Semester- III

Digital Forensics			
Course Code	22SCR31	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:2	SEE Marks	50
Total Hours of Pedagogy	50	Total Marks	100
Credits	4	Exam Hours	03

Course Learning objectives:
- Discuss about Digital Forensics, Investigative Process Methodologies
- To choose an appropriate tool for the chosen problem.
- Explain the Malware and Automated Computer Attacks
- To explore various Processing Crimes, Online Fraud

Module-1

Introduction to Digital Forensics, Investigative Process Methodologies

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://doi.org/10.4324/9781315194820

Module-2

Computer Hackers and Hacking

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://doi.org/10.4324/9780429343223

Module-3

Malware and Automated Computer Attacks

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://doi.org/10.4324/9780429343223

Module-4

Education, Training, and Awareness, Laws, Standards, and Regulations

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://doi.org/10.4324/9781315194820

Module-5

Online Fraud

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://prezi.com/ebwye4gtrmyj/chapter-9-computer-forensics-analysis-validation

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- Three Unit Tests each of **20 Marks**
- Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
  to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOKS

1. Digital Forensics and Investigations, ByJason Sachowski,1st Edition, 2018, Boca Raton,Imprint CRC Press
2. Cybercrime and Digital Forensics, ByThomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar,2022, London Imprint Routledge.

REFERENCE BOOKS

1. The Basics of Digital Forensics, John Sammons, Elsevier 2012

2. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Fourth Edition, Course Technology

Web links and Video Lectures (e-Resources):

- extension://elhekieabhbkpmcefcoobjddigjcaadp/https://booksite.elsevier.com/samplechapters/9781597495868/Front_Matter.pdf
- [Guide to computer forensics and investigation 3rd or 4th edition by Amelia Philips, Bill Nelson and Christopher Steuart.](#)
- https://www.intaforensics.com/2012/01/20/understanding-the-computer-forensics-process/
- https://www.coursehero.com/file/p3ip151/Understanding-Data-Recovery-Workstations- and-Software-Investigations-are/
- study.com/academy/lesson/raid-acquisitions-in-digital-forensics-definition-process.html
- https://prezi.com/ebwye4gtrmyj/chapter-9-computer-forensics-analysis-validation/
- https://www.thebalancesmb.com/copyright-definition-2948254
- https://www.ques10.com/p/24610/explain-a-standard-procedure-for-network-forensics/?
- https://www.taylorfrancis.com/books/mono/10.4324/9781315194820/digital-forensics-investigations-jason-sachowski?context=ubx
- https://www.taylorfrancis.com/books/mono/10.4324/9780429343223/cybercrime-digital-forensics-thomas-holt-adam-bossler-kathryn-seigfried-spellar?refId=88a2a46a-c48a-42a9-be5b-2a24c4c0ed3b&context=ubx
- https://www.youtube.com/watch?v=s01A-yqOby8

Skill Development Activities Suggested

- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify the Crimes using Digital forensics	L1
CO2	Select the Proper forensic tool for identifying crimes	L1
CO3	Discus the use Digital forensic in education field	L2
CO4	Determine the online fraud and malware attacks	L3

Program Outcome of this course

Sl. No.	Description	POs	
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1	
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2	
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.	PO3	
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.	PO4	
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	PO5	
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 and business practices.	PO6	
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7	
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8	
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9	
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.	PO10	
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11	
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.	PO12	

Mapping of COS and Pos

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	X											
CO2		X										
CO3				X								
CO4			X									

ADVANCED CRYPTOGRAPHY				
Course Code	**22SCR321**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Apply the Basics of Encryption Techniques.
- Illustrate the Basic Concepts in Number Theory
- Define Public key encryption and Key Management and Distribution

Module-1

Classical Encryption Techniques, Symmetric Cipher Model, Cryptography, Cryptanalysis and BruteForce Attack, Substitution Techniques, Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Hill Cipher, Poly alphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the Feistel Cipher structure, the Feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm.

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation/https://youtu.be/C7vmouDOJYM

Module-2

Basic Concepts in Number Theory and Finite Fields: Divisibility and The Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Groups, Rings, and Fields , Finite Fields of the Form GF(p) ,Polynomial Arithmetic , Finite Fields of the Form GF(2n). Advanced Encryption Standard : Finite Field Arithmetic, AES Structure General Structure Detailed Structure, AES Transformation Functions Substitute Bytes Transformation Shift Rows Transformation Mix Columns Transformation AddRound Key Transformation ,AES Key Expansion Key Expansion Algorithm Rationale ,An AES Example Results Avalanche Effect ,AES Implementation Equivalent Inverse Cipher Implementation Aspects. Block Cipher Operation:Multiple Encryption and Triple des Double DES Triple DES with Two Keys Triple DES with Three Keys , Electronic Code Book Cipher Block Chaining Mode Cipher Feedback Mode , Output Feedback Mod

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Module-3

Public-Key Cryptography and RSA, The RSA algorithm, Other Public-Key Cryptosystems: DiffieHellman Key Exchange The Algorithm Key Exchange Protocols Man-in-the-Middle Attack ,Elgamal Cryptographic System , Elliptic Curve Arithmetic Abelian Groups Elliptic Curves over Real Numbers Elliptic Curves over Zp Elliptic Curves over GF(2m) ,Elliptic Curve Cryptography Analog of DiffieHellman Key Exchange Elliptic Curve Encryption/Decryption Security of Elliptic Curve Cryptography

Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Module-4

Key Management and Distribution: Symmetric Key Distribution Using Symmetric Encryption Symmetric Key Distribution Using Asymmetric Encryption Distribution of Public Keys X.509 Certificates Public-Key Infrastructure , User Authentication Remote User-Authentication Principles Remote User-Authentication

		Using Symmetric Encryption Kerberos Remote User Authentication Using Asymmetric Encryption Federated Identity Management Personal Identity Verification 484.
	Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

	Module-5	
	Transport-Level Security Web Security Considerations Secure Sockets Layer Transport Layer Security HTTPS Secure Shell (SSH) Wireless Security Wireless Network Threats Wireless Security Measures Mobile Device Security Security Threats Mobile Device Security Strategy Pretty Good Privacy Notation Operational Description S/MIME RFC 5322 Multipurpose Internet Mail Extensions S/MIME Functionality S/MIME Messages S/MIME Certificate Processing Enhanced Security Services	
	Teaching-Learning Process	Chalk and talk method / PowerPoint Presentation

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**

to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper will have ten full questions carrying equal marks.
3. Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOKS
1. Cryptography and Network Security Principles And Practice William Stallings, Pearson Education, Eigth Edition.

Reference Books:
1. A Course in Number Theory and Cryptology, Neal Koblitz ,Springer, 1987
2. Cryptography and Network Security ,Behrouz A Forouzan, Debdeep Mukhopadh yay ,McGrawHill ,3rd Edition, 2015

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=rA_ZmWPormM
- https://youtu.be/C7vmouDOJYM

Skill Development Activities Suggested
- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Memorize the OSI security architecture and classical encryption techniques.	L1
CO2	Classify the various block cipher and stream cipher models.	L2
CO3	Apply the principles of public key cryptosystems, hash functions and digital signature.	L3
CO4	Compare various Cryptographic Techniques	L2

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1			X				X					
CO2	X											
CO3					X							
CO4				X								

Semester- III

Operating System Security			
Course Code	22SCR322	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Describe the software Security management.
- Choose an appropriate models and multics security for operating system.
- Identify the complexity of communication to secure operating system
- Analyze the case study for building secure operating security.

Module-1

Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://www.youtube.com/watch?v=fs3COGpVk4A

Module-2

Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://www.youtube.com/watch?v=i_7ofp7fK_E

Module-3

Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://slideplayer.com/slide/3926904/

Module-4

Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5

Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weight age of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
- Three Unit Tests each of **20 Marks**
- Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
  to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:
TEXT BOOK
1. Operating system security Trent Jaeger Morgan & Claypool Publishers, Springer Nature Switzerland AG 2022 Reprint of original edition.

 REFERENCE BOOK
1. Guide to Operating system Security Michael Palmer Thomson.

Web links and Video Lectures (e-Resources):

- https://www.iisecurity.in/courses/operating-system-security-course.php
- https://www.youtube.com/watch?v=i_7ofp7fK_E
- https://www.iisecurity.in/courses/operating-system-security-course.php
- https://slideplayer.com/slide/3926904/

Skill Development Activities Suggested
- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify the various goals and fundamentals of protection system	L1
CO2	Compare and Pick out the right models and multics security	L2
CO3	Discover new multics and reliability of communication to secure operating system	L3
CO4	Identify and evaluate the case studies for building secure operating security.	L1

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	x											
CO2			x									
CO3				x								
CO4		x										

Threat Hunting			
Course Code	**22SCR323**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Describe about Threat Hunting and Its Goals.
- Choose an appropriate requirement for hunt.
- Identify the complexity of threat hunting.
- Analyze and evaluate the data analysis and aggregation techniques in hunting.

Module-1

Threat Hunting and Its Goals, What Threat Hunting Is, Why Threat Hunting Matters, Who Threat Hunting Is For: The SOCS, The Threat Hunting Process as a Research Process

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://www.youtube.com/watch?v=R5mnIvjQn-g

Module-2

Should You Hunt?, Data Requirements, When You're Not Ready: Data, Operational Requirements, When You're Not Ready: Operations, Personnel Requirements, When You're Not Ready: Personnel

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents:

Module-3

A Hunting Process, Long-Term Preparation, Triggers, Starting the Hunt, The Hunt Itself, Ending the Hunt, Output from the Hunt

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://slideplayer.com/slide/3926904/

Module-4

A Dictionary of Threat Hunting Techniques, Core Concepts, The Cyber Kill Chain, Ranking Versus Detection, Finite Cases, Basic Techniques, Searching and Cross-Source Correlation, Lookup, Stack Counting, Histograms and Barplots, Watchlist Refinement: Indicators and Signatures, Indicator Webwalk

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5

Techniques for Discovering Indicators, Configuration Tracking and Baselining, Honey, Situational Awareness of Your Network: Mapping, Blindspots, Endpoint Detection, Identifying Weird Port Behavior, Producer/Consumer Ratio and Services, Know Your Calendar, Watch Invocation Sequences, Be Aware of Physical Locations, Data Analysis and Aggregation Techniques, Approximate String Matching, LRU Cache Depth Analysis, Leaky Buckets, Machine Learning, Visualization Techniques, Trellising and Sparklines, Radial Plots, Heat Mapping and Space Filling Curves.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weight age of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**

    to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOK

1. Threat Hunting by Michael Collins Released May 2018 Publisher(s): O'Reilly Media, Inc. ISBN: 9781492028253

REFERENCE BOOK

1. The Foundations of Threat Hunting: Organize and design effective cyber threat hunts to meet business needs by Chad Maurice (Author), Jeremy Thompson (Author), William Copeland (Author), Anthony Particini (Foreword), Packt Publishing (June 17, 2022)

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=6_7wxMRlESU
- https://www.viavisolutions.com/en-us/ptv/threat-hunting
- https://www.youtube.com/watch?v=6UQc3BIxXDg&list=PLjWEV7pmvSa5UTZlsWp5wRnURNbeMS-fu
- https://www.activecountermeasures.com/hunt-training/
- https://www.youtube.com/watch?v=egPzEssrbH0
- https://www.youtube.com/watch?v=Xp_KRJDIKks&list=PLjWEV7pmvSa5UTZlsWp5wRnURNbeMS-fu&index=2

Skill Development Activities Suggested

- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify the various goals and fundamentals of Threat hunting	L1
CO2	Compare and pick out the right requirements for hunt	L2
CO3	Discover new process and techniques for threat hunting.	L3
CO4	Identify and evaluate the Data analysis and aggregation Techniques in hunting.	L1

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	x											
CO2			x									
CO3		x										
CO4			x									
CO5	x											

Incident Response			
Course Code	**22SCR324**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Create and deploy an incident response capability within your own organization
- Perform proper evidence acquisition and incident response charter
- To Analyze the evidence collected and determine the root cause of a security incident
- To Integrate digital forensic techniques and procedures into the overall incident response process

Module-1

Foundations of Incident Response and Digital Forensics, Understanding Incident Response, The incident response process, The role of digital forensics, The incident response framework, The incident response charter, CSIRT, CSIRT core team, Technical support personnel, Organizational support personnel, External resources, The incident response plan, Incident classification, The incident response playbook, Escalation procedures, Testing the incident response framework.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://www.infosecinstitute.com/skills/learning-paths/incident-response/?utm_source=resources&utm_medium=infosec%20network&utm_campaign=ir%20learning%20path&utm_content=main&utm_term=ir

Module-2

Managing Cyber Incidents, Engaging the incident response team, CSIRT models, Security Operations Center escalation, SOC and CSIRT combined, CSIRT fusion center, The war room, Communications, Staff rotation, Incorporating crisis communications, Internal communications, External communications, Public notification, Investigating incidents, Incorporating containment strategies, Getting back to normal – eradication and recovery, Eradication strategies, Recovery strategies.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://studentprivacy.ed.gov/training/cybersecurity-and-incident-response-webinar

Module-3

Evidence Acquisition, Collecting Network Evidence, An overview of network evidence, Preparation, Network diagram, Configuration, Firewalls and proxy logs, Firewalls, Web proxy server, NetFlow, Packet captures, Tcpdump, WinPcap and RawCap, Wireshark, Evidence collection, Acquiring Host-Based Evidence, Preparation, Order of Volatility, Evidence acquisition, Evidence collection procedures, Acquiring volatile memory, Local acquisition, FTK Imager, WinPmem, RAM Capturer, Remote acquisition, WinPmem, Virtual machines, Acquiring non-volatile evidence, CyLR.exe, Checking for encryption.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents: https://slideplayer.com/slide/3926904/

Module-4

		Analyzing Evidence, Analyzing Network Evidence, Network evidence overview, Analyzing firewall and proxy logs, DNS blacklists, SIEM tools, The Elastic Stack, Analyzing NetFlow, Analyzing packet captures, Command-line tools, Moloch, Wireshark, Analyzing System StorageForensic platforms, Autopsy, Installing Autopsy, Opening a case, Navigating Autopsy, Examining a case, Web artifacts, Email, Attached devices, Deleted files, Keyword searches, Timeline analysis, MFT analysis, Registry analysis.
	Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5
Malware Analysis for Incident Response, Malware classifications, Malware analysis overview, Static analysis, Dynamic analysis, Analyzing malware, Static analysis, ClamAV, PeStudio, REMnux, YARA, Dynamic analysis, Malware sandbox, Process Explorer, Process Spawn Control,Cuckoo Sandbox, Writing the Incident Report, Documentation overview, What to document, Types of documentation, Sources, Audience, Incident tracking, Fast Incident Response, Written reports, Executive summary, Incident report, Forensic report.

	Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://www.youtube.com/watch?v=oEU93FZR954

Assessment Details (both CIE and SEE)

The weight age of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
   to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TEXT BOOK
1. Digital Forensics and Incident Response - Second Edition by Gerard Johansen Released January 2020 Publisher(s): Packt Publishing ISBN: 9781838649005

REFERENCE BOOK
1. Applied Incident Response Paperback – 9 March 2020 by Steve Anson.

Web links and Video Lectures (e-Resources):

- https://www.infosecinstitute.com/skills/learning-paths/incident-response/?utm_source=resources&utm_medium=infosec%20network&utm_campaign=ir%20learning%20path&utm_content=main&utm_term=ir
- https://studentprivacy.ed.gov/training/cybersecurity-and-incident-response-webinar
- https://www.youtube.com/watch?v=oEU93FZR954

Skill Development Activities Suggested

- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify proper evidence acquisition and handling	L1
CO2	Create and deploy an incident response capability within your own organization	L2
CO3	Apply incident response practices to ransomware attacks	L3
CO4	Discover the incident reports that document the key findings of your analysis	L1

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	Po1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	x											
CO2			x									
CO3		x										
CO4				x								

SOFTWARE METRICS & QUALITY ASSURANCE				
Course Code	**22SCR325**		CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0		SEE Marks	50
Total Hours of Pedagogy	40		Total Marks	100
Credits	03		Exam Hours	03

Course Learning objectives:
- Learn about Software quality assurance and benchmarking measurements
- Describe software development best practices for minimizing vulnerabilities in programming code
- Conduct a security verification and assessment (static and dynamic) of a software application..
- To discover an availability of metrics and measures.

Module-1

What Is Software Quality: Quality: Popular Views, Quality Professional Views, Software Quality, Total Quality Management and Summary. Fundamentals Of Measurement Theory: Definition, Operational Definition, And Measurement, Level Of Measurement, Some Basic Measures, Reliability And Validity, Measurement Errors, Be Careful With Correlation, Criteria For Causality, Summary. Software Quality Metrics Overview: Product Quality Metrics, In Process Quality Metrics, Metrics for Software Maintenance, Examples For Metrics Programs, Collecting Software Engineering Data.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://www.youtube.com/watch?v=Jj7dLM8cLuE

Module-2

Applying The Seven Basic Quality Tools In Software Development: Ishikawa's Seven Basic Tools, Checklist, Pareo Diagram, Histogram, Run Charts, Scatter Diagram, Control Chart, Cause And Effect Diagram. The Rayleigh Model: Reliability Models, The Rayleigh Model Basic Assumptions, Implementation, Reliability And Predictive Validity.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://www.youtube.com/watch?v=Jj7dLM8cLuE

Module-3

Complexity Metrics And Models: Lines Of Code, Halstead's Software Science , Cyclomatic Complexity Syntactic Metrics, An Example Of Module Design Metrics In Practice .Metric And Lessons Learned For Object Oriented Projects: Object Oriented Concepts And Constructs, Design And Complexity Metrics, Productivity Metrics, Quality And Quality Management Metrics, Lessons Learned For object oriented Projects.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents https://www.youtube.com/watch?v=KqDlDubS-OU

Module-4

Availability Metrics: Definition And Measurement Of System Availability, Reliability Availability And Defect Rate, Collecting Customer Outage Data For Quality Improvement, In Process Metrics For Outage And Availability .Conducting Software Project Assessment :Audit Ad Assessment , Software Process Maturity Assessment And Software Project Assessment , Software Process Assessment, A Proponed Software Project Assessment Method.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-5
Dos And Don'ts Of Software Process Improvement :Measuring Process Maturity, Measuring Process Capability, Staged Versus Continuous Debating Religion, Measuring Levels Is Not Enough, Establishing The Alignment Principle , Take Time Getting Faster, Keep it Simple Or Face Decomplexification, Measuring The Value Of Process Improvement , Measuring Process Compliance , Celebrate The Journey Not Just The Destination. Using Function Point Metrics to Measure Software Process Improvement: Software Process Improvement Sequences, Process Improvement Economies, Measuring Process Improvement at Activity Levels.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
3. to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:
TEXT BOOKS

   1. Metrics and Models in Software Quality Engineering, Stephen H Khan Pearson 2nd edition 2013
   REFERENCE BOOKS
   1. Software quality and Testing Market,. S.A.Kelkar PHI Learing, Pvt, Ltd 2012
   2. Managing the Software Inc,. Watts S Humphrey Process Pearson Education 2008

Web links and Video Lectures (e-Resources):
- https://www.bmc.com/blogs/software-quality-metrics/
- https://www.youtube.com/watch?v=KqDlDubS-OU
- https://www.youtube.com/watch?v=Jj7dLM8cLuE

Skill Development Activities Suggested
- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

@#25102023

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify and apply various software metrics, which determines the quality level of software	L1
CO2	Compare and Pick out the right reliability model for evaluating the software	L2
CO3	Discover new metrics and reliability models for evaluating the quality level of the software based on the requirement	L3
CO4	Identify and evaluate the quality level of internal and external attributes of the software product	L1

Semester- III

Cyber Security and Cyber Law			
Course Code	**22SCR331**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- To analyze and evaluate the cyber security needs of an organization.
- To determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
- To design and develop security architecture for an organization.
- To design operational and strategic cyber security strategies and policies

Module-1

Cyber Security: Introduction in Cyber Security -Hackers - Attackers -Types of Attackers Examples – Data   Recovery.

Cyber law: Features of Cyber Law - Significance of Cyber Law - Advantages. Data Security - Meaning - Fundamentals of Data Security - Requirements of Data Security - Precautionary Measures.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-2

Tools and Methods Used in Cyber crime: Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS DDoS Attacks, SQL Injection, Buffer Over Flow, Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft)Cybercrimes and Cyber security: The Legal Perspectives Why do we need Cyber law: The Indian Context, The Indian IT Act, Digital Signature and the Indian IT Act, Amendments to the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3

Authentication and Firewalls - Authentication & Access Control: Identification - Authentication - Authentication by Passwords - Protecting Passwords - Access Control Structure - Evidences - Law of Evidence on Electronic Records,

Hackers & its Types - Cracking - Pornography - Software privacy - Data Recovery - File Modification & File access, Recover Internet Usage Data, Recover Swap Files/Temporary/Cache Files, and Introduction to Encase Forensic.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4

	Cyber security: Organizational Implications Cost of Cybercrimes and IPR Issues: Lesson for Organizations, Web Treats for Organizations: The Evils and Perils, Security and Privacy Implications from Cloud Computing, Social Media Marketing: Security Risk and Perils for Organization, Social Computing and the Associated Challenges for Organizations, Protecting People's Privacy in the Organization, Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy, Incident Handling: An Essential Component, Intellectual Property in the Cyberspace of Cyber security, Importance of Endpoint Security in Organizations. .
Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5	
Concept of Cyber law and Cyber Space: Introduction - Meaning and Features of Cyber law - Significance and Advantages of Cyber Law - Meaning of Cyber Space - Inclusive of Cyber Space - Facilitating Functions of Cyber Space - Major Issues in Cyber Space. Need for an Indian Cyber law: Plans of National Information Technology Policy (NITP) - Need for Protection of data - Transactions in Security - Electronic Banking.	
Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
   to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

TextBooks:

1. Jonathan Rosenoer , Cyber law: The Law of Internet, Springer Verlog, Paperback, 17 September 2011
2. John W Ritting House, William M.Hancock, Cyber Security Operations Handbook, Read Elsevier,2004

Reference Books:

1. Sunit Belapure and Nina Godbole. Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives. Wiley India Pvt Ltd. 2013.
2. Surya PrakashTripathi, Ritendra Goyal, Praveen Kumar Shukla. Introduction to information security and cyber laws. Dreamtech Press. 2015.
3. Cybersecurity Essentials

   Charles J. Brooks, Christopher Grow, Philip A. Craig Jr., Donald Short, ISBN: 978-1-119-36239-5 October 2018.

Web links and Video Lectures (e-Resources):
- https://www.udemy.com/course/cybersecurity-law-policy
- https://www.udemy.com/course/cybersecurity-law-policy
- https://academy.apnic.net/en/course/introduction-to-cybersecurity
- https://www.coursera.org/specializations/intro-cyber-security
- https://www.coursera.org/learn/cybersecurity-for-everyone
- https://www.classcentral.com/tag/cybercrime

Skill Development Activities Suggested
- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Define and identify the cyber security needs of an organization.	L1
CO2	Predict and analyze the software vulnerabilities and security solutions to reduce the risk of exploitation.	L2
CO3	Identify the cyber crime and modify security architecture for an organization.	L3
CO4	Survey operational and strategic cyber security strategies, crimes and policies	L4(Through Assignment)

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	X											
CO2				X								
CO3			X									
CO4	X											

Security Threats and Vulnerabilities			
Course Code	22SCR332	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Study the different threats identity processes.
- Study how to find the vulnerabilities in different application
- Able to write their code for vulnerable applications.
- Know the Use of Agent Technology for Intrusion Detection, CSIRTs

Module-1

Threats and Vulnerabilities to Information and Computing Infrastructures: Internal Security Threats, Physical Security Threats, Fixed-Line Telephone System Vulnerabilities, E-Mail Threats and Vulnerabilities, E-Commerce Vulnerabilities, Hacking Techniques in Wired Networks , Hacking Techniques in Wireless Networks, Computer Viruses and Worms, Trojan Horse Programs, Hoax Viruses and Virus Alerts, Hostile Java Applets, Spyware.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-2

Wireless Threats and Attacks: Wireless Threats and Attacks, WEP Security, Bluetooth Security, Cracking WEP, Denial of Service Attacks, Network Attacks, Fault Attacks, Side Channel Attacks.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-3

Prevention: Keeping the Hackers and Crackers at Bay RFID and Security ,Cryptographic Privacy Protection Techniques, Cryptographic Hardware Security Modules, Smart Card Security, Client-Side Security, Server-Side Security ,Protecting Web Sites, Database Security, Medical Records Security, Access Control: Principles and Solutions, Password Authentication ,Computer and Network Authentication, Antivirus Technology, Biometric Basics and Biometric Authentication.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-4

Detection and Recovery: Intrusion Detection Systems Basics, Host-Based Intrusion Detection Systems , Network-Based Intrusion Detection Systems, Use of Agent Technology for Intrusion Detection, Contingency Planning Management, Computer Security Incident Response Teams (CSIRTs) , Implementing a Security Awareness Program, Risk Assessment for Risk Management, Security Insurance and Best Practices. Auditing Information Systems Security, Evidence Collection and Analysis Tools, Information Leakage: Detection and Countermeasures.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content

Module-5

Host-level Threats and Vulnerabilities-Malware: Trojan Horse, Spyware, Worms/Viruses Eavesdropping, Job Faults. Infrastructure, Level Threats and Vulnerabilities: Network-Level Threats and Vulnerabilities, Grid Computing, Threats and Vulnerabilities, Storage Threats and Vulnerabilities.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content:

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
- Three Unit Tests each of **20 Marks**
- Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
  to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books
- *Algorithmic Cryptanalysis ,* Antoine Joux , Chapman & Hall/CRC Cryptography and Series, 2009
- *Number Theory for Computing .* Song Y Yang Second Edition, Springer Verlag, 2010

Reference Book:
- *Stabilization, Safety, and Security of Distributed Systems,* Rachid Guerraoui and Franck Petit,Springer, 2010
- *Distributed Systems Security:Issues, Processes and Solutions,* Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, Wiley publications, 2009.

Web links and Video Lectures (e-Resources):

https://www.youtube.com/watch?v=_mxufDbcK5A
https://www.youtube.com/watch?v=HvZ-05RssYw

Skill Development Activities Suggested
- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Able the exploit development process to identify threats.	L1
CO2	Search for vulnerabilities in closed-source applications	L2
CO3	Write their own exploits for vulnerable applications	L2
CO4	Develop the security architecture designed for any system, systems and cloud based services and mitigate it.	L2

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1		X										
CO2					X			X				X
CO3	X					X				X		
CO4			X									X

PRESERVING AND RECOVERING DIGITAL EVIDENCE			
Course Code	**22SCR333**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Define what is digital evidence, investigation technology
- Illustrate about forensic examination of Unix system
- Explain how to apply digital evidence o network and transport layer.

Module-1

Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content: https://youtu.be/iANBytZ26MI

Module-2

Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices

Teaching-Learning Process	Chalk and talk/PPT/case study/web content: https://youtu.be/KqaPMCMHH4g

Module-3

Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content: https://youtu.be/b-IvmXoO0bU

Module-4

Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content: https://youtu.be/SqvAaB3vK8U

Module-5

Handling the digital crime scene, digital evidence examination guidelines.

Teaching-Learning Process	Chalk and talk/PPT/case study/web content: https://youtu.be/Ihl7DPBAZ1g

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:
- Three Unit Tests each of **20 Marks**
- Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks**
   to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:
- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

---

uggested Learning Resources:

Text Books

1. *Digital Evidence and Computer Crime Forensic science, Computers and Internet,* Eoghan Casey, Elsevier Academic Press, Second Edition.

 Reference Books

1. *Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data*, Terrence V.Lillard, Glint P.Garrison, Craig A.Schiller, James Steele Syngress

2. *The Best Damn Cybercrime and Digital Forensics Book Period,*Jack Wiles , Anthony Reyes , Jesse Varsalone ,Syngress ,Edition 1st, 2007

Web links and Video Lectures (e-Resources):

- https://youtu.be/s01A-yqOby8

Skill Development Activities Suggested

- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Explain Digital evidence and computer crime and Laws(can be attained through assignment or CIE)	L3
CO2	Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems	L2
CO3	Illustrate the Networks basics for digital investigators	L2
CO4	Able to investigate computer intrusions and cyber stalking(can be attained through assignment or CIE)	L3
CO5	Explain the basic concepts how to handling the digital crime scene, digital evidence examination guidelines	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1								X				X
CO2		X			X					X		
CO3												X
CO4	X							X				
CO5			X			X						

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

FILE SYSTEM FORENSIC ANALYSIS

Course Code	22SCR334	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Explore Volume analysis.
- Illustrate the File system analysis.
- Define NTFS Concepts and Ext2 & Ext3.
- Illustrate the working of UFS2 & UFS2.

Module-1

Computer foundations: Data organizations, booting process, Hard disk technology, Hard disk data acquisition- introduction, reading the source data, writing the output data. Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions

Teaching-Learning Process	Chalk and Talk method /PPT

Module-2

File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Module-3

NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools. NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture. NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures.

Teaching-Learning Process	Chalk and Talk method /PPT

Module-4

Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture. Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes.

Teaching-Learning Process	Chalk and Talk method /PPT

Module-5

UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor.

Teaching-Learning Process	Chalk and Talk method /PPT/ Case study/Web contents

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

- *File System Forensic ,* Brian Carrier, Pearson Education ,2005
- *Digital Evidence and Computer Crime,* Casey Eoghan ,Academic Press, Edition 3, 2011.

 Reference Books

1. Introduction to Linux A Hands-On Guide, MachteltGarrels, Fultus CorporationPublisher, Third Edition 2010.
2. Computer Forensics, Warren and Jay Heiser, Kruse, Addison Wesley, 2002.
3. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004
4. Forensic Discovery, Dan Farmer & WietseVenema, Addison Wesley, 2005

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=2ESqwX3qb94

Skill Development Activities Suggested
The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Explain the foundation of digital investigation and methods of data analysis	L2
CO2	Illustrate the role of computer forensics in the business and private world	L2
CO3	Identify some of the current techniques and tools for forensic examinations	L2
CO4	Familiarize the NTFS file systems	L2

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1				X								X
CO2		X			x				X			
CO3	X											X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

BIOMETRIC SECURITY

Course Code	**22SCR335**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning objectives:
- Explain Physiological Biometric Technologies and Iris scan.
- Able to demostrate Handprint Biometrics, DNA Biometrics
- Define Multi biometrics and multi factor biometrics

Module-1
Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems.

Teaching-Learning Process	Teaching-Learning Process

Module-2
Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths,

Teaching-Learning Process	Teaching-Learning Process

Module-3
Behavioural Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.

Teaching-Learning Process	Teaching-Learning Process

Module-4
Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Teaching-Learning Process	Teaching-Learning Process

Module-5
Case studies on Physiological, Behavioural and multifactor biometrics in identification systems.

Teaching-Learning Process	Teaching-Learning Process

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **20 Marks**
2. Two assignments each of **20 Marks** or **one Skill Development Activity of 40 marks** to attain the COs and POs

The sum of three tests, two assignments/skill Development Activities, will be **scaled down to 50 marks**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

- The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
- The question paper will have ten full questions carrying equal marks.
- Each full question is for 20 marks. There will be two full questions (with a maximum of four sub-questions) from each module.
- Each full question will have a sub-question covering all the topics under a module.
- The students will have to answer five full questions, selecting one full question from each module

Suggested Learning Resources:

Text Books

1. Biometrics –Identity verification in a networked World, Samir Nanavathi, Michel Thieme, and Raj Nanavathi ,Wiley Eastern, 2002

Reference Books

1. *Biometrics for Network Security* ,John Berger Prentice Hall 2004

Implementing Biometric Security ,John Chirillo and Scott Blaul ,Wiley, Eastern Publications 2005

Web links and Video Lectures (e-Resources):

- https://www.digimat.in/nptel/courses/video/106104119/L01.html
- http://www.digimat.in/nptel/courses/video/106104119/L07.html

Skill Development Activities Suggested

- The students with the help of the course teacher can take up relevant technical –activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set)

At the end of the course the student will be able to :

Mapping of COS and POs

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1			X	X								X
CO2		X							X			
CO3			X									X
CO4									X			
CO5									X			X

Program Outcome of this course

Sl. No.	Description	POs
1	Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and computer science and business systems to the solution of complex engineering and societal problems.	PO1
2	Problem analysis: Identify, formulate, review research literature, and analyze complex engineering and business problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO2
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.	PO3
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.	PO4
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	PO5
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 and business practices.	PO6
7	Environment and sustainability: Understand the impact of the professional engineering solutions in business societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PO7
8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering and business practices.	PO8
9	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PO9
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.	PO10
11	Project management and finance: Demonstrate knowledge and understanding of the engineering, business 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.	PO11
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.	PO12

PROJECT WORK PHASE – 1			
Course Code	**22SCR34**	CIE Marks	100
Number of contact Hours/Week	6	SEE Marks	--
Credits	03	Exam Hours	--

Course objectives:
- Support independent learning.
- Guide to select and utilize adequate information from varied resources maintaining ethics.
- Guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- Develop interactive, communication, organisation, time management, and presentation skills.
- Impart flexibility and adaptability.
- Inspire independent and team working.
- Expand intellectual capacity, credibility, judgement, intuition.
- Adhere to punctuality, setting and meeting deadlines.
- Instil responsibilities to oneself and others.
- Train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Project Phase-1 Students in consultation with the guide/s shall carry out literature survey/ visit industries to finalize the topic of the Project. Subsequently, the students shall collect the material required for the selected project, prepare synopsis and narrate the methodology to carry out the project work.

Seminar: Each student, under the guidance of a Faculty, is required to
- Present the seminar on the selected project orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit two copies of the typed report with a list of references.

The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:
At the end of the course the student will be able to:
- Demonstrate a sound technical knowledge of their selected project topic.
- Undertake problem identification, formulation, and solution.
- Design engineering solutions to complex problems utilising a systems approach.
- Communicate with engineers and the community at large in written an oral forms.
- Demonstrate the knowledge, skills and attitudes of a professional engineer.

Continuous Internal Evaluation
CIE marks for the project report (50 marks), seminar (30 marks) and question and answer (20 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Societal Project			
Course Code	**22SCR35**	CIE Marks	100
Number of contact Hours/Week	6	SEE Marks	__
Credits	3	Exam Hours	03

Course objectives:
- Build creative solutions for development problems of current scenario in the Society.
- Utilize the skills developed in the curriculum to solve real life problems.
- Improve understanding and develop methodology for solving complex issues.

Some of the domains to choose for societal projects:
- Infrastructure
- Health Care
- Social security
- Security for women
- Transportation
- Business Continuity
- Remote working and Education
- Digital Finance
- Food Security
- Rural employment
- Water and land management
- Pollution
- Financial Independence
- Agricultural Finance
- Primary Health care
- Nutrition
- Child Care
- E-learning
- Distance parenting
- Mentorship Etc

Course outcomes:
At the end of the course the student will be able to:
- Building solution for real life societal problems.
- Improvement of their technical/curriculum skills

Continuous Internal Evaluation:
Identifying the real life problems and producing literature report : 20 marks
Data sampling and Cleaning :10 Marks
Establishing the right Objective: 10 Marks
Developing the solution : 20 Marks
Propagating the solution to the stake holders 1)Lectures 2)Social Meetings 3)Social media 4)Street plays 5)Advertisement Either of the 3(evidence of the work through geo tag photo) Certified by stake holders and authorized by concerned government authorities..   Include in societal project
Project Report: 20 marks. The basis for awarding the marks shall be the involvement of the student in the project and in the preparation of project report. To be awarded by the internal guide in consultation with external guide if any.
Project Presentation: 10 marks.

The Project Presentation marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Evalution: 10 marks.

The student shall be evaluated based on the ability in the Question and Answer session for 10 marks.

INTERNSHIP			
Course Code	**22SCR36**	CIE Marks	50
Number of contact Hours/Week	3	SEE Marks	50
Credits	06	Exam Hours	03

Course objectives:

Internship/Professional practice provide students the opportunity of hands-on experience that include personal training, time and stress management, interactive skills, presentations, budgeting, marketing, liability and risk management, paperwork, equipment ordering, maintenance, responding to emergencies etc. The objective are further,

To put theory into practice.

To expand thinking and broaden the knowledge and skills acquired through course work in the field. To relate to, interact with, and learn from current professionals in the field.

To gain a greater understanding of the duties and responsibilities of a professional. To understand and adhere to professional standards in the field.

To gain insight to professional communication including meetings, memos, reading, writing, public speaking, research, client interaction, input of ideas, and confidentiality.

To identify personal strengths and weaknesses.

To develop the initiative and motivation to be a self-starter and work independently.

Internship/Professional practice: Students under the guidance of internal guide/s and external guide shall take part in all the activities regularly to acquire as much knowledge as possible without causing any inconvenience at the place of internship.

Seminar: Each student, is required to

- Present the seminar on the internship orally and/or through power point slides.
- Answer the queries and involve in debate/discussion.
- Submit the report duly certified by the external guide.
- The participants shall take part in discussion to foster friendly and stimulating environment in which the students are motivated to reach high standards and become self-confident.

Course outcomes:

At the end of the course the student will be able to:

- Gain practical experience within industry in which the internship is done.
- Acquire knowledge of the industry in which the internship is done.
- Apply knowledge and skills learned to classroom work.
- Develop a greater understanding about career options while more clearly defining personal career goals.
- Experience the activities and functions of professionals.
- Develop and refine oral and written communication skills.
- Identify areas for future knowledge and skill development.
- Expand intellectual capacity, credibility, judgment, intuition.
- Acquire the knowledge of administration, marketing, finance and economics.

Continuous Internal Evaluation

CIE marks for the Internship/Professional practice report (30 marks), seminar (10 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session by the student) by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Semester End Examination

SEE marks for the internship report (20 marks), seminar (20 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.

PROJECT WORK PHASE -2			
Course Code	**22SCR41**	CIE Marks	100
Practical /Field work/Week	8	SEE Marks	100
Credits	18	Exam Hours	03

Course objectives:
- To support independent learning.
- To guide to select and utilize adequate information from varied resources maintaining ethics.
- To guide to organize the work in the appropriate manner and present information (acknowledging the sources) clearly.
- To develop interactive, communication, organization, time management, and presentation skills.
- To impart flexibility and adaptability.
- To inspire independent and team working.
- To expand intellectual capacity, credibility, judgement, intuition.
- To adhere to punctuality, setting and meeting deadlines.
- To instill responsibilities to oneself and others.
- To train students to present the topic of project work in a seminar without any fear, face audience confidently, enhance communication skill, involve in group discussion to present and exchange ideas.

Project Work Phase - II: Each student of the project batch shall involve in carrying out the project work jointly in constant consultation with internal guide, co-guide, and external guide and prepare the project report as per the norms avoiding plagiarism.
- Follow the Software Development life cycle
- Data Collection ,Planning
- Design the Test cases
- Validation and verification of attained results
- Significance of parameters w.r.t scientific quantified data.
- Publish the project work in reputed Journal.

Course outcomes:

At the end of the course the student will be able to:

- Present the project and be able to defend it.
- Make links across different areas of knowledge and to generate, develop and evaluate ideas and information so as to apply these skills to the project task.
- Habituated to critical thinking and use problem solving skills
- Communicate effectively and to present ideas clearly and coherently in both the written and oral forms.
- Work in a team to achieve common goal.
- Learn on their own, reflect on their learning and take appropriate actions to improve it.

Continuous Internal Evaluation:

Project Report: 20 marks. The basis for awarding the marks shall be the involvement of the student in the project and in the preparation of project report. To be awarded by the internal guide in consultation with external guide if any.

Project Presentation: 20 marks.

The Project Presentation marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Project Execution: 50 Marks

The Project Execution marks of the Project Work Phase -II shall be awarded by the committee constituted for the purpose by the Head of the Department. The committee shall consist of three faculty from the department with the senior most acting as the Chairperson.

Question and Answer: 10 marks.

The student shall be evaluated based on the ability in the Question and Answer session for 10 marks.

Semester End Examination

SEE marks for the project report (60 marks), seminar (30 marks) and question and answer session (10 marks) shall be awarded (based on the quality of report and presentation skill, participation in the question and answer session) by the examiners appointed by the University.