ADVANCED COMPUTER FORENSICS

EnCE EnCase Forensics: The Official EnCase Certified Examiner Study Guide

CHAPTER 1

Computer Hardware Components

Computer Hardware Skills

- Necessary Skills to be successful
  - Troubleshooting and configuration fundamentals
    - Hardware
    - Booting
    - Partitions
    - File Systems

Computer Hardware Components (ROM & RAM)

- Hardware Components
  - Case
  - ROM – Read Only Memory
    - Ideal for startup configuration settings and boot code
  - RAM – Random Access Memory
    - Temporary and volatile memory space
    - NVRAM is not volatile so we *cannot* assume it is non0volatile
    - Forensically we usually encounter computers that are off – however because of “swap” files we can still access some of the RAM information. (hiberfil.sys)

Computer Hardware Components

- Hardware Components
  - Power Supply
  - Motherboard
    - CPU socket, BIOS, CMOS, CMOS batters, rtc, ram SLOTS, IDE controllers, SATA controllers, USB controllers, floppy, AGP, PCI/e
  - CPU – Central Processing Unit
  - Heat Sink and Fan
  - Hard Drive
    - 4,800-15,000 RPMs
    - Magnetic polarity for 1s and 0s
    - Sector – smallest amount of space on a drive that can be written to

Computer Hardware - Hard Drive

- Hardware Components
  - Hard Drive
    - C-H and S – C*H*S*512= total disk storage
    - Tracks, Cylinders, and read/write heads
    - Only good for older drives
    - ZBR – Zone Bit Recording was developed to overcome the wasted space in outer tracks
    - Newer drives use LBA – Logical Block Addressing
      - Use LBA*512 to establish the storage capacity of a drive using ZBR

Computer Hardware – Hard Drive Continued

- Hardware Components
  - Hard Drive
    - ATA – Advanced Technology Attachment or PATA – Parallel ATA
    - SATA – Serial Advanced Technology Attachment
    - SSD – Solid State Drive
      - No moving parts – Persistent (nonvolatile)
      - Housings – laptops, soldered to motherboard, rack mounted etc.
    - Hybrid
      - SSD with spinning platters (fast boots and reliable storage)

Computer Hardware – SCSI & IDE

- Hardware Components
  - SCSI – Small Computer Systems Interface
    - High speed and high performance
    - SCSI BIOS – queues read/write requests – High end systems
    - NO master-slave configurations – utilize ID numbers
  - IDE – Integrated Drive Electronics Controller
    - Any drive with its' own integrated controller
      - ATA only survivor from 3 – IDE and ATA are often used interchangeably
      - 2 connectors on mobo – primary and secondary each can handle 2 devices
      - One on each of the connectors is a master and the other is the slave on that connector

Computer Hardware – SATA & SAS

- Hardware Components
  - SATA – Serial Advanced Technology Attachment Controller
    - Up to 300 MBps as opposed to 133 for IDE drives
    - No pinning or jumpers
    - Contained in most modern motherboards
    - Forensic analysts can expect to see both SATA and IDE for some time to come
  - SAS – Serial Attached SCSI
    - Replaced SCSI (parallel) with point-to-point serial bus technology
      - Uses SCSI command sets
      - High end computers, server, data centers
      - Backward compatible with 2nd generation SATA – You can attach SATA drives to this backplane, but not an SAS drive to a SATA backplane (6Gbps-12Gbps)

Computer Hardware – RAID & Floppy

- Hardware Components
  - RAID – Redundant Array of Inexpensive Disks
    - 2 or more disks arranged in such a way to either increase performance or increase fault tolerance
      - RAID 0 – Striped over 2 or more disks – performance
      - RAID 1 – mirrored over drives in the array – fault tolerance
      - RAID 5 – 3 or more drives – striped over two drives and parity on a third – if one drive fails it can be “rebuilt”
      - RAID 0+1 – 4 drives one pair for striping and one pair as a mirror of the striped pair – performance and tolerance
      - RAID 1+0 – same as 0+1, but the mirror is built before the stipe
  - Floppy Drive
    - 1.44MB of data is the maximum
      - Used forensically as boot devices – ALWAYS PACK A 3.4 FLOPPY – INTERNAL
      - Being phased out, but still might be encountered!!

Computer Hardware – CD-ROM & DVD-ROM

- Hardware Components
  - CD-ROM – Compact Disc – Read Only or Read/Write Memory
    - Utilizes lasers to read indentations on flats as 1s and 0s
  - DVD-ROM – Digital Versatile Disc – Read Only or Read/Write Memory
    - Creates smaller pits then the CD and thus can allow for more data on the same space
      - CD – 700 MB of data
      - DVD – 8GB to 17GB of data if it is layered

Computer Hardware – USB, USB Port, & IEEE 1394

- Hardware Components
  - USB – Universal Serial Bus Controller
    - High speed input/output – plug-n-play devices
      - 1.1-1.5 Mbps
      - 2-480 Mbps
      - 3-5 Gbps
  - USB Port – Controller with pins
    - Cameras, storage devices, dongles, license keys, keyboards, mice, etc.
  - IEEE 1394 – FireWire
    - 1394A – 400 Mbps
    - 1394b – 800 Mbps
    - Daisy chain up to 63 devices
    - Different connection types

Computer Hardware – IEEE 1394a, IEEE1394b, & Thunderbolt Ports

- Hardware Components
  - IEEE 1394a Ports
    - Similar to USB except one end is slightly rounded
    - Used for high-speed external devices
    - 6 conductors
  - IEEE 1394b Ports – FireWire 800
    - Rectangular with a dimple for uniqueness
    - 9 conductors
    - 2 for shielding which assists in higher transfer rates
  - Thunderbolt Ports
    - 10 Gbps – bidirectional
    - High resolution graphics
    - Great for forensics

Computer Hardware – Expansion Slots & Sound Card

- Hardware Components
  - Expansion Slots
    - ISA, MCA, EISA, VL-Bus, PCI, AGP, PCI-Express
      - Obsolete – ISA, MCA, EISA, and VL-Bus
      - PCI – Peripheral Component Interconnect 32 or 64 bit interface
      - PCI-Express 1.0 – serial communications
      - AGP – based on PCI standards – connected for video (replaced by PCI-Express)
      - PCI – slated for extinction
      - Laptop use – PC Cards or PCMCIA cards – Personal Computer Card International Association (size of credit card)
  - Sound Card
    - Circuitry for multimedia sound
    - Chip on the mobo, hardware integrated – microphones, speakers, headphones

Computer Hardware – Video Card & RTC

- Hardware Components
  - Video Card (PCI, AGP, PCI-Express)
    - Images on a screen
      - Expansion card, chip on mobo, chipset
      - 15 pin VGA – Video Graphics Array (analog)
      - DVI – Digital Video Interface (analog/digital)
  - RTC – Real-Time Clock
    - System clock for storing date and time
    - Maintained by the CMOS battery and the CMOS chip
    - The CMOS chip is called the RTC / NVRAM – Nonvolatile RAM (CMOS data: type of floppy and HDD, amount of installed memory, other startup configurations)

Computer Hardware CMOS & CMOS Battery

- Hardware Components
  - CMOS – Complementary Metal-Oxide Semiconductor
    - How the RTC/NVRAM chip is produced
  - CMOS Battery
    - Powers the RTC/NVRAM chip
    - Long service life (10 years or more)
    - Some systems use a capacitor and battery or just a capacitor
    - BOOT BIOS password is retained by the CMOS chip

Computer Hardware – BIOS

- Hardware Components
  - BIOS – Basic Input Output System
    - Low-level software and drivers
      - Function as the interface between hardware and OS
      - Loads info into RAM
        - From mobo, adapter or disks – device drivers
  - BIOS and CMOS are often used interchangeably
    - User interface for settings in RTC/NVRAM is accessed through a setup program within BIOS. Settings are read by BIOS during boot
    - Forensically – RTC/NVRAM holds two important settings
      - System Date and Time
      - Boot Order

Computer Hardware – EFI, Mouse Port, & Keyboard Port

- Hardware Components
  - Extensible Firmware Interface (EFI) – UEFI
    - Designed to replace BIOS firmware
      - Sits between OS and hardware
      - Often called BIOS – Not correct
      - Intel – supports legacy PC BIOS – using EFI means that the boot loader is no longer needed
      - Macintosh computers utilize it as well in their Intel based computers
  - Mouse Port
  - Keyboard Port

Computer Hardware – NIC & MODEM

- Hardware Components
  - NIC – Network Interface Card
    - Can be an expansion card, on mobo or via USB
      - Unique hardware address (MAC) – Media Access Control
        - Utilized by the DLL – Data Link Layer to communicate with other MAC addresses on the network
        - Manufacturer and unique serial number
        - Need to disconnect the NW in order to avoid remote destruction of data
  - MODEM
    - Connect a computer to other computers using a telephone carrier
      - Modulates / demodulates – digital to analog / analog to digital

Computer Hardware – Parallel Port & Serial Port

- Hardware Components
  - Parallel Port
    - Legacy connection – replaced by USB
  - Serial Port
    - I/O port to connect serial data connections
    - RS-232 most common (becoming obsolete)

Boot Process

- Boot Process Flow Chart
  - Check out page 18
  - Review flow chard
- MBR – Master Boot Record
  - Located at offset 446 for 64 bytes (bytes 446-509)
    - hex 55AA – indicates boot partition
    - Much more detail in chapters to come – This area is EXTREMELY important to forensic examiners!!!!

Boot Process Prior to VISTA

Power

- CPU – Initializes itself and hands control to BIOS
- BIOS – runs POST – checking for HW issues
- Add on cards installed with their BIOS information
- BIOS looks to CMOS to establish boot order
- MBR – access first sector of boot disk
- BIOS – locates bootstrap loader – finds and launches OS
- Boot drive identified – VBR loads ***NTLDR / NTDETECT.COM*** on the volume

Boot Process VISTA and up

Power

- CPU – Initializes itself and hands control to BIOS
- BIOS – runs POST – checking for HW issues
- Add on cards installed with their BIOS information
- BIOS looks to CMOS to establish boot order
- MBR – access first sector of boot disk
- BIOS – locates bootstrap loader – finds and launches OS
- Boot drive identified – VBR loads ***BOOTMGR*** **– reads the BCD (Boot Configuration Data)**
  - ***BOOTMGR*** **– uses** ***WINLOAD.EXE*** **instead of** ***NTLDR*** **to load** ***NTOSKRNL.EXE***

Initial PC OS Required Files

- IO.SYS
- MSDOS.SYS
- COMMAND.COM
- CONFIG.SYS **OPTIONAL
- AUTOEXEC.BAT **OPTIONAL

Partitions

Partition

- Collection of consecutive sectors within a volume
  - Addressable by a single file system
- Volume
  - Collection of addressable sectors that are used by an OS or application to store data – do NOT have to be consecutive
    - Only needs to appear consecutive
    - When a volume has a single partition they are functionally the same
    - Volumes can span more than one partition or drive
    - Logical storage units with assigned drive letters by the OS – up to 24 volumes
    - Utilizes – Extended partitions to allow for the drive assignments

File Systems

Many different flavors

- FAT 12, FAT 16, FAT 32
- NTFS
- exFAT – proprietary
- Linux – EXT2/3/4 and Reiser
- Swap partitions
- Solaris – UFS
- Mac OS X – HFS+

Data – Bits-n-Bytes

- Bits-n-Bytes

[Instructor Selected Images]

Data

[Instructor Selected Images]

HEX

- One Hex = 4 bits or a nibble
- Usually written in pairs
  - 1 byte or 8 bits
- 1 byte = two hex characters

Conversions

[Instructor Selected Images]

- Binary to Hex

- Hex to Decimal

[Instructor Selected Images]

DOL Disclaimer and CCBY

This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.