**Subject Code:** 01CY0301

**Subject Name: Cyber Forensics and Incident Response**

**MTech. Year – 2 (Semester – 3)**

**Objective:**

|  |
| --- |
| To recreate the crime scene and investigate the same according to the forensics steps. Presentation and Reporting the crime scene in front of court or jurisdiction playing important role to prove. |

**Credits Earned:** 4 Credits

**Course Outcomes:** After completion of this course, student will be able to

* Describe Cyber Forensics and Investigation
* Digital Evidence
* Incident Response
* Forensics Investigator and their duties.

**Pre-requisite of course:** Basics knowledge of the crime scene.

**Teaching and Examination Scheme**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Teaching Scheme (Hours) | | | Credits | Theory Marks | | | Tutorial/ Practical Marks | | Total Marks |
| Theory | Tutorial | Practical | ESE (E) | Mid Sem (M) | Internal (I) | Viva (V) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents:**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | **Introduction to Cyber Forensics**   |  |  | | --- | --- | | |  | | --- | | Historical background of cyber forensics, Digital Forensics Science, The need for computer forensics, Cyber forensics and digital evidence, The rules of evidence, Study of unauthorized activities. | | | 6 |
| 2 | **Forensics Investigation Process**  Preservation, Acquisition, Analysis, Discovery, Documentation, Presentation of evidence, Litigation. | 7 |
| 3 | **Incident Response**  What is Incident Response? Types of Incidents, Criminal Investigation, Corporate Investigation, Private / Civil Investigation, Chain of Custody Concept, Typical Elements Addressed in a Forensics, Investigation Engagement Contract, Precaution to be taken when collecting electronic evidence, Digital Forensics Life Cycle. | 8 |
| 4 | |  | | --- | | **Role of Investigators**  Investigator Impartiality, Skills Set and Training, Evidence control and documentation, Investigation and Analysis, Reporting and Testifying, Understanding the requirements, Binary code analysis, Computer Hardware and Software system analysis practice. | | 10 |
| 5 | |  | | --- | | **Network Forensics**  Intrusion Detection System, Attack trace back, Packet sniffing and inspection, Log Analysis, Recovering Graphics files, Email Investigations, Phone call investigations and tracing, Anti forensics techniques. | | 9 |
|  | **Total Hours** | **40** |

**References:**

|  |  |
| --- | --- |
| 1. Computer Forensics -- [Robert C. Newman](http://www.amazon.com/s/ref=rdr_ext_aut?_encoding=UTF8&index=books&field-author=Robert%20C.%20Newman) [Auerbach Publications] 2. Incident Response and Computer Forensics -- Chris Prosise and Kevin Mandia [McGraw-Hill]. 3. Cyber Security, Willey, Nina Godbole  |  | | --- | |  | |

**Suggested Theory distribution:**

The suggested theory distribution as per Bloom’s taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Distribution of Theory for course delivery and evaluation | | | |  |
| Remember | Understand | Apply | Analyze | Evaluate | Create |
| 5% | 10% | 15% | 30% | 20% | 30% |

**Suggested List of Experiments:**

1. Practical on Surface Analysis. Calculating Hashes, Parsing Headers, Examining Imported Modules and APIs.
2. Practical on Dynamic Analysis. Capturing Registry file, Network I/O activities, Identifying C2 servers, Acquiring malware’s characteristics
3. Practical on unpacking malware and tracing process hollowing.
4. Practical on Finding String Decode Routines and Obtaining Decoded Strings.
5. Practical on Finding Dispatch Routines.
6. Practical on Finding out Evidence for Attack Tools' Execution, Passphrases for Encrypted Archives Such As RAR and 7zip.

**Instructional Method:**

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory