| **IS379 Digital Information Forensics** | | | |
|---|---|---|---|
| **Credit Hours:** | 2-1-3 | **Prerequisites** | IS201 |

**Course Learning Outcomes:**

| S No | CLO | Domain | Taxonomy Level | PLO |
|---|---|---|---|---|
| 1. | Understand the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing | Cognitive | 2 | 1 |
| 2. | Analyze the file system storage mechanisms of two common desktop opera ting systems (i.e. versions of Microsoft Windows and LINUX | Cognitive | 4 | 2 |
| 3. | Use tools for faithful preservation of data on disks for analysis and find data that may be clear or hidden on a computer disk | Psychomotor | 3 | 5 |
| 4. | Learn use of computer forensics tools used in data analysis, such as searching, absolute disk sector viewing and editing, recovery of files, password cracking, etc. | Psychomotor | 3 | 4 |

**Course Content:**

Introduction to Computer Forensics, Historical and current issues, Roles of Information Technology, Legal, and Law Enforcement professionals, Case examination and assessment, Evidence gathering, Systematic approaches to computer investigations, Conducting an investigation, Hardware and software requirements, Physical Layout of Lab, Review of file structures, boot processes, and data structures of popular operating systems, Preparing for an investigation, Processing the crime scene, Securing, cataloging and storing the evidence, Forensic cleansing, Identify methods, Utilization of various data acquisition tools, Hashing algorithms concepts, Utilization of various analysis tools, Recognizing, locating, recovering and analyzing images, Network Forensics, Email investigations, Reporting guidelines, Witness Requirements. Smartphone Forensics, Physical and Logical Keyword Searching, Data Carving,

Exporting and Bookmarking Data, Malware Scanning, Reporting, SIM Card Handling and Examination, SD Card Handling and Examination, Android and Malware Forensics

**Teaching Methodology:**

Lectures, Written Assignments, Semester Project, Presentations

**Course Assessment:**

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

**Reference Materials:**


1. Guide to Computer Forensics and Investigations 6th Edition, Bill Nelson, Amelia Phillips, Christopher Steuart, 2018
2. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet 3rd Edition, Eogan Casey, 2011
3. Real Digital Forensics: Computer Security and Incident Response, 1st Edition, Keith J. Jones, Richard Bejtlich, Curtis W Rose, 2005