**Elective IV: Digital Forensics**

**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 seven element 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.

**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, Case Histories.

**Unit VI:** The violation of privacy during information words. The individual exposed. Advanced computer Forensics systems and future directionsadvanced, encryption, hacking, advanced trackers, case studies. 44

**Text Books:** 1. Digital Forensics, Angus M. Marshall, 2nd Edition, Wiley-Blackwell, John Wiley and Sons, 2008.

2. Computer forensics: Computer Crime Scene Investigation, John R. Vacca, 2nd Edition, Charles River Media, 2002.

**Reference Books:** 1. Recovering and examining computer forensic evidence, Michael G. Noblett; Mark M. Pollitt and Lawrence A. Presley, 2000.

2. A Formalization of Digital Forensics, R Leigland, 2004.

3. Evaluating Commercial Counter-Forensic Tools, M. Geiger, DFRWS-2005.

4. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Albert J. Marcella and Robert S. Greenfield, Auerbach Publications, 2007.

5. Handbook of Computer Crime Investigation: Forensic Tools and Technology, Eoghan Casey, Academic Press, 2001.

6. Privacy Protection and Computer Forensics, Second Edition, Michael Caloyannides, Artech House, 2004.

 7. Computer Forensics: Incident Response Essentials, Warren G. Kruse and Jay G. Heiser, Addison Wesley, 2001