A

Course File Report

On

"CYBER FORENSICS"

Submitted by

Mr. Y.SHYAM SUNDAR

Assistant Professor

DEPARTMRENT OF COMPUTER SCIENCE AND ENGINEERING

CMR ENGINEERING COLLEGE

(Affiliated to JNTU, HYDERABAD)

Kandlakoya(v),Medchal -501 401

(2022-2023)

CONTENTS OF COURSE FILE:

1. Department vision & mission
2. List of PEOs, POs, PSOs
3. List of Cos (action verbs as per blooms)
4. Syllabus copy and suggested or reference books
5. Session plan/ lesson plan
6. Session execution log
7. Lecture notes
8. Assignment Questions (Samples Booklets)
9. Mid exam question papers (Samples Booklets)
10. Scheme of evaluation
11. Mapping of Cos with Pos and PSOs
12. Attainment of Cos, Pos and PSOs (Excel sheet)
13. University question papers or question bank.
14. Power point presentations (PPTs)
15. Websites or URLs e- Resources

Submitted By
Mr. Y.Shyam Sundar
Assistant Professor

1. Department vision & mission:

Vision

To produce globally competent and industry-ready graduates in Computer Science & Engineering by
imparting quality education with the know-how of cutting-edge technology and holistic personality.

Mission

1. To offer high-quality education in Computer Science & Engineering in order to build core competence for the graduates by laying a solid foundation in Applied Mathematics and program framework with a focus on concept building.

2. The department promotes excellence in teaching, research, and collaborative activities to prepare graduates for a professional career or higher studies.

3. Creating an intellectual environment for developing logical skills and problem-solving strategies, thus developing, an able and proficient computer engineer to compete in the current global scenario.

2. Program Educational outcome (PEO):

PEO 1: Excel in professional career and higher education by acquiring knowledge of mathematical computing and engineering principles.
PEO 2: To provide an intellectual environment for analyzing and designing computing systems for technical needs.
PEO 3: Exhibit professionalism to adapt current trends using lifelong learning with legal and ethical responsibilities.
PEO 4: To produce responsible graduates with effective communication skills and multidisciplinary practices to serve society and preserve the environment.

2.1 Program Outcome (PO):

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

2. **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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **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.

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

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

10. **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.

11. **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.

12. 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.

2.3 Program Specific Outcomes (PSOs):

PSO1: Professional Skills and Foundations of Software development: Ability to analyze, design and develop applications by adopting the dynamic nature of Software developments.

PSO2: **Applications of Computing and Research Ability:** Ability to use knowledge in cutting edge technologies in identifying research gaps and to render solutions with innovative ideas.

NBA Graduate Attributes

PO1 Engineering knowledge

PO2 Problem analysis

PO3 Design/development of solutions

PO4 Conduct investigations of complex problems

PO5 Modern tool usage

PO6 The engineer and society

PO7 Environment and sustainability

PO8 Ethics

PO9 Individual and team work

PO10 Communication

PO11 Project management and finance

PO12 Life-long learning

3. Course Outcomes

S. No	Course OutCome
CO1	Students will be able to understand the digital investigations and investigative process: identification, preservation, and analysis.**[Understanding]**
CO2	Students will be able to understand the collection and search of specific data that will serve as acceptable evidence in a court of law.**[Remembering]**
CO3	Will be able to identify and document potential security breaches of computer data that suggest violations of legal, ethical, moral, policy, and/or societal standards.**[Applying]**
CO4	Students will be to apply a solid foundational grounding in computer networks, and mobile devices to digital investigations and to the protection of computer network resources from unauthorized activity.**[Analyzing]**
CO5	Will be able to apply and work on operating systems, file systems, hardware, and law enforcement to advance digital investigations or protect the security of digital resources.**[Creating]**

4. Syllabus Copy

UNIT – I

Introduction of cybercrime: Types, The Internet spawns crime, Worms versus viruses, Computers' roles in crimes, Introduction to digital forensics, Introduction to Incident – Incident Response Methodology – Steps- Activities in Initial Response, Phase after detection of an incident

UNIT – II

Initial Response and forensic duplication, Initial Response & Volatile Data Collection from Windows system – Initial Response & Volatile Data Collection from Unix system – Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic. Duplicate/Qualified Forensic Duplicate of a Hard Drive

UNIT – III

Forensics analysis and validation: Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions.

Network Forensics: Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project.

UNIT – IV

Current Forensic tools: 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.

Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices.

UNIT – V

Working with Windows and DOS Systems: understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines

TEXT BOOKS:

- Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGraw Hill, 2006
- Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi.
- Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning

REFERENCES:

- R1: Real Digital Forensics by Keith J. Jones, Richard Bejtiich, Curtis W. Rose, Addison-Wesley Pearson Education
- R2: Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brian Jenkinson, Springer International edition.
- R3: Computer Evidence Collection & Presentation by Christopher L.T. Brown, Firewal Media.
- R4: Homeland Security, Techniques & Technologies by Jesus Mena, Firewall Media.
- R5: Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M.Slade, TMH 2005
- R6: Windows Forensics by Chad Steel, Wiley India Edition.

5.SESSION LOG LEESON PLAN

S.NO	Topic (JNTU syllabus)	Sub-Topic	NO. OF LECTURES REQUIRED	Suggested Books	Remarks
UNIT - I					
1	**Cybercrime (Unit-1)**	Introduction to Cybercrime, Types	L1	Computer Forensics, Computer Crime Investigation	**M1,M4**
2		Worms versus viruses, Internet spawns crime	L2	Computer Forensics, Computer Crime Investigation	**M1,M4**
3		Digital Forensics, Introduction to Incident	L3,L4	Computer Forensics, Computer Crime Investigation	**M1,M4**
4		Incident Response Methodology	L5	Computer Forensics, Computer Crime Investigation	**M1,M4**
5		Phase after detection of an	L6,L7	Computer Forensics,	**M1,M4**

		incident		Computer Crime Investigation	
6	**Initial Response and forensic duplication (Unit-2)**	Initial Response and forensic duplication	L8	Computer Forensics, Computer Crime Investigation	**M1,M4**
7		Initial Response & volatile Data Collection from Windows system	L9	Computer Forensics, Computer Crime Investigation	**M1,M4**
8		Initial Response & volatile Data Collection from Unix system	L10	Computer Forensics, Computer Crime Investigation	**M1,M4**
9		Forensic Duplication	L11	Computer Forensics, Computer Crime Investigation	**M1,M4**
10		Forensic Duplication Tool Requirements	L12, L13	Computer Forensics, Computer Crime Investigation	**M1,M4**
11		Creating Forensic	L14	Computer Forensics, Computer Crime Investigation	**M1,M4**
12		Duplicate of Hard Drive	L15	Computer Forensics, Computer Crime Investigation	**M1,M4**
13	**Computer Forensics analysis and validation (Unit-3)**	Computer Forensics analysis and validation: Determining what data to collect and analyze	L16	Computer Forensics and Investigations	**M1,M4**
14		validating forensic data	L17	Computer Forensics and Investigations	**M1,M4**

15		addressing data-hiding techniques	L18, L19	Computer Forensics and Investigations	**M1,M4**
16		performing remote acquisitions	L20	Computer Forensics and Investigations	**M1,M4**
17	**Network Forensics (Unit-3)**	Network Forensics overview	L21	Computer Forensics and Investigations	**M1,M4**
18		performing live acquisitions	L22	Computer Forensics and Investigations	**M1,M4**
19		developing standard procedures for network forensics	L23	Computer Forensics and Investigations	**M1,M4**
20		network tools	L24	Computer Forensics and Investigations	**M1,M4**
21		Examining the honey net project.	L25	Computer Forensics and Investigations	**M1,M4**
22	**Current Computer Forensic tools (Unit-4)**	Current Computer Forensic Tools: evaluating computer forensic tool needs	L26,L27	Computer Forensics and Investigations	**M1,M4**
23		computer forensics software tools	L28	Computer Forensics and Investigations	**M1,M4**
24		computer forensics hardware tools	L29	Computer Forensics and Investigations	**M1,M4**
25		validating and testing forensics software	L30,L31	Computer Forensics and Investigations	**M1,M4**
26		E-mail Investigations: Exploring the role of e-mail	L32	Computer Forensics and	**M1,M4**

		in investigation		Investigations	
27		exploring the roles of the client and server in e-mail	L33	Computer Forensics and Investigations	**M1,M4**
28		investigating e-mail crimes and violations	L34	Computer Forensics and Investigations	**M1,M4**
29	**Cell phone and mobile device forensics (Unit-4)**	understanding e-mail servers, using specialized e-mail forensic tools	L35	Computer Forensics and Investigations	**M1,M4**
30		Cell phone and mobile device forensics: Understanding mobile device forensics	L36,L37	Computer Forensics and Investigations	**M1,M4**
31		understanding acquisition procedures for cell phones and mobile devices	L38,L39	Computer Forensics and Investigations	**M1,M4**
32	**Working with Windows and DOS Systems (Unit-5)**	Working with Windows and Dos System: understanding file systems , ,.	L40,L41	Computer Forensics and Investigations	**M1,M4**
33		exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption	L42,L43	Computer Forensics and Investigations	**M1,M4**
34		windows registry, Microsoft startup tasks	L44,L45	Computer Forensics and Investigations	**M1,M4**
35		MS-DOS startup tasks, virtual machines	L46,L47	Computer Forensics and Investigations	**M1,M4**

METHODS OF TEACHING

M1 : Lecture Method	**M6 : Tutorial**
M2 : Demo Method	**M7 : Assignment**
M3 : Guest Lecture	**M8 : Industry Visit**
M4 : Presentation /PPT	**M9 : Project Based**
M5 : Lab/Practical	**M10 : Charts / OHP**

Individual Time Table :

Course: IV-B.Tech : CSE					W.E.F:03-02-2023			
IV-CSE-D SEM-II								
	9.10-10.10	10.10-11.00	11.00-11:50	11.50:12:40	12.40-01:20	1.20-2.20	2.20-3:10	3.00-4.00
Period→ Day↓	I	II	III	IV		V	VI	VII
MON					LUNCH BREAK	CF	CF	
TUE			CF	CF				
WED						CF	CF	CF

Unit. NO	TOPIC	SCHEDULED DATE	COMPLETED DATE	REMARKS
I	**Cybercrime**			COMPLETED
II	**Initial Response and forensic duplication**			COMPLETED
III	**Computer Forensics analysis and validation, Network Forensics**			COMPLETED
IV	**Current Computer Forensic tools, Cell phone and mobile device forensics**			COMPLETED
V	**Working with Windows and DOS Systems**			COMPLETED

CMR ENGINEERING COLLEGE

KANDALKOYA (V), MEDCHAL ROAD, HYDERABAD-501 401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Mid - I ASSIGNMENT QUESTIONS (A.Y 2022-23)

Assignment Questions along with sample Assignments Scripts

1. List and explain forensic data tools.[CO1]
2. Explain the steps for live data acquisition and forensic duplication.[CO2]
3. Write the requirements of forensic duplication tools.[CO1]
4. List and explain forensic duplication tools[CO1].
5. Give the steps to duplicate and preserve digital evidence.[CO2]

CMR ENGINEERING COLLEGE

KANDALKOYA (V), MEDCHAL ROAD, HYDERABAD-501 401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Mid - II ASSIGNMENT QUESTIONS (A.Y 2022-23)

1. Write the goals of incident response in forensic science. [CO3]
2. Write major components of incident response. [CO3]
3. Enumerate steps for live data acquisition.[CO3]
4. List and explain the indications for detecting the incident.[CO4]
5. Briefly explain data-hiding techniques.[CO4]

9. Mid exam Question Papers along with sample Answers Scripts

CMR Engineering College

Kandlakoya(V), Medchal Road, Hyderabad
Department of Computer Science & Engineering

IV B.Tech II-SEM MID-I Examinations

Subject: Cyber Forensics A.Y.2022-2023

Answer any two of the following Questions. 2*5M=10M

1. a) List and explain forensic data tools. (CO1)
   b) Write major components of incident response. (CO1)

2. Give the steps to duplicate and preserve digital evidence. (CO2)

OR

3. Explain the steps for live data acquisition and forensic duplication. (CO1)

4. a) List and explain forensic duplication tools. (CO2)
   b) Briefly explain data-hiding techniques. (CO2)

CMR ENGINEERING COLLEGE

KANDALKOYA (V), MEDCHAL ROAD, HYDERABAD-501 401
DEPARTMENT OF INFORMATION TECHNOLOGY

IV B.Tech II-SEM MID-II Examinations

Subject: Cyber Forensics A.Y.2022-2023

Answer any two of the following 2x5=10M

1. a). List out some network tools and their uses. [CO3]
b). Define Some computer forensics software tools. [CO3]
2. explain the investigation process of e-mail crimes and violations . [CO4]
3. Describe mobile device forensics and acquisition procedures for cell phones .[CO4]
4. Explain about NTFS disks and windows registry [CO5]

10. Scheme of Evaluation

MID-I

Sl. No.		THEORY	MARKS	TOTAL
1	a)	List and explain forensic data tools. (CO1)	2.5	5
	b)	Write major components of incident response. (CO1)	2.5	
2		Give the steps to duplicate and preserve digital evidence.	5	5
3		Explain the steps for live data acquisition and forensic duplication		5
4	a	List and explain forensic duplication tools.	2.5	5
	b	Briefly explain data-hiding techniques.	2.5	
TOTAL MARKS				10 MARKS

MID-II

Sl. No.		THEORY	MARKS	TOTAL
1	a)	List out some network tools and their uses.	2.5	5
	b)	Define Some computer forensics software tools	2.5	
2		explain the investigation process of e-mail crimes and violations .		5
3		Describe mobile device forensics and acquisition procedures for cell phones .		5
4		Explain about NTFS disks and windows registry		5
TOTAL MARKS				10 MARKS

11. Mapping of COs with POs and PSO's

COURSE OUTCOME PO&PSO Matrix	Relationship of Course Outcomes (CO) to Program Outcomes (PO)													
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO 8	PO9	PO10	PO11	PO1 2	PS O1	PSO 2
CO1				2	2			2						
CO2				3	2	1		2						
CO3				2	2	2		2						
CO4				2	1	2		2						
CO5		2		2	2	1		2						
AVERAGE														

12. University Question Papers/ Question Bank

10 MARKS EACH

1.Explain the phases of incident response Methodology with neat diagram.

2.Explain evidence handling procedure

3.Explain sample structure of incident reporting form.

4.Explain the steps for prevention of cyber crime

5.Explain the term Hacker, Cracker and Phreaker with example

6.Explain in brief various tools available for ethical hacking?

7.What all volatile information which you will be collecting before switching off computer system. Also explain its role in digital forensic investigation.

8.What is Digital Forensics? What are the phases of Digital Forensic process?

9.Define Forensic Duplicate? How you will create Forensic Duplicate of a hard drive

10.Workforce private Limited is a business process outsourcing (BPO) outfit handling business

11.What are possible investigation phase carried out in Data Collection and Analysis.

12.Explain importance of forensic duplication and its methods.

13.List and explain in brief steps taken to collect live data from UNIX system

14.Write short notes on Intrusion detection and IPS

15.Explain guidelines for incident report writing. Give one report writing example

16.What are the steps involved in computer evidence handling? Explain in detail.

17.Explain with figure incident response methodology

18.Which types of forensic images created by incident response team for processing? Which one is most preferable

19.Explain the term network forensics, its major goal and function. What are the steps involved

in a generic network forensic examination?

5 MARKS EACH

1.List and explain the different types of digital evidence

2.What are the challenges in handling evidence?

3.What is the relationship between incident response, incident handling, incident management?

4.Explain the steps in ethical hacking.

5.What is cybercrime? What are the different roles of computer with respects to cybercrime?

6.Discuss the techniques of tracing an email message.

7.Explain how law enforcement is done in computer forensic.

10.List down various Digital Forensic tools and explain one toll with case study example

11.Write short notes on Evidence validation

12.Explain the term; Forensic duplicate, Qualified Forensic Duplicate.

13.Explain technique used to recover the deleted files.

14.Explain the phases after the detection of an incident.