Faculty : Science And Technology

Program No. & Name of the Examination: 1T01236 / / T.E.(Information Technology Engineering) (SEM-VI)(Choice Base Credit Grading System) (R- 19) (C Scheme)

Subject (Paper Code) : 89388 / / Ethical Hacking and Forensic (DLOC)

DAT: 31/5/2022 QP CODE: 94008

==

======

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
Q1.	Definition of cybercrime is
Option A:	a criminal activity involving a computer, networked device or a network
Option B:	criminal activity involving a computer
Option C:	criminal activity involving a networked device
Option D:	any criminal activity that involves a network
Q2.	A copy which includes all necessary parts of evidence, which is closely related to the original evidence.
Option A:	Digital Evidence
Option B:	Best Evidence
Option C:	Original Evidence
Option D:	Complete Evidence
Q3.	CSIRT stands for ______________
Option A:	Computer security incident response team
Option B:	Computer software incident resource team
Option C:	Common security incident resolution team
Option D:	Computer security incident resource team
Q4.	Forensic Duplication is necessary
Option A:	as it preserves original digital evidence & allows recreation of the duplicate image
Option B:	as it creates restored image
Option C:	as it creates and stores mirror image
Option D:	as it helps in live system duplication
Q5.	Analyzing data collected from different sites, Firewalls and IDS is called as..?
Option A:	Computer Forensics
Option B:	Network Forensics
Option C:	Mobile Devices Forensics
Option D:	Memory Forensics
Q6.	Which one among the following statements is not a goal of good forensic report writing
Option A:	describe accurately the details of the incident
Option B:	Be understandable to decision makers
Option C:	Be able to withstand the legal scrutiny
Option D:	Cannot be easily referenced
Q7.	Which among the following is not an example of cyber crime
Option A:	SQL injection
Option B:	Identity theft
Option C:	Hacking
Option D:	Designing antivirus
Q8.	If there ought to be no doubt about the reality of the specialist's decision, then the evidence is said to be...?
Option A:	Authentic
Option B:	Admissible
Option C:	Believable

Option D:	Reliable
Q9.	In central incident response team how many teams handle incidents occurring in whole organization?
Option A:	1
Option B:	2
Option C:	3
Option D:	4
Q10.	Restoration Process involves
Option A:	blind sector to sector copy of the duplicate file
Option B:	collection of Digital Evidence
Option C:	creation of response toolkit
Option D:	check the dependencies

Q2 (20 Marks)	**Solve any Two Questions out of Three 10 marks each**
A	Compare active attacks vs Passive attacks. Classify the cybercrimes and explain any one briefly
B	Explain the phases of incident response Methodology with neat diagram
C	Explain Volatile Data Collection from Windows system

Q3 (20 Marks)	**Solve any Two Questions out of Three 10 marks each**
A	What are possible investigation phase carried out in Data Collection and Analysis
B	What do you understand by social engineering? Give classification
C	Briefly explain Types of digital Evidence with examples.

Q4 (20 Marks)	**Solve any Two Questions out of Three 10 marks each**
A	Explain importance of forensic duplication and its methods.
B	Explain various guidelines for digital forensic report writing along with its goals.
C	Discuss the techniques of tracing an email message.