U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING OPERATIONS

TECHNICAL OPERATIONS DIVISION

LESSON PLAN

CELLULAR FORENSIC SOFTWARE

3261 **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: (APR/08)

(b)(6) **nior Instructor, CFI (Team Leader)**
, Senior 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: **CELLULAR FORENSIC SOFTWARE**

COURSE NUMBER: **3261**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OPTION
6	11	2	19	MDIP	

DESCRIPTION:

The Investigator conducting a mobile device investigation will be confronted with a wide range of cellular file systems and devices. The use and understanding of Cellular Forensic Software is necessary for the Investigator to complete this task. In this block of instruction the Investigator will learn and demonstrate the ability to use Cellular Forensic Software.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given a scenario involving mobile devices in a criminal investigation the student will extract information using provided cellular forensic software programs in a manner that leads to evidentiary value.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Install the forensic software program on to an examination computer.

EPO #2: Install device drivers on an examination computer.

EPO #3: Locate and update system device drivers.

EPO #4: Extract and list data from the mobile device.

STUDENT SPECIAL REQUIREMENTS:

1. The student will install the forensic software programs supplied them.
2. The student will install the system device drivers supplied them.

METHOD OF EVALUATION:

1. Instructor led lab
2. Completion of a practical exercise

INSTRUCTOR GUIDE

METHODOLOGIES:

1. Lecture with questions
2. Discussion
3. Demonstration
4. Case study

TRAINING AIDS/EQUIPMENT:

1. Instructor:
    a. Computer with PowerPoint and projector.
    b. Writing surface.
    c. Forensic software programs
2. Student:
    a. Examination computer.
    b. Forensic software programs

INSTRUCTOR SPECIAL REQUIREMENTS:

1. Comprehensive and practical understanding of mobile device forensic software programs.
2. Comprehensive and practical experience installing and troubleshooting system device drivers.
3. Comprehensive and practical understanding of mobile device storage features.

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. One such benefit is the installation and use of cellular forensic software programs. These programs are designed to extract data that may be of evidentiary value from handheld and mobile devices that otherwise may not be available to the Investigator.
4. This block of instruction is designed to instruct the student in the proper installation and use of cellular forensic software, the proper installation of system device drivers, the troubleshooting of system device drivers and the extraction of data that may be of evidentiary value.

B. LESSON PLAN OVERVIEW

1. Terminal performance objective (TPO)

   Given a scenario involving mobile devices in a criminal investigation the student will extract information using provided cellular forensic software programs in a manner that leads to evidentiary value.

2. ENABLING PERFORMANCE OBJECTIVES (EPO)

   a. EPO #1: Install the forensic software program on to an examination computer.

   b. EPO #2: Install device drivers on an examination computer.

   c. EPO #3: Locate and update system device drivers.

   d. EPO #4: Extract and list data from the mobile device.

II. PRESENTATION

A. EPO #1: INSTALL THE FORENSIC SOFTWARE PROGRAM ON TO AN EXAMINATION COMPUTER.

1. Mobile and hand held cellular device investigations are on one hand unique, but in other respects no different than general computer forensic investigations. Any investigation that purports to have a forensic aspect must have certain field accepted methodologies and practices. This is also true of any tool used to produce a purported result.

2. There are a number of commercially available and Law Enforcement only tools available to the Investigator. In selecting these tools the Investigator should keep certain needs in mind, such as;

   a. Commercial or Law Enforcement Only tools.

      1) Commercially available tools produced by software manufacturer are available in a varying range of capability and price. These tools advertise a wide range of supported devices and claims of data extraction.

      2) Law Enforcement Only tools are forensic software tools generally produced by and distributed to members of the Law Enforcement community. Like its commercial counterpart they advertise a wide range of supported devices and claims of data extraction. These programs are generally restricted to sworn Law Enforcement Officers or those granted waivers as support members of the Law Enforcement community.

      3) Some of the more sophisticated commercially produced software products have versions that are sold only to the Law Enforcement community and other enterprise versions sold to companies and individuals.

   b. Forensic Software Tools system needs.

      Forensic software tools require different system attributes depending on the size of the program and program sophistication. All programs require minimum hard disk space and Random Access Memory or RAM sizes to properly function. Selecting a software program without the needed disk space or RAM size could result in degraded capabilities or software failure.

c. The ability to reliably report and reproduce findings.

1. After data extraction has been completed the software package should generate a report of its findings, detailing the physical location of the data. Along with the physical location some sort of digital fingerprint is preferable.

2. Testing should be conducted using the software package to ensure the results are not only verifiable but also re-producible. The software package should report the same results each time if it was used in the same manner and under the same conditions.

3. When installing forensic software tools on an examination computer the Investigator should not automatically accept the installation default settings. The examination computer must be configured in a way to segregate different cases and associated evidence files to ensure no cross contamination of the evidence files. This can be done by using separate hard disk or logical/extended hard disk partitions.

4. The Instructor will demonstrate and assist the students in the proper installation and configuration of the forensic software program(s).

NOTE**: Place notes to the instructor where appropriate for special guidance. This is an "outside border" with a 10% shading of gray. Shading does not have to be used but it helps if there is a border around the note to make it stand out and easy to read.**

B. EPO #2: INSTALL DEVICE DRIVERS ON AN EXAMINATION COMPUTER.

1. After installing the forensic software package on the examination computer the next step is to ensure that all device drivers are installed and up to date. Since there are hundreds if not thousands of different mobile and hand held device file systems available to users there are a like number of device drivers.

2. These device drivers ensure that proper connection and interaction between the examination computers operating system and the mobile or handheld device. Without the proper device drivers and system driver installed and updated there will likely be a communications failure between the device, the examination computer and forensic software program

3. Most operating systems in use today ie PC or Mac, allow the user access to system controls often called control panels. It is within this area the Investigator will check to ensure the drivers are installed properly and when needed updated.

4. Generally, forensic software programs are shipped with the latest device drivers supported by that version of the software. These drivers are usually installed on the installation disk within the setup folder in a sub folder titled “Drivers”. When the Investigator comes across a driver that is not included or located through the driver update function he should seek that device driver from the mobile or hand held device manufacturer.

5. The Instructor will now demonstrate and instruct the students in the proper method of installing device drivers, system drivers and searching manufacturer sites for device drivers.

C. EPO #3: LOCATE AND UPDATE SYSTEM DEVICE DRIVERS.

1. After installing forensic software and device driver and upon using these tools for the first the Investigator will most likely be prompted to update one or more device and system drivers. This occurs for a number of reasons. Some of which are;

   a. New devices such as the data transfer cables are being registered by the operating system for the first time.

   b. The mobile or hand held device has registered with the operating system but is unsure which of the drivers to use.

   c. A proper system or device driver for the mobile or hand held device cannot be located.

2. The Instructor will now lead the students in connecting a mobile or hand held device to the examination computer and assisting in the locating and updating of system and device drivers.

D. EPO #4: EXTRACT AND LIST DATA FROM THE MOBILE DEVICE.

1. Once the forensic software program and associated device drivers are installed the Investigator is ready to perform a forensic examination on the mobile or hand held device using agency approved principles, procedures and methodologies.

2. After a successful and secure device/system connection the Investigator can follow the forensic software programs extraction steps to obtain data.

3. After the Investigator has successfully completed the forensic examination the case should be secured in an agency accepted manner and a findings report generated.

4. The Instructor will demonstrate and lead the students in the extraction of data using the forensic software program and the examination computer.

5. If the student is unable to obtain a successful data extraction the Instructor should assist the student in troubleshooting possible causes. Some of the possible causes for failure include:

   a. The improper installation of the software program

   b. The lack of system requirements available on the examination computer

   c. The failure of the software to identify the data transfer cables and/or mobile or hand held device

   d. The lack of properly installed device or system drivers

6. The Instructor will furnish the students with mobile or hand held devices along with investigative scenarios to facilitate the learning process in a laboratory environment.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

EPO #1: Install the forensic software program on to an examination computer.

EPO #2: Install device drivers on an examination computer.

EPO #3: Locate and update system device drivers.

EPO #4: Extract and list data from the mobile device.

B. REVIEW OF TEACHING POINTS

1. Cellular Forensic Software is an important tool in the acquisition and investigation of crimes involving mobile and hand held devices. The well rounded investigator must understand the capabilities and limitation of the software programs.

2. Without proper training on the installation, operation and the resolution of technical issues involved with these programs the Investigator may lose valuable evidence thus leaving a criminal free to commit more crimes.

IV. APPLICATION

A. LABORATORY

1. The laboratory target audience will be students from the MDIP training and will consist of both scenario based laboratories and instructional laboratories.
2. The scenario based laboratories shall give the student a set of facts involving a simulated criminal investigation. The student will be supplied a list of evidentiary artifacts he/she shall attempt to located. The student will be supplied the corresponding mobile or hand held devices to complete the simulated investigation and extract the data. See Attachments 1 – 3.
3. The students will be supplied a number of different mobile and hand held devices and instructed in the proper methods to establish connection and data extraction. The Instructor will assist to the point necessary in the installing and updating of system and device drivers.

B. PRACTICAL EXERCISE

None

REFERENCES

None

BIBLIOGRAPHY

None

Pages 14 through 27 redacted for the following reasons:
- -
(b)(7)e

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed

Page to be removed