Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION(S), MAY 2019

Course Code: IT465

Course Name: Cyber Forensics

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks. Marks

1 a) List the steps involved in corporate cyber forensic investigation. What are the two types of threats that usually occur in corporate sector? (8)

b) Explain about types of law enforcement in computer forensic technology. (7)

2 a) Define Computer Forensics. Distinguish between spyware and Adware? (8)

b) Define the term Cyber stalking with example. (7)

3 a) How can a CF investigator analyse malicious software? (8)

b) Explain about Biometric Security Systems (7)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Explain the Storage Area Networks (SANs) ? (9)

b) Analyze the various countermeasures that can be taken for Microsoft Windows hacking by password cracking. (6)

5 a) Explain the encrypted satellite data transmitting and receiving mechanisms (7)

b) Why evidence is collected? (4)

c) Compare computer virus with computer worms (4)

6 a) Explain network disaster recovery system? (5)

b) Explain the effect of digital information in technology (6)

c) What is scanning? List different types of scan? (4)

PART C

Answer any two full questions, each carries 20 marks.

7 a) How can evidence be controlled from being contaminated? (7)

b) What are artifacts? (3)

c) What is the need of time synchronization? What is NTP? (10)

8 a) Explain the generalized digital investigation framework? (10)

b) What are the steps in investigating a web attack? (10)

9 a) Explain the Computer evidence processing steps involved in Cyber crimes. (10)

b) How to handle usable file format and unusable file formats (7)

c) List types of network attacks (3)

****