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

4th YEAR 1ST SEMESTER 2022/2023 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1407

COURSE TITLE: CYBERCRIME INVESTIGATIONS

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 multiple choice questions with four choices, A, B, C, and D and the candidate is supposed to tick the correct answer.

1. Which of the following is not a type of cyber crime?

A. Data theft

B. Forgery

C. Damage to data and systems

D. Installing antivirus for protection

2. Police departments have:

A. Reactive functions

B. Proactive functions

C. All of the above

D. None of the above

3. Key logger is a

A. Firmware

B. Antivirus

C. Spyware

D. All of the above

4. Cyber-laws are incorporated for punishing all criminals only.

a) True

b) False

5. What is the weakest link in cybersecurity?

A. Weak encryption.

B. Humans.

C. Short passwords.

D. Open doors

6. ------- are attempts by individuals to obtain confidential information from you to falsifying their identity.

A. Computer viruses

B. Phishing scams

C. Phishing trips

D. Spyware scams

7. All of the following are examples of traditional crimes that are now committed in the cyber space except for:

A. Bullying

B. Battery

C. Embezzlement

D. Fraud

8. All of the following are myths about cybersecurity except for:

A. Cybercrime can be prevented with virus protection software

B. When caught, cybercriminals go to prison

C. Most cybercriminals are skilled hackers

D. When caught, cybercriminals usually plead guilty and do not go to trial

9. Which of the following is not a challenge to tackling Cybercrime?

A. Scale

B. Anonymity

C. Global reach

D. None

10. The Altering of data so that it is not usable unless the changes are undone is

A. Biometrics

B. Encryption

C. Ergonomics

D. Compression

11. All of the following regarding sentencing patterns of cybercriminals are true, except for:

a) When convicted, most cybercriminals go to jail or prison

b) Male cyber offenders receive longer prison sentences than female cyber offenders

c) Most cyber offenders go to trial and do not plead guilty

d) All of the answers are true

12. Authentication is _____

A. To assure identity of user on a remote system

B. Insertion

C. Modification

D. Integration

13. Which of the following is the correct order in the procedure in digital evidence gathering?

A. Preservation, Identification, Analysis, Documentation, Presentation.

B. Preservation, Documentation, Analysis, Identification, Presentation.

C. Presentation Identification, Preservation, Analysis, Documentation,.

D. Identification, Preservation, Analysis, Documentation, Presentation.

14. What is the first thing you should do if your company is facing ransom-ware demands?

A. Determine if ransomware demand is legitimate and follow instructions to get your data back.

B. Ignore the demands, but back up all data just in case.

C. Contact the police and do not pay the ransom.

D. Ignore and do nothing

15. The investigator has to take the following precautions while collecting evidence (which option is incorrect):

A. videotaping the scene, to document the system configuration and the initial condition of the site before arrival

B. photograph the equipment with it serial number, model number & writing schemes.

C. seeks Magistrates permission before investigating a cognizable offence

D. labelling the evidence

16. Which of the following statements is true?

A. To prevent the alteration of digital evidence during collection, first responders should first document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen.

B. If the computer is on, turning off the computer is highly recommended to preserve the connections to criminal activity.

C. If a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should not be disconnected immediately.

D. Suspect's cell phones and other wireless devices should not be switched during cybercrime investigation.

17. The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organisation is termed:

A. Cyberspace

B. Cyber stalking

C. Pornography

D. None of these

18. Which are the following is not part of cyber space:

A. Computer

B. Computer network

C. Websites

D. Calculator

19. Hacking means:

A. unauthorized attempts to bypass the security mechanisms of an information system or network.

B. use of information and communication technologies to support deliberate, repeated and hostile behaviour

C. a form of fraud or cheating of another persons' identity in which someone pretends to be someone else by assuming that person's identity.

D. to download computer data without the permission of the owner.

20. Which of the following is not done by cyber criminals?

A. Unauthorized account access

B. Mass attack using Trojans as botnets

C. Email spoofing and spamming

D. Report vulnerability in any system

SECTION B: 30 Marks

Attempt all questions in this section. Answers to questions in this section must be written in the spaces provided. Answers must be precise and concise.

1. Define the following terms:

i) Phishing (2 marks)

ii) Cyber-stalking (2 marks)

iii) Exculpatory evidence (2 marks)

iv) Cyber-terrorism (2 marks)

v) Hashing (2 marks)

2. briefly describe some tools that are commonly used in cybercrimes against individuals. (4 marks)

3. state reasons why Dark Web is synonymous with Cybercrime (3 marks)

4. How does the Internet differ from cyberspace? (2 marks)

5. State two functions of an investigation report in a court of law (2 marks)

6. Differentiate between active digital footprint and passive digital footprint.(4 Marks)

7. Explain why an investigator needs a search warrant to carry out an investigation. (2 marks)

8. state the ways in which logfiles and IP addresses can be used to track the unauthorized user in cybercrime investigation. (3 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. a) What do you understand by the expression "unauthorized access"? (2 marks)

b) Mobile forensic is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions, explain the benefits and challenges of this technology (8Marks)

2. Describe the processes involved in preserving digital evidence in a cybercrime scene (10 marks)

3. a) Briefly describe what constitutes Cybercrime in Kenyan Laws as outlined in the Cybercrimes and Computer related Crimes act 2018 (6 marks)

c) Discuss any two challenges you can face during Cyber Crime investigation process in Kenya (4 marks)