<mailing address>`
Text input: *`a line of text`* from a text file

iii) Construct evidence networks: involves the development and testing of prompts aimed at linking isolated evidence to construct evidence networks, representing a unique contribution to the field. We establish connections by measuring the closest distance between two evidence entities in the text, under the assumption that evidence closer to each other may have potential connections. This can be achieved through either line distance (i.e., physical distance) or inferential distance (i.e., semantic distance) learned by LLMs. **iv) Gain insights into criminal behaviors**: focuses on deriving critical understandings and conclusions regarding criminal activities, behaviors, patterns, and relationships from evidence networks. These insights are obtained through the analysis of interconnected evidence entities within such networks.

3 Preliminary Results and Conclusion

Fig. 2 shows an LLM-reconstructed FIG from an Android 10 mobile phone [10]. To facilitate our discussion, we reconstruct the FIG only using three folders containing three popular Android apps, including *Phone*, *Facebook Messenger*, and *Snapchat*. Each node in the figure represents an evidence entity, with different colors indicating various types of evidence: Personal names (blue), addresses (green), phone numbers (red), and emails (yellow). Each edge represents a relationship between these evidence entities.

Table 1 shows the number of reconstructed evidence entities and relationships using two different approaches. **Baseline** indicates the "truth" (i.e., the initial manual investigation

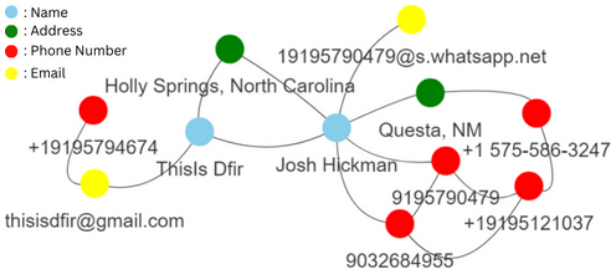

Figure 2: An LLM-reconstructed FIG from three popular Android Apps, including *Phone*, *Facebook Messenger*, and *Snapchat*

results) provided by the original creator of the Android disk image. **LLM-driven** is our automated approach. 'Match,' 'Added,' and 'Missed' indicate how the LLM-driven approach compares to the baseline in terms of matched, newly discovered, and overlooked entities and relationships. Our study indicates that the LLM-driven approach can discover new additional evidence entities (5) and relationships (11), while only missing one evidence entity and relation. We fixed the baseline by adding newly discovered entities and relationships. Thus, we calculate the evidence entity coverage as (6+5)/(6+5+1)=91.67% and relationship coverage as 93.75%.

Table 1: Comparison of Reconstructed FIG in Terms of Evidence Entities and Relationships.

	# of Reconstructed Evidence Entity		**# of Reconstructed Relationship**	
	Baseline	**LLM-driven**	**Baseline**	**LLM-driven**
Match	6	6	4	4
Added	0	5	0	11
Missed	1	0	1	0

Acknowledgments

This work is supported in part by BJA under 2019-DF-BX-K001 and by NSF under 2333949.

References

[1] Graeme Horsman and Nina Sunde. Unboxing the digital forensic investigation process. *Science & Justice*, 62(2):171–180, 2022.

[2] Jigar Patel. Forensic investigation life cycle (filc) using 6 'r'policy for digital evidence collection and legal prosecution. *Int. J. Emerg. Trends Technol.*, 2(1):129–132, 2013.

[3] André Årnes. *Digital forensics*. John Wiley & Sons, 2017.

[4] Weifeng Xu and Dianxiang Xu. Visualizing and reasoning about presentable digital forensic evidence with knowledge graphs. In *2022 19th Annual International Conference on Privacy, Security Trust (PST)*, pages 1–10, 2022.

[5] Sarfraz Shaikh, Lin Deng, and Weifeng Xu. A practical survey of data carving from non-functional android phones using chip-off technique. In *21st International Conference on Information Technology: New Generations*, Las Vegas, Nevada, USA, April 2024.

[6] Honghe Zhou, Lin Deng, Weifeng Xu, Wei Yu, Josh Dehlinger, and Suranjan Chakraborty. Towards internet of things (iot) forensics analysis on intelligent robot vacuum systems. In *The 20th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications (SERA 2022)*, Las Vegas, USA, May 2022. IEEE/ACIS.

[7] Jianwei Hou, Yuewei Li, Jingyang Yu, and Wenchang Shi. A survey on digital forensics in internet of things. *IEEE Internet of Things Journal*, 7(1):1–15, 2019.

[8] Albert M Villarreal, Robin Kumar Verma, Oren Upton, and Nicole Lang Beebe. Nondestructive data acquisition methodology for iot devices: A case study on amazon echo dot version 2. *IEEE Internet of Things Journal*, 10(5):4375–4387, 2022.

[9] Alan Roder, Kim-Kwang Raymon Choo, and Nhien-An Le-Khac. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv preprint arXiv:1804.08649*, 2018.

[10] Norwegian University of Science Svein Y. Willassen and Technology. Cell phones | digital corpora. https://digitalcorpora.org/corpora/cell-phones/. Accessed: May 21, 2024.