Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE AT GEORGE MASON UNIVERSITY

Adaptive Graph-based Framework for Multi-Source Digital Forensic Analysis

Lead PI: Yao Ma, Rensselaer Polytechnic Institute

Traditional and Digital Forensics

SUMMARY

This project seeks to improve digital forensics by advancing multi-source data analysis techniques. As digital footprints expand across various platforms and devices, investigators need more advanced tools to efficiently manage and analyze this growing amount of data. Current digital forensic tools and techniques, such as Autopsy, EnCase Forensic, Magnet AXIOM, and Cellebrite UFED, each offer unique capabilities to analyze and correlate data from different sources. While these tools represent the leading technology in their field, they face challenges including the need for significant manual input to detect correlation, difficulties in scaling and handling large data volumes, and limitations in performing real-time analysis. **Our project will address these issues and offer an integrated analysis solution across multiple data sources, enabling faster and more efficient resolution of cyber-related investigations.**

PROBLEM STATEMENT

Digital forensic practitioners struggle to keep up with the growing volume and complexity of data across multiple platforms and devices. Existing tools are limited by their reliance on manual input, scalability issues, and inability to perform real-time analysis, which hinder timely detection and investigation of cyber threats. As cyber incidents become more advanced, there is a critical need for integrated, scalable, and interpretable tools capable of efficiently correlating and analyzing data from multiple sources. This project will bridge this gap by developing a comprehensive solution that enhances the speed and accuracy of cyber investigations.

APPROACH

This project will employ a graph-based approach to analyze data from multiple sources. It builds correlation graphs to capture both explicit and implicit relationships across diverse datasets, enabling investigators to identify complex patterns and anomalies. Powered by machine learning, this framework enhances anomaly detection and provides interpretable results for forensic experts. By using this approach, the project addresses the increasing demand for integrated tools that support real-time, scalable, and accurate analysis, thereby strengthening cybersecurity efforts.

ANTICIPATED IMPACT FOR DHS

The project will enhance the speed, accuracy, and scalability of cyber investigations, enabling the Department of Homeland Security (DHS) to respond more effectively and efficiently to cyber incidents. By advancing multi-source digital forensic tools, the project directly supports DHS's mission to secure cyberspace and combat cyber threats. Specifically, the enhancement of multi-source analysis capabilities will boost the ability of federal, state, local, tribal, territorial agencies, and private sector partners to conduct swift and thorough cyber investigations. Ultimately, the contributions of this project will bolster national resilience against cyber threats.