Duration: 3hrs **[Max 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.

1		Attempt any FOUR	
	a	Differentiate passive and active attacks	[05]
	b	Explain the steps for investigating routers.	[05]
	c	Explain levels of culpability	[05]
	d	What are the different challenges of evidence handling?	[05]
	e	Explain the steps of volatile data collection for the Unix system.	[05]
2	a	Discuss different forensic image formats	[10]
	b	Explain the steps in detail required to investigate Windows systems	[10]
3	a	Which are possible investigation phases carried out in data collection and analysis?	[10]
	b	Explain Incident Response Methodology (IRM) with a neat diagram.	[10]
4	a	Explain various types of law and different levels of law in detail.	[10]
	b	Define cybercrime. Discuss various cybercrime categories in detail.	[10]
5	a	Discuss how network-based evidence is collected and analyzed.	[10]
	b	Write a short note on the Acquisition, Duplication, Analysis, and Recovery of digital evidence	[10]
6	a	What is Intrusion Detection System (IDS)? Discuss different types of IDS and types of intrusion detection systems methods.	[10]
	b	Discuss the necessity of forensic duplication	[10]

****