Faculty of Engineering & Technology
Master of Technology (M. Tech)
(W. E. F.: 2023-24)

Document ID: SUTEFETM-01

Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Technology (M.Tech.) – Cyber Security
Course Code	:	1MCS02
Course Title	:	Cyber Forensics & Investigation
Type of Course	:	Professional Core
Year of Introduction	:	2023-24

Prerequisite	:	A strong foundation in computer science, cybersecurity, and digital forensics tools
Course Objective	:	Develop the skills to investigate digital data theft, detect online footprints, and create incident response reports.
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Investigate theft of digital data
	CO2	Find footprints and generate alerts for online investigation.
	CO3	Write incidence response report.

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	**T**	**P**	**C**	**SEE**	**CIA**	**SEE**	**CIA**	
3	0	2	4	70	30	30	20	150

*Legends: **L**-Lecture; **T**–Tutorial/Teacher Guided Theory Practice; **P** – Practical, **C** – Credit, **SEE** – Semester End Examination, **CIA** - Continuous Internal Assessment (It consists ofAssignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**Introduction:** Introduction to the Incident Response Process What Is a Computer Security Incident? ,What Are the Goals of Incident Response? ,Who Is Involved in the Incident Response Process?, Incident Response Methodology, Pre-Incident Preparation, Detection of Incidents, Initial Response, Formulate a Response Strategy, Investigate the Incident, Reporting, Resolution .	03	10%	CO1
2	**Preparing for Incident Response Overview of Pre-incident Preparation**: Preparing for Incident Response Overview of Pre-incident Preparation , Identifying Risk ,	03	05%	CO3

	Preparing Individual Hosts, Preparing a Network, Establishing Appropriate Policies and Procedures, creating a response toolkit Establishing an Incident Response Team			
3	**After Detection of an Incident :** After Detection of an Incident Overview of the Initial Response Phase, Establishing an Incident Notification Procedure ,Recording the Details after Initial Detection, Incident Declaration, Assembling the CSIRT , Performing Traditional Investigative Steps , Conducting Interviews, Formulating a Response Strategy	04	10%	CO3
4	**Live Data Collection from Windows Systems and Unix Systems:** Live Data Collection from Windows Systems and Unix Systems Creating a Response Toolkit, Storing Information Obtained during the Initial Response, Obtaining Volatile Data, Performing an In-Depth Live Response, Is Forensic Duplication Necessary?	04	05%	CO2
5	**Forensic Duplication**: Forensic Duplicates As Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate of a Hard Drive, Creating a Qualified Forensic Duplicate of a Hard Drive	04	10%	CO2
6	**Collecting Network-based Evidence:** What Is Network-based Evidence?, What are the goals of network monitoring?, Types of Network Monitoring, Setting Up a Network Monitoring System, Performing a Trap-and-Trace Using tcp dump for Full-Content Monitoring, Collecting Network-based Log Files	06	05%	CO1
7	**Evidence Handling** : What Is Evidence, The Challenges of Evidence Handling, Overview of Evidence-Handling Procedures	03	05%	CO2
8	**Computer System Storage Fundamentals:** Hard Drives and Interfaces, Preparation of Hard Drive Media, Introduction to File Systems and Storage Layers	03	05%	CO2

9	**Data Analysis Techniques**: Preparation for Forensic Analysis, Restoring a Forensic Duplicate, Preparing a Forensic Duplication for Analysis In Linux, Reviewing Image Files with Forensic Suites, Converting a Qualified Forensic Duplicate to a Forensic Duplicate, Recovering Deleted Files on Windows Systems, Recovering Unallocated Space, Free Space, and Slack Space Generating File Lists, Preparing a Drive for String Searches.	06	05%	CO3
10	**Investigating Windows Systems**: Where Evidence Resides on Windows Systems, Conducting a Windows Investigation, File Auditing and Theft of Information, Handling the Departing Employee	04	05%	CO2
11	**Investigating Unix Systems**: An Overview of the Steps in a Unix Investigation, Reviewing Pertinent Logs, Performing Keyword Searches, Reviewing Relevant Files, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships, Detecting Trojan Loadable Kernel Modules	04	05%	CO2
12	**Analyzing Network Traffic**: Finding Network-Based Evidence, Generating Session Data with tcptrace, Reassembling Sessions Using tcpflow, Reassembling Sessions Using Ethereal, Refining tcpdump Filters	06	10%	CO3
13	**Investigating Hacker Tools:** What Are the Goals of Tool Analysis, How Files Are Compiled Static Analysis of a Hacker Tool, Dynamic Analysis of a Hacker Tool	04	05%	CO2
14	**Investigating Routers**: Obtaining Volatile Data Prior to Powering Down, Finding the Proof, Using Routers as Response Tools	03	05%	CO2
15	**Writing Computer Forensic Reports**: What Is a Computer Forensics Report?, Report Writing Guidelines, A Template for Computer Forensic Reports	03	10%	CO3

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**20**	**30**	**30**	**20**	**0**	**0**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorial	Teaching Hours
1	Write a program to create checksum.	02
2	Implement tools - Netcat, Cryptcat	02
3	Implement tools - lsof and netstat and analyze the importance of tools during initial response?	02
4	Write a program to capture session data.	02
5	Write a program to perform forensic analysis of a Windows system and a Unix system.	04
6	Implement Snort	02
7	Implement Wireshark.	02
8	Use a tool to acquire USB drive	02
9	Write a program to find Digital hash.	04
10	Compare two files created through text editor to determine whether the files are different at the hexadecimal level. Create a log file. Howto locate date and time in the metadata of a file?	04
11	Write a program to perform bit-shifting on a file. Also write a program to restore the file.	04

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	NETCAT
2	Wireshark.
3	Jupyter notebook
4	Kali Linus OS
5	VMWare

Suggested Learning Websites

Sr. No.	Name of Website
1	https://www.geeksforgeeks.org/cyber-forensics/
2	https://www.cfi.co.th/

Reference Books

Sr. No.	Name of Reference Books
1	Incident response and computer forensicsby Kevin Mandia,Chris Prosise and Matt Pepe - McGrawHill/Osborne
2	Guide to Computer Forensics and Investigations by Bill Nelson Amelia Phillips, Christopher Steuart - Cengage Learning