Working with Windows and DOS Systems

Objectives

- Explain the purpose and structure of file systems
- Describe Microsoft file structures
- Explain the structure of New Technology File System (NTFS) disks
- List some options for decrypting drives encrypted with whole disk encryption
- Explain how the Windows Registry works
- Describe Microsoft startup tasks
- Describe MS-DOS startup tasks
- Explain the purpose of a virtual machine

Understanding File Systems

Understanding File Systems

- **File system**
  - Methods and data structures
  - The way the **files** are organized (stored) on the disk
  - OS uses this to keep track of **files** on a disk or partition
  - Gives OS a road map to data on a disk
  - Directly related to an OS
- When you need to access a suspect's computer to acquire or inspect data
  - be familiar with the computer's platform
- **Understanding the Boot Sequence**
- **Understanding Disk Drives**

Understanding the Boot Sequence

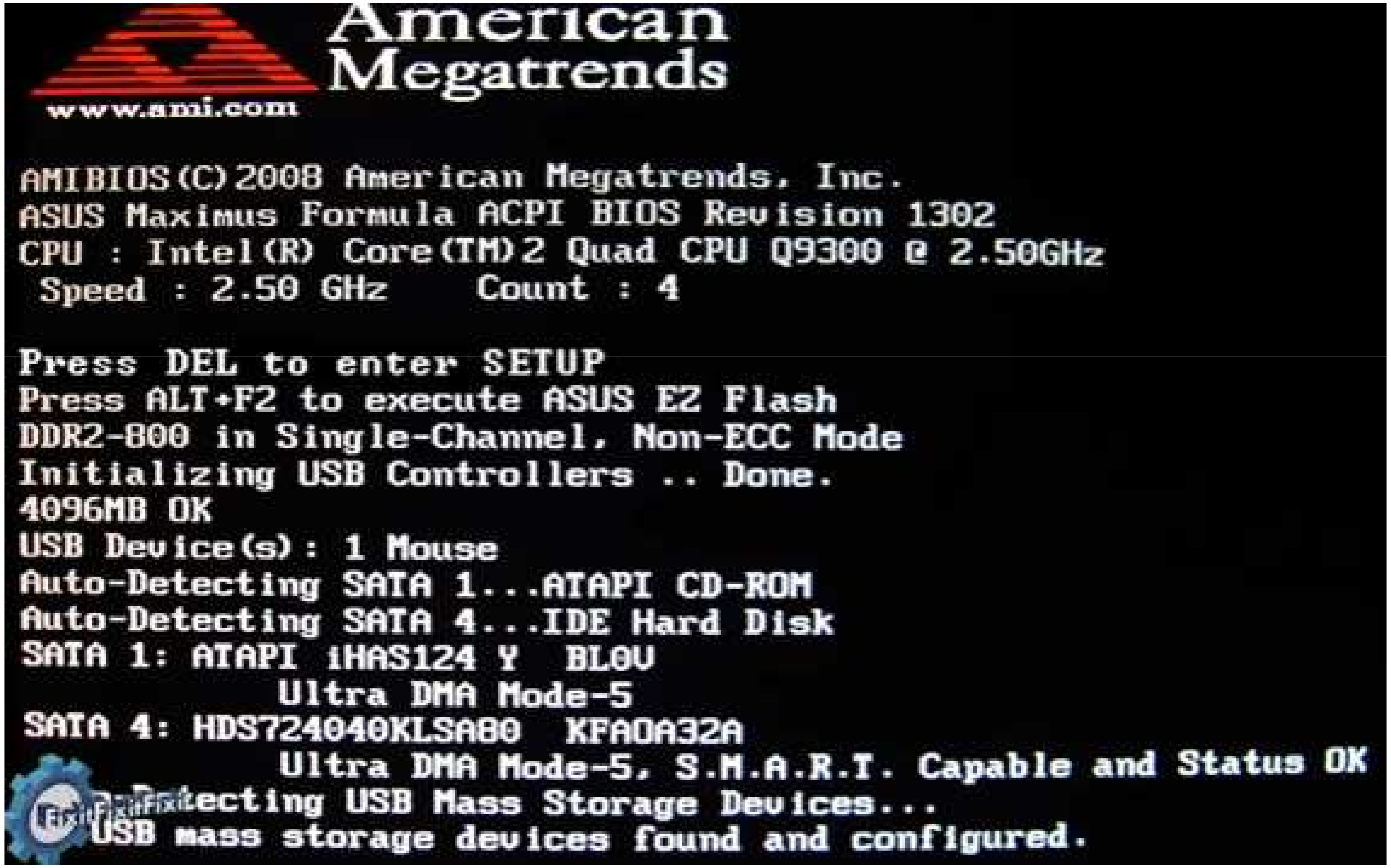
- Complementary Metal Oxide Semiconductor **(CMOS)**
  - Computer stores **system configuration and date and time information in the CMOS**
    - When power to the system is off

- Basic Input/Output System **(BIOS)**
  - Contains programs that perform **input and output at the hardware level**

Understanding the Boot Sequence (continued)

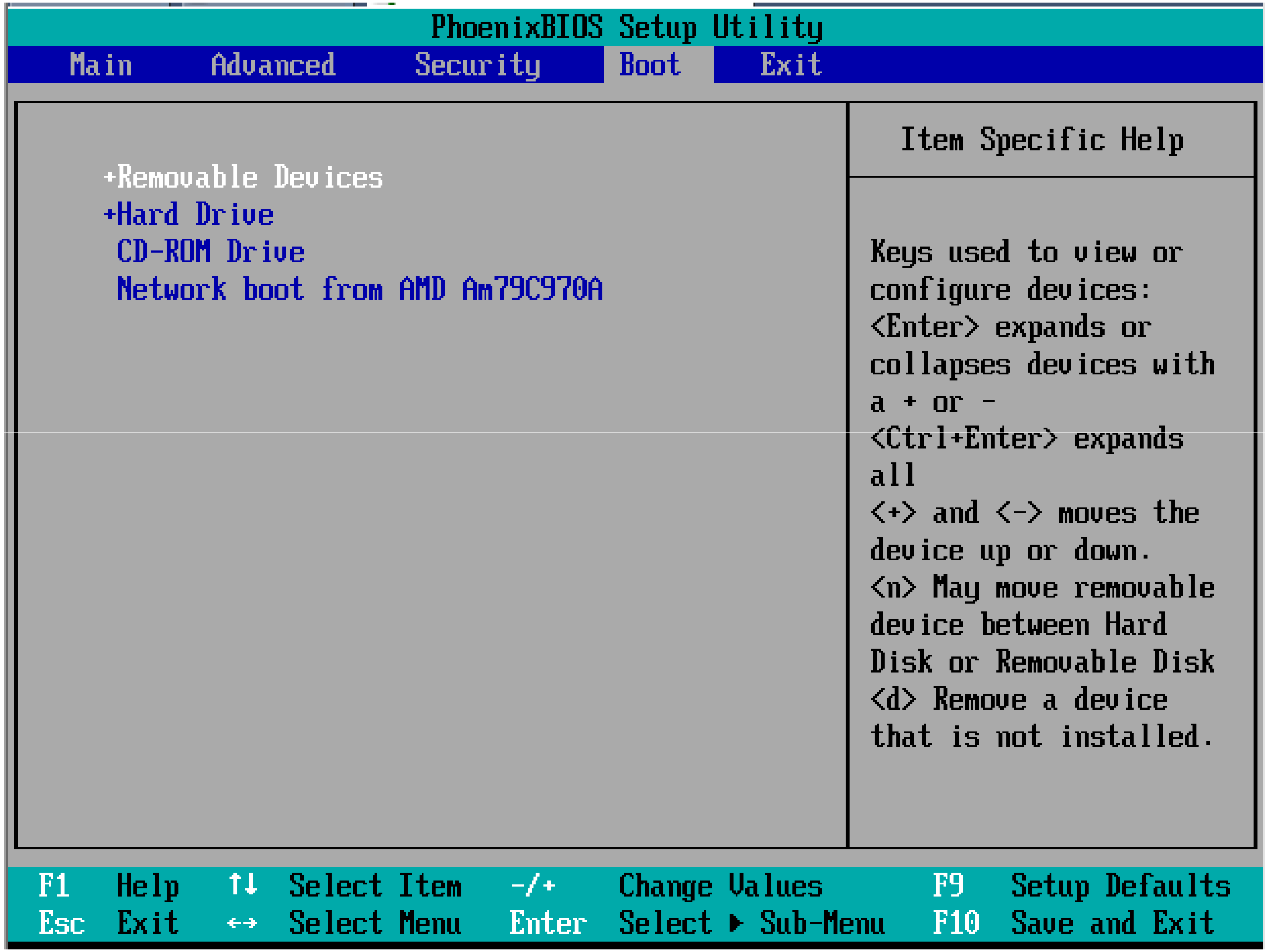
- **Bootstrap process**
  - Contained in ROM, tells the computer how to proceed
  - Displays the key or keys you press to open the CMOS setup screen
    - Could be Delete, F2, F10, Ctrl+Alt+Insert, Ctrl+A, Ctrl+S, Ctrl+F1, or something else
- CMOS should be modified to boot from a forensic floppy disk or CD

BIOS Setup Utility



```
AMIBIOS(C)2008 American Megatrends, Inc.
ASUS Maximus Formula ACPI BIOS Revision 1302
CPU : Intel(R) Core(TM)2 Quad CPU Q9300 @ 2.50GHz
 Speed : 2.50 GHz    Count : 4

Press DEL to enter SETUP
Press ALT+F2 to execute ASUS EZ Flash
DDR2-800 in Single-Channel, Non-ECC Mode
Initializing USB Controllers .. Done.
4096MB OK
USB Device(s): 1 Mouse
Auto-Detecting SATA 1...ATAPI CD-ROM
Auto-Detecting SATA 4...IDE Hard Disk
SATA 1: ATAPI iHAS124 Y  BL0V
            Ultra DMA Mode-5
SATA 4: HDS724040KLSA80  KFAOA32A
            Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK
Auto-Detecting USB Mass Storage Devices...
   USB mass storage devices found and configured.
```

BIOS Setup Utility

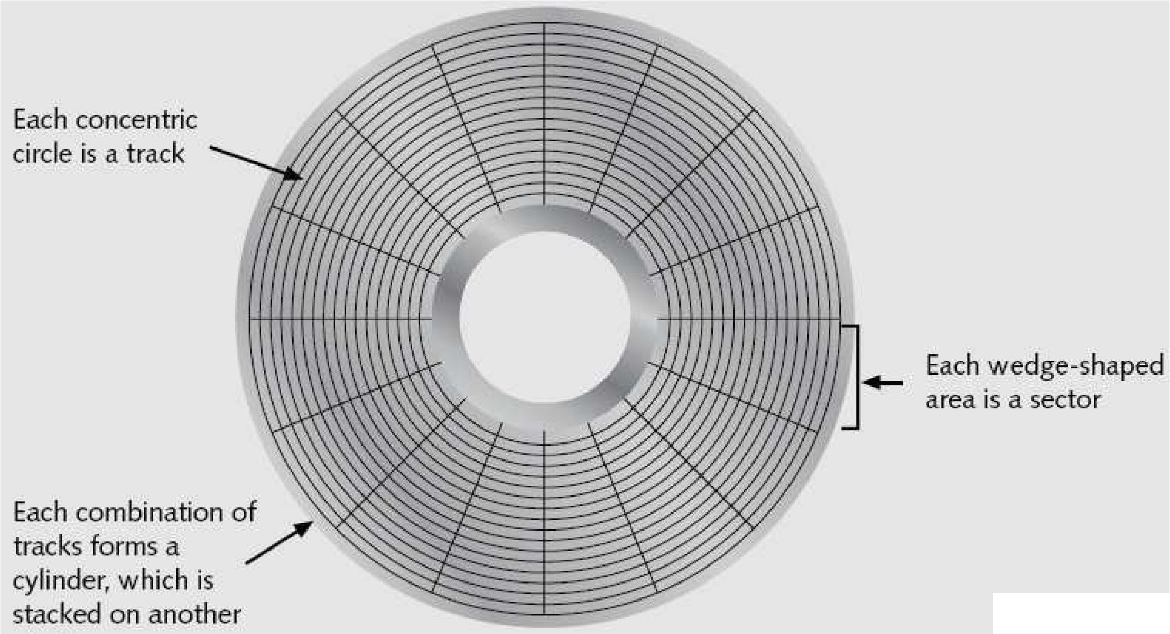


```
                      PhoenixBIOS Setup Utility
   Main      Advanced     Security     Boot     Exit

                                              Item Specific Help

     +Removable Devices
     +Hard Drive                            Keys used to view or
      CD-ROM Drive                          configure devices:
      Network boot from AMD Am79C970A       <Enter> expands or
                                            collapses devices with
                                            a + or -
                                            <Ctrl+Enter> expands
                                            all
                                            <+> and <-> moves the
                                            device up or down.
                                            <n> May move removable
                                            device between Hard
                                            Disk or Removable Disk
                                            <d> Remove a device
                                            that is not installed.

 F1   Help   ↑↓  Select Item   -/+    Change Values         F9   Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter  Select ▸ Sub-Menu     F10  Save and Exit
```

www.youtube.com/watch?v=6i16HtZnQvw

Understanding Disk Drives

- Be familiar with disk drives and how data is organized on a disk so that you can find data effectively
- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
  - Geometry - platters, tracks, and sectors
  - Head - device that reads and writes data to a drive
  - Tracks - concentric circles on a disk platter
  - Cylinders - column of tracks on two or more disk platters
  - Sectors - section on a track
    - Holds 512 bytes, you cannot read or write anything less than a sector


Each concentric circle is a track
Each wedge-shaped area is a sector
Each combination of tracks forms a cylinder, which is stacked on another platter

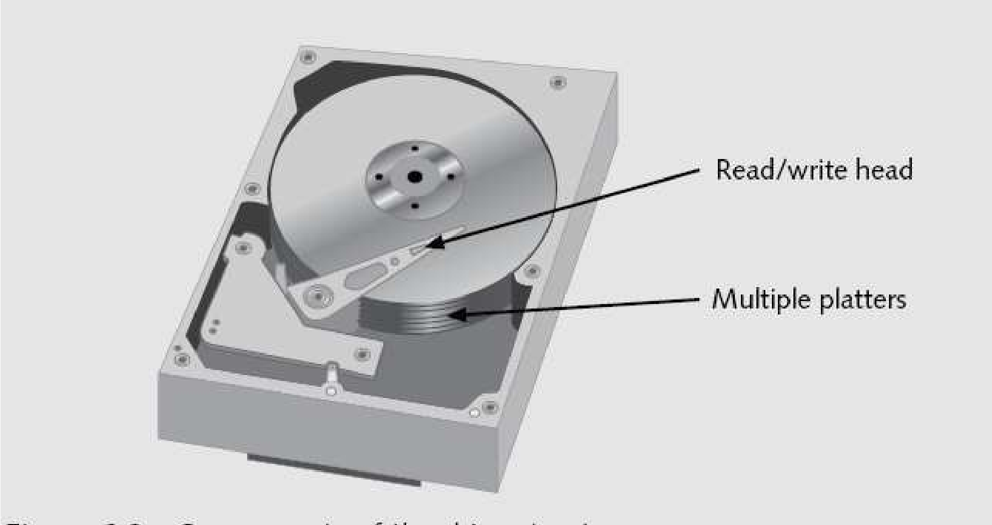


Figure 6-2 Components of the drive structure

www.youtube.com/watch?v=NtPc0jI21i0

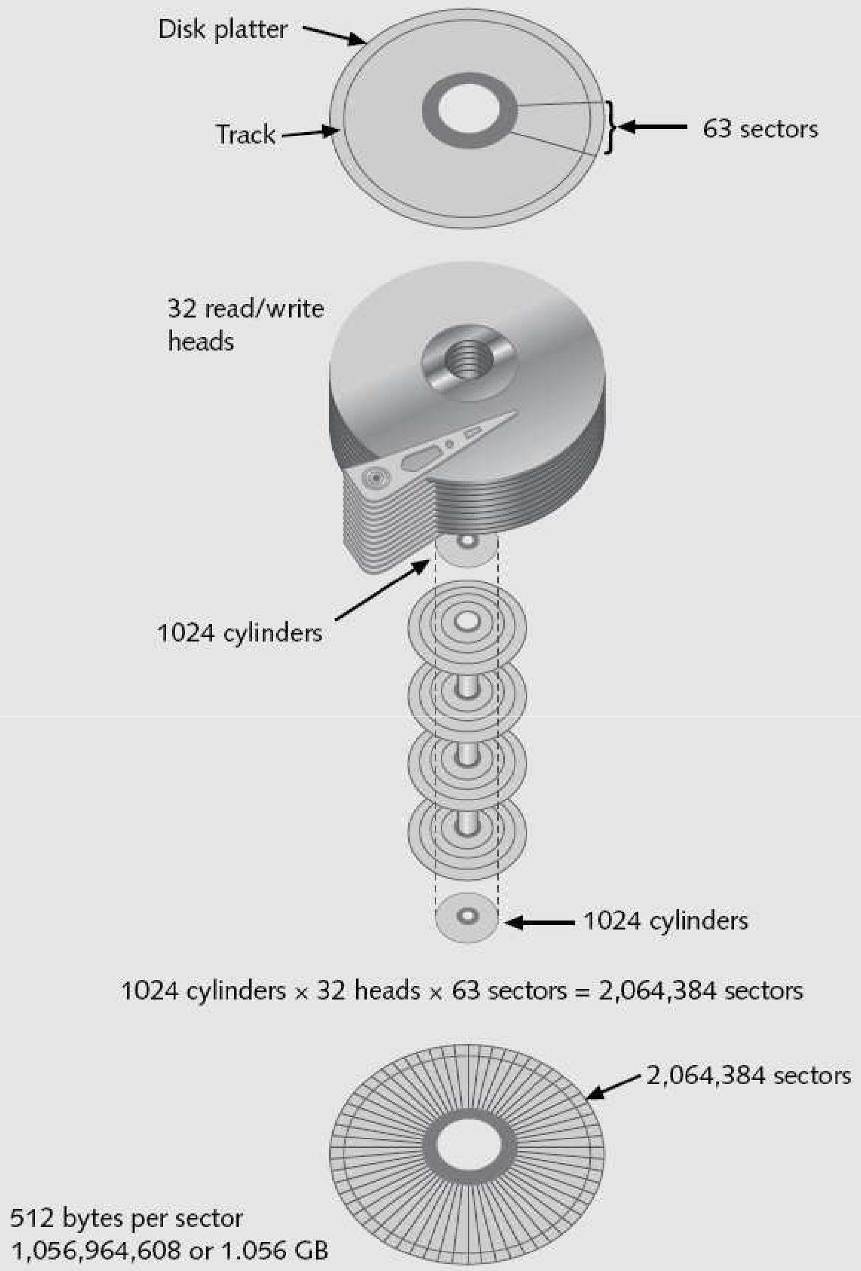


Figure 6-3 CHS calculation

Understanding Disk Drives (continued)

- Properties handled at the drive’s hardware or firmware level
  - Zoned bit recording (ZBR)
  - Track density
  - Areal density
  - Head and cylinder skew