COURSE CODE	COURSE TITLE	L	T	P	C
1152IT109	**Forensics and Cyber Applications**	**3**	**0**	**0**	**3**

Course Category:

~~Foundation (0)/ Program Core (1)~~**/ Program Elective (2)** / Allied Elec~~tive (3) / University Elective (4) / Value Education Elective (5) / Independent Learning (6) / Industry - Higher Learning Institute Interaction (7)~~

a.Preamble:

The Cyber forensics, sometimes referred to as computer forensic science, is a special branch of digital forensic science that deals with legal evidence accessed from computers and digital media. The goal of digital forensic programs is to examine digital media in detail with the aim of storing, recovering, examining and presenting factual evidence and opinions thereof, about the information

b. Pre-requisites:

Sl. No	Course Code	Course Name
1		Computer Networks

c. Related Courses:

Sl. No	Course Code	Course Name
1		**Cryptography and** network security
2		Web Technology
3		Project Work

d.Course Educational Objectives:

Students undergoing this course are expected to

- To study the basics of networks for Digital investigations.
- Plan and prepare for all stages of an investigation - detection, initial response and management interaction.
- Learn the importance of evidence handling and storage .
- Monitor network traffic and detect illicit servers and covert channels

CONos	Course Outcomes	Level of learning domain(Based on revised Bloom's taxonomy)
CO1	Discuss the security issues network layer and transport layer and Identify, design the new network models for Digital investigators.	K2
CO2	Study and Analyze various Cybercrime Law and Explain digital forensics.	K2
CO3	ıble to design, practice and use safe techniques on the ːal evidence.	K2
CO4	Able to handle various ethical issues related to Forensics	K2
CO5	yze and design different models of Hacking Tools	K3

Unit 1 Network Basics for Digital Investigators

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.

Unit 2 Digital forensics and digital investigation.

Foundations of digital Forensics, 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 3 Violent Crime and Digital Evidence, Cyber Crimes and Investigation Procedures

Violent Crime and Digital Evidence, Digital Evidence as Alibi, Gender Offenders on the Internet, Computer Intrusions, Cyber Forensic and Computer Crimes, Types of Cyber Crimes: Crimes targeting Computers, Online based Cyber Crimes.

Unit 4 Cyber stalking and Evidence Handling

Cyber stalking, Computer Basics for Digital Investigators, Applying Forensic Science to Computers , Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure

Unit 5 Digital Evidence and ETHICAL ISSUES

Digital Evidence on Windows Systems, Digital Evidence on UNIX Systems,Digital Evidence on Mobile Devices, Intellectual Property Rights.. Data Analysis Techniques - Investigating Live Systems (Windows &Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime.

TOTAL : 45 PERIODS

h.Learning Resources

i.Text Books:

1. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001
2. Skoudis. E., Perlman. R. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses.Prentice Hall Professional Technical Reference. 2001.

ii.**References:**

1.Bill Nelson,Amelia Philips and Christopher Steuart, “Guide to computer forensics and investigations”,course technology,4thedition,ISBN: 1-435-49883-6