Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
COURSE/PROGRAMME TITLE: CNS
END OF SEMESTER EXAMINATION
CNS: 42013-DIGITAL FORENSICS

DATE: 28th July 2023 Time: 13:00-15:00

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One

1. The main goal of computer forensics is to _____ data
   a. Identify
   b. Analyze
   c. Preserve
   d. Collect
   e. All of these

2. Hashing, filtering, and file header analysis make up which function of digital forensics tools?
   a. Validation and verification
   b. Acquisition
   c. Extraction
   d. Reconstruction

3. Hash values are used for which of the following purposes? (Choose all that apply.)
   a. Determining file size
   b. Filtering known good files from
   potentially suspicious data
   c. Reconstructing file fragments

d. Validating that the original data hasn't changed

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

5. Which of the following represents known files you can eliminate from an investigation? (Choose all that apply.)

a. Any graphics files

b. Files associated with an application

c. System files the OS uses

d. Any files pertaining to the company

6. For which of the following reasons should you wipe a target drive?

a. To ensure the quality of digital evidence you acquire

b. To make sure unwanted data isn't retained on the drive

c. Neither of the above

d. Both a and b

7. After you shift a file's bits, the hash value remains the same. True or False?

8. The National Software Reference Library provides what type of resource for digital forensics examiners?

a. A list of digital forensics tools that make examinations easier

b. A list of MD5 and SHA1 hash values for all known OSs and applications

c. Reference books and materials for digital forensics

d. A repository for software vendors to register their developed applications

9. Which of the following is NOT an artifact that will be irrevocably lost if the computer is shut down?

a. Running processes
b. Open network ports
c. Data stored in memory
d. System date and time

10. What is used to validate the tools and verify the evidence integrity?
    a. hashing algorithms
    b. steganography
    c. watermarks
    d. digital certificates
11. Choose the term which describes Digital forensics.
    a. Science of collecting and analyzing evidence
    b. process of Chasing the criminal
    c. Process of punishing the culprit
    d. preservation filtering and organization of evidence
12. E-mail headers contain which of the following information? (Choose all that apply.)
    a. The sender and receiver e-mail addresses
    b. An ESMTP number or reference number
    c. The e-mail servers the message traveled through to reach its destination
    d. The IP address of the receiving server
    e. All of the above

13. When you access your e-mail, what type of computer architecture are you using?
    a. Mainframe and minicomputers
    b. Domain
    c. Client/server
    d. None of the above

14. Phishing does which of the following?
    a. Uses DNS poisoning
    b. Lures users with false promises
    c. Takes people to fake Web sites
    d. Uses DHCP

15. An expert witness can give an opinion in which of the following situations?
    a. The opinion, inferences, or conclusions depend on special knowledge, skills, or training not within the ordinary experience of laypeople.
    b. The witness is shown to be qualified as a true expert in the field.
    c. The witness testifies to a reasonable degree of certainty (probability) about his or her opinion, inference, or conclusion.

d. All of the above

16. Which of the following describes fact testimony?

a. Scientific or technical testimony describing information recovered during an examination

b. Testimony by law enforcement officers

c. Testimony based on observations by lay witnesses

d. None of the above

17. Using Autopsy as a reference, describe two major features of forensics tools that an examiner can use to perform analysis of evidence.

(4 Marks)

Total (20 Marks)

Question Two

i. Briefly state Locard's principle and its relevance to Digital Forensics.

(2 Marks)

ii. Within the context of Locards exchange principle, explain any FOUR windows registry hives and the evidence that can be gathered from them.

(8 Marks)

iii. The following are types of digital evidence that can be found on a computer. Classify them as being either user-generated or machine-generated.

(3 Marks)

a) Browser data (browser history, cookies, download history)
b) Account details (username, picture, password)
c) GPS coordinates of a specific photo
d) Audio and video files
e) Computer logs.
f) Address book and calendar

iv. Explain how you will handle the case using the General Forensics Analysis Process.

(7 Marks)

Total (20 Marks)

Question Three

i. Discuss three challenges related to acquiring digital evidence. How can modern digital forensics tools overcome these challenges?

(6 Marks).

ii. List 2 different ways in which data is represented in a computer.

(2 Marks)

iii. Why is hexadecimal representation commonly used in digital forensics tools?

(2 Marks)

iv. Explain the role of the following concepts in digital forensics by describing two different types of crimes each that can use them as evidence.

a) Meta data

b) Digital fingerprinting

(4 Marks)

v. When performing analysis of memory, what are some of the pieces of digital evidence that can be found and what can they reveal to an investigator? Explain 3 of them.

(3 Marks)

Total (20 Marks)

Question Four

i. Describe THREE data hiding techniques that cyber criminals can use and the techniques you would use to overcome them.

(6 Marks)

ii. List 5 types of cyber-crimes that can be investigated using digital forensics.

(5 Marks)

iii. Explain how memory analysis differs from hard disk analysis by contrasting three different types of evidence found in each.

(6 Marks)

iv. In investigating emails, what is the most important source of evidence? What does it contain that can offer forensically useful clues?

(3 Marks)

Total (20 Marks)

Question Five

i. Differentiate between public sector and private sector (corporate)investigations using examples.

(4 Marks)

ii. Discuss two tasks performed by current modern digital forensics tools.

(4 Marks)

iii. How can you validate a digital forensics software tools?

(2 Marks)

iv. Discuss three anti-forensics techniques and how they can frustrate the efforts of an examiner. (6 Marks)

v. List the main components of a forensics report.

(4 Marks)

Total (20 Marks)