

Book 7 - Mobile Forensics


1.	FUNDAMENTALS OF MOBILE DEVICES AND CELLULAR NETWORK	2
2.	MOBILE FORENSICS PROCESS, METHODS AND TECHNIQUES.....	51
3.	MOBILE FORENSIC TOOLS	99
4.	MOBILE DEVICE FORENSICS	135
5.	U/SIM CARDS FORENSICS	173

1. Fundamentals of Mobile Devices and Cellular Network

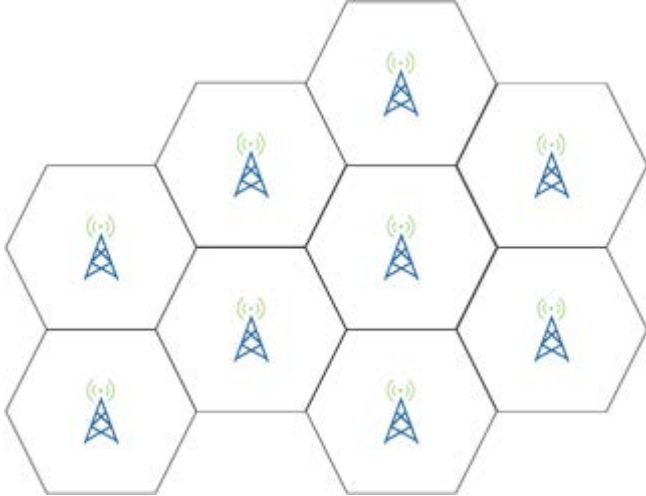
Scope Template															
Number	1														
Title	Fundamentals of Mobile Devices and Cellular Network														
Introduction	This chapter explains the core concepts of mobile devices and cellular networks. It starts by exploring the history of cellular networks, its architecture and the enabling technologies that facilitate it. Then, it highlights the evolution of mobile devices such as smartphones and smart cards. Finally, it briefly states the related standards, societies and common body of knowledge for mobile forensics.														
Outcomes	Demonstrate a solid understanding of the various mobile enabling technologies.														
Topics	1.1. Cellular Network 1.1.1. Evolution of Cellular Network and its History 1.1.2. Cellular Network Architecture and Technologies 1.1.3. Introduction to AT/AT+ Commands 1.2. Mobile Device Hardware 1.2.1. Evolution of Mobile Device and its History 1.2.2. Mobile Device Architecture and Technologies 1.2.3. Mobile Operating Systems 1.3. Smart Cards 1.3.1. Subscriber Identification Module (SIM/USIM) 1.3.2. SIM/USIM File Management 1.3.3. SIM/USIM Security 1.4. Standards, Societies and Body of Knowledge														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th><th>Time</th></tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td><td>2 hr</td></tr> <tr> <td>Textbook Content:</td><td>4 hr</td></tr> <tr> <td>Thinking (On-line discussions, Review questions)</td><td>1 hr</td></tr> <tr> <td>Tutorial Work:</td><td>3 hr</td></tr> <tr> <td>Related Course Work:</td><td>1 hr</td></tr> <tr> <td>Total</td><td>11 hours</td></tr> </tbody> </table> <ul style="list-style-type: none"> Required study time: 4 one-hour lectures, and 1 three-hour lab lecture for the introduction to AT commands (1.1.3). Required hardware/software: <ol style="list-style-type: none"> GSM Modem (unlocked). Putty for Windows. Required external resources including links and books: <ol style="list-style-type: none"> Rank, W., Effing, W. (2010). Smart Card Handbook, 4th Ed. Wiley. Retrieved from https://onlinelibrary.wiley.com/doi/book/10.1002/9780470660911 Mayes, K., & Markantonakis, K. (2008). Smart Cards, Tokens, Security and Applications. Springer. Retrieved from http://www.springer.com/computer/security+and+cryptology/book/978-0-387-72197-2 Limited, C. (2017). MOBILE NETWORKS MADE EASY: A simplified view of mobile networks for professional audience. AT Command Modem Manual (we will be using a Huawei modem) http://download-c.huawei.com/download/downloadCenter?downloadId=510 	Task	Time	Preparation (Introduction and On-line Planning):	2 hr	Textbook Content:	4 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	3 hr	Related Course Work:	1 hr	Total	11 hours
Task	Time														
Preparation (Introduction and On-line Planning):	2 hr														
Textbook Content:	4 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	3 hr														
Related Course Work:	1 hr														
Total	11 hours														

	47&version=120450&siteCode&usg=AOvVaw3RL07ZaVYO8 Ln23TpmIDVZ
--	---

Content Template	
Section Number	1.1
Section Title	Cellular Network
Introduction	<p>This section explores the history of cellular networks showing how the technology evolved from the first two-ways radio to the current 5G technology. It then illustrates the cellular networks architecture and its underlying enabling technologies. Finally, it introduces the AT/AT+ commands that are used to communicate with mobile devices.</p> <p>Upon completion of this section the student will be able to:</p> <ul style="list-style-type: none"> • Have clear understanding of the history of cellular networks, its architecture and underlying technology. • Correlate how the advances in cellular networks may affect mobile forensics. • Have a working understating of AT/AT+ commands.
Content	<p>With the widespread of mobile devices and the introduction of smartphones and wearable technology, mobile forensics has become a vital tool for investigators in solving many cases. In fact, a smartphone nowadays is an extremely personal device as opposed to computers and laptops; I bet you will not find two persons sharing the same smartphone yet you can find several people sharing a PC or a laptop.</p> <p>The excessive amount of information collected by these devices can indeed help in many forensic cases. Your smartphone can show your location history, it can point out your frequently called contacts, it maintains your conversations on social networks, it saves your web browsing history, it stores the photos that you have taken as well as where and when you have taken them, and much more. It can even indicate when you go to sleep and when you wake up.</p> <p>However, for a mobile device to work, it has to rely on a complicated infrastructure of interconnected wired and wireless communication networks also known as Cellular or Mobile Networks. This creates a challenge for mobile forensic investigators because artifacts are often fragmented among the different components of the cellular network.</p> <p>In this chapter, we will briefly explore the systems that constitute cellular networks and explain how their evolution affected mobile forensics.</p>

Content Template	
Section Number	1.1.1
Section Title	Evolution of Cellular Network and its History
Introduction	
Content	<p>Cellular Networks have undergone a tremendous evolution over the past decades, from the introduction of the first two-way HAM radio in 1921 to the production of the first mobile phone in 1983 and to the current state-of-the-art 5G technology (see Figure 1).</p> <p>Prior to the nineties, cellular networks used to operate using analogue networks, which often refers to as the first generation of cellular networks (1G). In that era (1970s-1980s), mobile phones were bulky devices, which weights over 1 kg, and can only make voice calls.</p>  <p>Figure 1. The Evolution of Mobile Devices.</p> <p>In the 1980s, the digital forensic tools were also basic tools that aim to retrieve lost or deleted files from computer systems. The mobile devices at that time did not have the capability to store and manage any relevant information. Therefore, mobile forensics did not exist at that time.</p> <p>The 1990s had witnessed the birth of the second generation of cellular networks (2G), which operated using digital technology as opposed to the first generation (1G) which operated using analogue networks. Furthermore, two new standards for cellular networks emerged that shaped the mobile industry for years to come worldwide; namely, the Global System for Mobile communications (GSM) standard by the European Union (EU) and the Code-Division Multiple Access (CDMA) standard by the USA. This allowed service providers to introduce new services such as Short Message Service (SMS), Multimedia Messaging Service (MMS), caller ID, internet access, navigational maps and many more.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>GSM network used A5/1 and A5/2 stream ciphers to encrypt the communications; however, both have serious security vulnerabilities. How can this affect mobile digital forensics?</p> </div>

	<p>As the use of cellular networks became more widespread in addition to the advancement that accompanied it to the mobile devices development, which were capable of doing much more than their predecessors 1G devices, have increased the demand for the mobile forensics field. Yet, investigators relied on manual techniques to examine the evidence by manually interacting with the mobile device and collecting the artifacts such as call logs and calendar entries. However, some cases required the use of non-forensic commercial tools such as "Flasher tools", which were used to read the content of the flash memory.</p> <p>By the 21th century, the third and the fourth generation of cellular networks (3G and 4G) have emerged bringing with them high-speed internet access and more bandwidth, which resulted in the birth of new genre of mobile devices such as smartphones, tablets and wearable gears. The Universal Mobile Telecommunications System (UMTS) is the new standard of the 3G of cellular network, which is based on the GSM standard. While, the Long Term Evolution (LTE) and the LTE Advanced standards succeeded the UMTS as the 4G standards.</p> <p>With the upcoming fifth generation of cellular network (5G) technology is just around the corner, carriers are planning for it to be deployed in selected markets by the end of 2018. This evolutionary technology promises significantly reduced latency at considerably higher speeds of maximum peek of up to 20 Gbps, which existing mobile devices do not have the necessary technology to accommodate it. Additionally, experts and industry leaders are working on expanding the current cellular network architecture to accommodate Device-to-Device (D2D) communication, which can take huge advantage from the high speed and low frequency that come with the 5G technology.</p> <p>In this era, mobile devices start being an essential part of day-to-day life and with the immense amount of information that these devices hold; the mobile forensics field has tremendously grown to accommodate this advancement. Nowadays, mobile forensics has evolved with new solution both at hardware and software level readily available to end-users to facilitate the examination process.</p> <p>In the near future, the evolutionary 5G technology will become a reality for the end consumers and it is anticipated that it will reshape the mobile forensics industry, but how?</p>
--	--

Content Template	
Section Number	1.1.2
Section Title	Cellular Network Architecture and Technologies
Introduction	
Content	<p>Cellular network is a complex infrastructure of interconnected wired and wireless networks operated by cellular network operator to provide its registered users with mobile network connection within predefined geographical locations.</p> <p>In order to satisfy the mobile nature of cellular network, the geographical area is divided into multiple "cells". In this context, cell refers to a virtual area covered by the cellular communication technology (see Figure 2).</p>  <p>Figure 2. Conceptual view of Cellular Network.</p> <p>Generally, cellular network consists of four key subsystems which are:</p> <ol style="list-style-type: none"> 1. Mobile Station (MS): consists of the Mobile Equipment (ME) such as smartphones and the SIM card, which both are referred to as the User Equipment (UE). 2. Access Network (AN): refers to the radio network that connects the MS subsystem to the Core Network. It consists of multiple Base Transceiver Station (BTS), Base Station Controller (BSC) and Antennas (cell towers). 3. Core Network (CN): is responsible for providing the mobile services such as voice calls, messages, roaming, internet access, etc. It consists of multiple subsystems that facilitate these functions in addition to connecting the MS to the external network. 4. External Network: a collection of different networks and their systems such as the internet and the landline phone system. <p>Figure 3 shows the architecture of the GSM cellular network and highlights its main components, followed by the definition of some of the key terminologies.</p>

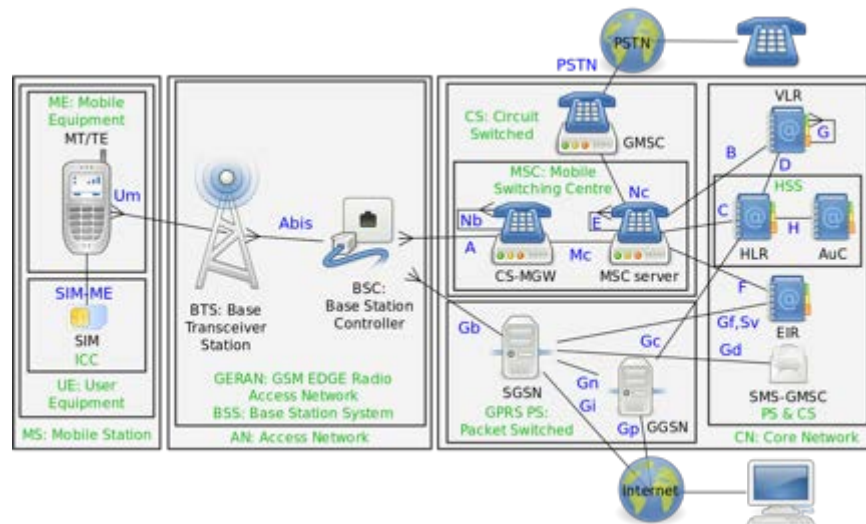


Figure 3. Architecture of the GSM Cellular Network.
[https://en.wikipedia.org/wiki/File:Gsm_structures.svg].

1. **Mobile Station Components:**

- Mobile Equipment (ME)** refers to any device capable of communicating on GSM cellular network such as mobile phones, MiFi modems and pagers.
- Subscriber Identification Module (SIM):** a type of smart cards that is used to store information about the Subscriber such as the IMSI, ICCID, MSISDN, address book and SMSs. Each SIM card holds a 128-bit key that is used to authenticate the SIM on the cellular network. SIM cards are used in the 2G cellular network.
- Universal Integrated Circuit Card (UICC):** It is considered as the new generation of SIM cards, which refers to the hardware that is running the USIM. UICC was introduced to support the functionalities of the 3G cellular networks.
- Universal Subscriber Identity Module (USIM):** refers to the application running on top to the UICC. It is similar in functionality to SIM but provide enhanced security, supports contactless payment and capable of running multiple applications.
- Subscriber:** a registered customer with a specific cellular network operator.
- User Equipment (UE):** combination of U/SIM and ME.

2. **Access Network Components:**

- Base Station Subsystem (BSS):** consists of one or more BTS and BSC.
- Base Transceiver Station (BTS):** consists of transceivers and antennas and it is responsible for handling the radio communications between the UE and the BSC. Each BTS corresponds to a single Cell.
- Base Station Controller (BSC):** is responsible for controlling multiple BTSs and perform tasks such as managing the radio channels allocation in addition to handling the handover of ME from one BTS to another.

	<p>3. <u>Core Network Components:</u></p> <ul style="list-style-type: none"> a. Network Switching Subsystem (NSS): consists of the following main parts (MSC, HLR, VLR, EIR and AuC). b. Mobile Switching Center (MSC): is the central service delivery component in cellular network responsible for setting up and releasing the end-to-end connection, in addition to prepaid accounts billing. c. Short Message Service Center (SMSC): is the component responsible for handling SMSs in cellular network. It provides message store and forward service, in addition to timestamping messages. d. Home Location Registering (HLR): a central database that stores the information of all the subscribers of the cellular network operator. e. Visitor Location Register (VLR): a distributed database that stores the information of roaming MSs (foreigner subscribers) within an MSC. f. Equipment Identity Register (EIR): a central database of band MSs often integrated within HLR and it is used to block or monitor stolen mobile devices. g. Authentication Center (AuC): a central database the holds a protected copy of the authentication key, which is stored on each subscriber's U/SIM card. <p>4. <u>External Network Components:</u></p> <ul style="list-style-type: none"> a. Public Switched Telephone Network (PSTN): a global system of interconnected network infrastructure such as telephone landlines, microwave transmission links, communications satellite links and undersea telephone cables that are controlled by switching centers, which facilitates national, regional, and local communications. <p>5. <u>Unique Identifiers:</u></p> <ul style="list-style-type: none"> a. Mobile Station International Subscriber Directory Number (MSISDN): is simply the telephone number that you use to call or text someone (e.g. 962-79-1234567). It consists of 3 main parts, which are, Country Code, National Destination Code, and Subscriber Number. b. International Mobile Subscriber Identity (IMSI): a unique number that is used to identify a subscriber in cellular network. It is used as the primary key in HRL and VLR. c. International Mobile Equipment Identity (IMEI): a unique number that is used to identify a ME in cellular network. It includes information about the mobile device manufacturer, origin, model, and serial number. d. Integrated Circuit Card Identifier (ICCID): a unique number that is used to identify a SIM card internationally in cellular network. <p>For mobile forensic investigator, recording the information of IMSI, IMEI, and MSISDN is an essential task to maintain the integrity of audit trail. This information can also be used later on as a part of the forensic report or even as evidence.</p>
--	--

	<p>Moreover, several forensic artifacts can be collected from the ME, U/SIM, VLR, HLR and many other nodes that make up the cellular network. For instance, a deleted SMS can be recovered, <i>in some cases</i>, from the SMSC.</p> <p>It is important for the mobile forensic investigator to understand how cellular networks and mobile devices operate in order to be able to interpret the findings of the forensic tools correctly and in some cases to extract them manually when the automated tools fail. In chapter 4, we will talk in detail about artifacts extraction from mobile devices.</p>
--	--

Content Template	
Section Number	1.1.3
Section Title	Introduction to AT/AT+ Commands
Introduction	
Content	<p>In 1977, Dennis C. Hayes invented the first PC modem, which revolutionized the telecommunication industry for years to come. In 1981, Hayes invented the "Hayes Standard AT command", which is a command language that allows the modem to be controlled by software using standard serial port. Until today, it still the standard method to communicate with modems. Hayes's language is referred to simply as AT Command, and the "AT" is short for attention. Over the past three decades, several extensions to the standard AT language have emerged, which added more functionalities to accommodate the advances in cellular network technology.</p> <p>AT commands can be classified into three classes:</p> <ol style="list-style-type: none"> Standard AT commands (AT): also referred to as basic AT commands. They do not start with the "+" sign as opposed to the second type. They are used to perform basic tasks such as answering calls and dialing calls. Extended AT commands (AT+): start with either the "+" sign or the "&" sign and are used to perform advanced tasks such as registering ME to mobile network, selecting operator and sending SMS. Proprietary AT commands: a set of AT commands that only works with specific modems. <p>AT commands have four types:</p> <ol style="list-style-type: none"> Read: AT commands that are used to retrieve information from the modem. Set: AT commands that are used to modify or set a parameter value. Test: AT commands that are used to determine if the parameter value was implemented correctly. Execute: AT commands that are used to perform actions such as dialing a phone number. <p>The first three types of AT commands are defined under the parameter commands, while the latter is defined under the action commands.</p> <p>As any other language, AT command has its own syntax and semantics. Fortunately, the commands are straightforward and consist of a series of predefined string commands. Following we describe the general syntax of AT commands as defined by the ITU-T V.250 standard:</p> <ol style="list-style-type: none"> AT commands are case insensitive. A command line consists of a prefix, body, and termination character. In most cases, the command line starts with the prefix "AT" and ends with the carriage return character (<CR>, ASCII 13). The prefix "A/" can be used to repeat the execution of the previous command. Strings must be enclosed between double quotation characters. Example: "This is a String".

4. The response must be enclosed between the carriage return character (<CR>, ASCII 13) followed by the linefeed character (<LF>, ASCII 10). Example: <CR><LF>*some answer*<CR><LF>.
5. More than one AT commands can be concatenated in one command line. In the case, the prefix will not be repeated and the AT commands in the body are separated with semicolon ";".

In order to work with AT commands, you will need three components: (A) modem device, (B) serial cable either hardware or emulated, and (C) Serial Terminal software such as *Microsoft HyperTerminal* or *Putty* for Windows and *minicom* for Linux.

Remember: learning AT commands is an important skill to have as a mobile forensic investigator; however, you are not expected to master it!

AT commands are like a Swiss Army knife for the mobile forensics investigator, you might find yourself working on a case that requires you to use them. We list some example below:

- The mobile phone you are examining is running a proprietary/unknown Operating System (OS) and the mobile forensic software that you are using is not able to communicate with it correctly.
- Similar to the case above but this time the cable is not a standard cable.
- You are working in a case involving a SIM box, a device that hosts many SIM cards and it can be used by criminals to redirect VoIP traffic illegal onto cellular networks. In this case, you will need AT commands to retrieve the devices information such as Manufacturer, IMEI, Model, HW Version, etc.
- You need to validate the results of an open-source tool or that you need to automate some of the tasks.

Content Template	
Section Number	1.2
Section Title	Mobile Device Hardware
Introduction	<p>This section presents the bottom layers of mobile devices. This is represented by the mobile devices hardware and operating systems. The awareness of the hardware capabilities of mobile devices along with the unique behavior of its operating systems enables better digital forensics tasks by security specialties.</p> <p>Upon completion of this section the student will be able to:</p> <ul style="list-style-type: none"> • Have a clear understanding of the history of mobile devices evolution. • Have a good awareness of the common mobile devices' architecture and hardware components. • Distinguish among the common mobile devices' operating systems in terms of the model, licensing, and architecture.
Content	<p>The mobile devices have evolved tremendously over the past two decades. The evolution went hand in hand with the growth of computer hardware capabilities, software capabilities, and network capabilities as well. The evolution included several dimensions such as the hardware components that comprise a mobile device, the services offered by a mobile device, the introduction of new types of sensors periodically, the operating systems capabilities, and the licensing models.</p> <p>Starting with a mobile device that is able to perform the basic phone functionality, mainly making a phone call and texting, and ending with a smart mobile device that has several new services such as Internet browsing, purchasing, viewing videos, listening to audio, geo-based services, sensors based services, and many others.</p> <p>The invention of touch-based mobile devices in 2007, started by Apple with their iPhone product, led to a huge growth in the number of mobile devices users, who are able to use these advanced services.</p>



Content Template	
Section Number	1.2.1
Section Title	Evolution of Mobile Device and its History
Introduction	
Content	<p>Since its invention in 1844 by John Taylor, the telephone has dominated the means of communication for over 100 years. It was in the form of landline, where it is fixed to a specific location.</p>  <p>Figure 4. Example of a Landline Rotary Dial Telephone. [https://commons.wikimedia.org/wiki/File:Alt_Telefon.jpg]</p> <p>Its static nature restricted its use to the location where it existed. It was up until 1983, when Motorola came up with the first mobile phone, DynaTAC. It was the first step toward creating mobile phones. Its bulky nature, the requirement for enormous batteries to reach out to far cellular networks, and expensive cost, over \$3000, restricted its use to a limited number of users that time, but it was a revelation toward the potential opportunities it can bring to individuals and organization alike.</p>  <p>Figure 5. The First Mobile Phone: Motorola DynaTAC (1983). [https://www.pinterest.com/pin/17592254767472476/]</p> <p>The idea of mobile phones was appealing to the market. The continuous growth in hardware and software technologies made it possible to manufacture mobile phones of acceptable cost at the end of the eighties. In 1988, it witnessed the birth of the so-called Candy Bar phones. It was a new era, in which mobile phones became cheap and small that can fit into a pocket.</p> <p>In the period of 1998 to 2008, a new set of features were added to the mobile phone such as the ability to take pictures, listen to music, and perform Internet browsing in a basic way.</p>



Figure 6. Motorola RAZAR V3 Mobile Phone (2003).

[https://bt.bmcdn.dk/media/cache/resolve/image_1240/image/51/516246/180669-tynd-men-fed-motorola--.jpg]

An example of such a phone is the Motorola RAZAR phone showing in the given Figure 6. In addition, this period included the invention of mobile phones with larger screen sizes, keyboards, and WiFi enabled. The concept of an operating system of a phone became a common thing. Nokia 9000 Communicator is a perfect example of phones from that era.



Figure 7. Nokia 9000 Communicator (1998). [<https://www.pctipp.ch/tipps-tricks/workshops/artikel/kennen-sie-diese-knochen-noch-58864/3/>]

Although the mobile devices included several new features that made it smarter, the use of these advanced features such as Internet browsing was somewhat limited to people of high tech skills.

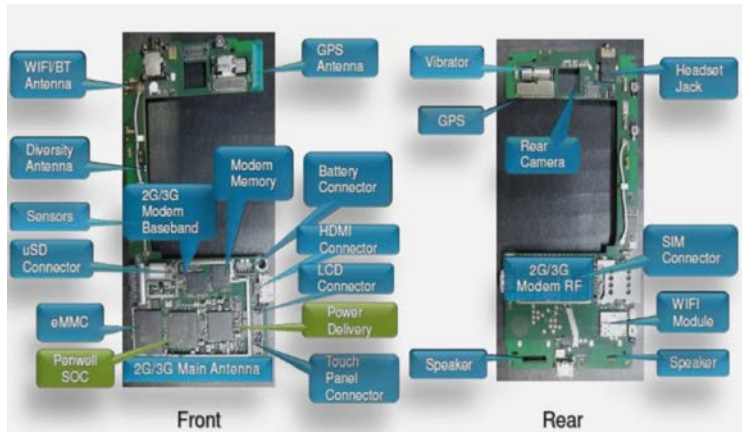
A major revolution was achieved in 2007. Apple started this with the invention of the iPhone as a touch phone. Several other companies followed their path of creating touch-based phones.



Figure 8. The First Generation iPhone from Apple (2007).

[<https://dayintechhistory.com/dith/june-29-2007-apple-releases-1st-gen-iphone-edge/>]

	<p>The phones from the touch era included a larger screen, with high resolutions, Wi-Fi support, 3/4G support, and the touch concept. The ability to operate most of your phone activities using touch activities was the most important change. It made it much easier for people to browse the Internet, to take pictures, to zoom in and out, to flip pages and images, and to scroll in all directions. This made it easier for people with a little technology background to use these advanced features. In addition, this era included the concept of third-party apps, and apps stores. This helped in growing the number of available applications to millions of applications, which created several innovative ways to use mobile devices in our daily tasks.</p>
--	--

Content Template	
Section Number	1.2.2
Section Title	Mobile Device Architecture and Technologies
Introduction	
Content	<p>Modern mobile phones have the following major hardware components:</p> <ol style="list-style-type: none"> 1. The main processor that executes the users' applications. 2. A 2G/3G/4G/5G baseband processor, which is responsible for executing the network activities, and control the radio actions. 3. A modern Memory 4. SIM cards. 5. Several peripheral devices for interacting with the user. Peripheral devices include sensors of several types such as light sensor, temperature sensor, etc. In addition, it includes Cameras, Microphone, Speaker, keypad or touch panel connector, display, 2G/3G/4G module and Antenna, WiFi/Bluetooth modules and Antennas, Battery, power connector, and USB/HDMI connector.  <p>The diagram illustrates the internal hardware components of a smartphone, divided into 'Front' and 'Rear' views. The 'Front' view labels include: WiFi/BT Antenna, Diversity Antenna, Sensors, uSD Connector, eMMC, Penwell SOC, 2G/3G Main Antenna, Modem Baseband, Modem Memory, Battery Connector, HDMI Connector, LCD Connector, Power Delivery, and Touch Panel Connector. The 'Rear' view labels include: GPS Antenna, Vibrator, GPS, Headset Jack, Rear Camera, SIM Connector, 2G/3G Modem RF, WiFi Module, and Speaker.</p> <p>Figure 9. Smartphone Components. [https://www.slideshare.net/ruliandi/system-on-chip-soc-44502780]</p> <p>Modern mobile devices became like a powerful PC, they have high processing capabilities, large memory sizes, and high bandwidth capabilities. This allowed mobile devices to compensate for the absence of a computer in many scenarios.</p>



Content Template	
Section Number	1.2.3
Section Title	Mobile Operating Systems
Introduction	
Content	<p>The operating systems of modern mobile devices can be categorized into three main categories:</p> <ul style="list-style-type: none"> • Licensed based • Proprietary • Open source <p>Examples of the licensed based OS is the Windows Mobile platform. Any company that manufactures mobile hardware can install the Window Mobile as a license and sell it along with the mobile phone. The user ends up paying for the license directly or indirectly.</p>  <p>Figure 10. Windows 10 Mobile OS. [http://www.sohu.com/a/229155256_413981]</p> <p>Apple uses a proprietary model for their iOS platform and operating system. It is closed from the outside, and its internals are kept as intellectual property to the company. Apple model combines the hardware with the operating system and sells this as one package.</p>  <p>Figure 11. Apple's iOS 7. [http://xtreme-mobile.com/iphone-5se-apples-next-4-incher-now-tipped-to-be-named.php]</p> <p>Google uses the open source model for their Android platform, where its mobile platform and operating system are open as a source code for the public to contribute to it. They do not charge for using the software. Any company that manufactures mobile phones can use the Android platform for free, once they are part of the Google established consortium.</p>



Figure 12. Android Logo. [https://www.taringa.net/+info/los-mejores-sistemas-mobiles_13cgen].

In general, the operating system of a mobile phone is similar in functionality to its peer in traditional systems. Figure 13 shows the architecture of the Android OS. The bottom layer is a customized version of Linux OS. On top of that comes the Android runtime system, which is a customized Java virtual machine, and next to it a set of libraries that can assist application developers to use ready built modules. One of the unique things about Android OS is the concept of managers. Different managers exist for different purposes. An application can use a manager to consume some mobile device service. For instance, a Sensor manager allows the applications to communicate with the different phone sensors. The availability of one instance of the manager to manage the sensors for all applications allows the Android OS to consume much fewer resources, which is a necessity in the world of mobile devices as the power resource of a mobile device, usually not connected to a charging source, is a precious resource for the end user.



Figure 13. Android OS Conceptual Framework.
[<https://developer.android.com/guide/platform/>]

Another unique thing about mobile devices' OS is the concept of an application process. In traditional operating systems, once a process is granted the resources to start, it will stay active, unless instructed by the end user to stop or ends by itself.

In the world of mobile devices where the resources are limited, the application process does not have the luxury to stay active all the time. For instance, the Android operating system views the processes as activities, and has a special activity life cycle as shown in the Figure 14. An activity goes to a stopped state if its window is covered by the window of another activity. This allows the Android OS to save power and memory resources.

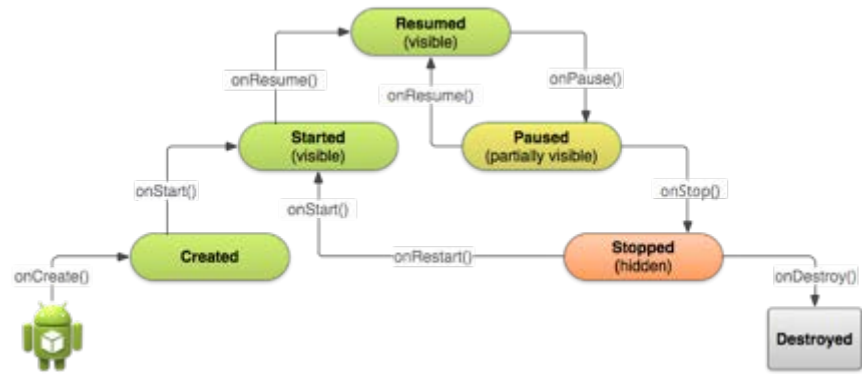


Figure 14. Android Activities Lifecycle. [<https://blog.eduonix.com/android-tutorials/how-to-manage-the-activity-lifecycle-stages-for-your-android-app/>]

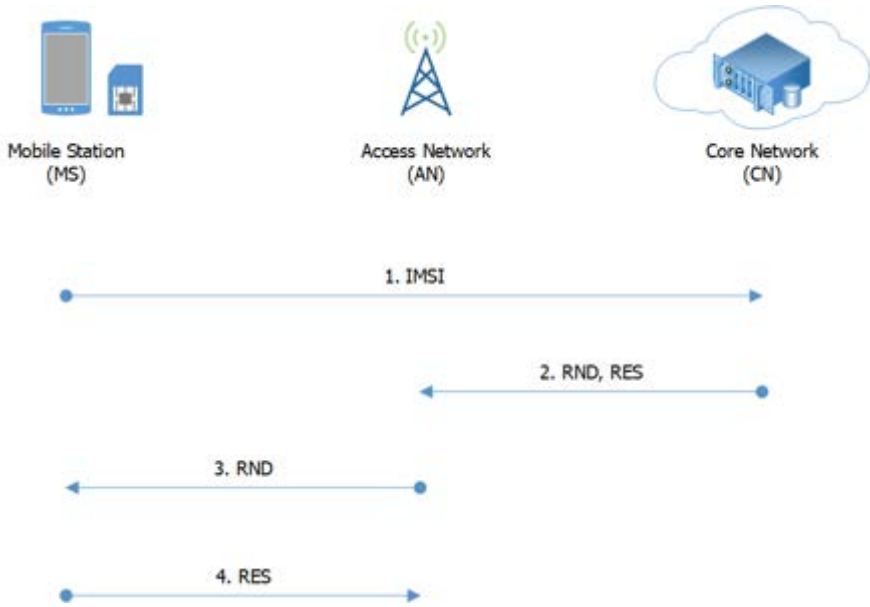
Content Template	
Section Number	1.3
Section Title	Smart Cards
Introduction	<p>This section starts by introducing smart cards, their history, technology, components and security features. Then, U/SIM cards are explored and their file management system is explained. Finally, the section is concluded by highlighting the security mechanisms used to protect U/SIM cards against common security attacks.</p> <p>Upon completion of this section the student will be able to:</p> <ul style="list-style-type: none"> • Have clear understanding of smart cards in general, U/SIM file management system, and U/SIM security controls. • Correlate how smart cards can affect mobile forensics.
Content	<p>Smart cards have been around since the late 1960s and undergo remarkable enhancement thereafter. A smart card is a microcomputer that is used primarily to store and exchange data in automated electronic transactions with heavy focus on security. Nowadays, smart cards are used in many applications such as banking, transportation, identity management, passports, telecommunications, healthcare, access control, entertainment and more. Smart cards come in many forms sizes, and shapes; typically, they are plastic cards or more accurately Polyvinyl Chloride card (PVC) such as credit cards and IDs. Alternatively, there is USB shaped cards such as authentication tokens (see Figure 16). Recently, smart cards have been implemented within smartphones.</p> <p>In essence, a smart card consist of processing unit, memory, power source (internal or external), and communication channel. The latter is used to distinguish between two main types of smart cards; that is, contact and contactless smart cards. As the name suggest, contact smart cards must make a physical contact with the reader in order to perform the transaction. They often have golden-plated contact pads that serve as the communication channel between the card and the reader. On the other hand, contactless smart cards rely on wireless technology to communicate with the reader such as Radio-Frequency Identification (RFID) and Near-Field Communication (NFC). The amount of memory varies between smart cards; it ranges from few bytes to hundreds of kilobytes.</p> <p>Some smart cards even host a tiny operating system that is used to run custom build applications. The Java Card OpenPlatform (JCOP) is such an example. Having an operating system running on the smart card allows the card to host many applications.</p>



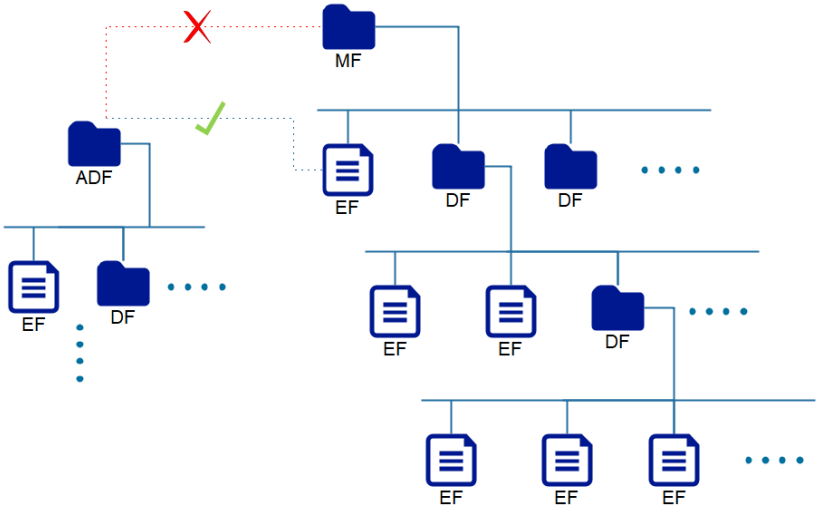
Figure 15. Example of Smart Cards.
 [https://commons.wikimedia.org/wiki/File:ImgSmartCards.JPG].

The level of security that a smart card employ varies differently depending on the application. Often, smart cards support several cryptographic algorithm such as asymmetric key generation, secure key management, encryption and decryption, hash functions, and random number generation.

From a forensic point of view, smart cards can be very useful in an investigation. It might be used to hide information about secret bank accounts or a forged card that was used to commit fraud. In mobile forensics, smart cards holds important artifacts such as IMSI, MSISDN, ICCID and other artifacts such as contacts and messages. In chapter 5, we will address SIM cards forensics in much detail.

Content Template	
Section Number	1.3.1
Section Title	Subscriber Identification Module (U/SIM)
Introduction	
Content	<p>During the 1G era of cellular networks, the information needed to authenticate the subscriber to the mobile network was stored directly into the mobile phone itself. This information was the MSISDN that is your phone number, and the Equipment Serial Number (ESN). The approach had many issues including lack of confidentiality, privacy and the fact that it was prone to fraud in which a criminal knowing someone MSISDN and ESN can clone them and make phone calls as if he/she was the legitimate subscriber. Another issue was that the user could not change his/her number without changing the phone itself. Since the introduction of 2G cellular network, specifically the GSM standard, this has all changed.</p> <p>The GSM standard introduced the use of the Subscriber Identification Module (SIM) Cards into the telecommunication industry. The primary role of a SIM card is to authenticate the subscriber to the cellular network securely prior granting him/her access to the network. Moreover, the SIM card can be used to hold more data such as address book, SMS settings and messages, preferred roaming list, last dialed numbers and much more. In section 5.2, we will address the artifacts that can be extracted from SIM cards in details. Because the SIM card can be removed, this meant that a user could change his/her phone simply by inserting the SIM card into the new phone as opposed to the previous approach in 1G networks.</p> <p>Furthermore, the security level was greatly improved. The data stored on SIM cards can be protected by a PIN code or multiple PIN codes. The subscriber authentication process to the cellular network was greatly improved as well. Instead of sending the MSISDN and ESN in clear, the GSM standard introduced a new challenge-response authentication mechanism. The mechanism works as follows (see Figure 18):</p>  <pre> sequenceDiagram participant MS as Mobile Station (MS) participant AN as Access Network (AN) participant CN as Core Network (CN) MS->>CN: 1. IMSI CN-->>MS: 2. RND, RES CN->>AN: 3. RND MS->>AN: 4. RES </pre> <p>Figure 16. Simplified Overview of GSM Subscriber Authentication Process.</p>

	<p>A. The ME sends the IMSI, which is stored on the SIM card, to the cellular network requesting registration. In fact, the IMSI is rarely exchanged; instead, a temporary value based on the IMSI also known as (TMIS) is used. Thus, improving the confidentiality.</p> <p>B. The cellular network generates a 128-bit random number (RND) and encrypt it using the corresponding key (128-bit) to the subscriber. This encrypted value is considered the response (RES). The network uses the IMSI/TMIS, which is mapped to the MSISDN, to locate the corresponding key.</p> <p>C. The network passes the random number to the ME, in which it passes it to the SIM card. Then, the SIM card encrypt the random number using its key and passes the result back to the ME in which it sends it to the network.</p> <p>D. If the value sent from the ME matches the one calculated by the network then the subscriber is authenticated.</p> <p>With the introduction of the third generation of cellular network (UMTS), the smart cards have witnessed tremendous improvements most notably is the logical separation between the application running on the smart card and the underlying hardware. In the UMTS system, the Universal Integrated Circuit Card (UICC) refers to the hardware portion of the smart card and is standardized by the ETSI TS 102 221 technical specification. While, the software of the smart card <i>in the telecom industry</i> is referred to as the Universal Subscriber Identity Module (USIM). The UICC serves as a general-purpose computing device for smart cards and the USIM maintains the functionalities of SIM cards in the GSM system such as the authentication of subscriber and network.</p> <p>This logical separation between hardware and software allows the smart card to host multiple applications at the same time while maintaining high level of security and backward compatibility. This also allows smart cards to be remotely provisioned; thus, allowing carriers to push updates to the U/SIM and perform Remote File Management (RFM) Over-The-Air (OTA).</p>
--	---

Content Template	
Section Number	1.3.2
Section Title	U/SIM File Management
Introduction	
Content	<p>Smart cards including U/SIM cards store data in files and each file consists of two parts, i.e. header and body. The header stores descriptive information about the file itself such as the file type, file structure and its access permissions. The body stores the actual data.</p> <p>The ISO/IEC 7816-4 standard defines the smart cards file system as a hierarchical tree structure composed of the following three main file types:</p> <ul style="list-style-type: none"> • Master File (MF) • Dedicated File (DF) • Elementary File (EF) <p>The Master File (MF) and the Dedicated File (DF) are directory file types; while the Elementary File (EF) is a data file type (See Figure 20).</p>  <p>Figure 17. Smart Cards File System Tree Hierarchy and File Types.</p> <p>Each MF, DF and EF has a unique Application Identification (AID) and a unique Name, which are defined by the 3GPP TS 51.011 specification for SIM cards and the 3GPP TS 31.102 for USIM cards. They can be selected using either their AIDs or Names depending on the SIM card. The AID is a predefined 2 bytes hexadecimal number.</p> <p>The Master File (MF) is the root directory of the file system, that is, the highest directory in any hierarchical file system. It contains all other dedicated and element files and its AID is '3F00'.</p> <p>The Dedicated File (DF) is similar to the "Folder" in modern computer operating systems, it contains lower level dedicated and element files and its AID starts with '7F'.</p> <p>It is worth mentioning that there is a special file type of DF defined by the ETSI TS 102 221 technical specification called Application Dedicated File (ADF). Unlike DF, ADF is not located under the MF. Under UMTS system, an</p>

	<p>ADF holds all DFs and EFs for a specific application; thus, allowing a single UICC to host multiple applications at the same time.</p> <p>The Elementary File (EF) is a formatted data structure similar to the "file" in modern computer operating systems. It contains user or operating system data needed for a specific application.</p> <p>The AID for EFs under MF start with '2F', whilst the AID for EFs under DFs start with '6F'.</p> <p>Elementary files are classified based on the application into Internal Elementary File (IEF) and Working Elementary File (WEF).</p> <p>The Internal Elementary File (IEF) is a system file type used by the operating system to store its data. Usually, access to IEFs is protected by the operating system and they are grouped into one or more DF.</p> <p>The Working Elementary File (WEF) is a user file type used by applications to store their data. Usually, each application organizes its WEFs under one DF.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>pySim is a Python utility that can be used to program several U/SIM cards. See extra material #1.6</p> </div> <p>Unlike modern operating systems, EFs have standardized file structures that dictate their size, usage, and supported commands. The EF structure is predefined by the smart card operating system and each application can choose which file structure to use for its files. For example, the phonebook application often utilize a record oriented liner fixed file structure; while, the last dialed numbers are often stored in a record oriented cyclic file structure.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Students are encouraged to read Chapter 12 from extra material #1.8 to understand the different Elementary File Structures.</p> </div> <p>As a mobile digital forensic investigator, you are expected to have a working understanding of smart cards file management. This will help you explain how artifacts are stored on and extracted from U/SIM cards.</p>
--	--

Content Template	
Section Number	1.3.3
Section Title	U/SIM Security
Introduction	
Content	<p>In general, a smart card applies a hierarchy of secret codes to protect the access to data and restrict its usage. The secret code is referred to as Personal Identification Number (PIN) codes and a smart card may use one or more PIN codes. In technical terms, the PIN is referred to as Cardholder Verification (CHV).</p> <p>A U/SIM card has two PIN codes, i.e. PIN 1 and PIN 2, and each PIN code has its own use. Generally, PIN 1 is the code that you enter when you turn on your mobile phone and is used to prevent unauthorized access to the SIM card and protect access to the user files such as SMSs and phonebook. On the other hand, PIN2 is used to restrict access to some functionalities of the SIM card such as limiting phone calls to numbers on the carrier's network or preventing broadband SIM cards from making phone calls all together.</p> <p>The PIN code in U/SIM is a number between 4 and 8 digits, usually preset by the carrier to a default and trivial 4 digits number (e.g. "0000", "1234", etc.). The PIN should only be known to the SIM card user to prevent unauthorized access. If the PIN was incorrectly entered 3 times, then it will be immediately blocked; thus, preventing access to any resource that is protected by it. For example if PIN 1 is blocked, then the user will not be able to make or receive phone calls or use the SIM card except for dialing pre-defined emergency numbers. To unblock a blocked PIN code, its corresponding PIN Unblocking Code (PUK) should be used (i.e. PIN1/PUK1, PIN2/PUK2). The PUK code is usually an 8 digits number known to the carrier and in most cases, PUK1 is also known to the subscriber. If the PUK code is entered 10 times incorrectly, then the SIM card will become blocked permanently and it has to be replaced with a new one.</p> <p>This mechanism prevent, <i>to some degree</i>, brute-force and guessing attacks against PIN codes. Considering a 4 digits PIN code, the probability of correctly guessing it in no more than 3 tries is 0.03%, which is relatively low.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Karsten Nohl from the Security Research Labs (SRLabs) presented an interesting talk on attacking SIM cards using OTA update SMSs. Students are encouraged to read his presentation from extra material #1.9</p> </div> <p>When working in digital forensic case involving mobile devices or smart cards, it is not recommended to try to brute-force or guess PIN codes as some PIN codes may not allow more than a single incorrect insertion. For U/SIM cards, you may ask the carrier to provide you (as a DF investigator) with the corresponding PUK code to reset the PIN code.</p>

Content Template	
Section Number	1.4
Section Title	1.4. Standards, Societies and Body of Knowledge
Introduction	<p>This section talks about the standards and societies related to mobile devices and mobile technologies in general.</p> <p>Upon completion of this section the student will be able to:</p> <ul style="list-style-type: none"> • Identify the main standards adopted in the industry with respect to mobile devices. • Identify the main standards adopted in the industry with respect to mobile networks.
Content	<p>One of the major problems that the mobile industry suffers from is the issue of device fragmentation. Device fragmentation is expressed by the large number of mobile device manufacturers, mobile software providers, and mobile platform providers.</p> <p>There are thousands type of mobile device hardware platforms. The variation is in the processor types, the screen sizes, the sensors support, and so on.</p> <p>This creates a challenge for all related parties, as developing an error-free application becomes a sophisticated task given these hardware and software varieties.</p> <p>In general, there is no one standard that is adopted by all mobile platform providers, Google, Microsoft, and Apple. Each one has its own set of standards.</p> <p>Due to its publicity, a large number of users, and open source nature, Google has established a consortium called the Open Handset Alliance (OHA). The purpose of the consortium is to develop open standards for mobile devices. The consortium includes several hardware manufacturers, Mobile Service Providers, in addition to Google. Example of such companies includes Sony, Motorola, Dell, Samsung, T-Mobile and so on.</p> <p>On the contrary to the hardware design, the mobile telecommunication standards are well defined by known international institutes such as IEEE. Whether baseband communication or WiFi, the industry includes a set of standards for every networking technology and protocol used.</p> <p>The most common standards include 1G, 2G, 3G, 4G, LTE, and 5G. In addition, the WiFi standards include IEEE 802.11 a,b,g,n, and ac.</p> <p>As a digital forensic investigator, it is crucial to establish and maintain your credibility in the digital forensics field. Several methods can be used to build and demonstrate your qualifications such as:</p> <ul style="list-style-type: none"> • Getting a higher education in digital forensic (diploma, master degree, or even PhD). • Certifications: many certification bodies offers industry recognized certifications in digital forensics (e.g. CHFI from EC-Council, CCFP from (ISC)², SANS FOR series from SANS Institute, CCE from ISFCE in addition to the vendor-specific certifications. • Experience: no amount of education and certifications could compensate for lack of technical experience. • Association membership: being a member of nationally/internationally recognized association of digital forensics.

	<p>Following are some of the well-recognized associations and groups in digital forensics:</p> <ul style="list-style-type: none"> • The International Society of Forensic Computer Examiners (ISFCE). • The International Association of Computer Investigative Specialists (IACIS). • High Technology Crime Investigation Association (HTCIA). • The American Society of Crime Laboratory Directors (ASCLD). • Scientific Working Group on Digital Evidence (SWGDE). • International Organization on Computer Evidence (IOCE). • European Network of Forensic Science Institutes (ENFSI). • European Cybercrime Training and Education Group (ECTEG). • European Cybercrime Centre (EC3). <p>Following are some of the international standards for digital forensics:</p> <ul style="list-style-type: none"> • ISO/IEC 27037:2012 (Guidelines for identification, collection, acquisition and preservation of digital evidence). • ISO/IEC 27041:2015 (Guidance on assuring suitability and adequacy of incident investigative method). • ISO/IEC 27042:2015 (Guidelines for the analysis and interpretation of digital evidence) • ISO/IEC 27043:2015 (Incident investigation principles and processes). • ISO/IEC 17025:2017 (General requirements for the competence of testing and calibration laboratories). • BS 10008:2014 (Evidential weight and legal admissibility of electronic information). • RFC 3227 (Guidelines for evidence collection and archiving).
--	--

Activity Template	
Number	1.1
Title	Identify two implications that might affect mobile forensic in the future as a result of the advancement in 5G technology.
Type	Reflection
Aim	ILOs: 4 The activity aims to let the student read more on cutting-edge technologies, and then correlate it to mobile forensics.
Description	1.1.2
Timeline	Time: 1-3 hours of reading.
Assessment	Each student is required to submit a one-page report of the possible implications and then present it in the class as open discussion session.

Activity Template	
Number	1.2
Title	Write a simple program to retrieve all SMS messages (sent and received) from a mobile phone using AT commands. Use any programming language you want.
Type	Reflection
Aim	ILOs: 1, 2 The activity aims to allow the student to have a hands-on experience on one of the main cellular network enabling technologies.
Description	1.1.3
Timeline	Time: 1-3 hours. Steps required: <ul style="list-style-type: none"> • Download the AT command manual for the modem of the mobile phone you will be used. • The mobile phone should have at least one SMS message stored on the SIM card or the device storage.
Assessment	The students will be divided into groups of three students (maximum). Each group is required to submit the source code of the program and demonstrate it in the classroom.

Activity Template	
Number	1.3
Title	Record a video explaining what smart cards are in non-technical terms (5 minutes maximum). Imagine that you are explaining them to a judge or juries with no technical background.
Type	Review
Aim	ILOs: 7 This activity aims to help developing the student skills in communicating technical forensic terms in non-technical manner.
Description	1.3
Timeline	Time: 1 hour
Assessment	The student will be assessed by their ability to explain the concept in non-technical terms.

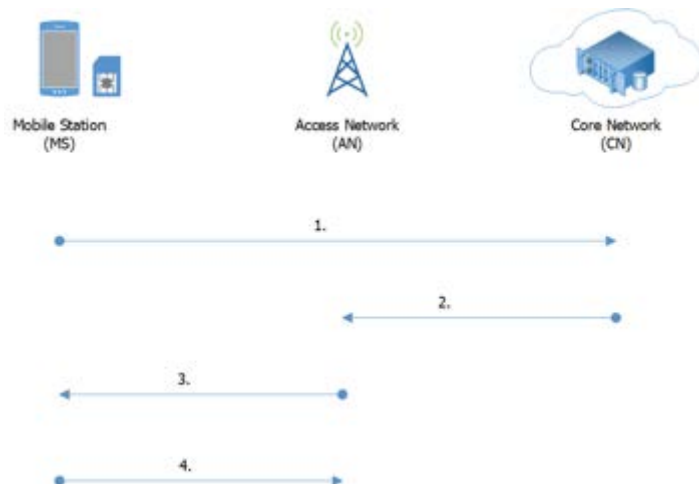
Think Template (MCQs)	
Number	1.1
Title	Evolution of Cellular Network and its History
Type	Fill in the blanks
Question	In the nineties, two new standards for cellular networks communications have emerged, which shaped the telecommunication industry for years to come. The two standards are the _____ standard developed by the European Union (EU) and the _____ standard developed by the United States (US).
Answers	<p>a) Global System for Mobile communications (GSM), Code-Division Multiple Access (CDMA).</p> <p>b) Code-Division Multiple Access (CDMA), Global System for Mobile communications (GSM).</p> <p>c) Serial Asynchronous Automatic Dialing and Control, ITU-T V.250.</p> <p>d) ITU-T V.250, Serial Asynchronous Automatic Dialing and Control.</p> <p>Answer: A</p>

Think Template (MCQs)	
Number	1.2
Title	Evolution of Cellular Network and its History
Type	Choose correct answer
Question	Which of the following uses analogue mobile networks
Answers	a) 1G b) 2G c) 2.5G d) 5G Answer: A

Think Template (MCQs)	
Number	1.3
Title	Cellular Network Architecture and Technologies
Type	Match pairs
Question	<p>Match the definition with the correct term.</p> <ul style="list-style-type: none"> a) A central database that stores the information of all the subscribers of the cellular network operator. b) A distributed database that stores the information of roaming mobile stations (foreigner subscribers) within an MSC. c) A central database of band mobile stations used to block or monitor stolen mobile devices. d) A central service delivery component in cellular network responsible for setting up and releasing the end-to-end connection, in addition to prepaid accounts billing.
Answers	<ul style="list-style-type: none"> i. VLR ii. HLR iii. MSC iv. EIR <p>Answer:</p> <ul style="list-style-type: none"> a >>> ii b >>> i c >>> iv d >>> iii

Think Template (MCQs)	
Number	1.4
Title	Cellular Network Architecture and Technologies
Type	Choose correct answer
Question	Deleted SMS can be sometime recovered from:
Answers	a) MSC. b) SMSC. c) BSC. d) UICC. Answer: B

Think Template (MCQs)	
Number	1.5
Title	Introduction to AT/AT+ Commands
Type	Fill in the blanks
Question	AT commands are case _____.
Answers	<p>a) Sensitive.</p> <p>b) Insensitive.</p> <p>Answer: B</p>

Think Template (MCQs)	
Number	1.6
Title	The title of the corresponding section.
Type	Match Pairs.
Question	 <p>The above figure shows the subscriber authentication process in GSM networks. Place the following steps in the correct order.</p>
Answers	<p>a) RND b) RES c) IMSI/TIMSI d) RES, RND e) IMEI f) ICCID</p> <p>Answer:</p> <p>1 >>> c 2 >>> d 3 >>> a 4 >>> b</p>

Think Template (MCQs)	
Number	1.7
Title	SIM/USIM File Management
Type	Rank options
Question	Smart cards file system uses a hierarchical tree structure of files to store data. Choose the correct ranking for smart cards file types in accordance to the ISO/IEC 7816-4 standard.
Answers	<p>a) MF, EF, DF.</p> <p>b) MF, ADF, DF, EF.</p> <p>c) MF, DF, EF, ADF.</p> <p>d) MF, DF, EF.</p> <p>Answer: D</p>

Think Template (MCQs)	
Number	1.8
Title	SIM/USIM Security
Type	Choose correct answer
Question	USIM cards use two PIN codes to secure stored data. PIN1 is considered the main code to access the SIM card. On the other hand, PIN2 is used to restrict access to secondary features and is NOT always enabled. In case PIN code 2 is blocked, then it can be unblocked using:
Answers	<p>a) CHV 1.</p> <p>b) CHV 2.</p> <p>c) PIN 1.</p> <p>d) PIN 2.</p> <p>e) A and C.</p> <p>f) B or D</p> <p>g) None of the above.</p> <p>Answer: F</p>

Extra Template	
Number	1.1
Title	Mobile Networks Made Easy: A simplified view of mobile networks for professional audience (Mobile cellular networks).
Topic	<ul style="list-style-type: none"> • 1.1.1 • 1.1.2
Type	<ul style="list-style-type: none"> • ISBN-10: 1549613952 • ISBN-13: 978-1549613951

Extra Template	
Number	1.2
Title	History of Mobile Forensics, NIST Document-3182.
Topic	<ul style="list-style-type: none"> • 1.1 • 1.2
Type	URL: https://www.nist.gov/document-3182

Extra Template	
Number	1.3
Title	Inventor Dennis C. Hayes - The Great Idea Finder.
Topic	1.1.3
Type	URL: http://www.ideafinder.com/history/inventors/hayes.htm

Extra Template	
Number	1.4
Title	AT Commands Reference Guide.
Topic	1.1.3
Type	URL: https://www.sparkfun.com/datasheets/Cellular%20Modules/AT_Commands_Reference_Guide_r0.pdf

Extra Template	
Number	1.5
Title	ITU-T Rec. V.250 (07/2003) Serial Asynchronous Automatic Dialling And Control.
Topic	1.1.3
Type	URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-V.250-200307-I!!PDF-E&type=items

Extra Template	
Number	1.6
Title	pySim Wiki
Topic	1.3.2
Type	URL: https://osmocom.org/projects/pysim/wiki

Extra Template	
Number	1.7
Title	Smart Cards, Tokens, Security and Applications.
Topic	1.3
Type	ISBN: 978-3-319-50500-8.

Extra Template	
Number	1.8
Title	Smart Card Handbook, Fourth Edition.
Topic	1.3
Type	<ul style="list-style-type: none"> • Print ISBN: 9780470743676 • Online ISBN: 9780470660911 • DOI: 10.1002/9780470660911

Extra Template	
Number	1.9
Title	Rooting SIM Cards, Black Hat Slides.
Topic	1.3.3
Type	URL: https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf

2. Mobile Forensics Process, Methods and Techniques

Scope Template															
Number	2														
Title	Mobile Forensics Process, Methods and Techniques														
Introduction	In this chapter, we will start by explaining the process that the mobile forensic investigator follows to preserve, collect, examine, analyse and finally report the digital evidence. Thereafter, we will explain the various data acquisition methods used in mobile forensics. Finally, we will conclude this chapter by briefly highlight some of the emerging techniques in mobile forensics.														
Outcomes	1. Understating of the mobile forensics process, its phases, and best practices and guidelines. 2. Understanding of the various acquisition methods used in mobile forensics. 3. Highlighting emerging techniques in mobile forensics.														
Topics	2. Mobile Forensics Process, Methods and Techniques 2.1. Mobile Forensics Process 2.1.1. Preservation 2.1.2. Acquisition 2.1.3. Examination and Analysis 2.1.4. Reporting 2.2. Acquisition Methods 2.2.1. Manual Acquisition 2.2.2. Logical Acquisition 2.2.3. Physical Acquisition 2.2.4. File-System Acquisition 2.2.5. JTAG and Chip-Off Acquisition 2.3. Emerging Techniques in Mobile Forensics														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th><th>Time</th></tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td><td>3 hr</td></tr> <tr> <td>Textbook Content:</td><td>3 hr</td></tr> <tr> <td>Thinking (On-line discussions, Review questions)</td><td>1 hr</td></tr> <tr> <td>Tutorial Work:</td><td>2 hr</td></tr> <tr> <td>Related Course Work:</td><td>3 hrs</td></tr> <tr> <td>Total</td><td>12 hours</td></tr> </tbody> </table> <ul style="list-style-type: none"> • Required study time: 12 hours • Required hardware/software: <ol style="list-style-type: none"> 1. N/A. • Required external resources including links and books: <ol style="list-style-type: none"> 1. See extra materials. 	Task	Time	Preparation (Introduction and On-line Planning):	3 hr	Textbook Content:	3 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	2 hr	Related Course Work:	3 hrs	Total	12 hours
Task	Time														
Preparation (Introduction and On-line Planning):	3 hr														
Textbook Content:	3 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	2 hr														
Related Course Work:	3 hrs														
Total	12 hours														

Content Template	
Section Number	2.1
Section Title	Mobile Forensics Process
Introduction	<p>In this section, we will explain the fundamental phases of mobile forensics process and highlight some of the globally recognized best practices and guidelines for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to:</p> <ul style="list-style-type: none"> • Have a clear understanding of the mobile forensics process. • Explain the main phases constituting the mobile forensics process. • Identify the tasks performed in each phase.
Content	<p>The mobile forensics process can be defined as a systematic approach flowed by the mobile forensic investigator in order to preserve, collect, examine, analyse and finally report the digital evidence involving a mobile device.</p> <p>It is similar in nature to the computer forensic process; nonetheless, carries certain distinctions that make it unique due to the mobility of evidence.</p> <p>Following a sound forensic process would maintain the audit trail, chain of custody, and evidence integrity.</p> <p>Several institutions have released guidelines and best practice manuals for digital forensics process including mobile forensics such as the:</p> <ul style="list-style-type: none"> ▪ SANS institute (see extra material #2.1), ▪ National Institute of Standards and Technology (NIST) (see extra material #2.2), ▪ Association of Chief Police Officers (ACPO) (see extra material #2.3), and ▪ European Network of Forensic Science Institutes (ENFSI) (see extra material #2.4). <p>Figure 1 highlights the mobile forensics process in accordance with the NIST SP 800–101 guideline.</p> <p>It is important to emphasize that no two cases are the same and the forensic process is highly influenced by the type of case being investigated such as criminal, civil, administrative, or incident response.</p>

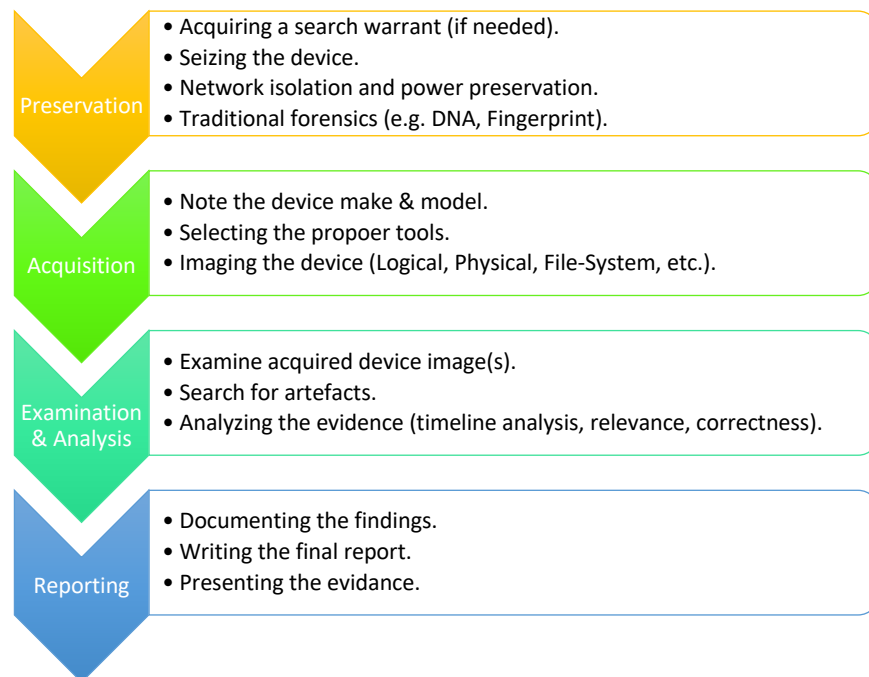


Figure 18. Mobile Forensics Process.

Other literature may define the mobile forensics process differently than what has been explained here. Although, the naming of the phases may differ, the chronological order and the tasks remain the same.

For example, in the EC-Council's Computer Hacking Forensic Investigator (CHFI) the mobile forensics process phases are defined as:

1. Collect and Preserve the Evidence.
2. Document the Scene.
3. Imaging and Profiling.
4. Acquire and Analyse Information.
5. Generate Report.

On the other hand, the ACPO's Good Practice Guide identify the phases of digital forensics process as:

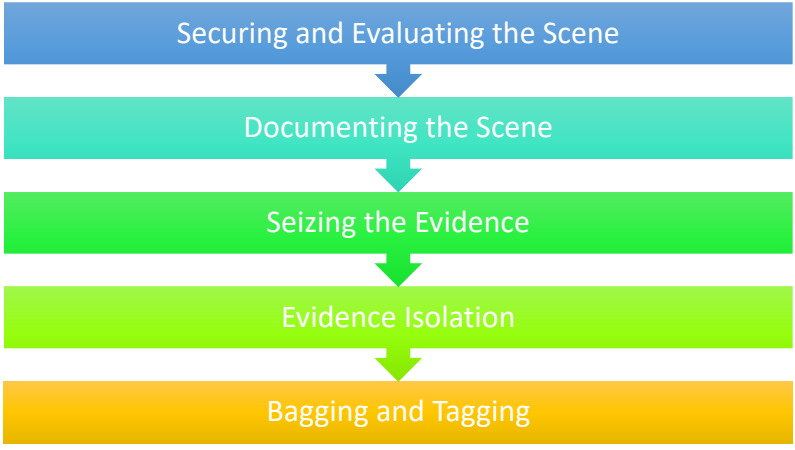
1. Plan.
2. Capture.
3. Analyse.
4. Present.

While, the ENFSI defines four phases for the digital forensics process, which are:

1. Identify.
2. Acquire.
3. Analysis.
4. Report.

Alternatively, there is a general digital forensics process (see: extra material #2.11) defined by the following three phases:

	<ol style="list-style-type: none">1. Data Collection.2. Examination and Analysis.3. Reporting. <p>The digital forensic investigator must follow the methodology defined/accepted by the local laws, regulations, and/or standards.</p>
--	--

Content Template	
Section Number	2.1.1
Section Title	Preservation
Introduction	
Content	<p>Evidence Preservation is the first phase of the mobile forensics process. It refers to the process of securing the crime scene and seizing the evidence in secure, documented and formal manner without changing its content while maintaining the audit trail and chain of custody.</p> <p>Prior starting this phase the investigator must acquire a search warrant in accordance with the imposed laws and regulations essentially in criminal cases. However, in specific circumstances a search warrant is not necessarily required. This is highly different from one country to another. For instance, in the USA it is possible to perform warrantless search and seizure under the following circumstances:</p> <ul style="list-style-type: none"> ▪ Consent: when an individual agrees to be searched or that his/her property be searched. The consent must be obtained freely and voluntarily without coercion and trickery. ▪ Plain View: when the evidence is in the plain sight of a law enforcement officer, yet he/she still must have a probable cause. ▪ Search Incident to Arrest: when the search is conducted in connection with an arrest. ▪ Protective Sweep: when the search is performed following an arrest to prevent probable danger to the law enforcement officer. ▪ Exigent Circumstances: when there is a probable cause to believe that an imminent destruction of evidence would occur before the warrant is obtained, or in emergencies. ▪ International Borders: border control, custom and immigration officers have the right to conduct warrantless search and seizure; moreover, they are not required to have a probable cause. <p>After obtaining the proper search warrant for the case, the investigator can begin conducting the evidence preservation. In this phase, the main objective is to secure the evidence and prepare it for processing.</p>  <pre> graph TD A[Securing and Evaluating the Scene] --> B[Documenting the Scene] B --> C[Seizing the Evidence] C --> D[Evidence Isolation] D --> E[Bagging and Tagging] </pre> <p>Figure 19. Main Tasks of Evidence Preservation.</p>

	<p>Figure 2 shows the main tasks conducted during the preservation phase as defined by the NIST SP 800–101 guideline.</p> <p>The first task performed during the evidence preservation phase is to Secure and Evaluate the Crime Scene. This task is exceptionally important because improper handling of the evidence may cause data loss and/or evidence contamination.</p> <p>The crime scene has to be secured in order to prevent evidence contamination in addition to ensure the safety of the public as well as the investigation team. Referring to <i>Locard's exchange principle</i>, when interacting with a crime scene one would bring something into the scene and leave with something from it. Therefore, only limited number of authorized and trained professionals should be allowed to enter the crime scene to minimize the chance of crime scene contamination.</p> <p>Moreover, in some cases the crime scene might pose a danger to the public and/or the investigation team (e.g. explosives, biohazards, etc.). Under such circumstances, certain procedures must be taken to ensure the public and the investigation team safety prior entering the crime scene. How to handle such situations is highly dependent on the type of the hazard.</p> <p>Furthermore, the crime scene must be evaluated to determine if traditional forensics investigation might be needed (e.g. forensic DNA analysis, forensic Bloodstain Pattern Analysis (BPA), forensic fingerprint analysis, etc.) and in that case, special care must be taken in order not to alter the evidence status or change the data.</p> <p>The second task performed during the evidence preservation phase is to Document the Crime Scene. During this task, information about the evidence and the crime scene is identified, recorded and photographed. The status of all digital devices including computers, mobiles devices, network devices, and cables should be recorded.</p> <p>Moreover, information about the mobile device should be recorded such as:</p> <ul style="list-style-type: none"> ▪ Power status (i.e. on or off) ▪ Lock status (i.e. locked or unlocked). ▪ Date and time (including the time zone if possible). ▪ Battery level. ▪ Damages, if any, (e.g. broken screen, bloated battery). ▪ Running apps (i.e. foreground, background). <p>The third task involves Seizing the Evidence with all tangential equipment such as: data cables, power adapters, SIM cards and their plastic holster, memory cards, removable media, and computers. Printed documents and notepads may be seized as well as it may contain relevant information to the case or help in unlocking the device.</p> <p>After seizing the evidence, it should be isolated from the network to prevent intentional and unintentional modifications to the evidence data. This is known as Evidence Isolation.</p> <p>Unintentional modifications can be introduced by several factors such as system and application updates, notifications, incoming calls and messages, GPS location update, cellular network location update, and scheduled jobs.</p> <p>On the other hand, intentional modifications, as the name indicates, are deliberately made by the perpetrator or his/her affiliates in order to destroy</p>
--	---

the evidence. Intentional modifications are more dangerous than the unintentional ones because they often result in destroying the evidence.

Nowadays, most mobile devices allow the user to remotely lock, wipe, and locate the device using a cloud service or by simply sending an SMS to the device.

Several techniques can be employed to isolate the device from the network including:

- Enabling the **Airplane Mode**, which will disable cellular network (data, calls and messages), Wi-Fi and Bluetooth but not GPS and NFC.
- Using a **Cellular Network Isolation Card (CNIC)**, which prevents the mobile device from connecting to the cellular network. Wi-Fi, Bluetooth, GPS and NFC still function under this method.
- Putting the device inside a **Single Shielded Container**, such as Faraday bag, Paraben's wireless StrongHold bag, RF shielded box, and Arson cans. They are usually rated to block certain ranges of wireless signals.
- Using a signal **Jamming** device, which works by emitting a stronger signal; thus, prevents the device from connecting to the network. They are also rated to block certain ranges of wireless signals.



Figure 20. Example of Windowless Faraday Bag. [<http://produtos-para-emagrecer.info/faraday-bag.html>].



Figure 21. Paraben's Wireless StrongHold Bag.
[<https://www.idstronghold.com/products/small-stronghold-bag-5x6>].



Figure 22. Example of RF Shielded Box. [https://www.rohde-schwarz.com/us/product/ts7124-productstartpage_63493-204033.html]



Figure 23. Example of Arson Can.
[<https://www.arrowheadforensics.com/products/arson-investigation.html>]



Figure 24. Example of Signal Jamming Device. [<https://www.cell-jammers.com>]

Regardless of the technique used to isolate the evidence, the goal should be to block all network activates including Cellular, Wi-Fi, Bluetooth, IR, GPS, Satellite, RFID and NFC.

It is important to note that all signal-shielding techniques drain the device's battery; therefore, it is highly recommended to attach the device to a power source (e.g. power-bank) to prevent it from shutting down.

Single Shielded Containers are designed to block certain range of frequencies and are rated for shielding effectiveness measured by decibel (dB) at frequency. Make sure to test it in the lab prior using it.

Finally, **Bagging and Tagging** of the seized devices is performed, in which the seized evidence is labelled and packaged using sealed forensic container. The container should prevent unauthorized access, moisture, fire, overheating and vibration.

At the end of the preservation phase, the mobile device becomes forensically ready to undergo forensic acquisition.

Content Template	
Section Number	2.1.2
Section Title	Acquisition
Introduction	
Content	<p>Acquisition refers to the process of making a forensics image of the seized device and collect any related data. In mobile forensics, data may be acquired from:</p> <ul style="list-style-type: none"> ▪ Mobile device internal storage. ▪ External memory card. ▪ U/SIM card. ▪ Cellular service provider (Carrier). ▪ Cloud service providers. <p>The data collected from the mobile device internal storage constitutes the bulk of forensic data that the investigator has to work with; followed by the external memory card (noting that not all the mobile devices support external memory storage such as Apple iPhones). Feature phones used to rely primarily on SIM cards to store phonebooks, messages and other information because the phone internal storage was quite limited back then. Nowadays, most of the data are stored either on the device internal storage or on the cloud (e.g. iCloud, Google Drive, Dropbox, Samsung Cloud, etc.).</p> <p>Cellular service provider (i.e. carrier) usually store data about the customer such as Call Detail Records (CDRs), leased IP address, location info, registered device IMEI, SIM card PUK1/2, sent/received SMS and many other data. However, three main challenges may face the investigator when requesting data from the carrier:</p> <ul style="list-style-type: none"> ▪ The request, most likely, has to come from a law enforcement agency with a proper warrant, which limits the access of private investigators to such information. ▪ Each carrier will store the data for a specific time in accordance with the local laws, regulations, standards and policies. Collected data may have been destroyed when the requested. ▪ Privacy laws varies between countries and it might not be possible to access such information. <p>In the evidence acquisition phase, the first task is to identify the mobile device make and model. This information includes the device manufacturer and the device specific model. It can be inferred from the:</p> <ul style="list-style-type: none"> ▪ Device Physical Characteristics (screen size, weight, colour, form factor, data/power/audio connectors etc.). ▪ Device Label located usually under the battery (see Figure 8). ▪ ESN or MEID for CDMA devices and IMEI for GSM devices. ▪ ICCID for U/SIM cards.



Figure 25. Example of Mobile Device Label.

Some tools such as *Cellebrite UFED Phone Detective* can help in identifying the mobile device make and model.

The second task is to **select the tool(s)** appropriate to perform the data acquisition based on the device type, make and model in addition to the method of acquisition needed (e.g. physical, logical, etc.). Acquisition methods are explained in detail in section 2.2.

The third task is to **perform the data acquisition** either on-site (live triage acquisition) or in the lab (post-mortem triage acquisition). Under certain circumstances, the seized device has to be processed on-site using **Live Triage** acquisition (e.g. searching mobile device at airports/checkpoints). In that case, specific data are extracted from the device, examined and analysed immediately on-site.

It is important to note that the data acquisition process is influenced by the device power states (i.e. ON or OFF). Figure 9 shows the current best practice process to acquire an image of a mobile device.

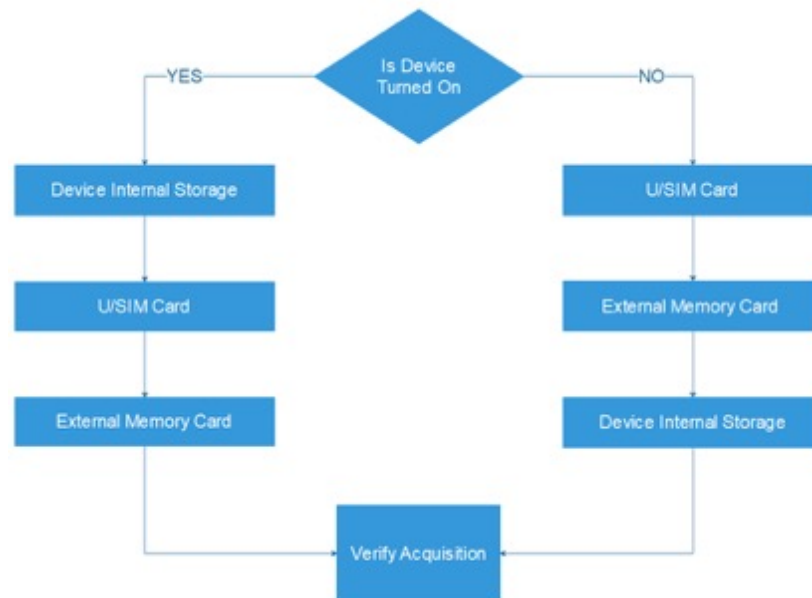


Figure 26. Mobile Device Forensic Acquisition Process.

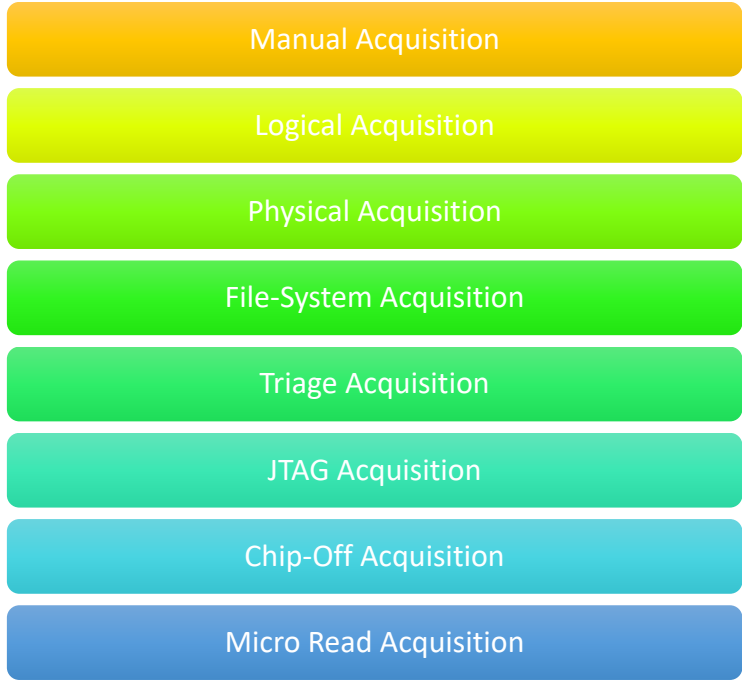
In cases where the mobile device was seized turned on; then, the device internal storage should be imaged first while the U/SIM card and the external memory card are still in the device. Then, both the U/SIM and the external memory cards are imaged separately from the device.

Conversely, if the mobile device is seized turned off; then, the U/SIM and the external memory card are imaged first separately from the device followed by the device internal storage.

On some models of mobile devices, removing the U/SIM card and/or the external memory card requires removing the device battery first. In that case, if the device was seized turned on, then it should not be turned off unless it can be unlocked.

Content Template	
Section Number	2.1.3
Section Title	Examination and Analysis
Introduction	
Content	<p>Examination is the process of finding the evidence using a systematic and reproducible methodology, in which the status of the evidence (e.g. deleted, hidden, encrypted, etc.), the location where it was found, its content and its significance should be noted. On the other hand, Analysis is the process of evaluating the outputs from the examination process for its relevance to the case.</p> <p>Usually, the examination process is performed by the digital forensics examiner, who is a technical professional specialized in finding the evidence. Whereas, the analysis process is conducted by the digital forensics analyst, who is not necessarily a technical person but should have an analytical mind and is responsible for interrupting the findings of the examination process and putting the evidence pieces together.</p> <p>It is important for the digital forensic examiner and analyst to be briefed about the case background by the investigator prior starting their tasks in order to be able to in order to be able to evaluate the significance of each digital artefact and its relevance to the case.</p> <p>The forensic toolkit plays a crucial role at this stage, it is highly recommended to verify the findings of one tool by trying to reproduce them using a different tool and following the same methodology.</p> <p>Anti-forensics and data hiding techniques may be employed in order to render the examination process useless; therefore, the forensics examiner should be trained to identify such techniques and take the appropriate actions to defeat them.</p> <p>Similarly, the forensics analyst should be able to conduct timeline analysis to determine at which time each event occurred and put the events in the correct chronological order.</p> <p>At the end of this phase, the forensics investigator should be able to formulate a scientifically sound conclusion (e.g. guilty vs. innocent) based on the found evidence.</p>

Content Template	
Section Number	2.1.4
Section Title	Reporting
Introduction	
Content	<p>Reporting is the final phase of the mobile forensics process and has as much importance as all other phases. In the reporting phase, a detailed summary of all the previous phases is prepared and the conclusion is clearly defined.</p> <p>The forensic report should clearly describe the:</p> <ul style="list-style-type: none"> ▪ Hypothesis that the investigator formulated. ▪ Evidence preservation techniques. ▪ Acquisition steps and methods ▪ Examination and analysis tools and findings. ▪ Conclusion. <p>A forensic report can be presented in several format based on the type of the case:</p> <ul style="list-style-type: none"> ▪ Formal Written Report: often used for criminal and civil cases. ▪ Formal Verbal Report: often used for testimonies and depositions. ▪ Informal Written Report: often used for major administrative investigations that might lead to civil or criminal case in addition incident response investigations. ▪ Informal Verbal Report: often used for minor administrative investigations. <p>Moreover, the forensic report should be written in a language that a nontechnical person could easily understand. Technical details should be explained in the appendices. It should be self-contained, well structured, logically organized and should not contain grammatical errors or typos.</p>

Content Template	
Section Number	2.2
Section Title	Acquisition Methods
Introduction	<p>In this section, we will explain the various mobile data acquisition methods. Upon the completion of this section, the student is expected to:</p> <ul style="list-style-type: none"> • Have a clear understanding of the various acquisition methods used in mobile forensics. • Be able to explain the difference between each acquisition methods. • Be able to identify the type of data that each acquisition method can retrieve.
Content	<p>Acquisition is the process of making a forensics image and collect any related data from the seized device.</p> <p>In mobile forensics, there are several methods for acquisition as shown in Figure 10.</p>  <p>Figure 27. Mobile Forensics Acquisition Methods.</p> <p>Micro Read is a special acquisition method, in which the digital gates on a NAND or NOR memory chip are physically examined under an electronic microscope to determine their value and thus reading the data. This requires special lab equipment and highly specialised technical experience, which most digital forensics labs do not have not, frankly, need. Micro read should be the last resort where all the other acquisition methods fail and you are dealing with a high profile case.</p> <p>Triage acquisition is a special method for data acquisition as well. However, unlike micro read acquisition, it is widely used among digital forensic examiners. Triage acquisition is classified into two main types:</p> <ul style="list-style-type: none"> ▪ Live triage acquisition.


	<ul style="list-style-type: none"> ▪ Post-Mortem triage acquisition. <p>In the Live Triage acquisition, the device is processed immediately on-site, where specific data are extracted (e.g. emails, images, word-list hits, etc.) from the device, examined and analysed in order to find an indication of specific intel (e.g. drugs, human trafficking, terrorism, etc.). Live triage is often performed at borders and security checkpoints to minimize the time required to search a suspect mobile device for intelligence. It is also commonly used during incident response investigations to collect volatile and critical evidence sources from infected devices.</p> <p>On the other hand, Post-Mortem Triage acquisition is performed in the lab to prioritize the seized devices in order of relevance and potential existence of evidence.</p> <p>Which acquisition method to use is predicted on several factors including:</p> <ul style="list-style-type: none"> ▪ Device make and model. ▪ Device status (i.e. ON/OFF, locked/unlocked, damaged/working). ▪ USB debugging for Android devices. ▪ Jailbreaking for iOS devices. ▪ Rooting for Android devices. ▪ Acquisition tool.
--	--

Content Template	
Section Number	2.2.1
Section Title	Manual Acquisition
Introduction	
Content	<p>Manual acquisition is the simplest and least technical acquisition method. It involves searching the seized device for potential evidence manually without using any tools.</p> <p>This method is often used for minor administrative investigation where the suspect is not a technical person or on boarder control where they do not have access to triage acquisition tools.</p> <p>With manual acquisition, deleted and hidden data cannot be recovered. Moreover, the investigator has to take special care not to modify any data and to document the process in excruciating details.</p> <p>Moreover, if the device display or keyboard were broken, it would be difficult to use this method.</p>

Content Template	
Section Number	2.2.2
Section Title	Logical Acquisition
Introduction	
Content	<p>Logical acquisition is the process of acquiring user accessible files from logical partitions in a forensically sound manner. With logical acquisition, only files and folders that are accessible by the user are retrieved; while, system protected files/folders, deleted data, unallocated space are not captured.</p> <p>The acquisition is conducted using the device OS API commands via the device data interface either wired or wireless.</p> <p>This method is supported by most mobile forensics tools and it can be conducted on most unlocked devices. It is also fast and reliable.</p> <p>Although, logical acquisition does not capture deleted data in unallocated space, it may recover deleted data that are marked for deletion but has not been deleted yet.</p> <p>For mobile devices, logical acquisition usually retrieves the user's data such as calls, messages, contacts, calendars, multimedia files, etc.</p> <p>It can also be helpful in validating the outcomes of manual data parsing from physical acquisition.</p>

Content Template	
Section Number	2.2.3
Section Title	Physical Acquisition
Introduction	
Content	<p>Physical acquisition refers to the process of making a bit-by-bit image of the mobile internal storage. It extracts raw data from the mobile device internal storage, which then has to be parsed and decoded by the acquisition tool. Moreover, the device memory (RAM) is also extracted.</p> <p>This acquisition method is sometime used to bypass locked devices, <i>under certain conditions</i>, and can retrieve deleted and hidden data; in addition to the system protected files and unallocated space.</p> <p>For iOS devices with A5 chip or higher, bypassing locked devices with physical acquisition is not an easy task because and the physical image do not include the areas of the unallocated space. On the other hand, an Android device has to enter what is called a "Download Mode" in order to make a physical acquisition. The download mode is used to flash the device with a custom ROM image, which leaves traces on the seized device.</p> <p>Each tool may use different techniques in order to acquire a physical image of the device. It is important to know how the tool accomplish this task in order to be able to explain the changes/traces that each technique may leave on the device.</p> <p>Devices that have built-in hardware encryption such as iOS devices or allow full device encryption can be challenging to acquire especially if the device is locked or turned off.</p> <p>Physical acquisition may be required in situations where anti-forensics techniques are expected or when recovering deleted data is needed.</p>

Content Template	
Section Number	2.2.4
Section Title	File-System Acquisition
Introduction	
Content	<p>File-system acquisition is a special type of logical acquisition, where the file-system structure, system configurations, apps data, user's configurations as well as user's data are captured. It can be seen as the middle way between logical and physical acquisitions.</p> <p>However, not all mobile forensic tools support file-system acquisition and not all system files can be retrieved. Moreover, the system files may be retrieved in raw format; therefore, decoding and parsing of such data has to be done either manually or using a special tool.</p> <p>Deleted data from SQLite databases may be recovered using file-system acquisition; nonetheless, recovering deleted data from unallocated space is not always possible with file-system acquisition.</p> <p>The type of system files retrieved via file-system acquisition is highly dependent on the mobile OS and the tool used in the acquisition.</p> <p>Additionally, in most cases, the device has to be unlocked and USB debugging must be enabled for Android devices in order for file-system acquisition to work.</p>

Content Template	
Section Number	2.2.5
Section Title	JTAG and Chip-Off Acquisition
Introduction	
Content	<p>JTAG (Joint Test Action Group) is an industry standard for testing printed circuit boards (PCBs) initially developed in the mid-80s and standardized in 1990 as IEEE 1491. It also refers to the hardware interface that allows direct communication with ICs on PCBs. JTAG implements a serial communication interface to an on-chip called Test Access Ports (TAPs). JTAG can be used to test, debug, verify the design, program and reprogram hardware (e.g. processors, memory chips) after manufacture.</p> <p>JTAG is considered a non-destructive method to directly access the device internal storage, perform physical data acquisition and bypass security measure. JTAG can be used to acquire a physical image of locked Android devices even if USB debugging is not enabled and it is most likely required to perform physical acquisition on Windows Phone devices.</p> <p>Although, JTAG can be very useful for mobile forensics examiners, it is not always supported by all manufacturers and it may not be supported on all models from the same manufacturer. Moreover, JTAG acquires data in raw format meaning that if data is stored encrypted it will be acquired in an encrypted format.</p> <p>Figure 11 shows the JTAG TAPs on a Samsung S4 device (see extra material #2.7).</p>  <p>Figure 28. JTAG TAPs on Samsung S4. [https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337)]</p> <p>JTAG is considered an invasive acquisition method because in most cases it requires the disassembly of the mobile device in order to access the JTAG TAPs.</p> <p>When all the previous acquisition methods fail, the Chip-Off acquisition method should be considered. It includes removing the mobile device internal flash memory chip and making a bit-by-bit image directly off the chip. Before the extracted data can be used forensically, the Wear Levelling algorithm (see section 4.1) employed must be known in order to save the data as bit-stream image.</p>

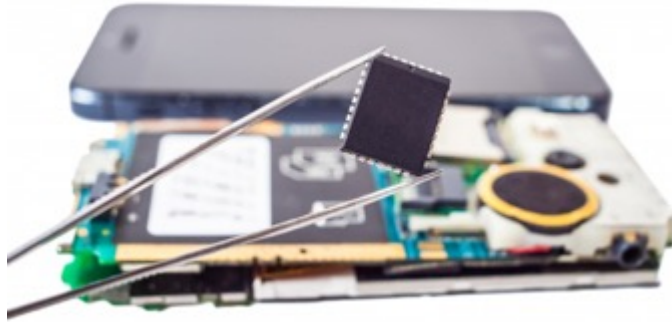


Figure 29. Example of a Chipped-Off Flash Memory Chip.
[https://www.forensicswiki.org/wiki/Chip-Off_Forensics]

Usually, the chip-off acquisition is used to recover data from severely damaged devices (e.g. burned, broken) as long as the flash memory chip is intact; chip-off acquisition is possible.

Chip-off acquisition is considered both invasive and destructive method; in addition, it requires extremely technical skills and intensive training. Moreover, it is highly dependent on the flash memory type and manufacturer. It also requires special tools to remove the memory chip from the device PCB and special readers to extract data from the chipped-off memory chip.

Figure 13 shows an eMPC flash memory reader commonly used to recover data from Samsung Note4 flash memory chip.



Figure 30. Example of Flash Memory Chip Reader.
[<https://www.amazon.co.uk/ALLSOCKET-eMMC169-eMCP162-eMCP221-Programmer/dp/B071NV1Z5S>]

Content Template	
Section Number	2.3
Section Title	Emerging Techniques in Mobile Forensics
Introduction	<p>In this section, we will explain emerging techniques in mobile forensics.</p> <p>Upon the completion of this section, the student is expected to have a basic understanding of the currently emerging techniques in mobile forensics.</p>
Content	<p>With iOS 11.4.1, Apple introduced the USB Restricted Mode, which when engaged prevents the device from sending or receiving data over the lightning port and restrict its functionality to charging only. The USB restricted mode engages after the device has been locked for an hour. Even though, USB restricted mode seems like a small change, in fact it successfully managed to render many forensics tools useless by bypassing iOS security measures.</p> <p>With iOS 12, Apple enhanced the USB Restricted Mode in a way that it will engage under several conditions other than the one hour passed from last unlocked condition. One of which is that an hour has passed from the last time the device disconnected from a USB accessory (any USB accessory).</p> <p>USB restricted mode has changed how digital forensics investigators handle iOS devices. Currently, when seizing an iOS mobile device it is highly recommended to connect it first to a compatible lightning port accessory (e.g. Lightning to USB 3 Camera Adapter) to prevent USB restricted mode from engaging while the device is transferred to the lab. Then, to follow the traditional evidence isolation techniques (i.e. use of external power source, disable networking and RF).</p> <p>Students are encouraged to read extra material #2.9 and #2.10 to know more about the implications of USB restricted mode on mobile forensics.</p>

Activity Template	
Number	2.1
Title	Compare between the ACPO's Good Practice Guide and the NIST SP 800–101 guideline in terms of mobile forensics process. Make sure to give your opinion.
Type	Review
Aim	ILOs: 4 The activity aims to let the student explore more mobile forensics process best practices than what has been taught in the textbook.
Description	2.1
Timeline	1 hour
Assessment	Each student is required to submit a one-page report. The report will be assessed based on completeness, correctness and overall quality.

Activity Template	
Number	2.2
Title	Compare between the different data acquisition methods explained in the textbook in terms of the data that each method can recover, complexity, requirements, supports by forensics tools, and when it should be used.
Type	Review
Aim	ILOs: 1, 4 The activity aims to reinforce the student understanding of the various data acquisition methods.
Description	2.2
Timeline	1 hour
Assessment	Each student is required to submit a one-page report. The report will be assessed based on completeness, correctness and overall quality.

Activity Template	
Number	2.3
Title	Write a report about the changes/traces that the different mobile forensics tools may leave on the device when acquiring a physical image. Choose one tool. You should validate your findings experimentally.
Type	Research
Aim	ILOs: 4 The activity aims to allow the student to understand how forensic tools works.
Description	2.2.3
Timeline	1-3 hours
Assessment	Each student is required to submit a one-page (minimum) report. The report will be assessed based on completeness, correctness and overall quality.

Think Template (MCQs)	
Number	2.1
Title	Mobile Forensics Process
Type	Choose correct answer
Question	The Association of Chief Police Officers (ACPO) Good Practice Guide identify the phases of digital forensics process as:
Answers	<ul style="list-style-type: none"> a. Plan, Capture, Analyse, Present. b. Identify, Acquire, Analysis, Report. c. Collection, Analysis, Reporting. d. Collect, Document, Acquire, Analyse, Report. <p>Answer: A</p>

Think Template (MCQs)	
Number	2.2
Title	Mobile Forensics Process
Type	Fill in the blanks
Question	Mobile Forensics Process is the systematic to ____, collect, ____, ____ and finally report the digital evidence involved in a mobile forensics investigation.
Answers	<ul style="list-style-type: none"> a. Plan, Analyse, Present. b. Identify, Acquire, Analyse. c. Preserve, Examine, Analyse. d. Document, Acquire, Analyse. <p>Answer: C</p>

Think Template (MCQs)	
Number	2.3
Title	Preservation
Type	Rank options
Question	<p>Arrange the main tasks of evidence preservation in the correct order:</p> <ul style="list-style-type: none"> a. Bagging and Tagging. b. Documenting the Scene. c. Evidence Isolation. d. Securing and Evaluating the Scene. e. Seizing the Evidence.
Answers	<p>Answer:</p> <ul style="list-style-type: none"> 1. Securing and Evaluating the Scene. 2. Documenting the Scene. 3. Seizing the Evidence. 4. Evidence Isolation. 5. Bagging and Tagging.

Think Template (MCQs)	
Number	2.4
Title	Acquisition
Type	Choose correct answer
Question	In the evidence acquisition phase, the first task is to identify the mobile device make and model. This information includes the device manufacturer and the device specific model.
Answers	<p>a. True</p> <p>b. False</p> <p>Answer: A</p>

Think Template (MCQs)	
Number	2.5
Title	Examination and Analysis
Type	Choose correct answer
Question	The analysis process is conducted by the digital forensics analyst, who is a technical professional specialized in finding the evidence.
Answers	<p>a. True</p> <p>b. False</p> <p>Answer: B</p>

Think Template (MCQs)	
Number	2.6
Title	Reporting
Type	Fill in the blanks
Question	Formal Verbal Report is often used for _____ and _____.
Answers	<ul style="list-style-type: none"> a. Testimonies, Depositions. b. Criminal, Civil Cases. c. Major Administrative, Incident Response Investigations. d. Minor Administrative, Incident Response Investigations. <p>Answer: A</p>

Think Template (MCQs)	
Number	2.7
Title	Acquisition Methods
Type	Choose correct answer
Question	In the Live Triage acquisition, the device is processed immediately on-site, where specific data are extracted from the device, examined and analysed to find an indication of the evidence.
Answers	<p>a. True</p> <p>b. False</p> <p>Answer: A</p>

Think Template (MCQs)	
Number	2.8
Title	Acquisition Methods
Type	Choose correct answer
Question	Which of the following acquisition methods can be used to retrieve deleted data from unallocated space?
Answers	<ul style="list-style-type: none"> a. Manual. b. Logical and File-System. c. Physical, JTAG, Chip-Off. d. Physical, JTAG, Chip-Off, Micro Read. <p>Answer: D</p>

Think Template (MCQs)	
Number	2.9
Title	JTAG and Chip-Off Acquisition
Type	Choose correct answer
Question	Which of the following acquisition methods can be used to retrieve data from severely damaged devices?
Answers	<ul style="list-style-type: none"> a. Logical b. Chip-Off. c. JTAG. d. None of the above. <p>Answer: B</p>

Think Template (MCQs)	
Number	2.10
Title	Mobile Forensics Techniques
Type	Rank options
Question	<p>You are a digital forensics investigator and you were involved in a case where an iPhone X is to be seized. Arrange the steps that you will take in order to preserve the device.</p> <ol style="list-style-type: none"> Power it down. Isolate it from the network. Attach it to a power bank. Identify its make and model. Connect it to a "Lightning to USB 3 Camera" Adapter.
Answers	<p>Answer:</p> <ol style="list-style-type: none"> Connect it to a "Lightning to USB 3 Camera" Adapter. Isolate it from the network. Attach it to a power bank.

Extra Template	
Number	2.1
Title	Developing Process for Mobile Device Forensics, Version 3, Cynthia A. Murphy, 2013.
Topic	2.1
Type	URL: https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf

Extra Template	
Number	2.2
Title	Guidelines on Mobile Device Forensics, NIST Special Publication 800 – 101 Revision 1, Rick Ayers, Sam Brothers, Wayne Jansen, May 2014.
Topic	2.1
Type	URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Extra Template	
Number	2.3
Title	ACPO Good Practice Guide for Digital Evidence, Version 5, Janet Williams, March 2012.
Topic	2.1
Type	URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Extra Template	
Number	2.4
Title	Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01 (vs.01), the European Network of Forensic Science Institutes (ENFSI), November 2015.
Topic	2.1
Type	URL: http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf

Extra Template	
Number	2.5
Title	Jusas, V.; Birvinskas, D.; Gahramanov, E.; Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. <i>Symmetry</i> 2017, 9, 49.
Topic	2.2
Type	URL: https://www.mdpi.com/2073-8994/9/4/49/pdf

Extra Template	
Number	2.6
Title	JTAG Explained (finally!): Why "IoT", Software Security Engineers, and Manufacturers Should Care. Senrio's Blog. September 28, 2016.
Topic	2.2.5
Type	URL: https://blog.senr.io/blog/jtag-explained

Extra Template	
Number	2.7
Title	JTAG Samsung Galaxy S4 (SGH-I337). Forensics Wiki. July 24, 2013.
Topic	2.2.5
Type	URL: https://forensicswiki.org/wiki/JTAG_Samsung_Galaxy_S4_(SGH-I337)

Extra Template	
Number	2.8
Title	[Case Study] Chip-Off Forensics: How to Extract data from Damaged Mobile Devices. SalvationDATA. April 4, 2018.
Topic	2.2.5
Type	URL: https://blog.salvationdata.com/2018/04/04/case-study-chip-off-forensics-how-to-extract-data-from-damaged-mobile-devices

Extra Template	
Number	2.9
Title	[Case Study] Mobile Forensics: Apple Enhanced USB Restricted Mode in iOS 12. SalvationDATA. October 22, 2018.
Topic	2.3
Type	URL: https://blog.salvationdata.com/2018/10/22/case-study-mobile-forensics-apple-enhanced-usb-restricted-mode-in-ios-12

Extra Template	
Number	2.10
Title	iOS 12 Enhances USB Restricted Mode. Oleg Afonin, ElcomSoft Blog. September 20, 2018.
Topic	2.3
Type	URL: https://blog.elcomsoft.com/2018/09/ios-12-enhances-usb-restricted-mode

Extra Template	
Number	2.11
Title	Basic Concepts of Forensics. July 30, 2018.
Topic	2.1
Type	URL: https://resources.infosecinstitute.com/domain-risk-management

Extra Template	
Number	2.12
Title	Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 30, 2018.
Topic	2.1.1
Type	URL: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

3. Mobile Forensic Tools

Scope Template															
Number	3														
Title	Mobile Forensic Tools														
Introduction	In this chapter, we will explore the various commercial mobile forensics solutions including Cellebrite UFED, Oxygen Forensics, MSAB and Magnet Forensics. Moreover, we will explore the free and open-source mobile forensics tools such as Santoku, SANS SIFT Workstation, DEFT Workstation, TSK, Autopsy, and LiME.														
Outcomes	1. Understanding the various commercial and open-source mobile forensics solutions.														
Topics	3. Mobile Forensic Tools 3.1. Cellebrite 3.2. Oxygen Forensics 3.3. MSAB 3.4. Magnet Forensics 3.5. Open-Source Mobile Forensic Tools														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th><th>Time</th></tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td><td>2 hr</td></tr> <tr> <td>Textbook Content:</td><td>2 hr</td></tr> <tr> <td>Thinking (On-line discussions, Review questions)</td><td>1 hr</td></tr> <tr> <td>Tutorial Work:</td><td>2 hr</td></tr> <tr> <td>Related Course Work:</td><td>1 hrs</td></tr> <tr> <td>Total</td><td>8 hours</td></tr> </tbody> </table> <ul style="list-style-type: none"> Required study time: 8 hours Required hardware/software: <ol style="list-style-type: none"> N/A. Required external resources including links and books: <ol style="list-style-type: none"> See extra materials. 	Task	Time	Preparation (Introduction and On-line Planning):	2 hr	Textbook Content:	2 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	2 hr	Related Course Work:	1 hrs	Total	8 hours
Task	Time														
Preparation (Introduction and On-line Planning):	2 hr														
Textbook Content:	2 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	2 hr														
Related Course Work:	1 hrs														
Total	8 hours														


Content Template	
Section Number	3.1
Section Title	Cellebrite
Introduction	<p>In this section, we will explore Cellebrite's Universal Forensic Extraction Device (UFED) series solutions for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different Cellebrite's UFED solutions.</p>
Content	<p>Cellebrite is a leading mobile forensics company that provides digital intelligence solutions for security and law enforcement agencies in more than 60 countries. Founded in 1999, as a subsidiary of the Sun Corporation to produce hardware and software solutions for the cellular industry. In 2007, the company established its mobile forensics division and thereafter, Cellebrite has been known as the world leader in mobile forensics solutions.</p> <p>The Universal Forensic Extraction Device (UFED) is Cellebrite flagship solution for mobile forensics. It is capable for making bit-stream images of mobile devices including smartphones, tablets, feature phones, PDAs, GPS devices and more. It also facilitates deep analysis, decoding and easy artefacts extraction from captured device images.</p> <p>Cellebrite UFED series include several solutions such as:</p> <ul style="list-style-type: none"> ▪ UFED Touch/Touch2 Logical: perform logical data extraction, SIM data extraction, password extraction, and SIM card cloning. ▪ UFED Touch/Touch2 Ultimate: perform the same functionalities as the UFED Touch in addition to file system and physical data extraction.  <p>Figure 31. UFED Touch2. [https://www.policemag.com]</p>



Figure 32. UFED Touch2 Ruggedized. [<https://www.cellebrite.com>]

- **UFED Touch Ruggedized:** provides a strong toolkit for in field mobile data extraction and analysis.
- **UFED 4PC:** is a software-only solution that can be installed on a Windows compatible PC, and it comes in two license versions (Logical and Ultimate).



Figure 33. UFED 4PC. [<https://www.cellebrite.com>]

- **UFED Turnkey:** is a rugged all-in-one mobile forensic solution designed for tough conditions. It utilizes Panasonic Toughbook CF19/CF53 or Panasonic Toughpad G1.



Figure 34. UFED Turnkey. [<http://www.mynewsdesk.com>]

- **UFED Ruggedized Laptop:** it replaced the UFED Turnkey line and added an option for a lightest and thinnest semi-rugged laptop (i.e. Panasonic Toughbook CF54).



Figure 35. UFED Ruggedized Laptop (Panasonic Toughbook CF54). [<https://www.cellebrite.com>]

- **UFED Chinex:** is a solution that provides physical extraction and decoding from phones manufactured with Chinese chipsets using proprietary boot loaders.



Figure 36. UFED Chinex. [<http://aimtech.ru>]

- **UFED Logical Analyzer:** is a comprehensive analysis and reporting application for logical extraction.
- **UFED Physical Analyzer:** is an advanced application that supports comprehensive analysis and reporting for physical and file-system extraction.
- **UFED Reader:** is a tool that allows examiners to open and share reports generated by UFED Logical/Physical Analyzer with other users without installation or licensing.
- **UFED Phone Detective:** is an application to help the examiner identify the mobile device make and model.
- **UFED Link Analysis:** is a software to provide intelligent analysis by identifying and visualizing the connections between multiple mobile devices.

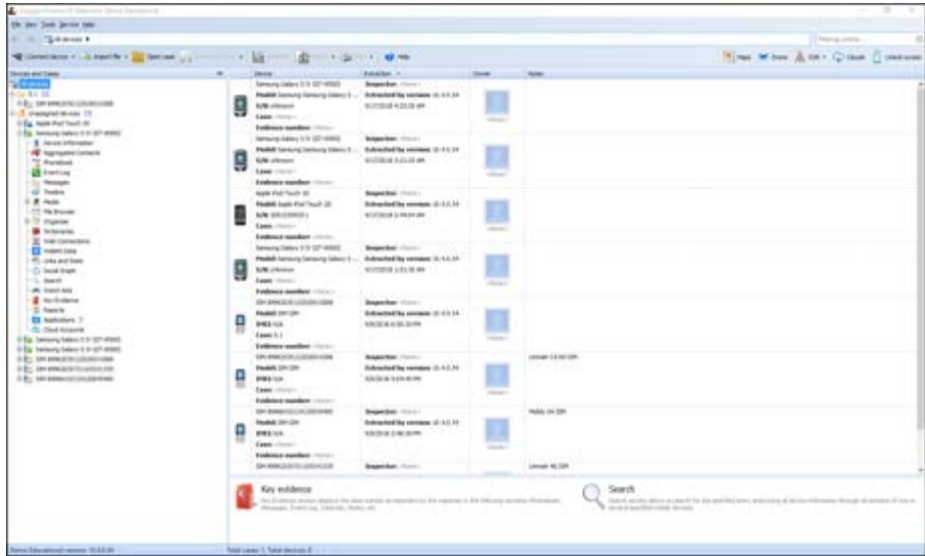
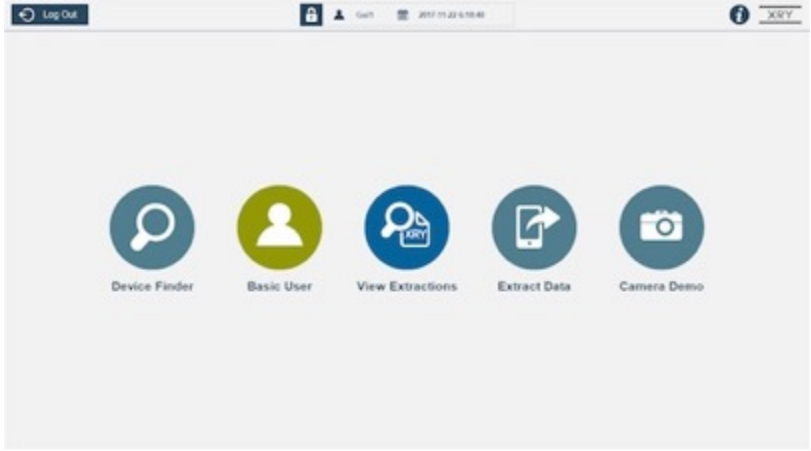
Content Template	
Section Number	3.2
Section Title	Oxygen Forensics
Introduction	<p>In this section, we will explore Oxygen Forensics solutions for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different Oxygen Forensics solutions.</p>
Content	<p>Oxygen Forensics, Inc. was founded in 2000 and specialized in developing PC-to-Mobile solutions. Its solutions have been used in more than 100 countries.</p> <p>Oxygen Forensics provides several solutions for mobile forensics such as:</p> <ul style="list-style-type: none"> ▪ Oxygen Forensic® Detective: is an all-in-one software solution to extract and analysis data from mobile devices including smart and feature phones, tablets, SIM cards, IoT devices and drones. The software also supports processing and analysing Call Data Records (CDR) and Cloud data (WhatsApp, iCloud, Facebook, Twitter, etc.).  <p>The screenshot displays the Oxygen Forensic Detective application window. On the left, there is a tree view showing various categories of data such as 'Messages', 'Contacts', 'Call Logs', and 'SMS'. The main area shows a list of extracted data items, including 'Messages', 'Contacts', 'Call Logs', and 'SMS'. Each item has a status indicator (e.g., 'Extracted') and a date. At the bottom, there is a 'Key evidence' section with a search bar and a list of items.</p> <p>Figure 37. Oxygen Forensic® Detective.</p> <ul style="list-style-type: none"> ▪ Oxygen Forensic® Detective Enterprise: allows organizations with multiple users and remote workstations to manage their licensing needs in a distributed and cost-effective manner by leasing the license to the users when needed.



Figure 38. Oxygen Forensic® Extractor. [<https://www.oxygen-forensic.com>]

- **Oxygen Forensic® Extractor:** is a data extraction software that can perform logical, physical and file-system data extraction from multiple devices. It can also import and parse data from device's images and backup files.
- **Oxygen Forensic® Viewer:** is a stand-alone tool for viewing and sharing information collected with other Oxygen Forensic® products, *as stated on their website.*

Content Template	
Section Number	3.3
Section Title	MSAB
Introduction	<p>In this section, we will explore Micro Systemation AB (MSAB) solutions for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different MSAB solutions.</p>
Content	<p>Micro Systemation AB (MSAB) is a Swedish company established in 1984 as a consultation company focusing on data communications. In 2003, the company shifted its focus to mobile forensics and produced its first mobile forensics solution (i.e. SoftGSM-XRY) and by 2008, the company become a key player in mobile forensics industry.</p> <p>MSAB provides several solutions for mobile forensics including:</p> <ul style="list-style-type: none"> ▪ MSAB XRY: is a suite of data extraction tools that supports both logical and physical data extraction from more than 25,000 mobile devices including smartphones, tablets, cloud, IoT devices, drones and more. XRY includes an image recognition engine, which can understand the contents of images and classifies them accordingly into categories such as drugs, weapons and people.  <p>The screenshot shows the MSAB XRY web application interface. At the top, there is a navigation bar with a 'Log Out' button, a user profile icon, and a timestamp '2017-11-28 15:58:49'. Below the navigation bar, there are five circular icons arranged horizontally, each with a label underneath: 'Device Finder' (magnifying glass icon), 'Basic User' (person icon), 'View Extractions' (document with magnifying glass icon), 'Extract Data' (document with arrow icon), and 'Camera Demo' (camera icon).</p> <p>Figure 39. MSAB XRY. [https://www.forensicfocus.com]</p> <ul style="list-style-type: none"> ▪ MSAB XAMN: is a suite of data analytical tools that help investigators analyse data extracted from mobile devices quickly and effectively.

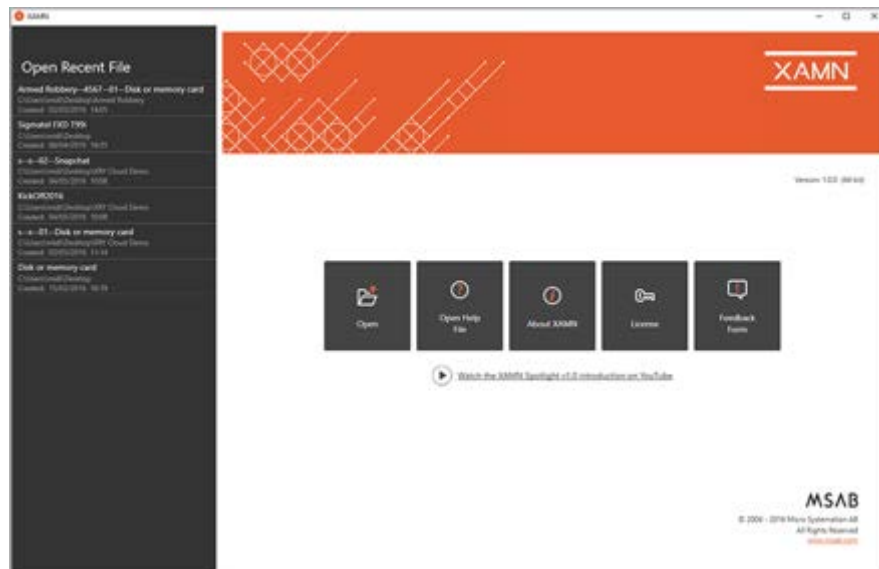


Figure 40. MSAB XAMN. [<https://www.forensicfocus.com>]

- **MSAB XEC:** is a suite of tools that allow organizations to centrally manage and control MSAB mobile forensics tools.

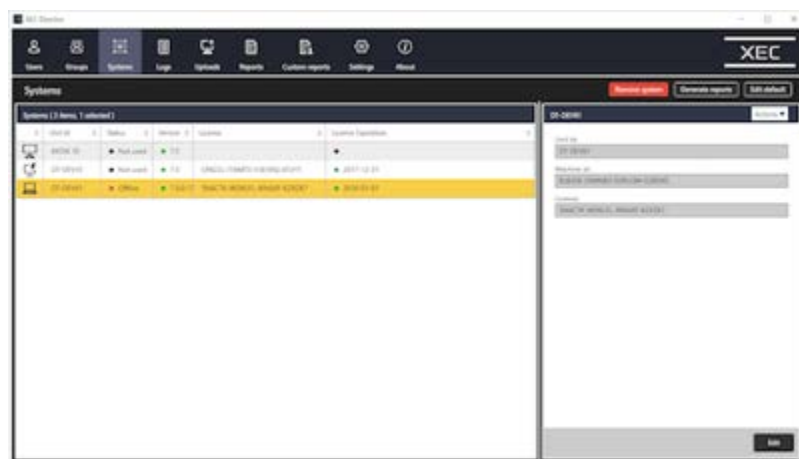


Figure 41. MSAB XEC. [<https://www.forensicfocus.com>]

- **MSAB iVE:** is a forensics tool designed to identify, extract and analyse data from vehicles.

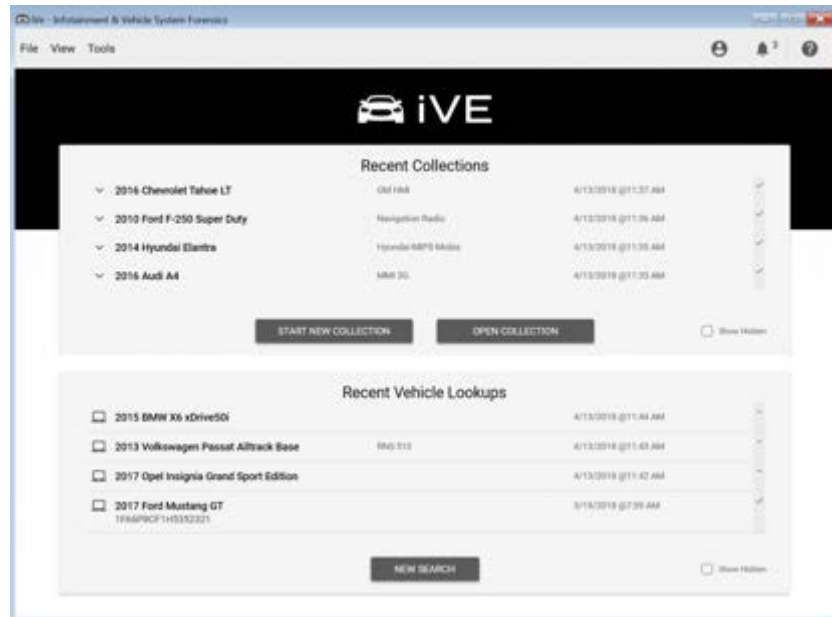
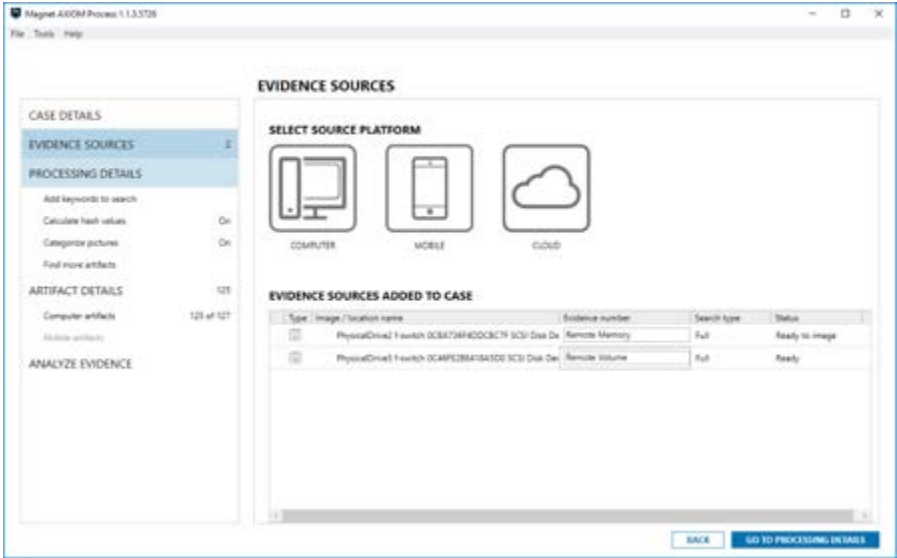


Figure 42. MSAB iVE. [<https://www.forensicfocus.com>]

Content Template	
Section Number	3.4
Section Title	Magnet Forensics
Introduction	<p>In this section, we will explore MAGNET solutions for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different MAGNET solutions.</p>
Content	<p>Magnet is a pioneer digital forensics company founded in 2011 by a Canadian forensics examiner. The company has a global present in addition to several authorized sales partners around the world.</p> <p>Magnet provides several solutions for both computer and mobile forensics such as:</p> <ul style="list-style-type: none"> ▪ Magnet AXIOM: is a complete digital forensics solution that allows the investigators to recover, examine and report evidentiary data from multiple sources including: smartphones, computers, cloud services and IoT devices. AXIOM has a built-in AI module capable of identifying sexual, drugs, weapons, and nudity in text conversations as well as in images.  <p>Figure 43. Magnet AXIOM. [https://www.magnetforensics.com]</p> <ul style="list-style-type: none"> ▪ Magnet IEF: the Internet Evidence Finder (IEF) is a software designed to accelerate analyse and search of the digital evidence. IEF can be run from a flash drive to perform a triage acquisition.

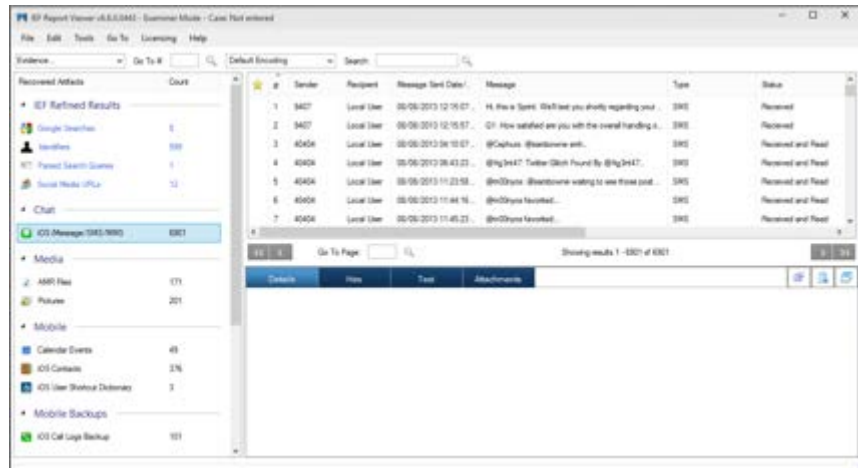


Figure 44. Magnet IEF. [<https://www.magnetforensics.com>]

- **Magnet ACQUIRE:** is a FREE forensic imaging software for acquiring digital forensics images from computers, hard drives, removable media, and smartphones. Currently, it only supports iOS and Android.

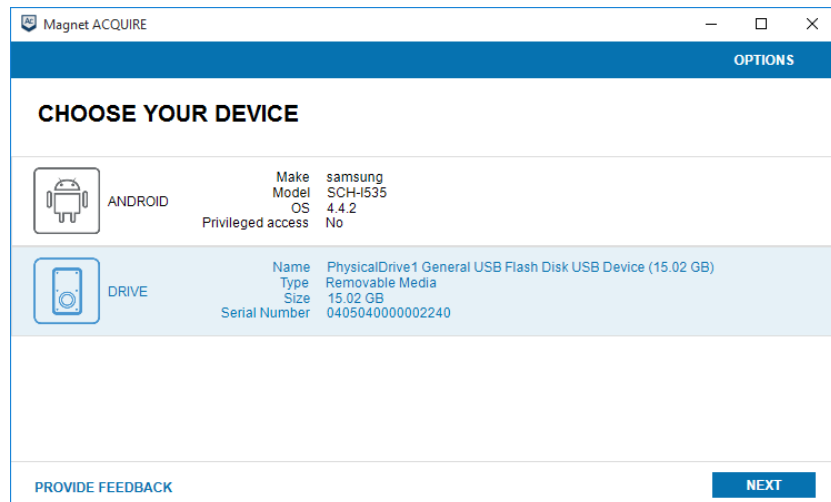


Figure 45. Magnet ACQUIRE. [<https://www.magnetforensics.com>]

- **Magnet ATLAS:** is a management solution designed to protect the chain of custody for digital evidence, manage the investigation teams, provides built-in ticketing system and asset management as well as facilitating budget management.

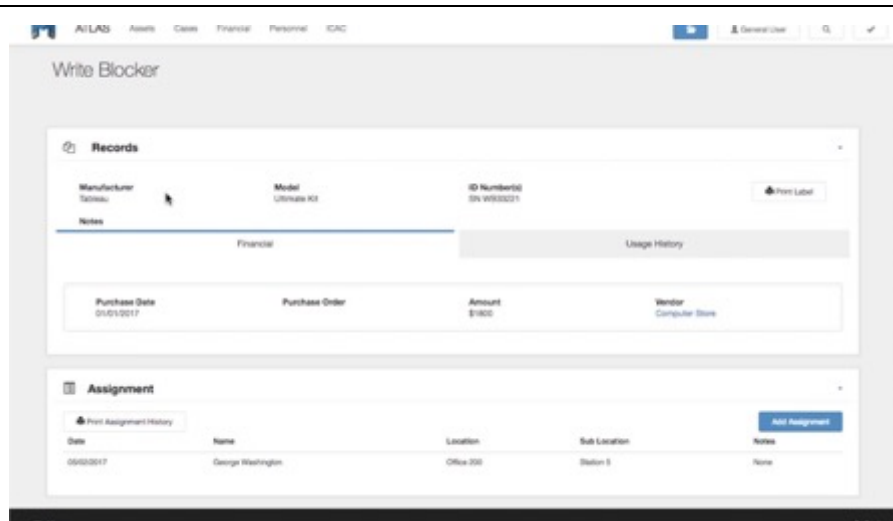




Figure 46. Magnet ATLAS. [<https://www.magnetforensics.com>]

Magnet provides many free tools for digital forensics such as:

- Magnet AXIOM Wordlist Generator.
- Dropbox Decryptor.
- Encrypted Disk Detector (EDD).
- Magnet RAM Capture.
- Magnet Process Capture.
- Web Page Saver.

Content Template	
Section Number	3.5
Section Title	Open-Source Mobile Forensic Tools
Introduction	<p>In this section, we will explore several open-source solutions for mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different open-source mobile forensics solutions.</p>
Content	<p>Santoku (current version 0.5) is a free and open-source bootable Linux distro based on lightweight Lubuntu with preinstalled applications for mobile forensics, mobile malware analysis and mobile Apps security assessment. The Santoku project started in 2012 and stopped in 2014.</p>  <p>Figure 47. Santoku (v0.5).</p> <p>Kali Linux is the de facto free solution in advanced penetration testing. Kali is built based on Debian Linux and it hosts several toolkits, scripts and frameworks for security penetration testing and digital forensics.</p>  <p>Figure 48. Kali Linux (v2018.4).</p>



The **SANS Investigative Forensic Toolkit (SIFT)** is a comprehensive workstation (current version 3.0) to perform digital forensics investigation using open-source tools. The SIFT workstation is maintained by SANS institute and is used in their training courses. Although, the SIFT workstation is based on Ubuntu LTS 16.04, it can be installed on Windows 10. Nonetheless, SANSS SIFT workstation is not designed specifically for mobile forensics; it can be used as a general-purpose workstation to perform digital forensics in a virtual environment as well as in education and training setup.



The **Digital Evidence & Forensics Toolkit (DEFT)** is a live GNU Linux distribution (current version is DEFT X. Oct 26, 2018) made for Digital Forensics and Incident Response (DFIR). DEFT includes a wide-range collection of free and open-source tools to perform DFIR tasks including mobile forensics, malware analysis, devices imaging, network forensics, Open-Source Intelligence (OSINT), artefacts extraction, data recovery, passwords extraction, and more.



Figure 51. CAIN v10 Workstation.

The **Computer Aided Investigative environment (CAIN)** is a live GNU Linux distribution (current version is v 10.0. Dec 18, 2018) for digital forensics investigation. CAIN includes tools to perform memory, network, mobile, and disk forensics as well as malware analysis. Additionally, CAIN includes Live Windows forensics tools such as Nirsoft tools and FTK Imager.



Figure 52. The Sleuth Kit (TSK) Logo.

The Sleuth Kit (TSK) (current version v4.6.5. Jan 15, 2019) is a framework for digital forensics, which includes several command line tools and libraries. TSK is considered the de facto tool for open-source digital forensics. It works on both Linux-based and Windows systems. Physical images from Android devices can be loaded as normal images and analysed using The Android Analyzer module.



Figure 53. Autopsy Logo.

Autopsy (current version v4.10.0. Dec 18, 2018) is a GUI interface for TSK and it supports both Linux-based and Windows systems.

Linux Memory Extractor (LiME) is a free and open-source Loadable Kernel Module (LKM) that is used to capture full RAM image from Linux-based systems such as Android devices. Captured memory images can be saved directly to the device or over the network.

Activity Template	
Number	3.1
Title	
Type	Reflection
Aim	<p>ILOs: 2, 6, 7</p> <p>The activity aims to let the student explore several open-source mobile forensic tools other than what have been taught in the textbook.</p>
Description	<p>3.5</p> <p>Download SANS SIFT Workstation or DEFT Workstation, then choose one of the preinstalled mobile forensics tools and write a step-by-step manual of how to use it. You may work in a group of maximum two (2) students.</p>
Timeline	1-3 hours
Assessment	<p>Each group is required to submit a detailed manual of how to use the selected tool.</p> <p>The manual will be assessed based on completeness, correctness, and overall quality.</p>

Activity Template	
Number	3.2
Title	Identify one (1) commercial tool for mobile digital forensics not mentioned in the textbook and write a short report (1-3 pages) documenting its features.
Type	Review
Aim	ILOs: 4 The activity aims to let the student explore new commercial mobile forensic tools other than what have been taught in the textbook.
Description	3.1-3.4
Timeline	1 hour
Assessment	Each student is required to submit a three pages (maximum) report. The report will be assessed based on completeness, correctness and overall quality.

Activity Template	
Number	3.3
Title	<p>Develop a mobile application to help investigators identifying the make and model of mobile devices from the device picture and or video. You may work in groups.</p> <p>This activity is optional and may be used as an idea for the final project.</p>
Type	Research
Aim	<p>ILOs: 4, 6</p> <p>The activity aims to let the student work in a group and apply computer science technologies to facilitate mobile digital forensics.</p>
Description	3
Timeline	N/A
Assessment	<p>Each group is required to submit a working tool in addition to a complete documentation following sound software engineering methods.</p> <p>The tool will be assessed based on correctness, easy-of-use, and overall quality.</p>

Think Template (MCQs)	
Number	3.1
Title	Cellebrite
Type	Choose correct answer
Question	Which of the following Cellebrite UFED solutions can perform Physical acquisition of mobile devices?
Answers	<ul style="list-style-type: none"> e. UFED Touch2 Logical f. UFED Touch2 Ultimate g. UFED 4PC Logical h. UFED Physical Analyzer i. UFED Chinex <p>Answer: B, E</p>

Think Template (MCQs)	
Number	3.2
Title	Oxygen Forensics
Type	Choose correct answer
Question	Which of the following tools can decode and analyse Call Data Records (CDRs)?
Answers	<ul style="list-style-type: none"> a. Oxygen Forensic Detective b. UFED Link Analysis c. MSAB iVE d. Magnet ATLAS <p>Answer: A</p>

Think Template (MCQs)	
Number	3.3
Title	MSAB
Type	Fill in the blanks
Question	_____ includes an image recognition engine, which can understand the contents of images and classifies them accordingly into categories such as drugs, weapons and people.
Answers	<ul style="list-style-type: none"> a. MSAB XEC b. MSAB XRY c. MSAB iVE d. MSAB Santoku <p>Answer: B</p>

Think Template (MCQs)	
Number	3.4
Title	Magnet Forensics
Type	Choose correct answer
Question	Magnet ACQUIRE is a paid forensic imaging software for acquiring digital forensics images from computers, hard drives, removable media, and smartphones.
Answers	<p>a. True.</p> <p>b. False.</p> <p>Answer: B</p>

Think Template (MCQs)	
Number	3.5
Title	Open-Source Mobile Forensic Tools
Type	Match pairs
Question	<p>Match the tool with its corresponding category:</p> <ul style="list-style-type: none"> a) SANS SIFT Workstation b) DEFT X Workstation c) TSK d) Santoku e) Autopsy f) LiME
Answers	<ul style="list-style-type: none"> i. Linux Distro ii. Framework iii. Tool iv. GUI <p>Answer:</p> <ul style="list-style-type: none"> a >>> i b >>> i c >>> ii d >>> i e >>> iv f >>> iii

Extra Template	
Number	3.1
Title	Cellebrite Website
Topic	3.1
Type	URL: www.cellebrite.com

Extra Template	
Number	3.2
Title	Oxygen Forensics Website
Topic	3.2
Type	URL: www.oxygen-forensic.com

Extra Template	
Number	3.3
Title	MSAB Website
Topic	3.3
Type	URL: www.msab.com

Extra Template	
Number	3.4
Title	Magnet Forensics Website
Topic	3.4
Type	URL: www.magnetforensics.com

Extra Template	
Number	3.5
Title	DEFT Website
Topic	3.5
Type	URL: www.deftlinux.net

Extra Template	
Number	3.6
Title	SANS SIFT Website
Topic	3.5
Type	URL: https://digital-forensics.sans.org/community/downloads

Extra Template	
Number	3.7
Title	Santoku Website
Topic	3.5
Type	URL: https://santoku-linux.com/

Extra Template	
Number	3.8
Title	LiME GitHub Repository
Topic	3.5
Type	URL: https://github.com/504ensicsLabs/LiME

Extra Template	
Number	3.9
Title	Autopsy Website
Topic	3.5
Type	URL: www.autopsy.com

Extra Template	
Number	3.10
Title	The Sleuth Kit (TSK) Website
Topic	3.5
Type	URL: www.sleuthkit.org

Extra Template	
Number	3.11
Title	Computer Aided Investigative Environment (CAIN) Website
Topic	3.5
Type	URL: www.caine-live.net

4. Mobile Device Forensics

Scope Template															
Number	4														
Title	Mobile Device Forensics														
Introduction	<p>Mobile devices have become an integral part of our daily modern life style. Nowadays, smart phones, tablets, smart watches, and even drones are running full operating system with enhanced security controls that improves user's privacy. However, these controls might complicate the mobile forensic investigator job.</p> <p>In this chapter, we start by introducing the mainstream mobile operating systems from a digital forensic point-of-view. Then, we explain the current best practices for collecting and handling mobile evidence. Thereafter, we describe the various type of artefacts that can be extracted from mobile devices, in addition to the tools and techniques to recover deleted data from mobile devices in a forensically sound manner. Finally, we highlight the methods that can be used to bypass the mobile security controls to gain access to the device.</p>														
Outcomes	<ol style="list-style-type: none"> Understanding the differences between mobile operating systems and their effects on mobile forensics. Understanding the various type of artefacts that can be extracted from mobile devices. Acquire, collect, examine and analyse artefacts from different mobile devices (Android, iOS, BlackBerry, Windows). Validate the results of mobile forensics solutions. 														
Topics	<ol style="list-style-type: none"> Mobile Device Forensics <ol style="list-style-type: none"> Android, BlackBerry, iOS and Windows Mobile Forensics Artefacts Extraction <ol style="list-style-type: none"> Contacts and Phone Call Artefacts SMS Artefacts Network and Location Artefacts System Artefacts Multimedia Files Artefacts Data and File Carving Deleted Files Recovery Bypassing Security Controls 														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th><th>Time</th></tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td><td>4 hr</td></tr> <tr> <td>Textbook Content:</td><td>8 hr</td></tr> <tr> <td>Thinking (On-line discussions, Review questions)</td><td>2 hr</td></tr> <tr> <td>Tutorial Work:</td><td>9 hr</td></tr> <tr> <td>Related Course Work:</td><td>1 hrs</td></tr> <tr> <td>Total</td><td>24 hours</td></tr> </tbody> </table> <ul style="list-style-type: none"> Required study time: 24 hours Required hardware/software: <ol style="list-style-type: none"> Mobile devices (Android, iOS, etc.) or forensic images of mobile devices. Cellebrite UFED or any other forensic tool that can perform mobile devices extraction and analysis. Required external resources including links and books: <ol style="list-style-type: none"> See extra materials. 	Task	Time	Preparation (Introduction and On-line Planning):	4 hr	Textbook Content:	8 hr	Thinking (On-line discussions, Review questions)	2 hr	Tutorial Work:	9 hr	Related Course Work:	1 hrs	Total	24 hours
Task	Time														
Preparation (Introduction and On-line Planning):	4 hr														
Textbook Content:	8 hr														
Thinking (On-line discussions, Review questions)	2 hr														
Tutorial Work:	9 hr														
Related Course Work:	1 hrs														
Total	24 hours														

Content Template													
Section Number	4.1												
Section Title	Android, BlackBerry, iOS and Windows Mobile Forensics												
Introduction	<p>In this section, we introduce the major mobile operating systems in today's market and explain the main features that could affect the mobile forensics process.</p> <p>Upon the completion of this section, the student is expected to be familiar with the different types of mobile operating systems.</p>												
Content	<div data-bbox="466 582 1377 1359" data-label="Figure"> <table border="1"> <caption>Percentage Market Share Data (2018)</caption> <thead> <tr> <th>Operating System</th> <th>Market Share (%)</th> </tr> </thead> <tbody> <tr> <td>Android</td> <td>70.46%</td> </tr> <tr> <td>iOS</td> <td>28.22%</td> </tr> <tr> <td>Windows Phone</td> <td>0.12%</td> </tr> <tr> <td>BlackBerry</td> <td>0.05%</td> </tr> <tr> <td>Others</td> <td>1.15%</td> </tr> </tbody> </table> </div> <p>Figure 54. Mobile Operating System Market Share (2018).</p> <p>Android is the most prominent mobile operating system with an average market share of 70.46% in 2018 (ending in August) as shown in Figure 1 (see: www.netmarketshare.com). This makes it most likely to be encountered during a forensic investigation.</p> <p>Android operating system is based on Linux 2.6 kernel, which is responsible for communicating with the hardware.</p> <p>User and system data are usually stored internally (internal memory). However, some of the user/applications data might be stored externally on an SD card (physical or emulated). This constitutes an extra challenge for mobile forensic investigators, in cases where an SD card is available. Applications may use it to store some or all of its data on the SD card and if it is removed, data corruption might occur.</p> <p>Therefore, investigators should follow the current best practice when acquiring an image of an Android device with SD card:</p>	Operating System	Market Share (%)	Android	70.46%	iOS	28.22%	Windows Phone	0.12%	BlackBerry	0.05%	Others	1.15%
Operating System	Market Share (%)												
Android	70.46%												
iOS	28.22%												
Windows Phone	0.12%												
BlackBerry	0.05%												
Others	1.15%												

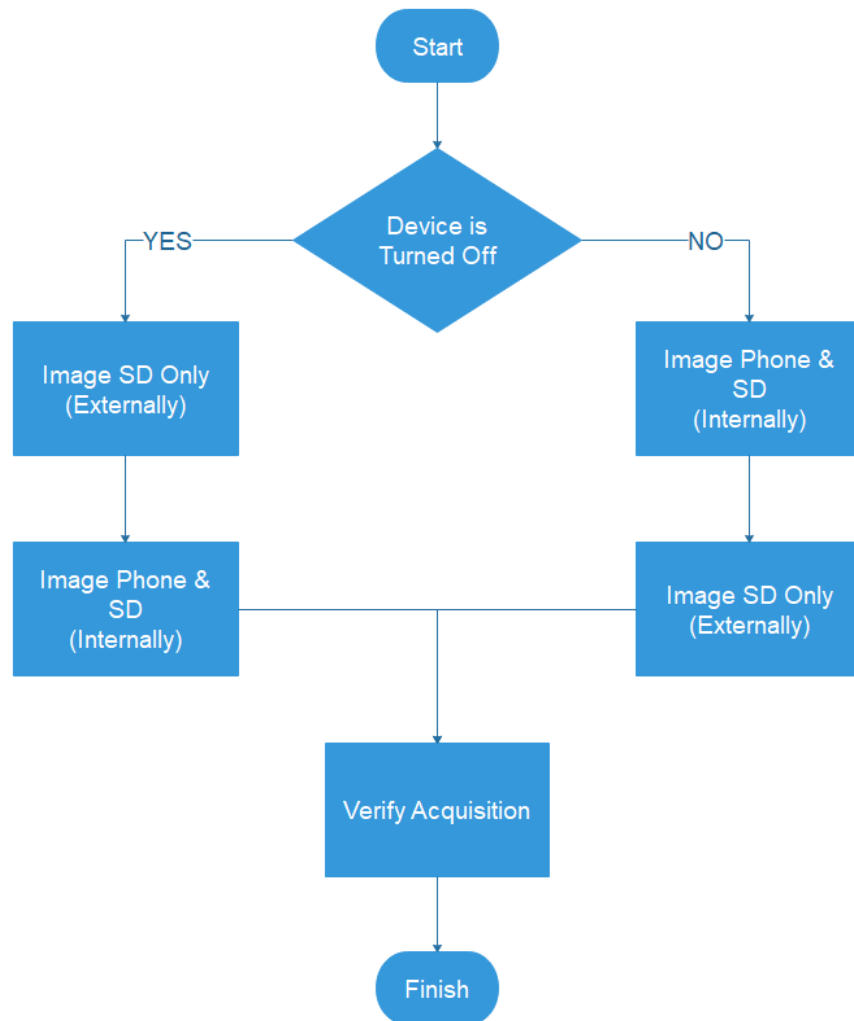


Figure 55. Android with SD Card Image Acquisition Process.

- If the device is turned off, then image the SD card first externally (separate from the device) then image the device and the SD card together.
- If the device is turned off, then image the device and the SD card together (internally) then image the SD card externally (separate from the device).
- Always verify the acquisition.

Figure 2 summarizes the image acquisition process for Android devices with SD Card Memory.

As with most modern mobile devices, the internal storage is made up of NAND flash memory. The NAND memory is made up of multiple cells, which is the smallest unit. Multiple cells are organized into a Page, and the data is written into pages. Multiple pages are grouped into a block and data can be removed only in blocks. Empty cells are filled with binary ones instead of zeros '1'b. See Figure 3.

With NAND memory, when a file is changed, a new copy is created and saved in a new page(s) and the old data is marked for deletion. However, as data can only be deleted in block(s), the old data will not be erased until the *Garbage Collector* (GC) is engaged. This process is called *Wear Levelling* and is meant to extend the life of NAND memory lifespan.

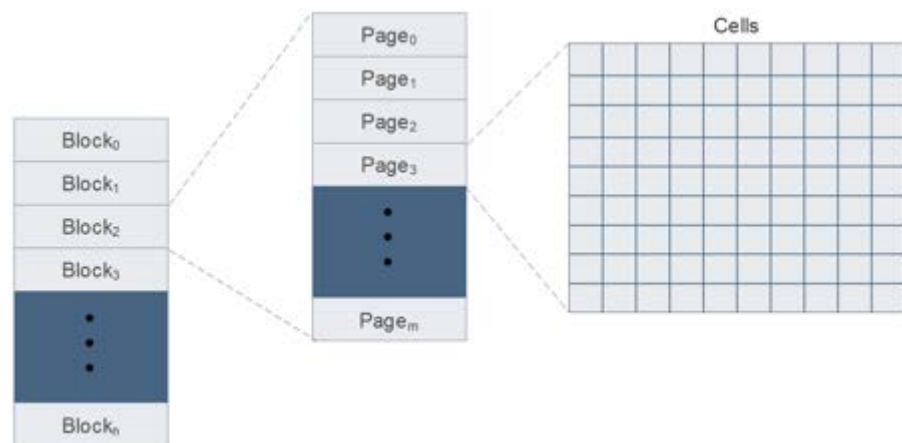


Figure 56. NAND Flash Memory.

Android usually uses one of the following File Systems:

- Fourth Extended File System (EXT4)
- Yet Another Flash File System 2 (YAFFS2)
- Robust File System (RFS)

EXT4 is the most common file system used in Android devices since Android 2.3. Knowing what file system an Android device uses is important when dealing with physical images. YAFFS2 engages the garbage collector more often than the other two file systems, typically, every two seconds. This results in erasing data blocks with modified or deleted files more rapidly in order to increase the amount of available free blocks. Therefore, deleted data has less chance of being recovered when YAFFS2 is used. Samsung devices usually use the later file system, i.e. RFS, which is based on FAT file system.

Android devices are often connected with a Google account and common Google apps such as Gmail, Contacts, Calendar, YouTube, Google Drive, etc. are often synced automatically.

Similar to "Find My iPhone" on iOS, Android devices "Android Device Manager", which is connected to the user's Google Account and allows the user to remotely find/ring/wipe a lost/stolen device. Samsung devices have a similar feature called "Find My Mobile", which is connected to the user's Samsung account as shown in Figure 4.



Figure 57. Google Find My Device.

Forensically, having the ability to wipe the device remotely is very critical and can destroy the evidence. Once, the device is seized, certain procedures should be taken to disable the device communications such as: putting it in Airplane Mode, disable Wi-Fi, GPS, NFC, Hotspots, Bluetooth and using signal shielding devices (e.g. Faraday bags, Arson cans, Signal Jamming, Network Isolated SIM card, etc.).

Always remember to connect the device to an external power source (e.g. power bank) to prevent battery from draining as a result of using signal shielding devices.

In order to acquire an image from an Android device, most forensic tools require the "USB Debugging" to be enabled. Cellebrite UFED is the only tool available that can physically image an Android device without USB Debugging.

Moreover, most forensic tools require a root access to perform advanced acquisition (e.g. physical) and often offer to do that automatically.

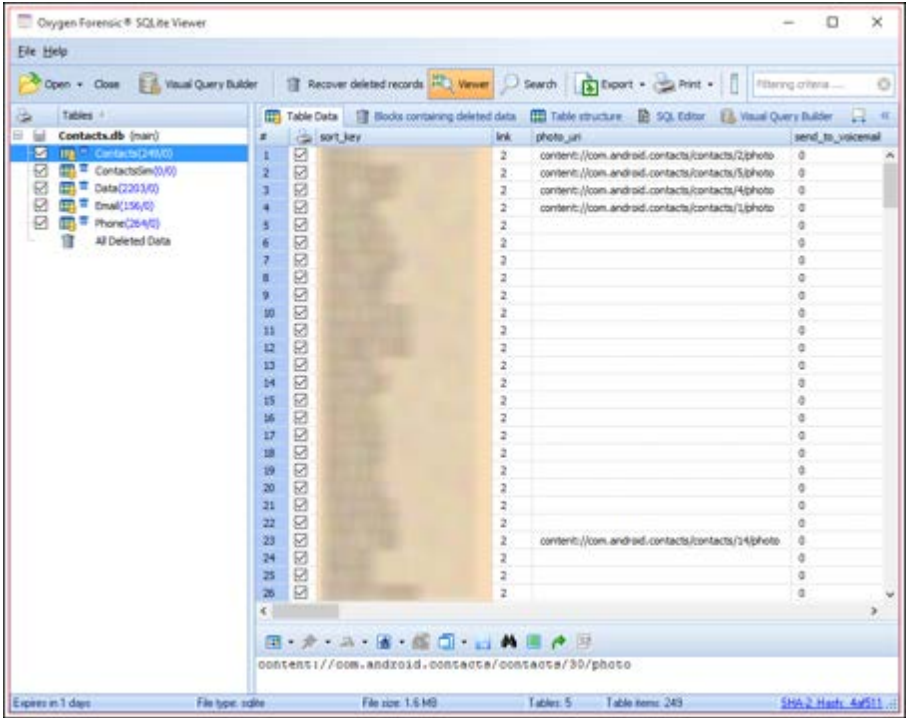
It is important to notice and document the status of device (rooted or not) prior performing the acquisition. If the device is rooted by the user, then expect to be dealing with an advanced user. Rooting the device is a very risky task that might cause in some cases the user data partition "/data/" to be

	<p>overwritten, thus contaminating the evidence. Make sure to test it on a dummy/practice device prior trying it on the evidentiary device.</p> <p>iOS is the second most popular operating system for mobile devices and it is exclusively associated with Apple's devices (e.g. iPhone, iPad, iPod Touch). On the other hand, Apple Watch and Apple TV run similar operating systems called watchOS and tvOS respectively, which are based on iOS.</p> <p>iOS devices do not have an external memory storage, which makes the forensic investigation process a bit easier. Moreover, they may or may not have a SIM card depending on the carrier network (GSM or CDMA) and the device model. The rule of thumb is that any iPhone released after 2011, will have a SIM card slot.</p> <p>iOS devices may use one of two proprietary file systems developed by Apple:</p> <ul style="list-style-type: none"> • Apple File System (APFS): is used by devices running iOS 10.3 and later, watchOS 3.2 and later, and tvOS 10.2 and later. • Hierarchical File System Plus (HFS+). <p>In iOS, data is stored in SQLite databases and Plist files (similar to XML files). Apple employs a hardware level encryption to protect the data on iOS devices. An AES-256 cryptographic chip sits between the NAND flash memory and the system memory (RAM), encrypts all the data from the flash memory to the system memory, and decrypt it on the other direction.</p> <p>Apple devices are synced and backed up via iTunes and iCloud. iTunes can be used to take local backups from iOS devices, which can be imported as an image by most forensics tool. Also, "Find My iPhone" can be used to remotely wipe an iOS device or lock it using a new passcode.</p> <p>It is also important to notice and document whether an iOS device is Jailbroken (equivalent to Rooted Android devices). Most forensic tools will report this status. Yet, an investigator has to verify it.</p> <p>BlackBerry devices are often associated with corporate/government users, they used to be popular but now they occupy less than 0.05% of the market share. This can be a challenge by itself, because most forensic tools tend to focus on the mainstream devices.</p> <p>Older BlackBerry devices run a proprietary operating system, i.e. RIM OS, which is based on J2ME. The newer BlackBerry devices (produced after 2013) run yet a another proprietary operating system, i.e. BlackBerry 10, which is based on QNX operating system (a Unix-Like OS for embedded systems).</p> <p>Blackberry Enterprise Software (BES) is a server-side software that is used to manage BlackBerry devices in corporate/government organizations. This can include remote wiping the device and disabling data ports.</p> <p>BlackBerry devices are known for the high level of security controls applied in some cases that might prevent any type for forensics acquisition. Locked BlackBerry devices cannot be acquired (logical, system, physical, or backup file) unless the passcode is known. Moreover, the device will be wiped after 10 failed attempts to enter the passcode (by default).</p> <p>Windows 10 Mobile is Microsoft's new unified operating system released in 2015 for mobile devices and tablets, which replaced Windows Phone OS. It uses NTFS file system and it is not encrypted by default, even though, it can be enabled in the settings.</p> <p>A Windows 10 Mobile device is often associated with a Microsoft account and cloud backup/storage via OneDrive. Similarly, a "Find My Phone" feature is available and it might be used to wipe the device remotely.</p>
--	--

	<div>Windows Phone Internals (WPinternals) is a free tool that can be used to unlock the bootloader on devices running the discontinued Windows Phone OS and get root access; thus, allowing physical imaging of the device. (see: www.wpinternals.net).</div> <p>Physical acquisition of a Windows 10 Mobile device is highly dependent on the device model and in some cases (e.g. Lumia 435); only chip-off techniques can be used to acquire a physical image (see Section 2.2.5).</p>
--	---

Content Template	
Section Number	4.2
Section Title	Artefacts Extraction
Introduction	<p>In this section, we will explore the different artefacts that can be extracted from mobile devices, including contacts, call logs, messages, network information, location information, apps history, user's online accounts and more.</p> <p>Upon the completion of this section, the student is expected to</p> <ul style="list-style-type: none"> • Be familiar with the different types of mobile artefacts. • Be able to extract the mobile artefacts from different mobile operating systems.
Content	<p>Artefacts extraction from a mobile device is a highly dependent process and many factors can affect it such as:</p> <ul style="list-style-type: none"> • Device make and model. • Device working status (e.g. working normally, physically damaged, damaged screen, etc.). • Device power status when acquisitioned (ON or OFF). • Device locking status and method (e.g. locked, unlocked, face ID, fingerprint, PIN code, etc.). • Device encryption status (i.e. encrypted or not). • Device remote management (e.g. MDM app, BES). • USB Debugging for Android devices. • Rooted/Jailbroken. • SD card usage. • SIM card usage. <p>According to the current best practices for collecting and handling mobile evidence, there are two generally acceptable methods:</p> <ol style="list-style-type: none"> 1. "Always turn off" method. 2. "Leave it as is" method. <p>In the first method, the device is always turned off upon seizing, the battery is removed (if possible), and it is never turned on until it is ready for examination.</p> <p>This method is recommended when the device will not be examined immediately or shortly after the seizing, and the risk of evidence contamination is high. For example, if the device is seized as part of homicide case and has to be sent first for DNA and fingerprints analysis. In this scenario, leaving the device ON will most likely result in evidence contamination.</p> <p>Nonetheless, with this method violate data will be lost and if the device is locked or encrypted, it might not be possible to extract artefacts when powered back on.</p> <p>The second method suggests to leave the device in the same status it was found in; if the mobile device is found ON then do not turn it OFF, and if it turned OFF do not turn it ON.</p>

	<p>For turned ON devices, place them a network-isolated environment and disable wireless communications (if possible). Attach the device to a power source (e.g. power bank) and make sure that the power will not act as an external antenna. If the device was unlocked, make sure to disable the auto locking (if possible) or increase the auto locking duration.</p> <p>This method has the highest chance of recovering data from the device and it is often used when the device is examined immediately on the scene or is sent directly to the digital forensic lab.</p> <p>It is important to remember that both methods are acceptable and actually used in practice based on the situation.</p>
--	---

Content Template	
Section Number	4.2.1
Section Title	Contacts and Phone Call Artefacts
Introduction	
Content	<p>Contacts and phone calls logs can be stored on many locations depending on the device make/model, device settings and installed Apps.</p> <p>Common places to store contacts is Google Account, phone internal storage and SIM card. When performing manual extraction, make sure to verify displayed contacts source.</p> <p>On Android devices, contacts and call logs are often stored in the same SQLite database. However, it is mostly device specific and may even vary based on region.</p>  <p>Figure 58. Android Contacts Information – File “contacts.db”.</p> <p>Contacts and call logs can be found, on older Android devices, under “/data/data/*.providers.contacts/databases/*.db”. The file is in SQLite3 format and is named either “contacts.db”, “contacts2.db”, or “logs.db”. On newer Android devices, contacts can be found under “/data/data/com.android.providers.contacts/databases/contacts2.db”. Whilst, call logs can be found under “/data/data/com.sec.android.provider.logspvprovider/databases/log s.db”.</p> <p>Figure 5 shows the “contacts.db” database parsed using Oxygen Forensics SQLite Viewer.</p>

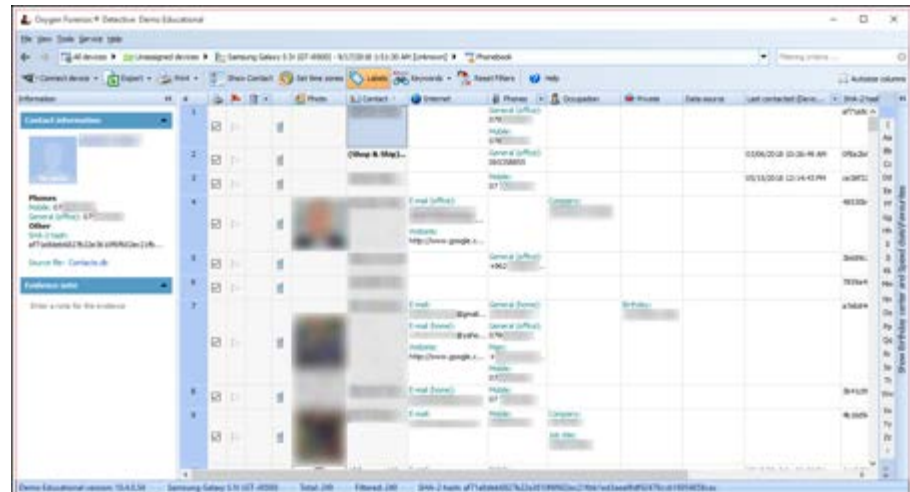


Figure 59. Android Contacts Data Parsed.

Figure 6 shows the contacts information using Oxygen Forensics Detective.

Date information is stored in Unix Epoch Time Stamp format. Many converters are available to decode/convert it to known timestamp format (see: www.unixtimestamp.com/index.php).

The call **duration** is recorded in seconds.

The **Type** values are:

- Incoming: (1).
- Outgoing: (2).
- Missed: (3).

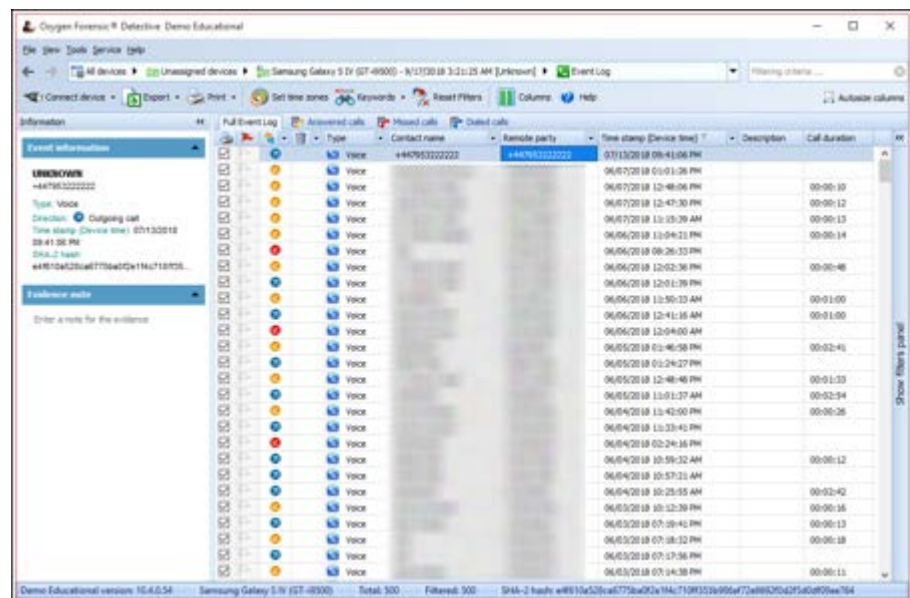
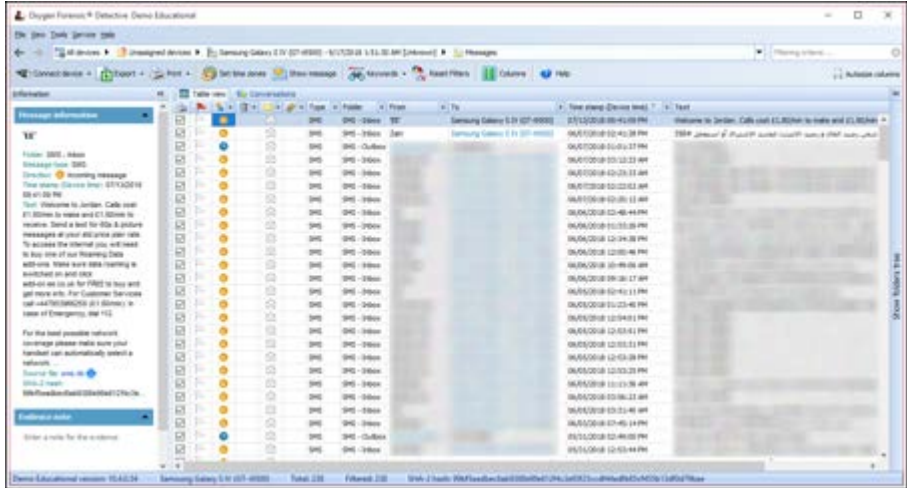


Figure 60. Android Calls Log Parsed.

For iOS devices, contacts are also stored in SQLite database under "**Library/AddressBook/AddressBook.sqlitedb**" and each contact is stored in an ABPerson Class (see extra material #4.2).

	<p>Call logs on iOS devices can be found under two locations, depending on the iOS version, and if the iOS was upgraded from an older version.</p> <p>For devices running iOS 8 and later, call logs can be found under "Library/CallHistory/callhistory.storedata", otherwise, under "Library/CallHistory/call_history.db". If iOS was upgraded, you may have logs stored in both locations, it is recommended to examine them both.</p> <p>For Windows phones, data is stored in Extensible Storage Engine (ESE) database format. Contacts/SMS data can be found under "Data:/Users/WPCOMMSERVICES/APPDATA/Local/Unistore/Store.vol" and Call logs data can be found under "Users/WPCOMMSERVICES/APPDATA/Local/UserData/Phone". See extra material #4.3 and #4.4 for more information about Windows phone and Windows 10 Mobile artefacts location and parsing.</p>
--	---

Content Template	
Section Number	4.2.2
Section Title	SMS Artefacts
Introduction	
Content	<p>Messages (SMS/MMS) data on Android devices can be located in a SQLite3 format database file under "/data/data/com.android.providers.telephony/databases/mmssms.db". Again, this is can vary based on the device make/model. Figure 8 shows SMS parsed using Oxygen Forensics Detective.</p>  <p>Figure 61. Android SMS Information Parsed.</p> <p>Date information is stored in Unix Epoch time stamp format.</p> <p>Read status has two values:</p> <ul style="list-style-type: none"> • Unread: (0) • Read: (1)

#	id	thread_id	address	person	date	date_sent	protocol	read	status
1	1	1	WhatsApp		1518268337825	1518268203000	0	1	-1
2	2	2	booking.com		1518271411633	1518271276000	0	1	-1
3	3	2	booking.com		1518272118936	1518271984000	0	1	-1
4	4	2	booking.com		1518272626976	1518272492000	0	1	-1
5	5	3	CAREEM		1518273379011	1518273245000	0	1	-1
6	6	4	Uber		1518274133415	1518273997000	0	1	-1
7	7	4	Uber		1518299157832	1518299025000	0	1	-1
8	8	4	Uber		1518301672702	1518301531000	0	1	-1
9	9	4	Uber		1518301674980	1518301531000	0	1	-1
10	10	5			1518336108971	1518334151000	0	1	-1
11	11	6	ZainJo		1518336122166	1518329242000	0	1	-1
12	12	6	ZainJo		1518336131690	1518329244000	0	1	-1
13	13	6	ZainJo		1518336135024	1518329242000	0	1	-1
14	14	6	ZainJo		1518336144494	1518329388000	0	1	-1
15	15	6	ZainJo		1518336150924	1518329386000	0	1	-1
16	16	4	Uber		1518336156650	1518336022000	0	1	-1
17	17	6	ZainJo		1518336159234	1518329392000	0	1	-1
18	18	4	Uber		1518336228285	1518336053000	0	1	-1
19	19	5			1518376212190	1518374579000	0	1	-1
20	20	5			1518376218543	1518341136000	0	1	-1
21	21	5			1518376224667	1518366306000	0	1	-1
22	22	5			1518376233705	1518367399000	0	1	-1
23	23	7	150		1518421068774	0	0	1	-1
24	24	7	150		1518421074120	1518421072000	0	1	-1
25	25	7	150		1518421139705	1518421132000	0	1	-1
26	26	7	150		1518425206744	0	0	1	-1

Figure 62. Android SMS Information – File “sms.db”.

For iOS devices, SMS data can be found under “**Library/SMS/sms.db**”. Date is also stored in Unix Epoch time stamp format. However, for iMessage the Mac Epoch time stamp format is used. Figure 9 shows the “sms.db” database parsed using Oxygen Forensics SQLite Viewer.

Content Template	
Section Number	4.2.3
Section Title	Network and Location Artefacts
Introduction	
Content	<p>Information about the cellular network on Android devices can be found in the "cache.cell" file under folder "\data\data\com.google.android.location\files\", which contains information about the last 50 Cell Towers the phone was connected to.</p> <p>Information about the last 200 Wi-Fi Access Points (AP) the device was connected to can be found in "cache.wifi" file under the same location as the "cache.cell" file, which contains the MAC address of each AP in addition to the longitude and latitude.</p> <p>Both files, "cache.wifi" and "cache.cell", are binary formatted and need to be decoded/parsed. Most forensic tools can decode these files and many free tools are available online such as "android-locdump" (see: www.github.com/packetss/android-locdump).</p> <p>On Android device, location information can be found on different locations mainly under the folder "\data\data/com.google.android.apps.maps/database/" and several database files may be found here.</p> <p>The "da_destination_history.db" and "search_history.db" are the first place to check. The first contains information about the longitude and latitude of navigation start and destination using Google Maps. The second contains information about locations searching for using Google maps or suggested by the same app.</p> <p>iOS collects information about Cell towers and Wi-Fi Aps that the device connects to and where within their vicinity. Cell towers information can be found in an encrypted SQLite database file "Data/root/library/Caches/locationd/cache_encryptedA.db", while the Wi-Fi AP information is stored in "cache_encryptedB.db" under the same location. The information is stored for 7 days. However, for iOS version 4 the information is stored indefinitely in the "consolidated.db" file.</p>

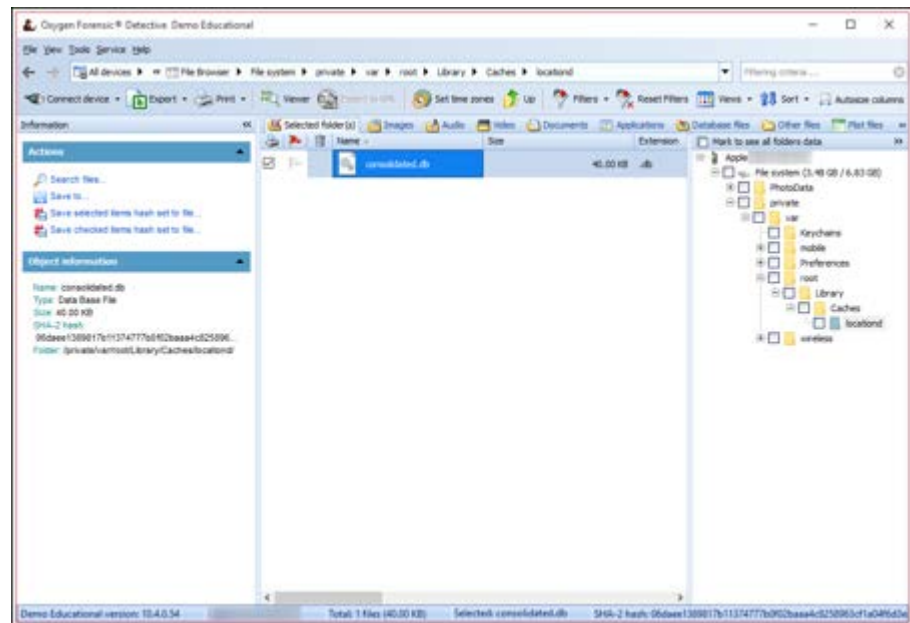


Figure 63. iPhone Location Information – File “consolidated.db”.

Content Template	
Section Number	4.2.4
Section Title	System Artefacts
Introduction	
Content	<p>In Android devices, the System artefacts can be found under "/data/system/" folder. Accessing this folder requires root privileges. The common artefacts that can be extracted from this folder are the following:</p> <ul style="list-style-type: none"> • The list of installed Apps and their location/permissions, which can be extracted from "packages.xml" file. • The apps usage history, including last run time, which can be found under "usagstats/usage-history.xml" file. • The accounts that are available on the device (e.g. Google, Facebook, Dropbox, etc.), which can be found in a SQLite database file under "users/0/accounts.db". The database stores a list of available accounts including username, password (hashed), and account provider. • The screen lock password hash file, which can be found under "password.key". • The screen lock pattern hash file, which can be found under "gesture.key". <p>Unlike Android, on iOS devices the accounts information is not stored in a central location, but it is scattered in many locations.</p>

Content Template	
Section Number	4.2.5
Section Title	Multimedia Files Artefacts
Introduction	
Content	<p>Multimedia files may be stored on the internal or the external storage (i.e. SD card) on Android devices.</p> <p>Images/videos captured from the camera can be usually found under the "DCIM" folder on the internal/external folder. These files may contain Exchangeable Image File (EXIF) tags that store several metadata about the file, with a particular reference to the information on where the picture was taken.</p> <p>Each app stores its multimedia files differently. They might be stored in a SQLite database file(s) or in their original formats in the application folder. For example, WhatsApp stores the multimedia files (e.g. videos, pictures, voice notes, etc.) in their original format under its folder.</p> <p>On iOS devices, multimedia files can be found in the internal memory since they do not have an external memory storage. By default, camera images/videos are stored in the "DCIM/" folder. Moreover, iOS tracks all multimedia files information (e.g. location, upload/share, last interact timestamp, etc.) and stores these information under "photos.sqlite" database file. Information about Deleted multimedia files can be found here.</p>

Content Template	
Section Number	4.3
Section Title	Data and File Carving
Introduction	<p>In this section, we explain the concept of file carving and highlight its importance in mobile forensics.</p> <p>Upon the completion of this section, the student is expected to be familiar with the general concept of carving and how carving can affect the forensic investigation.</p>
Content	<p>Carving is the process of extracting data or files from raw data (usually physical images). It is often associated with data recovery and it is used in digital forensics to recover deleted files from unallocated spaces.</p> <p>Multiple techniques can be utilized in file and data carving:</p> <ul style="list-style-type: none"> • File Signature: searching for known file-types signature using file header/footer. For example, JPG/JPEG files always start with "FF D8 FF". The website "www.filesignatures.net" has a comprehensive and searchable database of file signatures. • Block-based: scan for data block-by-block, where the block size is fixed. • Statistical: applies statistical analysis techniques to extract the data (e.g. letters frequency). • Linguistic: applies linguistic analysis methods (e.g. semantic analysis) and natural language processing to find contents that might be related. <p>In digital forensics, file carving plays a crucial role in finding deleted files. Cellebrite UFED Physical Analyzer can perform file carving for images on both physical and logical device images. It supports signature-based and block-based scanning from unallocated spaces.</p>

Content Template	
Section Number	4.4
Section Title	Deleted Files Recovery
Introduction	<p>In this section, we explain the tools and techniques that can be used to find and recover deleted files.</p> <p>Upon the completion of this section, the student is expected to have a general understanding of how deleted files might be recovered during the mobile forensic investigation.</p>
Content	<p>As explained in Section 4.1, NAND flash memory utilizes a process called "Wear Levelling" to even out the write operations across all cells of the memory. Because data can only be deleted in Blocks, traces of deleted files might be found and even old copies or deleted copies might be recovered (fully or partially).</p> <p>With logical images, deleted files recovery from unallocated space is not possible. However, with file system acquisition, recovery is possible, even though parsing the files might not be correct and/or complete. Only with physical image acquisition deleted files recovery might be possible.</p> <p>Deleted data might be recovered from SQLite database files regardless of the acquisition method. Mari DeGrazia has released a free and open-source tool "SQLite Deleted Records Parser" written in Python to parse and recover deleted records from SQLite database files (see: www.github.com/mdegrazia/SQLite-Deleted-Records-Parser).</p> <p>The following steps can be followed to search for deleted files:</p> <ol style="list-style-type: none"> 1. Perform physical acquisition (if possible). 2. Use keyword search to look for potential key words that might appear in deleted files (e.g. top-secret). 3. Search for traces of deleted files on SD and SIM cards (if applicable). 4. Examine SQLite database files for deleted records. 5. Examine cache locations. 6. Perform file carving (if possible). 7. Check backup files and cloud storage for potential deleted files.

Content Template	
Section Number	4.5
Section Title	Bypassing Security Controls
Introduction	<p>In this section, we highlight some of the techniques that can be used to bypass security controls and gain access to locked devices to perform forensic acquisition.</p> <p>Upon the completion of this section, the student is expected to be familiar with these techniques and be able to distinguish between them.</p>
Content	<p>Bypassing the security controls on mobile devices is not an easy task, yet not impossible. However, this is highly dependent on the device manufacturer and model, as well as on the operating system version.</p> <p>Usually, forensic tools such as Oxygen Forensic Extractor use publicly known vulnerabilities to bypass these controls. On the other hand, Cellebrite develops its own proprietary vulnerabilities and bootloaders in order to bypass security controls and locked devices (see: extra material #4.5, #4.6).</p> <p>Cellebrite Advanced Services (CAS) is an extra service offered by Cellebrite to law enforcement agencies to unlock and decrypt protected phones. At the time of writing, the following devices are supported:</p> <ul style="list-style-type: none"> • All iPhone models (iPhone 4S to iPhone X), iPad, iPad mini, iPad Pro and iPod touch, running iOS 5 to iOS 11. • Most Samsung devices including Galaxy S6/S7/S8, A5/A7/A8, J1/J3/J5/J7, Note 5/Note 8. <p>CAS service requires the device to be shipped to Cellebrite to be unlocked.</p> <p>Android Debug Bridge (ADB) can be used to bypass locked Android devices. Forensic tools such as Cellebrite UFED and XRY utilize this technique; however, USB debugging must be enabled for this to work. Nonetheless, Cellebrite UFED is capable of bypassing some locked Android devices even when USB debugging is not enabled.</p> <p>JTAG technique (see Section 2.2.5) can be used to bypass Android locked devices even when USB debugging is disabled. However, JTAG technique is dependent on the device make and model; in addition, that requires specialized tools and advanced skills.</p> <p>It is also worth looking for a backup image of the mobile device on a computer used to synchronize with the device. Check iTunes for iOS devices and Kies for Samsung devices.</p> <p>Some third-party tools offer to brute-force PIN codes on locked devices (e.g. iP-Box for iPhone, discontinued). However, brute-forcing is not a forensically recommended task because some phones are configured to wipe all data after 10 (default) failed attempts.</p> <p>Jailbroken iPhones usually have SSH root access enabled without password, which can be used to bypass locked devices. It is worth it to check whether the iPhone has been jailbroken or not.</p> <p>Cellebrite and XRY have built-in tools to decode pattern lock and simple PIN code lock on Android devices. Oxygen Forensic has similar tools for some LG devices.</p> <p>Emergency Download (EDL) mode is a feature on some Qualcomm chipsets that allows the chipset to boot into emergency mode in order to flash a new</p>

software (in this case Android bootloader) on the device. This requires access to a tool called "programmer", which is unique for the chipset type/version.

EDL is a powerful technique that can be used to bypass locked devices (both Android and Windows) where USB debugging is not enabled and acquires physical image.

Several methods may be used to put a device in an EDL mode. However, they all depend on the make and model of the device. The easiest method is to use ADB commands to reboot the device into EDL mode, but it requires USB debugging to be enabled.

The second method is to use a special EDL cable (also called "deep flash cable"), which is often used to flash devices. Although the cable cost is usually very cheap (less than \$20), it might not work with all devices.



Figure 64. Example of an EDL Cable. Adopted from: <https://m.it.aliexpress.com/item/32821478160.html>

The third method involves shorting the CMD JTAG pins ("Command In / Response Out") on the device, which might require disassembling the device. Moreover, not all devices have JTAG pins.

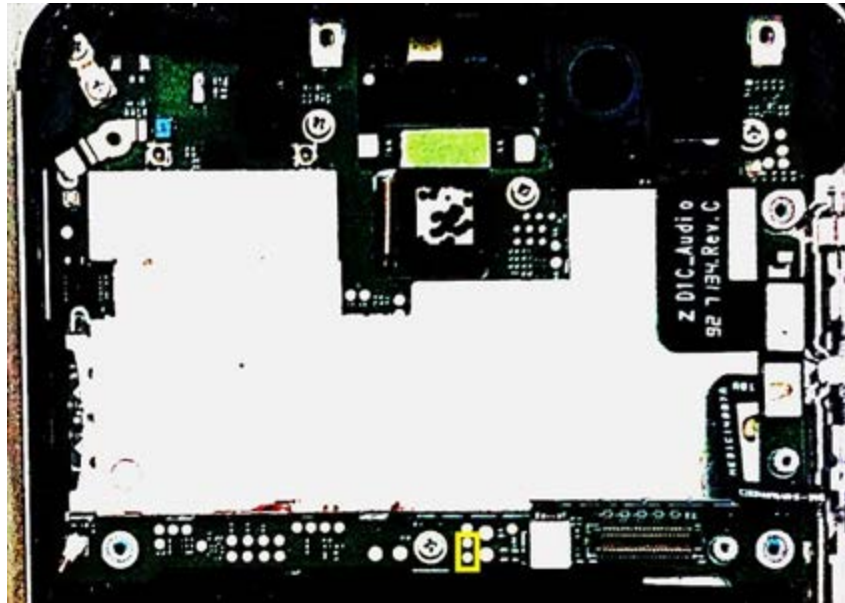


Figure 65. CMD JTAG Pins on Nokia 6. Adopted from: <https://alephsecurity.com/2018/01/22/qualcomm-edl-1/?resub>

Students are encouraged to read the articles on EDL mode by "Aleph Research" (see extra material #4.7).

On Windows Mobile devices, loaded registry hives are locked by the operating system and cannot be normally copied by forensic tools. However, Windows use Flash Abstraction Layer (FAL) library "fal.lib" to access the NAND memory. Data can be read from the memory by calling the ReadSector() function. XRY utilizes the FAL library to bypass the operating system lock and get direct access to the registry hives from the memory.

Windows Phone 8 and Windows 10 Mobile devices employ Trusted Boot and Code Signing to secure the boot process. This limits the forensic tools ability of acquiring physical image from the device. Usually, Chip-off techniques can be used to bypass this, However, it requires advanced skills and tools and a single mistake can be fatal to the device.

Windows Phone Internals (WPinternals) is a free tool that can be used to unlock the bootloader on Windows Phone devices, thus allowing physical imaging of the device (See: www.wpinternals.net).

EDL mode technique can also be used to bypass the secure boot control on some Windows Phone devices (e.g. Nokia 5/6).

Activity Template	
Number	4.1
Title	<p>Identify 3 different mobile artefacts that were not mentioned in Section 4.2 and write a brief report describing their:</p> <ol style="list-style-type: none"> 1. Location (Mainly in Android and iOS). 2. Structure. 3. Extracting and Parsing techniques.
Type	Research
Aim	<p>ILOs: 1</p> <p>The activity aims to let the student explore more forensic artefacts than what has been taught in the textbook.</p>
Description	4.2
Timeline	1-3 hours
Assessment	<p>Each student is required to submit a three pages (minimum) report.</p> <p>The report will be assessed based on completeness, correctness and overall quality.</p>

Activity Template	
Number	4.2
Title	Perform image acquisition, data extraction and analysis from a mobile device (or a mobile device image) using one of the Mobile forensics tools available at your University's Lab. Make sure to recover any deleted files/data. Work in a group of 2-3 students to produce a complete and comprehensive forensic report. Present your findings in 10 minutes slot.
Type	Reflection
Aim	<p>ILOs: 2, 3, 4, 5, 6, 7</p> <p>The activity aims to develop the student's ability to work effectively within a team to perform SIM forensic analysis and reporting practically in a forensically sound manner.</p>
Description	4.2, 4.3, 4.4, 4.5
Timeline	6-9 hours
Assessment	<p>Each group is required to submit a comprehensive forensic report detailing the process, techniques, tools and findings.</p> <p>The report will be assessed based on completeness, correctness, overall quality, soundness of the process followed, team work efforts and presentation.</p>

Activity Template	
Number	4.3
Title	<p>Forensic tools utilize different techniques in order to acquire an image from mobile devices. Some tools use custom bootloaders, agent apps, exploits to gain root access, and several other techniques.</p> <p>Locard's Exchange Principle dictates that these changes must leave traces on the device, which can be forensically identified.</p> <p>Devise an experiment to determine what kind of forensic traces each technique leaves on the evidentiary device (pick one technique, one tool). Present your finding in a research paper format.</p>
Type	Reflection, Research
Aim	<p>ILOs: 1, 2, 3, 4</p> <p>The activity aims to build the student's ability to conduct research and development in order to find solution for new problems.</p>
Description	5.1.9
Timeline	9-15 hour
Assessment	<p>The student is assessed based on the scientific quality of the produced research paper.</p> <p>This is an advanced activity and it is not expected that many students will attempt.</p>

Think Template (MCQs)	
Number	4.1
Title	Android, BlackBerry, iOS and Windows Mobile Forensics
Type	Fill in the blanks
Question	<p>NAND memory is made up of multiple _____, which are organized into _____, which are grouped into _____.</p> <ul style="list-style-type: none"> a. Blocks b. Cells c. Pages d. Sectors e. Tracks
Answers	Answer: Cells, Pages, Blocks

Think Template (MCQs)	
Number	4.2
Title	Android, BlackBerry, iOS and Windows Mobile Forensics
Type	Choose correct answer
Question	<p>Apple Watch Series 4 is running watchOS v5.0, which uses a proprietary file system developed by Apple, which is:</p> <ul style="list-style-type: none"> a. HFS+ b. APFS c. HFS d. YAFFS2
Answers	Answer: B

Think Template (MCQs)	
Number	4.3
Title	Contacts and Phone Call Artefacts
Type	Choose correct answer
Question	<p>Date information stored in the "logs.db" and "contacts2.db" SQLite database files are encoded using Mac HFS+ timestamp.</p> <p>a. True</p> <p>b. False</p>
Answers	Answer: B

Think Template (MCQs)	
Number	4.4
Title	Data and File Carving
Type	Choose correct answer
Question	<p>The correct signature for JPG/JPEG files is:</p> <ul style="list-style-type: none"> a. "F6 C8 F6" b. "6F D8 6F" c. "FF D8 FF" d. "FF C8 FF"
Answers	Answer: C

Think Template (MCQs)	
Number	4.5
Title	Bypassing Security Controls
Type	Fill in the blanks
Question	<p>_____ is a powerful technique to bypass locked devices where USB debugging is not enabled and acquire physical image.</p> <ul style="list-style-type: none"> a. Emergency Download Mode b. ADB c. WPinternals d. CAS
Answers	Answer: A

Extra Template	
Number	4.1
Title	Apple File System Basics
Topic	4.1
Type	URL: https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html

Extra Template	
Number	4.2
Title	ABPerson Class
Topic	4.2.1
Type	URL: https://developer.apple.com/documentation/addressbook/abperson?language=objc

Extra Template	
Number	4.3
Title	Windows Phone 8.10 MMS (for Lumia 530)
Topic	4.2
Type	URL: http://cheeky4n6monkey.blogspot.com/2015/12/windows-phone-810-mms-for-lumia-530.html

Extra Template	
Number	4.4
Title	An Initial Peep at Windows 10 Mobile (Lumia 435)
Topic	4.2
Type	URL: http://cheeky4n6monkey.blogspot.com/2016/04/an-initial-peep-at-windows-10-mobile.html

Extra Template	
Number	4.5
Title	Cellebrite: What You Need to Know About Cell Phone Forensics - North Star Post 20160223
Topic	4.5
Type	URL: https://let.snowden.in/2016/02/25/cellebrite-what-you-need-to-know-about-cell-phone-forensics-north-star-post-20160223/


Extra Template	
Number	4.6
Title	Snippets on Cellebrite's Samsung Solution and Blackberry Solution
Topic	4.5
Type	URL: https://blog.cyberwar.nl/2016/03/snippets-on-cellebrites-samsung-solution-and-blackberry-solution-ocrd-from-legal-complaint-against-competitor/

Extra Template	
Number	4.7
Title	Exploiting Qualcomm EDL Programmers (*)
Topic	4.5
Type	URL: <ul style="list-style-type: none"> • https://alephsecurity.com/2018/01/22/qualcomm-edl-1 • https://alephsecurity.com/2018/01/22/qualcomm-edl-2 • https://alephsecurity.com/2018/01/22/qualcomm-edl-3 • https://alephsecurity.com/2018/01/22/qualcomm-edl-4 • https://alephsecurity.com/2018/01/22/qualcomm-edl-5

5. U/SIM Cards Forensics

Scope Template															
Number	5														
Title	U/SIM Cards Forensics														
Introduction	<p>SIM cards forensics constitutes an integral part of the overall Mobile Forensics process. Although, small in form factor U/SIM cards maintains several extremely important information that in some cases might be a key that make or break the case.</p> <p>In this chapter, we start by exploring the various artefacts that can be extracted from SIM cards and convey industry best practices for artefacts extraction and analysis in a forensically sound manner. Then, we introduce the concept of SIM card cloning and explain its role within mobile forensics. Thereafter, we present the various forensic tools and solutions that facilitate artefacts extraction and evidence analysis from SIM cards. Then, we briefly highlight the techniques that can help in bypassing SIM card security controls. Finally, we conclude the chapter by introducing Application Protocol Data Unit commands and response and explain their role in artefacts extraction.</p>														
Outcomes	<ol style="list-style-type: none"> 6. Understanding the various type of artefacts that can be extracted from SIM cards. 7. Collect and analyse artefacts from SIM cards. 8. Validate the results of mobile forensics solutions. 														
Topics	<ol style="list-style-type: none"> 5. U/SIM Cards Forensics <ol style="list-style-type: none"> 5.1. U/SIM Card Artefacts Extraction <ol style="list-style-type: none"> 5.1.1. Integrated Circuit Card Identifier (ICCID) 5.1.2. International Mobile Subscriber Identity (IMSI) 5.1.3. Mobile Station International Subscriber Directory Number (MSISDN) 5.1.4. Abbreviated Dialling Numbers (ADN) 5.1.5. Fixed Dialling Numbers (FDN) 5.1.6. Last Number Dialed (LND) 5.1.7. Location Information 5.1.8. Phonebook 5.1.9. Messages 5.2. U/SIM Card Cloning. 5.3. U/SIM Card Forensic Tools 5.4. Bypassing U/SIM Card Security Controls 5.5. APDU Commands 														
Study Guide	<table border="1"> <thead> <tr> <th>Task</th><th>Time</th></tr> </thead> <tbody> <tr> <td>Preparation (Introduction and On-line Planning):</td><td>2 hr</td></tr> <tr> <td>Textbook Content:</td><td>6 hr</td></tr> <tr> <td>Thinking (On-line discussions, Review questions)</td><td>1 hr</td></tr> <tr> <td>Tutorial Work:</td><td>6 hr</td></tr> <tr> <td>Related Course Work:</td><td>1 hrs</td></tr> <tr> <td>Total</td><td>16 hours</td></tr> </tbody> </table> <ul style="list-style-type: none"> • Required study time: 16 hours • Required hardware/software: <ol style="list-style-type: none"> 1. GSM Modem (unlocked). 2. Putty for Windows or Minicom for Linux. 3. Cellebrite UFED or any other forensic tool that can perform SIM card extraction and analysis. • Required external resources including links and books: 	Task	Time	Preparation (Introduction and On-line Planning):	2 hr	Textbook Content:	6 hr	Thinking (On-line discussions, Review questions)	1 hr	Tutorial Work:	6 hr	Related Course Work:	1 hrs	Total	16 hours
Task	Time														
Preparation (Introduction and On-line Planning):	2 hr														
Textbook Content:	6 hr														
Thinking (On-line discussions, Review questions)	1 hr														
Tutorial Work:	6 hr														
Related Course Work:	1 hrs														
Total	16 hours														

	1. See extra materials.
--	--------------------------------

Content Template	
Section Number	5.1
Section Title	U/SIM Card Artefacts Extraction
Introduction	<p>In this section, we will explore the various forensic artefacts that might be extracted from SIM card in addition to how to extract the artefacts in a forensically sound manner.</p> <p>Upon the completion of this section, the student is expected to:</p> <ul style="list-style-type: none"> • Have a clear understanding about the different types of SIM card forensic artefacts. • Be able to explain the process of extracting artefacts from SIM card. • Be able to practically extract and analyse SIM card artefacts.
Content	<p>SIM Cards are used in many mobile devices (smartphones, drones, 3G/4G Wi-Fi routers, etc.). The main application of SIM card is to authenticate the subscriber to the network and vice-versa in a secure manner.</p> <p>Additionally, it can hold many personal information such as phonebook, messages, location information, emergency numbers and more. For that, a combination of read-only memory, i.e. ROM, and rewritable memory, i.e. EEPROM, is used to store the data in SIM card. Usually, the SIM card memory capacity ranges between 8KB to 1GB.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Samsung announced the S-SIM™ card back in 2006, which is a revolutionary SIM card with 1GB NAND flash memory storage at the same small form factor of conventional SIM cards.</p> </div> <p>GSM-based and UMTS mobile phones always have a SIM card inside the phone. Sometimes even two SIM cards in dual SIM phones, which are popular in the EMEA region. On the other hand, traditional CDMA mobile devices, which are popular in the USA and China, do not use SIM card. Nonetheless, some CDMA devices have a Removable User Identity Module (R-UIM) card, which is similar in functionality to the traditional SIM card. Newer CDMA devices (i.e. CDMA2000 mobile technology) use a CDMA Subscriber Identity Module (CSIM) card, which runs on top of the UICC similar to the USIM card.</p> <div style="text-align: center;">  </div> <p>Figure 66. Motorola i940 Push-to-Talk Smartphone running Android (v2.1). [https://motorola-global-portal-pt.custhelp.com]</p> <p>Push-to-Talk (PTT) mobile phones operate using Integrated Digital Enhanced Network (iDEN) or Wideband Integrated Digital Enhanced Network (WiDEN) technology. They are common in North and South America, Saudi Arabia and Israel. Newer PTT devices also use a SIM card similar to GSM but not</p>

compatible. iDEN SIM card also stores information that can be useful in a forensic investigation.

Some tools such as Cellebrite UFED will ask you to identify the SIM card type prior beginning the extraction process.



Figure 67. Cellebrite UFED SIM Card Extraction Menu.
[<http://forensedigital.com.br>]

Forensically, the information stored on SIM card constitutes valuable artefacts for the investigation. It is important to know that some of data is stored on the read-only memory. However, most of it is stored on the rewriteable memory. Since using a write-blocker when extracting data from SIM card is not possible, the investigator has to take extra care when examining SIM cards to avoid changing the status of the information and contaminating the evidence.


The current best practices for extracting data from a SIM card in a forensic investigation are the following:

6. Remove the evidentiary SIM card from the device.
7. Create a clone (network-isolated) SIM card.
8. Place the cloned SIM card in the device.
9. Extract data from the evidentiary SIM card.
10. Reserve the evidentiary SIM card in the evidence locker.
11. Extract data from the device.

Extracting data from the mobile device whilst the evidentiary SIM card is still in the device is considered a serious common mistake among new investigators as it can lead to evidence contamination! Whenever possible, remove the evidentiary SIM card from the device prior extracting data from them.

Sometimes, it is not possible to remove the SIM card without removing the battery first from the device. In that case, you should refer to the mobile device data extraction best practices described in Section 4.2 to determine whether to shut down the device or not.

	A SIM card can hold more than 40 different type of forensic Artefacts. In the following subsections, we will discuss the most important SIM card Artefacts.
--	---

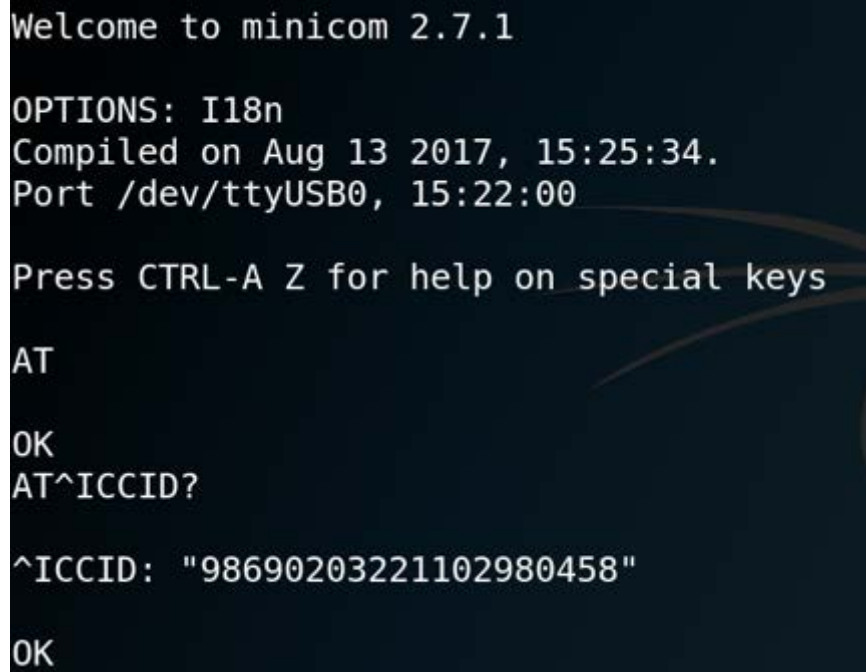
Content Template																																								
Section Number	5.1.1																																							
Section Title	Integrated Circuit Card Identifier (ICCID)																																							
Introduction																																								
Content	<p>The Integrated Circuit Card Identifier (ICCID) is a 19 or 20 digits unique number that is used to identify a SIM card internationally. In some context, it is referred to as SIM Serial Number (SSN).</p> <p>The ICCID is often printed on the SIM card itself and most forensic tools can extract it even if the SIM card was locked.</p> <div></div> <p>Figure 68. Example of ICCID printed on SIM Card.</p> <p>The last digit of the ICCID is a checksum digit to detect potential errors. The checksum value is calculated using the Luhn algorithm as defined by ISO/IEC 7812-1, Annex B (www.ee.unb.ca/cgi-bin/tervo/luhn.pl).</p> <p>The ICCID format for SIM cards is defined by the ITU-T Rec. E.118 as follows:</p> <table><tr><th colspan="8">ICCID</th></tr><tr><th colspan="3">IIN¹</th><th colspan="4">IAIN</th><th rowspan="2">C</th></tr><tr><th>MII</th><th>CC</th><th>IIN²</th><th colspan="4">operator specific format</th></tr><tr><td>89</td><td>962</td><td>03</td><td>02</td><td>21</td><td>12</td><td>089408</td><td>5</td></tr><tr><td>Telecom</td><td>Jordan</td><td>Umniah</td><td>MM</td><td>DD</td><td>YY</td><td>SSN</td><td>⊗</td></tr></table> <ul style="list-style-type: none">• IIN¹ (Issuer Identification Number) as defined by ITU-T Rec. 118 can be 6-7 digits long and consists of MMI, CC and IIN².• MII (Major Industry Identifier) is a 2-digits prefix as defined by the ISO/IEC 7812-1 standard. It is always '0x89' for telecommunications.• CC (Country Code) as defined by ITU-T Rec. E.164 and it can be 1-3 digits long (e.g. JO: 962, PS: 970).• IIN² (Issuer Identifier Number) can be 1-4 digits long, which uniquely identifies mobile operators within a country (e.g. JO/Umniah: 03, JO/Orange: 77, PS/Jawwal: 05, PS/Wataniya: 06).• IAIN (Individual Account Identification Number) can have variable length up to 12 digits and it has operator specific format.• C (Checksum) is a parity check digit calculated using the Luhn algorithm.	ICCID								IIN ¹			IAIN				C	MII	CC	IIN ²	operator specific format				89	962	03	02	21	12	089408	5	Telecom	Jordan	Umniah	MM	DD	YY	SSN	⊗
ICCID																																								
IIN ¹			IAIN				C																																	
MII	CC	IIN ²	operator specific format																																					
89	962	03	02	21	12	089408	5																																	
Telecom	Jordan	Umniah	MM	DD	YY	SSN	⊗																																	

A collection of tools to parse and analyse telecommunication numbers, such as ICCID, IMSI, etc., are available online such as:

- www.numberingplans.com
- www.sndeeep.info

AT Commands can be used to extract the ICCID manually. The exact AT command is different depending on the modem used.

The example below shows how to extract the ICCID via AT commands using Huawei E173u-1 Modem (see the complete AT commands reference at extra material #5.5).



```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Aug 13 2017, 15:25:34.
Port /dev/ttyUSB0, 15:22:00

Press CTRL-A Z for help on special keys

AT

OK
AT^ICCID?

^ICCID: "98690203221102980458"

OK
```

Figure 69. Extract ICCID via AT Command "AT^ICCID?"

The ICCID is stored in the EF_{ICCID} file with AID '2FE2' which is located directly under the MF with AID '3F00'.

The ICCID structure and format is defined by the GSM 11.11 protocol:

- 10 bytes.
- Binary Coded Decimal (BCD) coding.
- Left justified and padded with '0xF'.
- Little-Endian bit order within the byte.
- Swapped digits within the byte.

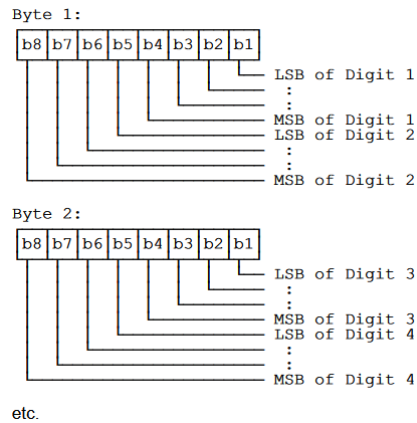


Figure 70. ICCID Bit/Byte order as defined by the GSM 11.11 protocol.

In the example above: the ICCID is stored as "98 69 02 03 22 11 02 98 04 58", which is decoded to "89962030221120894085".

If an error code is returned when using AT commands instead of the expected value, refer to the GSM error codes at extra material #5.7 for more information.

Content Template																																			
Section Number	5.1.2																																		
Section Title	International Mobile Subscriber Identity (IMSI)																																		
Introduction																																			
Content	<p>The International Mobile Subscriber Identity (IMSI) is a unique number (up to 15 digits) used by the carrier to identify the subscribers in its cellular network.</p> <p>Most forensic tools can extract the IMSI; however, if the SIM card is locked, then the IMSI cannot be retrieved without knowing the PIN code (CHV1). The IMSI is stored under the DF_{GSM} folder with AID '7F20' in the EF_{IMSI} file with AID '6F07'.</p> <p>The IMSI format is defined by the ITU-T Ref. E.212 as follows:</p> <table><tr><th colspan="3">IMSI</th></tr><tr><th>MCC</th><th>MNC</th><th>MSIN</th></tr><tr><td>416</td><td>03</td><td>2110524133</td></tr><tr><td>Jordan</td><td>Umniah</td><td>Subscriber ID</td></tr></table> <ul style="list-style-type: none">MMC (Mobile Country Code) is a 3-digit number that is used in conjunction with MNC to uniquely identify the mobile carriers internationally. The first digit identifies the geographic region of the carrier as shown below:<table><tr><th>Digit</th><th>Region</th></tr><tr><td>0</td><td>Test networks.</td></tr><tr><td>1</td><td>Not used.</td></tr><tr><td>2</td><td>Europe.</td></tr><tr><td>3</td><td>North America and the Caribbean.</td></tr><tr><td>4</td><td>Asia and the Middle East.</td></tr><tr><td>5</td><td>Oceania.</td></tr><tr><td>6</td><td>Africa.</td></tr><tr><td>7</td><td>South and Central America.</td></tr><tr><td>8</td><td>Not used.</td></tr><tr><td>9</td><td>Worldwide.</td></tr></table>MNC (Mobile Network Code) is a 2-3 digits number that uniquely identifies the mobile carriers within a country. The European standard uses 2 digits while the North American standard uses 3 digits.MSIN (Mobile Subscription Identification Number) is the subscriber unique identifier and it can be up to 10 digits. <p>AT Commands can be used to extract the IMSI manually assuming that the SIM card is unlocked or the PIN1 code (CHV1) is known. The exact AT command is different depending on the modem used.</p>	IMSI			MCC	MNC	MSIN	416	03	2110524133	Jordan	Umniah	Subscriber ID	Digit	Region	0	Test networks.	1	Not used.	2	Europe.	3	North America and the Caribbean.	4	Asia and the Middle East.	5	Oceania.	6	Africa.	7	South and Central America.	8	Not used.	9	Worldwide.
IMSI																																			
MCC	MNC	MSIN																																	
416	03	2110524133																																	
Jordan	Umniah	Subscriber ID																																	
Digit	Region																																		
0	Test networks.																																		
1	Not used.																																		
2	Europe.																																		
3	North America and the Caribbean.																																		
4	Asia and the Middle East.																																		
5	Oceania.																																		
6	Africa.																																		
7	South and Central America.																																		
8	Not used.																																		
9	Worldwide.																																		

The example below shows how to extract the IMSI from a locked SIM card via AT commands. For the explanation of each AT command/response meaning, refer to extra material #5.5).

```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Aug 13 2017, 15:25:34.
Port /dev/ttyUSB0, 17:51:52

Press CTRL-A Z for help on special keys

AT

OK
AT+CPIN?

+CPIN: SIM PIN

OK
AT+CPIN="0000"

OK
AT+CPIN?

+CPIN: READY

OK
AT+CIMI

416032110524133

OK
```

Figure 71. Extract IMSI from Locked SIM via AT Command "AT+CIMI".

Content Template																				
Section Number	5.1.3																			
Section Title	Mobile Station International Subscriber Directory Number (MSISDN)																			
Introduction																				
Content	<p>The Mobile Station International Subscriber Directory Number (MSISDN) is a number (up to 15 digits) that identifies a subscriber in the network, and is used by other subscribers to call/message him/her.</p> <p>Most carriers do NOT hard-code the MSISDN to the SIM card, which makes it hard to extract forensically unless the user saved it to the SIM card. The MSISDN is stored in the EF_{MSISDN} file with AID '6F40' which is under the DF_{TELECOM} folder with AID '7F10'.</p> <p>The MSISDN has multiple formats, which are defined by the ITU-T Ref. E.164 as follows:</p> <table><tr><th colspan="3">MSISDN</th></tr><tr><th>CC</th><th>NDC</th><th>SN</th></tr><tr><td>962</td><td>079</td><td>1234567</td></tr><tr><td>JO</td><td>Zain</td><td>Subscriber Phone Number</td></tr><tr><td>970</td><td>0229</td><td>12345</td></tr><tr><td>PS</td><td>Ramallah</td><td>Subscriber Phone Number</td></tr></table> <ul style="list-style-type: none">• CC (Country Code) is 1-3 digits long number (e.g. JO: 962, PS: 970).• NDC (National Destination Code) is a unique number, usually 2-4 digits, that is assigned to an area or a network service provide within a country.• SN (Subscriber Number) is a unique number that identifies the subscriber within the carrier network. <p>AT Commands can be used to extract the MSISDN manually assuming that the SIM card is unlocked or the PIN1 code (CHV1) is known. The exact AT command is different depending on the modem used.</p> <p>The example below shows how to extract the MSISDN from an unlocked SIM card via AT commands.</p>		MSISDN			CC	NDC	SN	962	079	1234567	JO	Zain	Subscriber Phone Number	970	0229	12345	PS	Ramallah	Subscriber Phone Number
MSISDN																				
CC	NDC	SN																		
962	079	1234567																		
JO	Zain	Subscriber Phone Number																		
970	0229	12345																		
PS	Ramallah	Subscriber Phone Number																		

```
Welcome to minicom 2.7.1

OPTIONS: I18n
Compiled on Aug 13 2017, 15:25:34.
Port /dev/ttyUSB0, 20:53:29

Press CTRL-A Z for help on special keys

AT

OK
AT+CNUM

+CNUM: "Own Number","07981169364",129

OK
```

Figure 72. Extract MSISDN from Unlocked SIM via AT Command "AT+CNUM".

Content Template	
Section Number	5.1.4
Section Title	Abbreviated Dialling Numbers (ADN)
Introduction	
Content	<p>The Abbreviated Dialling Numbers (ADN) is the standard address book storage available in both U/SIM cards.</p> <p>The ADN list is stored in the EF_{ADN} file with AID '6F3A' under the DF_{TELECOM} folder.</p> <p>AT Commands can be used to extract the ADN list manually from the SIM card. The exact AT command is different depending on the modem used.</p> <p>The example below shows how to extract the ADN list from the SIM card via AT commands.</p>  <pre> AT+CPBS=? +CPBS: ("SM", "EN", "ON") OK AT+CPBS="EN" OK AT+CPBS? +CPBS: "EN",2,50 OK AT+CPBR=1,2 +CPBR: 1,"911",129,"" +CPBR: 2,"112",129,"" OK </pre> <p>Figure 73. Extracting Emergency Numbers from SIM card.</p> <p>The AT command (AT+CPBS=?) shows the types of memory storage for the phonebooks that might be available. The possible values are:</p> <ol style="list-style-type: none"> 1. SM: U/SIM main phonebook. 2. EN: Emergence Numbers list on U/SIM. 3. ON: Owner Number on U/SIM (this is not the MSISDN). 4. FD: Fixed Dialling phonebook (see section 5.1.5 on FDN). 5. ME: Mobile Equipment internal phonebook. <p>The AT command (AT+CPBS="XX") selects a specific memory storage.</p>

The AT command (**AT+CPBS?**) shows the selected phonebook. In this case, it was the main phonebook. It also shows the total number of available records (250 contacts) and the number of used records (33 contacts).

The AT command to retrieve contacts/records from the selected phonebook is (**AT+CPBS=<start_index>,<end_index>**). The response format includes an index, the address, type of address, and the name of address. The common possible values for the type of address field are listed below.

Value	Description
125	Email type
129	Unknown type
145	International type (MSISDN)
161	National type (ISDN)
177	Network specific number

```

AT+CPBS=?
+CPBS: ("SM","EN","ON")

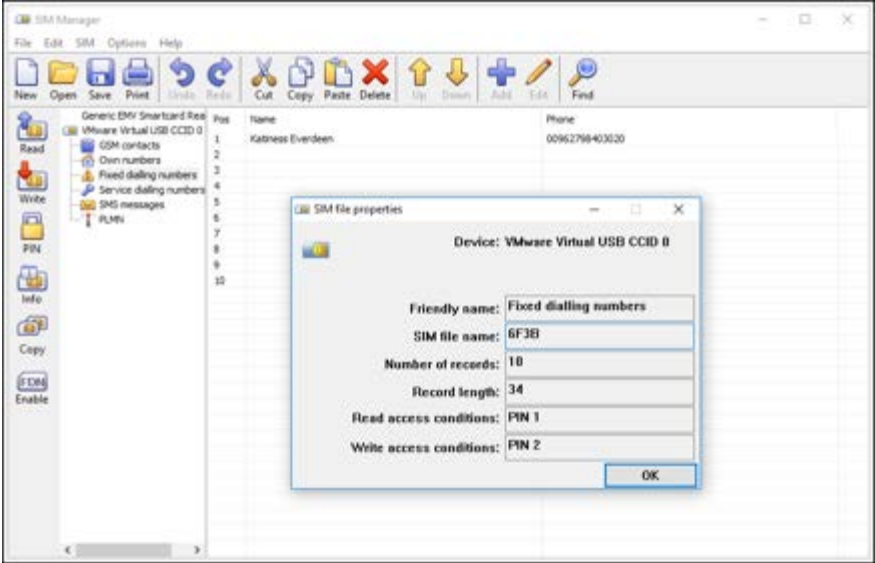
OK
AT+CPBS?
+CPBS: "SM",33,250

OK
AT+CPBR=1
+CPBR: 1,"*888#",129,"3G Mob Internet Bundle"

OK
AT+CPBR=1,33
+CPBR: 1,"*888#",129,"3G Mob Internet Bundle"
+CPBR: 2,"1313",129,"Aghanilak"
+CPBR: 3,"*133#",129,"Balance Check"
+CPBR: 4,"1399",129,"Block Service"
+CPBR: 5,"98000",129,"Chat (SMS)"
+CPBR: 6,"962788001333",129,"Customer Care Service"
+CPBR: 7,"*135#",129,"Delete Super Number"
+CPBR: 8,"962788001345",129,"Directory Inquiries"
+CPBR: 9,"90008000",129,"DJ Call"
+CPBR: 10,"1330",129,"Fav Countries Menu"
+CPBR: 11,"98111",129,"Flash (SMS)"
+CPBR: 12,"99888",129,"Friend Finder (SMS)"
+CPBR: 13,"962788001344",129,"Internet Customer Care"
+CPBR: 14,"*11#",129,"MissedCalls"
+CPBR: 15,"98080",129,"Pay4me (SMS)"
+CPBR: 16,"*1333*1*1*1#",129,"Phone Configuration"
+CPBR: 17,"*140#",129,"Pointing"
+CPBR: 18,"*1333#",129,"Self Service Menu"
+CPBR: 19,"*100#",129,"Umniah Portal"

```

Figure 74. Extracting Main Phonebook from U/SIM card.

Content Template	
Section Number	5.1.5
Section Title	Fixed Dialling Numbers (FDN)
Introduction	
Content	<p>The Fixed Dialling Numbers (FDN) is a list of phone numbers that, when enabled, restricts your outgoing calls to the numbers stored in this list.</p> <p>The list is stored in the EF_{FDN} file with AID '6F3B' under the DF_{TELECOM} folder.</p> <p>Updating the EF_{FDN} file is usually protected by PIN2 (CHV2), but it also can be protected by ADM or PIN1.</p>  <p>Figure 75. Extracting FDN List from SIM Card using SIM Manager.</p> <p>As a forensic examiner, it is considered a good practice to always perform the following: double-check the results of the forensic tools in order to verify their accuracy, correctness and completeness.</p> <p>In Figure 10, the SIM Manager was used to extract the FDN list and it showed that it contains a single record. Then, Oxygen Forensics® Extractor was used to acquire a logical image of the SIM card. Finally, the image was analysed using Oxygen Forensics® Detective (as shown in Figure 11), which also reported a single record under source file '6F3B'.</p> <p>Nonetheless, when manually examined, another record was found in the EF_{FDN} file, which was not reported by either tools as shown in Figure 12.</p>

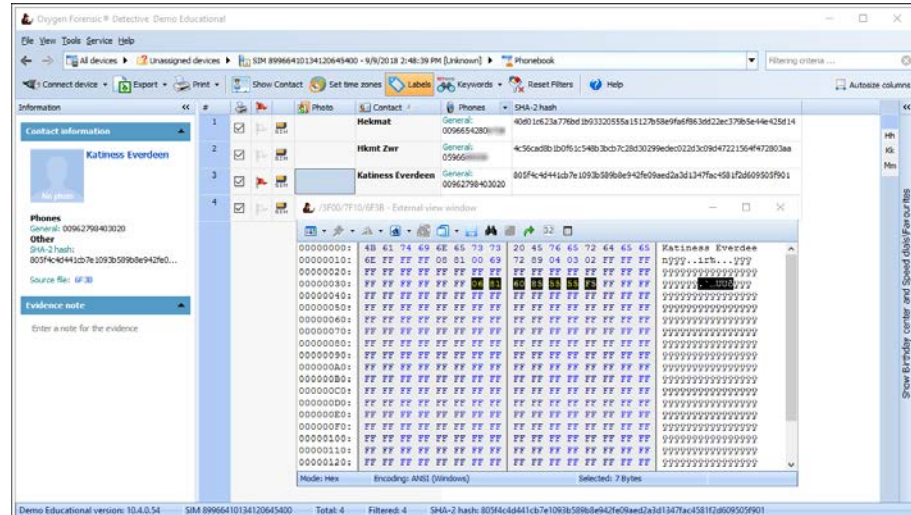


Figure 76. Examining FDN List - using Oxygen Forensics® Detective.

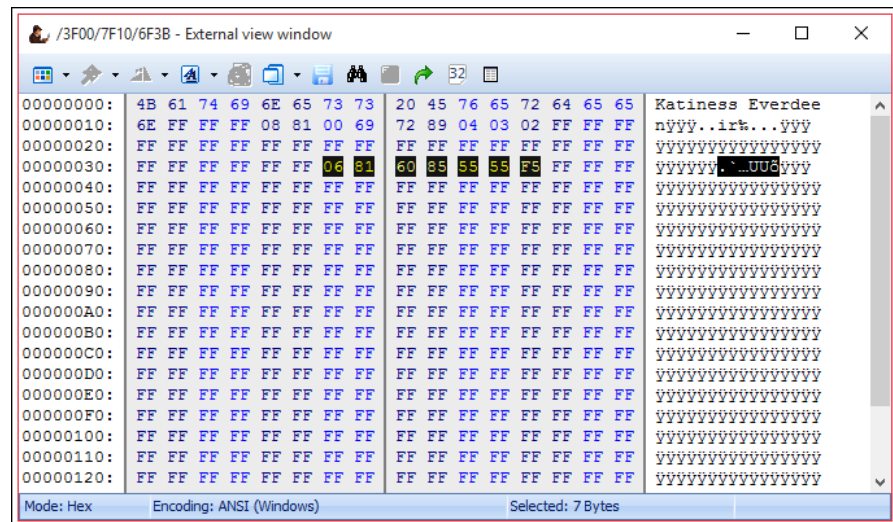


Figure 77. Manually Examining EF_{FDN} file.

The first record of the FDN starts at offset 0 in the EF_{FDN} file. The decoded recorded is explained below:

The first record (hexadecimal value):

4B 61 74 69 6E 65 73 73 20 45 76 65 72 64 65 65 6E FF FF FF 08 81 00 69 72 89 04 03 02

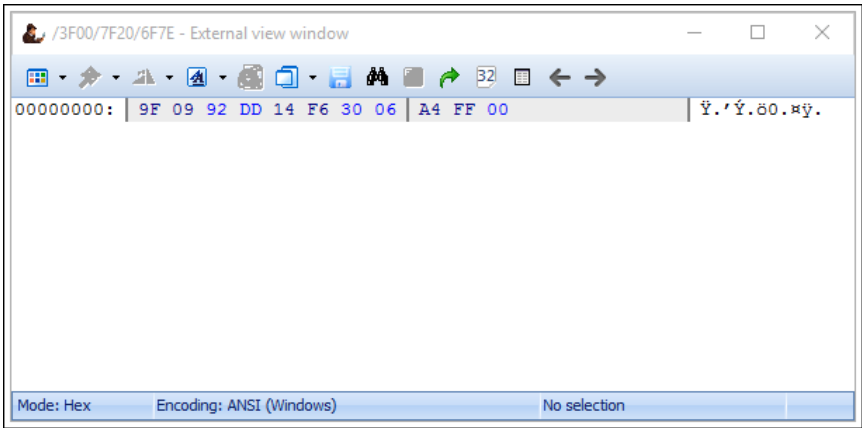
The first 20 bytes (4B 61 74 69 6E 65 73 73 20 45 76 65 72 64 65 65 6E FF FF FF) contain the Name in ASCII coding and padding with FF.

The next byte (08) is the length of the FDN in bytes including the next byte (TON).

The next byte (81) is the Type of Number (TON) indicator, which distinguishes whether the dialling number is in National, International, Subscriber, Partial, or Unknown format (see: GSM 04.08, 10.5.4.6). Common values are '0x91' for International and '0x81' for Unknown format.

	<p>Following this byte, there is the Fixed Dialling Number "00 69 72 89 04 03 02" stored in reverse nibble format and padded with '0xF'. The correct value is "00962-79-8403020".</p> <p>The unreported record was found at offset 54 (decimal), highlighted in Figure 12.</p> <p>The record Hexadecimal value is:</p> <p style="text-align: center;">06 81 60 85 55 55 F5</p> <p>The first byte '0x06' is the length of the FDN in bytes including the next byte. The TON identifier is a one-byte field; the value '0x81' indicates an unknown format similar to the first record.</p> <p>The next five bytes "60 85 55 55 F5" are the fixed dialling number also in reverse nibble format and padded with '0xF'. The correct value is "06-5855555".</p> <p>Contrarily to the first record (the one both tools extracted), the second record does not have a name (which is an optional field), which might explain why it was not extracted.</p> <p>This shows that, although the forensic tools can facilitate the artefacts extraction and examination process, it is highly recommend verifying their results with manual extract and examination whenever possible.</p>
--	--

Content Template	
Section Number	5.1.6
Section Title	Last Number Dialed (LND)
Introduction	
Content	<p>The Last Number Dialed (LND) is a list that stores the last calls originated from the mobile station holding the SIM card. This list only contains the outgoing calls. Incoming and missed calls are stored on the mobile station.</p> <p>It is worth mentioning that the list of LND stored on the mobile station may differ from the one stored on the SIM card.</p> <p>The LND can be found under the DF_{TELECOM} folder in the EF_{LND} file with AID '6F44'.</p> <p>The phone number is encoded in the reverse nibbles format, in a similar way to how ICCID and FDN were stored. Most forensic tools can decode it correctly. Remember to reverse the byte digits order when extracting it manually.</p>

Content Template	
Section Number	5.1.7
Section Title	Location Information
Introduction	
Content	<p>In order to determine the service area, the network carrier is constantly tracking the SIM card location in order to establish the region where the device is located. It also establishes the route for calls and messages to improve is service level.</p> <p>Location information are recorded on multiple files on the SIM card:</p> <ul style="list-style-type: none"> • Location Information: EF_{LOCI} file ('6F7E'), available on U/SIM under the DF_{GSM} folder ('7F20'). • Packet Switched location information: EF_{PSLOCI} file (AID '6F73'), available on USIM under ADF_{USIM} folder. • EPS location information: EF_{EPSLOCI} file (AID '6FE3'), available on USIM under ADF_{USIM} folder. • GPRS Location Information: EF_{LOCIGPRS} file (AID '6F53'), available on SIM under the DF_{GSM} folder.  <p>The EF_{LOCI} file (11 bytes) contains the following information:</p> <ul style="list-style-type: none"> • Temporary Mobile Subscriber Identity (TMSI): it is a temporary IMSI (4 bytes) that is generated whenever the device is either power cycled or new carrier is selected. The TMSI is used to protect the IMSI from eavesdropping attacks. The TMSI can indicate the location of the device. • Location Area Information (LAI): it is a unique identifier (5 Bytes) that is broadcasted regularly by each Public Land Mobile Network (PLMN) and picked up by the mobile station then stored on the SIM card. • TMSI Time: the current value of the periodic Location Updating Timer (1 byte). Used in USIM, RFU in SIM. • Location Update Status: an indicator (1 byte) of whether the location was updated or not. <p>In Figure 14, the TMSI value is (9F 09 92 DD), the LAI value is (14 F6 30 06 A4), the TMSI Time value is (FF) indicating that it is not used because it is a</p>

	Phase 2 ME. Finally, the location update status indicator shows that the location was updated.
--	--

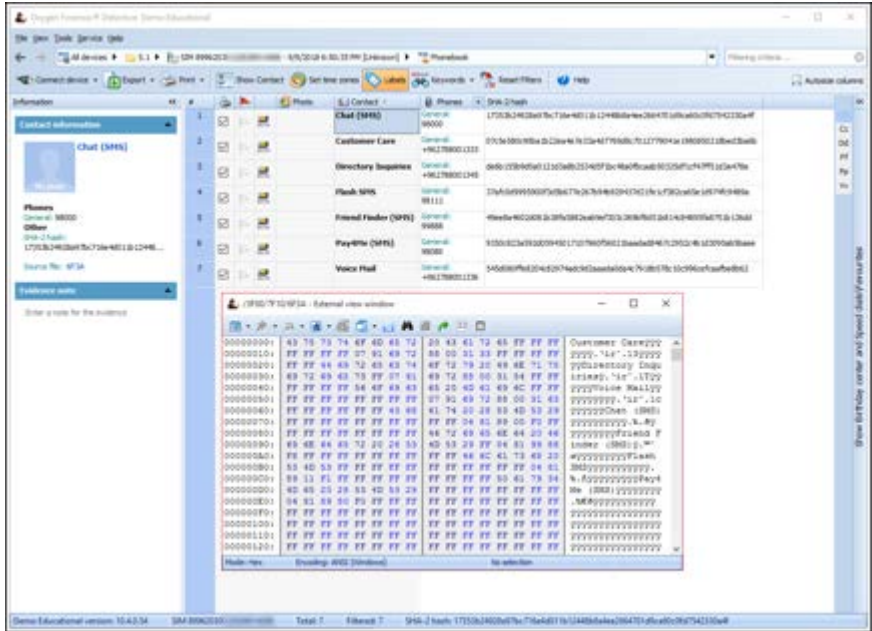
Content Template	
Section Number	5.1.8
Section Title	Phonebook
Introduction	
Content	<p>The standard address book is available in the EF_{ADN} file ('6F3A') under the DF_{TELECOM} folder.</p> <p>USIM card have an additional phonebook with advanced features (e.g. 3 additional phone numbers, second name and e-mail address) other than the standard ADN in SIM cards. The phonebook is stored in its own DF_{PHONEBOOK} folder ('5F3A') with the same AID under the ADF_{USIM} folder.</p>  <p>The screenshot shows a software application with a contact list on the left and a hex dump of the EF6F3A file on the right. The contact list includes entries like 'Chat (SMS)', 'Customer Care', 'Directory Inquiries', 'Flash SMS', 'Friend Finder (SMS)', 'PayTime (SMS)', and 'Voice Mail'. The hex dump shows the raw data of the EF6F3A file, with columns for address, data, and a corresponding text representation of the data.</p>

Figure 80. Extracting the Standard Phonebook.

Figure 81. Comparing Phonebook in SIM vs USIM.

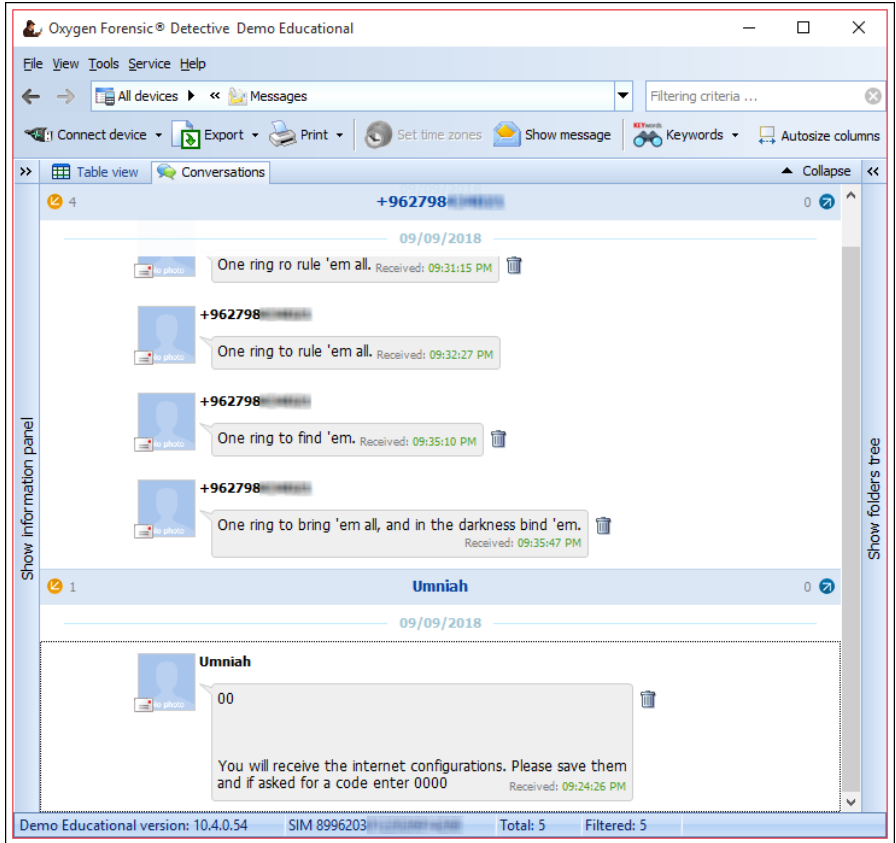
Content Template	
Section Number	5.1.9
Section Title	Messages
Introduction	
Content	<p>The messages (SMSs) are stored in the EF_{SMS} file ('6F3C') under the DF_{TELECOM} folder.</p> <p>Each message has a status byte indicator, which shows whether the message is read, sent, sending, pending (outgoing), or deleted. The deleted messages are marked with '0x00' and might be recovered fully or partially, if not overwritten.</p> <p>Moreover, each message is timestamped with day, month, year, hour, minute, second and time-zone information.</p>  <p>The screenshot shows the Oxygen Forensic Detective software interface. It displays a list of extracted SMS messages from a SIM card. The messages are organized by date (09/09/2018) and contact (+962798). The messages include: <ul style="list-style-type: none"> 'One ring ro rule 'em all. Received: 09:31:15 PM' 'One ring to rule 'em all. Received: 09:32:27 PM' 'One ring to find 'em. Received: 09:35:10 PM' 'One ring to bring 'em all, and in the darkness bind 'em. Received: 09:35:47 PM' One message is expanded to show a status code '00' and a text message: 'You will receive the internet configurations. Please save them and if asked for a code enter 0000'. The status code '00' indicates a deleted or partially recovered message.</p>

Figure 82. Extracting and Analyzing SMS from SIM Card.

The SMS record has slightly different structure depending on whether the message is sent or received. The SMS record structure is defined in the 3GPP TS 03.40 and ETSI TS GSM 03.40 technical specifications and is explained below:

Sent messages are referred to as **SMS-SUBMIT PDU** (Mobile Originated).

Received messages are referred to as **SMS-DELIVER PDU** (Mobile Terminated).

Each record has a fixed length (i.e. 176 bytes), padded with '0xFF' as fillers and all fields are mandatory.

The first byte is the message **Status** indicator and its possible values are:

Hex	Description
00	Free space (might contain deleted SMS).
01	SMS-DELIVER PDU: Read.
03	SMS-DELIVER PDU: Unread.
05	SMS-SUBMIT PDU: Sent, status report is not requested.
07	SMS-SUBMIT PDU: Pending (Not sent yet).
0D	SMS-SUBMIT PDU: Sent, status report is requested but is not received yet.
15	SMS-SUBMIT PDU: Sent, status report is received but is not saved to EF _{SMR} *.
1D	SMS-SUBMIT PDU: Sent, status report is received and is saved to EF _{SMR} *.

* The EF_{SMR} file ('6F4F') is located under the DF_{GSM} folder ('7F10').

The status indicator is followed by the **Service Centre Address (SCA)** information, which is the SMSC. The SCA field has a variable length (1-12 bytes). The SCA is structured as follows:

1 byte	1 byte	0-10 bytes
Length	TON	SMSC

The first byte indicates the length of TON and SMSC fields in bytes (e.g., if Length=07, then length of (TON+SMSC) is 7 bytes).

Possible values for the TON field are '0x91' for International and '0x81' for Unknown format (see section 5.1.5 for explanation).

The SMSC values is stored in BCD encoding, reverse nibbles, padded with '0xFF' format. For example, the correct representation for "69 72 88 99 00 58" is "962-78-8990085".

The SCA field is followed by the **PDU Type** indicator, a 1-byte field with 5 indicators. Explaining each indicator is beyond the scope of this book. However, students are encouraged to read their explanation in extra material #5.9 and #5.10. Common values for the PDU type indicator are '0x04' (SMS delivered) and '0x44' (Multipart SMS delivered).

Following the PDU type indicator is the **Originator Address (TP-OA)** field, which specifies the message's sender phone number. The TP-OA field has a variable length (2-12 bytes) and has a similar format of the SCA. The TP-OA structure is represented as follows:

1 byte	1 byte	0-10 bytes
Length	TON	OA

Thereafter, the **Protocol Identifier (TP-PID)** is a 1-byte field that indicates the PDU protocol type. Common values for the TP-PID are:

- '0x00': Store and Forward message (default).
- '0x24': Voice call.
- '0x26': National Paging System.
- '0x40': Short message – Type 0.
- '0x41-0x47': Replace short message – Type X (X is 1-7).

TP-PID='0x00' is the default protocol ID for SMS.

TP-PID='0x40' also referred to as class 0 or “flash” SMS is often used for sending emergency alerts. When a Type 0 SMS is received, the ME must acknowledge it but may discard its content.

Forensically, this is very important to check for, as the message is only displayed on the device screen and NOT stored on the message store. This type has been known to be used in fraud campaigns and to spread spam messages.

Google Nexus devices running Android v4.4 had a vulnerability that could be exploited via Type 0 SMS, which causes the device to reboot constantly (DoS).

iPhone devices had two similar vulnerability (CVE-2015-1063 and CVE-2018-4140) as well, affecting all iPhones running any iOS before 11.3.



Figure 83. Example of SMS Type 0.

[https://www.iphonejd.com/iphone_jd/2013/07/wireless-emergency-alerts-iphone.html]

TP-PID='0x40-0x47' are used to replace messages that have already been received and possibly read by the user. This type is also important forensically as it may be used by criminals and terrorists in an attempt to mask their conversations.

Following the TP-PID is the **Data Coding Scheme (TP-DCS)** field. It is a 1-byte field that is mainly used to define the encoding schema for the User Data (TP-UD) field. It also defines the:

- Message Class, which determines the intended device to process the message (e.g. ME, UICC, etc.).
- The TP-UD compression indicator.

- The action to be taken after the device is done processing the message (i.e. discard or store).

The message contents can be encoded in one of three types of encoding schemas, which are **GSM 7-bit** encoding, **GSM 8-bit** encoding, and **UCS-2** encoding (16-bit).

When the GSM 7-bit encoding is used, the maximum length of a single message content is 160 characters (GSM 8-bit encoding allows for maximum 140 characters). On the other hand, UCS-2 only supports 70 characters per message.

Common values for the TP-DCS are:

- '0x00': default message class with GSM 7-bit encoding.
- '0x04': default message class with GSM 8-bit encoding.
- '0x08': default message class with UCS-2 encoding.
- '0x10': Type 0 message with GSM 7-bit encoding.
- '0x14': Type 0 message with GSM 8-bit encoding.
- '0x18': Type 0 message with UCS-2 encoding.
- '0x1C': Type 0 message with unspecified encoding.

For more information about the different values of the **TP-DCS** field, refer to ETSI TS 123.038 technical specification.

After the TP-DCS field, the **Service Centre Time Stamp (TP-SCTS)** field is presented. The TP-SCTS is a 7-byte field that defines the time of message delivery from the SMSC to the device. The structure of the TP-SCTS field is as follows:

1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte
YY	MM	DD	HH	MM	SS	TZ

The last 2-digits of the year are stored (e.g. 2018 becomes 18).

All fields are stored in reverse nibbles format.

The **Time Zone (TZ)** field is decoded as follows:

1. Reverse octets order (e.g. '0x21' becomes '0x12').
2. Convert it to binary (e.g. '0x12' becomes '00010010'b).
3. Convert the MSB to time zone offset sign as follows:
 - '0'b: '+'.
 - '1'b: '-'.
4. Split the remaining bits into two nibbles (e.g. '0010010'b becomes '001'b and '0010'b).
5. Convert each nibble into decimal digit (e.g. '001'b becomes '1'd and '0010'b becomes '2'd).
6. Concatenate the two decimal digits (e.g. '1'd and '2'd become '12'd).
7. Multiply the result by 0.25 (e.g. $12 * 0.25 = 3$).
8. The **TZ** offset is **GMT+3**.

	<p>Example: TP-SCTS field is "70 10 90 90 24 00 8A", and the correct timestamp is "09/01/2007 09:42:00 GMT-7".</p> <p>Following is the User Data Length (TP-UDL), a 1-byte field, which defines the length of the TP-UD field (i.e. message contents).</p> <p>To calculate the length of the user data when the TP-DCS is set to GSM 7-bit encoding, the following is performed:</p> <ol style="list-style-type: none"> 1. Convert the TP-UDL value from hexadecimal to decimal (e.g. '0x15' becomes '21'd). 2. Divide the result by 8 (e.g. $21 / 8 = 2.625$). 3. Multiply the result by 7 (e.g. $2.625 * 7 = 18.375$). 4. Round up the result (e.g. 18.375 becomes 19). 5. The length of the UD is 19 bytes. <p>For GSM 8-bit and UCS-2 encodings, the TP-UDL value indicates the length of the user data directly in bytes.</p> <p>Finally, the User Data (TP-UD) field is presented, which holds the contents of the message. For messages where the TP-DCS is set to GSM 7-bit encoding, the TP-UD has to be decoded back to 8-bit/16-bit coding to be readable. A good online tool is available at (smstools3.kekekasvi.com/topic.php?id=288).</p> <p>One thing we have noticed when using Oxygen Forensics® Detective to extract and analyse SMSs stored on SIM card is that the read status indicator and the deleted message indicator are both inaccurate <i>in some cases</i>.</p> <p>As shown in Figure 19, the highlighted message is indicated by Oxygen Forensics® Detective as read and deleted. However, when examining the Message Status Indicator (first byte) it shows that its values is '0x03', which translates to an Unread SMS-DELIVER PDU. This is also true for the fourth and fifth messages (counting from the bottom to top).</p> <p>Moreover, the second message is shown as deleted and read, when in fact it was deleted without reading it. The status "deleted" is correct in this case, but the "read" status is not as shown in Figure 20. Nonetheless, this is NOT a problem of the tool, as it is impossible from parsing the EF_{SMS} file only to determine whether a deleted message was read prior its deletion or not.</p> <p>The third message was correctly parsed, both status indicators were correct.</p> <p>This goes to show that manually analysis is an integral part of any forensic analysis task, even if market-leading tools were utilized in the investigation.</p>
--	--

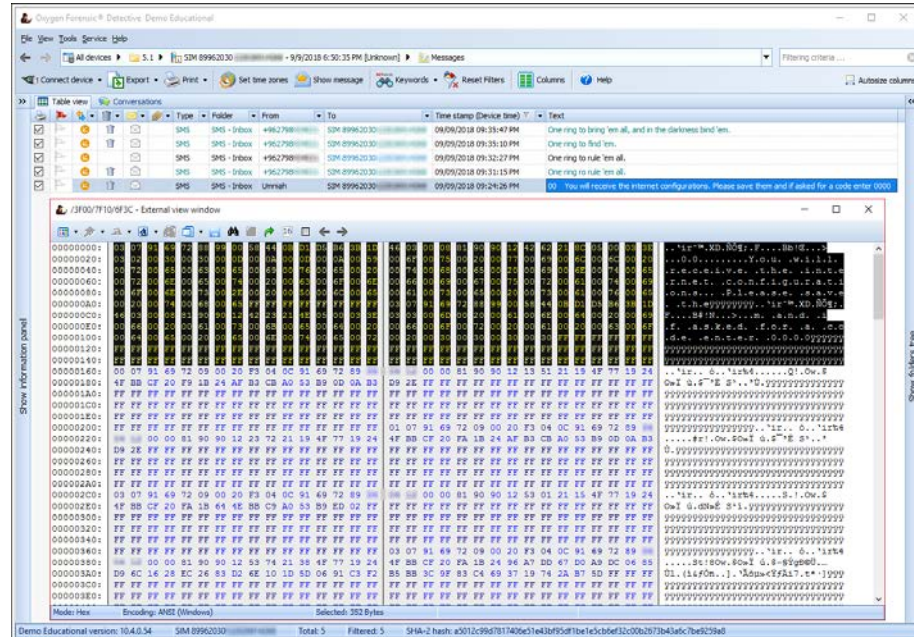


Figure 84. Manually Examining SMS (1).

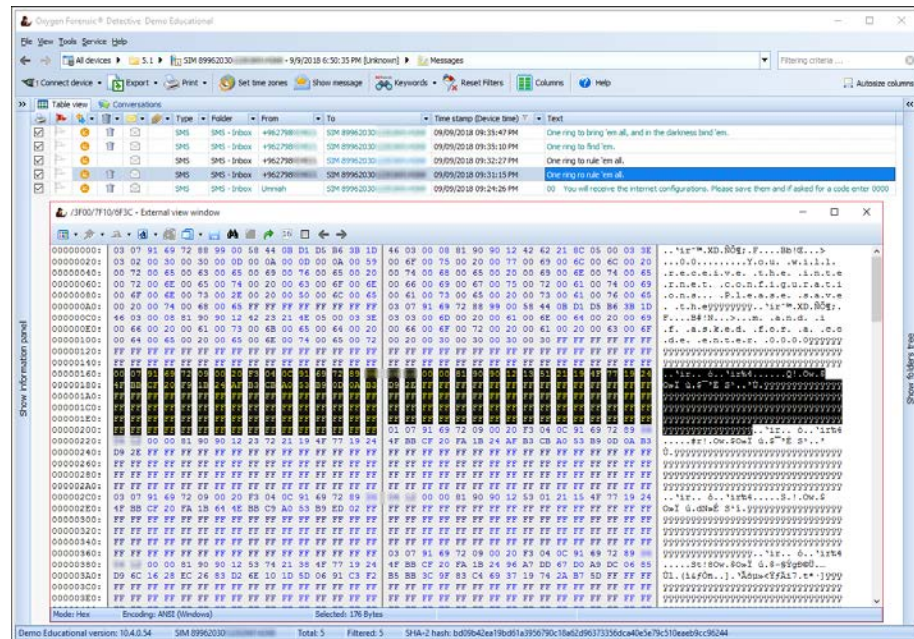


Figure 85. Manually Examining SMS (2).

Content Template	
Section Number	5.2
Section Title	U/SIM Card Cloning
Introduction	<p>This section explains the concept of SIM card Cloning and elaborate on its benefits.</p> <p>Upon the completion of this section, the student is expected to have a clear understanding about SIM card cloning, its benefits and usage.</p>
Content	<p>SIM card cloning is the process of creating a duplicate SIM card to be used in the forensic investigation. It might be a full clone or partial clone depending on the software and the card used. In Cellebrite UFED and many other forensic tools, only the ICCID and the IMSI of the evidentiary SIM card are copied to the cloned card (<i>called SIM Access ID card</i>). The other data will NOT be cloned.</p> <p>The cloned SIM card cannot be used to register a device on the network because the subscriber authentication key (Ki) is not copied as part of the cloning process. Therefore, it is considered is a network-isolated card.</p> <p>Cloning the SIM card is a highly recommend practice that has many benefits:</p> <ul style="list-style-type: none"> • In cases where the evidentiary SIM card is not available or it has been damaged, a cloned card can be created manually if IMSI and ICCID are known. • If the evidentiary SIM card is protected by an unknown PIN code and it is not possible to get the PUK code, then a cloned SIM card can be used to bypass the PIN code protection and access the device. • Because a cloned SIM card is a network-isolated card, it can be used to shield the device from the network thus preventing intentional and unintentional changes to the device from the network. <p>Students are encouraged to perform activity #5.2 if their lab equipment include SIM cloners.</p>

Content Template	
Section Number	5.3
Section Title	U/SIM Card Forensic Tools
Introduction	<p>This section presents some of the well-known tools and software used to extract forensic artefacts from SIM cards.</p> <p>Upon the completion of this section, the student is expected be able to cite the name and main features of the popular SIM card forensic tools.</p>
Content	<p>Oxygen introduced in 2017 a new SIM card data extraction and analysis module to its mobile forensic solution. The new module in the Oxygen Forensic® Extractor tool allows the investigator to extract data from SIM cards using SIM cards readers, acquire/import an image of the SIM card then analyse it via Oxygen Forensic® Detective software. The acquisition tools allows the investigator to use watch lists to search for words associated with crimes such as drugs, money laundry, and child pornography. It is also possible to search for deleted files and do a full acquisition of all the system and data files on the SIM card, which is a time consuming task.</p> <p>Figure 86. Oxygen Forensic® Extractor – UICC Acquisition.</p> <p>Once the SIM card acquisition is done, the image is saved (by default) to folder with the case name and date-time timestamp at "%APPDATA%\oxyForensic\" with ".ofsi" extension.</p> <p>The image can be imported and examined by Oxygen Forensic® Detective software. It has a very comprehensive data analysis and reporting capabilities.</p>



The screenshot shows the Oxygen Forensic Detective Demo Educational version interface. The main window displays the analysis of a Samsung SM-N960U device. The interface is divided into several sections:

- Common information:**
 - Model: SM-N960U/XXU1T1/USQ241218
 - Internal name: UOCC
 - Platform: GSM
 - IMEI: N/A
 - Location information: MCC: Jordan (410), MNC: JMSA (02), LA: 1199, TAG: 11999999, TAC: 11999999, TAC: 11999999
 - IMEI: F46B6 (02), IMEI (02)
 - IMEI: 410021120241218
 - IMEI: 899620120241218
- Device extended information:**
 - Device image: 410021120241218.img
- Extraction information:**
 - Extracted by version: 10.4.0.14
 - Extraction started: 5/6/2018 1:40:12 AM
 - Extraction finished: 5/6/2018 1:40:12 AM
 - Extraction duration: 00:01:31
 - Hash algorithm: SHA-2
- Case attributes:**
 - Inspector: None
 - Case: None
 - Evidence number: None
 - Associated incident number: None
 - Place: None
- Device owner information:**
 - Owner: None
 - Mobile phone: None
 - Email: None
 - Mobile phone: (Enter mobile number, e.g. 0000110123)

The bottom status bar indicates the demo version is 10.4.0.14, the device is SM-N960U/XXU1T1/USQ241218, and the extraction time is 5/6/2018 1:40:12 AM.

Figure 88. Oxygen Forensic[®] Detective – SIM Card Info.

The “File Browser” section allows you to explore the SIM card file system as if you were browsing files and folders on Windows OS. The EFs and DFs are named after their Application Identifiers (AIDs), a two bytes hexadecimal number that uniquely identifies the file. EFs can be viewed via the built-in hexadecimal viewer.

Figure 24 shows the EF storing the ICCID (AID=2FE2) which is located directly under the MF (AID=3F00). The ICCID is stored in hexadecimal format with reverse nibble order (e.g. 89 is stored as 98). In our case, the ICCID "89962030721105241335" is stored as "98 69 02 03 27 11 50 42 31 53".

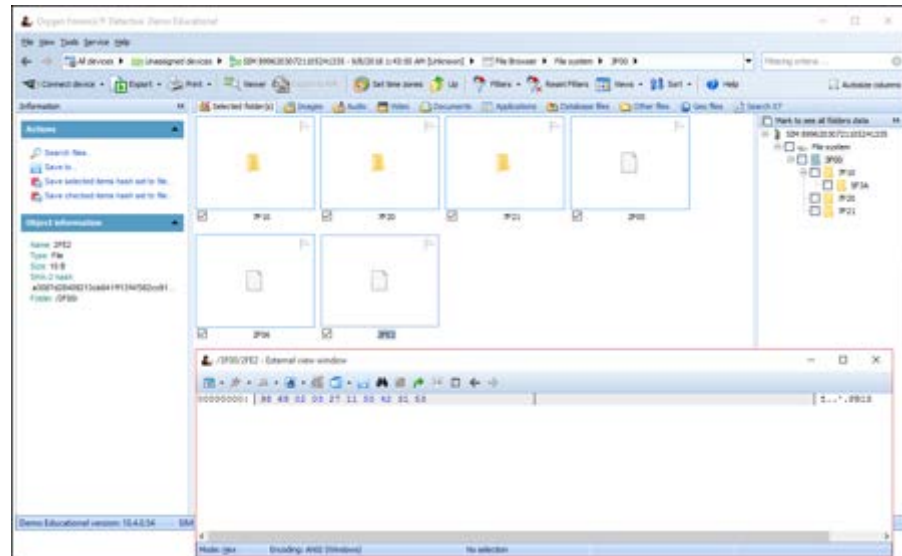


Figure 89. Oxygen Forensic® Detective – SIM Image File Explorer.

Crownhill Associates Ltd is a UK company specialized in telecommunications forensics and provides a wide range of tools to facilitate SIM forensics (www.crownhillmobile.com). **SIMIS 3G** is a SIM card interrogation tool from Crownhill that allows the investigator to:

- Get read-only access to SIM data.
- Dump SIM content in raw data format.
- Store SIM data in searchable database.
- Generate comprehensive HTML reports (see a sample report at www.crownhillmobile.com/sample-report).



Figure 90. SIMIS Mobile Reader from Crownhill.
[<http://www.crownhillmobile.com>]

Dekart SIM Explorer (www.dekart.com) has great capabilities that can be very helpful when working with SIM cards such as side-by-side SIM card comparison, read-only access to SIM data, live and offline SIM card analysis.

Dekart SIM Manager can be used to backup, copy and write SIM card data such as contacts, messages, ADN, LDN, FDN, SDN and more. It can also manage PIN/PUK codes and view basic information such as ICCID, IMSI, SPN, etc.

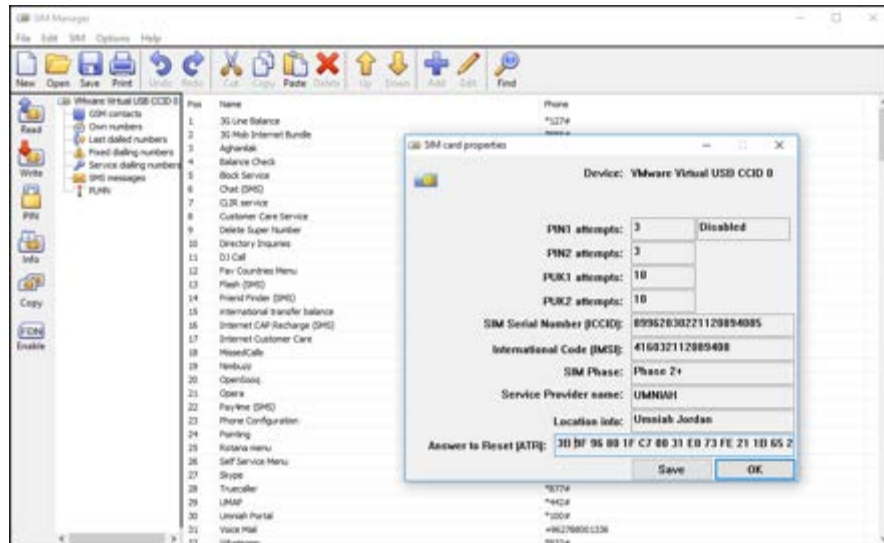


Figure 91. Dekart SIM Manager.

MOBILedit SIM Clone tool (www.mobiledit.com) by Compelson Labs is a forensic tool that creates network-isolated SIM cards. It can set the cloned card ICCID and IMSI values to arbitrary values as well as copying the phonebook, messages and other data from the evidentiary SIM card to the cloned one.

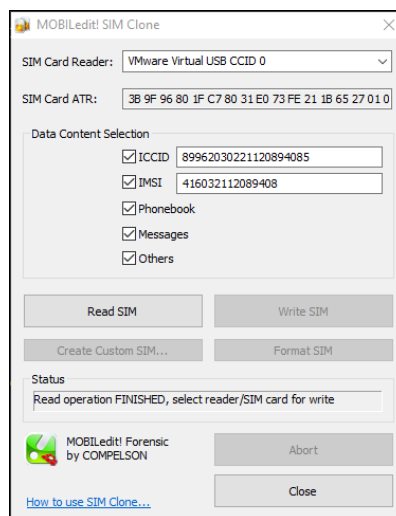


Figure 92. MOBILedit SIM Clone.

PISWORDS is a Chinese company specialized in manufacturing blank smart cards including RFID/NFC cards, JCop smart cards which are often used in banking sector (credit/debit cards), as well as SIM cards. They manufacture blank writable and programmable USIM cards that can be used to create workable cloned SIM cards that can register to the network. Information such as ICCID, IMSI, CHV1/2, ADM, Ki, OP/OPc and more can be written to the blank SIM card.



Figure 93. Generic EMV Smart Card Reader/Writer and Blank LET USIM Cards.

PISWORDS SIM Card Tool can be used to read and write data to the SIM card. Any EMV smart card reader that is compatible with ISO7816 can be used.

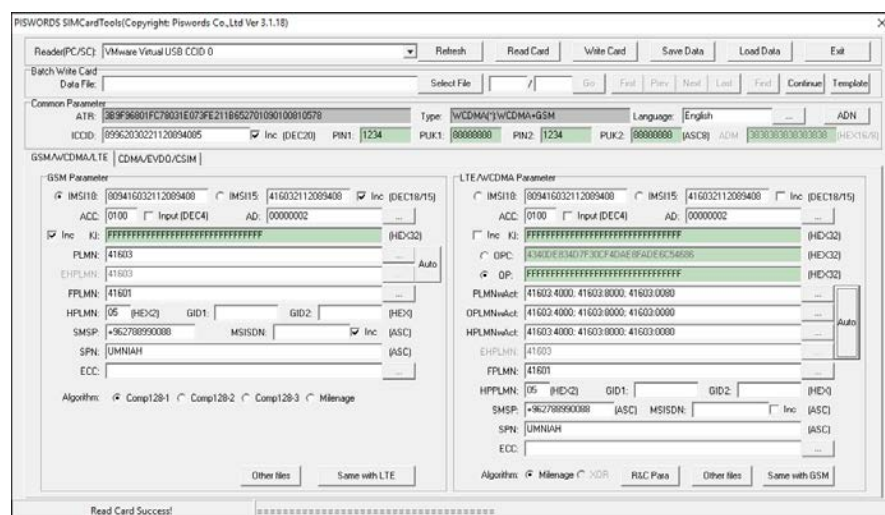


Figure 94. PISWORDS SIM Card Tool.

Although it is not a forensic software, **Sim-Emu** is a great software to read and write data to and from SIM cards. However, it only supports 3 types: Green/Green2 cards and Silver cards. It also provides the ability to read from and write to the EEPROM directly. Nonetheless, the software is NOT maintained by a known entity and many of the versions available online are in fact infected with trojan horses and malware. Ask your lab supervisor to provide you with a "clean" copy if needed.

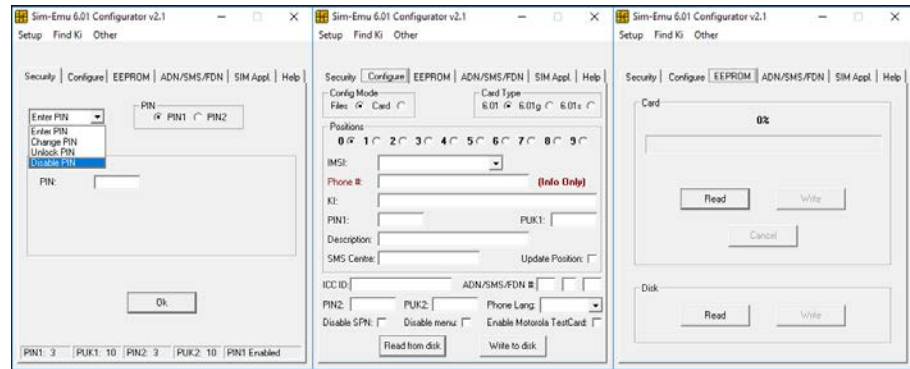


Figure 95. Sim-Emu Software.

Another good tool is **Woron Scan**, which can brute force the subscriber authentication key (Ki) value. The tool utilizes a vulnerability in the COMP128-1 algorithm (hash function with poor entropy). However, most telecommunication service providers stopped using it long time ago and most cards manufactured after 2002 are most likely use one of its successors COMP128-2/3, or MILENAGE algorithms (most recent and most likely to be used in USIM cards). Ask your lab supervisor for a “clean” copy if you need it.

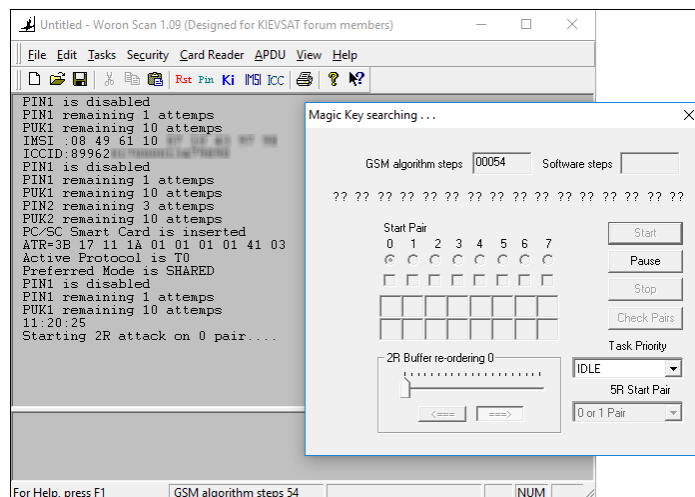


Figure 96. Woron Scan Tool.

Smart Card Toolset Pro from SCard Soft (www.scardsoft.com) is an advanced tool that allows you to communicate with compatible smart cards via APDU commands (see section 5.5). The tool is not intended for digital forensics usage and can be a bit advanced to work with. However, it will give you tremendous capabilities over the other tools.

pcsc_scan is a Linux program developed by Ludovic Rousseau that scans all connected PC/SC readers and outputs information about the card inserted in the reader. It also performs Answer To Request (ATR) analysis to identify the card manufacturer information. ATR parsing and analysis can be performed manually at (smartcard-atr.appspot.com).


```

root@kali:~/pysim# pcsc_scan
Using reader plug'n play mechanism
Scanning present readers...
0: VMware Virtual USB CCID 00 00

Fri Sep  7 22:18:58 2018
Reader 0: VMware Virtual USB CCID 00 00
Card state: Card inserted.
ATR: 3B 9F 95 80 1F C3 80 31 E0 73 FE 21 13 57 86 81 02 86 98 44 18 A8

ATR: 3B 9F 95 80 1F C3 80 31 E0 73 FE 21 13 57 86 81 02 86 98 44 18 A8
+ TS = 3B --> Direct Convention
+ T0 = 9F, Y(1): 1001, K: 15 (historical bytes)
TA(1) = 95 --> Fi=512, Di=16, 32 cycles/ETU
125000 bits/s at 4 MHz, (Max for Fi = 5 MHz => 156250 bits/s)
TD(1) = 80 --> Y(i+1) = 1000, Protocol T = 0
-----
TD(2) = 1F --> Y(i+1) = 0001, Protocol T = 15 - Global interface bytes following
-----
TA(3) = C3 --> Clock stop: no preference - Class accepted by the card: (30) A 5V B 3V
+ Historical bytes: 80 31 E0 73 FE 21 13 57 86 81 02 86 98 44 18
Category indicator byte: 80 (compact TLV data object)
Tag: 3, len: 1 (card service data byte)
Card service data byte: E0
- Application selection: by full DF name
- Application selection: by partial DF name
- BER-TLV data objects available in EF.DIR
- EF.DIR and EF.ATR access services: by GET RECORD(s) command
- Card with MF
Tag: 7, len: 3 (card capabilities)
Selection methods: FE
- DF selection by full DF name
- DF selection by partial DF name
- DF selection by path
- DF selection by file identifier
- Implicit DF selection
- Short EF identifier supported
- Record number supported
Data coding byte: 21
- Behaviour of write functions: proprietary
- Value 'FF' for the first byte of BER-TLV tag fields: invalid
- Data unit in quartets: 2
Command chaining, length fields and logical channels: 13
- Logical channel number assignment: by the card
- Maximum number of logical channels: 4
Tag: 5, len: 7 (card issuer's data)
Card issuer data: 86 81 02 86 98 44 18
+ TCK = A8 (correct checksum)

Possibly identified card (using /root/.cache/smartcard_list.txt):
NONE

```

Figure 97. pcsc_scan Linux Program.

pySim (osmocom.org/projects/pysim) is a Python command line tool that can read basic SIM card information and write data to it including but not limited to ICCID, IMSI, Ki and OP/OPc. At the time of writing, the tool can support writing to 10 types of SIM card (Fairwaves SIM, fakemagicsim, grcardsim, magicsim, OpenCells SIM, supersim, sysmosim-gr1, sysmoSIM-GR2, sysmoUSIM-GR1, and sysmoUSIM-SJS1).

```

root@kali:~/pysim# ./pySim-read.py -p 0
Reading ...
ICCID: 8996277010409071160
IMSI: 416770107727727
SMSP: 4d6573736167652043656e747265fdffffffffffffffffffffffff07916972070061f1fffffffff
PLMNsel: 02f81062f03002f40214f51032f11032f80322f60106f21062f83022f28824f55014f72032f
ffffffffffffffffffffffffffffffffffffffffffffffff
PLMNwAcT: Can't read file -- SW match failed! Expected 9000 and got 9404.
OPLMNwAcT: Can't read file -- SW match failed! Expected 9000 and got 9404.
HPLMNwAcT: Can't read file -- SW match failed! Expected 9000 and got 9404.
ACC: 0000
MSISDN: Not available
Done !

```

Figure 98. pySim Reading SIM Card Basic Data.


```

root@kali:~/pysim# ./pySim-prog.py -p 0 --type="OpenCells SIM" --name="UMNIAH"
--country=962 --mcc=416 --mnc=03 --smc=00962788990088 --iccid=8996203072110524
1335 --imsi=809416032112089408 --k1=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF --op=FFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF --pin-adm=3838383838383838 --dry-run
Generated card parameters :
> Name      : UMNIAH
> SMSP      : e1ffffffffffffffffffffffff088100697288990088ffffff000000
> ICCID     : 89962030721105241335
> MCC/MNC   : 416/3
> IMSI      : 809416032112089408
> K1        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
> OPC       : 4340de834d7f30cf4dae8fade6c54686
> ACC       : None

Dry Run: NOT PROGRAMMING!
Done !

```

Figure 99. pySim Writing SIM Card Basic Data.

An interesting comparison between the capabilities of the most common SIM card forensic tools is presented at the Annual ADFSL Conference on Digital Forensics, Security and Law. Students are encouraged to read the article from extra material #5.1.

Content Template	
Section Number	5.4
Section Title	Bypassing U/SIM Card Security Controls
Introduction	<p>In this section, some of the techniques to bypass the security controls implement in U/SIM cards are explored.</p> <p>Upon the completion of this section, the student is expected to have clear understanding of the options available to bypass the security controls of U/SIM cards.</p>
Content	<p>U/SIM cards employ multiple levels of security to prevent unauthorized accesses or changes to the card (refer to section 1.3.3 for more details).</p> <p>This presents a challenge for digital forensic investigators tasked to extract data from locked SIM card (most files are protected by PIN1).</p> <p>The first challenge is that, unlike traditional passwords, brute-forcing PIN1/PIN2 is NOT really possible. If PUK1/PUK2 is known to the investigator, then the corresponding PIN can be changed first then disabled second, thus getting access to the files protected by that particular PIN (e.g. read access to EF_{IMSI} is protected by PIN1).</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>EF_{ICCID} has ALWAYS read access, meaning that is can be read even if PIN1 is enabled and even if the SIM card was locked.</p> </div> <p>For this to work, the SIM card packaging must be seized as the PUK and PIN values are usually printed on the packaging. Otherwise, the PUK values can be requested from the carrier, but it is not always guaranteed as carriers have different polices limits the time to store such information.</p> <p>If all the previous strategies failed, you may resort to guessing the PIN code. However, you have to keep in your mind that if this also failed, then the SIM card might be locked permanently.</p> <p>The most common and usually default value for PIN1 is either "0000" or "1234", whilst the default value for PUK1 is "88888888".</p> <p>Since PIN1 will be blocked after 3 failed tries, it is recommended to first check the number of tries left. If it is 3, then try to unlock PIN1 with "0000" and "1234".</p> <p>If both attempts failed, it is recommended to stop guessing immediately, and use a tool like Cellebrite UFED to make a basic clone of the SIM card, thus preserving the evidentiary SIM card in the evidence locker.</p> <p>In this way, if later on PIN1 was somehow found, you will still have 1 try left to access the SIM data.</p> <p>Older phones require a SIM card to be present in order to work, a cloned SIM card can be used to bypass a SIM locked phone.</p>

Content Template																					
Section Number	5.5																				
Section Title	APDU Commands																				
Introduction	<p>In this section, the Application Protocol Data Unit commands are explained as the method of communicating with smart cards including U/SIM cards.</p> <p>Upon the completion of this section, the student is expected to have a general understanding of how the smart card reader and the smart card communicates with each other.</p>																				
Content	<p>Smart cards communicate with readers in accordance with standardized protocols defined by several ISO standards (i.e. ISO/IEC 7816 standards).</p> <p>When a contact smart card is inserted in a smart card reader, the card is powered and a reset signal is sent to the card.</p> <p>Thereafter, the card responds to the reset signal with an Answer To Reset (ATR) message. The ATR message is a series of bytes that convey information about the card such as type, manufacturer, speed, capabilities, clock frequency, etc.</p> <p>The reader parses the ATR message and uses the information provided in order to synchronize its clock with the card’s clock and setup other parameter such as preferred voltage and speed, thus allowing further communications between the two devices.</p> <p>The subsequent communication between the card and the reader is performed via a series of Application Protocol Data Unit (APDU) commands and responses. The APDU structure is defined by the ISO/IEC 7816-4 standard. The exact APDU commands and responses are dependent on the smart card.</p> <p>The structure of the APDU command is as follows:</p> <table><tr><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>1 byte</td><td>0-3 bytes</td><td>0-X bytes</td><td>0-3 bytes</td></tr><tr><td>CLA</td><td>INS</td><td>P1</td><td>P2</td><td>Lc</td><td>DATA_{IN}</td><td>Le</td></tr></table> <ul style="list-style-type: none">• CLA: Class of instruction, which indicates the type of command. For GSM, the CLA is always '0xA0'• INS: Instruction code, which indicates the specific command performed (e.g. write, read, update, etc.).• P1/P2: Instruction Parameter.• Lc: Length of DATA.• DATA_{IN}: Instruction Data to be sent to the card.• Le: Length of expected APDU response. <p>The structure of the APDU response is much simpler:</p> <table><tr><td>1 byte</td><td>1 byte</td><td>0-X bytes</td></tr><tr><td>SW1</td><td>SW1</td><td>DATA_{OUT}</td></tr></table>	1 byte	1 byte	1 byte	1 byte	0-3 bytes	0-X bytes	0-3 bytes	CLA	INS	P1	P2	Lc	DATA _{IN}	Le	1 byte	1 byte	0-X bytes	SW1	SW1	DATA _{OUT}
1 byte	1 byte	1 byte	1 byte	0-3 bytes	0-X bytes	0-3 bytes															
CLA	INS	P1	P2	Lc	DATA _{IN}	Le															
1 byte	1 byte	0-X bytes																			
SW1	SW1	DATA _{OUT}																			

- **SW1/SW2:** Status Word, which indicates the APDU command processing status (e.g. OK, Error, etc.).
- **DATA_{out}:** APDU Response Data.

Each smart card implements its own set of commands and instructions. For SIM cards, the list of common APDU commands is listed below, and for the full list refer to the website (www.decodesystems.com/smartcards.html):

COMMAND	CLS	INS	P1	P2	Lc (HEX)	DATA
CHANGE CHV	A0	24	00	01 CHV1 02 CHV2	10	CHV NEW_CHV
DISABLE CHV	A0	26	00	01 CHV1 02 CHV2	08	CHV
ENABLE CHV	A0	28	00	01 CHV1 02 CHV2	08	CHV
GET RESPONSE	A0	C0	00	00	length	-
READ BINARY	A0	B0	Offset (high)	offset (low)	length	-
SELECT	A0	A4	00	00	02	AID
UNBLOCK CHV	A0	2C	00	00 CHV1 02 CHV2	10	PUK NEW_CHV
VERIFY CHV	A0	20	00	01 CHV1 02 CHV2	08	CHV

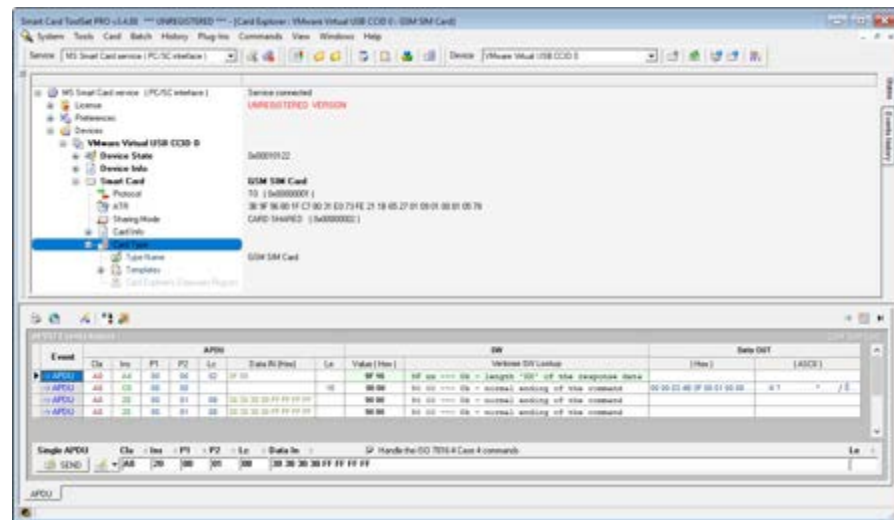


Figure 100. Example of APDU Commands.

In Figure 35, an example of APDU commands and their responses is shown.

The first APDU command "A0 A4 00 00 02 3F 00 -" is a SELECT command and it requests the MF folder '3F00'. The value of SW1/2 "9F 16" indicates that the APDU command was executed successfully and 16 bytes can be requested.

The second APDU command "A0 C0 00 00 - - 16" is a GET RESPONSE command and it requests the first 16 bytes of the MF folder '3F00'. The value of SW1/2 "90 00" indicates that the command was executed successfully.

	<p>The third APDU command "A0 28 00 01 08 30 30 30 30 30 FF FF FF FF -" is an ENABLE CHV command and it tries to enable PIN1, which requires the PIN1 value "0000" to be executed. The value of SW1/2 "90 00" indicates that the command was executed successfully. Therefore, PIN1 was enabled.</p> <p>The last APDU command "A0 20 00 01 08 30 30 30 30 30 FF FF FF FF -" is a VERIFY CHV command and it attempts to verify that PIN1="0000". The value of SW1/2 "90 00" indicates that the command was executed successfully. Therefore, the PIN1 value is correct.</p> <p>For the complete list of APDU response values and their description, see extra material #5.12.</p>
--	--

Activity Template	
Number	5.1
Title	<p>Identify 3 different artefacts of SIM cards that were not mentioned in the textbook and write a brief report describing their:</p> <ol style="list-style-type: none"> 1. Location (DF\EF, AID). 2. Structure. 3. Extracting and Parsing techniques.
Type	Research
Aim	<p>ILOs: 1</p> <p>The activity aims to let the student explore more forensic artefacts than what has been taught in the textbook.</p>
Description	5.1
Timeline	1-3 hours
Assessment	<p>Each student is required to submit a three pages (minimum) report.</p> <p>The report will be assessed based on completeness, correctness and overall quality.</p>

Activity Template	
Number	5.2
Title	Perform SIM card cloning using one of the mobile forensics tools available at your University's Lab. In case more than one tool is available, then use 2-3 tools and compare their results and features. Document the steps taken to produce the cloned SIM card and the findings in a detailed technical report (use snapshots of your work).
Type	Reflection
Aim	ILOs: 2, 7 The activity aims to allow the student to experiment with different forensics tools and learn how to perform SIM cloning practically in a forensically sound manner.
Description	5.2
Timeline	3 hours
Assessment	Each student is required to submit a report, which details the process taken to produce the cloned SIM card. The report will be assessed based on completeness, correctness, overall quality and soundness of the process followed.

Activity Template	
Number	5.3
Title	Perform data extraction and analysis from a SIM card using one of the Mobile forensics tools available at your University's Lab. Work in a group of 2-3 students to produce a complete and comprehensive forensic report. Present your findings in 10 minutes slot.
Type	Reflection
Aim	ILOs: 2, 3, 4, 5, 6, 7 The activity aims to develop the student's ability to work effectively within a team to perform SIM forensic analysis and reporting practically in a forensically sound manner.
Description	5.1, 5.3
Timeline	3-6 hours
Assessment	Each group is required to submit a comprehensive forensic report detailing the process, techniques, tools and findings. The report will be assessed based on completeness, correctness, overall quality, soundness of the process followed, team work efforts and presentation.

Activity Template	
Number	5.4
Title	Use APDU commands to extract the ICCID, IMSI and MSISDN from a locked SIM card. Validate your findings using any forensic tool available at your University's Lab. Submit a one-page (maximum) report including only the APDU commands used and a single screenshot showing the findings.
Type	Reflection
Aim	ILOs:2, 3, 4, 7 The activity aims to allow the student to understand how forensic tools works at a basic level and learn how to perform manual data extraction.
Description	5.5
Timeline	2-3 hours
Assessment	Each student is required to submit a one-page report. The report will be assessed based on completeness, correctness, overall quality.

Activity Template	
Number	5.5
Title	Devise an experiment to determine what kind of forensic artefacts does Type-0 SMS leaves on the receiving device (if any). Present your finding in a research paper format.
Type	Reflection, Research
Aim	ILOs: 1, 2, 3, 4 The activity aims to build the student's ability to conduct research and development in order to find solution for new problems.
Description	5.1.9
Timeline	9-15 hour
Assessment	The student is assessed based on the scientific quality of the produced research paper. This is an advanced activity and it is not expected that many students will attempt.

Think Template (MCQs)	
Number	5.1
Title	U/SIM Card Artefacts Extraction
Type	Match pairs
Question	<p>Match the SIM card type to their mobile technology:</p> <p>g) CSIM</p> <p>h) USIM</p> <p>i) R-UIM</p> <p>j) SIM</p> <p>k) iDEN SIM</p>
Answers	<p>v. CDMA2000</p> <p>vi. CDMA</p> <p>vii. WiDEN</p> <p>viii. GSM</p> <p>ix. UMTS</p> <p>Answer:</p> <p>a >>> i</p> <p>b >>> v</p> <p>c >>> ii</p> <p>d >>> iv</p> <p>e >>> iii</p>

Think Template (MCQs)	
Number	5.2
Title	U/SIM Card Artefacts Extraction
Type	Rank options
Question	<p>Put the following steps in the correct order in accordance to the current best practice for extracting data from SIM card in forensically sound manner.</p> <ul style="list-style-type: none"> f. Extract data from the device g. Reserve the evidentiary SIM card in the evidence locker h. Extract data from the evidentiary SIM card i. Remove the evidentiary SIM card from the device j. Place the cloned SIM card in the device k. Create a clone (network-isolated) SIM card
Answers	<p>Answer:</p> <ul style="list-style-type: none"> 12. Remove the evidentiary SIM card from the device 13. Create a clone (network-isolated) SIM card 14. Place the cloned SIM card in the device 15. Extract data from the evidentiary SIM card 16. Reserve the evidentiary SIM card in the evidence locker 17. Extract data from the device





Think Template (MCQs)	
Number	5.3
Title	Integrated Circuit Card Identifier (ICCID)
Type	Choose correct answer
Question	Major Industry Identifier (MII) is a two digits prefix defined by the ISO/IEC 7812-1 standard. It is value for telecommunication companies:
Answers	<p>j. 91 (hexadecimal)</p> <p>k. 91 (decimal)</p> <p>l. 89 (decimal)</p> <p>m. 89 (hexadecimal)</p> <p>n. 81 (hexadecimal)</p> <p>o. 81 (decimal)</p> <p>Answer: D</p>

Think Template (MCQs)	
Number	5.4
Title	Fixed Dialling Numbers (FDN)
Type	Choose correct answer
Question	The correct representation of the following Fixed Dialling Number (FDN) "69 62 85 04 03 0F" is:
Answers	<p>a. "962-6-5840300"</p> <p>b. "00962-6-5840300"</p> <p>c. "+69-6-2850403"</p> <p>d. "69-6-28504030"</p> <p>Answer: A</p>

Think Template (MCQs)	
Number	5.5
Title	Phonebook
Type	Fill in the blanks
Question	<p>The standard address book is available in the EF_{ADN} file, which AID is _____ and is located under the _____ folder.</p> <p>USIM card have an additional phonebook and is stored in DF_{PHONEBOOK} folder with AID _____.</p>
Answers	<p>a. '6F3C', DF_{GSM}, '6F3A'</p> <p>b. '6F3A', DF_{TELECOM}, '5F3A'</p> <p>c. '6F3A', MF, '5F3A'</p> <p>d. '6F3A', DF_{GSM}, '6F3C '</p> <p>Answer: B</p>

Think Template (MCQs)	
Number	5.6
Title	Messages
Type	Choose correct answer
Question	Deleted messages can be identified by Message Status Indicator.
Answers	<p>a. '0x00'</p> <p>b. '0x03'</p> <p>c. '0x01'</p> <p>d. None</p> <p>Answer: A</p>

Think Template (MCQs)	
Number	5.7
Title	U/SIM Card Cloning
Type	Fill in the blanks
Question	In Cellebrite UFED, only the _____ and the _____ of the evidentiary SIM card are copied to the SIM Access ID card.
Answers	<p>a. ICCID</p> <p>b. IMSI</p> <p>c. Ki</p> <p>d. MSISDN</p> <p>Answer: A, B</p>

Think Template (MCQs)	
Number	5.8
Title	U/SIM Card Forensic Tools
Type	Match pairs
Question	<p>Match the tool image with its name:</p> <div style="display: flex; flex-wrap: wrap; justify-content: space-around;"> <div style="text-align: center;">  <p>(a)</p> </div> <div style="text-align: center;">  <p>(b)</p> </div> <div style="text-align: center;">  <p>(c)</p> </div> <div style="text-align: center;">  <p>(d)</p> </div> </div>
Answers	<p>i. Cellebrite UFED Touch ii. Oxygen Forensic® Extractor iii. Oxygen Forensic® Detective iv. Crownhill SIMIS Mobile Reader v. MOBILedit SIM Clone vi. Dekart SIM Manager</p> <p>Answer:</p> <p>a >>> iii b >>> iv c >>> v d >>> i</p>

Think Template (MCQs)	
Number	5.9
Title	Bypassing U/SIM Card Security Controls
Type	Choose correct answer
Question	The value of IMSI can ALWAYS be read from the EF _{IMSI} file even if the SIM card is locked.
Answers	<p>c. True</p> <p>d. False</p> <p>Answer: B</p>

Think Template (MCQs)	
Number	5.10
Title	APDU Commands
Type	Choose correct answer
Question	The correct APDU command to verify PIN2="607080" is:
Answers	<p>a. "A0 20 00 01 04 60 70 80"</p> <p>b. "A0 28 00 02 08 60 70 80 FF FF FF FF FF"</p> <p>c. "A0 20 00 02 08 36 30 37 30 38 30 FF FF"</p> <p>d. "A0 28 00 01 04 60 70 80"</p> <p>e. "A0 20 00 02 08 60 70 80 FF FF FF FF FF"</p> <p>f. "A0 20 00 02 08 36 30 37 30 38 30"</p> <p>Answer: C</p>

Extra Template	
Number	5.1
Title	SIM Card Forensics: Digital Evidence.
Topic	<ul style="list-style-type: none"> • 5.1 • 5.3
Type	<p>Ibrahim, Nada; Al Naqbi, Nuha; Iqbal, Farkhund; and AlFandi, Omar, "SIM Card Forensics: Digital Evidence" (2016). <i>Annual ADFSL Conference on Digital Forensics, Security and Law</i>. 3. https://commons.erau.edu/adfsl/2016/thursday/3</p>

Extra Template	
Number	5.2
Title	Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011 version 4.15.0 Release 4).
Topic	5.1
Type	URL: https://www.etsi.org/deliver/etsi_ts/151000_151099/151011/04.15.00_60/ts_151011v041500p.pdf

Extra Template	
Number	5.3
Title	Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 10.14.1 Release 10).
Topic	5.1
Type	URL: https://www.etsi.org/deliver/etsi_ts/131100_131199/131102/10.14.01_60/ts_131102v101401p.pdf

Extra Template	
Number	5.4
Title	ITU-T Recommendation E.118; Overall network operation, telephone service, service operation and human factors; International operation – General provisions concerning administrations; The international telecommunication charge card.
Topic	5.1.1
Type	URL: <ul style="list-style-type: none"> • www.itu.int/en/ITU-T/inr/forms/Pages/iin.aspx • https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.118-200605-I!!PDF-E&type=items

Extra Template	
Number	5.5
Title	HUAWEI ME909s Series LTE Module; V100R001; AT Command Interface Specification
Topic	5.1
Type	URL: http://download-c.huawei.com/download/downloadCenter?downloadId=50263&version=119077

Extra Template	
Number	5.6
Title	ETSI GSM Technical Specification 11.11; Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11).
Topic	5.1.1
Type	URL: https://www.etsi.org/deliver/etsi_gts/11/1111/05.01.00_60/gsm11.11v050100p.pdf

Extra Template	
Number	5.7
Title	GSM Equipment Related Errors
Topic	5.1
Type	URL: https://www.micromedia-int.com/en/gsm-2/73-gsm/669-cme-error-gsm-equipment-related-errors

Extra Template	
Number	5.8
Title	ITU-T Recommendation E.212; Overall network operation, telephone service, service operation and human factors; International operation – Maritime mobile service and public land mobile service; The international identification plan for public networks and subscriptions.
Topic	5.1.2
Type	URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.212-201609-I!!PDF-E&type=items

Extra Template	
Number	5.9
Title	3GPP Technical Specification 03.40; 3rd Generation Partnership Project; Technical Specification Group Terminals; Technical realization of the Short Message Service (SMS); (3GPP TS 03.40).
Topic	5.1.9
Type	URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=141

Extra Template	
Number	5.10
Title	ETSI Technical Specification GSM 03.40; Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP); (GSM 03.40).
Topic	5.1.9
Type	URL: https://www.etsi.org/deliver/etsi_gts/03/0340/05.03.00_60/gsmts_0340v050300p.pdf

Extra Template	
Number	5.11
Title	ETSI TS 123.038 Technical Specification; Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Alphabets and language-specific information (3GPP TS 23.038).
Topic	5.1.9
Type	URL: https://www.etsi.org/deliver/etsi_ts/123000_123099/123038/10.00.00_60/ts_123038v100000p.pdf

Extra Template	
Number	5.12
Title	Complete list of APDU responses.
Topic	5.5
Type	URL: https://www.eftlab.co.uk/index.php/site-map/knowledge-base/118-apdu-response-list