MODULE - III

PROCESSING CRIME AND INCIDENT SCENE

Identifying Digital Evidence – Collecting Evidence – Processing Law Enforcement Crime Scenes – Preparing for a Search – Securing a Digital Incident or Crime Scene - Seizing Digital Evidence at the Scene – Storing Digital Evidence – Obtaining a Digital Hash – Working with Windows and CLI Systems.

Identifying Digital Evidence

Digital evidence can be any information stored or transmitted in digital form. Becausewe can't see or touch digital data directly, it's difficult to explain and describe.

U.S. courts accept digital evidence as physical evidence, which means digital data is treated as a tangible object, such as a weapon, paper document, or visible injury, that's related to a criminal or civil incident.

ISO standard 27037 gives guidance on what procedures countries should have in place for digital evidence. However, each country has its own interpretation of what can or can't be presented in court or accepted as evidence. Some countries used to require that all digital evidence be printed to be presented in court, and this requirement, at one time, was true for many U.S. states.

Groups such as the Scientific Working Group on Digital Evidence (SWGDE; *ww.swgde.org*) set standards for recovering, preserving, and examining digital evidence.

Following are the 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 while processing a crime or incident scene must be done systematically. To minimize confusion, reduce the risk of losing evidence, and avoid damaging evidence, only one team should collect and catalog digital evidence at a crime scene or lab, if practical. If there's too much evidence or too many systems to make it practical for one team to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloging evidence.

Challenge of investigators:

- An important challenge investigators face is establishing recognized standards for digital evidence.
- For example, there are cases involving police raids being conducted simultaneously in many countries as well as anti-cartel investigations taking place in several locations around the world.
- As a result, hundreds of pieces of digital evidence, including hard drives, cell phones, and other storage devices, are seized in multiple sites.

- If law enforcement and civil organizations in these countries have agreed on proper procedures, the evidence can be presented in any jurisdiction confidently.
- Evidence collection is now even more complicated as mobile devices and cloud storage becomes the norm.

Understanding Rules of Evidence

Consistent practices help verify your work and enhance your credibility, so you musthandle all evidence consistently. Apply the same security and accountability controlsfor evidence in a civil lawsuit as in a major crime to comply with your state's rulesof evidence or with the Federal Rules of Evidence (FRE). Also, keep in mind thatevidence admitted in a criminal case might also be used in a civil suit, and vice versa.

For example, suppose someone is charged with murder and acquitted at the criminal trial because the jury isn't convinced beyond a reasonable doubt of the person's guilt. If enough evidence shows that the accused's negligence contributed to a wrongful death, however, the victim's relatives can use the evidence in a civil lawsuit to recover damages.

The following are some that apply to digital forensicsinvestigations:

- Business records, including those of a public agency
- Certain public records and reports
- Evidence of the absence of a business record or entry
- Learned treatises used to question an expert witness
- Statements of the absence of a public record or entry

Another way of categorizing digital records is by dividing them into

- Computer generated records and
- Computer-stored records.

Computer-generated records are data the system maintains, such as system log files and proxy server logs. They are output generated from a computer process or algorithm, not usually data a person creates. Computer-stored records are electronic data that a person creates and saves on a computer or digital device, such as a spreadsheet or word processing document. Some records combine computer-generated and computer-stored evidence, such as a spreadsheet containing mathematical operations (computer-generated records) generated from a person's input (computer-stored records).

Digital Evidence Collection

There are numerous challenges in collecting digital evidence in cyber security because technology changes all the time and many new issues come up like the inconsistency of cyber environments. Initially, the data volatility is a big challenge because important evidence is completely altered or lost with ease in running systems if not captured on time. Also accessing encrypted information or data that is protected poses its own difficulties thus one requires more than just ordinary passwords but decryption methods as well as legal authorization in order to access such information.

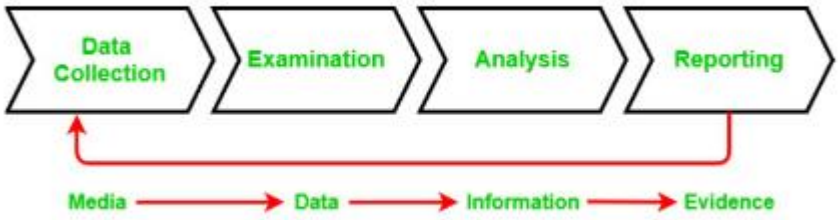
Ensuring data integrity and authenticity is critical, as any alteration during collection can render the evidence inadmissible in court. Additionally, legal and jurisdictional issues often arise, especially when evidence spans multiple regions or countries, necessitating compliance with

diverse legal frameworks and international cooperation. Finally, the rapid phase of technological advancement means forensic tools and methodologies must constantly evolve to keep up with new forms of digital evidence and cyber threats, demanding continuous training and adaptation by cyber security professionals.

Process Involved in Digital Evidence Collection

The main processes involved in digital evidence collection are given below:

- **Data collection:** In this process, data is identified and collected for investigation.
- **Examination:** In the second step the collected data is examined carefully.
- **Analysis:** In this process, different tools and techniques are used and the collected evidence is analyzed to reach some conclusion.
- **Reporting:** In this final step all the documentation and reports are compiled so that they can be submitted in court.



Types of Collectible Data

The computer investigator and experts who investigate the seized devices have to understand what kind of potential shreds of evidence could there be and what type of shreds of evidence they are looking for. So, that they could structure their search pattern.

Crimes and criminal activities that involve computers can range across a wide spectrum, they could go from trading illegal things such as rare and endangered animals, and damaging intellectual property, to personal data theft, etc. has been deleted from the computer, they could be dead, **ca**n be encrypted, or The files investigator should be familiar with a variety of tools, methods, and also software to prevent the data from damaging during the data recovery process.
There are two types of data, that can be collected in a computer forensics investigation:

- **Persistent data:** It is the data that is stored on a non-volatile memory type storage device such as a local hard drive **the** external storage devices like SSDs, HDDs, pen drives, CDs, The. The data on these devices is preserved even when the computer is turned off.
- **Volatile data:** It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, an investigator must know how to reliably capture it.

Types of Evidence

Collecting the shreds of evidence is important in any investigation to support the claims in court. Below are some major types of evidence.

- **Real Evidence:** These pieces of evidence involve physical or tangible evidence such as flash drives, hard drives, and documents, an eyewitness can also be considered as a shred of tangible evidence.
- **Hearsay Evidence:** These pieces of evidence are referred to as out-of-court statements. These are made in courts to prove the truth of the matter.
- **Original Evidence:** These are the pieces of evidence of a statement that is made by a person who is not a testifying witness. It is to prove that the statement was made rather than to prove its truth.
- **Testimony:** Testimony is when a witness takes oath in a court of law and gives their statement in court. The shreds of evidence presented should be authentic, accurate, reliable, and admissible as they can be challenged in court.

Challenges Faced During Digital Evidence Collection

- Evidence should be handled with utmost care as data is stored in electronic media and it can get damaged easily.
- Collecting data from volatile storage.
- Recovering lost data.
- Ensuring the integrity of collected data.

Collecting Evidence in Private-Sector Incident Scenes

Private-sector organizations include

- small to medium businesses,
- large corporations and
- non-government organizations (NGOs) which might get funding from thegovernment or other agencies.

In the United States, NGOs and similar agencies mustcomply with state public disclosure and federal Freedom of Information Act (FOIA)laws and make certain documents available as public records. State public disclosure laws define state public records as open and available for inspection. For example, divorces recorded in a public office, such as courthouse, become matters of publicrecord unless a judge orders the documents sealed. Anyone can request a copy of apublic divorce decree.

Investigating and controlling computer incident scenes in private-sector environments is much easier than in crime scenes.

In the private sector, the incident scene is often a workplace, such as a contained office or manufacturing area, where a policy violation is being investigated. Everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority—that is, company management.

Typically, businesses have inventory databases of computer hardware and software. Having access to these databases and knowing what applications are on suspected computers help identify the forensics tools needed to analyze a policy violation and the best way to conduct the analysis.

For example, companies might have a preferred Web browser, such as Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome.

Knowing which browser a suspect used helps you develop standard examination procedures to identify data downloadedto the suspect's workstation.

To investigate employees suspected of improper use of company digital assets, a company policy statement about misuse of digital assets allows private-sector investigators to conduct covert surveillance with little or no cause and access company computer systems and digital devices without a warrant, which is an advantage.

Law enforcement investigators can't do the same, however, without sufficient reason fora warrant. However, if a company doesn't display a warning banner or publish a policy statingthat it reserves the right to inspect digital assets at will, employees have an expectationof privacy.

When an employee is being investigated, this expected privacy prevents the employer from legally conducting an intrusive investigation.

A well-defined company policy, therefore, should state that an employer has the right to examine, inspect, or access any company-owned digital assets.

If a company issues a policy statement to all employees, the employer can investigatedigital assets at will without any privacy right restrictions; this practice mightviolate the privacy laws of countries in the EU, for example.

As a standard practice,companies should use both warning banners and policy statements.

For example, ifan incident is escalated to a criminal complaint, prosecutors prefer showing juries warning banners instead of policy manuals.

A warning banner leaves a much strongerimpression on a jury.

However, if a company doesn't display a warning banner or publish a policy stating that it reserves the right to inspect digital assets at will, employees have an expectation of privacy.

When an employee is being investigated, this expected privacy prevents the employer from legally conducting an intrusiveinvestigation.

A well-defined company policy, therefore, should state that an employerhas the right to examine, inspect, or access any company-owned digital assets.

If acompany issues a policy statement to all employees, the employer can investigatedigital assets at will without any privacy right restrictions; this practice mightviolate the privacy laws of countries in the EU, for example.

As a standard practice,companies should use both warning banners and policy statements. For example, ifan incident is escalated to a criminal complaint, prosecutors prefer showing jurieswarning banners instead of policy manuals.

If you discover evidence of a crime during a company policy investigation, first determine whether the incident meets the elements of criminal law.

You might have to consult with your organization's attorney to determine whether the situation is a potential crime.

Next, inform management of the incident; they might have other concerns, such as protecting confidential business data that could be included with the criminal evidence called as "commingled data". In this case, coordinate with management and the organization's attorney to determine the best way to protect commingled data. After you submit evidence containing sensitive information to the police, it becomes public record.

Public record laws do include exceptions for protecting sensitive company information; ultimately, however, a judge decides what to protect.

Your next step is to work with the attorney to write an affidavit confirming your findings.

The attorney should indicate in the affidavit that the evidence is commingled with company secrets, and releasing the information will be detrimental to the company's financial health.

When the affidavit is completed, you sign it before a notary, and then deliver the affidavit and the recovered evidence with log files to the police, where you make a criminal complaint.

At the same time, the attorney goes to court and requests that all evidence recovered from the hard disk that's not related to the complaint and is a company trade secret be protected from public viewing.
You and the attorney have reported the crime and taken steps to protect the sensitive data.

Preparing for search

Preparing for search and seizure of computers or digital devices is probably the mostimportant step in digital investigations. The better you prepare, the smoother your investigation will be.
The following sections discuss the tasks you should performbefore you search for evidence

- **Identifying the Nature of the Case**

Start the investigation by identifying the nature of the case, including whether it involves the private or public sector.

For example, a private-sector investigation might involve an employee abusing Internet privileges by surfing the Web excessively or an employee who has filed an equal employment opportunity (EEO), e-mail harassment, or other ethics complaint.

Serious cases might involve an employee abusing company digital assets to acquire or deliver contraband. Law enforcement cases could range from a check fraud ring to a homicide.
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**

Next, determine the type of OSs involved in the investigation. For law enforcement, this step might be difficult because the crime scene isn't controlled. Determine the OS: Microsoft, Linux, macOS, Apple iOS, Android, and so forth. Estimate the size of the storage device on suspect computers and determine how many digital devices you have to process atthe scene. Determine what hardware might be involved, such as PCs or mobiledevices, including smartphones, tablets, Fitbits, and laptops. For private-sector investigators, configuration management databases make this step easier. Consultants to the private sector or law enforcementofficers might have to investigate more thoroughly to determine these details.

You also need to consider cloud storage, which has become more widespread. Most smart phones, for example, are automatically backed up to the cloud, and people oftenstore their files, music, and pictures in the cloud. You might need a separate warrant or subpoena to access this information.

- **Determining Whether You Can Seize Computers and Digital Devices**

Generally, the ideal situation for incident or crime scenes is seizing computers and digital devices and taking them to your lab for further processing. However, the type of case and location of the evidence determine whether you can remove digital equipment from the scene.
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 shouldn't be taken offsite, unless you have disclosed the effect of the seizure to the judge. An additional complication is files stored offsite that are accessed remotely. You must decide whether the drives containing these files need to be examined.

If you aren't allowed to take the computers and digital devices to your lab,determine the resources you need to acquire digital evidence and which tools canspeed data acquisition. With large drives, such as a terabyte or more, acquisition times can increase to several hours.
Some softwarecompresses data while making forensic images. For large drives, this compressionmight be necessary.

- **Getting a Detailed Description of the Location**

The more information you have about the location of a digital crime, the more efficiently you can gather evidence from the crime scene.

Environmental and safety issues are the main concerns during this process. Before arriving at incident or crimescenes, identify potential hazards to your safety as well as that of other examiners.
Some cases involve dangerous settings, such as a drug bust of a methamphetaminelab or a terrorist attack using biological, chemical, or nuclear contaminants. For these types of investigations, you must rely on the skills of **hazardous materials (HAZMAT)**teams to recover evidence from the scene.

The recovery process might include decontaminating digital components needed for the investigation, if possible. If the decontamination procedure might destroy electronic evidence, a HAZMAT specialist or an investigator in HAZMAT gear should make an image of a suspect's drive. If you have to rely on a HAZMAT specialist to acquire data, coach the specialist on how to connect cables and how to run the software. You must be exact and articulate in your instructions.
Ambiguous or incorrect instructions could destroy evidence.

- **Determining Who Is in Charge**

  A company needs an established line of authority to specify who can instigate or authorize an investigation. Private-sector investigations usually require only one person to respond to an incident or crime scene. Processing evidence usually involves acquiring an image of a suspect's drive. In law enforcement, however, many investigations need additional staff to collect all evidence quickly. For large-scale investigations, a crime or incident scene leader should be designated. Anyone assigned to a large-scale investigation scene should cooperate with the designated leader to ensure that the team addresses all details when collecting evidence.

- **Using Additional Technical Expertise**

  After you collect evidence data, determine whether you need specialized help to process the incident or crime scene. For example, suppose you're assigned to process a crime scene at a data center running Windows servers with several RAID drives and high-end Linux servers.
  If you're the lead on this investigation, you must identify the additional skills needed to process the crime scene, such as enlisting help with a high-end server OS.

  Other concerns are how to acquire data from RAID drives and how much data you can acquire. RAID servers typically process several terabytes of data, and standard imaging tools might not be able to handle such large data sets.

  When working at high-end computing facilities, identify the applications the suspect uses, such as Oracle databases.

  You might need to recruit an Oracle specialistor site support staff to help extract data for the investigation.

  In addition, mobiledevices are found at most incident scenes, so having someoneon hand who knows how to handle them is essential.

- **Determining the Tools You Need**

  After you have gathered as much information as possible about the incident or crime scene, you can start listing what you need at the scene. Being over prepared is better than being underprepared, especially when you determine that you can't transfer the computer to your lab for processing. To manage your tools, consider creating an initial-response field kit and an extensive-response field kit. Using the right kit makes processing an incident or crime scene much easier and minimizes how much you have to carry from your vehicle to the scene.

Your initial-response field kit should be lightweight and easy to transport. With this kit, you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible. Figure below shows some items you might need, and Table below lists the tools you might need in an initial-response field kit.

Table 4-1 Tools in an initial-response field kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	Set of Japanese Industrial Standard (JIS) screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wrist bands
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	USB drives (or a portable hard drive)

Table 4-2 Tools in an extensive-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	Set of JIS screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wristbands
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
10	USB drives of varying sizes
2	External hard drives (1 TB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives or USB drives for data acquisition

- **Preparing the Investigation Team**

Before you initiate the search and seizure of digital evidence at incident or crime scenes, you must review all the available facts, plans, and objectives with the investigation team you have assembled. The goal of scene processing is to collect and secure digital evidence successfully.
The better prepared you are, the fewer problems you encounter when you carry out the plan to collect data. Keep in mind that digital evidence is volatile. Develop the skills to assess the facts quickly, make your plan, gather the needed resources, and collect data from the incident or crime scene. In some digital investigations, responding slowly might result in the loss of important evidence for the case.

Seizing Digital Evidence at the Scene

When seizing digital evidence at a crime scene, law enforcement officers should follow best practices to ensure the evidence is collected properly and securely:

- Secure the scene: Protect the area from tampering or destruction.
- Identify potential evidence: Look for digital devices such as computers, phones, storage devices, and cameras.
- Document the scene: Take photos of the device, its cords and cables, and any other relevant items.
- Seize the evidence: Document how the device is seized and placed into evidence.
- Avoid data manipulation: Leave the device in its current power state, if possible.
- Gather additional items: Collect any associated chargers, cables, peripherals, and manuals.
- Consider forensic experts: For highly sensitive investigations, it's best to bring in forensic experts before you do anything.
- Confirm legal authority: Make sure you have the legal authority to seize the evidence.
- Keep evidence away from damaging elements: Keep all media away from magnets, radio transmitters, and other potentially damaging elements

Storing Digital Evidence

With digital evidence, we need to consider how and on what type of media to saveit andwhat type of storage device is recommended

Optical Media:

The choice of mediafor storing digital evidence usually depends on how long we need to keep it. If you investigate criminal matters, store the evidence as long as you can. The ideal storage media for digital data used to be CDs and DVDs. Since the lifespan of CDs and DVDs is now 2 to 5 years. The optimum choice now is solid-state USB drives. Although they're more expensive than CDs andDVDs, they're more durable.

Magnetic Tape:

We can also use magnetic tape to preserve evidence data. The 4-mm DAT magnetic tapes store from 40 to 72 GB or more of data, but they're slow at reading andwriting data. If you're using these tapes, test stored data by copying the contents fromthe tape back to a disk drive. Then verify that the data

is good by examining it withforensics tools or doing an MD5 hash comparison of the original data and the newlyrestored data. Evidence is routinely kept for long periods. In the United States, for example, tensof thousands of rape kits kept in storage have never been processed, and as you've probably heard, cold cases from 20, 30, or even 50 years ago are now being solvedbecause of advances in technology. If a 30-yearlifespan for data storage is acceptable for your digital evidence, then older DLT magnetictape cartridge systems are a good choice.

Keep in mind that you never know howlong it will take for a case to go to trial. DLT systems have been used with mainframecomputers for several decades and are reliable data-archiving systems. Depending on the size of the DLT cartridge, one cartridge can store up to 80 GB of data in compressedmode.

Speed of data transfer from a hard drive to a DLT tape is also faster thantransferring data to a CD or DVD. The only major drawback of a DLT drive and tapes iscost. A drive can cost from $400 to $800, and each tape is about $40.

Manufacturers such as Quantum Corp. introduced a high-speed, high-capacitytape cartridge drive system called Super Digital Linear Tape (Super-DLT or SDLT).

Thesesystems are specifically designed for large RAID data backups and can store more than 1 TB of data. Smaller external SDLT drives can connect to a workstation through a SCSIcard.

In addition, many external USB drives can hold 1 or more TB of information.

Reliable offsite storage and encrypted cloud storage are other options. Don't rely on one media storage method to preserve your evidence, however. Be sure to make two copies of every image to prevent data loss. Also, if practical, use different tools to create the two images because every tool has strengths and weaknesses.

For example, you can use the Linux dd command to create the first imageand FTK Imager Lite to create the second image.

Obtaining a Digital Hash

To verify data integrity, different methods of obtaining a unique identity for file data have been developed. One of the first methods was the **Cyclic Redundancy Check (CRC)**,a mathematical algorithm that determines whether a file's contents have changed. The most recent version is CRC-32. CRC, however, is not considered a forensic hashing algorithm. The first algorithm used for digital forensics was **Message Digest 5 (MD5)**.Like CRC, MD5 is a mathematical formula that generates a hexadecimal code, or **hash value**, based on the contents of a file, a folder, or an entire drive.

If a bit or byte in the filechanges, it alters the hash value, a unique hexadecimal value that can be used to verifythat a file or drive hasn't changed or been tampered with.

Before you process or analyzea file, you can use a software tool to calculate its hash value. After you process the file,you produce another digital hash.

If it's the same as the original one, you can verify theintegrity of your digital evidence with mathematical proof that the file didn't change.

According to work done by Wang Xiaoyun and her associates from Beijing's Tsinghua University and Shandong University of Technology, there are 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.

Another hashing algorithm is **Secure Hash Algorithm version 1 (SHA-1)**, developed by the **National Institute of Standards and Technology (NIST)**.

Keyed hash set vs non keyed hash set

Most digital forensics hashing needs can be satisfied with a **non keyed hashset**, which is a unique hash number generated by a software tool, such as the Linuxmd5sum command.

The advantage of this type of hash is that it can identify knownfiles, such as executable programs or viruses, that hide themselves by changing theirnames.

For example, many people who view or transmit pornographic material changefilenames and extensions to obscure the nature of the contents.

However, even if afile's name and extension change, the hash value doesn't.

The alternative to a non keyed hash is a **keyed hash set**, which is created by anencryption utility's secret key.

You can use the secret key to create a unique hash valuefor a file. Although a keyed hash set can't identify files as non keyed hash methods can,it can produce a unique hash set for digital evidence.

Securing a Digital Incident or Crime Scene

Securing the Crime Scene first responders should guarantee the safety of all the people at the crime scene further as defend the integrity of the proof. Once inbound at the location, the first responders should move to the scene of the incident and establish the victim devices, **networks**, so on and mark a fringe.

Some of the best practices to secure the crime scene include:

• Follow customary procedures and policies of the legal authority whereas securing the scene
• Make positive that the scene is safe for the res-ponders
• Verify the sort of the incident
• Secure all electronic devices, as well as personal or moveable devices
• Verify any information that's related to the offence
• Remove all persons from the crime scene or the world containing proof
• Do not permit a person to access the scene or electronic devices
• Deny any provide of facilitate or technical help
• Isolate alternative persons who area unit gift at the scene
• Locate and facilitate the victim
• Transmit further flash messages to alternative responding units
• Request further facilitate at the scene if required
• Establish a **security** perimeter to check if the offenders area unit still gift at the crime scene space
• Protect and preserve the proof that's in danger of being simply lost
• Protect destructible knowledge (e.g., pagers and caller ID boxes) physically and electronically
• Make positive that the devices that contain destructible knowledge area unit secured, documented, and photographed
• Find phone lines that area unit connected to devices like modems and caller ID boxes
• Document, disconnect, and label phone lines and network cables
• Observe the present state of affairs at the scene and record observations
• Protect physical proof or hidden fingerprints that will be found on keyboards, mice, diskettes, and DVDs.

Working with Windows and CLI Systems

Alternate data streams Ways data can be appended to the existing files, they can find evidence intentionally or by coincidence American standard code for information interchange (ASC II) 8-bit configuration Areal density Number of bits in one square inch of disk platter Attribute ID Record contains file or folder of info, divided into record fields, each record field is referred to as an attribute ID Boot.ini Displays boot menu on NT Loader BootSect.dos A hidden file which contains the address (boot sector location) of each OS Bootstrap process Part of the CMOS set-up, tells the computer how to proceed Clusters Sectors are grouped to form clusters, which store one or more sector, 512 bytes-32,000 bytes. Combining the sectors minimizes the overhead of writing or reading files to a disk Cylinders Is a column of tracks on two or more disk platters. Typically, each platter has two surfaces, top and bottom Data runs Files larger than 512 bytes = non- resident outside of MFT, the cluster addresses for these non-resident fields are known as data runs Device drivers Contain instructions for the OS for hardware devices, such as the keyboard, mouse and video card and are stored in the system root\Windows\System32\Drivers Drive slack Unused space in a cluster between the end of an active file's content and the end of the cluster

Encrypting file system (EFS) Windows 2000 added the optional built-in encryption to NTFS, uses both a public key and private key methods of encrypting files, folders, or disk volumes (partitions) File allocation table (FAT) File structure database that Microsoft designed for floppy disks File slack Just extra space in a file File system A hierarchal structure of how OS group their files Geometry A disk's logical structure of platters, tracks, and sectors Hal.dll Hardware Abstraction Layer (HAL) dynamic link library, located in the system root\Windows\System32 folder Head Device that reads and writes data to a drive Head and cylinder skew Improving disk performance, read and

write heads move from one track to another starting sectors are offset to minimize lag time High performance file system (HPFS) Within the OS/2 operating system with IBM. NT provided backward compatibility so that NT could read OS/2 and HPFS disk drives Info2 file Windows stores information about the original path and filename because this is the control file for the recycle bin Iso image An archived file of an optical disk Logical addresses Cluster numbers assigned to the 1 sector of the disk (contains system area, boot record, and a file structure database)