Computer Forensics Hardware Tools

- Hardware is hardware; whether it’s a rack-mounted server or a forensic workstation, eventually it fails.
- For this reason, you should schedule equipment replacements periodically—ideally, every 18 months if you use the hardware fulltime.
- Most computer forensics operations use a workstation 24 hours a day for a week or

longer between complete shutdowns.

…………..

- You should plan your hardware needs carefully, especially if you have budget limitations.
- The longer you expect the forensic workstation to be running, the more you need to anticipate physical equipment failure and the expense of replacement equipment.

Forensic Workstations

- Many computer vendors offer a wide range of forensic workstations that you can tailor to meet your investigation needs.
- Forensic workstations can be divided into the following categories:
- Stationary workstation—A tower with several bays and many peripheral devices
- Portable workstation—A laptop computer with a built-in LCD monitor and almost as many bays and peripherals as a stationary workstation
- Lightweight workstation—Usually a laptop computer built into a carrying case with a small selection of peripheral options.

Building Your Own Workstation

- If you have the time and skill to build your own forensic workstation, you can customize it to your needs and save money, although you might have trouble finding support for problems that develop.
- For example, peripheral devices might conflict with one another, or components might fail. If you build your own forensic workstation, you

should be able to support the hardware. ……

- If you decide that building a forensic workstation is beyond your skills, several vendors offer workstations designed for computer forensics, such as the F.R.E.D. unit from Digital Intelligence or the Dual Xeon Workstation from Forensic PC.
- Having a vendor-supplied workstation has its advantages.

Using a Write-Blocker

- The first item you should consider for a forensic workstation is a write-blocker.
- Write blockers protect evidence disks by preventing data from being written to them. Software and hardware write-blockers perform the same function but in a different fashion.
- Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode (for example, DOS).

……..

- If you attempt to write data to the blocked drive, an alarm sounds, advising that no writes have occurred.
- With hardware write-blockers, you can connect the evidence drive to your workstation and start the OS as usual.
- Hardware write-blockers are ideal for GUI forensics tools. They prevent Windows or Linux from writing data to the blocked drive.
- Hardware write-blockers act as a bridge between the suspect drive and the forensic workstation

……

- Many vendors have developed write-blocking devices that connect to a computer through FireWire, USB 2.0, SATA, and SCSI controllers.
- Most of these write-blockers enable you to remove and reconnect drives without having to shut down your workstation, which saves time in processing the evidence drive.

Validating and Testing Forensics Software

- Using National Institute of Standards and Technology (NIST) Tools :NIST has created criteria for testing computer forensics tools, which are included in the articlen“General Test Methodology for Computer Forensic Tools”.

Testing Standards:

- Establish categories for computer forensics tools
- Identify computer forensics category requirements
- Develop test assertions
- Identify test cases
- Establish a test method
- Report test result

Using Validation Protocols

- After retrieving and examining evidence data with one tool, you should verify your results by performing the same tasks with other similar forensics tools.
- For example, after you use one forensics tool to retrieve disk data, you use another to see whether you retrieve the same information.
- Although this step might seem unnecessary, you might be asked on the witness stand “How did you verify your results?” To satisfy the need for verification, you need at least two tools to validate software or hardware upgrades.
- The tool you use to validate the results should be well

tested and documented.

Computer Forensics Examination Protocol

1. First, conduct your investigation of the digital evidence with one GUI tool.
2. Then perform the same investigation with a disk editor to verify that the GUI tool is seeing the same digital evidence in the same places on the test or suspect drive's image.
3. If a file is recovered, obtain the hash value with the GUI tool and the disk editor, and then compare the results to verify whether the file has

the same value in both tools.

Computer Forensics Tool Upgrade Protocol

- In addition to verifying your results by using two disk-analysis tools, you should test all new releases and OS patches and upgrades to make sure they’re reliable and don’t corrupt evidence data.
- New releases and OS upgrades and patches can affect the way your forensics tools perform.