Crime Involving Handheld Computing Devices

—Course Overview—

LESSON 1: MOBILE TECHNOLOGY INTRODUCTION AND OVERVIEW

Overview: (6 learning modules)
The modules in this lesson will describe various handheld devices popular in society today. The course material will allow the student to identify a number of different handheld devices. The lessons will discuss the functionality and capabilities of various handheld devices. Additionally, the student will be made aware that there is a high probability of these devices being present due to their prevalence. The student will also be aware of the potential evidentiary value of the data stored on these handheld devices and the value of collecting these devices in criminal investigations.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Recognize a variety of handheld devices.
2. Articulate the need to collect these devices.
3. Identify potential evidence that may be contained on the handheld device based on the device’s functionality.

LESSON 2: OVERVIEW OF POTENTIAL CRIMES ASSOCIATED WITH HANDHELD DEVICES

Overview: (6 learning modules)
The modules in this lesson focus on reviewing actual law enforcement cases that were aided by digital evidence obtained from handheld devices. The student will walk through actual cases where data from handheld devices were instrumental to the investigation. These case studies will help the student apply the theoretical concepts of digital evidence to real life investigations.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Conduct investigations using data created by or stored on handheld devices.
2. Apply conceptual information about technology to real-world investigations.
3. Conduct evidence-gathering techniques based on data from handheld devices to ongoing investigations.

LESSON 3: LEGAL DOCUMENTS FOR OBTAINING INFORMATION

Overview: (3 learning modules)
The modules in this lesson introduce legal concepts pertaining to digital evidence on handheld devices. A review of the Fourth Amendment, search warrants, subpoenas, preservation orders, and other legal tools helpful to law enforcement in obtaining devices and data are covered. These lessons are intended to augment federal, state, and local laws and existing agency
policies and guidelines related to collecting information from or about handheld devices.

**Learning Objectives:**

By the end of this lesson, you should be able to:

1. Prepare proper legal documents to preserve, identify, and obtain information related to handheld devices.
2. Identify the location of the information related to the device.
3. Collect data from people involved in the investigation, third parties and providers of services, and other custodians of records related to the handheld device.

**LESSON 4: IDENTIFYING MOBILE DEVICES**

**Overview:** (4 learning modules)

This series of identifying mobile devices introduces the student to the various types of handheld devices, media form factors, and how they are essential in the collection of potential evidence. This training module block provides the introduction to handheld devices and their media, as well as their intricate part as linked evidence in completing the process of data storage, transmission, and essential functions of the associated devices.

**Learning Objectives:**

By the end of this lesson, you should be able to:

1. Recognize common types of phones and associated features.
2. Identify a phone’s make, model, operating system, and carrier.
3. Identify the types of evidence linked to a cell phone (e.g. removable media, SIM card, phone bill, network and cell tower usage data).

**LESSON 5: LINKED EVIDENCE AND SEIZURE**

**Overview:** (3 learning modules)

These modules will explore associated evidence with handheld devices beyond the actual device. The potential associated evidence includes paper documents, financial records, and network carrier records, as well as traditional evidence familiar to investigators. This lesson block will conclude with the best practice for seizing cell phones accompanied with an easy reference seizure flowchart.

**Learning Objectives:**

By the end of this lesson, you should be able to:

1. Describe the types of data held by a cell phone provider that will be valuable to an investigation and the means to acquire these data.
2. Describe the methods for accessing the data held by a service provider.
3. Identify the paper trail evidence connected to a cell phone device and user account.
4. Properly seize, document, transport, and store a cell phone connected to a criminal investigation.
5. Prevent a device from communicating with a cellular network using multiple methods.
LESSON 6: HOMICIDE CASE STUDY, PART I (5 LEARNING MODULES)

The first case study in our 3000 series describes a homicide case from Bucks County, PA. In this first section, we focus on the particulars of the case and the collection of the linked evidence that leads to the eventual prosecution of the suspect. We also incorporate modules that describe how wireless carriers manage networks, collect billing information, and operate cell phone towers, as this information is germane to the case and crucial in the investigatory process.

Learning Objectives:
By the end of this lesson, you should be able to:

1. Use appropriate language that should be included in search warrants, court orders, and preservation orders addressed to wireless carriers.
2. Explain the basic operational design of a cellular network and how cell sites function.
3. Identify carrier codes and other information that can help distinguish different cell phones and carriers.
4. Articulate how the suspect’s alibi from the case study may be validated or proven false using cell phone data.

LESSON 7: HOMICIDE CASE STUDY, PART II

Overview: (7 learning modules)

In the second portion of our Homicide case study, we explain how the call detail records provided by the cellular carrier were used to identify the location of the suspect and ultimately show the suspect was lying about his location at the time of the murder. Additional modules provide further information about how location-based information can be found on various handheld devices, and how enabling technologies such as Global Positioning Satellites (GPS) and Wi-Fi network information can also be used to locate individuals. The lesson concludes with a discussion of how some of those technologies might be used by investigators to locate persons of interest of other individuals involved in a police investigation if call detail records are not available.

Learning Objectives:
By the end of this lesson, you should be able to:

1. Explain how call detail records are generated by the carrier and why they have evidentiary value.
2. Describe how call detail records were used to disprove the suspect’s alibi in the case study.
3. Articulate how GPS works and the constraints and limitations of GPS.
4. Name specific applications commonly installed on handheld devices that can be used to derive location information of the user.
5. Explain, in general, how hotspots work and how they can provide location information to a user (or an investigator).
OPTIONAL: Exam for Certificate of Technical Competency in the Identification, Preservation, and Collection of Evidence Related to Handheld Devices

The optional exam is comprised of 50 questions that address the topics and content presented in Lessons 1-7. Students who score 80 or higher on the exam will receive a certificate issued by Drakontas LLC and BKForensics. Students who score less than 80 can retake the exam multiple times, as necessary, in order to achieve a passing score and receive a certificate. The certificate confirms the student's technical competency in the identification and seizure of handheld devices and in compliance with best practices and rules of evidence.

PLEASE NOTE: The exam must be taken in a single sitting. There are 50 questions on the exam. Please set the appropriate amount of time aside prior to starting. You may retake the exam at a later date if you do not earn a grade of 80 or above. Certificates, along with a list topics covered on the technical competency exam, will be sent electronically (via email) within five weeks of passing the exam.

LESSON 8: HANDHELD DEVICE OVERVIEW

Overview: (7 learning modules)

This lesson introduces you to the types of handheld device form factors and models that you are most likely to encounter in a criminal investigation. Additional modules in this lesson delve into the specifics of handheld platforms, including their operating systems and applications, in order to familiarize you with the devices, their features, user interfaces and related capabilities that you may find of interest in an investigation.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Identify the different types of handheld devices an investigator may encounter during an investigation.
2. Describe the features and applications found on handheld devices.
3. Articulate the evidentiary value of the capabilities offered by handheld devices.

LESSON 9: ENABLING TECHNOLOGIES

Overview: (8 learning modules)

This lesson introduces many of the features and their corresponding data typically found on handheld devices today. Additional modules address GPS and personal navigation mapping, operating systems, PAN and Bluetooth, cameras and EXIF data, USB connections, and removable media storage form factors. This lesson will assist you in understanding the features and capabilities handheld devices provide that may provide evidentiary information you can obtain and use during an investigation.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Describe the various types of features provided by handheld devices.
2. Demonstrate the data outputs these features produce and their utility to investigators.
3. Articulate the evidentiary value of the features offered by handheld devices.

LESSON 10: NETWORKING TECHNOLOGIES

Overview: (5 learning modules)
This lesson introduces the technical aspects of handheld devices, including the types of carrier networks and codes used to identify handheld devices. Additional modules in this lesson describe the various methods and technologies handheld devices use to connect to networks and to exchange voice and data traffic, and the linked evidence collected by carrier networks.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Describe the different types of carrier networks used by handheld devices.
2. Identify the types of codes and the locations of each on handheld devices.
3. Describe the technologies used by handheld devices to connect to a network.
4. Articulate the linked evidence offered by carrier networks and the utility of call detail records.

LESSON 11: ADVANCED CRIMINAL JUSTICE ISSUES

Overview:
This lesson is comprised of a variety of learning modules and covers emerging criminal justice issues in society today. This lesson, which will be updated regularly with new materials, will assist law enforcement in understanding the types of emerging criminal justice issues that involve handheld devices and how these devices are being used to commit criminal activities.

Learning Objectives:
By the end of this lesson, you should be able to:
1. Articulate emerging criminal justice issues with respect to handheld technologies and crime.
2. Describe the different methods in which handheld devices are used to commit or facilitate crimes.
3. Communicate the potential sources of linked evidence as they relate to these emerging criminal justice issues.

This course was developed by Drakontas, in partnership with Drexel University and BKForensics. The U.S. Department of Justice Bureau of Justice Assistance sponsored the project under Award # 2011-BE-BX-K001.