U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING OPERATIONS

TECHNICAL OPERATIONS DIVISION

LESSON PLAN

DATA ACQUISITION

3224 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~~

DEVELOPED BY: (JAN/89)

(b)(6) **, Senior Instructor, FFI (Team Leader)**
r Instructor, FFI
ogram Specialist, FFI

REVISED BY: (MAR/02)

(b)(6) **Senior Instructor, FFI (Team Leader)**
Deputy Sheriff, Palm Beach County (FL), Sheriff’s Office
or Instructor, FFI
Program Specialist, FFI

REVISED BY: (JAN/04)

(b)(6) **ior Instructor, FFI (Team Leader)**
r Instructor, FFI
Senior Instructor, FFI

REVIEWED BY: (NOV/04)

(b)(6) **Branch Chief, CFI**

REVIEWED BY: (JAN/06)

(b)(6) **Senior Instructor, CFI**

REVIEWED BY: (JUL/07)

(b)(6) **Senior Instructor, CFI**
gram matrix)

CFI changed to TOD January 2009

REVISED BY: (AUG10)

(b)(6) **Instructor, TOD**

REVIEWED BY: (SEP/2010)

(b)(6) **Branch Chief, TOD**
Format update

TABLE OF CONTENTS

TABLE OF CONTENTS **4**

SYLLABUS **5**

INSTRUCTOR GUIDE **7**

OUTLINE OF INSTRUCTION **8**

I. .........INTRODUCTION **8**

A. RAPPORT AND OPENING STATEMENT 8

B. LESSON OVERVIEW 8

II. ........PRESENTATION **9**

A. EPO #1 : IDENTIFY APPROPRIATE LEGAL AND TECHNICAL TERMINOLOGY TO BE USED IN AN AFFIDAVIT FOR A SEARCH WARRANT WHEN COMPUTER EQUIPMENT IS INVOLVED 9

B. EPO #2: IDENTIFY SEVERAL WAYS IN WHICH THE EXECUTION OF A SEARCH WARRANT IN A COMPUTER ENVIRONMENT WILL VARY FROM THE TRADITIONAL EXECUTION OF A SEARCH WARRANT. 9

C. EPO #3: LIST SEVERAL CONSIDERATIONS THAT MUST BE ADDRESSED DURING THE PLANNING PHASE OF A COMPUTER SEARCH AND SEIZURE ..10

D. EPO #4: : IDENTIFY APPROPRIATE PROCEDURES FOR OFFICERS TO FOLLOW WHEN ENTERING THE SITE OF THE EXECUTION OF A SEARCH WARRANT.. 12

E. EPO #5: LIST SEVERAL ACTIONS THAT MUST BE TAKEN IN A COMPUTER RELATED SEARCH TO ENSURE THE INTEGRITY OF THE SEIZED MAGNETIC AND ELECTRONIC MEDIA 13

F. EPO #6: DISCUSS THE COMPONENTS OF A BOOT DISK THAT HAS APPROPRIATE PROGRAMS FOR PRESERVING THE INTEGRITY OF THE DATA ON THE SEIZED COMPUTER SYSTEM AND FOR PERFORMING A CURSORY ANALYSIS ON SITE 15

III. ....SUMMARY **16**

A. REVIEW OF PERFORMANCE OBJECTIVES 16

B. REVIEW OF TEACHING POINTS 16

IV. ....APPLICATION **17**

A. LABORATORY 17

B. PRACTICAL EXERCISE 17

REFERENCES .... **A**

BIBLIOGRAPHY .... **B**

ATTACHMENTS .... **C**

SYLLABUS

COURSE TITLE: **DATA ACQUISITION**

COURSE NUMBER: **3224**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OBJECTIVES
3			3	DEASTP	ALL
2			2	AFOSI-ECCTP	1,2,3,4,5
3			3	FRDE	ALL

DESCRIPTION:

This course relates various innovative as well as traditional investigative techniques to be used in computer criminal investigations. Topics discussed include types of evidence encountered, protecting evidentiary integrity, and preparing for and executing search warrants in computer environments. Also discussed during this course are considerations during the preparation process to executing a search warrant and taking information from a computer system at the search site. These considerations include technical equipment needed in a computer seizure tool kit, as well as the procedures to be performed to secure the computer system at the search site. Participants will discuss procedures to execute a search warrant in an automated environment.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given an investigative scenario involving a computer related crime, the participant will prepare an investigative plan that addresses steps taken before, during and after the crime scene search, in such a way as to facilitate a successful prosecution.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Identify appropriate legal and technical terminology to be used in an affidavit for a search warrant when computer equipment is involved.

EPO #2: Identify several ways in which the execution of a search warrant in a computer environment will vary from the traditional execution of a search warrant.

EPO #3: List several considerations that must be addressed during the planning phase of a computer search and seizure

EPO #4: Identify appropriate procedures for officers to follow when entering the site of the execution of a search warrant

EPO #5: List several actions that must be taken in a computer related search to ensure the integrity of the seized magnetic and electronic media

EPO #6: Discuss the components of a boot disk that has appropriate programs for preserving the integrity of the data on the seized computer system and for performing a cursory analysis on site.

STUDENT SPECIAL REQUIREMENTS:

NONE

METHOD OF EVALUATION:

DEASTP: Graded Practical Exercise (DEASTP Final PE #3233)

AFOSI-ECCTP: Completion of Course

FRDE: Graded Practical Exercise (FRDE Final PE)

INSTRUCTOR GUIDE

METHODOLOGIES:

1. Lecture\Discussion

TRAINING AIDS:

1. Instructor:
    - a. PowerPoint Presentation
    - b. Computer system connected to overhead projection system
2. Student:
    - c. None

SPECIAL INSTRUCTOR REQUIREMENTS:

None

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

Within the DEASTP, you have had extensive instruction on recovering data from seized computer systems after the computer systems (or data) have been seized. The discussion now should be on the procedures before and during the execution of the search warrant. You have had instruction on the legal principles governing search and seizure and computer related evidence. Now is the time to apply that knowledge to the execution of the search warrant. We will discuss the preparation of the Affidavit for Search Warrant that has the potential of involving computers, and the considerations for the form of the computer related evidence, as well as the discussions that should occur during the planning phase. The techniques use to protect the integrity of magnetic media will also be discussed. During the execution of a search warrant on a professional business environment, it is very unlikely that there will not be a computer system present, and this course will prepare you to properly handle the seizure of the computer system/data.

B. LESSON OVERVIEW

1. TERMINAL PERFORMANCE OBJECTIVE (TPO)

   Given an investigative scenario involving a computer related crime, the participant will prepare an investigative plan that addresses steps taken before, during and after the crime scene search, in such a way as to facilitate a successful prosecution.

2. ENABLING PERFORMANCE OBJECTIVES (EPO)

   EPO #1: Identify appropriate legal and technical terminology to be used in an affidavit for a search warrant when computer equipment is involved.

   EPO #2: Identify several ways in which the execution of a search warrant in a computer environment will vary from the traditional execution of a search warrant.

   EPO #3: List several considerations that must be addressed during the planning phase of a computer search and seizure

   EPO #4: Identify appropriate procedures for officers to follow when entering the site of the execution of a search warrant

   EPO #5: List several actions that must be taken in a computer related search to ensure the integrity of the seized magnetic and electronic media

   EPO #6: Discuss the components of a boot disk that has appropriate programs for preserving the integrity of the data on the seized computer system and for performing a cursory analysis on site.

II. PRESENTATION

A. EPO #1 : IDENTIFY APPROPRIATE LEGAL AND TECHNICAL TERMINOLOGY TO BE USED IN AN AFFIDAVIT FOR A SEARCH WARRANT WHEN COMPUTER EQUIPMENT IS INVOLVED

1.

2.

3.

4.

5.

(b) (7)e

6.

B. EPO #2: IDENTIFY SEVERAL WAYS IN WHICH THE EXECUTION OF A SEARCH WARRANT IN A COMPUTER ENVIRONMENT WILL VARY FROM THE TRADITIONAL EXECUTION OF A SEARCH WARRANT.

1. (b) (7)e

2.

3.

4.

5. (b) (7)e

6.

7.

C. **EPO #3: LIST SEVERAL CONSIDERATIONS THAT MUST BE ADDRESSED DURING THE PLANNING PHASE OF A COMPUTER SEARCH AND SEIZURE**

1.

2.

3. (b) (7)e

4.

5.

6.

(b) (7)e

7.

8.

9.

10.

11.

12. (b) (7)e

D. EPO #4: IDENTIFY APPROPRIATE PROCEDURES FOR OFFICERS TO FOLLOW WHEN ENTERING THE SITE OF THE EXECUTION OF A SEARCH WARRANT

1.

2.

3.

4.

(b)(7)e

5.

6.

(b)(7)e

E. EPO #5: LIST SEVERAL ACTIONS THAT MUST BE TAKEN IN A COMPUTER RELATED SEARCH TO ENSURE THE INTEGRITY OF THE SEIZED MAGNETIC AND ELECTRONIC MEDIA

1.

2.

(b)(7)e

3.

4.

5.

6.

(b)(7)e

7.

8.

(b)(7)e

9.

F. EPO #6: DISCUSS THE COMPONENTS OF A BOOT DISK THAT HAS APPROPRIATE PROGRAMS FOR PRESERVING THE INTEGRITY OF THE DATA ON THE SEIZED COMPUTER SYSTEM AND FOR PERFORMING A CURSORY ANALYSIS ON SITE

1.

(b)(7)e

2.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

1. EPO #1: Identify appropriate legal and technical terminology to be used in an affidavit for a search warrant when computer equipment is involved.
2. EPO #2: Identify several ways in which the execution of a search warrant in a computer environment will vary from the traditional execution of a search warrant.
3. EPO #3: List several considerations that must be addressed during the planning phase of a computer search and seizure
4. EPO #4: Identify appropriate procedures for officers to follow when entering the site of the execution of a search warrant
5. EPO #5: List several actions that must be taken in a computer related search to ensure the integrity of the seized magnetic and electronic media
6. EPO #6: Discuss the components of a boot disk that has appropriate programs for preserving the integrity of the data on the seized computer system and for performing a cursory analysis on site.

B. REVIEW OF TEACHING POINTS

1. Criminal investigators should consider any financial investigation to be a computer related investigation simply because computers are inevitably used to maintain financial records in business, in government, and in personal finances.
2. For agents untrained in the area of computer investigations, a review of the material covered in this course will be beneficial prior to executing a computer related search warrant. Some things to keep in mind

   a. A person knowledgeable of the system being investigated should be present at the search site. For personal computers this may be the case agent or other investigator.

   b. Be very careful when handling computer evidence. Avoid electromagnetic exposure and extreme temperatures.

   c. When executing a warrant, immediately isolate the system.

   d. Determine ahead of time whether the computer will be seized or just copies of files.

   e. Prior to executing a search warrant review the elements of ECPA-86 and PPA.

3. It is becoming necessary to have someone on the search team that is computer literate and is knowledgeable about procedures and techniques used when seizing a computer system or its data at the search site. Many agencies are beginning to train Investigators and Special Agents within their agencies that show the willingness, desire and ability to become Computer Seizure Specialists. Others are training all Investigators and Special Agents in just what they need to know to (b)(7)e

(b)(7)e

4. Planned time for asking and answering questions.

IV. APPLICATION

A. LABORATORY

NONE.

B. PRACTICAL EXERCISE

1. This course is evaluated in FRDE Final PE, and DEASTP Final PE, Course #3433

2. There is no formal evaluation of this material in AFOSI-ECCTP

REFERENCES

National Institute of Justice; Computer Crime: Criminal Justice Resource Manual (current edition); Washington; 2000.

Stohl, Clifford; The Cuckoo's Egg; Doubleday; New York; 1990

Hafner, Katie, and Markovich, John; Cyberpunks; Simon & Schuster, New York, 1991

Decision of U.S. District Court, Middle District of Texas; Steve Jackson Games v. United States, et al.; 1993

Federal Statute; Electronics Communications Privacy Act of 1986.

Federal Statute; Personal Privacy Act.

Federal Statute; Federal Computer Crime Statute (18 USC 1030)

Enfinger, Frank et al; Guide to Computer Forensics and Investigations, Thompson Course Technology, 2003.

~~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.~~

BIBLIOGRAPHY

None

~~**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.**~~

ATTACHMENTS

Attachment A: PowerPoint Presentation