Transforming Digital Forensics with Large Language Models: Unlocking Automation, Insights, and Justice

Eric Xu
University of Maryland
College Park, Maryland, USA
exu17288@terpmail.umd.edu

Wenbin Zhang
Florida International University
Miami, Florida, USA
wenbin.zhang@fiu.edu

Weifeng Xu
University of Baltimore
Baltimore, Maryland, USA
wxu@ubalt.edu

ABSTRACT

In the pursuit of justice and accountability in the digital age, the integration of Large Language Models (LLMs) with digital forensics holds immense promise. This half-day tutorial provides a comprehensive exploration of the transformative potential of LLMs in automating digital investigations and uncovering hidden insights. Through a combination of real-world case studies, interactive exercises, and hands-on labs, participants will gain a deep understanding of how to harness LLMs for evidence analysis, entity identification, and knowledge graph reconstruction. By fostering a collaborative learning environment, this tutorial aims to empower professionals, researchers, and students with the skills and knowledge needed to drive innovation in digital forensics. As LLMs continue to revolutionize the field, this tutorial will have far-reaching implications for enhancing justice outcomes, promoting accountability, and shaping the future of digital investigations.

CCS CONCEPTS

• **Computing methodologies** → **Reasoning about belief and knowledge**.

KEYWORDS

Digital Forensics, Large Language Model, Automation, Evidence Analysis, Knowledge Graph Reconstruction

ACM Reference Format:

Eric Xu, Wenbin Zhang, and Weifeng Xu. 2024. Transforming Digital Forensics with Large Language Models: Unlocking Automation, Insights, and Justice. In *Proceedings of the 33rd ACM International Conference on Information and Knowledge Management (CIKM '24), October 21–25, 2024, Boise, ID, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3627673.3679091

1 TARGET AUDIENCE AND PREREQUISITES FOR THE HALF-DAY TUTORIAL

The intended audience for this tutorial is researchers, professionals, and students interested in the tutorial is intended for researchers, professionals, and students interested in the interdisciplinary field of digital forensics and Artificial Intelligence (AI). This includes digital forensic investigators and analysts, AI/ML researchers and practitioners interested in applying large language models (LLMs) to digital forensics, cybersecurity experts and incident responders, as well as law enforcement officials and legal professionals involved in digital evidence handling.

While no specific background is required, participants will benefit most from the tutorial if they have a basic understanding of AI and LLMs and their applications. This foundation will help attendees fully grasp the novel applications and challenges discussed in the tutorial.

This topic is particularly important and interesting to the CIKM community for several reasons. The increasing use of AI and LLMs in digital forensics significantly impacts the field, enhancing efficiency, accuracy, and scalability. The tutorial also explores innovative uses of LLMs in digital forensics, such as storytelling, summarizing, and profiling, areas that can benefit from the expertise of CIKM researchers and practitioners. Additionally, digital forensics intersects with AI, cybersecurity, and law enforcement, making it a natural fit for the CIKM community.

Participants can expect to gain a comprehensive understanding of the capabilities and limitations of LLMs in digital forensics. They will also receive practical insights into the application of LLMs in this field and be introduced to novel uses of LLMs. Moreover, attendees will have the opportunity to network with other professionals and researchers in digital forensics and AI, fostering valuable connections.

2 TUTORS

Eric Xu
Affiliation: University of Maryland, College Park
Email: exu17288@terpmail.umd.edu
Address: College Park, MD 20742
Phone: (+1) 667-240-6996

Wenbin Zhang
Affiliation: Florida International University
Email: wenbin.zhang@fiu.edu
Address: 11200 SW 8th St, Miami, FL 33199
Phone: (+1) 305 348-2000

Weifeng Xu
Affiliation: University of Baltimore
Email: wxu@ubalt.edu
Address: 1420 N. Charles Street, Baltimore, MD 21201
Phone: (+1) 410-837-5302

CIKM '24, October 21–25, 2024, Boise, ID, USA

ACM ISBN 979-8-4007-0436-9/24/10
https://doi.org/10.1145/3627673.3679091

3 TUTORS' BIO AND RELATED EXPERIENCE

Eric Xu is an undergraduate student majoring in Computer Science with a concentration in Machine Learning at the University of Maryland, College Park. He specializes in applied AI for digital forensics, focusing on generative AI for identifying and extracting forensic evidence from multi-medium sources. His research interests lie at the intersection of AI innovation and cybercrime investigation, aiming to bridge the gap between theoretical advancements and practical applications.

Dr. Wenbin Zhang is an Assistant Professor in the Knight Foundation School of Computing and Information Sciences at Florida International University and an Associate Member at the Te Ipu o te Mahara Artificial Intelligence Institute. His research investigates the theoretical foundations of machine learning with a focus on societal impact and welfare. In addition, he has worked in a number of application areas, highlighted by work on healthcare, digital forensics, geophysics, energy, transportation, forestry, and finance. He is a recipient of best paper awards/candidates at FAccT'23, ICDM'23, DAMI, and ICDM'21, as well as the NSF CRII Award and recognition in the AAAI'24 New Faculty Highlights. He also regularly serves in the organizing committees across computer science and interdisciplinary venues, most recently Travel Award Chair at AAAI'24, Volunteer Chair at WSDM'24 and Student Program Chair at AIES'23.

Dr. Weifeng Xu is a professor and director of the Cyber Forensics program in the School of Criminal Justice at the University of Baltimore, specializing in digital forensics and cybercrime investigations. Notably, the research and educational resources created by Dr. Xu and his team, available on GitHub [13], have garnered **significant recognition, accumulating over 1,400 stars from the digital forensics community**. Additionally, he brings real-world digital forensics experience gained as a visiting scholar for the Department of Defense (DoD), and Department of Homeland Security (DHS),

4 TUTORIAL OUTLINE

(1) Introduction
  1.1 Overview of digital forensics and its importance
  1.2 Challenges in digital forensic investigations
  1.3 The limitations of Artificial Intelligence (AI) in digital forensics
  1.4 Introduce large language models (LLMs) and their capabilities
  1.5 LLMs are revolutionizing digital forensics by enabling automation and providing new insights
(2) LLM-assisted Automation in Digital Forensics
  2.1 Text Analysis: sentiment analysis, entity extraction, topic modeling
    2.1.1 Email
    2.1.2 Chat log
    2.1.3 Social media monitoring
    2.1.4 Browser history
  2.2 Image Analysis: person and environment analysis
    2.2.1 Facial expression
    2.2.2 Body language
    2.2.3 Location identification
    2.2.4 Time estimation
    2.2.5 Activity identification
(3) LLM-assisted Insight Discovery
  3.1 Storytelling (i.e., from images and videos)
  3.2 Summarizing (i.e., from documents, audio, and videos)
  3.3 Profiling (i.e., from search keywords)
  3.4 Question answering (i.e., from reports)
  3.5 Evidence knowledge reconstruction
    3.5.1 Evidence entity relationship inference
    3.5.2 Reconstruct forensic Knowledge graphs
(4) Challenges and Limitations of Leveraging LLM in Digital Forensics
  4.1 Data quality and bias
  4.2 Evidence hallucination
  4.3 Explainability and transparency
  4.4 Non-standardization of LLMs and prompts
(5) Justice and Regulations for Generative AI in Digital Forensics and Society
  5.1 US Regulations regarding AI tools validation in digital forensics
  5.2 US Regulations concerns the admissibility of AI-generated investigation results
  5.3 Potential Regulations addressing the fairness of AI-related evidence
(6) Future Directions
  6.1 Standardization of prompts for digital forensics
  6.2 Multimodal analysis
  6.3 Retrieval Augmented Generation (RAG) for digital forensics
  6.4 Fine-turning LLMs with Low-Rank Adaptation (LoRA) for digital forensics
  6.5 Explainable digital forensics analysis
  6.6 Assessment of LLM-generated evidence
  6.7 Digital forensic reports generation and comprehension
  6.8 Human-AI Collaboration
(7) Conclusion

5 TUTORIAL ENVIRONMENT SET UP

Participants will delve into a serial of guided exercises and case studies designed to emulate real-world forensic investigations using LLMs. While there are no specific audio, video, or computer prerequisites for accessing the tutorial, it's imperative to guarantee that the hands-on tutorial environment is adequately configured and accessible to all participants. To accomplish this, we'll leverage a blend of pre-configured online AI platforms, LLM models, tools, and datasets to conduct forensic analysis on digital evidence. The key components of the lab environment for the tutorial include:

- An online AI platform: We utilize Google Colab [8], a cloud-based platform that enables users to write, execute, and share Python code directly through their web browser. Google Colab is particularly popular for machine learning, data analysis, and educational purposes.
- A free LLM: We employ Google's cutting-edge AI model, Gemini 1.5 [10], for the tutorial. This version enables users

to generate a free API key, facilitating programmatic access to the model via Google Colab.
- A flexible framework for all LLMs: We leverage the LangChain framework [1] to streamline the tutorial involving LLMs. This framework additionally enables participants to seamlessly integrate various LLMs through standardized interfaces.
- Open-source case study materials: All hands-on case studies, complete with code and datasets, will be made available on the author's esteemed GitHub repository at [13].

6 A CASE STUDY: PROFILING SUSPECTS THROUGH WEB HISTORY ANALYSIS

We've conducted a suspect profiling case study to showcase that each hands-on tutorial included in the course is meticulously crafted to exemplify the effects of LLMs within the realm of digital forensics. The dataset and code can be accessed here https://github.com/frankwxu/digital-forensics-lab/tree/main/AI4Forensics/CKIM2024/.

6.1 Motivation of the case study

Suspect profiling, also known as criminal profiling, is a technique used in criminal investigations for nearly a century to identify potential suspects based on various psychological, behavioral, and demographic characteristics [3, 4, 9]. Dr. Walter C. Langer, a psychiatrist, was commissioned by the Office of Strategic Services (OSS) to profile Adolf Hitler, marking one of the earliest known attempts at profiling in the 1940s [7].

The process involves analyzing the evidence from a crime scene, as well as the nature of the crime itself, to create a profile that can help law enforcement narrow down their search for the perpetrator. Today, suspect profiling is recognized as an important tool in forensic psychology and criminal investigations, continually refined through research and practical application [11, 12].

Cybercrime has significantly increased in recent years due to our growing reliance on digital technologies. The FBI's Internet Crime Complaint Center (IC3) reports an annual rise in cybercrime complaints, with financial losses reaching billions of dollars [5]. Understanding how advanced technologies, such as LLMs, can assist cybercrime investigators in profiling suspects using digital evidence is crucial. Such digital evidence includes browser history, emails, chats, and activity on social media platforms.

6.2 Dataset acquisition

In this tutorial, we will showcase the creation of a comprehensive suspect profile leveraging browser history, a digital footprint that offers valuable insights into an individual's thoughts, interests, and behaviors. To facilitate this demonstration, one of our authors has generously donated his own Google Chrome browser history dataset. This dataset was acquired using Google Takeout [6], a service provided by Google that enables users to export and download a copy of their data stored within various Google products. The acquired dataset includes 231 records of visited URLs spanning from 20:30 on March 12th to 11:57 on March 13th, 2024. Below is one URL visit record in JSON, which consists of how the web page is accessed, the title of the web page, the web page URL, and when the web page was accessed in Unix Epoch time. We only focus on profiling a person based on the title of the web pages he visited.

```
{
    "page_transition": "LINK",
    "title": "Browser History | Kaggle",
    "url": "https://www.kaggle.com/datasets/shawon10/
        browser-history",
    "time_usec": 1710345049975391
}
```

Listing 1: One example URL visit record in JSON

6.3 Profiling ground truth and scenario

To provide context for our demonstration, it's essential to understand the background of the individual who generated the browser history dataset. The creator is a cybersecurity researcher at a university, with a professional interest in exploring the potential of AI-driven analysis of digital forensics information, including browser history. In his personal life, he regularly engages in online activities such as watching YouTube videos, checking emails, and making personal payments, which are reflected in their browser history.

6.4 Prompt design

Our prompt comprises three core components showing in Table 1: role definition, data provision, and initiation instruction. The role definition specifies the role's name, overall objective, task specifics, and any applicable constraints. The provided data component outlines the required datasets for task completion. The initiation instruction serves as a trigger, prompting the role to carry out the task.

Table 1: Prompt Design Example: Profiling a Person Based on Web History

Prompt Element	**Profiling a Person Based on Web History**
Role name	Criminal profiler
Role objective	Create a psychological profile based on browsing history
Role task specifics	Motivations, psychological characteristics, behavioral patterns, relevant insights
Role restrictions	Avoid identification or accusations, no legal advice
Data provision	List of web pages visited with titles and timestamps
initiation instruction	Asking the role to perform the task with the provided data.

6.5 Profiling results

The LLM-driven analysis yields impressive results, with Gemini successfully capturing the creator's intent. The following profile results exemplify two types of forensic insights: Possible Motivations and Psychological Characteristics. Each category provides additional analysis details, with some analyses even incorporating supporting evidence. Notably, Gemini is able to infer personal interests in history, as evidenced by the creator's engagement with the "South China Sea Arbitration Case", demonstrating the model's ability to uncover nuanced aspects of the individual's personality.

```
Possible Motivations:
  Academic curiosity or research: Browsing websites and
      papers related to technology, career development,
      and academic topics suggests a keen interest in
      knowledge acquisition and professional advancement
      .
```

```
  Exploration of personal interests: The suspect may be
       exploring topics of personal interest, such as
       history (e.g., the South China Sea Arbitration
       Case) and entertainment (e.g., YouTube videos).
Psychological Characteristics:
  Inquisitive and learning-oriented: The suspect's
       browsing history shows a desire for knowledge and
       a willingness to engage with a variety of subjects
       .
  Skeptical and critical: The suspect seems to be
       discerning in their information consumption, as
       evidenced by the visit to a website on how to
       analyze browser history critically.
```

Listing 2: Example Profiling Results

7 PREVIOUS RELATED TUTORIALS

The intersection of LLMs and digital forensics remains an underrepresented topic in the CIKM community. To address this gap, our tutorial takes a comprehensive approach to leveraging LLMs in digital forensics, covering insight discovery, legal and technical challenges, and social implications.

Distinguishing itself from prior workshops, such as the DFRWS 2023 [2], which were limited to demonstrating search queries using prompts to uncover evidence from text, our tutorial offers a far-reaching and in-depth examination of insights derived from diverse real-world data sources, including text, images, and videos. Our systematic approach encompasses a broad range of forensic techniques to gain criminal insights, including storytelling, summarization, profiling, and evidence knowledge graph reconstruction, providing a comprehensive understanding of the applications of LLMs in digital forensics.

By introducing this novel topic to the CIKM community, our tutorial positions itself as a pioneering resource in the rapidly evolving AI technology landscape. It offers a holistic view of the challenges, solutions, and future directions at the intersection of digital forensics and AI technology, delving into both the technical aspects of empowering LLMs for digital investigation automation and insight discovery, as well as exploring the complex legal landscape surrounding these issues.

8 STRATEGIES FOR ENGAGEMENT AND INTERACTIVITY

To foster an immersive and interactive learning experience in our tutorial, we will employ several strategies to keep participants engaged and motivated throughout the session.

We will begin by presenting real-world digital forensic case studies that highlight the potential of Large Language Models (LLMs) in uncovering insights from text, images, and videos. These relatable examples will encourage participants to share their own experiences and insights, sparking meaningful discussions and debates within the group.

To further stimulate engagement, we will incorporate interactive exercises that challenge attendees to apply LLMs in digital forensic scenarios. For instance, participants will be tasked with analyzing a mock crime scene dataset, using LLMs to identify potential evidence entities, and reconstructing an evidence knowledge graph. This hands-on activity will allow participants to explore the capabilities of LLMs in digital forensics and share their findings with the group.

Additionally, we will provide a demo of cutting-edge tools and techniques for leveraging LLMs in digital investigation automation and insight discovery. Participants will have the opportunity to experiment with these tools firsthand, discuss their observations, and receive feedback from the instructors.

9 POTENTIAL SOCIETAL IMPACTS

Exploring the intersection of LLMs and digital forensics in this tutorial can drive meaningful societal change. By equipping professionals, researchers, and students with the knowledge and tools to utilize LLMs for digital investigation automation and insight discovery, we can enhance the efficiency and effectiveness of digital forensic investigations, leading to faster crime resolution and improved justice outcomes.

Furthermore, this tutorial can foster a culture of accountability and transparency in the digital realm, as LLMs can help uncover hidden patterns and relationships in large datasets. It can also support the development of more sophisticated AI-powered tools for law enforcement agencies, enabling them to stay ahead of cybercriminals and other malicious actors.

Ultimately, promoting a deeper understanding of LLMs' potential in digital forensics aims to contribute to a safer, more equitable, and just society. By empowering individuals and organizations with the knowledge and skills to effectively leverage these technologies, we can unlock new opportunities for innovation, collaboration, and progress.

ACKNOWLEDGMENTS

This project was partially funded by the Bureau of Justice Assistance (2019-DF-BX-K001) and the U.S. National Science Foundation (2039289 and 2333949).

REFERENCES

[1] Harrison Chase. 2024. LangChain. https://www.langchain.com/ Accessed: 2024-05-23.
[2] DFRWS. 2023. APAC 2023 Program. https://dfrws.org/apac-2023-program/ Accessed: 19 May 2024.
[3] John E Douglas and Alan E Burgess. 1986. Criminal profiling: A viable investigative tool against violent crime. *FBI L. Enforcement Bull.* 55 (1986), 9.
[4] John E Douglas and Mark Olshaker. 1998. *Mindhunter: Inside the FBI's elite serial crime unit.* Simon and Schuster.
[5] Federal Bureau of Investigation. 2021. 2020 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf Accessed: 2024-05-27.
[6] Google. 2011. Google Takeout. https://takeout.google.com/. Accessed: 2024-05-27.
[7] Walter Charles Langer, Henry Alexander Murray, Ernst Kris, and Bertram David Lewin. 1943. *A psychological analysis of Adolph Hitler: His life and legend.* MO Branch, Office of Strategic Services.
[8] Google Research. 2024. Google Colaboratory. https://colab.research.google.com/. Accessed: 2024-05-23.
[9] Robert K Ressler, Ann Wolbert Burgess, and John E Douglas. 1988. *Sexual homicide: Patterns and motives.* Simon and Schuster.
[10] Google AI Studio. 2024. API Key. https://aistudio.google.com/app/apikey Accessed: 2024-05-23.
[11] Brent E Turvey. 2011. *Criminal profiling: An introduction to behavioral evidence analysis.* Academic press.
[12] Brent E Turvey and Criminal Profiling. 2012. An introduction to behavioral evidence analysis. *Criminal Profiling: An Introduction to Behavioural Evidence Analysis* (2012).
[13] Weifeng Xu. 2023. frankwxu/digital-forensics-lab: Free hands-on digital forensics labs for students and faculty. https://github.com/frankwxu/digital-forensics-lab. (Accessed on 05/12/2023).