

CS 798: Digital Forensics and Incident Response

Lecture 19 - Mobile Forensics

Diogo Barradas

Winter 2025

University of Waterloo

Wireless devices play crucial role in crime

- Mobile devices create new opportunities for criminals
 - While providing valuable sources of evidence

Mobiles used in high-tech terror

By CNN's Jim Boulden
Monday, April 5, 2004 Posted: 0232 GMT (1032 HKT)

LONDON, England (CNN) -- Mobile phones are in the hands of millions of people around the world. And increasingly, it appears, in the hands of terrorists.

The bombers who targeted commuter trains in Madrid on March 11 used the built-in alarm clock in mobile phones to set off explosives.

Cellphone tracking used to catch Boston bomber, local criminals

By: [Laura Warren - Email](#)
News 12 at 6 o'clock / Monday, April 22, 2013

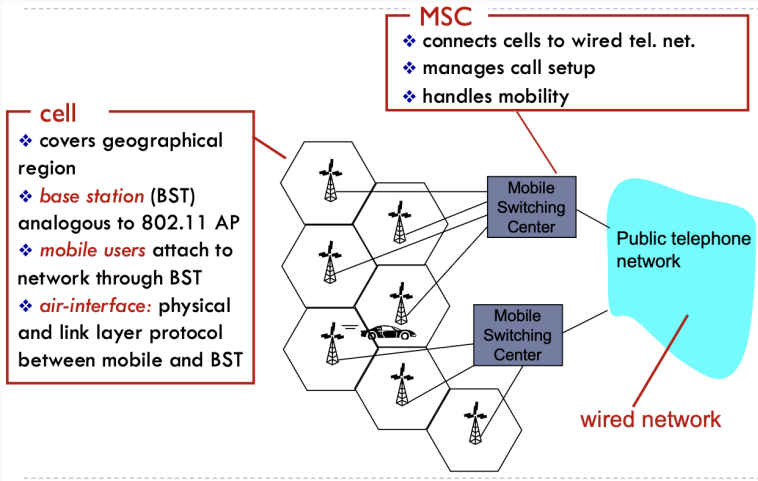
AUGUSTA, Ga. (WRDW) -- The whole world watched as police searched for the second suspect in the Boston bombings. A cellphone left behind in a hijacked car helped lead them to Dzhokhar Tsarnaev's hiding spot.

Ed Deveau, chief of police in Watertown, says, "We were able to ping that phone and find out it was in Watertown, and it was heading in a certain neighborhood of Watertown."

1. Cellular network investigation
2. Evidence in Android devices
3. Evidence extraction from Android devices

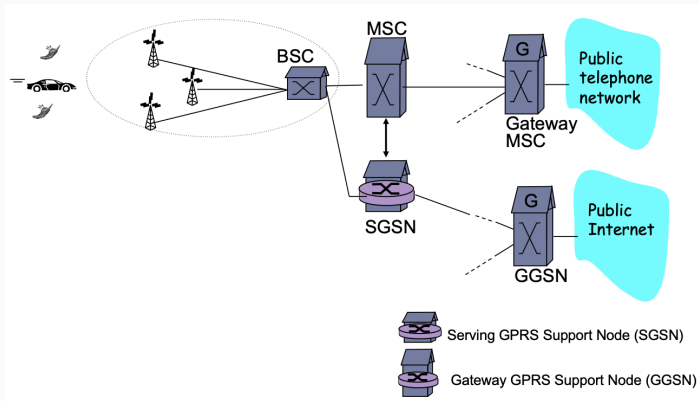
Cellular network investigation

Components of cellular network architecture



2.5G network architecture onwards

- Subscribers connected both to circuit switched networks (e.g., PSTN) and packet switched networks
 - voice network unchanged in core
 - data network operates in parallel



Aspects to consider in cellular nets investigations

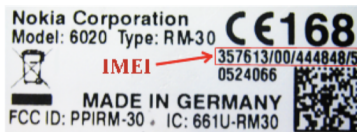
- What kind of evidence is there to collect and analyze?
- How to collect and analyze evidence?
- How to locate cellular devices?

IMEI are quite valuable for investigators

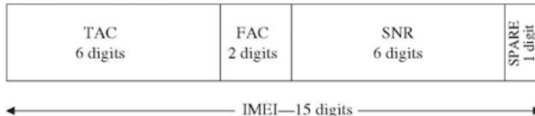
- The International Mobile Equipment Identifier (IMEI) is a unique number associated with a particular device
 - Has no permanent or semi-permanent relation to the subscriber
 - Used to blacklist stolen devices
 - IMEI can be used to obtain stored data from carriers
 - To monitor traffic associated with a particular device
 - To keep track of a mobile device across carriers



IMEI format



IMEI format prior to 2004



Type Allocation Code

Identifies the mobile device
(manufacturer, model, internal model number)

Final Assembly Code

Location of device's construction
2003/01-2004/04: FAC = 00



Obtain class characteristics from an IMEI

- Search an online IMEI database
 - <http://www.imei.info/>

**BEST WAY TO GET TO KNOW
YOUR PHONE BETTER**

Every mobile phone, GSM modem or device with a built-in phone / modem has a unique 15 digit IMEI number. Based on this number, you can check some information about the device, eg brand or model. Enter the IMEI number below:

357613004448485 **CHECK**


Information about your phone

Model: 6020
Brand: NOKIA
IMEI: TAC: 357613 FAC: 00 SNR: 444848 CD: 5

BASIC INFORMATION:

Device type:	Phone
Design:	Classic
Released:	2004 r.
SIM card size:	Mini Sim - Regular
GSM:	✓ 900 1800 1900
Dimensions (H/W):	106 x 44 x 20 mm, vol. 70 cm³
Display:	LCD Color (64K) 128x128px
Touch screen:	✗
Weight:	90 g
Time GSM (talk/stand-by):	3 / 330 hrs. (13.8d)
Battery:	Li-Ion 760 mAh
Built-in memory:	✓ 3.5 MB
OS:	Vendor

READ MORE

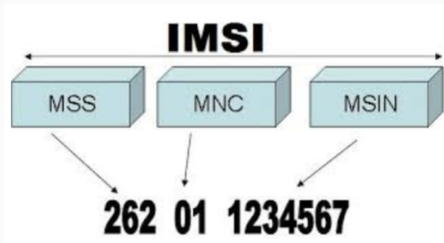


Device leaves traces the moment it's turned on

- When powered on, the device announces itself to the network, starting the authentication process
- The authentication process is based on the IMSI
 - Identity Mobile Subscriber Identity (IMSI) is a unique # stored on the SIM card and associated with a particular subscriber
 - IMSI is not directly sent over the network, but replaced with a Temporary Mobile Subscriber Identity (TMSI), which is logged
- Investigators can ask NSPs to query their systems for all activities relating to a particular subscriber account

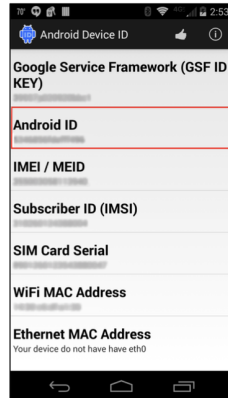
International Mobile Subscriber Identity (IMSI)

- Globally-unique code number that identifies a GSM subscriber to the network
 - Located in the SIM card
- IMSI format:
 - Mobile Country Code (MCC)
 - Mobile Network Code (MNC)
 - Mobile Subscriber Identification Number (MSIN)



Mobile advertisement IDs

- Mobile advertising identifier (MAID)
 - unique pseudo-anonymous identifier tied to a mobile phone
 - collect data about the phone and its usage patterns
- By design, these identifiers are resettable



Mobile advertisement IDs

- Logs maintained by a provider can help determine past usage of the phone and communications between individuals
- Logs are generated from **Call Detail Records** (CDRs) maintained for billing purposes:
 - Telephone number of user
 - Numbers called
 - IMEI number of mobile device
 - Information about the cell
 - SMS sent (excluding the text)
 - Date, time, and duration of the calls
- By design, these identifiers are resettable

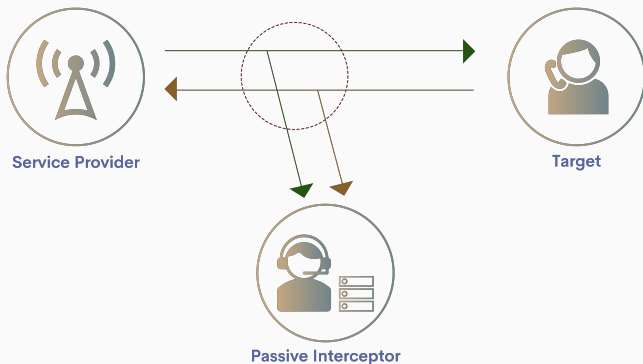
- What kind of evidence is there to collect and analyze?
- **How to collect and analyze evidence?**
- How to locate cellular devices?

Interception of evidence on mobile networks

- In general, the freedom and privacy of personal communications are inviolable rights that can be compromised only if authorized by **judicial authorities**
- For **privacy** protection, legal systems dictate limitations to admissibility of interceptions:
 - Interceptions are allowable only in certain specific crimes
 - Interceptions must be authorized
- Typically, interceptions done in collaboration with providers

How telephone (or data) interception works

- The provider duplicates a suspect's communication line and deviating it to a call **Monitoring Center** (MC) as specified in a warrant by the Judicial Authorities
- In principle, the provider should not gain knowledge of the contents of the tapped telephone calls

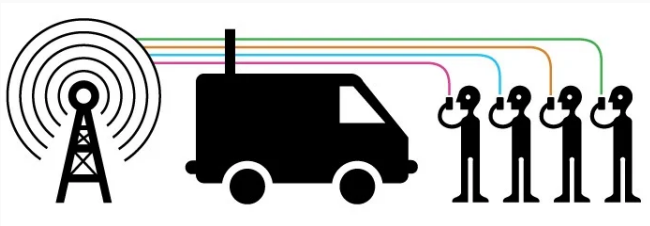


Advanced features in interception systems

- Voice recognition
 - Central database for storage of recognized voices complete with sample recordings and personal notes
- Analysis of target behavior
 - Predictive target behavior analysis and graphic analysis for interaction among targets

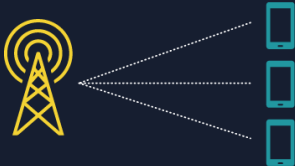
Alternative approach to interception: IMSI-catcher

- IMSI-catcher subjects the phones in its vicinity to a MITM attack, acting to them as a fake base station
 - Exploits GSM security hole where the network doesn't need to authenticate
- The FBI adopts this technique using the Stingray IMSI-catcher



Stingray

1. A stingray mimics a cell phone tower, sending a signal to nearby cell phones.



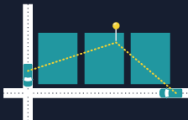
2. Phones in the area connect to the stingray if it is the strongest signal.



3. Stingrays can send a signal to a phone forcing it to share its unique ID code, called an IMSI.



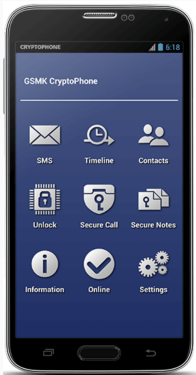
4. Stingrays can be used in vehicles to measure the signal strength of a target phone from different positions to determine the location of a phone.



5. Stingrays can also trick phones into sending data without encryption, allowing for surveillance of a phone's network activity.



Crypto phones

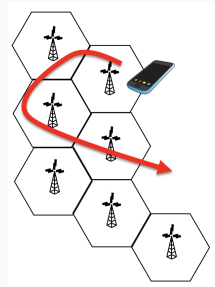


- To prevent eavesdropping and electronic surveillance, use crypto phones
- Crypto phones encrypt the voice signals end-to-end
 - Implement automatic variation of session key
 - Cryptographic chip handles crypto operations
- This represents a limit for investigations, unless encryption can be broken

- What kind of evidence is there to collect and analyze?
- How to collect and analyze evidence?
- **How to locate cellular devices?**

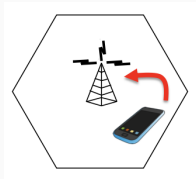
Location parameters

- Location parameters: info that can be combined to localize an active mobile device and its related user
- Determine device's position: There's a timeframe where mobile devices "announce" themselves to the network
 - Turning on a device and leaving it in an idle state generates data on the network that can help determine its location
 - As a device is moved, it updates the network



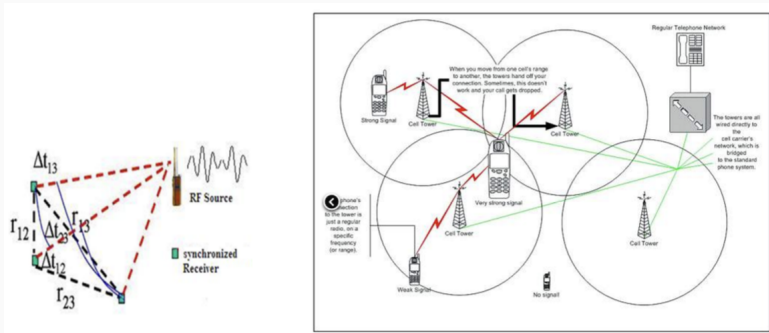
Position tracking methods: Cell identification

- The mobile device can be reached by looking at the cell to which it is currently connected
- There is a range of accuracy
 - Starts from a few hundred meters in urban areas, up to 32 km in suburban
- Accuracy depends on the known range of the particular base station



Position tracking methods: TDOA

- Time difference of arrival (TDOA) aka multilateration
 - Measures the time it takes for a signal to travel from a device to multiple base stations to estimate the device location
 - Commonly used in civil and military surveillance applications



Evidence in Android devices

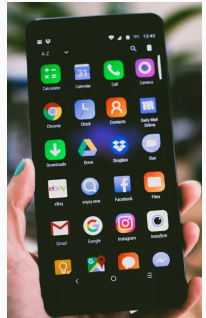
- Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions
- Why?
 - Everybody has 1+ mobile devices
 - Lots of information on devices
 - Major target of malware
 - Proliferation of fake apps

(Lots of) app data on Android devices

- SMS
- MMS
- Chat messages
- Backups
- E-mails
- Call logs
- Contacts
- Pictures
- Videos
- Browser history
- GPS data
- Files/documents
- Social media apps
- Calendar
- Shopping history
- Financial info
- Audio collections
- Driving directions
- ...

What data is stored?

- Android devices store a lot of sensitive data through the use of apps
- There are a number of sources for apps:
 - Apps that come along with Android
 - Apps installed by the manufacturer
 - Apps installed by a wireless carrier
 - Apps installed by the user
- Beyond data from apps, the Kernel and Android stack provide info through logs, debugging, and other services

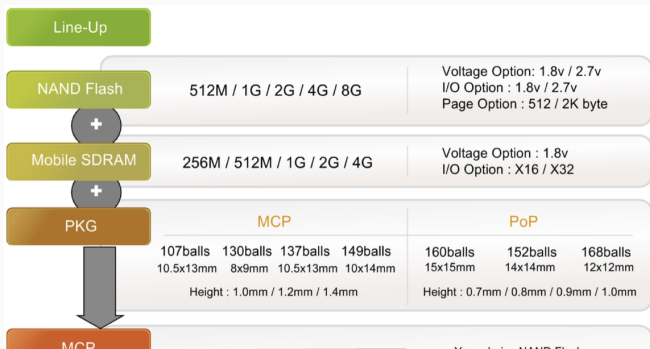


Where is data stored

- Android applications primarily store data in two locations: internal and external storage
- External data storage (SD card)
 - Data can be stored in any location
- Internal data storage
 - The location is predefined and controlled by the Android APIs
 - Internal data of all apps is saved in `/data/data/<apppkg>`
 - e.g., e-mail client location `/data/data/com.android.email`

Memory

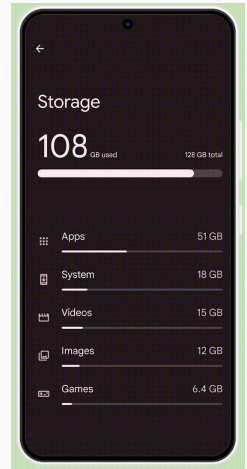
- Android devices have two primary types of memory
 - Volatile: random-access memory (RAM)
 - Non-volatile: NAND flash memory
- NAND flash
 - Critical for forensic investigation
- MCP
 - RAM and NAND in a single multichip package



How data is stored

- Developers have five methods for storing data on a device
 - Which option to be used depends on the underlying data

- The five methods are:
 - Shared preferences
 - Internal storage
 - External storage
 - SQLite database
 - Network

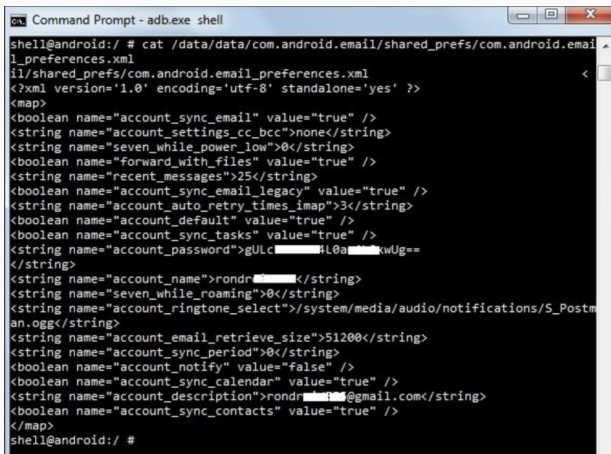


1. Shared preferences

- This location provides a framework to store key-value pairs of primitive data types in the `.xml` format
 - Primitive data types: boolean, float, int, long, and string
 - Strings are stored in the UTF-8 format
 - Location: `/data/data/<package_name>/shared_prefs`
- Many applications use shared preferences to store sensitive data, because it is lightweight
- Thus, they can be a key source of information during a forensic investigation

Example of useful shared preferences

- Contents of file `com.android.email_preferences.xml`
 - `account_name`, `account_password`, `recent_messages` are interesting from a forensic viewpoint



```
Command Prompt - adb.exe shell
shell@android:/ # cat /data/data/com.android.email/shared_prefs/com.android.email_preferences.xml
il/shared_prefs/com.android.email_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="account_sync_email" value="true" />
<string name="account_settings_cc_bcc">none</string>
<string name="seven_while_power_low">0</string>
<boolean name="forward_with_files" value="true" />
<string name="recent_messages">25</string>
<boolean name="account_sync_email_legacy" value="true" />
<string name="account_auto_retry_times_imap">3</string>
<boolean name="account_default" value="true" />
<boolean name="account_sync_tasks" value="true" />
<string name="account_password">gULc[REDACTED]:L0a[REDACTED]kwUg==
</string>
<string name="account_name">rondr[REDACTED]</string>
<string name="seven_while_roaming">0</string>
<string name="account_ringtone_select">/system/media/audio/notifications/S_Postm
an.ogg</string>
<string name="account_email_retrieve_size">51200</string>
<string name="account_sync_period">0</string>
<boolean name="account_notify" value="false" />
<boolean name="account_sync_calendar" value="true" />
<string name="account_description">rondr[REDACTED]@gmail.com</string>
<boolean name="account_sync_contacts" value="true" />
</map>
shell@android:/ #
```

2. Files on internal storage

- Files allow developers to store more complicated data
- Files are stored in the internal storage
 - Typically in the application's /data/data subdirectory
- Data stored here is private and cannot be accessed by other applications
 - Even the device owner is prevented from viewing the files (unless they have root access)
 - The developer can allow other processes to modify and update these files

Identifying custom files

- There is a typical organization for the /data/data subdir:

```
ahoog@ubuntu:~/data/data/com.google.android.apps.maps$ ls -l
total 24
drwxr-x--x 5 ahoog ahoog 4096 2011-01-18 03:42 app_
drwxr-x--x 3 ahoog ahoog 4096 2010-09-15 10:59 cache
drwxr-x--x 2 ahoog ahoog 4096 2011-01-23 10:30 databases
drwxr-x--x 2 ahoog ahoog 4096 2011-01-23 20:55 files
drwxr-xr-x 2 ahoog ahoog 4096 1980-01-06 09:41 lib
drwxr-x--x 2 ahoog ahoog 4096 2011-01-24 04:13 shared_prefs
```

- Files are typically under app_ and files
 - cache: files cached by app
 - databases: SQLite and journal files
 - lib: custom library files required by app
 - shared_prefs: XML file of shared preferences
- Other folders are custom folders created by the app developer

3. Files on external storage

- Files can be stored by the apps in external storage
 - Can be a removable media (SD card) or non-removable storage that comes with the phone
- SD cards are usually formatted with the FAT32 FS
 - FSs, such as EXT3 and EXT4, are also being used
- External storage does not have strict security enforcements
 - Data stored here is public: can be accessed by other apps
 - Typically mounted on `/sdcard` or on `/mnt/sdcard`
- Some devices emulate SD card directly on NAND flash

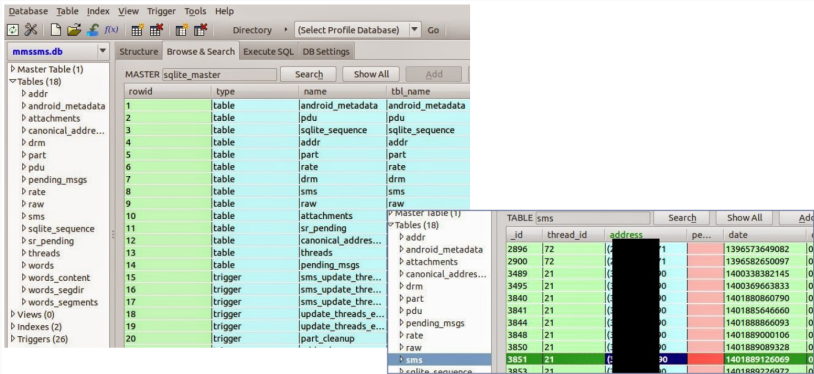


4. SQLite database

- Another NAND/SD card-based storage that developers leverage is a specific type of file-an SQLite database
 - DBs are used for structured data storage and SQLite is a popular database format
- Android SDK provides dedicated APIs that allow developers to use SQLite DBs in their applications
 - Generally stored under `/data/data/<pkg>/databases`
- From a forensic point of view, they are highly valuable
 - Often store a lot of important data handled by the application

Forensic analysis of SQLite databases

- For example, using SQLite Manager



The screenshot displays the SQLite Manager interface for a database named 'mmssms.db'. The left sidebar shows a tree view of the database structure, including tables and triggers. The main window shows the 'sqlite_master' table, which contains metadata for all tables in the database. A secondary pane shows the 'sms' table, which contains text message data.

MASTER sqlite_master

rowid	type	name	tbl_name
1	table	android_metadata	android_metadata
2	table	pdu	pdu
3	table	sqlite_sequence	sqlite_sequence
4	table	addr	addr
5	table	part	part
6	table	rate	rate
7	table	drm	drm
8	table	sms	sms
9	table	raw	raw
10	table	attachments	attachments
11	table	sr_pending	sr_pending
12	table	canonical_addresses	canonical_addresses
13	table	threads	threads
14	table	pending_msgs	pending_msgs
15	trigger	sms_update_thre...	sms_update_thre...
16	trigger	sms_update_thre...	sms_update_thre...
17	trigger	sms_update_thre...	sms_update_thre...
18	trigger	update_threads_e...	update_threads_e...
19	trigger	update_threads_e...	update_threads_e...
20	trigger	part_cleanup	part_cleanup

TABLE sms

_id	thread_id	address	pe...	date
2896	72	[REDACTED]	1	1396573649082
2900	72	[REDACTED]	1	1396582650097
3489	21	[REDACTED]	0	1400338382145
3495	21	[REDACTED]	0	1400369663833
3840	21	[REDACTED]	0	1401880860790
3841	21	[REDACTED]	0	1401885646660
3844	21	[REDACTED]	0	1401888866093
3848	21	[REDACTED]	0	1401889000106
3850	21	[REDACTED]	0	1401889089328
3851	21	[REDACTED]	0	1401889126069
3853	21	[REDACTED]	0	1401889226972

5. Network

- Another data storage mechanism available to developers
 - Store and retrieve data from web-based services
 - Of course requires a remote storage service
- Example: Dropbox

```
ahoog@ubuntu:~/htc-inc/data/data$ tree com.dropbox.android/  
com.dropbox.android/  
|-- databases  
|   |-- db.db  
|-- files  
|   |-- log.txt  
|-- lib  
|-- shared_prefs  
|   |-- DropboxAccountPrefs.xml
```

Example: Dropbox logs

- Items of potential interest from the log, e.g:
 - All actions have timestamps
 - Successfully authenticate user, user name provided

```
4 1296055134550 com.dropbox.android.DropboxApplication Authenticating username:
book@viaforensics.com
4 1296055136507 com.dropbox.android.DropboxApplication Successfully
authenticated
6 1296055137501 com.dropbox.android.activity.LoginActivity Dismissed nonexistent
dialog box
4 1296055137525 com.dropbox.android.activity.LoginOrNewAcctActivity Successful
account login
4 1296055137549 com.dropbox.android.activity.delegate.MenuDelegate Successful
login
4 1296055137735 com.dropbox.android.activity.SimpleDropboxBrowser Query is:
content://com.dropbox.android.Dropbox/metadata/
6 1296055137742 com.dropbox.android.provider.QueryStatus Querying with query
id: DB2
```

Example: Dropbox database

- The database provides important forensic data
 - The Android intro.pdf file was automatically synced to the Dropbox account
 - When the PDF file was viewed, it was cached on the SD card

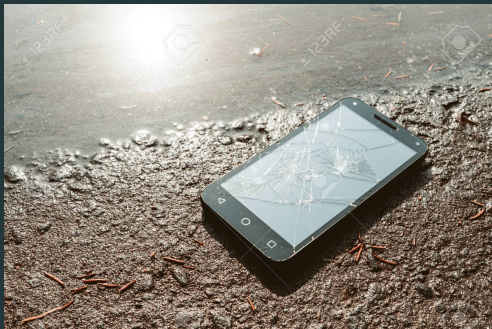
```
sqlite> select * from dropbox where _id = 2;
      _id = 2
      _data = /sdcard/dropbox/Android intro.pdf
    modified = Wed, 26 Jan 2011 15:18:40 +0000
      bytes = 176607
    revision = 10
      hash =
      icon = page_white_acrobat
    is_dir = 0
      path = /Android intro.pdf
      root =
      size = 172.5KB
    mime_type = application/pdf
  thumb_exists = 0
    parent_path = /
  _display_name = Android intro.pdf
    is_favorite =
local_modified = 1296055191000
  local_bytes = 176607
local_revision = 10
      accessed =
    sync_status = 2
```

Evidence extraction from Android devices

What's special about data acquisition in mobiles

- Can't remove persistent memory off the device
 - Depend on the device's firmware / OS to access the data
- The firmware / OS of the device restricts access to data
 - e.g., Android's debug bridge can't read app's private data
- Linked with outside world via wireless
 - Commands issued via 4G and WiFi may cause data destruction
- Depend on battery for power supply
 - Data may get lost (or made inaccessible) when battery runs out

A smartphone has been found in the crime scene and it is **powered off**.



What would you do?

Bring the device and power and data cables

- It is always prudent to seize the cables directly from the scene
- It is possible that a newer device is in use and the forensic toolkits do not yet have an appropriate cable



Smudge attack

- Infer the lock pattern from the oil smudge left on the display's surface
- First responders must minimize contact with the screen



A smartphone has been found in the crime scene and it is **powered on**.



What would you do?

Network isolation

- Isolate the device from the network
 - Messages can be received or removed by triggers outside our control
 - In the worst case, a remote wipe could be initiated on the device
- Isolation should **prevent** reception of new calls, messages, or commands that could **alter or destroy** evidence
- Need to cover several wireless interfaces:
 - GSM, WiFi, Bluetooth, etc.

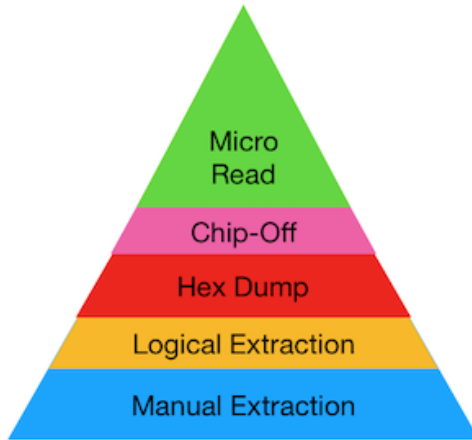


How to isolate a device

- Place the device in airplane mode
 - We modify the device settings
- Suspend account with mobile carrier
 - Process may take time and require court order
- Remove the SIM card
 - Does not disable WiFi
- Turn off the device
 - Modifies system state and we lose temporal data
- Place the device in a Faraday bag
 - Debate around effectiveness and can drain battery over time

Approaches for cell phone forensics

- Most analysis is logical data or screen capture



Approaches for cell phone forensics

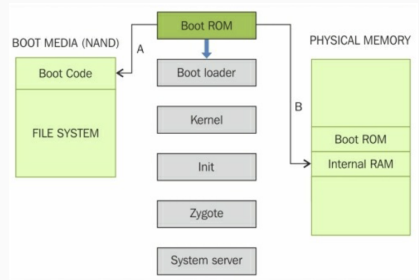
- Screen captures
 - The simplest way. Use a camera to take pictures of what's on the screen. Reporting tools are available.
- Sw-based logical analysis
 - Extracting the data on the device that you see and can access on the device. No deleted information with this method. Call logs, phone books, SMS messages, pictures, email, browsing, etc. The active information on the device can be extracted using a logical extraction tool. Standard method today.
- Sw-based physical analysis
 - The practice of extracting data from the physical memory of the device, and removable memory. Like PC forensics, you are getting the raw binary / hex data. Requires decoding and understanding of language and techniques used by device manufacturers. Physical analysis is the way to deleted information, but it is difficult and sparsely supported. Only a few tools

Logical techniques

- Logical forensic techniques extract data that is allocated
 - i.e., extractions that do not recover deleted data, or do not include a full bit-by-bit copy of the evidence
 - Typically achieved by accessing the file system
- For the most part, user data may be recovered logically:
 - Contacts
 - Call logs
 - SMS/MMS
 - Application data
 - System logs
- The bulk of this data is stored in SQLite databases

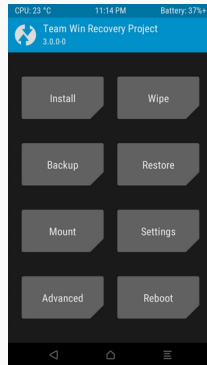
Android boot process

- Understanding the boot process of an Android device will help understand other forensic techniques which involve interacting with the device at various levels
- Sequence of steps:
 - Boot ROM code execution
 - The boot loader
 - The Linux kernel
 - The init process
 - Zygote and Dalvik
 - The system server



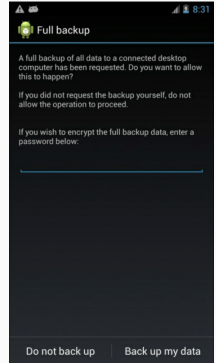
Manual ADB data extraction

- ADB pull command to pull single files or directories directly from the device
 - Device must be rooted to access /data/data
- To be forensically sound, ideally ADB data extractions should not be used against a phone while it is turned on
 - While the device is running, timestamps can be modified and applications may be running and updating files in the background
- To avoid this, an examiner should place the device into a custom recovery mode



ADB Backups

- Google implemented ADB backup functionality which allows users (and forensic examiners) to backup app data to local computer over ADB
- This process does not require root, and is therefore highly useful for forensic purposes
- However, it does not acquire every application installed on the device
- User must approve the backup on the device
 - Thus, cannot be done without bypassing screen locks



Screen capture

- Sometimes, taking a picture is the only way to take data off of a phone



Physical techniques

- Forensic techniques provide access to much more data
 - Data deleted or deemed obsolete by the system
- Physical techniques fall into two broad categories:
 - Software: Techniques which run as software on devices with root access and provide full physical image of data partitions
 - Hardware: Methods which connect hardware to the device or physically extract device components

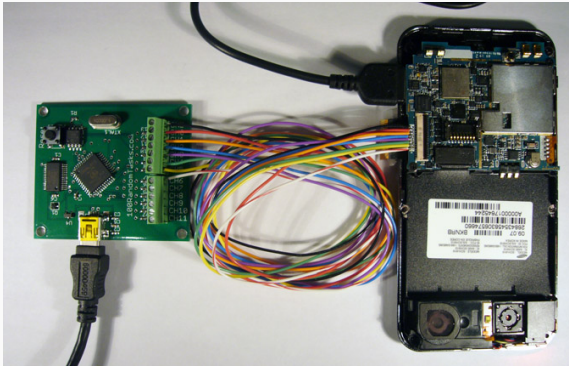
Software-based physical techniques

- Extract the data using an imaging tool, e.g., dd
 - Execute dd on the device from the ADB shell
 - Requires root permissions
- Analyze using standard forensic tools, e.g, Autopsy

```
dd if=/dev/block/mmcblk0 of=/sdcard/blk0.img bs=4096 conv=noerror
```

Hardware-based physical techniques: JTAG

- JTAG interface: used during the device production process to communicate with the processor for testing
 - Allows examiners to communicate directly with the processor and retrieve a full physical image of the flash memory



Hardware-based physical techniques: Chip-off

- Chip-off involves heating the device's circuit board until the solder holding the components to the board melts, and then removing the flash memory chip
 - The memory chip can then be read using commercial tools, resulting in a full physical image



Takeaways

- Wireless and mobile communications represent an increasingly growing amount of network traffic
- WiFi and cellular networks are amongst the most popular technologies used today
- Therefore, it is important for digital investigators to be able to collect and analyze evidence from such networks
- Mobile devices, in particular Android-based, carry a lot of forensically interesting data about their users

- **Textbook:**
 - Tamma – Chapters 1, 8–9
- **Other resources:**
 - TBD
- **Acknowledgements:**
 - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon