

NR23 B.Tech CSE(CS) Syllabus

NRCM

CYBER CRIME INVESTIGATION AND DIGITAL FORENSICS

B. Tech. III Year II Sem

Course Code	Category	Hours/ Week			Credits	Maximum Marks		
23CY602	Professional core	L	T	P	3	CIE	SEE	TOTAL
		3	0	0		40	60	100
Contact Classes:48	Tutorial Classes:16	Practical Classes:				Total Classes:64		
		Nil						

Prerequisites

1. Knowledge of computer hardware, operating systems ,applications and networking is required.

Course Objectives:

- Know about role of digital devices in cyber crime investigation
- Learn about cyber crime investigation process and methodologies
- An introduction to the methodology and procedures associated with digital forensic analysis in a network environment.

Course Outcomes:

- To obtain and analyze digital information for possible use as evidence in civil,criminal or administrative cases.
- To learn about the importance of digital forensic principles and procedures
- To know legal considerations and digital evidence controls
- To learn about digital forensic tools

UNIT-I

Foundations of Digital Forensics: Digital Evidence, Principles of Digital Forensics, Challenging aspects of Digital Evidence, The Role of computers in crime, Cyber Crime Law.

UNIT-II

Digital Investigations: Digital Investigation process models, Applying Scientific method in Digital Investigations, Handling a digital Crime scene: Fundamental Principles, Surveying and Preserving Digital Investigation.

UNIT- III

Violent Crime and Digital Investigation: The role of Computers in violent crime, Processing Digital crime scene, Investigative Reconstruction, Digital Evidence as Alibi.

UNIT-IV



NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE
Accredited by NBA & NAAC with 'A' Grade

NR23 B.Tech CSE(CS) Syllabus

NRCM

Cyber stalking, Computer basics for Digital Forensics, Applying Forensics science to computers, Digital Evidence on windows systems, Digital Evidence on Unix systems.

UNIT-V

Network Forensics: Networks basics for Digital Investigators, Applying Forensics science to networks, Digital Evidence on physical and data link layers, Digital Evidence on Network and Transport layers.

TEXTBOOK:

1. Digital Evidence and computer Crime by Eoghan Casey Academic Press Third Edition.

REFERENCEBOOKS:

1. Real Digital Forensics for Handheld Devices, E.P.Dorothy, Auer back Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J.Sammons, Syngress Publishing, 2012.
3. Handbook of Digital Forensics and Investigation, E.Casey, Academic Press, 2010.