Q. P. Code: 38873

(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) Explain qualified forensic duplicate, restored image and mirror image.	05
	(c) What volatile data can be obtained from investigation of routers?	05
	(d) What are the different ways to recover deleted files from a Unix system?	05
2.	(a) What do you mean by incident response methodology? Explain the different phases.	10
	(b) Briefly explain the process of collecting the volatile data in Windows system.	10
3.	(a) Briefly explain the role of Windows registry in collecting forensic evidence.	10
	(b) Explain the method for performing the mobile forensic.	10
4.	(a) Discuss the steps for investigating routers.	10
	(b) Explain the steps for e-mail forensic investigation.	10
5.	(a) What are the requirements of forensic duplication tools? Elaborate different ways of creating a forensic duplicate of a hard-disk.	10
	(b) What is digital evidence? What are the different types of digital evidence?	10
6.	Write a short note on**:(any two)**	20

(1) Challenges of performing mobile forensic.

(2) Layout of report writing

(3) Chain of custody

****