U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING OPERATIONS

TECHNICAL OPERATIONS DIVISION

Homeland Security

LESSON PLAN

MDIP FINAL EXAM

3267 **SEP/10**

~~**WARNING**~~

~~**This document is FOR OFFICIAL USE ONLY (FOUO)/LAW ENFORCEMENT SENSITIVE (LES). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid 'need-to-know' without prior authorization of an authorized Department of Homeland Security Official.**~~

~~**FOR OFFICIAL USE ONLY**~~

LAW ENFORCEMENT SENSITIVE

DEVELOPED BY: (SEP/10)

(b)(6) Senior Instructor, TOD

REVIEWED BY: (SEP/10)

(b)(6) Branch Chief, Technical Operations Division

Changes to the TPOs and/or EPOs and the lesson plans security markings were updated via the template.

TABLE OF CONTENTS

SYLLABUS

COURSE TITLE: **MDIP Final Exam**

COURSE NUMBER: **3267**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OPTION
		4	4	MDIP	

DESCRIPTION:

In the Mobile Device Investigations Program (MDIP) students participate in the final examination by taking a written test and performing a practical exercise that demonstrates their knowledge of cell technology. Prior to this exercise, cell phones are prepared with a data set that follows a given scenario. Each student is required to examine one of those devices and utilize the associated call detail records to map the suspect's call history and answer questions related to the scenario.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given a cell phone (with SIM), call detail records, the proper forensic tools, mapping software, and a scenario, students will examine and extract data using mapping techniques to track the suspect's movements.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Identify significant evolutionary milestones in communications technology that have contributed to the current status of the cellular communications industry.

EPO #2: Describe the technology involved in cellular phone communications.

EPO #3: EPO #3: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

EPO #4: Define Call Handoff and list the locations where evidentiary artifacts are stored.

EPO #5 Define the Hexagon Grid and its importance to the Cellular Network.

EPO #6: List the five main components of a wireless network and their responsibilities.

EPO #7: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

EPO #8: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

EPO #9: List the administrative task of the Control Channel.

EPO #10: Define TDMA and list TDMAs advantages.

EPO #11: Define CDMA and list how its signals are spread.

EPO #12: Define GSM and list the four subsystems required for this standard.

EPO #13: Define SIM Card and the information that is stored there.

EPO #14: Define *i*DEN and list the two types of HLRs and VLRs.

EPO #15: Define PCS and list the two types of services provided by these wireless networks.

EPO #16: Define “Call detail Reports” and identify how they are acquired.

EPO #17: Define the term “cell phone mapping” and use appropriate mapping techniques to determine subject locations at specific dates and times.

EPO #18: Define the term “cell phone tracking” and describe appropriate tracking techniques to locate an investigative subject in real-time.

STUDENT SPECIAL REQUIREMENTS:

1. Students must score a passing grade on the written exam in order to graduate from the program.
2. Students must also score a passing grade on the practical exercise in order to graduate from the training program. Students will be tested on their proficiency in the extraction/acquisition of data from mobile devices.
3. Students must also use the data acquired from the device, in conjunction with the call detail records, to answer questions regarding the scenario and map the suspect’s movements through call history.

METHOD OF EVALUATION:

Graded Written/Practical Exercise

INSTRUCTOR GUIDE

METHODOLOGIES:

Graded Written/Practical Exercise

TRAINING AIDS/EQUIPMENT:

1. Instructor:

   Practical Exercise Scenario and answer sheet.

2. Student:

   a. CelleBrite or Susteen Secure View2 (or other applicable forensic tool).

   b. Computer

   c. Microsoft Trips and Streets

   d. Cell Phone with SIM

   e. Call Detail Records

INSTRUCTOR SPECIAL REQUIREMENTS:

There should be at least two instructors to monitor student progress and answer questions. Instructors should be familiar with the cell phone forensic tools and software used in the class.

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

1. During this training course you have received instruction on the extraction/acquisition of digital evidence from mobile devices using multiple forensic tools. You have also learned how to utilize that data, along with call detail records, to map a suspect's movements, through his call history.
2. A comprehensive practical exercise will be administered to test your knowledge and ability to perform these functions in a real-world setting.
3. You will demonstrate your knowledge of cell technology, through written and practical exercise. Prior to this exercise, cell phones are prepared with a data set that follows a given scenario. Each student is required to examine one of those devices and utilize the associated call detail records to map the suspect's call history and answer questions related to the scenario.

B. LESSON PLAN OVERVIEW

1. Terminal performance objective (TPO)

   Given a cell phone (with SIM), call detail records, the proper forensic tools, mapping software, and a scenario, students will examine and extract data using mapping techniques to track the suspect's movements.

2. ENABLING PERFORMANCE OBJECTIVES (EPO)

   a. EPO #1: Identify significant evolutionary milestones in communications technology that have contributed to the current status of the cellular communications industry.

   b. EPO #2: Describe the technology involved in cellular phone communications.

   c. EPO #3: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

   d. EPO#4: Define Call Handoff and list the locations where evidentiary artifacts are stored.

   e. EPO #5: Define the Hexagon Grid and its importance to the Cellular Network.

   f. EPO #6: List the five main components of a wireless network and their responsibilities.

g. EPO #7: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

h. EPO #8: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

i. EPO#9: List the administrative task of the Control Channel.

j. EPO #10: Define TDMA and list TDMAs advantages.

k. EPO #11: Define CDMA and list how its signals are spread.

l. EPO #12: Define GSM and list the four subsystems required for this standard.

m. EPO #13: Define SIM Card and the information that is stored there.

n. EPO #14: Define *i*DEN and list the two types of HLRs and VLRs.

l. EPO #15: Define PCS and list the two types of services provided by these wireless networks.

p. EPO #16: Define "Call detail Reports" and identify how they are acquired.

q. EPO #17: Define the term "cell phone mapping" and use appropriate mapping techniques to determine subject locations at specific dates and times.

r. EPO #18: Define the term "cell phone tracking" and describe appropriate tracking techniques to locate an investigative subject in real-time.

II. PRESENTATION

A. EPO #1: IDENTIFY SIGNIFICANT EVOLUTIONARY MILESTONES IN COMMUNICATIONS TECHNOLOGY THAT HAVE CONTRIBUTED TO THE CURRENT STATUS OF THE CELLULAR COMMUNICATIONS INDUSTRY.

1. In the beginning, prior to the 1950's, mobile telephones did not exist (as such). If people wanted to communicate they used mobile radios.

2. About 1950 Mobile Telephone Service (MTS) was introduced.

   a. Luggage-sized transceiver weighing up to 45 pounds;

   b. Tube electronics (of course);

   c. Required phone operator interface (contact the telephone

operator who would 'patch' you into the phone system);

d. VHF Frequencies (152 – 159Mhz);

e. Very limited number of user;

f. One tower per city.

g. Half-duplex;

h. Speak or listen (but not both);

i. This standard lasted for 13 years.

3. In 1964 the Improved Mobile Phone Service (IMPS) was introduced.

   a. No operator interface required;

   b. Multiple channels allowed for more simultaneous users;

   c. Smaller radio-telephones;

   d. Weight now to typically 25 pounds.

   e. New frequency range: 450 – 460Mhz;

   f. Still one tower per city but it had a range of 50 miles;

   g. No privacy. All calls were public.

4. In 1970 mobile technology first offered duplexing: the ability to listen and speak at the same time.

5. In 1974 'cellular technology' was born when the FCC defined the specifications for multiple channels, multiple towers, and a bevy of other specifications that would evolve into today's cellular industry.

6. An offshoot of these FCC specifications was the birth of a new set of telecommunications standards collectively referred to as Advanced Mobile Phone Service (AMPS)

   Although AMPS was designed for analog wireless service, today over 98% of AMPS communications is digital

7. In 1984 the Nextel Corporation was founded. Nextel technology was 'different' in that it combined the facility of mobile radios (push-to-talk) with cell phones and offered both services in a single device.

   a. Push-to-Talk (PTT) is a technology developed by Motorola and has since its introduction been very popular with public service organizations that typically need both radio and cellular service.

   b. This technology is referred to as 'iDENT' and requires markedly different technology used by ordinary cell phones.

c. In 2006 Nextel merged with Sprint.

8. In the early 1990's, as digital wireless became popular, new technologies arose to replace the current analog devices.

   a. TDMA, CDMA, and GSM. Each of these technologies, and how they relate to cellular forensics, will be explored in the 'Cell Phone Technology' course.

   b. The birth of digital wireless is widely considered 'Second Generation' wireless technology

9. In the mid-1990's wireless service providers began harnessing evolving technology and offering new cellular phone features such as text messaging (Short – or Simple – Message Service (SMS)), Internet connectivity, and mid-range bandwidth to support live television.

   a. This, in turn led to the development of a variety of 'hybrid' devices that combines cell phone features, email messaging features, MP3 players, and other communications service in single devices.

   b. Sometimes referred to as 'Smartphones'.

10. The year 2008 will see an evolution to what many refer to as 'Fourth Generation' wireless technology with new technical features:

    Broader bandwidth (100Mhz to 1Ghz) will allow for on-demand, real time, audio and video communications.

11. Changes in the wireless industry:

    a. In November 1997 there were less than 1,000,000 cell phones subscriptions in the U.S. On November 13, 2007, there were 250,000,000 subscriptions

    b. In June 2006, there were 20,000,000 'Prepaid' cellular subscriptions. In March 2008, there were over 50,000,000.

    c. In July 1995, there were no 'cellular only' households. In March 2008, over 15% of households in the U.S. were 'cellular only'.

    d. In June 1995 there was an annual average of 31.5 million minutes of cell phone use. In March 2008, there were over 2 trillion minutes.

    e. In June 1995 there were 19,844 cell towers. In June 2007 there were 210,360 towers.

    f. In June 1995 there were no messages. By June 2007, there

were 240.8 billion per year.

12. As of March 2008, the largest cell service providers in the U.S. (by subscribers) were:

a.	AT&T	(70.1 million)
b.	Verizon	(63.7M)
c.	Sprint/Nextel	(54M)
d.	T-Mobile	(28.7M)
e.	Alltel	(12.5M)

B. EPO #2: DESCRIBE THE TECHNOLOGY INVOLVED IN CELLULAR PHONE COMMUNICATIONS.

1. At its most fundamental level, a cell phone is a two-way radio. The specifications and technology is defined by the FCC and provided to the end user by several commercial Cell Service Providers (CSP's).

   AT&T Cellular, Verizon, Alltel, Sprint, and T-Mobile are examples of CSP's. Although each is a licensed corporation, their services are carefully regulated by the FCC.

2. Cell phones are of limited power and range. They are designed to communicate with a cell phone tower which is typically located within a few city blocks (in an urban environment) or within 10-miles-or-less (for a rural environment). The tower relays the voice signal from the user to the CSP's "Mobile Telephone Switching Office" (MTSO). The MTSO in turns relays the voice signal to either:

   a. Another cell phone communicator (the voice message respondent) via a series of cell towers; or

   b. To the Public Switched Telephone Network (PSTN) if the caller is communicating with someone on a land line.

3. The "cell" is the fundamental component of the cellular network. There are several "cells" within a CSP's assigned geographical area. All the cells within a geographical area create an analogous honeycomb effect with each cell tower communicating with up to 6 adjacent cells.

4. The center of the cell is the cell tower. Although cell towers have become ubiquitous on the landscape, many towers are effectively disguised. Cell towers can be established in trees, church steeples, roofs of buildings, commercial advertising signs, and in any number of other creative locations.

5. Each cell tower is assigned 56 voice channels. Additionally, the

carrier uses 42 channels for non-voice controls. These control channels communicate invisibly with the users' phones and with the carriers MTSO.

6. Each voice channel is "duplex" which means that the users can speak and listen simultaneously.

   Technically, each carrier is assigned 832 frequency per assigned geographical area. 42 of these frequencies are for control signals; the other 790 are divided and assigned to each cell "honeycomb" – 112 frequencies per cell (two frequencies – for speaking and listening – per channel).

7. Of the six cells surrounding a single cell (the "honeycomb"), none share frequencies. That is, no adjacent cells will ever have the same channel assignments.

8. When a user moves from one cell to another, the control channels are used to transfer communications to a new cell. This transfer of channels is called a "handoff". It is done transparently to the user and there should never be an audible interruption of service.

9. The 56 channels per tower is usually not sufficient to handle the traffic demands on the cell if each user had a dedicated channel. Technology has evolved which allows several users to share a channel with no degradation of service. Multiple users per channel is referred to as "multiplexing". Different multiplexing technologies are used by different carriers. The three multiplexing technologies now in use in the United States are:

   a. TDMS (Time Division Multiple Access): the oldest multiplexing technology. It multiplexes voice only and is being phased out since the demand has grown for other types of cell communications. TDMA can easily multiples three users per channel.

   b. CDMA (Code Division Multiple Access): This is a US-only technology used by several CSP's and can multiplex voice, text, graphics, Internet/Broadband, and perhaps other types of non-aural communications. CDMA typically multiplexes up to 10 users per channel.

   c. GSM (Global Systems for Mobile Communications): This is the standard multiplexing technology for most of the world, being the standard in 168 countries. Within the USA, TDMS users (such as AT&T) are evolving to GSM as their new multiplexing technology.

i. A benefit of GSM is that the user can communicate (or should be able to communicate!) with the same mobile phone when traveling throughout the world.EPO #3: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

C. EPO #3: DEFINE FREQUENCY REUSE AND HOW THIS SYSTEM IS GEOGRAPHICALLY POSITIONED TO ENSURE ITS ABILITY TO OPERATE.

1. Cellular Technology enables mobile communication because they use of a complex two-way radio system between the mobile unit and the wireless network. It uses radio frequencies (radio channels) over and over again throughout a market with minimal interference, to serve a large number of simultaneous conversations. This concept is the central tenet to cellular design and is called frequency reuse.

2. Frequency Reuse and Planning is the act of repeatedly reusing radio frequencies over a geographical area. Most frequency reuse plans are produced in groups of seven cells.

   a. There are numerous seven cell frequency reuse groups in each cellular carrier's Metropolitan Statistical Area (MSA) or Rural Service Areas (RSA).

   b. Higher traffic cells will receive more radio channels according to customer usage or subscriber density.

3. A frequency reuse plan is defined as how radio frequency (RF) engineers subdivide and assign the FCC allocated radio spectrum throughout the carriers market.

   a. In concept frequency reuse maximizes coverage area and simultaneous conversation handling.

   b. Cellular communication is made possible by the transmission of RF. This is achieved by the use of a powerful antenna broadcasting the signals.

   c. If you have one powerful antenna you would be able to handle conversations based on the number of channels you have available.

   d. The first step for frequency reuse is the development of the cell system network.

4. Each antenna, in the various cells, operate on the same RF that they are assigned. If your original antenna could handle 7 calls and you increased the number of antennas by 10 you can now handle 70 simultaneous calls.

5. The concept goes beyond the number of antennas and deals with how the radio frequency itself is used and reused.

    a. Each cell has its own antenna and low power Base Station to handle the traffic within its area.

    b. Each Base Station is assigned frequencies with neighboring base Stations being assigned different frequencies.

    c. Carriers are then able to reassign these frequencies to other areas that are not too geographically close to the other Base Stations and cells.

6. Consider your local radio station broadcast. As you travel farther away from the radio base it weakens until you lose the signal.

    a. Now consider all the cars driving around you are listening are listening to different stations.

    b. The radio station would be the Base Station and the vehicles would be the cells.

7. A key component in this system is the Distance to Reuse Ratio. The Distance to Reuse ratio defines how much geographical distance is required between cells in a cell system to avoid and limit interference.

    a. The overall geographic sizes of cell base stations, along with the power of the antenna, determine the distance to reuse ratio.

    b. What happens when I move about a cell coverage area or move into another cell area?

    c. Another requirement of the wireless system is frequency agility. This is the ability of the mobile unit to operate on any given frequency within their assigned spectrum.

    d. This allows the mobile unit to switch from one channel to the another seamlessly and allows for another a important component of cellular technology – Call Hand Off

D. EPO#4: DEFINE CALL HANDOFF AND LIST THE LOCATIONS WHERE EVIDENTIARY ARTIFACTS ARE STORED.

1. Call handoff can best be defined as the process of passing from one Base Transceiver Station (BTS) to another maintaining connection to your network.
    a. When you are leaving your particular network and passed to another network - the roaming process begins.
    b. This is transparent to the user.
    c. Without Call Handoff, Frequency Reuse would not be possible and vice versa.
2. The Mobile Switch Center or MSC monitors the power levels of the mobile units.
    a. Base station coverage overlap with other cells in the area and it is this overlapping that allows call handoff to occur.
    b. This action is handled by a microprocessor at the MSC and is seamless to the user.
3. This is a complex act that uses frequency synthesizers, the controller, and memory functions within the wireless handset.
    a. This is why cellular phones must have frequency agility or the ability to change from one channel to another.
    b. When the MSC detects the mobile unit power levels degrading ,it seeks out another BTS.
4. The FCC requires the use of United States Geographical Survey maps in the planning and development of the wireless network.
    a. As it relates to planning it is important that all carriers use the same maps to lend conformity to the planning process.
    b. Since the BTS operates at specific power levels it is very important to know where other towers are to avoid and/or minimize interference.

E. EPO #5: DEFINE THE HEXAGON GRID AND ITS IMPORTANCE TO THE CELLULAR NETWORK.

1. (b)(7)e

2.

3. (b)(7)e

F. EPO #6: LIST THE FIVE MAIN COMPONENTS OF A WIRELESS NETWORK AND THEIR RESPONSIBILITIES.

1. There are five main components to a wireless network. They are;
   a. The Mobile Unit
   b. The Cell Base Station
   c. The Backhaul or Fixed Network
   d. The Mobile Switching Center
   e. The interconnection to the Public Switched Telephone Network (PSTN)
2. The Mobile Unit
   a. The Portable telephone or device – these are your small handsets, portable devices with network connection capabilities such as PDA's and GPS units.
   b. The Mobile telephone or device – devices that are mounted in the locomotion device, such as installed telephones and GPS units.
3. The Cell Base Station
   a. The Cell Base Station is the physical location of some of the equipment needed to operate the wireless network, such as antennas, GPS timing systems, cell towers etc.
   b. The size of the base station is dependent upon its location and system needs.

1. Raw Land Sites - These sites consists of typical stand alone towers with the necessary equipment to keep them functional.
2. Rooftop Sites – These towers are mounted on rooftops and the equipment can either be placed outdoors or linked to components inside the building.
3. Water Tank Sites – Since water towers are still present throughout the landscape they provided the height and the stability needed for Cell Base Stations.
4. Co-located Sites - With limited landscape and space available the FCC and local communities have mandated, when possible, that CSPs share Cell Base Stations.
5. Stealth Sites – Local communities have also required that CSPs make every attempt possible in populated areas to disguise Cell Base Stations so the blend into the surrounding environment.
6. Microcell – an outdoor network base station usually on rooftops, water tanks and the like. The Base Station range of a Microcell is generally 100 meters to 1000 meters.
7. Picocell – the smallest, usually used indoors and intended to provide coverage for a small area. The Base Station range of a Picocell is generally less than 100 meters. Typically found in airports, e.g.
8. Nanocell – are mobile and easily installed. Nanocell can be mounted on walls, in vehicles or outdoor weatherproof enclosure. Coverage is dependant you configuration.

4. The Backhaul or Fixed Network – Base Station Controller

Is a complex collection of systems that connect the Base Stations to the Base Station Controller. This network connects the mobile users to others on its network and to the outside world.

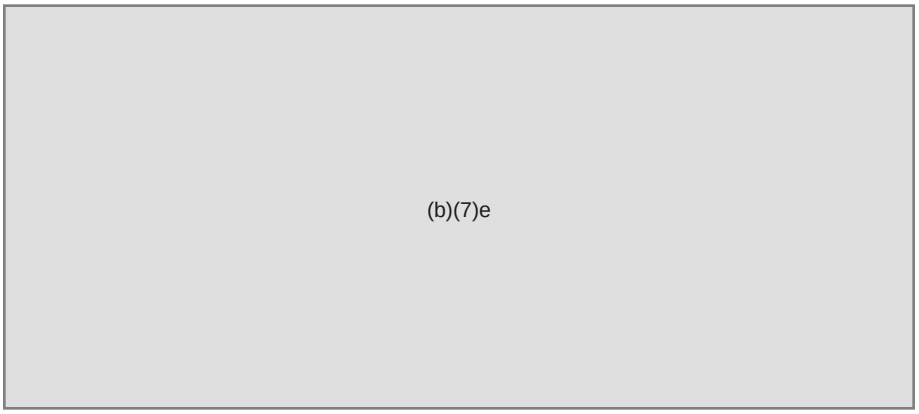
a. (b)(7)e

b.

c.

d.

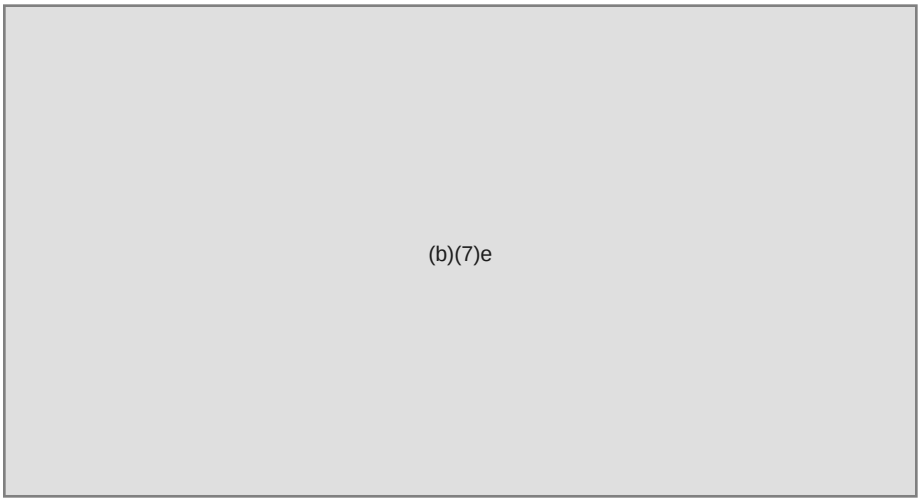
e.



5. The Mobile Switching Center

a.

b.



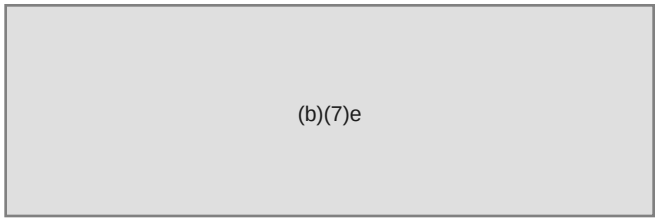
6. The MSC provides subscriber management functions such as;

a.

b.

c.

d.



These functions are carried out by various databases, among which are the Home Location Registry, the Visitor Location Registry, Equipment Identity Register and the Authentication Center (AuC) in GSM systems.

G. EPO #7: DEFINE THE HOME LOCATION REGISTRY AND THE VISITOR LOCATION REGISTRY AND LIST WHAT INFORMATION IS STORED WITHIN EACH.

1. The Home Location Registry or HLR is a database that contains records of all subscribers. The HLR is used to identify and verify a subscriber on a network and a record of what services the subscriber has.
2. The HLR connects and interacts with a number of other components on the system;
   a. The Gateway MSC for handling incoming calls
   b. The VLR for handling request from mobile phones to attach to the network
   c. The Short Message System Center or SMSC is for handling incoming SMS or text messages.
   d. The voice system for delivering notification to the mobile phone that a message is waiting
3. (b)(7)e
4.
5.

6.

7.

8.

9.

(b)(7)e

10.

11.

12.

(b)(7)e

13.

14.

H. EPO #8: LIST THREE FACTORS OF RADIO FREQUENCY COVERAGE FROM BASE STATIONS AND THE TWO ON-GOING ISSUES FACING WIRELESS CARRIERS.

1.

2.

3. (b)(7)e

4.

5.

6.

7.

(b)(7)e

8.

9.

10.

11.

12.

13.

14.

15.

16.

(b)(7)e

17.

18.

19.

I. EPO #9: LIST THE ADMINISTRATIVE TASK OF THE CONTROL CHANNEL.

1.

2.

3.

4. (b)(7)e

5.

J. EPO #10: DEFINE TDMA AND LIST TDMAS DISADVANTAGES.

1. (b)(7)e

2.

3.

4. (b)(7)e

5.

K. EPO #11: DEFINE CDMA AND LIST HOW ITS SIGNALS ARE SPREAD.

1.

2. (b)(7)e

3.

4.

5.

6.

7.

(b)(7)e

8.

9.

10.

11.

12.

13.

14.

15. (b)(7)e

16.

17.

18.

L. EPO #12: DEFINE GSM AND LIST THE FOUR SUBSYSTEMS REQUIRED FOR THIS STANDARD.

1. (b)(7)e

2.

3.

4.

5.

6.

(b)(7)e

7.

8.

9.

10.

11.

12.

(b)(7)e

13.

14.

15.

16.

(b)(7)e

17.

18.

19.

20.

(b)(7)e

21.

22.

23.

24.

(b)(7)e

25.

M. EPO 13: DEFINE SIM CARD AND THE INFORMATION THAT IS STORED THERE.

1.

2.

(b)(7)e

(b)(7)e

N. EPO #14: DEFINE *I*DEN AND LIST THE TWO TYPES OF HLRS AND VLRS.

1.

2.

3.

4.

5.

(b)(7)e

6.

7.

(b)(7)e

8.

9.

10.

O. EPO # 15: DEFINE PCS AND LIST THE TWO TYPES OF SERVICES PROVIDED BY THESE WIRELESS NETWORKS.

1.

2.

3.

4. (b)(7)e

5.

6.

7.

8.

9.

10.

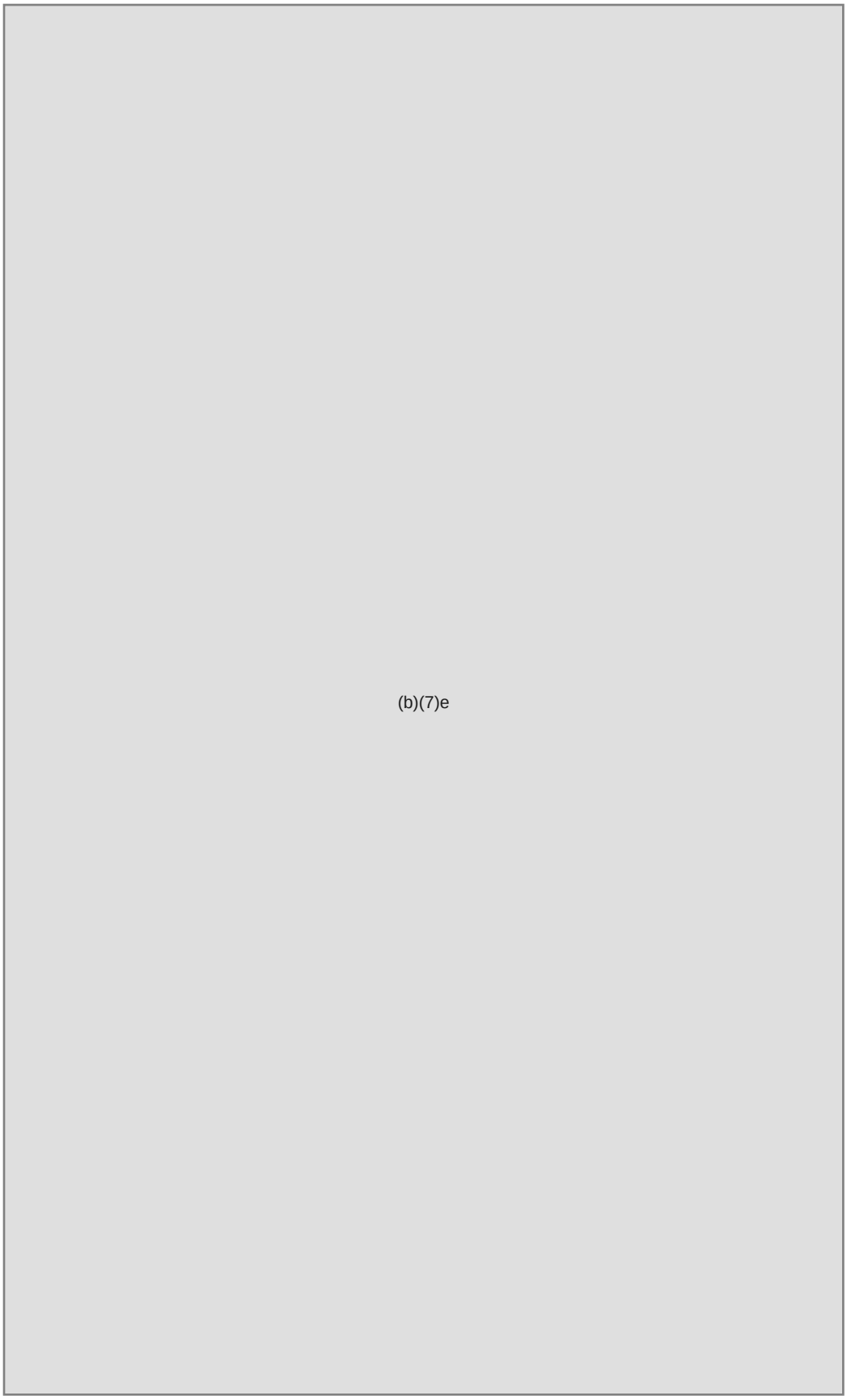
11. (b)(7)e

P. EPO#16: DEFINE "CALL DETAIL REPORTS" AND IDENTIFY HOW THEY ARE ACQUIRED.

1. (b)(7)e
2.
3.
4.
5.
6.
7.

Q. EPO#17: DEFINE THE TERM "CELL PHONE MAPPING" AND USE APPROPRIATE MAPPING TECHNIQUES TO DETERMINE SUBJECT LOCATIONS AT SPECIFIC DATES AND TIMES.

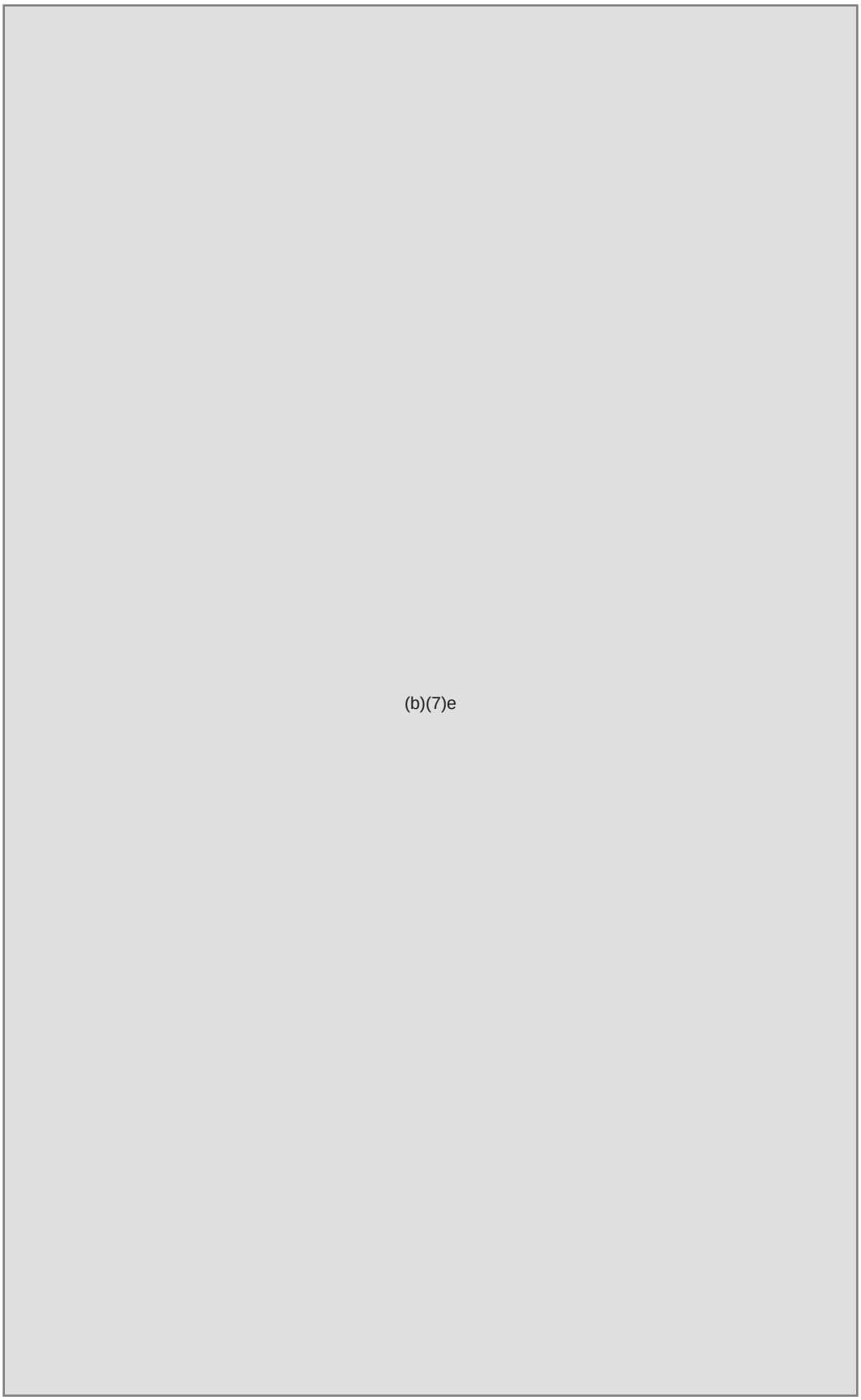
(b)(7)e

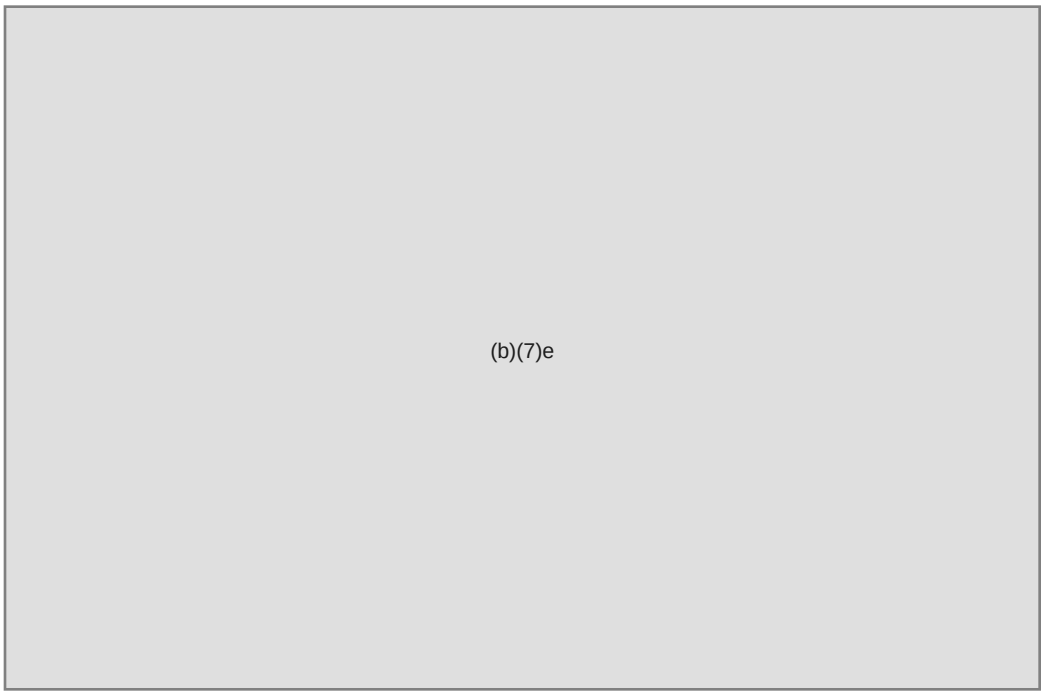

(b)(7)e

(b)(7)e

R. EPO#18: DEFINE THE TERM "CELL PHONE TRACKING" AND DESCRIBE APPROPRIATE TRACKING TECHNIQUES TO LOCATE AN INVESTIGATIVE SUBJECT IN REAL-TIME.

(b)(7)e


(b)(7)e



8. Some situations in which tracking might be appropriate:
    a. Child abductions;
    b. Kidnapping;
    c. immediate location of an investigative subject (example: drug buy operation);
    d. Determining real-time locations of subject as he/she moves from place to place.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

EPO #1: Identify significant evolutionary milestones in communications technology that have contributed to the current status of the cellular communications industry.

EPO #2: Describe the technology involved in cellular phone communications.

EPO #3: EPO #3: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

EPO #4: Define Call Handoff and list the locations where evidentiary artifacts are stored.

EPO #5 Define the Hexagon Grid and its importance to the Cellular Network.

EPO #6: List the five main components of a wireless network and their responsibilities.

EPO #7: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

EPO #8: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

EPO #9: List the administrative task of the Control Channel.

EPO #10: Define TDMA and list TDMAs advantages.

EPO #11: Define CDMA and list how its signals are spread.

EPO #12: Define GSM and list the four subsystems required for this standard.

EPO #13: Define SIM Card and the information that is stored there.

EPO #14: Define *i*DEN and list the two types of HLRs and VLRs.

EPO #15: Define PCS and list the two types of services provided by these wireless networks.

EPO #16: Define “Call detail Reports” and identify how they are acquired.

EPO #17: Define the term “cell phone mapping” and use appropriate mapping techniques to determine subject locations at specific dates and times.

EPO #18: Define the term “cell phone tracking” and describe appropriate tracking techniques to locate an investigative subject in real-time.

B. REVIEW OF TEACHING POINTS

Based on information learned about cell technology, call detail records and mapping techniques, students participate in a final written/practical exercise. Prior to this exercise, cell phones are prepared with a data set that follows a given scenario. Each student is required to examine one of those devices and utilize the associated call detail records to map the suspect’s movements, through call history, and answer questions related to the scenario.

IV. APPLICATION

A. LABORATORY

None

B. PRACTICAL EXERCISE

This graded practical exercise requires 4 hours to complete. The elements of the PE are thoroughly documented in the Attachments section.

REFERENCES

Bedell, Paul. (2001). *Wireless Crash Course.* McGraw Hill: New York

Brain, M., Layton, J., & Tyson, J. (2000). *How Cell Phones Work*. Retrieved from http://electronics.howstuffworks.com/cell-phone.htm

Cellular Technology Industry Association. (n.d). *Wireless 101*. Retrieved from http://www.ctia.org/consumer_info/service/index.cfm/AID/10319

Stetz, Penelope. (2002). *The Cell Phone Handbook, 2nd Ed*. FindTech, Ltd.: Cleveland, OH

Wikipedia. (2005) *History of Mobile Phones*. Retrieved from http://en.wikipedia.org/wiki/History_of_mobile_phones

BIBLIOGRAPHY

ATTACHMENTS

1. Student Written Practical
2. Written Practical
3. Dung Mapping PE