International Journal of Grid and Distributed Computing
Vol. 9, No. 10 (2016), pp.331-346
http://dx.doi.org/10.14257/ijgdc.2016.9.10.30

A Research Paper on Cell Phone Technology

Lalit Mohan Joshi

BTKIT Dwarahat, India
Lalitm.joshi9@gmail.com

Abstract

This paper describes the different types of networks and standards used by cell phones. Here I discuss the evolution of cell network generations and the technical aspects attributed to each. On cell phone and mobile technology a brief background use in public, private and government health is reviewed. Main focus of this paper is how to use and introduction of different mobile networks. This paper is a research about the wireless network generation and technologies associated with each as well as standards of different cellular network. It is found that the necessary precautions equipment and related actions required to properly and safely seizing different phone equipment. It demonstrates the proper use the important safety equipment that assists investigators to safely and clearly seize mobile phone equipment. This paper also discuss the different imaging methodologies that exist using the latest cell phone forensic software and the pros and cons to each one as well as performs hands-on imaging scenarios utilizing several different tools.

Keywords*: Seizure, Generation, Network, Gsm, Cell Phone, Wireless, Tool, Imsi*

1. Introduction

As a previous year, cell phones are the most widely used and distributed electronic devices with over 2.5 billion users worldwide installed with robust operating systems and increasing storage capacity; cell phones have similar functionally as some high end computer systems. More reliable network coverage, competitive rates among services providers, and high- speed broadband internet connectivity make cell phone the communication method of choice. The seemingly anonymous nature of prepaid cell phones services introduce additional challenges when tracking usage and locating suspects on the wireless network. Investigators should use the same care and caution when seizing mobile phone devices as when they seize other types of evidence. Mobile phones can be very volatile and proper care should be exercised when handling and seizing. Investigators should carefully consider what kind of evidence they want from the phone before they handle it. If they wish to process for fingerprints, as well as there is a need to care specially to preserve the phone in a state that will not destroy potential fingerprint evidence. a constant challenge is faced by the digital forensic and investigating team to stay with the new and advanced technologies those may be used relevant suspects exposed in an investigation and inspection by the investigator. As we know that now a days mobile phones are very common and easily handed, used by many users like personal, professional and government purpose. Mobile phone forensic is known as the science to recover all the necessary digital evidence under forensically conditions that how and when mobile phone was being used with the help of accepted methods. Cell phones vary in design, feature, use, development and are continually undergoing change in handling as well as with the existing technologies those are improved and enhanced technologies introduced. When a cell phone is founded and encountered during an investigation process by the relevant team, There are lot of the questions arise:- What should be done about backing up power as well as maintenance? How should the phone

ISSN: 2005-4262 IJGDC

be taking over? How should precious or potentially relevant data in the form of information have the device be examined? The answering key about these questions is knowing well about the cell phones hardware as well as software characteristics.

2. Wireless Network Generation and Network Generation

The evolution of cell phone technology has seen many changes since the first mobile radio telephone was released commercially in 1946 by Motorola. These radio telephones were different from two way radios used by police and taxis in that they were connected to the telephone network related to public switched.

2.1. First Generation

Commercially released in 1980's as an analog voice only standard currently being phased out in most countries. Cell Phone systems implemented following the IG standard**:**

- NMT (Nordic Mobile Telephone)
- AMPS(Advanced Mobile Phone System)
- TACS(Total Access Communication System)
- JTAGS
- CNETZ
- Radiocomm 2000
- RTMI

2.2. Second Generation

Fully digital cell phone network that was commercially released in 1991 on the GSM (Global System for Mobile communications) standard.

- Voice Conversations digitally encrypted for added security.
- Data services introduced.
  - SMS Text Message
  - Multimedia
  - Email
  - Narrowband Internet

Further divided into TDMA and CDMA- based standards

- GSM (TDMA) – Used by over 80% of cell phone users around the world.
- PDC (TDMA) – Used in Japan
- IDEN (TDMA) – Used in USA but has since migrated over to GSM standard.

2.3. Third Generation

Based on IMT- 2000 (International Mobile Telecommunication) standards, and offers a broad range of services with wider network capacity.

- Wide area voice telephony
- Video Conferencing
- Broadband Internet

System implemented based on 3G standard include**:**

- W-CDMA (UMTS)
- CDMA 2000
- TD-CDMA / TD-SCDMA
- DECT
- Mobile Wimax

2.4. Fourth Generation

No formal definition exists for this yet to be released standard. Industry experts expect 4G to include a complete IP solution to end users will be provided at a much higher data transfer speed than previous generations.

3. GSM (2G)

Previously second generation phones are the most widely used cell phone technology with the GSM standard amassing over 80% of subscribers (over 3 billion people) around the world. A key feature of the GSM standard is the SIM (Subscriber Identity Module) card, is highly portable and can be easily interchanged among compatible GSM devices. The SIM card contains the user's subscriber information with phone book. It also contains a lot of additional key information that can help the investigator determine how the cellular device is being used on the network?

3.1. ICCID

Integrated Circuit Card Identification is digitally store unique number up to 19 or 20 digits stored in the SIM card and engraved on the face of the card during personalization. The format of the ICCID depends on the network carrier, but the following fields are consistent:

Example: ICCID = 01234567890123456789
1st 3 digit (012) = MCC (Mobile Country Code)
Next 2 digits (34) = MNC (Mobile Network Code)
Next 12 digits (567890123456) = Home Location register, typically found in two left most digits of the sequence.
20th Digit = Checksum (redundancy check for error checking)

3.2. IMSI

International Mobile Subscriber Identity is known as a unique number which is used to identify a SIM card on its individual network. The wireless provider to connect phone calls and communicate with the SIM card uses this number.

3.3. LAI

Local Area Identity is up to 10 digit unique identifier stored on the SIM card that identifies the public land mobile land network (PLMN), or device proximity to land based radio base stations broadcasting the LAI. As the device changes locations, it picks up new broadcast LAI'S from the land based radio substations and stores them on the SIM card. This information could provide the investigators with approximate geographical location of the device during the last time of use.

3.4. SMSC

Short Message Service Center is a unique network ID service provider that delivers SMS messages. A copy of all SMS messages are stored at the SMSC and forwarded to the recipient.

3.5. SMS Message

Short Message Service Message is a text messages sent /or received by the device to the SMSC and forwarded to the intended recipient.

3.6. Phonebook

It contains location on the SIM card that maintains Name with Phone number in a combined way, which typically will only store a fixed number of name/number combinations, but newer cards with higher storage capacity can store over 256 entries.

4. Gsm Frequency Bands

Second generation networks implemented on the GSM standard operate on specific frequencies or bands depending on country or region. Each cellular device must be configured with compatible hardware that can operate on the frequency bands in each specific region. Quad Band Device can operate on networks in any region listed below.

4.1. GSM 900 (890-915 MHz), GSM 1800(1710-1785 MHz)

It is used in most parts of world including: Europe, Africa, Middle East, Africa, Asia (Most Countries), Costa Rica, Brazil, Guatemala, and EI Salvador

4.2. GSM 850(824-849 MHz), GSM 1900(1850-1910 MHz)

It is used in USA and BRAZIL.

4.3. GSM 450(450.4-457.6 MHz)

It uses same frequency like 1G (First Generation) system like NMT used in E. Europe, Finland, Sweden, and Russia. Rarely use 2G frequency band known only to have operated in Tanzania. Previously, all wireless providers known to operate in Tanzania function on the GSM 9/GSM 1800 Spectrum.

5. CDMA-ONE (2G)

CDMA-ONE (IS-95) is CDMA (Code Division Multiple Access) technology based first digital standard which is used to send voice and data between mobile devices. CDMA allows several cellular devices to share the same frequency band (800 MHz and 1.9GHz) and be active all at the same time. Wireless providers offering this standard are capable to provide their services to a larger customer base with less number of cell towers than other standards. As previous year record, wireless networks using the CDMA standard compromised 13% of worldwide cellular service subscribers and is offered in various countries around the world including USA, Canada, Mexico, brazil, India, China, New Zealand, and Vietnam to name a few.

6. D- AMPS (2G)

2^{nd} generation wireless technology D-AMPS (Digital AMPS) replaced the 1^{st} generation analog AMPS wireless system which is based on the TDMA (Time Division Multiple Access) technology standard. D-APMS was developed to compete with the GSM 2^{nd} Generation Standard, and was once prevalent by GSM and CDMA 2000 technologies. The largest carrier, AT+T Mobility (USA) has begun to tear down the D-AMPS network in favor of GSM and UMTS technologies. D-AMPS has the distinction of being the first wireless standard to be developed with security and authentication features.

7. IMT-2000 (3G)

3^{rd} generation wireless technologies were first seen in 2001 in JAPAN and provide more advanced services such as broadband wireless data and video calls, and greater network capacity than 2^{nd} generation wireless systems. IMT-2000 (International Mobile

Telecommunication) is the global standard for 3rd generation (3G) wireless technologies. As of 1999, several wireless interface specifications were approved for use by the ITU (International Telecommunication Union).

7.1. W-CDMA

High speed wireless network used in various systems such as the FOMA and UMTS (3GSM). It uses a wideband mobile air interface to achieve higher data transfer rates and more users.

7.2. CDMA 2000

High speed wireless network developed as the successor to 2G wireless network cdma-one. it is incompatible with UMTS standard.

7.3. TD-CDMA/ TD-SCDMA

It is a high speed mobile network closely related to W- CDMA. It is developed as the on air interface to UMTS-TDD.

7.4. EDGE

For GSM evolution, Edge is the enhanced data rates with high speed wireless network that allows for increased data transmission rates and reliability over 2G GPRS networks. It can be used for any packet switched application.

8. CDMA 2000 (3G)

3rd generation wireless network CDMA 2000 is a CDMA standard based technology and was developed as the successor to 2G cdma-one. CDMA 2000 is defined to operate on the following frequencies: 450 MHz, 700 MHz, 800 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, and 2100 MHz. This wireless standard has gone through many evolutions and improvements since its inception to include the new standards CDMA 2000 EV-DO (Evolution Data Optimized) and CDMA 2000 EV-DV (Evolution Data/Voice) that provide even higher data transmission rates (3.1 Mb/s download) and more reliable voice services.

9. UMTS (3G)

3rd Generation wireless network standard UMTS (Universal Mobile Telecommunications System), which referred sometimes to as 3GSM, was developed on the high speed W-CDMA air interface and was designed to replace the GSM standard. UMTS supports up to 14.0 Mb/s data transfer rates (in theory), which is much greater than the 2G GSM data transfer speed of 9.6 kb/s. The first UMTS networks were launched in 2002 with an emphasis on mobile TV and video calls. However studies have discovered that interest in these features has declined due to the high availability of 802.11 (Wi-Fi) network si. Mobile devices such as smart phones and PDA's usually come equipped with 802.11 adapters and can connect to these networks to send and receive data at much higher transmission rates (up to 54 Mb/s) 802.11g networks.

10. Seizure Equipment

Investigators should be properly equipped with the necessary equipment to handle the various types of mobile phone devices they may encounter. Standard equipment normally brought to process crime scenes is usually required, but in addition, specialized equipment

is usually required to process mobile devices at the scene as well as document their seizure due to volatility.

11. Seizure Equipment - TOOLKIT

Investigators should have the following tools available to them in a standard "raid" kit:

- Screwdrivers for Precision
- Anti-Static Bags
- Aluminum foil
- Flash Drive with 2GB
- Micro SD Cards with Adapter
- USB Write Block
- USB Forensic Card Reader
- Portable Power supplies
- Faraday Bags

12. Seizure Equipment - TOOLKIT

Investigators should have the following tools available to them in a standard "raid" kit:

- Table Top Vice
- MiniDV Camcorder
- Digital Camera & Storage Cards
- Camera Traveler Tripod
- Legal Notepads
- Pens
- Pencils
- Permanent Markers

13. Office Safety

Officer safety is always a concern when processing crime scenes. Mobile Phones are commonly used as remote detonators for explosives and extra caution should be exercised when seizing mobile phones. Investigators should closely examine mobile phones visually before they are physically touched to make sure they are not attached or connected to other devices. Suspicious looking mobile devices be examined by appropriate safety personal before they are handled or seized.

14. Seizure

Investigators are likely to encounter countless different scenarios where mobile devices could be encountered and seized. These scenarios can be categorized into two separate groups, when the phone is found in the "on state as well as in the "off" state", the following procedures are recommended:

If phone is off

- Photograph, document & seize
- Seize charger and accessories
- Phone should not be turned on unless there is a need to process immediately and proper precautions are taken to shield it from the network.

If an investigator encounters a phone that is on, the following procedures are recommended:

If phone is on

- Photograph & Document
- A decision needs to be made- turn off/leave on

- If you leave on, shield from network
  - Use Faraday or jammer
  - If you turn off, phone can lock and you must know the unlock PIN.

If the Investigator decides to leave the phone on, several precautions need to be taken in order to preserve the identity of the information on the phone.

If the phone is on and you decide to leave on:

- Shield from cell Network.
- Do you have the equipment available to process the phone at the scene? If not, can you shield from network and still transport to laboratory for processing.
- What is the battery life? Can you seize the charger?
- Will phone auto-lock if no keys are pressed within a certain time?
- Can you change the locking code, just in case? How do you document that?

15. On-scene Incident Response

An investigator may decide to process the phone on-scene due to the need for instant information. Investigators need to make sure and bring all the necessary processing equipment as well as the specialized documentation equipment as well as the specialized documentation equipment (camera, video, vise *etc.*,), due to the various types of phone that may be encountered on scene. Investigators need to make sure they all the necessary forms they normally fill out in the laboratory at the time of processing.

If the time is critical, on-scene processing may be necessary.

- Is the necessary processing equipment available?
- Video equipment available to document processing?
- Necessary forms available?

16. Isolation of Radio Frequencies

Acquisition is defined as supposition, imagining process or to obtain data as information from a digital device and its peripheral equipment or tool and media. The plus point of an acquisition performance at the scene is the loss of information because of battery damage, depletion, destroys, etc. In the transportation and storage process it is always avoided. However, it contains a setting in which user has to work that must be controlled, that must have the appropriate and exact equipment and tools ,in which other prerequisties satisfied may not be possible at the scene, but within a laboratory setting it can be readily achievable. For the purpose, throughout this paper a laboratory environment is assumed. Devices handled with care and caution those are powered on in shielded work area with a radio frequency or have their disabled wireless communications.

Radio Isolation Techniques: There are number of ways to isolate the phone connecting to a cell tower in order to establish communications. Once the communications are blocked, the handset will continue to try and make connections at maximum strength, draining he cell phone device more rapidly. Prior to examination and consideration the device must be fully charged in battery that must be given to having a fixed as well as attached with portable power source.

16.1. Jamming Device

One way is to emit a signal stronger then the cell phones or to render a cell phone useless interfering with the signal. An additional way is to trick the phone as a “no device” signal is generating from the nearest cell tower.

Figure 1. Jamming Device

16.2. Shielded Work Area

You can also utilize a "Faraday tent" that will shield an entire area making communications safe in a target area. One drawback of the Faraday Tent is the work space becomes more restrictive.

16.3. Shielded Container

Faraday Bags can also be utilized which will shield the phone from communications. This type of shielding allows the investigator to be mobile, which still protecting the communication device.

16.4. Substitute (U) SIM

It mimic the original and prevents network identify that access by the handset in which believe that they are the original SIM. To be conducted safely at any location the techniques allow examinations

Figure 2. SIM

16.5. Disable Network

The service that might be induced to disable service, provide cellular carrier to the device. The service or network provider contacted with details as well as operator must be determined to identify disabled service like contact number, equipment identifier, subscriber. Such information is not always available on text, so this imposes delay by the process of coordination and confirmation.

At a forensic laboratory when available acquisition or imagining should occurred, once the seized equipment has checked in and arrived. The preliminary information should be recorded from the device such as:

- The Type of Device
- Operating System
- Carrier
- And Any Other Unique Identifying Marks.

There are only a few tools available on the market today to take acquisition from cell phones, and there is not one solution for all types of phones. Each program has different strengths and a mixture of the several tools may encompass a much more through search.

17. Device Identification

One of the first steps would be to properly record the service provider make, model. To select the correct tools for acquisition and imaging this Information allows investigation. Criminals may try to thwart investigators by changing the device's information to conceal its true make and model. To make the device appear differently as well as behave differently than expected, criminals can modify the operating system, its application. For example:- splash screens replacing and removing is a widely discussed modification in phone forums.

If the phone is switched on, identification of the phone can be seen by the information displayed on the screen. On the display screen the manufacturer's or service provider's logo or name may appear, the family of operating system is indicated by the screen layout. The battery cavity may also contain information relevant to the manufacturers make and model (*e.g.*, MAKE, MODEL, IMEI, and ESN). Always be careful if you are removing the battery from the device due to lack of power it can affect its state, particularly the volatile memory and its related contents. Mostly cell devices keep user data in non-volatile memory as on the safe side, with the certain smart phones exception.

17.1. Device Characteristics

By its particular characteristics a phone manufacturing can sometimes be identified, if there is an unique design elements exist if it is observable. To identify a particular device that can be queried and obtain its specifications and features on selected attributes, for this there are various web sites contain phones databases, on selected

17.2. Device Interface

The power connector if often specific to a manufacturer and a reliable aid to identification. Manufacturer of certain devices can be readily identified with familiarization and experience. To create a connection to host a computer then the size, number of contacts, and shape of a phone data cable interface are often specific to a particular manufacturer and may prove helpful in.

17.3. Device Label

If phone is switched off, particularly when appropriate database is coupled, the information obtained can be revealing within the battery cavity, The Federal Communications Commission Identification Number (FCC ID), which is the model number of the phone as well as unique identifiers and an equipment identifier (IMEI or ESN) often listed by the manufacturer's label. In the U.S. domestics market, the FCC and equipment identifiers can be found on the cell phones then sold. The SIM is usually located under the battery and Integrated Circuit Card Identification (ICCID) is typically imprinted with GSM or other SIM bearing phones, an unique identifier For powered on GSM and UMTS phones, with the help of keying in *#06# the International Mobile Equipment Identifier(IMEI) can be obtained. To obtain the Electronic Serial number (ESN) from powered offer databases, where similar codes exist for querying the identifier and providing information about the devices.

17.4. IMEI

In this there are 15 digit numbers those indicate country of approval for GSM devices as well as the model and manufacturer type. Type Allocation Code (TAC) defined as the starting 8- digit portion which gives the model and origin of the IMEI. An IMEI reminder is manufacturer specific at the end with a check digit. From the GSM numbering plan Website, a database lookup service is always available.

17.5. ESN

Unique 32-bit identifier recorded on a secure chip in a mobile phone with the help of the manufacturer. With the help of first 8-14 bits, manufacturer is identified then the serial number assigned by bits those are remained. In many phones have codes that can be input into the handset to display the ESN. Besides the ESN, the phone number of the device as a useful information can be obtained. At the telecommunication Industry Association Web Site the manufacturer codes can be checked on-line

17.6. The ICCID

ICCID can be up to 20 digit long and country code follow an industry identifier prefix (89 for telecommunications), an issuer identifier number, and identification number of an individual account. ICCID determined the country and network operator name. If the ICCID does not appear on the SIM it can always be obtained with a SIM acquisition tool. GSM numbering plan Website supports ICCID Queries for this information.

18. Tool Selection

Once you have identified the make and model, you can review available manuals from different cell forensic hardware and software to find out which one best match up to your device. Again remember forensic software each piece's has strengths and weakness against the available manuals that select the mist appropriate tool with the help of measuring up the device. On the Google or another search engine additionally you can try typing the model number which can be also reveal a significant requirements for forensic tools as a fundamental set, it should be considered when a choice of tools is available:-

- **Usability**
  Useful point for an investigator is that the ability to present data in a form.
- **Comprehensive**
  To present all data to an investigator, Inculpatory and exculpatory evidence can be identified the ability.
- **Accuracy**
  A margin of error as certained and the output of the tool has been verified defines the quality.
- **Deterministic**
  To produce the same output, when given the same set of instructions and input data tool defines the ability
- **Verifiable**
  To ensure accuracy of the output by having access and to present the results and intermediate translation.

Here is a list of the most utilized tools for conducting an acquisition for cellular devices:-

18.1. Nuetrino

Guidance software has the ability to gather logical or physical image from cell phones (Supports limited amount of phones).

FIGURE 3. Nuetrino

18.2. Cellebrite

It has the ability to gather logical image only (active system) from cell, phone but supports numerous cell phones. (May require writes to device for image gathering).

FIGURE 4. Cellebrite

18.3. Data Pilot Secure View

It works in conjunction with Susteen cables to gather a logical image only of cellular device.

FIGURE 5. Data Pilot Secure View

18.4. Mobile Edit

It works in conjunction with Susteen Cables to gather a logical image only of cellular device.

18.5. XRY

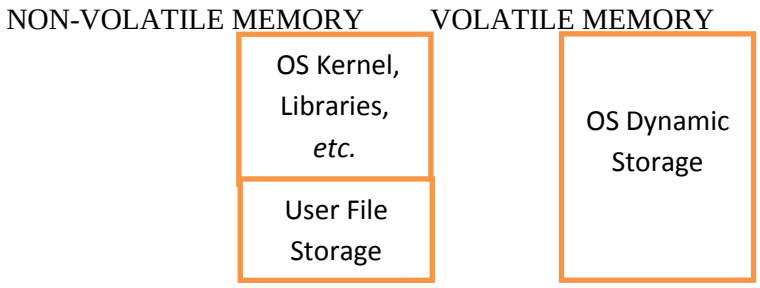
Physical device that allows logical imaging while producing an encrypted data file to protect the contents against unwarranted eyes.

FIGURE 6. XRY

19. Evidentiary Value Information-Memory:-

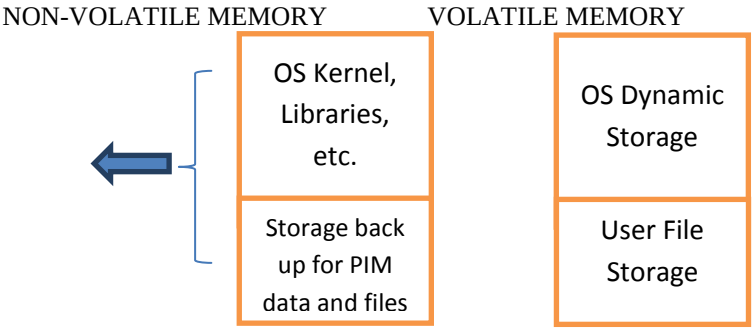
A mobile phone exists with volatile and non-volatile memory which can include:-

- Storage for the device drivers, system libraries and operating system code, including the kernel.
- Memory for storing and user applications execution loaded onto the device for applications of executing operating system.
- To user storage for different kinds of text, image, audio, video, and other data files, which include PIM application data.



STORAGE ASSIGNMENTS

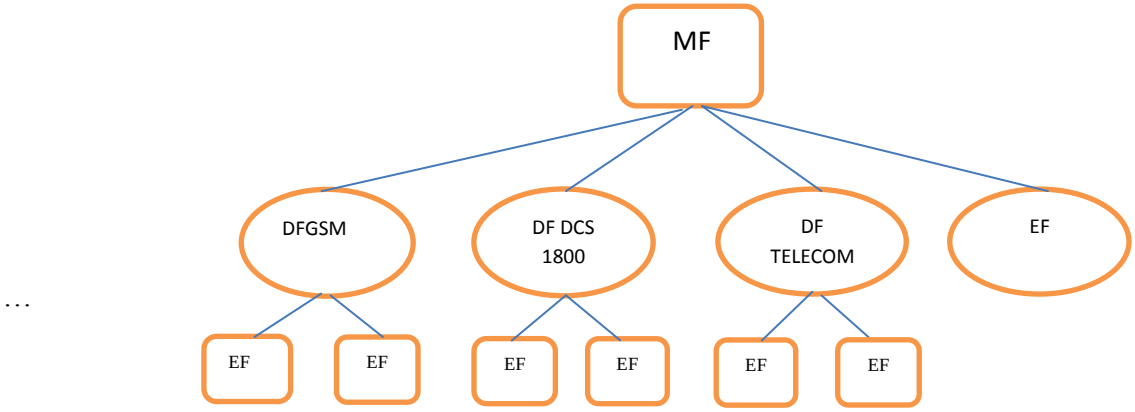
Phone memory structure may be distributed for certain data into fixed areas, such as entries in phonebook, call logs, and SMS messages (Text, Multimedia *etc*.,) or dynamically assign of memory that may also be structured more rigorously from a common shared pool. By using mainly in smart phones with PDA heritage the arrangement of a common alternative memory, is shown below. For dynamic storage and user file storage, volatile memory is used. To hold the operating system code a non-volatile memory is used, and it is possible that by the user from the volatile memory PIM data or files are backed up.



ALTERNATIVE STORAGE ASSIGNMENTS

A SIM has both volatile and non-volatile memory and it is similar to a mobile phone that can contain the same data with general categories as found in a mobile phone. From sub processor SIM draws power that's why it can be thought as a trusted sub-processor like phone interfaces. SIM file system is organized as tree structure in a hierarchical format resides in nonvolatile memory and it is composed of three types of elements: File system root (MF), subordinate directory files (DF), and elementary data which contain files (EF). Diagram explains the file system structure below. The EFs under DF (GSM) and (DCS 1800) vary mainly information based on network for operation of different frequency bands. The EFs under DF (Telco) contain service related information.

In elementary data files scattered throughout the file system there is a lot of different digital evidence reside and be recovered from a SIM. Some of the same information held in the SIM may be maintained in the mobile phone memory and encountered as same. Other than the standard files defined in the GSM specifications. Many of the general categories of evidences those can be found in elementary data files with standard are as follows:



…

19.1. Service Related Information

SIM Unique identifiers are the Subscribers, the Integrated Circuit Card Identification (ICCID) and the International mobile Subscriber Identity (IMSI).

19.2. Phonebook and Call Information

Abbreviated Dialing Numbers (AND) and Last Numbers Dialed (LND).

19.3. Messaging Information

Short Message Service (SMS) textual messages and Enhanced Messaging Service (EMS) simple multimedia messages.

19.4. Location Information

Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications.

20. Cell Phone Imaging

20.1. Mobile Phone Acquisition

Many times the initial investigator will submit phones for laboratory processing with only recovery of specific items request, like that phone call logs record. If the investigators should have any questions about the scope of the information to search for or recover, the investigator should contact the person for clarification the exam initiation is recommended. To recover all available data though it is not always necessary, To redo the process later always avoided by complete acquisition, if other data is needed, and the possibility that technical problems may on a later attempt.

The data and time maintained on the mobile device is an important piece of information. Just as in conducting incident response procedures on a suspect or victim computer system, gathering the data and time of the cellular device is extremely important. The date and time may be obtained from the network or manually set by the user. Criminals or suspects may manually set the time with date from the actual one to a completely different value in the cell and messages records found on the phone to leave misleading values. If the phone was on when seized, the date and time to correlate how much the date and time of the cellular device id off compared to the current time and date. When the phone seized and switched off, the time with date maintained and it has differences of references clock that should be recorded as soon as possible in the laboratory when first turned on. Note that during acquisition process action must be taken, It may affect the time value maintained such as to view the device label we have to remove the battery label.

After an acquisition is finished, the forensic experts must confirm that the device contents were captured in a correct way. Thus, where possible, to have multiple tools available, it is always advisable and be ready to switch to another with the initial tool if difficulties occur. This is known as validation process.

Not for whole data viewable on a phone menus available used logical acquisition capture. For example, archived and draft messages sometimes can't be recovered by forensic tools. The contents via phone interface scrutinize manually menus the process not only allows such items to be consistent with observable data while video recording. With care and caution, manual acquisition must always be done, the integrity of the device is preserved in case further, more elaborate acquisitions need to be conducted.

21. GSM Considerations

CDMA phones and other mobile phones does not use identify module, these are pretty straightforward as the acquisition single device entailed in the above considerations which to be addressed. GSM phones on the other hand are slightly more complex because of the handset/SIM partitioning of the phone. Depending on the type of phone, whether it is on or off, and other conditions, the phone and SIM card could be acquired separate or together. If the handset in active mode, a joint acquisition of the SIM card and handset contents should be carried out before the SIM is acquired directly. A direct acquisition recovers deleted messages present on a SIM, while via the handset an indirect acquisition does not. For direct acquisition the SIM must be inserted into an appropriate reader and removed from the phone. First reason for this sequence is that SIM removal, which is typically beneath the battery, Just because of the power disruption this can result in the non-volatile memory loss. Additionally, It's a fact in an active state that the device was kept when seized may be an indication that if power is lost some concern exists about triggering authentication or another security mechanism

If the handset is inactive mode, the SIM contents may be acquired independently before the inactive mode of handset. The SIM acquisition should be done directly through a SIM reader. When the SIM is not present the handset acquisition must be attempted in this case, an acquisition under such conditions permitted by many phones, allowing PIN entry for the SIM to be bypassed, if it were enabled. In the case of unsuccessful of acquisition attempt is, the SIM can be inserted again and another second attempt made. When a separate acquisition which is not dependent is performing (i.e. acquiring the SIM before acquiring the handsets contents) avoids any operating system based on forensic issues those are associated with SIM data indirect read. However, SIM on some phones removal can reportedly cause data to be deleted. In addition, to gain access to the SIM, battery removal is required. In certain phones, date and time loss values can occur. Similarly, from certain smart phones or handsets, when the battery will be removed, in volatile memory the user data can be lost if a second battery with good backup is not built-in to support replacement of battery or for a sufficient time that cannot maintain volatile memory. In that situation where lost data can occur, at the beginning of this section the acquisition sequence described for active phones should be followed.

21.1. SIMS

Similar to a mobile handset, data acquiring from a SIM a connection need to be established from the workstation of forensic or cellular device from the physical device by using a reader. As previous, the tool version being used should be documentation format, along with any applicable patches or errata from manufacturer applied to the tool. Once the connection has been established, the forensic software tool can be proceed to acquire data from device.

Capturing a direct image of the SIM data is not possible reason behind it is the mechanisms of protection built into the module. Instead, command directives sent by

forensic tools called Application Protocol Data Units (APDUs) to the SIM to extract data logically, without modification, from each elementary file system's data file. The APDU protocol defined as the normal command response exchange. Each file system element has a unique numeric identifiers assigned which is defined in the GSM standards, which may be used to walk through the file system, element reference recover a data and some operation are performed, such as contents reading.

22. Conclusion

Emerging wireless technologies have made cell phones units the most widely used electronic devices in the world with over 3 billion subscribers. Understanding the capabilities of wireless networks is critical for investigators to remain in step with the latest trends in communication and the capabilities end users have with the increasing availability of high-speed networks. Investigators should have a properly equipped toolbox in order to respond to the various types of situations they may counter. Depending on the type of investigation on scene processing may be necessary. Investigators should be prepared with all the necessary forms, processing equipment and documentation capabilities. Various phone types and operating systems require different individual processing equipment. In this paper i have discussed how to protect devices when seized at the crime scene from being accessed, how to identify what tools are the best choice imaging or acquisitions, and what information can will be obtained. So in order to make sure I access the device correctly we must protect the device from outside communications, determine what device you have seized, Choose tool for imaging, verify you have correct image, document everything.

References

[1] R. Diclemente, "Brief Cellphone delivered counseling as a novel strategy to enhance the maintenance of HIV behavioral intervention efficacy", Handout from World Aids Conference, **(2010)** July 16.
[2] J. Wills, M. Parker and G. Wills, "Social and community Informatics and social theories of networks", University of Southampton, United Kingdom.
[3] The majority of the Labs case study is drawn from - Parker MB, B.Tech, M.Tech b Wills J, BA(Hons), MA b Wills GB, BEng (Hons), PhD. Reconstructed Living Lab: supporting drug users and families through co-operative counseling using mobile phone technology.
[4] M. R. Mothokoa, "Research Update. Pretoria: Directorate Health Systems Research, Research Co-ordination and Epidemiology", National Department of Health, South Africa, vol. 5, no. 2, **(2003)**, pp. 1-3.
[5] R. Velleman and L. Templeton, "Family interventions in substance misusers: A guide to theory and practice", In: Petersen T, Mc Bridge A, eds. Working with substance misusers. London: Routledge; **(2002)**, pp. 145–52.
[6] A. J. Flisher, C. D. H. Parry, J. Evans, M. Muller and C. Lombard, "Substance use by adolescents in Cape Town: Prevalence and correlates", Journal of Adolescent Health 003; vol. 32, no. 1, pp. 58–65.
[7] A. E. Barrett and R. J. Turner, "Family structure and substance use and early adulthood: Examining explanations for the relationship", Addiction vol. 101, no. 1, **(2006)**, pp. 109–20.
[8] A. C. Dumaret, M. C. Kuntz and M. Titrant, "Early intervention in poor families confronted with alcohol abuse and violence: Impact on families' social integration and parenting", Families in Society, vol. 90, no. 1, **(2009)**, pp.11–7.
[9] J. Garrett, J. Landau-Stanton and J. Stanton, "ARISE: A method for engaging reluctant alcohol and other drug dependent individuals", Journal of Substance Abuse Treatment, vol. 14, no. 3, **(1997)**, pp. 235-248.
[10] B. F. Skinner, "Science and Human Behavior", New York: Free Press. Retrieved October 17, 2007, from http://www.bfskinner.org/SHBtext.pdf Google Scholar, **(1953)**.
[11] K. J. Helsinki, "Radiation safety of handheld mobile phones and base stations, STUK–A 161, **(1999)**.
[12] A. W Preece, G. Iwi, A. Davies-Smith, K. Wesnes, S. Butler, E. Lim and A. Varey, "Effect of a 915-MHz simulated mobile phone signal on cognitive function in man", Int J Radiat Biol, vol. 75, pp. 447, **(1999)**.
[13] S. Braune, C. Wrocklage, J. Raczek, T. Gailus and C. H. Lucking, "Resting blood pressure increase during exposure to a radio frequency electromagnetic field", Lancet, vol. 351, pp. 1857, **(1998)**.
[14] K. J. Rothman, J. E. Loughlin, D. P. Funch and N. A. Dreyer, "Overall mortality of cellular telephone customers", Epidemiology, vol. **7**, pp. 303, **(1996)**.

[15] N. A Dreyer, J. E. Loughlin and K. J. Rothman, "Cause-specific mortality in cellular network telephone users". JAMA, vol. 282, **(1999)**, pp. 1814.
[16] L. Hardell, "Use of cellular telephones and the risk for brain tumors: a case–control study", Int. J Oncology, vol. 15, **(1999)**, pp. 113.
[17] M. K. Hansson, "Comparison of symptoms experienced by users of analogue and digital mobile phones", Arbetslivsrapport, vol. 23, **(1998)**.
[18] C. Johansen and J. H. Olsen, "Cellular telephones, magnetic field exposure, risk of brain tumors and cancer at other sites: a cohort study" Radiate Prot Dosim., vol. 83, **(1999)**, pp. 155
[19] J. Jarrat and J. F. Coates, "Future Use of Cellular Technology: Some Social Implications", Telecommunications Policy, **(1990)** February, pp. 78–84.
[20] K. Lange, "Some concerns about the future of mobile communications in residential markets", In M Christ offers on (Ed.), Telecommunication: Limits to deregulation Amsterdam: IOS Press, **(1993)**, pp. 197–210.
[21] L. F. Rakow and V. Navarro, "Remote mothering and the parallel shift: Women meet the cellular telephone", Critical studies in mass communication, vol. 10, **(1993)**, pp. 144-157.
[22] R. Ling, and B. Yttri, "Micro and hyper-coordination through the use of the mobile telephone", In Katz, J. and Aakhus, M. (Eds.), Perpetual contact: Mobile communication, private talk, public performance. Cambridge: Cambridge University Press, **(2002)**.
[23] C. Licoppe, "Connected presence: the emergence of a new repertoire for managing social relationships in a changing communications techno scape", Environment and planning: Society and space, vol. 22, **(2004)**, pp. 135–156.
[24] T. H. Christensen, "Connected presence' in distributed family life", New Media & Society, vol. 11, no. 3, **(2009)**, pp. 433–451.

