Code No: 117BW **R13**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, November/December- 2017
COMPUTER FORENSICS
(Computer Science and Engineering)

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

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART- A

(25 Marks)

1.a) What are the categories of computer investigations and forensics? Explain. [2]
b) Enumerate the basic steps for investigating Attorney-Client Privilege investigations.[3]
c) Explain the tasks to be completed before searching for evidence. [2]
d) Enumerate the guidelines for seizing digital evidence at the computer incident or crime scene. [3]
e) Why should companies appoint an authorized requester for computer investigations?[2]
f) Explain in brief the three modes of protection of defense in depth. [3]
g) Describe procedures for acquiring data from cell phones and mobile devices. [2]
h) What are e-mail servers? Explain their role in forensic investigations. [3]
i) List some third party and open source whole disk encryption tools. [2]
j) What are the startup files of windows XP? Explain. [3]

PART-B

(50 Marks)

2. Which organization has guidelines on how to operate a computer forensics lab? What term refers to labs constructed to shield EMR emissions? [10]

OR

3. What are the guidelines for media leak investigations? Mention the steps for investigating media leaks. [10]

4. What do we need a technical advisor? What are the responsibilities of technical advisors? Explain. [10]

OR

5. What are the steps to create image files of digital evidence? How is digital evidence stored? Explain. [10]

6. What is the standard procedure used for network forensics? List the different network tools and explain any two. [10]

OR

7. What are the primary concerns in conducting forensic examination of virtual machines? Give an overview of network forensics. [10]

8. What is a personal digital assistant? What are the different types of peripheral memory cards used with PDAs? Explain in detail. [10]

OR

9. Explain the components found inside mobile device. Also explain iPhone readers. [10]

10. What are the metadata records in the master file table of NTFS? Explain the attributes in the master file table. [10]

OR

11. Enumerate the features of the current whole disk encryption tools. What are the hardware and software requirements of Microsoft's Bitlocker? Explain. [10]

--ooOoo--