Total No. of Questions: 6 *Total No. of Printed Pages:2*

Enrollment No.....

Faculty of Engineering
End Sem Examination Dec-2023
IT3EL11 Cyber Security & Forensics

Programme: B.Tech. Branch/Specialisation: IT

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. Which malware does not replicate or clone through an infection? **1**
(a) Trojans (b) Worms (c) Rootkits (d) Virus

ii. Identify the term which denotes that only authorized users can access the information? **1**
(a) Confidentiality (b) Availability
(c) Integrity (d) Non-repudiation

iii. Which of the following is a type of cyber security? **1**
(a) Cloud Security (b) Network Security
(c) Application Security (d) All of these

iv. Computer forensics, also known as- **1**
(a) Digital forensic science
(b) Computer crime
(c) Computer forensic science
(d) Computer forensics investigations

v. What are the difficulties in handling Digital Evidence? **1**
(a) Easy to destroy (b) Easy to sustain
(c) Hard to get (d) Both (a) and (b)

vi. Which of the following is NOT a category of digital evidence? **1**
(a) Network Logs (b) Emails
(c) Eyewitness testimony (d) Social Media posts

vii. Which of the following is a commonly used mobile forensic tool **1**
(a) Fingerprint scanner
(b) Bloodstain pattern analysis Kit
(c) DNA Sequencing machine
(d) Cellebrite

viii. How many Digits are in the string IMSI numbers? **1**
(a) 15 (b) 16 (c) 17 (d) 18

ix. Section 66F of IT Act deals with- **1**
(a) Cyber stalking (b) Email bombing
(c) Child pornography (d) Cyber terrorism

x. In cyber law terminology DDoS means- **1**
(a) Distributed Denial of Services
(b) Disc Operating system
(c) Distant Operating services
(d) None of these

Q.2 i. Define cyber security importance. **2**

ii. Define computer vs network security. **3**

iii. What is CIA triad? Explain importance of CIA in cyber security. **5**

OR iv. List out the types of cyber crime and discuss chain of custody. **5**

Q.3 i. What are the critical steps involved in preserving digital evidence? **4**

ii. Explain seizure methodology, with diagram and example. **6**

OR iii. List out types of digital evidence with example. **6**

Q.4 i. Discuss principle of digital forensics. **4**

ii. Explain digital forensics dimensions. Also discuss application tools. **6**

OR iii. Explain Investigation models? How scientific method in digital investigation is more feasible? **6**

Q.5 i. Define ram dumping with example. **3**

ii. What are the live forensic tools? Explain network forensic tools in detail. **7**

OR iii. Discuss source of mobile evidence. Briefly describe mobile forensic tools. **7**

Q.6 Write short note on any two:

i. Cyber investigative roles **5**

ii. Application of digital forensic **5**

iii. Cyber crime prevention **5**

******

Marking Scheme
Cyber Security & Forensics (T) - IT3EL11 (T)

Q.1	i)	a) Trojans	**1**
	ii)	b) Availability	**1**
	iii)	All the above	**1**
	iv)	Computer forensics science	**1**
	v)	Both (a) & (b)	**1**
	vi)	c) Eyewitness testimony	**1**
	vii)	a) Fingerprint scanner	**1**
	viii)	a) 15	**1**
	ix)	c) Child Pornography	**1**
	x)	a) Distributed Denial of Services	**1**

What are the difficulties in handling Digital Evidence?
a) Easy to destroy

Q.2	i.	Define Cyber Security Importance	1 Mark	**2**
		Define and example of importance	1 Mark	
	ii.	Define Computer vs Network security	1 Mark	**1+2**
		Definition and example	2 Marks	
	iii.	What is CIA triad	2 Marks	**2+3**
		Importance of CIA in cyber security.	3 Marks	
OR	iv.	List out the types …….Custody	2 Marks	**2+3**
		All type of cyber crime ……. explain	3 Marks	
Q.3	i.	List all the steps with detailed explanation	(As per explanation)	**7**
	ii.	Define Seizure	2 Marks	**2+2+2**
		Methodology	2 Marks	
		Diagram	2 Marks	
OR	iii.	List …… with example	(As per explanation)	**6**

Q.4	i.	Discuss Principle of Digital Forensics	1 Marks	**1+3**
		Explain and point out all the principle	3 Marks	
	ii.	Explain Digital Forensics Dimensions	3 Marks	**3+3**
		Also discuss application tools	3 Marks	
OR	iii.	Explain Investigation Models	3 Marks	**3+3**
		Scientific Method ….. feasible	3 Marks	
Q.5	i.	Define Ram Dumping with example	1 Marks	**1+2**
		Definition and example	2 Marks	
	ii.	What are the Live Forensic Tools	2 Marks	**2+5**
		Explain Network Forensic Tools in details	5 Marks	
OR	iii.	Discuss Source of Mobile … Forensic Tools	3 Marks	**3+4**
		Define mobile ……. forensics	4 Mark	
Q.6		Attempt any two:		
	i.	List all possible roles [7 points]		**5**
	ii.	Mention all the application serial [8 points]		**5**
	iii.	Stepwise mention [10 points]		**5**

******