(3 Hours) **Total Marks: 80**

N.B.: (1) Question No.1 is compulsory.
(2) Attempt any three questions from the remaining five questions.
(3) Make suitable assumptions wherever necessary but justify your assumptions.

1.	(a) What is hacking? Who are the different types of hackers?	**05**
	(b) What is incident and what are the goals of incident response?	**05**
	(c) What volatile data can be obtained from investigation of routers?	**05**
	(d) What are the challenges in evidence handling?	**05**
2.	(a) Classify the different categories of cyber crime with examples of each. Identify the type of cyber-crime for each of the following situations: i) Hacking into a Web server and defacing legitimate Web pages ii) Introducing viruses, worms, and other malicious code into a network or computer iii) Unauthorized copying of copyrighted software, music, movies, art, books. iv) Internet gambling and trafficking	**10**
	(b) Briefly explain the role of the following tools in digital forensics: i) netstat ii) psloggedon iii) tcptrace iv) netcat v) cryptcat	**10**
3.	(a) Briefly explain the process of collecting the volatile data in Windows system.	**10**
	(b) Briefly explain each of the following: Qualified forensic duplicate, restored image, mirror image.	**10**
4.	(a) Explain e-mail forensic investigation methods.	**10**
	(b) Discuss the steps for investigating routers.	**10**
5.	(a) Briefly explain the role of Windows registry in collecting forensic evidence.	**10**
	(b) Explain different bodies of law.	**10**
6.	Write a short note on: (1) CFAA (2) Storage layer of File system	**20**

****