Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, DECEMBER 2018

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)	Define corporate cyber forensics. What are the types of information that a corporate spy usually seek?	(7)
	b)	Explain the different types of Business computer Forensic Technology?	(8)
2	a)	How can a CF investigator analyse large scale data breach cases?	(9)
	b)	How to avoid Pitfalls with Firewalls?	(6)
3	a)	Give any two cyber crimes against society.	(5)
	b)	What is meant by cyber defamation? Illustrate with an example.	(3)
	c)	Describe about Internet Tracing Method?	(7)

PART B

Answer any two full questions, each carries 15 marks.

4	a)	Explain Internet security architecture?	(10)
	b)	What are the different obstacles in evidence collections?	(5)
5	a)	What are the functions performed by intrusion detection system?	(5)
	b)	Draw the hacking life cycle diagram and explain all the steps that are involved in it.	(7)
	c)	Identify various classes of hackers that are defined by the security expert.	(3)
6	a)	List out and explain the participants and elements involved in payment processing network?	(7)
	b)	Distinguish the roles of training and education in digital forensics.	(7)

PART C

Answer any two full questions, each carries 20 marks.

7	a)	What is volatile evidence? How is it useful in computer forensic investigation? Explain the method and tools for capturing volatile data.	(10)
	b)	How to handle usable file format and unusable file formats	(6)

	c)	What is the need of analysing network traffic?	(4)
8	a)	What are the steps involved in the collection of Evidence in cyber crimes?	(10)
	b)	Describe how to reconstruct the Past Events.	(10)
9	a)	What are the duties and support functions of a Computer Forensic investigator?	(10)
	b)	Distinguish Router Forensics and Cyber Forensics	(10)

****