

**DIGITAL FORENSICS****Course Code:** 13CS2106**L P C**  
**4 0 3****Pre requisites:** Secure Protocols, Image processing.**Course Outcomes:**

Upon completion, the student will be able to

CO1 : Utilize a systematic approach to computer investigations.

CO2 : Utilize various forensic tools to collect digital evidence.

CO3 : Perform digital forensics analysis upon Windows,MAC and  
LINUX operating systems

CO4 : Perform email investigations.

CO5 : Analyze and carve image files both logical and physical

**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 systems, 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 with Risk Management Techniques, Computer Forensics Investigative Services, Forensic Process Improvement, Course Content, Case Histories.

**TEXT BOOKS:**

1. Angus M. Mashall, “Digital Forensics”, 2<sup>nd</sup> Edition, Wiley-Blackwell, A John Wiley & Sons Ltd Publication, 2008.
2. John R. Vacca, “Computer forensics : Computer Crime Scene Investigation”, 2<sup>nd</sup> 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).