

U.S. DEPARTMENT OF HOMELAND SECURITY
FEDERAL LAW ENFORCEMENT TRAINING CENTER
OFFICE OF TRAINING OPERATIONS
TECHNICAL OPERATIONS DIVISION



Homeland Security

LESSON PLAN

CELL PHONE INVESTIGATIONS

3001

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/06)

(b)(6)

, Senior Instructor, CFI (Team Leader)
Instructor, CFI
Instructor, CFI

REVISED BY: (Mar/07)

(b)(6)

Senior Instructor, CFI (Team Leader)
ces; cosmetic and editorial changes)

CFI changed to TOD January 2009
(Template Revised SEP/10)

REVIEWED BY: (SEP/10)

(b)(6)

Branch Chief, TOD

TABLE OF CONTENTS

SYLLABUS.....	1
INSTRUCTOR GUIDE	2
OUTLINE OF INSTRUCTION	3
I. INTRODUCTION.....	3
A. RAPPORT AND OPENING STATEMENT.....	3
B. LESSON PLAN OVERVIEW.....	4
II. PRESENTATION.....	4
A. EPO #1: IDENTIFY ASPECTS AND FEATURES OF CELL PHONE TECHNOLOGY AS THEY RELATE TO LAW ENFORCEMENT APPLICATIONS.....	4
B. EPO #2: IDENTIFY THE TYPES OF EVIDENCE LIKELY TO BE RECOVERED FROM A SEIZED CELL PHONE.....	7
C. EPO #3: IDENTIFY THE FOUR CRITICAL RULES OF CELL PHONE SEIZURE AND ANALYSIS.....	8
D. EPO #4: IDENTIFY HARDWARE AND SOFTWARE TOOLS NECESSARY FOR IMAGING AND ANALYZING CELL PHONES.....	10
E. EPO #5: IDENTIFY FEDERAL STATUTES WHICH MAY INFLUENCE THE LAWFUL SEIZURE AND ANALYSIS OF CELL PHONES.....	11
F. EPO #6: IDENTIFY OR DEMONSTRATE THE PROCESS OF ACQUIRING AND ANALYZING CELL PHONE DATA.....	14
III. SUMMARY	15
A. REVIEW OF PERFORMANCE OBJECTIVES.....	15
B. REVIEW OF TEACHING POINTS.....	15
IV. APPLICATION.....	15
A. LABORATORY	15
B. PRACTICAL EXERCISE.....	15
REFERENCES.....	A
BIBLIOGRAPHY	B
ATTACHMENTS	C

~~FOR OFFICIAL USE ONLY~~

LAW ENFORCEMENT SENSITIVE

SYLLABUS

COURSE TITLE: CELL PHONE INVESTIGATIONS

COURSE NUMBER: 3001

COURSE DATE: SEP/10

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OPTION
2	0		2	FRDE	#1 - #5

DESCRIPTION:

Cell telephones are among the most ubiquitous electronic communications devices and certainly the most frequently encountered portable electronic device. They will be encountered at most crime scenes and during the execution of many search warrants. A great potential exists for encountering valuable evidence on a cell phone. This course discusses the types of evidence likely to be recovered from cell phones and the proper technique for cell phone seizure and subsequent data analysis.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given an investigative scenario relating to the seizure of digital evidence, the officer will demonstrate the ability to seize, transport and store a cell phone in such a way as to preserve evidentiary integrity.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Identify aspects and features of cell phone technology as they relate to law enforcement applications.

EPO #2: Identify the types of evidence likely to be recovered from a seized cell phone.

EPO #3: Identify the four critical rules of cell phone seizure and analysis.

EPO #4: Identify hardware and software tools necessary for imaging and analyzing cell phones.

EPO #5: Identify Federal statutes which may influence the lawful seizure and analysis of cell phones.

EPO #6: Identify or demonstrate the process of acquiring and analyzing cell phone data.

STUDENT SPECIAL REQUIREMENTS:

There are no special requirements.

METHOD OF EVALUATION: Graded Practical Exercise (FRDE: Course #3002)

~~FOR OFFICIAL USE ONLY~~

LAW ENFORCEMENT SENSITIVE

INSTRUCTOR GUIDE

METHODOLOGIES:

- Lecture with questions
- Discussion
- Demonstration

TRAINING AIDS/EQUIPMENT:

1. Instructor:
 - a. Cell phone seizure hardware kit (including cabling and charger);
 - b. Demonstration cell phone(s);
 - c. Cell phone seizure software;
 - d. Shielded Faraday (“stronghold”) bag.
2. Student:
 - Shielded Faraday (“stronghold”) bag.

INSTRUCTOR SPECIAL REQUIREMENTS:

There are no special requirements

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

1. Never in the history of civilization has any gadget become so quickly instilled as part of the culture as has cell telephones. Though the technology (in its current incarnation) is barely a decade old, cell phones are globally ubiquitous. According to the Washington Post (July 28, 2005), there are over 190 million cell phone service subscriptions in the United States, representing fully one-half of the population. When one subtracts the number of pre-adolescents and geriatrics from the population, then it can safely be said that “almost everyone” has a cell phone.
2. In spite of these statistics, law enforcement has been largely remiss in incorporating cell phone technology into its standard library of enforcement procedures.
3. Typically, a cell phone is far more than a voice communications instrument. It is a compact personal storage device for a wide array of data and information. Rightfully, the cell phone should always be considered as evidence when making an arrest or when executing a search warrant.
4. In 2006 a police officer in Washington State acquired a cell phone during the course of an investigation. Having never received training on proper cell phone seizure and transportation, the officer sent the unprotected phone to the crime lab for further analysis. The lab analyst found no data on the cell phone. Later it was determined that the suspect had immediately after the seizure called his cell provider (T-Mobile), and reported his phone stolen. T-Mobile then remotely deleted all data from the seized phone – prior to its arrival at the crime lab. Had the officer been aware of the rules for handling seized cell phones this potentially valuable evidence would not have been destroyed.
5. In another investigation, the Los Angeles Police Department found a dead body in a dumpster in a city back alley. The body had a cell phone which was recovered and sent to a crime lab for analysis. Analysts found the cell phone to contain a digital appointment calendar indicating the victim was to meet a named associate near the back alley on the evening of his death. An arrest for murder was affected within 24 hours of finding the body, based on evidence recovered from the cell phone.

6. This course discusses the types of evidence which may be recovered from a cell phone and the proper procedures for seizing, transporting, and storing cellular telephones.

B. LESSON PLAN OVERVIEW

1. Terminal Performance Objective (TPO)

Given an investigative scenario relating to the seizure of digital evidence, the officer will demonstrate the ability to seize, transport and store a cell phone in such a way as to preserve evidentiary integrity.

2. Enabling Performance Objectives (EPO)

EPO #1: Identify aspects and features of cell phone technology as they relate to law enforcement applications.

EPO #2: Identify the types of evidence likely to be recovered from a seized cell phone.

EPO #3: Identify the four critical rules of cell phone seizure and analysis.

EPO #4: Identify hardware and software tools necessary for imaging and analyzing cell phones.

EPO #5: Identify Federal statutes which may influence the lawful seizure and analysis of cell phones.

EPO #6: Identify or demonstrate the process of acquiring and analyzing cell phone data.

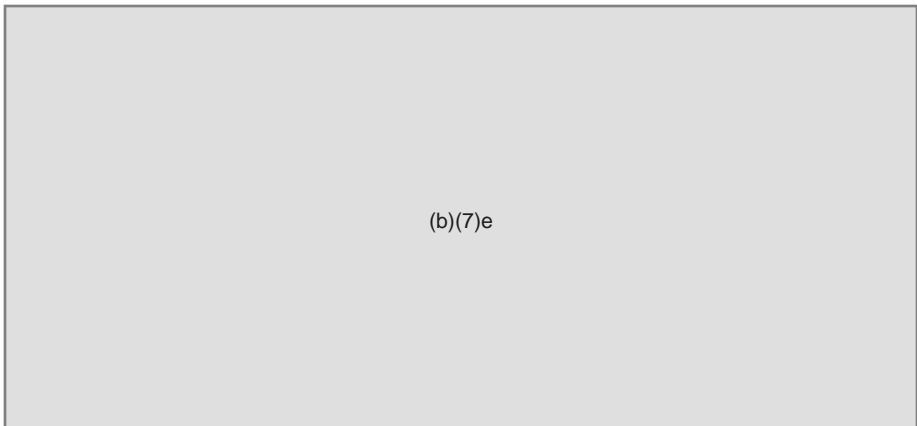
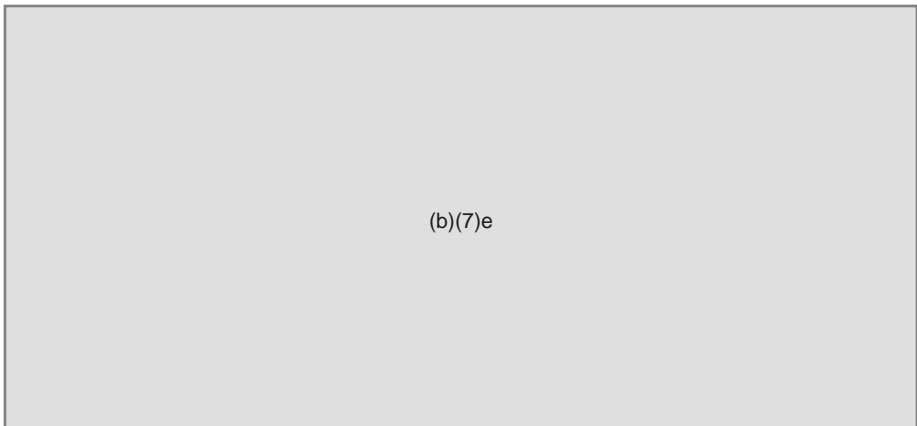
II. PRESENTATION

A. EPO #1: IDENTIFY ASPECTS AND FEATURES OF CELL PHONE TECHNOLOGY AS THEY RELATE TO LAW ENFORCEMENT APPLICATIONS.

1. Cell phones are, at their most fundamental level, two-way radios, granted, very sophisticated radios. They differ from simpler radios in a few ways:
 - a. A walkie-talkie has one channel and can communicate wirelessly over a distance of about a mile.
 - b. A CB radio has 40 channels and can communicate over a distance of about 5 miles.

- c. A cell phone has a minimum of 1,664 channels and communicates with a cell tower typically less than 10 miles away. Individual calls are bounced from tower to tower.
 - 1) The geographical area surrounding a tower is called a “cell”. Communications providers try to erect towers (thus, defining cells) in such locations so that all cell phone users are within communications range of a tower.
 - a) If there is no tower within reach of a cell phone, the cell phone is said to be in a “dead spot” and out of communications range.
- d. Because of FCC frequency allocations, each cell can handle about 56 different simultaneous phone calls of analog messages.
- e. The “First Generation” cell service was deployed with the Advanced Mobile Phone Service (AMPS) and used Frequency Division Multiple Access (FDMA) to deliver analog signals.
- f. Digital technology came about in the “Second Generation”. There are several Second Generation technologies:
 - 1) TDMA: (Time Division Multiple Access). Number of users per cell is triple that of analog cells. TDMA is “voice only”; no text messaging, internet browsing, photo or file transfer. TDMA was “state of the art” from the early 1990’s to the late ‘90’s.
 - 2) CDMA: (Code Division Multiple Access). Since several different calls can be multiplexed over a single channel, there is no finite number of calls that can be simultaneously carried in each cell. CDMA can also handle text messaging, file transfers, and Internet interaction.
 - 3) GSM: (Global System for Mobile Communications). An international standard used in 168 countries (including US).
 - a) GSM allows for international roaming.
 - b) The single most visible feature of a GSM phone is that it uses a SIM memory chip for all cell phone storage.

- c) Changing GSM phones is as simple as taking the chip out of one phone and inserting it the other.
 - g. 3rd generation technology introduced faster speeds and greater multimedia support.
 - h. 4th generation technology or 4G is the era of IP packet switched networks.
 - 2. A cell phone network has the following components:
 - a. A transmitting/receiving cell phone.
 - b. A cell phone tower.
 - 1) This receives the incoming call, changes the frequency, and retransmits it – either to another transceiving tower or, eventually, to a base station.
 - c. The base station is called an “MTSO” (Mobile Telephone Switching Office).
 - 1) Each cell phone service provider will have a single MTSO in each “home” area.
 - 2) If the incoming call is to another cell the MTSO routes the call appropriately through the cell network (to another MTSO).
 - 3) If the incoming call is to a “land-line”, the MTSO routes it to a “PSTN” (Public Switched Telephone Network). The PSTN is the local land-based phone company (BellSouth, Qwest, etc.).
 - 3. Cell Phone Acronyms that all law enforcement officers should know:

- a. 
- b. 
- c. 

(b)(7)e

4. The officer should also be aware that the MTSO maintains a “real-time” database of all locally assigned cell phones and the identification of the cell in which the phone is currently located.

a.

b.

(b)(7)e

B. EPO #2: IDENTIFY THE TYPES OF EVIDENCE LIKELY TO BE RECOVERED FROM A SEIZED CELL PHONE.

1. The cell phone industry applies a variety of technologies and an even wider variety of integrated cell phone capabilities. Any or all of the following may be found on a functioning cell phone.

a.

b.

(b)(7)e

c.

d.

- e. Contact lists
 - 1) Includes names, aliases, phone numbers for work, residence, cells, fax, email addresses, etc.
 - f. Memos (constructed personal messages).
 - g. To-Do Lists
 - h. Personal Calendar/Appointments.
 - i. Internet web pages.
2. Modern cell phones are truly hybrid electronic devices. For under \$300, a user can purchase a cell phone with a built-in digital camera (85% of all cell phones purchased now have integrated cameras), Internet browsing software, MP3 Player potential, a text messaging keyboard, and a gaggle of other gadgets.
3. In addition to the evidence stored internally on a cell phone, the cell phone provider can potentially provide a wealth of other evidence relating to cell phone subscribers. Different legal authority is required depending on the type of evidence desired.
- a. Customer name and billing address.
 - b. User name and account for on-line support.
 - c. Billing account details.
 - d. Other subscriber phone numbers.
 - e. Call logs, including cell origination, destination, times and duration.

C. EPO #3: IDENTIFY THE FOUR CRITICAL RULES OF CELL PHONE SEIZURE AND ANALYSIS.

1.



2.

3.

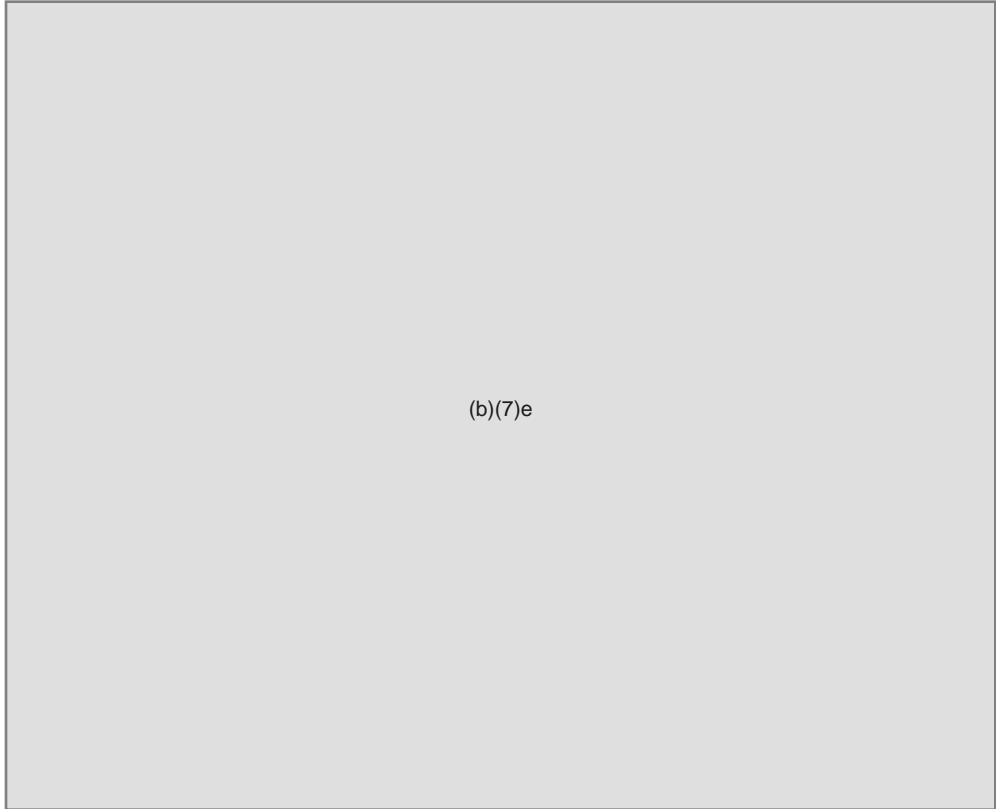
4.

(b)(7)e

D. EPO #4: IDENTIFY HARDWARE AND SOFTWARE TOOLS NECESSARY FOR IMAGING AND ANALYZING CELL PHONES.

1. Acquiring cell phone data in a useful and legal manner requires a few tools in addition to a standard personal computer.

2.



(b)(7)e

a) File format for most software tools is HTML and can be viewed after downloading with an Internet browser.

2) Single-purpose software can be acquired from the cell phone manufacturer for a cost of about \$30.

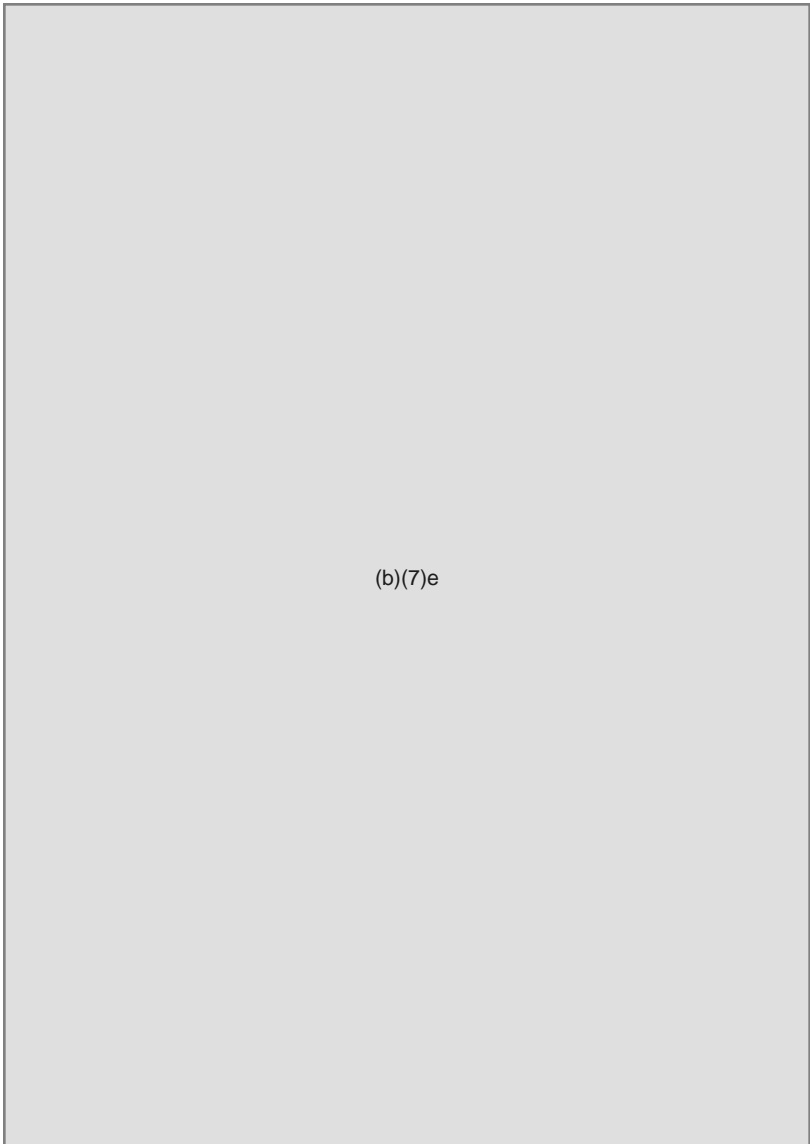
3) Universal software that works with most cell phone models is also available from a limited number of manufacturers.

c. Cell phone forensics hardware and software providers.

1) The two most commonly used providers of cell



(b)(7)e



(b)(7)e

E. EPO #5: IDENTIFY FEDERAL STATUTES WHICH MAY INFLUENCE THE LAWFUL SEIZURE AND ANALYSIS OF CELL PHONES.

1. The traditional laws and procedures relating to search and seizure are not enough when seizing cell phones. At least two additional statutes may come into play at one time or another and will impact the legality of cell phone investigations. They are discussed here.
2. Wiretapping Statutes (aka: Title III of the Omnibus Crime Control and Safe Streets Act of 1969): 18 U.S.C. 2510 – 2520.

Pages 15 through 17 redacted for the following reasons:

(b)(7)e



4.

(b)(7)e

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

EPO #1: Identify aspects and features of cell phone technology as they relate to law enforcement applications.

EPO #2: Identify the types of evidence likely to be recovered from a seized cell phone.

EPO #3: Identify the four critical rules of cell phone seizure and analysis.

EPO #4: Identify hardware and software tools necessary for imaging and analyzing cell phones.

EPO #5: Identify Federal statutes which may influence the lawful seizure and analysis of cell phones.

EPO #6: Identify or demonstrate the process of acquiring and analyzing cell phone data.

B. REVIEW OF TEACHING POINTS

1. Cell phones have a dynamic impact on our culture and on the actions of law enforcement officer. Any failure to consider cell phones during the act of enforcing an arrest or during the execution of a search warrant is a serious shortcoming.
2. Cell phones can be a rich source of evidence during the course of an investigation. However, proper seizure requires the following of stringent procedural and legal guidelines.

IV. APPLICATION

A. LABORATORY

1. NONE.

B. PRACTICAL EXERCISE

1. NONE.

REFERENCES

"How Cell Phones Work". <http://www.howstuffworks.com/cell-phone.htm>. Sep. 2006

National Public Radio; "Surveillance Via Cell Phones";
<http://www.npr.org/templates/story/story.php?storyId=5053410>; Dec. 14, 2005.

"Cell Seizures" ; Unpublished Training Manual ; Paraben Corporation ; Orem, UT; 2006.

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (July 2002 (Amended)); U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS); <http://www.cybercrime.gov/s&smanual2002.htm>; (Current as of Sept. 2006).

"Mobile Phones"; Wikipedia ; http://en.wikipedia.org/wiki/Mobile_phone. 2006.

Grant, August E. and Meadows, Jennifer H.; Communication Technology Update, Tenth Edition; Focal Press; 2006.

Bedell, Paul; Wireless Crash Course; McGraw-Hill; New York; 2006.

BIBLIOGRAPHY

None

ATTACHMENTS

1. PowerPoint Presentation.