COURSE CODE	COURSE TITLE	L	T	P	C
1152CS128	FORENSICS AND CYBER APPLICATIONS	3	0	0	3

Course Category: Program Elective

A. Preamble:

Computer and communication technologies have become the key components to support critical infrastructure services in various sectors of our society. In an effort to share information and streamline operations, organizations are creating complex networked systems and opening their networks to customers, suppliers, and other business partners. Increasing network complexity, greater access, and a growing emphasis on the Internet have made information and network security a major concern for organizations. Students will learn different aspects of computer and cybercrime and ways in which to uncover, protect, exploit, and document digital evidence. Forensics is the application of scientifically proven methods to gather, process, interpret, and to use digital evidence to provide a conclusive description of cybercrime activities. Cyber forensics also includes the act of making digital data suitable for inclusion into a criminal investigation.

B. Prerequisite Courses:

Sl No	Course Code	Course Name
1	1151CS111	Computer Networks
2	1152CS101	Cryptography and Network Security

C.Related Courses:

Sl No	Course Code	Course Name
1	1156CS601	Minor Project
2	1156CS701	Major Project

D. Course Educational Objectives:

Students undergoing this course are familiarized to:

- Basics of Computer Networks.
- Fundamentals of Mac Protocols.
- Foundations of digital Forensics.
- Cyber Applications.
- Digital Evidence.

E. Course Outcomes:

Upon the successful completion of the course, students will be able to:

CO Nos.	Course Outcomes	Knowledge Level (Based on revised Bloom's Taxonomy)
CO1	Describe the basic concepts of computer networks.	K2
CO2	Illustrate MAC protocol operation and MAC addressing.	K2
CO3	Summarize Principles, Preservation, Motive, and Technology of Computer Crime Digital Investigation	K2
CO4	Apply Forensic Science on Computer based Digital Investigation of Cyber applications.	K3
CO5	Explain about Digital Evidence on various Layers.	K2

F. Correlation of COs with POs:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO 1	PSO 2	PSO 3
CO1	**H**	**L**	**L**										**L**		
CO2	**M**	**M**	**L**	**L**									**L**	**L**	**L**
CO3	**M**	**M**	**L**	**L**	**M**								**M**	**L**	
CO4	**H**	**M**	**M**	**L**	**L**	**L**		L					**L**	**M**	**L**
CO5	**H**	**M**	**L**	**L**		**L**		L					**L**	**L**	**L**

G. Course Content:

UNIT I Basics of Computer Networks **9**

Protocols and Standards-OSI Model, TCP/IP Model, Network topology (Physical & logical), LAN standards, Ethernet (802.3)-Transmission media: Guided transmission media - Twisted Pair, Coaxial and Fiber-optic cables, switching techniques: Circuit switching, Packet switching and message switching-Network Hardware Components: Connectors, Repeaters, hubs, NICs, Bridges and Switches

UNIT II Fundamentals of Mac Protocols **9**

Motivation for a specialized MAC, Fundamentals of MAC protocols, Sensor MAC Case Study (Protocol overview, Periodic listen and sleep operations, Schedule selection and coordination, Adaptive listening, Message passing), IEEE 802.15.4 protocol: Physical, MAC layer, naming and addressing, Assignment of MAC addresses, Distributed assignment of locally unique addresses, content based and geographic addressing

UNIT III Foundations of digital Forensics **9**

Language of Computer Crime Investigation- Digital Evidence of Courtroom-Cybercrime Law: United State Perspective, Indian Perspective, Indian IT Act, conductive Digital Investigation, Handling a Digital Crime Scene: Principles, Preservation, Modus Operandi, Motive, and Technology.

UNIT IV Cyber Applications **9**

Violent Crime and Digital Evidence-Digital Evidence as Alibi- Gender Offenders on the Internet-Computer Intrusions-Cyber Stalking-Computer Basics for Digital Investigators-Applying Forensic Science to Computers

UNIT V Digital Evidence **9**

Digital Evidence on Windows Systems-Digital Evidence on UNIX Systems- Digital Evidence on Mobile Devices- Intellectual Property Rights-Network Basics for Digital Investigators-Applying Forensic Science to Networks- Digital Evidence on the Internet-Digital Evidence on Physical and Data-Link Layers-Digital Evidence at the Network and Transport Layers, Security and Fraud detection in Mobile and wireless networks.

Total 45 Hours

H. Learning Resources

i. Text Books:

1 Digital Evidence& Computer Crime, Eoghan Casey Bs Ma Ac, ELSEVIER-Academic Press, Third Edition (2011), ISBN 13: 978-0123742681, ISBN 10 : 0123742684

2. Kurose, Ross "Computer Networking a Top Down Approach Featuring the Internet", Pearson; 6th edition (March 5, 2012), ISBN-10: 0132856204, ISBN-13: 978-0132856201

ii. Reference Books:

1.Guide to Computer Forensics & Investigation, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning, Fourth Edition, ISBN 13: 978-1435498839, ISBN 10: 1435498836

2. Ivan Stojmenovic, Handbook of Wireless Networks and Mobile Computing, Wiley India Student Edition, ISBN 978-81-265-0768-9

3. Unix and Linux System Administration Handbook, EviNemeth, Garth Snyder, et al, Person Publication,

iii. Online resources

1. http://resources.infosecinstitute.com/computer-forensics-tools
2. http://www.cybrary.it/course/computer-hacking-forensics-analyst