DIGITAL FORENSICS
(Elective-1)

Course Code: 13CS2106 **L P C**
4 0 3

Course Outcomes:

At the end of the course, a student will be able to:

CO1: Describe evidential potential of digital devices and device handling and examination principles

CO2: Explain Seven element model of digital security and ISO/OSI Model

CO3: Explain essential elements and characteristics of computer Forensics

CO4: Compare and contrast Military and Business Computer Forensic Technologies

CO5: Describe Homeland Security Systems

UNIT-I

Introduction & evidential potential of digital devices - Key developments, Digital devices in society, Technology and culture, Comment, Closed vs. open systems, evaluating digital evidence potential.

Device Handling & Examination Principles : Seizure issues, Device identification, Networked devices, Contamination, Previewing, Imaging, Continuity and hashing, Evidence locations.

UNIT-II

A sevenelement security model, A developmental model of digital s ystems, Knowing,Unknowing, Audit and logs, Data content, Data context. Internet & Mobile Devices The ISO/OSI model, The internet protocol suite, DNS, Internet applications, Mobile phone PDAs, GPS, Other personal technology.

UNIT-III

Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/ Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps Taken by Computer Forensics Specialists, Who Can Use Computer Forensic Evidence?, Case Histories, Case Studies.

UNIT-IV

Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer
Forensic Technology, Types of Business Computer Forensic Technology, Specialized
Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption
Methods and Vulnerabilities, Protecting Data from Being Compromised, Internet Tracing Methods 65.

UNIT-V

Homeland Security Systems. Occurrence of Cyber Crime, Cyber Detectives, Fighting Cyber Crime withRiskManagement Techniques, Computer Forensics Investigative Services, Forensic Process improvement, Course Content, Case Histories.

Text Books:

1. Angus M.Mashall, "Digital Forensics", 2nd Edition,Wiley-Blackwell, A John Wiley & Sons Ltd Publication, 2008.
2. John R. Vacca, " Computer forensics: Computer Crime Scene Investigation", 2nd Edition,Charles River Media, Inc. Boston, Massachusetts.

References:

1. Michael G. Noblett; Mark M. Pollitt, Lawrence A. Presley (October 2000), "Recovering and examining computer forensic evidence", Retrieved 26 July 2010.
2. Leigland, R (September 2004). "A Formalization of Digital Forensics".(Pdf document).
3. Geiger, M (March 2005). "Evaluating Commercial Counter-Forensic Tools"(Pdf document).