# Chapter 3 - Mobile Phone Forensics

The field of mobile forensics has exploded in recent times and is now one of the most important areas of research, for several reasons. First and foremost, the capabilities of cellphones have been greatly enhanced. These devices are arguably more important than desktop or laptop computers because they are generally always turned on and usually always mobile. Therefore, they continually record our movements and our activities and provide tremendous insight into our behaviour. Communication on a cellphone is very different compared to a traditional computer. Interestingly, criminals often say or text things on a cellphone that they would never do on a traditional computer.

Cellphone forensics has not always been taken seriously. Even in 2008, if you had asked someone in law enforcement about investigating cellphones, you would have typically heard that nobody in the laboratory worked on cellphones or that cellphones did not hold anything of value. Some people might even have said that the only reason for cellphone forensic software was that some suspicious spouses bought the software to see if their partner was cheating.

Hardware imaging devices have also been used for a number of years but were not originally used for investigations. Cellebrite sold its hardware to cellphone retailers who needed a device to copy the contents of a customer's cellphone and its SIM card to another cellphone, usually when the customer wanted to upgrade to a new phone. When law enforcement became involved in cellphone investigations, Cellebrite made some minor modifications and began selling many more devices.

Cellphone forensics was always important, but not many people realized its importance. This is not surprising: The available cellphone forensic software could not work with the vast majority of cellphones. After Internet capabilities were added to cellphones, their importance to investigations grew. With this demand came better forensic software. Suddenly, more evidence was available, including email, Internet searches, and social networking activity. Today just about every computer forensics laboratory has cellphone forensic capabilities. Additionally, there has been a separation of duties in larger laboratories. For example, one investigator may be responsible for extracting evidence from the cellphone, while another investigator might be responsible for much of the paperwork, including subpoenas to cellphone carriers. Yet another investigator may be responsible for gathering and analyzing data from base transceiver stations. A **base transceiver station (BTS)** is the equipment found at a cell site that facilitates the communication of cellphone users across a cellular network.

Cellphone forensics has tremendous challenges, however. A huge number of cellphones still cannot be imaged. Forensic software and hardware supports only the most popular cellphones more than a hundred new cellphones come to market each year, but many will never be supported by forensic tools. Some of the most problematic cellphones to examine are the inexpensive pay-as-you-go phones from companies like TracFone. Issues also exist with some cellphones from the other smaller cellular companies, like Virgin Mobile, Boost, and MetroPCS.

The issue of encrypted mobile platforms and applications for mobile devices developed by companies like Silent Circle is also relevant. The Blackphone is another challenge for investigators because the developers claim to protect the user's privacy through advanced encryption. Investigators also face a plethora of operating systems running on cellphones today. An investigator working with a laptop will generally encounter a Microsoft Windows operating system or Apple's Mac OS X (operating system). An investigator who obtains a cellphone, on the other hand, could encounter a Symbian, RIM, Windows, iOS, Android, or other mobile device operating system.

In looking to the future, our dependency on cellphone forensics will only increase, and the number of vendor-supported cellphones and tablets will expand. The vociferous market for Android and iOS devices means that the investigator must look outside the device more to the synced computer, to the synced devices in the home and at work, and to the cloud. Cellphones continue to have a growing dependence on cloud computing, which means that investigators will increasingly rely on evidence that goes beyond the scope of the network carrier. Integrated user applications found on the cellphone, like Facebook and Gmail, are important and will increase in importance.

## 3.1 Recent developments in mobile technology

### 1. Multi-platform/Multi-architecture Application Development Tools

Most organizations will need application development tools to support a "3 x 3" future — three key platforms (Android, iOS and Windows) and three application architectures (native, hybrid and mobile Web). Tool selection will be a complex balancing act, trading off many technical and non-technical issues (such as productivity versus vendor stability), and most large organizations will need a portfolio of several tools to deliver to the architectures and platforms they require.

**2. HTML5**

HTML5 won't be a simple panacea for mobile application portability because it's fragmented and immature and therefore poses many implementation and security risks. However, as HTML5 and its development tools mature, the popularity of the mobile Web and hybrid applications will increase. Hence, despite many challenges, HTML5 will be an essential technology for organizations delivering applications across multiple platforms.

**3. Advanced Mobile User Experience Design**

Leading mobile apps are delivering exceptional user experiences, which are achieved by a variety of new techniques and methodologies, such as motivational design, "quiet" design and "playful" interfaces. Designers are also creating apps that can accommodate mobile challenges, such as partial user attention and interruption, or that can exploit technologies with novel features or "wow" factors, such as augmented reality. Leading consumer apps are setting high standards for user interface design, and all organizations must master new skills and work with new partners to meet growing user expectations.

**4. High-Precision Location Sensing**

Knowing an individual's location to within a few meters is a key enabler of the delivery of highly relevant contextual information and services. Apps exploiting precise indoor location currently use technologies such as Wi-Fi, imaging, ultrasonic beacons and geomagnetics. In 2014, Gartner expects growth in the use of wireless beacons using the new Bluetooth Smart standard. In the longer term, technologies such as smart lighting will also become important. Precise indoor location sensing, combined with mobile apps, will enable a new generation of extremely personalized services and information.

**5. Wearable Devices**

The smartphone will become the hub of a personal-area network consisting of wearable gadgets such as on-body healthcare sensors, smart jewelry, smart watches, display devices (like Google Glass) and a variety of sensors embedded in clothes and shoes. These gadgets will communicate with mobile apps to deliver information in new ways and enable a wide range of products and services in areas such as sport, fitness, fashion, hobbies and healthcare.

**6. New Wi-Fi Standards**

Emerging Wi-Fi standards such as 802.11ac (Waves 1 and 2), 11ad, 11aq and 11ah will increase Wi-Fi performance, make Wi-Fi more relevant to applications such as telemetry, and enable Wi-Fi to provide new services. Over the next three years, demands on Wi-Fi infrastructure will increase as more Wi-Fi-enabled devices appear in organizations, as cellular offloading becomes more popular, and as applications such as location sensing demand denser access-point placement. The opportunities enabled by new standards and the performance required by new applications will require many organizations to revise or replace their Wi-Fi infrastructure.

**7. Enterprise Mobile Management**

"Enterprise mobile management" or "EMM" is a term that describes the future evolution and convergence of several mobile management, security and support technologies. These include mobile device management, mobile application management, application wrapping and containerization, and some elements of enterprise file synchronization and sharing. Such tools will mature, grow in scope and eventually address a wide range of mobile management needs across all popular OSs on smartphones, tablets and PCs.

**8. Mobile-Connected Smart Objects**

By 2020, the average affluent household in a mature market will contain several hundred smart objects, including LED light bulbs, toys, domestic appliances, sports equipment, medical devices and controllable power sockets, to name but a few. These domestic smart objects will be a part of the Internet of Things, and most will be able to communicate in some way with an app on a smartphone or tablet. Smartphones and tablets will perform many functions, including acting as remote controls, displaying and analyzing information, interfacing with social networks to monitor "things" that can tweet or post, paying for subscription services, ordering replacement consumables and updating object firmware.

**9. LTE and LTE-A**

Long Term Evolution (LTE) and its successor LTE Advanced (LTE-A) are cellular technologies that improve spectral efficiency and will push cellular networks to theoretical peak downlink speeds of up to 1 Gbps, while reducing latency. All mobile users will benefit from

improved bandwidth, and superior performance combined with new features such as LTE Broadcast will enable network operators to offer new services.

**10. Metrics and Monitoring Tools**

The diversity of mobile devices makes comprehensive app testing impossible, and the non-deterministic nature of mobile networks and the cloud services that support them can result in performance bottlenecks that are hard to locate. Mobile metrics and monitoring tools, often known as application performance monitoring (APM), can help. APM provides visibility into app behaviour, delivers statistics about which devices and OSs are adopted, and monitors user behaviour to determine which app features are being successfully exploited.

## 3.2 Cell Phone Theory

### 3.2.1 The Cellular Network

A cellular network is a group of cells . A cell refers to a geographic area within a cellular network. A cell site is a cell tower located in a cell. When you make a call with your cellphone, you connect with a cell tower. The communication is then transmitted to the Mobile Switching Center. The **Mobile Switching Center (MSC)** is responsible for switching data packets from one network path to another on a cellular network. If the user is calling a user on a cellular network managed by another carrier, the call is routed from the MSC to the Public Switched Telephone Network. The **Public Switched Telephone Network (PSTN)** is an aggregate of all circuit-switched telephone networks. The purpose of the PSTN is to connect all telephone networks worldwide, this is where tolls for connecting calls across different networks are calculated. Figure below details the path of a cellphone call.

### 3.2.2 Base Transceiver Station

A cell site, also known as a cell tower, can be a stand-alone tower or can be attached to a building or other structure. The cell tower generally has an antenna with three panels on each side. Typically, each antenna has three sides. Usually the middle panel is a transmitter, and the two outer panels are receivers. The cell tower is generally over 200 feet high. A tower can contain multiple antennae, which are owned by different carriers. An antenna can be located on a cell tower or placed on the side or top of a building.

The Base Transceiver Station (BTS) is the equipment at the cell site that facilitates communication between the cellphone user and the carrier’s network. A **Base Station**

**Controller (BSC)** manages the radio signals for Base Transceiver Stations, in terms of assigning frequencies and handoffs between cell sites. When moving through an area, several Base Transceiver Stations might handle your call a handoff would occur from one BTS to another. There are two types of handoff.

In a **soft handoff** , a cellular communication is conditionally handed off from one base station to another, and the mobile equipment is simultaneously communicating with multiple Base Transceiver Stations. The handoff is conditional because the signal strength on a new BTS are adjudicated. In a **hard handoff** , the communication is handled by one Base Transceiver Station at a time, with no simultaneous communication.

### 3.2.3 Mobile Station

The **mobile station** consists of mobile equipment (handset) and, in the case of a GSM network, a Subscriber Identity Module (SIM). An **International Mobile Equipment Identity (IMEI)** number uniquely identifies the mobile equipment or handset. The initial six or eight digits of the IMEI are the Type Allocation Code . The **Type Allocation Code (TAC)** identifies the type of wireless device. The website www.nobbi.com/tacquery.php allows an investigator to enter a TAC or IMEI to discover details about a specific device. The IMEI is generally found by removing the back of the cellphone and then looking under the battery.

A **Universal Integrated Circuit Card (UICC)** is a smart card used to uniquely identify a subscriber on a GSM or UMTS network. With a GSM network, the smart card is a SIM; with a UMTS, the smart card is a Universal Subscriber Identity Module (USIM).

A **Mobile Equipment Identifier (MEID)** is an internationally unique number that identifies a CDMA handset (mobile equipment). The MEID was previously referred to as an Electronic Serial Number (ESN) before it was replaced by a global MEID standard around 2005. An **Electronic Serial Number (ESN)** is an 11-digit number used to identify a subscriber on a CDMA cellular network. The ESN contains a manufacturer code and a serial number that identifies a specific handset. Both the ESN and the MEID are noted on the handset in both decimal format and hex format. The website www.meidconverter.com allows users to convert between ESN and MEID and also view both decimal and hex values of an ESN or MEID. Some providers, like Virgin Mobile USA, provide a lookup feature for subscriber details using the MEID.

### 3.2.4 SIM Card

The **SIM card** identifies a user on a cellular network and contains an IMSI. SIM cards are found in cellphones that operate on GSM cellular networks and usually in iDEN network cellphones. A user can simply add a SIM card to an unlocked cellphone. Not all U.S. cellphone carriers allow a user to purchase a SIM card and use the handset on another network. In the European Union (E.U.), generally all GSM-compatible cellphones can be unlocked. In fact, in some E.U. countries, it is illegal for cellphones to be locked.

The **International Mobile Subscriber Identity (IMSI)** is an internationally unique number on the SIM card that identifies a user on a network. The **Mobile Country Code (MCC)** is the first three digits of the IMSI. The proceeding two to three digits are the Mobile Network Code (MNC). For example, MNC 026 for MCC 310 represents the carrier T-Mobile USA. The final part of the IMSI is the MSIN, which consists of up to 10 digits.

A **Mobile Subscriber Identity Number (MSIN)** is created by a cellular telephone carrier and identifies the subscriber on the network. The **Mobile Subscriber ISDN (MSISDN)** is essentially the phone number for the subscriber. The MSISDN is a maximum of 15 digits and is comprised of the Country Code (CC), the Numbering Plan Area (NPA), and the Subscriber Number (SN). Country Codes are relatively easy to find. For example, in the Americas the CC is 1 because it is in Zone 1. For Trinidad and Tobago, it is 1-868. European countries are in Zone 3 and Zone 4. For example, Ireland, in Zone 3, is 353, and the United Kingdom, in Zone 4, is 44. The Numbering Plan Area for Nassau County, New York, is 516 and is also referred to as the area code.

The SIM card also includes an ICCID. The **Integrated Circuit Card ID (ICCID)** can be a 19- to 20-digit serial number physically located on the SIM card, or it can contain fewer numbers.


**Fig: SIM Card**

The first two digits of the ICCID are referred to as the Major Industry Identifier (MII). The ICCID can be accessed via the SIM card in the EF_ICCID file.

### 3.2.5 International Numbering Plans

The website www.numberingplans.com is a tremendous resource for mobile forensics examiners working with GSM cellphones. The website provides "Number Analysis Tools", which allow the user to conduct an analysis of the following:

- Phone number
- IMSI number
- IMEI number
- SIM number
- ISPC number

An **International Signalling Point Code (ISPC)** is a standardized numbering system used to identify a node on an international telecommunications network.

### 3.2.6 Authenticating a Subscriber on a Network

The Mobile Switching Center is where user information passes to the Home Locator Register, Visitor Locator Register, and Authentication Center. The **Home Locator Register (HLR)** is a database of a carrier's subscribers and includes those users' home addresses, IMSI, telephone numbers, SIM card ICCIDs, and services used. The **Visitor Locator Register (VLR)** is a database of information about a roaming subscriber. A subscriber can be found on only one HLR but can exist in multiple VLRs. The current location of a mobile station (handset) can be found on a VLR as well. The VLR also contains the Temporary Mobile Subscriber Identity. The **Temporary Mobile Subscriber Identity (TMSI)** is the handset is switched on, and is based on the geographic location.

The **Equipment Identity Register (EIR)** is used to track IMEI numbers and decide whether an IMEI is valid, suspect, or perhaps stolen. The **Authentication Center (AuC)** is a database that contains the subscriber's IMSI, authentication, and encryption algorithms. The Authentication Center issues the subscriber an encryption key that encrypts wireless communications between the mobile equipment and the network.

## 3.3 Smart Operating Systems

A phone's operating system (OS) has a significant impact on any forensic examination. The OS

determines what artifacts are created and how they are stored. Modern cell phone operating systems include Symbian, Apple iOS, Windows CE and Windows Mobile, Google's Android, RIM OS and Blackberry OS.

**Android OS:**

Android is an open-source OS that is currently developed by Open Handset Alliance. In 2005, Google acquired the Android OS from Android, Inc. In 2007, the Open Handset Alliance was formed and has been developing the OS ever since. The Open Handset Alliance "is a group of 84 technology and mobile companies who have come together to accelerate innovation in mobile and offer consumers a richer, less expensive, and better mobile experience" (Open Handset Alliance, 2007). Some of the members include Sprint, T-Mobile, LG Electronics, Inc., Kyocera, Motorola, Google, and eBay. Thousands of third-party apps are available to augment Android's core functionality. Android is found on handsets produced by Motorola, Sony Ericsson, and HTC (Barbara, 2010b).

**Symbian OS:**

**Symbian** is a mobile device operating system developed by Nokia and currently maintained by Accenture. Symbian was the most popular mobile operating system as of 2012, although Android was the fastest-growing OS. Symbian OS can be found on Nokia, Sony Ericsson, Samsung, and Hitachi handsets, to name but a few. However, Nokia has been moving away from Symbian OS, in favour of Windows OS. Nokia has transferred support for Symbian OS to Accenture.

**Research in Motion (RIM) OS:**

**RIM OS** is the operating system developed by Research in Motion (RIM) for use on BlackBerry smartphones and tablets. Although they are limited, BlackBerry APIs are available to allow for third party development. The BlackBerry OS is now open source system, however. Because many organizations issue their employers BlackBerry devices, these smartphones can provide a wealth of evidence. The BlackBerry was developed with corporate productivity in mind, so this device can attain Internet access through a carrier's data plan but can also work in Wi-Fi hotspots.

In fact, with BlackBerry 7.1 OS, the device can connect to a hotspot and then become a mobile hotspot for up to five devices. BlackBerry Tablet OS is an operating system developed for the

BlackBerry PlayBook tablet computer. Unlike Google's Android OS, which runs on handsets manufactured by a wide variety of providers, RIM OS works only on BlackBerry devices.

It is important for an investigator to understand that, even without access to the BlackBerry handset, the investigator can access a wealth of handset evidence from the computer that a suspect or victim synced to. An IPD Backup File is file backup from a BlackBerry that is found on a synced computer or medium. The files can be recognized by their .ipd file extension. More importantly, these IPD files are unencrypted and might be more accessible from a computer than from the device itself (which could be PIN protected).

Many tools available allow an investigator to parse, view, and search through these files. One tool is Elcomsoft Blackberry Backup Explorer. The software works with the IPD files on a Mac or Windows computer and can extract email, SMS, MMS, call logs, Internet activity, appointments, photos, and other user-created files. Elcomsoft also produces a password recovery utility for purchase.

**Windows OS:**

**Windows** is a Microsoft operating system that can be found on personal computers, mobile phones, and tablets. It resides on mobile phones manufactured by HTC, Samsung, Nokia, and others. Examining Windows smartphones can be problematic and often requires JTAG to download data from the handset. The good news is that the files downloaded using JTAG are NTFS and do not need to be converted. **Internet Explorer Mobile** is the web browser, based on Internet Explorer 9, found on Windows Phone devices. **People Hub** is an address book tool found on Windows Phone devices that can synchronize contacts from social networking sites like Facebook, Twitter, and LinkedIn. Windows Phone supports POP and IMAP email protocols, including Hotmail, Gmail, and Yahoo! Mail, and can sync contacts and calendars from these services. Zune is the application used for managing multimedia files on Windows Phone devices. As one would expect, .WMV files are supported, but so too are AVI, MP4, MOV, and 3GP/3G2 file formats.

**iOS:**

Apple's popular iOS can be found not only on the iPhone but also on other mobile devices such as the iPad and the iPod touch. iOS is based on Apple's Mac OS X, which is used on their laptops and desktops. iPhones make heavy use of third-party apps that are purchased/downloaded from the Apple App Store.

## 3.4 Mobile Phone Forensics

Mobile devices are dynamic systems that present challenges from a forensic perspective. Additionally, new models of phones are being developed globally, with some experts postulating that five new phone models are released every week. The growing number and variety of mobile devices makes it difficult to develop a single process or tool to address all eventualities. In addition to a growing variety of smart phones and platforms including Android systems, Blackberry, Apple iPhone, and Windows Mobile, there are a massive number of low-end phones using legacy OS systems.

Furthermore, there are some unique considerations when preserving mobile devices as a source of evidence. Most mobile devices are networked devices, sending and receiving data through telecommunication systems, WiFi access points, and Bluetooth piconets. Digital evidence in mobile devices can be lost completely as it is susceptible to being overwritten by new data or remote destruction commands it receives over wireless networks. Additionally, in order to extract information, it is necessary to interact with the device, often altering the system's state. As with any computer, interacting with a mobile device can destroy or alter existing evidence.

Mobile devices are challenging from a data recovery and analysis standpoint as well. With their increasing functionality and growing data stores, mobile devices are becoming analogous to computers with specific functions (mainly as a conduit for communications and Internet access). Keeping up with all of the various file systems, data formats, and data sources on mobile devices is an ongoing challenge.

However, a major advantage of mobile devices from a forensic perspective is that they can contain deleted information even after an individual has attempted to render it unrecoverable. The underlying reason for this persistence of deleted data on mobile devices is in the use of Flash memory chips to store data. Flash memory is physically durable against impact, high temperature, and pressure, making it more difficult to destroy. In addition, Flash memory has a limited number of writes and can only be erased block-by-block, and mobile devices generally wait until a block is full before erasing data. Furthermore, mobile devices use proprietary wear levelling algorithms to spread write/erase across Flash memory blocks, which can result in deleted data remaining for some time while new data are written to less used portions of memory. In order to access and recover older/deleted copies of data, it is necessary to acquire a full copy of physical memory.

For all the collection, extraction, and analysis issues mobile devices present, they are an excellent source of digital evidence and can provide insight unavailable from other devices. Additionally, the personal nature of the device makes it easy to establish the last mile evidence required to tie a device to an individual.

## 3.5 Logical v/s Physical extraction

The data on a cell phone can be acquired in one of two ways: physically or logically. A physical acquisition captures all of the data on a physical piece of storage media. This is a bit-for-bit copy, like the clone of a hard drive. This acquisition method captures the deleted information as well. In contrast, a logical acquisition captures only the files and folders without any of the deleted data. Data can be collected using non-forensic tools such as those used to synchronize or back up the data on the cell phone. While this process is similar to the one used to acquire a hard drive, there is one important difference. In this instance no write blocking device is used. The phone must be able to interact with the phone's hardware and software.

Mobile forensic tools provide a logical or physical extraction of evidence from a cellphone or sometimes both. Similar to examining a personal computer, a logical examination of a cellphone provides a traditional view of the directories, files, and folders, and it can be compared to the interface we see with Windows File Explorer on a PC or Finder on a Mac. The physical view refers to the actual location and size of files in memory. Only a physical examination can retrieve deleted messages and other deleted files.

A major difference with computer forensics and mobile forensics is that, with a physical view of files on a computer, we can find file fragments. However, when an SMS text message is deleted, you can typically be certain that the message has been removed and no message fragments exist. A physical extraction can resurrect some deleted files, however.

## 3.6 Mobile Phone Forensics Tools

There are many, many different tools available to forensically examine a phone. These tools can come in the form of hardware or software. One of the realities is that not all of these tools support all cell phones. To further complicate matters, two tools that actually support a given phone may not read and recover the same information.

A close examination of the function and features shows that no single tool does it all. One glaring difference is the number of phones that are supported. Forensic tools are in constant

development to provide a convenient means of extracting specific data from various mobile devices, typically logically via cable, infrared, and Bluetooth or physically via cable or JTAG. All of these tools function in a similar way, sending commands to the phone and recording responses that contain information stored in the phone's memory. The information that can be extracted using these methods depends on both the connection mechanism and model of the phone.

Logical mobile phone acquisition systems interact with the phone operating system to extract data, much in the same way the vendor synchronization systems do. As such, there are limitations to the information retrievable, and only information relevant to the Operating System is available. As such, information potentially relevant in a forensic investigation might not be acquired, information such as deleted items won't be extracted. Mobile phones generally have a baseline of extractable data from such tools: phone address book, call register, SMS and photographs, but additional information is not guaranteed.

The limitation to these forms of applications is that it relies on the assumption that the desktop application and the investigator are assuming that the phone's logic is not making any changes to other areas of the phone's memory. However, this assumption cannot be verified without the source code and circuit schematics of the phone's software and hardware, which are rarely, if ever, publicly available.

**MicroSystemation XRY** (http://www.msab.com) is one of the market leaders in mobile device acquisition. MicroSystemation sell products to capture mobile phones and other small-scale devices logically via USB, infrared, and Bluetooth. XRY also has an additional component, XACT, that expands capability by performing physical acquisition via the JTAG interface. XACT also allows for the acquisition of specific models of GPS receiver. Figure 20.14 shows the XRY acquisition interface.

**Logicube CellDEK** (http://www.logicubeforensics.com) is a system designed to acquire data from mobile phones and other small-scale devices such as GPS receivers. CellDEK conducts logical extraction of data via USB, infrared, and Bluetooth.

**MOBILedit! Forensic** (http://mobiledit.com) is another logical data acquisition tool. MOBILedit! Forensic can be purchased as a software-only tool or as part of a kit including cables and infrared reader.

**iXAM** (http://www.ixam-forensics.com) is a forensic acquisition system specifically for the

Apple iPhone and Apple iPod Touch. iXAM acquires data via the USB interface, but has full physical extraction of data. Ixam is a niche system, only providing acquisition of a small number of devices from a single manufacturer.

**BitPim** is a robust open-source application that was not built for forensic purposes. BitPim is designed to work with CDMA phones that are produced by several vendors, including LG and Samsung among others. BitPim can recover data such as the phonebook, calendar, wallpapers, ring tones, and file system (http://www.bitpim.org/).

**Oxygen Forensic Suite** is a forensic program specifically designed for cell phones. It's a tool that supports more than twenty-three hundred devices. It extracts data such as phonebook, SIM card data, contact lists, caller groups, call logs, standard and custom SMS/MMS/e-mail folders, deleted SMS messages, calendars, photos, videos, JAVA applications, and GPS locations (http://www .oxygen-forensic.com/en/).

**Paraben Corporation** offers several hardware and software products targeted to mobile device forensics. In addition to cell phones, their tools also support GPS devices such as those from Garmin (http://www.paraben.com/handheldforensics.html)

**AccessData's MPE+** supports over thirty-five hundred phones. It's an on-scene, mobile forensic recovery tool that can collect call history, messages, photos, voicemail, videos, calendars, and events. It can analyze and correlate multiple phones and computers using the same interface. (http://accessdata.com/ products/computer-forensics/mobile-phone-examiner).

**The Cellebrite UFED** (Universal Forensic Extraction Device) is a stand-alone, self-contained hardware device used to extract Phonebook, images, videos, SMS, MMS, call history, and much more. It supports over twenty-five hundred phones and is designed to extract information on scene. It also has a SIM card reader and cloner. As an interesting aside, Cellebrite devices (the nonforensic version) can be found in many cell phones stores. They're used to transfer a customer's data from one device to another.

(http://www.cellebrite.com/forensicproducts/ forensic-products.html?loc=seg).

**EnCase Smartphone Examiner** is an EnCase tool designed to review and collect data from smartphones and tablet devices. It collects data from Blackberries, iTune backups, and SD cards. Once the information is collected, it is easily imported into the EnCase Forensic suite for continued investigation.

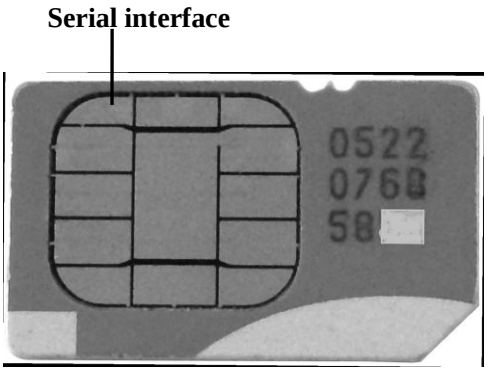
(http:// www.guidancesoftware.com/encase-smartphone-examiner.htm).

## 3.7 SIM Card Forensics

The two primary functions of a SIM card are to identify the subscriber to a cellular network and to store data. We have already discussed the mechanism by which the IMSI on the SIM identifies a user on a GSM or iDEN network. More important to the investigator is the SIM card's storage of important evidence. A SIM is essentially a smart card that is comprised of a processor and memory.

**SIM Hardware**

SIM cards have different form factors. The Mini-SIM is 25mm × 15 mm, and the Micro-SIM is 15mm × 12mm. There are also embedded SIM cards. Printed on the outside is a unique serial number called an ICCID. The serial interface is the area where the SIM card communicates with the handset, as in Figure.




**SIM File System**

The Electronically Erasable Programmable Read Only Memory (EEPROM) is where the hierarchical file system exists. The operating system, user authentication, and encryption algorithms are found on the SIM card's read-only memory (ROM).

There are three primary components of the file system:

**1.** Master File (MF) that is the root of the file system

**2.** Dedicated Files (DFs), which are basically directories

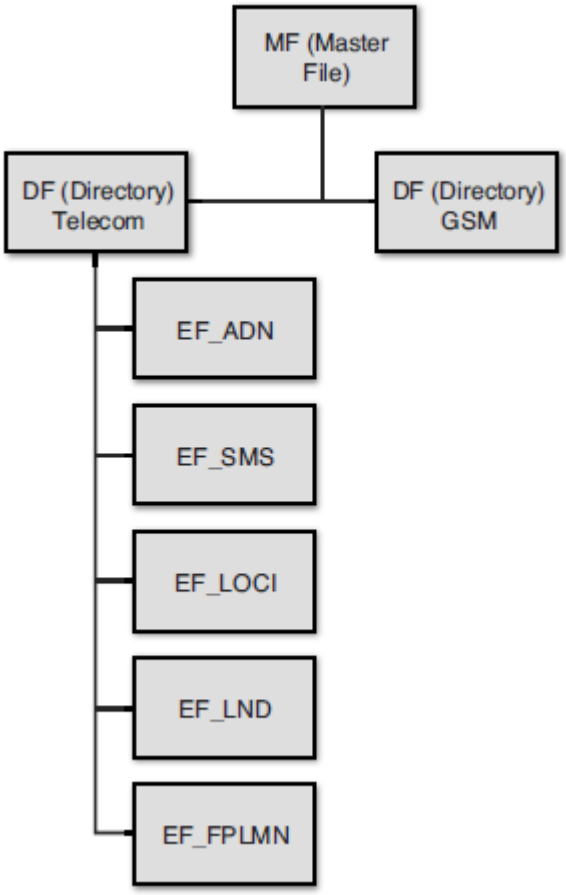
**3.** Elementary Files (EFs), where the data is held

The latter is where investigators can retrieve a tremendous amount of subscriber information. **Abbreviated Dialing Numbers (ADN)** contains the contact names and numbers entered by the subscriber. On the SIM, these contacts are located in the folder EF_ADN. **Forbidden Public Land Mobile Network (FPLMN)** refers to cellular networks to which a subscriber attempted to connect but was not authorized to do so. This information can be found in EF_FPLMN. This data can assist investigators who want to know where a suspect was located, even if he or she was unsuccessful in connecting to a network. **Last Numbers Dialled (LND)** refers to a list of all outgoing calls made by the subscriber. The folder EF_LND holds this information. EF_LOCI contains the Temporary Mobile Subscriber Identity TMSI, which is assigned by the Visitor Locator Register (VLR).

The TMSI represents the location where the mobile equipment was last shut down. The TMSI is four octets long and will make no sense to the investigator. However, the investigator could contact the carrier for assistance with determining the location represented by the TMSI. Table below provides the definitions of the acronyms used in the SIM file system.

| Acronym | Definition |
|---|---|
| EF_ADN | Abbreviated Dialing Numbers (ADN) |
| EF_FPLMN | Forbidden Public Land Mobile Network (FPLMN) |
| EF_LND | Last Numbers Dialled (LND) |
| EF_LOCI | Area where the user last powered down the phone. |
| EF_SMS | Short Message Service (SMS) |

**Fig: shows the SIM directory structure.**




**Access to the SIM:**

Gaining access to the data on a SIM is challenging if the SIM card has been PIN protected. A PIN on a SIM is usually four digits long but can be up to eight digits. An investigator has three attempts to get the PIN correct before the SIM is locked. After that, the device prompts for a PUK (Pin Unlock Key) or PUC (Personal Unblocking Code. An investigator can request a PUC from the carrier. A **Personal Unblocking Code (PUC)** is a code that is available from the carrier and allows a user to remove the PIN protection from the SIM card.

**Note:** A user can go online and change the PUK. The investigator then would be unable to access the contents of the SIM without the cooperation from the subscriber.

**SIM Card Clone:**

Similar to hard disk drive cloning, an investigator often chooses to clone a SIM card instead of examining the original SIM card. As a best practice, a SIM card clone should be used in the investigation in place of the original. Most cellphone forensic tools enable the investigator to clone a SIM card.

**Types of Evidence:**

The range of evidence available from a cellphone is quite different from what can be acquired from a laptop or desktop. One of the primary differences is the existence of SMS and MMS messages, which the following section explains in detail.

**Short Message Service (SMS):**

**Short Message Service (SMS)** is a text message communication service found on mobile devices. These text messages can be found in memory on a mobile handset or on a SIM card in the handset. SMS messages are mostly saved on the handset, but when stored on the SIM card, they can be found in the DF_TELECOM file. An investigator can determine whether an SMS message has been read, deleted, or sent based on the status flag. The byte value changes based on the status of the message. Table below identifies the values of the status flag and their meanings.

| Status Flag Value (Binary) | Description |
|---|---|
| 00000000 | Deleted message |
| 00000001 | Read message |
| 00000011 | Unread message |
| 00000101 | Sent message |
| 00000111 | Unsent message |

When viewing the text message with a hex editor, an unread SMS message begins with 11, a deleted message begins with 00, and so forth.

**Multimedia Messaging Service (MMS):**

**Multimedia Messaging Service (MMS)** is a messaging service found on most cellphones that allows the user to send multimedia content, like audio, video, and images. Using a cellphone forensics tool, the investigator can carve this multimedia content out of the user's messages. MMS can be retrieved from a SIM or from the mobile device.

## 3.8 Call Data Records

Call detail records (CDR) are normally used by the provider to troubleshoot and improve the networks performance. The CDR is also valuable to examiners.

They can show us:

■ Date/time the call started and ended.

■ Who made the call and who was called.

■ How long the call lasted.

■ Whether the call was incoming or outgoing.

■ The originating and terminating towers.

Although the CDRs can tell us a lot, what they cannot tell is who actually made the call. You get what you ask for, therefore it is important to understand the difference between the CDR and the subscriber information. Subscriber information and the call detail records are not the same. Typical subscriber information would include things such as the name, address, and telephone. Other items included with subscriber information are account numbers, e-mail addresses, services, payment mechanisms, and so on.

Every service provider keeps all of these records for a predetermined period of time. The time period is spelled out in their data retention policies.

The retention period is also not uniform across all of the data types. For example, some carriers may keep SMS data for only seven to fourteen days. By contrast, cell sector information could be kept a year or longer. The takeaway here is that you don't have an unlimited amount of time to file the necessary paperwork to ensure that the records you seek won't get purged.

Carriers generally maintain meticulous records of subscribers and their activities for billing and other purposes. This stockpile of information can be enormously helpful during an investigation. These carrier records can tell us the subscriber's name, address, additional phone numbers, Social Security number, and so on. The credit information on file can give investigators billing addresses, credit card numbers, and more.

The call detail records describe the specifics of each incoming and outgoing call. These should not be confused with toll records. Toll records refer to landline information rather than mobile phones. When asking for the call detail records, you must specify a date range. It's a wise

practice to pad your request with a day or two on both ends.

The call detail records, when combined with the physical addresses of the towers, can show us the call's origination and termination locations. These records also show the cell sites that were used, the length of the call, the time the call began, the numbers dialled by the target phone, and so on.

The billing records do not represent a complete list of the inbound and outbound calls. The call logs will include data that have not yet made it into the billing system.

Information kept by the carriers will likely have a short, predetermined shelf life. Each carrier has some discretion on how these data are preserved and how long they're stored. This is usually described in the company's retention policies. In light of this practice, the legal paperwork should be generated and served sooner rather than later. This will help to ensure that your evidence won't get purged before it can be preserved and collected.

Cell phones can be located (with varying degrees of accuracy) by a few different means. Triangulation is one of the better-known methods. In triangulation, the phone's approximate location is determined using its distance from three different towers. The distance is calculated by determining the signal delay from the phone (or handset) to the three towers. A directional antenna can also be used for this purpose. Again, the signal delay is used to determine the distance, but this time only two towers are needed since they are able to also determine the direction. Finally, the location can be determined via GPS using latitude and longitude.