CSE 469: Computer and Network Forensics

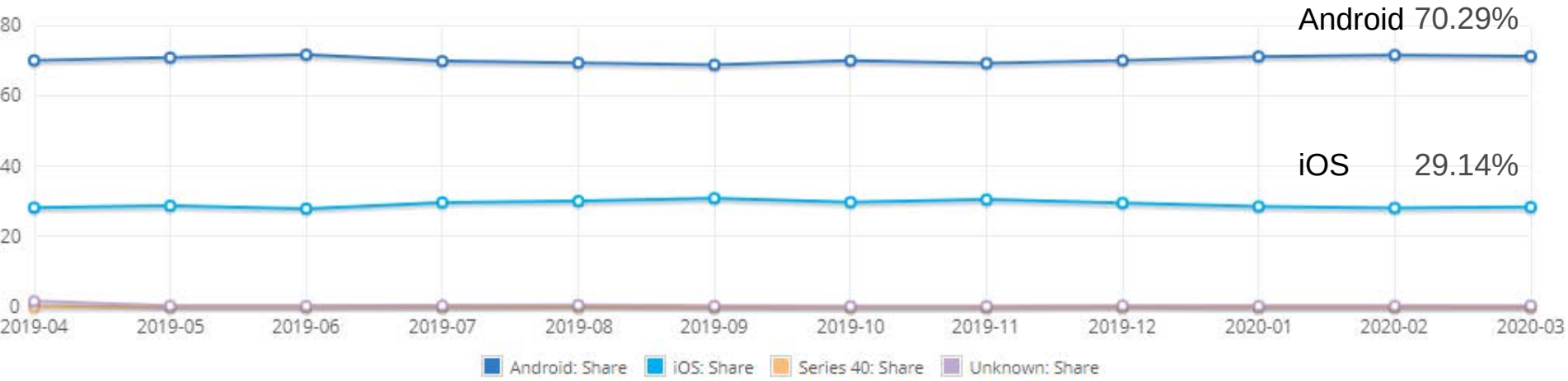
Topic 7: Mobile Forensics

Dr. Jaejong Baek | Spring 2020

What is Mobile Forensics?

- Wikipedia Definition: “a branch of digital forensics relating to **recovery of digital evidence or data from a mobile device under <u>forensically sound</u> conditions**.”
- Involves recovering data specific to mobile platforms.
- Can refer to any devices with internal memory and communication, like smartphones or GPS devices.
- There are multiple methods / tools for data extraction, and no single method is best.

Mobile Operating System Market Share

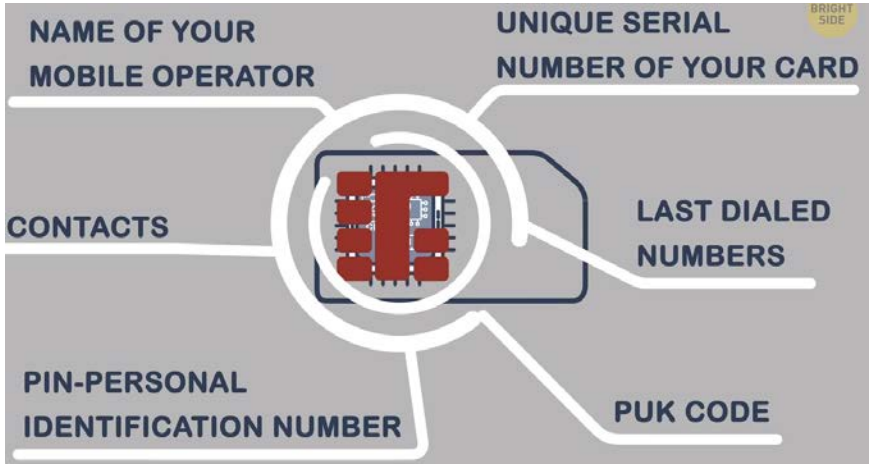


https://netmarketshare.com/

Overview of Mobile Forensics

- Originated in Europe and focused on the GSM SIM card. Roaming of Devices from Network and Radio Frequency Required (Identity Info on SIM) – Also SMS, Phonebooks, and Last dialed numbers.
- Terrorists use mobile phones to detonate IEDs.

  - To examine and analyze batteries and electric wires discover particular types of containers, wrappings, fuses, or circuits used by specific terrorists.
- With increased the demand, Mobile 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.

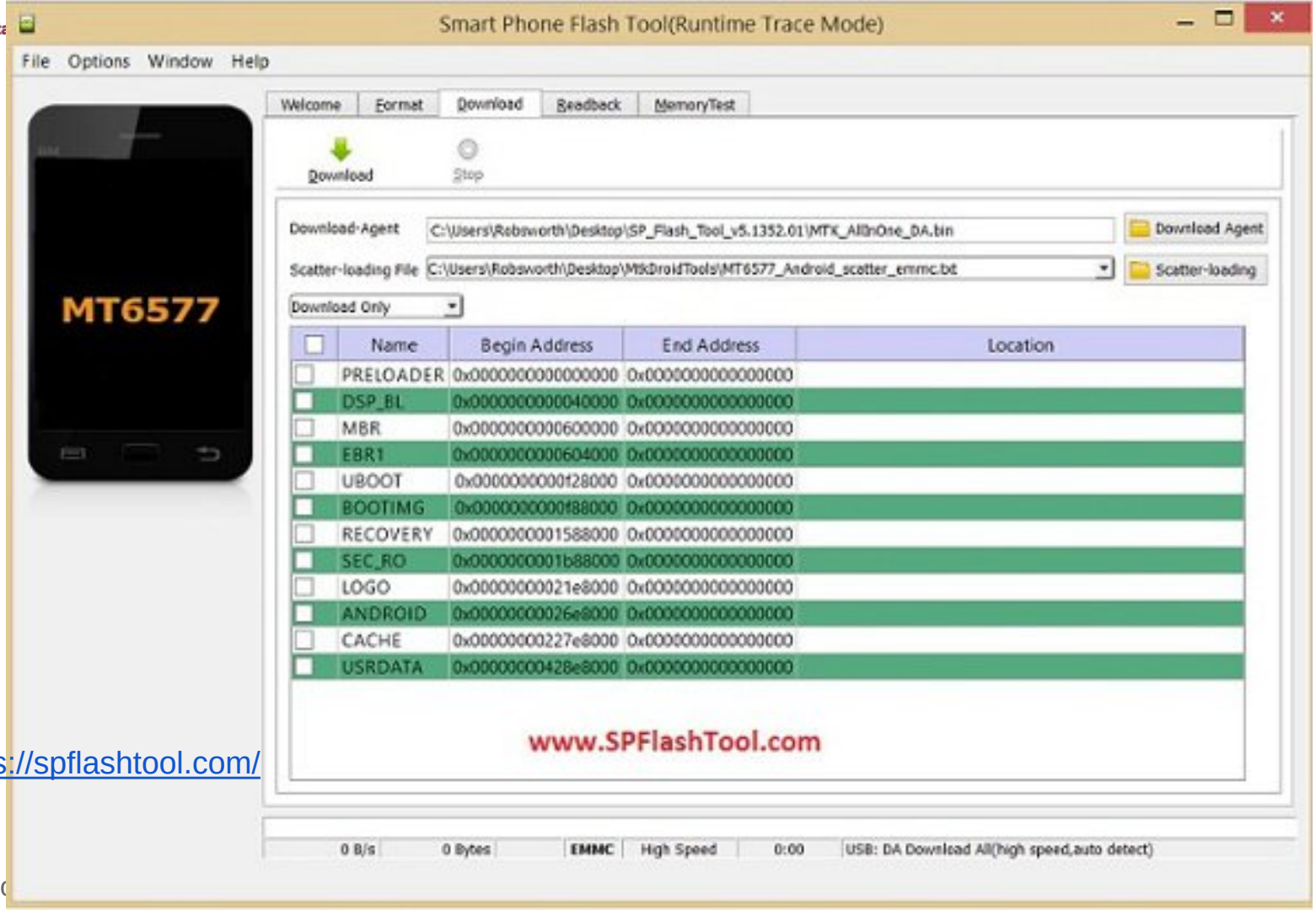

NAME OF YOUR MOBILE OPERATOR
UNIQUE SERIAL NUMBER OF YOUR CARD
CONTACTS
LAST DIALED NUMBERS
PIN-PERSONAL IDENTIFICATION NUMBER
PUK CODE

Brief History (1)

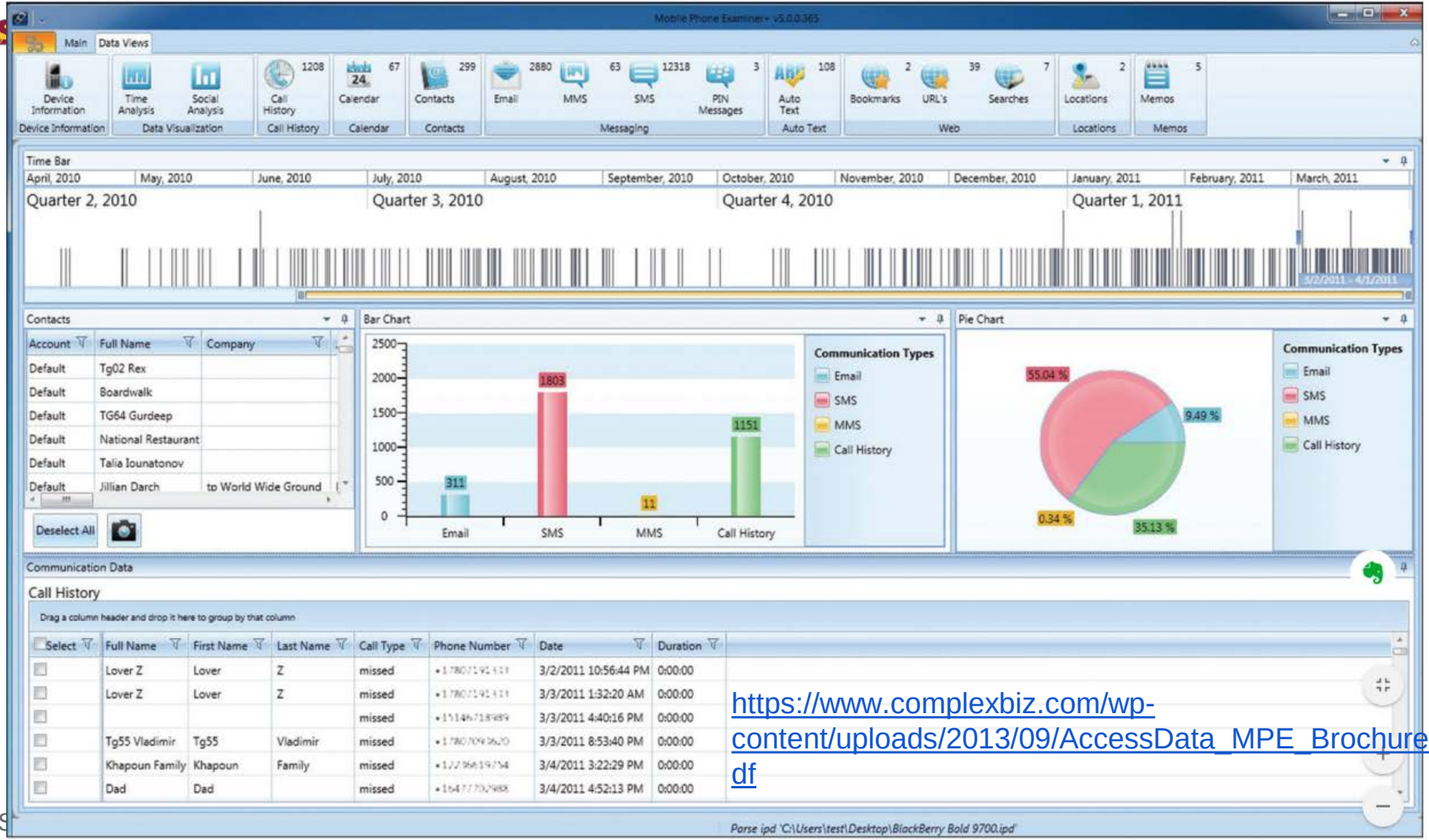
- Mobile Forensics recognized as a subset of Computer Forensics in late 90's / early 2000's.
- Early Examination Methods:
  - Manually operating through the devices – Became more challenging with complex devices.
  - Using synchronization software – Unable to recover deleted data.

Brief History (2)

- More Modern Examination Methods:
  - Use of OEM flash tools
    - Debugging, Overwriting non-volatile memory (ROM), copying the memory.
    - Potentially compromise data integrity.
    - Ex. Samsung Kies, SP Flash Tool, Odin, Emma
  - Use of Automated Commercial / Specialized tools
    - Little risk of losing data integrity
    - Can recover deleted data
    - Ex. Belkasoft Evidence Center, MPE+ (Access Data)



https://spflashtool.com/



https://www.complexbiz.com/wp-content/uploads/2013/09/AccessData_MPE_Brochure.pdf

Demo

- How to Create a Forensic Image of Android Phone using Magnet Acquire
  https://www.hackingarticles.in/how-to-create-a-forensic-image-of-andorid-phone-using-magnet-acquire/
- CalPoly Android Image
  https://www.dfir.training/resources/downloads/ctf-forensic-test-images/more-images/1684-calpoly-android-image

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.
  - Imaging the static storage devices
- Mobile Forensics:
  - Major Operating Systems: Android, iOS, etc (frequently updated)
  - Imaging the dynamic and various systems: contacts, SMS, phots, videos, logs of call, sensors, camera, and various communication tech.
- Mobility Aspect:
  - Phones are live things roaming around and constantly communicating.
  - Easy to be contaminated and hard to be isolated
  - Frequently changed: operating system file structures, data storage, services, peripherals, and even pin connectors and cables
  - Not only the types of data but also the way mobile devices are used constantly evolve.

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 Dialed (sometimes, not always, depends on the phone)
  - SMS: Text Messages, Sent, Received, Deleted, Originating Number, Service Center (also depends on Phone)

SIM Personalize tools(Copyright: GreenCard Co.,Ltd Ver 3.1.0)

Reader(PC/SC): | Refresh | Read Card | Write Card | Save Data | Load Data | Exit

Batch Write Card

APDU | Data File: | Select File | / | Go | First | Prev | Next | Last | Find | Continue | Template

Common Parameter

ATR: 3B9F96801FC78031E073F62113674D45150049070182 | Type: | Language: English | ... | ADN

ICCID: 8901260645139937443F | Inc (DEC20) | PIN1: 1234 | PUK1: 88888888 | PIN2: 1234 | PUK2: 88888888 (ASC8) | ADM: 3838383838383838 (HEX16/8)

GSM/WCDMA/LTE | CDMA/EVDO/CSIM

GSM Parameter

IMSI18: 809310260[redacted] | IMSI15: 310260643993744 | Inc (DEC18/15)

ACC: 0010 | Input (DEC4) | AD: 00000003 | ...

Inc KI: 8BAF473F2F8FD09487CCCBD7097C6863 (HEX32)

PLMN: 310320; 31032; 311040; 31104; 310020; 310450; 310410; 310150; 31(| ... | Auto

EHPLMN: | ...

FPLMN: | ...

HPLMN: 01 (HEX2) | GID1: 534D | GID2: | (HEX)

SMSP: +12063130004 | MSISDN: 18084629288 | Inc (ASC)

SPN: | (ASC)

ECC: 911; 112 | ...

Algorithm: Comp128-1 | Comp128-2 | Comp128-3 | Milenage

Other files | Same with LTE

LTE/WCDMA Parameter

IMSI18: 809310260[redacted] | IMSI15: 310260643993744 | Inc (DEC18/15)

ACC: 0010 | Input (DEC4) | AD: 00000003 | ...

Inc KI: 8BAF473F2F8FD09487CCCBD7097C6863 (HEX32)

OPC: E734F8734007D6C5CE7A0508809E7E9C (HEX32)

OP: | (HEX32)

PLMNwAct: 310260:4000; 310260:8000; 310260:0080 | ...

OPLMNwAct: 46000:4000; 46000:8000; 46000:0080; 45412:4000; 45412:8000; 4541 | ... | Auto

HPLMNwAct: 46000:4000; 46000:8000; 46000:0080 | ...

EHPLMN: 46000; 46007; 46002; 46008 | ...

FPLMN: 46001; 46003; 46004; 46020 | ...

HPPLMN: 50 (HEX2) | GID1: | GID2: | (HEX)

SMSP: + (ASC) | MSISDN: | Inc (ASC)

SPN: CMCC (ASC)

ECC: | ...

Algorithm: Milenage | XOR | R&C Para | Other files | Same with GSM


Store No: 2224012
SIM Card
Micro SIM
Nano SIM

What data is obtainable?

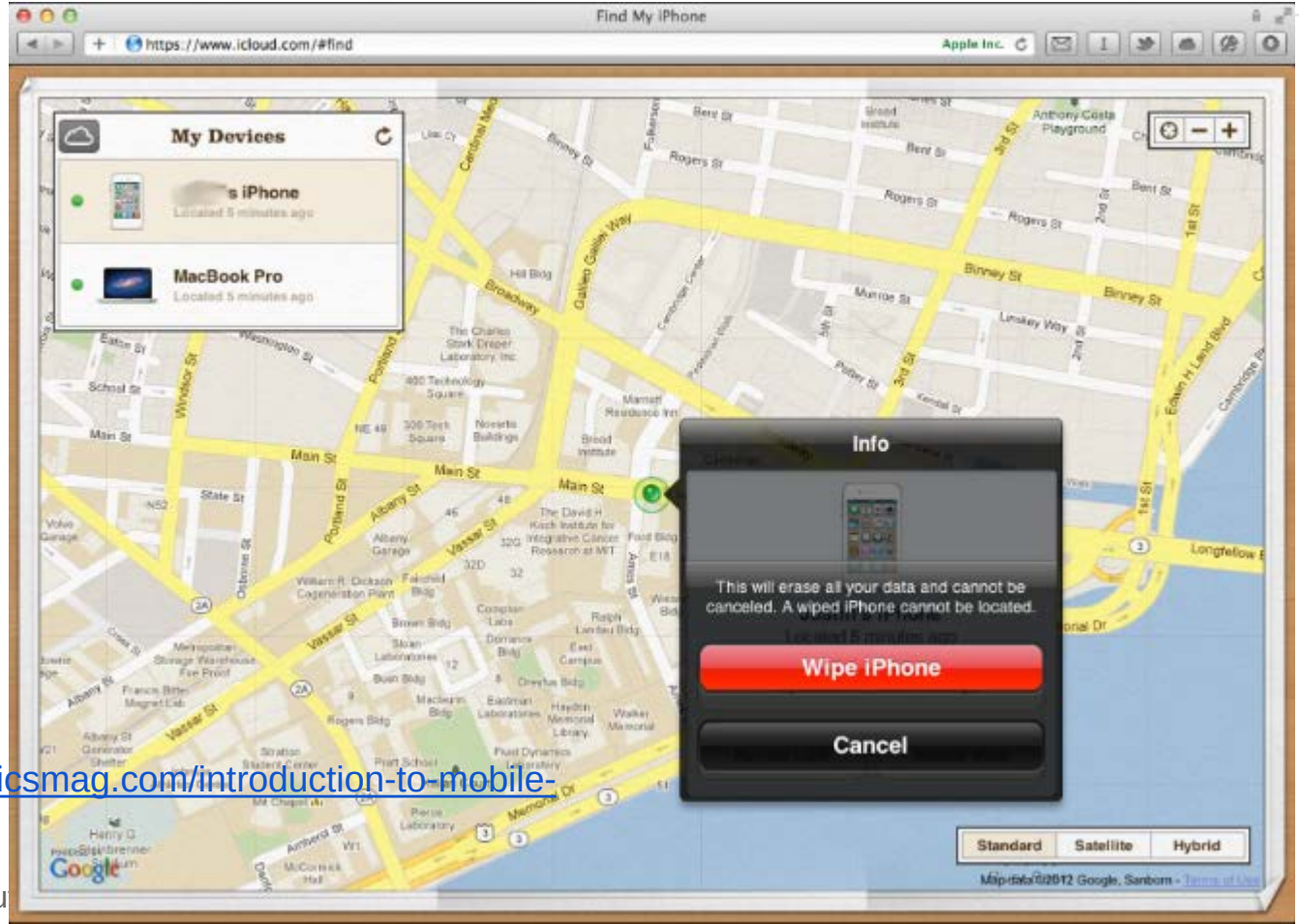
- Phonebook
- Call History and Details (To/From)
- Call Durations
- Text Messages with identifiers (sent-to, and originating) Sent, received, deleted messages
- Multimedia Text Messages with identifiers
- ***Photos and Video (also stored on external flash)***
- Sound Files (also stored on external flash)
- 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

Challenges in Mobile Forensics Process

- Investigator does not alter device state after seizure to ensure data integrity.
  - Suspect uses remote wipe to erase evidence.

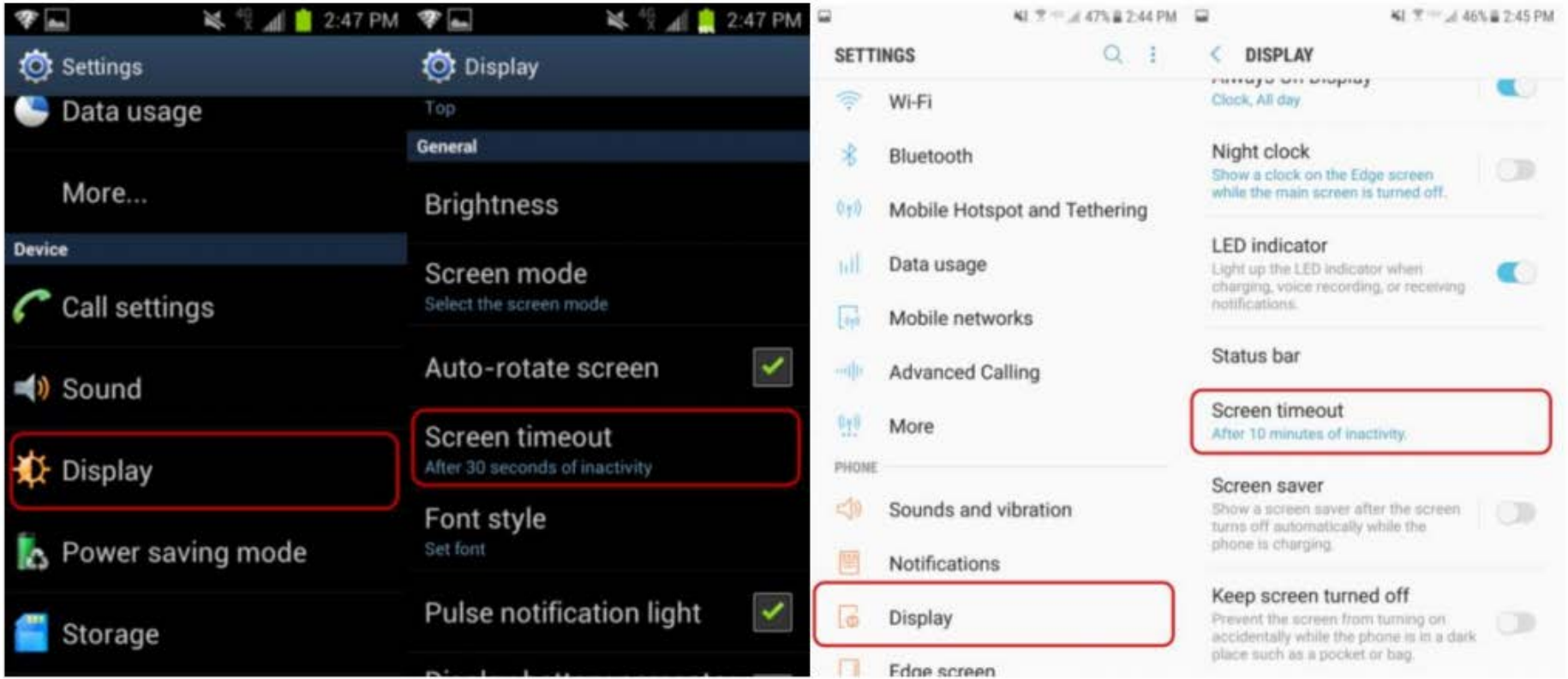
- Investigator uses Faraday Bag to block communications
  - Battery is drained causing device to power down.
- Investigator switches device to Airplane mode.
  - Network isolation

Remote wiping command of an IPhone



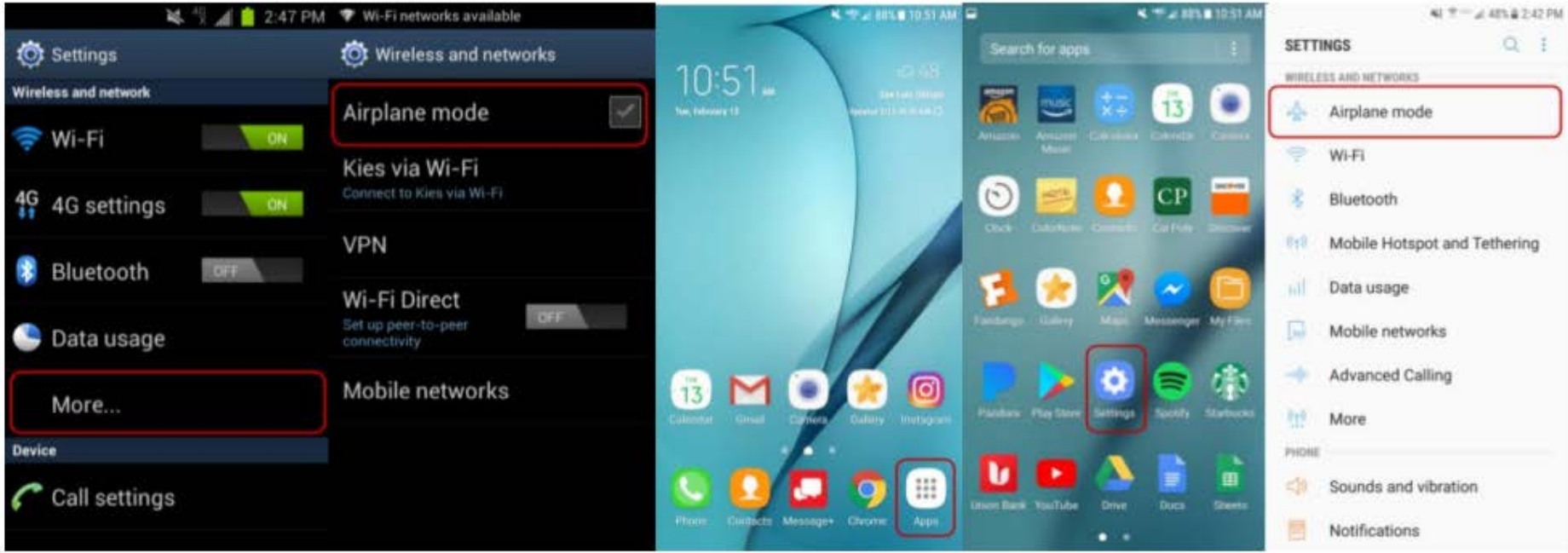
https://eforensicsmag.com/introduction-to-mobile-forensics/

Authentication for accessibility



https://cci.calpoly.edu/2019-digital-forensics-downloads

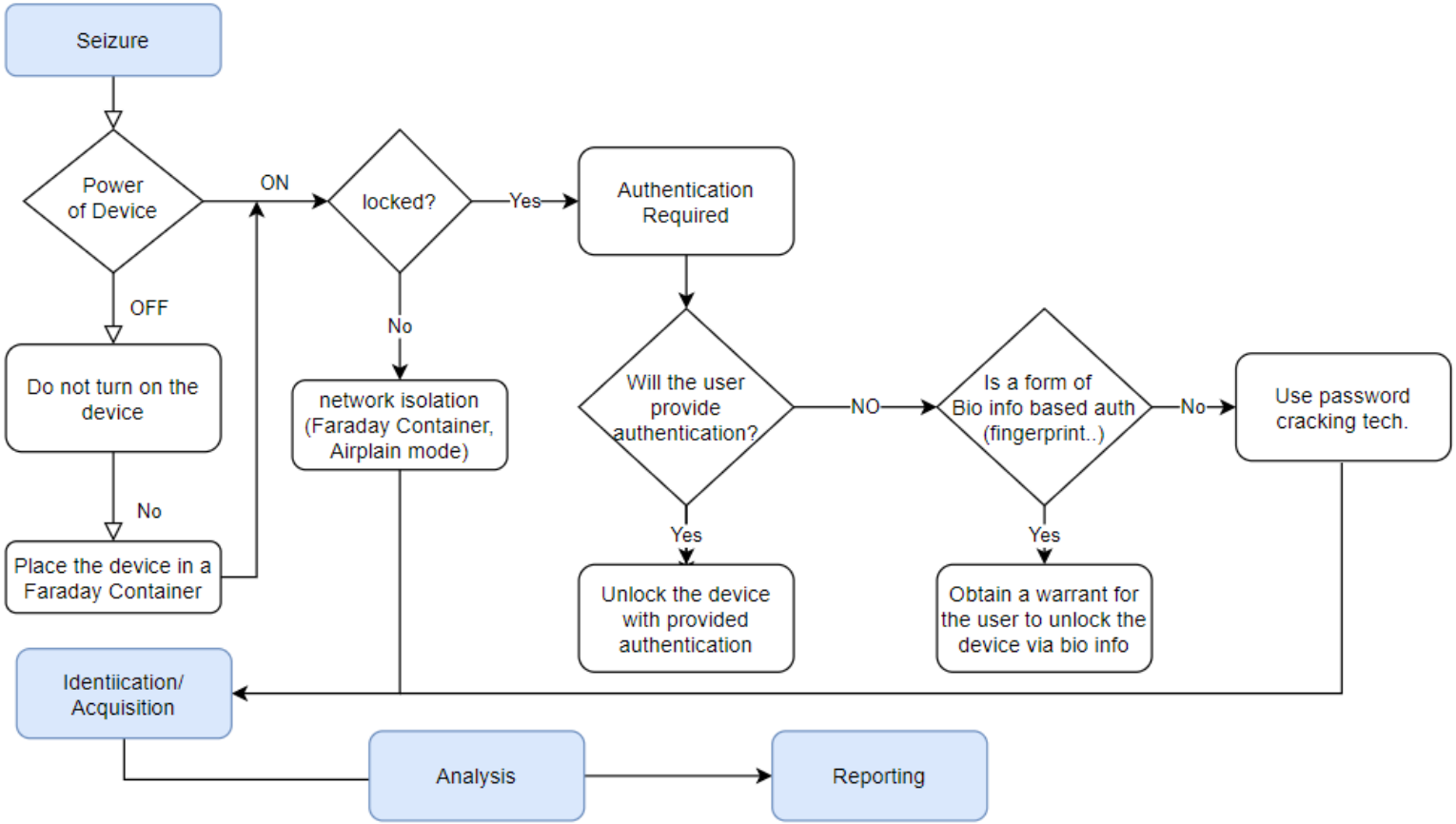
Network Isolation



https://cci.calpoly.edu/2019-digital-forensics-downloads

Device Cables

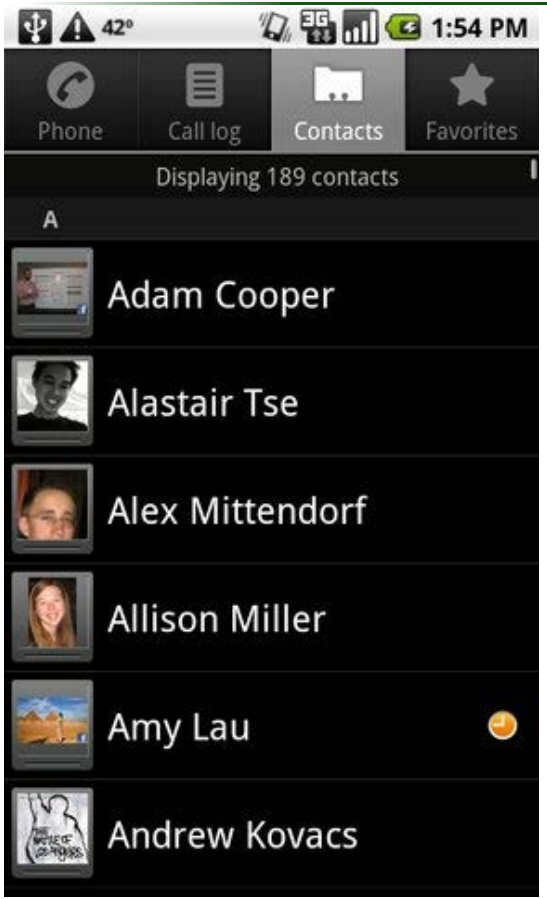
Mobile Forensic Process

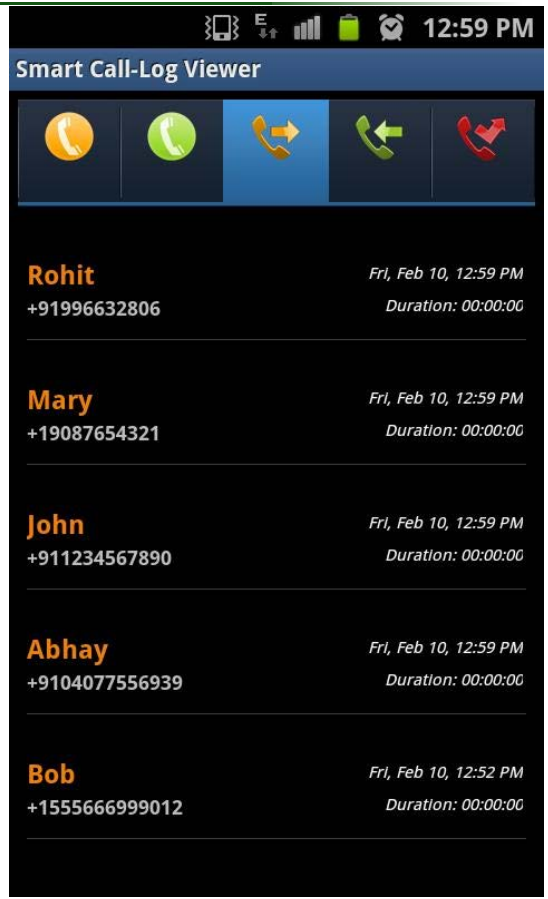


Acquisition Techniques

- Manual Acquisition:
  - Manually interfacing with the device.
- File System (logical) Acquisition:
  - Can obtain targeted subset or deleted data of logical (partition) storage 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(logical) Acquisition

- File System
  - diagnostics
  - filesystem
    - private
      - HFSMetaImg.sparsebundle
      - Library
        - Logs
        - Preferences
          - SystemConfiguration
      - var

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: JTAG

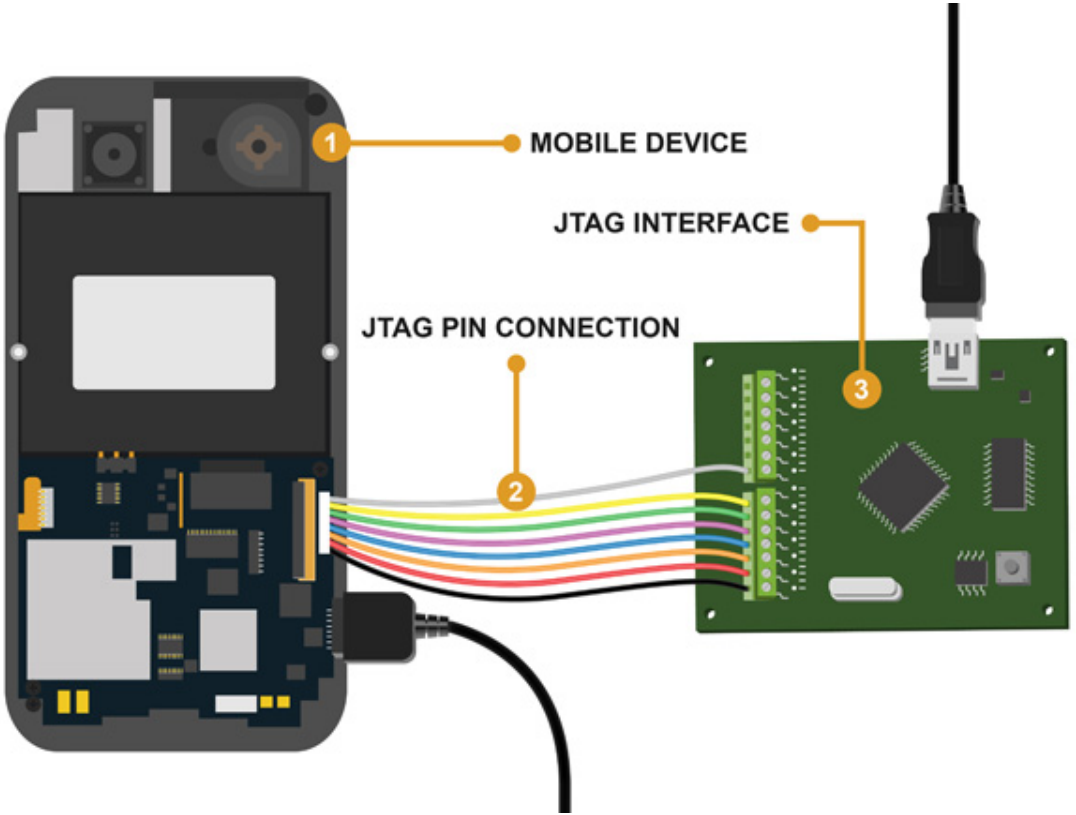
(Joint Test Action Group)

- An advanced level data acquisition method which involves connecting to Test Access Ports (TAPs) on a device

IEEE Std. 1149.1

- Instructing the processor to transfer the raw data stored on connected memory chips.
- Used for programming, debugging and extracting fully physical image from faulty devices.

JTAG is more than debugging and programming



https://www.datarecovery.co.za/faq/what-is-jtag.html

Physical Acquisition

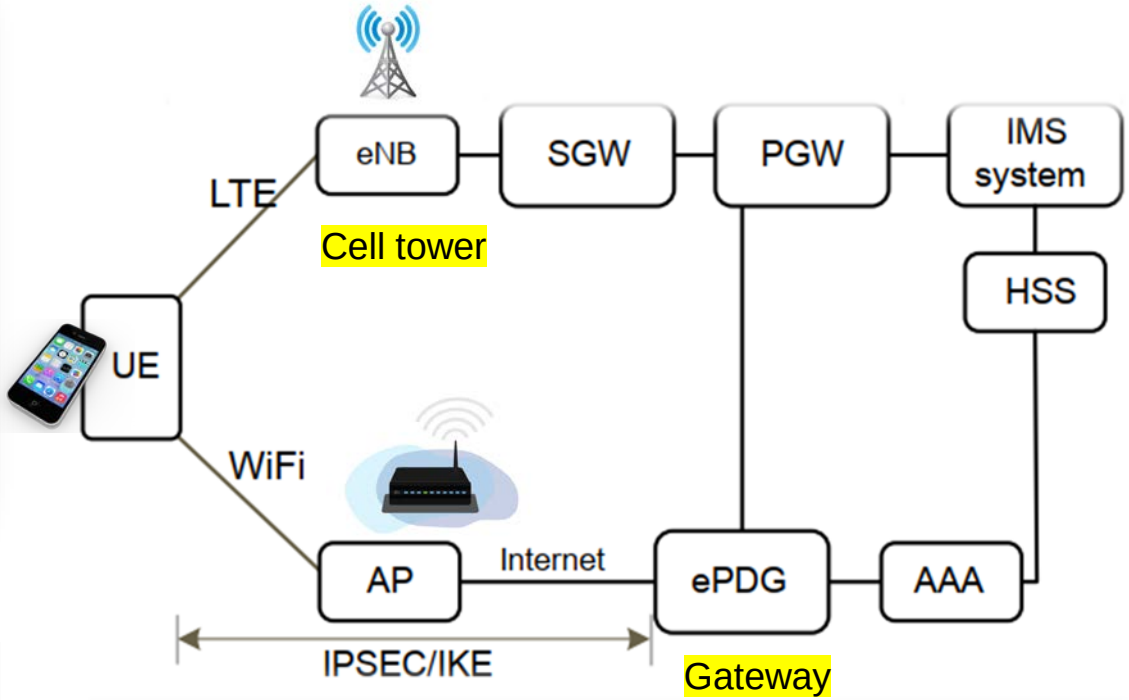
memory.img

Dec | Text search

Go To Offset | Find

```
6F 3A 69 76 61 6C 65 6E 7A 75 65 6C 61 3E 20 28 24 29 20   ael-Valenzuela-Espejo:ivalenzuela> ($)
6E 74 65 72 6E 65 74 20 63 6F 6E 6E 65 63 74 69 6F 6E 73   netstat -na.Active Internet connections
0A 50 72 6F 74 6F 20 52 65 63 76 2D 51 20 53 65 6E 64 2D    (including servers).Proto Recv-Q Send-
20 20 20 20 20 20 46 6F 72 65 69 67 6E 20 41 64 64 72 65   Q  Local Address          Foreign Addre
70 34 20 20 20 20 20 20 20 30 20 20 20 20 20 20 30 20 20   ss        (state).tcp4       0      0
20 20 20 2A 2E 2A 20 20 20 20 20 20 20 20 20 20 20 20 20   *.24745                *.*
20 20 20 20 20 30 20 20 20 20 20 20 30 20 20 31 39 32 2E         LISTEN.tcp4       0      0  192.
31 33 2E 32 37 2E 32 32 33 2E 32 32 33 2E 38 30 20 20 20   168.0.10.50173     213.27.223.223.80
20 20 20 30 20 20 20 20 20 20 30 20 20 31 39 32 2E 31 36      LAST_ACK.tcp4       0      0  192.16
2E 32 37 2E 32 32 33 2E 32 32 33 2E 38 30 20 20 20 20 20   8.0.10.50172     213.27.223.223.80
```

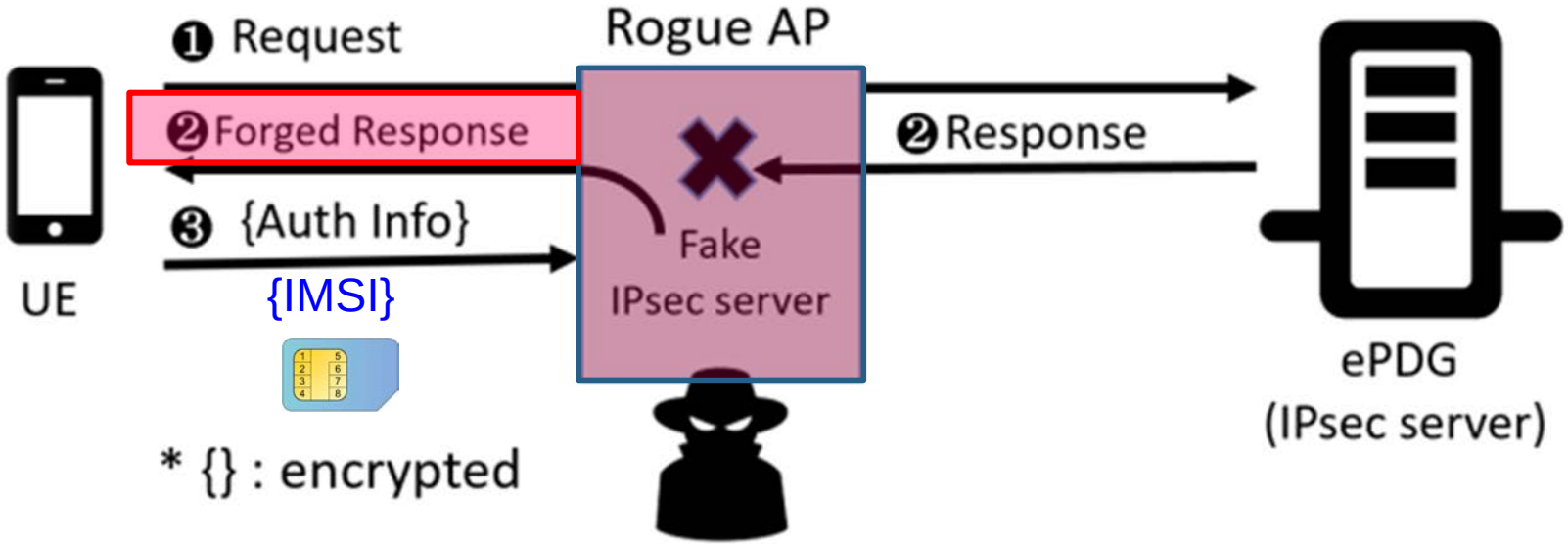
Analysis case in Wi-Fi calling



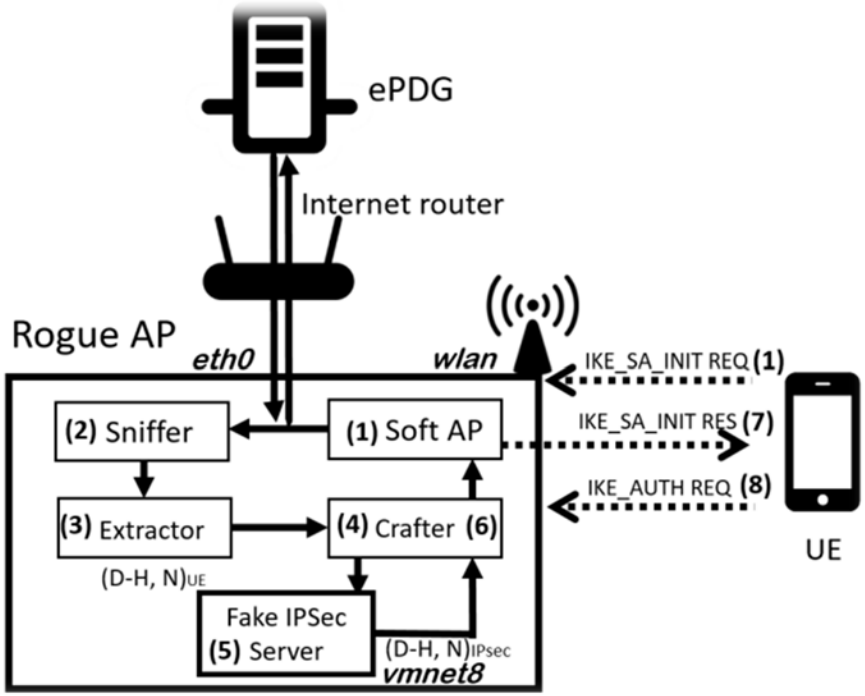
≠

Acquisition of IMSI

International Mobile Subscriber Identity



Rogue AP Components and Attack Flows



Decrypted packet sample (T -Mobile)

```
Exchange type: IKE_AUTH (35)
Payload: Encrypted and Authenticated (46)
   Initialization Vector: 94c8d09f9948e4eb0890bca2ba0c1299 (16 bytes)
   Encrypted Data (336 bytes) <AES-CBC-256 [RFC3602]>
   Decrypted Data (336 bytes)
      Contained Data (323 bytes)
         Payload: Identification - Initiator (35)
            ID type: ID_RFC822_ADDR (3)
            Identification Data:0310260xxxxxxxxx@xxx.mnc260.mcc310.XXXXX
         Payload: Certificate Request (38)
            Certificate Type: X.509 Certificate - Signature (4)
            Certificate Authority Data: 88eef7b9d185ac98b94b493764f589eb92
         Payload: Identification - Responder (36)
            ID type: KEY_ID (11)
            Identification Data:
               ID_KEY_ID: xxxxx
         Payload: Security Association (33)
         Payload: Traffic Selector - Initiator (44) # 1
         Payload: Traffic Selector - Responder (45) # 1
         Payload: Notify (41) - HTTP_CERT_LOOKUP_SUPPORTED
```

IMSI

APN

Resources

Demo: https://youtu.be/-ilGLXSqwPA
Open source: https://github.com/sefcom/Wi-Fi-Calling-source-code