UNIVERSITY OF ESWATINI

Faculty of Science and Engineering

Department of Computer Science

MAIN EXAMINATION

October 2021

Title of Paper: Digital Forensics

Course Code: CSC 464

Time Allowed: 3 Hours **Total Marks:** 100

Instructions to Candidates:

*This Question Paper Consists of **THREE (3) Questions in SECTION A** and **THREE (3) Questions in SECTION B**.*

*Answer **ALL Questions in SECTION A** and **ONE (1) Question in SECTION B**.*

Marks are indicated in Square Brackets.

NB: You Are Not Allowed To Open This Examination Paper Until Permission Has Been Granted By The Invigilator

QUESTION ONE [35]

1.1 Describe two (2) main purposes of digital forensics.
[2]

1.2 Discus any three (3) challenges that can be encountered in digital forensics.
[3]

1.3 List three (3) main items that should be included in a case report.
[3]

1.4 Explain the concept of forensic soundness and how it can be ensured.
[5]

1.5 Briefly discus how the concept of hearsay affects digital forensic investigations.
[3]

1.6 If you had a friend who was asked to be an expert witness, what advice would you give your friend to successfully prepare for trial?
[3]

1.7 Suppose you are involved in the analysis phase of an investigation of a cyberattack. All potentially relevant data objects have been collected and examined. In order to proceed, what do you need to ensure with regard to the evidence integrity and authenticity? How will you do this, and why?
[4]

1.8 Why is the order of volatility important when collecting digital evidence? [2]

1.9 State and explain the five (5) main principles of digital forensics.
[5]

1.10 Describe the criteria that should be followed when evaluating electronic evidence.

[5]

QUESTION TWO [25]

2.1 What is a civil investigation? [1]

2.2 What is the General Data Protection Regulation (GDPR) and what is its impact on investigations involving digital data?
[3]

2.3 Briefly discus the guiding factor(s) for investigators when conducting a search and seizure.

[3]

2.4 Does seizure of computer data take place in the collection phase of the digital forensic process? Explain the relation between the digital forensic process and the rules of search and seizure.

[4]

2.5 Why it is impossible for privacy law to adequately govern issues involving the use and protection of personal data.

[2]

2.6 Describe inn detail the Daubert Standard.

[5]

2.7 State the criteria that must be met to obtain a search warrant.

[2]

2.8 State five (5) ethical principles that should be followed by digital forensics investigators.

[5]

QUESTION THREE [15]

3.1 Define the following terms:

a. Due care [1]
b. Corroboration [1]
c. Nonrepudiation [1]
d. Integrity monitoring solutions[1]

3.2 Briefly describe how cell phone forensics is differs from traditional computer forensics.

[2]

3.3 Describe how accurate time synchronization can be achieved in an Enterprise Data Warehouse.

[3]

3.4 What is the benefit of gathering evidence from multiple data sources?

[2]

3.5 What would you consider when analysing a storage device?

[4]

SECTION B

QUESTION FOUR [25]

4.1 What difficulties are associated with investigating Advanced Persistent Threats (ATPs)?

[2]

4.2 Why may Network Address Translations (NATs) be a challenge during investigations?

[2]

4.3 What should a digital forensic practitioner take into consideration before conducting a network forensic investigation?
[3]

4.4 What digital evidence could be extracted by a digital forensics investigator from a firewall?
[3]

4.5 Describe the following phases of the intrusion kill chain:
a. Command and Control [3]
b. Exfiltration [2]

4.6 Briefly discus the steps that can be taken by an organization to remediate risk once an intrusion has been detected.
[4]

4.7 Describe any three (3) Indicators of Compromise that can be used by a digital forensic investigator when an ATP occurs.
[3]

4.8 Briefly describe the type of data that can be obtained from the Windows Registry. [3]

QUESTION FIVE [25]

5.1 State three (3) types of media that can be found on a mobile device.
[3]

5.2 List four (4) types of information that can be extracted from Internet browsers of mobile devices.
[4]

5.3 Describe the processing phase of mobile devices.
[4]

5.4 State and explain three (3) investigation methods that can be used when carrying out a mobile forensic investigation.
[6]

5.5 What challenges can be encountered when conducting a mobile device forensics investigation?
[3]

5.6 The handling of evidence is an important consideration. The crime scene investigator has found a phone on the scene of crime, and suspects that there is crucial evidence in the phone. The phone seems to have some droplets inside the cracked screen. He hands you the phone, and says that due to the importance of the digital evidence, you should acquire the data first, and then the other forensic experts will look for fingerprints and biological traces after you are finished. How should you handle the device? What should you do in order to minimize the health hazards? And how to minimize the impact you leave on the other traces? [5]

QUESTION SIX [25]

6.1 List the steps that should be followed by an investigator during the acquisition phase when analysing a computer system.
[3]

6.2 Briefly describe the difference between a physical copy and a logical copy.
[2]

6.3 State two (2) reasons for performing the second hash calculation.
[2]

6.4 Describe the triaging technique.
[4]

6.5 State eight (8) artifacts that can be obtained from Internet browsers during a digital forensic investigation.
[4]

6.6 A single date or time on a system can be unreliable given the many ways that they can be manipulated or even updated through the normal course of the operating system's functions. What type of analysis can be used to corroborate the accuracy of an event's timestamp? What other evidence might be identified from this technique?
[4]

6.7 State two (2) challenges that can be encountered when acquiring data from a cloud or a remote storage.
[2]

6.8 Describe the process for handling mass data. [3]

6.9 List four (4) background evidence that can be obtained from computer systems during an investigation. [2]