Working with Windows and DOS Systems

Understanding File Systems

- **File system**
  - The way the **files** are organized (stored) on the disk
  - OS uses this to keep track of **files** on a disk or partition
- **CMOS**
- **BIOS**

Understanding Disk Drives

- Disk drive components
  - Geometry
  - Head
  - Tracks
  - Cylinders
  - Sectors

Exploring Microsoft File Structures

- Clusters
- File Allocation Table (FAT)
- New Technology File System (NTFS)

Examining FAT Disks

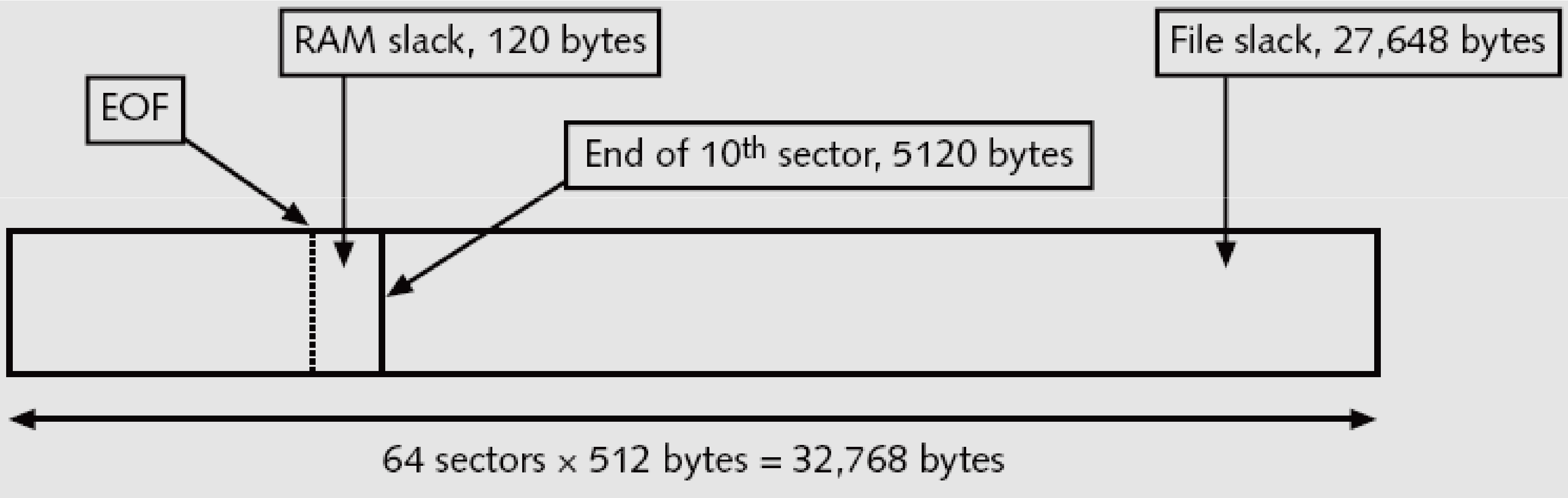
RAM slack, 120 bytes
File slack, 27,648 bytes
EOF
End of 10th sector, 5120 bytes
64 sectors × 512 bytes = 32,768 bytes

Figure 6-7 File slack space

Examining NTFS Disks

- In NTFS, everything written to the disk is considered a file
- On an NTFS disk
  - First data set is the **Partition Boot Sector**
  - Next is **Master File Table (MFT)**

Understanding Whole Disk Encryption

- **Personal identity information (PII)** and trade secrets caused by computer theft
- Current whole disk encryption tools offer the following features:
  - Preboot authentication
  - Full or partial disk encryption with secure hibernation
  - Advanced encryption algorithms
  - Key management function
  - A **Trusted Platform Module (TPM)** microchip to generate encryption keys and authenticate logins

Examining Third-Party Disk Encryption Tools

- Some available third-party WDE utilities:
  - PGP Whole Disk Encryption
  - Voltage SecureDisk
  - Utimaco SafeGuard Easy
  - Jetico BestCrypt Volume Encryption
  - SoftWinter Sentry 2020 for Windows XP
- Some available open-source encryption tools:
  - TrueCrypt
  - CrossCrypt
  - FreeOTFE

Understanding the Windows Registry

- **Registry**
  - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
- To view the Registry, you can use:
  - Regedit
  - Regedt32

Exploring the Organization of the Windows Registry

- Registry terminology:
  - Registry
  - Registry Editor
  - HKEY
  - Key
  - Subkey
  - Branch
  - Value
  - Default value
  - Hives

Understanding Microsoft Startup Tasks

- All Windows NT computers perform the following steps when the computer is turned on:
  - Power-on self test (POST)
  - Initial startup
  - Boot loader
  - Hardware detection and configuration
  - Kernel loading
  - User logon

Startup Process for Windows Vista

- Three boot utilities
  - Bootmgr.exe—displays list of operating systems
  - Winload.exe—loads kernel, HAL, and drivers
  - Winresume.exe—restarts Vista after hibernation

Startup Files for Windows XP

- NT Loader (NTLDR)
- Boot.ini
- BootSect.dos
- NTDetect.com
- NTBootdd.sys
- Ntoskrnl.exe
- Hal.dll
- Pagefile.sys
- Device drivers

Understanding MS-DOS Startup Tasks

- Two files are used to configure MS-DOS at startup:
  - **Config.sys**
  - **Autoexec.bat**

Understanding Virtual Machines

- **Virtual machine**
  - Allows you to create a representation of another computer on an existing physical computer
- In computer forensics
  - Virtual machines make it possible to restore a suspect drive on your virtual machine