Exam.Code: 1047
Sub. Code: 35464

2124

M.E. Computer Science and Engineering (Cyber Security)
Third Semester
CSN 8302: Digital Forensics

Time allowed: 3 Hours **Max. Marks: 50**

NOTE: ***Attempt five questions in all, including Question No. 1 which is compulsory and selecting two questions from each Part.***

x-x-x

I	i) What is Email Forensics Investigation?	(1)
	ii) List down the steps of Investigation process in Digital Forensics.	(1)
	iii) Briefly explain the characteristics of Digital Evidence.	(1)
	iv) Briefly explain how volatile information is recovered in Windows Forensics.	(1)
	v) List down various types of investigation in digital forensics.	(1)
	vi) Briefly explain how FTK Imager is used in digital forensics.	(1)
	vii) What is Wireshark in digital forensics?	(1)
	viii) How Foremost is used to recover lost files from forensic images?	(1)
	ix) What is Password Cracking?	(1)
	x) What is data carving in digital forensics?	(1)
	PART-A	
II	a) Explain roles of forensic investigator.	(5)
	b) What are various issues facing computer forensics?	(5)
III	a) Explain steps for preparing first responder's toolkit.	(5)
	b) Explain various steps for forensic readiness planning.	(5)
IV	a) What is the boot process in digital forensics?	(5)
	b) How deleted files and partitions are recovered in Windows forensics?	(5)
	PART-B	
V	a) Explain the use of Autopsy as forensic tool in digital forensics.	(5)
	b) What is network forensics? Explain different steps used in network forensics.	(5)
VI	a) How logs are captured and analyzed?	(5)
	b) What is Mobile device forensics?	(5)
VII	a) Explain Image metadata extraction using Imago.	(5)
	b) Explain different types of web attacks.	(5)

x-x-x