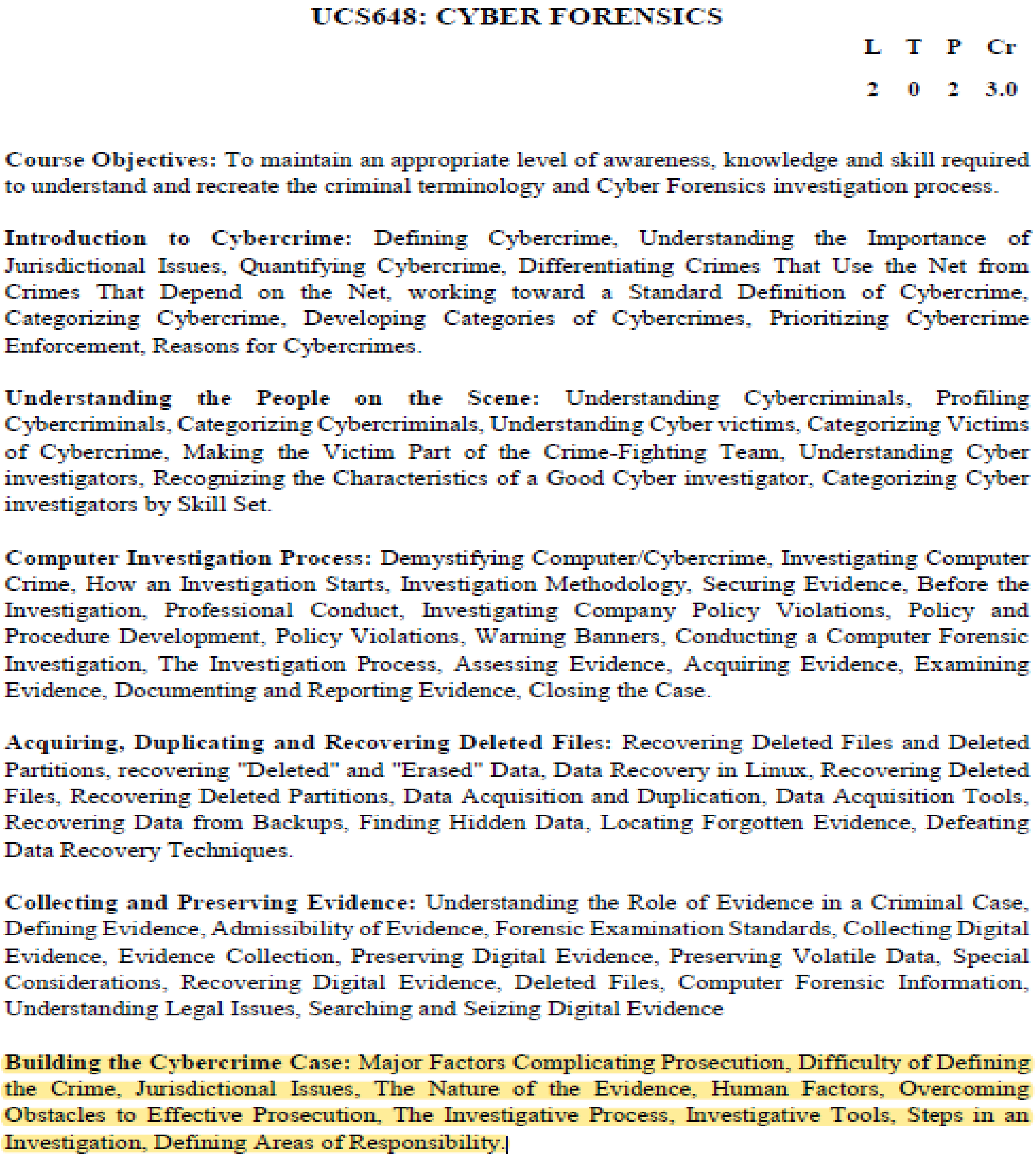
Chapter – 11

“Building the Cybercrime Case”

Reference: Shinder L. D., Cross M., Scene of the Cybercrime, Syngress.

Outline

- Major factors Complicating Prosecution
- Difficulty of Defining the Crime
- Jurisdictional Issues
- The Nature of the Evidence
- Human factors
- Overcoming Obstacles to Effective Prosecution
- The Investigative Process
- Steps in an Investigation
- Defining Areas of Responsibility



UCS648: CYBER FORENSICS

L	T	P	Cr
2	0	2	3.0

Course Objectives: To maintain an appropriate level of awareness, knowledge and skill required to understand and recreate the criminal terminology and Cyber Forensics investigation process.

Introduction to Cybercrime: Defining Cybercrime, Understanding the Importance of Jurisdictional Issues, Quantifying Cybercrime, Differentiating Crimes That Use the Net from Crimes That Depend on the Net, working toward a Standard Definition of Cybercrime, Categorizing Cybercrime, Developing Categories of Cybercrimes, Prioritizing Cybercrime Enforcement, Reasons for Cybercrimes.

Understanding the People on the Scene: Understanding Cybercriminals, Profiling Cybercriminals, Categorizing Cybercriminals, Understanding Cyber victims, Categorizing Victims of Cybercrime, Making the Victim Part of the Crime-Fighting Team, Understanding Cyber investigators, Recognizing the Characteristics of a Good Cyber investigator, Categorizing Cyber investigators by Skill Set.

Computer Investigation Process: Demystifying Computer/Cybercrime, Investigating Computer Crime, How an Investigation Starts, Investigation Methodology, Securing Evidence, Before the Investigation, Professional Conduct, Investigating Company Policy Violations, Policy and Procedure Development, Policy Violations, Warning Banners, Conducting a Computer Forensic Investigation, The Investigation Process, Assessing Evidence, Acquiring Evidence, Examining Evidence, Documenting and Reporting Evidence, Closing the Case.

Acquiring, Duplicating and Recovering Deleted Files: Recovering Deleted Files and Deleted Partitions, recovering "Deleted" and "Erased" Data, Data Recovery in Linux, Recovering Deleted Files, Recovering Deleted Partitions, Data Acquisition and Duplication, Data Acquisition Tools, Recovering Data from Backups, Finding Hidden Data, Locating Forgotten Evidence, Defeating Data Recovery Techniques.

Collecting and Preserving Evidence: Understanding the Role of Evidence in a Criminal Case, Defining Evidence, Admissibility of Evidence, Forensic Examination Standards, Collecting Digital Evidence, Evidence Collection, Preserving Digital Evidence, Preserving Volatile Data, Special Considerations, Recovering Digital Evidence, Deleted Files, Computer Forensic Information, Understanding Legal Issues, Searching and Seizing Digital Evidence

Building the Cybercrime Case: Major Factors Complicating Prosecution, Difficulty of Defining the Crime, Jurisdictional Issues, The Nature of the Evidence, Human Factors, Overcoming Obstacles to Effective Prosecution, The Investigative Process, Investigative Tools, Steps in an Investigation, Defining Areas of Responsibility.

Introduction

- Constructing a criminal case is a long and complex process.
- The more technical the facts of the case, the more difficult it is to build a good case.
- Many people such as investigators, crime scene technicians, crime lab personnel, law enforcement officers and members of assisting Agencies together actively contribute in the construction of the case.
- To obtain a rightful conviction in court, a well prepared case file containing documentation of all the evidence needs to be prepared.

Major Factors Complicating Prosecution

Few criminal prosecutions are as simple as they seem at first glance. For example: Even a straightforward speeding ticket can turn into a complex matter if it goes to trial. Officers can be asked to prove : -

- That they have been adequately trained in the use of radar equipment.
- The genuineness of that equipment can be brought into question based on a many of theoretical technical possibilities.
- Prosecuting more serious offenses requires even more preparation.
- Cybercrimes are inherently complex by their very nature.
- Computers—which are complicated machines, the operation of which is really understood by very few people—always play a key role in every cybercrime case.
- Cybercrimes are often poorly defined in the law because the legislators who make those laws don’t understand the complex technology.
- Jurisdictional ambiguities can further create problems for investigators and as well as for prosecutors.
- Much of the evidence in a cybercrime case might be both intangible and circumstantial.
- Therefore , there are many obstacles that make prosecution a complex process.

Difficulty of Defining the Crime

- Tech people - have only a vague understanding of the law and what constitutes a crime.
- The more laws there are on the law books, the more potential there is for two conflicting , which can lead developments such as:
  - ❑ There is more potential for abuse of the laws, resulting in innocent people being punished.
  - ❑ There is more potential for the laws to be ignored, resulting in guilty people going unpunished.

- Because the law is complicated with ever-changing rules, many non-lawyers do not try to understand:
  - ○ how the legal system works.
  - ○ the differences between different bodies and types of law.
  - ○ how all these different laws interact with one another.

- Generally, laws can be divided into three different “bodies.”
  - ❑ Criminal law
  - ❑ Civil law
  - ❑ Administrative/Regulatory law

- Each of these bodies of law has:
  - ➢ Its own rules of procedure
  - ➢ Different penalties for violation
  - ➢ Different enforcement agencies and courts that have jurisdiction.
  - ➢ The burden of proof and the level of proof required to win a case are different, depending on the applicable body of law.

Criminal Law

- Criminal laws are designed to protect society, as well as individual persons from harmful acts.
- They are also designed to punish offenders and to ensure that they are unable to pose a further risk to society by placing them in prison.
- Criminal complaints can be filed by the individual(s) who are harmed or by law enforcement officers or citizens who observe the offense.
- In a criminal case, the person or entity that files the charges is referred to as the *complainant, and the person (or company)* against whom the charges are brought is called the *defendant.*
- Illegal – means against the law- can it be always considered criminal?

For Example:

- Software *piracy (which involves* making and distributing copies of copyrighted software without the authorization of the copyright holder) is a criminal offense in some circumstances and jurisdictions, but giving away a copy you purchased legally is not.
- However, doing so might be a breach of —the End-User Licensing Agreement (EULA) that a person "signs" when he or she installs the software.
- This means the software vendor could file a civil law suit against you in the court asking for monetary damages.

- A *criminal offense must be specifically defined as such by a locality's, state's, or* country's written statutes.

- **For example:** In India, Cybercrimes are covered under **Information Technology Act (IT Act)** and the **Indian Penal Code**. The IT Act, 2000, which came into force on October 17, 2000, deals with cybercrime and electronic commerce. The IT Act was later amended in the year 2008. The Act defines cyber crimes and punishments.

- **Criminal offenses** are generally classified according to the seriousness of the crime and the severity of the penalty.

- These classifications can include the following:

  - ❑ *violations, the least serious offenses, the* penalty for which is only a fine
  - ❑ *misdemeanors, more serious than violations with a* penalty of fine or jail term
  - ❑ *felonies, the most serious offenses, which carry a* penalty of imprisonment (and in some jurisdictions, the death penalty for the most serious cases).

- Cybercrimes span the range of classifications and penalty grades. **For Example:** a network intrusion that causes little loss is a misdemeanor, whereas an attack that results in large monetary losses to the victim/organization is a felony.

- In many jurisdictions, offenses such as theft, property damage, and others that cause monetary loss are classified according to the amount of the loss or damage.

Some important sections of the IT Act under which cyber crimes may be registered are :

- **Section 65** – Tampering with Computer Source Documents. Penalties if found guilty can be imprisonment up to 3 years and/or up-to Rs 2 lakh fine. An example of such crime is: Employees of a telecom company were held guilty by the court for tampering with the Electronic Serial Number of cellphones of another company that had locked the handset before selling it so as to work with its SIM only.
- **Section 66** – Hacking with computer systems or unauthorised usage of computer system and network. Punishment if found guilty can be imprisonment up to three years and/or a fine of up to Rs 5 lakh. An example: When a criminal hacked into an academy network by unauthorized access of broadband and modified the passwords of users to deny access. The criminal was punished under Section 66 of IT Act.
- **Section 66C** – Identity theft using passwords, digital signatures, biometric thumb impressions or other identifying features of another person for fraudulent purposes. An example is – when a criminal obtained the login and password of an online trading account and transferred the profit to his account by doing online transactions in the trading account in an unauthorized manner. The criminal was charged under Section 66C.
- **Section 66D** – Cheating by Personation Using Computer Resources. Punishment if found guilty can be imprisonment up to three years and/or up to Rs 1 lakh fine. An example: A criminal who posed as a woman and tried to gain trust of a businessman to extort Rs 96 lakh from him by creating a fake email Id and trapping him in a cyber relationship. The criminal was arrested and charged under Section 66D and various other IPC sections.
- **Section 66E** – Taking pictures of private areas, publishing or transmitting them without a person's consent is punishable under this section. Penalties if found guilty can be imprisonment up to three years and/or up to Rs 2 lakh fine.
- **Section 66F** – Acts of cyber terrorism. Guilty can be served a sentence of imprisonment up to life! An example: When a threat email was sent to the Bombay Stock Exchange and the National Stock Exchange, which challenged the security forces to prevent a terror attack planned on these institutions. The criminal was apprehended and charged under Section 66F of the IT Act.
- **Section 67** – Publishing Obscene Information in Electronic Form. In this case, the imprisonment is up to five years and a fine up to Rs 10 lakh. An example: When an accused from Mumbai posted obscene information about the victim on the internet after she refused to marry him. The criminal was implicated under Section 67 of the IT Act in addition to various sections of IPC.
- Apart from the above laws, there are many more sections under IT Act and IPC, which have provisions for cybercrime.

- The law enforcement agencies can take recourse to the following IPC, 1860 sections if the IT Act is insufficient to cover specific cyber offences:

- **Section 379** – Punishment for theft for up to three years and/or fine. Since many cybercrimes are committed using stolen mobile/computers or stolen data this IPC Section comes into the picture.
- **Section 420** – Cheating and dishonestly inducing delivery of property. Cybercrimes like creating Bogus websites, cyber frauds are punishable under this section of IPC with a seven-year jail term and/or fine. This section of the IPC deals with crimes related to password thefts for committing frauds or creating fraudulent websites.
- **Section 463** – Making false documents or false electronic records. Crimes such as Email spoofing are punishable under this section with imprisonment of up to seven years and/or fine.
- **Section 468** – Committing forgery for the intention of cheating attracts imprisonment of up to seven years and/or a fine. Email spoofing is one such crime punishable under this section.

Check:
https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india/

- Penalties for violating a criminal law can range from light to severe, including:
    - ❑ A warning citation (usually in the case of traffic laws or other lowest level misdemeanors)
    - ❑ A citation that imposes a fine (monetary payment that goes to the state)
    - ❑ Compensation or restitution (monetary payment that goes to the victim)
    - ❑ Community service (mandatory “volunteer” work for some charitable organization or governmental body)
    - ❑ Probation (supervision or oversight by the government for a specified period of time in lieu of confinement, which can include court-order restrictions on behavior such as no use of computers or required attendance at counseling sessions)
    - ❑ Confinement in jail (usually for a limited time, such as a few days to a year)
    - ❑ Confinement in prison (usually for a more extended time, ranging from a few months to life)
    - ❑ The death penalty (in some jurisdictions; usually limited to people convicted of murder)

Civil Law

- Civil law undertakes disagreements(disputes) between persons or entities (*parties to the suit or action).*
- Civil wrongs are not crimes; they are called *torts.*
- *Civil litigation is the legal process of petitioning* a court for compensation or correction of these torts.
- In a civil suit, the party who initiates the lawsuit is called the *plaintiff, and the person against* whom the suit is brought is called the *respondent.*
- The losing party in a civil suit does not generally go to jail or prison unless also convicted of a criminal offense such as contempt of court. Instead, they faces one of the two types of court orders:

❑ An order requiring that the respondent pay monetary damages. These damages can include *compensatory damages for the actual and anticipated* losses suffered by the plaintiff—both tangible and intangible—and *punitive damages beyond the actual losses, designed to punish the party who* committed the wrong.

❑ An injunction requiring that the respondent do some specified act or *not* do some specified act. For example, an injunction could order that the party stop sending e-mail to the plaintiff. An injunction is a legally binding order, and ignoring it can result in criminal charges.

- Now , An act can be both a crime and a civil wrong.

  - Cybercrime investigators may find that the evidence in their cases is also evidence in a civil lawsuit.
  - For Example: When a company's network is invaded, in addition to filing criminal charges against the hacker, the company can also file a civil suit that seeks to directly collect monetary compensation for damages such as loss of worker productivity and lost sales due to the hacker's actions.

- Another important concept in civil law is that of *vicarious liability. This is the* legal responsibility that one person or entity has for someone else's actions.

  - Vicarious liability is usually created by some sort of "oversight" relationship. A person or entity that has oversight or control over another person can be held civilly liable for wrongs committed by that person.

  - This means a parent can be held liable for a child's acts, and an employer can be held responsible for an employee's acts. For Example:

  - if a hacker uses company equipment and time to illegally break into other networks to commit a cybercrime, the employing company could be sued for allowing it to happen.

Administrative/Regulatory Law

- Administrative laws are **neither criminal nor civil** but have the authority of law within their **areas of jurisdiction**.

- This body of law consists of rules and regulations that are enacted by a governmental agency under authority given to it by the legislative body .

- Administrative law apply to a particular occupational field or a body that govern a particular area of life.

- Examples include Environmental Protection Agency regulations as well as rules that govern the practice of medicine, law, engineering.

- **For Example:** an administrative action can be brought against a government employee, a doctor or a lawyer etc. who violates the state regulatory agency's rules.

- Administrative actions can involve imposing fines, revoking licenses or suspension from the post held.

- The proceedings of administrative actions are quasijudicial. The actions are conducted according to procedures set out by the law similar to that of a court, but the hearing counsels are not officers of the court.

- **For Example:** cybercriminal working in the finance industry who discovers and misuses insider information in a stock trade might be subject to both criminal charges and administrative sanctions.

Types of Law

(Based upon Origin of Law)

Laws of all three types i.e. criminal, civil, and administrative/ regulatory—come into being in one of three ways:

- They're passed by a legislative body (example: parliament)
- They're created through court decisions,
- They arise out of tradition and practice.

The origin of a law determines law as:

- ❑ Statutory law
- ❑ Case law
- ❑ Common law

- ***Statutory Law***
- *Statutory law carries the most weight of the three types of law and is what we* usually think of when we think of “the law.”

- Statutory laws are created through a formal process known as *legislation*.

- *They are introduced as proposed laws, or bills*, debated, amended, voted upon, and passed by one or more legislative bodies and signed into law by an executive officer of the jurisdiction.

- In most cases, both the members of the legislative body and the executive officer are elected by popular vote of the citizens.

- Statutory laws are written and published as statutes, then *codified (collected into codes) and enforced by police and other* law enforcement agencies.

Case Law

- *Case law is based on judicial interpretation of laws that have been enacted by legislative* bodies (statutory law) and governing documents.

- Case law doesn't carry the same weight as statutory law.

- The judicial opinions that form the basis of case law do establish *precedent, which means* case law is given weight by other judges making decisions in subsequent cases.

- In both criminal and civil court, an attorney cites previous case decisions to back up his or her case, and this forms an important part of the basis for a judge's decision.

Common law (based on the English common law system) was an important way of governing society in a time when far fewer laws were formally enacted.

- Common law is based on practice, or "the way we've always done it."

- For Example: Two persons can become legally married without obtaining a marriage license from the state by meeting the common law requirements (public declaration, registration, etc).

Jurisdictional Issues

- Cybercrime cases often involve complex jurisdictional issues that can present both legal and practical obstacles to prosecution.

Defining Jurisdiction

- *Legal jurisdiction refers to the scope of authority given to a law enforcement* agency to enforce laws or to a court to pronounce legal judgments.
- All governmental powers are jurisdictional in nature.
- That is, they are applicable only in regard to specific places or subject matter.
- Cyberspace complicates matters because a person can now—via computer—commit an act in any country accessible through the Internet without physically being there.
- There are different types and levels of jurisdictional authority.

Types of Jurisdictional Authority

The jurisdiction of an enforcement agency or of a court can be based on the following :

- **The legal system under which the law falls** Police agencies have jurisdiction over criminal cases but no jurisdiction over civil matters. Citizens often ask police officers to intervene in civil disputes, but police are legally unable to do so. This must be done by agencies of the civil system. Courts likewise have jurisdiction over either civil or criminal cases; some courts have jurisdiction over both.

- **The case type** Courts sometimes are limited to jurisdiction over specific types of cases (for example, family courts that hear only child custody and juvenile cases).

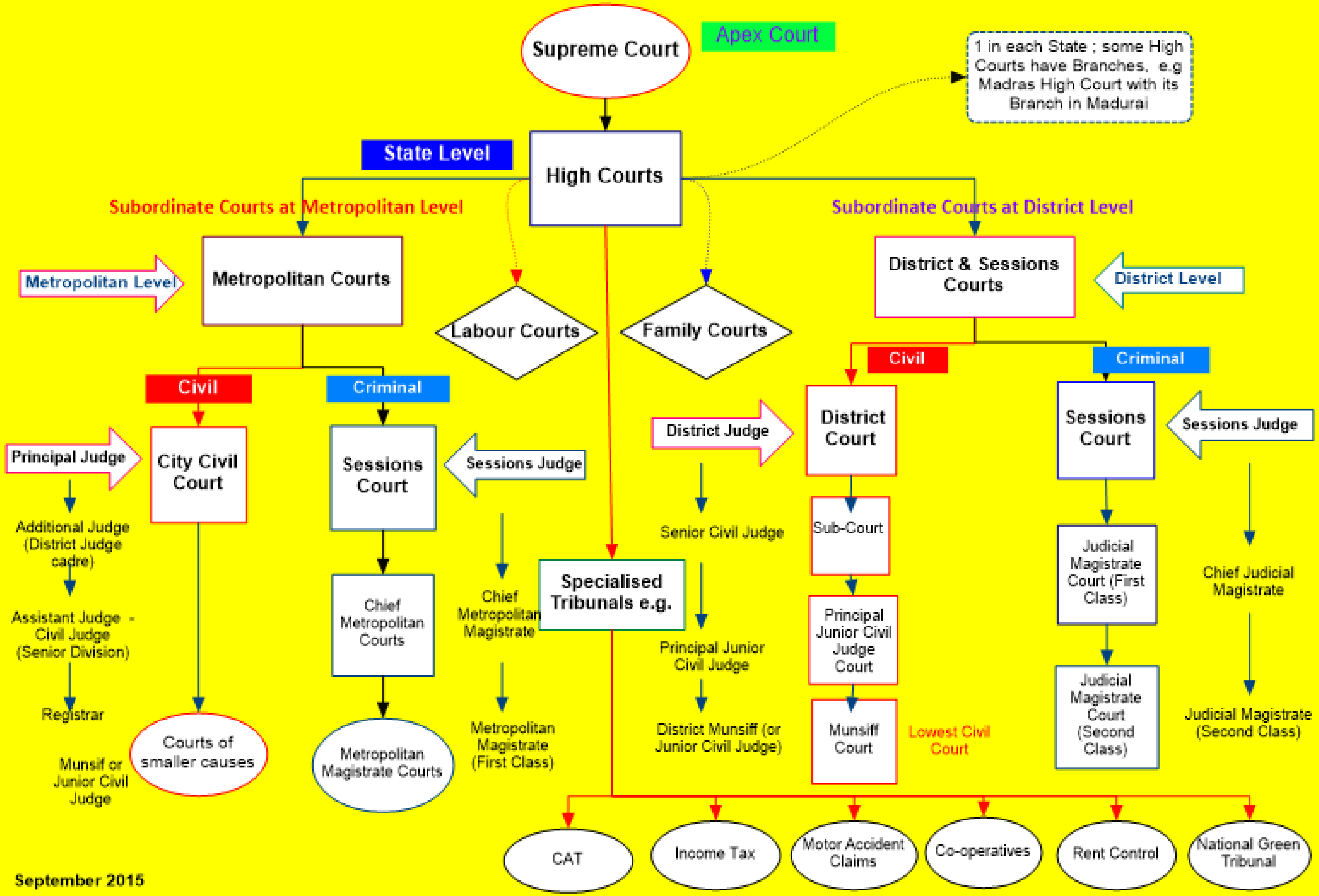
- **Offense grade** Courts often hear cases related to particular grades of offense.

- **Monetary damages** Some civil courts hear cases based on limits on the amount of monetary damages claimed.

- **Government level** Both enforcement agencies and courts are assigned jurisdiction based on level of government. Courts, too, operate at the municipal, county, state, and levels.

- **Geographic area** Geographic jurisdiction refers to the physical area over which an agency or court has jurisdiction. Municipal police officers have jurisdiction within their city limits, state police have statewide jurisdiction, and so on.

HIERARCHY OF COURTS IN INDIA - A Flow Diagram



Supreme Court

Apex Court

High Courts

State Level

1 in each State ; some High Courts have Branches, e.g Madras High Court with its Branch in Madurai

Subordinate Courts at Metropolitan Level

Metropolitan Level

Metropolitan Courts

Civil

City Civil Court

Principal Judge

Additional Judge (District Judge cadre)

Assistant Judge - Civil Judge (Senior Division)

Registrar

Munsif or Junior Civil Judge

Courts of smaller causes

Criminal

Sessions Court

Sessions Judge

Chief Metropolitan Courts

Chief Metropolitan Magistrate

Metropolitan Magistrate Courts

Metropolitan Magistrate (First Class)

Labour Courts

Family Courts

Specialised Tribunals e.g.

CAT

Income Tax

Motor Accident Claims

Co-operatives

Rent Control

National Green Tribunal

Subordinate Courts at District Level

District & Sessions Courts

District Level

Civil

District Court

District Judge

Senior Civil Judge

Principal Junior Civil Judge

District Munsiff (or Junior Civil Judge)

Sub-Court

Principal Junior Civil Judge Court

Munsiff Court

Lowest Civil Court

Criminal

Sessions Court

Sessions Judge

Chief Judicial Magistrate

Judicial Magistrate (Second Class)

Judicial Magistrate Court (First Class)

Judicial Magistrate Court (Second Class)

September 2015

Level of Jurisdiction

- Levels of jurisdiction correspond to the levels of law. Jurisdiction of enforcement agencies and courts can be local (city or county), statewide, federal, or international.
- Jurisdictional levels can overlap(*double jeopardy).* A person can be charged and tried twice for the same act if those charges are brought at different jurisdictional levels.
- Likewise, a cybercriminal could be charged with unauthorized network access under a state's computer crimes laws and also be charged at the central level for the same act if the offense involved matters that come under different levels of jurisdiction.

The Problem with Cyberspace

- Jurisdiction presents a special problem in cybercrime cases because the offenses are by definition committed in cyberspace, which is not a physical "place."
- The criminal and the victim are often miles apart, and the criminal might never set foot in the state or country where the harm occurs.
- Another complicating factor is the **cyberspace culture**.
- Many believe that the Internet should remain a "free zone" where no governmental regulation or laws apply.
- Others believe that existing laws are sufficient and can be effectively applied to the cyberspace environment.
- Still many others think of having special "cybercops" whose jurisdiction *is the Internet. This again* brings up more questions:
  - ❑ For whom would these cybercops be employed—an international entity such as the U.N.? If so, would they have jurisdiction only in member nations?
  - ❑ Would an international body have authority to pass laws regulating behavior on the Internet?
  - ❑ What would happen if or when those laws conflicted with laws in the states or nations that belong to the international body?

International Complications

- In international law, the concept of *territoriality is based on the principle that* nations should not exercise their jurisdiction outside their own territory.

- *However, nations are allowed to exercise* jurisdiction inside their territory over acts committed by their own citizens when outside their territory.

- Furthermore, they generally are permitted to exercise jurisdiction over a criminal act in which part of the act occurred within their territory (that is, the offense either originated in their territory and was completed outside or originated outside their territory but was completed inside it).

How does this concept affect cybercrime cases?

- Can a nation apply its laws to persons who reside outside its territory who, for example, operate Web sites that violate the laws of that nation?

- All these questions must be answered before cybercrime can be addressed on a global scale.

- Proposed international treaties such as *the International Convention to Combat Cyber Crime and Cyber Terrorism* always end up highlighting the fact that there is a great deal of disagreement among and within nations as to what constitutes cybercrime.

Practical Considerations

- There are a number of practical reasons law enforcement agencies and prosecutors choose not to pursue cybercrime cases that take them outside their normal jurisdictions which include :

❑ The cost of travel to investigate leads in distant cities, states, or countries.

❑ The difficulty of bringing in witnesses and records from far away for the trial.

❑ The difficulty of extraditing a suspect who is located in another jurisdiction.

❑ The political reality that citizens generally want their police agencies to address local crime first.

❑ The lack of technical understanding and expertise within the enforcement agency and prosecutor’s office.

❑ The paperwork and “red tape” that are often involved in obtaining the cooperation of agencies in other jurisdictions, especially in other countries.

❑ The language barriers that often make it difficult to communicate with agencies and witnesses in other countries.

Nature of the Evidence Complicate Prosecution

- In addition to the difficulty of defining the offense and the jurisdictional issues that complicate prosecution, another obstacle that stands in the way of building and winning a case against a cybercriminal is the nature of much of the evidence.

- The law generally recognizes three types of evidence:

  ■ **Physical evidence** Tangible items that provide proof of the commission of an offense and/or the identity of the offender.

  ■ **Direct evidence** The testimony of witnesses who saw the offense occur, observed the accused taking preparatory steps toward committing the offense, or otherwise have direct knowledge of the crime.

  ■ **Circumstantial evidence** Facts and circumstances that tend to support the theory that the accused person committed the offense but that do not offer definitive proof.

- Much of the evidence in cybercrime cases is digital; this means that it is not tangible evidence but rather which is made up of electronic or magnetic pulses that are stored in the form of electromagnetic charges on the media of a disk or tape.

- Not only is this evidence largely intangible, but it is also fragile.

- The inability to produce the original evidence tends to weaken the prosecution's case.

- Hackers with technical expertise can destroy the evidence by going through multiple servers to get to their targets and then, once they've accomplished their objective, deleting the log files on each server to cover their tracks.

- Because digital evidence is intangible, fragile, and easily destroyed (either deliberately or accidentally), proper evidence handling is even more important in cybercrime cases than in other types of crimes.

- Investigators should work only on the copies of original, preserving the integrity of the original evidence. In addition, all actions taken on related to evidence should be documented carefully.

Human Factors

- So far, the obstacles to prosecution of cybercrime cases pertain to legal or technical issues.

- However, other factors such as Human Factors make it difficult to build a cybercrime case.

- These factors pertain to the necessity that law enforcement officers and IT professionals work together to most effectively put together a prosecutable case and the difficulties that both sides often encounter in doing so.
- Law Enforcement "Attitude"
  - Nobody understands a cop except another cop.
- Lifestyle Differences: between a cop and Tech workers
- Natural-Born Adversaries?
  - At first glance, police officers and IT professionals don't mix at all. Police officers feel superior by virtue of their governmental authority, whereas tech people feel superior based on their positions in the business world.
  - Many IT professionals see nothing wrong with trading software or downloading music through file-sharing services , while the police see this as breaking the law.

But commonalities also exist between them : working long and odd hours, problem solvers by nature, both are generally dedicated to their jobs.

Overcoming Obstacles to Effective Prosecution

Many obstacles that stand in the way of effectively prosecuting cybercrime cases include

- The difficulty of defining the crime
- The jurisdictional nightmares that arise when suspect and victim are in different geographic locations
- The attitudes and lifestyle differences that make it difficult for police and IT professionals to work together

It is possible to overcome all these challenges and put together a case that will stand up in court.

- Law enforcement agencies can work with prosecutors to clarify definitions and ensure that they understand the elements that must be proven to arrest and convict in a cybercrime case.

- IT personnel who anticipate working with law enforcement on cybercrime cases must learn the basics of how the criminal justice system operates, and both must know how civil, criminal, and regulatory laws differ and which specific acts fall under which bodies of law in their jurisdiction.

- Investigators must be prepared for legal complications when cybercrimes cross state or national boundaries (jurisdiction problems).

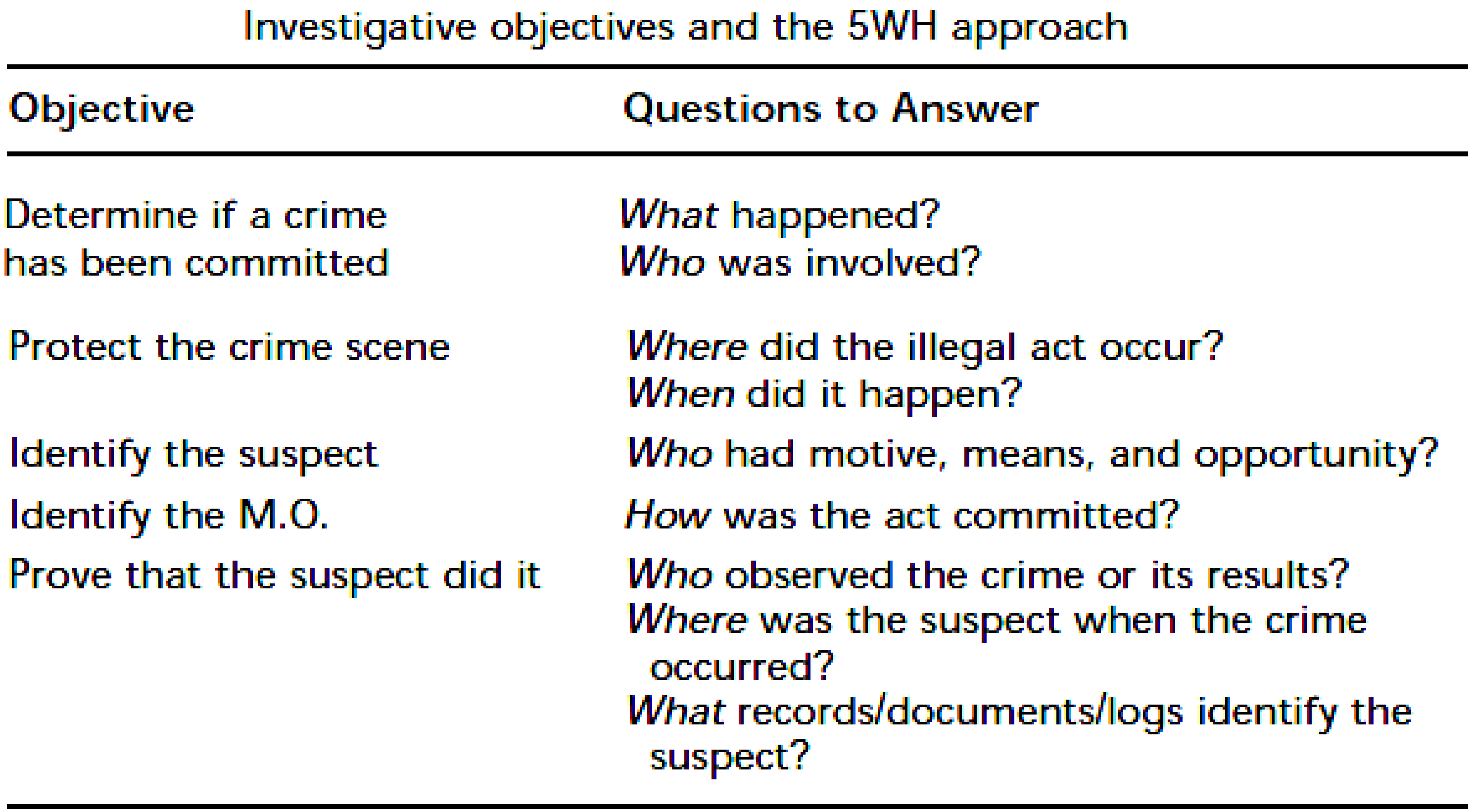
- Law enforcement officers and IT professionals can learn to work together on cybercrime cases, resulting in much more effective investigations than either could conduct alone.

- An important part of building the bridge is learning to “talk the talk.” Police officers need to learn technical terminology, and IT personnel need to become comfortable with the language of law and police jargon so the two can better understand one another.

- A successful prosecution is based on the work of many people and on many factors. An important element in building a solid case hinges on proper implementation of the investigative process.

The Investigative Process

- An investigation should be objective.
- The purpose of an investigation is not to indict a particular person but to determine the truth.
- The Investigators should put aside personal feelings and approach the investigation
- The rule of thumb for investigation is to find out *who, what, when, where, why ,and how, that are also known as the 5WH method.*
- *These are the questions that must be asked and answered before you—as a* writer or as an investigator



Investigative objectives and the 5WH approach

Objective	Questions to Answer
Determine if a crime has been committed	*What* happened? *Who* was involved?
Protect the crime scene	*Where* did the illegal act occur? *When* did it happen?
Identify the suspect	*Who* had motive, means, and opportunity?
Identify the M.O.	*How* was the act committed?
Prove that the suspect did it	*Who* observed the crime or its results? *Where* was the suspect when the crime occurred? *What* records/documents/logs identify the suspect?

Investigative Tools

- An investigator builds a case using standard investigative tools.
- The “Three I’s” form the investigator’s toolkit are:

1. Information
2. Interview and interrogation
3. Instrumentation

1. Information

- *Information, the foundation of the case, can be obtained in many different ways.*

- Here we refer to the information that an investigator can gather through observation, examination of documents or electronic data, and examination of physical evidence.

- One important means of obtaining this information is through the *crime scene search*.

- *In the case of a cybercrime,* much of the evidence might be on the computer—stored on its hard disk or even still in memory.

- However, it's important for investigators to resist tunnel vision that leads them to focus solely on the computer, because the crime scene can encompass the area around the computer as well.

- If there is evidence on the system showing that a particular computer was used to commit a cybercrime, you still must establish a link between the computer and the suspect. Then traditional crime scene techniques are appropriate, such as dusting for fingerprints and conducting a thorough area search that can turn up such evidence as printouts of computer data, notes jotted by the suspect that pertain to the offense, backup diskettes or tapes containing evidentiary information, and so forth.

- It is also important to remember that evidence can be stored off site where it has been uploaded over the Internet or physically transported on removable media.

2. Interview and Interrogation

- *Interview and interrogation refer to the questioning of persons involved in the* cybercrime.
- The difference lies in the person's role in the crime and in the manner of questioning.
- An *interview involves questioning witnesses, victims,* and other people who might have information relevant to solving the crime.
- These people could include technical experts who can explain how the crime was committed and who may also testify as expert witnesses at trial or who may merely provide background information to help the investigator understand the technicalities of the offense.
- An *interrogation involves questioning persons suspected of committing or* aiding in the commission of the offense. The interrogation is generally recorded, and it is important to document that the suspect has been advised of his or her rights before questioning.
- An interrogation is often adversarial in nature, but it doesn't have to be. One of the best ways to get useful information from a suspect is to gain his or her confidence, make the suspect think that you're sympathetic to his or her cause.
- In cybercrimes involving hacking and technical exploits, it can be useful to have an officer who is technically savvy to interrogate the suspect, because someone who "speaks the same language" might be able to draw the suspect into bragging about the technical prowess necessary to pull off the job.
- There are many different interrogation techniques, and the investigator should use those that work best for them. Some tried and true techniques, in addition to the sympathetic approach, include:

■ **Logical approach** Use reasoning to convince the suspect that it's in his or her best interest to confess.

■ **Indifference** Pretend you don't need a confession because you already have enough evidence without it. This can work well with multiple suspects when you can imply to each that the other(s) has already "spilled the beans."

■ **Facing-saving approach** Allow the suspect to provide excuses for the behavior and show understanding of why he or she committed the crime.

- For both interviews and interrogations, the same basic guidelines apply to cybercrime witnesses as well:
  - ■ Separate the persons being interviewed or interrogated. Even in the case of witnesses who are not innocent of any crime, witnesses can be influenced by one another's statements. Suspects can reveal their guilt by telling conflicting stories.
  - ■ Use *kinesic interview techniques; note body language, voice tone, facial* expression, and other nonlinguistic communication that provides clues to whether or not a person is telling the truth.
    - Use *mirroring, in which the* investigator subtly emulates the other person's body language to create a sense of rapport with the person.
    - Have a tactical plan for the interview or interrogation; be aware of all the available facts about the case and know exactly what information is going to be acquired.
  - ■ Ensure that standard procedures are followed for recording and/or obtaining written statements.
    - The obtained information should be analyzed to determine its value, correctness and admissibility.
    - This analysis can be based on the answers to the following questions:
      - ○ Does the information substantiate one or more elements of the offense (is it material?)
      - ○ Could the information negate a suspect's defense or alibi?
      - ○ Does the information confirm a suspect's confession?

3. Instrumentation

- *Instrumentation refers to the use of technology to obtain evidence. For Example:* In cybercrime cases, use of data recovery techniques/ tools to recover "deleted" and "erased" information on disks is a type of instrumentation. Other, more traditional examples include forensics techniques for collecting and analyzing trace evidence, DNA analysis, and the like.

General Steps involved in an Investigation : Moving Towards Prosecution

- Investigators should follow the same step-by-step process each time they conduct investigations and prosecute in courts.

- These steps should be documented in a procedure manual that can be part of the agency's policies and procedures. A suggested set of steps follows:

1. Analyze the complaint.
2. Collect physical evidence.
3. Seek expert advice, if necessary.
4. Interview witnesses and interrogate suspects.
5. Construct the case file.
6. Analyze the case.
7. Follow up investigations.
8. Decide whether to prosecute.

1. Analyzing the Complaint

Upon receiving a complaint or notification that a cybercrime has occurred, the investigator first must analyze the complaint to determine:

- If a crime was committed
- If so, what crime was committed

The analysis of complaint includes:

- Evaluating the plausibility of allegations that a violation of the law has occurred.
- Considering the nature and seriousness of the crime.
- Considering factors such as jurisdiction that might complicate the crime’s prosecution.
- In reality, manpower limitations and other considerations can prevent pursuing less serious cases.
- If the analysis of the complaint determines that a crime was committed and warrants a preliminary investigation, the next step is to start collecting evidence.

2. *Collecting Physical Evidence*

- *Physical evidence in this context refers to tangible items(such as the disk) that can be gathered,* marked or tagged, and stored in a secure location until trial.

- There might be other physical evidence in addition to digital information, including fingerprints, documents,devices , and so forth. These should be preserved in accordance with standard crime scene practices.

- Traditional crime scene techniques such as making crime scene sketches, photographs, and videotapes can be useful. This is especially true if, when investigators seize the computer, there is information on the screen that is not saved on disk.

- There might be information in memory and status information (network connections that are open, applications and processes that are running, and the like) that is useful as evidence but will be lost when the computer is powered down.

- Saving the contents of memory or other information or dumping the contents of memory to a file changes the system so that you've altered it and can no longer testify that it is exactly as you found it.

- One way to avoid this problem is to use photography to record the displayed information.

- Another is to transfer the data to another computer. Remember that every time you perform a task on a computer, even something as simple as saving a file, you change it in some way.

- Handle digital evidence so that no changes are made as per the standard procedures.

3. Seeking Expert Advice

- When a crime involves technical details that are beyond the knowledge of the investigator and/or prosecutor, it is often necessary as part of the investigation to seek advice and help from an expert in the field.

- Seek the services of an interpreter if all the witnesses at a crime scene spoke a language with which you weren’t familiar.

- When investigating a cybercrime in which a corporate network is the victim, why not just use the IT personnel there as your experts?
  - The expert you consult for technical advice should be objective, and it is often difficult to obtain objective opinions from people whose own networks have been victimized.

- Even if the company IT professionals *are completely objective, there could* be a perception that they are otherwise, and this perception could be exploited if defense attorneys discover that they provided you with technical guidance.

- Agencies might be able to find IT experts within the community who are willing to volunteer their expertise for a good cause.

- One good place to look is the academic world; computer science and computer security instructors at local colleges are often happy to help with technical questions in cybercrime cases.

- Associations of computer professionals might also be able to point you in the right direction.

4. *Interviewing and Interrogating*

Interviewing witnesses and interrogating suspects can be an ongoing process throughout the investigation.

- New witnesses and new Suspects might be discovered in the course of investigation.

- Follow up interviews with witnesses who have already been interviewed might be necessary as the case develops.

- Investigators should be sure to get contact information from all witnesses, even those who might not need to be interviewed at the time.

- A witnesses can also leave a company or move during the course of an investigation, making them difficult to locate if you have only one set of contact information. It is also a good idea to get witness e-mail addresses and permanent address.

5. *Construct the case file.*

- After physical evidence has been gathered and documented and interviews and interrogations have been conducted, the next step is to start putting together the physical case file. This is an important element in *case preparation.*
- *Case* is defined as *"an aggregate collection of facts which furnishes occasion* for the exercise of the jurisdiction of a court."
- *Preparation, is "the action or process of making something* ready."
- Hence, a simple definition of *case preparation can be stated as "a compilation of information made ready for court presentation."*
- The case file will contain all documentation of the case, including (but not limited to):

  - ■ Initial incident report from the officers or investigator who responded to the complaint
  - ■ Followup reports
  - ■ Documentation of evidence collection by crime scene technicians
  - ■ Documentation of proof of the elements of the offense, the legality of the entry/search/seizure/arrest, and the preservation of the chain of custody.
  - ■ Lab reports by forensics lab personnel
  - ■ Written statements of witnesses, suspects, and experts
  - ■ Crime scene sketches, photographs, and videotapes
  - ■ Printouts of digital evidence, where applicable.

- The case file is used to organize information and evidence in one place and will be used by the prosecutor in making a decision as to whether to prosecute the case and at trial.

6. Case Analysis

- When the case file has been constructed and all documentation included, the next step is to analyze the legal significance of the information and the evidence it contains.
- This step should usually be done in conjunction with the prosecutor, who might be able to provide the investigator with guidance as to the weaknesses of the case and what additional information or evidence needs to be obtained to strengthen it.
- This could be the first of several *pretrial meetings between members* of the prosecution team and the investigator(s).

7. Followup

- After the case analysis, you might need to obtain additional evidence or clarify facts and information.
- Re-interviewing witnesses at this point can serve several purposes.
- In addition to obtaining specific additional information, the second interview will help refresh their memories about the case, refresh the investigator's memory about the case, and prepare the witnesses for the courtroom process if and when the case goes to trial.

8. Decision to Prosecute

- After all additional information has been collected and the case file is considered complete, the prosecutor will make the decision to prosecute .
- At this time, the selection of the charge will also take place. In some cases, several different offenses could be charged. The prosecutor will select based on the provability of the elements and difficulty of obtaining a conviction as well as the severity of the punishment.

For example, a suspect's actions might contain the elements of two different offenses—for example, unauthorized access and theft of trade secrets.

- If the first charge is a misdemeanor and second as felony, the prosecutor may choose to charge only the more serious offense.

Defining Areas of Responsibility

- Rarely will a complex investigation be conducted by one person.

- The investigative team might consist of one or more persons namely :
  - Detectives,
  - Crime scene technicians,
  - Crime scene photographers and videographers,
  - Evidence recorders and custodians,
  - Specialists such as computer forensics team.

- It is important that there be one person who is designated to be in charge of the investigation.

- This is the team leader and is often a senior investigator.

- The team leader should assign each team member a specific *area of responsibility.*

- *Team* members should be accountable for their designated areas of responsibility (for example, collecting, tagging, documenting, and securing the physical evidence) and should not overstep their bounds and perform tasks that fall under other members' areas of responsibility, unless approved by the team leader.

Thank you