CYBER FORENSICS

(Professional Elective – II)

Course Code	20IT4601A	**Year**	III	**Semester**	II
Course Category	PE-II	**Branch**	IT	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	-
Continuous Internal Evaluation:	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		**Blooms Taxonomy Level**
Upon successful completion of the course, the student will be able to		
CO1	Understand the basic terminology of cybercrimes	**L2**
CO2	Apply a number of different computer forensic tools to a given scenario	**L3**
CO3	Understand the basics of computer forensics	**L2**
CO4	Analyze and validate digital evidence data	**L3**
CO5	Analyze acquisition methods for digital evidence related to system security	**L3**

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations (3:Substantial, 2: Moderate, 1:Slight)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO 11**	**PO 12**	**PSO1**	**PSO2**
CO1				3	3	3						3		
CO2				3	3	3						3		
CO3				3	3	3						3	3	3
CO4				3	3	3						3	3	3
CO5				3	3	3						3	3	3

Syllabus		
Unit No	**Contents**	**Mapped CO**
I	**Introduction To Cybercrime**: Introduction, Role of Electronic Communication Devices and Information and Communication Technologies in Cybercrime, Types of Cybercrime, Cybercrime against Individuals, Property, Nation, Crimes associated with mobile electronic communication devices, classification of cybercriminals, Execution of cybercrime, tools used in cybercrime, factors influencing cybercrime, challenges to cybercrime, strategies to prevent cybercrimes.	**CO1**
II	**Classification of Cybercrime:** Introduction, Cybercrime against individuals, cybercrime against property, cybercrime against nation. **Cybercrime the present and the future:** Introduction to cyber war, crypto currency, bitcoin, ethereum, comparison between bitcoin and ethereum, blockchain, ransomeware, deep web and dark web and its challenges.	**CO1**
III	**Introduction to cyber forensics**: Interrelation among cybercrime, cyber forensics, and cyber security, cyber forensics, disk forensics, network forensics, wireless forensics, database forensics, malware forensics, mobile forensics, gps forensics ,email forensics, memory forensics, building forensic computing lab, incident and incident handling, computer security incident	**CO2,CO 3**
IV	**Digital Evidence**: Introduction to digital evidence and evidence collection procedure, sources of evidence, digital evidence from standalone computers/electronic communication devices. **Cyber forensics-The present and Future:** Forensic tools, cyber forensic suite, Drive Imaging and validation tools, Forensic tools for integrity verification and hashing, data recovery, ram analysis, analysis of registry, encryption/decryption, analysing network, mobile devices, email analysis, Need for computer forensic investigators, career prospects for forensic investigators.	**CO2,CO 4**
V	**Acquisition and handling of digital evidence:** preliminaries of electronic or digital evidence, acquisition and seizure of evidence, chain of custody and digital evidence collection form, fourth amendment and seizure, acquisition of computer and electronic evidence. acquisition of evidence form optical and removal media, digital cameras.	**CO4,CO 5**

Learning Resources
Text book
1.Dejay, Murugan, Cyber Forensics Oxford university press India Edition, 2018.
References
1.CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2015.
e-Resources and other Digital Material
1.http://www.cyberforensics.in/ 2.https://evestigate.com/computer-forensics-links/