|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Savitribai Phule Pune University**  **Fourth Year of Computer Engineering (2019 Course)**  **Elective III**  **410244(C):** **Cyber Security and Digital Forensics** | | | | |
| **Teaching Scheme: TH: 03 Hours/Week** | | **Credit 03** | **Examination Scheme: In-Sem (Paper): 30 Marks End-Sem (Paper): 70 Marks** | |
| **Prerequisite Courses:** Computer Networks and Security(310244), Information Security(310254(A)) | | | | |
| **Companion Course:** 410246: Laboratory Practice IV | | | | |
| **Course Objectives:**   * To enhance awareness cyber forensics. * To understand issues in cyber crime and different attacks * To understand underlying principles and many of the techniques associated with the digital forensic practices * To know the process and methods of evidence collection * To analyze and validate forensic data collected. * To apply digital forensic knowledge to use computer forensic tools and investigation report writing. | | | | |
| **Course Outcomes:** At the end of the course, the student should be able to:  CO1: Analyze threats in order to protect or defend it in cyberspace from cyber-attacks. CO2: Build appropriate security solutions against cyber-attacks.  CO3:Underline the need of digital forensic and role of digital evidences. CO4: Explain rules and types of evidence collection  CO5: Analyze, validate and process crime scenes  CO6: Identify the methods to generate legal evidence and supporting investigation reports. | | | | |
| Course Contents | | | | |
| **Unit 1** | **Introduction to Cyber Security** | | | **06 Hours** |
| Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: crime against an individual, Crime against property, Cyber extortion, Drug trafficking, cyber terrorism. Need for Information security, Threats to Information Systems, Information Assurance, Cyber Security, and Security Risk  Analysis. | | | | |
| **#Exemplar/Case Studies** | | Data Breach Digest – Perspective & Reality : <http://verizonenterprise.com/databreachdigest> | | |
| **\*Mapping of Course Outcome for Unit I** | | CO1 | | |
| **Unit 2** | **Cyber Crime Issues and Cyber attacks** | | | **06 Hours** |
| Unauthorized Access to Computers, Computer Intrusions, Viruses, and Malicious Code, Internet Hacking and Cracking, Virus and worms, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Cybercrime prevention methods, Application security (Database, E-mail, and Internet), Data Security Considerations-Backups, Archival Storage and Disposal of Data, Security Technology-Firewall and  VPNs, Hardware protection mechanisms, OS Security | | | | |
| **#Exemplar/Case Studies** | | Cyber Stalking types & their cases respectively | | |
| **\*Mapping of Course Outcome for Unit II** | | CO2 | | |
| **Unit 3** | **Introduction to Digital Forensics** | | | **06 Hours** |
| What is Computer Forensics?, Use of Computer Forensics in Law Enforcement, Computer Forensics  Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Professional Forensics Methodology, Steps taken by Computer Forensics Specialists Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement — Computer Forensic Technology, Types of Business Computer Forensic Technology Computer Forensics Evidence and Capture: Data Recovery Defined, Data Back-up and Recovery, The Role of Back-up in Data  Recovery, The Data-Recovery Solution. | | | | |
| **#Exemplar/Case Studies** | | Demonstrate practice Linux networking security recovery commands.&  Study Tools viz; FTK & The Sleuth Kit | | |
| **\*Mapping of Course Outcome**  **for Unit III** | | CO3 | | |
| **Unit 4** | **Evidence Collection and Data Seizure** | | | **06 Hours** |
| Why Collect Evidence? Collection Options ,Obstacles, Types of Evidence — The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene — Computer Evidence Processing Steps, Legal Aspects of Collecting and Preserving Computer Forensic Evidence Computer Image Verification and Authentication: Special Needs of  Evidential Authentication, Practical Consideration, Practical Implementation. | | | | |
| **#Exemplar/Case Studies** | | | Understand how computer forensics works by visiting: <http://computer.howstuffworks.com/computer-forensic.htm/printable>(23  December 2010) | |
| **\*Mapping of Course Outcome for Unit IV** | | | CO4 | |
| **Unit 5** | **Computer Forensics analysis and validation** | | | **06 Hours** |
| Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, and performing remote acquisitions Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project. Processing Crime and Incident Scenes: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash,  reviewing a case | | | | |
| **#Exemplar/Case Studies** | | | Discuss cases under Financial Frauds, Matrimonial Frauds, Job Frauds,  Spoofing, and Social media. Then write down safety tips, precautionary measures for the discussed fraud cases. | |
| **\*Mapping of Course Outcomes**  **for Unit V** | | | CO5 | |
| **Unit 6** | **Current Computer Forensic tools** | | | **06 Hours** |
| Evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations,  understanding e-mail servers, using specialized e-mail forensic tools. | | | | |
| **#Exemplar/Case Studies** | | | Install Kali Linux & practice following examples:  1. [https://www.youtube.com/watch?time\_continue=6&v=MZXZctqIU-](https://www.youtube.com/watch?time_continue=6&v=MZXZctqIU-w&feature=emb_logo) [w&feature=emb\_logo](https://www.youtube.com/watch?time_continue=6&v=MZXZctqIU-w&feature=emb_logo) | |
| **\*Mapping of Course Outcome for**  **Unit VI** | | | CO6 | |
| **Learning Resources** | | | | |
| **Text Books:**   1. John R. Vacca, “Computer Forensics”, Computer Crime Investigation Firewall Media, New Delhi. 2. Nelson, Phillips Enfinger, Steuart, “Computer Forensics and Investigations”, CENGAGE Learning | | | | |
| **Reference Books:** | | | | |

|  |
| --- |
| 1. Keith J. Jones, Richard Bejtiich, Curtis W. Rose, “Real Digital Forensics”, Addison- Wesley Pearson Education 2. Tony Sammes and Brian Jenkinson, “Forensic Compiling”, A Tractitioneris Guide, Springer International edition. 3. Christopher L.T. Brown, “Computer Evidence Collection & Presentation”, Firewall Media. 4. Jesus Mena, “Homeland Security, Techniques & Technologies”, Firewall Media. |
| **e books:**   1. [**https://www.pdfdrive.com/computer-forensics-investigating-network-intrusions-and-cyber-crime-**](https://www.pdfdrive.com/computer-forensics-investigating-network-intrusions-and-cyber-crime-e15858265.html)[**e15858265.html**](https://www.pdfdrive.com/computer-forensics-investigating-network-intrusions-and-cyber-crime-e15858265.html) 2. [**https://dokumen.pub/handbook-of-computer-crime-investigation-forensic-tools-and-technology-**](https://dokumen.pub/handbook-of-computer-crime-investigation-forensic-tools-and-technology-1stnbsped-0121631036-9780121631031.html)[**1stnbsped-0121631036-9780121631031.html**](https://dokumen.pub/handbook-of-computer-crime-investigation-forensic-tools-and-technology-1stnbsped-0121631036-9780121631031.html) 3. **Massachusetts Institute of Technology Open Courseware:** [**https://ocw.mit.edu/courses/electrical-**](https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/)[**engineering-and-computer-science/6-858-computer-systems-security-fall-2014/**](https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/) |
| **MOOC Courses Links:**   * **MIT Open CourseWare: https://ocw.mit.edu/courses/** |

|  |  |
| --- | --- |
| **410244(C): Cyber Security and Digital Forensics** | |
| Any 5 assignments from group 1 and 1 Mini project from group 2 is mandatory. | |
| **Group 1** | |
| **1.** | Write a program for Tracking Emails and Investigating Email Crimes. i.e. Write a program to  analyze e–mail header |
| **2.** | Implement a program to generate and verify CAPTCHA image |
| **3.** | A person on a nearby road is trying to enter into a WiFi network by trying to crack the Password to use the IP Printer resource; write a program detect such attempt and prohibit the access.  Develop the necessary scenario by Using an IEEE 802.11, configure a Wi-Fi adapter and Access Point |

|  |  |
| --- | --- |
| **4.** | Write a computer forensic application program for Recovering permanent Deleted Files and  Deleted Partitions |
| **5.** | Write a program for Log Capturing and Event Correlation |
| **6.** | Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT |
| **7.** | Study of Honeypot |
| **Group 2** | |
| **8.** | **Mini–project-** Design and develop a tool for digital forensic of images |
| **9.** | **Mini Project -** Design and develop a tool for digital forensic of audio |
| **10.** | **Mini Project -:** Design and develop a tool for digital forensic of video |
| **11.** | **Mini Project** - Design a system for the analysis of cyber crime using various cyber forensic  techniques and compare each technique with respect to integrity, confidentiality, availability |