Lecture 10- Smart Devices Forensics

Dr. Zunera Jalil
Email: zunera.jalil@mail.au.edu.pk

Understanding Mobile Devices

- The term "mobile devices" encompasses a wide array of gadgets ranging from **mobile phones, smart phones, tablets, MP3 Players, Smartwatches and GPS units to wearables, Drones, PDAs and many more**.
- Small-sized digital devices collect huge quantities of data on a daily basis, which can be extracted to facilitate the investigation.
- Successful examination of mobile devices requires special knowledge and skills of mobile forensics experts.
- Fast changes in the technology challenge experts in their daily business.

Understanding Mobile Devices

- Dealing with **diverse range devices** constitutes a challenge for the digital forensics examiner, as he needs to know the specialties of each device to successfully extract as much data from it as possible.
- When the examiner become familiar with a platform and how to extract and analyze it, manufacturers of operating systems make changes in their security concept and the vicious circle starts again.

Manufacturers:

- The **first step** in the investigational process is the identification of the phone.
  - Not easy…hundreds of device manufacturers.
- Mobile phones can sometimes be **identified by removing the device´s battery**, but that also indicates the risk of forcing a user lock or losing data of volatile memory

Understanding Mobile Devices

- Identifying a smartphone only by looking at it can be extremely hard even for mobile forensics experts.
- Mobile forensics toolkits offer the possibility to identify devices automatically when they are connected.

Connectors

- To connect a phone successfully, an expert must choose the **appropriate plug**. The next step is to find the **appropriate driver** to establish a connection to the computer.
- Common mobile forensics toolkits do the work automatically. If one computer has several mobile forensics toolkits installed, the examiner must be careful, as the driver packs from different vendors can interfere with each other.
- If the **USB connection** doesn't work, there's also the possibility of using wireless connection like **Bluetooth** to retrieve data from a mobile device.

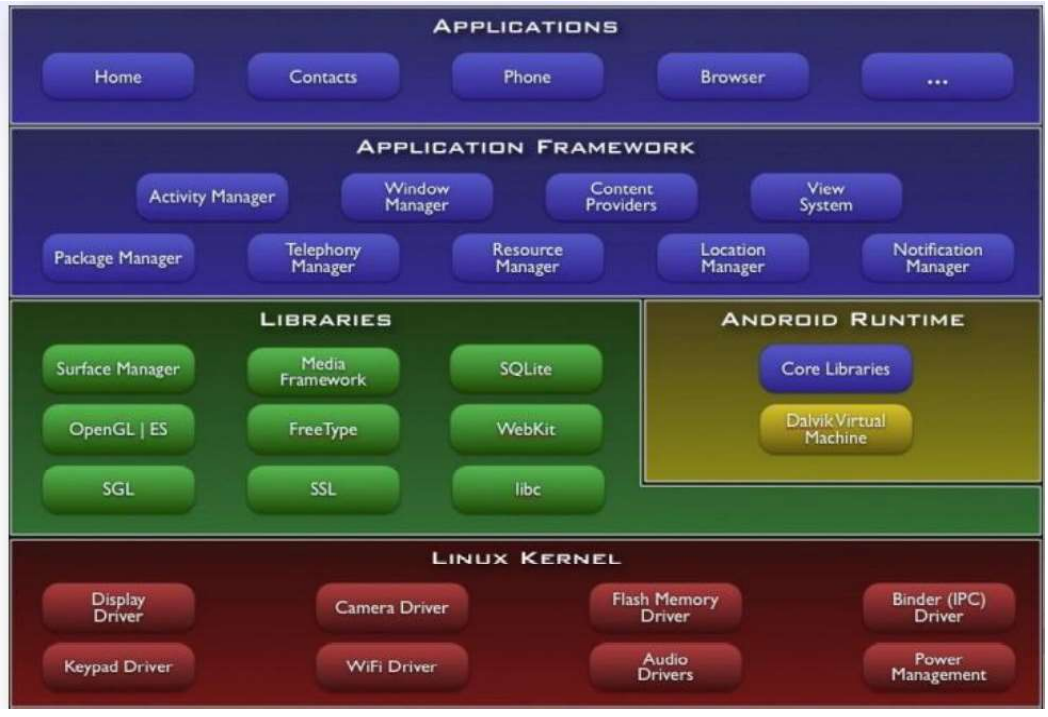
Understanding Mobile Devices

Operating Systems:

- Market shares of mobile OS manufacturers can change extremely fast. Every year new mobile devices are released, which can easily change the constellation of the OS market shares.
- Operating systems offer mostly the same functions but differ extremely in terms of data storage, security concepts and other characteristics.
- Android is used by different manufacturers, and it's often customized.
- Smartphone OS receive frequent major updates nearly every month.
- New security policies, new features, or changes in data storage of the OS constitute immense challenges for mobile forensics experts.

Date	Event
July 1, 2005	Google acquires Android, Inc.
November 12, 2007	Android launched
September 23, 2008	Android 1.0 platform released
February 13, 2009	Android Market: USA takes paid apps
April 15, 2009	Android 1.5 (Cupcake) platform released
September 16, 2009	Android 1.6 (Donut) platform released
October 5, 2009	Android 2.0/2.1 (Eclair) platform released
May 20, 2010	Android 2.2 (Froyo) platform released
December 6, 2010	Android 2.3 (Gingerbread) platform released
February 2, 2011	Android 3.0 (Honeycomb) preview released
November 14, 2011	Android 4.0 (Ice Cream Sandwich), 3.0 source released
July 9, 2012	Android 4.1 (Jelly Bean) platform released

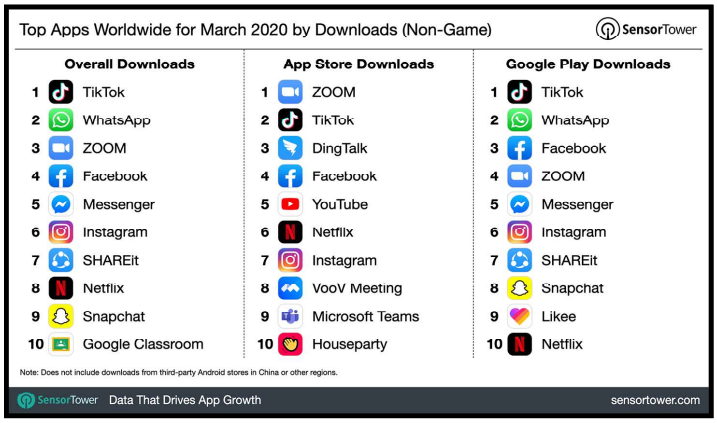
Android OS



Understanding Mobile Device

Applications

- Apps often store most information in SQLite databases, so those databases will contain a major part of the case data. Mobile forensics toolkits decode databases automatically and display them in a structured way
- Depending on the toolkit, only **a few hundred different apps** are supported, which is a comparatively small number, as there were about **4 million apps available**



Understanding Mobile Device

Cloud Data

- An increasing amount of data containing information very valuable to forensic investigations, is never saved on mobile devices in the first place but in cloud storage instead – be it by the devices OS or third- party apps data.
- Cloud backups also offer the chance to recover data deleted by the user or the data of locked, broken or wiped devices.
- However, acquiring this data is not only difficult because of legal constraints, depending on the country the investigation takes place in, but also because of security mechanisms like separate passwords and 2-factor authentication methods.
- Specialized software is required to acquire cloud data in a forensically way

Mobile Device Forensics

- People store a **wealth of Information on Cell Phones** but hardly think about securing their phones
- A search warrant might be needed to examine mobile devices
  - Lots of private information

- **Items stored on cell phones**

- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS) messages and Short Message Service (SMS) messages
- E-mail accounts
- Instant-messaging (IM) logs

- Web pages
- Pictures, video, and music files
- Calendars and address books
- Social media account information
- GPS data (Nav maps)
- Voice recordings and voicemail

Why Mobile Device Forensic is Challenging? 1/3

- **Hardware differences** - The market is flooded with different models of mobile phones from different manufacturers
  - Different models, sizes, OS & features
- **A range of different types of OS**
  - Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's webOS, Nokia's Symbian OS
- **Security features**
  - Modern mobiles contains built-in features for security and privacy

Why Mobile Device Forensic is Challenging? 2/3

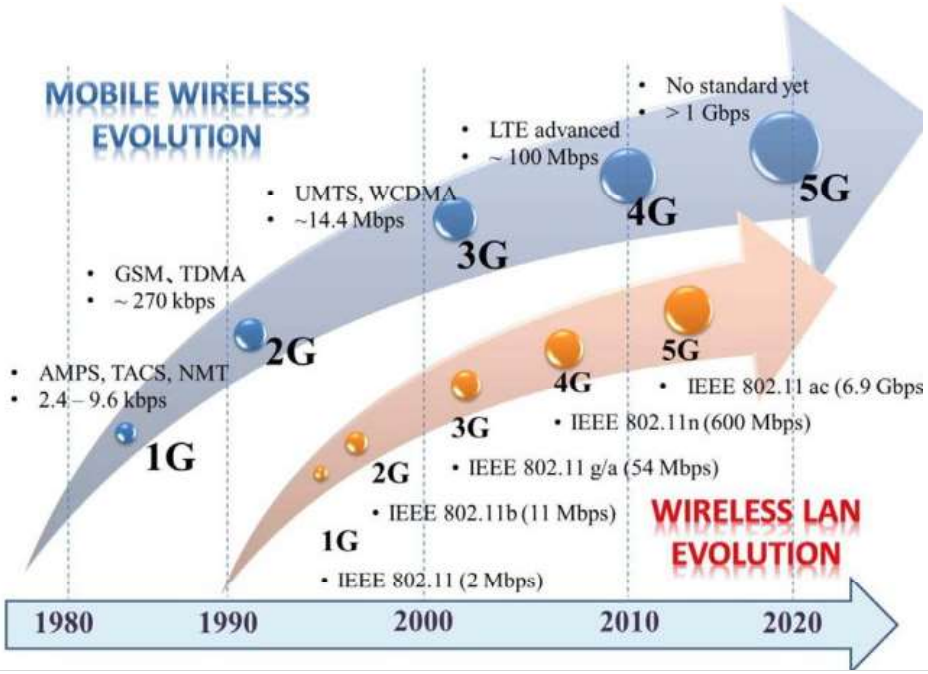
- **Lack of Resources**
  - Market diversity is leading to a bigger set of accessories that need to be maintained by forensic examiners
  - Cables, batteries, chargers etc.
- **Generic state of the device**
  - Even if a device appears to be in an off state, background processes may still run
- **Anti-forensic techniques**
  - Data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult

Why Mobile Device Forensic is Challenging? 3/3

- **Dynamic nature of evidence**
  - Digital evidence may be easily altered either intentionally or unintentionally
- **Reset Functionality**
  - can be reset to factory status
- **Legal issues**
  - Mobile devices might be involved in crimes, which can cross geographical boundaries

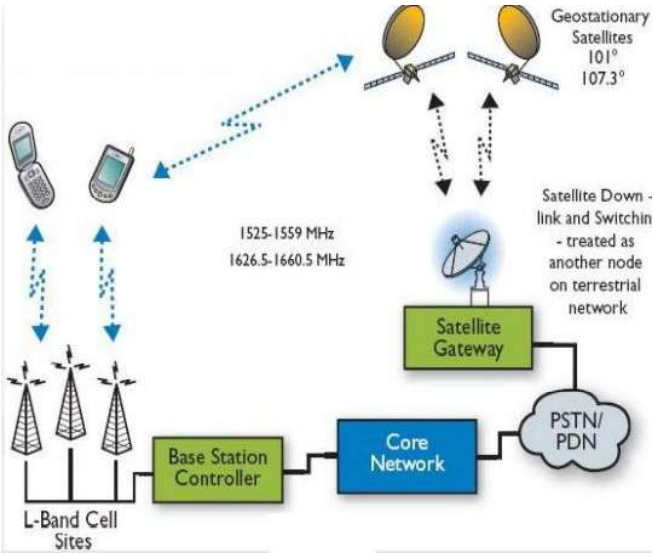
Cellular Communication System

Cellular technology has advanced rapidly

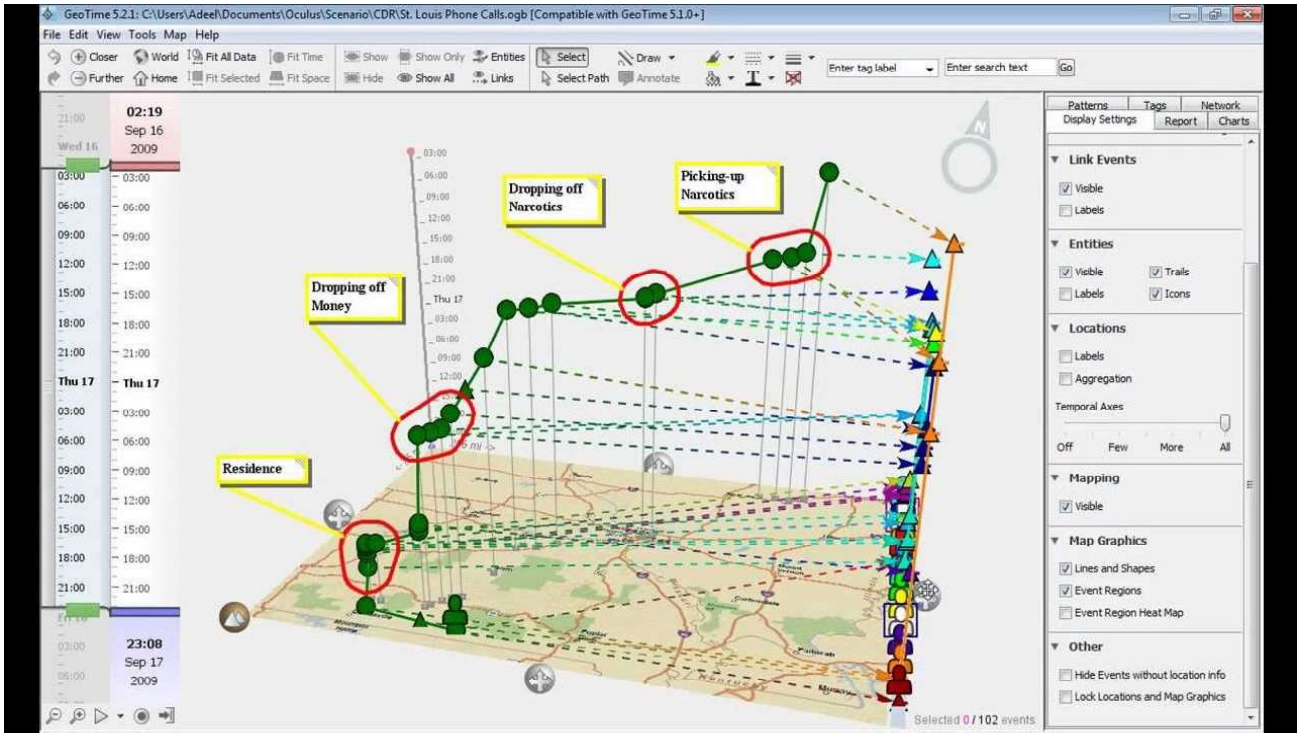


Cellular Communication System

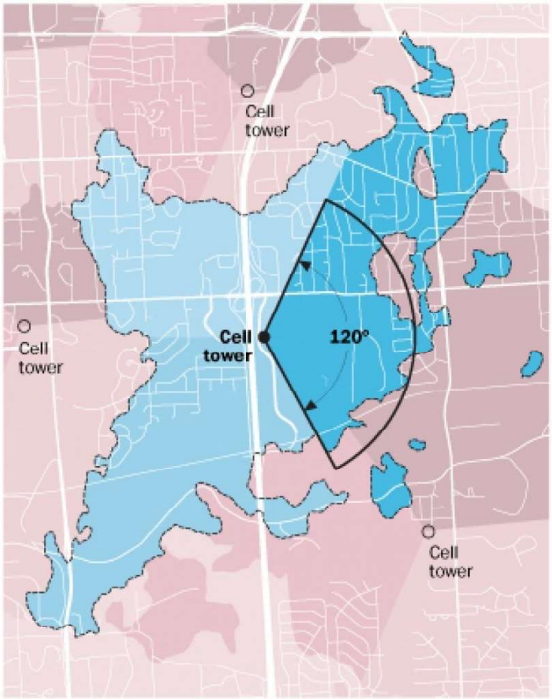
- Most Code Division Multiple Access (CDMA) networks conform to :-
  - These systems are referred to as CDMAOne
  - When they went to 3G services, they became CDMA2000
- Global System for Mobile Communications (**GSM**) uses the Time Division Multiple Access (TDMA) technique in which multiple phones take turns sharing a channel



Cell Site Analysis



Cell Site Analysis



Law enforcement says ...

IT'S A WEDGE
Most cell towers have three antennas. Analysts draw coverage areas as wedges radiating 120 degrees from each. They say the range is generally 1-2 miles.

Cellular experts say ...

IT'S A BLOB
Phone company coverage maps show that radio waves don't behave uniformly. They can be blocked by topography and other obstacles and can "leak" to areas outside the 120-degree focus area. Also, the range can vary from a few feet to more than 20 miles.

Also, experts say a cellphone call doesn't necessarily use the nearest tower, complicating efforts to link a caller to a crime scene. They say that when a phone is in range of more than one tower, an algorithm chooses a tower based on factors such as signal strength, tariffs and traffic already using that tower.

Cellular Communication Systems

Main components used for communication:

- **Base transceiver station (BTS)**
  - Cell phone tower and associated equipment
- **Base station controller (BSC)**
  - Hardware & software that controls the BTS
- **Mobile switching center (MSC)**
  - Routes calls
  - Has a database of subscribers with account and location data

Cellular Communication Systems

Generation	Speed	Technology	Features
2G	9.6/14.4 kbps	TDMA, CDMA	2G capabilities are achieved by allowing multiple users on a single channel via multiplexing. 2G enabled mobile phones can be used for data along with voice communication.
3G	3.1 Mbps (peak) 500-700 Kbps	CDMA 2000 (1XRTT, EVDO) UMTS, EDGE	3G provides amazing internet browsing speeds. Opens the door to a whole bag of oppurtunities with video calling, video streaming, etc. In 3G, universal access ad portability across different device types are made possible. (Telephone & PDA's)
3.5G	14.4 Mbps (peak) 1 3 Mbps	HSPA	3.5G supports even higher speeds and enhances higher data needs.
4G	100-300 Mbps (peak) 3-5 Mbps	WiMAX LTE	Speeds for 4G are increased to lightning fast in order to keep up with data access demand used by various services. It also supports HD streaming. HD phones can be fully utilized on a 4G network.

Mobile Device Basics

- Mobile devices can range from simple phones to small computers
  - Also called smart phones
- **Hardware components**
  - Microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces, LCD display, sensors, camera etc.
- Most basic phones have a **proprietary OS**

Mobile Device Basics

- What can be pulled from the device
- Logical tools acquiring call logs, pics, phonebooks
- SIMs on many androids providing last numbers dialled and SMS messages
- Physical access is improving.
- Practitioners **rooting device** to obtain more data – parsing required.

Inside Mobile Device- Memory

- Mobile devices contain both **non-volatile and volatile** memory
  - Non-volatile memory is a type of EEPROM
    - Enables service providers to reprogram phones without having to physically access memory chips
- Mobile devices contain 1 / 2 different types of non-volatile flash memory
  - **NAND and NOR**
- NOR flash has faster read times but slower write times than NAND
  - NOR flash is nearly immune to corruption and bad blocks while allowing random access to any memory location

Inside Mobile Device- Memory

- NAND flash offers higher memory storage capacities, is less stable and only allows sequential access
- Feature Phone – 1G memory configuration
  - NOR System and user data
  - RAM – Run time execution
- Smartphone – **2G** memory configuration
  - NOR, NAND & RAM
- Smartphone – **3G** memory configuration
  - NAND & RAM

Inside Mobile Device- Memory

- **RAM** is the most difficult to capture accurately due to its volatile nature
- **NOR memory** is best location for **1G** memory devices
  - operating system code, the kernel, device drivers, system libraries, memory for executing operating system applications
- **NAND memory** is also useful in almost all modern smart phones
  - **PIM** data (calendars, contacts etc), graphics, audio, video, and other user files

Mobile Forensics Process

Acquisition Procedure for Mobile Device

- Depending on the warrant or subpoena, the time of seizure might be relevant
  - Messages might be received on the mobile device after seizure
- Isolate the device from incoming signals with one of the following options:
  - Place the device in airplane mode
  - Use the Paraben Wireless StrongHold Bag
  - Turn off the device

SANS DFIR Recommendations

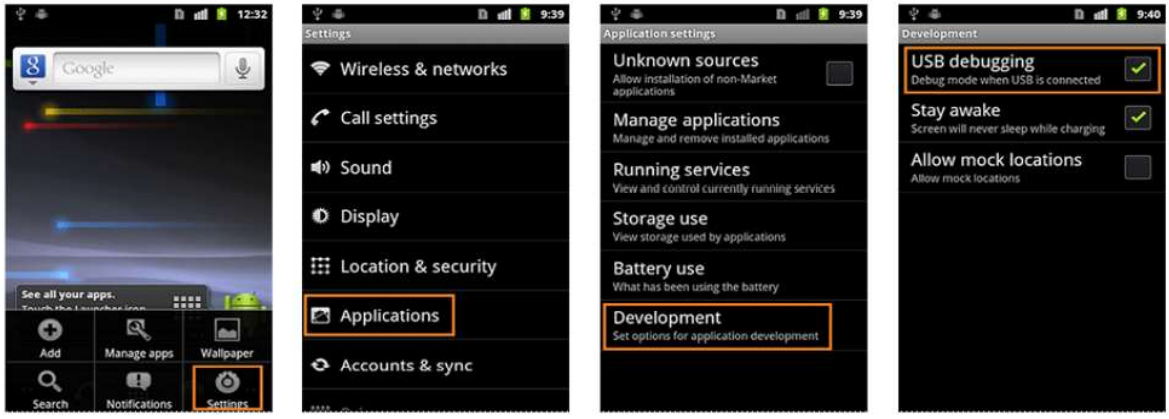
- **If device is on and unlocked**
  - isolate it from the network, disable the screen lock, remove passcode
- **If device is on and locked**
  - what you can do varies depending on the type of device
- **If device is off**
  - attempt a physical static acquisition and turn the device on

Mobile Device Isolation Techniques

- **Jamming**
  - The jammers are devices, also known as radio jammers, used to block the use of mobile phones sending radio waves with the same frequency used by mobile phones. This causes an interference, which inhibits the communication between mobiles and BTS, paralyzing every phone activity in its range of action.
- **Airplane mode**
  - The airplane mode is one of the options that can be used to protect the mobile collected into the crime scene to avoid in and out radio transmission.
  - It is a risky option because it is necessary to interact with the mobile phone, and possible only if the phone is not protected with Passcode.

Mobile Device Isolation Techniques

- **Activation of debug USB:**
  - Activation of this option allows a major access on the device with Android Debug Bridge (ADB) connection. This option will be a great tool for the forensic examiner during the extraction data process.
  - On Android devices, this option can be found in Settings | Development



Acquisition from Mobile Device

- Check these location for Information
  - Internal memory
  - SIM card
  - Removable or external memory cards
  - Network provider
  - Choice of logical or physical (bit-by-bit) acquisitions is also critical
    - Physical acquisitions can recover deleted files

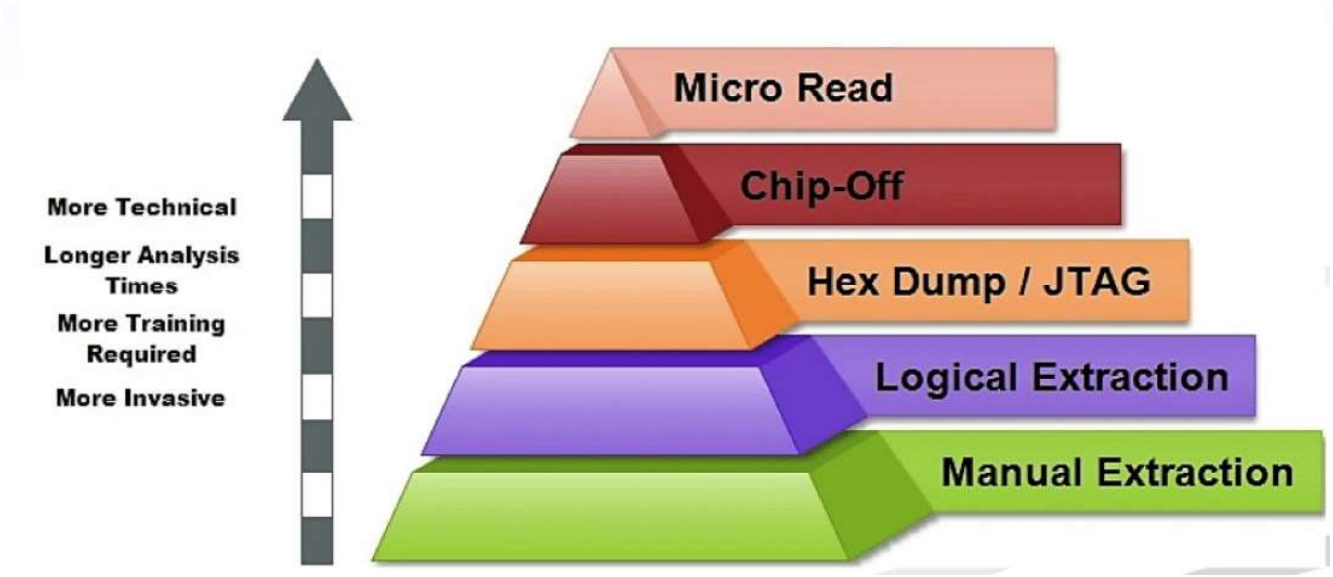
Acquisition from Mobile Device

- Basic Information that can be retrieved falls into four categories
  - **Service-related data**
    - Identifiers for the SIM card and the subscriber
  - **Call register** e.g. dialed, received and missed calls
  - **Message** information
  - **Location** information
- Modern smartphones have several other critical data
  - Pictures, videos, WhatsApp and Facebook logs etc.
- If power has been lost, PINs or other access codes might be required to view files

Mobile Forensics Equipment

- SIM card readers
  - A combination hardware/software device used to access the SIM card
  - You need to be in a forensics lab equipped with appropriate antistatic devices
  - A variety of SIM card readers are available

Mobile Forensics – Tool Classification Pyramid



Mobile Forensics Equipment

NIST guidelines list types of data extraction

1. Manual extraction
2. Logical extraction
3. Physical Acquisition
4. Hex dumping and Joint Test Action Group (JTAG) extraction
5. Chip-off
6. Micro read

Manual Extraction Method

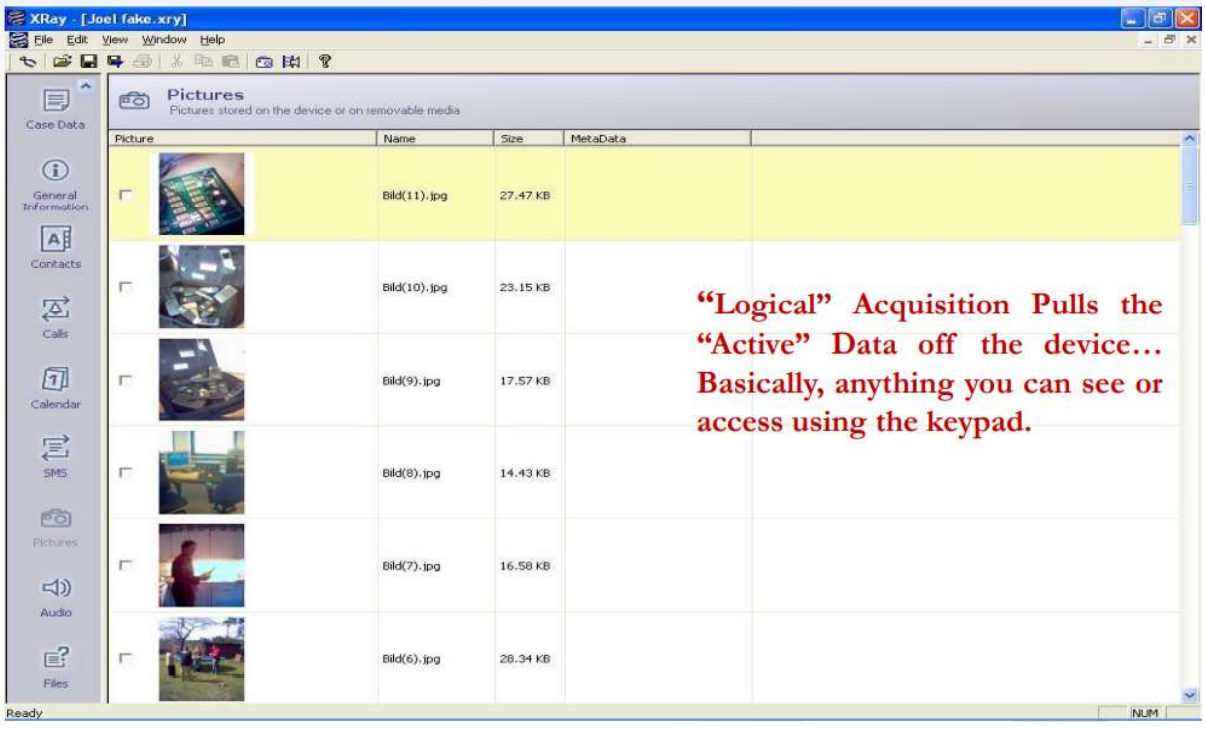
- Viewing the data content stored on a mobile device via LCD screen
  - requires the manual manipulation of the buttons, keyboard or touchscreen to view the contents of the mobile device
- Language problems might also occur
  - Phone might be displaying a different language unknown to investigator
- If there is **a large amount of data**, a manual extraction can be very **time consuming**
  - Carrying the danger of modifying, deleting or overwriting as a result of the examination

Logical Extraction

- Mobile device and the forensics workstation are connected with a wire (e.g., USB or RS-232) or wireless (e.g., IrDA, WiFi, or Bluetooth)

- The examiner should be aware of the issues associated with each connection type
  - Associated protocols may result in data being modified

Logical Extraction



Physical Acquisition

- Today Top Tools: XRY Physical & UFED Physical
- **Flasher Box**
  - Used Primarily For "Unlocking" Phones from the Network – Many have ability to dump raw data, and have been adopted by digital examiners for acquiring and validating data's

Hex Dumping

- Hex Dumping (FWS + Flasher Box + Mobile Phone)
  - A software is uploaded to mobile device via its data port which brings it in diagnostic mode
  - A series of commands is then sent by Flasher box to extract flash memory contents
    - Which then are sent to Forensic Workstation
- Need a cable connection
  - In rare cases WiFi can also be used

JTAG

- JTAG - Joint Test Action Group
  - defines a common test interface for processor, memory, and other semiconductor chips
- JTAG testing unit
  - used to request memory addresses from the JTAG-compliant component and accept the response for storage and rendition
- Proper training is required for extracting and analyzing binary images with JTAG

Chip-Off

- refer to the acquisition of data directly from a mobile device's flash memory
- Requires the physical removal of flash memory

- Chip-Off provides examiners with the ability to create a binary image of the removed chip
  - Identical to hard disk imaging
- Extensive training is required in order to successfully perform extractions at this level

Micro Read

- Involves recording the physical observation of the gates on **a NAND or NOR chip** with the use of an electron microscope

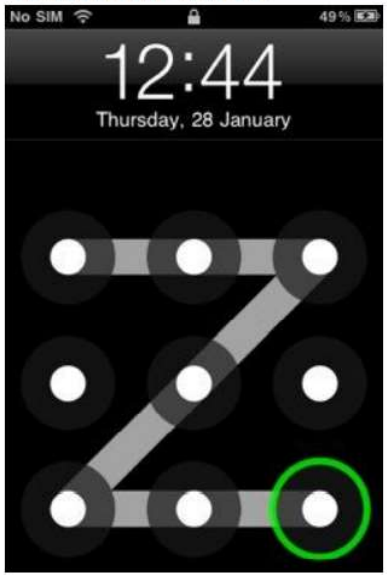
- Extreme level of technicalities are involved
  - only be attempted for high profile cases equivalent to a national security crisis

Forensic Analysis

- Analyzing acquired data
  - File System Analysis
  - SQLite Analysis
  - Directory Structure
  - FAT Analysis
  - SD Card Analysis

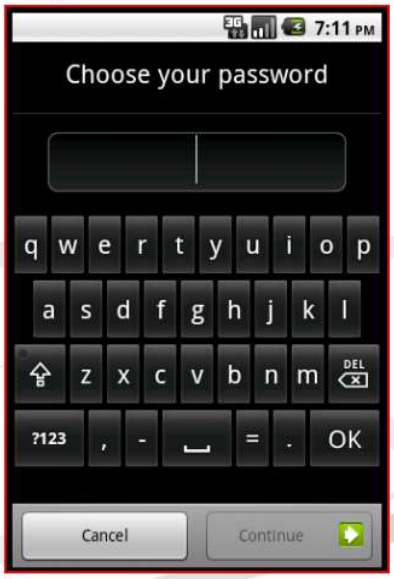
Passcode Types

Pattern lock



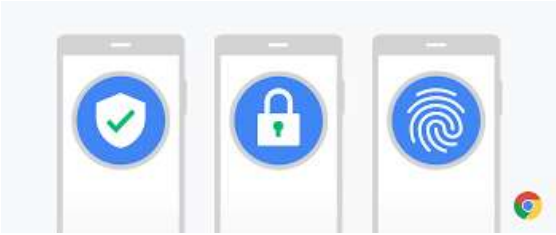
PIN

Alphanumeric



New Passcode Types

Facial recognition



Mobile Forensic Tools

- **Paraben** Software offers several tools:
  - Device Seizure - used to acquire data from a variety of phone models
  - Device Seizure Toolbox - contains assorted cables, a SIM card reader, and other equipment
- **BitPim** - used to view data on many CDMA phones
- **Cellebrite UFED** Forensic System - works on smartphones, PDAs, tablets, and GPS devices
- **MOBILedit** Forensic - contains a built-in write-blocker
- **SIMcon** used to recover files on a GSM/3G SIM or USIM card

Mobile Forensic Tools

- **Cellebrite** is often used by law enforcement
- Can determine the device's make and model, hook up the correct cable, turn the device on, and retrieve the data
- **Limitation**
  - There are more than half a million aps for mobile devices and Cellebrite can analyze data from only a few hundred

Challenges

- Many mobile forensics tools are available (many not free)
- Methods and techniques for acquiring evidence will **change** as market continues to expand and mature
- **Type 2 hypervisors** for mobile devices are under development and will add another level of complexity to forensics investigations
- Number of devices that connect to the Internet is higher than the amount of people
  - That number is expected to grow even larger as more devices are being developed to attach to the Internet
- Wearable computers will pose many new challenges for investigators

https://www.techtarget.com/searchitoperations/tip/Whats-the-difference-between-Type-1-vs-Type-2-hypervisor

Inside Mobile Device

- GSM refers to mobile phones as "mobile stations" and divides a station into **two** parts
  1. Universal Integrated Circuit Card (UICC)
  2. Mobile equipment (ME)
- **UICC** is known as Identity modules
  - Subscriber Identity Module [SIM],
  - Universal Subscriber Identity Module [USIM],
  - CDMA Subscriber Identity Module [CSIM]
- UICC's main purpose
  - authenticating the user to the network
  - offers storage for personal information e.g. contacts, text messages

Inside Mobile Device

- **UICC stands for Universal Integrated Circuit Card**.
- It is a new generation SIM (Subscriber Identification Module) included in cell phones or notebooks used in some high speed wireless 3G.
- The UICC identifies you to your wireless carrier so they know your plan and services.
- It can store your contacts and enables a secure and reliable voice and multi-media data connection, global roaming and remotely adding new applications and services.
- The UICC is the best and only universal application delivery platform that works with any 3G or 4G device

Inside Mobile Device

- A UICC can contain up to three applications: **SIM, USIM and CSIM**
  - UICC usually refers to a physical card
- UICC is a special type of smart card
  - Processor and memory (EEPROM, ROM & RAM)
- The UICC's file system resides in persistent memory and stores data e.g. phonebook entries, messages
  - UICC operating system controls access to elements of the file system

Inside Mobile Devices – UICC SIM on GSM Phones

- IMSI: International Mobile Subscriber Identity
- ICCID: Integrated Circuit Card Identification (SIM Serial No.)
- MSISDN: Mobile Station Integrated Services Digital Network (phone number)
- Network Information
- LND: Last Number Dialled (sometimes, not always, depends on the phone)
- ADN: Abbreviated Dialled Numbers (Phonebook)
- SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)
- SMS Service Center Info: GPRS Service Center Info:
- Location Information: The GSM channel (BCCH) and Location Area Code (LAC) when phone was used last.

* When SIM Locked – Cannot Be Cracked without Network Operator Assistance.

Not on SIM, but Exclusive To GSM Devices

- IMEI: International Mobile Equipment Identity. - To Find IMEI, Type #*06#. IMEI is on the Device, registers with the network, along with IMSI. IMSI+IMEI+MSISDN the most detailed identity information of user.

Mobile Forensic Tools OSForensics

Video

Crimes Committed Through Mobile Phones

- Blue jacking: Sending of messages from a Bluetooth device to another Bluetooth enabled device. ...
- Blue Bugging
- Vishing
- Smishing (SMS Phishing)
- Malware
- **Mobile phone** as bomb trigger
- Banker
- Spyware

Reading Task

Current and Future Trends in Mobile Device Forensics: A Survey

by

KONSTANTIA BARMPATSALOU, TIAGO CRUZ, EDMUNDO MONTEIRO, and PAULO SIMOES, University of Coimbra

Uploaded on GCR