NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	3CS5201
Course Title:	Digital Forensics
Course Type:	(√ **Core**/ □ Value Added Course / □ Department Elective / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

L	**T**	**Practical Component**				**C**
		LPW	**PW**	**W**	**S**	
2	-	2	-	-	-	3

Course Learning Outcomes (CLOs):

At the end of the course, the student will be able to –

1. illustrate forensic duplication and file system analysis (BL2)
2. identify the need of digital forensic and role of digital evidences (BL3)
3. compare the use of various tools for data recovery (BL4)
4. assess the network forensics to collect digital evidences (BL5)

Syllabus: **Total Teaching hours: 30**

Unit	**Syllabus**	**Teaching hours**
Unit-I	**Introduction to Ethical Hacking:** Difference between Hacking and Ethical hacking, Steps of Ethical Hacking, Tools for ethical hacking	02
Unit-II	**Introduction to Cyber Crime:** Types of cybercrime, categories of cybercrime, Computers' roles in crimes, Prevention from cyber-crime, Hackers, Crackers, Phreakers	02
Unit-III	**Digital Forensics and Digital Evidences:** Rules for Digital Forensic, The Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics, Types of digital evidences and their characteristics, Challenges in digital evidence handling	04
Unit-IV	**Computer Security Incident Response:** Introduction to Computer Security Incident, Goals of Incident response, Incident Response Methodology, Formulating Response Strategy, Incidence Response Process, Data Collection on Unix based systems	06
Unit-V	**Forensic Duplication:** Forensic Image Formats, Traditional Duplication, Live System Duplication, Forensic Duplication tools	02
Unit-VI	**Disk and File System Analysis:** Media Analysis Concepts, File System Abstraction Model, Partition Identification and Recovery, Virtual Machine Disk Images, Forensic Containers Hashing, Carving, Forensic Imaging	04
Unit-VII	**Data Analysis:** Data Analysis Methodology, Investigating Applications, Malware Handling	02

207

Unit-VIII	**Network Forensics:** Technical Exploits and Password Cracking, Analyzing Network Traffic, Collecting Network based evidence, Evidence Handling, Investigating Routers, Handling Router Table Manipulation Incidents, Using Routers as Response Tools	04
Unit-IX	**Forensic Tools:** Need and types of computer forensic tools, tasks performed by computer forensic tools, Study of different tools to acquire, search, analyze and store digital evidence	04

Self-Study: The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response and computer forensics, Tata McGraw Hill.
2. Nilakshi Jain, Dhananjay Kalbande, Digital Forensic: The fascinating world of Digital Evidences, Wiley India Pvt Ltd.
3. Cory Altheide, Harlan Carvey, Digital forensics with open-source tools, Syngress Publishing, Inc.
4. Chris McNab, Network Security Assessment, O'Reily.
5. Clint P Garrison, Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data, Syngress Publishing, Inc.
6. Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations, Cengage Learning
7. Debra Littlejohn Shinder Michael Cross Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, Inc.
8. Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson, Preston Galla, How Personal and Internet Security Work, Que Publications

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Study different data recovery tools.	04
2	Implement experimental analysis of data recovery tools studied in practical 1 on any two different deletion cases and at least two different makes of flash drives.	04
3	Implement photo and multimedia data recovery using open-source tool(s).	04
4	Identifying the types of logs available with different operating systems for forensic investigation. Study different open-source tools for reading logs	04
5	Study different forensic investigation tools and prepare a comparative analysis of the study. Moreover, perform experimentation using open-source digital forensic tools for a given case study.	08
6	Perform penetration testing using appropriate tool(s) and generate a report on different security glitches identified.	06