The ICT University

Spring 2025 Continuous Assessment №1

School of *ICT*

Course Code: CYS 3251
Course Title: Computer/Network Forensics
Instructor: Engr. Daniel Moune

NAME : DAHIROU BACHAN

MATRICULE : ICTU20223102

EMAIL : dahirou.bachan@ictuniversity.edu.cm

PHONE NUMBER : 699836308

Chapter 1

Entering the World of Cybercrime:

Summary of chapter 1

Cybercrime: is define as the use of internet computers or any digital tool to perform a crime

Such an action is usually performed by crackers which are untrained and majorly by hackers which are very trained individuals

Cybercrime differ from traditional crime

Cybercrime knows no physical or geographic boundaries because the internet provide access to people, institutions, and business around the glob

There are crimes that are not possible without the use of computers such as

HACKING: which is define as an unauthorized access in to an individual computer

MALWARE: they are malicious software that causes damage to a computer or it gain access to a computer to steal information from it such software include, spyware. viruses, worms.

PHISHING: It is a type of cyber attack where scammers try to trick you by revealing you personal information such as passwords, credit card number, or login credentials by pretending to be a trustworthy individual or source this is done through fake email address or convincing messages to steal you private information or sensitive database

CRACKING: attempt to gain unauthorized access to a computer system so as to commit another crime, such as destroying information contained in that system.

IMPACTS OF CYBERCRIME

- REPUTATION DAMAGE: lost of trust in businesses or individuals affected by cyber crimes
- LEGAL CONSEQUENCES: organisations may face lawsuits or fines for failing to protect sensitive data
- EMOTIONAL AND PSYCOLOGICAL IMPACT: victims may experience stress fear or anxiety

How to prevent cyber attack

- *Use strong passwords*
- *Install antivirus and firewall software*
- *Keep software updated*
- *Secure wifi network*

Chapter 2:
Forensics Investigations and Electronic Evidence

COMPUTER FORENSICS: it is a branch of forensics science that focuses on criminal procedures law and evidence as applied on computer and related devices
Criminal Law: these are law dealing with public offenses that is action that are harmful to society as a whole
Civil law—Law: these are laws that governs the relationships between private parties, including both individuals and organizations.
Administrative Law: these are laws that that focuses on the exercise of government authority by the executive branch and its agencies.

Administrative agencies are created through “enabling legislation.”
1 : To determine if agency rules and regulations have been violated.
2: To investigate crimes committed against them
3: To determine if employees of the agency have engaged in misconduct or criminal activity

Acquisition isThe process of evidence retrieval in computer forensics investigations—from the search for the evidence to its collection and documentation.
And some questions it answer are:

- Which evidence was obtained
- Which individual or individuals retrieved the evidence
- Where the evidence was gathered

The most common practice is to seize a computer during a cybercrime investigation and take it off site—typically to a forensic lab—for a search of its contents for evidence.

IDENTIFICATION
It is a stage in which an investigator explains and documents the origin of the evidence and its significance
KEYWORD SEARCHING
It is used by a computer user when he or she seeks to locate a specific file on the computer that contains one or more of the words specified by the user
FILE CARVING
it is A means of searching for specific files in a hard drive based on the header, footer, and other identifiers in the file.
Presentation
The stage of a computer forensics investigation in which data pertinent to the case that were found during the investigation are reported.

Importance of network forensics

1: tracks cybercriminals activities
2: supports legal investigations
3: identifies security branches
4: prevent features attacks
5: protect sensitive data

Chapter 3

Laws Regulating Access to Electronic Evidence

Chapter summary

This chapter is concern with regulation of telecommunication and electronic communication data, the difference between relevant and nonrelevant data. it outlines privacy laws, government rules data, and the conditions under which services providers may voluntarily compelled to steal data

Traffic and Location Data

Traffic data consists of data about a communication. Among other things, it includes:

1: Determine the type of communication used like phones \
2: Trace and identify the source of a communication
3: Identify the destination of a communication
4: Determine the date, time, and duration of a communication

KEY TERMS

Traffic data: Data about a communication, including the type, source, destination, and time/length of communication.

Location data: Data about the location from which a particular communication was made

Content data: The words spoken in a conversation or the written in a message.

Non-content data: Communication data such as the telephone number, customer information such as name and address, and email addresses of the message sender and recipient

Data preservation and Data retention Data preservation that is, the ad hoc "freezing" of communications data is based on targeted surveillance, where "it affects only a limited number of individuals during specific periods rather than the entire population all of the time."[15] This practice provides "authorities with the power to order the logging and disclosure of traffic data in regards to … communications"

IMPORTANCE OF LAWS REGULATING ACCESS TO ELECTRONIC EVIDENCE

- Protecting individual privacy by setting limits on data access

- Ensures due process in legal investigation
- Prevent abuse of power by law enforcement agencies
- Clarifies legal procedures for accessing electronic evidence
- Promote transparency and accountability in government surveillance

Chapter 4

Searches and Seizures of Computers and Electronic Evidence

Summary of chapter 4

Search and seizure: A legal procedure whereby law enforcement agents conduct an examination of a premises and forcibly take property of potential evidentiary value from a person who is suspected of violating or has violated the law.

This chapter examines the right to privacy and its applications to computer and electronic devices, it highlights that individuals generally have a reasonable expectation

This chapter also focuses on the challenges of searching digital devices, which

Often contain vast amount of personal and confidential information to prevent unnecessary privacy violations, seme advocate for search protocol that limit investigative scope. However, critics warn that such limit might prevent the discovery of crucial evidence. Special procedures have therefore been developed to manage privileged information, aiming to balance privileged information, aiming to balance privacy rights with effective law enforcement

KEY TERMES:

Privacy: A multivalent social and legal concept, defined in ways ranging from the right to be let alone, to the capacity to keep certain things secret, to the right to control other individuals' access to oneself and information about oneself

Exclusionary rule: A rule that makes evidence that was obtained in violation of the Fourth Amendment generally inadmissible in court.

Inevitable discovery exception: An exception to the exclusionary rule that allows evidence that has been illegally obtained to be introduced in court if it would have inevitably been discovered through lawful means

Particularity: In regard to a search warrant, the idea that the search warrant needs to specify the place that will be searched and the items that will be seized.

Search Protocols

The process of searching a computer for electronic evidence can easily turn into a sweeping examination of a wide array of information

Importance searches and seizures of computer and electronic evidence in point form

- Links suspects to crimes: digital footprint can tie individuals to specific actions or locations
- Track criminal networks: help law to increase identification and monitors organized crime
- Provide real time insights: electronic surveillance can offer ongoing intelligence during investigation
- Supports court cases: lawfully obtained electronic evidence can be used in trial to strengthen

CHAPTER5:

Cybercrime Laws; Which statute for which Crime?

This chapter explains the types of crimes and incidents involved in computer forensics investigation.

Website Defacement; A type of attack in which one or more individuals alter or replace the content of a website without authorization.

Malware creation

Worms and Viruses; Worms automatically self-propagate and are delivered to their targets via a network of physical media.

Trojan Horses; imitates legitimate files and can be either a joke program or a software delivery mechanism for viruses**.**

Computer spying and intrusions

Adware; A computer program used to track user's online activities.

Denial of Service Attacks and Distributed Denial of Service Attacks

- **SYN Flood attack;** In which the attacker floods the network server with phony authentication request.
- **TCP handshake;** it is a process to set up a TCP connection between two computers.
- **TCP;** The language that computers use on the internet to communicate with one another.

KEY TERMS

Fraud;

Falsely representing a fact either by conduct or by words to induce a person to rely on the misrepresentation of something of value.

Auction fraud;

A type of fraud in which the seller of an item at an auction engages in some sort of deception to defraud the would be buyer.

investment fraud: A type of fraudulent behaviour involving market manipulation.

Cybersmart investment scheme: A type of financial fraud in which the offender tries to lower the price of a stock by circulating false rumours about it.

Securities and Exchange Commission: Agency responsible for regulating the securities industry and enforcing relevant securities laws

Credit card fraud: A crime in which an individual obtains, uses, sells, or buys another individual's credit card information.

Intellectual Property Theft and Economic Espionage

Intellectual property is intangible property that the law grants ownership rights to. Federal Law protects four distinct areas of intellectuel propret :

Intellectual Property Theft and Economic Espionage

Intellectual property is intangible property that the law grants ownership rights to. Federal law protects four distinct areas of intellectuel property:[66]

CHAPTER 1

Chapter1: Entering the world of cybercrime

Critical Thinking Question

While many crimes have been transformed or facilitated by ICT , Some traditional crimes remains relatively untouched. Here are some examples

- Violent crime like Murder, robbery
- Theft of physical Goods
- Domestic Violence
- Drug dealing
- Human trafficking

Review Questions

1. **What is cybercrime?**

- Cybercrime refers to illegal acts that involve computing devices and networks.

2. **How does computer crime differ from traditional crime?**

- Computer crime involves illegal activities conducted via computers or networks such as hacking and online fraud meanwhile traditional crime involves physical actions and direct interactions such as Drug dealing and human trafficking.

3. **Identify and describe two or three traditional crimes in which computers are now used as an instrument. How has the nature of these crimes changed as a result of the technology?**

- **Harassment:** Online platforms have enabled stalking and harassment to occur anonymously to target victims without geographical limitations.
- **Fraud:** Traditional fraud like credit card fraud have shifted to online practices such as phishing.

4. **What are the two main categories of Cybercrime? Provide few examples of each**

- **Crimes Against Property:**

Hacking: unauthorized access to systems or data

Ransomware: Malware that encrypts data and demands payment for access

- **Crimes against individuals**

Cyber Bullying: Harassment through digital platforms

Identity Theft: Stealing personal information to impersonate some one

5. **How can vandalism occur online?**

- **Social media attacks:** Hacking social media accounts to post inappropriate content
- **Spam:** Flooding platforms with spam messages that disrupt normal interactions
- **Website Defacement:** Unauthorized alteration of a website content often replacing it with inappropriate messages.

6. **What is malware? Provide a few examples of it**

- It is any software designed to cause damage to a computer, server, and network.
- Examples include; viruses, worm, Ransomware

7. **What is a botnet? How does it work**

- A botnet is a network of compromised computers or devices often referred to as bots

How botnets work

Devices are infected through phishing malware download.

Infected devices connect to a C&C server that sends command.

Botnets can perform tasks such as data theft, Spam campaigns.

Some botnets can spread to other devices by exploiting vulnerabilities.

Botnets often include features to remain undetected.

8. What **is embezzlement?**

- It as a form of financial fraud in which an individual in a position of trust misappropriates or steals funds.

9. **How does copyright infringement occur?**

- It occurs when someone uses copyrighted work without the permission of the copyright holder.

10. **What are the dangers associated with online sales of prescription drugs?**

- Many online pharmacies sell fake or substandard drugs that may contain incorrect ingrdients
- Consumers may obtain medications without a valid prescription.
- Some online sellers may operate as scams

11. **Which problems does cybercrime pose to authorities seeking to invigilate it?**

- Anonymity; cybercriminals often use techniques to mask their identities such as VPNs proxies and dark web.
- Volume data; investigators must sorts through vast amounts of data and digital evidence

Chapter2: An introduction to Computer Foerensics Investigations and Electronic Evidence

Practical Exercise

Hearsay Evidence: Hearsay is generally inadmissible in court. In this case, the prosecution misused the radio dispatch to prove the truth of the matter asserted, violating evidentiary rules.

Types of Evidence

Direct Evidence: Testimony from officers who observed who threw the gun.

Circumstantial Evidence: Context of the arrest

Impact of Evidence Authenticity: The inadmissibility of hearsay evidence compromised the prosecution's case, reinforcing the need for adherence to evidentiary standards.

Review Questions

1. What is computer forensics?

- Computer forensics is the process of collecting, analyzing, and preserving digital evidence from computers and other electronic devices for use in legal proceedings.

2. What are the major differences between public and private investigations?

- Public investigations are conducted by government agencies while private investigations are carried out by private individuals or firms often for personal or corporate interests.

3. What are the similarities and differences between criminal and civil law?

- Both criminal and civil law involve legal disputes, but criminal law deals with offenses against the state and involves penalties like imprisonment, while civil law addresses disputes between individuals or entities typically involving compensation.

4. Why do administrative agencies conduct investigations?

- Administrative agencies conduct investigations to enforce regulations ensure compliance with laws and protect public interests.

5. Describe the computer forensics process.

- The computer forensics process includes identifying preserving, analyzing and presenting digital evidence in a manner that is legally admissible.

6. When should a search be conducted on site?

- A search should be conducted on site when immediate access to evidence is necessary and there is a risk of loss or destruction.

7. When should a search be conducted off site?

- An off-site search is appropriate when evidence is located in a controlled environment such as a data center where specialized tools and techniques can be applied.

8. What is slack space?

- Slack space refers to unused space on a storage device that may contain remnants of deleted files which can be recovered during forensic analysis.

9. Which different types of evidence exist?

- Types of evidence include direct evidence, circumstantial evidence documentary evidence physical evidence and testimonial evidence.

10. What is the difference between circumstantial and direct evidence?

- Direct evidence directly proves a fact while circumstantial evidence requires inference to connect it to a conclusion

11. When is hearsay evidence admissible in court?

- Hearsay evidence may be admissible under certain exceptions, such as excited utterances or business records, but generally, it is inadmissible unless it meets specific criteria.

12. How can electronic evidence be authenticated?

- Electronic evidence can be authenticated through metadata digital signatures and corroborating evidence that establishes its integrity and origin.

13. What are the standards of evidence?

- The standards of evidence refer to the rules and criteria that determine what evidence is admissible in court, including relevance, reliability, and authenticity.

Chapter3: Laws Regulating Access to Electronic Evidence

Review Questions

1. Traffic Data: Information about the transmission details of data over a network including time, duration and destination but excluding the content of the communications.

2. Location Data: Data that identifies the geographic location of a device or user typically gathered from mobile devices or GPS technology.

3. Content vs. Non-Content Data:

- Content Data: The actual information exchanged in communications (examples; text of emails).

- Non-Content Data: Metadata that outlines details about the communication such as sender recipient and timestamps.

4. ECPA Permit law: The Electronic Communications Privacy Act permits law enforcement to access certain electronic communications and data usually requiring a warrant or court order.

5. Obtaining Subscriber Records: U.S. government agencies can obtain subscriber records through subpoenas court orders or warrants depending on the type of data requested.

6. Accessing a Suspect's Email: A government agency can obtain a suspect's email with a warrant particularly if the email has been stored for over 180 days.

7. Voluntary Disclosure by Providers: Providers may voluntarily disclose emails and records to the government if they believe it's necessary for protecting life or complying with legal obligations.

8. ECPA and USA Patriot Act Regulations: The ECPA regulates the interception and access to electronic communications while the USA Patriot Act expands government access to these communications and records under specific conditions.

9. Regulating Personal Information: Laws such as the Privacy Act of 1974 and the Freedom of Information Act (FOIA) govern the handling of personal information stored in government databases.

10. Sarbanes-Oxley Act Sections: Significant sections resulting from the financial scandals include Section 404 (requiring internal controls) and Section 302 (corporate responsibility for financial disclosures), aimed at enhancing accountability and transparency.

Chapter4: Searches and Seizures of Computers and Electronic Evidence

Critical Thinking Questions

1. Thoughts on the Carey-Winick Approach:

The Carey-Winick approach emphasizes the protection of sensitive information and privacy rights, which is essential in today's digital landscape. While it can be seen as beneficial for safeguarding individual rights and ensuring ethical handling of data, it may also pose challenges for law enforcement and investigations. Balancing privacy with the need for effective law enforcement is crucial; thus, the approach can be both beneficial and problematic depending on the context of its application.

2. Best Strategy for Reviewing Privileged Information:

The best strategy for reviewing privileged information on computers is to employ a neutral third party or legal expert to conduct the review. This ensures that privileged communications are identified and protected while maintaining the integrity of the investigation. Using a separate entity reduces the risk of bias and ensures compliance with legal standards, ultimately fostering transparency and trust in the investigative process. This approach minimizes the potential for inadvertent disclosure of sensitive information.

Review questions

1. Why is privacy important?

Privacy is vital for personal autonomy, security, and dignity. It enables individuals to control their personal information, fosters trust in relationships, and is essential for the exercise of free expression and association.

2. Is all evidence that is illegally searched and seized inadmissible in court? Why do you think this is the case?

Not all illegally obtained evidence is inadmissible. While the exclusionary rule generally excludes such evidence, exceptions exist where law enforcement acted under a reasonable belief that their actions were lawful. This balance aims to deter unlawful police conduct while addressing practical legal needs.

3. How is the "reasonable expectation of privacy" test applied to computers?

The "reasonable expectation of privacy" test considers societal norms regarding privacy and the context of the situation. In computers, it assesses whether a user has a legitimate expectation that their digital communications and data will remain private, based on factors like ownership, usage, and the nature of the information.

4.Does an employee have a reasonable expectation of privacy in the workplace?

Employees generally have a limited reasonable expectation of privacy at work, particularly when using company resources. Employers often have the right to monitor communications and activities, especially if policies are in place informing employees of such monitoring.

5. When does the government need a search warrant to search and seize a suspect's computer?

The government typically needs a search warrant to search and seize a suspect's computer, especially if it contains private information. A warrant is usually required unless exigent circumstances justify a warrantless search.

6. What are some examples of warrantless searches, and under what circumstances may they be conducted?

Examples of warrantless searches include consent searches, searches incident to arrest, and emergencies where evidence might be destroyed or public safety is at risk. These searches must meet specific legal criteria to be considered lawful.

7. Under what circumstances can a portable electronic device be seized and searched after a suspect is arrested?

A portable electronic device can be seized and searched if it is within the suspect's immediate control at the time of arrest or if there is an imminent threat of evidence destruction, allowing for a warrantless search under exigent circumstances.

8. Which type of exigent circumstances might arise in respect to computers?

Exigent circumstances for computers might include scenarios where there is a risk of data destruction, an immediate threat to public safety, or the need to prevent harm, justifying a warrantless search.

9. When can a third party consent to a search?

A third party can consent to a search if they have common authority over the property or if the suspect has granted them explicit permission to do so. The consent must be voluntary and informed.

10. Should search protocols be used in investigations? Why or why not?

Yes, search protocols should be used in investigations to ensure systematic and lawful procedures are followed

Chapter5: Cybercrime Laws: Which Statute for Which Crime?

Critical Thinking

Cybercrime Scenario: Ransomware Attack Summary

Scenario:

A mid-sized hospital is hit by a ransomware attack that encrypts patient records and operational files, with attackers demanding a $500,000 ransom in cryptocurrency. This disrupts hospital operations and compromises patient care.

Investigation Focus:

Key evidence to gather includes:

1. Malware Samples: To analyze the attack methods and identify the ransomware strain.

2. Network Logs: To pinpoint the attack's entry point and timeline.

3. Affected Systems: To assess the malware's spread and impact.

4. User Activity Logs: To identify compromised accounts and trace attacker actions.

5. Communication Records: To gather information on the attackers' demands and identity.

6. Backup Systems: To evaluate recovery options without paying the ransom.

7. Endpoint Security Logs: To check for prior alerts or malware detections.

8. Cryptocurrency Transactions: To track payments and potentially identify the attackers.

Conclusion

Collecting this evidence will enhance understanding of the ransomware attack, inform preventive strategies, and support efforts to bring the perpetrators to justice.

Review Questions

1. What are computer viruses? Worms? Describe the main effects of one virus or worm. Was the perpetrator (or perpetrators) of the virus or worm caught after its release into the wider community?

- Computer Viruses: Malicious software that attaches itself to legitimate programs and spreads when the infected program is executed.

- Worms: Standalone malware that replicates itself to spread across networks without needing to attach to other programs.

2. Distinguish between a Trojan horse, a computer virus, and a worm.

- Trojan Horse: Malicious software disguised as legitimate software that tricks users into installing it.

- Computer Virus: Attaches itself to files and programs, spreading when those files are executed.

- Worm: Self-replicating malware that spreads across networks without user interaction.

3. What is the difference between spyware and adware?

- Spyware: Software that secretly monitors user activity and collects personal information without consent.

- Adware: Software that displays unwanted advertisements, often tracking user behavior to target ads, but does not necessarily collect personal information covertly.

4. Which sections of 18 U.S.C. § 1030 could be used against someone who launched a DoS or DDoS attack?

- Sections 1030(a)(2) (unauthorized access) and 1030(a)(5)(A) (intentional damage) can be applied to DoS or DDoS attacks. Some may argue that section 1030(a)(4) (fraud) might not apply if there is no intent to defraud, but the damage caused can still warrant charges under the other sections.

5. What is a TCP handshake? How does a SYN flood attack occur?

- TCP Handshake: A three-step process (SYN, SYN-ACK, ACK) that establishes a connection between a client and server.

- SYN Flood Attack: An attacker sends numerous SYN requests without completing the handshake, overwhelming the server and consuming resources, leading to denial of service.

6.List the types of fraud that people engage in.

- Identity theft

- Credit card fraud

- Insurance fraud

- Investment fraud

- Cyber fraud

7. Name and describe two types of investment fraud.

- Ponzi Scheme: A fraudulent investment operation where returns are paid to earlier investors using the capital from newer investors, rather than from profit earned.

- Pump and Dump: A scheme where the price of a stock is artificially inflated through false or misleading statements, allowing the fraudsters to sell their shares at a profit before the price crashes.

8. What is intellectual property? Why should it be protected?

- Intellectual Property: Creations of the mind, such as inventions, literary and artistic works, and symbols.

- Protection Importance: Protecting Intelectual property encourages innovation and creativity by ensuring creators can benefit from their work without fear of unauthorized use.

9. What are trade secrets? Why should the theft of trade secrets be criminalized?

- Trade Secrets: Confidential business information that provides a competitive edge, such as formulas, practices, or designs.

- Criminalization Importance Theft undermines fair competition and can lead to significant financial loss for businesses, stifling innovation and economic growth.

10. What is the main difference between cyberharassment and cyberstalking?

- Cyberharassment: Repeated, unwanted online behavior intended to intimidate or annoy another person.

- Cyberstalking: A more severe form of harassment involving threats, tracking, or persistent unwanted communication that causes fear or emotional distress.