“Digital Forensic Evidence - The New Frontier”

Steve Williams
Investigator/Analyst Expert Consultant
International Narcotics & Law Enforcement (INL) – US Antiterrorism Assistance (ATA) - Broward County Sheriff’s Office – Fort Lauderdale Police Department
Mobile Forensics Process

• Using proper seizure and processing techniques are critical to what can and cannot be recovered from a mobile device and avoiding digital data contamination.

• The Seizure & Collection Process:
  • Identification/Handling
  • Collection/Preservation
  • Acquisition/Image
Identification/Handling

- **Identification:**
  - Safety first – visually check the smartphone for external connections and physical evidence.
  - Ensure properly documentation or photograph has been obtained prior to moving the smartphone.
  - Check battery life.
Collection/Preservation

• Preservation:
  • To avoid pressing buttons, handle the phone by the corners
  • Avoid unnecessary usage of the smartphone
    • Do not:
      ➢ Make or receive calls
      ➢ Check the call logs
      ➢ Check messaging
      ➢ Using 3rd-party Apps
      ➢ Attempt to unlock/lock
      ➢ Power the phone on or off
Collection/Preservation

- **Preservation:**
  - Check Bluetooth connections and history for external evidence:
    - Smart watch (places the phone to the suspect)
    - Connection with vehicle and/or GPS device
  - Place the phone in “airplane mode” to isolate the device from the network.
  - If the device is locked?
    - Use faraday packaging or heavy duty aluminum foil.
Acquisition/Extract

- Acquisition/Extract:
- Used validated forensics software to acquire/extract evidence:
  - Oxygen Forensic Detective
  - Cellebrite Mobile Forensics
  - MSAB XRY
  - MobilEdit
Acquisition/Extract

- Evidence from the mobile:
  - Evidence:
    - SMS
    - Call History
    - Phonebook
    - Email
    - Multimedia
    - Documents
    - GPS Data
  - 3rd party Communication apps (Skype, Whatsapp, Instagram, Snapchat)
  - Social Media Apps (Facebook, Google+, Twitter)
Evidence from the SIM Card:

- **ICCID** – Integrated Circuit Card ID, which is the *SIM card serial number* and can be traced to the purchaser of the SIM card.

- **LAI** – Local Area Identity, which is the last cell tower the SIM card connected to.
Acquisition/Extract

- Evidence from the microSD card:
  - Pictures (transferred to the phone) and Photos (taken by the phone)
  - Audio and video files
  - Documents
  - The mobile device database, which is transferred to the phone
  - Mobile device application databases
Acquisition/Extract

• Connecting the Suspects:
  • Once mobile evidence, 3rd-party communication apps and social networking applications extracted, suspects communications are analyzed and linked.
Questions