

Enrollment No.....



Faculty of Science
End Sem Examination Dec 2024
FS3SE07 Digital & Fraud Investigation

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.

		Marks	BL	PO	CO	PSO
Q.1	i. Which of the following is not a common type of cyberattack?	1	1	1,4	1	
	(a) Phishing					
	(b) DDoS (Distributed Denial of Service)					
	(c) Social engineering					
	(d) GPS tracking					
	ii. Which of the following is an example of a social engineering attack?	1	1	1,4	1	
	(a) Installing antivirus software					
	(b) Sending spam emails					
	(c) Tricking someone into revealing their password					
	(d) Updating computer firmware					
	iii. Which layer changes bits into electromagnetic signals?	1	1	1,4	2	
	(a) Session layer					
	(b) Data link layer					
	(c) Physical layer					
	(d) Transport layer					
	iv. Which of the protocols provides connection-oriented transmission?	1	1	1,4	2	
	(a) UDP					
	(b) TCP					
	(c) OSPF					
	(d) IS					

[2]				
v.	In data recovery logical extraction of data involves-	1	3	1,4 3
	(a) Recovering data data from allocated space			
	(b) Recovering data data from allocated and unlocated space			
	(c) Recovering data from secondary storage			
	(d) None of these			
vi.	Which social media tool is used to identify sentiments of the public on a specific topic?	1	3	1,4 4
	(a) Tin eye (b) Yandex			
	(c) Google search (d) Social searcher			
vii.	What data can be extracted from a mobile device?	1	4	1,4 3
	(a) SMS Logs (b) Call Logs			
	(c) Images (d) All of these			
viii.	In social media forensics, what is metadata-	1	1	1,4 4
	(a) The content of social media posts			
	(b) The time and date a post was made			
	(c) The total number of likes on a post			
	(d) The post's location on the internet			
ix.	Which of the following is an example of a malware attack?	1	1	1,4 1
	(a) Sending fraudulent emails to steal login credentials			
	(b) Installing a firewall to protect a network			
	(c) Physically stealing a computer			
	(d) Running a software update			
x.	Which tool is used to recover data from a mobile device?	1	1	1,4 5
	(a) UFED (b) Oxygen			
	(c) Both (a) and (b) (d) None of these			
Q.2	i. What is eavesdropping and salami attack?	2	1	1,4 1
	ii. What is the function of TC, IP and UDP protocol in the OSI model?	3	1	1,4 1
	iii. What are the different sections of the IT Act that can be used to punish cybercrime? Explain any five.	5	1	1,4 1
OR	iv. What are various types of cyber-attacks? Explain in detail.	5	1	1,4 1
Q.3	i. What is spoofing and internet time theft?	2	1	1,4 2

[3]				
	ii. What is WEP and WPA in Wi-Fi security? Explain different types of WEP and WPA authentication methods.	8	1	1,4 2
OR	iii. Explain the seven layer OSI model in detail.	8	1	1,4 2
Q.4	i. Define the following: (a) Cell phone forensic (b) Computer forensic (c) Network forensic	3	1	1,4 3
	ii. What are the three different types of forensically important files present in the SIM file system?	7	1	1,4 3
OR	iii. What are the steps involved in mobile forensic investigation? Explain any two tools used in a mobile forensic investigation.	7	4	1,4 3
Q.5	i. What is social media forensic? Explain any three sources of social media evidence for social media investigation.	4	3	1,4 4
	ii. What are the steps involved in social media investigation explain in detail.	6	1	1,4 4
OR	iii. What are the different types of data available on social networking sites? Explain different evidence collection methods from social networking sites.	6	3	1,4 4
Q.6	Attempt any two:			
	i. Define computer forensics. What are various GUI-based tools used by indian forensic laboratories to conduct computer investigations?	5	3	1,4 5
	ii. What do you mean by command-line forensic tools? Give an Introduction and the importance of the sleuth kit tool.	5	2	1,4 5
	iii. Explain: (a) Hashing (b) Forensic imaging (c) Cloning (d) Write blocker (e) Forensic workstation	5	1	1,4 5

Marking Scheme
FS3SE07(T) Digital Fraud Investigation (T)

Q.1	i)	d	1
	ii)	c	1
	iii)	c	1
	iv)	b	1
	v)	a	1
	vi)	d	1
	vii)	d	1
	viii)	b	1
	ix)	a	1
	x)	c	1

Q.2	i.	Eavesdropping and Salami Attack	1 Mark each	2
	ii.	TC, IP and UDP protocol	1 Mark each	3
	iii.	Any five act	1 Mark each	5
	OR iv.	Any five types of cyber-attacks	1 Mark each	5

Q.3	i.	a.) Spoofing	1 Mark each	2
		b.) Internet Time Theft	1 Mark each	
	ii.	WEP types	4 Marks	8
		WPA types	4 Marks	
OR	iii.	Definition	1 Mark each	8
		Seven layers with function	1 Mark each	

Q.4	i.	a.) Cell Phone Forensic.	1 Mark each	3
		b.) Computer Forensic.	1 Mark each	
		c.) Network Forensic	1 Mark each	
	ii.	Any Seven forensically important files in SIM.	1 Mark each	7
OR	iii.	Steps Involved in Mobile Forensic Investigation	4 Marks	7
		Any Two Tools	1.5 Marks each 3 Marks	

Q.5	i.	Definition	1 Mark each	4
		Any three Sources	3 Marks	
	ii.	Steps in Social Media Investigation	6 Marks	6
OR	iii.	Types of Data Available on Social Networking Sites.	3 Marks	6
		Any three evidence collection methods from social networking sites.	3 Marks	

Q.6

i.	Definition	1 Mark	5
	Any two tools used by FSL in investigation with an explanation.	2 Marks each	
ii.	Command Line Tool	1 Mark each	5
	Sleuth Kit with explanation	4 Marks	
iii.	a.) Hashing.	1 Mark each	5
	b.) Forensic Imagin	1 Mark each	
	c.) Cloning	1 Mark each	
	d.) Write blocker	1 Mark each	
	e.) Forensic Workstation	1 Mark each	
