Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 15

Computer Basics for Digital Investigators

- Basic Operation:
    - Power Supply
    - CPU
        - CU
        - ALU
    - BIOS
    - POST: Contained in the BIOS and tests the hardware components
    - CMOS: Intel based systems (Complementary Metal Oxide Silicon). Chip that holds date, time, and hardware configuration. Before POST starts, you can enter the CMOS configuration tool and update the CMOS. **This is where you can find the system time!
    - From the BIOS you go to the OS.
- Basic computer hardware (inside of a computer).
- How is data stored on a computer (binary).
- From binary to "readable" characters: ASCII, then Unicode.
- Big-Endian, Little-Endian. Windows Unicode (mostly LE).
- Why is this important? Depends on how data is stored for the particular file that you are looking at.
- File formats and carving:
    - Many files have a standard set of characters that are placed at the top of the file, called a file signature. Table 15-4.
    - Carving: the process of searching for a certain file signature and attempting to extract the associated data.
    - PP, jpeg raw data.
    - When you carve a file you will not get the info that is stored by the OS, like time stamps. But at least you get the file.
    - Carving is used to recover deleted files.
- Hard Drives:
    - IDE (Integrated Disk Electronics),
    - ATA (Advanced Technology Attachment),
    - SATA (Serial ATA),
    - SCSI (Small Computer System Interface),
    - SAS (Serial Attached SCSI),
    - How is data stored?
    - Disk platter style.
        - Data is recorded in concentric circles called tracks (cylinder all tracks with same radius on drive),
        - Track is broken down into sectors (usually 512 bytes big),
        - A cluster is the basic storage unit on the disk.

    - CHS (Cylinder, head, sector) addressing,
    - The number of CHS on the drive is usually written on the outside of the drive. Can use to calculate the size of the drive if it isn't printed. Use that to ensure you copied all of the data from the drive.
    - SMART information.
  - Solid state (flash chips)
- Data Hiding:
  - Usually the first cylinder on a disk is not used by the OS, instead it is used to store drive information. Modern forensic tools automatically check this area.
  - Also, you can hide data in the DCO (drive configuration overlay) or the HPA (host protected area).
  - Both of these areas are rarely used, but can be used.
  - Hidden partitions and encrypted disks.
  - Modern forensics tools examine these hidden partitions.
  - Encryption is a major problem.
- File Systems:
  - Used to keep track of where files are on the disk.
  - Common File Systems:

UDF	Universal Disk Format	DVDs
ISO		CDs, disk image
Joliet		CDs
CDFS	Compact Disc File Sys.	CDs
FAT 12/16/32	File Allocation Table	DOS/WIN9x OS/Solid State Media
EXT 2/3/4	Extended File System	Linux OS
NTFS	New Tech. File System	WIN NT/>9x
NTFS Compressed		
HFS/HFS+/HFSX	Hierachical File System	Mac OS
ReiserFS		Elive, Xandros, Linspire, GoboLinux, Yoper Linux
VXFS	Veritas File System	
AFF	Advanced Forensic Format	

  - First, a drive has to have a partition created.
  - Then it is formatted with a file system.
  - First sector of the drive gets the MBR. This contains the partition table.
  - Reformatting does not necessarily delete the data.
  - Boot sector (look at diskedit) contains the information about the partition.
  - Partition (volume) slack.
  - When a file is placed into a cluster, if it doesn't use all of the cluster then the rest of the space is unused and called file slack space.
  - When a file is deleted the FAT table is updated to indicate that the clusters are unallocated.

- If the new file doesn’t take the entire cluster, then you can get “bits” of the old file that remains on the cluster.

- Data hiding, continued:
    - Changing file names. (file signatures)
    - Checking the hidden file box on Windows.
    - Embedding information in other files (JPG into PP)
    - Steganography.
    - Password protection. (PRTK)
    - Encryption:
        - Private Key Encryption (DES, IDEA).
        - Public Key Encryption (RSA, DSA)
        - PGP