Introduction to Computer Crime Investigations

Objectives

During this session, participants will:

- Understand when and how digital evidence is created.
- Explore various devices that contain digital evidence.
- Discuss the first steps of the digital evidence collection process.

I. CRIMES CREATE DIGITAL EVIDENCE

A. Any crime can create digital evidence

1. Computer to commit crime: these are commonly known as "cyber crimes"
   a. Illegal access to computer systems permits criminals to accomplish the activities described below
   b. Interference with data or computer systems by malicious programs can destroy data or result in theft of information
   c. Online identity theft is a huge problem that costs the world billions of dollars each year, and victimizes businesses, governments, and individuals
2. Computer to store evidence of crime
   a. Child pornography; digital photographs and the Internet have facilitated an explosion in child exploitation and pornography
   b. Pirated movies and other intellectual property are usually found in digital format
   c. Records of criminal transactions: everyone keeps records on computers, including the criminals
3. Computer for communication
   a. E-mail, instant messaging, and Internet chat rooms
   b. Voice and video communications
   c. Transfer documents and photographs

B. Computers make their own records

1. Computers create transaction logs of many activities, including logging in, sending and receiving email, saving and retrieving files, connecting to the Internet, and many other applications
2. Electronic documents, photos, and email contain hidden information that is very helpful to investigators; this information may include dates and times, address and routing information, deleted and edited data, and more

II. DIGITAL EVIDENCE IS EVERYWHERE

A. Computers, and their hard drives and memory chips, are only the beginning of possible places where digital evidence may be located

B. Other digital storage devices

1. CD, DVD, and other disks
2. Thumb drives, flash drives
3. Personal digital assistants (PDA)
4. Digital cameras
5. Media players – iPod, MP3
6. Game consoles – PlayStation, Xbox
7. Automobiles? – OnStar, GPS

C. Printers, scanners, copiers, and fax machines are often overlooked and contain transaction records, phone books, and digital copies of documents

D. Mobile phones can contain huge amounts of information, including dialing records, photos and videos, address books, documents, music, and other applications

E. Networks and the Internet

1. Computers rarely stand alone; any two digital devices connected together create a network; networked devices communicate with each other and share information; sometimes, a computer can be controlled from a remote location
2. Networks can be simple, such as a home computer connected to a printer, or complex, such as those found in large organizations; complex networks have servers and routers, which are specialized network computers; wireless networks are everywhere
3. The Internet permits communication and information sharing across the globe
4. All digital information is located SOMEWHERE, not in an imaginary “cyberspace” or cloud, but on a computer, a server, or some other digital storage device

F. Service providers

1. Internet infrastructure relies on service providers
2. Service providers control important digital evidence
    a. Electronic communications
    b. Stored data
    c. Customer information

G. Data is volatile

1. Deleted by a keystroke
2. Service providers, businesses, other entities, and individuals may delete data in the normal course of business
3. Read only memory (RAM) is lost when a computer is turned off
4. Specialized knowledge and tools are needed to recover deleted data
5. Some data cannot be recovered

III. COLLECTING DIGITAL EVIDENCE

A. Preparing to conduct the search and seizure

1. Assemble a team that includes the investigator, technical expert, and the prosecutor
2. Learn about the computer system
    a. Hardware: Type of computer? Peripheral devices? Other electronic devices?
    b. Network: Connected to a network, peripheral devices, the Internet?
    c. Software: Operating system? Encryption? Other software?
    d. Physical location and conditions
3. Formulate the plan and a backup plan, for example:
    a. Who will be conducting the search? Are the right tools available?
    b. Will the search of the data take place on scene or at the forensic lab?
    c. Is the computer and related equipment to be seized? How will this affect a third-party business or other ongoing activity not related to the seizure?
4. A critical part of preparation is taking the steps necessary to obtain legal authority to conduct the search and seizure. In the U.S., this is most often accomplished by receiving a search warrant from the court. A warrant and accompanying affidavit must describe the object of the search and the property to be seized accurately and particularly, and explain the possible search strategies (as well as the practical and legal issues that helped shape them).

B. On location

1. Secure and evaluate the scene
    a. Follow established procedures; do not alter the condition of any electronic devices
    b. Protect perishable data physically and electronically
    c. Identify telephone lines and other cables attached to devices
    d. Collect physical evidence; for example, a keyboard may have fingerprints
    e. Conduct preliminary interviews
2. Document the scene
    a. Observe and document the physical scene
    b. Document the condition and location of the computer system and other devices
    c. Identify and document related electronic components
    d. PHOTOGRAPH the entire scene, the computers and other devices (front and back), what appears on the monitor; in addition, videotaping may be appropriate
3. Collect the evidence
    a. Imaging drives and other digital storage devices is critical for data preservation and analysis
    b. Procedures for stand-alone and laptop evidence will be different than those for computers in complex environments
    c. Gather other electronic devices and peripheral evidence
    d. Don’t forget non-electronic evidence!
    e. Package, transport, and store everything to protect and preserve the evidence
4. Forensic examination – on scene, at the lab?

C. Special considerations: The evidence may not be on the scene or may be mingled with other digital information

1. Service providers often have established procedures for providing digital evidence to law enforcement
    a. Internet service providers (ISP)
    b. Website hosting and data storage providers
2. Businesses and other networked entities may be disrupted or harmed by a search
3. International issues arise when digital evidence is located outside of a country; this occurs frequently, especially when ISPs are involved

---

This presentation was developed by the Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, www.cybercrime.gov