**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES**

**COURSE HANDOUT**

**Part A: Content Design**

|  |  |
| --- | --- |
| **Course Title** | **Cyber Crimes, Forensics and Incident Handling** |
| **Course No(s)** | **SS ZG588** |
| **Credit Units** | 4 |
| **Course Author** | Mohammad Saleem Bagewadi |
| **Version No** | 1.1 |
| **Date** |  |

**Course Objectives**

|  |  |
| --- | --- |
| **No** | **Description** |
| **CO1** | Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes |
| **CO2** | Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues |
| **CO3** | Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response |

|  |  |
| --- | --- |
| **Text Book(s)** | |
| T1 | Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University |
| T2 | Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009 |
| T3 | Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia |
| R1 | Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart |
| R2 | The Basics of Digital Forensics, by John Sammons |
| R3 | Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza |
| R4 | Computer Forensics\_ Investigating Network Intrusions and Cyber Crime: EC-Council Press |

**Learning Outcomes:**

|  |  |
| --- | --- |
| **No** | **Learning Outcomes** |
| LO1 | Fundamental understanding and Information on Cyber Crimes, Digital Forensics  Objectives and Incident Detection and Response Reports. |
| LO2 | Learn on how to prepare investigation on computer-related incidents or crimes and summarize. |
| LO3 | Understand on digital forensics process, models and analysis by taking a systematic approach |
| LO4 | Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues |

**Part B: Content Development Plan**

|  |  |
| --- | --- |
| **Academic Term** | Second Semester 2021- 2022 |
| **Course Title** | **Cyber Crimes, Forensics and Incident Handling** |
| **Course No** | SS ZG588 |
| **Credit** | 4 |
| **Instructor –in-charge** | Amit Dua |

**Glossary of Terms**

|  |  |  |
| --- | --- | --- |
| **Module** | **M** | Module is a standalone quantum of designed content. A typical course is delivered using a string of modules. M2 means module 2. |
| **Contact Session** | **CS** | Contact Session (CS) stands for a 2 hour long live session with students conducted either in a physical classroom or enabled through technology. In this model of instruction, instructor led sessions will be for 16 CS. |
| **Recorded Lecture** | **RL** | RL stands for Recorded Lecture or Recorded Lesson. It is presented to the student through an online portal. A given RL unfolds as a sequences of video segments interleaved with exercises. |
| **Lab Exercises** | **LE** | Lab exercises associated with various modules |
| **Self-Study** | **SS** | Specific content assigned for self-study |
| **Homework** | **HW** | Specific problems/design/lab exercises assigned as homework |

**Modular Structure**

1. Introduction to Cyber Crime, Digital Forensics and Incident Handling
   1. Information On Cyber Crime
   2. Types Of Cyber Hackers
   3. Cyberspace and Criminal Behavior
   4. Traditional Problems Associated with Computer Crime
   5. The Changing Landscape of Cybercrime
   6. Preamble and Scheme Of Information Technology Act
   7. Overview of Digital Forensics and Incident Handling
2. Foundation for Forensics
   1. Networking Concepts required for Forensics
   2. Working with Windows and DOS Systems; Linux Boot Processes and CLI Systems
   3. Introduction to Forensics Science and Need for Digital Forensics; Digital Forensic Techniques
   4. Understanding the Digital Forensics Profession
3. Computer Crime and Identity Theft/Fraud
   1. Traditional Computer Crime; Contemporary Computer Crime
   2. Identity Theft and Identity Fraud; Identifying Digital Evidence; Preparing for a search; Securing a computer crime scene;
   3. Seizing Digital Evidence at the scene; Storing Digital Evidence; Obtaining a Digital Hash; Reviewing a Case
4. Digital Forensic Process, Analysis and Validation
   1. Phases of Digital Forensic Process
   2. Digital Forensic Process Models
   3. Digital Forensics Analysis and Validation
5. Disk Structures (File Systems) and Data-hiding techniques
   1. Learn about different Disk Structures (File Systems); RAID Data Acquisitions, acquiring data from different media/tools
   2. Learn data-hiding techniques, Hiding Partitions; Steganography; Encrypted Files; Recovering Passwords
   3. Learn the different types of graphics files; Locate and recover graphics files
6. Network and Cloud Forensics; Mobile Device and Security
   1. Network Forensics, Cloud Forensics and Virtual Machine Forensics
   2. Honeypots; Security in Mobile Systems and Cloud
   3. Mobile Device Forensics: Inside Mobile Devices; SIM Card File Structure
   4. Investigating Network Traffic; Investigating Web Attacks and Wireless Attacks
7. Digital Forensic Tools and Labs
   1. Digital Forensics Hardware and Software Tools
   2. Evaluating Digital Forensics Tools Needs ;Understand Tasks done by Digital Forensics Tools and Labs;
   3. Understanding Forensics Lab Accreditation Requirements
   4. Determining the Physical Requirements for a Digital Forensics Lab
8. Organizations and Cyber Crime, Criminology and Organized Crime
   1. Organizations and Cyber Crime
   2. Criminology and Theories
   3. Organized Crime and Technology
9. Investigating Internet Crime and E-Mail Crime
   1. Introduction to Investigating Internet Crime; Conducting an Investigation and Completing the case
   2. Processing Crime and Incident Scenes, Steps for Investigating Internet Crime
   3. Examining E-mail Headers, Tracking E-Mails
   4. Investigating E-Mail Crime and Violations
   5. Remediation Case Study
10. Cyberspace Infrastructure and Enterprise Security
    1. Computer Communication Networks; Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks
    2. Enterprise Security Attacks and Challenges
    3. Information Security Protocols and Best Practices
11. Incident Detection and Characterization
    1. Pre-Incident Preparation
    2. Getting the Investigation Started
    3. Initial Development of Leads
    4. Discovering the Scope of the Incident
12. Incident Response and software Tools
    1. Incident Response process and handling an Incident
    2. Investigating Applications
    3. Incident Capture Tools; Analysis Tools; Response Tools
    4. Remediation Introduction and Case Study
13. Incident Report Writing
    1. Processing of Evidence and Report Preparation
    2. Reporting Standards and Guidelines for Writing Reports
    3. Report Writing for High-Tech Investigations
    4. Generating Report Findings with Forensics Software Tools
14. Emerging Cybercrime Trends, Recommendations and Practical Issues
    1. Cybercrime Challenges, Issues, Recommendation and Suggestion in Indian context
    2. Traditional Problems and Recommendations
    3. Additional Approaches to Internet Crime
    4. Future Trends and Emerging Concerns
15. Miscellaneous Topics
    1. Data Protection Law In The Age Of Big Data And AI
    2. Malicious Cyber Activity Distribution, Attribution and Jurisdiction
    3. Information Privacy, Law Enforcement and Privacy Law Fundamentals
    4. Models of Internet Governance

**Module Summary**

|  |  |
| --- | --- |
| **No.** | **Title of the Module** |
| M1 | Introduction to Cyber Crime, Digital Forensics and Incident Handling |
| M2 | Foundation for Forensics |
| M3 | Computer Crime and Identity Theft/Fraud |
| M4 | Digital Forensic Process, Analysis and Validation |
| M5 | Disk Structures (File Systems) and Data-hiding techniques |
| M6 | Network and Cloud Forensics; Mobile Device and Security |
| M7 | Digital Forensic Tools and Labs |
| M8 | Organizations and Cyber Crime, Criminology and Organized Crime |
| M9 | Investigating Internet Crime and E-Mail Crime |
| M10 | Cyberspace Infrastructure and Enterprise Security |
| M11 | Incident Detection and Characterization |
| M12 | Incident Response and software Tools |
| M13 | Incident Report Writing |
| M14 | Emerging Cybercrime Trends, Recommendations and Practical Issues |
| M15 | Miscellaneous Topics |

**Modular Content Structure**

**Contact Session Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Session** | **Title** | **Topics** | **Reference** |
| 1 | Introduction to Cyber Crime , Forensics and Incident Handling | Information On Cyber Crime | T1, R3 |
| Types Of Cyber Hackers |
| Cyberspace and Criminal Behavior |
| Traditional Problems Associated with Computer Crime |
| The Changing Landscape of Cybercrime |
| Preamble and Scheme Of Information Technology Act |
| Overview of Digital Forensics and Incident Handling |
| 2 | Foundation for Forensics | Networking Concepts required for Forensics | T1, T2 |
| Working with Windows and DOS Systems; Linux Boot Processes and CLI Systems |
| Introduction to Forensics Science and need for Digital Forensics; Digital Forensic Techniques |
| Understanding the Digital Forensics Profession |
| 3 | Computer Crime and Identity Theft/Fraud | Traditional Computer Crime; Contemporary Computer Crime | T1,T2, R1 |
| Identity Theft and Identity Fraud; Identifying Digital Evidence; Preparing for a search; Securing a computer crime scene; |
| Seizing Digital Evidence at the scene; Storing Digital Evidence; Obtaining a Digital Hash; Reviewing a Case |
| 4 | Digital Forensic Process, Analysis and Validation | Phases of Digital Forensic Process | T1, R1, R2 |
| Digital Forensic Process Models |
| Digital Forensics Analysis and Validation |
| 5 | Disk Structures (File Systems) and Data-hiding techniques | Learn about different Disk Structures (File Systems); RAID Data Acquisitions, acquiring data from different media/tools | T2, R1 |
| Learn data-hiding techniques, Hiding Partitions; Steganography; Encrypted Files; Recovering Passwords |
| Learn the different types of graphics files; Locate and recover graphics files |
| 6 | Network and Cloud Forensics; Mobile Device and Security | Network Forensics, Cloud Forensics and Virtual Machine Forensics | T1, R1, R3, R4 |
| Honeypots; Security in Mobile Systems and Cloud |
| 7 | Network and Cloud Forensics; Mobile Device and Security | Mobile Device Forensics: Inside Mobile Devices; SIM Card File Structure | T2, R4 |
| Investigating Network Traffic; Investigating Web Attacks and Wireless Attacks |
| 8 | Digital Forensic Tools and Labs | Digital Forensics Hardware and Software Tools | T1, R1, R2 |
| Evaluating Digital Forensics Tools Needs ;Understand Tasks done by Digital Forensics Tools and Labs; |
| Understanding Forensics Lab Accreditation Requirements |
| Determining the Physical Requirements for a Digital Forensics Lab |
| 9 | Organizations and Cyber Crime, Criminology and Organized Crime | Organizations and Cyber Crime | T1, R1 |
| Criminology and Theories |
| Organized Crime and Technology |
| 10 | Investigating Internet Crime and E-Mail Crime | Introduction to Investigating Internet Crime; Conducting an Investigation and Completing the case | T2, R1,R4 |
| Processing Crime and Incident Scenes, Steps for Investigating Internet Crime |
| Examining E-mail Headers, Tracking E-Mails |
| Investigating E-Mail Crime and Violations |
| 11 | Cyberspace Infrastructure and Enterprise Security | Computer Communication Networks; Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks | T3, R3 |
| Enterprise Security Attacks and Challenges |
| Information Security Protocols and Best Practices |
| 12 | Incident Detection and Characterization | Pre-Incident Preparation | T3 |
| Getting the Investigation Started |
| Initial Development of Leads |
| Discovering the Scope of the Incident |
| 13 | Incident Response and software Tools | Incident Response process and handling an Incident | T3, R1 |
| Investigating Applications |
| Incident Capture Tools; Analysis Tools; Response Tools |
| Remediation Introduction and Case Study |
| 14 | Incident Report Writing | Processing of Evidence and Report Preparation | T1, T3, R1 |
| Reporting Standards and Guidelines for Writing Reports |
| Report Writing for High-Tech Investigations |
| Generating Report Findings with Forensics Software Tools |
| 15 | Emerging Cybercrime Trends, Recommendations and Practical Issues | Cybercrime Challenges, Issues, Recommendation and Suggestion in Indian context | T1, R2 |
| Traditional Problems and Recommendations |
| Additional Approaches to Internet Crime |
| Future Trends and Emerging Concerns |
| 16 | Miscellaneous Topics | Data Protection Law In The Age Of Big Data And AI | <https://papers.ssrn.com/>  <https://www.ardcindia.org/ccpwc/>  <https://www.eccouncil.org/what-is-digital-forensics/> |
| Malicious Cyber Activity Distribution, Attribution and Jurisdiction |
| Information Privacy, Law Enforcement and Privacy Law Fundamentals |
| Models of Internet Governance |

**Evaluation Scheme**:

Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Name | Type | Duration | Weight | Day, Date, Session, Time |
| EC-1 | Assignment-I | Online | - | 10% | February 14-24, 2022 |
| EC-1 | Assignment-II | Online | - | 10% | March 14-24, 2022 |
| EC-2 | Mid-Semester Test | Open Book | 2 hours | 30% | Sunday, 13/03/2022 (FN)  10 AM - 12 Noon |
| EC-3 | Comprehensive Exam | Open Book | 2 hours | 50% | Sunday, 22/05/2022 (FN)  10 AM - 12 Noon |

**Note: Assignment can be replaced by QUIZ also.**

Syllabus for Mid-Semester Test (Open Book): Topics in Session Nos. 1 to 8

Syllabus for Comprehensive Exam (Open Book): All topics (Session Nos. 1 to 16)

**Important links and information:**

Elearn portal: https://elearn.bits-pilani.ac.in

Students are expected to visit the Elearn portal on a regular basis and stay up to date with the latest announcements and deadlines.

Contact sessions: Students should attend the online lectures as per the schedule provided on the Elearn portal.

Evaluation Guidelines:

1. EC1 consists of two assignments. Announcements will be made on the portal, in a timely manner.
2. For Closed Book tests: No books or reference material of any kind will be permitted.
3. For Open Book exams: Use of books and any printed / written reference material (filed or bound) is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
4. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam which will be made available on the Elearn portal. The Make-Up Test/Exam will be conducted only at selected exam centres on the dates to be announced later.

It shall be the responsibility of the individual student to be regular in maintaining the self study schedule as given in the course handout, attend the online lectures, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout.