Unit 5
ANALYSIS AND VALIDATION

Chamundeswari Arumugam
Professor
SSN College of Engineering, Chennai

Sep 2017

Outline

- Validating Forensics Data
- Data Hiding Techniques
- Performing Remote Acquisition
- Network Forensics
- Email Investigations
- Cell Phone and Mobile Devices Forensics

Cell Phone and Mobile Devices Forensics

Understanding Mobile Device Forensics

- Item stored in a Phone
  - Incoming, outgoing, and missed calls
  - Text and Short Message Service (SMS) messages
  - E-mail, Instant messaging (IM) logs, Web pages
  - Pictures, Personal calendars, Address books, Music files, Voice recordings
- Cell phones used to - log in to bank accounts and transfer funds from one cell phone to another
- Investigating cell phones and mobile devices - one of the most challenging tasks in digital forensics
- Digital networks- CDMA, GSM, TDMA, iDEN, D-AMPS, EDGE, OFDM
- Mobile Phone Basics - 3G (technologies-CDMA, GSM, TDMA and EDGE), 4G (technologies- OFDM, Mobile WiMAX, UTMS, MIMO, LTE)
- Inside Mobile Devices - hardware components, OS, SIM Cards, Personal digital assistants (PDAs).
- SIM card purpose - Identifies the subscriber to the network, Stores personal information, Stores address books and messages, Stores service-related information

Cell Phone and Mobile Devices Forensics (Contd..)

Understanding Acquisition Procedures for Cell Phones and Mobile Devices - Introduction

- All mobile devices have volatile memory - dont lose power to retrieve RAM data.
- Mobile devices synchronize with applications on a users PC - disconnected from the PC
- Depending on the warrant - time of seizure is important.
- Isolate the device from incoming signals
- Retrieve the data in forensics lab - internal memory, SIM card, any removable or external memory cards, system server
- Need information from the service provider - to check voicemail, backups of address books, etc.
- Volatile memory requires power - contains data that changes frequently, such as missed calls, text messages, and sometimes even user files.
- Nonvolatile memory - contains OS files, personal information manager (PIM) and backed-up files.
- File system for a SIM card is a hierarchical structure - root of the system (MF), directory files (DF), elementary data (EF).
- Data from a SIM card - Service-related data, Call data, Message information, Location information
- PIN to access mobile

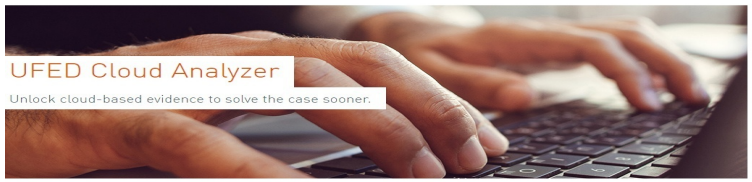
Cell Phone and Mobile Devices Forensics (Contd..)

Understanding Acquisition Procedures for Cell Phones and Mobile Devices - Mobile Forensics Equipment

- Identify the mobile device - install the software on forensics workstation.
- Attach the phone to its power supply - connect the correct cables
- Start the forensics program- begin downloading the available information
- SIM Card Readers - access the SIM card use forensics lab equipped with antistatic devices. Text and SMS messages can be accessed but pictures of each screen can be valuable.

Understanding Acquisition Procedures for Cell Phones and Mobile Devices - Mobile Forensics Equipment (Contd..)

- iPhone Forensics - device is practically impenetrable, access only files included in a standard backup, acquire a forensic image of the devices data, tools - MacLockPick II, MDBackUp Extract
- Mobile Forensics Tools - Paraben Software offers Device Seizure, Device Seizure Toolbox. DataPilot (interface cables), Bitpim (view the data), Cellebrite UFED Forensic System (PDA and cell phone), MOBILedit!(built-in writeblocker, forensic tool), SIMCon (read image files)



Evidence and Forensics in the Cloud: Challenges and Future Research Directions