

Duration: 3 Hours

Total Marks: 80

- N.B.:** (1) Question No 1 is Compulsory.  
 (2) Attempt any three questions out of the remaining five.  
 (3) All questions carry equal marks.  
 (4) Assume suitable data, if required and state it clearly.

Q1.	Attempt any four	Marks
a.	Describe Goals of Incident Response.	5
b.	Define the term Digital Forensics and types of Digital Forensics.	5
c.	Explain Social Engineering with example.	5
d.	How to Present Digital Evidences?	5
e.	Differentiate attack and vulnerabilities.	5
<b>Q2.</b>	a. What is cybercrime? Explain the categories of cybercrime with example.	<b>10</b>
	b. Differentiate between Computer worm, virus, Trojan horse and Trapdoor.	<b>10</b>
<b>Q3.</b>	a. Draw and explain the Incidence Response Methodology in detail.	<b>10</b>
	b. List and explain the forensic image format with proper diagram.	<b>10</b>
<b>Q4</b>	a. Discuss the necessity of forensic duplication and explain the use of dd, dcfldd, foremost, scapel command.	<b>10</b>
	b. List and explain the steps involved in collecting volatile data in windows system.	<b>10</b>
<b>Q5</b>	a. Case Study: A corporate lady was getting some threat mails. She decided to file a complaint. What steps should be taken to investigate those mails?	<b>10</b>
	b. Explain with example CFAA act.	<b>10</b>
<b>Q6</b>	a. Explain various types of laws and level of laws in details.	<b>10</b>
	b. Write a short note on CAN Spam Act.	<b>10</b>