

| B.Sc. Forensic Science: Semester-V |                               |
|------------------------------------|-------------------------------|
| FST501: Digital Forensics          |                               |
| <b>Teaching Scheme</b>             | <b>Examination Scheme</b>     |
| Lectures: 3 hrs/Week               | Class Test -12 Marks          |
| Tutorials: 1 hr/Week               | Teachers Assessment – 6 Marks |
|                                    | Attendance – 12 Marks         |
| Credits: 4                         | End Semester Exam – 70 marks  |

Course Objectives: After studying this paper the students will know –

- The basics of digital forensics.
- The cases which fall under the purview of digital crimes.
- The types of digital crimes.
- The elements involved in investigation of digital crimes.

**Unit 1: Fundamentals and Concepts**

Fundamentals of computers Hardware and accessories – development of hard disk, physical construction, CHS and LBA addressing, encoding methods and formats. Memory and processor. Methods of storing data. Operating system. Software. Introduction to network, LAN, WAN and MAN.

**Unit 2: Computer Crimes**

Definition and types of computer crimes. Distinction between computer crimes and conventional crimes. Reasons for commission of computer crimes. Breaching security and operation of digital systems.

**Unit 3: Malware and Other Crimes**

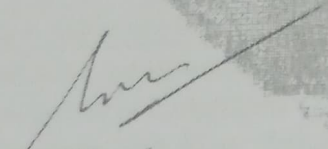
Computer virus, and computer worm – Trojan horse, trap door, super zapping, logic bombs. Types of computer crimes – computer stalking, pornography, hacking, crimes related to intellectual property rights, computer terrorism, hate speech, private and national security in cyber space. An overview of hacking, spamming, phishing and stalking.

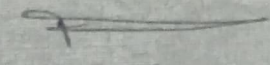
**Unit 4: Computer Forensics Investigations**

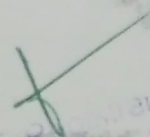
Seizure of suspected computer. Preparation required prior to seizure. Protocol to be taken at the scene. Extraction of information from the hard disk. Treatment of exhibits. Creating bitstream of the original media.

**Unit 5: Collection and Seizure of Magnetic Media**

Legal and privacy issues. Examining forensically sterile media. Restoration of deleted files. Password cracking and E-mail tracking. Encryption and decryption methods. Tracking users.

  
Head  
Department of Biotechnology  
Invertis University, Bareilly (U.P.)

  
Dean  
Faculty of Science  
Invertis University, Bareilly (U.P.)

  
Registrar  
Invertis University  
Bareilly