Total No. of Questions: 25 **Enrollment No :** ____________________

MEDICAPS UNIVERSITY

Faculty of Science

End Semester Examination May 2025

FS3EL04 Digital & Cyber Forensic Science

Programme	:	B. Sc. (Hons.)	**Branch/Specialisation**	:	FS
Duration	:	3 hours	**Maximum Marks**	:	60

Note: *All questions are compulsory. Internal choices, if any, are indicated. Assume suitable data if necessary. Notations and symbols have their usual meaning.*

Section 1 (Answer all question(s))

Marks CO BL

Q1. Web defacement is a type of cybercrime where? **1 1 2**

○ A website is overloaded with traffic ● A website's content is altered illegally
○ Data is encrypted for ransom ○ A server is shut down permanently

Q2. Which of the following is a characteristic of a logic bomb? **1 1 1**

● It activates under specific conditions ○ It replicates itself
○ It spreads through email attachments ○ It disguises itself as legitimate software

Q3. What is slack space in digital forensics? **1 2 2**

○ Unused space on a track of a hard disk ○ Unused space on a sector of a hard disk
● Unused space in a file cluster ○ A secure file encryption method

Q4. What is the primary characteristic of non-volatile digital evidence? **1 2 1**

● It persists even after power loss ○ It is stored in RAM
○ It is easily altered ○ It is temporary

Q5. What is the purpose of partitioning a hard disk? **1 3 2**

○ To increase storage capacity ● To separate different storage areas
○ To speed up processing ○ To remove malware

Q6. What is the primary purpose of a file system like FAT or NTFS? **1 3 2**

○ To store data permanently ○ To prevent unauthorized access
● To organize and manage files on a storage device ○ To encrypt data

Q7. What is the first step in the incident response process? **1 4 2**

○ Detection ○ Recovery
○ Containment ● Preparation

Q8. What is a common mistake made by first responder during an incident? **1 4 1**

○ Documenting the incident thoroughly ● Immediately shutting down the system
○ Maintaining chain of custody ○ Preserving digital evidence

Q9. Which tool is widely used for network packet analysis? **1 5 2**

○ Snipping tool ○ AutoCAD
○ ISP ● Wireshark

Q10. What is the purpose of a write-blocker in digital forensics? **1 5 1**

● To prevent data alteration ○ To encrypt data
○ To recover deleted files ○ To analyze network traffic

Section 2 (Answer any 2 question(s))

Marks CO BL

Q11. Define cybercrime. Explain its different types with suitable examples. 5 1 2

Rubric	Marks
Definition of cybercrime.	1
Any four types of cybercrime with proper explanation.	4

Q12. Describe the role of hacking in cybercrime and its different types. 5 1 3

Rubric	Marks
Definition of hacking	1
Any 3 types of hacking.	4

Q13. What are some standard prevention measures for cybercrimes? 5 1 3

Rubric	Marks
any 5 standard prevention measures	5

Section 3 (Answer any 2 question(s))

Marks CO BL

Q14. Discuss the admissibility of digital evidence in court and its challenges. 5 2 2

Rubric	Marks
Legal act for admissibility of digital evidence.	3
Challenges of admissibility of digital evidence in court	2

Q15. Define digital evidence and explain its types. 5 2 1

Rubric	Marks
Definition of digital evidence.	1
Types of digital evidence.	4

Q16. Describe the role of routers, hubs, and switches in digital forensics. 5 2 3

Rubric	Marks
Description of the role of routers, hubs, and switches.	5

Section 4 (Answer any 2 question(s))

Marks CO BL

Q17. What are the differences between FAT and NTFS file systems? 5 3 3

Rubric	Marks
5 differences between FAT and NTFS file systems	5

Q18. Describe the basic structure of a hard disk with a well labelled diagram. 5 3 3

Rubric	Marks
structure of a hard disk	3
well labelled diagram.	2

Q19. Discuss forensic techniques for recovering deleted data. **5 3 3**

Rubric	Marks
Tools or procedures for recovering deleted data.	5

Section 5 (Answer any 2 question(s))

Marks CO BL

Q20. Describe the steps involved in the incident response methodology. **5 4 3**

Rubric	Marks
Procedure or steps for incident response	5

Q21. Analyze the challenges faced during incident investigation. **5 4 2**

Rubric	Marks
Any five challenges.	5

Q22. Differentiate between containment and eradication in incident response. **5 4 3**

Rubric	Marks
Any five differences.	5

Section 6 (Answer any 2 question(s))

Marks CO BL

Q23. Discuss various cyber forensic tools and their applications in digital forensics. **5 5 3**

Rubric	Marks
any five tools with their applications.	5

Q24. Explain the challenges and limitations of using cyber forensic tools in real-world cases. **5 5 2**

Rubric	Marks
Any five challenges and limitations.	5

Q25. Explain the process of network traffic analysis using Wireshark. **5 5 3**

Rubric	Marks
The procedure of network traffic analysis using Wireshark	5

******