CSSF3022	**Digital Forensics**	L	T	P	C
Version 1.0		4	0	0	4
Pre-requisites/Exposure					
Co-requisites					

Course Objectives

The course on Digital Forensics aims to provide students with the fundamental concepts and principles of digital forensics, including digital evidence acquisition, analysis and interpretation, malware analysis, network forensics, file system forensics, memory forensics, legal and ethical considerations, report writing and expert testimony, and incident response and cybercrime investigation. The course covers various aspects of digital forensics, including acquiring digital evidence, analysing evidence, analysing malware, investigating network-based cyber incidents, and preparing comprehensive forensic reports. The course also covers legal and ethical considerations, including chain of custody, privacy issues, admissibility of evidence, and expert testimony.

Course Outcomes

CO 1	To have a thorough understanding of digital forensics fundamental concepts, including evidence acquisition, analysis, interpretation, and incident response methodologies.
CO 2	To enhance digital evidence analysis skills by acquiring, analysing, and interpreting digital evidence from various sources, using appropriate forensic tools and methodologies.
CO 3	To have advanced knowledge in malware analysis techniques, dissecting malicious software, and investigating network-based cyber incidents using network forensics tools and methods.
CO 4	To understand legal and ethical considerations in digital forensics investigations, including chain of custody, privacy, evidence admissibility, and expert testimony, to ensure compliance with legal frameworks and ethical standards.
CO 5	To gain skills in order to prepare comprehensive forensic reports, provide expert testimony in legal proceedings, and effectively communicate forensic analysis results.

CO-PO Mapping

Program Outcomes	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PSO1**	**PSO2**	**PSO3**

Course Outcomes															
CO 1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
CO 2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
CO 3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
CO 4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
CO 5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	3
Average	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**

1 – Weakly Mapped (Low) 2 – Moderately Mapped (Medium)

3 – Strongly Mapped (High) "_" means there is no correlation

Syllabus

Unit I: Introduction to Digital Forensics **Lecture Hours: 9**

Overview of digital forensics: definition, importance, and applications, Fundamental concepts and principles of digital forensics, Legal and ethical considerations in digital forensics investigations, Introduction to digital evidence acquisition, analysis, and interpretation.

Unit II: Digital Evidence Acquisition **Lecture Hours: 9**

Techniques for acquiring digital evidence from various sources: computers, mobile devices, cloud environments, Chain of custody and preservation of digital evidence, Hands-on exercises: acquiring and preserving digital evidence using forensic tools.

Unit III: Analysis and Interpretation of Digital Evidence **Lecture Hours: 9**

Methods and tools for analysing and interpreting digital evidence, File system forensics: understanding file systems, recovering deleted data, Memory forensics: extracting and analysing volatile memory, Practical sessions: analysing digital evidence from case studies.

Unit IV: Malware Analysis and Network Forensics **Lecture Hours: 9**

Malware analysis techniques: static and dynamic analysis, behavioural analysis, Network forensics: investigating network traffic, identifying intrusions and attacks, Case studies: analysing malware incidents and network-based cyber incidents.

Unit V: Report Writing, Expert Testimony, and Incident Response **Lecture Hours: 9**

Principles of forensic report writing: documenting findings, methodologies, and conclusions, Providing expert testimony in legal proceedings, Incident response procedures and methodologies for cybercrime investigations, Final project: preparing a comprehensive forensic report and presenting findings.

Total lecture Hours - 45

Textbooks

1. Carrier, B., & Spafford, E. (2005). Digital Forensics with Open Source Tools. Syngress.
2. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.

Reference Books

1. Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to Computer Forensics and Investigations. Cengage Learning.
2. Sammes, A. J., & Jenkinson, G. (2012). Forensic Computing: A Practitioner's Guide. Springer.

Modes of Evaluation: Quiz/Assignment/ presentation/ extempore/ Written Examination

Examination Scheme

Components	IA	MID SEM	End Sem	Total
Weightage (%)	50		50	100

Detailed breakup of Internal Assessment

Internal Assessment Component	Weightage in calculation of Internal Assessment (100 marks)
Quiz 1	15%
Quiz 2	15%
Class Test 1	15%
Class Test 2	15%
Assignment 1/Project	20%
Assignment 2/Project	20%