
Creating a Forensic Computer System: Basic Hardware and Software Specifications

SEARCH Training Services
August 2006



SEARCH

The National Consortium for Justice Information and Statistics

7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831

Phone: (916) 392-2550 • Fax: (916) 392-8440 • Internet: www.search.org

Overview

The following is a description of the basic hardware and software specifications required for a forensic computer system. The Training Services staff of SEARCH, in cooperation with law enforcement agencies throughout the United States, developed these specifications.

The type of system described in this document provides the greatest flexibility and most efficiency when performing computer data forensics. The system should be able to handle 95% of the cases and types of equipment most law enforcement agencies will come across at the present time.¹

The basic functions any forensic system should be able to perform are:

- Make a true and accurate copy of a hard drive to another hard drive or an image file.
- Make a true and accurate copy of a hard drive to a removable and portable media.
- Restore the true and accurate copy onto a second forensic hard drive from the removable media or image files.
- Perform a media analysis of a subject drive or image file.
- A good reference for information is the National Institute of Standards and Technology – Computer Forensics Tool Testing Web site:
www.cftt.nist.gov

In addition to the recommended hardware and software, this document provides a list of optional hardware. Law enforcement agencies will eventually need most of these packages, but some can be purchased on an as-needed basis.

The recommended hardware and software is not intended to be an exclusive or exhaustive list. If you have suggestions of hardware and software to add to the list, please contact SEARCH Training Services staff at 916/392-2550 (Pacific time).

¹ As of the date of publication, August 2006

Creating a Forensic System

The system described here can perform the major functions required of a forensic system in a highly efficient manner and will provide optimal flexibility when conducting forensic analysis. The following are recommendations for forensic computer system hardware.

Hardware Recommendations

Motherboard and Processor

- A Pentium IV dual core processor with hyper threading (3.2+ GHz) or AMD Athlon 5000+ processor. You should strongly consider purchasing a 64-bit processor.
- Be sure to choose a motherboard that uses the latest socket style. For example, while you can still purchase processors for the AMD 939 socket, AMD is in the transition to the AM2 socket. In this example, you would purchase an AMD processor that uses the AM2 socket, not a 939 socket.
- Three to five PCI expansion slots
- PCI Express x16 Slot. While you may not need the high-speed graphics this bus provides, there are many inexpensive graphic cards that will work in this slot.
- Two ATA/100 or ATA/133 EIDE controller ports
- At least one standard 3½-inch floppy disk port
- Two serial ports
- One SPP/EPP/ECP parallel port
- Minimum of two USB2 ports (better if the ports are on the front of the computer)
- Adaptec FireWire card or similar quality or built-in FireWire ports
- Serial ATA controller port(s)
- A built-in Gigabit network connection

The motherboard must have auto-sensing BIOS supporting LBA and C/H/S mode hard drives.

Sound, Network and SCSI Cards

- A SoundBlaster AWE32-compatible sound card (built-in cards are fine)
- An Adaptec 29160N SCSI adapter card or similar quality and cabling to match the card

Case and Drive Mounting

A full ATX tower case with five to eight external 5¼-inch drive bay slots and two 3½-inch floppy drive bay slots. All hard drives can be mounted using removable drive bays with dual fans (one fan in the rack and one in the tray). Slide racks install in the computer, which allow for the easy addition and removal of hard drives. In addition, you need a 2½-inch to 3½-inch adapter (converts a laptop hard drive to fit a standard 40-pin IDE cable) and an ATA to Serial ATA adaptor (converts PATA to Serial ATA).

Power Supply

A minimum of a 400 watt modular power supply is needed. Consult your motherboard and processor guides for exact power requirements.

Monitor

One 21-inch and one 19-inch monitor (two 21-inch monitors are preferred). Also, LCD monitors are preferred because they take up less space and generate less heat. Some of the newer monitors provide DVI input.

Hard Drives

One Serial ATA hard drive per operating system (that is, one for Win2K, one for Linux, etc.). We recommend a minimum of two 160+ gigabyte hard drives for the forensic drives. The hard drives should be Serial ATA for performance reasons.

Floppy Drive

A 3½-inch floppy.

CD Drives

A CD-RW is needed in order to review CDs, transfer data to investigators and archive data.

DVD Burner

A DVD player is recommended in order to view DVDs and load some software. A DVD burner can be used to archive information. A dual-layer DVD burner will allow you to store more information.

Memory (RAM)

Four gigabytes of RAM (Random Access Memory) are recommended but no less than two gigabytes. The memory must match the motherboard's RAM specifications and should be the fastest type possible for it.

Video Display Card

A PCI Express 16x display card with a minimum of 256 megabytes of memory (DDR is preferred) that is capable of supporting DirectX writes is needed. Ideally, the video card will support two monitors at a time. Choose a card that provides dual DVI output. If the card does not support two monitors, then a second card will be needed if you want to use two monitors. The PCI express card must match what is on the motherboard. Cards may not be interchangeable.

Peripherals

A laser printer is recommended for high-speed printing of text or black-and-white photos. For color photos, either a color laser printer or a good quality inkjet printer is recommended.

Removable Media Reading Devices

Consider the amount of removable media, including memory sticks, Compact Flash, Secure Digital and others. These removable media are found in PDAs, digital cameras and many other devices. A device that reads all these different formats needs to be purchased.

Hard Drive Blockers

A hard drive blocker is a physical device that sits between your suspect's drive and your computer. This device prevents any writes to the suspect's hard drive.

Caution: All hard drive blockers must be validated before using.

Validation is independently verifying that the hard drive blocker works the way it claims to. The following are Web sites of companies offering hard drive blocker hardware:

www.digitalintel.com

www.vogon.us

www.encase.com

www.mykeytech.com

www.wiebetech.com

www.blackbagtech.com

www.ics-iq.com

www.acard.com

A good reference for write-blocker information is: www.cftt.nist.gov

Software Recommendations

The following software recommendations are for drive duplication, image processing and miscellaneous purposes (including graphics and text viewers, miscellaneous utilities and operating systems).

Drive Duplication Software

Drive duplication software makes a true and accurate copy of the drive. It is recommended that you have at least two of these programs because all programs do not work in all situations. A good source of information on making true and accurate copies of media is: www.cfft.nist.gov

Caution: All programs that make a duplicate image of a drive must be validated before using. Validation is independently verifying that the duplicate image program works the way it claims to.

| Product | Company | Drive-to-Drive? | Drive-to-Image? | Segmented? | Website |
|------------------------|------------------------|-----------------|-----------------|------------|--|
| Byte Back ² | Tech Assist, Inc. | Yes | Yes | Yes | www.toolsthatwork.com |
| EnCase | Guidance Software | No | Yes | Yes | www.encase.com |
| Forensic Toolkit | AccessData | No | Yes | Yes | www.accessdata.com |
| Ghost ³ | Symantec | No | Yes | Yes | www.symantec.com |
| ILook | Law enforcement only | No | Yes | Yes | www.ilook-forensics.org/ |
| Linux DD | | No | Yes | Yes | www.cfft.nist.gov/disk_imaging.htm |
| ProDiscover | Technology Pathways | No | Yes | Yes | www.techpathways.com |
| SafeBack ⁴ | New Technologies, Inc. | Yes | Yes | Yes | www.forensics-intl.com |
| SMART | ASR Data | No | Yes | Yes | www.asrdata.com |

² Has additional features and data recovery capability.

³ Ghost in the RAW mode.

⁴ Version 2.2 supported by Encase, ILook and FTK. Version 3 supported only by Encase.

Image Processing Software

These four programs actually process an image. They perform file searches, text searching and data recovery, including on deleted files.

| Product | Company | Processes an Image? | Makes a Duplicate Image? | Reads SafeBack Images? | Reads EnCase Images? | Reads DD Images? | Website |
|--------------------------|----------------------|---------------------|--------------------------|------------------------|----------------------|------------------|--|
| EnCase | Guidance Software | Yes | Yes | Yes | Yes | Yes | www.encase.com |
| Forensic Toolkit | AccessData | Yes | Yes | Yes | Yes | Yes | www.accessdata.com |
| ILook | Law enforcement only | Yes | Yes | Yes | Yes | Yes | www.ilook-forensics.org/ |
| ProDiscover ⁵ | Technology Pathways | Yes | Yes | No | No | Yes | www.techpathways.com |

Miscellaneous Software

Programs from the *Graphics and Text Viewers* table, as well as from the *Miscellaneous Utilities* table, will be needed. It is recommended that a forensic toolkit have at least two programs from the *Graphic and Text Viewers* table.

You need to have at least one anti-virus program and one spyware remover. They should be separate programs.

Graphics and Text Viewers

| Product | File Viewer? | Graphics Viewer? | Website |
|----------------------|--------------|------------------|--|
| ACDSee | No | Yes | www.acdsee.com |
| Adobe Acrobat Reader | PDF only | No | www.adobe.com |
| Conversions Plus | Yes | Yes | www.dataviz.com |
| Firehand Ember | No | Yes | www.firehand.com |
| Graphics Workshop | No | Yes | www.mindworkshop.com |
| IrfanView | No | Yes | www.irfanview.com |
| KeyView Pro | Yes | Yes | www.keyview.com |
| LView Pro | No | Yes | www.lview.com |
| PhotoStudio | No | Yes | www.stuffware.co.uk |
| Quick View Plus | Yes | Yes | www.avantstar.com |
| ThumbsPlus | No | Yes | www.cerious.com |

⁵ Prodiscover has a free version.

Miscellaneous Utilities

| Product | Company | Able to Unerase? | Text Search? | Operating System | Notes | Website |
|---------------------------|-----------------------|------------------|--------------|--|---|--|
| Camtasia | TechSmith | No | No | All Win versions | Makes movie-clip screen captures | www.techsmith.com |
| Captain Nemo | Runtime Software | No | Yes | All Win versions | Allows for viewing of WinNT, Win2K and Linux hard drives from Win98 | www.runtime.org |
| DiskExplorer for NTFS | Runtime Software | No | Yes | Win2K/WinXP | Disk editor and explorer | www.runtime.org |
| DriveSpy | Digital Intelligence | Yes | Yes | Win9x – Logical, Win2K, WinNT, Linux at physical level | Runs from a boot floppy: file uneraser, drive hasher, key word searcher | www.digitalintel.com |
| Easy Recovery Pro | Ontrack Data Recovery | No | No | Win9x | Recovers a formatted drive | www.ontrack.com |
| E-mail Examiner | Paraben | No | No | All Win versions | Email viewer | www.paraben-forensics.com |
| Mailbag Assistant | Fookes Software | No | No | All Win versions | Email viewer | www.fookes.com |
| NTFSDOS Professional | Winternals | No | No | Boot floppy | Allows a boot floppy to view Win NT/Win2k | www.winternals.com |
| Password Recovery Toolkit | AccessData | No | No | All Win versions | Password cracker for applications | www.accessdata.com |
| RecoverNT | LC Technology | Yes | No | All Win versions | Allows for recovery of formatted drives | www.lc-tech.com |
| SnagIt | TechSmith | No | No | Win95B or better | Captures screen images | www.techsmith.com |
| WhatFormat | (Shareware) | No | No | All Win versions | Determines file format from header | www.jozy.nl/whatfmt.html |

Operating Systems

In order to process a drive, you may need an operating system identical to that used by the suspect so that the same conditions can be created. A variety of operating systems are useful to have. The following list is a good summary of the operating systems you might need:

- Windows 98
- Windows ME
- Windows Home and Media Center
- Windows XP Pro
- Windows 2000 Professional
- Windows 2003 Server
- Linux

Optional Hardware

Scanner

A high-end scanner is recommended so that paper evidence can be converted into electronic evidence, and then put on a CD. Using OCR (Optical Character Recognition) will also make the scanned files somewhat text searchable, depending on the quality of the document to begin with.