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

Eric Xu[1] Wenbin Zhan[2] Weifeng Xu[3]

[1]Department of Computer Science, University of Maryland, College Park
[2]Department of Computer Science, Florida International University
[3]Cyber Forensics, School of Criminal Justice, University of Baltimore

August 1, 2024

Outline

What Is Digital Forensics?

Digital forensics is the process of collecting, analyzing, and preserving electronic evidence for use in legal proceedings or investigations. It involves examining digital devices and data to uncover information related to cybercrimes, fraud, or other illegal activities.

Common Types Of Digital Evidence

- **Personal Identifiers**: Name, Address, Phone number, Email address, Social Security number, Date of birth
- **Network Information**: IP address, MAC address, Login credentials
- **Communication Records**: Emails, Text messages, Social media messages and posts
- **Financial Data**: Bank account information Credit card numbers, Transaction ID, Cryptocurrency wallet addresses
- **Location Data**: GPS latitude and longitude, Geotags on photos
- **Internet Activity**: Browsing URL, Search queries, Download URL

Common Types Of Relationships Between Digital Evidence

- **Communication Relationships**: [Phone number A, calls, Phone number B] [Email address A, sends email to, Email address B] [User A, messages, User B] on a social media platform
- **Ownership/Association**: [Person, owns, Device] [Email address, belongs to, Person] [IP address, associated with, Physical location]
- **Temporal Relationships**: [File A, created before, File B] [Event A, occurs simultaneously with, Event B] [User, logs in, Timestamp]
- **Spatial, Data Flow, Access, Modification, Financial Transactions, Social Connections, Content, ...**

Limitation Of Training-based AI For Digital Forensics?

- Data scarcity
  - obtaining sufficient training data involved in real-world cyber incidents
- AI models lack adaptability
  - An AI model often is designed for the specific evidence-extracting task
- Extract evidence relations is hard
  - Many different relationships exist

Why LLMs For Digital Forensics

LLMs are trained on vast amounts of text data with pattern and structure learning capabilities. LLMs have the great potential to automate digital forensics for reliable and efficient discovery and interpretation of digital evidence.

Outline

Evidence Analysis Leveraging LLMs

- Forensic evidence entity recognition
  - Evidence entity recognition
  - Visualize evidence and their relations
- Evidence knowledge graphs reconstruction
  - Construct a knowledge graph in STIX (zero-shot)
  - Construct a knowledge graph in STIX (one-shot)
  - Compare one-shot vs. zero-shot
- Profiling suspect based on browser history
- Political insights analysis based on Hillary's leaked Emails

You can access colab here

Outline

Challenges Inherited From LLMs

- **Hallucinations**: Risk of false leads or erroneous conclusions in investigations
- **Interpretability and Explainability**: Difficulty in explaining how LLMs arrive at certain conclusions
- Political insights analysis based on Hillary's leaked Emails
- **Lack of Domain-Specific Knowledge**: General-purpose LLMs may lack specialized forensic knowledge
- **Bias and Fairness**: Risk of unfair using of evidence

Challenges Of Applying LLMs In Justice

- **Chain of Custody Issues**: Challenges in maintaining and documenting the integrity of evidence when processed by LLMs
- **Non-deterministic**: LLMs can produce different responses to the same prompt, even under identical conditions
- Political insights analysis based on Hillary's leaked Emails
- **Lack of Standardization**: Absence of industry standards for using LLMs in forensic investigations
- **Training and Expertise Requirements**: Need for investigators to develop new skills in effectively using LLMs

Outline

Potential Societal Impacts

Exploring the intersection of LLMs and digital forensics can drive meaningful societal change

- Promoting a deeper understanding of LLMs' potential in digital forensics aims to contribute to a safer, more equitable, and just society.
- Important to foster a culture of accountability and transparency in the digital realm

Thanks

Thank You!