CYBR 472: Cybercrime Investigations

Test

20 March 2025

Time allowed: 50 minutes

Instructions:

- Answer all questions.
- Identify the one **best** response for the multichoice questions.
- Short answers should not exceed the size of the provided boxes.
- Write all your answers in the booklet and return at the end of the test.
- Calculators, electronic devices or reference materials are not permitted.
- Paper hardcopy dictionaries to translate words from English to other languages are permitted.

1. (1 point) What is digital forensics?
    A. The process of recovering deleted files and hidden data from electronic devices for investigative purposes.
    B. The science of identifying, collecting, and analyzing digital evidence through the application of scientific methods and techniques.
    C. The technical procedure for examining computers and digital media to find evidence of illegal activities.
    D. The practice of securing digital devices and analyzing security breaches by examination of compromised systems.

2. (1 point) Place the following steps of the digital forensic process in the correct order:
    1. Analysis
    2. Identification
    3. Presentation
    4. Preservation
    5. Collection
    6. Documentation

    A. 2, 4, 5, 1, 6, 3
    B. 2, 5, 4, 1, 3, 6
    C. 4, 2, 5, 1, 6, 3
    D. 2, 4, 1, 5, 6, 3

3. (1 point) How does Locard's Exchange Principle need to be adapted for digital environments?
    A. It applies exactly the same way in digital environments as in physical environments.
    B. It does not apply at all to digital environments because there is no physical contact
    C. In digital environments, traces exist only because the systems were designed to record information
    D. In digital environments, traces are always more reliable than in physical environments

4. (1 point) What does the "remote access search" refer to in New Zealand's legal framework?

   A. Physical search of remote locations

   B. Search of data not stored on the device being examined

   C. Access to computing devices from a distance

   D. Searching for remote control devices

5. (1 point) What does the principle of "proportionality" in digital forensics primarily refer to?

   A. The ratio of digital to physical evidence in a case

   B. Balancing evidence collection with privacy rights

   C. The mathematical proportion of compromised data

   D. Equal treatment of all suspects in an investigation

6. (1 point) Which New Zealand legislation provides the primary framework for obtaining, preserving and analyzing digital evidence?

   A. Privacy Act 2020

   B. Evidence Act 2006

   C. Search and Surveillance Act 2012

   D. Crimes Act 1961

7. (1 point) A digital forensics analyst working for a corporate investigation team discovers evidence of financial fraud during an authorized investigation of an employee's laptop. The investigation was initially conducted for a policy violation related to unauthorized software installation. Upon examination of the device, the analyst also finds private medical information about the employee's family member and personal photos not related to the case. What is the most appropriate ethical approach?

   A. Report all findings including medical information since the examiner has authorization to search the entire device

   B. Report only unauthorized software, as the original scope did not include financial activities

   C. Report both unauthorized software and potential fraud, while excluding medical information and personal photos from the report

   D. Report all findings since company property contains no expectation of privacy

   E. Report all findings but anonymize the medical information before including it in the report

8. (1 point) Which of the following is NOT a characteristic of the Advanced Forensic Format (AFF)?

    A. It offers both compressed and uncompressed options

    B. It has no size restrictions

    C. It provides built-in metadata storage

    D. It is a proprietary format that can only be used with specific tools

    E. It has internal consistency checks for self-authentication.

9. (1 point) An investigator uses a hardware write blocker to acquire an image from a suspect's SSD. After creating the initial forensic image with the hash value H1, the SSD is stored securely for one month. When creating a second image for verification purposes, the hash value H2 does not match H1, despite using the same hardware write blocker. Which of the following best explains this discrepancy and the appropriate investigation approach?

    A. The hardware write blocker failed during the second acquisition; the investigation should rely on H1 as the authentic image

    B. The suspect remotely accessed and altered the SSD; the investigation should be considered compromised

    C. The SSD's internal TRIM, garbage collection, and wear leveling processes altered data in unallocated space despite the write blocker; investigators should document this limitation and focus on allocated data analysis

    D. Write blockers are ineffective with SSDs; the investigation should have used logical acquisition instead of physical acquisition

    E. The hash algorithm produced a collision; both images are valid and the investigation can proceed with either one

10. (1 point) An investigator arrives at a crime scene and finds a computer with a RAID 0 array that may contain evidence. One of the drives appears to have physical damage. What is the most significant implication for the investigation?

    A. The investigation will take longer, but all data can still be recovered

    B. Only the data on the undamaged drives can be recovered

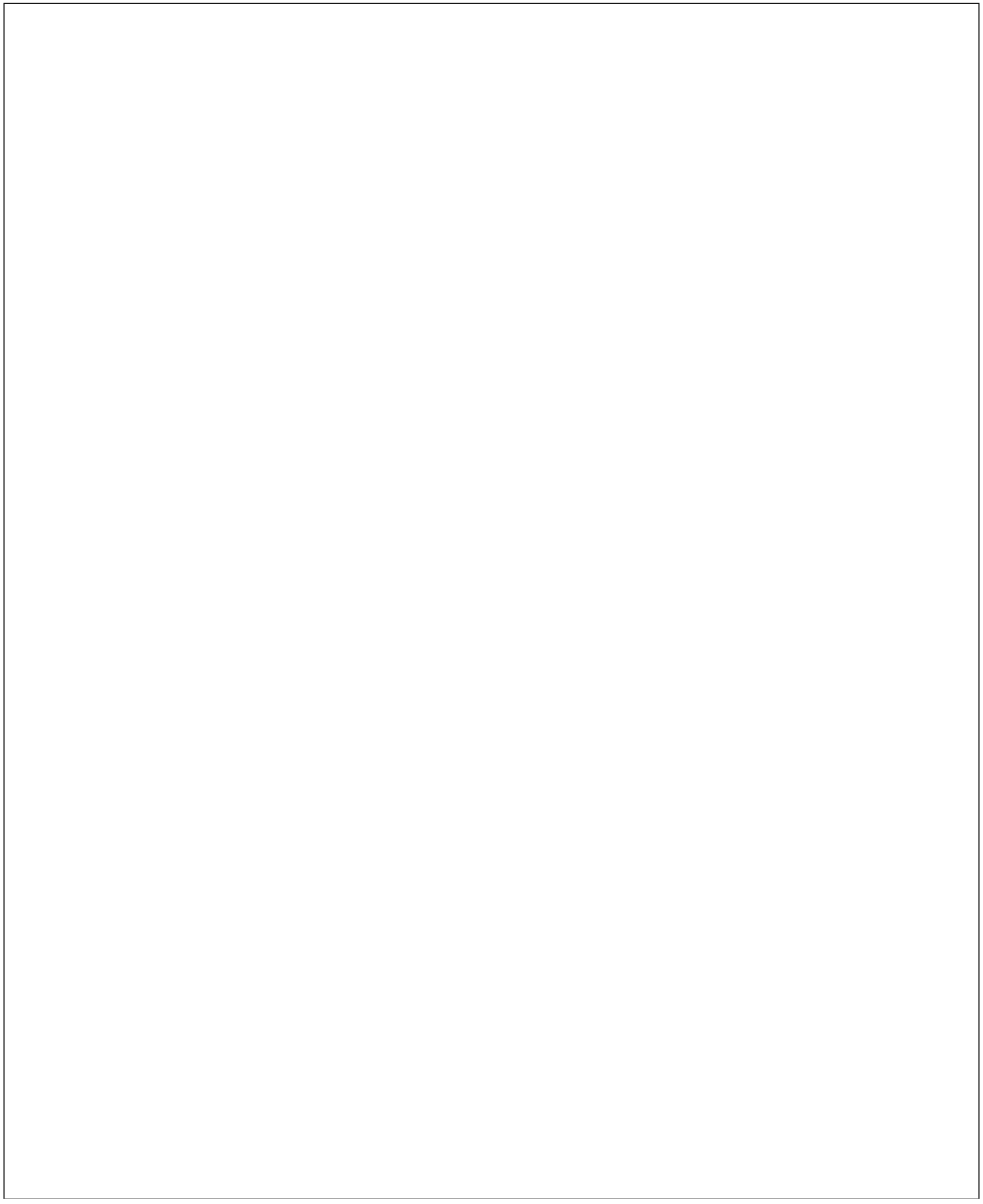
    C. Access to all data on the RAID array may be lost

    D. The damaged drive can be replaced with a new one without data loss.

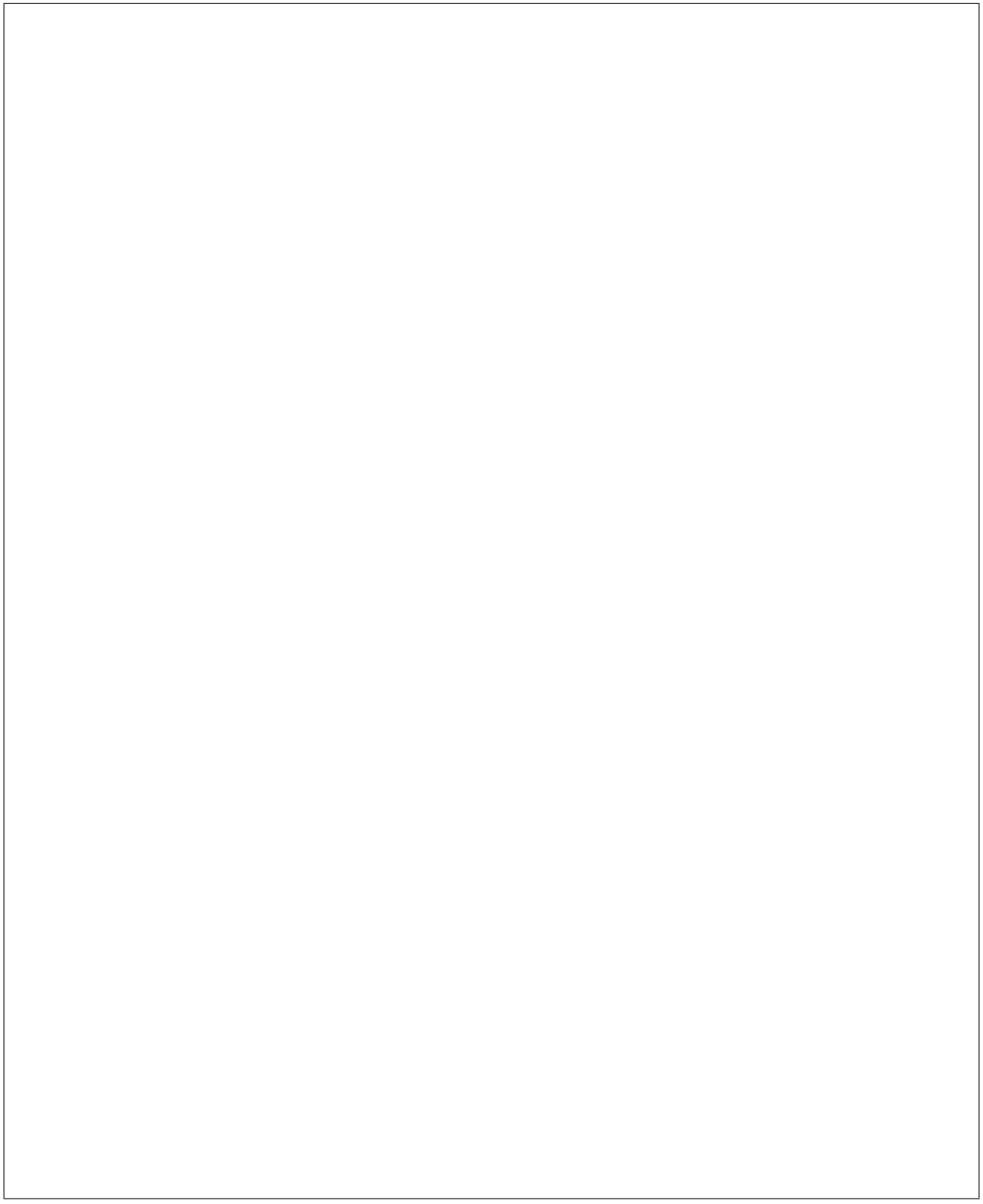
Spare Page for Working

This page will not be marked

11. (10 points) Compare and contrast explicit and implicit digital traces in terms of their purpose of creation, system design requirements, and evidentiary reliability. Using a specific case scenario (e.g., investigating unauthorized data access), explain how these two types of traces would complement each other in reconstructing the sequence of events. (max 250 words)



12. (10 points) Analyze the jurisdictional challenges that digital forensic practitioners in New Zealand face when investigating systems where data is distributed across multiple countries. Discuss how the Dotcom case has influenced New Zealand's approach to sharing digital evidence with international authorities. Explain the current mechanisms for international cooperation and discuss how the Budapest Convention might change this landscape in the future. Reference relevant New Zealand legislation and cases that have shaped the approach to cross-jurisdictional digital evidence. (max 250 words)



13. (10 points) Contrast the various acquisition methods discussed: static versus live acquisition, and traditional (full) versus logical and sparse acquisition. Describe the circumstances in which each would be the most appropriate, their key differences, and potential challenges. Include the four key considerations that influence your choice of method and how acquisition planning might differ when dealing with Solid State Drives (SSDs) versus traditional Hard Disk Drives (HDDs). (250 words)

******** Test ends here ********