Smartphone Forensics

Omveer Singh
Scientist 'E' / Addl. Director
CERT-In, New Delhi

Smartphone

- A category of mobile phones (handsets) that provide advanced capabilities beyond a typical mobile phone
- Smartphones run on compete operating system
- Support APIs (Appl'n Prog'ing i/f) – allows 3rd party apps to integrate & run with the OS & hardware of smartphone

Smartphone

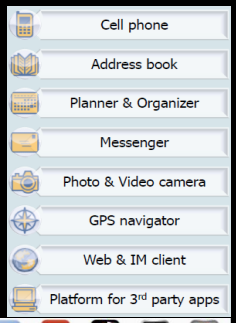
- Advanced capabilities beyond a typical mobile phone
- Runs on a completed operating system
- Components
  - ROM (firmware), CPU
  - RAM

Smartphone Components

- Flash memory for data storage
- CPU
- **SIM** (GSM) / RUIM (CDMA) Card
- MicroSD Card
- Cloud based accounts for data storage / backups
- Backups on Synced computer(s)

The Future of Smartphone Forensics

- Smartphone is a small PC
  - Android Devices
  - Blackberry (RIM)
  - Apple iOS (iPhone)
  - Windows Mobile
- Standard Phone Data + data from thousands of Apps / Apks



Smartphone

Combined functions of a:

- Feature phone
- PDA (Personal Digital Assistant)
- Portable media player
- Compact digital camera
  - Front, Rear
- GPS navigation
- Touch screens
- Web browsers
- Wi-Fi / Mobile Data
- Mobile Apps / Apks
- Mobile Commerce

Smartphones: Operating Systems

- Symbian (Nokia)
- Windows Mobile (Microsoft)
- iOS (Apple)
  - iPhone
- Android (Google)
  - Samsung
- Blackberry (RIM)
- Palm
- Linux

- Superphones
- Phablets

Smartphones: Information of interest for investigation

- e-Mail, IM
- SMS, MMS, BMS
- Camera & Multimedia Images
- Videos, Movies, Photos
- Audios, Music
- Web History
- Apps with Data
- eBooks, info'n in files
- Maps

Computer to sync Smartphone

- Smartphones are required to be connected to the Computers for:
  - Syncing the contacts, etc.
  - Back-ups / Restore
  - Download & installing New Apps
  - Updating of OS, Apps with latest versions

SQLite Databases

- Widely used in Smartphones for data storage and organisation
- Each database consists of one or more pages which are logical units that store data

SQLite Deletion

- When data is deleted from the database, pages containing that data are not in active use
- Unused pages are stored on freelist and are reused when additional pages are required
- Most forensic tools would not completely recover all deleted SQLite entries

Smartphone Forensics

- Application of forensic process to find information and answer questions
  - Application of scientific knowledge to answer the legal queries
    - How the smartphone was (or was not) involved in a particular incident or cyber crime
  - Widely tied to Locard's Exchange Principle –
    - "Every contact leaves a trace"

Mobile Phone Forensic Investigation Process

- Similar to digital forensics –
  - Identification
  - Seizure
  - Preservation
    - **Isolation**
  - Examination
  - Analysis
  - Report
- Additional process in 'ISOLATION'

Handling of Smartphones

- Unique challenges to investigators
  - So many different makes, models, and OS
  - Designed to connect wirelessly
  - No one-size-fits-all forensic solution
  - When powered ON – data is continuously changing
  - No write-blocking solution available
  - Traditional digital forensic concepts not applicable to flash memory

Smartphone Volatility

- When the smartphone is turned ON –
  - Generate traces, even if user does not operate or use the device
  - Device authenticates itself with the network
  - Device connects to network and stores last location (cell tower)
- To extract data from smartphone, it may be required to turn it ON a few times
  - Every time hash value will be different

Evidence Preservation

- Wiping of data by another wirelessly connected remote device is possible
- Block incoming & outgoing signals from the phone by –
  - Faraday Bags – high failure rate, unreliable
    - Difficult to operate touchscreen devices
  - RF Shielded Boxes / Containers
  - Signal Jammers
  - Airplane Mode

Seizing of Smartphone as Evidence

- Two Options:
  1. If examination of the phone is going to be delayed for significant time
     - Always turn the phone off upon seizing it as evidence and remove the battery
  2. If the phone can be examined soon in a timely manner
     - Leave the phone OFF, if it is already OFF; and leave it ON, if it is already ON; as well as, isolate it from RF signal from cell tower; no network connectivity
     - Maintain power to the battery – connect power adapter to phone

Legal Considerations

- Be sure you have proper 'legal authority' to perform the forensic examination
- Legal Authority will vary by jurisdiction – depend on the location / area of the incident
- In USA, aforesaid legal authority is limited to extract the data and analyse; and does not authorise examiners to use uid & pwd associated with the web based accounts

Data Acquisition from Smartphones

- Manual Acquisition
- Logical Acquisition
- File System Acquisition
- Physical Acquisition

Manual Acquisition

- Examiner physically scrolls through the mobile device to document contents
- Photographs or video of displayed data is captured
- Supported for all devices unless physically damaged
- Simple reporting, but time consuming

Logical Acquisition

- Includes active information from logically stored data
- Is supported for most devices by most tools
- Obtains contents of logical storage objects (call logs, contacts, SMS, pictures, video, calendar, etc.)
- Generally costs less
- Easy reporting

File System Acquisition

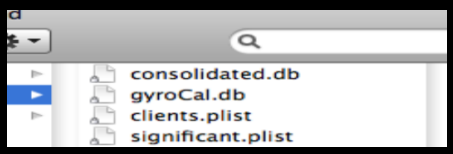
- Includes active files and folders
- May contain remnants of deleted items
- Is supported for most devices by most tools
- Obtains full file system and associated data (directories and files) from mobile devices
- Reporting may be more complex

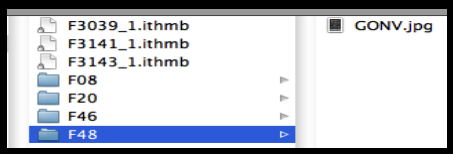
Physical Acquisition

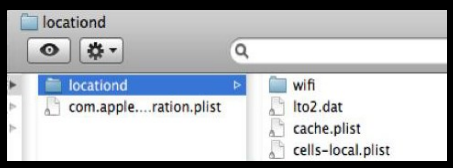
- Includes active and deleted data
- Absolute vs. Records
- Not supported for all devices
- Obtains all data from first to last bit on one or more chips in the mobile device
- Reporting is generally more complex

Analysis Tool: PC interface software

- Physical tools
  - iXAM, MPE+
- Logical Analysis tools
  - Paraben, XRY, Lantern 2.0
- Consolidated.db storing the tracking info
- Geodata in .plist format, include Wifi, cell id, neighbour cell id etc.
- Sync image and thumbs images indicate copy of the same images in the Desktop PC Mobile interface software
- PC interface software for iPhone - iTune's, Samsung - Kies etc also helps





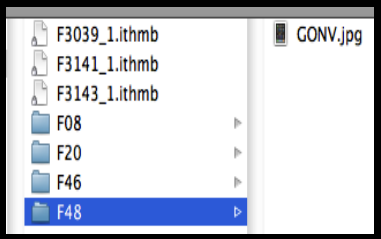


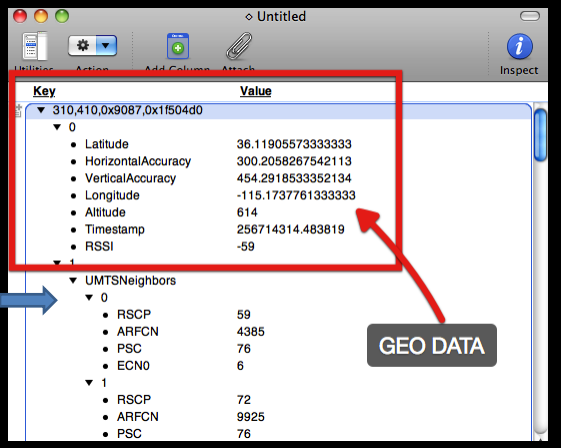
Smartphone Forensic Toolkits

- iPhone:
  - Lantern 2 (Katana)
    - Image, analyse, report
- Mobile Phone Examiner Plus (MPE+) (AccessData)
- Smartphone Examiner (EnCase)
- Device Seizer (Paraben)

Metadata available in Images

- Captured images store the latitude and longitude (GPS) information, time and date.
- Cell tracking info along with Network provider info confirms the presence of the suspect at the crime location.





Data Acquisition from Smartphones

- BlackBerry
  - BlackBerry Desktop Software
- iPhone
  - Full Backup by ‘iTunes’
- Samsung
  - Kies, Samsung Galaxy Desktop Manager
- Nokia Smartphones
  - Nokia PC Suite

iOS (Apple iPhone) Forensic

The Analysis of Apple Mobile Devices

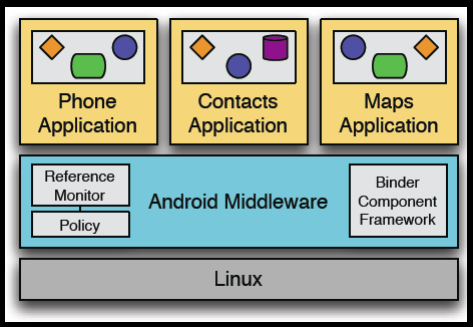
- Disconnect from cellular network
  - Put the mobile in ‘Airplane Mode’
- Remove SIM card
- Use GUI to
  - Turn off Wi-Fi and Bluetooth and
  - Disable ‘Screen Lock’
- use a Faraday Bag, if necessary

Physical Image of iPhone

- Most of the mobile forensic tools can not create physical image of iPhone without jail-breaking the Device
- While booting, exploits are run to jailbreak
- Jailbreaking is a privilege escalation and provides root access in iOS
- Necessary to install unauthorised applications

What is Android ?

- Smartphone open source Operating System, developed by Google.
- Based on the Linux 2.6 kernel
- Expanded to support cellular based communication GSM, CMDA
- Java like middleware
- File systems used
  - YAFFS2
  - ext4



Android Flavours

- **4.4 Kit Kat**
- **4.1 - 4.3 Jelly Bean**
- 4.0 Ice Cream Sandwich
- 3.0 Honeycomb
- **2.3 Gingerbread**
- 2.2 Froyo
- 2.0 - 2.1 Eclair
- 1.6 Donut
- 1.5 Cupcake
- 1.1 Petit Four

- To know the version of Android in your handset:

Main Menu > Settings > About Phone > Software Information

Android Memory Forensics

- Physical Memory Dump
  - DMD module developed by Joe Sylve
- Insert module into device (insmod dmd)
  - Creates /dev/dmd device
- Get start and end memory address(es)
  - grep –i “system ram” /proc/iomem
- Dump memory to removable media
  - echo “0x80c00000 0x9fdfffff sdcard/mem.dump”>/dev/dmd

USB Debugging

- Allows the handset to communicate with the forensic tool
- Accessed via a switch or through the Build Number
- Must be enabled to access the device by most of the tools
- Samsung Galaxy S4: Settings>>About phone>>tap ‘Build number’ 7 times ➔ ‘Developer mode has been enabled’

ADB (Android Debug Bridge)

- Part of Android SDK
- Commands can be run allowing the examiner to communicate with the handset
  - Pull commands
- Requires USB Debugging to be enabled
- Device must be rooted to pull the /data partition

Challenges in Smartphone Forensics

- Processor Optimisation
  - Power consumption
  - Digital Signal Processing
  - Peripherals Integration
  - Multimedia Acceleration
  - Code Density
- Battery Life
- Storage Memory
- Advance Imaging
- Cloud Computing
- 4G and beyond

Conclusion

- Phone forensics is a permanent race.
- No enforcement to Manufacturer by the govt.
- Certification before launch into market
- No study on exhaustive model basis for reference by the security agency.
- To get real results one must remain constantly aware of technical evolutions.
- Need developer community to join.

REFERENCES

- Course Documents: SANS Forensics 585 – Advanced Smartphone Forensics
- ‘Smartphone Forensic Investigation Process Model’; Int’l Journal of Computer Science & Security, Vol 6 Issue 5:2012
- ‘Android Forensics’ by Manish Chasta; Hackin9 Mobile Security Journal, Vol 2 No. 2, Issue 02/2012 (3)