Roll No. □□□□□□□□□□

B.E. / B.Tech. (Full Time) DEGREE END SEMESTER EXAMINATIONS, APRIL / MAY 2014

Computer Science and Engineering/Information Technology

Sixth Semester

CS 9031 Cyber Forensics

(Regulation 2008)

Time: 3 Hours　　　Answer ALL Questions　　　Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. Define the term cyber forensics and distinguish it from network security.

2. List any four agendas for action in computer forensics methods.

3. What is a registry analysis? How it is useful in cyber forensics.

4. What is digital evidence? What are the types of evidence? What are the characteristics of good evidence?

5. State and list the Order of Volatility of evidence

6. What is network forensics? If a company wants to tap an employee, is it permitted? Justify the decision with the relevant cyber law.

7. What is a virus? What are the types of viruses? What is the incident handling procedure for handling virus?

8. What is information warfare? How is it different from conventional warfare?

9. **Answer the following.**

   (i) A hacker contacts you over phone or email and attempts to acquire your password. This is called as -----------------.

   A) spoofing

   B) phishing

   C) spamming

   D) bugging

The phrase __________ describes viruses, worms, Trojan horses, attack applets, and attack scripts.

A) malware

B) spam

C) phish

D) virus

10. List out and describe at least four surveillance tools.

Part – B (5 x 16 = 80 marks)

11. What is a windows artifact? How evidence is collected in a window system and how is it preserved. Explain with an example.

12. a) Explain how data backup and recovery is done in computer forensics. How is it helpful in disaster management?

(OR)

b) How Authenticode works with VeriSign Digital ID'S? Discuss in detail and explain how it is helpful in maintaining the integrity of the evidence.

13. a) 1. Read the following passage and give data recovery solution and justify it.

One and a half hours before take-off, a businesswoman's laptop was returned to her after a routine maintenance check by her IT department. It contained her PowerPoint presentation, crucial to the meeting she was meant to be attending. While rebooting for a final run-through in the departure lounge, a message appeared saying the boot sector was corrupt. (8)

2. Explain the steps in "Evidence Search and Seizure". (8)

(OR)

b) Read the following passage and give data recovery solution and justify it.

Roll No. □□□□□□□□□□

Case Study: Companies who recycle their computers by selling them on to someone else will aim to erase all data on their hard drive. However, this may not always be successful.

(i) Outline how formatting the disk may not in fact achieve this aim.
(4)

(ii) Outline the possible effects on privacy if all of the data is **not** erased.
(4)

(B) Discuss the various approaches for network forensics scenarios briefly.
(8)

14. a) List out the macro threats used for sabotaging in information warfare. List out and explain how it is used by governments to sabotage the enemy countries.

(OR)

b) List out the tactics of a terrorist and rogues? How those tactics can be countered? Explain how hackers control tanks, planes and warship with an example.

15. a) What is an encryption? List out some of the encryption algorithms and explain its role in cyber forensics.

(OR)

b) Who is a hacker? What are his responsibilities? Explain how a hacking is performed in web pages.