NIJ

APR. 08

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

Chapter 1. Electronic Devices: Types, Description and Potential Evidence

NCJ 219941

Chapter 1. Electronic Devices: Types, Description, and Potential Evidence

Internally attached computer hard drives, external drives, and other electronic devices at a crime scene may contain information that can be useful as evidence in a criminal investigation or prosecution. The devices themselves and the information they contain may be used as digital evidence. In this chapter, such devices will be identified, along with general information about their evidential value.

Some devices require internal or external power to maintain stored information. For these devices, the power must be maintained to preserve the information stored. For additional information about maintaining power to these devices, please refer to chapter 3 of this guide, the device manufacturer's Web site, or other reliable sources of information.

Computer Systems

Description: A computer system consists of hardware and software that process data and is likely to include:

- A case that contains circuit boards, microprocessors, hard drive, memory, and interface connections.
- A monitor or video display device.
- A keyboard.
- A mouse.
- Peripheral or externally connected drives, devices, and components.

Computer systems can take many forms, such as laptops, desktops, tower computers, rack-mounted systems, minicomputers, and mainframe computers. Additional components and peripheral devices include modems, routers, printers, scanners, and docking stations. Many of these are discussed further in this chapter.

Types of Computer Systems

PC, monitor, keyboard, and mouse

Apple G3 computer, monitor, keyboard, and mouse

Apple iMac, keyboard, and mouse

Laptop computer

Potential evidence: A computer system and its components can be valuable evidence in an investigation. The hardware, software, documents, photos, image files, e-mail and attachments, databases, financial information, Internet browsing history, chat logs, buddy lists, event logs, data stored on external devices, and identifying information associated with the computer system and components are all potential evidence.

Storage Devices

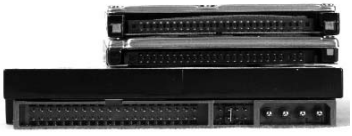
Description: Storage devices vary in size and the manner in which they store and retain data. First responders must understand that, regardless of their size or type, these devices may contain information that is valuable to an investigation or prosecution. The following storage devices may be digital evidence:

- **Hard drives.** Hard drives are data storage devices that consist of an external circuit board; external data and power connections; and internal magnetically charged glass, ceramic, or metal platters that store data. First responders may also find hard drives at the scene that are not connected to or installed on a computer. These loose hard drives may still contain valuable evidence.

Types of Hard Drives

SCSI drives SATA drive IDE drive Laptop hard drives

IDE 40-pin 2.5" IDE 44-pin



IDE power and data connections

Serial ATA (SATA)

SCSI HD 68-pin SCSI IDC 50-pin

- **External hard drives.** Hard drives can also be installed in an external drive case. External hard drives increase the computer's data storage capacity and provide the user with portable data. Generally, external hard drives require a power supply and a universal serial bus (USB), FireWire, Ethernet, or wireless connection to a computer system.

External Hard Drive Cases

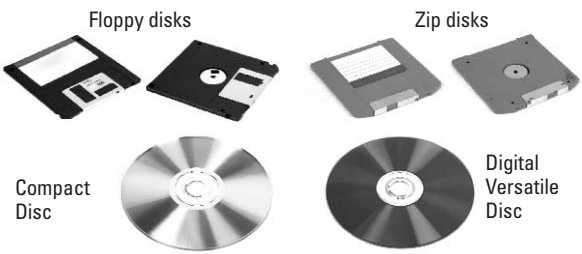
3.5" Hard drive

2.5" Hard drive

Network storage device

- **Removable media.** Removable media are cartridges and disk-based data storage devices. They are typically used to store, archive, transfer, and transport data and other information. These devices help users share data, information, applications, and utilities among different computers and other devices.

Removable Media



- **Thumb drives.** Thumb drives are small, lightweight, removable data storage devices with USB connections. These devices, also referred to as flash drives, are easy to conceal and transport. They can be found as part of, or disguised as, a wristwatch, a pocket-size multitool such as a Swiss Army knife, a keychain fob, or any number of common and unique devices.

Common Thumb Drives

Other Types of Thumb Drives

- **Memory cards.** Memory cards are small data storage devices commonly used with digital cameras, computers, mobile phones, digital music players, personal digital assistants (PDAs), video game consoles, and handheld and other electronic devices.

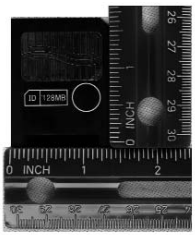
Memory Cards

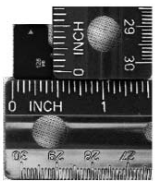
Smart media (SM) card

Secure digital (SD) card

Mini secure digital card

Micro secure digital card





Compact flash card

Memory stick

Potential evidence: Storage devices such as hard drives, external hard drives, removable media, thumb drives, and memory cards may contain information such as e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, financial records, and event logs that can be valuable evidence in an investigation or prosecution.

Handheld Devices

Description: Handheld devices are portable data storage devices that provide communications, digital photography, navigation systems, entertainment, data storage, and personal information management.

Handheld Devices

Potential evidence: Handheld devices such as mobile phones, smart phones, PDAs, digital multimedia (audio and video) devices, pagers, digital cameras, and global positioning system (GPS) receivers may contain software applications, data, and information such as documents, e-mail messages, Internet browsing history, Internet chat logs and buddy lists, photographs, image files, databases, and financial records that are valuable evidence in an investigation or prosecution.

It is important to note that—

- Data or digital evidence may be lost if power is not maintained.
- Data or digital evidence on some devices such as mobile or smart phones can be overwritten or deleted while the device remains activated.
- Software is available for mobile and smart phones that can be activated remotely to render the device unusable and make the data it contains inaccessible if the phone is lost or stolen. This software can produce similar results if activated on a device seized by law enforcement. First responders should take precautions to prevent the loss of data on devices they seize as evidence.

Peripheral Devices

Description: Peripheral devices are equipment that can be connected to a computer or computer system to enhance user access and expand the computer's functions.

Peripheral Devices


Keyboard and mouse


Microphones


USB and FireWire hubs


Web cameras


Memory card readers


VoIP devices

Potential evidence: The devices themselves and the functions they perform or facilitate are all potential evidence. Information stored on the device regarding its use also is evidence, such as incoming and outgoing phone and fax numbers; recently scanned, faxed, or printed documents; and information about the purpose for or use of the device. In addition, these devices can be sources of fingerprints, DNA, and other identifiers.

Other Potential Sources of Digital Evidence

Description: First responders should be aware of and consider as potential evidence other elements of the crime scene that are related to digital information, such as electronic devices, equipment, software, hardware, or other technology that can function independently, in conjunction with, or attached to computer systems. These items may be used to enhance the user's access of and expand the functionality of the computer system, the device itself, or other equipment.

Data storage tape drives

Surveillance equipment

Digital cameras

Video cameras

Digital audio recorders

Digital video recorders

MP3 players

Satellite audio, video receiver, and access cards

Video game consoles

Computer chat headset

Keyboard, mouse, and video (KM) sharing switch

Sim card reader

Global Positioning System (GPS) receiver

Thumb print reader

Reference material

Potential evidence: The device or item itself, its intended or actual use, its functions or capabilities, and any settings or other information it may contain is potential evidence.

Computer Networks

Description: A computer network consists of two or more computers linked by data cables or by wireless connections that share or are capable of sharing resources and data. A computer network often includes printers, other peripheral devices, and data routing devices such as hubs, switches, and routers.

Computer Networks

Network hub

Laptop network card and ethernet cable

Internet modems

Network switch and power supply

Wireless access points

Wireless network server

Wireless cards and devices

Wireless card for PC

Wireless USB device

Directional antenna for wireless card

Potential evidence: The networked computers and connected devices themselves may be evidence that is useful to an investigation or prosecution. The data they contain may also be valuable evidence and may include software, documents, photos, image files, e-mail messages and attachments, databases, financial information, Internet browsing history, log files, event and chat logs, buddy lists, and data stored on external devices. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including Internet protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses may all be useful as evidence.