U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING OPERATIONS

TECHNICAL OPERATIONS DIVISION

Homeland Security

LESSON PLAN

HOW CELL PHONES WORK

3259 **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: (MAY/08)

(b)(6) **nior Instructor, CFI (Team Leader)**
, Senior Instructor, CFI
r Instructor, CFI

REVIEWED BY: (JUL/09)

(b)(6) **, Senior Instructor, Technical Operations Division (Team**

(b)(6) Program Specialist, Technical Operations Division

LP updated as follows:

Division Title changed from CFI to TOD, and FOUO/LES markings added.

There were no changes to the TPO or EPOs

(Template Revised SEP/10)

REVIEWED BY: (SEP/10)

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

TABLE OF CONTENTS

SYLLABUS

COURSE TITLE: **HOW CELL PHONES WORK**

COURSE NUMBER: **3259**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OPTION
1.5			1.5	MDIP	

DESCRIPTION:

Cell phone investigators can, if not careful, be overwhelmed by the intimidating technology of cellular phones. Cellular technology provides to law enforcement valuable tools, such as mapping, tracking, call detail reports, and other evidentiary tools. However, before these tools can be applied the investigator must have an understanding of what they are, why they exist, and how they are evolved or created. While this course does not purport to provide an exhaustive discussion of cellular technology, it does provides all the law enforcement officer needs to know about the technology in order to effectively perform his or her investigative tasks.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given a potential investigative scenario involving cellular telephones, the learner will apply cellular technology in order to successfully complete the assigned investigation.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Describe the technology involved in cellular phone communications.

EPO #2: Identify ways in which cellular technology can assist in criminal investigations.

STUDENT SPECIAL REQUIREMENTS:

None

METHOD OF EVALUATION:

Completion of course

INSTRUCTOR GUIDE

METHODOLOGIES:

1. Lecture with questions
2. Discussion

TRAINING AIDS/EQUIPMENT:

1. Instructor:
   a. Computer with PowerPoint and projector.
   b. Writing surface.
2. Student:
   None

INSTRUCTOR SPECIAL REQUIREMENTS:

Comprehensive understanding of cellular technology.

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

1. Cellular technology is relatively new, having inundating contemporary American (and world) culture within the past decade. However, with the flood of cell phones, law enforcement is confronted with new tools of criminal activity and, as well, new investigative tools.

2. Law enforcement largely ignorant of the tremendous investigative assets that accompanies cell phone technology. MDIP addresses that lack by presenting to the journey level law enforcement officer an understanding of this new technology and its investigative benefits.

3. In order to fully understand and apply the investigative tools provided by cellular technology, the officer needs to have a basic understanding of the technology. While this course does not provide an exhaustive discussion of the overwhelming technology involved in cellular communications, it does provide enough material information so that law enforcement officers can understand and apply the technology to their benefit.

B. LESSON PLAN OVERVIEW

1. Terminal performance objective (TPO)

   Given a potential investigative scenario involving cellular telephones, the learner will apply cellular technology in order to successfully complete the assigned investigation.

2. ENABLING PERFORMANCE OBJECTIVES (EPO)

   a. EPO#1: Describe the technology involved in cellular phone communications.

   b. EPO#2: Identify ways in which cellular technology can assist in criminal investigations.

II. PRESENTATION

A. EPO#1: 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.

Note: A more thorough discussion of multiplexing technology and how it relates to cell phone forensics is presented in the MDIP course “Cell Phone Technologies”

B. EPO#2: IDENTIFY WAYS IN WHICH CELLULAR TECHNOLOGY CAN ASSIST IN CRIMINAL INVESTIGATIONS.

1. There are several aspects of cell technology that, a knowledge of which, can benefit law enforcement. First, there is the concept of “cell registration”. When a user powers on their cell phone, a signal is sent (via cell tower) to the nearest MTSO which reads the users:

    a. ESN (Electronic Serial Number): The ESN is a unique 48-bit identifier (typically represented in Hex Code) for each individual cell phone. The user’s CSP has correlated the proper ESP for each subscriber.

b. SID (System Identification): The SID is a unique code identifying both the CSP and the assigned geographical area.

c. MIN (Mobile Identification Number): This is the 10-digit assigned telephone number to that single cell phone.

2. This information, along with the cell tower identification number, is forwarded to the cell phones CSP. Within the computer network of the CSP is a very dynamic database called the Home Location Registry (HLR). It keeps track of all local subscribers to the CSP and in what cell they are currently located.

3. Thereafter, if anyone calls the subscriber, the CSP knows exactly which cell to forward the call. As a subscriber moves from cell to cell the HLR is immediately updated to keep track of the subscriber's (or at least the phone's) physical location.

   It is safe to say that any time a subscriber has their cell phone powered on, the CSP knows in what cell they are physically located. In crisis management, or other emergency situations, this information may prove invaluable.

4. If the cell phone user is roaming, the current owner of the local cell service maintains a record of the user's cell location in a dynamic database called the Visitor Location Registry (VLR). This is primarily so that the user's CSP can be properly charged for any cell phone use while roaming.

5. A word about roaming. A subscriber is assigned service in a single geographical area (note: refer to the course "History of Cell Technology" for a discussion of Metropolitan Service Areas and Rural Service Areas. There are 734 such Geographical Markets - and several more PCS Service Areas - in the U.S.). When a user is outside their assigned service area, they are "roaming". They may be roaming within an area serviced by their own CSP, or they may be roaming in an area serviced by a competing CSP. To the user the difference is transparent, but it may be relevant for billing purposes as the non-subscriber CSP charges the originating CSP for roaming fees. These fees will typically be passed on the subscriber.

6. A word about assigned telephone numbers. The CSP keeps track of two 10-digit phone numbers for each subscriber. The first is the MDN ("Mobile Device Identifier"); the other is the MIN ("Mobile Identification Number"). Here's how it works. When a customer approaches a CSP (example: Alltel) and requests a new cell service, the user is assigned a 10-digit phone number. At this time the MDN and MIN are identical. The MIN is the 'official' phone

number; the MDN is the number that friends and family will call to reach the subscriber. Suppose that a year later the subscriber decides to change CSP's, this time approaching Verizon for service. The customer desires to keep their Alltel-assigned phone number. Verizon will create a new account with a new MIN for the customer, but the MDN will remain the same.

a. The law enforcement officer should be careful when communicating with a CSP since there can arise confusion if the subject of the investigation has two different MIN/MDN's.

b. A web site www.primeris.com ("fonefinder" link) can provide the name of the CSP and geographical area for any MIN. However, fonefinder does not keep track if the MDN is a different number. Another web site www.neustar.com does provide records of ported phone numbers (generally referred to as the North American Numbering Plan Administration - NANPA. Although NeuStar is a paid site, it has free NANPA service for registered law enforcement officers. Officers can register at the web site.

7. CSP's can also provide beneficial, real-time, information to investigators because of the manner in which tower mapping is implemented. Every cell tower has an assigned number (more accurately, each cell to which the tower is central has a designation) and each tower is mapped by the CSP using GPS coordinates. In emergency situations the CSP can provide the current active cell and GPS coordinates of a powered on cell phone.

   As an example, a missing child with an active cell phone can be generally located by the CSP providing real-time data as to the current cell of communication. Further, the GSP can provide an estimate of the radius of the cell, allowing the location of the child's phone to be at least broadly identified.

8. Other than a general location provided by cell location, the technology of the cell industry can enable the investigator to further pinpoint a more precise location of the active cell phone. There are three types of cell towers, each providing unique and helpful location information for the queried cell phone:

   a. Omni-directional towers. These towers, relatively rare and found most frequently in very rural locations (southwest deserts, pacific mountains, etc.), transmit and receive throughout the entire 360-degree range of the cell.

   b. Far more common is the three-sectored tower. It is triangular in shape (with one leg of the triangle invariably positioned to

true north) and allots its 56 channels to each of three legs of the triangle (there are three sets of transceivers on the triangular tower). The CSP can provide to the investigator the channel number assigned to the active cell phone and also determine which of the three 120-degree sectors the active cell phone is in. Since the CSP also can read the amount of power being transmitted by the active cell phone, a rough determination can be made as to how far from the tower the cell phone is located. All considered, the CSP can narrow the location of the active cell phone down to an area less than 10% the size of the cell.

c. Becoming more familiar (although still relatively limited in number) is the six-sectored tower. With these, the channels are distributed across six sectors (instead of the previously discussed three) with each sector corresponding to a 60-degree portion of the cell.

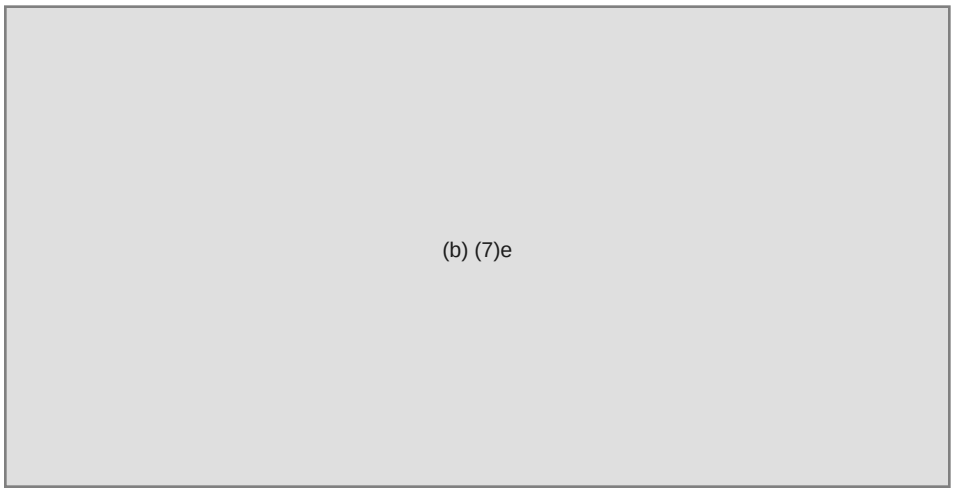
9. In a real-time crisis situation (such as the abducted child scenario mentioned above), the investigator, working with the CSP law enforcement liaison officer, can track the movement of a cell phone as it moves from sector to sector (within a cell) or from cell to cell. By tracking this data and plotting it on a map, direction of travel can be determined and perhaps an anticipation of where the subject will be at some future identified time.

10. The process of cell phone contacting the nearest tower to report status, identity and location is called “registration” (in cell jargon: “pinging”). An active cell phone will ping the nearest tower every seven-to-nine minutes. However, a CSP can ping a cell phone from the MTSO console at any time without waiting for the phone’s automatic (and infrequent) registration.

11. The scenarios identified above, involving the real-time tracking of an active cell phone is imprecise, with only geographic generalities provided. However, these general locations provided by tower, sector, and power meter can be very helpful. When exact location is required, the cell industry has an appropriate tool call “Stingray” and works on the principal of signal triangulation.

a.

b. (b) (7)e

c. 

12. Another useful investigative benefit of cell phones is the ability to map historical cell phone data. Consider this scenario: a Letter of Preservation is delivered to the CSP for a subject cell phone (example: investigators desire to map the physical movement of a subject). The letter will request the CSP retain for a specific time period all cell data for the subject's phone including tower identification of all calls and registrations (note: tower data for registrations are typically not retained by the CSP). When the requested data is delivered (per subpoena), the investigators have:

    a. A record of all cell communications during the date range including tower-specific tower (with GPS coordinates);

    b. A record of subject phone pings (also with GPS coordinates).

13. Given this information, the investigator may be able to identify the general physical location of the Subject at specific points in time.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

EPO #1: Describe the technology involved in cellular phone communications.

EPO #2: Identify ways in which cellular technology can assist in criminal investigations.

B. REVIEW OF TEACHING POINTS

1. An understanding of cell phone technology opens many doors for t he savvy criminal investigator that were hitherto unavailable.

2. With an understanding of cell phone technology, the investigator can work more effectively with the Cell Service Provider (CSP), the

maintainer of valuable records.

3. Using appropriate (and free) web sites, the officer can determine, when a cell number is provided, the CSP and the geographical region of subscription.

4. Understanding cell phone technology leads to the application of several helpful investigative tools:

   a. The ability to locate an active cell phone (and, presumably, the owner of the cell phone);

   b. The ability to passively map the physical location of a cell phone over a defined period of time;

   c. Using triangulation, and appropriate legal authority, the ability to precisely locate, in real-time the subject cell phone.

IV. APPLICATION

A. LABORATORY

NONE

B. PRACTICAL EXERCISE

NONE

REFERENCES

Stetz, Penelope; The Cell Phone Handbook; 2nd Ed.; FindTech, Ltd.; Cleveland, OH; 2002.

Bedell, Paul; Wireless Crash Course; McGraw Hill; New York; 2001.

Layton, Julia, Marshall Brain and Jeff Tyson. "How Cell Phones Work." 14 November 2000. HowStuffWorks.com. <http://electronics.howstuffworks.com/cell-phone.htm> 03 April 2008.

Unaccredited article. “Wireless 101”; 19 May, 2008. Cellular Technology Industry Association. http://www.ctia.org/consumer_info/service/index.cfm/AID/10319.

Unaccredited article. “History of Mobile Phones.” 14 April 2005. WikipediA. <http://en.wikipedia.org/wiki/History_of_mobile_phones> 05 April 2008.

“Fone Finder”; www.primeris.com; Primeris Corporation; 19 May, 2008.

“North American Numbering Plan Administration (NANPA)”; www.neustar.com; NeuStar Corporation; 19 May, 2008 (specifically “law enforcement administration”).

BIBLIOGRAPHY

None

ATTACHMENTS

None