This question paper consists of TWO (2) sections. Answer ALL questions in the answer booklet provided. **[100 MARKS]**

SECTION A **(60 Marks)**

There are THIRTY (30) questions in this section. Answer ALL questions in the answer booklet provided.

1. Which of the following is **NOT** a recommended step when handling digital evidence at an electronic crime scene?

   A. Recognize and identify digital evidence
   B. Modify and alter digital evidence
   C. Label and preserve the evidence
   D. Document the scene

2. Why is it crucial to maintain power on mobile digital devices during evidence collection?

   A. To increase the storage capacity of the device
   B. To render the device unusable remotely
   C. To keep the device in a usable state
   D. To prevent the device from being activated remotely

3. What does the property of authenticity entail for evidence?

   A. It must be admissible in court with proper carriage
   B. It must be transparent in terms of biases
   C. It must be linked to the incident
   D. It must be true or false with complex documentation

4. What core ethics are expected of a Digital investigator professional?

   A. Avoid professional association with reputable individuals
   B. Perform activities and duties without ethical principles
   C. Provide service with competence and honesty
   D. Engage in any crimes or improper practices

5. What environmental conditions should be maintained in an evidence storage facility?

   A. By Freezing temperatures, low moisture, and bright sunlight
   B. High humidity, direct sunlight, and excessive heat
   C. Dry, closed system and warm temperatures
   D. Low humidity, room temperature, and secured

6. What does digital evidence include?

   A. Only information that is easily verifiable
   B. Information stored on paper and computer
   C. Tangible objects like documents and photos
   D. Anything that causes belief in the truth

7. What tasks should an analyst perform when creating a snapshot of the system run state?

   A. Disable the antivirus software
   B. Minimize fingerprints
   C. Run heavy processes to stress-test the system
   D. Unplug the network connection

8. Which Linux Live CD distributions are mentioned as well-designed for computer forensics?

   A. Ubuntu
   B. CentOS
   C. Fedora
   D. Sleuth kit

9. How can digital evidence devices be protected during collection?

   A. Exposing them to static electric current
   B. Recording data that is directly available
   C. Using proper packaging techniques
   D. Interacting with each other during packing

10. What does acquiring data using Linux Live CD distributions typically involve?

    A. Writing data to the original drive during acquisition
    B. Automatically mounting connected storage media
    C. Accessing drives that aren't mounted
    D. Using a write-blocker device

11. What is the primary purpose of putting digital evidence in anti-static materials during packing?

    A. To prevent exposure to static electricity
    B. To expose them to static electric current
    C. To prevent them from being packed and labelled
    D. To make them interact with each other

12. Why is periodic auditing important in an evidence management program?

A. To ensure the device is digitally isolated and not modified
B. To save time and resources to sustain more evidence
C. To tamper with evidence in favor of the court and chain of custody
D. To verify the effectiveness of the program over time

13. In contingency planning for image acquisitions, what measures are recommended for creating duplicate copies of evidence image files?

A. Copy only the user-accessible data, excluding system files
B. Ignore the host protected area of a disk drive
C. Make at least two images using different tools
D. Use the same tool or technique for both copies

14. What are potential drawbacks associated with remote network acquisition tools?

A. Antispyware can be configured to ignore remote access programs
B. Remote access is immune to any security configurations on the suspect's computer
C. Remote acquisition tools always trigger alarms, providing immediate notification
D. Suspects may be unable to install their security tools

15. Why is it important to maintain a chain of custody for digital evidence?

A. It establishes bias towards the investigator's findings.
B. It causes doubt about the integrity of the evidence.
C. It demonstrates the evidence was not tampered with.
D. It complicates the process of documentation.

16. When acquiring data from a live system, why is it crucial to use a write blocker?

A. To allow making changes to the original data
B. To prevent modifying the source evidence
C. To increase the acquisition time
D. To bypass any encryption present

17. What key principle relates to ensuring the party acquiring digital evidence is competent?

A. Objectivity
B. Clarity
C. Professional competence
D. Transparency

18. Why should evidence collection activities be documented thoroughly with notes and photographs?

    A. To provide too much unimportant detail
    B. To allow fabrication of false documentation
    C. To capture potential evidence that may be overlooked
    D. To draw conclusions about guilt or innocence

19. What technique can help provide transparency in the process followed during a digital forensic investigation?

    A. Using proprietary closed-source tools
    B. Relying on manual notes rather than automated logging
    C. Deleting logs after the investigation is complete
    D. Comprehensive logging at each step

20. When acquiring a disk image in a forensically sound manner, what practice should be avoided?

    A. Validating the integrity of the image
    B. Using a write blocker
    C. Storing the image read-only
    D. Altering the original data

21. What characteristic of digital evidence allows non-invasive acquisition and examination?

    A. Ease of duplication
    B. Mutable nature
    C. Physical tangibility
    D. Decay over time

22. Why should forensic examiners avoid relying solely on file extensions when analyzing digital evidence?

    A. File extensions provide absolute confirmation of file types
    B. File extensions are set manually by users
    C. File extensions can be manipulated to hide true file types
    D. Forensic tools ignore file extensions during analysis

23. What practice helps ensure integrity when acquiring evidence from a live system?

    A. Disabling antivirus software
    B. Allowing remote access during acquisition
    C. Using unverified tools
    D. Cryptographic hashing

24. Why should the impact of forensic investigation on a systems state be minimized?

A. To cover up any evidence found
B. To preserve the original data
C. To allow remote access for attackers
D. To bypass security controls

25. Which party is responsible for establishing good faith and competence in handling evidence?

A. Prosecutor
B. Defendant
C. Investigator
D. Forensic examiner

26. What practice helps confirm the authenticity of an acquired forensic image?

A. Using proprietary tools
B. Retaining the hard drive only
C. Providing vague documentation
D. Cryptographic hashing

27. Why are technical validations like hashing useful when acquiring digital evidence?

A. They detect unintentional changes
B. They bypass encryption
C. They identify suspects
D. They directly access deleted data

28. What advantage does acquiring a physical disk image have compared to a logical file and folder copy?

A. It is slower
B. It omits recoverable data
C. It always triggers antivirus alerts
D. It contains file system metadata

29. What practice helps clearly tie cryptographic hashes to the relevant evidence?

A. Using sequential generic names like Image1.img
B. Deleting hash files after verification
C. Including identifying details in hash file names
D. Storing hash files on shared media

30. Why should forensic image files be stored read-only?

A. To allow other investigators to modify them
B. To prevent alteration
C. To enable remote access
D. To facilitate easier transfer

SECTION B **(40 Marks)**

There are TWO (2) questions in this section. Answer all questions.

Question 1

Explain key considerations when collecting and preserving different types of digital evidence such as network traffic, mobile devices, and cloud environments. Provide your opinion on what happens if these considerations are ignored. (20 marks)

Question 2

What are the ethical responsibilities of a digital forensic investigator? Explain at least **FOUR (4)** key ethical guidelines that investigators should adhere to when conducting examinations and reporting findings. (20 marks)

***** END OF QUESTION PAPER *****