
Creating a Forensic Computer System: Basic Hardware and Software Specifications

SEARCH Training Services
July 2004



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.cfft.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, July 2004.

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 (3.2+ GHz) or AMD Athlon 3200+ processor
- Three to five PCI expansion slots
- PCI Express Slot (fairly rare but have more speed for network connections and graphics)
- Two ATA/100 or ATA/133 EIDE controller ports
- At least one standard 3-1/2-inch floppy disk port
- Two serial ports
- One SPP/EPP/ECP parallel port
- 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)
- An 8x AGP port
- A build-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
- 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 eight to 10 external 5-1/4-inch drive bay slots and two 3-1/2-inch floppy drive bay slots. All hard drives are 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 2-1/2-inch-to-3-1/2-inch adapter (converts a laptop hard drive to fit a standard 40-pin IDE cable) and an ATA to Serial ATA adaptor (converts ATA to Serial ATA).

Power Supply

A minimum of a 400 watt power supply is needed. Consult your motherboard and processor guides for exact power requirements. Some power supplies are certified by motherboard manufacturers as being compatible with their equipment.

Monitor

A 19-inch monitor is recommended. Two 19-inch monitors are ideal, however. Also, LCD monitors are preferred because they take up less space and generate less heat.

Hard Drives

One 60 gigabyte Serial ATA hard drive is the minimum needed for every operating system you run as the operating system on your computer (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 floppy drive with both 3-1/2-inch and 5-1/4-inch media slots is recommended. However, because 5-1/4-inch drives are less common, having only a 3-1/2-inch drive will be sufficient in most situations.

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.

Memory (RAM)

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

Note: If you are going to use Windows 98 on this box, there is a limitation of 768 MB of RAM that Windows 98 can work with. Any more than 768 MB and Windows 98 can become very unstable.

Video Display Card

An 8x AGP display card with a minimum of 128 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. If the card does not support two monitors, then a second card will be needed if you want to use two monitors. The AGP card must match what is on the motherboard. AGP 2x, 4x and 8x are not 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				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?	Reads Snapback Images?	Website
EnCase	Guidance Software	Yes	Yes	Yes	Yes	Yes	No	www.encase.com
Forensic Toolkit	AccessData	Yes	No	Yes	Yes	Yes	Yes	www.accessdata.com
ILook	Law enforcement only	Yes	Yes	Yes	Yes	Yes	No	www.ilook-forensics.org/
ProDiscover	Technology Pathways	Yes	Yes	No	No	No	No	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. It is recommended that all forensics toolkits have a copy of Norton's Utilities and Drivespy, as well as other software as needed.

Graphics and Text Viewers

Product	File Viewer?	Graphics Viewer?	Website
ACDSee	No	Yes	www.acdsee.com
Adobe Acrobat Reader	Yes	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

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
DiskSearch Pro	New Technologies	No	Yes	Boot floppy	Searches for key words on a physical or logical level	www.forensics-intl.com
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
Maresware: The Suite ⁵	Mares and Company	No	Yes	Boot floppy	Suite of programs (key word searcher, drive hashing program, etc.)	www.dmares.com
Norton's Utilities	Symantec	Yes ⁶	Yes ⁷	Win9x/ME	Suite of programs (disk editor, file undeleter, etc.)	www.symantec.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
PDBlock	Digital Intelligence	No	No	Boot floppy	Hard drive write blocker	www.digitalintel.com
PowerDesk Pro	Ontrack Data Recovery	No	No	All Win versions	File manager	www.ontrack.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

⁵ Part of a suite of programs for evidence processing.

⁶ FAT16 and FAT 32 only.

⁷ Can search only one word at a time.

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:

- Dos 6.22
- Windows 98SE
- Windows ME
- Windows NT WorkStation
- Windows NT Server
- Windows XP Pro
- Windows 2000 Professional
- Windows 2003 Server
- Linux

Optional Hardware

ZIP drive

The 750 megabyte and 100 megabyte models of the Iomega ZIP drive. This is because the 750 megabyte model is not always a backward-compatible drive for loading software, making forensic copies and reviewing seized ZIP disks.

DAT Tape Drive

An HP 4mm or 8mm DAT drive (40/80 gigabyte) for digital tapes.

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.