# FACULTY OF COMPUTER SCIENCE

## Master of Computer Application (Sem-IV)

In Effect from Academic Year 2017-18

| Subject Code : 1CS2010408 | Subject Title: CYBER SECURITY & FORENSIC (CSF) |
|---|---|
| Pre-requisite : | Basic fundamental knowledge of Networking , Web Application, Mobile Application and Relational Database Management System |

Course Objective:

The objectives of the course are to:

- To understand the major concepts of Cyber Security and Forensics and to create the Awareness through simple practical tips and tricks and to educate the students to learn How to avoid becoming victims of cyber crimes.
- The subject and the course content will help to the student who wish to take up cyber Forensics as career as well as those who want to seek careers in cyber security.
- To gain experience of doing independent study and research in the field of cyber Security and cyber forensics.

| Teaching Scheme (Hours per week) | | | | Evaluation Scheme (Marks) | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | Theory | | Practical | | |
| Lecture | Tutorial | Practical | Credit | University Assessment | Continuous Assessment | University Assessment | Continuous Assessment | Total |
| 4 | -- | 3 | 7 | 60 | 40 | 30 | 20 | 150 |

| Subject Contents | | | |
|---|---|---|---|
| Sr. No | Topic | Total Hours | Weight (%) |
| 1 | **Introduction to Cybercrime:**<br>Introduction, Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Newsgroup Spam/Crimes from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses , Software Piracy, Password Sniffing, Credit Card Frauds and Identity Theft. Cyber offenses: How Criminals Plan that attack, Categories of Cybercrime, How Criminals Plan the Attacks: Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, Cyber stalking,<br>Cyber cafe and Cybercrimes, Botnets : The Fuel for Cybercrime, Attack Vector and Cloud Computing. | 8 | 20 |
| 2 | **Cybercrime: Mobile and Wireless Devices:**<br>Introduction, Proliferation of Mobile and Wireless Devices, 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,<br>Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era and Laptops. | 7 | 10 |
| 3 | **Tools and Methods Used in Cybercrime:**<br>Introduction, Proxy Servers and A nonymizers , Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.<br>Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft): Types of Identity Theft, Techniques of ID Theft, Identity Theft-Countermeasures, How to Protect your Online Identity. | 12 | 25 |

| | | | |
|---|---|---|---|
| **4** | **Cybercrimes and Cyber security: The Legal Perspectives:**<br>Introduction, Why Do We Need Cyber laws: The Indian Context, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Amendments to the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario. | 5 | 10 |
| **5** | **Understanding Computer Forensics:**<br>Introduction, Historical Background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber forensics and Digital Evidence, Forensics Analysis of E-Mail : RFC282, 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, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing and Anti forensics. | 10 | 25 |
| **6** | Forensics of Hand-Held Devices:<br>Introduction, Hand-Held Devices and Digital Forensics, Toolkits for Hand - Held Device Forensics: EnCase, Device Seizure and PDA Seizure, Palm DD, Forensics Card Reader, Cell Seizure, MOBILedit!, ForensicSIM, Organizational Guidelines on Cell Phone Forensics:<br>Hand - Held Forensics as the Specialty Domain in Crime Context. | 6 | 10 |

**Course Outcome:**

At the end of this course, the student would be able

- To Understand Cybercrimes and solve the problem.
- To Understand Computer Forensics Techniques.
- To be able to Understand Cybercrimes and Cyber security Legal Perspectives.

**List of References:**

1. Nina Godbole, Sunit Belapur, “Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley India Publications, April, 2011
2. James Graham, Richar Howard,Ryan Olson, “Cyber Security Essentials”, CRC Press, Tailor And Francis Group, 2011.

**Indicative Practical List:**

1. Study of following network emulators:
   a. WHOIS Search
   b. Whois CLI Command
   c. Nslookup
   d. Host
   e. Ping
   f. Traceroute
   g. Netstat
2. Configuring a LAN, MAN and WAN to show how the communication takes place using Packet Tracer.
3. Create a malicious program that is:
   a. Virus
   b. Worm
   c. Trojan
   d. Dropper
4. TCP scanning using NMAP .
5. Port scanning using NMAP .
6. TCP / UDP connectivity using Netcat .

7. Network vulnerability using OpenVAS .
8. Web application testing using DVWA .
9. Manual SQL injection using DVWA .
10. Automated SQL injection with SqlMap .
11. Explain in details collected during live analysis.
12. Perform image acquisition of the first partition carry out a dead analysis on image.
13. Perform a forensic analysis through autopsy sleuth kit.
14. Perform forensic analysis through helix.
15. Study “omni peek “ and perform live network analysis to capture packets.
16. Perform forensic data recovery through(Icare) a disk drill.
17. Perform forensic hash analysis and integrity check of evidence through FCIV and windiff.