

**(Established under the Presidency University Act, 2013 of the Karnataka Act 41 of 2013)**

**[2023-24 ODD/ FALL SEMESTER]**

**COURSE PLAN**

**SCHOOL:** SOCSE&IS **DEPT:** CSE-CS **DATE OF ISSUE:** 28.08.2023

**NAME OF THE PROGRAM : B. Tech in Computer Science & Engineering (CS)**

**P.R.C. APPROVAL REF.** **: PU/AC-21.X/SOCSE 02/CCS//2023**

**SEMESTER/YEAR : V/III**

**COURSE TITLE & CODE : Cyber Forensics & CSE2037**

**COURSE CREDIT STRUCTURE : 2-2-3**

**CONTACT HOURS : 4 Hrs Per Week**

**COURSE IC : Mr. J. John Bennet**

**COURSE INSTRUCTOR(S) : Mr. J. John Bennet**

**COURSE URL : https://www.camu.in/index**

**PROGRAM OUTCOMES:**

Graduates of the B. Tech. Program in Computer Science and Engineering will be able to:

PO1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems

PO2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences

PO3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations

PO6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8. Ethics: Apply ethical principles and commit to professional ethics, responsibilities and norms of the engineering practice.

PO9. Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11.Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

**PROGRAM SPECIFIC OUTCOMES:**

**PSO1. Problem Analysis**: Identify, formulate, research literature, and analyze complex engineering problems related to AI & ML principles and practices, Programming and Computing technologies reaching substantiated conclusions using first principles of mathematics, natural sciences and engineering sciences

**PSO2. Design/development of Solutions**: Design solutions for complex engineering problems related to AI & ML principles and practices, Programming and Computing technologies and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, cultural, societal and environmental considerations.

**PSO3. Modern Tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities related to AI & ML principles and practices, Programming AI & ML Computing & analytics with an understanding of the limitations.

**COURSE PREREQUISITES:** CSE3078 - Cryptography and Network Security

**COURSE DESCRIPTION:**

The purpose of this course is to introduce to the students Cyber Forensic concepts. The course is both conceptual and analytical and is understood with various open-source software’s. The course develops critical thinking like correctly collect and analyze computer forensic evidence, analyze and validate Forensics Data, study the tools and tactics associated with Cyber Forensics. The course involves quizzes, assignments with various open-source software.

**COURSE OBJECTIVES:** The objective of the course is to familiarize the learners with the concepts of Cyber Forensics Learning and attain **SKILL DEVELOPMENT** through **Experiential Learning** techniques.

**COURSE OUTCOMES:**

**On successful completion of the course the students shall be able to:**

|  |  |  |
| --- | --- | --- |
| **TABLE 1: COURSE OUTCOMES** | | |
| **CO Number** | **CO** | **Expected BLOOMS LEVEL** |
| CO1 | Define various digital investigation terminologies and methods | Remember |
| CO2 | Recognize various file formats | Remember |
| CO3 | Classify the importance of digital forensic duplication and various tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications | Understand |
| CO4 | Apply various techniques for forensic investigation | Apply |

**MAPPING OF C.O. WITH P.O [H- HIGH, M- MODERATE, L-LOW]**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE 2a: CO PO Mapping ARTICULATION MATRIX** | | | | | | | | | | | | |
| **CO.**  **No** | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO 10 | PO 11 | PO 12 |
| **CO1** | H | - | - | - | L | - | - | - | - | - | - | - |
| **CO2** | H | L | - | **-** | - | - | - | - | L | - | - | - |
| **CO3** | - | M | - | **-** | M | - | - | - | - | - | - | - |
| **CO4** | - | M | M | **-** | M | **-** | - | L | M | - | - | - |

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLE 2b: CO PSO Mapping ARTICULATION MATRIX** | | | |
| **CO. No** | PSO1 | PSO2 | PSO3 |
| **CO1** | - | - | - |
| **CO2** | **H** | **L** | **L** |
| **CO3** | **L** | **H** | - |
| **CO4** | **H** | **H** | **M** |

**COURSE CONTENT (SYLLABUS):**

Module 1: Digital Investigation [L-9 P-6 Total: 15 Hrs] [Remember]

Digital Evidence and Computer Crime - History and Terminology of Computer Crime Investigation- Technology and Law - The Investigative Process -Investigative Reconstruction - Modus Operandi, Motive and Technology -Digital Evidence in the Courtroom.

# Module 2: Understanding Information [L-9 P-6 Total: 15 Hrs] [Remember]

Methods of storing data: number systems, character codes, record structures, file formats and file signatures - Word processing and graphic file formats - Structure and Analysis of Optical Media Disk Formats - Recognition of file formats and internal buffers - Extraction of forensic artifacts– understanding the dimensions of other latest storage devices – SSD Devices.

# Module 3: Computer Basics For Digital Investigators [L-9 P-6 Total: 15 Hrs] [Understand]

Computer Forensic Fundamentals - Applying Forensic Science to computers - Computer Forensic Services - Benefits of Professional Forensic Methodology -Steps taken by computer forensic specialists. Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components – Contemporary Computer Crime-Identity Theft and Identity Fraud – Organized Crime &Terrorism. Computer forensic cases: Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence –Processing Evidence and Report Preparation – Future Issues.

Module 4: Computer Forensic Evidence And Data Recovery [L-9 P-6 Total: 15 Hrs] [Apply]

Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution, Hiding and Recovering Hidden Data.

Data Collection and Data seizure: 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. Reconstructing the Attack.

**SKILL SETS TO BE DEVELOPED:**

Graduate of the B.Tech. Program in Computer Science and Engineering shall be able to;

1. **An attitude of enquiry.**
2. **Confidence and ability to tackle new problems.**
3. **Ability to interpret events and results.**
4. Ability to work as a leader and as a member of a team.
5. **Assess errors in systems/processes/programs/computations and eliminate them.**
6. Observe and measure physical phenomena.
7. **Write reports**.
8. **Select suitable equipment, instrument, materials & software**
9. **Locate faults in system/Processes/software.**
10. Manipulative skills for setting and handling systems/Process/ Issues
11. The ability to follow standard /Legal procedures.
12. An awareness of the Professional Ethics.
13. Need to observe safety/General precautions.
14. **To judge magnitudes/Results/issues without actual measurement/actual contacts**

**DELIVERY PROCEDURE (PEDAGOGY):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 3: SPECIAL DELIVERY METHOD/ PEDAGOGY PLANNED WITH TOPICS** | | | | |
| **S. No** | **Lecture Number** | **Subtopic as per lesson Plan** | **Pedagogy title/ short explanation of adopted pedagogy** | **\*\* At end of semester please update whether activity was done** |
| **1** | **P6** | Implement MC method with custom environment for Blackjack game | **Flipped Class pedagogy** |  |
| **2** | **32** | **Applications of RL with custom environments** | **Activity Based Learning – DEMO OF CODE** |  |

**REFERENCE MATERIALS:**

**Text book:**

**T1:** Eoghan Casey, “Digital Evidence and Computer Crime”, Elsevier Publication, 3rd Edition.

**T2:** John R. Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Cengage Learning, 2nd Edition, 2019

**T3**: Marjie T. Britz, “Computer Forensics and Cyber Crime”, Pearson Publication, 2nd Edition.

**Reference Book(s):**

**R1.** Ravi Kumar & B Jain, “Cyber Forensics - Concepts and Approaches”, icfai university press, 2006

**R2.** ChristofPaar, Jan Pelzl,”Understanding Cryptography: A Textbook for Students and Practitioners”, Springer’s, Second Edition, 2010.

**R3.** Ali Jahangiri,” Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts”, First edition, 2009.

**R4.** Computer Forensics: Investigating Network Intrusions and Cyber Crime”, Ec-Council Press, 2010.

**R5.** C. Altheide& H. Carvey,” Digital Forensics with OpenSource Tools, Syngress”, 2011, ISBN: 781597495868., https://esu.desire2learn.com

**Web Based Resources and E-books:**

**W1.** **NPTEL**: <https://onlinecourses.swayam2.ac.in/cec21_ge10/preview>

**W2. Udemy**: <https://www.udemy.com/topic/digital-forensics/>

**E1.**http://182.72.188.195/cgi-bin/koha/opac-detail.pl?biblionumber=14073&query\_desc=ti%2Cwrdl%3A%20CYBER%20FORENSIC

**Tool/IDLE: Autopsy, FTK Imager, and Volatility, Wire shark, NMap, SANS Investigative Forensics Toolkit**

**SPECIFIC GUIDELINES TO STUDENTS:**

1. Follow the instructions of course instructor in both class and lab.
2. Avoid being absent in labs as it will affect the understanding of the experiments.

**COURSE SCHEDULE:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 4: COURSE BROAD SCHEDULE** | | | | |
| **Sl.**  **No.** | **Activity** | **Starting Date** | **ConcludingDate** | **Total Number**  **of Periods** |
| **01** | **Over View of the course** | 28th Aug | 28th Aug | 1 |
| **02** | **Module: 01** | 28th Aug | 15th Sep | 7 |
| **03** | **Module: 02** | 18th Sep | 13th Oct | 8 |
| **04** | **Midterm** | 16th Oct | 20th Oct |  |
| **05** | **Module:03** | 23rd Oct | 24th Nov | 8 |
| **06** | **Module:04** | 27th Nov | 19th Dec | 10 |
| **08** | **Course Integration** | 20th Dec | 20th Dec | 1 |
| **09** | **Program Integration** | 21st Dec | 21st Dec | 1 |
| **10** | **Revision and Conclusion of the Course** | 22nd Dec | 22nd Dec | 1 |

**DETAILED SCHEDULE OF INSTRUCTION:**

**Main pedagogy: PPT + Chalk Board and Lecture**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE 5: DETAILED COURSE SCHEDULE/ LESSON PLAN** | | | | | | | | | | | | | | | | |
| **Session no.** | **Topic** | | | **Sub Topic** | | | **LOL**  **(Lower Ordering Learning)** | | | **HOL**  **(Higher Ordering Learning)** | | | **Course Outcome Number** | | | **Reference** |
| 1 | **Module 1:** Digital Investigation | | | Over View of the course. Digital Evidence and Computer Crime  LO1: **Name** some common examples of digital evidence that can be collected in computer crime investigations  LO2: **Recognize** the tools and techniques are commonly used by digital forensics experts to recover, analyse, and preserve digital evidence. | | | L1  L3 | | |  | | | CO1 | | | T1  Ch:3  Pg. No: 49-81 |
| 2 | Digital Investigation | | | History and Terminology of Computer Crime Investigation  LO1: **Describe** the process of "data carving" in digital forensics and its importance in recovering deleted or hidden information  LO2: **Discuss** the tension between law enforcement's need for digital evidence and individuals' right to privacy | | | L1  L3 | | |  | | | CO1 | | | T1  Ch:1  Pg. No: 10-14 |
| 3 | Digital Investigation | | | Technology and Law  LO1: **Outline** the use of advanced technology impact the collection, preservation, and admissibility of digital evidence in court  LO2: **Describe** the concept of "going dark" and how it relates to challenges faced by law enforcement in accessing encrypted information | | | L1  L3 | | |  | | | CO1 | | | T1  Ch 4  Pg. No: 85-182 |
| 4 | Digital Investigation | | | The Investigative Process  LO1: **List** the crucial steps that investigators take during the initial phase of a digital investigation.  LO2: **Define** how investigators collect and acquire digital evidence from various sources, such as computers, mobile devices, and cloud services. | | | L1  L3 | | |  | | | CO1 | | | T1  Ch 8  Pg No: 255 -282 |
| 5 | Digital Investigation | | | Investigative Reconstruction  LO1: **Describe**, how to ensure the accuracy and completeness of the timeline during the reconstruction process?  LO2: **Determine** the techniques used to link digital artifacts that are relevant to the investigation. | | | L2  L3 | | |  | | | CO1 | | | T1  Ch 8  Pg No: 255 -282 |
| 6 | Digital Investigation | | | Modus Operandi  LO1: **Describe** how do patterns contribute to understanding the tactics and techniques employed by the perpetrator  LO2: **Explain** methods were used to transfer sensitive information out of the victim's environment | | | L1  L2 | | |  | | | CO1 | | | T1  Ch 9  Pg.No: 287-296 |
| 7 | Digital Investigation | | | Motive and Technology  LO1:**Outline** the potential motives behind the digital crime or incident being investigated  LO2: **Demonstrate** the perpetrator's affiliations and beliefs contribute to understanding their motives? | | | L1  L3 | | |  | | | CO1 | | | T1  Ch 9  Pg.No: 297-303 |
| 8 | Digital Investigation | | | Digital Evidence in the Courtroom  LO1: **Predict** legal criteria were met to ensure that the digital evidence is admissible in court  LO2: **Determine** how to use demonstrative exhibits (diagrams, charts, screenshots) to present the digital evidence? | | | L1  L3 | | |  | | | CO1 | | | T1  Ch 2  Pg.No: 49-81 |
| 9 |  |  | | | Revision and Course Integration | | | | | | | | | | | |
| 10 | **Module 2:** Understanding Information | | | Methods of storing data: number systems, character codes  LO1: **How** will I back up my data to ensure data security and prevent data loss?  LO2: **Discuss** about the importance of data access speed? Do I need the faster performance of an SSD, or is an HDD sufficient? | | | L1  L2 | |  | | | CO2 | | T1  Ch No: 16  Pg. No:466 - 467 | | |
| 11 | Understanding Information | | | Record structures, file formats and file signatures  LO1: **What** is a record structure, and why is it important in data management?  LO2: **List** and discuss about the measures can be taken to detect and handle corrupted or malicious files based on their signatures? | | | L1  L2 | |  | | | CO2 | | T1  Ch No: 16  Pg. No: 514-516 | | |
| 12 | Understanding Information | | | Word processing  LO1: **Define** word processing, and why is it an essential tool for many individuals and organizations?  LO2: **How** can I customize the layout and formatting of my document, including setting page size, margins, and line spacing? | | | L1  L3 | |  | | | CO2 | | T1  Ch No: 16  Pg. No: 517-519 | | |
| 13 | Understanding Information | | | Graphic file formats  LO1: **What** is a graphic file format, and why are there so many different formats available?  LO2: **Discuss** about the key differences between raster (bitmap) and vector graphic file formats, and when should I use each type? | | | L1  L3 | |  | | | CO2 | | T1  Ch No: 16  Pg. No:520- 523 | | |
| 14 | Understanding Information | | | Structure and Analysis of Optical Media Disk Formats  LO1: **Determine** the different types of optical disc formats, such as CD-ROM, DVD-RW, and BD-RE, and what are their specific use cases?  LO2: **How** are data organized on optical discs, and what is the role of sectors, tracks, and sessions in this organization? | | | L1  L2 | |  | | | CO2 | | T1  Ch No: 16  Pg. No:524-526 | | |
| 15 | Understanding Information | | | Recognition of file formats and internal buffers  LO1: **Why** is it essential in data processing and software applications?  LO2: **Paraphrase** the challenges and considerations when working with proprietary or custom file formats that may lack standard signatures? | | | L1  L2 | |  | | | CO2 | | T1  Ch No: 16  Pg. No: | | |
| 16 | Understanding Information | | | Extraction of forensic artifacts  LO1: **How** do you define forensic artifacts, and what distinguishes it from regular data?  LO2: **Discuss** the legal and ethical considerations should be observed when extracting and handling forensic artifacts, especially in criminal investigations? | | | L1  L2 | |  | | | CO2 | | T2  Ch No: 6  Pg. No:226 | | |
| 17 | Understanding Information | | | Understanding the dimensions of other latest storage devices  LO1: **What** are the latest trends in Network-Attached Storage (NAS) devices, and how are they enhancing data sharing and remote access?  LO2:  **Are** there any ground-breaking storage technologies on the horizon, such as DNA storage, quantum storage, or other experimental concepts? Justify. | | | L1  L2 | |  | | | CO2 | | T2  Ch No: 5  Pg. No: 191 | | |
| 18 | Understanding Information | | | SSD Devices  LO1: **What** is a Solid-State Drive (SSD), and how does it differ from traditional Hard Disk Drives (HDDs) in terms of operation and technology?  LO2: **Discuss** write endurance in SSDs, and how is it measured? How do different types of NAND flash memory affect endurance? | | | L1  L2 | |  | | | CO2 | | T2  Ch No: 5  Pg. No:203 | | |
| 19 |  |  | | | Revision and Course Integration | | | | | | | | | | | |
|  |  |  | | | **Midterm** | | | | | | | | | | | |
|  |  |  | | | **Midterm** | | | | | | | | | | | |
|  |  |  | | | **Midterm** | | | | | | | | | | | |
| 20 |  |  | | | **Midterm Question paper discussion and Paper distribution** | | | | | | | | | | | |
| 21 | **Module 3:** Computer Basics for Digital Investigators | | Computer Forensic Fundamentals  - Applying Forensic Science to computers - Computer Forensic Services  LO1: **What** is the two fold process a digital investigator has to follow in surveying a crime scene?  LO2: **Discuss** the major aspect of preserving digital evidence in a way that minimizes the changes in evidence. | | | L1  L2 | |  | | | CO3 | | | | T2  Ch 1 Pg. No 10 - 33 | |
| 22 | Computer Basics for Digital Investigators | | Benefits of Professional Forensic Methodology  LO1: **Outline** the things a computer forensic professional should ensure Before handling the subjected computer system.  LO2: **Classify** The impartial computer forensics expert who helps during discovery will typically have experience on a wide range of computer hardware and software. Explain. | | | L1  L3 | |  | | | CO3 | | | | T2  Ch 1 Pg. No 17 - 18 | |
| 23 | Computer Basics for Digital Investigators | | Steps taken by computer forensic specialists  LO1: **Name** the person who is responsible for doing computer forensics.  LO2: **What** are the necessary steps a computer forensics specialist will take to identify and attempt to retrieve possible evidence that may exist on a subject computer system? Explain. | | | L1  L2 | |  | | | CO3 | | | | T2  Ch 1  Pg. No 7 | |
| 24 | Computer Basics for Digital Investigators | | Information warfare: Arsenal – Surveillance Tools – Hackers and Theft of Components  LO1: Classify the three general categories of hackers.  LO2: Define hacking and discuss in detail about the evolution, motivation and hierarchy of hacking. | | | L1  L2 | |  | | | CO3 | | | | T3  Ch No: 3  Pg No:47-71 | |
| 25 | Computer Basics for Digital Investigators | | Contemporary Computer Crime-Identity Theft and Identity Fraud  LO1: **Define** eco-terrorism.  LO2: **Discuss** in detail about the amount of money consumers are losing through online fraud. | | | L1  L2 | |  | | | CO3 | | | | T3  Ch No: 4  Pg No: 74-144 | |
| 26 | Computer Basics for Digital Investigators | | Organized Crime &Terrorism.  LO1: **Define** organized crime.  LO2: **Summarize** and explain the organized crime in detail. | | | L1  L2 | |  | | | CO3 | | | | T3  Ch No: 6  Pg No: 148-181 | |
| 27 | Computer Basics for Digital Investigators | | Computer forensic cases: Developing Forensic Capabilities  LO1: **What** are the rules to be followed in all investigation related with computer forensic science.  LO2: **Discuss** the various traditional problems in computer Investigation. | | | L1  L2 | |  | | | CO3 | | | | T3  Ch No: 10  Pg No:264-293 | |
| 28 | Computer Basics for Digital Investigators | | Searching and Seizing Computer Related Evidence  LO1: **What** are the options were available once the evidence is detected?  LO2: **List** the rules for collecting the electronic evidences and explain the same in detail. | | | L1  L2 | |  | | | CO3 | | | | T1  Ch 6  Pg. No 217 - 225 | |
| 29 | Computer Basics for Digital Investigators | | Processing Evidence and Report Preparation – Future Issues  LO1: **List** the reasons why the criminals are using the internet as noticed by National Institute of Justice.  LO2: **Demonstrate** the different aspects of the data analysis in processing of evidence and generating the report. | | | L1  L3 | |  | | | CO3 | | | | T3  Ch No: 12  Pg No: 325-345 | |
| 30 |  |  | | | Revision and Course Integration | | | | | | | | | | | |
| 31 | **Module 4:** Computer Forensic Evidence And Data Recovery | | Data Recovery Defined, Data Backup and Recovery  LO1: **Summarize** the obstacles rises while backing up applications.  LO2: **Discuss** briefly about he elements of a backup and recovery design and review the improvements being made with necessary diagrams. | | | L1  L3 | |  | | | CO4 | | | | T2  Ch 5  Pg. No 191 - 200 | |
| 32 | Computer Forensic Evidence And Data Recovery | | The Role of Backup in Data Recovery, The Data-Recovery Solution, Hiding and Recovering Hidden Data  LO1: **List** the factors which affects back up of data.  LO2: **Explain** the different types of data recovery solutions with suitable examples. | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 5  Pg. No 200 - 209 | |
| 33 | Computer Forensic Evidence And Data Recovery | | Data Collection and Data seizure: why collect evidence? - Collection Options, Obstacles  LO1: **Justify** why Electronic crime is difficult to investigate and prosecute.  LO2: **Explain** the context: "It is common knowledge that what is deleted from the computer can sometimes be brought back". | | | L1  L3 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 217-218 | |
| 34 | Computer Forensic Evidence And Data Recovery | | Types of Evidence, The Rules of Evidence  LO1: **Differentiate** Testimonial Evidence and Hearsay.  LO2: **Summarize** and Explain the five rules which are to be taken in account of collecting electronic evidence | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 219-223 | |
| 35 | Computer Forensic Evidence And Data Recovery | | Volatile Evidence, General Procedure  LO1: **List** the order of volatility which determines what evidence to be collected first.  LO2: When collecting and analysing evidence, there is a general four-step procedure you should follow. List and Explain. | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 223-224 | |
| 36 | Computer Forensic Evidence And Data Recovery | | Collection and Archiving, Methods of Collection  LO1: **Explain** the two methods available in collecting the evidences.  LO2: **Describe**, how collecting and archiving of the data is also important, as it can affect how the data is perceived. | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 224-226 | |
| 37 | Computer Forensic Evidence And Data Recovery | | Artifacts, Collection Steps,  LO1: **Define** Artifacts.  LO2: **Explain** in detail about the steps to be performed in collecting the evidences. | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 226-227 | |
| 38 | Computer Forensic Evidence And Data Recovery | | Controlling Contamination:  The Chain of Custody. Reconstructing the Attack.  LO1: **Which** data has to be used for forensic examination?  LO2: "Once the data has been collected, it must be protected from contamination. **List** and Explain in detail about what can be done with the original copies once they were collected." | | | L1  L2 | |  | | | CO4 | | | | T2  Ch 6  Pg. No: 228-229 | |
| 39 | Program Integration | | | | |  | |  | | | CO1,CO2,CO3,CO4 | | | |  | |
| 40 | Revision and Conclusion of the Course | | | | |  | |  | | | CO1,CO2,CO3,CO4 | | | |  | |

**COURSE CONTENT &TASK SCHEDULE FOR LABORATORY COMPONENT:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sl.No** | **Session No** | **Task** | **Sub Topic** | **LOL(Lower Order Learning)** | **HOL(Higher Order Learning)** | **Number of Lab Sessions required to complete the**  **task** | **Skills to be developed** | **Course Outcome to be developed** |
| **01** | P1 | **MODULE1:**  Disk Forensics | Identify digital evidences  & Acquire the evidence.  LO1: **Recognize** the type of crime or incident that occurred and what kind of digital evidence might be relevant. This could include cybercrimes, intellectual property theft, financial fraud, etc.  LO2: **Choose** appropriate acquisition methods: Depending on the source and type of evidence, select the appropriate methods for acquisition. This could involve forensic imaging, data extraction tools, network captures, etc | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8,SK14 | CO1 |
| **02** | P2 | Disk Forensics | Authenticate the evidence &  Preserve the evidence.  LO1: **Identify** which methods can be used in the laboratory ensure that the evidence received is the same as that collected at the crime scene?  Are there any signs of tampering, contamination, or degradation in the evidence?  LO2: **Examine** the data generated during analysis protected from unauthorized access or manipulation?Are there protocols in place to ensure data integrity? | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8,SK14 | CO1 |
| **03** | P3 | Disk Forensics | Analyse the evidence.  LO1: **Recognizing** the evidence is a crucial step in the investigative process, as it helps uncover insights and patterns that can be used to build a case or draw conclusions. What tools and software are used to examine digital evidence (forensic analysis software, data recovery tools)?  LO2: **Interpreting** the evidence is a crucial step in any investigation or scientific inquiry. Are there quality control measures in place to ensure the reliability and accuracy of the analysis | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO1 |
| **04** | P4 | Disk Forensics | Report the findings  LO1: **Identify** a disk forensics report involves documenting the findings of a digital investigation related to storage media such as hard drives, solid-state drives, or other types of disks. Determine the type of storage media was analysed (e.g., hard drive, USB drive)  LO2: **Examine** any deleted or fragmented files recovered from the storage media?  What tools or techniques were used for data recovery? | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO1 |
| **05** | P5 | **MODULE2:**Network Forensics | Intrusion detection and Logging.  LO1: **Identify** which type of IDS is in place (host-based, network-based, signature-based, and behaviour-based)?  How frequently are IDS signatures updated to detect the latest threats?  LO2: **Choose** the integrity of logs maintained to prevent tampering or unauthorized modification?  Are logs secured to prevent unauthorized access? | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO2 |
| **06** | P6 | Network Forensics | Correlating intrusion detection and logging.  LO1: **Label** how the timestamp accuracy ensured across different logs from various devices? Are time synchronization mechanisms in place to align events accurately?  LO2: **Determine** the criteria which are used to validate the accuracy of intrusion detection alerts through log data?Are there cases where an alert is confirmed or discarded based on log evidence? | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO2 |
| **07** | P7 | Network Forensics | Logging  LO1: **Relate** a logging policy that outlines what needs to be logged and for how long? How does your organization determine the scope and retention period for different types of logs?  LO2: **Examine** how to ensure the accuracy of timestamps in logs, considering different time zones and synchronization mechanisms? | LO1  LO3 |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO2 |
| **08** | P8 | **MODULE3:**Device Forensics | Mobile Phone  Digital Music | **✓** |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO3 |
| **09** | P9 | Device Forensics | Printer & scanner forensics | **✓** | Forensic analysis of a VM | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO3 |
| **10** | P10 | Device Forensics | Credit Card forensics | **✓** |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO3 |
| **11** | P11 | Device Forensics | Credit Card forensics | **✓** |  | **1** | SK1, SK2,SK3,SK5,SK8, SK14 | CO3 |

**Topics relevant to “SKILL DEVELOPMENT”:** Real time data analysis for Skill Development through Experiential Learning techniques. This is attained through the Lab Experiments as mentioned in the assessment component.

**ASSESSMENT SCHEDULE:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE 6 ASSESSMENT SCHEDULE** | | | | | | | |
| **Sl.**  **No.** | **Assessment type** | **Contents** | **Course out come Number** | **Duration (In Hours)** | **Marks** | **Weightage** | **Venue,**  **Date & Time** |
| **1** | Quiz 1 (surprise component) | Module 1 | CO1 | 20 mins | 10 | 5% | 3rd week or 4th week of Sep in the lab |
| **2** | Midterm Exam(Lab with theory) | Module-1 and 2 | CO1,CO 2 | 1  Hour 30 Mins | 60 | 30% | As per COE schedule |
| **3** | Quiz 2 | Module 3 | CO3 | 20 mins | 10 | 5% | 28th Nov |
| **4** | **CA lab - 1**  A report on a specific application of RL – group  **Review of digital / e-resources from Pres. Univ. link given in the References Section -(Mandatory to submit screenshot accessing digital resource. Otherwise it will not be evaluated**) | EXP 1-11  [**https://web.s.ebscohost.com/ehost/detail/detail?vid=9&sid=cbc51846-7bf7-482b-8aac-fbd99ab97ee4%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#**](https://web.s.ebscohost.com/ehost/detail/detail?vid=9&sid=cbc51846-7bf7-482b-8aac-fbd99ab97ee4%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d) | CO1, CO 2, CO3, CO4 | Lab hours | 10 | 5% | NA |
| **5** | **CA lab - 2** (daily completion of tasks in lab) | EXP 1-11 | CO1, CO 2, CO3, CO4 | Lab hours | 10 | 5% | Lab |
| **6** | End Term Exam (lab with theory) | Full Syllabus | CO1, CO 2, CO3, CO4 | 3 hrs | 100 | 50% | As per COE schedule between 3rd Jan 2024 – 24th Jan 2024 |

**COURSE CLEARANCE CRITERIA: “AS PER ACADEMIC REGULATIONS OF THE UNIVERSITY”**.

**MAKEUP EXAM POLICY: “AS PER ACADEMIC REGULATIONS OF THE UNIVERSITY”**.

CONTACT TIMINGS IN THE CHAMBER FOR ANY DISCUSSIONS:

As per the prior appointment from the faculty, student can meet the faculty member. Schedule of the same to be announced in the class.

**SAMPLE THOUGHT PROVOKING QUESTIONS:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABLE 7: SAMPLE THOUGHT PROVOKING QUESTIONS** | | | | |
| **Sl No.** | **Question** | **Marks** | **Course Outcome No.** | **Bloom’sLevel** |
| 1 | Recognize the importance of cyber security and what measures can be taken to prevent cyber crime | 10 Marks | CO1 | **Remember** |
| 2 | Label the forensic analysis of file system. | 10 Marks | CO2 | **Remember** |
| 3 | Suppose a person is suspected with credit card fraud using his cell phone. Discuss the Forensic steps to be followed to collect evidence. | 10 Marks | CO3 | **Understand** |
| 4 | In city railway station police arrested a suspected terrorist based on his sketch, it was found that he has Android phone. How can the legal authorities produce potential evidence from his Android phone? | 10 Marks | CO4 | **Apply** |

**TARGET SET FOR COURSE OUTCOME ATTAINMENT:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TABLE 8: TARGET SET FOR ATTAINMENT OF EACH CO and ATTAINMENT ANALYSIS AFTER RESULTS** | | | | | | |
| **Sl.no** | **C.O. No.** | **Course Outcomes** | **Threshold Set for the CO** | **Target set for attainment in percentage** | **Actual C.O. Attainment**  **In Percentage \*** | **Remarks on attainment &Measures to enhance the attainment\*** |
| 01 | CO1 | Understand various digital investigation terminologies and methods | 40 | 65% |  |  |
| 02 | CO2 | Understand various file formats | 40 | 60% |  |  |
| 03 | CO3 | Recognize the importance of digital forensic duplication and various tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications | 45 | 60% |  |  |
| 04 | CO4 | Apply techniques for forensic investigation | 45 | 60% |  |  |

**\* LAST TWO COLUMNS ARE TO BE FILLED AFTER END TERM EXAM WITH ACTUAL ATTAINMENT VALUES**

Signature of the course Instructor In-Charge (s)

APPROVAL:

This course has been duly verified Approved by the D.A.C.

Signature of the Chairperson D.A.C.

Name and signature of the Instructor In-Charge (s) AFTER completing entries in Table number 3 and 8 at end of semester:

Name and signature of the DAC Chairperson AFTER completing entries in Table number 3 and 8 at end of semester:

**BLOOM'S TAXONOMYSAMPLE VERBS**

Learning Outcomes Verbs at Each Bloom Taxonomy Level to be used for writing the course Outcomes.



