Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrolment No.....

Faculty of Science

End Sem Examination May-2024

FS3EL04 Digital & Cyber Forensic Science

Programme: B.Sc. (Hons.) Branch/Specialisation: Forensic Science

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Computers can be involved in which of the following types of crime: **1**

(a) Sexual assault
(b) Identity theft or intellectual property theft
(c) Civil disputes
(d) All of these

ii. Computer forensics involves all of the following stated activities except: **1**

(a) Extraction of computer data
(b) Manipulation of computer data
(c) Preservation of computer data
(d) Interpretation of computer data

iii. The volatile memory of the computer is known as: **1**

(a) RAM (b) ROM (c) BIOS (d) All of these

iv. A valid definition of digital evidence is; **1**

(a) Data stored or transmitted using a computer
(b) Information of probative value
(c) Digital data of probative value
(d) Any digital evidence on a compute

v. The areas of files and disks that are not apparent to the user, and sometimes not even to the operating system, is termed: **1**

(a) Latent data (b) Hidden data
(c) Exceptional data (d) Missing data

vi. The most common storage device for the personal computer is the: **1**
(a) Floppy disk (b) Hard disk drive
(c) Zip disk (d) USB thumb drive

vii. In file digital forensics, MAC is important because: **1**
(a) Modified, accessed and created are key concepts in files and recorded by F system.
(b) The maximum Access Control list is used to say what a person can access on the NTFS
(c) The MAC address is necessary to connect to the server to download the files
(d) Mac and cheese are important to keep us fed and working

viii. Incident response is a vast field encompassing actions that take place: **1**
(a) Only before attack (b) Before, during and after an attack
(c) Only during attack (d) Only after attack

ix. The most popular software forensic tools include all of the following except: **1**
(a) Quicken (b) Forensic autopsy
(c) Forensic toolkit (d) All of these

x. A set of instructions compiled into a program that performs a particular task is known as: **1**
(a) Hardware (b) Software
(c) Both (a) and (b) (d) Cryptoware

Q.2 i. Define cybercrime and its prevention measures. **4**
ii. Write a note on: **6**
(a) Packet sniffing
(b) Malicious codes including trojans
(c) Logic bombs
OR iii. Write a note on: **6**
(a) Viruses (b) Online based cyber crimes
(c) Phishing and its variants

Q.3 i. Explain digital evidence with types of digital evidence. **4**
ii. Point out difference between digital evidence and physical evidence. **6**
OR iii. Discuss about volatile and non-volatile digital evidence. **6**

Q.4 i. Who is computer forensic expert? Discuss about goals of the forensic investigation. **4**
ii. Discuss the steps taken in cyber forensic investigation. **6**
OR iii. What is computer forensic? Point out the need of computer forensic. **6**

Q.5 i. Explain incident response process. **4**
ii. Describe role of first responder officer and common mistakes of first responder officer. **6**
OR iii. Write a note on: **6**
(a) Overview of pre-incident preparation
(b) Identifying risk after detection of an incident.

Q.6 Attempt any two:
i. Explain the working procedure of Sleuth Kit. **5**
ii. Explain the working procedure of forensic autopsy. **5**
iii. How to analyse the physical and logical data of a device using forensic toolkit? Explain the procedure. **5**

******

Marking Scheme

Digital & Cyber Forensic Science (T) - FS3EL04 (T)

Q.1	i)	**d) All of the above**		**1**
	ii)	**b) Manipulation of computer data**		**1**
	iii)	**a) RAM**		**1**
	iv)	**c) Digital data of probative value**		**1**
	v)	**d) Missing data**		**1**
	vi)	**b) Hard disk drive**		**1**
	vii)	**c) The MAC address is necessary to connect to the server to download the files**		**1**
	viii)	**d) Only after attack**		**1**
	ix)	**a) Quicken**		**1**
	x)	**b) Software**		**1**
Q.2	i.	Definition –	1 Marks	**4**
		prevention measures –	3 Marks	
	ii.	A) Packet Sniffing -	2 Marks	**6**
		B) Malicious Codes including Trojans –	2 Marks	
		C) Logic Bombs –	2 Marks	
OR	iii.	A) Viruses -	2 Marks	**6**
		B) Online based Cyber Crimes –	2 Marks	
		C) Phishing and its variants –	2 Marks	
Q.3	i.	Intro of digital evidence –	1 Marks	**4**
		3 types of digital evidence –	3 Marks	
	ii.	of each difference	1 Marks	**6**
OR	iii.	Volatile evidence –	3 Marks	**6**
		Non-Volatile evidence –	3 Marks	
Q.4	i.	Intro of expert-	2 Marks	**4**
		Goals –	2 Marks	
	ii.	for each step	1 Marks	**6**
OR	iii.	Definition of computer forensic –	2 Marks	**6**
		Need of computer forensic –	4 Marks	
Q.5	i.	4 step Process –	4 Marks	**4**
		Ref TRP	1 Marks	
		Steps /Process	3 Marks	
	ii.	role of first responder officer –	3 Marks	**6**
		Common Mistakes of first responder officer –	3 Marks	
OR	iii.	A) Overview of Pre-incident Preparation –	3 Marks	**6**
		B) Identifying risk after detection of an incident –	3 Marks	
Q.6		Attempt any two:		
	i.	Working procedure of Sleuth kit –		**5**
		Definition -	1 Marks	
		Working Process -	3 Marks	
		Advantage and Disadvantage -	1 Marks	
	ii.	Working procedure of autopsy –		**5**
		Definition -	1 Marks	
		Working Process -	3 Marks	
		Advantage and Disadvantage -	1 Marks	
	iii.	Working procedure of FTK –		**5**
		Definition -	1 Marks	
		Working Process -	3 Marks	
		Advantage and Disadvantage -	1 Marks	

******