ASU
Arizona State University

CSE 469: Computer and Network Forensics

Topic 7: Mobile Forensics

Dr. Mike Mabey | Spring 2019

Overview of Mobile Forensics

- Originated in Europe and focused on the GSM SIM card. Roaming of Devices from Network and Spectrum Required - I.D. Info on SIM – Also SMS, Phonebooks, and Last Numbers Dialled on SIM
- Terrorist use of phones as IED detonators Increased the demand for mobile forensics. Mobile device forensics is making a real impact in the war on terror.
- Adoption Has Moved Quickly From Federal to Local Level and Now Enterprise, Prisons, Schools, etc.

What is Mobile Forensics?

- A branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.
- Involves recovering data specific to mobile platforms.
- Can refer to any device with internal memory and communication ability, like PDA or GPS devices.
- There are multiple methods / tools for data extraction, and no single method is best.

Brief History (1)

- Mobile Forensics recognized as a branch of Computer Forensics in late 90's / early 2000's.
- Early Examination Methods:
  - Manually operating through the devices – Became more challenging with complex devices.
  - Using synchronization software – Unable to recover deleted data.

Brief History (2)

- More Modern Examination Methods:
  - Use of OEM flasher tools – Used by OEMs to program the device memory
    - Debugging, Overwriting non-volatile memory, copying the memory.
    - Potentially compromise data integrity.
  - Use of Automated Commercial / Specialized tools
    - Little risk of losing data integrity
    - Can recover deleted data
    - Eg. Lantern (Katana Forensics), MPE+ (Access Data)

Mobile Forensics Stats

- 80% of All Criminal Investigations in Europe Involve Mobile Device Forensics
- 90% of All Criminal Investigations in UK
- 70% in US (estimate and growing)
- Quickly Becoming The Necessary Part of Every Investigation!

Mobile Forensics vs Computer Forensics

- Computer Forensics:
  - Major Operating System Standards: Windows, Mac, Linux.
  - Standard practice is to image the Hard drive and Examine Data.
- Mobile Forensics:
  - Multiple Operating Systems.
  - Various Communication Standards.
  - Mobile Forensics is becoming more like computer forensics in some ways.
- Mobility Aspect:
  - Phones are Live Things Roaming Around.
  - It's not only just about what's on the device, but where has it been and what connections have been made?

What data is obtainable?

- FROM SIM Cards:
- IMSI: International Mobile Subscriber Identity
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- MSISDN: Mobile Station Integrated Services Digital Network (phone number)
- LND: Last Number Dialled (sometimes, not always, depends on the phone)
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)

What data is obtainable?

- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- ***Photos and Video (also stored on external flash)***
- Sound Files (also stored on external flash)
- Network Information, GPS location
- Phone Info (CDMA Serial Number)
- ***Emails***, memos, calendars, documents, etc. from PDAs.
- ***Facebook Contacts, Skype, YouTube data, Username and Passwords***
- Location from GPS, Cell Towers and Wi-Fi networks

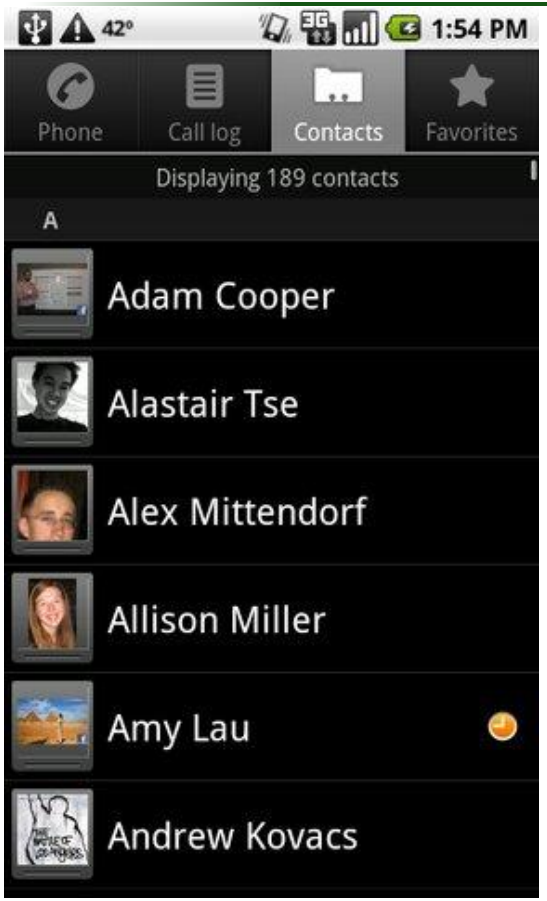
Mobile Forensics Process

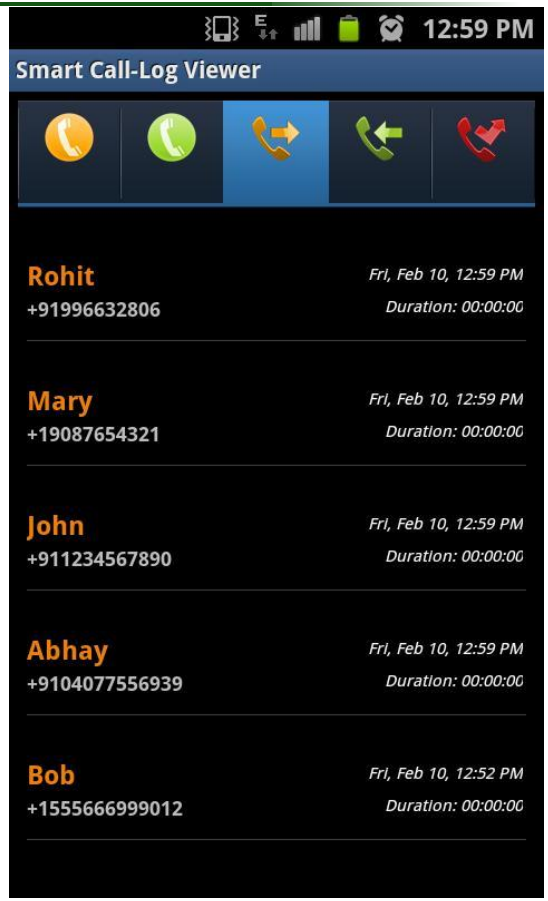
- Differences and Challenges
  - Lose – Lose – Lose situation:
    - Investigator does not alter device state after seizure to ensure data integrity.
      - Suspect uses remote wipe to erase evidence.
    - Investigator uses Faraday Bag to block communications
      - Battery is drained causing device to power down.
    - Investigator switches device to Airplane mode.
      - Memory is slightly changed.

Acquisition Techniques

- Manual Acquisition:
  - Manually interfacing with the device.
- File System Acquisition:
  - Can obtain some deleted data through synchronization.
- Physical Acquisition:
  - Bit-by-bit copy of the device's flash memory / disk.

Manual Acquisition

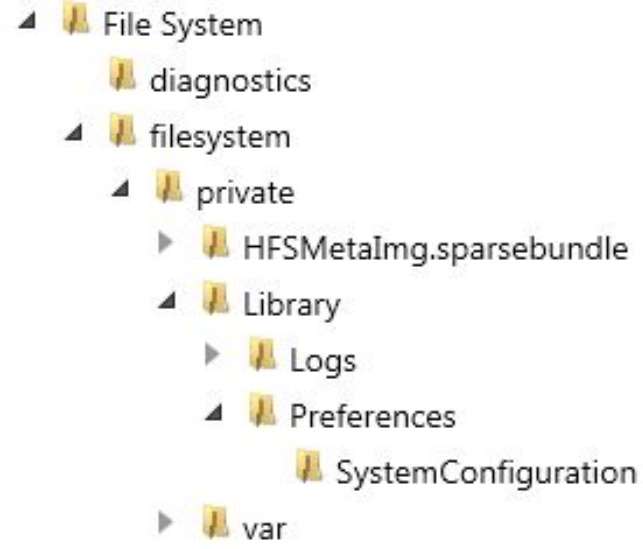




Manual Acquisition and Analysis

- Pros:
  - No prior setup / external tools required
  - Easily performed
- Cons:
  - Very slow at extracting large quantities of information.
  - Compromises data integrity
  - Can be halted if the device is locked.
  - Cannot recover hidden /deleted information.

File System Acquisition



Files In Selected Folder

Drag a column header and drop it here to group by that column

Original Name	Original Path
AddressBook.sqlitedb	/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb
AddressBook.sqlitedb-shm	/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb-shm
AddressBook.sqlitedb-wal	/private/var/mobile/Library/AddressBook/AddressBook.sqlitedb-wal
AddressBookImages.sqlitedb	/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb
AddressBookImages.sqlitedb-shm	/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb-sh
AddressBookImages.sqlitedb-wal	/private/var/mobile/Library/AddressBook/AddressBookImages.sqlitedb-wa

About iOS HFSX / HFS+

- HFS+ stands for Hierarchical File System (plus), and is used in modern iOS devices.
- For Logical Extractions, most information is extracted from sqlite database files.
  - Contacts: filesystem\private\var\mobile\Library\AddressBook\
  - Messages: filesystem\private\var\mobile\Library\SMS\
  - History: filesystem\private\var\mobile\Applications\...\safari\
  - Calendar: filesystem\private\var\mobile\Library\Calendar\
  - Accounts: filesystem\private\var\mobile\Library\Accounts\
- Epoch Time Conversion: www.epochconverter.com
  - Not completely correct format (but close).

File System Acquisition and Analysis

- Pros:
  - Quickly extracts large amounts of information for analysis.
  - Can recover some deleted information via database analysis – Some OS's mark data in databases as "deleted" w/o removing.
- Cons:
  - Use of this technique is limited as it requires the OS to keep track of deleted files.
  - Does not recover all deleted information.

Physical Acquisition