AMITY UNIVERSITY
MADHYA PRADESH
Established vide Government of Madhya Pradesh Act No. 27 of 2010

# Syllabus

| **Programme Name:** B. Tech. (Computer Science and Engineering) | | **Session:**2024-28 |
|---|---|---|
| **Course Code:** IT 402 | **Course Name:** CYBER SECURITY AND DIGITAL FORENSICS | **Semester:** IV |

| **Credits (Total)** | **L** | **T** | **P** | **Marks (Internal/External** | | **Contact Hours (per week)** | **Independent Study Hour (per week)** | **Section (Group)** |
|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 0 | 0 | 40 | 60 | 3 | 3 | |
| **UG level** | | | | | | **Basic and applied** | **Student-specific course outcome** | **Higher Education Research Placement** |

**Course Objective:**

To provide an understanding of Computer forensics fundamentals. To analyze various computer forensics technologies. To provide computer forensics systems. To identify methods for data recovery. To apply the methods for preservation of digital evidence.

**Course outcomes:** After completion of course, the student will be able to:

| | |
|---|---|
| **CO-1** | Understand the definition of Digital forensics fundamentals. |
| **CO-2** | Describe the types of digital forensics technology. |
| **CO-3** | Analyze various digital forensics systems. |
| **CO-4** | Illustrate the methods for data recovery, evidence collection and data seizure. |
| **CO-5** | Summarize duplication and preservation of digital evidence. |

**Teaching Pedagogy:**

| | |
|---|---|
| **T1** | Classroom teaching (white board), Power Point Presentations, Interactive lectures, Inquiry based teaching |
| **T2** | ABL activities, Assignments, Flip Class/ Seminars, Quiz, Oral Viva-voce examination |

**Assessment Tools**

| | |
|---|---|
| **AT1-1** | Quiz |

| | |
|---|---|
| **AT1-2** | Activity Based Learning |
| **AT1-3** | Midterm Exams |
| **AT1-4** | Flip Class |
| **AT1-5** | Seminar Presentation |
| **AT1-6** | Assignments |
| **AT1-7** | Poster |
| **AT1-8** | Oral Viva-voce examination |
| **AT1-9** | Industrial Visit Report |

**Prerequisites:** Basic knowledge of computer networks.

| | |
|---|---|
| **Suggested reading:** | ● Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley<br>● Jennifer L. Bayuk, J. Healey, P. Rohmeyer, Marcus Sachs, Jeffrey Schmidt, Joseph Weiss Cyber Security Policy Guidebook, John Wiley & Sons 2012.<br>● Vivek sood, Cyber law simplified, Tata Mc GrawHill, E ducation (India). Eoghan Casey, Handbook of digital forensic and investigation.<br>● References:<br>● Clint P Garrison, Digital forensic for network, internet and cloud computing.<br>● Panagiotis Kandlis, Digital crime and forensic science in cyberspace, information society S.A Greece IDEA Group Publishing.<br>● John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, Charles, River Media, 2005 ISBN: 1584503890, 9781584503897 |
| **Suggested e- resources (Websites/e-books)** | **https://onlinecourses.nptel.ac.in/noc23_cs127/preview** |

# SYLLABUS

| Module wise contents details | Assessment tools |
|---|---|
| **Module I: Introduction: (9 Hours)**<br>Introduction, Classifications of Cyber Crimes: E - Mail Spoofing, Spamming, Cyber defamation, Industrial Spying/Industrial Espionage, Hacking, Software Piracy, Password Sniffing, Credit Card Frauds, Cyber stalking, Botnets , Phishing, Pharming, Man - in - the - Middle attack, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, DoS and DDoS Attacks , SQL Injection, Buffer Overflow | Quiz<br>Mid-term Exam<br>Assignment |
| **Module II: Cybersecurity Concepts: (9 Hours)**<br>Introduction to Cyber Security, Cyber Security Goals, Cyber Security policy, Domain of Cyber Security Policy, Elements, Cyber Security Evolution, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team | Mid-Term Quiz<br>Assignment |
| **Module III: Digital Forensics Fundamentals: (9 Hours)**<br>Introduction to Digital Forensics, Use of Digital Forensics in Law Enforcement, Digital Forensics Assistance to Human Resources/Employment Proceedings, Digital Forensics Services, Benefits of Professional Forensics Methodology. | Mid-Term Oral Viva-voce examination<br>Seminar<br>Presentation |
| **Module IV: Types of Computer Forensics Technology: (9 Hours)**<br>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. Protecting Data from Being Compromised, Avoiding Pitfalls with Firewalls | Quiz, Assignment, Industrial Visit,Report Seminar, Presentation |
| **Module V: Cyber Law and Cyber Crime: (9 Hours)**<br>Introduction to IT laws & Cyber Crimes, Cyber Laws, IPR, Legal System of Information Technology, Social Engineering. Reporting Cybercrime, Difference between cyber forensics and cyber security. | Quiz, Assignment, Industrial Visit, Report, Poster, Oral Viva-voce examination |

**Assessment Plan:**

| **Component of Evaluation** | **Description** | **Code** | **Weightage %** |
|---|---|---|---|
| Continuous Internal Evaluation | Mid Term | CT | 15% |
| | Seminar/Viva-Voce/Quiz/Home Assignment | S/V/Q/HA | 20% |
| Attendance | A minimum of 75% Attendance is required to be maintained by a student to be qualified for taking the End Semester examination. The dispensation of 25% includes all types of leaves. including medical leaves. | A | 5% |
| End Semester Examination | End Semester Examination | ESE | 60% |
| **Total** | | | **100%** |

**Abbreviations:** CT: Class Test, HA: Home Assignment, S/V/Q: Seminar/Viva/Quiz, ESE: End Semester Examination; A: Attendance

**Course Articulation Matrix (Mapping of COs with POs)**

| **Course Outcomes** | **Correlation with POs** | | | | | | | | | | | | **Correlation with PSOs** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO10** | **PO11** | **PO12** | **PSO1** | **PSO2** | **PSO3** |
| **CO1** | 3 | 3 | 1 | 3 | 1 | | | | 2 | | 2 | 1 | | | |
| **CO2** | 3 | 2 | 2 | 2 | 2 | | | | 2 | | 1 | 1 | | | |
| **CO3** | 3 | 2 | 2 | 2 | 2 | | | | 3 | | 3 | 1 | | | |
| **CO4** | 3 | 3 | 2 | 3 | 2 | | | | 1 | | 2 | 1 | | | |
| **CO5** | 2 | 2 | 1 | 2 | 3 | | | | 2 | | 2 | 1 | | | |

1: strongly related, 2: moderately related and 3: weakly related