4. Acquire and make the forensic image of the compromised drive.
5. Perform the comparison between files on forensic image and the original installatio image. Also compare the common files hash values, such as Win.exe and standard DLL and find out whether they have altered.

2.7 Exam Pack (Review Questions)

☛ **Syllabus Topic : Introduction to Network Forensics and Tracking Network Traffic**

Q. 1 What is network forensics ? *(Refer section 2.1)* (5 Marks)

Q. 2 What is mean by securing a network ? *(Refer section 2.1)* (5 Marks)

☛ **Syllabus Topic : Reviewing Network Logs**

Q. 3 What is mean by reviewing logs? *(Refer section 2.2)* (5 Marks)

☛ **Syllabus Topic : Network Forensic Tools**

Q. 4 Write a short note on network forensic tools? *(Refer section 2.3)* (5 Marks)

☛ **Syllabus Topic : Performing Live Acquisitions**

Q. 5 What is the general procedure given for live acquisition ? *(Refer section 2.4)* (5 Marks)

☛ **Syllabus Topic : Order of Volatility**

Q. 6 What is order of volatility ? *(Refer section 2.5)* (5 Marks)

☛ **Syllabus Topic : Standard Procedures**

Q. 7 What is the standard procedure used in network forensics ? *(Refer section 2.6)* (5 Marks)

Chapter End

Unit I

CHAPTER 3

Cell Phone and Mobile Device Forensics

Syllabus Topic : Overview

3.1 Overview

Q. 3.1.1	What type of information does the mobile phone contains ? *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.2	Explain the digital networks for mobile phones. *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.3	Explain the technologies where the 4G network can be used. *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.4	What are the main components used with cell phone for communication ? *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.5	Explain SIM card *(Ref. Sec. 3.1)*	**(5 Marks)**

- Cell phone and mobile device forensics is a fast changing field as maximum work is done by mobile device.
- In cell phone people save lots and lots of data, so if in case you lose your mobile phone, the data stored in the cell phone also get lost and it may be used for wrong purposes. It is observed that many people do not secure their cell phones, though they regularly lock and secure laptops or desktops.
- Now a day's maximum transactions are done via mobile like people log into their bank accounts and transfer the funds and perform other banking work. Your mobile phone contains the following information.
- Incoming calls, outgoing calls, and missed calls
  - Text and Short Message Service (SMS) messages

- E-mail
- Instant Messaging (IM) logs like messenger and whatsapp messaging
- Web pages
- Photos and videos
- Personal calendars
- Address books
- Songs
- Voice recording
- Banking details.

Now a day's maximum people are storing more information on their cell phones than th computers, and it is resulting in crimes or cases. Recent days the mobile phone data is used a many cases as evidence. But it is very challenging to investigate the cell phones and mobi devices in computer forensics. The following are the challenges while investigating the mobi devices and cell phones :

1. For storing the message no single standard id exist although many of the phones use sam storage scheme.
2. As technology is changing new phones are coming in the market about eve 5 to 6 months and they are merely compatible with the previous model of the phone. I near future the cables and accessories may become obsolete in a short time.
3. As cell phones are often combined with PDAs, which can make forensics investigatio more complex.

☛ Mobile phone basics

- In 1970, Motorola introduced cell phones, and it is developed rapidly. There we 3 generations of the mobile phones till 2008, and they are: analog, digital Person Communications Service (PCS), and third-generation (3G).
- 3G gives the increased bandwidth, as compare to analog and PCS. It gives 384 Kbps f pedestrian use, 2 Mbps in fixed locations, such as office buildings and 128 Kbps in moving vehicle.

- Digital networks for mobile phones :

1. Code Division Multiple Access (CDMA)
2. Global System for Mobile Communication (GSM)
3. Time Division Multiple Access (TDMA)
4. Integrated Digital Enhanced Network (iDEN)
5. Digital Advanced Mobile Phone Service (D-AMPS)
6. Enhanced Data GSM Environment (EDGE)
7. Orthogonal Frequency Division Multiplexing (OFDM)

➜ 1. Code Division Multiple Access(CDMA)

- CDMA is developed by Qualcomm. To define the channels CDMA uses complete radio frequency spectrum. Sprint and Verizon uses the CDMA networks.
- Many of the CDMA networks match to IS-95, which is created by the TIA (Telecommunications Industry Association). These systems are known as cdmaOne, and when they go to 3G services, they will become cdma2000.

➜ 2. Global System for Mobile Communication (GSM)

- GSM is used by AT&T and T-mobile. It is a standard in Asia and Europe.
- It uses Time Division Multiple Access (TDMA) technique, thus many phones get turns sharing a channel, a lot like token ring networks.

➜ 3. Time Division Multiple Access (TDMA)

- The TDMA network divides a radio frequency into timeslots. GSM also uses the same techniques. TDMA refers to the IS-136 standard, which introduced sleep mode to enhance battery life.
- TDMA can work in the cell phone with frequency 800 MHz to 1000 MHz) or PCS (1900 MHz) frequency, as a result it is compatible with a number of cell phone networks.

➜ 4. Integrated Digital Enhanced Network (iDEN)

It is a Motorola protocol which combines various services including data transmission, into one network.

➜ **5. Digital Advanced Mobile Phone Service (D-AMPS)**

D-AMPS is a digital version of original analog standard for cell phone.

➜ **6. Enhanced Data GSM Environment (EDGE)**

- EDGE digital network is used to deliver data and it is a faster version of GSM. It is specially designed for 3G.
- The 3G standard is developed by the International Telecommunication Union (ITU). It's compatible with CDMA, TDMA, and GSM.

➜ **7. Orthogonal Frequency Division Multiplexing (OFDM)**

OFDM technology for 4G network utilizes energy more efficiently than 3G networks. It is more immune to inference.

☛ **4G networks can use the following technologies**

1. Orthogonal Frequency Division Multiplexing
2. Mobile WiMAX
3. Ultra Mobile Broadband (UTMS)
4. Multiple Input Multiple Output (MIMO)
5. Long Term Evolution (LTE)

➜ **1. Orthogonal Frequency Division Multiplexing (OFDM)**

- Orthogonal Frequency Division Multiplexing (OFDM) this techniques uses radio wave broadcast over dissimilar frequencies it uses power more resourcefully, and is more resistant to interference.

➜ **2. Mobile WiMAX**

- This technology supports transmission speeds of 12Mbps. It is chosen by Sprint for its 4G network.
- This technology uses the OFDMA and IEEE 802.16e standard.

➜ **3. Ultra Mobile Broadband (UTMS)**

- CDMA network provider use this technology to switch to 4G and to support the transmission speed of 100 Mbps.

- This technology also known as CDMA2000 EV-DO.

➜ **4. Multiple Input Multiple Output (MIMO)**

- Airgo developed this technology and Qualcomm acquired it.
- It is expected to support 312 Mbps transmission speeds.

➜ **5. Long Term Evolution (LTE)**

- LTE technology supports the transmission speed of 45 Mbps to 144 Mbps and is designed for UMTS and GSM technology, is expected to support 45 Mbps to 144 Mbps transmission speeds.
- The main components used for communication with these cells are : BTS, BSC and MSC.

➜ **(i) Base Transceiver Station (BTS)**

- BTS is made up of radio transceiver equipment.
- It describes cells and communicates with mobile phones.

➜ **(ii) Base Station Controller (BSC)**

- BSC is a combination of hardware and software.
- BSC manages BTSs and allots channels by connecting to the mobile switching center.

➜ **(iii) Mobile Switching Center (MSC)**

- MSC connects calls by routing digital packets for the network and relies on a database to support subscribers.
- This central database has location data, account data, and other key information needed during an investigation. To access information from a carrier's central database warrant or subpoena is needed.

☛ **Inside Mobile Devices**

- The hardware the Mobile devices consists of is ROM, RAM, a microprocessor, a digital signal processor, a microphone and speaker, a radio module, hardware interfaces (for example, cameras, keypads, and GPS devices), and an LCD display, removable memory cards (in some mobile), Bluetooth and Wi-Fi, Oprating system (such as, Linux, Windows Mobile, Android, RIM OS, Palm OS, Symbian OS, Mac OS X).

- Usually, data is stored in the phone electronically erasable programmable read-only memory (EEPROM).
- It allows the service providers to reprogram phones without accessing memory chips physically. Many users take advantage of this facility and reprogram their phone to add new features or switch to different service providers.

SIM Cards

- Subscriber identity module (SIM) cards are used in GSM devices and consist of a microprocessor and 16 KB to 4 MB EEPROM or more than that. SIM cards are like to standard memory cards, but the connectors are associated differently.
- To find the SIM card, open the panel covering GSM. GSM refers to mobile phones as mobile stations.
- The mobile station is divided into two parts : The SIM card and the Mobile Equipment (ME), which is the remainder of the phone. The SIM card is needed for the mobile equipment to work and serves these following additional purposes :
  - To identify the subscriber to the network.
  - To store personal information.
  - To store address books and messages.
  - To store service-related information.
- You will get SIM cards in two sizes. The most standard size is 0.75 mm thick. SIM card is portable; simply by switching a SIM card between compatible phones, you can move your information to another phone.
- If you are travelling to neighboring countries then you have two SIM cards, one for your country and other is for foreign country, you can easily switch to new SIM card.

Inside PDAs

- Personal Digital Assistants (PDAs) are separate devices from mobile phones. The majority users carry them in place of a laptop to keep track of appointments, deadlines, address books, and so forth.
- Most of the PDAs have integrated phones. PDAs consists of RAM, microprocessor, flash ROM, and a variety of hardware components. You can retrieve the user's calendar, address book, Web access, and other items from PDA's.

PDA's uses many peripheral memory cards :

(i) **Compact Flash (CF) :** These cards are used for extra storage and work .

(ii) **MultiMedia Card (MMC) :** These cards are designed for mobile phones, but you can use with PDAs to give another storage area.

(iii) **Secure Digital (SD) :** These cards are like MMCs, only extra security features are added to protect data.

Syllabus Topic : Acquisition Procedures for Cell Phones and Mobile Devices

3.2 Acquisition Procedures for Cell Phones and Mobile Devices

Q. 3.2.1	Explain acquisition procedures for cell phones and mobile devices. *(Ref. Sec. 3.2)*	**(5 Marks)**
Q. 3.2.2	Explain mobile forensic. *(Ref. Sec. 3.2)*	**(5 Marks)**
Q. 3.2.3	Explain SIM card reader and the problems with SIM card reader *(Ref. Sec. 3.2)*	**(5 Marks)**

- It is important to have proper search and seizure procedures for cell phones. The main fear with mobile devices is loss of power and synchronization with PCs. As all the mobile devices have volatile memory, So ensure that you retrieve the RAM data before the power off.
- If you are investing a scene then specify that mobile device is on or off. If the device is off then connect the charger as soon as possible or if it is on then check the LCD display for the battery's current charge level.
- As you know mobile devices are connected to the PC via cable cradle station should be disconnected immediately from the PC. It helps to prevent automatic synchronization that might occur on a fixed schedule and overwrite data on the device.
- Additionally, collect the PC and any peripheral devices that determine whether the hard drive consists of any information that's not on the mobile device.
- Based on the warrant, the time of seizure may be relevant. It may be possible that messages may be received after seizure that may or may not be admissible in court. If you are turning of the device to protect the battery power or attacks then note down the date and time when you have taken this step.

- The solution is to isolate the device from incoming signals by using any one of the following options :
  - Put the device in a paint can, preferably one that previously contained radio wave blocking paint.
  - Make the use of the Paraben Wireless Stronghold Bag.
  - Make the use of eight layers of antistatic to block the signal.
- The disadvantage of using isolating options is that the mobile device is put into roaming mode, which speed ups battery drainage. The solution to this is using portable mean of power, like a battery-powered charger. Some mobile phones or devices shut themselves off or enter a "sleep state" after reaching a certain low battery level.
- In the forensic lab when you come back then you have to assess what can be retrieved. You have to check following 4 areas for critical information :
  - The SIM card
  - The internal memory
  - Any removable card or external memory cards
  - The system server.
- For checking the system server warrant is required, so to check the voicemail you need warrant. Help from service provider is also needed to discover the time of a call, to access backups of address books, and other.
- On mobile device, there is both, volatile and non-volatile memory available for storage. Volatile memory needs power to preserve its contents, but non-volatile memory does not.
- Though the exact locations of data differ from one phone model to the next, volatile memory typically contains frequently changed data like missed calls, text messages, and sometimes even user files. Non-volatile memory contains OS files and stored user data, for example, backed-up files and a Personal Information Manager (PIM).
- As you know memory resides in the phone itself and in the SIM card, if the device is equipped with one. SIM card's file structure is hierarchical structure. This file structure starts with the root of the system (MF).
- In the next level there are Directory Files (DF) and under DF there are files which contain elementary data (EF). In the Fig. 3.2.1, the EFs in the GSM and DCS1800 DFs have network data on different frequency bands of operation. The EFs in the Telecom DF contain service-related data.

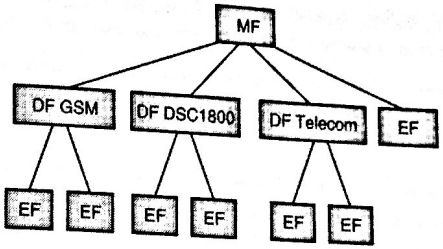

Fig. 3.2.1 : SIM file structure

- From SIM card you can recover moderately a little of data. The recovered information falls into four categories :
  - Service-related data, for example identifiers for the SIM card and subscriber
  - Call data, like dialed numbers
  - Message information
  - Location information
- If power is lost, you require PINs or other access codes to view files. normally, users keep the original PIN assigned to the SIM card, so while collecting evidence at the scene, seek users' manuals and additional documentation that can help you access the SIM card. In many SIM cards you have 3 attempts of entering an access code before the device is locked, else you need to call the service provider or you have to wait for a certain amount of time before trying again.

Mobile Forensics

- In mobile forensics the biggest challenge is constantly changing models of cell phones and what works with the current cell phone model will not work with upcoming model.
- Like computer forensics we cannot recover deleted files in mobile forensics. In mobile forensics usually you are performing two tasks :

  (a) By synchronizing PC with the device

  (b) Reading the SIM card.

- The first step in mobile forensic is to identifying the mobile device. Many users do not change their device, but some users don't alter their devices, but some file off serial numbers, modify the display to show deceptive data, and so on.

- There are many online sources available to identify the phone. For example www.phonescoop.com, www.cellphoneshop.com and www.mobileforensicscentral.com
- Second way is to ensure that mobile device software is installed on your forensic machine. Keep in mind that not all the devices are supported with the required software; several/many tools are expensive.
- Some tools simply take pictures of screens as you scroll through them. Forensically, this validation is not a good approach, but if no other alternative is available then you can use it.
- Third way is to attach the phone to its power supply and connect the correct cables. ... cables to connect to devices or cables for the model you're investigating may or may not be available.
- Lastly, after connecting the device, start the forensics program and start downloading the available information.

SIM Card Readers

With mobile devices, next step is to access SIM card using the combination hardware/software device called a SIM card reader. To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present in the inside of the case, so you should consult the lab investigator when you're ready to process in this way. The general procedure is as follows:

1. Take out the back panel of the device.
2. Take out the battery.
3. Under the battery, take out the SIM card from its holder.
4. Now into the card reader insert the SIM card.

Problems with SIM card Reader

1. To understand the data collection procedure of cell phones and mobile devices. There are many different types of SIM card readers available in market. Some SIM card readers are forensically sound and some are not; note down this feature of the device in your investigation log.
2. Second problem is related to the text and SMS messages. It is very difficult to document the deleted messages. In such situation use a tool that takes pictures of each screen can be helpful in this situation. These screen captures can provide extra documentation.

3.3 Exam Pack (Review Questions)

Syllabus Topic : Overview

Q. 1 What type of information does the mobile phone contains? (Refer section 3.1) (5 Marks)

Q. 2 Explain the digital networks for mobile phones. (Refer section 3.1) (5 Marks)

Q. 3 Explain the technologies where the 4G network can be used. (Refer section 3.1) (5 Marks)

Q. 4 What are the main components used with cell phone for communication? (Refer section 3.1) (5 Marks)

Q. 5 Explain SIM card. (Refer section 3.1) (5 Marks)

Syllabus Topic : Acquisition Procedures for Cell Phones and Mobile Devices

Q. 6 Explain acquisition procedures for cell phones and mobile devices. (Refer section 3.2) (5 Marks)

Q. 7 Explain mobile forensic. (Refer section 3.2) (5 Marks)

Q. 8 Explain SIM card reader and the problems with SIM card reader. (Refer section 3.2) (5 Marks)

❑❑❑

Chapter Ends...