

UNIT II Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for organisations, Organisational Measures for Handling Mobile, Organisational Security Policies and Measures in Mobile Computing Era, Laptops. TOOLS AND METHODS USED IN CYBERCRIME : Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft).
(12 Hours)
UNIT III UNDERSTANDING COMPUTER FORENSICS : Introduction, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics. Forensics and Social Networking Sites: The Security/Privacy Threats, Computer Forensics from Compliance Perspective, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing, Anti Forensics.
(12 Hours)
Textbooks : 1. Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives”, Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013. 2. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, KLSI. “Introduction to information security and cyber laws”. Dreamtech Press. ISBN: 9789351194736, 2015. 3. Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions”, Copyright © 2014 by John Wiley & Sons, Inc
Semester - III
CSCH 501: DIGITAL FORENSICS
Course Objectives : 1. To make the student aware of the need to perform forensic of the computer and digital devices from the point of forensic investigation. 2. To make the student aware of the procedures required to keep the digital trail of

crimes, in the modern world
Course Outcomes : 1. Student gets the skills required to preserve the digital trail of crimes, both computer crimes and conventional crimes 2. Student gets the skill required to perform the forensic investigation in line with the legal framework of the nation
UNIT I Introduction To Digital Forensics : Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness, Computer Forensics Investigation Process : Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyse The Data, Report The Investigation, Digital Evidence And First Responder Procedure, Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics
(16 Hours)
UNIT II Understanding Storage Media And File System : Hard Disk Drive, Details Of Internal Structure Of Hdd, The Booting Process, File System, Windows Forensics : Introduction, Recovering Deleted Files And Partitions, More About Recovering Lost Files/Data, Logs & Event Analysis And Password Cracking : Introduction, Windows Registry, Windows Event Log File, Windows Password Storage, Application Passwords Crackers, Network Forensics : Introduction, Network Components And Their Forensics Importance, Osi, Forensics Information From Network, Log Analysis, Forensics Tools, Wireless Attacks : Introduction, 4.3 wireless Fidelity (Wi-fi)(802.11), Wireless Security, Wireless Attacks Detection Techniques, Wireless Intrusion Detection Systems
(16 Hours)
UNIT III Investigating Web Attacks : Introduction, Types Of Web Attacks, Web Attack Forensics, Web Application Forensics Tools, Investigating Email Attacks : Introduction, Email Attacks And Crimes, Privacy In Emails, Email Forensics, Email Forensic Tools, Mobile Device Forensics : Introduction, Challenges In Mobile Forensics, Mobile Communication, Evidences In A Mobile Device, Mobile Forensic Process, Forensic Acquisition Tools, Investigative Reports, Expert Witness And Cyber Regulations : Introduction, Report Preparation, Legal Aspects Of Computing
(16 Hours)
Textbooks : 1. “Digital Forensics”, Dr.Jeetendra Pande, Dr. Ajay Prasad, Uttarakhand Open