Computer Forensics Tutorials

Instructor	Dr.Abdul Rehman Al-Ghamdi	Phone	+966-503770707
Office	CCIT	Version	Two
Office Hours	0800 – 1400Hours	Email	

2.1 The required skill for a computer forensics expert

Digital forensic experts need to have a vast array of knowledge regarding computers, on both the hardware and software sides. They must have intricate knowledge of computer operating systems, including the BIOS, and should be very familiar with Linux, Mac OS and Windows.Besides all these computer skills a digital forensic experts must also possess strong analytical and investigative skills.

2.2 Role of forensic experts.

The job of a forensic computer investigator or digital forensic expert often includes:

- *Recovering data from damaged or erased hard drives*
- *Tracing hacks*
- *Gathering and maintaining evidence*
- *Writing and reviewing investigative reports*
- *Working with computers and other electronic equipment*
- *Working closely with other police officers and detectives*

2.3 The bottom-up view of a computer

The modern computer is much like the human body. Different modules each perform simple tasks; put them together in the right way, and amazingly complex tasks can be completed. A heart pumps blood. The lungs move air around. Eyes process light to create images. These are very basic tasks that work simultaneously to sustain life. Computers work in a similar way. A processor performs operations. A hard disk stores

1s and 0s. A video card converts those 1s and 0s to signals a monitor can understand. Put them together and you get the computer and all the possibilities that go along with it.

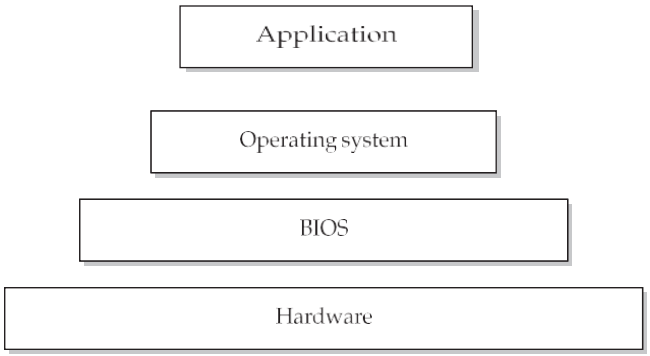

Figure 2-1 The layers of a computer

2.4 Computers Memory

Computers use two basic types of memory: volatile and nonvolatile. Volatile memory is difficult to retrieve when the computer is turned off. Examples of this type of memory are main memory (RAM, or Random Access Memory) and cache memory. Nonvolatile memory is not difficult to retrieve when the computer is turned off. This is usually the secondary memory source, such as hard disks or flash memory. Figure 2-3 shows the interaction of the various types of memory.

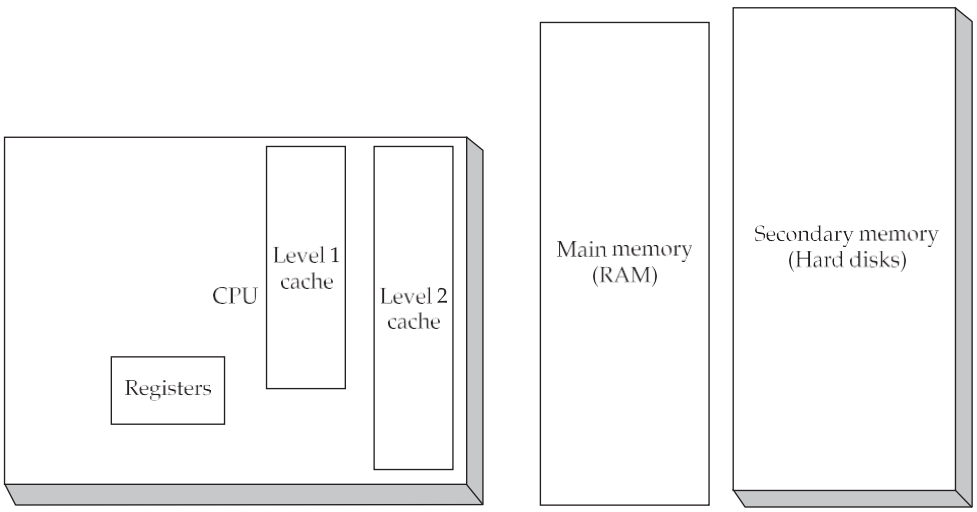

Figure 2-3 The memory hierarchy of a computer

2.5 Basic Input and Output System (BIOS)

The BIOS provides simple methods for software to interact with hardware. When you first turn on the computer, the BIOS runs a series of self-checks (called the Power On Self-Test, or POST) and then turns control over to the operating system. This transition occurs by way of what is called the Master Boot Record (MBR) on the hard drive.

An effective BIOS manages the allocation of resources (via interrupt requests, or IRQs, and direct memory access, or DMA) to the peripherals and handles basic security measures. The BIOS provides only raw access to the resources; it does nothing to manage or allocate those resources for performance. Its function is strictly to act as the interface between the OS and the hardware.

2.6 The Operating System

The OS is by far the most complex piece of software on any given computer. It acts as the translation layer between the end-user applications and the BIOS or hardware. The OS manages the users, the memory, the applications, and the processor time on the computer. A well-written OS can breathe new life into an old computer, same as a poorly written one can bog down even the fastest of machines. As an investigator, I recommend that you spend time learning the mainstream OSs inside and out.

NOTE *Learning about an OS is not a trivial task. Windows XP has more than 5 million lines of code. The file system, the swap space, and the memory map are all artifacts of the OS installed on the machine. We devote Chapters 6, 7, and 8 to discussions of various operating systems.*

2.7 The Applications

Applications are why you use a computer in the first place. They balance our checkbooks, allow us to browse the Internet, or entertain us with games, movies, or other activities. From a forensics perspective, it is beneficial for you to become familiar with the ins and outs of a few select applications.

2.8 Types of media

As discussed in the preceding section, investigations will focus primarily on the secondary memory area—hard disks, CD-ROMs, tape backups, and most other types of commonly used storage. Each of these types of media has its own nuances and pitfalls in an investigation. Let's look at the three most common types of media—magnetic, optical, and RAM—in detail.

2.8.1 Magnetic Media

You will spend the majority of your time dealing with magnetic media, including hard disks, floppy disks, and tape backups. The theory for all of these types is the same: Some kind of metal or magnetic surface holds a series of positive or negative magnetic charges. This series represents 1s or 0s, depending on the charge of the magnet. When data is changed on the media, the magnetic charge is changed. This means several things: First, there are moving parts, and moving parts are susceptible to breaking. Always have backups. Second, the media is open to being affected by external magnets. This means that your forensic lab procedures and storage policies must consider this, and you must be able to prove that this hasn't happened when dealing in a court of law.

If you learn the complete architecture for just one media type, make it the hard drive. Ninety percent of an investigator's time will be spent imaging, searching, or wiping hard drives, and none of these are as easy as they might seem. Let's break down a hard drive's components and how those components interact.

2.8.1.1 Physical Parts of the Hard Drive

Before we look at how data is stored on a hard drive, we need to talk a bit about the physical components of the drive. Hard drives are marvels of modern engineering. Imagine a plane traveling Mach 1 with an altitude of about 2 feet above the runway. This is the rough equivalent to what a hard drive does every time it spins up and reads or writes data. Figure 2-4 shows the parts of a hard drive.

Platters are the circular discs that actually store the data. A single hard drive will include multiple platters often made of some aluminum alloy, but newer drives use a

glass or ceramic material. These platters are covered with a magnetic substrate so that they can hold a magnetic charge. Hard drive failures rarely occur within the platters. In fact, nine times out of ten, if you send a drive off to a data recovery firm, it will take the drive apart and mount the platters in a new drive assembly to retrieve the data from them.

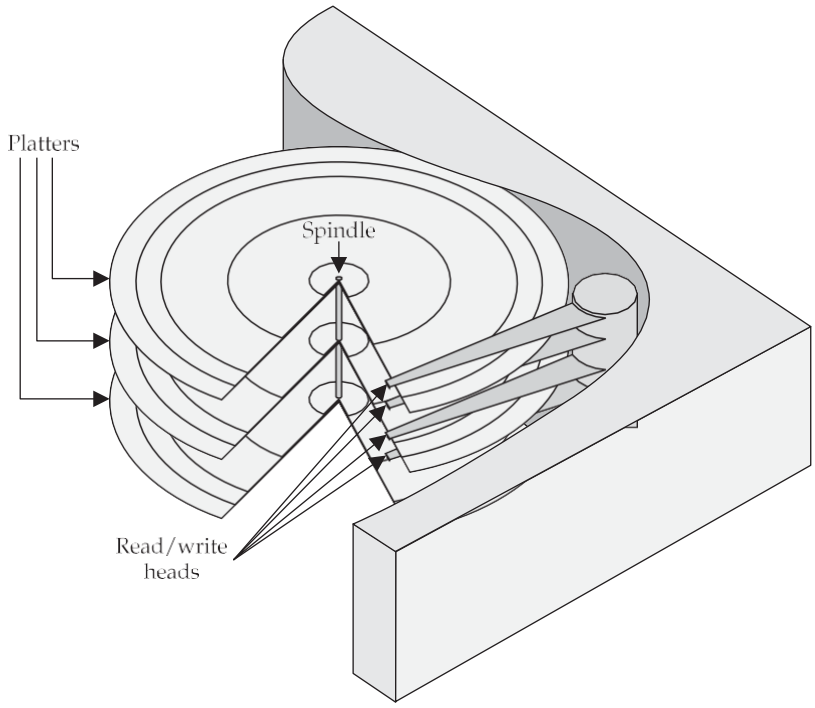

Figure 2-4 the parts of a hard drive

2.8.2 Optical Media

These days, optical media is everywhere in the forms of CD-ROM and DVD. With the widespread ability for users to burn their own discs, such media are finding their way into more and more court cases. Chances are you will deal with them either directly as evidence or as a transport mechanism for opposing counsel to give you evidence during discovery. It's important that you understand how these technologies work and how they can be manipulated.

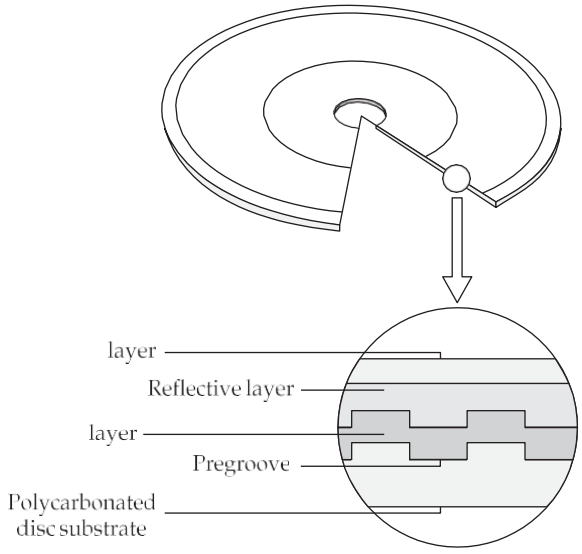

Figure 2-5 Parts of a CD-ROM

2.8.3 Memory Technologies

If you have used a digital camera,USB flash, an MP3 player, or a PDA/smartphone, you have used a memory technology. These are the memory cards and cartridges that store the pictures, music, and data for these devices. As you can imagine, they often become evidence in investigations, so it's a good idea for you to understand how they work and what you are up against.