C. U. SHAH UNIVERSITY, WADHWAN CITY.

Faculty of: **Computer Science**
Course: **Master of Computer Applications**
Semester**: III**
Subject Code**: 5CS03CFS1(Elective – I)**
Subject Name: **Cyber Security and Forensic Science**

Sr. No	Subject Code	Subject Name	Teaching hours/ Week			Credit hours	Credit Points	Evaluation Scheme/ Semester								
								Theory				Practical				Total
								Internal Assessment		End Semester Exams		Internal Assessment		End Semester Exams		
			Th	Tu	Pr			Marks	Duration	Marks	Duration	Marks	Duration	Marks	Duration	
2	5CS03CFS1	Cyber Security and Forensic Science	4	--	--	4	4	30	1½	70	2½	--	--	--	--	100

AIM:

The Course provides a State-of-Art in Cybercrime, Cyber Laws, IT Act 2000, Cyber Forensics, and Application Password Crackers, Logs Investigating, and Network Forensics & Traffic.

COURSE CONTENTS

Sr. No.	Chapter Name	Chapter Topics	Total Hours
1	Introduction	Cybercrime Definition & Origins of the Word, Cybercrime and Information Security, Cybercriminals	02
2	Cybercrime: The Legal Perspectives	Indian Information Technology Act 2000(ITA 2000), The Indian Laws, Provisions in Indian Cybercrime Laws and Punishment, Cybercrime Era: Survival Mantra for the Netizens	03
3	Cyber Forensics Essentials	Windows Forensics: Volatile Information, Network and Process Information, Non-Volatile Information, Memory Dump, Parsing Process Memory, Inside the Registry, System Information, User Activity, Analysing Restore Point Registry Settings, Cache, Cookie and History Analysis, Message Digest Function:MD5, Prefetch Files, Static Analysis Process, Export Table Analysis, Types of Metadata, Understanding Events, Parsing IIS Logs, FTP Logs and Firewall Logs, Evaluating Account Management Events, Searching with Event Viewer & Forensics Tools	18
4	Application Password Crackers	Password Terminology, Types of Password, Password Cracker, How does a Password Cracker Work, Password Cracking Techniques, Types of Password Attacks, System Software Password Cracking, Application Software Password Cracking, Default Passwords & Password Cracking tools.	15

5	Network Forensics, Investing Logs & Network Traffic	Introduction of Network Forensics, Network Forensics Mechanism, Intrusion Detection System(IDS), Firewall, Honeypot, Network Vulnerabilities, Types of Network Attack, New Line Injection Attack, Timestamp Injection Attack, Investigating Network Traffic, Acquiring Traffic using DNS Poisoning Techniques, Evidence Gathering From ARP Table, Traffic Capturing and Analysis Tools.	10
		Total	48

REFERENCE BOOKS:

- "Cyber Security Understanding Cyber Crimes, Computer Forensics & Legal Perspectives", Wiley India,Belapure &Godbole , ISBN No:8126521791
- "Cybersecurity and Cyberwar", Oxford University Press, P.W. Singer, ISBN No: 0199918112
- "Computer Forensics: Investigating Network Intrusion and Cyber Crime". Ec-Council Press Series, ISBN No: 1435483529