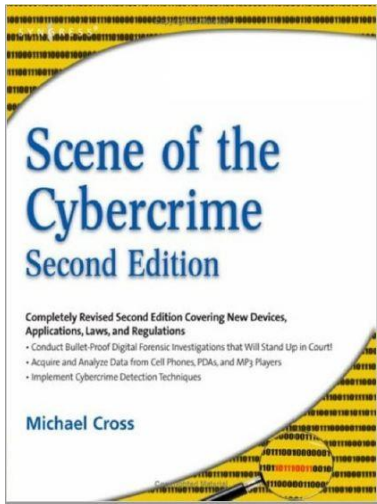
Chapter – 2

"Understanding the people on the Scene"

In this chapter, we take a look-at all these people on the scene of the cybercrime.



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

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.

Self-Learning Contents:

Objectives

- We take a look up close and personal—at all these people on the scene of the cybercrime.
- Examine the roles
  - Cybercriminals
  - Cyber victims
  - how they interact

Outline

- 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

Understanding Cybercriminals

- A cybercrime always involves at least one human being who originates, plans, prepares, and initiates the criminal act.
- A number of scientific disciplines are devoted to gaining a better understanding of criminals and criminal behavior.
- *Criminal psychology is the study of the criminal* mind and what leads(motivates) a person to engage in illegal or socially deviant behavior.
- Criminal psychologists often focus on studying the cases of criminals to detect *patterns*, analyze *behaviors*, and make *predictions* and *profiles* based on their analyses.
- Investigative psychology is a psychological specialty that involves applying knowledge of psychological principles to police work and criminal investigation.
- To catch criminals, it is important for Law Enforcement Officer or IT professional involved in investigating cybercrimes to "understand" the cybercriminal's mindset and his/her motivations.

Profiling Cybercriminals

- Profiling is one tool for conducting an initial investigation and building a criminal case.
- *Criminal profiling is the art and science of developing a description of a criminal's* characteristics (physical, intellectual, and emotional) based on information collected at the scene(s) of the crime(s).
- A *criminal profile is a psychological assessment* made before the fact i.e. without knowing the identity of the criminal.
- It consists of a set of defined characteristics that are likely to be shared by criminals who commit a particular type of crime.
- A profile will provide only an idea of the general *type of person who committed a crime and will not point to a specific person as the suspect.*
- A profile is *not evidence; rather, it is a starting point that* can help investigators focus on the right suspect(s) and begin to gather evidence.
- Good profiles can be highly accurate as to the offender's occupation, educational background, childhood experiences, marital status, and even general physical appearance.

How Profiling Works

Profilers draw inferences about the criminal's personality and other characteristics based on the following indicators:

- Their observations of the crime and crime scene.
- The testimony of witnesses and victims.
- Their knowledge of human psychology and criminal psychology.
- The existence of patterns and correlations between different crimes.
- Comparing the facts and impressions from a group of crimes and determining whether it is likely that the crimes were committed by the same person/group?
- Repeat criminals? They continue to commit crimes. They tend to do things in the same way maximum time; this is known in popular parlance as the criminal's modus operandi (method of operation).

Types of Profiling

Inductive Profiling

- *relies* on statistics and comparative analysis to create a profile.
- Information is collected about criminals who have committed a specific type of crime.
- Information can take the form:

1. Formal studies of convicted criminals.
2. Informal observation of known criminals, clinical or other interviews with criminals known to have committed certain/ similar crimes.
3. Data already available in databases.

Deductive Profiling

- *relies* on the application of deductive reasoning to the observable evidence.
- The deductive method involves several distinct steps:
  1. A problem is stated.
  2. Information is collected.
  3. A working hypothesis is formulated.
  4. The hypothesis is tested.
  5. Results of the test are examined.
  6. One or more conclusions are reached.
- Success depends upon the ability of the profiler to "get inside the mind" of the criminal.

Using logs: System logs, Application logs, Network logs .

- Log files are seen as electronic fingerprints and when properly managed, can be used as evidence for prosecution.

Example:

- If an attack on the network is detected by an installed software and lasts longer than a few minutes without interruption, a computer forensic examiner can enable traffic regulating systems such as a separate router or a gateway. These systems can be used to log the network traffic needed to perform the analysis afterwards. The network protocol itself can also offer evidence regarding a cybercriminal's M.O.

Cybertrail: A cybertrail is considered a virtual version of a signature left at a crime scene. A computer forensic examiner approaches the computer and analyze any clues left behind by the cybercriminal.

- Through the signatures, social media posts, and Internet cache, the following can be detected in the cybercriminal's writing:
  - nicknames, pattern of typing mistakes, particular phrases, and writing style.
- These traits can be looked into when a criminal profiler develops the potential education level in a cybercriminal profile.

Cybertrail Example

Similar to a signature left by a criminal at a crime scene, cybercriminals can also leave their mark when committing a cybercrime. The most notable example was the leaked DNC e-mails in 2016. Criminal profilers were able to create a profile with the help of computer forensic analysis. Profilers were able to conclude that they were looking for a person or group of Russian descent based off a few results. First, cybersecurity experts were able to find a signature left by the hacker in Russia's Cyrillic alphabet (Meyer, 2016). Second, through the remaining forensic evidence, DNC's cybersecurity firm concluded that their investigation should focus on Russian intelligence groups due to the firm's familiarity with Russian attacks. Both Russian proxy groups, Advanced Persistent Threat (APT) 28 and APT 29, have infiltrated U.S. government departments before and the forensic evidence collected has their similarities in each case (Meyer, 2016).

https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak

- Example Cybertrails: popular case of DNC email LEAKS in US Presidential Elections 2016 indicating Russian involvement – hacking group "Guccifer 2.0" .

- Some of the malware found on DNC computers is believed to be the same as that used by two hacking groups believed to be Russian intelligence units, codenamed APT (Advanced Persistent Threat) 28/Fancy Bear and APT 29/Cozy Bear by industry researchers who track them. Malware found on the DNC computers was programmed to communicate with an IP address associated with APT 28/Fancy Bear.

- The attackers registered a deliberately misspelled domain name used for email phishing attacks against DNC employees, connected to an IP address associated with APT 28/Fancy Bear.

- Some of the phishing emails were sent using Yandex, a Moscow-based webmail provider.

- Metadata in a file leaked by "Guccifer 2.0" shows it was modified by a user called, in cyrillic, "Felix Edmundovich," a reference to the founder of a Soviet-era secret police force. Another document contained cyrillic metadata indicating it had been edited on a document with Russian language settings.

- Peculiarities in a conversation with "Guccifer 2.0" that Motherboard magazine published in June suggests he is not Romanian, as he originally claimed.

Profiling Examples

This was the case with the B.T.K. killer in 2004.

Dennis Rader was found guilty of murdering ten people over the course of 30 years. Although he is not categorized as a cybercriminal, Rader was infamously known for using technology to stay in contact with officials through taunting poems, puzzles, clues, and documents (Precision Computer Investigations, 2010). Throughout the 30 years of unsolved cases, criminal profilers predicted that they were looking for a middle-aged man with a low level of education due to his writing quality in the materials he sent to law enforcement. The breakthrough was when the police received a floppy disk from Rader that included a Microsoft Word document with the grammatical errors and phrases that matched prior documents. Computer forensic examiners analyzed the disk and noticed there was a deleted document that listed the name Dennis as the creator and the location of where the document was last modified (Precision Computer Investigations, 2010).

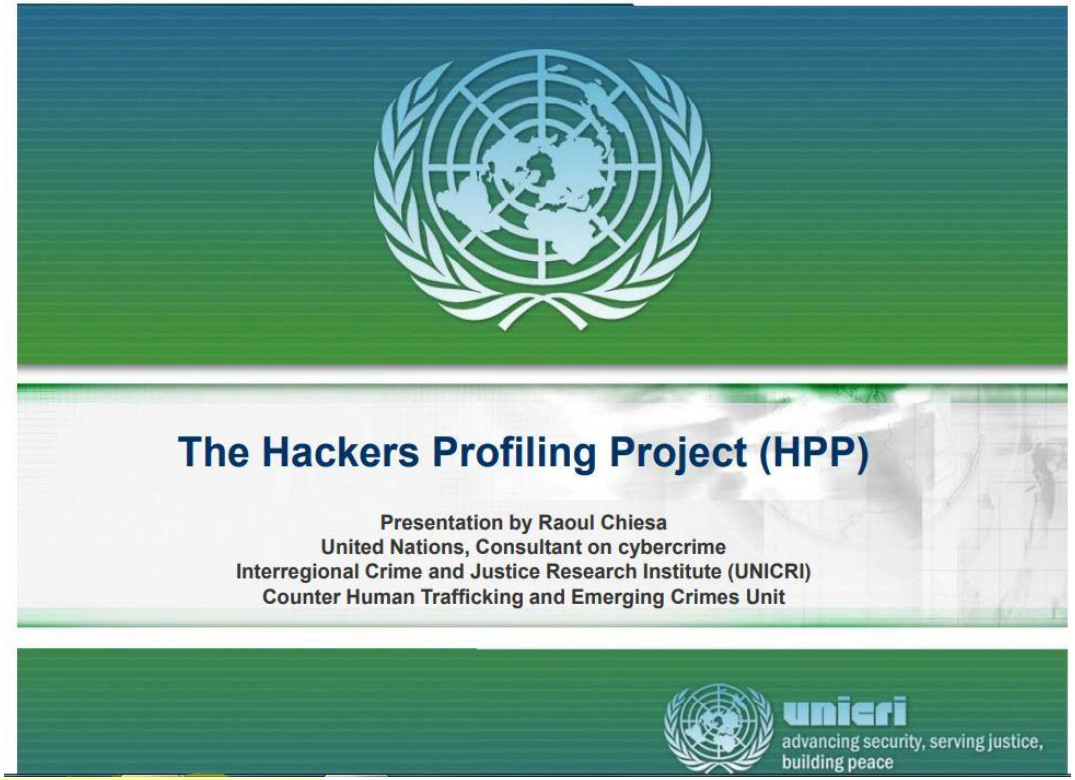
Example

Along with investigators, companies can benefit from increased research regarding profiling an intellectual property (IP) thief, for example. Studies have shown that the majority of IP criminals are males who hold a technical position and 75% of them had authorized access to the information they stole (Bada & Nurse, 2016). With continued research, the criminal profile of said IP thief can continue to develop and help companies and investigators alike in both prevention and offensive circumstances.

Source: Bada, M., & Nurse, J. (2016, April 18). Profiling the cybercriminal. *Global Cyber Security Capacity Centre. Retrieved from https://www.sbs.ox.ac.uk/cybersecuritycapacity/*content/profiling-cybercriminal

Example

Images and file metadata have played a key role in profiling cybercriminals who partake in the possession or distribution of Sexually Exploitative Imagery of Children (SEIC). When offenders' hardware is confiscated for analysis, criminal profilers can extract behavior traits from the images that are extracted and its metadata. In 2015, there was a notable study of 15 cases involving SEIC that studied the analysis of computer forensics and applied it towards behavioral evidence analysis (Mutawa, Bryce, Franqueira, & Marrington, 2015). From the study, researchers concluded that the majority of the cybercriminals were employed and had no prior arrests (Mutawa et al., 2015). There were several learned characteristics about the way the cybercriminals stored the images of children once computer forensic examiners located the evidence on their computers. 93% of the cybercriminals hid their possession of SEIC through "basic methods" such as deleting the files into their recycling bin and deleting any peer-to-peer networking software (Mutawa et al., 2015). This could imply that the cybercriminals did not have the technical skill set to hide their files or they were confident enough that they would not be caught (Mutawa et al., 2015).



- The Hacking Profiling Project (2004) is one of the prominent studies that involves cybercrime criminal profiling. This project provided information regarding twenty hackers that the five researchers studied such as their:
  - Demographics (age and gender),
  - Socioeconomic upbringing,
  - Psychological traits,
  - Trends and habits regarding their hacking activity, and their favourite *modus operandi*
  - Social relationships.
- The profiling framework established during this study is seen as an important step towards developing databases of criminal profiling cybercriminals to help reduce the margin of error when creating future profiles.

- Another popular profiling guideline is the *Behavioral Evidence Analysis (BEA) framework.*
- The discovery and **examination of behavioral clues of the offender and the victim** from digital evidence is known as *Behavioral Evidence Analysis (BEA)*
- Categorized as a deductive, case based strategy, used in crimes such as *Cyberbullying, Cyberstalking, email spamming*.

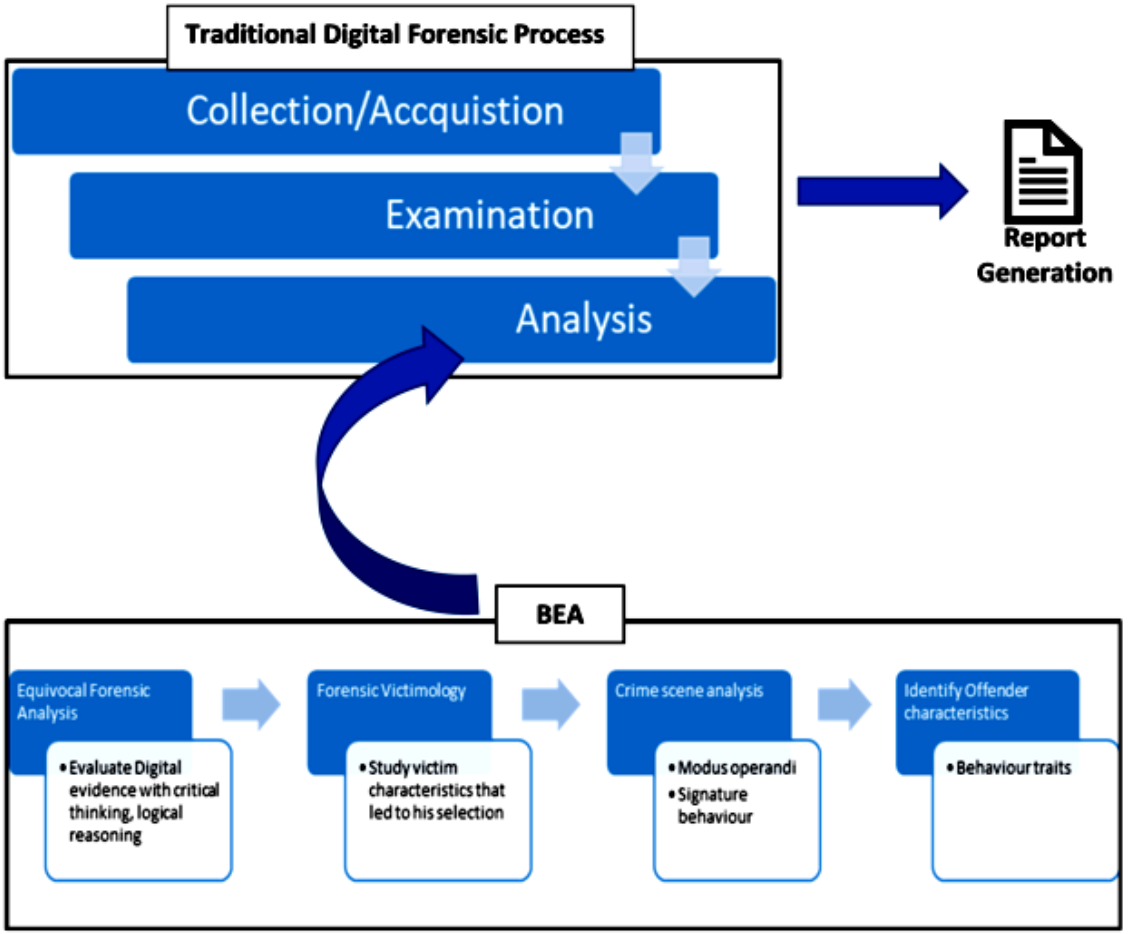
This framework consists of 4 stages:

1. Equivocal forensic analysis: *focuses on reviewing the case with a scientific standpoint and objectively develop theories of the crime.*

2. Victimology: *assesses the traits of the victims such as their physical, lifestyle, age, and occupation.*

3. Assessment of the crime scene: *that can help provide answers about the victim(s) and create connections to the criminal's decisions / actions / modus of operandi / signature.*

4.Criminal's characteristics: *uses information from the crime scene to determine both behavioral and personality characteristics and build an outline for his/her criminal profile.*



Myths and Misconceptions About Cybercriminals

- All cybercriminals are “nerds”—bright but socially inept.
- All cybercriminals have very high IQs and a great deal of technical knowledge.
- All cybercriminals are male, usually teenage boys.
- All teenage boys with computers are dangerous cybercriminals.
- Cybercriminals aren’t “real” criminals because they don’t operate in the “real world.”
- Cybercriminals are never violent.
- All cybercriminals neatly fit one profile.

Categorizing Cybercriminals

Cybercriminals can be categorized:

1. Based on their *motivations for committing crimes.*
2. *Internet –using offenders* i.e. by the role that the internet plays in their criminal activity. This role generally breaks down into two broad categories:
   A) Criminals who use the *Net as a tool of the crime*
   B) Criminals who use the *Net incidentally to the crime*

A. Criminals who use the Net as a tool of the crime

A network can be used as a crime tool by different types of cybercriminals.

A network is used as a tool by:

1. White-collar criminals
2. Computer con artists
3. Hackers/Crackers/Network attackers.

1. White-collar criminals : derived from the image of the office worker or professional.

White-collar cybercrimes can include many different offenses such as :

- Changing company computer records to provide the criminal with an unauthorized pay raise or to eliminate or change bad employee evaluations or pad expense accounts.
- Accessing and using insider information for purchasing stocks or securities.
- Selling company information to outsiders; using insider information to obtain kickbacks from clients, business partners, or competitors; or using confidential information for blackmail purposes.
- Manipulating electronic accounts to appropriate the company's or clients' money or property for oneself.
- "Cooking" the company books or financial statements to provide false information to creditors, investors, the Internal Revenue Service, internal auditors, and so on — often to cover other crimes .

White-collar offenders fall under several sub categories:

1. The *resentful white-collar criminal* cheats the company because he or she feels cheated by the company.
2. The *deliberate white-collar criminal* has no personal ethics that would prohibit stealing
3. The *desperate white-collar criminal* steals in response to serious personal financial problems such as medical or legal crisis in the family.

White-collar criminals often give themselves away by leaving clues that arouse investigators' suspicions, such as:

- Unexplained income, property, or lifestyle that is far greater than the person's job makes feasible.
- Many large cash transactions.
- Multiple bank accounts in different banks, especially banks in different cities or countries.
- Multiple businesses listed at the same address.
- "Paper" corporations that have no physical assets and seem to make no product and provide no services.

2. Computer Con Artists : use the Internet as a tool, to reach "marks" (their terminology for victims) that they could never reach otherwise. E-mail, Websites and chat rooms can all become tools for scammers to propagate their fraudulent schemes.

Frequently reported Cons include:

- **Internet auctions** Bidders send their money but do not receive the promised product, or they receive property that is not what it was represented to be.
- **Internet Service Scams** Customers prepay for access services and then companies fold and disappear, or customers are enticed into paying for services they don't want (for example, by official-looking notices that imply that you will lose your domain name registration if you don't send money).
- **Credit card fraud** This type of fraud involves individuals and shady companies that pretend to (or actually do) sell a service or product via credit card, for the purpose of collecting the victim's credit card information and using it to make fraudulent purchases. Transferring the information from a card to another counterfeit card is a practice called *skimming.*
- **Web "cramming"** This crime involves offers for free services such as Web hosting for a trial period with no obligation, after which users are charged on their phone bills or credit cards, even though they never agreed to continue the service after the trial period.
- **"Computer Tech Support Scam"** A crook calls you on the phone, poses as a technician from a big company like Microsoft, and claims he's detected a virus on your computer. then asking for access to your computer in order to "help" you.
- **"Fraudulent Refund"** Scammers contact victims stating that they are owed a refund for prior services. The scammers generally convince victims to provide them with access to their computers to process an online wire transfer. Instead of refunding the money, however, the fraudsters use the victims' account information to charge consumers.
-

- **Multilevel marketing (MLM) and pyramid schemes Con artists** play on users' greed and desire to get rich quickly by signing recruits—for a hefty fee—and promising them huge profits if they recruit others.
- **Travel and vacation scams** Travel "bargains" and "free" vacation scams (that include all manner of hidden costs). These include selling frequent-flyer miles that are on the verge of expiration, selling travel vouchers in conjunction with pyramid schemes, bait-and-switch offers, and other too-good-to-be-true travel deals.
- **Business and investment "opportunities"** These range from work at - home scams that require you to purchase an expensive starter kit and don't provide actual jobs to day-trading programs and solicitations for investment in worthless real estate.
- **Scams involving health-care products and services** These include weight loss, antiaging, and alternative health products that are marketed under false or unproven claims; online prescription drug sales that don't require the patient to be seen by a physician; multilevel marketing of health products; and other con games that seek to take advantage of people who are ill or frightened about their health.

3. Hackers/ Crackers/Network Attackers :

- The hacker culture also divides itself into two groups:

1. **Black hats** break into systems illegally, for personal gain, notoriety, or other less-than-legitimate purposes.

2. **White hats** write and test open-source software, work for corporations to help them beef up their security, work for the government to help catch and prosecute black-hat hackers, and otherwise use their hacking skills for noble and legal purposes.

- A hacker who identifies him- or herself as a white-hat hacker might succumb to the temptation to engage in an illegal act, and a self-professed black hat can reform and become one of the “good guys.”

The following are some hackers and crackers that made newspaper headlines:

- **John Draper**, known as "Cap'n Crunch", discovered that the toy whistle from some cereal boxes produces a 2600 Hz tone that authorizes a free telephone call. He was arrested for illegal use of the telephone company's system in May 1972.

- **Robert Morris**, known as "RTM", accidentally released the **first Internet worm** in 1988 that infected thousands of computers worldwide. He was the first person convicted under the Federal Computer Fraud and Abuse Act of 1986.

- **Kevin Mitnick**, known as "Condor", was arrested in 1995 for **hacking and downloading 20,000 credit card numbers**. Mitnick became the first hacker to be on the FBI's Most Wanted List. He gained notoriety by cracking into the security system at the San Diego Supercomputer Center, ironically, by hacking information from the network security chief's, Tsutomu Shimomura, computer.

- **Kevin Polsen**, known as "Dark Dante", was arrested in 1990 for **hacking into the phone system** of a radio station so that he could be the 102nd caller in a contest to win a Porsche. He also hacked into the FBI's computer to obtain undercover business names and was featured on NBC's Unsolved Mysteries.

- **Vladimir Levin** was the first to **rob a bank through the institution's own network**, from a laptop in London, England. The Russian hacker group hacked into the Citibank system, obtained accounts, and passwords, and transferred $10 million to various accounts in United States, Finland, the Netherlands, Germany, and Israel.

- **Ian Murphy**, known as "Captain Zap", hacked into the AT&T system and changed the internal clocks, which **changed the phone rates** for day and night time users.

- https://techcrunch.com/2022/12/30/meet-the-cybercriminals-2022/

Cybercrime Indian case studies

Refer document : Cyber crime case studies in india.pdf

- **CBI arrests Russian 'hacker' in 2021 JEE-Main tampering case**

- **Mikhail Shargin**, a Russian, helped the other accused persons in hacking into the software platform on which the examination was held. He was intercepted by the immigration officials at the airport on the strength of a look-out circular opened against him.
  - "During investigation, it came to light that some foreign nationals were involved in compromising many online examinations, including the JEE (Mains)...the role of one Russian national was revealed, who had allegedly tampered with the iLeon software — the platform on which the JEE(Main)-2021 examination was conducted," said a CBI official.

- **Delhi: Man arrested for duping firms by hacking emails of executives,2020**

- **A 34-year-old Tejas Yashwant Parmar**, member of a gang of fraudsters, which used to allegedly hack into email accounts of senior executives of multinational companies and use their IDs to ask the firm's accountant to transfer money into his own bank account.

B. Criminals who use the Net Incidentially to the crime

- Net is not an actual tool of the crime but can be used to prepare for or keep records of that criminal activity.

- Even in cases in which the network is not a tool of the crime, it can still provide evidence of criminal intent and clues that help investigators track down the criminals.

Examples of this type include:

1. Criminals who use the Net to find victims.
2. Criminals who use computers or networks for record keeping, planning a crime.
3. Criminals who use e-mail or chat services to correspond with accomplices.

Real-Life Noncriminals Who Commit Crimes Online

- In some situations, people who are not criminals in real life but get involved in criminal conduct online.
- They commit illegal acts online because of their ignorance of the law or lack of familiarity with the technology.
- These include *Accidental cybercriminals* and *Situational cybercriminals.*
- **Accidental Cybercriminals:** They do not realize they are committing a crime. Example: A person using the broadband Internet access available in some hotels and opens up the Network Neighborhood folder on his computer (the network browse list) and sees other computers listed there and look into private data on other computers.
- **"Forwarding rumours, defamatory messages can come under the purview of law"**
- **Situational Cybercriminals:** In real life they are law abiding, but when online, they indulge in illicit activity. They lead double lives.

Understanding Cybervictims

- **Crime Victim** is the person/organization *to whom the crime happens, the one who is harmed by a criminal's illegal act.*
- *Crime victim is also the* **key witness** against the offender.
- ***Victimology*** *involves collecting data about, and in effect* ***profiling*** **the victims** of crime.
- **Cyber victimology** is a new sub-discipline of victimology that focuses on the study of victims of cyber crimes.

Victim profiling information is useful for law enforcement officers :

1. To predict what people or personality types are more likely to become victims of certain crimes and warn them. This in turn gives the potential victims the opportunity to take steps to protect themselves.
2. To better profile the criminal, because **patterns in victim choice** are an important part of the criminal profile.
3. To use the victim profile to bait criminals i.e. to draw them out into the open.
4. To understand the methods criminals likely employ to victimize people.

- Just as an individual person has victimology-based characteristics, so do organizations.
- The key task is to understand the victimological profile of both the organization and the organization's leadership.
- An organization's
  - Business interests
  - Political action campaigns
  - Vigilance level
  - Protection abilities
  - Cyber risk tolerance

  are just some of the characteristics that can determine if an organization is more likely to be attacked, by who, how, and why.

  For Example: For instance, pharmaceutical companies that test their products on animals are targeted by animal rights groups in various ways, including denial of service attacks against their Web and e-mail servers to disrupt their daily operations.
- Organizations have leadership and each member of that leadership team is a human being with traits of victimology.

  For Example: A CEO at an high profile organization whose business or political action campaigns do not resonate well with certain hacking groups can personally be targeted for both cyber-based attacks as well as physical attacks.
  - This can provide cyber security administrators actionable information about how to best protect their organization and its executive leadership from attacks.

Categorizing Victims of Cybercrime

Common cyber victim characteristics include:

1. People who are **new to the Net.**
   - Unaware of common security practices.
     -- Might not realize that their systems can be infected with viruses simply by opening an e-mail attachment.
   - They could believe that because they are honest in their online communications (chats), everyone else is, too.

2. People (certain groups such as youngsters and elderly) who are **naturally naïve**.
   - **Youngsters** are naturally curious and eager to explore, which can be a dangerous when they are at unethical online places.
   - Many **elderly people** feel uncomfortable with new technology because they didn't grow up with it. Also, they might enjoy helping people, a trait that scammers can exploit.

3. People who are mentally or physically **disabled or disadvantaged.**
   - Cybercriminals who—with the goal of identifying potential victims—search online databases and join mailing lists that are intended as support groups for people with disabilities.

4. "Desperados" who are greedy, lonely, or have other emotional needs.
   - Excellent targets for cybercriminals.
   - Their desperation makes-them vulnerable by causing them be at unethical online places.

5. Pseudo-victims who report being victimized but actually are not i.e. *sometimes a victim is not just a victim.* There are array of motivations of these *pseudo-victims:*
   - People who take revenge or express their anger at another person by falsely accusing that person of a crime.
   - People who want attention; pretending to be a crime victim makes them feel "special".
   - People who claim to be crime victims to cover up the fact that they themselves committed the crime.
   - People who pretend to be victims in order to claim money from victim relief funds, charitable organizations, or insurance companies.

6. People who are simply unlucky: enough to be in the wrong place at the wrong time
   - Criminals sometimes choose their victims at random —first come, first served.

Making the Victim Part of the Crime-Fighting Team

- Victims should be "empowered" through education and access to resources.
- Many agencies now appoint crime victims' liaisons, professionals who are trained to offer counseling and guidance to victims.
- To "protect" the victims from hostile personals, Victims' rights have been granted by state laws such as:
  - ❑ The right to be notified when the offender will come to trial
  - ❑ The right to be present at the trial, either personally or through representation of an attorney
  - ❑ The right to be informed of the disposition of the case.
  - ❑ If the suspect is convicted, the right to be informed and to give input when the suspect comes up for parole.
  - ❑ The right to be informed if and when the suspect is released from prison.
  - ❑ The right to be treated with dignity by the criminal justice system.
  - ❑ The right to be informed of victim social services and financial assistance that are available.
  - ❑ The right to be compensated for their loss, when possible.

Understanding Cyber Investigators

A good cyber investigator must possess the following qualities:

- **Excellent observation skills** An investigator must notice things, including the "little things."
- **Good memory** In order to put together the many clues that pop up over the course of an investigation, a investigator must be able to remember facts, names, places, and dates.
- **Organization skills** A good investigator not only remembers information but is able to organize it in a logical way so that patterns and correlations become apparent.
- **Documentation skills** A good investigator doesn't keep all this information in his head; instead, he is able and willing to meticulously put it into writing so that it can be shared with others and used as a foundation for building the case.
- **Objectivity** The investigator must not allow personal prejudices, relationships, or feelings to affect his or her ability to evaluate the evidence objectively.
- **Knowledge** An effective investigator knows the criminal laws, the rules of evidence, victimology, criminal psychology, and investigative concepts and procedures and knows about scientific aids, lab services, and resources inside and outside the agency.
- **Ability to think like a criminal** The best investigators have a "native" awareness of criminal mental processes and can put themselves in the place of an offender and predict the offender's actions.
- **Intellectually controlled constructive imagination** The investigator must be creative enough to consider all possibilities, to examine facts and then extrapolate conclusions.

- **Curiosity** The best investigators are innately curious. They aren't satisfied with simply clearing the case. It's not enough for them to determine that the suspect committed the crime; they want to know why and exactly how the crime was committed.

- **Stamina** Investigation is hard work, often involving long hours of acquisition and examination of evidence. A good investigator must be physically up to the challenge.

- **Patience** Investigation is often a drawn-out process. Progress is frequently made one tiny step at a time. Leads often lead to nowhere, and the investigator must back up and start over from scratch. Also prime suspects turn out to have alibis.

- **Love for learning :** Learning is really what investigation is all about— learning the facts of a case, learning about the people involved, learning new concepts and methods of examination: sometimes even becoming an "instant expert" in another field, such as computer hardware and networking, in order to understand the technical aspects of the crime.

Categorizing Cyber investigators by Skill Set

Cyber investigators can be categorized according to their potential or skill set:

1. **Investigators who specialize in criminal cases** They are usually law enforcement officers or corporate security personnel. They are investigators first, with a secondary interest in technology.

2. **Computer specialists who conduct investigations** They often work as consultants to law enforcement agencies. They are IT professionals first, with a secondary interest in law enforcement/investigation.

3. **Those who are equally skilled, trained, or interested in investigation and IT** They are involved in computer/cybercrime from the beginnings of their careers; they may have parallel training in both fields, such as a double degree in criminal justice and network engineering or programming. They may work for law enforcement agencies or as independent consultants.

4. **Those who have no real skills or interest in either investigation or IT** These could be police officers who were “transferred” to the detective division and drew into a cybercrime case. They aren’t really interested in investigative work and they have no training in or love of computers and networking.

Some additional characteristics:

An investigator who specializes in cybercrime also needs a few additional characteristics:

- **A basic understanding of computer science** The more the investigator knows about how computers work (including both hardware and software), booting process etc...

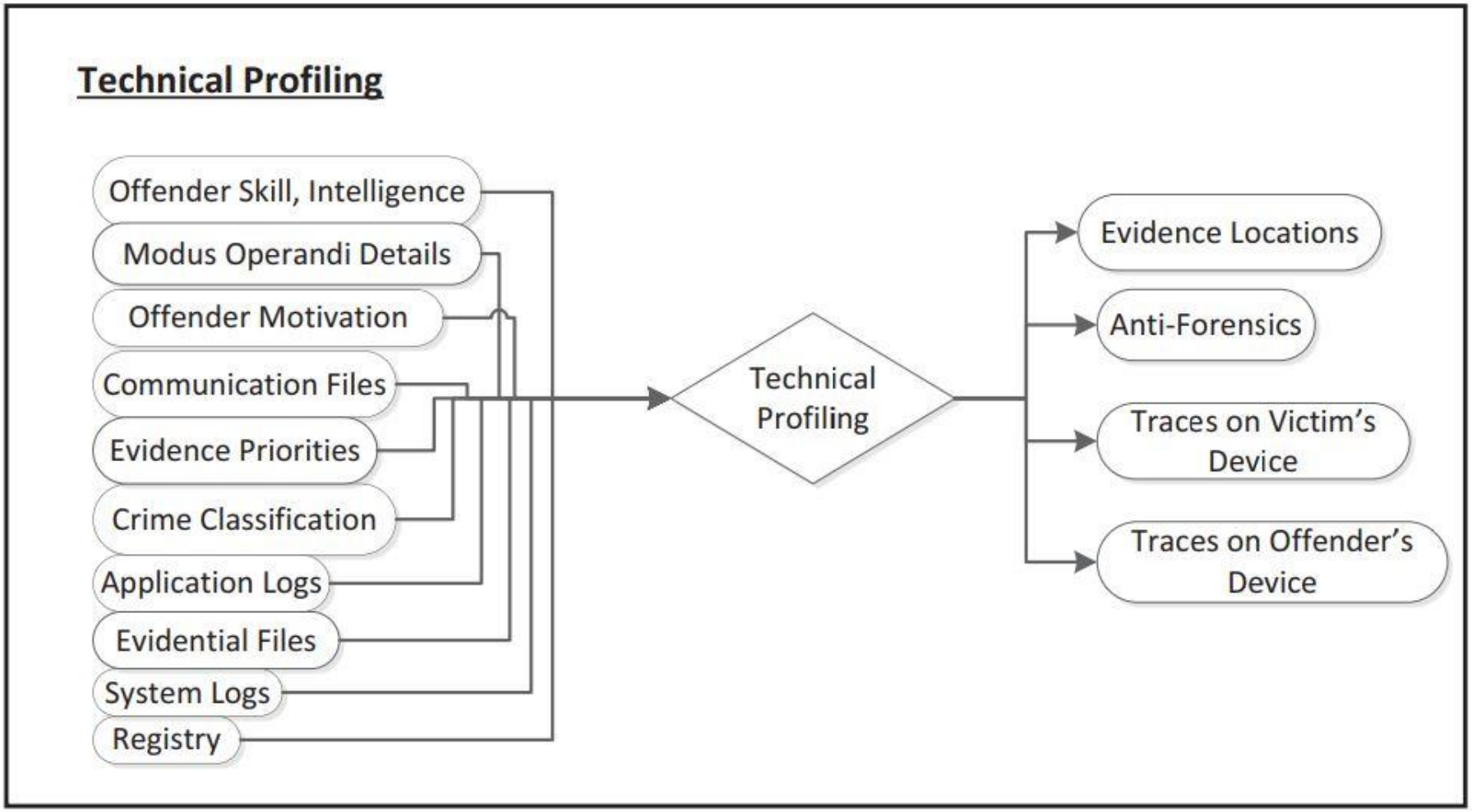
- **An understanding of computer networking protocols** Cybercrime, by definition, involves a network. Even if the investigator has a good grasp of computer technology in a standalone context, it doesn't mean he or she will understand how network intrusions and attacks work, what happens to e-mail when it leaves the sender's system, or how a Web browser requests and downloads pages, graphics, or scripts.

- **Knowledge networking security issues** In order to investigate hacking or intrusion and network-attack crimes, the investigator should be familiar with common security "holes," security products (such as firewalls), and security policies and practices.

- **Knowledge of computer jargon** All vocations and most avocations have a unique *jargon, terminology that has little meaning outside the* field that members use as "shorthand" to communicate with one another. A good investigator must be able to "speak the technological language "

- **An understanding of hacker culture** It's been said that it takes a hacker to catch a hacker (usually by reformed hackers selling their services as security experts). It's much easier to track own hackers if you understand their mentality and the protocols of interacting in the hacker community/culture.

Thank you



Source: A Digital Forensics Profiling Methodology for the Cyberstalker
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7057130