Memory Forensics-Guided Execution Reconstruction for Android Devices

Summary
Cybercrimes are getting more advanced, especially on mobile devices, making it hard to trace digital evidence. This study aims to improve forensic methods by creating a tool that can recover and understand data from Android devices' memory. Access to this information will empower investigators, aiding in the precise location of evidence, vigilant monitoring of cyber threats, and swift detection of cyber-criminals.

Problem Statement
The project focuses on improving digital forensic investigations through the development of an execution reconstruction algorithm, leveraging in-memory artifacts, enhancing reconstructing methodologies for user activities on mobile devices, addressing limitations in current memory analysis techniques for cybercrime cases, and exploring the impact and generalization of the proposed algorithm across various applications and platforms.

Approach
The proposed approach introduces a new method called, Memory forensics-guided execution reconstruction. Our proposal outlines three main contributions: 1) Android in-memory program code extraction; 2) Symbolic execution engine development for Android Dex analysis; 3) Concolic execution algorithm development using in-memory object allocation graphs.

This approach, combining in-depth binary analysis with memory forensic capability, represents a significant advancement in digital forensics, offering the potential to reconstruct user activities with high-level accuracy.

Anticipated Impact for DHS
The proposed Symbex engine and execution algorithm aim to support DHS's capabilities to investigate illegal activities, particularly on encrypted platforms like Telegram, recovering deleted content and providing context for recent user actions. This initiative, aiding the DHS, enhances cyber threat preparedness and aligns with safeguarding cyberspace goals. By supporting DHS's operational needs, it strengthens the Homeland Security Enterprise (HSE) framework, benefiting law enforcement and intelligence communities. The memory-forensics execution reconstruction tool complements existing cybercrime investigation tools and offers stronger evidence admissible in court. The primary DHS components whose missions this research would serve to include: 1) Homeland Security Investigations (HSI) and the 2) Cybersecurity and Infrastructure Security Agency (CISA). CINA will socialize this project with DHS HSI and CISA by presenting the research and results to the HSI Department of Cyber and Operational Technology and the CISA Cybersecurity Division.