SPECIFY TYPE OF EXAMINATION

FIRST ATTEMPT ☐
FIRST RESIT ☐
SECOND RESIT ☐
RE-TAKE ☐

JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF IT

2nd YEAR 1ST SEMESTER 2022/2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1208

COURSE TITLE: CRIMINALISTICS AND FORENSIC LAB.

DATE: **TIME:**

TIME: 2 HOURS

Instructions:

Answer ALL questions in Section A and B and ANY other TWO questions in Section C

Tick the most correct alternative in Section A

Answers to Questions in Section B and C must be written in the spaces provided on the question paper.

Candidates must ensure they submit their work by clicking "finish and submit attempt" button at the end.

SECTION A: 20 Marks (Each question carries 1 mark)

NB: These are <u>multiple choice questions</u> with four choices, A, B, C, and D and the candidate is supposed to tick the correct answer.

1. Which of the following statements best defines computer forensics?

A. Computer forensics is the use of evidence to solve computer crimes.
B. Computer forensics is the use of digital evidence to solve a crime.
C. Computer forensics is only used to find deleted files on a computer.
D. Computer forensics is only used to examine desktop and laptop computers.

2. The science that determines the existence and the number of drugs, poisons or toxins in body is called:

A. Forensic Pathology
B. Forensic Accounting
C. Forensic Toxicology
D. Forensic Anthropology

3. The type of digital forensics that focuses on electronic evidence related to security attacks, intrusions, worms, viruses or malware attacks is called:

A. Mobile forensics
B. Network forensics
C. Memory forensics
D. Computer forensics

4. The digital forensic subdiscipline that aims to find an evidence related to a person's location is termed:

A. Media device forensics
B. Social media forensics
C. GPS forensics
D. Computer games forensics

5. The phase in which all electronic evidence can be validated and finally prepared for the court is:

A. Preservation
B. Collection
C. Analysis
D. Presentation

6. Seizing a computer that is found in the crime scene is from:

A. The identification phase
B. The presentation phase
C. Examination phase
D. Preservation phase

7. Using a USB cable to transfer data from the original evidence to the copy machine directly is a:

A. Forensic method
B. Non forensic method
C. Semi-forensic method

8. A chain of custody (CoC) form is used to document which of the following?

A. Law enforcement officers who arrest and imprison a criminal suspect
B. A chain of letters or emails used in an investigation
C. Anyone who has been in contact with evidence in a case
D. None of the above

9. Which of the following can be of evidentiary value to a computer forensics examiner?

A. A SIM card
B. An Xbox
C. A digital camera
D. All of the above

10. Which of the following statements best describes a bit-stream imaging tool?

A. A bit-stream imaging tool produces a bit-for-bit copy of the original media.
B. A bit-stream imaging tool often provides the examiner with deleted files.
C. Neither A nor B is correct.
D. Both A and B are correct.

11. Which of the following are benefits of email evidence?

A. Email evidence generally exists in multiple areas.
B. It can often be found easier than other types of evidence.
C. It has been accepted as admissible evidence in a number of cases.
D. All of the above.

12. Which of the following statements is not true about photo images?

A. Images can possess evidence of where the suspect has been.
B. Images cannot be easily found using bit-stream imaging tools such as FTK.
C. An image can identify the make and model of the digital camera.
D. Basically just one type of digital image is used today.

13. Which of the following terms best describes the hiding, altering, or destroying of evidence related to an investigation?

A. Spoliation of evidence
B. Manipulation of evidence
C. Inculpatory evidence
D. Exculpatory evidence

14. The Computer Analysis and Response Team (CART) is a unit of which government agency?

A. USSS
B. FBI
C. CIA
D. ICE

15. Which of the following organizations is an independent body that provides forensics lab guidelines and certification?

A. ASCLD
B. ASCLD/LAB
C. ESI
D. SWGDE

16. Which of the following is not a rule of Evidence?.

A. Admissible
B. Effective
C. Authentic
D. Complete

17. Which of the following values are found in binary?

A. 0 or 1
B. 0–9 and A–F
C. 0–9
D. A–F

18. What is the name of the non-volatile storage that can generally not be modified and is involved in the boot process?

A. RAM
B. Flash memory
C. Partition
D. ROM

19. Which of the following best describes the information contained in the MFT?

A. File and folder metadata
B. File compression and encryption
C. File permissions
D. All of the above

20. Which of the following Windows features allows the user to extend virtual memory using a removable flash device?

A. BitLocker
B. Volume Shadow Copy
C. ReadyBoost
D. Backup and Restore

SECTION B: 30 Marks

A<u>ttempt all questions</u> in this section. Answers to questions in this section must be written in the spaces provided. Answers must be precise and concise.

a) What information must be included in any notes taken at the crime scene? (2 marks)

b) List any two criminal activities that take place on Dark Web marketplaces and state why they have been so successful (3 marks)

c) What is the first critical step in crime-scene investigation? Why is this step so important? (4 marks)

d) What are the possible consequences of failing to maintain a proper chain of custody? (4 marks)

e) List three common types of digital crime (3 marks)

f) List the three methods of crime-scene recording. (3 marks)

g) Explain the difference between law enforcement agency and corporate investigations (3 marks)

h) List the main functions of the forensic scientist. (2 marks)

i) What is meant by ‘Locard’s exchange principle’? (2 marks)

j) How does the testimony of an expert witness differ from the testimony of a lay witness? (2 marks)

k) Digital evidence requires three basic elements that are necessary during the collection. Identify any two of these elements. (2 marks)

SECTION C:20 Marks

There are a total of three (3) questions, each carrying ten (10) marks. You are expected to answer any two (2) questions.

1. Write brief explanations for the following:

i) What is evidence bag? [2 Marks]

ii) Why should your evidence be “write protected”? [2 Marks]

iii) What should be on an evidence control from? [2 Marks]

iv) Forensic toxicology [2 Marks]

v) Finger – Print technology [2 Marks]

2. Briefly describe the five standard steps for computer investigations [10 Marks]

3. a) What is a standard/reference sample and why is it important to the criminalist? [2 marks]

b) List the types of computer investigations typically conducted in the corporate environment. [3 marks]

b) When cases go for trial, you as the forensics expert can either be a technical witness or an expert witness. With examples, explain the two roles. [5 Marks]