

Branch Name:	Bachelor of Science (CS)
Program Code:	ET112
Semester/Year:	Semester - VI/ Third Year
Course Title:	Ethical Hacking & Cyber Security
Course Code:	16-CSM304-3C
Pre-requisite Course:	Computer Network, Basics of Security

Course Objectives: The objective of this course is to provide students with fundamental knowledge of Ethical Hacking, security principles, and legal aspects of cybersecurity practices. The course focuses on Footprinting, scanning, vulnerability assessment, exploitation techniques, malware analysis, sniffing, session hijacking, and DoS/DDoS attacks. It also aims to develop the ability to analyze security issues in web, wireless, and mobile environments and apply defensive mechanisms such as intrusion detection systems, firewalls, honeypots, and secure system configurations.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
3	0	2	4	50	25	-	25	100

Course Contents:

Unit No	Topic	Total Hours	Weight age (%)
1	Ethical hacking fundamentals: Security Fundamental, Security testing, Hacker and Cracker, Penetration Testing Methodology, Cyber Kill Chain Model, Overview of Security Testing Frameworks (NIST, OWASP), Types of penetration testing (Black Box, White Box, Grey Box), Cyber security attack lifecycle, Responsible disclosure and vulnerability reporting	3	05
2	Technical foundations & network attacks: The Attacker's Process, The Ethical Hacker's Process, Security and the Stack, TCP/IP vulnerabilities, Common network attack vectors, Introduction to Kali Linux and penetration testing environment	4	10
3	Foot printing & scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface, Active vs Passive reconnaissance, DNS enumeration techniques, Introduction to tools: Nmap, Shodan, Maltego	5	10
4	Malware Threats: Viruses and Worms, Trojans, Covert Communication, Keystroke Logging and Spyware, Malware Counter measures, Ransomware attacks, Fileless malware, Malware analysis basics	5	15
5	Sniffing & DoS attacks: Sniffers, Session Hijacking, Denial of Service and Distributed Denial of Service, Man-in-the-Middle attacks, ARP poisoning, DNS spoofing attacks	5	15

6	Web Application Security: OWASP Top 10 vulnerabilities, SQL Injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Command injection, Directory traversal, Burp Suite, OWASP ZAP	5	15
7	Wireless & mobile security: Wireless Technologies, Mobile Device Operation and Security, Wireless LANs, WPA2 vs WPA3 security, Rogue access point attacks, Evil twin attack, Mobile application security threats	5	10
8	IDS, firewall & defense: Intrusion Detection Systems, Firewalls, Honeypots, Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), Network monitoring tools-Snort, Suricata, Splunk	4	10
9	Application & cloud security: SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security, API security vulnerabilities, Authentication bypass attacks, Cloud application security basics	4	10

Reference Books:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification
2. Hacking the Hacker, Roger Grimes, Wiley
3. The Unofficial Guide to Ethical Hacking, Ankit Fadia, Premier Press
4. CEH v12 Study Guide – Ric Messier
5. Web Application Hacker's Handbook – Dafydd Stuttard

List of Experiments:

1. Introduction to Kali Linux tools
2. Footprinting using WHOIS, Shodan, Maltego
3. Network scanning using Nmap
4. Vulnerability scanning using Nessus / OpenVAS
5. Packet sniffing using Wireshark
6. Password cracking using John the Ripper / Hydra
7. Web application testing using Burp Suite / OWASP ZAP
8. Wireless network security analysis
9. Mini penetration testing project

Course Learning Outcomes (CLO):

CLO	Course Learning Outcome	Bloom's Taxonomy Level
CLO1	Explain fundamental security concepts, ethical hacking principles, phases, and legal considerations.	1. Remembering, 2. Understanding
CLO2	Perform foot printing, scanning, and enumeration to assess vulnerabilities in network systems.	3. Applying, 4. Analyzing
CLO3	Analyze cyber-attack techniques including malware, sniffing, session hijacking and denial of service.	4. Analyzing, 5. Evaluating
CLO4	Evaluate and apply hacking techniques for web applications, databases, wireless and mobile systems.	3. Applying, 5. Evaluating
CLO5	Recommend and configure security controls such as IDS, Firewalls, Honeypots and mitigation strategies.	5. Evaluating, 6. Creating

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	M	M	-	-	M	H	-	H	-	-	-	M	M	H	M	-
CLO2	H	H	M	H	H	-	-	-	M	M	-	M	H	H	H	M
CLO3	M	H	-	H	H	M	-	M	-	-	-	M	H	H	H	-
CLO4	M	H	H	H	H	M	-	M	M	M	-	M	H	H	H	M
CLO5	M	M	H	H	H	M	-	M	M	M	M	H	H	H	H	H

H: High, M: Medium, L: Low

Branch Name:	Bachelor of Science (CS)
Program Code:	ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Cyber Forensics
Subject Code:	16-CSM305-3C
Pre-requisite:	Computer Networks, Ethical Hacking, Basic knowledge of Windows, Mac and Linux OS

Course Objective: The objective of this course is to provide students with fundamental knowledge of cyber forensic investigation techniques, digital evidence handling, and forensic tools used to investigate cybercrimes. The course enables students to analyze digital evidence from various platforms including operating systems, networks, mobile devices, cloud environments, and storage devices.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
3	0	2	4	50	25	-	25	100

Subject Contents				
Sr. No.	Topic	Total Hours	Weightage (%)	
1	Introduction to Cyber Forensics: Cybercrime and its types, Basics of Cyber Forensics, Cyber Forensic Investigation Process, Digital Evidence and Evidence Handling, Challenges in Cyber Forensics, Skills required for Cyber Forensic Experts	04	10	
2	Operating System Forensics: Digital Evidence in Windows, File System Analysis Timeline Analysis, Challenges in OS Forensics, Digital Evidence in Macintosh Systems, Digital Evidence in UNIX/Linux Systems	08	15	
3	Network Forensics: Network Forensic Concepts, Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts, Investigation of Network Attacks, ICMP Attacks and Network Intrusion Detection	07	15	
4	Mobile Device Forensics: Introduction to Mobile Forensics, Acquisition Protocols, Android Operating System Forensics, Manual Extraction Methods, Physical Acquisition, Challenges in Mobile Forensics	07	15	
5	Cloud, Web and Email Forensics: Introduction to Cloud Forensics, Cloud Artifacts and Investigation, Challenges in Cloud Environment, Forensics as a Service (FaaS), Web Attack Forensics, Intrusion and Database Forensics, Email Forensics and Header Analysis, Introduction to Blockchain Technology and Cryptocurrency Investigation	11	25	
6	Solid State Device (SSD) Forensics: SSD Components, SSD Architecture and Working, Challenges in SSD Forensics, Forensic Analysis of SSD Storage	04	10	
7	Forensic Report Writing: Importance of Documentation in Investigation, Structure of a Forensic Report, Guidelines for Preparing Investigation Reports, Legal Aspects of Digital Evidence Documentation	04	10	

List of Reference Books:

1. Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations – Niranjana Reddy
2. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet – Eoghan Casey
3. CyberForensics: Understanding Information Security Investigation – Jennifer Bayuk
4. Cyber Forensics: From Data to Digital Evidence – Albert J. Marcella Jr.
5. Guide to Computer Forensics and Investigations – Nelson, Phillips & Stuart

List of Suggested titles of Experiments:

Students will perform hands-on experiments using digital forensic tools to investigate cyber incidents.

Practical activities include:

1. Study of digital forensic tools (Autopsy, FTK Imager, EnCase, Wireshark)
2. Recovery of deleted or lost files
3. Disk imaging and analysis
4. Network packet analysis
5. Email header investigation
6. Mobile forensic data extraction
7. Preparation of forensic investigation report

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Understand the fundamentals of cyber forensics and cybercrime investigation	1. Remembering 2. Understanding,
CLO2	Analyze and validate digital forensic evidence from multiple platforms	3. Applying 4. Analyzing
CLO3	Use forensic tools and techniques for investigating cyber incidents	3. Applying 4. Analyzing
CLO4	Prepare professional forensic investigation reports	4. Analyzing 5. Evaluating

Mapping of CLOs with Pos & PSOs:

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M									M	H	M	L	-
CLO2	M	H	H	M	H	M	M	M	M	L	L	H	M	H	M	L
CLO3	M	H	H	M	H	M	M	M	M	M	M	H	H	M	H	M
CLO4	M	H	H	M	L	M	M	M	M	M	M	H	M	H	H	L

H: High, M: Medium, L: Low

Branch Name:	Bachelor of Science (CS)
Program Code:	ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Cyber Crime and Law
Subject Code:	16-CSM306-3C
Pre-requisite:	Basics of knowledge of computer and Information technology.

Course Objective: The objective of this course is to provide students with fundamental knowledge of Cybercrime and Cyber Law concepts, cyberattack techniques, and digital investigation methods. The course focuses on understanding cybercrime investigation procedures, cyber laws, and digital evidence regulations applicable to modern computing environments. It also aims to develop the ability to analyze and apply cyber law principles in real-world cybercrime and digital forensic cases.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
03	00	02	04	50	25	-	25	100

Subject Contents			
Sr. No	Topic	Lecture Hours	Weight age (%)
1	Introduction to cyber-crime: Definition and evolution of cybercrime, Cyber crime vs traditional crime, Cyber-crime and information security, Cyber criminals: motives and characteristics, Classification of cyber-crimes, Common cyber-crimes: Email spoofing, Spamming, Cyber defamation, Data diddling, Salami attacks, Software piracy, Internet time theft, Cyber-crime ecosystem and digital underground economy	06	10
2	Cyber offenses & social engineering: Cyber-attack lifecycle, how cyber criminals plan attacks, Active and passive cyber-attacks, social engineering attacks, Types of social engineering techniques, Cyber stalking and online harassment, Cyber-crimes in public networks and cyber cafes, Botnets and command-and-control infrastructure, Attack vectors and entry points, Cyber-crime in cloud computing environments	08	20
3	Tools and techniques used in cybercrime: Proxy servers and anonymizers, Phishing attacks and phishing kits, Password cracking techniques, Keyloggers and spyware, Malware types: viruses, worms, trojans, Backdoors and remote access tools, DoS and DDoS attacks, SQL injection attacks, Buffer overflow attacks, Wireless network attacks, Digital footprint tracking and anonymization	08	25

4	Phishing and Identity Theft: Phishing attacks and their evolution, Methods and techniques of phishing, Types of phishing attacks: Spear phishing, Whaling, Clone phishing, Business Email Compromise (BEC), Identity theft: concepts and impact, Techniques used in identity theft, financial fraud and OTP fraud, Countermeasures and preventive strategies	08	20
5	Cyber law and IT Act: Overview of cyber law, Information Technology Act 2000, IT Amendment Act 2008, Offenses and penalties under IT Act, Cyber tribunals and adjudication process, Digital evidence and Indian Evidence Act, Cyber law enforcement agencies, Limitations of cyber law, International cyber law and conventions (Budapest Convention)	06	20

List of Reference Books:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives By Nina Godbole, Sunit Belapur, Wiley
2. Understanding Cybercrime: Phenomena, and Legal Challenges Response, ITU 2012
3. Cyber Laws – Bare Act with Short Notes – Universal Publications
4. Cybercrime Law – Jonathan Clough

List of Suggested titles of Experiments:

1. Study of major cybercrime case studies
2. Analysis of phishing email samples
3. Demonstration of social engineering attacks (simulation)
4. Cybercrime reporting process in India
5. Study of IT Act 2000 sections related to cybercrime
6. Demonstration of network traffic analysis using Wireshark
7. Basic digital evidence analysis
8. Study of cybercrime investigation workflow
9. Case study of ransomware attacks
10. Legal analysis report on a recent cybercrime case

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Course Learning Outcome	Bloom's Taxonomy Level
CLO1	Explain major types of cybercrimes, attackers' motives and crime techniques.	1. Remembering, 2. Understanding
CLO2	Identify cyber vulnerabilities and evaluate exploitation techniques including malware, DoS, phishing and social engineering.	2. Understanding, 3. Applying, 5. Evaluating
CLO3	Interpret and apply legal provisions related to cybercrime investigation and digital evidence under the IT Act and international cyber laws.	2. Understanding, 3. Applying, 5. Evaluating
CLO4	Recommend and apply cyber law enforcement strategies for prevention, detection and control of digital crimes.	3. Applying, 5. Evaluating, 6. Creating

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	M	L	M	M	H	H	L	M	L	L	M	M	M	M	L	-
CLO2	M	M	H	M	H	H	M	M	M	M	M	H	H	H	H	M
CLO3	M	M	H	M	H	H	H	H	M	H	H	H	H	H	H	M
CLO4	H	M	H	M	H	H	H	H	M	H	H	H	H	H	H	H

H: High, M: Medium, L: Low

Branch Name:	B.Sc. (CS)
Program Code:	ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Machine Learning
Subject Code:	16-CSE302-3C
Pre-requisite:	Logic, Calculus, Linear Algebra, and Statistics

Course Objective: The objective of this course is to provide students with fundamental knowledge of Machine Learning techniques and their applications in cybersecurity. The course focuses on applying machine learning methods for detecting cyber threats, anomalies, malware behavior, and intrusion activities using security data and network traffic analysis. It also aims to develop skills in designing and implementing machine learning models and Python-based solutions for cyber-attack detection and threat intelligence applications.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
03	00	02	04	50	25	-	25	100

Subject Contents			
Sr. No	Topic	Total Hours	Weight (%)
1	Introduction to Machine Learning and Cyber Security Applications: Need for ML in Cyber Security, Types of Machine Learning (Supervised, Unsupervised, Reinforcement Learning), ML workflow in cyber security analytics, Machine Learning challenges in security systems, Data sources in cyber security: Network traffic data, Log data, Malware datasets, Big data analytics for cyber threat intelligence, Data visualization for security monitoring	8	20
2	Data Preprocessing and Feature Engineering for Security Data: Understanding security datasets, Data cleaning and preprocessing, Feature extraction from network traffic, Feature selection techniques, Dimensionality reduction (PCA, LDA), Handling imbalanced datasets in cyber security, Learning theory fundamentals, Concept learning and modelling	8	20
3	Similarity-based Learning and Regression for Security Analytics: Instance-based learning, K-Nearest Neighbor (KNN) algorithm, Weighted KNN, Nearest centroid classifier, Regression models for prediction, Linear regression, Logistic regression for classification, Model validation techniques, Applications: Spam detection, Network anomaly detection, Phishing email classification	8	20

4	Decision Trees and Bayesian Learning for Threat Detection: Decision tree classifiers, Impurity measures (Entropy, Gini Index), Decision tree regression, Random Forest concepts, Bayesian learning fundamentals, Naive Bayes classifier, Probabilistic models for classification, Applications: Malware classification, Intrusion detection systems, Email spam filtering	8	20
5	Clustering and Reinforcement Learning for Security Systems: Clustering techniques: K-Means clustering, Hierarchical clustering, Clustering for anomaly detection, Reinforcement learning basics, Q-learning, Adaptive security systems using RL, Applications: Insider threat detection, Botnet detection, Fraud detection in financial systems	8	20

List of Reference Books:

1. S Sridhar and M Vijayalakshmi, “Machine Learning”, Oxford University Press, 2021.
2. M N Murty and Ananthanarayana V S, “Machine Learning: Theory and Practice”, Universities Press (India) Pvt. Limited, 2024.
3. Tom M. Mitchell, “Machine Learning”, McGraw-Hill Education, 2013.
4. Miroslav Kubat, “An Introduction to Machine Learning”, Springer, 2017.

List of Suggested titles of Experiments:

1. Data preprocessing on network intrusion dataset
2. Implement spam detection using Naive Bayes
3. Network anomaly detection using KNN
4. Malware classification using Decision Tree
5. Intrusion detection using Random Forest
6. Clustering network traffic using K-Means
7. Feature selection on cybersecurity datasets
8. Phishing email detection using ML
9. Build intrusion detection model using Python (Scikit-Learn)
10. Mini project: ML based cyber-attack detection system

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Course Learning Outcome	Bloom's Taxonomy Level
CLO1	Explain machine learning concepts and their application in cyber security analytics.	1. Remembering, 2. Understanding
CLO2	Apply supervised learning techniques to detect cyber-attacks and classify security events.	3. Applying, 4. Analyzing
CLO3	Evaluate machine learning models for intrusion detection and threat intelligence.	4. Analyzing 5. Evaluating
CLO4	Apply unsupervised learning methods for anomaly detection in network traffic.	3. Applying, 4. Analyzing
CLO5	Design machine learning solutions for cyber security problems using modern tools.	5. Evaluating 6. Creating

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3	PSO 4
CLO1	H	H	M	M	M	L	-	-	L	L	-	M	H	M	L	-
CLO2	H	H	H	H	H	M	-	-	M	M	-	M	H	H	H	M
CLO3	M	H	H	H	H	M	-	-	M	M	-	H	H	H	H	H
CLO4	M	M	H	H	H	L	-	-	M	M	-	M	M	H	H	M
CLO5	H	M	H	M	H	M	-	-	H	H	M	H	H	H	H	H

H: High, M: Medium, L: Low

Branch Name:	Bachelor of Science (DS/CS)
Program Code:	ET111/ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Image Processing
Subject Code:	16-DSE307-3C
Pre-requisite:	Logic, Calculus, Linear Algebra, and Statistics

Course Objective: The objective of this course is to provide students with fundamental knowledge of Digital Image Processing and computer vision techniques used for image analysis and intelligent systems. The course focuses on applying image processing methods for pattern recognition, surveillance, biometrics, and security-related applications. It also aims to develop practical skills in implementing image analytics solutions using machine learning, data science techniques, and Python libraries such as OpenCV and Scikit-image.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
03	00	02	04	50	25	-	25	100

Subject Contents				
Sr. No	Topic	Lecture Hours	Weight age (%)	
1	Digital Image Fundamentals and Data Representation: Introduction to Digital Image Processing, Image representation as data (pixels and matrices), Human visual system, Image sampling and quantization, Image datasets and formats, Image acquisition systems, Applications in Data Science and Cyber Security: surveillance systems, biometric authentication, malware image visualization	6	15	
2	Image Enhancement and Feature Extraction Gray level transformations, Histogram equalization and histogram matching, Spatial filtering (low-pass, high-pass filters), Edge detection (Sobel, Prewitt, Canny), Feature extraction from images, Image preprocessing for machine learning, Applications: object detection in surveillance, face detection systems, preprocessing images for data analytics	10	25	
3	Frequency Domain Processing and Image Restoration: Fourier Transform in image processing, Frequency domain filtering, Image smoothing and sharpening, Homomorphic filtering, Noise models in images, Image restoration techniques, Image denoising using machine learning, Applications: forensic image analysis, enhancement of CCTV images, improving low-quality security footage	10	25	
4	Colour Image Processing and Image Compression: Colour models (RGB, HSV,	8	20	

	YCbCr) , Colour image processing techniques , Image compression fundamentals, Lossless and lossy compression, Huffman, Arithmetic and LZW coding, JPEG compression standard, Applications: multimedia data analysis, secure transmission of image data, storage optimization for surveillance systems		
5	Morphological Processing and Computer Vision Applications: Morphological operations (erosion, dilation), Opening and closing operations, connected component analysis, Shape analysis and pattern detection, Image segmentation basics, Applications: biometric authentication systems, facial recognition and access control, anomaly detection in visual data	8	15

List of Reference Books:

1. Digital Image Processing, Second Edition by Rafael C. Gonzalez and Richard E. Woods, Pearson Education
2. Digital Image Processing by Bhabatosh Chanda and Dwijesh Majumder, PHI
3. Fundamentals of Digital Image Processing by Anil K Jain, PHI
4. Digital Image Processing Using Matlab, Rafael C. Gonzalez and Richard E. Woods, Pearson Education

List of Suggested titles of Experiments:

1. Image preprocessing using Python (OpenCV)
2. Histogram equalization and contrast enhancement
3. Edge detection using Sobel and Canny filters
4. Feature extraction from images
5. Image denoising techniques
6. Image compression using JPEG algorithm
7. Morphological operations on images
8. Face detection using OpenCV
9. Object detection from surveillance images
10. Mini project: Image analytics for security or data science application

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Course learning outcome	Bloom's Taxonomy Level
CLO1	Explain digital image formation and image data representation.	1. Remembering, 2. Understanding
CLO2	Apply image enhancement and feature extraction techniques for data analysis.	2. Understanding 3. Applying,
CLO3	Analyze images using frequency domain processing and restoration methods.	3. Applying, 4. Analyzing
CLO4	Apply compression and color processing techniques for multimedia data management.	3. Applying, 4. Analyzing
CLO5	Develop image processing solutions for applications in data science and cyber security.	3. Applying, 5. Evaluating

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3	PSO 4
CLO1	M	M	M	M	H	L	-	-	M	L	-	M	M	M	L	-
CLO2	M	M	H	M	H	L	-	-	M	M	-	M	H	H	M	L
CLO3	M	M	H	H	H	M	-	-	M	M	-	H	H	H	H	M
CLO4	M	M	H	H	M	L	-	-	M	M	-	M	M	H	H	M
CLO5	M	M	H	M	H	M	-	-	M	M	-	H	H	H	H	H
CLO6	M	M	M	M	H	L	-	-	M	L	-	M	M	M	L	-

H: High, M: Medium, L: Low

Branch Name:	Bachelor of Science (DS/CS)
Program Code:	ET111/ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Digital Communication
Subject Code:	16-DSE308-3C
Pre-requisite:	Basic knowledge of Analog Communication, Digital Electronics, and Signal Processing concepts

Course Objective: The objective of this course is to provide students with fundamental knowledge of Digital Communication systems and their core building blocks. The course focuses on understanding the differences between analog and digital communication and the advantages of digital transmission techniques. It also aims to develop analytical skills in sampling, quantization, coding methods, and various digital modulation techniques used in modern communication systems.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
03	00	02	04	50	25	-	25	100

Subject Contents				
Sr. No	Topic	Total Hours	Weight (%)	
1	Introduction to Digital Communication Basics of communication systems – analog vs digital; advantages of digital systems; block diagram of digital communication system; sampling theorem; noise and SNR.	6	15%	
2	Pulse and Baseband Digital Modulation Sampling, quantization, coding; PCM, DPCM, Delta modulation; time division multiplexing (TDM); line coding schemes (NRZ, RZ, Manchester).	8	20%	
3	Passband Modulation Techniques ASK, FSK, PSK, QPSK, M-ary modulation; transmitter and receiver models; detection techniques; probability of error; performance in AWGN.	10	20%	
4	Information Theory and Source Coding Concept of information and entropy; mutual information; source coding – Shannon-Fano and Huffman coding; channel capacity; Shannon's theorem.	7	15%	
5	Channel Coding and Error Control Error detection and correction; linear block codes; Hamming and cyclic codes; convolutional codes; Viterbi decoding; comparison of codes.	8	15%	
6	Multiplexing, Multiple Access and Wireless Channels TDM, FDM, CDMA; multiple access techniques; fading and multipath effects; introduction to OFDM; applications in modern communication networks.	6	15%	

List of Reference Books:

1. Simon Haykin, Digital Communications, John Wiley & Sons.
2. Bernard Sklar, Digital Communications: Fundamentals and Applications, Pearson.
3. Taub & Schilling, Principles of Communication Systems, McGraw-Hill.
4. B.P. Lathi, Modern Digital and Analog Communication Systems, Oxford University Press.

List of Suggested titles of Experiments:

1. Study of analog vs digital communication system components.
2. Simulation of PCM and DPCM systems.
3. Implementation of Delta Modulation and reconstruction of original signal.
4. Study and simulation of line coding techniques (NRZ, RZ, Manchester).
5. Simulation of ASK, FSK, PSK, and QPSK modulation & demodulation.
6. Plot and analyze BER vs SNR for different modulation schemes.
7. Implementation of Shannon-Fano and Huffman source coding for text data.
8. Demonstration of Hamming code generation and error correction.
9. Study of TDM and FDM multiplexing using simulation.
10. Mini-project: Design a simple digital communication link (transmitter–receiver) in software or hardware.

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Course Learning Outcome	Bloom's Level
CLO1	Explain digital communication system model, sampling theorem, noise and SNR.	1. Remembering, 2. Understanding
CLO2	Analyze and apply baseband modulation techniques including PCM, DPCM, and TDM.	3. Applying, 4. Analyzing
CLO3	Analyze performance of passband modulation schemes (ASK, FSK, PSK, QPSK) in AWGN.	4. Analyzing, 5. Evaluating
CLO4	Apply information theory concepts including entropy, coding techniques and channel capacity.	3. Applying, 4. Analyzing
CLO5	Apply channel coding and error control techniques and evaluate system robustness.	3. Applying, 5. Evaluating
CLO6	Design and simulate digital communication models using modern tools.	3. Applying 6. Creating,

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3	PSO 4
CLO1	H	H	M	M	M	L	-	-	L	L	-	M	M	M	L	-
CLO2	H	H	H	M	H	L	-	-	M	M	-	M	H	H	M	L
CLO3	H	H	H	H	H	M	-	-	M	M	-	H	H	H	H	M
CLO4	M	M	H	H	M	L	-	-	M	M	-	M	M	H	H	M
CLO5	M	M	H	M	H	M	-	-	M	M	-	H	H	H	H	H
CLO6	M	M	H	M	H	M	-	-	H	H	M	H	H	H	H	H

H: High, M: Medium, L: Low

Branch Name:	B.Sc. (IT/DS/CS)
Program Code:	ET110/ET111/ET112
Semester/Year:	Semester - VI/ Third Year
Subject Title:	Social media and Blog Writing
Subject Code:	16-AEC223-3C
Pre-requisite:	Basic Internet usage

Course Objective: To familiarize students with writing skills for the different kinds of media. To equip them with practical knowledge for the evolving writing ecology and empower them for employment.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
-	-	04	02	-	-	25	25	50

Subject Contents			
Sr. No	Topic	Total Hours	Weight (%)
1	The Basics of Writing and Types of Writing - The basics of writing mechanics – Grammar, vocabulary, phrases and clauses - How to write – construction of clear, simple and precise sentences. - Writing for the reader – Role of reader and broadening the Reader – Response theory. - Different kinds of writing – Fiction, Non-fiction (including historical writing, travel writing, memoirs), scientific writing, journalistic writing	8	15
2	Exploring the New Avenues for Writing - Differences between traditional print writing (Newspapers, magazines, books etc.) and writing in the age of the internet – need to adapt to change. - Different forms of media – Print, social media websites, blogs, online platforms etc. - Understanding writing for different media through examples.	10	25
3	Customizing Online Writing Based on the Online Platform: - Long forms of writing- language, writing style, content, vocabulary focus, title, introduction and conclusion – film review, blog posts, scientific writing, e –magazines- with a minimum of two examples each. - Shorter forms of writing – language, writing style, content, vocabulary, focus, caption – Twitter feeds/poems, fanfiction, instagram stories,	10	25

	facebook posts etc – with a minimum of two examples each. • Photo and Video writing – language, writing style, content, vocabulary, focus, caption, introduction and conclusion, synchronizing content – Video logging, photo blogging etc		
4	Journalistic and Ad Writing: • Comparing Print and online writing – for newspapers, magazines, journals. • Understanding the evolving dynamics of the adspace - including pop up ads, scrolls, flash ads- change in language, font, style and incorporating doodling with ad writing	8	20
5	Writing and Publishing: • Students must undergo hands-on –training from a recognized print/digital media. • Publish an article in a print/digital media.	8	15

List of Reference Books:

1. How Images think – Burnett 2004.
2. Online Journalism – Reporting, Writing and Editing for New Media – Richard Craig 2005 CENGAGE Learning.
3. Broadcast News Handbook – Writing, Reporting, Producing in a converging Media –C.A. Juggle,Forrest Carr and Suzanne Huffman McGraw-Hill, 2011
4. Writing Machines –Katherine Hayles 2002.
5. Writing For The Media ; Author, Sunny Thomas ; Publisher, Vision Books, 1997 ; ISBN, 8170942993, 9788170942993
6. The Language of New Media –Lev Manovich (MIT Press, 2001)
7. How to start Vlogging: A complete Beginner’s Guide –Derrick Hayes 2019
8. Twitter for success: Achieve writing success 25 words at a time –Angela Booth 2nd edition (22 December 2011);
9. Blogging for beginners: Learn how to start and maintain a successful blog the simple way –Terence Lawfield 2015.
10. Writing New Media: Theory and Applications for Expanding the Teaching of Composition. January 2004. Authors: Anne Frances Wysocki

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Comprehend how to write with clarity, purpose and precision	1 Remembering 2. Understanding 3 Applying
CLO2	Understand how to modify writing styles based on the media employed	2 Understanding 3 Applying
CLO3	Use these skills to pursue higher education in other allied fields	3 Applying 4 Analyze
CLO4	Could use the knowledge to take up freelance writing assignments/projects and other related employment.	3 Applying 4 Analyze 5 Evaluate

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO 1	PSO 2	PSO 3	PSO 4
CLO1	L	L			H											H
CLO2	M	M			H											H
CLO3	L	M			H											M
CLO4	M	M			H											M

H: High, M: Medium, L: Low