Code No: **R42122** **R10** **Set No. 1**

IV B.Tech II Semester Regular/Supplementary Examinations, April - 2015

COMPUTER FORENSICS

(Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions

All Questions carry equal marks

****

1 a) Explain the Legal process in a Criminal investigation. [8]

b) Explain about corporate Investigations and Company Policies. [7]

2 a) Identify the duties of lab manager and staff and also about lab budget planning. [8]

b) What are the minimum requirements for a computer forensics lab of any size? [7]

3 a) How to determine best data acquisition method? [8]

b) Explain about modifying the registry for USB Write-Blocking. [7]

4 a) Explain how to secure a computer Incident or Crime Scene. [10]

b) Explain how to process and handle the Digital Evidence. [5]

5 a) Explain about crime data validation and discrimination. [8]

b) Explain about the Crime scene Reconstruction. [7]

6 a) Explain common data-hiding techniques. [12]

b) For what legal and illegal purposes can you use steganography? [3]

7 a) Explain lossless and lossy data compression. [8]

b) Explain the standard procedures for network forensics. [7]

8 a) Explore the role of client and server in Email. [8]

b) Explain how to examine UNIX Email servers. [7]

Code No: **R42122** **R10** **Set No. 2**

IV B.Tech II Semester Regular/Supplementary Examinations, April - 2015

COMPUTER FORENSICS

(Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
****

1 a) What is Professional Conduct? Why is it Important? [8]

b) Why should companies appoint authorized requester for Computer Investigation? [7]

2 a) Explain the process of conducing High Risk Investigations [8]

b) Recommendations for secure storage container with respective key padlock practices. [7]

3 a) Explain about Contingency Planning for Image Acquisition. [5]

b) Describe about RAID acquisition methods. [10]

4 a) Explain the process of getting Digital hash in the investigations. [10]

b) Explain how to process a data center with RAID system. [5]

5 a) List & Briefly explain the tasks performed by Computer Forensic Tools. [8]

b) Explain about the extraction of crime scene data. [7]

6 a) How to use steganography to hide the data. [7]

a) Explain briefly about the tools used to validate data. [8]

7 a) Searching for recovering digital photography evidence. [10]

b) Explain the copy right issues with graphics. [5]

8 a) Explain the acquisition procedures for cell phones and mobile devices. [10]

b) Explain how to examine Microsoft server logs. [5]

Code No: **R42122** **R10** **Set No. 3**

IV B.Tech II Semester Regular/Supplementary Examinations, April - 2015

COMPUTER FORENSICS

(Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1 a) Explain the standard system analysis steps, when preparing for a Case. [10]

b) Explain how to plan your Digital Forensics Investigation. [5]

2 a) Explain the recommendations for securing storage containers in a forensics lab? [10]

b) What are the facility components and practices lab audits should include? [5]

3 a) Explain about Remote Network Acquisition with Pro-discover [7]

b) Explain about acquiring data with a LINUX Boot CD and a live CD distribution. [8]

4 a) Explain how to acquire the digital Evidence from the crime scene. [8]

b) List out the procedures for storing digital evidence at the crime scene. [7]

5 a) What are key point to be considered when evaluating the Forensics tools. [5]

b) Explain about the UNIX forensics tools. [10]

6 a) Determine what data to analyze in a computer forensics investigation. [8]

b) Explain the process of Carving data from unallocated space. [7]

7 a) Explain the steganography in graphic files. [10]

b) Explain how to use steganalysis tools. [5]

8 a) Describe tasks in investigating e-mail crimes and violations. [8]

b) Briefly explain the basic concepts of mobile device forensics. [7]

Code No: **R42122** **R10** **Set No. 4**

IV B.Tech II Semester Regular/Supplementary Examinations, April - 2015

COMPUTER FORENSICS

(Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1 a) Explain the steps for conducting Attorney- Client Privilege (ACP). [10]

b) Explain about displaying banners in the company systems. [5]

2 a) To determine the types of operating systems needed in your lab, list two sources of Information you could use. [5]

b) What items should your business plan include? [5]

c) What three items should you research before enlisting in a certification program? [5]

3 a) Explain about Windows validation methods. [7]

b) Explain the procedure of capturing an image with access data FTK imager. [8]

4 a) Describe how to secure a computer incident or crime scene. [8]

b) List the steps in preparing for an evidence search. [7]

5 a) Describe available computer forensics software tools. [10]

b) What are the sub functions of the extraction function? [5]

6 a) How to perform remote acquisition. [10]

b) Which FTK search option is more likely to find text hidden in unallocated space? Justify your answer. [5]

7 a) Explain how to identify the unknown file formats that your computer forensics tool doesn’t recognize. [10]

b) Explain how to use steganalysis tools. [5]

8 Explain the steps involved in the general procedure for a Live acquisition. [15]