

Specialized Investigators’ Basic Course Workbook Series Student Materials

**Learning Domain 63
Computers and Computer Crimes
Version Two**

**Basic Course Workbook Series
Student Materials
Learning Domain 63
Computers and Computer Crimes
Version Two**

© Copyright 2007
California Commission on Peace Officer Standards and Training (POST)
All rights reserved.

Published June 2002
Published July 2007

This publication may not be reproduced, in whole or in part, in any form or by any means electronic or mechanical or by any information storage and retrieval system now known or hereafter invented, without prior written permission of the California Commission on Peace Officer Standards and Training, with the following exception:

California law enforcement or dispatch agencies in the POST program, POST-certified training presenters, and presenters and students of the California basic course instructional system are allowed to copy this publication for non-commercial use.

All other individuals, private businesses and corporations, public and private agencies and colleges, professional associations, and non-POST law enforcement agencies in-state or out-of-state may purchase copies of this publication, at cost, from POST as listed below:

From POST's Web Site:
www.post.ca.gov
Go to Ordering Student Workbooks

POST COMMISSIONERS

John Avila	Narcotics Detective Fresno County Sheriff's Department
Anthony W. Batts	Chief Long Beach Police Department
Lai Lai Bui	Sergeant Sacramento Police Department
Collene Campbell	Public Member
Robert G. Doyle	Sheriff Riverside County
Robert T. Doyle	Sheriff Marin County
Bonnie Dumanis	District Attorney San Diego County
Floyd Hayhurst	Deputy Sheriff Los Angeles County
Deborah Linden	Chief San Luis Obispo Police Department
Ronald Lowenberg	Director, Golden West College
Henry Perea	Councilman City of Fresno
Laurie Smith	Sheriff Santa Clara County
Michael Sobek	Sergeant San Leandro Police Department
Jerry Brown, Attorney General	Ex Officio Member Attorney General's Office
Hal Snow	Interim Executive Director

THE ACADEMY TRAINING MISSION

The primary mission of basic training is to prepare students mentally, morally, and physically to advance into a field training program, assume the responsibilities, and execute the duties of a peace officer in society.

FOREWORD

The California Commission on Peace Officer Standards and Training sincerely appreciates the efforts of the many curriculum consultants, academy instructors, directors and coordinators who worked with POST to develop this workbook. The Commission extends its heartfelt appreciation to the California law enforcement agencies who freely offered personnel who gave of their time to participate in the development of this training material.

This student workbook is part of the POST Basic Course Training System. The workbook component of this system provides self-study documents for every learning domain that makes up the basic course. Each workbook is intended to be a supplement to, not a substitute for, classroom instruction. Its objective is to improve learning and retention of information by a student attending the academy.

The content of each workbook is organized into sequenced learning modules to meet requirements as proscribed both by California law and the POST Training and Testing Specifications for the Basic Course.

It is our hope that the collective wisdom and experience of all who contributed to this book helps you, the student, to successfully complete the academy course, to advance to the Field Training Officer program and to enjoy a safe and rewarding career as a peace officer serving the communities of California.

A handwritten signature in black ink, appearing to read "Hal Snow". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

HAL SNOW
Interim Executive Director

LD 63: Computers and Computer Crimes

Table of Contents

Topic	See Page
Preface	iii
Introduction	iii
How to Use the Workbook	iv
Chapter 1: Introduction to Computer Crimes	1-1
Overview	1-1
Introduction to Computer Crimes	1-3
Specific Crimes	1-5
Laws Regarding Computer Crime	1-9
Chapter Synopsis	1-13
Workbook Learning Activities	1-14
Chapter 2: Computers and Computer Systems	2-1
Overview	2-1
Hardware Components	2-3
Software Components	2-6
Chapter Synopsis	2-8
Workbook Learning Activities	2-9
Chapter 3: Computer Crime Investigation	3-1
Overview	3-1
Pre-seizure Considerations	3-3
Computer Crime Search Warrants	3-5
Chapter Synopsis	3-9
Workbook Learning Activities	3-11
Glossary	G-1

Continued on next page

Table of Contents, Continued

This page was intentionally left blank.

Preface

Introduction

Student workbooks

The student workbooks are part of the POST Basic Course Instructional System. This system is designed to provide students with a self-study document to be used in preparation for classroom training.

Specialized Investigators' Basic Course training requirement

All law enforcement officers occupying positions as peace officers, as recognized by the California Penal Code and where the POST-required standard is the POST Specialized Investigators' Basic Course, must complete the course prior to the exercise of peace officer powers. The Specialized Investigators' Basic Course is comprised of 42 instructional units, called leaning domains (LD), from the Regular Basic Course, and 4 LDs specifically developed for the Specialized Investigators' Basic Course.

The content of each workbook is organized into sequenced learning modules designed to meet the requirements of the training specification document for the Specialized Investigators' Basic Course.

Student workbook elements

The following elements are included in each workbook:

- chapter contents, including a synopsis of key points,
 - supplementary material, and
 - a glossary of terms used in this workbook.
-

How to Use the Student Workbook

Introduction

This workbook provides an introduction to the training requirements for this Learning Domain. You may use the workbook in several ways: for initial learning, for test preparation, and for remedial training.

Workbook format

To use the workbook most effectively, follow the steps listed below.

Step	Action
1	Begin by reading the first two sections (POST Welcome and How to Use the Workbook), which provide an overview of how the workbook fits into the POST training program and how it should be used.
2	Refer to the Chapter Synopsis section at the end of each chapter to review the key points that support the chapter objectives.
3	Read the text.
4	Complete the Workbook Learning Activities at the end of each chapter. These activities reinforce the material taught in the chapter.
5	Refer to the Glossary section for a definition of important terms. The terms appear throughout the text and are bolded and underlined the first time they appear (e.g., <u>term</u>).

Chapter 1

Introduction to Computer Crimes

Overview

Learning need Investigators need to know the common uses of computers in criminal activity.

Learning objectives The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	E. O. Code
<ul style="list-style-type: none">• explain how a computer can be a target of criminal activity.	63.01.EO10
<ul style="list-style-type: none">• explain instrument of criminal activity.	63.01.EO11
<ul style="list-style-type: none">• explain repository of criminal activity.	63.01.EO12
<ul style="list-style-type: none">• discuss specific crimes associated with computers, including:<ul style="list-style-type: none">- child pornography- fraud schemes- counterfeiting- stalking- hacking- identify theft	63.01.EO13
<ul style="list-style-type: none">• discuss the federal laws relating to computer crimes.	63.01.EO14
<ul style="list-style-type: none">• discuss the state laws relating to computer crimes.	63.01.EO15

Continued on next page

Overview, Continued

In this chapter This chapter focuses on categories and statutes regarding computer crimes. Refer to the following chart for specific topics.

Topic	See Page
Introduction to Computer Crimes	1-3
Specific Crimes	1-5
Laws Regarding Computer Crime	1-9
Chapter Synopsis	1-13
Workbook Learning Activities	1-14

Introduction to Computer Crimes

[63.01.EO10, 63.01.EO11, 63.01.EO12]

Introduction Computer crime is a term that refers to a broad spectrum of criminal activity. This spectrum can generally be divided into three categories: target, instrument, and repository.

Target Either data or a computer component can be the **target of criminal activity**.

Data is the information stored on a computer or its storage media. It may consist of text documents, databases, computer programs, graphics, video, music, or any digital content on a hard drive or inside a computer.

Computer component refers to all hardware and software that comprise a computer system.

Instrument A computer is the **instrument of criminal activity** when it is the means by which the crime is perpetrated.

Repository A computer is the **repository of criminal activity** when it is the storage place for evidence of a crime.

Examples Example: A customer attempts to purchase an 18 round magazine for his Glock handgun on the Internet. He pays for the item through electronic funds and his credit card is charged four times for the same item and the merchandise was never delivered.

Continued on next page

Introduction to Computer Crimes, Continued

Examples (continued)

- Example: A hacker's computer is seized pursuant to a search warrant. The computer contains a software program that had been used to access illegally the victim's computers. The hacker's computer is the instrument of the crime and, if it contains the stolen data, is also a repository.
- Example: A computer contains an individual's personal data that a suspect wants to steal for identity theft. The data is the target of criminal activity.
- Example: An individual uses his work computer to send an e-mail to everyone in his company. The e-mail contained a virus. The computer is the instrument of criminal activity.
- Non-example: An investigator arrests a man for manufacturing fake driver's licenses and selling them to minors. A search warrant is executed on the man's residence, and a computer is found in the kitchen. However, evidence reveals that the man forged all the licenses by hand. The man has not committed a computer crime.
- Non-example: A woman is suspected of driving under the influence. At the time she is stopped, her personal digital assistant (PDA) is on the driver's seat. The woman has not committed a computer crime.
-

Specific Crimes

[63.01.EO13]

Introduction

Certain types of criminal conduct tend to be associated with computer crime. Investigators should be familiar with these specific crimes and be prepared to encounter the use of computers during their investigations.

Child pornography

Computers are often used to commit crimes involving **child pornography**. It is illegal to possess, distribute, prepare or advertise child pornography.

Child pornography is a common computer crime because the computer allows the perpetrator to possess and access the images in a semisecret manner.

Individuals use the Internet to find and download child pornography, to locate other individuals with whom to exchange pornography, and to target and exploit children.

Example: An individual meets children through on-line social networking websites and chat rooms (i.e., My Space or Yahoo Personals) and entices them into sending him sexually explicit pictures of themselves.

NOTE: Crimes associated with child pornography are generally covered under *Penal Code Section 311.11*.

Fraud schemes

Fraud schemes often involve the entire telecommunications industry, since computers rely on telecommunication systems to transmit and receive data. Computer and telecommunications fraud and abuse are difficult to quantify because so much is undetected. Fraud schemes can include insiders, trusted users who abuse their access to systems to defraud employers and/or other persons for purposes of greed or to retaliate for a perceived wrong.

Example: Through a series of electronic transactions, a bank employee stole over \$10,000,000 from his employer.

Continued on next page

Specific Crimes, Continued

Fraud schemes (continued)

Example: An e-mail scheme to solicit contributions to a fraudulent disaster relief fund.

Example: A telemarketing scheme targeting elderly victims was set up with a tape recorded solicitation and a computer programmed to dial hundreds of victims each day.

NOTE: Crimes associated with fraud schemes are covered under *Penal Code Sections 487, 502, 503, and 18 U.S. Code 1343*.

Counterfeiting

Computers are used in **counterfeiting** money, documents, and identification. Computers are used to develop high-resolution graphics that can be printed on high-quality printers.

Example: A high school student printed \$100 bills on a color laser printer and tried to sell them to other students.

Example: A counterfeiting gang forged Social Security cards and state ID cards using personal computers and color printers.

NOTE: Crimes associated with counterfeiting are generally covered under *Penal Code Section 470*.

Continued on next page

Specific Crimes, Continued

Stalking

Stalkers use the anonymity of the Internet to select and track victims. Stalkers often try to gain as much information as possible about a person in order to victimize that person at a later time. Stalkers engage in electronic harassment by using chat rooms and newsgroups or by sending e-mail **viruses** or electronic junk mail.

Example: A man repeatedly asked a woman for a date, but she rebuffed him. The man then impersonated the woman in Internet chat rooms and online bulletin boards, posting messages and sending e-mails that she fantasized about being raped. He posted the woman's home address and telephone number, directions to her residence, and explained how to defeat her home security system. Men came to her door in the middle of the night intending to rape her. The victim was terrorized for months before she finally moved out of the area.

NOTE: Crimes regarding stalking are covered under *Penal Code Section 646.9*.

Hacking

Hackers are individuals who use their computer skills to gain access to computerized information without permission. Using a variety of systems and technologies, hackers identify a system, learn about it, find the weaknesses, and exploit them.

Example: A hacker accessed the computerized data of three publicly-traded companies and stole trade secrets.

Example: A hacker intrudes into a computer system and illegally changes information posted on a website.

Example: A group of individuals use computers to attack and disrupt utility services.

NOTE: Crimes regarding hacking are covered under *Penal Code Section 502*.

Continued on next page

Specific Crimes, Continued

Identity theft

Identity theft is misappropriation of an individual's personal information in order to engage in criminal activity.

Example: An identity thief illegally gained someone else's name and Social Security number through the Internet. The thief then opened a credit card account in the victim's name, causing unpaid charges to be reported against the victim's credit rating.

Example: An Internet website offered discounted interest rates on credit cards. Individuals filled out on-line credit card applications with their personal information. The website operator used the victims' identities to open checking accounts in their names. Crimes regarding identity theft are covered under *Penal Code Section 530.5*.

Example: "**Phishing**" is a scheme that baits an individual to volunteer personal information through an internet source or by phone to suspect(s) for committing criminal acts.

Laws Regarding Computer Crime

[63.01.EO14, 63.01.EO15]

Introduction

Investigators should be familiar with privacy acts and statutes relating to computer crime.

Electronic Communications Privacy Act

The federal Electronic Communications Privacy Act governs the interception of real-time data transmission (*18 U.S. Code 2703*).

Privacy Protection Act

The federal Privacy Protection Act governs and controls subscriber and electronic transaction information (*42 U.S. Code 2000aa*).

Cable Communications Privacy Act

The federal Cable Communications Privacy Act governs content, transaction, and subscriber information. It also requires the cable provider to notify the subscriber before releasing information (*47 U.S. Code 521*).

Continued on next page

Laws Regarding Computer Crime, Continued

California statutes

California has enacted legislation specifically addressing computer related crimes. The following chart describes California's computer crime statutes. All descriptions refer to a "computer, etc.," which means a computer, a computer system, or a computer network.

Description	Crime Classification	Penal Code Section
Accessing and altering or using a computer, etc., to defraud or control	felony	502(c)
Accessing and taking or using data from a computer, etc.	felony	502(c)
Using or causing computer services to be used	felony if value of services is more than \$400	502(c)
Accessing and altering software in a computer, etc.	felony	502(c)
Disrupting or causing disruption of services to an authorized user of a computer, etc.	felony	502(c)
Providing or assisting in providing a means of access to a computer, etc.	infraction, misdemeanor, or felony depending on damage	502(c)

Continued on next page

Laws Regarding Computer Crime, Continued

California statutes (continued)

Description	Crime Classification	Penal Code Section
Accessing or causing a computer, etc., to be accessed	infraction, misdemeanor, or felony depending on damage	502(c)
Introducing a contaminant into any computer, etc.	infraction, misdemeanor, or felony depending on damage	502(c)
Using the Internet domain name of another to send e-mail, causing damage to a computer, etc.	infraction or misdemeanor depending on damage	502(c)

Related statutes

A computer crime could be prosecuted under an alternative statute, even if that crime is not specific to computer crimes. The following chart lists related statutes that can be used to prosecute computer crimes:

Description	Crime Classification	Penal Code Section
Stalking	felony	646.9
False personation	felony	529.3
Manufacture or sale of counterfeit birth certificate	misdemeanor	529a
Manufacture or sale of false identity card or driver's license	misdemeanor	529.5(a)

Continued on next page

Laws Regarding Computer Crime, Continued

Related statutes
(continued)

Description	Crime Classification	<i>Penal Code Section</i>
Knowing possession of a false identity card or driver's license	misdemeanor	<i>529.5(c)</i>
False personation to obtain money or property	punishable the same as theft	<i>530</i>
Use of personal identifying information to attempt to obtain credit, goods, services, or medical information	felony	<i>530.5</i>
Forgery of legal instruments	felony	<i>470/114</i>
Hate crimes	felony	<i>11411</i>
Computer theft	punishable the same as theft	<i>484, 487</i>
Theft of trade secrets	felony	<i>499C</i>

Chapter Synopsis

Learning need Investigators need to be familiar with the many uses of computers in criminal activity.

Target
[63.02.EO10] Either data or a computer component can be the target of criminal activity.

Instrument
[63.02.EO11] A computer is the instrument of criminal activity when it is the means by which the crime is perpetrated.

Repository
[63.02.EO12] A computer is the repository of criminal activity when it is the storage place for evidence of a crime.

Specific crimes
[63.02.EO13] Specific crimes associated with computers include child pornography, fraud schemes, counterfeiting, computer theft, stalking, hacking, and identity theft.

Federal laws
[63.02.EO14]

- Electronic Communications Privacy Act governs the interception of real-time data transmission.
- Privacy Protection Act governs and controls subscriber and electronic transaction information.
- Cable Communications Privacy Act governs content, transaction, and subscriber information.

California statutes
[63.02.EO15] California has enacted legislation specifically addressing computer related crimes. All descriptions refer to a “computer, etc.,” which means a computer, a computer system, or a computer network.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity questions

1. Name three types of criminal activity associated with computer crime and give one example of each.

2. List four related statutes in which a computer can be used but is not a necessary element of the crime. Give an example of each.

Continued on next page

Workbook Learning Activities, Continued

Student notes

Chapter 2

Computers and Computer Systems

Overview

Learning need Investigators need to become familiar with the terminology used to discuss hardware, software, and certain computer processes.

Learning objectives The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	E. O. Code
• describe the hardware components of a computer system.	63.02.EO7
• define the term storage media.	63.02.EO8
• give examples of storage media.	63.02.EO9
• describe the software components of a computer system.	63.02.EO10

Continued on next page

Overview, Continued

In this chapter This chapter focuses on commonly used terminology in computers and computer systems. Refer to the following chart for specific topics.

Topic	See Page
Hardware Components	2-3
Software Components	2-6
Chapter Synopsis	2-8
Workbook Learning Activities	2-9

Hardware Components

[63.02.EO7, 63.02.EO8, 63.02.EO9]

Introduction Investigators should be familiar with the hardware components of computer systems.

Hardware Hardware refers to the physical components of a computer or computer system.

Storage media Storage media are different forms in which information or data can be stored.

Term	Description
Hard drive	Most common storage media that is found in almost all computers. Hard drives store programs and data.
Removable storage devices	Examples of removable storage devices include Floppy Disks, DAT, Flash cards, CDR, CDR-W, CD-ROM, DVD, Memory Sticks, Thumb Drive, Flash Drive, and USB Drives. Each of these devices may require its own drive.
Offsite storage	Data storage at a separate location that is electronically linked to the computer, including the internet (e.g., wired network, wireless drives, ISP).

Continued on next page

Hardware Components, Continued

Input/ output devices

Term	Description
Keyboard	A typewriter-like keypad that a user can use to enter alphanumeric data into a computer
Monitor	Television-like screen that the computer uses to provide visual information to the user
Printer	A device that can be used to print documents from a computer on paper
Mouse	A device used to direct the computer by moving a pointer and selecting items that are highlighted by the pointer
Scanner	A device that can read (“scan”) a paper document into a computer
Digital camera/Web cam	Digital cameras store images electronically; digital cameras can also record short video clips
Modem	A device that connects computers electronically using telecommunication lines
Speakers	Speakers provide audio output to the user
Microphones	Microphones allow the computer to receive audio input
<u>Central Processing Unit (CPU)/ Tower</u>	The processor of a computer system; runs programs and processes all the data in the system (houses the main components of the computer system)
<u>Uninterruptible power supply (UPS)</u>	A UPS contains a battery that is automatically used to power a PC if electric voltage drops

Continued on next page

Hardware Components, Continued

Other electronic devices

The following chart lists additional related terms:

Term	Description
Network	A system of connections between computers that allows computers to communicate with each other
<u>Personal Digital Assistants (PDA)</u>	Small computing devices that allow the user to store data and which may have wireless capability. (i.e., Palm Pilot, Black Berry, Smart Phones, Cell Phones, PDA, Laptop/Note Books, I-Pod/MP3)

Software Components

[63.02.EO10]

Introduction

Investigators should recognize common software applications and terms.

Software

Software is a term used to describe computer programs. A computer program is the series of instructions that operates the computer. Two common examples of software are operating system software and application software.

Operating system software

Operating system software is the program that the computer uses to manage other programs. When the computer starts, the operating system software is loaded first. Examples may include DOS, Windows, Mac Operating System, Unix, and Linux.

Application software

Application software enables a computer to perform different tasks. The following chart lists terms that describe common application software:

Application	Description
Graphics	Creates and edits digital images
Database	Categorizes and stores information into tables or groups. The information in a database can consist of virtually anything, from names and telephone numbers to pictures, music, and audio
Word processing	Creates letters, text documents, and virtually any document that centers around text
Communication	Connects to other computers and exchanges files
Spreadsheet	Works with large amounts of numbers and calculation formulas

Continued on next page

Software Components, Continued

Application software

Application	Description
Virus	A malicious program that can “infect” a computer through communication with another computer. Viruses are commonly spread through the Internet, a floppy disk from an infected computer, or through e-mail
Hacking and cracking tools	Malicious programs created by hackers for illegally breaking into other computers
Forensic tools	Recovers and analyzes data
Optical character recognition (OCR)	Converts scanned documents into word processing documents
Web browser	Software to communicate with internet services
Financial programs (i.e., Quickens, Quick Books)	Financial analysis programs
Voice recognition	Interprets verbal commands spoken through a microphone

Chapter Synopsis

Learning need Investigators need to become familiar with the terminology used to discuss hardware, software, and certain computer processes.

Hardware
[63.01.E07,
63.01.E08] Hardware refers to the physical components of a computer or computer system. Hardware can be roughly grouped into storage media, input/output devices, and processing components.

Storage
media
[63.01.E09] Storage media are different forms in which information or data can be stored.

Definition
and types
of software
[63.01.E010] Software is a term used to describe computer programs. A computer program is the series of instructions that tell the computer what to do. Two common types of software are operating system software and application software.

Workbook Learning Activities

Introduction

To help you review and apply the material covered in this chapter, a selection of learning activities has been included. No answers are provided. However, by referring to the appropriate text, you should be able to prepare a response.

Activity questions

1. Name seven hardware components.

2. Name methods to store data.

Continued on next page

Workbook Learning Activities, Continued

**Activity
questions**
(continued)

3. List five examples of removable storage devices.

4. Explain the difference between application software and operating system software. Give examples of each.

Chapter 3

Computer Crime Investigation

Overview

Learning need Investigators need to know methods of gathering evidence in computer crime investigations.

Learning objectives The chart below identifies the student learning objectives for this chapter.

After completing study of this chapter, the student will be able to:	E. O. Code
• discuss the importance of gathering intelligence.	63.03.EO1
• describe the need for proper technical terminology in search warrant affidavits.	63.03.EO2
• discuss topics for which expert consultation may be advisable.	63.03.EO3
• demonstrate the importance of securing the electronic scene.	63.03.EO4
• explain the importance of properly recording the scene.	63.03.EO6
• discuss considerations for processing the scene.	63.03.EO7

Continued on next page

Overview, Continued

In this chapter This chapter focuses on recognizing, identifying, and gathering evidence of computer crimes. Refer to the chart for a specific topic

Topic	See Page
Pre-seizure Considerations	3-3
Computer Crime Search Warrants	3-5
Chapter Synopsis	3-9
Workbook Learning Activities	3-11

Pre-seizure Considerations

[63.03.EO1, 63.03.EO2, 63.03.EO3]

Introduction Investigators should be aware of pre-seizure considerations in computer crime investigations.

Intelligence gathering In addition to gathering as much information as possible, the investigator should specifically attempt to gather intelligence on the following topics:

- suspect's level of computer sophistication
 - number of individuals using the computer(s)
 - physical layout of the site(s)
 - network configuration
-

Informant If relying on information from an informant, the investigator should consider the informant's level of technical knowledge.

Multiple sites Investigators should be aware that computer crimes often involve multiple locations and/or jurisdictions.

Affidavits Affidavits in support of computer search warrants must be very specific and complete. Proper use of technical terminology is required in order to specify sufficient probable cause to allow proper seizure and post-seizure searches. The investigator should be able to articulate the evidence that is likely to be derived from the computer and must be able to state the connection between the computer and the crime.

NOTE: Please refer to LD 16 *Search and Seizure* for details on search warrant affidavits. Please refer to specific agency rules and regulations concerning search warrants for computer crimes.

Continued on next page

Pre-seizure Considerations, Continued

Computer expert

During the investigation, consult with a qualified computer expert. Specific topics about which the investigator might seek consultation can include the following:

- items to be seized that should be included in the search warrant affidavit
 - applicable time and/or notice restrictions
 - equipment needed to seize and transport
 - evidence storage facilities
 - who will conduct forensic examination of seized items
 - seizure procedures
-

General boot process

When a computer is turned on, the CPU starts running a program stored in the **Basic Input/Output System chip BIOS**. The first program run from the BIOS is the **Power-on Self-Test (POST)**.

When POST completes, the BIOS looks for an operating system to load from a storage drive. Typically, the first disk drive checked is the floppy drive, followed by the CD-ROM drive, and then the hard drive.

This process is the boot process. After the boot process is finished, the operating system software takes over the operation of the computer.

Computer Crime Search Warrants

[63.03.EO4, 63.03.EO5, 63.03.EO6, 63.03.EO7]

Introduction Investigators should become familiar with how to execute a computer crime search warrant.

Internet service providers Investigators should be aware that information maintained by Internet providers (ISP) is time-sensitive and is not generally preserved in any permanent form.

Synchronize entry If executing a search warrant with multiple sites, investigators should synchronize timing of the entry. A properly synchronized entry reduces chances that suspects will destroy evidence before computers can be seized.

Secure physical scene As with any search warrant execution, officer safety is a primary concern. In securing the physical environment, the investigator should:

- look for **booby traps** that might have been triggered by the entry
 - be aware of counter-surveillance devices
-

Secure electronic scene Investigators should be aware of the importance of securing the electronic scene as well as the physical scene.

- Evidence may be destroyed with a few simple keystrokes. Keep unauthorized individuals away from the computers, plugs, switches, and power supplies.
-

Continued on next page

Computer Crime Search Warrants, Continued

Secure electronic scene (continued)

- Investigators should be aware of physical equipment such as magnets or electronic devices that can corrupt or destroy computer evidence.
- For devices other than a desktop computer that you may come across, be sure to ask for expert advice. For example, a Personal Digital Assistant (Palm) may need to be plugged in to maintain a charge and therefore the data, a FAX machine must remain powered in order to ensure that the documents stored in the memory be saved, or that a laptop must have its battery removed.
- An investigator, not trained in computer seizures, can accidentally destroy valuable evidence by pressing the wrong button or pulling the wrong cord. The most important principle is to “Do No Harm.”
- Investigators should be alert to the possibility of remote access as it relates to the destruction of evidence. To prevent the continued transmission of data to and from the computer after entry, a qualified investigator should disconnect the modem and network cable.

Record scene

Before processing the scene and altering the configuration of the computers, record everything in its original setup. Photograph or videotape the following:

- any programs that are running on the suspect monitors
- all cables and devices, connected or unconnected
- location of all books, cables, and notes

Do not touch anything while recording the scene. Evidence that is not obvious at the time of the recording may be noticed later (e.g., proximity of items to each other may show criminal intent and activity).

Continued on next page

Computer Crime Search Warrants, Continued

Passwords

Investigators should search for passwords and seize them. Individuals may use a series of passwords or encryption notes. By asking suspect(s), they may tell you those password(s). The following is a list of common places where passwords may be hidden:

- under mouse pad
 - on desk
 - self-adhesive notes
 - under the keyboard
 - on the monitor
 - personal organizer
 - calendars
 - spiral bound notebook
-

Processing the scene

Investigators processing the scene should follow basic search warrant execution protocol and specific agency guidelines. The following chart lists recommendations for the investigator:

Recommendation	Reason
Label and mark room(s)	Explains evidence log and clarifies scene
Diagram scene, including computer location and configuration	Provides visual reminders of the scene
Inventory evidence	Documents chain of custody
Seize all media and manuals authorized by the search warrant	May have evidentiary and/or forensic value
Question suspects about computer operation and content(s)	May have evidentiary and/or forensic value

Continued on next page

Computer Crime Search Warrants, Continued

**Processing
the scene**
(continued)

Recommendation	Reason
Disconnect power source from the back of the <u>computer case</u>	Disconnection from the wall socket may trigger destruct programs
Leave intact as much as possible, disassembling only where necessary; mark all cables and ports	Ease of transportation and reassembly for further investigation
Package components securely, and transport with caution	Physical impact or jarring may destroy evidence
Transport and store all components away from radios, power supplies, magnet on emergency lights, and heat sources	Avoid contamination or loss of digital evidence

Chapter Synopsis

Learning need Investigators need to know methods of gathering evidence in computer crime investigations.

Intelligence gathering
[63.03.EO1] In addition to gathering as much information as possible, the investigator should specifically attempt to gather intelligence on the suspect's level of computer sophistication, number of individuals using the computer(s), and physical layout of site(s).

Affidavits
[63.03.EO2] Affidavits in support of computer search warrants must be very specific and complete. Proper use of technical terminology is required in order to specify sufficient probable cause to allow proper seizure and post-seizure searches. The investigator should be able to articulate the evidence that is likely to be derived from the computer and must be able to state the connection between the computer and the crime.

Computer expert
[63.03.EO3] During the investigation, it may be advisable to consult with a qualified computer expert. Specific topics about which the investigator might seek consultation can include items to be seized that should be included in the search warrant affidavit, applicable time and/or notice restrictions, equipment needed to seize and transport, evidence storage facilities, and who will conduct forensic examination of seized items.

Secure electronic scene
[63.03.EO4, 63.03.EO5] Investigators should be aware of the importance of securing the electronic scene as well as the physical scene.

Record scene
[63.03.EO6] Before processing the scene and altering the configuration of the computers, record everything in its original setup. If possible, photograph or videotape any programs that are running on the suspect monitors, all cables and devices, connected or unconnected, and location of all books, cables, and notes.

Continued on next page

Chapter Synopsis, Continued

**Processing
the scene
[63.03.E07]**

Investigators processing the scene should follow basic search warrant execution protocol and specific agency guidelines.

GLOSSARY

Introduction **The following glossary terms apply only to Learning Domain 63:
Computers and Computer Crimes.**

application software Enables a computer to perform different tasks

Basic Input/Output System chip (BIOS) Contains a program that is run by the central processing unit (CPU) when the system is turned on; that program initializes the system, runs a power-on self-test (POST), and then runs the operating system that is stored on storage media

booby traps May include destructive software programs that could destroy electronically stored data; may also be explosives attached to the computer's hard drive which are set to explode when the computer is turned on

Central Processing Unit (CPU)/ Tower The processor of a computer system; runs programs and processes all the data in the system

child pornography Pornography using a child or children as the subject

computer case Houses the main components of the computer, and is often referred to as "the box"

computer component Refers to all hardware and software that comprise a computer system

Continued on next page

Glossary, Continued

contaminant	Any one of a number of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information
counterfeiting	Computers are used to make imitation money to be used fraudulently or deceptively as genuine
data	Information stored on a computer or its storage media
fraud schemes	Deceitful plans
hackers	Individuals who use their computer skills to gain access to computerized information without permission
hardware	Refers to the physical components of a computer or computer system; hardware can be roughly grouped into storage media, input/output devices, and processing components
identity theft	Misappropriation of an individual's personal information in order to engage in criminal activity
instrument of criminal activity	The means or equipment by which the crime is perpetrated

Continued on next page

Glossary, Continued

**operating
system
software**

Program that the computer uses to manage other programs

**Personal
Digital
Assistants
(PDA)**

Small computing devices that allow the user to store data and which may have wireless capability

phishing

A scheme that baits an individual to volunteer personal information through an internet source or by phone

**Power-On
Self-Test
(POST)**

A test a computer runs each time it is powered on

**repository
of criminal
activity**

The storage place for evidence of a crime, such as a computer

software

A term used to describe computer programs

stalkers

Individuals who use the anonymity of the Internet to select and track victims

**storage
media**

Different equipment or devices in which information or data can be stored

Continued on next page

Glossary, Continued

target of criminal activity

Either data or a computer component can be the target of criminal activity

uninterruptible power supply (UPS)

Contains a battery that is automatically used to power a PC if electric voltage drops

virus

A computer instruction that is self-replicating or self-propagating and designed to contaminate other computer programs or data, consume computer resources, modify, destroy, record or transmit data or in some fashion take over the normal operation of the computer, computer system, or network
