AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Autonomous)

(Approved by A.I.C.T.E., New Delhi & Affiliated to J.N.T.U.H, Hyderabad)

NAAC "A" Accredited Institute

Gunthapally (V), Abdullapurmet (M), R.R (Dist), Near Ramoji film City, Hyderabad, Pin -501512.

www.aietg.ac.in, principalavih@avanthi.edu.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Course Structure

Program– M. Tech Computer Science and Engineering

(Applicable from the Academic Year 2025-2026 to 2028-2029)

Program: M. Tech Computer Science and Engineering **Regulation: R25**

II Year I Semester - Course Structure

S. No	Category	Course Code	Course Title	Hours per Week			
				Lecture	Tutorial	Practical	Credits
1	PE	R25D58301 R25D58302 R25D58303 R25D58304	**Professional Elective – V** 1. Digital Forensics 2. Advanced Operating Systems 3. Quantum Computing 4. Prompt Engineering	3	0	0	3
2	OE	R25D58305 R25D58306 R25D58307 R25D58301	**Open Elective** 1. Intellectual Property Rights 2. Generative AI 3. Intrusion Detection Systems 4. Digital Forensics	3	0	0	3
3	CC	MTCS2109	Dissertation Work Review - II	0	0	18	6
Total				**06**	**0**	**18**	**12**

Category	Courses	Credits
PE - Professional Elective Course	01	03
OE - Open Elective Course	01	03
CC - Compulsory Course	01	06
Total	**03**	**12**

Chairperson
Board of Studies (CSE)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Course Structure

Program– M. Tech Computer Science and Engineering

(Applicable from the Academic Year 2025-2026 to 2028-2029)

Program: M. Tech Computer Science and Engineering **Regulation: R25**

II Year II Semester - Course Structure

S. No	Category	Course Code	Course Title	Hours per Week			
				Lecture	Tutorial	Practical	Credits
1	CC	R25D58401	Dissertation Work Review - III	0	0	18	6
2	CC	R25D58402	Dissertation Viva-Voce	0	0	42	14
Total				**0**	**0**	**60**	**20**

Category	Courses	Credits
CC - Compulsory Course	02	20
Total	**02**	**20**

*Note: For Dissertation Work Review - I, Please refer 7.10 in R25 Academic Regulations.

Audit Course I & II:

1. English for Research Paper Writing
2. **Disaster Management**
3. Sanskrit for Technical Knowledge
4. Value Education
5. **Constitution of India**
6. Pedagogy Studies
7. Stress Management by yoga
8. Personality Development through Life Enlightenment Skills

Open Electives for other Departments:

1. **Intellectual Property Rights**
2. Generative AI
3. Intrusion Detection Systems
4. Digital Forensics.

Chairperson
Board of Studies (CSE)

R25D58301 **DIGITAL FORENSICS (PE - V)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: criminalistics as it relates to the investigative process, analysis of cyber criminalistics area, holistic approach to cyber-forensics.

UNIT - II

Cyber Crime Scene Analysis:
Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation:
Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, and complete a case, Critique a case.
Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.
Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.
Recent trends in mobile forensic technique and methods to search and seizure electronic evidence.

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCES:

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN : 1838648178.
2. Thomas J. Holt , Adam M. Bossler, Kathryn C. Seigfried-Spellar , Cybercrime and Digital Forensics: An Introduction, Routledge.

Chairperson
Board of Studies (CSE)

R25D58302 ADVANCED OPERATING SYSTEMS (PE - V) 3 0 0 3

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. To study, learn, and understand the main concepts of advanced operating systems (parallel processing systems, distributed systems, real time systems, network operating systems, and open source operating systems), Hardware and software features that support these systems.

Course Outcomes:

1. Understand the design approaches of advanced operating systems
2. Analyze the design issues of distributed operating systems.
3. Evaluate design issues of multi-processor operating systems.
4. Identify the requirements Distributed File System and Distributed Shared Memory.
5. Formulate the solutions to schedule the real time applications.

UNIT - I

Architectures of Distributed Systems: System Architecture Types, Distributed Operating Systems, Issues in Distributed Operating Systems, Communication Primitives. Theoretical Foundations: Inherent Limitations of a Distributed System, Lamport's Logical Clocks, Vector Clocks, Causal Ordering of Messages, Termination Detection.

UNIT - II

Distributed Mutual Exclusion: The Classification of Mutual Exclusion Algorithms, Non-Token – Based Algorithms: Lamport's Algorithm, The Ricart-Agrawala Algorithm, Maekawa's Algorithm, Token-Based Algorithms: Suzuki-Kasami's Broadcast Algorithm, Singhal's Heurisric Algorithm, Raymond's Heuristic Algorithm.

UNIT - III

Distributed Deadlock Detection: Preliminaries, Deadlock Handling Strategies in Distributed Systems, Issues in Deadlock Detection and Resolution, Control Organizations for Distributed Deadlock Detection, Centralized- Deadlock – Detection Algorithms, Distributed Deadlock Detection Algorithms, Hierarchical Deadlock Detection Algorithms.

UNIT - IV

Multiprocessor System Architectures: Introduction, Motivation for multiprocessor Systems, Basic Multiprocessor System Architectures Multi Processor Operating Systems: Introduction, Structures of Multiprocessor Operating Systems, Operating Design Issues, Threads, Process Synchronization, Processor Scheduling.

Distributed File Systems: Architecture, Mechanisms for Building Distributed File Systems, Design Issues

UNIT - V

Distributed Scheduling: Issues in Load Distributing, Components of a Load Distributed Algorithm, Stability, Load Distributing Algorithms, and Requirements for Load Distributing, Task Migration, and Issues in task Migration Distributed Shared Memory: Architecture and Motivation, Algorithms for Implementing DSM, Memory Coherence, Coherence Protocols, and Design Issues.

TEXT BOOK:

1. Advanced Concepts in Operating Systems, Mukesh Singhal, Niranjan G. Shivaratri, Tata McGraw-Hill Edition 2001.

REFERENCE BOOK:

1. Distributed Systems: Andrew S. Tanenbaum, Maarten Van Steen, Pearson Prentice Hall, Edition – 2, 2007.

Chairperson
Board of Studies (CSE)

R25D58303 **QUANTUM COMPUTING (PE - V)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. To introduce the fundamentals of quantum computing
2. The problem-solving approach using finite dimensional mathematics.

Course Outcomes:

1. Understand basics of quantum computing
2. Understand physical implementation of Qubit
3. Understand Quantum algorithms and their implementation
4. Understand the Impact of Quantum Computing on Cryptography

Unit-I

Introduction to Essential Linear Algebra

Some Basic Algebra, Matrix Math, Vectors and Vector Spaces, Set Theory

Complex Numbers

Definition of Complex Numbers, Algebra of Complex Numbers, Complex Numbers Graphically, Vector Representations of Complex Numbers, Pauli Matrices, Transcendental Numbers

Unit-II

Basic Physics for Quantum Computing

The Journey to Quantum, Quantum Physics Essentials, Basic Atomic Structure, Hilbert Spaces, Uncertainty, Quantum States, Entanglement

Basic Quantum Theory

Further with Quantum Mechanics, Quantum Decoherence, Quantum Electrodynamics, Quantum Chromo dynamics, Feynman Diagram Quantum Entanglement and QKD, Quantum Entanglement, Interpretation, QKE

Unit-III

Quantum Architecture

Further with Qubits, Quantum Gates, More with Gates, Quantum Circuits, The D-Wave Quantum Architecture.

Quantum Hardware

Qubits, How Many Qubits Are Needed? Addressing Decoherence, Topological Quantum Computing, Quantum Essentials.

Unit-IV

Quantum Algorithms

What Is an Algorithm? Deutsch's Algorithm, Deutsch-Jozsa Algorithm, Bernstein-Vazirani Algorithm, Simon's Algorithm, Shor's Algorithm, Grover's Algorithm.

Unit-V

Current Asymmetric Algorithms: RSA, Diffie-Hellman, Elliptic Curve.

The Impact of Quantum Computing on Cryptography: Asymmetric Cryptography, Specific Algorithms, Specific Applications.

TEXT BOOKS:

1. Nielsen M. A., Quantum Computation and Quantum Information, Cambridge University Press
2. Dr. Chuck Easttom, Quantum Computing Fundamentals, Pearson

REFERENCES:

1. Quantum Computing for Computer Scientists by Noson S. Yanofsky and Mirco A. Mannucci
2. Benenti G., Casati G. and Strini G., Principles of Quantum Computation and Information, Vol. Basic Concepts, Vol
3. Basic Tools and Special Topics, World Scientific. Pittenger A. O., An Introduction to Quantum Computing Algorithms.

Chairperson
Board of Studies (CSE)

R25D58304 **PROMPT ENGINEERING (PE - V)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. To introduce the principles and techniques of effective prompt engineering for generative AI models.
2. To understand the architecture, capabilities, and evolution of large language models such as GPT-3.5, GPT-4, Gemini, and LLaMA.
3. To explore standard practices in structured and unstructured text generation using tools like ChatGPT.
4. To apply chunking, tokenization, and formatting techniques for improving text generation and manipulation.
5. To understand the role of embeddings, vector databases (FAISS, Pinecone), and Retrieval-Augmented Generation (RAG) in modern NLP systems.

Course Outcomes:

1. Explain and apply the core principles of prompt engineering for guiding generative AI outputs effectively.
2. Describe the underlying architecture and functionality of state-of-the-art large language models (LLMs).
3. Generate and manipulate structured outputs (JSON, YAML, CSV) using ChatGPT with advanced prompting techniques.
4. Implement text chunking, tokenization, and format control using tools like SpaCy, Tiktoken, and Python.
5. Utilize vector databases such as FAISS and Pinecone in Retrieval-Augmented Generation (RAG) pipelines for efficient information retrieval.

UNIT – I

Fundamentals and Principles of Prompting

Overview of the Five Principles of Prompting: Give Direction, Specify Format, Provide Examples, Evaluate Quality, Divide Labor.

UNIT – II

Introduction to Large Language Models for Text Generation

What Are Text Generation Models, Vector Representations: The Numerical Essence of Language, Transformer Architecture: Orchestrating Contextual Relationships, Probabilistic Text Generation: The Decision Mechanism, Historical Underpinnings: The Rise of Transformer Architectures, OpenAI's Generative Pretrained Transformers, GPT-3.5-turbo and ChatGPT, GPT-4, Google's Gemini, Meta's Llama and Open Source.

UNIT – III

Standard Practices for Text Generation with ChatGPT- Part-A

Generating Lists, Hierarchical List Generation, When to Avoid Using Regular Expressions, Generating JSON, YAML Filtering YAML Payloads, Handling Invalid Payloads in YAML, Diverse Format Generation with ChatGPT, Mock CSV Data, Universal Translation Through LLMs, Ask for Context, Text Style Unbundling, Identifying the Desired Textual Features, Generating New Content with the Extracted Features, Extracting Specific Textual Features with LLMs.

UNIT – IV

Standard Practices for Text Generation with ChatGPT- Part-B

Chunking Text, Benefits of Chunking Text, Scenarios for Chunking Text, Poor Chunking Example, Chunking Strategies, Sentence Detection Using SpaCy, building a Simple Chunking Algorithm in Python, Sliding Window Chunking, Text Chunking Packages, Text Chunking with Tiktoken, Encodings, Understanding the Tokenization of Strings.

UNIT – V

Vector Databases with FAISS and Pinecone

Retrieval Augmented Generation (RAG), Introducing Embeddings, Document Loading Memory Retrieval with FAISS, RAG with Lang Chain, Hosted Vector Databases with Pinecone, Self-Querying, Alternative Retrieval Mechanisms.

TEXTBOOK:

1. Phoenix J, Taylor M. Prompt engineering for generative AI. " O'Reilly Media, Inc."; 2024 May 16.

REFERENCES:

1. Tunstall L, Von Werra L, Wolf T. Natural language processing with transformers. " O'Reilly Media, Inc."; 2022 Jan 26.

2. Foster D. Generative deep learning. " O'Reilly Media, Inc."; 2022 Jun 28.

Chairperson
Board of Studies (CSE)

R25D58305 **INTELLECTUAL PROPERTY RIGHTS (OE)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. Distinguish and explain various forms of IPRs.
2. Identify criteria to fit one's own intellectual work in particular form of IPRs.
3. Apply statutory provisions to protect particular form of IPRs.

UNIT – I

Introduction to Intellectual property: Introduction, types of intellectual property, international organizations, agencies and treaties, importance of intellectual property rights.

UNIT – II

Trade Marks: Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting, and evaluating trade mark, trade mark registration processes.

UNIT – III

Law of copyrights: Fundamental of copyright law, originality of material, rights of reproduction, rights to perform the work publicly, copyright ownership issues, copyright registration, and notice of copyright, international copyright law.

Law of patents: Foundation of patent law, patent searching process, ownership rights and transfer

UNIT – IV

Trade Secrets: Trade secret law, determination of trade secret status, liability for misappropriations of trade secrets, protection for submission, trade secret litigation.

Unfair competition: Misappropriation right of publicity, false advertising.

UNIT – V

New development of intellectual property: new developments in trade mark law; copyright law, patent law, intellectual property audits.

International overview on intellectual property, international – trade mark law, copyright law, international patent law, and international development in trade secrets law.

TEXT & REFERENCE BOOKS:

1. Intellectual property right, Deborah. E. Bouchoux, Cengage learning.
2. Intellectual property right – Unleashing the knowledge economy, prabuddha ganguli, Tata McGraw Hill Publishing company ltd.

Chairperson
Board of Studies (CSE)

R25D58306 **GENERATIVE AI (OE)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Course Objectives:

1. To introduce the foundations, evolution, and core concepts of AI, ML, DL, NLP, and Generative AI.
2. To develop understanding of advanced neural architectures and generative models such as GANs, VAEs, and Transformers.
3. To explore Large Language Models, prompt engineering, and their real-world applications.
4. To familiarize learners with frameworks, multimodal applications, and ethical considerations in Generative AI.

Course Outcomes:

1. Demonstrate knowledge of AI foundations, generative models, and advanced neural architectures.
2. Apply generative AI techniques to create solutions for text, image, video, and multimodal tasks.
3. Design, fine-tune, and optimize Large Language Models for specific applications.
4. Evaluate ethical, social, and legal implications of Generative AI deployments and propose mitigation strategies.

UNIT – I

Foundations of AI and Generative Models

Introduction and historical evolution to Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP)and Deep Learning (DL), Structure of Artificial Neural Networks (ANNs), Mathematical and computational foundations of generative modeling, Overview of generative models and their applications across various domains; Importance of Generative AI in modern applications, Transfer learning and in advancing Generative AI.

UNIT – II

Advanced Neural Architectures for Generative AI

Variational Auto encoders (VAEs): principles and applications, Generative Adversarial Networks (GANs): architecture and working principles; Transformer architecture and attention mechanisms (in detail); Long Short-Term Memory Networks (LSTMs) and the limitations of traditional RNNs/LSTMs, Advanced Transformer architectures and techniques, Pre-training and transfer learning strategies for generative models.

UNIT – III

Large Language Models and Prompt Engineering

Overview of Large Language Models (LLMs), GPT architecture, variants, and working principles, Pr-training and fine-tuning GPT models for applications (e.g., chatbots, text generation), Case study: GPT-based customer support chatbot, BERT architecture, pre-training objectives, and fine-tuning, Prompt Engineering: Designing effective prompts, controlling model behavior, and improving output quality, Fine-tuning language models for creative writing and chatbot development

UNIT – IV

Multi-Agent Systems and Generative AI Applications

Introduction to Multi-Agent Systems (MAS),Types of agents: reactive, deliberative, hybrid, and learning agents, Multi-agent collaboration and orchestration for generative tasks, Use cases: autonomous research assistants, cooperative creative generation, distributed problem-solving, Frameworks and tools: AutoGen, CrewAI, Hugging GPT for LLM-powered multi-agent systems, Generative AI applications: Art, Creativity, Image/Video generation, Music composition, Healthcare, Finance, Real-world case studies and deployment challenges

UNIT – V

Frameworks, Multimodal Applications, and Ethics

LangChain framework: components and LLM application development, Retrieval-Augmented Generation (RAG), Embeddings, Indexing networks, and Vector databases, Generative AI across modalities: Text, Code, Image, and Video generation, Image and Video generation using GANs and VAEs, Multimodal Generative AI: integration and training strategies, Ethical considerations: bias, fairness, trust, and responsible AI deployment, Social and legal implications of Generative AI, Risk mitigation strategies and real-world ethical case studies.

TEXTBOOK:

1. Altaf Rehmani, Generative AI for Everyone: Understanding the Essentials and Applications of This Breakthrough Technology.

2. Charu C. Aggarwal, Neural Networks and Deep Learning: A Textbook.Joseph Babcock, Raghav Bali, Generative AI with Python and TensorFlow 2, 2024.

REFERENCES:

1. Josh Kalin, Generative Adversarial Networks Cookbook.

2. Jesse Sprinter, Generative AI in Software Development: Beyond the Limitations of Traditional Coding, 2024.

Chairperson
Board of Studies (CSE)

R25D58307 **INTRUSION DETECTION SYSTEMS (OE)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Prerequisites: Computer Networks, Computer Programming

Course Objectives:

1. Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.

2. Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

Course Outcomes:

1. Understand fundamental knowledge of intrusion detection and prevention.

2. Understand different types of attacks in network layer and code injection human layer.

3. Analyze different anomaly detection algorithms.

UNIT - I

The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN's -Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS.

UNIT - II

Classes of attacks - Network layer: scans, denial of service, penetration Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers Kids/hackers/sop, Hesitated groups-Automated: Drones, Worms, Viruses.

UNIT - III

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS.

UNIT - IV

Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)-Host-based Anomaly Detectors-Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection.

UNIT - V

Attack trees and Correlation of alerts- Autopsy of Worms and Botnets-Malware detection - Obfuscation, polymorphism- Document vectors.

Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation Traitors, Decoys and Deception-Future: Collaborative Security

TEXT BOOKS:

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press ISBN 0-321 30545-3.

2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses.

REFERENCE BOOKS:

1. Saiful Hasan, Intrusion Detection System, Kindle Edition.

2. Ankit Fadia, Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection.

Online Websites/Materials:

1. https://www.intechopen.com/books/intrusion-detection-systems.

Online Courses:

1. https://www.sans.org/course/intrusion-detection-in-depth.
2. https://www.cybrary.it/skill-certification-course/ids-ips-certification-training-course**.**

Chairperson
Board of Studies (CSE)

R25D58301 **DIGITAL FORENSICS (OE)** **3 0 0 3**

M.Tech II Year I Semester (Computer Science & Engineering)

Pre-Requisites: Cybercrime and Information Warfare, Computer Networks

Course Objectives:

1. Provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
2. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
3. Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools.
4. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics.

Course Outcomes: On completion of the course the student should be able to

1. Understand relevant legislation and codes of ethics.
2. Computer forensics and digital detective and various processes, policies and procedures.
3. E-discovery, guidelines and standards, E-evidence, tools and environment.
4. Email and web forensics and network forensics.

UNIT - I

Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber criminalities area, holistic approach to cyber-forensics

UNIT - II

Cyber Crime Scene Analysis:

Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

UNIT - III

Evidence Management & Presentation:

Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

UNIT - IV

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, and complete a case, Critique a case, Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

UNIT - V

Mobile Forensics: mobile forensics techniques, mobile forensics tools.

Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Recent trends in mobile forensic technique and methods to search and seizure electronic evidence

TEXT BOOKS:

1. John Sammons, The Basics of Digital Forensics, Elsevier
2. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

REFERENCES:

1. William Oettinger, Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt Publishing; 1st edition (30 April 2020), ISBN: 1838648178.

2. Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge.

Chairperson
Board of Studies (CSE)