21CYS05	DIGITAL FORENSICS	L	T	P	C
		3	0	0	3

Course Objectives

- To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
- To understand how to examine digital evidences such as the data acquisition, identification analysis.

UNIT I	Fundamentals of Forensics	9 Hours

Understanding of forensic science, digital forensic, The digital forensic process, Locard's exchange principle, Scientific models. Basic computer organization, File system, Memory organization concept, Data storageconcepts , Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues.

UNIT II	Computing Investigations	9 Hours

Introduction to cybercrime scene, Documenting the scene and evidence, maintaining the chain of custody, forensic cloning of evidence, Live and dead system forensic, Hashingconcepts to maintain the integrity of evidence, Report drafting.

UNIT III	Processing Crime and Incident Scene	9 Hours

Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case.

UNIT IV	Data Acquisition	9 Hours

Data acquisition- understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools.

UNIT V	Forensics Tools	9 Hours

Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-Mail investigations- investigating email crime and violations, understanding E-Mail servers, specialized E-Mail forensics tool.

UNIT VI	CASE STUDIES	

Case studies on digital forensics tools and techniques

TOTAL PERIODS: 45

Course Outcomes:

At the end of the course, Students can able to

- Describe Forensic science and Digital Forensic concepts
- Determine various digital forensic Operandi and motive behind cyber attacks
- Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective.
- Demonstrate various forensic tools to investigate the cybercrime and to identify the digital pieces of evidence
- Analyze the digital evidence used to commit cyber offences.

Text books:

1. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
2. Nelson, B, Phillips, A, Enfinger, F, Stuart, C., "Guide to Computer Forensics and Investigations, 2nd ed., Thomson Course Technology, 2006, ISBN: 0-619-21706-5.

Reference Books:

1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.