Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous Institute Affiliated to University of Mumbai)

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
CPE8034	Elective-III Digital Forensics	4	-	-	4	-	-	4
		Examination Scheme						
		ISE		MSE	ESE			
		10		30	100 (60% Weightage)			

Pre-requisite Course Codes		CPC702(Cryptography and System Security)
At end of successful completion of this course, student will be able to		
Course Outcomes	CO1	Understand the role of digital forensics.
	CO2	An ability to analyze a problem, and identify and define the Computing requirements appropriate to its solution.
	CO3	Better understand the research challenges of digital forensics
	CO4	An understanding of professional, ethical, legal, security and social issues and responsibilities.

Module No.	Unit No.	Topics	Ref.	Hrs.
1	1.1	**Introduction:**		09
	1.2	Introduction of Cybercrime: Types, The Internet spawns crime, Worms versus viruses, Computers' roles in crimes, Introduction to digitalforensics.	1,2	
	1.3	Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response, Phase after detection of an incident.	1,2	
2	2.1	**Initial Response and forensic duplication**		08
	2.2	Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system – Forensic.	2,3	
	2.3	Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic, Duplicate/Qualified Forensic Duplicate of a Hard Drive.	2,3	
3	3.1	**Preserving and Recovering Digital Evidence**		09
	3.2	File Systems: FAT, NTFS - Forensic Analysis of File Systems – Storage	1,2	
	3.3	Fundamentals: Storage Layer, Hard Drives Evidence Handling: Types of Evidence, Challenges in evidence handling, Overview of evidencehandling procedure	1,2	
4	4.1	**Network Forensics**		07
	4.2	Intrusion detection; Different Attacks in network, analysis	1,5	

		Collecting		
	4.3	Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing- Internet Fraud.	1,5	
5	**5.1**	**System investigation**		08
	5.2	Data Analysis Techniques - Investigating Live Systems (Windows & Unix) Investigating	2,3	
	5.3	Hacker Tools - Ethical Issues – Cybercrime.	2,3	
6	**6.1**	**Bodies of law**		07
	6.2	Levels of law: Local laws, State laws, Federal laws, International laws , Levels of culpability: Intent, Knowledge, Recklessness, Negligence.	2,4	
	6.3	Level and burden of proof : Criminal versus civil cases ,Vicarious liability, Laws related to computers: CFAA, DMCA, CAN Spam, etc.	2,4	
			Total	**48**

References:

[1] Kevin Mandia, Chris Prosise, "Incident Response and computer forensics", Tata McGrawHill, 2006

[2] Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999

[3] Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001

[4] Skoudis. E., Perlman. R. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses.Prentice Hall Professional Technical Reference. 2001.

[5] Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information From a Computer", Paladin Press, 2000

[6] Bill Nelson, Amelia Philips and Christopher Steuart, "Guide to computer forensics investigation "Course technology, 4th edition