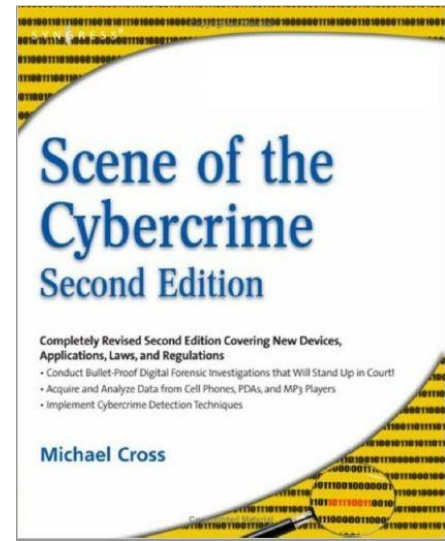


Chapter – 1

Introduction to Cybercrime

Reference:

L. D. Shinder and Michael Cross, **Scene of the Cybercrime**, Syngress.



Outline

- 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 and Developing Categories of Cybercrimes
- Prioritizing Cybercrime Enforcement
- Reasons for Cybercrimes.

Defining Cybercrime

- The word *Cybercrime* *doesn't appear in most dictionaries.*
- Each organization and the authors of each piece of legislation have their own ideas of what cybercrime is.
- Generally, **Cybercrime** can be defined as **a subcategory of computer crime** and the term refers to *criminal offenses committed using the Internet or another computer network as a component of the crime*. These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams, and expanded upon in other malicious acts.
- **Computers and Networks** can be involved in crimes in several different ways:
 - ❑ The computer or network can be the **tool of the crime** (used to commit the crime)
 - ❑ The computer or network can be the **target of the crime** (the “victim”)
 - ❑ The computer or network can be **used for incidental purposes related to the crime**

- To be enforceable, laws must be specific and definitions should be as narrow as possible to avoid confusion and vagueness. For Example:

The U.S. Department of Justice (DoJ) has been criticized for a definition of *computer crime* that specifies “any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution” (reported in the August 2002 *FBI Law Enforcement Bulletin*).

Under such a definition, *virtually any crime* could be classified as a *computer crime*, simply because a detective searched a computer database as part of conducting an investigation.

For example,

- the definition of the term *service provider* is so vague that it could be applied to someone who sets up a two-computer home network.
- Similarly, the definition of term *computer data*, because it refers to any representation of facts, information, or concepts in any form suitable for processing in a computer system, would comprise almost every possible form of communication, including handwritten documents and the spoken word (which can be processed by handwriting and speech recognition software).
- It is useful to provide a general definition, but generally criminal offenses consist of specific acts or omissions, together with a specified culpable mental state.
- It is difficult for IT personnel, users and victims, police officers, detectives, prosecutors, and judges to discuss the offense intelligently.

Working Definition of Cybercrime

- **International organization** (United Nations Congress on the Prevention of Crime and Treatment of Offenders) provide **two categories** of cybercrime and thus a standard definition of the crime :
- (A) **Cybercrime in a narrow sense (*computer crime*)**: Any illegal behavior directed by means of electronic operations that **targets the security of computer systems and the data processed by them.**
- (B) **Cybercrime in a broader sense (*computer-related crime*)**: Any illegal behavior committed by means of, or in relation to, a computer system or network, including **such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.**
- More concrete **examples** of cybercrime include:
 - Unauthorized access and computer espionage
 - Damage to computer data or programs
 - Computer sabotage
 - Unauthorized interception of communications

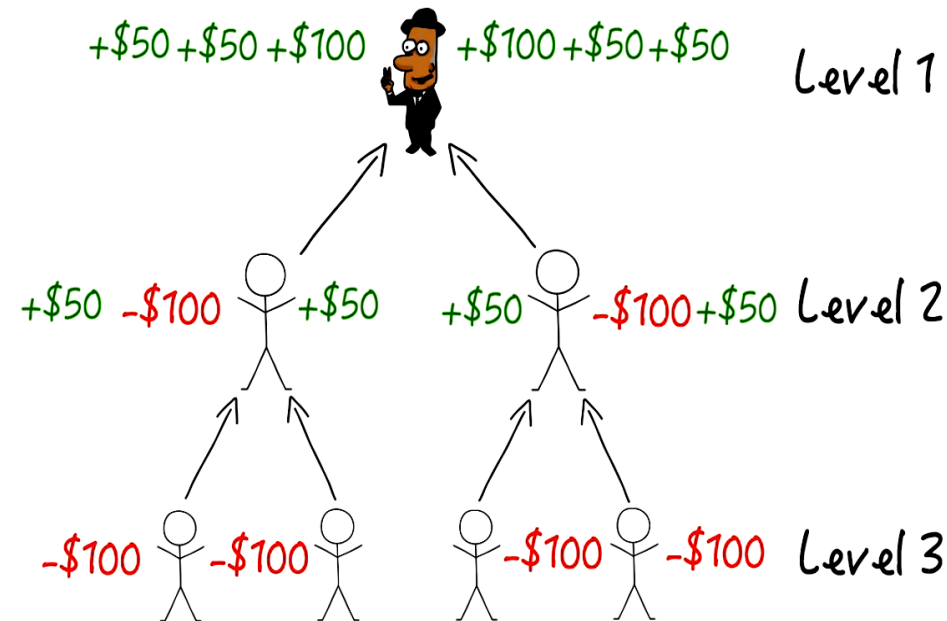
Importance of Jurisdictional Issues

- **Jurisdictional Dilemma**: laws in different jurisdiction define **terms** differently.
- It is important for:
 - **Law Enforcement Officers**: who investigate cybercrime and
 - **IT Professionals/Network Administrators**: who want to become involved in prosecuting cybercrimes committed against their networks.

----> to become familiar with the applicable laws.
- Generally, criminal behavior is **subject to the jurisdiction** in which it occurs.
- Because laws can differ drastically in different geographic jurisdictions (state laws), an **act that is outlawed in one location could be legal in another**.
- Even if the act that was committed is illegal across jurisdictions, however, **no one wants to prosecute** because of the geographic nightmare involved in doing so.
- Discussed in chapter 11 in more Detail.

Differentiating Crimes: That Use the Net from Crimes That Depend on the Net

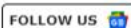
- The “cyber” aspect is not a necessary element of the offense; it merely provides the **means to commit the crime**.
- **For Example** : a person could **use the Internet** to:
 - ☐ Run a pyramid scheme or ponzi scheme or any other fraud,
 - ☐ Take bets for illegal gambling,
 - ☐ Set up clients for prostitution services,
 - ☐ Obtain pornographic pictures of minors.
- All these acts are already criminal in certain jurisdictions and could be committed without the use of the computers/network.
- **In other cases**, the crime is unique and came into existence with the **advent of the Internet**. **For Example**: unauthorized access by breaking into other networks, listening to network communications, releasing a virus malware over the internet etc.



Pyramid scheme

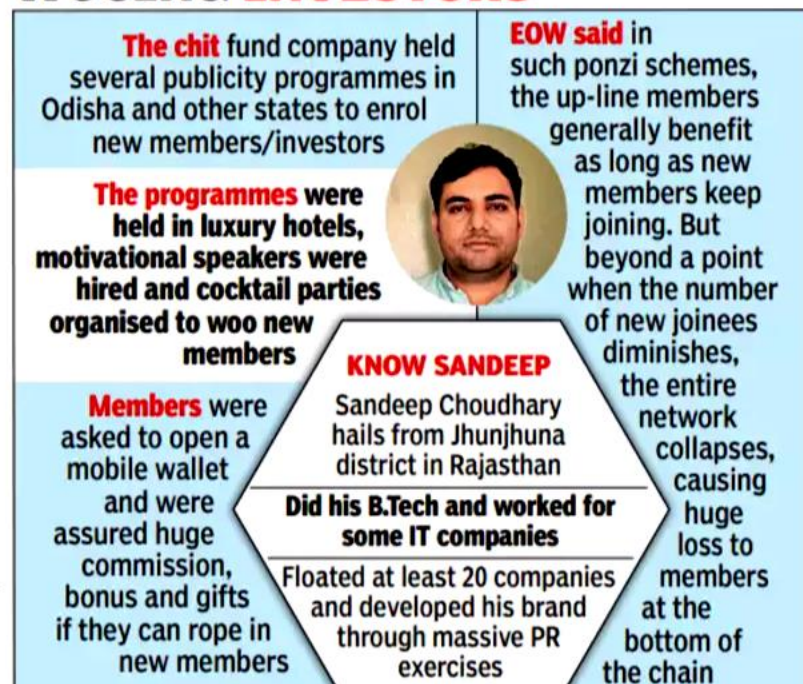
Ponzi co head, who duped 2.5 lakh of Rs 200 crore, arrested

TNN / Updated: Nov 18, 2023, 11:55 IST



The CEO of an online Ponzi scheme in India has been arrested while attempting to escape to Dubai. Sandeep Choudhary, along with his two associates, is accused of duping around 2.5 lakh investors of approximately Rs 200 crore (\$27 million) in different states. The company, called YES World, operated an illegal pyramid-structured online Ponzi scheme under the guise of crypto investments. The scheme attracted over 8,000 investors in Odisha alone, with an additional 2.5 lakh investors from other states. Choudhary is also accused of money laundering activities through multiple shell companies.

WOONG INVESTORS



Categorizing Cybercrime


Two broad categories:

- 1) **Violent or Potentially Violent Cybercrime** : that use computer networks and are of highest priority because : **these offenses pose a physical danger to some person or the community**. The types of violent or potentially violent cybercrime include:
 - **Cyberterrorism**: refers to terrorism that is **committed, planned, coordinated in cyberspace**—that is, via computer networks. It can include threatening /attacking national critical infrastructure:
 - **e-mail for communications between co-conspirators.**
 - **sabotaging air traffic control computer systems.**
 - **infiltrating water treatment plant computer systems to cause contamination.**
 - **hacking into hospital databases and sabotaging critical patient information.**
 - **disrupting the electrical power grid.**
 - **Assault by threat** : This cybercrime involves placing people in fear for their lives or threatening the lives of their loved ones. **For example**: sending e-mailed /SMS bomb threats to businesses or governmental agencies or an individual.
 - **Cyberstalking** : is a form of electronic harassment, often involving express or implied physical threats that **create fear in the victim** and that could escalate to real-life stalking and violent behavior.
 - **Child pornography** : Child pornography becomes a cybercrime ,when computers and networks are used for any of the following activities,
 - **people who create pornographic materials using minor children or involving juvenile.**
 - **people who distribute these materials.**
 - **people who access them.**

Fire Sale
attack
RedEcho
Cyber Attack
Stuxnet attack

2) **NonViolent Cybercrime** : Many crimes have been termed as non-violent in nature and are further divided into subcategories as follows:

- **Cybertrespass**:- the criminal accesses a computer's or network's resources **without authorization** but **does not misuse or damage the data there**. **Common Example**:
 - A hacker who breaks into networks just “because he (or she) can”—**to sharpen hacking skills**, to prove him- or herself to peers, or because it's a personal challenge.
 - “**Snooping**” - reading personal e-mail and documents and noting what programs are available on the system, what Web sites have been explored, and so forth, **but they don't do anything with the information they find**.
- **Cybertheft**:- using a computer and network to steal information, money, or other valuables. **Cybertheft include the following offenses**:
 - **Embezzlement**: *which involves **misappropriating money** or property for self use* that has been entrusted to you by someone else.
 - **Unlawful appropriation**: *which differs from embezzlement in that the criminal was never entrusted with the valuables but **gains access from outside the organization** and transfers funds, modifies documents giving him title to property he doesn't own.*
 - **Corporate/industrial espionage**: *in which persons inside or outside a company **use the computer/network to steal trade secrets** , financial data, confidential client lists, marketing strategies, or other information that can be used to sabotage the business or **gain a competitive advantage**.*

- **Plagiarism:** *which is the theft of someone else's original writing with the intent of passing it off as one's own.*
- **Piracy:** *which is the unauthorized copying of copyrighted software, music, movies, art, books, and so on, resulting in loss of revenue to the legitimate owner of the copyright.*
- **Identity theft:** *in which the Internet is used to obtain a victim's personal information, such as Social Security and driver's license numbers, in order to assume that person's identity to commit criminal acts or to obtain money or property or use credit cards or bank accounts belonging to the victim.*
- **DNS cache poisoning:** *a form of unauthorized interception in which intruders manipulate the contents of a DNS cache to redirect network transmissions to their own servers.* 
- **Doxing:** *when someone shares another person's personal information with anyone without their consent. The personal information may be in the form of someone's full name, address, history, password, and other identifying information.*

- **CyberFraud:** involves **promoting falsehoods** in order to obtain something of value or benefit. **For example:** trapping you into false belief to send money for helping a poor child.
 - **fraud** differs from **theft** in that, the victim *knowingly and voluntarily gives the* money or property to the criminal due to **misrepresentation by the criminal**.
 - **Cyberfraud can take other forms** as well such as any modification of data **to obtain a self benefit can constitute fraud** . **For examples,**
 - a student hacking into a school system's computer network to change grades is committing a fraud.
 - a person who accesses a online police records to remove his previous crimes or delete speeding challans from his driving record.

- **Transaction manipulation:** Also common in billing schemes, these involve at random **fraudulently increasing or reducing amounts** charged **to a particular account**. **For example:** applying different interest rates for loans.
- **Extraneous transactions:** These are **illegal transactions initiated by a trusted insider**, such as unauthorized billing transactions that result in **disbursement of company funds to the perpetrator or a shell company** he or she controls.
- **Unauthorized program modification:** These involves making unauthorized changes to automated payment or accounting software programs. A common form of this crime involves **programming the system to execute high numbers of mini frauds** such as *rounding of numbers (Salami slicing)*, *fraudulently adding service charges*, or *diverting amounts of money* so small as to fall below the radar of internal controls on accounts owned by the fraudster.
- **Counterfeiting/Forgery:**
 - **Forgery:** a genuine document that has been unlawfully altered
 - **Counterfeit:** a illegal copy of a genuine document

- **Destructive Crimes:** include those in which network services are disrupted or data is damaged or destroyed, rather than stolen or misused. These crimes include:
 - Hacking into a network/computer and deleting data or program files.
 - Hacking into a Web server and “vandalizing / deleting” Web pages.

Cybervandalism can be a random act done “just for fun” by bored hackers with a malicious streak, or it might be a form of computer sabotage for profit (erasing all the files of a business competitor). In some cases, cybervandalism might be performed to make a personal or political statement (as in cybergraffiti).

- Introducing viruses, worms, and other malicious code into a network or computer.
- Mounting a Denial of Service(DoS) attack that brings down the server or prevents legitimate users from accessing network resources. For eg. Ping of death attack, Ping flood, Teardrop attack, SYN flood attack, Smurf attack.

■ Other Nonviolent Cybercrimes:

- Internet gambling
- *Illegal Items sales:* It is an act of purchasing or selling illicit goods online, such as psychotropic substances, drugs, guns, and more prohibited items.
- Advertising/soliciting prostitution /illegal services over the Internet
- *Cyberlaundering*, involves using the Internet to hide the origins of money that was obtained through illegal means.
- *Cybercontraband*, or transferring illegal items, that is banned in some jurisdictions, over the internet. For example: hacking program, encryption technology, malware, creative content distributed in violation of copyright laws, obscene materials.
- *Slander:* A slander is an act of posting libel against another organization or person.
- *Cybersquatting:* Cybersquatting is a term used to describe a domain that is a misspelling of another domain with the intention of profiting from a goodwill of a trademark, company name, or personal name. The act is illegal because of the bad faith intent of the squatter.



cybercrime.gov.in
पर अपनी शिकायत दर्ज करें





Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India



सत्यमेव जयते



वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

Sabka Saath
Sabka Vikas
Sabka Vishwas
Sabka Prayas



साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Full Member



Operational
Member



Accredited
Member



Welcome to CERT-In



CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed



Latest Security Alert

- ▶ **CERT-In Vulnerability Note CIVN-2024-0014** NEW
(January 17, 2024)
Remote Code Execution Vulnerability in Atlassian Confluence Server and Data Center

- ▶ **CERT-In Vulnerability Note CIVN-2024-0013** NEW



Current Activities

- ▶ **Guidelines for Secure Application Design, Development, Implementation & Operations** NEW
(September 25, 2023)
One of the key reason for vulnerabilities in the applications are lack of secure design, development, implementation, and

Prioritizing Cybercrime Enforcement

Factors to consider in deciding which types of cybercrime will get **top enforcement priority** include:

- **Extent of harm:** Cybercrimes that involve violence or potential violence against people (especially crimes against children) are normally of **high priority**; crimes that result in the largest amount of monetary loss generally take precedence over crimes for which the amount of loss is less.
- **Frequency of occurrence:** Cybercrimes that occur with more frequency usually result in more concerted efforts than those that seldom occur.
- **Availability of personnel :** Cybercrimes that can be investigated easily by one detective might get more agency attention simply because **there are not sufficient personnel resources** to set up sophisticated investigations that require many investigators.
- **Training of personnel :** Which cybercrimes cases are investigated and which aren't , sometimes depends on the type of the case, **investigators have the technical training to handle the cyber crime**.
- **Jurisdiction:** Agencies generally prefer **to focus their resources on crimes that affect local citizens**. Even if the agency has legal jurisdiction, it might choose not to spend resources on cybercrimes that cross jurisdictional boundaries.
- **Difficulty of investigation:** Closely related to the two preceding factors, the difficulty of the investigation and **the likelihood of a successful outcome** could affect which crimes get top priority.
- **Political factors:** The prevailing political climate often **influences an agency's priorities**. If the politicians who govern the agency have a special concern about specific crimes, enforcement of those crimes is likely to take precedence.

Reasons for Cybercrime

Why do cyber attacks happen?

❑ Most often, cyber attacks happen because criminals want:

- Customers' financial details (eg credit card details, bank account numbers)
 - Sensitive personal data
 - Login credentials
 - Customer databases
 - Clients lists
 - Rivals Business' financial details
 - Intellectual property (trade secrets or product designs)
 - Intellectual challenge
 - Making a social or political point
- ❑ Unawareness of general public to technology
- ❑ Factors of the web fascinates crime: speed of doing things, no physical appearance, anonymity, borderless activities.

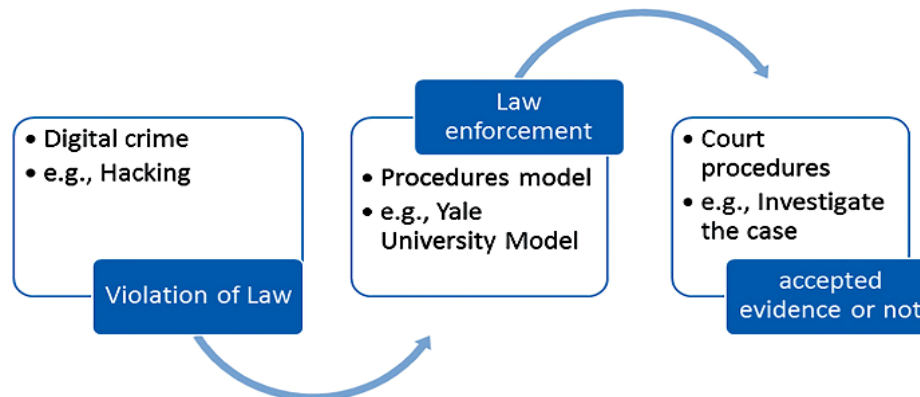
Fighting Cybercrime

Need to:

- Educate Cybercrime Investigators
- Educating Legislators and Criminal Justice Professionals
- Educating Information Technology Professionals
- Educating and Engaging the Community
- Using Technology to Identify and Fight Cybercrime

Cyber/Computer Forensics

- Unlawful activities giving rise to **digital crime**: frauds, embezzlement, hacking, identity theft, child pornography, theft of trade secrets etc..
- There is growing **need for investigators to search digital devices** for **data of evidential value** including *emails, photos, video, text messages, log files, etc.* that can assist in the reconstruction of a crime and identification/verification of the perpetrator.
- **Forensics** is defined as a study or practice relating to legal proceedings or augmentation.
- **Cyber forensics** is therefore concerned with **extracting digital evidence** from suspect systems, doing it in a way that **preserves its legal worth**, using that evidence to **construct and prove hypotheses about crimes**, and ultimately, **giving prosecutors the proof** they need to bring criminals to justice.
- **There are two main components of cyber forensics:**
 - **Digital investigation** i.e. technical aspect of performing forensic analysis on digital media.
 - **Legal proceedings**: maintaining and evaluating evidences and proving sequence of events.



Digital investigators often use a **variety of techniques** to help solve crimes or uncover information.

- Data acquisition
- Disk volume analysis
- Deleted Data recovery
- Keyword Search
- Hidden data detection
- Extraction of windows registry information
- Cracking
- Logfile analysis
- Timeline analysis
- Reverse engineering
- Document metadata analysis
- Multimedia forensic analysis
- Network traffic analysis
- IP trace


- Computer forensics includes **several sub-branches / investigating environments:**

- Memory Forensics
- Operating System Forensics
- File System Forensics
- Network Forensics
- Mobile Devices/IOT forensics
- Cloud Forensics
- Database Forensics
- Financial Forensics

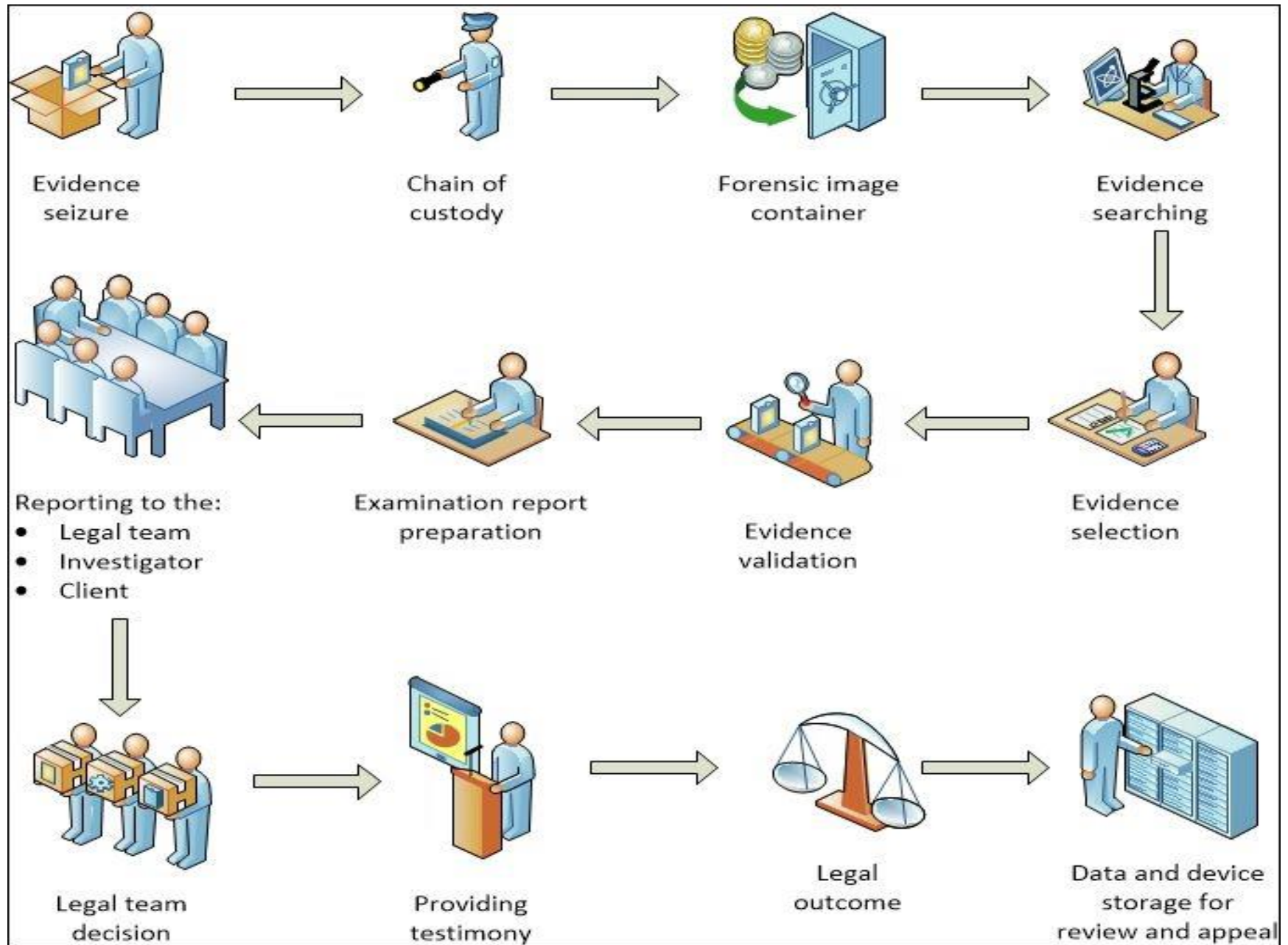
Digital Forensic sub-tasks:

- Preparation
- Investigation
- Collection
- Analysis
- Presentation

Cyber Forensic Models

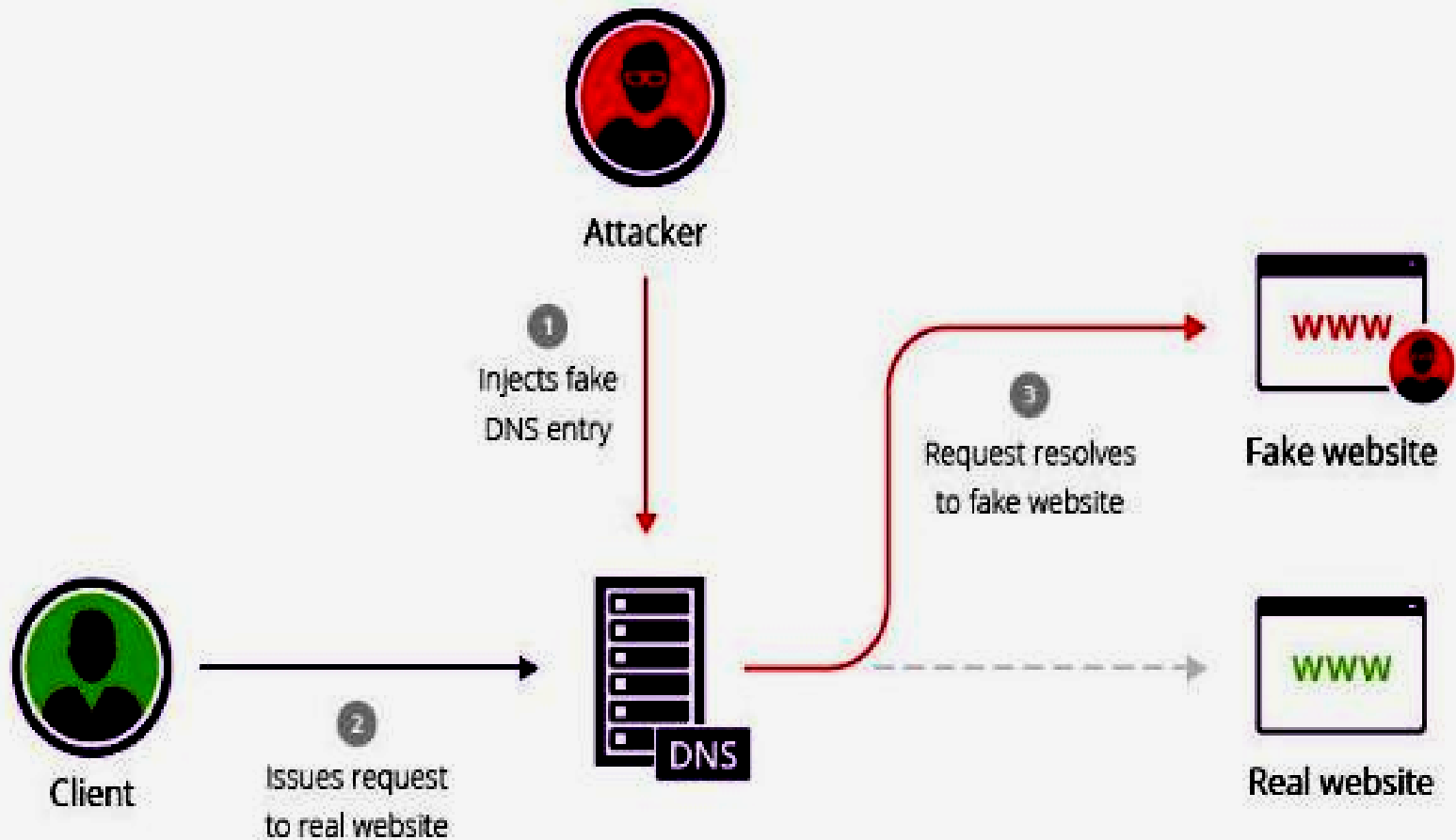
- **Kruse and Heiser (2001)**
 - *Assess, Acquire, Analyze and Report* 
- **Casey(2001) Yale University Model:** This model is developed by Casey who was then the security supervisor of Yale University's IT systems.
 - *Identification, Collection, Preservation, Examination, Analysis and Reporting*
- **Rodney Mckemmish Model** This model is proposed from Australia Police's officer. This model is comprised from four phases through the investigation:
 - *Identification, Preservation, Analyze and Presentation*
- **Ambhire and Meshram(2012)**
 - Planning phase (preparation)
 - Scene phase(Identification, Collection and Preservation)
 - Lab phases(Examination, Analysis and Report)

Investigative process

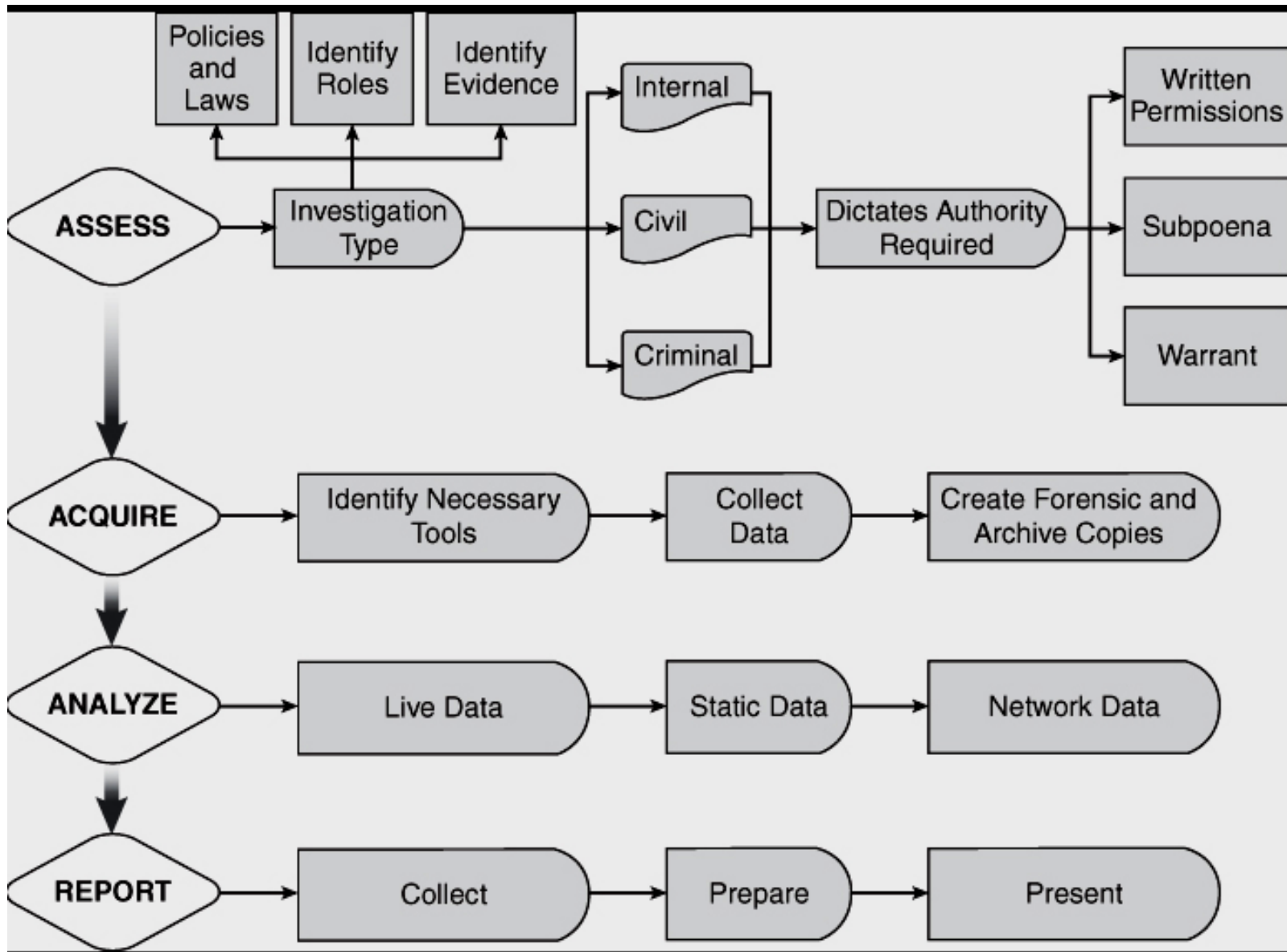


Thank you

DNS Spoofing



Kruse and Heiser (2001)



- **Casey(2001) Yale University Model:** This model is developed by Casey who was then the security supervisor of Yale University's IT systems.
 - *Planning, Identification, Collection, Preservation, Examination, Analysis and Reporting*

