Catalog

2.1. Processing Crime and Incident Scenes

Digital Evidence

– Can be any information stored or transmitted in digital form

- **U.S. courts accept digital evidence as physical evidence**

  – Digital data is treated as a tangible object

- Groups such as the Scientific Working Group on Digital Evidence (SWGDE) set standards for recovering, preserving, and examining digital evidence
- **General tasks investigators perform when working with digital evidence:**
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting digital devices and processing a criminal or incident scene must be done systematically

Understanding Rules of Evidence

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence
- Data you discover from a forensic examination falls under your state's rules of evidence

  - Or the Federal Rules of Evidence (FRE)
- Digital evidence is unlike other physical evidence because it can be changed more easily

  -The only way to detect these changes is to compare the original data with a duplicate

- Most federal courts have interpreted computer records as hearsay evidence

  - Hearsay is secondhand or indirect evidence

- Business-record exception

  -Allows "records of regularly conducted activity," such as business memos, reports, records, or data compilations

  Generally, digital records are considered admissible if they qualify as a business record

- Computer records are usually divided into:
  - **Computer-generated records**
  - **Computer-stored records**
- Computer and digitally stored records must be shown to be authentic and trustworthy

  -To be admitted into evidence

- Computer-generated records are considered authentic if the program that created the output is functioning correctly

  -Usually considered an exception to hearsay rule

- Collecting evidence according to the proper steps of evidence control helps ensure that the computer evidence is authentic
- When attorneys challenge digital evidence

  -Often they raise the issue of whether computer-generated records were altered or damaged

- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records

  - The author of a Microsoft Word document can be identified by using file metadata

- Follow the steps starting on page 141 of the text to see how to identify file metadata
- The process of establishing digital evidence's trustworthiness originated with written documents and the "best evidence rule"

- **Best evidence rule states**:

  To prove the content of a written document, recording, or photograph, ordinarily the original writing, recording, or photograph is required

- **Federal Rules of Evidence**

  Allow a duplicate instead of originals when it is produced by the same impression as the original

- **As long as bit-stream copies of data are created and maintained properly**

  The copies can be admitted in court, although they aren't considered best evidence

- Example of not being able to use original evidence
  - Investigations involving network servers
  - Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong

Collecting Evidence in Private-Sector Incident Scenes Private-sector organizations include:

Businesses and government agencies that aren't involved in law enforcement

- Non-government organizations (NGO) must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws and make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies
- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers

  Except for activities that are deemed to create an emergency situation

- Investigating and controlling computer incident scenes in the corporate environment
  - Much easier than in the criminal environment
  - Incident scene is often a workplace

- Typically, businesses have inventory databases of computer hardware and software
  - Help identify the computer forensics tools needed to analyze a policy violation and the best way to conduct the analysis
- Corporate policy statement about misuse of digital assets
  - Allows corporate investigators to conduct covert surveillance with little or no cause and access company systems without a warrant
- Companies should display a warning banner and publish a policy
  - Stating that they reserve the right to inspect computing assets at will
- Corporate investigators should know under what circumstances they can examine an employee's computer
  - Every organization must have a well-defined process describing when an investigation can be initiated
- If a corporate investigator finds that an employee is committing or has committed a crime
  - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
  - Not seeking out and prosecuting employees
- Corporate investigators are, therefore, primarily concerned with protecting company assets
- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don't violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney on how to respond to a police request for more information

Processing Law Enforcement Crime Scenes

- You must be familiar with criminal rules of search and seizure

- You should also understand how a search warrant works and what to do when you process one
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
  - Refers to the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest
- With probable cause, a police officer can obtain a search warrant from a judge
  - That authorizes a search and seizure of specific evidence related to the criminal complaint
- The Fourth Amendment states that only warrants "particularly describing the place to be searched, and the persons or things to be seized" can be issued

Understanding Concepts and Terms Used in Warrants

- Innocent information
  - Unrelated information
  - Often included with the evidence you're trying to recover

- Judges often issue a limiting phrase to the warrant
  - Allows the police to separate innocent information from evidence
- **Plain view doctrine**
  - Objects falling in plain view of an officer who has the right to be in position to have that view are subject to seizure without a warrant and may be introduced in evidence
  - Three criteria must be met:
- Officer is where he or she has a legal right to be
- Ordinary senses must not be enhanced by advanced technology in any way
- Any discovery must be by chance
- The plain view doctrine's applicability in the digital forensics world is being rejected
- Example - In a case where police were searching a computer for evidence related to illegal drug trafficking:

If an examiner observes an .avi file and find child pornography, he must get an additional warrant or an expansion of the existing warrant to continue the search for child pornography

List the steps followed in preparing for an evidence search

Preparing for a Search

- Preparing for a computer search and seizure
  – Probably the most important step in computing investigations
- To perform these tasks
  – You might need to get answers from the victim and an informant
- Who could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the **person of interest** to the investigation

Identifying the Nature of the Case

- When you're assigned a digital investigation case
  – Start by identifying the nature of the case
- Including whether it involves the private or public sector
- The nature of the case dictates how you proceed
  – And what types of assets or resources you need to use in the investigation

Identifying the Type of OS or Digital Device

- For law enforcement
  – This step might be difficult because the crime scene isn't controlled
- If you can identify the OS or device
  – Estimate the size of the drive on the suspect's computer
- And how many devices to process at the scene
- Determine which OSs and hardware are involved

Determining Whether You Can Seize Computers and Digital Devices

- The type of case and location of the evidence
  – Determine whether you can remove digital evidence

- Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab

- If removing the computers will irreparably harm a business

  The computers should not be taken offsite

- Additional complications:
  - Files stored offsite that are accessed remotely
  - Availability of cloud storage, which can't be located physically
- Stored on drives where data from many other subscribers might be stored
- If you aren't allowed to take the computers to your lab

  – Determine the resources you need to acquire digital evidence and which tools can speed data acquisition

Getting a Detailed Description of the Location

- Get as much information as you can about the location of a digital crime
- Identify potential hazards

  – Interact with your HAZMAT (hazardous materials) team
- HAZMAT guidelines
  - Put the target drive in a special HAZMAT bag
  - HAZMAT technician can decontaminate the bag
  - Check for high temperatures

Determining Who Is in Charge

- Corporate computing investigations

  – Usually require only one person to respond to an incident
- Law enforcement agencies

  – Typically handle large-scale investigations
- Designate lead investigators in large-scale investigations

  – Anyone assigned to the scene should cooperate with the designated leader to ensure the team addresses all details when collecting evidence

Using Additional Technical Expertise

- Determine whether you need specialized help to process the incident or crime scene
- You may need to look for specialists in:
  - OSs
  - RAID servers

– Databases

- Finding the right person can be a challenge
- Educate specialists in investigative techniques

Prevent evidence damage

Determining the Tools You Need

- Prepare tools using incident and crime scene information
- Create an initial-response field kit
  - Should be lightweight and easy to transport
- Create an extensive-response field kit
  - Includes all tools you can afford to take to the field
  - When at the scene, extract only those items you need to acquire evidence

Fig: Items in an initial Response field kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cables
1	Forensic boot media containing an acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop or tablet computer
1	FireWire or USB dual write-protect external bay
1	Flashlight
1	Digital camera with extra batteries or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or digital dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	External USB devices or a portable hard drive

Fig: Tools in an initial Response field kit

Number needed	Tools
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Laptop or tablet with cables and connectors
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from digital devices

Fig: Tools in an extensive Response field kit

Preparing the Investigation Team

- Before initiating the search:
  - Review facts, plans, and objectives with the investigation team you have assembled
- Goal of scene processing
  - To collect and secure digital evidence
- Digital evidence is volatile
  - Develop skills to assess facts quickly
- Slow response can cause digital evidence to be lost

Securing a computer incident or crime scene Securing a Computer Incident or Crime Scene includes

- Goals
  - Preserve the evidence
  - Keep information confidential
- Define a secure perimeter
  - Use yellow barrier tape
  - Legal authority for a corporate incident includes trespassing violations
  - For a crime scene, it includes obstructing justice or failing to comply with a police officer
- Professional curiosity can destroy evidence
  - Involves police officers and other professionals who aren't part of the crime scene processing team
- Automated Fingerprint Identification System (AFIS)
  - A computerized system for identifying fingerprints that's connected to a central database
  - Used to identify criminal suspects and review thousands of fingerprint samples at high speed

- Police can take elimination prints of everyone who had access to the crime scene

Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
  - With a proper warrant
- Corporate investigators might have the authority only to make an image of the suspect's drive
- When seizing digital evidence in criminal investigations
  - Follow U.S. DoJ standards for seizing digital data
- Civil investigations follow same rules
  - Require less documentation though
- Consult with your attorney for extra guidelines

Preparing to Acquire Digital Evidence

- The evidence you acquire at the scene depends on the nature of the case
  - And the alleged crime or violation
- Ask your supervisor or senior forensics examiner in your organization the following questions:
  - Do you need to take the entire computer and all peripherals and media in the immediate area?
  - How are you going to protect the computer and media while transporting them to your lab?
  - Is the computer powered on when you arrive?
- Ask your supervisor or senior forensics examiner in your organization the following questions (cont'd):
  - Is the suspect you're investigating in the immediate area of the computer?
  - Is it possible the suspect damaged or destroyed the computer, peripherals, or media?
  - Will you have to separate the suspect from the computer?

Processing an Incident or Crime Scene

- Guidelines

  – Keep a journal to document your activities –

  Secure the scene

- Be professional and courteous with onlookers
- Remove people who are not part of the investigation

  – Take video and still recordings of the area around the computer

- Pay attention to details
  - Sketch the incident or crime scene
  - Check state of computers as soon as possible
  - Don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system
  - Save data from current applications as safely as possible
  - Record all active windows or shell sessions
  - Make notes of everything you do when copying data from a live suspect computer
  - Close applications and shut down the computer – Bag and tag the evidence, following these steps:
- Assign one person to collect and log all evidence
- Tag all evidence you collect with the current date and time, serial numbers or unique features, make and model, and the name of the person who collected it

Maintain two separate logs of collected evidence

- Maintain constant control of the collected evidence and the crime or incident scene
- Guidelines (cont'd)

  – Look for information related to the investigation

- Passwords, passphrases, PINs, bank accounts

  – Collect documentation and media related to the investigation

- Hardware, software, backup media, documentation, manuals

Processing Data Centers with RAID Systems

- Sparse acquisition
  - Technique for extracting evidence from large systems
  - Extracts only data related to evidence for your case from allocated files
- And minimizes how much data you need to analyze
- Drawback of this technique
  - It doesn't recover data in free or slack space

Using a Technical Advisor

- A technical advisor can help:
  - List the tools you need to process the incident or crime scene
  - Guide you about where to locate data and helping you extract log records
- Or other evidence from large RAID servers
  - Create the search warrant by itemizing what you need for the warrant
- Responsibilities
  - Know all aspects of the seized system
  - Direct investigator handling sensitive material
  - Help secure the scene
  - Help document the planning strategy
  - Conduct ad hoc trainings
  - Document activities
  - Help conduct the search and seizure

Documenting Evidence in the Lab

- Record your activities and findings as you work
  - Maintain a journal to record the steps you take as you process evidence
- Your goal is to be able to reproduce the same results
  - When you or another investigator repeat the steps you took to collect evidence
- A journal serves as a reference that documents the methods you used to process digital evidence

Processing and Handling Digital Evidence

- Maintain the integrity of digital evidence in the lab
  - As you do when collecting it in the field
- Steps to create image files:
  - Copy all image files to a large drive
  - Start your forensics tool to analyze the evidence
  - Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash
  - Secure the original media in an evidence locker

List of procedures for storing digital evidence

Storing Digital Evidence

- The media you use to store digital evidence usually depends on how long you need to keep it
- CDs, DVDs, DVD-Rs, DVD+Rs, or DVD-RWs
  - The ideal media
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years
- Magnetic tapes - 4-mm DAT
  - Capacity: 40 to 72 GB
  - Lifespan: 30 years
  - Costs: drive: $400 to $800; tape: $40
- Super Digital Linear Tape (Super-DLT or SDLT)
  - Specifically designed for large RAID data backups
  - Can store more than 1 TB of data
- Smaller external SDLT drives can connect to a workstation through a SCSI card
- Don't rely on one media storage method to preserve your evidence
  - Make two copies of every image to prevent data loss
  - Use different tools to create the two images

Evidence Retention and Media Storage Needs

- To help maintain the chain of custody for digital evidence
  – Restrict access to lab and evidence storage area
- Lab should have a sign-in roster for all visitors
  – Maintain logs for a period based on legal requirements
- You might need to retain evidence indefinitely
  – Check with your local prosecuting attorney's office or state laws to make sure you're in compliance

Documenting Evidence

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  – Identifies the evidence
  – Identifies who has handled the evidence
  – Lists dates and times the evidence was handled
- You can add more information to your form
  – Such as a section listing MD5 and SHA-1 hash values
- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence
  – Use antistatic bags for electronic components

Obtaining a Digital Hash

- **Cyclic Redundancy Check (CRC)**
  – Mathematical algorithm that determines whether a file's contents have changed
  – Not considered a forensic hashing algorithm
- **Message Digest 5 (MD5)**
  – Mathematical formula that translates a file into a hexadecimal code value, or a **hash value**

  - If a bit or byte in the file changes, it alters the hash value**,** which can be used to verify a file or drive has not been tampered

- Three rules for forensic hashes:
  - You can't predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change
- **Secure Hash Algorithm version 1 (SHA-1)**
  - A newer hashing algorithm
  - Developed by the **National Institute of Standards and Technology (NIST)**
- In both MD5 and SHA-1, collisions have occurred
- Most digital forensics hashing needs can be satisfied with a **nonkeyed hash set**
  - A unique hash number generated by a software tool, such as the Linux md5sum command
- **Keyed hash set**
  - Created by an encryption utility's secret key
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file
  - Or an entire drive

Review a case to identify requirements and plan your investigation

Reviewing a Case

- General tasks you perform in any computer forensics case:
  - Identify the case requirements
  - Plan your investigation
  - Conduct the investigation
  - Complete the case report
  - Critique the case **Sample Civil Investigation**
- Most cases in the corporate environment are considered **low-level investigations**
  - Or noncriminal cases
- Common activities and practices – Recover specific evidence
- Suspect's Outlook e-mail folder (PST file)

- Its use must be well defined in the company policy
- Risk of civil or criminal liability
  - **Sniffing** tools for data transmissions

Sample Criminal Investigation

- Computer crimes examples
  - Fraud
  - Check fraud
  - Homicides
- Need a warrant to start seizing evidence
  - Limit searching area

Reviewing Background Information for a Case

- Throughout the book, you use data files from the hypothetical M57 Patents case
  - A new startup company doing art patent searches
  - A computer sold on Craigslist was discovered to contain "kitty" porn
  - It was traced back to M57 Patents

Reviewing a case to identify requirements and plan your investigation

Planning Your Investigation

- Background information on the case – Main players:
- Pat McGoo, CEO
- Terry, the IT person
- Jo and Charlie, the patent researchers
- Police made forensic copies of:
  - The image of the computer sold on Craigslist
  - Images of five other machines found at M57
  - Images of four USB drives found at M57
- Police made forensic copies of (cont'd):
  - RAM from the imaged machines
  - Network data from the M57 Patents servers

2.2. Working with Windows and DOS Systems

Purpose and structure of file systems. Understanding File Systems

- **File system**
  - – Gives OS a road map to data on a disk
- Type of file system an OS uses determines how data is stored on the disk
- When you need to access a suspect's computer to acquire or inspect data
  - – You should be familiar with both the computer's OS and file systems

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) or Extensible Firmware Interface (EFI)
  - – Contains programs that perform input and output at the hardware level
- **Bootstrap process**
  - – Contained in ROM, tells the computer how to proceed
  - – Displays the key or keys you press to open the CMOS setup screen
- CMOS should be modified to boot from a forensic floppy disk or CD

Understanding Disk Drives

- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
  - – Geometry
  - – Head
  - – Tracks
  - – Cylinders
  - – Sectors

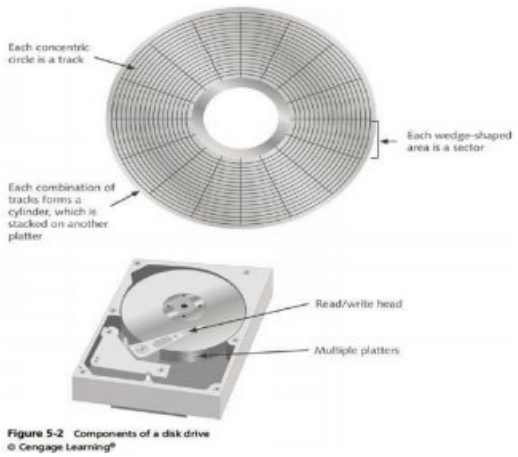

Figure 5-2 Components of a disk drive
© Cengage Learning®

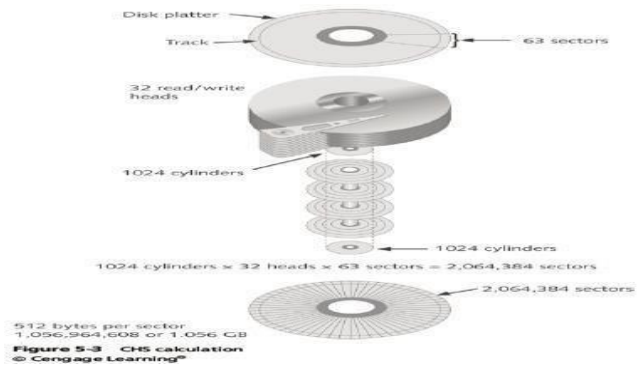

Figure 5-3 CHS calculation
© Cengage Learning®

- Properties handled at the drive's hardware or firmware level
  - Zone bit recording (ZBR)
  - Track density
  - Areal density
  - Head and cylinder skew **Solid-State Storage Devices**
- All flash memory devices have a feature called **wear-leveling**
  - An internal firmware feature used in solid-state drives that ensures even wear of read/writes for all memory cells
- When dealing with solid-state devices, making a full forensic copy as soon as possible is crucial
  - In case you need to recover data from unallocated disk space

Exploring Microsoft File Structures

- In Microsoft file structures, sectors are grouped to form **clusters**
  - Storage allocation units of one or more sectors
- Clusters range from 512 bytes up to 32,000 bytes each
- Combining sectors minimizes the overhead of writing or reading files to a disk
- Clusters are numbered sequentially starting at 0 in NTFS and 2 in FAT
  - First sector of all disks contains a system area, the boot record, and a file structure database
- OS assigns these cluster numbers, called **logical addresses**

- Sector numbers are called **physical addresses**
- Clusters and their addresses are specific to a logical disk drive, which is a disk partition

Disk Partitions

- A partition is a logical drive
- Windows OSs can have three primary partitions followed by an extended partition that can contain one or more logical drives
- Hidden partitions or voids
  - Large unused gaps between partitions on a disk
- Partition gap
  - Unused space between partitions

- The partition table is in the **Master Boot Record (MBR)**
  - Located at sector 0 of the disk drive
- MBR stores information about partitions on a disk and their locations, size, and other important items
- In a hexadecimal editor, such as WinHex, you can find the first partition at offset 0x1BE
  - The file system's hexadecimal code is offset 3 bytes from 0x1BE for the first partition

Examining FAT Disks

- File Allocation Table (FAT)

– File structure database that Microsoft originally designed for floppy disks

- FAT database is typically written to a disk's outermost track and contains:
  - Filenames, directory names, date and time stamps, the starting cluster number, and file attributes
- Three current FAT versions
  - FAT16, FAT32, and exFAT (used by Xbox game systems)
- Cluster sizes vary according to the hard disk size and file system

Drive size	Sectors per cluster	FAT16
8–32 MB	1	512 bytes
32–64 MB	2	1 KB
64–128 MB	4	2 KB
128–256 MB	8	4 KB
256–512 MB	16	8 KB
512–1024 MB	32	16 KB
1024–2048 MB	64	32 KB
2048–4096 MB	128	64 KB

Fig :Sectors and bytes per duster

- Microsoft OSs allocate disk space for files by clusters – Results in **drive slack**
- Unused space in a cluster between the end of an active file and the end of the cluster
- Drive slack includes:
  - **RAM slack** and **file slack**
- An unintentional side effect of FAT16 having large clusters was that it reduced fragmentation

– As cluster size increased

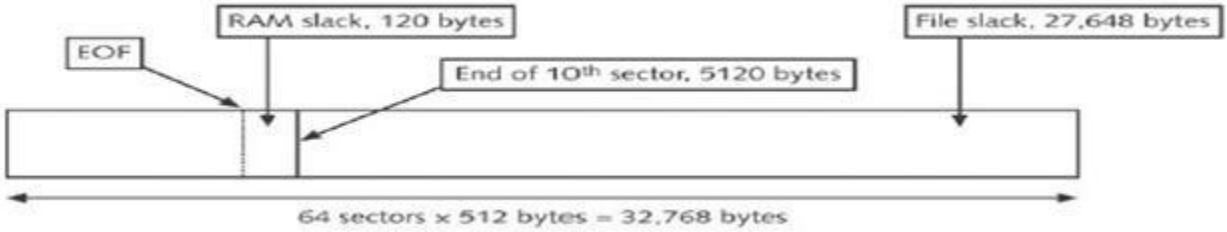

Fig: File Stack space

- When you run out of room for an allocated cluster
  - OS allocates another cluster for your file, which creates more slack space on the disk
- As files grow and require more disk space, assigned clusters are chained together
  - The chain can be broken or fragmented
- When the OS stores data in a FAT file system, it assigns a starting cluster position to a file

Data for the file is written to the first sector of the first assigned cluster

- When this first assigned cluster is filled and runs out of room
  - FAT assigns the next available cluster to the file
- If the next available cluster isn't contiguous to the current cluster
  - File becomes fragmented

Deleting FAT Files

- In Microsoft OSs, when a file is deleted
  - Directory entry is marked as a deleted file
- With the HEX E5 character replacing the first letter of the filename
- FAT chain for that file is set to 0
- Data in the file remains on the disk drive
- Area of the disk where the deleted file resides becomes **unallocated disk space**
  - Available to receive new data from newly created files or other files needing more space

NTFS Disks

- **NT File System (NTFS)**
  - Introduced with Windows NT
  - Primary file system for Windows 8
- Improvements over FAT file systems
  - NTFS provides more information about a file
  - NTFS gives more control over files and folders
- NTFS was Microsoft's move toward a journaling file system
  - It records a transaction before the system carries it out
- 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)**
- NTFS results in much less file slack space
- Clusters are smaller for smaller disk drives

- NTFS also uses **Unicode**
  - An international data format

Drive size	Sectors per cluster	Cluster size
7–512 MB	8	4 KB
512 MB–1 GB	8	4 KB
1–2 GB	8	4 KB
2 GB–2 TB	8	4 KB
2–16 TB	8	4 KB
16–32 TB	16	8 KB
32–64 TB	32	16 KB
64–128 TB	64	32 KB
128–256 TB	128	64 KB

Fig: Cluster sizes in an NTFS disk

NTFS System Files

- MFT contains information about all files on the disk
  - Including the system files the OS uses
- In the MFT, the first 15 records are reserved for system files
- Records in the MFT are called metadata

Filename	System file	Record position	Description
$Mft	MFT	0	Base file record for each folder on the NTFS volume; other record positions in the MFT are allocated if more space is needed.
$MftMirr	MFT 2	1	The first four records of the MFT are saved in this position. If a single sector fails in the first MFT, the records can be restored, allowing recovery of the MFT.
$LogFile	Log file	2	Previous transactions are stored here to allow recovery after a system failure in the NTFS volume.
$Volume	Volume	3	Information specific to the volume, such as label and version, is stored here.
$AttrDef	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
$	Root filename index	5	This is the root folder on the NTFS volume.
$Bitmap	Cluster bitmap	6	A map of the NTFS partition shows which clusters are in use and which are available.
$Boot	Boot sector	7	Used to mount the NTFS volume during the bootstrap process; additional code is listed here if it's the boot drive for the system.
$BadClus	Bad cluster file	8	For clusters that have unrecoverable errors, an entry of the cluster location is made in this file.
$Secure	Security file	9	Unique security descriptors for the volume are listed in this file. It's where the access control list (ACL) is maintained for all files and folders on the NTFS volume.
$Upcase	Upcase table	10	Converts all lowercase characters to uppercase Unicode characters for the NTFS volume.
$Extend	NTFS extension file	11	Optional extensions are listed here, such as quotas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

Fig: Metedata records in the MFT

MFT and File Attributes

- In the NTFS MFT
  – All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information
  – This information is divided into record fields containing metadata
- A record field is referred to as an attribute ID
- File or folder information is typically stored in one of two ways in an MFT record:
  – Resident and nonresident
- Files larger than 512 bytes are stored outside the MFT
  – MFT record provides cluster addresses where the file is stored on the drive's partition
- Referred to as **data runs**
- Each MFT record starts with a header identifying it as a resident or nonresident attribute
- When a disk is created as an NTFS file structure
  – OS assigns logical clusters to the entire disk partition

- These assigned clusters are called **logical cluster numbers (LCNs)**
  – Become the addresses that allow the MFT to link to nonresident files on the disk's partition
- When data is first written to nonresident files, an LCN address is assigned to the file

  This LCN becomes the file's **virtual cluster number (VCN)**

MFT Structures for File Data

- For the header of all MFT records, the record fields of interest are as follows:
  – *At offset 0x00* - the MFT record identifier FILE
  – *At offset 0x1C to 0x1F* - size of the MFT record
  – *At offset 0x14* - length of the header (indicates where the next attribute starts)
  – *At offset 0x32 and 0x33* - the update sequence array, which stores the last 2 bytes of the first sector of the MFT record

NTFS Alternate Data Streams

- **Alternate data streams**
  - – Ways data can be appended to existing files
    - Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, an alternate data stream becomes an additional file attribute
  - – Allows the file to be associated with different applications
- You can only tell whether a file has a data stream attached by examining that file's MFT entry

NTFS Compressed Files

- NTFS provides compression similar to FAT DriveSpace 3 (a Windows 98 compression utility)
- Under NTFS, files, folders, or entire volumes can be compressed
- Most computer forensics tools can uncompress and analyze compressed Windows data

NTFS Encrypting File System (EFS)

- **Encrypting File System (EFS)**
  - – Introduced with Windows 2000
    - Implements a **public key** and **private key** method of encrypting files, folders, or disk volumes
- When EFS is used in Windows 2000 and later
  - – A **recovery certificate** is generated and sent to the local Windows administrator account
- Users can apply EFS to files stored on their local workstations or a remote server

EFS Recovery Key Agent

- Recovery Key Agent implements the recovery certificate
  - – Which is in the Windows administrator account

- Windows administrators can recover a key in two ways: through Windows or from an MS-DOS command prompt
- MS-DOS commands
  - cipher
  - copy
  - efsrecvr (used to decrypt EFS files) **Deleting NTFS Files**
- When a file is deleted in Windows NT and later
  - The OS renames it and moves it to the Recycle Bin
- Can use the Del (delete) MS-DOS command
  - Eliminates the file from the MFT listing in the same way FAT does **Resilient File System**
- Resilient File System (ReFS) - designed to address very large data storage needs – Such as the cloud
- Features incorporated into ReFS's design:
  - Maximized data availability
  - Improved data integrity
  - Designed for scalability
- ReFS uses disk structures similar to the MFT in NTFS

List some options for decrypting drives encrypted with whole disk encryption.

Understanding Whole Disk Encryption

- In recent years, there has been more concern about loss of
  Personal identity information (PII) and trade secrets caused by computer theft
- Of particular concern is the theft of laptop computers and other handheld devices
- To help prevent loss of information, software vendors now provide whole disk encryption
- 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

- Whole disk encryption tools encrypt each sector of a drive separately
- Many of these tools encrypt the drive's boot sector
  - To prevent any efforts to bypass the secured drive's partition
- To examine an encrypted drive, decrypt it first
  - Run a vendor-specific program to decrypt the drive
  - Many vendors use a bootable CD or USB drive that prompts for a **onetime passphrase**

Examining Microsoft BitLocker

- Available Vista Enterprise/Ultimate, Windows 7 and 8 Professional/Enterprise, and Server 08 and 12
- Hardware and software requirements
  - A computer capable of running Windows Vista or later
  - The TPM microchip, version 1.2 or newer
  - A computer BIOS compliant with Trusted Computing Group (TCG)
  - Two NTFS partitions
  - The BIOS configured so that the hard drive boots first before checking other bootable peripherals **Examining Third-Party Disk Encryption Tools**

- Some available third-party WDE utilities:
  - **PGP Full Disk Encryption**
  - **Voltage SecureFile**
  - **Utimaco SafeGuard Easy**
  - **Jetico BestCrypt Volume Encryption**
  - **TrueCrypt**

How the Windows Registry works

- 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 (Registry Editor) program for Windows 9x systems
  - Regedt32 for Windows 2000, XP, and Vista
  - Both utilities can be used for Windows 7 and 8

Exploring the Organization of the Windows Registry

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

Understanding Microsoft Startup Tasks

- Learn what files are accessed when Windows starts
- This information helps you determine when a suspect's computer was last accessed
  - Important with computers that might have been used after an incident was reported

Startup in Windows 7 and Windows 8

- Windows 8 is a multiplatform OS
  - Can run on desktops, laptops, tablets, and smartphones
- The boot process uses a boot configuration data (BCD) store
- The BCD contains the boot loader that initiates the system's bootstrap process
  - Press F8 or F12 when the system starts to access the Advanced Boot Options

Startup in Windows NT and Later

- All NTFS 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 Files for Windows Vista:

– The Ntldr program in Windows XP used to load the OS has been replaced with these three boot utilities:

- Bootmgr.exe
- Winload.exe
- Winresume.exe
  - Windows Vista includes the BCD editor for modifying boot options and updating the BCD registry file
  - The BCD store replaces the Windows XP boot.ini file
- Startup Files for Windows XP:
  - NT Loader (NTLDR)
  - Boot.ini
  - Ntoskrnl.exe
  - Bootvid.dll
  - Hal.dll
  - BootSect.dos
  - NTDetect.com
  - NTBootdd.sys
  - Pagefile.sys

Windows XP System Files

Filename	Description
Ntoskrnl.exe	The XP executable and kernel
Ntkrnlpa.exe	The physical address support program for accessing more than 4 GB of physical RAM
Hal.dll	The Hardware Abstraction Layer (described earlier)
Win32k.sys	The kernel-mode portion of the Win32 subsystem
Ntdll.dll	System service dispatch stubs to executable functions and internal support functions
Kernel32.dll	Core Win32 subsystem DLL file
Advapi32.dll	Core Win32 subsystem DLL file
User32.dll	Core Win32 subsystem DLL file
Gdi32.dll	Core Win32 subsystem DLL file

Fig: Windows XP System Files

- Contamination Concerns with Windows XP
  - When you start a Windows XP NTFS workstation, several files are accessed immediately
- The last access date and time stamp for the files change to the current date and time
  - Destroys any potential evidence
- That shows when a Windows XP workstation was last used **2.7 Describe MS-DOS startup tasks**

✓ MS-DOS uses three files when starting, with the same names as in Windows 9x/Me: Io.sys, Msdos.sys, and Command.com.

✓ Two other files are then used to configure MS-DOS at startup: Config.sys and Autoexec.bat.

✓ Although MS-DOS and Windows 9x use some of the same startup filenames, there are some important differences between the files in these OSs.

➢ Io.sys is the first file loaded after the ROM bootstrap loader finds the disk drive. Io.sys then resides in RAM and provides the basic input and output service for all MS-DOS functions.

➢ Msdos.sys is the second program to load into RAM immediately after Io.sys.

➢ As mentioned, this file is the actual OS kernel, not a text file as in Windows 9x

and Me.

- After Msdos.sys finishes setting up DOS services, it looks for the Config.sys file to configure device drivers and other settings.
- Config.sys is a text file containing commands that typically run only at system startup to enhance the computer's DOS configuration.
- Msdos.sys then loads Command.com, which contains the same internal DOS commands in MS-DOS 6.22 as in Windows 9x. As the loading of Command.com nears completion, Msdos.sys looks for and loads Autoexec.bat, a batch file containing customized settings for MS-DOS that runs automatically.
- In this batch file, you can define the default path and set environmental variables, such as temporary directories. MS-DOS then accesses and resets the last access dates and times on files when powered up.

- **Virtual machine**
  - Allows you to create a representation of another computer on an existing physical computer .A virtual machine is just a few files on your hard drive
  - Must allocate space to it
- A virtual machine recognizes components of the physical machine it's loaded on
  - Virtual OS is limited by the physical machine's OS .

2.3. Current Computer Forensics Tools: Software/ Hardware Tools

Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible
- Questions to ask when evaluating tools: – On which OS does the forensics tool run – What file systems can the tool analyze?
  - Can a scripting language be used with the tool to automate repetitive functions?
  - Does it have automated features?
  - What is the vendor's reputation for providing support?

Types of Digital Forensics Tools

- Hardware forensic tools
  - Range from single-purpose components to complete computer systems and servers
- Software forensic tools – Types
- Command-line applications
- GUI applications
  - Commonly used to copy data from a suspect's disk drive to an image file

Tasks Performed by Digital Forensics Tools

- Follow guidelines set up by NIST's Computer Forensics Tool Testing (CFTT) program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRs) should use validated tools
- Five major categories:
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting **Acquisition**
  - Making a copy of the original drive

- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote, live, and memory acquisitions
  - Two types of data-copying methods are used in software acquisitions:
- Physical copying of the entire drive
- Logical copying of a disk partition – The formats for disk acquisitions vary
- From raw data to vendor-specific proprietary

You can view the contents of a raw image file with any hexadecimal editor

  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
- Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensics drive images on a network

Validation and Verification

– **Validation**

- A way to confirm that a tool is functioning as intended

– **Verification**

- Proves that two sets of data are identical by calculating hash values or using another similar method
- A related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data.

– **Subfunctions**

- Hashing
  - CRC-32, MD5, SHA-1 (Secure Hash Algorithms)
- Filtering

– Based on hash value sets

- Analyzing file headers
  - Discriminate files based on their types
  - National Software Reference Library (NSRL) has compiled a list of known file hashes
- For a variety of OSs, applications, and images

Validation and discrimination

- Many computer forensics programs include a list of common header values
  - With this information, you can see whether a file extension is incorrect for the file type
- Most forensics tools can identify header values

Extraction

- Recovery task in a digital investigation
- Most challenging of all tasks to master
- Recovering data is the first step in analyzing an investigation's data

Subfunctions of extraction

- Data viewing
- Keyword searching
- Decompressing or uncompressing
- Carving
- Decrypting
- Bookmarking or tagging

- **Keyword search** speeds up analysis for investigators
- From an investigation perspective, encrypted files and systems are a problem
- Many password recovery tools have a feature for generating potential password lists
  - For a **password dictionary attack**

- If a password dictionary attack fails, you can run a **brute-force attack**
  - **Reconstruction**
    - Re-create a suspect drive to show what happened during a crime or an incident
    - Methods of reconstruction
  - Disk-to-disk copy
  - Partition-to-partition copy
  - Image-to-disk copy
  - Image-to-partition copy
  - Rebuilding files from data runs and carving – To re-create an image of a suspect drive
  - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
  - Simplest method is to use a tool that makes a direct disk-to-image copy

Examples of disk-to-image copy tools:

- Linux dd command
- ProDiscover
- Voom Technologies Shadow Drive

Reporting

- To perform a forensics disk analysis and examination, you need to create a report
- Subfunctions of reporting
  - Bookmarking or tagging
  - Log reports
  - Report generator
- Use this information when producing a final report for your investigation

Function	ProDiscover Basic	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Acquisition				
Physical data copy	✓	✓	✓	✓
Logical data copy	✓	✓	✓	
Data acquisition formats	✓	✓	✓	✓
Command-line processes				✓
GUI processes	✓	✓	✓	✓
Remote acquisition		✓	✓	✓
Validation and verification				
Hashing	✓	✓	✓	✓
Verification	✓	✓	✓	✓
Filtering		✓	✓	✓
Analyzing file headers		✓	✓	✓
Extraction				
Data viewing	✓	✓	✓	✓
Keyword searching	✓	✓	✓	✓
Decompressing			✓	✓
Carving		✓	✓	✓
Decrypting		✓	✓	
Bookmarking	✓	✓	✓	✓
Reconstruction				
Disk-to-disk copy	✓	✓	✓	✓
Partition-to-partition copy	✓	✓	✓	✓
Image-to-disk copy	✓	✓	✓	✓
Image-to-partition copy	✓	✓	✓	✓
Disk-to-image copy	✓	✓	✓	✓
Rebuilding files	✓	✓	✓	✓
Reporting				

Fig: Comparison of forensic tool functions

- Considerations
  - Flexibility
  - Reliability
  - Future expandability
- Create a software library containing older versions of forensics utilities, OSs, and other programs

Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

Command-line Forensics Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
- One of the first MS-DOS tools used for computer investigations
- Command-line tools require few system resources
- Designed to run in minimal configurations
- Current programs are more powerful and have many more capabilities

Linux Forensics Tools

- **UNIX** has been mostly replaced by Linux
  - You might still encounter systems running UNIX
- **Linux** platforms are becoming more popular with home and business end users
- **SMART**
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer
- **Helix 3**
  - One of the easiest suites to begin with
  - You can load it on a live Windows system
- Loads as a bootable Linux OS from a cold boot

  **Some international courts have not accepted live acquisitions as a valid forensics practice

- **Kali Linux**
  - Formerly known as BackTrack

- Includes a variety of tools and has an easy-to-use KDE interface

- **Autopsy and SleuthKit**
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI browser interface used to access Sleuth Kit's tools

Other GUI Forensics Tools

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- **Advantages**
  - Ease of use
  - Multitasking
  - No need for learning older OSs
- **Disadvantages**
  - Excessive resource requirements
  - Produce inconsistent results – Create tool dependencies
- Investigators' may want to use only one tool
- Should be familiar with more than one type of tool

Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements periodically
- When planning your budget consider:
  - Amount of time you expect the forensic workstation to be running
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

Forensic Workstations

- Carefully consider what you need
  - Categories

    -Stationary workstation
  - Portable workstation
  - Lightweight workstation
- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances
- Police agency labs
  - Need many options
  - Use several PC configurations
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization
- Some vendors offer workstations designed for digital forensics
- Examples
  - F.R.E.D. unit from Digital Intelligence
  - Hardware mounts from ForensicPC
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation **Using a Write-Blocker**
- **Write-blocker**
  - Prevents data writes to a hard disk
- **Software-enabled blockers**
  - Typically run in a shell mode (Windows CLI)
  - Example: PDBlock from Digital Intelligence
- **Hardware options**
  - Ideal for GUI forensic tools

  - Act as a bridge between the suspect drive and the forensic workstation
- You can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies – FireWire

  USB 2.0 and 3.0

  SATA, PATA, and SCSI controllers

Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- With Firewire and USB write-blocking devices
  - You can acquire data easily with Digital Intelligence FireChief and a laptop computer
  - FireWire
- If you want to reduce hardware to carry:
  - WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon
- Recommendations when choosing stationary or lightweight workstation:
  - Full tower to allow for expansion devices
  - As much memory and processor power as budget allows
  - Different sizes of hard drives
  - 400-watt or better power supply with battery backup
  - External FireWire and USB 2.0 ports
  - Assortment of drive adapter bridges
  - Ergonomic keyboard and mouse
  - A good video card with at least a 17-inch monitor
  - High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use highend game PCs

Validating and Testing Forensic Software

It is important to make sure the evidence you recover and analyze can be admitted in court

- You must test and validate your software to prevent damaging the evidence

Using National Institute of Standards and Technology Tools

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on computer forensics tools
- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
    ISO 17025 criteria for testing items that have no current standards
- Your lab must meet the following criteria
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- ISO 5725 - specifies results must be repeatable and reproducible
- NIST created the National Software Reference Library (NSRL) project
  - Collects all known hash values for commercial software applications and OS files
- Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information
  - Can use RDS to locate and identify known bad files

Using Validation Protocols

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how forensics tools work

- One way to compare results and verify a new tool is by using a disk editor
  – Such as Hex Workshop or WinHex
- Disk editors do not have a flashy interface, however they:
  - Are reliable tools
  - Can access raw data
- Computer Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools
- Digital Forensics Tool Upgrade Protocol – Test
- New releases
- OS patches and upgrades
  – If you find a problem, report it to forensics tool vendor
- Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools.