1	Dates	
2	End Module Assessment	
3	Lab Assessment	
4	Evaluation Details	T - Theory L - Lab A - Assignments / Mid module Evaluations

Centre for Development of Advanced Computing Software Training and Development Centre (Kochi & Thiruvananthapuram)					
PG - DCSF Feb 2025					
WEEK	MODULE NAME	DURATION (120 Hours)			EVALUATION DETAILS
		THEORY	LAB	REVISION	
	Cyber Forensics	56 Hours	60 Hours	4 Hours	60 Marks (20 T + 20 L + 20 A)
SCHEDULE					
Date	Theory Session (09:30 AM to 01: 00 PM)		Lab Session (02:00 PM to 06:00 PM)		
	Data Acquisition • Data Storage Fundamentals • Introduction to Cyber Crimes • Cyber Forensics Principles • Digital Evidence Seizure • Forensic Hardware Tools		• Seizing data with Forensic Hardware and Software		

	Cyber Forensics Analysis • Windows File System – FAT and NTFS • Linux File System • Cyber Forensics Analysis	• Familiarizing file system concepts • Tools – Disk Explorer, Win-Hex, Nfi, Lads, Autopsy	
	Disk Forensics • Disk Forensics Analysis o Partitioning o Registry o File Carving • Windows Analysis o Browser o Event log o Prefetch o Volume Shadow Copy o Recycle Bin o Client based Email Analysis o Page file o Hibernation o Meta Data	• Disk Analysis using CyberCheckSuite (3hrs), Magnet Axiom,	

	○ Spool files ○ Link Files ○ Reparse Point • Linux Analysis		
	Live Forensics • Live Forensics ○ Live seizing and acquisition ○ Live forensic analysis	• Win-LiFT	
	• Memory Forensics ○ Memory Dumping ○ Memory Analysis	• Analysis of Live Artifacts – DumpIt, , Volatility, Magnet Axiom	
	Network Forensics • Network Packet Capturing, Monitoring and Analysis	• NeSa, WireShark	

	Mobile Phone Forensics • Mobile Phone Forensics • Sim Card Forensics • Call Data Record Analysis	• Analysis of Mobile Phone Artifacts – MobileCheck, Sim Xtractor, Cellbrite, CDR analyzer	
	Malware Analysis and Reverse Engineering • Malwares Classification • Recent trends in malwares • Setting up a malware analysis lab • Dynamic/Behaviour based analysis of malware samples • Working with Fileless malwares • Analyzing a malware infected host • Analyzing memory resident malware • Process Injection Techniques • Basic static analysis	• Analysis of Malware Artifacts – Autorun, Procmon, Mitre, Regshot, Bintext, IDAPro, Volatility	

	IoT Forensics
	• Protocols and File Systems
	  ○ Storage and interfaces
	  ○ File systems
	• Multimedia Analysis
		• IoT Forensics with Open Source Tools	

	• GPS Tracking • Wi-Fi Cracking • Security Challenges		