KUMARAGURU
college of technology
character is life

Register Number: ………….

B.E DEGREE EXAMINATIONS: APRIL/MAY 2016

(Regulation 2013)

Sixth Semester

COMPUTER SCIENCE AND ENGINEERING

U13CSTE21**:** Cyber Forensics

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Criteria for equipment in the double tier approach results in the following except:

a) Quick to learn
b) Totally Reliable
c) Robust and Durable
d) Legally Operable

2. The objective of Computer Forensics is to recover, analyze, and present computer-based material in such a way that it is _______________.

3. Establishing a corporate Internet security policy involves the following, except

a) High-level management policy statement
b) Systematic analysis of organization’s assets
c) Examination of risks
d) Low-level management policy statement

4. Preserving a chain of custody for electronic evidence includes ______ copying process

5. Documentary evidence has become the keystone in cases involving ______.

a) Burglary
b) Sexual discrimination
c) Murder
d) Stock options

6. Ambient data is stored in Windows ______.

7. Information peace keeping is

a) Media Manipulation
b) psychological operations
c) IT for military peace keeping
d) IT for national policy objectives

8. The battle space of information warfare is defined by the _____, _______ and _______ of interactions between the players.

9. ________ helps us to convert thoughts into computer commands.

a) Human Computer Interaction
b) Web Browser
c) BioFusion
d) Smart dust

10. ________ can be a tiny bundle of electronic brains, laser communications system, power supply, sensors, and even a propulsion system that can spy in the war field.

PART B (10 x 2 = 20 Marks)

(Answer not more than 40 words)

11. List 4 important responsibilities of a computer forensics specialist.

12. "Protection of evidence in computer system is critical". How can this be ensured?

13. "Denial of service attacks occur in larger organizations". Is it true? Defend your answer

14. Examine the usefulness of corporate information

15. Examine the order of volatility of information

16. If a company wants to tap an employee, is it permitted? Evaluate your decision with the relevant cyber law.

17. Distinguish between conventional and information warfare.

18. What is command and control warfare?

19. What is a packet sniffer?

20. Interpret decoy network as a useful tool.

PART C (5 x 14 = 70 Marks)

(Answer not more than 400 words)

Q.No. 21 is Compulsory

21. (i) Illustrate computer evidence processing procedures with suitable examples. (10)

(ii) XYZ enters a bank branch in the CBE area and deposits a check. The bank video camera captures an image of XYZ entering the branch and matches it against its database of customers. The image is time and date stamped. Later that day, XYZ's savings account is accessed via Internet banking from an IP address located in Italy. During a routine correlation of data, the apparent discrepancy is detected by the bank's forensics system. How would you as a Computer Forensics specialist, go about investigating this incident? (4)

22. (a) (i) What is the need for backup? Enumerate the components of backup techniques followed. Review the procedures followed and suggest improvements (8)

(ii) Read the following passage and formulate data recovery solution and justify it. (6)
One and a half hours before take-off, a business space woman'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, "boot sector corrupt" message appears.

(OR)

(b) (i) An adult roommate was accused of using another's computer to make unauthorized purchases on a popular Internet shopping site. What did the computer forensics Specialist do after he conducted an investigation? (7)

(ii) When downloading software, the customers find it difficult to trust the software which is devoid of assurance of integrity and publisher’s identity. Formulate a technique to ensure content source and integrity with illustrations. (7)

23. (a) (i) How can past events be analysed and reconstructed to extract and present evidence? Demonstrate by considering the following case: (7)
Offensive jokes were being posted in various locations in the offices of a large corporation. Management had identified four possible suspects but each denied involvement. The company’s IT department could not find out whether the documents had been created on any computer in the office. A CFS team (CFST) was called to consult on the matter. Using forensic analysis, how did the CFST analyse and reconstruct the events to provide evidence to solve the problem?

(ii) “The use of SOPs is fundamental to both law enforcement and forensic science”- Defend by giving suitable arguments. (7)

(OR)

(b) (i) A CFST needs to ascertain the authenticity of a critical piece of electronic evidence sent as an email. The senders’ email did not quote contract terms, while the recipient’s email explicitly confirmed the contract terms. A network security system has been retaining all network packet information for the past six months. High volume of data is involved. What techniques and tools can be used to identify suspect communications? Suggest the network forensic tool that can be used and describe its components. (8)

(ii) What is the purpose of incident reporting forms? What are its elements? (6)

24. (a) List out the macro threats used for sabotaging in information warfare. Demonstrate how it is used by governments to sabotage the enemy countries.

(OR)

(b) List out the tactics of terrorist and rogues. Suggest methods to counter such tactics. Illustrate how hackers control tanks, planes and warships with an example.

25. (a) Discuss in detail the principle, technology of electromagnetic bombs, defense mechanisms against these bombs and their limitations.

(OR)

(b) Discuss in detail about cyber tools for information warfare.

****