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)

Solution:

Comparison of Explicit and Implicit Digital Traces

Explicit and implicit digital traces differ fundamentally in their characteristics and creation purpose. Explicit traces are direct records deliberately created as part of normal system operation (e.g., log files, database transactions, email headers) with structured formats typically containing timestamp information. They exist because systems were specifically programmed to record these events, offering high reliability as contemporaneous documentation. However, their existence depends entirely on system design decisions - if no logging was implemented, these traces simply won't exist.

In contrast, implicit traces are indirect artifacts requiring interpretation (e.g., deleted file fragments, cache artifacts, memory remnants, temporary files). These traces weren't deliberately created for documentation purposes but exist as by-products of system operations. Their reliability varies based on system activity since creation and requires contextual analysis to become meaningful evidence.

Case Scenario: Unauthorized Data Access Investigation

In an unauthorized data access investigation, these trace types would complement each other effectively. Explicit traces might include authentication logs showing login attempts, access control records documenting which files were accessed, and VPN connection logs establishing network paths. These provide a documented timeline where logging was implemented. However, if an attacker disabled logging or exploited systems where comprehensive logging wasn't designed in, implicit traces become crucial. Browser cache might contain viewed document fragments, memory analysis could reveal credentials still in RAM, and file system artifacts might show recently accessed paths.

Integration of Trace Types

By correlating explicit traces (showing recorded events) with implicit traces (revealing activities not deliberately logged), investigators can construct a comprehensive timeline even when faced with incomplete logging or deliberate anti-forensic measures, recognizing that the absence of traces may simply reflect system design limitations rather than absence of activity.

Marking Guide

Explicit traces explanation (2 marks)

2 marks: Clear definition emphasizing deliberate design/programming for recording events

- Example: "Explicit traces are direct records deliberately created as part of normal system operation for the specific purpose of documenting events. They exist only because systems were programmed to record them, such as log files, database transaction records, and email headers."

1 mark: Basic definition without addressing system design requirements

- Example: "Explicit traces are records like logs and database entries that show system activity."

0 marks: Incorrect or missing definition

Implicit traces explanation (2 marks)

2 marks: Clear definition emphasizing their nature as by-products requiring interpretation

- Example: "Implicit traces are indirect artifacts that weren't created for documentation purposes but exist as by-products of system operations. They require forensic interpretation to become meaningful evidence, such as deleted file fragments, cache artifacts, memory remnants, and temporary files."

1 mark: Basic definition without addressing interpretive requirements

- Example: "Implicit traces are things like deleted files and cache data that weren't meant to be logs."

0 marks: Incorrect or missing definition

Comparison of system design requirements (2 marks)

2 marks: Detailed comparison addressing how system design decisions impact trace availability

- Should explain that explicit traces only exist if specifically programmed into the system, while implicit traces exist as side effects of operations but their persistence depends on system configuration. Should address how design choices (what to log, how long to retain data, etc.) directly determine what evidence will be available during an investigation.

1 mark: Basic comparison without addressing design implications

0 marks: No comparison of system design considerations

Case scenario application (3 marks)

3 marks: Comprehensive scenario with specific examples showing how system design affects available evidence

- Should include concrete examples of both trace types in context of unauthorized access, demonstrate understanding of limitations (e.g., if logging is disabled), and show how different types of system artifacts might reveal different aspects of the incident.

2 marks: Good scenario with limited examples of both trace types

1 mark: Basic scenario without addressing design considerations

0 marks: No scenario application

Integration explanation (1 mark)

1 mark: Clear explanation of how the trace types complement each other, acknowledging design limitations

- Should explain how explicit traces provide reliable documentation where available, while implicit traces fill gaps where logging was insufficient or disabled. The explanation should acknowledge that neither type alone provides a complete picture, and that correlation between types strengthens the overall forensic conclusion.

0 marks: No explanation of the complementary relationship

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)

Solution:

Model Answer:

Digital forensic practitioners in New Zealand face significant jurisdictional challenges when investigating systems with distributed data. Cloud services often store data across multiple countries, creating uncertainty about which country's laws apply. Determining where data "is" located becomes conceptually difficult with distributed systems, and service providers without physical presence in New Zealand may not consider themselves bound by New Zealand orders.

The Dotcom case (2014) fundamentally changed New Zealand's approach to international digital evidence sharing. When authorities seized electronic devices from Kim Dotcom's residence and intended to send complete forensic copies to US authorities without filtering, the Supreme Court established a crucial precedent: sending entire digital device clones overseas without first filtering for relevance was unlawful. This landmark ruling established that digital searches require specific authorization due to their intrusive nature, and that law enforcement must separate relevant material from irrelevant personal information before sharing evidence internationally.

Currently, New Zealand authorities address these challenges through Mutual Legal Assistance Treaties (MLATs), production orders served to local offices of international companies, and cooperation through organizations like INTERPOL. The Search and Surveillance Act's definition of "remote access search" (Section 132) provides some framework but remains problematic for cross-border investigations.

New Zealand has signed the Budapest Convention on Cybercrime, with alignment legislation currently before Parliament (expected report by April 2025). This international treaty will streamline cooperation between signatory countries, establishing standardized procedures for accessing digital evidence across borders while respecting sovereignty and privacy protections, significantly enhancing New Zealand's capability to address jurisdictional challenges.

Answer Guide:

A comprehensive answer should address:

Introduction and Context (2 marks)

- **2 marks**: Clear introduction that identifies key jurisdictional challenges in digital forensics with specific reference to cloud and distributed systems

- **1 mark**: Basic introduction with limited identification of jurisdictional challenges
- **0 marks**: No clear introduction or failure to identify jurisdictional challenges

Analysis of the Dotcom Case (3 marks)

- **3 marks**: Comprehensive analysis of the Dotcom case, explaining how it established principles for international sharing of digital evidence, with specific reference to privacy concerns and requirements for filtering relevant material
- **2 marks**: Adequate explanation of the Dotcom case with some connection to international evidence sharing
- **1 mark**: Minimal reference to the Dotcom case without clear explanation of its significance
- **0 marks**: No mention of the Dotcom case

Current International Cooperation Mechanisms (2 marks)

- **2 marks**: Correctly identifies international cooperation mechanisms (MLATs, INTERPOL, production orders) with basic description of their purpose
- **1 mark**: Basic mention of at least one cooperation mechanism
- **0 marks**: No mention of international cooperation mechanisms

Budapest Convention Discussion (2 marks)

- **2 marks**: Mentions the Budapest Convention and indicates its potential future impact on cross-jurisdictional investigations
- **1 mark**: Basic mention of the Budapest Convention
- **0 marks**: No mention of the Budapest Convention

Reference to Relevant Legislation and Cases (1 mark)

- **1 mark**: Appropriate references to New Zealand legislation (Search and Surveillance Act, Privacy Act) and relevant cases
- **0 marks**: No reference to relevant legislation or cases

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)

Solution:

Marking Guide for Acquisition Methods Question

Model Answer (Full Marks)

The lecture notes describe two primary acquisition types: static and live. Static acquisition occurs when the system is powered off, while live acquisition is performed with the system running. These represent fundamentally different approaches with distinct advantages.

Static acquisition provides complete access to storage media without interference from active processes, ensuring a stable data environment. This approach allows access to system files that might be locked during operation and prevents contamination by halting processes that might alter data. However, it sacrifices volatile data such as RAM contents, running processes, and network connections. Static acquisition requires hardware or software write blockers to prevent data modification and careful configuration of BIOS/UEFI settings to boot from forensic media like Kali Linux, CAINE, or Mini WinFE.

Live acquisition preserves volatile data but risks evidence contamination as the system continues to operate. The acquisition software itself changes the system state by consuming resources. This approach is typically used when critical evidence exists in RAM or when the system cannot be taken offline.

When limited by time constraints, the lecture identifies two specialized acquisition methods: 1. Logical acquisition - captures only specific files of interest to the case 2. Sparse acquisition - collects fragments of unallocated deleted data

These methods "trade comprehensiveness for speed and efficiency" as the lecture explicitly states, and are appropriate when complete disk imaging isn't feasible or necessary.

The lecture outlines four specific collection methods: 1. Physical disk to image file - creating a bit-by-bit copy (most common, offering "greatest flexibility") 2. Physical disk to disk copy - an alternative when imaging isn't possible 3. Partition to partition copy - copying specific partitions 4. Partition to data file - simple file copying (typically in live situations)

Four key considerations influencing acquisition method choice are explicitly identified: 1. Size of the suspect's disk (storage requirements) 2. Whether the original disk can be retained as evidence for later examination 3. Time available for acquisition 4. Location and accessibility of the evidence

SSDs present unique forensic challenges compared to HDDs. The lecture explains that SSDs use NAND flash memory rather than magnetic platters, with fundamentally different data structures. Three critical SSD technologies impact forensic acquisition: 1. TRIM - allows the OS to inform the SSD which blocks are no longer in use 2. Garbage collection - consolidates and erases blocks with deleted data 3. Wear leveling - distributes writes across memory cells

These technologies mean that "unlike with HDDs where deleted file data often remains untouched until overwritten, SSD deleted data may be completely unrecoverable after periodic maintenance." The lecture specifically advises that "it's critical to disable TRIM before acquisition when possible, or to acquire the drive as quickly as possible after it's been secured."

When selecting an acquisition method, the appropriate choice depends on the specific investigation circumstances. Static acquisition with physical disk imaging is preferred when preserving all potential evidence and the system can be taken offline. Live acquisition is necessary when volatile data is critical or when system downtime is unacceptable. Logical acquisition is appropriate for targeted collection of known relevant files when time or storage is limited. Sparse acquisition offers a middle ground when deleted data is of primary interest but full acquisition isn't feasible. For SSDs, immediate acquisition upon securing the device is crucial to prevent evidence loss through automated maintenance processes.

- **Comparison of acquisition types (6 marks)**
  - 6 marks: Thoroughly compares static vs. live acquisition as described in Section 3.2 AND clearly explains logical and sparse acquisition methods, noting they "trade comprehensiveness for speed and efficiency" as stated in the lecture
  - 3 marks: Adequately compares some methods but misses key distinctions or omits logical/sparse acquisition
  - 0 marks: Incorrect or superficial comparison
- **Collection methods and key considerations (5 marks)**
  - 5 marks: Correctly identifies the four collection methods from Section 3.2: "Physical disk to image file, Physical disk to disk copy, Partition to partition copy, Partition to data file" AND correctly lists all four considerations influencing method choice: "size of the suspect's disk", "whether you can retain the original disk as evidence", "time available for acquisition", and "location and accessibility of the evidence"
  - 3 marks: Identifies some methods and considerations but not all
  - 0 marks: Fails to identify methods and considerations from the lecture
- **SSD vs. HDD acquisition challenges (5 marks)**

  - 5 marks: Accurately explains SSD challenges as presented in Section 3.5, including TRIM, garbage collection, and wear leveling; explains how these technologies impact forensic acquisition differently from HDDs; correctly notes that "unlike with HDDs where deleted file data often remains untouched until overwritten, SSD deleted data may be completely unrecoverable after periodic maintenance"
  - 3 marks: Mentions some SSD challenges but lacks comprehensive understanding from lecture
  - 1 mark: Minimal mention of SSD vs. HDD differences
  - 0 marks: No discussion of SSD vs. HDD considerations
- **Application of understanding (4 marks)**
  - 4 marks: Demonstrates clear understanding of when each acquisition method would be most appropriate based on the lecture; shows understanding of how acquisition planning differs between approaches
  - 2 marks: Shows basic understanding of application but lacks depth
  - 0 marks: No demonstration of applied understanding

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