Digital Forensic Investigations
COS783
Digital Forensic Tools – Hardware

Prof HS Venter
hventer@cs.up.ac.za
Copyright © HS Venter (2015)

Contents

• Introduction
• Computers
  – Power supply, Hard drive, Motherboard
• Laptops/Tablets
• External storage
• Servers
• iPods/PDAs/Cell phones/media players
• Hardware tools overview
• Conclusion
Introduction

• The purpose of this lecture is to familiarise to you the hardware components used most often in a DF investigation
• Hardware forensics is not only about computers
  – Includes other devices and more as on previous slide
• Mainly interested in the storage components
• Many people have basic understanding of how to use a computer, but not how it works!
• ANY device capable of storing digital data

Computers

• Main components
  – Motherboard
    • I/O modules
      – IDE (ATA)
      – SATA
    • CPU/GPU
    • System bus
    • Expansion slots
    • BIOS
  – Input devices
  – Output devices
  – Storage
    • HDD (SSD)
    • USB
  • Primary RAM
Laptops/Tablets

• Components very similar to desktop computer, just more compact and integrated.
• Typically no expansion slots
• Graphics interface, network interface, etc all integrated on motherboard
• RAM is about only expansion component for laptops

External storage

• Old floppy/stiffie disks (not really used anymore)
• USB flash drives
  – EEPROM
  – Why is it called a “flash” drive?
• External HDDs/SSDs
• Optical drives
  – CDROM
  – DVD
  – BluRay
Servers

- Servers also very similar to desktop computer, just faster and more expensive hardware
- And biggest issue in terms of DF – MUCH more storage capacity!
- Client/server environment

iPods/PDAs/Cell phones/media players

- Small & compact
- Popular
- All comes with significant storage capacities
  - SSDs
  - Flash memory
  - SIM cards (what does SIM stand for?)
  - Networking capabilities
    - Bluetooth
    - GSM/GPRS/HSDPA/LTE/3G/4G
    - WiFi
Hardware digital forensic tools

• Features and advantages of hardware tools are based on techniques that substitute software because it is compact and easy to operate, e.g.
  – Embedded development that has been completed, saving space and time and generally simplifying the acquisition process
  – The greater portability of the products
  – The increased speed of acquiring of digital data

• HDD write protection tools (write blockers)
  – No write
  – Wiebetech’s FireWire DriveDock
Hardware digital forensic tools

• HDD write protection tools (write blockers)
  – LockDown by Paraben

• HDD write protection tools (write blockers)
  – Write Protect Card Reader: Intelligent Comp. Solutions
  – Serial-ATA DriveLock Kit & DriveLock IDE HDD write protection from Intelligent Computer Solutions (ICS)
Hardware digital forensic tools

• Wipe MASSter (ICS) is a commercial drive wiper

Hardware digital forensic tools

• ImageMASSter Solo-3 IT from ICS designed exclusively for forensic data acquisition
• ImageMASSter 4002i for fast direct imaging between two HDDs
• ImageMASSter 3002SCSI – even faster
• ImageMASSter 3002SCSI for SATA
Hardware digital forensic workstations

- Combinations of hardware (and software) can be put together to actually form a DF workstation
- Moore’s law: Hardware ages +- every 18 months
  - Then needs to be replaced
  - Hardware often fail when it ages
  - Need to replace hardware BEFORE it fails!
- Hardware planning needs to be done carefully, especially when you have a constrained budget

Hardware digital forensic workstations

- 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 almost as many bays and peripheral devices than a stationary workstation
    - Often much more expensive due to the same hardware requirements as the stationary workstation, but has the mobility factor added (causing the cost to rise significantly)
  - Lightweight workstation
    - Still portable, but built into a carry case (like a laptop) with less peripheral devices
• Be careful when selecting a basic workstation – cannot support many peripherals
• If you need a forensic workstation in a police department, you need many peripherals
• Should keep a hardware library in addition to software library
  – Need different configurations in different scenarios
• In private/internal environment, can streamline the workstation more to suit the particular needs

• Can build your own workstation from scratch if you have the necessary background
• Determine what the nature of your cases will be
  – The wider the range of cases might be, the more hardware/peripherals you will need, and the more expensive it will get
• Newer write-blockers use USB, and direct connection to IDE/SATA is not necessary anymore, but need both types to be compatible with acquiring data off older disks
Hardware digital forensic workstations

- Minimal configuration for light-weight workstation
  - Full tower
    - Allows for expansion of 2.5” and 3.5” drives
  - As much RAM as budget allows (at least 16GB)
  - As much processing power as possible (at least 3.5Ghz 8-core CPU)
  - As much Drive space as budget allows (> 4TB)
  - 500W power supply or more
  - Battery backup (UPS)
  - Extra power & data cables
  - SCSI card, firewire & USB ports
  - Ergonomic keyboard & mouse
  - Good video card and at least 21” monitor (or multiple)

Hardware Security Tools used in Digital Forensic Operations
Core labs

- Email tracking
- Interviewing suspects and witnesses
- Gathering physical evidence
- Gathering digital evidence
- Password cracking
- Investigating log files
- Imaging drives
- Extracting digital evidence
- Investigating Web hacking incidents
- Restoring files
- Investigating wireless incidents
- Understanding biometric techniques…

Hardware Forensics (1) – Different methods of acquiring images

- Different types, each with different advantages & disadvantages
  - Direct connection
    - Connect drive directly to IDE ribbon cable
    - Fast
  - External HD case
    - Fast if used with USB3
  - Network acquisition
    - Connect computer with cross-over cable
Hardware Forensics (1) – Different methods of acquiring images

- # dd if=/dev/fd0 of=/home/doc.img bs=512
  - Make a bit-by-bit copy of a device to an image file.

Firewire/USB connection with write-blocker

Write-block is necessary for imaging under Windows
Direct IDE connection

No write-blocker necessary if imaging under Linux

External Firewire drive connector
Hardware Forensics (2) – Authenticate the evidence

- # md5sum /dev/fd0 > evidence.md5
  - Generate a one-way hash of the (original) floppy, redirect to a file.
- # md5sum floppy.dd >> evidence.md5
  - Do the same for our bit image copy, append the value to our evidence.md5 file
- # cat evidence.md5
  - Are they the same? Good!
- # date
  - Other side of the sandwich

Hardware Forensics (3) – Preview & image with Linux: Analyze with Windows

- File system maximum file sizes
  - FAT32 = 4 GB, NTFS = 2 Terabytes
  - EXT2/3 = 2 Terabyte, ReiserFS = 1 Exabyte
  - (LFS) Large Files System support must be compiled in.
- Easy to copy files to and from FAT32 drive
  - Limited to 4GB, very small?
- How to copy a very large file from Linux to an NTFS volume
  - Not well supported by Linux, but getting better
  - Supported by some 3rd party commercial drivers
Linux Forensics – References

- Free Linux distributions
  - Fedora Core (based on Redhat)
    • fedora.redhat.com
  - FIRE: Forensic Incident Response Environment
    • fire.dmzs.com
  - Knoppix (bootable CD, HD installable)
    • www.knoppix.org
  - Kali Linux

Conclusion

- Hardware forensics is a “quick” solution to accomplish some of the basic tasks in a DF investigation
- Hardware is typically more expensive than software and it will depend heavily on the available DF budget
  - Needs should be clarified before money is spent on expensive hardware
- Using the right combination of hardware is important
- Choices in hardware effect choices in software