Module No.	Unit No.	Topics	Hrs.
1.0		**Introduction to Cybercrime and Hacking**	**08**
	1.1	Cybercrime, Categories of Cybercrime (Cybercrime against people, Cybercrime Against property, Cybercrime Against Government), Types of cybercrime (Violent- Cyber terrorism, Assault by Threat, Cyberstalking, Child Pornography, Non-violent - Cybertrespass, Cyber Theft, Cyberfraud, Destructive Cybercrimes), Computers' role in crimes	
	1.2	Hacking, Life cycle of Hacking, Types of Hackers (White Hat hackers, Black Hat hackers, Grey Hat hackers), Hacking techniques, Passive and Active Attacks, Social Engineering, Attacks vs Vulnerabilities, Prevention of Cybercrime	
		Self-learning topics: Distinction between computer crimes and conventional crimes.	
2.0		**Introduction to Digital Forensics**	**07**
	2.1	Objectives of digital forensics, Process of digital forensics, Types of digital forensics, Challenges faced by digital forensics	
	2.2	Introduction to Incident - Computer Security Incident, Goals of Incident Response, CSIRT, Incident Response Methodology, Phase after detection of an incident	
		Self-learning topics: Distinction between Computer virus, worm, Trojan horse and trap door.	
3.0		**Digital Evidence and Forensics Duplication**	**07**
	3.1	Digital evidence, Admissibility of evidence, Challenges in evidence handling, collecting digital evidence, Preserving digital evidence, Documenting evidence	
	3.2	Necessity of forensic duplication, Forensic duplicates as admissible evidence, Forensic image formats, Forensic duplication techniques, Disk imaging, Analysis of forensic images using FTK Imager	
		Self-learning topics: Digital Evidence Investigation using Autopsy	
4.0		**System Investigation**	**08**
	4.1	Live/volatile data collection from Windows and Unix Systems	
	4.2	Investigating Windows systems, Investigating UNIX systems, Investigating applications, Web browsers, Email tracing	
	4.3	Recovering digital evidence, Acquiring, Analyzing and duplicating data: dd, dcfldd, foremost, scalpel	
		Self-learning topics: Methods of storing data (RAM and Hard disk)	
5.0		**Network Forensics**	**05**
	5.1	Introduction to intrusion detection systems, Types of IDS, Understanding network intrusion and attacks	
	5.2	Analyzing network traffic, collecting network based evidence, Evidence handling. Investigating routers	
		Self-learning topics: Use of packet sniffing tools like Wireshark	
6.0		**Laws related to cyber crime**	**04**
		Constitutional law, Criminal law, Civil law, Levels of law: Local laws, State laws, Federal laws, International laws. Levels of culpability: Intent, Knowledge, Recklessness, Negligence. CFAA, DMCA, CAN Spam	
		Self-learning topics: Relevant law to combat computer crime –Information Technology Act	
		Total	**39**