ITMS 538 Assignment 03b_rds

Alan Palayil

Due Date: 10/02/2022

Nelson Text Review Questions from Chapter 1:

Q1: Digital forensics and data recovery refer to the same activities. True or False?

- False

Q2: Police in the United States must use procedures that adhere to which of the following?

a. Third Amendment

b. Fourth Amendment

c. First Amendment

d. None of the above

- b. Fourth Amendment

Q3: The triad of computing security includes which of the following?

a. Detection, response, and monitoring

b. Vulnerability assessment, detection, and monitoring

c. Vulnerability/threat assessment and risk management, network intrusion detection and incident response, and digital investigation

d. Vulnerability assessment, intrusion response, and monitoring

- c. Vulnerability/threat assessment and risk management, network intrusion detection and incident response, and digital investigation

Q4: What's the purpose of maintaining a network of digital forensics specialists?

- Maintaining a network helps to increase our knowledge and be able to get information and referrals whenever possible.

Q5: Policies can address rules for which of the following?

a. When you can log on to a company network from home

b. The Internet sites you can or can't access

c. The amount of personal e-mail you can send

d. Any of the above

- d. Any of the above

Q6: List two items that should appear on a warning banner.

- i. The access to either the system or network is restricted to authorized users.

  ii. The organization has the right to inspect and monitor system and network usage in officially.

Q7: Under normal circumstances, a private-sector investigator is considered an agent of law enforcement. True or False?

- False

Q8: List two types of digital investigations typically conducted in a business environment.

- i. Internet and email abuse investigations.

  ii. Industrial espionage and employee termination cases.

Q9: What is professional conduct, and why is it important?

- Professional conduct is the ethics, morals, and standards by which employees are expected to behave in workplace as it determines their credibility.

Q10: What's the purpose of an affidavit?

- Affidavit is used by an organization to deal with abuse investigations by issuing a warrant.

Special Problems:

SP01.1

1. Define Carrier's 3 phases of a digital crime scene investigation.
   - The following are the Carrier's 3 phases of a digital crime scene investigation:
   - System Preservation Phase: The first phase is to try to preserve the state of the digital crime scene like creating a copy.
   - Evidence Searching Phase: This phase is to search for evidence through the digital devices that can support or disprove theories regarding the incident.
   - Event Reconstruction Phase: The last phase is to use the evidence to reconstruct the events that occurred in the system.
2. For a hard disk, what are **Carrier's** 4 phases of analysis?
   - The following are the Carrier's 4 phases of analysis:
   - Physical Media Analysis
   - Volume Analysis
   - File System Analysis
   - Application Analysis
3. Discuss how your responses to (1) and (2) above compare with the **Nelson** text.
   - Nelson, in contrast to Carrier, divides the investigation process into two categories, the private-sector and public-sector investigations. He explains the laws and

procedures for conducting a digital investigation differ for both sectors and suggests a systematic approach for doing so, maintaining the chain of custody which Carrier doesn't discuss. In short Nelson's method is more organized, systematic, and detailed than Carrier's. It does not specifically discuss how to conduct a hard disk analysis.

SP01.2

For a country other than the United States, identify the part of that country's constitution or laws that are as close to the U.S. Constitution's 4th amendment.

If you are originally from a country other than the U.S., use your country of origin's constitution or laws.

Write a description of the above that includes:

• An identification of the part of the constitution or laws

• A direct, relevant quotation in English of the constitution or laws.

- In the Constitution of India, the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and by Part III of the Constitution of freedom. It is held also by the Supreme Court as right to privacy which is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the constitution.
  However, currently India still doesn't have any written privacy laws in sight. This leaves the data regulation open to a wide variety of sectoral regulations.

Nelson Text Review Questions from Chapter 2:

Q4: The manager of a digital forensics' lab is responsible for which of the following? (Choose all that apply.)

a. Making necessary changes in lab procedures and software

b. Ensuring that staff members have enough training to do the job

c. Knowing the lab objectives

d. None of the above

- a. Making necessary changes in lab procedures and software

  b. Ensuring that staff members have enough training to do the job

  c. Knowing the lab objectives

Q5: To determine the types of operating systems needed in your lab, list two sources of information you could use.

- Statistics from the Uniform Crime Report within a certain area or organization along with the list of cases that were handled.

Q8: Why is physical security so critical for digital forensics labs?

- It is critical to prevent data from being stolen, corrupted, or lost from the evidence in the digital forensics' lab.

Q9: If a visitor to your digital forensics' lab is a personal friend, it's not necessary to have him or her sign the visitor's log. True or False?

- False

Q11: Large digital forensics labs should have at least _____ exits.

- 2

Q13: Digital forensics facilities always have windows. True or False?

- False

Q14: Evidence storage containers should have several master keys. True or False?

- False

Q15: A forensic workstation should always have a direct broadband connection to the Internet. True or False?

- False

Q17: Which organization has guidelines on how to operate a digital forensics lab?

- The ANSI National Accreditation Board (ANAB) has the guidelines on how to operate a digital forensics lab by providing accreditation services and training to public- and private-sector organizations, serving the global marketplace.