
Digital Evidence Acquisition Specialist Training Program (DEASTP)

Up one level

The primary purpose of the DEASTP course is to equip criminal investigators with the knowledge, skills, and abilities to properly identify and seize digital evidence. Through a combination of lecture, demonstration, hands on exercises, labs and a practical exercise investigators learn about a computer's boot process; changing the boot sequence and BIOS setup of a computer; setting jumpers on hard drives for master, slave, single and cable select settings; disk wiping; formatting and partitioning hard drives; assembling external drive enclosures; creating a forensically sound boot disk; file compression; investigative techniques for seizing digital evidence from personal computer (PC) and notebook computer hard drives, floppy diskettes, compact disks (CDs), DVDs, thumb drives, and various flash media by acquiring forensically valid images of the digital media; previewing digital media prior to acquisition to determine if the media contains key text strings, unlawful graphics, etc; using external storage devices; using hardware and software write blockers; using device drivers; writing batch files; using command line programs; essential internal and external DOS commands; installing software; installing and uninstalling hardware; IDE, USB, and Firewire cables and devices; and legal aspects pertaining to the seizure and search of electronic evidence. Investigative hardware and software used in the class are issued to the students so that they are prepared to put the skills learned in the class to use immediately upon return to their duty stations.

The DEASTP program is an intense course that requires substantial computer aptitude. Successful completion of a graded practical exercise is required for graduation.

At the conclusion of the training program, the participants will be able to successfully seize digital evidence. This knowledge will be demonstrated through the completion of a 10 hour practical exercise on the last full day of the training program. The practical exercise includes a simulated search warrant scenario. [Note: The search warrant scenario does not include tactics (e.g. dynamic building entry, handcuffing suspects, use of firearms, etc)]. The practical exercise requires each student to work independently to acquire various types of digital evidence.

It is recommended that you attend this course before attending the Seized Computer Evidence Recovery Specialist (SCERS) training program. SCERS students are required to possess the skills and technical information presented in this course before they attend the SCERS training program.

Type: Advanced

Length: The training program encompasses 2 weeks (76 Hours), beginning on a Monday and ending on the second Friday, with the graduation scheduled at approximately 11:00 to 11:30 a.m. Travel days are Sunday and Friday after 12pm.

Curriculum

- Electronic Law and Evidence
- Computer POST and Boot Process
- DOS Commands – Internal and External
- GDISK, Format, Partitions, Diskwipe
- Hard Drive Jumpers
- Hard Drive Adapters (USB, SATA)
- PCI Cards (IDE, SATA, USB, Firewire)
- Cables

- Diskette Write Protection
- Hard Drive Write Blocker
- Flash Media Write Blocker
- Software Write Blockers
- External Case Assembly
- Validation of Data -- Hash
- File Compression
- Creating a Forensically Sound Boot Disk
- Process Disk Utilities
- Acquisition of Digital Evidence
 - Diskette
 - 2.5" IDE Hard Drive (aka PATA Drive)
 - 3.5" IDE Hard Drive (aka PATA Drive)
 - SATA Hard Drive
 - SCSI Hard Drive
 - Compact Disk (CD)
 - DVD
 - Thumb Drive
 - Flash Media (e.g. Compact Flash, Secure Digital, xDPicture)
- Digital Evidence Acquisition using Various Methods
 - DOS
 - NIC-to-NIC
 - Windows
 - Pre-Installed Environment CD
- Preview Digital Media Prior to Acquisition
- Search Warrant / Consent Search Techniques
- Final Digital Evidence Acquisition Practical Exercise

Training Materials

Description of Items Issued During DEASTP FY2007

- 4-Pin Molex Male to SATA Power Cable
- 4-Pin Molex Power Extension Cable
- 4-Pin Molex Power Y cable for 3.5" FD, 18 awg
- 4-Pin Molex Power Y cable, 18 awg (2)
- Adapter, 2.5" Notebook HD to 3.5" IDE HD
- Adapter, Green Grounding (2)
- Adapter, IDE to USB (2)
- Adapter, SATA to IDE
- Adapter, SATA to USB
- ADF Triage-ID™
- Anti-Static Bags (2 Sizes)
- Anti-Static Wrist Strap
- Binder, 3-ring, 1" with student handouts
- Book – File System Forensic Analysis
- Book - How Computers Work
- Book - Pocket PC Reference
- Book – Upgrading & Fixing PCs for Dummies
- CD-R media
- Diskettes 3.5" 1.44MB
- DVD-ROM / CD-ROM Drive
- External Enclosure -- IDE to USB for CD/DVD Drive
- Firewire 800 PCI Card
- Firewire 800 PCMCIA Card
- Flashlight

- Hard Disk Drive Cooler (2)
- Hard Drive, IDE, 320 GB
- Hard Drive, SATA, 320 GB
- Mini Storage Box w/ Hardware Assorted Pak
- MISC free software utilities (included on student CD)
- MISC free to law enforcement software utilities
- MISC Supplies (permanent marker, pen, pencil, highlighter, paper)
- Network Crossover Cable 14'
- Network Crossover Cable Adapter, 8 "
- Norton System Works Premier ®
- PCI Power Bracket
- Student CD containing PowerPoints, Exercises, Software
- Thumb Drive – 1 GB
- Thumb Drive – 2 GB
- Tool Kit, Standard, 11 piece
- Ultra IDE Cable – 18"
- Ultra SATA/300/ATA/133 PCI Card
- UltraBlock – Forensic Card Reader and Writer
- UltraBlock – IDE hardware write block device with cables
- USB 2.0 A Female to A Male Cable, 6 ft.
- USB 2.0 A Male to 4 pin Mini B Male Cable, 6 ft.
- USB 2.0 A Male to 5 pin Mini B Male Cable, 6 ft.
- USB 2.0 A Male to B Male Cable, 6 ft.
- USB 2.0 Adapter A Female to B Female
- USB 2.0 Adapter A Male to B Female
- USB 2.0 PCI Card
- WinHex Specialist Edition®

All of these items are subject to change without notice. List effective May 16, 2007. Items issued at export courses may vary.

Prerequisites for Attendance

A functional knowledge of computers is required. More specifically, this means:

1. Experience with the majority of the functions of a Word Processor (e.g. Word or Word Perfect).
2. Training or background in the use of a mouse, and knowledge of the basic concepts governing the use of Microsoft Windows, version 9X, Me, 2000, XP, or Vista.
3. Use of command/system prompts. In other words, using a computer in some way other than mouse-clicking Windows controls. Students must possess knowledge of the usage of basic Command Prompt commands, including, but not limited to
 - DIR Create "Subdirectories" on a diskette/hard disk (MD) and store data within the subdirectories; also access the subdirectories (CD), and remove the subdirectories (RD).
 - COPY one file/many files/entire diskettes
 - DEL/ERASE one file/many files
 - TYPE to view the contents of Text Files
4. Use of My Computer or Explorer file management program provided with Windows to navigate through the directories / folders and files contained on a computer.

Students who need training in any of the above requirements are referred to any of several sources including: Internet online training courses, adult training courses typically offered in local colleges and universities or other sources, commercial training providers that offer courses in fundamental computer usage.

Contact Information

DEASTP Program Coordinator

Computer & Financial Investigations Division
Bldg. 210
Federal Law Enforcement Training Center
Glynco, GA 31524
(912)267- 2747 or (912)267-2876
(912)267-2500 (fax)
FLETC-CFI-TechnicalInvestigationsBranch@dhs.gov

Training Dates

DEASTP-703 / Glynco, GA -- June 11, 2007 to June 22, 2007

* last modified May 21, 2007 16:47