U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF TRAINING OPERATIONS

TECHNICAL OPERATIONS DIVISION

LESSON PLAN

FORENSIC HARDWARE

3245 **SEP/10**

~~**WARNING**~~

~~**This document is FOR OFFICIAL USE ONLY (FOUO). 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: (NOV/95)

(b)(6)

enior Instructor, FFI (Team Leader)
d Instructor, FFI
enior Instructor, FFI
, Program Specialist, FFI

REVISED BY: (NOV/02)

(b)(6)

Senior Instructor, FFI (Team Leader)
enior Instructor, FFI
ior Instructor, FFI
Palm Beach County (FL) PD
, Program Specialist, FFI

REVISED BY: (DEC/03)

(b)(6)

or Instructor, FFI (Team Leader)
or Instructor, FFI
Senior Instructor, FFI
, Senior Instructor, FFI

REVIEWED BY: (JUN/04)

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

REVISED BY: (MAR/06)

(b)(6) **, Instructor, CFI (Team Leader)**

REVISED BY: (AUG/10)

(b)(6)

or Instructor, TOD
, Instructor, TOD

Changed to new template SEP/2010

TABLE OF CONTENTS

SYLLABUS

COURSE TITLE: **FORENSIC HARDWARE**

COURSE NUMBER: **3245**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM
2	3		5	DEASTP

DESCRIPTION:

A computer forensic investigation begins with the hardest job, imaging the data from the suspect computer system. It is very important to acquire the data without modifying the original media or the evidence media. Ensuring the data can be submitted into a criminal or civilian court. There are many computer programs that are designed to make an image of the suspect hard drive or other digital media. We will be acquiring the image in the form of a file that is later analyzed with forensic software such as (EnCase, Forensic ToolKit or other Forensic software). When imaging data, it is important to understand how and where imaging applications write data. Also, we must ensure the appropriate use of the Write Blocking hardware. This course discusses partitioning, imaging and Write Blocking hardware. This course also discusses imaging and partitioning, as well as options for writing imaged suspect data to magnetic media.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given a computer and a potential investigation requiring the imaging of digital evidence, the student will properly create a computer disk partition preparing it to receive evidence, and imaging the data transferring it to the evidence drive without change.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Define terminology associated with imaging suspect data.

EPO #2: Identify various types of physical write blockers, ensuring control and connections, and transfer data to the evidence drive.

EPO #3: Use software to create partitions on a hard disk.

STUDENT SPECIAL REQUIREMENTS:

1. Each student must have a computer system with an additional hard disk to partition.
2. The laboratory exercise must be completed properly for the final practical exercise to be completed.

METHOD OF EVALUATION:

Successful completion of classroom exercises.

INSTRUCTOR GUIDE

METHODOLOGIES:

1. Lecture
2. Laboratory Exercise

TRAINING AIDS:

3. Instructor: Note whether the use of the training aides/equipment is required or optional.
    a. Same computer system as the students with additional hard drive - required
    b. PowerPoint presentations – required
    c. Physical Write Blockers - required
4. Student: Note whether the use of the training aides/equipment is required or optional.
    a. PowerPoint presentations - required
    b. An additional computer hard disk per student - required
    c. Physical Write Blockers - required

SPECIAL INSTRUCTOR REQUIREMENTS:

1. Each student must have a computer system with an additional hard disk to partition along with appropriate physical write blockers.
2. The laboratory exercise must be completed properly for the DEASTP practical exercise to operate properly

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

1. A computer forensic investigation begins with the hardest job, imaging the data from the suspect computer system. It is very important to acquire the data without modifying the original media or the evidence media. Ensuring the data can be submitted into a criminal or civilian court. There are many computer programs that are designed to make an image of the suspect hard drive or other digital media. We will be acquiring the image in the form of a file that is later analyzed with forensic software such as (EnCase, Forensic ToolKit or other Forensic software). When imaging data, it is important to understand how and where imaging applications write data. Also, we must ensure the appropriate use of the Write Blocking hardware. This course discusses partitioning, imaging and Write Blocking hardware. This course also discusses imaging and partitioning, as well as options for writing imaged suspect data to magnetic media.

B. TERMINAL PERFORMANCE OBJECTIVE (TPO)

Given a computer and a potential investigation requiring the imaging of digital evidence, the student will properly create a computer disk partition preparing it to receive evidence, and imaging the data transferring it to the evidence drive without change.

C. ENABLING PERFORMANCE OBJECTIVES (EPO)

EPO #1: Define terminology associated with imaging suspect data

EPO #2: Identify various physical write blockers, ensuring control, connectivity, and acquisition of data to the evidence drive

EPO #3: Use software to create partitions on a hard disk

II. PRESENTATION

A. EPO #1: DEFINE TERMINOLOGY ASSOCIATED WITH IMAGING SUSPECT DATA

1. Disk – Physical; Drive – Logical
2. Cylinder/Head/Sector (001), beginning of Master Boot Record, which occupies entire 1st cylinder of 1st side, which contains the Partition Table
3. LBA (Logical Block Address)
4. Partitioning– Prepares the drive for use, dividing it into logical areas for different uses.
5. Two types of partitions
    a. Primary – In Windows, there can be four primary partitions and only one can be active at a time. Windows searches for the first active bootable hard drive to start the operating system.
    b. Extended – there can be multiple extended partitions on a physical drive.

6. Control, Connectivity Acquire (CCA)

   a. As a digital acquisition specialist, you must be in control of the digital environment. You must ensure that the evidence drive is properly connected to the evidence without making any data changes. Finally, when Acquiring the data, the investigator must ensure that no data changes are made. These steps must be appropriately documented.

7. EnCase proprietary "E0x" file.

   a. Three parts to the E0x file, header, checksum, and data block, ensures a record of any changes.

   b. Allows compression.

   c. Adjustable Block size up to 2 GB, and adjustable Error Granularity.

B. EPO #2: IDENTIFY HARDWARE CONNECTIONS AND THE APPROPRIATE WRITE BLOCKERS TO ACQUIRE EVIDENCE

1. IDE/PATA
2. SATA
3. Flash Media
4. Optical Media
5. Thumb Drive
6. SCSI
7. USB
8. Floppy Drive

C. EPO #3: USE SOFTWARE TO CREATE PARTITIONS ON A HARD DISK

1. See PowerPoint presentation (Attachment C: "GDISK"), all slides
2. Run GDISK and GDISK32
3. Instructor should lead students through an exercise, creating three logical drives on a physical hard disk – one 50% of the hard disk, and the other two, 25 of the hard disk.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

1. EPO #1: Define terminology associated with imaging suspect data
2. EPO #2: Identify hardware connection and the appropriate write blocker to acquire evidence.
3. EPO #3: Use software to create partitions on a hard disk

B. REVIEW OF TEACHING POINTS

1. GDISK and partitioning are vital to ensuring forensically sound evidence is obtained. If the image is not acquired correctly the analysis of the restored imaged data may not be performed and may be unreliable, unusable and not acceptable in court.
2. The student must be familiar with various types of hardware used in forensically sound acquisitions.
3. Questions?

IV. APPLICATION

A. LABORATORY

1. Students are guided through creating partitions on another physical hard disk.
2. Students must create the partitions in the lab in order to complete the practical exercises.

B. PRACTICAL EXERCISE

NONE.

REFERENCES

Carrier, Brian. File System Forensic Analysis. Pearson Education, Inc. Rights and Contracts Department, Boston, MA. 2008.

White, Ron and Downs, Timothy Edward. How Computers Work. 9th ed. Que Publishing, Indianapolis, IN, 2008.

Glover, Thomas J, (et al) Pocket PCRef. 14th edition, Sequoia Publishing, Inc., Littleton , CO, 2010

BIBLIOGRAPHY

None

ATTACHMENTS

1. Laboratory Exercise
2. PowerPoint Presentation: GDISK

Attachment 1
Laboratory Exercise

PARTITIONS AND HARD DISK STRUCTURES

LABORATORY EXERCISE

1. Delete all partitions on another hard disk

2. Create three logical drives on the hard disk

   a. Sizes of drives =50 percent, 20 percent and 1 percent
   b. What has to be done before the drives are recognized properly by the operating system?

3. What has to be done before data can be placed on the drives?

4. What is the hard disk physical and logical size?

5. How much disk space is remaining outside of partition boundaries?

6. What is the file system on the drives – why?

Attachment 2

PowerPoint Presentation: GDISK