Post 1

Friday, January 25, 2019 12:12 AM

MOBILE DEVICE FORENSICS: CH1 NOTES

May 27, 2018 Moo Comments 0 Comment

Myth: Mobile devices don't contain much relevant and transactional data than a personal computer

History	Initiated by Bell Labs in 1946 in St. Louis Missouri **1973: Martin Cooper/Motorola** • Built a device to enable people to walk/talk in street w/out attached wires • **April 3:** Demonstrated mobile phone w/call to Joel Engle @Bell Labs (Motorola's main competitor) ○ Call routed via base station Motorola installed atop Burlingham House into ATT landline system

DynaTAC 8000x (DYNamic Adaptive Total Area Coverage)

- **Portable phone:** Allowed usrs to call another portable/landline/radio phone
- Approved by FCC: Sep. 21, 1983: Offered commercially 1984
- Weight: 2.5lbs (mostly battery)
- First talk approx. 20 minutes: Took 10 hours to charge bet. Use: Ranged from $2,000-$4,000

1984: Car phone: Offered better transmission/reception b/c/constant battery

Bag phone: Labeled b/c it could be carried in zippered big: Device capable of being removed from vehicle

1989: Motorola MicroTAC released: Smaller than DynaTAC but still costly

1996: Motorola StarTAC released: Changes happened: $1,000

- Sizing changes started to occur in mid/late 90's

Data Evolution: Need to send messages typed in QWERTY KB

- **SMS (Short Message Service)** born
- Limit 140 chars: Still the limit today

Concatenated SMS or PDU (Protocol Data Unit) mode SMS: More widely used

- 160 chars by changing 8 bits per char to 7
- Killed off pagers

Walkie-Talkies: Donald L. Hings: 1st used as portable field radio: Pilots flying around Canada

- **1937**: 1st walkie-talkie: Hings referred to as '2-way radio'

Storage Evolution:

Nonvolatile data: Data that would exist w/out constant power onto device's mem chip was not possible initially

- Data visible on devices wouldn't be stored: Device shut down? Data gone

TDMA	**Time Division Multiple Access** When US began to transition to GSM: Global Systems for Mobile Comm: • Device info: Phone book/SMS could be stored onto **SIM: Subscriber Identity Module** • Already popular in EU • Storage areas: Contacts/SMS/Last #'s dialed already built into SIM standards dev. by ETSI **ETSI: European Telecomm Standards Institute:** Data could be written to/stored to smart chip • Sim cards: Already storing data: Used in auth process: Added values that stored contacts, SMS/last # dialed • Already used as 'key' to cellular network **TDMA devices:** Could store set # of contacts: Limited # of SMS (15-25) could be re-read **NVM: Nonvolatile memory:** Data could be stored/saved if device turned off w/SIM/battery was rem **Visor PDA:** Volatile mem/mobile devices: 8MB of RAM: Didn't store data if no power supplied

Mobile Devices in Media: 2014: Pew Research Center reported 90% of US adults owned a cell phone: 135 million users

Write Blockers/Mobile:

Write blocker: SW/HW device that stops specific comm from computer to mass storage device

- Many diff types

SW based: Can use simple Win Registry change

HW based: Sophisticated boxes that are coupled to examination device via cable attached to other side

- Some allow connection directly to pins on drives conducting forensic analysis
- Others have USB connections to plug removable USB/flash drives into available ports

HW tools: Can be used to protect disk access through interrupt 13 BIOS int of PC

- Mass storage device attached to HW write blocker: IO cmds sent from PC monitored
- Any cmd that could modify HDD aren't passed onto it: Intercepted by write-blocking device

SW Tools: Also block writing to attached drives plugged into USB drive/mounted drives/by classes

- Can be changed by editing Registry of Win PC/using SW tools
- Write blocker: Acts as traffic signal to data: Requests made by PC/processed
- If request to write data to protected device on other side of write protector is made
    - Stopped/not allowed to reach device
- Not considered forensically sound but employment process is

P2K Commander: Free tool for browsing Motorola PK device/FS/SW

Data Transfer to Forensics: Mobile sync SW enables usr to add/del items such as contacts/calendars from device

- SW/HW no diff from sync SW, with 1 exception: Write/Transfer button or selection not enabled

- Devices/apps simply allowed data to be read from device not written to it

Processes/Procedures: Examiners must have a set in place: An automated tool w/out direction could be detrimental

AMPS/NMT/TACS: 1980’s:

AMPS	**Advanced Mobile Phone System**: Analog standard used in US • Transmission: Operated in **800MHz band** bet **824 – 894MHz**
NMT	**Nordic Mobile Telephone:** Analog standard in Nordic countries • Transmission: **450 – 900MHz**
TACS	**Total Access Communication Systems:** Analog standard in UK • Transmission: **900MHz**

Transmission/reception of data ranged from 20kHz-50Hz for no collision

Later termed 1G: First Generation cell phone transmission technology

TDMA/GSM/CDMA: Code Division Multiple Access: 2G tech

- Handheld wireless scene 90’s

Main standards for 2G:

- GSM
- IS-95: Interim-Standard
- IS-136 (digital amps)
- iDEN

iDEN: Integrated Digital Enhanced Network

- Biggest change was analog to digital w/2G: Digital encryption of transmission
- 1st commercial 2G network on GSM: Made available by Radiolinja: Finnish operator
- Brought ability to send data other than voice over wireless networks

SMS born: 1st txt reportedly sent from PC to mobile device December 1992: Neil Papworth to colleagues at Vodafone

- Said MERRY CHRISTMAS
- 2G to 3G progression slow

2.5G: GPRS: General Packet Radio Service: Improved network stability

2.75G: EDGE: Enhanced Data rates for GSM Evolution: Improved speed of transmission

UMTS/CDMA2000

UMTS: Universal Mobile Telecommunications System and **IS-2000 (CDMA2000):** 3G cellular systems

- Established by specifications outlined in **IMT-2000: International Mobile Telecomm**
- Introduced large gains w/Internet access/video/data streaming: Early 2000’s
- **3GPP: 3G Partnership Project: Standardized UMTS: Uses W-CDMA: Wide-Band for transmission: EU/CH/JP**
- **3GPP2: Standardized CDMA2000: Uses EV-DO: Evolution-Data Optimized for transmission: US/NA/SK**

UMTS upgraded to HSDPA: High-Speed Downlink Packet Access: Combined w/**HSUPA: High-Speed Uplink Packet Access**

- **Formed: HSPA: High Speed Packet Access**: Still most widely deployed tech globally
- 3.5G debated as HSPA+LTE: Long-Term Evolution
- LTE mentioned w/regard to 4th by ITU to call it 4G: 1st commercial LTE networks launched in Norway/Sweden 2009

LTE-Advanced: Defined by ITU and is a true 4G system: Standardized 2010: 3GPP

- Dependent on infrastructure of underlying cellular network
- Also dependent on processes w/in mobile devices

SIM: Subscriber Identity Modules: SIM cards

- Developed to enable portability/store info to enable auth on cellular network
- Auth here: Meant device could register/allow usrs to make/receive calls
- SIM card acts as key to network: Usr could switch equip by rem smart chip/inserting into diff GSM device
- Storage made it easy to move: Amt of data that can be stored determined by GSM standards

SIM not the same as a USIM: Universal Subscriber Identity Module: USIM is an application on the UICC

- USIM app enables mobile device to be identified on UMTS, HSPA, LTE sys
  - Also contain SIM app: Allows for backwards compatibility to 2G
- May also contain another app called **CSIM: CSMA SIM**
  - Allows access to CDMA networks/an app called ISIM

ISIM: IP-Multimedia Subsystem SIM: Allows for secure use of IP/backbone of LTE

- Support for VoIP/SMS/Emergency
- CDMA SIM cards called **R-UIM: Removable User Identify Module cards**
- Contained primitive ver of CSIM app/SIM app for GSM

Media Storage Cards: Created in effort to expand avail storage for mobile
4 diff types:

- **SDSC: Standard-Capacity**
- SDHC: High-Capacity
- SDXC: Extended-Capacity
- SDIO: Input/Output

Four types come in 3 diff form factors

- **Original:** 32 x 34mm
- **Mini:** 21.5 x 20mm
- **Micro:** 11 x 15mm

SDHC standard released in 2006: Supports capacity of 32GB: Micro most prevalent

SDXC: released 2009: Supports 2TB using MS exFAT FS: Some cards support up to 128GB

Many new devices: Especially Android: Have internal microSDHC and SDXC cards soldered to add storage

Mobile Device Backups:
Windows XP: \Documents and Settings\username\Application Data\Apple Computer\MobileSync\Backup\
Win Vista/7/8: \Users\username\AppData\Roaming\AppleComputer \MobileSync\Backup
Mac: ~/Library/Application Support/Mobile Sync/Backup/
Blackberry:
Windows: My Documents\BlackBerry\Backup
Mac: /Users/username/Documents/BlackBerry Backups
Depending on ver of BlackBerry SW used to create backup: File will have .ipd or .bbb extension

- **.ipd** Will have files created w/earlier ver of BB Desktop Manager (up to ver 6)
- **.bbb** Created by BB Desktop Manager 7/new Link SW: Fully encrypted

BES: BlackBerry Enterprise Server: 1st platform allowed enterprise to store data from mobile to central loc

Educational Resources:
www.phonescoop.com
www.gsmarena.com

From <https://www.piratemoo.net/moosings/mobile/mobile-device-forensics-ch1-notes/>

Post 2

Friday, January 25, 2019 12:13 AM

MOBILE DEVICE FORENSICS CH2

June 3, 2018 Moo Comments 0 Comment

Phys img of HDD/storage device: Practitioners refer to obtaining every bit/byte from 1st/last sector: Exact copy of media is truest

Frye v US **293 F.1013**	Testimony must be based on scientific methods sufficiently established/accepted
Daubert v. Merrill Dow Pharmaceuticals **509 US 579**	Scientific knowledge: Established if it demonstrates conclusion • Product of sound 'scientific methodology' from scientific method Decision by Federal Rule of Evidence 702: Rests on shoulders of trial judge

Greatest impedance: Overcoming/recognizing write-protected devices ineffective to protect integrity of evidence

Computer Forensics Defined

IACIS	**International Association of Computer Investigative Specialists:** Volunteer non-profit corp **Grants CFCE: Certified Forensic Computer Examiner certification** • Doc describes forensics: Acquisition/reconstruction/examination/analysis of data stored on electronics • Pre-exam/legal issues/comp fundamentals • Partitioning schemes/Win FS's/data recovery/Win artifacts/presentation of findings **Required**: 7 competency areas: Obtain peer review/conduct practical exams/pass written exam
ISFCE	**International Society of Forensic Computer Examiners:** Private org: Research/dev of new/emerging tech in forensics **Grants CCE: Certified Computer Examiner certification** • Competencies: Ethics/law/sw/hw ID/networks/OS/seizure/forensic exam procedures/FS's/media • Media geometry/prepare media for imging/boot disks/low-lvl analysis/processing issues/practical exam skills **Required:** Attend CCE boot camp from auth training/18 mos verifiable work/doc self-study in forensics by board

Seizure: Any investigation into electronic evidence: Must start w/legal seizure/received

ESI: Electronically Stored Information

- Proper legal steps determined by situation
- In place that search warrant must be obtained/perm must be given by owner/corporately owned?
- If data tainted by questions of legality, info collected dismissed in proceedings
- Exercise extreme care at onset

Collection: Extract data from device in manner that enables showing it didn't change/same as when collected

Presentation: Outline entire process, including problems encountered from seizure to analysis

Approach: Most computer examiners consider mobile forensics nonscientific b/c of single limitation

- Write blocker stops writes to mass storage device: Maintaining integrity of device from which img created
  - HW/SW switch inhibits writes to ensure data isn't overwritten/allows for a duplicate img of devices
  - Examiner can obtain hash of all data
- Isn't recognized as a mass storage device/write blocker can't be used: Some believe img must be labeled unreliable
- **When plugged in:** Devices initiate change in PC's OS: Recognizes device has been plugged in
- Makes changes to op to allow for comm w/computer
- **Can be tethered to computer using 7 means:** IR/BT/WiFi/serial/USB cable
- Connection will always need driver: **"bridges gap"** bet devices
- Drivers primary pain points for processing mobile device

Communication: Important: For mobile to be recognized/comm w/sys via driver: Has to be powered on

- **If device on:** Possible data constantly changing on device from cellular network/Wi-Fi
- Data in constant flux

Different protocols used for diff devices: Sometimes multiple protocols used depending on access needed

NIST:2008	**Forensic Filtering of Cell Phone Protocols** • Describes protocol filter: Can be applied to SW to intercept comm that poses risk to integrity • Contains valuable info how forensic tools combat limitations when a write-protection feature can't be used • Explains functionality of forensic device tools based on same protocols used by manufacturer mgmt tools
NIST: 2007	**Guidelines on Cell Phone Forensics:** Explains digital forensic community challenges to devices/investigations

Several objections to notion of a process in conducting device collections and thorough investigations

2 most prominent objections:

1. Lack of Time
2. Simplicity of tool = no training needed

Lack of time: Examiners began to incorporate word

- The excuse typically used in mobile forensics comm when it comes to a full exam/extraction of data from mobile device
- Attitude: Critical deficiency
- Hasty examination of digital data is like reading 1st/last chapters of a review

Simplicity of Tool Equates to no training needed:

- SW/HW tools have been designed/marketed to express to purchaser that little-to-no training is needed
- Inverse is true: The simpler the tool, the more training needed to testify about what is occurring
- Did DW on the device, once button pushed, query a DB to retrieve contacts/SMS?
- What DB did it query? Etc..

SOP: Standard Operating Procedure Document

- Cover not only person conducting exam: Those collecting/seizing device/holding data
- Outline process/procedures to be followed from seizure to reporting data
- Creating doc: 1st step
- SWGDE: Scientific Working Group on Digital Evidence: Maintains prior SOP:
  - Will assist in best practices for collecting/acquiring/analyzing/documenting data in digital examinations

Purpose/Scope

- SOP should outline purpose/scope of each possible loc at which device/collection could occur
- **Purpose:** WHY section/SOP being used to ID goal of section
  - Should be detailed so reader will recognize what doc/section will cover
  - 7 purpose statements can exist in a single SOP, only 1 purpose statement per SOP section
  - Can also explain what will be needed/covered in section
  - Clear/ID areas not going to be covered/outside scope of doc

Purpose	*Purpose of procedure is to seize/sec/collect digital data from mobile device at off-site location to maintain integrity of device/contents for further analysis/processing*
Scope	*SOP outlines process/procedures to follow when conducting mobile forensic assistance at off-site loc. SOP not training doc, but set of procedures to follow at off-site loc.*

Definitions: Should list/define all acronyms/tech words included in procedural part of SOP

Mobile	Portable devices use network comm/have digital storage capabilities: Cell phone/tablet
Mobile External media	Storage media: Examples: microSD/SD cards
Mobile Internal media	Storage media part of device: Soldered to internal components

Equip/Materials: Statement should include all items needed to accomplish procedure successfully: Cover every contingency

Equipment	The equipment that will be needed includes the following items: • Digital camera

	• Sterilized portable USB HDD • Media card write-blocking tools • RF shielding device • Mobile device collection tools • Mobile device cables/SIM card readers • Evidence packaging materials

General Info: To define limitations/BG info regarding performing duties outlined in SOP: Impt limitations should be clarified

- On-site/off-site seizures/collections

General info Limitations:	If device has network access: Data destruction can occur If device shut down/loses power: May lock, essentially eliminating further access If device locked on seizure: Further access might not be possible unless passcode obtained Some SW tools don't collect all data on device

Procedure: In procedure portion of SOP: Reader walked through performance of task

- Not exact process: Guide to best practices

Place device into airplane mode by navigating to Settings > Tools > Network > Airplane Mode

General: Scene should be sec/safe for all people: Protect devices/evidence contained on devices

- ID areas of scene to be searched
- Photograph area/each potential item of evidentiary value

Mobile Devices: Photograph device/any data on screen

- Block mobile device from receiving RF sigs: Airplane mode/RF shielding device
- If device can't be shielded: Device should be turned off: Packaged/submitted for processing asap

References/Documents: Should include other SOP's that are related to current SOP

Mobile Forensic Seizure On-Site Procedures

- Should cover procedures usrs will take preparing for arriving to site/scene where evidence related to device will be
- Cover equip/safety/ID of device/SIM cards/external storage/USB cables/manuals/loc of passwds/PIN

Img Collection On-Site Procedures	○ Should cover procedures if device img collected using forensic tools where usr is on site/scene ○ Equip needed to create forensic img/SIM/removable media/procedures for isolation
Img Collection Lab Procedures	○ Should cover procedures usrs should take for processing/analyzing device in lab setting ○ Steps required to complete isolation of device, depending on state received ○ Specifications for how device info should be obtained ○ Understanding capabilities prior to extraction ○ Guidance on what to do if device supports SIM/SW needed to conduct exam on SIM

Creation of a Workflow
Forensic SW: US-CERT: US Computer Emergency Readiness Team: Defines computer forensics as:
“The discipline that combines elements of law/computer science to collect/analyze data from sys/networks/wireless/storage in way that is admissible as evidence in court of law”

- SW app generic set of instr: Defined by 2 classes: sys SW/op-app SW
- **System SW:** Used by computer sys itself and doesn’t involve user [writing of data to disk/displaying graphic]
- **Application SW:** Facilitates tasks usr needs to perform his/her work [word processing/img creation/forensic examinations]

From <https://www.piratemoo.net/moosings/mobile/mobile-device-forensics-ch2/>

Post 3

Friday, January 25, 2019 12:13 AM

MOBILE DEVICE FORENSICS CH 3

June 4, 2018 Moo Comments 0 Comment

Lawful Device Seizure:

4th amendment: Protects from unreasonable search/seizure by gov't agent/priv citizen acting on behalf of gov't agent

- If person not acting on behalf of gov't: Using wiretap/electronic surveillance/search devices w/out consent LEGAL
  - Search/seizure by private citizens not covered by 4th
  - Citizens not immune from being sued for invasion of privacy by subject of search
- **Agents of gov't must comply with Fed/state/local law of personal property:** Must be lawfully authorized
- If seizure occurs w/out lawful auth: Any data collected not used in court/negates seizure

Chain of custody: Details in order, every piece of evidence: Seizure to disposition: Can play large role in civil cases

- Should be clearly in report that defines details

2 diff kinds of chains of custody:

1. Phys device
2. Data collected from phys device

Info gathered at scene might implicate guilt/innocence: Can be dismissed at trial b/c phys device wasn't properly seized

Lemons v. State	**298 S.W.3d 658 (Tex. Ct. App. – Tyler 2009)** • Even if consent given for call details, photos can't be observed • Used under consent given
US v. Finley	**477 F.3d 250 (5th Cir. 2007)** • Even though cell phone owned by company Finley worked for • Personal data stored on device • Reasonable expectation of privacy for data contained on device

Before Data Seizure: Answer questions

1. Search warranted not executed: Has device owner consented to search?
2. Search warrant executed: Is device included on original warrant?
3. Device included on warrant: Contents of device defined?
4. Corporate situation: Is device owned by individual/employer?
5. Corporate policy: Is one in place to allow collection/analysis?
6. Could device contain personal info?

4th Amendment Rights: Grants "right to one's privacy"

- Gov't/agents can't examine person's digital devices w/out court order/search warrant issued by judiciary
- **Africa:** Mobile contents subject to search only after agent receives

search warrant for contents
- **UK:** Malone v. UK: Numbers dialed by subject "protected telephonic comm" Any other data protected as well

Supreme Court/Mobile Device Data Seizure

2 cases: Lay foundation for changes in doctrine long used when conducting search of mobile device:

Riley v. CA	Stop for traffic violation led to Riley's arrest for weapons charge: Incident to arrest
US v. Wurie	**Wurie had been arrested/transported to station:** Officers rem device from arrestee • Noticed calls: Investigated number: Search warrant executed on residence • SCOTUS: Supreme Court of US: Decided data on device should be covered by same protection in 4th • Overturning both previous decisions

Warrantless Searches: Civilians can do things w/out warrant
- People may have expectation of privacy: If violated by an ordinary citizen, no 4th violation
  - As long as they didn't violate any laws to examine device
- Ordinary citizens don't need consent of party to extract data from mobile device: **Private search doctrine**

US v. Grimes	**244 F. 3d 375 (5th Cir. 2001)** • Private citizen searched computer w/out consent of owner • Recovered illegal pictures: Turned over to police • B/C citizen wasn't acting as agent of gov't: Search deemed valid: Recovery of data not suppressed
Chimel v. CA	**395 US. 752** • Search incident to arrest limited to immediate control of arrestee when officer's safety concern • Prevents destruction of evidence
US v. Robinson	**414 US. 218** • Used Chimel to explain search of pack of smokes found on arrestee was valid • Risks ID'd are always present in custodial arrests: Even when no concern for officer safety/loss of evidence
Arizona v. Gant	**556 US. 332** • **Deals w/search of vehicle:** Arrestee has access to passenger compartment/other places • Vehicle believed to be holding evidence of crime person arrested for • Law enforcement had precedent to extend search to mobile device incident to lawful arrest

Consent: Law enforcement officer can stop/search under reasonable suspicion based on "specific/arguable facts"

Terry v. Ohio	**392 US 1.** • Officer loc mobile on person's possession • Could req consent from person to look into device only if 7 conditions satisfied • Consent interesting exception to warrant
US v Meador	**2008 WL 4922001 (E.D. Jan. 7 2008)** • Parental consent to search mobile device owned by son: But could not be given
Smith v. State	**713 N.E.2d 338 (Ind. Ct. App. 1999)** • Gov't agents req to search vehicle for things but didn't specify mobile

	• Mobiles seized/suppressed at trial b/c exceeded scope of consent

When obtaining consent to search mobile: Must create doc that:

- Clearly details ownership
- Explains what to occur
- Lists tools to be used
- Provides outcome if illegal info recovered

Exigent circumstances: When not enough time to obtain warrant for fear of phys harm to govt agent/others

- Escape of suspect/destruction of evidence

US v. Parada	**289 F. Supp. 2d 1291 (D.Kan. 2003)** • Indicated b/c mobile limited storage: Possibility info contained on device could be del/overwritten • Search to retrieve data needed immediately to preserve evidence

Training today focuses on maintaining device in isolated state: Network connections not allowed

- Negates this type of exigency in most cases

US v. Morales-Ortiz	**376 F. Supp. 2d 1131 (D. N.M. 2004)** • Argued access had to be made to address book under exigent circumstances • Unlike Parada, which involved call logs, search/seizure wasn't justified

Abandoned/Lost Property: Murky waters

People v. Schutter	**249 P.3d 123 (2011)** • iPhone left in gas station bathroom/searched after business owner gave phone to police • Schutter returned to try to find device • Not looked at as lost/abandoned: Info agent recovered suppressed
State v. Dailey	**2010 WL 3836204 (Ohio Ct. App. 3 Dist, Oct. 4, 2010** • Person caught after shoplifting fled scene leaving behind jacket • Inside jacket was mobile: Later examined by agents • Discovered address book used to find suspect • Evidence allowed in trial since suspect abandoned property when fled

Location to Be Searched: Physical Location

- Legal doc to search phys place (residence/bus/site):
  - Affiant signs affidavit for warrant: Must describe phys place/addr/what should be searched for
- Info gathered after investigation/knowledge based on probable cause that items exist at loc/place defined

Affiant must explicitly define clearly:

- Color of home: Type of home construction (brick/wood paneling)
- Color of accents (shutters/trim/windows)
- Address
- Trees/toys/vehicles/front of residence/features unique
- What to be searched for once at location

Following info regarding place to be searched:

- Manufacturer
- Device model
- Serial number

- Color of device
- Type of cover for device
- Wallpaper visible on device screen/lock screen
- Presence of cam in front/back
- Presence of headphone jack: top/bottom/side
- Description of any specific details unique to device

Items to Seize: Scope dictated by type of event constituted search of device as described in affidavit

When specifying data to be seized from mobile follow guidelines:

- Research device/data types that can be loc on it: phonescoop /GSMarena can help loc usr data types
  - Manufacturer's site to ascertain types of data that may be contained
- Today's comm occur via 3rd party apps: Include seizure of this info
- Doc everyday life: Capturing bus docs/impt notes often done using device built in cam/mic.
  - Imgs/video/audio saved can be uploaded/transmitted via built-in media viewer: 3rd party app/NFC
  - Info to include not only transmission but reception is critical for collection
- Txt/multimedia msging can transmit/receive notes/passwds/keys/company info/threats/confessions/audio/etc..
- **PIM: Personal Information Manager**: Data can include call logs/contacts/cal/notes
- Including del data in all mobile warrant apps should be substantiated by type of data category (SMS/MMS/Apps)
  - Today's devices: Data on flash mem/nonvolatile flash mem stores data even if del by usr
  - Apps used by smart devices use DB files that can store data prev. del by usr

Data Volatility at Scene:

- Transmissions occur via radio waves: Can originate/terminate device via cell signal/WiFi
- Remote wipe sig can be sent to device
- Inhibiting reception of this sig ensures it won't be remotely wiped
- Isolation must occur immediately

Device Sec: 2 types can be enabled:

1. Usr auth device security
2. Data security

User auth sec: Passwds/PINs/passcodes/passphrases/patterns/biometrics: Each provide diff lvl of sec

- **Legacy devices:** Passcode of #'s and if SIM avail: Pin/**PUK: Pin Unblocking Key** can be used
- Smart phones can use locking device ranging from passcodes to biometrics

PINs/PUKs: Numbers comprising up to 8 digits: Typically 4 for PIN and 8 for PUK

- PIN unlocks SIM card

- PUK used to unblock SIM that has been PIN-locked

Device/storage encrypted? Harder to analyze

- **Android 5.0:** Data encryption turned on by default
- **iOS:** Data encryption by default/enable usr to force device to produce encrypted backup: 2nd passwd needed to decrypt
- **Win Phones:** Not capable of using Phone BitLocker encryption: Unless device managed
    - Device must be under Mobile Device Mgmt sys at enterprise lvl to allow encryption
- **BlackBerry:** Enable usrs to turn on encryption in settings/media card: 2nd passwd to decrypt

Consider obtaining sec keys from owner: Biometrics? Device must be unlocked by owner at loc device seized/sec measures rem

Backups: Valuable info can also be loc from backups

- **iOS:** Creates backup of data from device on comp which has been connected
- **BlackBerry/Win Phone/Android:** Can also backup data
- All these OS's can also encrypt info that has been backed up

From <https://www.piratemoo.net/moosings/mobile/mobile-device-forensics-ch-3/>

Post 4

Friday, January 25, 2019 12:13 AM

MOBILE FORENSICS: CH 4 NOTES

June 5, 2018 Moo Comments 0 Comment

Before Seizure: Understanding Mobile Comm
Active device: Attached to 7 networks: Can allow outside comm to int w/phys collection/extraction
Cellular Comm: 7 factors RF used affect way team/examiner rem possibility it will initiate/receive comm during/after seizure

- Switch device off/Airplane mode
- Wrap device in material that blocks cellular sig
- Place device in radio isolation box
- Large radio isolation room completely devoid of win/lined w/special copper wallpaper

Radio isolation techniques: Michael Faraday: 1836: Faraday cage

- Faraday: 1791-1867: Scientist who discovered electrically charged particles approach metal object
- Cage shields items inside cage from static electrical fields
- All electrostatic charges/electromagnetic radiation distributed across exterior of cage
- Blocks electric charges/radiation from entering cage
- Similar devices/bags can be used to block RF sigs from reaching mobile

Device Frequencies:
True 4Gmust use FDD: Frequency Division Duplexing | TDD: Time Division Duplexing LTE: Long-Term Evolution

- FDD LTE: Globally more carriers || TDD: Gaining carriers: China/Middle East
- Newer smart phones beginning to use both freq for comm
- **LTE frequency bands: Extended to 44 w/addition of TDD-LTE**
- **Band 43 in LTE spectrum: 3600 – 3800 MHz**
    - Not covered by a lot of isolation bags/enclosures

FDD LTE Bands/Frequencies: Freq. Allocation Table

LTE Band	Uplink (MHz)	Downlink (MHz)
1	1920-1980	2110-2170
2	1850-1910	1930-1990
3	1710-1785	1805-1880
4	1710-1755	2110-2155
5	824-849	869-894
6	830-840	875-885
7	2500-2570	2620-2690

8	880-915	925-960
9	1479.9-1784.9	1844.9-1879.9
10	1710-1770	2110-2170
11	1427.9-1452.9	1475.9-1500.9
12	698-716	728-746
13	777-787	746-756
14	788-798	758-768
15	1900-1980	2600-2620
16	2010-2025	2585-2600
17	704-716	734-746
18	815-830	860-875
19	830-845	875-890
20	832-862	791-821
21	1447.9-1462.9	1495.5-1510.9
22	3410-3500	3510-3600
23	2000-2020	2180-2200
24	1625.5-1660.5	1525-1559
25	1850-1915	1930-1995
26	814-849	859-894
27	807-824	852-869
28	703-748	758-803
29	NA	717-728
30	2305-2315	2350-2360
31	452.5-457.5	462.5-467.5
32	Downlink only	1452-1496

TDD LTE Bands/Freq: Freq Allocation Table

LTE Band	**Allocation**
33	1900-1920
34	2010-2025
35	1850-1910
36	1930-1990
37	1910-1930
38	2570-2620
39	1880-1920
40	2300-2400
41	2496-2690
42	3400-3600
43	3600-3800
44	703-803

Bluetooth Comm: Usr can move data bet mobile/PC: Attach headsets/headphones/speakers to device

SANS research paper *"Dispelling common Bluetooth Misconceptions"*

- Orgs consider BT short-range **BUT class 1** devices op in ranges typical of wireless: **100 meters (328 ft)**
  - To op at that: Class 1 device would have to be at both ends of comm
- Today's mobile: Android/iOS devices op as **class 2: 10 meters (33 feet)**
- **Some companies employ BT Smart Beacons:** Enable retailers to transmit loc info to smart devices

Loc can ID/target device: Send loc specific data to device to notify of sale/gather analytics

Loc-based tech: Originated from Bluejacking:

Bluejacking	Sending msgs/controls via BT to another BT-enabled device
Not **Bluesnarfing**	Access to info on mobile compromised/stolen from device
Not **Bluebugging**	Controls device to become listening one

BT hacking techniques limited by distance: Most devices can't be accessed from more than 10 meters

Bluesniping	**Directional amplified antennas:** Can penetrate BT sec at up to 1 mile: • Most cars today use class 1 BT devices

iOS/Android/Win Phones/BlackBerrys: Allow BT connections/maintain list of devices that connect w/associated MAC

- Lists can be obtained using forensic SW: Observe connections made w/device/those avail that didn't connect
- Android/Win phones must have BT visibility on/avail to BT-enabled devices: Paired to other to transmit
- Current Android SDK doesn't allow unpaired connections
- **iOS:** Connection to device must be encrypted/key must be shared bet devices

Wi-Fi Comm: Enables device to be connected to AP connected to Internet/LAN

- **1st device: Calypso Wireless C1250i:** 2006 3GSM World Congress trade show: Barcelona
- Uses freq band ID by IEEE using 802.11 MAC/phys layer specs for WLAN comm using 2.4, 3.6 5, 6, 60GHz freq
- **Typically limited:** freq/range increases w/max **70 meter (230 ft)**
- Wi-Fi enabled mobile must be rem ASAP
  - B/C of vulns, like BT are stored w/in file maintained in mobile
  - Allows device to connect immediately to known/auth sites/devices

Prior to iOS 5	Maintained list of all Wi-Fi connections avail to device: Not just used by • **List stored in consolidated.db file in FS** • It ID'd all Wi-Fi connections along w/latitudes/longitudes • Used to track device/person using it/moved to diff locs • **Vuln fixed:** consolidated.db moved to OS partition Back w/iOS7 but w/limited info
Android	Notorious for storing each/every successful connection to device • Info could lead to sec issues if AP compromised

	• True for most devices set to auto connect to AP • If device not properly isolated from Wi-Fi during seizure: Vuln to pen • Can exploit via rogue AP: Creating ad hoc network/ID'ing network w/same SSID **Some devices:** iOS/AT&T pre-config for attwifi: Vuln

NFC: Near Field Comm: Devices can op as NFC xfer/receive data by being near other NFC/sys set up to transmit/receive sig

- **Short-range wireless tech:** Enables connect by touching devices together w/in few inches
- Small amts of data shared bet NFC tag/mobile device bet 2 devices capable of comm by NFC

NFC Tag: Based on NDEF: NFC Data Exchange Format

- **NFC capable devices:** Make transactions/exchange content/connect devices
- Lots of components of contactless card tech
- Can be used to control multiple instances of contactless card (hotel keys/work key cards/etc.)
- **Proximity based:** Unlikely problems will occur during seizure
- Attacks typically occur w/other devices using relay sys to capture data from device/xfer it to proxy card/device emulation
    - Allows relay sys to act as POS machine/capture data b/c individual device believes it's comm w/POS
    - SW installed on device act as relay sys to fraudulent card emu comm w/reader device

Mobile Sec: Multiple settings: Passwd/PIN/SIM: Subscriber ID Module PIN/encryption passwd/passwd for backup encryption

Apple iOS Devices: Sec depends on model/OS ver/usr config

1st gen	**Simple passcode:** 4 digit # || SIM PIN: Avail only GSM markets until 2010 • iOS device capable of running on Verizon after Gens after: Allow both simple/complex passcodes/SIM PIN up 37 chars Largest gen iOS devices allow for simple/complex/biometric sec • Apple doc/passcode screen indicate device wiped after 10 failed attempts ○ **11th failed entry that initiates wipe**

Failed Attempt Consequences for iOS Devices

Failed Attempts	Added Waiting Time	Total Waiting Time
1 to 5	None	None
6	1 minute	1 minute
7	5 minutes	6 minutes
8	15 minutes	21 minutes
9	60 minutes	81 minutes
10	60 minutes	141 minutes
11	Black screen	Wiped Device

Starting w/iOS 4: Full disk encryption

- Any unallocated space on device remained fully encrypted even if passwd known

- Also enabled usr to encrypt backups using iTunes setting
- **When enabled:** Set flag on iOS device when synced to encrypt data stream as it left device for backup
- **Even if device not protected by passwd:** Data collected encrypted if iTunes passwd unknown
- No visible setting on iOS to indicate whether device has been set to encrypt backup

To see if encryption enabled: Launch iTunes: Examine SW device info screen: Indicates if backup encryption enabled

- Access Data's MPE+ will indicate whether encryption enabled during connection
- Investigator should req iTunes passwd if usr refuses: Forensic tools can be used to bypass/recover limited usr data

iOS 8.0	**Released 2014:** Apple changed way device encryption worked to allow greater sec • Can use passcode to encrypt device so Apple unable to recover data stored if unknown **Prior to iOS 8:** Police allowed to send locked devices w/court docs to Apple sec/would receive img of partition • No longer uses same methods/unable to assist • Passwd must be obtained from usr of device
Android	**Brought new type of sec to mobile: Pattern** • 1st release of Android OS allowed: **4 point pattern w/in 3×3 grid** • Newer devices allow use of all **9 points** • Increased number of points elevated sec: Still lowest form of sec for Android **9 point pattern: 50K restricted (same dot only) pattern combinations possible** • **w/4 point restricted pattern: 1400** combinations possible **Smudge attack:** Typically can reveal pattern of Android usr if device held at 60% angle to light source • Smudge Attacks on Smartphone Touch Screens: Dept of CIS: Uni Penn

Hash stored in key file w/in Android FS: Can be extracted/analyzed to reveal pattern used to sec device

BC various sec vulns: More sec options added to later ver of Android

- Now allow use of patterns/PINs/passcodes/passwds w/letters/numbers/symbols/biometrics
- Usr enables sec settings
- If examiner knows type of sec enabled: Can determine viability of a bypass during collection
- More than 12K Android devices avail on global market: ID'ing exact type of sec is difficult
- Look at device screen for clues to type of sec in use
- All biometric sec features are backed up w/another form of sec: PIN

No matter sec: Can be accessed w/mobile forensic tools if ADB: Android Debug Bridge enabled: Not on by default

- If enabled on device after seized: Can be forensically analyzed even if locked

Prior to Android 3	**Full device encryption not avail** **4.0:** Encryption included sys settings/usr choose/along w/data on external mem card

	5.0: Encryption by default: Won't inhibit standard usr data collection of forensic tools • **Impt device be placed into ADB ASAP**
Win Mobile/Phone	**Transitioned from simple PIN/strong alphanumeric passcodes in Win Mobile 6.0/6.1** • Passwds only in 7/8 devices • All devices can also use SIM PINs to block calling features • Extremely difficult to examine w/out knowledge of passcode/PIN
BlackBerry	**Always known for sec: Not easily bypassed** • Later ver could use PIN/passcode/passphrase/passwd for data encryption • No known way to bypass BB device sec to collect device's data w/out handset's lock code/forensic tools • **BES: BB Enterprise Server** can reset device passcode if part of BES/setting enabled ○ If device has a passcode set for data encryption: Must also be known ○ Can create backup of their data: Can also be protected by passcodes/PINs ○ If pass/PIN known: Unencrypted backup can be produced ○ If passwd/PIN not entered for handset lock: Backup can't be initiated **BB 10:** Added to FS sys backup: Even If passwd known: usrname for BB Link SW must be entered **BB Link SW: RIM: Research in Motion** SW used to update firmware/SW/sync mobile w/PC

Photographing Evidence at Scene: Impt: Assign evidence # to device/xfer to agency evidence tag before taking pic

- Placed next to device to be photographed/seized || Shoot all angles

Impt for many reasons: Provides visual doc of device as found

- Dispels potential accusations device destroyed/damaged by person collecting it
- Can be used to determine whether device has evidentiary value
- If powered on: Screen saver/wallpaper may provide info of interest
- Date/time appears on screen impt info

Tagging/Marking Evidence: Each piece of mobile evidence has unique chars/requires specific handling procedures

- Can be sensitive to changes in state: Must take care
- Wear gloves: Smudge marks can determine passcode/phrase later
- Before mark/tag/bag mem cards: Be grounded electrically to avoid sending ESD's onto card

Mem cards/SIM conductors highly susceptible to ESD

- Small static charge from conductors op in range of **1.8-5 volts** can be corrupted/destroyed by as little as **30 volts**
- High voltage can be delivered in process ID'ing bagging mem/SIM cards
- **Tagging:** ID each piece w/unique number: Include yr/dept case #/loc #/article #

Tag/label should indicate	○ Date/Time | Collector's name/ID | Evidence # ○ Descrip of artifact following guidelines
Mark evidence loc/number	**If marking made on artifact**: Doc why necessary

	If placed in container: Affix label/tag container
Doc Evidence at Scene	**Item #:** Value assigned to seized property **Quantity**: # of items for single item type **Property Description:** Serial #'s/markings/etc **Owner/Loc found**

Mobile Device: Serial #/make/model/color/size/condition/telecom co/status – on/off?/SIM/mem card?: USB/cables/cases/etc

SIM Card: Multiple SIMs may not be inserted, but could contain valuable info

- Loc of each card should be indicated along w/ICCID: Integrated Circuit Card ID'r/#/Type/Color/condition/co.
- ICCID: Serial # on SIM card: Unique

Mem Cards: Can be difficult b/c serial #'s not loc on exterior

Device State Issues:

- **Device not locked/no current sec:** Processed immediately by examiner
- **Powered on/passwd known:** Don't attempt to enter passwd at scene
- **Powered on/sec enabled:** Owner will not unlock: Power off/bag
- **If remaining on:** Attach portable power source to maintain charge
- Remain isolated using both airplane mode/Faraday bag

iOS 7/Later	Swipe up from bottom of iOS device screen: Exposes submenu w/airplane icon
Previous iOS	Airplane mode from main page of settings app: Tap gears icon: Switch toggle to OFF
Android	Press/hold power button on upper-right corner of phone: Airplane setting
Win 7/8	Similar to laptop: Home screen: Flick left: Settings: Airplane mode

Properly Bagging Mobile Device Evidence:

Exterior switches	Some devices have exterior toggle switch to turn sound on/off/up/down Cover switches w/evidence tape to maintain position at time of seizure
USB port	Cover any exterior ports w/evidence tape
Headphone port	Cover w/evidence tape
Camera lens	Cover all lenses w/tape to prevent pic capturing after seizure
Battery	Access to battery area would allow access to SIM/mem card: Cover w/tape

From <https://www.piratemoo.net/moosings/mobile/mobile-forensics-ch-4-notes/>

Post 5

Friday, January 25, 2019 12:13 AM

CELLULAR NETWORKS

June 9, 2018 Moo Comments 0 Comment

Cellular network: Device to cell tower —> Cell tower to **MSC: Mobile Switching Center**

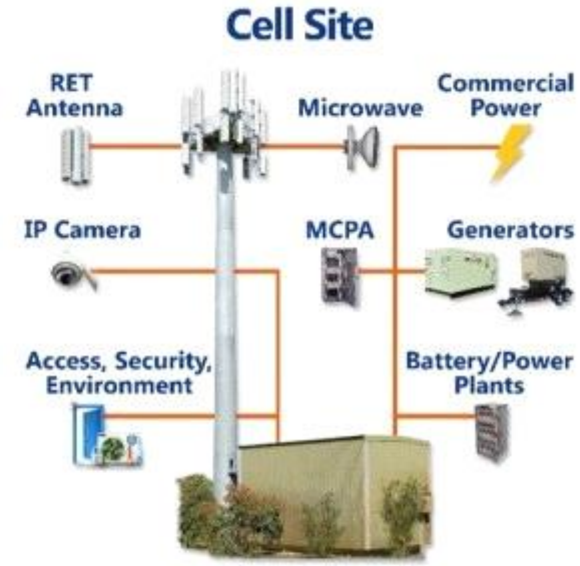
- **If call is out of network:** MSC sends sig to PSTN: Public Switched Telephone Network ——> Out to caller

Cellular-to-cellular convo: Don't move from MSC to PSTN

- Stay inside MSC: Routed back into network: No extra fees

Cell Towers: 3 Panels per side

- **Transmitter**: Middle panel (usually)
- **2 outside receiver panels:** Listen for inbound sigs
- **Comparing differences:** Tower learns about loc
    - Helps handoffs bet handoffs when caller mobile



Cellular network: Group of cells

Cell: Group of cell sites in an area

Cell site: The cell tower: Specific point in cell

Areas in middle represent cell sites: Base stations/radio equip/antennas located.

- **Cell site:** gives radio coverage to cell
- Best location of cell site: Along edges at intersections of octagons: Not center of it
- Design ensures no gaps

Network Systems:

2G	**IS-95:** Digital Service CDMA based **IS-136:** Digital AMPS [TDMA] • **GSM:** Digital service incompatible w/95/136 • **iDEN:** Proprietary OS built by Motorola

3G	**EDGE:** GSM 2.75ish: Marketing • WCDMA: GSM • CDMA2000 CDMA
Pre 4G	LTE: Long Term Evolution • WiMax • WiBro [Mobile WiMax] • HSPA+ [T-Mobile]
True 4G	LTE: Advanced • WiMaxMAN: Advanced

ITU: International Telecomm Union: only 2 4G techs are actually 4G

Handset Transmission Techniques:

- **TDMA: Time Division Multiple Access**
- **CDMA: Code Division Multiple Access**
- **FDMA: Frequency Division Multiple Access**
- **CDMA2000**
- **WCDMA: Wide Band CDMA**
- **UMTS: Universal Mobile Telecomms System**
- **LTE: Long-Term Evolution**
- **HSPA+: High Speed Packet Access**

TDMA	**Time Division Multiple Access** Allows multiple callers to use same freq chan by dividing sig into diff time slots, called bursts **Burst:** Small packet data traveling along spectrum: Voice traffic digitized/portioned/put into a bit stream 1 seg at time • Purely digital • Divides signal into time slots • Allows multiple simultaneous calls • Purely digital transmission • Portions of calls transmitted in bursts • IS-136 network OS • Base of current GSM: Most 2G systems
CDMA	**Code Division Multiple Access** • **Used by IS-95 cell sys: Spread-spectrum:** Tags multiple convos w/specific digital code • **IS-95B: 2.5G**: CDMA2000 1xRTT: 2.75G • **CDMA2000:** 3G: Backwards compatible **1xEV-DO Tech:** • Rel 0 • Rev A [3.5-9G] • Rev B [3.5-9G] **Spread spectrum:** Electromagnetic energy generated : BW spread in freq of domain: Sig w/wider BW • Used for variety of reasons: Establish sec comm/increase resistance to interference/jamming • Prevent detection **Each transmitter:** Assigned code to allow multiple transmitters to use same freq chan at same time • Tags each part of multiple convos w/digital code • Code let's OS resemble calls at base station using filters • More efficient than TDMA: More usrs per BW

GSM	**Global Systems for Mobile Communications** • Complies w/ETSI: EU Telecomm Standard Inst. • Uses TDMA/FDD: Freq Division Duplex • GSM 900/1800 standards: 2100:3G • GSM 850/1900/1700: North America • GPRS in early 2000 for packets • EDGE now UMTS: 3G: WCDMA • All digital **Most popular standard: Contain user's sub info/phonebook** • Used on most 2G networks: Uses bursts: Info xferred based on time w/TDMA • Utilizes UMTS and WCDMA • 4G: Utilizing HSPA/HSPA+/LTE
iDEN	**Integrated Digitally Enhanced Network** • Dev by Motorola • Radio: Tx: 806-821MHz; Rx: 851-866MHz: Cell phone **Uses:** • Speech compression/TDMA/3 units [6 convos]: 12 for PTT per chan • WiDEN: Comm across 4 25KHz chans: More BW: 2.5G tech **Provides usrs benefits of trunked radio/cell phone: Compared to analog cell/2-way radio sys** • Not as efficient as CDMA networks b/c only small convos can occur • **PTT: Push to Talk:** Radio tech allows cell to act like walkie-talkie • PTT: Cell network/towers not in use **WiDEN: SW upgrade for iDEN: Alows comm across 4 25Khz chans combined** • Up to 100KB of BW • Generally 2.5G tech

Cellular Network:

Mobile Station: Mobile equip used by subscriber [cell phone/SIM]

Base Station Subsystem: Cell tower that comm's w/mobile equip

Network Subsystem: MSC/DB's used to auth w/network

Mobile Station	**Consists of:** • **ME: Mobile Equip** • **SIM: Subscriber Identity Module** ME Identified by IMEI: International Mobile Equipment ID
SIM card	**Consists of:** • **IMSI: International Mobile Subscriber ID:** ID's subscriber to system: Secret key for auth • **ICC-ID: Integrated Circuit Card Identifier**

Base Station Subsystem:

BTS	**Base Transceiver Station:** Cell tower: Handles convo w/mobile device or station
BSC	**Base Station Controller:** Where freq. hopping/handoffs controlled

Handoff in GSM:

- **Hard hand-off:** GSM handset can be attached to only 1 tower at time
- As handset moves through network/gets farther from tower: Needs to attach to another tower

Handoff in CDMA:

- **Soft hand-off:** Can be attached to multiple towers at same time
- Phone will op w/tower w/strongest sig: Can also be attached to 2nd/3rd

tower

- If call overloading/handset moving through sys: Readily moved to another tower w/out usr knowledge

MSC	**Mobile Switching Center** • Router of the sys: Where info moved to HLR/VLR/EIR/Auth Center • Where in-out/network call info moved through sys
HLR	**Home Locater Register:** Largest DB's maintained on SP's servers **HLR contains subscriber's:** • Home address/Phone Number • IMSI: International Mobile Subscriber ID • SIM card's ICC-ID • GSM services that sub has requested/been given • Only 1 exists for each sub
VLR	**Visitor Location Register:** Largest DB's maintained on SP's servers • Temporary DB that contains info about subs who have roamed into areas it servers **VLR contains:** • IMSI: International Mobile Subscriber ID • Auth data • Sub's phone number • GSM services that sub allowed to access • HLR address of sub • Current loc of handset • TMSI: Temporary Mobile Subscriber ID **Info is sent to HLR/updated via specific protocols** • VLR's can have many logs for each sub b/c based on geography
EIR/AC	**Equipment Identity Register** • Standard GSM network element • Allows mobile network to check type/serial # of mobile device • Determines whether/not to offer service • DB contains info about ID of mobile equip • Can store info to log file **White-listed:** Contains all known/valid IMEI #'s **Grey-listed:** Contains all IMEI #'s of devices under observation by network **Black-listed:** All defect/stolen devices **Authentication Center:** Secured DB handling auth/encryption keys • Secured DB: Auth's each SIM that attempts to connect to core network • Once auth successful: HLR allowed to manage SIM/services • Encryption key also generated/used to encrypt all wireless comms [voice/txt/etc] **If auth fails:** No services possible

From <https://www.piratemoo.net/moosings/mobile/cellular-networks/>

Post 6

Friday, January 25, 2019 12:15 AM

MOBILE FORENSIC TOOL OVERVIEW P1

June 19, 2018 Moo Comments 0 Comment

Logical Collection:

2007: NIST SP 800-101: Logical acquisition implies **bit-by-bit cop**y of logical storage objects that reside on logical store

2013: SWGDE: Scientific Working Group on Digital Evidence: Removed bit-by-bit classification proposed by NIST

- Stated logical acquisition implies copy of logical storage of objects that reside on a logical store
- 2013 publication: Process that provides access to usr-accessible files
- Logical analysis process will "not generally provide access to deleted data"

2014: NIST: SP 800-101R: Logical acquisition is capturing a copy of logical storage objects that reside on a logical store

SWGDE's definition is too general

Logical collection should be interpreted as extraction of usr data from a mobile device w/out collection of a device's FS

Data extracted from mobile device using proprietary protocols/queries/displayed in SW usr int

  - **Example:** Using SW tool on Android device w/APK: Android App Package file
  - APK queries device's internal DB/returns data to SW int: Data displayed in SW's user int
  - Does not return a FS, but data that is represented by contents of files on device

Accepted definition makes assumption that all logical collections/recovered data from mobile by SW are similar

File System Collection: Bridges gap between logical/physical collection

- Contains much more info than defined logical collection: Should be considered a step-up
- Contains files/folders that device uses to populate apps/sys configs/usr configs along with usr storage areas

MSC, MTP, PTP

- Points of storage: Mobile Device FS collection must occur in multiple places
- Storage area can be loc where imgs/vids/audio stored/accessible by usr via comp/cable
- Another area can be internal storage point also stores app data/sys log files/docs

MSC: USB Mass Storage Class:

MTP: Media Transfer Protocol: 2008

- Originally part of MS Framework: Became standard by USB-IF (Implementers Forum) as USB type
- Recognizable when device plugged into PC/auto mounted as device, rather than a drive
- Access occurs via MTP: Subset of PTP: Picture Transfer Protocol: Adds enhancements
  - Enables comm bet mobile/PC to cp/mv/replace/del files from/to device

Move away from MSC to MTP made in most modern devices

- If device was in MSC mode: Couldn't store/comm w/default storage point: Made device useless during connection
- Couldn't access apps/take pics/op so MTP mode implemented

Media in MTP: Refers to bin data and isn't restricted to audio/video fmts

- Any file stored can be recovered using MTP

Internal Sys Collection/Display

OS	Type	Type of Data
Apple iOS	PTP	Imgs/Vids
Android, BB 10, Win Phone	MTP	Imgs/Vids/Media

Non-Invasive Physical Collections:

SWGDE: "Involves a process that provides physical acquisition of phone's data w/out requiring opening case of phone"

- SW must be able to comm w/device to allow for a bin data "dump" of device
- In most cases: Will not yield physical img as defined by NIST (bit-by-bit copy)
- Should yield a representation of data targeted by SW's comm in file fmt stored on device

Examples of non-invasive method:

- Flasher box to USB's port or FBUS connection: Dumping mem from predefined offsets known to contain usr info
- Collecting Android device using tools like Oxygen Forensic Analyst, Detective, UFED, XRY
    - Selecting phys option for particular device that isn't locked with Android Debugging enabled
    - Tools comm w/device to obtain partition info using ADB: Android Debug Bridge
    - Subsequently extract returned partition table/partitions w/out altering device partitions/OS structure

Target only what is visible by comm methods: Various partitions not enumerated by device's OS

Invasive Physical Collections

Provides physical acquisition of a phone's data/requires disassembly of phone for access to the circuit board

Examples:

- **JTAG: Joint Test Action Group:** Allows for comm w/mobile using device TAPS: Test Access Points
- Not a direct read of actual mem module (flash)
- Method to comm w/device processor to access NAND area of device/obtain bin file containing representation of partitions of device
- If SW is interacting w/device microprocessor, it will dictate what mem stores are avail/where to read from
- Use of JTAG is classified as invasive b/c direct interaction w/circuit board
- Necessary when soldering to the TAPs or using specialized connections directly to board

Another example:

- **Removal of mem chip from device: Chip-off**
- Chip-offs are destructive methods: Generally device will be non-functional w/technique
- Will enable direct read of mem chip using specialized HW/SW
- Examiner can create full bin file of device mem flash w/out limitations typically imposed by a device microprocessor
- Physical collection method would conform to bit-by-bit representation of entire device physical store
- Resultant data must be interpreted by SW/represented FS compiled from the bin file in order to further analyze

As devices progress along w/FS encryption of device at FS lvl will hamper JTAG/Chip-off examinations

Collection Pyramid:

- Dev by Sam Brothers of US Customs/Border Protection
- Outlines tool classification that can be used as a practitioner's approach when conducting device examination
- Step away from classifying tool as logical and/or physical

Collection pyramid: Visually represented ranging from most invasive/specialized [smallest part] and largest/base of pyramid least specialized

Level 1: Manual Extraction	• Involves capturing stored device info either by photography/written doc • Photographing info would be more reliable in legal proceedings/preferred method • Commando method: Thumb Jockying device: Manual manip of device to usr stored areas • Involves navigating device to usr stored areas/photographing/writing down content observed in device's viewing area
Level 2: Logical Analysis	• Logical extraction occurs using a built in device xfer method [USB, Wi-Fi, IrDa, BT] used by device • Connection made w/device using data xfer method: SW can comm using device protocols to extract data using cmds comprehended by device • Data returned to SW, which can be further analyzed/reported • Type of collection currently offered by most examiners as well as forensic SW vendors
Level 3: HEX Dumping/JTAG	• Uploads specialized SW into volatile mem of device • Bypasses built-in sec that would inhibit access to device internal mem store • Devices that have chip-lvl encryption enabled will still pose problems • Custom app/package installed onto device in effort to act as original app/package/ROM on

	device that contained sec measure • Once vuln patched w/vendor’s app/package/allowing access to device that was inhibited: Examiner can access files using cmds/procedures used by mobile device • Typically a raw FS represented in fmt used on mobile device extracted • Subsection of this pyramid belongs to flasher boxes/JTAG methods • By using JTAG TAPs in device, examiner has access to flash mem. • Using specialized tools comprising HW/SW examiner uses DW to comm via HW to microprocessor of device that ints w/flash storage medium • Examiner accesses flash area: circumventing passwd sec to obtain partition info/usr storage areas ○ JTAG is invasive: Device is disassembled ○ Leads can be soldered to TAPs on circuit board ○ Some instances preconfig’d jigs can be used ○ Output when using JTAG bin file of selected partition/mem area **Flasher Boxes:** • Output produced is represented by what HW flashing device has been config’d to output • Output can be encrypted, segmented or altered (boot loader added to start of img) • Or it can be a flat bin file • Truly a hex representation of data living on device **Limitations to flashers:** Numerous: Proprietary output to flash area mem constraints • Data output produced w/use of JTAG methods offers better representation of data w/little interference w/digital data output • Preferred method but can be more destructive
Level 4: Chip-Off	• Involves phys removal of device flash mem • Examiner disassembles device/rem flash mem from circuit board • Once flash module is removed intact it’s placed into a specialized component to read mem modules • These mem module adapters are specific to type of flash mem/config • Bin file produced upon reading that must be interpreted by SW that specializes in decoding/interpretation of this type of file • Examiner conducting these should be well trained: Evidence could be easily compromised • Chip-off exam is invasive • Once chip removed: Would need to be reballed and reinstalled into device so it could op as it had previously • Extremely labor intensive/expensive • Once device disassembled at chip level – inoperable
Level 5: Micro Read	• Flash mem medium is read by an electron microscope • Not only theoretical but hasn’t been conducted publicly on device evidence • Involves using electron microscope to read/count electrons that occupy cell on a flash mem chip • If electrons present: 1 represented: If not 0 represented • Referred to as gating • After combining bin data manually: Can be translated into raw data/interpreted • Most examiners will never experience this form of examination/collection – likely national sec related

Micro Read
Chip-Off
HEX Dumping/JTAG
Logical Analysis
Manual Extraction
——————————————-
Micro Read
Chip-Off
Physical (Invasive)

Physical (Non-invasive)
File System
Logical
Photograph and Document
Manipulate and Document

Boot Loaders: Code that loads in a runtime env or os: can be used in nearly all digital devices that have underlying OS

- Boot loader can change depending on HW as well as service carrier
- If code becomes corrupted: Device can't be started/will continue to restart over/over – boot loop
- Non-invasive physical classification

To use a custom boot loader: Examiner places device into certain mode

- **iOS: DFU:** Device Firmware Update mode
- **Android:** Recovery/Download mode
- Can occur operationally by SW, but examiner places device into this state w/combination of key presses
- **Once in correct mode:** Selects device: Some instances of Android replaces the ROM w/custom one
- SW begins process of calling instr code to complete collection of mobile data store
- Customized ver of boot loader/ROM loaded onto device has been designed to allow full access to mem store and additional settings for data transfer
- W/customized ver in place: Comm can occur w/SW to otain unadulterated access to device
- On completion of data collection if boot loader/ROM exchanged: Original boot loader/ROM returned to mem/released on restart
- Physical non-invasive should include subset that describes tools/analysis if using custom boot loader
- Otherwise should be classified as physically invasive

Not all bin collections described as physical non-invasive have boot loaders/ROM altered to obtain hex dump of mem store

Manual Examination Tools: Can consist of taking pics of device's onscreen digital content using tripod/digi cam

Paraben Project-A-Phone ICD8000/Paraben Project-A-Phone-Flex	• Cam setups allow for both HD vid/8MP pics • ICD8000 uses clamping mech that inadvertently press buttons on side of mobile device including power button on right side • Improper clamping could change settings/power off device Project-A-Flex doesn't use a vise, but a mat on which device can be placed to photo evidence
Fernico ZRT3	• Combines cam/HD cam along w/materials to hold device/cams in place • Device connects directly w/SW installed onto PC to capture pics • Uses OCR: Object Char Recognition to translate imgs containing txt to searchable txt w/in report • Includes mat onto which evidence can be placed to conduct interrogation of device
Teel Technologies Eclipse 2	Similar to ZRT3/combines a cam/mount/platform w/SW solution to capture/doc imgs collected

Flasher Box: Service tool typically used by device technicians to fix nonresponsive device/add features/unlock device for unrestricted access w/any carrier

- Derived from action that device built to perform
- Flashes new ver of device firmware/ROM/OS/Settings
- Could be used to add language packs/change serial # of device
- Altering serial number (IMEI) for GSM/ESN/MEID(CDMA) is illegal
- By changing serial number: Some devices can op on a network blacklisted by original number

Box	**Support**
Ns Pro	Samsung
Z3x	Various Samsung devices [Agere, Sysol, Swift, Infineon, OMAP, Qualcomm]
Octopus Box	LG/Samsung
SHU Box	Nokia/Sony Ericsson

ATF: Advance Turbo Flasher	Nokia Legacy, Nokia Lumia Series (SL3)
Vygisoft Toolbox	LG
Infinity-Box	MTK, ZTE, Huwei
IP-BOX	iOS PIN unlock

From <https://www.piratemoo.net/moosings/mobile/mobile-forensic-tool-overview-p1/>

Post 7

Friday, January 25, 2019 12:15 AM

MOBILE FORENSIC TOOL OVERVIEW P2 (JTAG/CHIP-OFF)

June 19, 2018 Moo Comments 0 Comment

JTAG

JETAG: Joint European Test Action Group: 1985 in EU as standard for boundary-scan testing

- **Boundary scanning** context of mobile devices efficiently tests connections on printed circuit board in effort to program/debug device w/out needing phys access to flash

1986: Members from NA joined: **JTAG: Joint Test Action Group**

1986-1988: Group proposed/published series of proposals to IEEE Testability Bus Standards Committee

- Final version of JTAG 2.0 accepted
- Published 1990/updated several times w/current specs ID'd as IEEE Std. 1149.2013
- At core: JTAG is standardization of TAPs/boundary-scanning arch

JTAG: Variety of meanings: From directly programming sys to debugging, from Xbox hacking to forensics

- Process of setting/reading values on test pins accessible on PCB of mobile device
- By using the TAPs comm can occur via the boundary-scan path, interfacing w/BSR: Boundary Scan Registers that int w/components on the PCB
- Components can be programmed/read w/out removal independently reading/programming each separately

In order for comm to occur w/components IEEE Std. 1149.1 indicates a min that 3 input connection and 1 output connection ports must be on a PCB

- The TAP is a multipurpose port that allows access to test support functions built into a component and the standard outlines that the TAP shall include TCK: Test Clock, TMS: Test Mode Select, TDI: Test Data In and TDO: Test Data out as connections

An optional input port, TRST: Test Reset can also be used

Debugger/Programmer Solution	Mobile Device
Data Output	TDI
Mode Select	TMS
Clock	TCK
Data Input	TDO

TCK	**Test Clock** • Port enables sync of internal state of device bet components

	• Devices are made of many components that could be using diff forms of timing • TCK maintains standard across them during a test
TMS	**Test Mode Select** • Port controls the TAP controller and relies on the TCK to determine the state of the process
TDI	**Test Data In** • Port accepts data from SW debugger/programmer and sends it to target
TDO	**Test Data Out** • Port accepts data from target and sends it to debugger/programmer SW
TRST	**Test Reset** • Port is optional but can be used to reset the TAP

TAPs for mobile not readily doc: Manufacturers making it more difficult to loc them on PCB

- Some manufacturers like BB: Massive lengths to hide TAPs: Place them where any access destroys device
- JTAG HW for mobile: Another type of flasher box, but point of comm/interaction differ
  - Difference: Serial comm occurs to/from TAPs located on the mobile device PCB
  - Flasher boxes: Comm using traditional USB connector pin-outs on device

ID TAPs: JTAG Pin Finder from 100RandomTasks: Enables examiner to attach wiring from JTAG PIN finder to TAPs on PCB and use associated scanning SW to determine correct ports

- Both collection of port/collection involves soldering wire to appropriate TAP
- In some instances: Special Molex connectors can be used that snap directly onto a female molex connector on PCB
  - No need to solder

Certain tools can import/analyze such imgs obtained from JTAG collection:

- Cellebrite Physical Analyzer
- Micro Systemation XRY
- Oxygen Forensic Analyst

Commonly Used JTAG Boxes in Mobile Device Collections

Box	**Support**
RIFF Box	Samsung, HTC, Nokia, Huawei, LG, ZTE, Others
Medusa Box	HTC, Huawei, LG, Samsung, Sony Ericsson, ZTE, Others
ORT JTAG	Samsung, LG, HTC, Huawei, ZTE, SKY, SE, Others
GPG JTAG	Google, HTC, Dopod, Others

Chip-Off

- The removal of a device’s flash mem module/analyzing it referred to as a chip-off
- Procedure is labor intensive in both removal and reading stored data

- Phone model storage types could range from
    - **TSOP: Thin Small Outline Package to**
    - **FBGA: Fine-pitch Ball Grid Array**
- Can become expensive

TSOP chips: Pins attach the chip to PCB are exposed: Can be easily removed by heating solder joints

BGA chips: Must be heated to the correct temp to remove solder joints/adhesives and then carefully removed from the PCB

- Their solder joints aren't accessible along the exterior as are TSOP chips

Both chips must be rem w/caution bc they can't be reattached after removal

- After removal, chips must be cleaned, examined, inspected
- After chips can be attached to appropriate adapter and read in chip programmer

Chip programmer: Tool that allows for the collection of raw data from the mem chip

- Can also be a detriment, like flasher/JTAG boxbc it can write/erase a mem chip if used incorrectly

Analysis of file produced by reading mem chip often most tedious

Mobile device mem chip based on flash mem (NOR/NAND) chips

- Inherent advantage of I/O when compared to HDD's is biggest detriment at chip lvl examination
- NOR flash mem: Older tech: Allows for high read perf: Doesn't allow for high capabilities
- NAND flash mem: Both faster programming/erases: Can consume power bc higher functioning/complicated I/O int

How Flash Memory Works

Flash mem in NAND arrays stored in series of blocks: Also happen to be smallest erasable entities on a NAND mem chip

- W/in blocks are pages, which are the smallest programmable entities on a flash chip
- Pages include sectors/chunks
- Pages contain a data area/area for mem mgmt called OOB: Out of Band data
- OOB data for each sector/chunk w/in page that can contain metadata specific to the page's status (valid/invalid/bad)
- OOB can also contain metadata on associated page/block and doesn't have to be following the sector but al can be at the end of the page

NAND mem chips: Don't have finite lifetime: Measured according to # of erases that occur

- # of erases w/out failure of the mem chip far exceeds the lifetime of the mobile device
- Very impt measurement when discussing the way data is often written to the flash mem
- Data is written to a flash cell in the form of 0 or 1
- 1 is empty 0 is full

- If data was written to a block, a 1 can be replaced by a 0
- A 9 can never be changed to 1 to alter data
- The entire block would have to be written to another block and the previous one would be erased during another background process
    - Technique called wear-leveling

Wear-Leveling: Way for flash mem to make sure areas of mem aren't exceeding the # of erases over the surface of the flash chip

- In turn, when a file is updated on the flash, it's not possible to program the current page: Completely rewrittn to another loc [page/pages/block/blocks]
- Loc doesn't have be in the same block/blocks
- During this process the OOB area is marked as active for the new page/old page is marked as inactive

Garbage collection: Another flash mech: Function of reclaiming entire blocks if # of inactive pages exceeds a given threshold

- **If this occurs:** Entire active page(s) are written to a new block: The entire block is then erased to allow for new data to be written and become avail for new data
- Extends the life of the flash mem

Various types of traditional FS: FAT/FAT32/VFAT/HFS+/EXT/EXT3/EXT4/NTFS and actual flash FS: JAFFS2/YAFFS/UFS can be observed from a chip-off collection

- **Diff bet 2 types:** whether or not the FS needs a transition layer or whether the FS uses a system of DB's to manage flash mem
- **Traditional FS:** Must be a FTL: Flash Translation Layer that will op as interpreter for FS/allow it to act as a block FS/emulate flash file sys
- Diff FTL ints use diff specs: MMC/eMMC/MSD/ATA
- As data written to various areas of flash to conduct wear-leveling/other procedures the FTL presents info to traditional FS as though written to a static loc so it ops normally
- A flash FS handles all the wear-leveling/creates its own data structures w/out the need of an FTL
- These data structures are generally mounted into RAM/contain flash info such as bad blocks, block erases, pointers to files for mobile
- Written to flash upon shutdown rewritten into RAM on startup

Non-contiguous: Spread out data that looks disjointed

Traditional Mobile Device Forensic Tool Classification

Tool	Logical	FS	Physical (Non-Invasive)	Physical (Invasive)	Limited Support
BlackLight	X	X			X
UFED 4PC	X	X	X	X	
Device Seizure	X	X	X	X	
EnCase	X	X	X		
Lantern	X	X	X		X
MOBILedit Forensic	X	X			

MPE+	X	X	X	X	
Oxygen	X	X	X	X	
Secure View	X				
XRY	X	X	X	X	

Open Source Tools: BitPim, TUL2G handle feature phones: Both are no longer updated

iOS Devices: All tools covered here allow access to device w/out enabled sec: Passcode for handset/iTunes passwd must be known if enabled

iPBA2: iPhone-Backup-Analyzer-2: Dev by Mario Piccinelli: Can be used to decode iPhone backups up to iOS 6.x

- Doesn't conduct collection of device, but allows browsing backup
- Backup must be obtained prior to using
- Hasn't been updated since 03/2013
- Parses a number of user/app db's and browsing complex file types

Santoku: Suite of tools used for mobile investigations, malware analysis/mobil sec assessment all rolled into 1 int using a Linux vm

- Can be added to a Mac partition to dual-boot

OSAF: Open Source Android Forensic Toolkit: Concentrates on malware analysis on Androids

- Contains APKInspector which Santoku doesn't have: Static analysis of APK files to ID malware injections
- Dynamic malware analysis using OSAF is completed using wireshark
- Uses viaFOrensics AFLogical code/comparable to extraction using both the stand-alone/santoku ver

BB: MagicBerry: Allows parsing of both IPD/BBB files created using BB Desktop Manager SW

Freeware Tools:

- **NowSecure Forensics Suite (Community Edition)**
- **iFunbox**

Commercial Tools:

- **MPE+**
- **Cellebrite**
- **Oxygen Forensic Analyst and Detective**

From <https://www.piratemoo.net/moosings/mobile/mobile-forensic-tool-overview-p2-jtag-chip-off/>

Post 8

Friday, January 25, 2019 12:15 AM

SIM CARD ANALYSIS PART 1 (TON/NPI IN OTHER PORTION)

June 25, 2018 Moo Comments 0 Comment

Smart cards: *“microprocessor equipped tokens…store/process diverse range of data/apps”*

Many use UICC/SIM interchangeably

- HW portion of smart card
- SIM/USIM: SW apps included on card

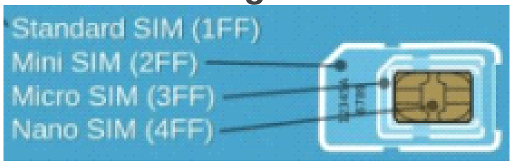
UICC: Universal Integrated Circuit Card: SIM: Only GSM originally: Key to mobile op on network w/HW/SW

- Used in most smart devices: CDMA included
- **R-UIM: Removable User Identity Module**
- **CSIM: CDMA2000 Sub ID Module cards:** Part of CDMA devices can be used globally
- Defined by ETSI: Adopted by 3GPP: Apps: **USIM/SIM/ISIM/CSIM**

Coverage sub cards:

UMTS network	USIM app maintains control of comm: Includes data to op device on network • 2G/EDGE on GSM: SIM used • Only a SIMM w/app that can’t op on UMTS-only • UICC w/both SIM/USIM app can op on GSM/UMTS

UICC Size Progression: Defined by ETSI



1. **1FF ID-1 UICC:** Never used in mobile: Credit card size
2. **2FF Plug-in UICC:** Found in devices until 2004
3. **3FF Mini-UICC:** Made its way into most smart devices
4. **4FF Nano-UICC: 2012:** Newer iOS/Android/BB/Win phones

UICC cards today: Still original size: Majority use Nano-UICC

- Microprocessor didn’t change bet SIM/Nano-UICC: Shell containing did
- Forensics SW: Replicates cmds used by device to comm w/apps on UICC

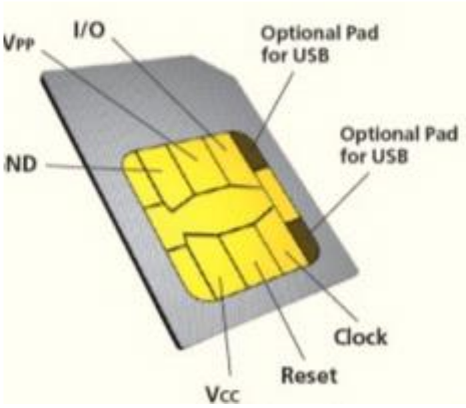
SIM Card Analysis: Collects data using APDU cmds

- Cmds comm w/device and UICC: Obtain/store data by writing info to UICC
- **UICC is passive**: Doesn’t initiate contact w/device: Listens for APDU cmds sent

APDU: Application Protocol Data Unit: Serial #/Last SMS/Last known loc

SIM’s contain	Microprocessor (CPU) || RAM || ROM firmware ||

	• Electrically Erasable Programmable ROM: Nonvolatile storage **Physical chars of UICC**: • Needs all contact points connected w/device terminal pins • Accepts comm via I/O contact • 6-8 points along reciprocal contacts of mobile: Most: 6 pins • Reading/querying/writing to UICC occurs at points



APDU commands: 2 components:

1. Always initiated outside of UICC [forensic SW]
2. Response always returned even if incorrect

Response can be: Successful/unsuccessful | Successful w/sec problems/return of data

Commands
CLA INS P1 P2 Le Data
Response
Data SW1 SW2

Any sec/perms needed to be satisfied: Have to be entered as APDU cmds

Security conditions for SIM cards:

- **ADM (Admin)**
- **CHV: Card Holder Verification**

Once at file ID:

- APDU cmd must send INS that tells SIM what to happen at file ID
- File ID must be selected to include additional INS

APDU cmds need to navigate SIM FS first using INS (instructions) cmds on way to right file ID

- ID for file acted on: If using select INS: Fills data portion of cmd structure
- Whatever length of data portion in bytes: # added to **Le block** of cmd

File ID	Made of 2 bytes
Select file ID	Cmd must include **A4** as **INS**

Example:

A0	**A4**	00	00	02	3F00	**Select Master File**
A0	**A4**	00	00	02	2FE2	**Select ICCID**
A0	B0	00	00	0A		**Read 10 bytes (Bin)**
98	68	32	02	01	00	00 00 10 13 **Returned ICCID**

First cmds: Navigate to ICCID via FS: ID's file: Sends INS code to read # of bytes loc w/in record

Return cmd contains ICCID: Success

ICCID: Integrated Circuit Card ID

Reverse nibble format: Each byte flipped to create actual value

FS UICC Structure	**MF: Master File** **DF: Dedicated File** UICC FS made up of 7 lvls that contain 4 file types: **ADF: Application Dedicated Files** **EF: Elementary Files** Which include file ID: **3F00**

Only 1 MF on UICC: Similar to root folder: DIR on files/ID's: Described by ETSI

- Can be 7 DF's on UICC: [GSM, DCS1800, TELECOM, USIM, PHONEBOOK]

SIM partitions: Apps: W/in apps various files referenced as file ID's

- **UMTS sys avail: USIM partition/app used**
- **CDMA system: CSUM partition/app used**

USIM app: Can contain addl phonebook entries over/above those in SIM app

- **UICC FS:** Layers w/in each app/FS: Some contain duplicate info: Only written once to card

Network Info Data Locations

- **Ki:** Ciphering key: For auth process/contained on all SIMs: Unavail to examiners using SW
- No other smart card on network uses same number

Loc on exterior of smart card: Max 20 digits

- **Even if UICC locked w/PIN:** ICCID can be attained: Used to obtain PIN
- **Unblock key PUK to change PIN/access:** Send appropriate court order

ICCID: Similar to serial # of UICC: Represents unique # assigned to single UICC: Emergency calls exception

- Reverse nibble
- Record found directly under MF's in **EF_ICCID**
- Each byte must be reversed to interpret ICCID digits

1st 2 digits	**System code:** Constant value: **89**
Next 2-3 digits	**Country code** for UICC: **US: 01**
Next 2-3 digits	**Issuer ID #**: Like 1st/2nd digits on a credit card Made of 10 bytes that comprise 7 values: **ID's card issuer:** Visa/MC: For UICC: T-Mobile/ATT/Etc.. • 1st 3 data groups: Can't exceed 7 digits
Remaining digits	UICC #: Made up of yr/mo of manufacturing/config/specs/UICC #
Final digit	Checksum

Example: 8931017010511316860 1

- **893 System code**
- **3101 Country code**
- **170 Issuer ID #**
- **511316860 UICC #**
- **1 Checksum**

IMSI: International Mobile Subscriber Identity: Unique # that ID's sub on cell network

- **GSM/CDMA:** Needed for contact

GSM/UMTS standards:

- **9 bytes**: Max # 15 digits
- Values under **EF_IMSI** in UICC
- Reverse nibble: Must reverse
- **1st byte:** Always **x08**

1st digit	**9** Dropped b/c not part of IMSI value
Proceeding bytes	IMSI reverse nibble
1st 3 bytes	**MCC: Mobile Country Code**
Next 2 digits	**MNC: Mobile Network Code**
Remaining digits	ID #

IMSI: Protected file: If UICC locked w/PIN: Inaccessible

Example: 310260123456789

- **310** Mobile Country Code
- **260** Mobile Network Code
- **12345678** Subscriber identification number

ID's geographic area where device was last successfully powered off

- LOCI writes last tower loc device was registered when power off occurred
- Quicker access when powered on
- If battery rem/not powered off right: File may not be avail/correct

LOCI: Elementary File under DF_GSM (DF structure for GSM):

Examiners can use key to ID geo loc by contacting carrier of record w/key info

IMSI

File ID	Length (Bytes)	Bytes	Need
6F07	9	**1: Length** **2-9: IMSI**	Mandatory

TMSI: Temporary Mobile Sub ID

LAI: Location Area Information

TMSI Time

Location Update status

LOCI comprised of:

TMSI	Temp random ID assigned via VLR: Visitor Loc Register to sub • Actual IMSI not sent via handset • Possible to capture/ID mobile sub • Temp IMSI changes when device moves to diff VLR • Temp Mobile Sub ID
LAI	The **MCC: Mobile Country Code** • **MNC: Mobile Network Code** • **LAC: Location Area Code** Location Area Info • Examiner can ID country/carrier to contact www.mcc-mnc.com

LOCI

File ID	Length (Bytes)	Bytes	Need
6F7E	11	**1-4: TMSI** **5-9: LAI** **10: TIMSI TIME** **11: Loc Update status**	Mandatory

PLMN:

- **Elementary File under DF_GSM:** ID's networks which carrier doesn't have agreement

PLMN: Both MCC/MNC: written to FPLMN if network rejects loc update

- **Limit 4 records:** Can hold up to n records
- When record added to FPLMN EF: Record placed after last one
- No additional slots? 1st record rem: New record added to last slot

FPLMN: Forbidden Public Land Mobile Network

- **Examiner:** FPLMN: ID's country codes along w/carrier of record: Used to ID geo region

File ID	Length (Bytes)	Bytes	Need
6F7B	12	**1-3: PLMN 1** **4-6: PLMN 2** **7-9: PLMN 3** **10-12: PLMN 4**	Mandatory

SMS: Short Message Service: Another Elementary File located on UICC

- 7 records that define aspects of msg/service
- 3GPP TS 23.040 || ETSI 123 040 for UMTS defines records as msgs
  - Either originate from ME/received from sub network
- **Record length:** No more than 176 bytes

1st byte	Status of record
Remaining bytes	Arch of message

Status byte indicates unused: Content still contained in bytes 2-176? Msg del

- ME changes status of record/doesn't rem content
- Shows unused record slot avail/can be overwritten w/new msg

Bytes 2-176	Content w/set length for actual msg content • Depends on how data formed • Often **TPDU: Transport Protocol Data Unit**

Elementary File

SMS-SUBMIT	Whether msg sent
SMS-DELIVER	Whether msg received

SMS

File ID	Length (Bytes)	Bytes	Need
6F3C	176	**1: Status info** **2-176: Remainder**	Optional

Slack space: Partial SMS msgs: Not possible from SIM b/c way records written to card

Message status byte

Binary	Value Status	Hex Value
00000000	Unused	**X00**
00000001	Mobile Terminated, read	**X01**
00000011	Mobile Terminated, unread	**X03**
00000101	Mobile Originated, sent to network	**X05**
00000111	Mobile Originated, msg to be sent (Unsent)	**X07**
00001101	Status report requested but not yet received	**X0D**
00010101	Status report requested, received, but not stored in EF-SMSR	**X15**
00011101	Status report requested, received, stored in EF-SMSR	**X1D**

Length of SMSC Info

- Number of octets (8 bits/or/1 byte) used to store type of #
- Number of service center

Short Message Service Center: Use of service center # internal to mobile device

- Not all handsets have this
- **Missing:** SMSC obtained from handset along w/TON/NPI service center #

SMS-SUBMIT	**Typically 00**

From <https://www.piratemoo.net/moosings/mobile/sim-card-analysis-part-1-ton-npi-in-other-portion/>

Post 9

Friday, January 25, 2019 12:16 AM

SIM CARD ANALYSIS P2 TON/NPI

June 26, 2018 Moo Comments 0 Comment

TON/NPI

- Single octet
- Indicates type of number telephone will represent
- Byte representative of bin num created
- 1st bit: Always 1
- Combined with TON: 3 bits and 4 bits NPI
- Type of Number/Numbering Plan Indicator

SMS-SUBMIT Structure

Type	Description	Need
TP-MTI	TP-Message-Type-Indicator	Mandatory
TP-RD	TP-Reject-Duplicated	Mandatory
TP-VPF	TP-Validity-Period-Format	Mandatory
TP-RP	TP-Reply-Path	Mandatory
TP-UDHI	TP-User-Date-Header-Indicator	Optional
TP-SRR	TP-Status-Report-Request	Optional
TP-MR	TP-Message-Reference	Mandatory
TP-DA	TP-Destination-Address	Mandatory
TP-PID	TP-Protocol-Identifier	Mandatory
TP-DCS	TP-Data-Coding-Scheme	Mandatory
TP-VP	TP-Validity-Period	Optional
TP-UDL	TP-User-Data-Length	Mandatory
TP-UD	TP-User-Data	Optional

Example: Number is international conforming to ISDN: Number dropping first MSB: Always 1

- Decoding following 3 bits for TON: Remaining 4 bits for NPI
- **Common value: x91**: Converted to bin: **1 001 0001**: Indicates + attached to number in front of country code

SMS-DELIVER Structure

Type	Description	Need
TP-MTI	TP-Message-Type-Indicator	Mandatory
TP-MMS	TP-More-Messages-to-Send	Mandatory
TP-RP	TP-Reply-Path	Mandatory
TP-UDHI	TP-User-Date-Header-Indicator	Optional

TP-SRI	TP-Status-Report-Indication	Optional
TP-OA	TP-Originating-Address	Mandatory
TP-PID	TP-Protocol-Identifier	Mandatory
TP-DCS	TP-Data-Coding-Scheme	Mandatory
TP-SCTS	TP-Service-Center-Time-Stamp	Mandatory
TP-UDL	TP-User-Data-Length	Mandatory
TP-UD	TP-User-Data	Optional

Binary Representation of TON/NPI Key of SMS Messages

TON Binary	**Interpreted**	**NPI Binary**	**Interpreted**
000	Unknown	**0000**	Unknown
001	International Number	**0001**	ISDN/Tele # Plan
010	National Number	**0011**	Data Numbering Plan
010	National Number	**0011**	Data Numbering Plan
011	Network Specific Number	**0100**	Telex Number Plan
100	Subscriber Number	**0101**	Service Center Specific
101	Alphanumeric (7bit)	**0110**	Service Center Specific
110	Abbreviated Number	**1000**	National Numbering Plan
111	Reserved	**1001**	Private Numbering Plan

Service Center Number	Value represents # of service centers used to route SMS msg • Stored in semi-octets **BCD: Bin Coded Decimal** fmt • Reverse nibble • Numbering doesn't complete octet: F added to complete it
1st Octet of TPSM	**1st Octet of Short Msg Transfer Protocol** • Single byte indicates type of msg from 6 defined types • Hex byte should be converted to bin • 2 Least significant bits: Used to determine type of SMS msg • These bits referred to as TP-MTI
Address Length	Single octet represents length of actual sender number • Byte needs to be converted to dec to obtain number of nibbles represented • **Unlike SMSC length:** Value won't include following byte that indicates TON/NPI
TON/NPI	Determines number plan/sender
Sender Number	Semi-octets/reverse nibble
TP-PID	**TP-Protocol-Identifier** • Octet ID's protocol used for transmission of msg • Standard ME to SC comm: **Likely 00**
TP-DCS	**TP-Data Coding Scheme** • Octet represents coding used to encode msg • Value assists ME in decoding fmt once received **All other values:** When converted to bin, can be interpreted to determine it • **00** to indicate default 7-bit data code scheme Countries like China/Korea/Japan: Others use chars outside ASCII range

	• Value will be diff b/c UCS2 most likely used • **X04 TP-DCS** section of **SIM**: **bin 01 00**: 8-bit data: **class 0 msg**
TP-SCTS	**TP-Service Center Time Stamp** • Value represented by semi-octets and reverse nibble (BCD) • **Ordering:** Yr/Mo/Day/Hr/Min/Sec/Time zone **Time zone:** # of 1/4 hr from local time to GMT time • Most significant bit of 1st octet indicates whether # is local time • ME can display received time in local fmt • Time zone local to sending entity
TP-UDL	**TP-User Data Length** • Integer value represented in HEX: Length of data contained in msg • Value determined by TP-DCS/data fmt **TP-DCS default:** 7-bit length represented by septets (2 bytes) • 8-bit/UCS2 represented by octets (1 bytes) • After converting # into dec value: Can ID Length of msg data • Max length: 140 bytes: If msg fmtted **Msg fmtted using 7-bit GSM:** Records don't go over 160 chars • **Fmtted using 8-bit:** Record content shouldn't exceed 140 chars • **When examining SMS output/UCS2 coding** ○ Msg length shouldn't go over 70 chars using 16-bit UCS2 alphabet fmt • Allow for transmission/reception of msgs in multiple langs • 7-bit GSM alphabet: Mandatory for network providers **Countries use langs not supported by extended ASCII of GSM**alphabet • China, Korea, Japan • Use UCS2 16-bit fmt **ME:** Will always default to 7-bit but as soon as char entered not part of 7-bit **GSM alphabet**: Msg re-encoded into UCS2
TP-UD	**TP- User Data** • User Data portion of SMS contains msg in 7-bit, 8-bit or UCS2 fmt • Data represented in forensic tools as hex values
TP-MR	**TP-Message Reference** • Single octet found in sent msgs indicate integer value of msg reference • Value is typically **x00** but can **range** from **0-255**

Bin Representation of TP-SM Byte of SMS Msgs: Indicates Msg Protocol Used

TP-MTI	Direction	Message Type
0 0	MS -> SC	**SMS-DELIVER-REPORT**
0 0	SC -> MS	**SMS-DELIVER**
0 1	MS -> SC	**SMS-SUBMIT**
0 1	SC -> MS	**SMS-SUBMIT-REPORT**
1 0	MS -> SC	**SMS-COMMAND**
1 0	SC -> MS	**SMS-STATUS-REPORT**

Bin Representation of TP-DCS Byte of SMS Msgs: Indicates Data Coding Protocol Used

Bits 3 and 2	Translated	Bits 1 and 0	Translated
00	Default Alphabet	**00**	Class 0

01	8 bit data	**01**	ME -Specific
10	UCS2	**10**	SIM Specific Msg
11	Reserved	**11**	TE Specific

Both SMS-SUBMIT/DELIVER use a combo of items:

- **DELIVER:** Describes values/decodes data in figure
- Sometimes chars are w/in BCD values: Must be represented as 0
- These can be seen w/in HEX values throughout SIMs

Contacts: On a UICC: referred to as **AND: Abbreviated Dialing Numbers**

- **Elementary File:** SIM app under **DF_TELECOM**
- Can also be in USIM app under **DF_Phonebook**
- Often phonebooks coexist/contain duplicate records

Global phonebook: Multiple phonebooks avail under **DF_Telecom/DF_Phonebook**: App specific

- Like other data on UICC: Data w/in ADN record coded in semi-octet (BCD) fmt

Alpha identifier: A name associated w/listed phone #

- When used: 7-bit GSM alphabet/left justified
- All unused byte will use FF/UCS2 fmts
- Can be 0-242 bytes in length

Rest of record: Include AND length/Ton/NPI/AND/Config record/Ext record: Must be 14 bytes

- AND coded in BCD fmt: Preceded by length of AND/TON/NPI
- Length much like SMS embedded Address Length
- TON/NPI determined by examiner before decoding actual AND

ADN: Larger than 20 chars: Written to ext file under **EX_EXT1**: Indicated in last byte of ADN record

Configuration record/capability record: Preceding byte: Whether additional config needed for call

- Points to record in **EF_CCP1**

Abbreviated Dialing Number (EF_ADN) Are Contacts that can be found in both USIM/SIM app

File ID	Length (Bytes)	Bytes	Need
4F3A	N+14	**1 to n:** Alpha identifier **n+1:** Length of BCD # **n+2:** TON/NPI **n+3 to n+12:** Dialing # **n+13:** Capability/Config **n+14:** Extension1 record identifier	Optional

Call Logs: UICC stores only LND: Last Numbers Dialed: Doesn't store incoming calls to ME's SIM mem

- Incoming calls stored on device itself
- **Elementary File LND:** Under **DF_Telecom** in both SIM/USIM app
- **LND record:** Similar to **EF_ADN** in storage capacity/data layout
- LND can store an alpha ID/byte to ID length of #/byte for TON/NPI and actual dialing # in BCD fmt
- Config/capability byte/extension byte

EF_LND: Limited records: depends on carrier: No more than 10 records can be stored to UICC

- **When new call made:** All records occupied 1st record rem/all records shift up
- New record taking last position
- Most devices today don't store call history directly to device

Dialing Number: Carrier relies on **EF_IMSI** to ID mobile user w/in network

- Dialing # doesn't need to be stored on UICC

If EF_MSISDN not found in investigation: Doesn't indicate device wasn't used/not in service

- **Not dependent on MSISDN**: Only valid **EF_IMSI** needed
- **EF_MSISDN:** Under **DF_Telecom** for both SIM/USIM app
- Can include 7 records w/in file depending on carrier

Multiple EF_MSISDN records:

- Allow usr of UICC to have phone # for business/person/fax/etc w/only single EF_IMSI
- Enables device to be associated w/multiple dialing #'s

From <https://www.piratemoo.net/moosings/mobile/sim-card-analysis-p2-ton-npi/>

Post 10

Friday, January 25, 2019 12:16 AM

NOTES: CH 11: IOS ANALYSIS PART 1

NOTES: CH 11: IOS ANALYSIS PART 1

July 2, 2018 Moo Comments 0 Comment

iOS FS:

Apple devices: Some OS X foundation: Diff framework: OS X apps won't run on iOS

UNIX based FS: Structures similar but diff: Ways each store apps/usr data

- **iOS:** Apps interact w/FS: Limited/sandboxed by design: Each has a container/# of containers w/specific roles
- Both iOS/OS X use a HFS: Hierarchical File System

iOS	HFSX | HFS+
OS X	HFX+

Difference: Latter contains case sensitive filenames

Forensic tools originally: Could interpret HFS+:

When it came to H+ 0x400 offset of disk img: Process failed

- **HFS/HFSX FS contains HX:** Had to change X to a + in order for tools to mount FS properly

- **SW:** Had to negotiate/rebuild FS/raw disk img
- **To display mnt/dir structure:** Had to interpret correct block size during collection/decoding [512 bytes]
- No longer issue

Devices prior to A5 chip: Non-invasive collection of entire raw disk

- Both sys/usr partitions w/in iOS: Much like HDD w/dir structure/file slack/unallocated areas
- Unallocated space/free area w/in partition great: Ended w/iOS5

iOS 5: Apple changes way data encrypted on disk: Data protection class keys/FS key

- Examiners req to obtain keybag/keys to decrypt/analyze extracted partition at file lvl perms to rebuild/analyze

2008: Burghardt/Feldman: Use journal file w/in Mac OS partition to loc/ID file entries for del files w/limited results

- Extended by Bedrune/Sigwald: w/in iphone-dataprotection code using Py script
- **Journal file:** Extremely small: Only a number of files can be recovered
- **Unallocated space:** Limited carving

DFU: Device Firmware Update:

- **A5 chip:** Mode still worked: Every attempt to use w/automated tool no longer allowed for collection
- Didn’t accept custom RAM disk: Blocked from acquiring device using non-invasive phys technique

iOS4: Enables usr to encrypt/backup w/in iTunes: Passwd used to encrypt backup instead of HW key of device

- Backup keybag accessible w/in backup: Possible to decrypt w/out iOS itself
- Encryption backup: Not setting usr can set/disable on actual device: Not on by default

Efforts to discover ways of accessing iOS device: Tools allowed a backup of iOS using iTunes/AFC: Apple File Conduit protocol

- Used by iTunes to move files on/off for device-lvl comm
- *Limited only to media unless jailbroken*
- **Altered/installed to device: AFC2 made: Access to complete FS of iOS: Not viable to forensics: Jailbreak**

Services:
com.apple.mobile.house_arrest
com.apple.mobile.file_relay

- Dev by Apple as internal testing mech for file xfer: Part of libimobiledevice code of 2009
- If backup not invoked: Encryption wasn’t triggered/any data xfer wouldn’t be encrypted

house_arrest	**Enables access to app folder/contents** • Could conduct mobile device forensic exam even if iTunes passwd unknown • Able to extract PIM: Personal Information Manager data/app data

2015: Ex-employee of mobile forensic company outed Apple’s sec flaw: Not new info: iOS 8 closes backdoor

All ver pre-iOS 8: Still allow for connections to house_arrest/file_relay

Commonly Collected by Automated Tools

User Data	File Type	Path in FS /private/var/
Contacts	SQLite DB	mobile/Library/AddressBook/Addressbook.sqlitedb
Call logs	SQLite DB	<iOS 7: mobile/Library/CallHistory/CallHistory.db iOS 7: wireless/CallHistory/call_history.db iOS 8x: mobile/Library/CallHistoryDB/CallHistory.storedata
SMS	SQLite DB	mobile/Library/SMS/sms.db
MMS	SQLite DB	mobile/Library/SMS/sms.db
Calendar	SQLite DB	mobile/Library/Calendar/Calendar.sqlitedb
Notes	SQLite DB	mobile/Library/Notes/notes.sqlite
Imgs	Individual .jpg IMG_	mobile/Media/DCUM/1XXAPPLE
Videos	Individual .mov IMG_	mobile/Media/DCIM/1XXAPPLE
Bookmarks	SQLite DB	mobile/Library/Safari/Bookmarks.db

App Data: Sandbox concept/partitions: Storage value contained w/in Docs/Lib/Temp

- Stored directly under main app folder w/in iOS FS

/private/var/mobile/Applications

iOS 8x: /private/var/mobile/Containers/Data/Application

- App name w/in raw iOS FS is a GUID: Globally Unique ID’r
- GUID can change on app updates

Landmarks w/in App File/Folder Structure

Folder	Data Description
Documents	Usr generated content: Dev would place data accessible to app usr: Avail to usr along w/Plist files
Documents/Inbox	Enable app to access files opened from outside reqs: Mail app: Backed up by iTunes
Library	Top-lvl dir: Store data : Doesn’t want to expose to usr: Uses subdir structure • Any folders w/exception of caches subdir backed up by iTunes
Lib/App Support	Subfolders/files used by app for function support: Ad support/db files supporting features/addl app settings
Lib/Caches	**house_arrest/file_relay** service on jailbroken device: Not avail on iTunes backup: cache
Lib/Cookies	**cookies.binarycookies** file: Persistent session cookies used by app • Can hold 2nd Cookies.binarycookies file appended w/ **-corrupt**flag • **-corrupt:** Failed auth/corrupted file marked so new file created • Can be decoded w/Py scripts securitylearn.net | PyScriptor
Lib/Preferences	Preferences
tmp	Temp storage

Installed Apps: Services Daemon ID’rs

file: **com.apple.lsdidentifers.plist** /var/db/lsd/

- Apps installed launched by LSD service: Actual vendor ID GUID assigned to app
- Compare to **Manifest.plist** to determine whether app existed/was rem

Bundle ID Folder: com.company.appname

- **Apps w/in an app:** One w/bundle ID consistent w/actual app
- **Once located: Cache.db/ApplicationCache.db** should be avail w/in it
- **Cache.db:** Can also be loc in another subfolder w/in parent

Typically contains 5 tables: 3 of significance

- **cfurl_cache_response**
- **cfurl_cache_blog_data**
- **cfurl_cache_receiver_data**

File represents data app received from outside source: Holds in cache for speed:

cfurl_cache_response	Table contains data requested/response including URL/time of request • **isDataOnFs field** • **If contains 1**: Data stored w/in another folder on iOS device w/in Caches folder
cfurl_cache_blob_data	**Contains BLOB: Bin Large Object** data w/response from server • **BLOB of 4096/larger?** Stored locally/assigned **GUID** • All other files will be stored w/in db represented by **0**
cfurl_cache_receiver_data	Contains received data from server in response to **cfurl_cache_response**
fsCacheData	**Located under bundle ID: S**ubfolder of cache that used to store file data/imgs/etc

Additional FS Locs

Path	**Description /Library/**
/Accounts/Accouts3.sqlite	Usrnames of app accts including data/time
/Caches/	Vast numbers of property lists/files cached by Apple Services: **file_relay** • **Standard iTunes backup**: Not accessible w/most forensic tools • **Jailbroken?** Avail w/cached data
/Calendar/Extras.db	Current alarms/set/no longer used
/ConfigurationProfiles/ProfileTruth.plist	Contains key:**forceEncryptedBackup:**Indicates whether backup encrypted • Calling iTunes backup
/Mail/Recents.db	Recent e-mail/SMS addresses: Name/phone/dates accessed/last accessed: • Recents.db
/MobileBluetooth/com.apple.MobileBluetooth.ledevices.paired.db	Devices paired w/device
/Maps/Bookmarks.plist	**Bin Plist contains bookmarks || iOS 8**: **/Containers/Application**
/Maps/Directions.mapsdata	Start point/destination w/internal mapping ||**iOS 8: /Containers/Application**
/Maps/FailedSearches.mapsdata	
/Maps/History.mapsdata	
/Maps/SearchResults.mapsdata	

/Library/Preferences

com.apple.conference.plist	FaceTime settings
com.apple.conference.history.plist	History of FaceTimea: ID/Email of usr: Msg sent
com.apple.identityservices.idstatuscache.plist	FaceTime: iMessage: e-mail: Confirm validity of usr creds w/ESS: Enterp Shared Services
com.apple.ids.service.com.apple.ess.plist	**Accounts capable of auth on Apple ESS:**AppleID/VettedAliases/LoginAs info • Phone numbers/e-mail of device usr
com.apple.ids.service.com/apple.madrid.plist	ID services property list for iMessage: e-mail/phone that have been used
com.apple.imservice.FaceTime.plist	FaceTime creds
com.apple.imservice.iMessage.plist	iMessage creds
com.apple.locationd.plist	Apps that have been accessed/currently using loc services
com.apple.madrid.plist	Whether **ReadReceiptsEnabled** set to on/off: Whether receiver of iMessage read msg
com.apple.Maps.plist	Last map loc searched for by long/lat: Last view creds for iMessage
com.apple.MobileBluetooth.devices.plist	ID's paired BT devices w/MAC/LastSeenTime
com.apple.MobileBluetooth.ledevices.plist	BT listing of ID'd BLE devices
com.apple.mobileipod.plist	Music/Last media item played
com.apple.mobilephone.plist	Last # displayed on dialer screen: Key called AddressBookLastDialedUid
com.apple.mobilephone.settings.plist	ID's call-fwding #: General settings
com.apple.mobilephone.speeddial.plist	Favs from contact list

Other /Library

/SpringBoard/IconState.plist	Lays out icons/folders for apps currently displayed to usr on device • 7 keys w/in property list impt • Key button bar ID's apps located along bottom of main screen • **key listType** ID's folder • **key displayName:** Id's name of folder • **Above displayName:** ID's by array number
/TCC/TCC.db	ID's apps such as mic/photos/Contacts/calendar/Twitter: Which services have access
/Voicemail/voicemail.db	VM date/sender/duration/when del • **.amr files:** Contain actual messages ID'd by rowid in DB • VM deleted can be recovered here

/Media/

/Recordings/Recordings.db	Voice recordings made w/iOS: Date/duration: .m4a ext

/PhotoData/Thumbnails	Thumbnail files of imgs in DCIM: Can contain del pics

/var/preferences/SystemConfiguration/

com.apple.network.identification.plist	IP addresses used/dassigned on both cellular WAN/WiFi • Domain IP's of router/timestamps of each event
com.apple.wifi.plist	WiFI addr/connected to: Auto-joined: AP names: MACS: Type of sec
preferences.plist	Config prefs for comm: ID's device under **HostName** and **ComputerName** keys

/var/wireless/

/Databases/CellularUsage.db	**subscriber_info** table w/in db: Lists sub ID: IMSI: sub MDN: Last update date • Update date when IMSI/MDN were last used • Contains all SIM cards inserted/used w/in device
/Databases/DataUsage.db	**LiveUsage | Process:** • Tables contain app name/process associated w/app/timestamps of usage • Data coming in/out via WAN • When put together using foreign key OPT: SQL query shows activity of app/process
/Preferences/com.apple.commcenter.plist	Property list ID's ICCID along with phone assigned to device

From <https://www.piratemoo.net/moosings/mobile/notes-ch-11-ios-analysis-part-1/>