### ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION

Programme: B.Sc. Honours in Cyber Forensics (Major)

w.e.f. AY 2023-24

**COURSE STRUCTURE**

<table>
<thead>
<tr>
<th>Year</th>
<th>Semester</th>
<th>Course</th>
<th>Title of the Course</th>
<th>No. of Hrs /Week</th>
<th>No. of Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>1</td>
<td>Introduction to Classical Biology</td>
<td>3+2</td>
<td>4</td>
</tr>
<tr>
<td>I</td>
<td>I</td>
<td>2</td>
<td>Introduction to Applied Biology</td>
<td>3+2</td>
<td>4</td>
</tr>
<tr>
<td>I</td>
<td>II</td>
<td>3</td>
<td>Fundamentals of Computer</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>I</td>
<td>II</td>
<td>4</td>
<td>Networking &amp; Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>III</td>
<td>5</td>
<td>Cyber Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>III</td>
<td>6</td>
<td>Network Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>III</td>
<td>7</td>
<td>Cyber Law &amp; Intellectual Property Rights</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>III</td>
<td>8</td>
<td>Advanced Cyber Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>IV</td>
<td></td>
<td>9</td>
<td>Cyber Tools &amp; Techniques</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>IV</td>
<td></td>
<td>10</td>
<td>Digital Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>IV</td>
<td></td>
<td>11</td>
<td>Data Recovery Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Networking &amp; Security Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Law &amp; Intellectual Property Rights Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Advanced Cyber Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Tools &amp; Techniques Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Digital Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data Recovery Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Year</td>
<td>Semester</td>
<td>Course</td>
<td>Title of the Course</td>
<td>No. of Hrs /Week</td>
<td>No. of Credits</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>---------------------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>III</td>
<td>V</td>
<td>12</td>
<td>Mobile Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mobile Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13</td>
<td>Multimedia Forensics &amp; Speaker Identification</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia Forensics &amp; Speaker Identification Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14</td>
<td>Ethical Hacking (OR) Introduction to Programming</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Ethical Hacking (OR) Introduction to Programming Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>Cryptography &amp; Steganography (OR) Drone Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cryptography &amp; Steganography (OR) Drone Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VI</td>
<td></td>
<td></td>
<td>Semester Internship/Apprenticeship with 12 Credits</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>16</td>
<td>Operating Systems</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operating Systems Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17</td>
<td>Social Media Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Social Media Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18</td>
<td>Reverse Engineering &amp; Malware Analysis</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reverse Engineering &amp; Malware Analysis Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VII</td>
<td></td>
<td></td>
<td>SEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>19</td>
<td>Incident Response</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Incident Response Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
<td>Forensic Robotics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Forensic Robotics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21</td>
<td>Android &amp; IOS Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Android &amp; IOS Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22</td>
<td>Vulnerability Assessment &amp; Penetration Testing</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Vulnerability Assessment &amp; Penetration Testing Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Year</td>
<td>Semester</td>
<td>Course</td>
<td>Title of the Course</td>
<td>No. of Hrs /Week</td>
<td>No. of Credits</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>--------</td>
<td>-----------------------------------------</td>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td>Cloud Security &amp; Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cloud Security &amp; Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>SEC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td>Artificial Intelligence in Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Artificial Intelligence in Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td>Cyber Threats &amp; Solutions</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Threats &amp; Solutions Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
SEMESTER-I

COURSE 1: INTRODUCTION TO CLASSICAL BIOLOGY

Theory Credits: 4 5 hrs/week

Learning objectives

The student will be able to learn the diversity and classification of living organisms and understand their chemical, cytological, evolutionary and genetic principles.

Learning Outcomes

1. Learn the principles of classification and preservation of biodiversity
2. Understand the plant anatomical, physiological and reproductive processes.
3. Knowledge on animal classification, physiology, embryonic development and their economic importance.
4. Outline the cell components, cell processes like cell division, heredity and molecular processes.
5. Comprehend the chemical principles in shaping and driving the macromolecules and life processes.

Unit 1: Introduction to systematics, taxonomy and ecology.

1.2. Nomenclature – ICBN and ICZN, Binomial and trinomial nomenclature.
1.3. Ecology – Concept of ecosystem, Biodiversity and conservation.
1.4. Pollution and climate change.

Unit 2: Essentials of Botany.

2.1. The classification of plant kingdom.
2.2. Plant physiological processes (Photosynthesis, Respiration, Transpiration, phytohormones).
2.3. Structure of flower – Micro and macro sporogenesis, pollination, fertilization and structure of mono and dicot embryos.
2.4 Mushroom cultivation, floriculture and landscaping.

Unit 3: Essentials of Zoology

3.1. The classification of Kingdom Animalia and Chordata.
3.2 Animal Physiology – Basics of Organ Systems & their functions, Hormones and Disorders
3.3 Developmental Biology – Basic process of development (Gametogenesis, Fertilization, Cleavage and Organogenesis)
3.4 Economic Zoology – Sericulture, Apiculture, Aquaculture

Unit 4: Cell biology, Genetics and Evolution


4.3. Central Dogma of Molecular Biology.

4.4. Origin of life

Unit 5: Essentials of chemistry

5.1. Definition and scope of chemistry, applications of chemistry in daily life.

5.2. Branches of chemistry

5.3. Chemical bonds – ionic, covalent, noncovalent – Vander Waals, hydrophobic, hydrogen bonds.

5.4. Green chemistry

References


ACTIVITIES:

1. Make a display chart of life cycle of nonflowering plants.
2. Make a display chart of life cycle of flowering plants.
3. Study of stomata
4. Activity to prove that chlorophyll is essential for photosynthesis
5. Study of pollen grains.
6. Observation of pollen germination.
7. Ikebana.
8. Differentiate between edible and poisonous mushrooms.
9. Visit a nearby mushroom cultivation unit and know the economics of mushroom cultivation.
10. Draw the Ultrastructure of Prokaryotic and Eukaryotic Cell
11. Visit to Zoology Lab and observe different types of preservation of specimens
13. Visit to Zoo / Sericulture / Apiculture / Aquaculture unit
14. List out different hormonal, genetic and physiological disorders from the society
SEMESTER-I

COURSE 2: INTRODUCTION TO APPLIED BIOLOGY

Theory                                                        Credits: 4                                                        5 hrs/week

Learning objectives

The student will be able to learn the foundations and principles of microbiology, immunology, biochemistry, biotechnology, analytical tools, quantitative methods, and bioinformatics.

Learning Outcomes

1. Learn the history, ultrastructure, diversity and importance of microorganisms.
2. Understand the structure and functions of macromolecules.
3. Knowledge on biotechnology principles and its applications in food and medicine.
4. Outline the techniques, tools and their uses in diagnosis and therapy.
5. Demonstrate the bioinformatics and statistical tools in comprehending the complex biological data.

Unit 1: Essentials of Microbiology and Immunology

1.1. History and Major Milestones of Microbiology; Contributions of Edward Jenner, Louis Pasteur, Robert Koch and Joseph Lister.
1.2. Groups of Microorganisms – Structure and characteristics of Bacteria, Fungi, Archaea and Virus.
1.3. Applications of microorganisms in – Food, Agriculture, Environment, and Industry.
1.4. Immune system – Immunity, types of immunity, cells and organs of immune system.

Unit 2: Essentials of Biochemistry

2.2. Biomolecules II – Amino acids & Proteins.
2.3. Biomolecules III – Nucleic acids -DNA and RNA.
2.4. Basics of Metabolism – Anabolism and catabolism.

Unit 3: Essentials of Biotechnology

3.2. Environmental Biotechnology – Bioremediation and Biofuels, Biofertilizers and Biopesticides.
3.3. Genetic engineering – Gene manipulation using restriction enzymes and cloning vectors; Physical, chemical, and biological methods of gene transfer.
Unit 4: Analytical Tools and techniques in biology – Applications

4.1. Applications in forensics – PCR and DNA fingerprinting
4.2. Immunological techniques – Immunoblotting and ELISA.
4.3. Monoclonal antibodies – Applications in diagnosis and therapy.
4.4. Eugenics and Gene therapy

Unit 5: Biostatistics and Bioinformatics

5.1. Data collection and sampling. Measures of central tendency – Mean, Median, Mode.
5.3. Introduction, Genomics, Proteomics, types of Biological data, biological databases- NCBI EBI, Gen Bank; Protein 3D structures, Sequence alignment
5.4. Accessing Nucleic Acid and Protein databases, NCBI Genome Workbench

REFERENCES


ACTIVITIES

1. Identification of given organism as harmful or beneficial.
2. Observation of microorganisms from house dust under microscope.
3. Finding microorganism from pond water.
4. Visit to a microbiology industry or biotech company.
5. Visit to a waste water treatment plant.
6. Retrieving a DNA or protein sequence of a gene’
7. Performing a BLAST analysis for DNA and protein.
8. Problems on biostatistics.
9. Field trip and awareness programs on environmental pollution by different types of wastes and hazardous materials.
10. Demonstration on basic biotechnology lab equipment.
11. Preparation of 3D models of genetic engineering techniques.
12. Preparation of 3D models of transgenic plants and animals.

[NOTE: In the colleges where there is availability of faculty for microbiology and biotechnology, those chapters need to be handled by microbiology and biotechnology faculty. In other colleges, the above topics shall be dealt by Botany and Zoology faculty]
SEMESTER-II

COURSE 3: FUNDAMENTALS OF COMPUTER

<table>
<thead>
<tr>
<th>Theory</th>
<th>Credits: 3</th>
<th>3 hrs/week</th>
</tr>
</thead>
</table>

**Learning Objectives:** The students will be able to understand the fundamentals of computers & networks.

**Learning Outcomes:** On successful completion of the course the student will be able to:

1. Demonstrate computer and its components
2. Identify basic input and output devices
3. Learn types of printers and their configuration
4. Assembling and dissembling of computer
5. Identify preventive maintenance and troubleshooting process

**Unit I: Computer**
Basics, History, Characteristics, Applications, Types, Components; Input/ Output Devices, Storage Devices, Peripheral Devices; Central Processing Unit- Input/Output Unit, Arithmetic Logical Unit, Control Unit, Memory Unit. Operating System & Types; Desktop icons and Control panel objects; Files and Folders.

**Unit II: Networks**
Computer Networks- Introduction, Characteristics, Types and Topologies; Types of Network Devices; Internet, Internet Service Providers and their connection types.

**Unit III: Components of Computer & Printers**
Computer Hardware-Power Supplies, Motherboards, Internal PC Components, External Ports and Cables; Selection of Computer Components; Lab safety Procedures; Procedures to Protect Equipment and Data; Proper use of tools- Software Tools, Antistatic Wrist Strap. Printers-Installing and configuring printers, Configuring Options and Default Settings, Maintenance and Troubleshooting of Printers, Troubleshooting Printer Issues, Common Problems and Solution.

**Unit IV: Assembling and Dissembling of Computer**
Computer Assembling- Installation of Motherboard, Drives, Cables and Adapter Cards; Dissembling the Computer- Cables, RAM, Motherboard, Heatsink, Hard drives; BIOS Beep Codes and Setup, BIOS and UEFI Configuration, Upgradation and Configuration of a computer.

**Unit V: Preventive Maintenance and Troubleshooting**
Preventive Maintenance and the Troubleshooting Process, Benefits, Tasks; Inspection of Internal Components; Problem in the Computer: Identification, Root Cause; Plan of Action, Resolution of the problem and implementation.
Suggested Readings

1. Introduction to IT essentials Version 6 by CISCO
2. Fundamentals of Computers by Balagurusamy.
3. Fundamentals of computers by Rajaraman
4. Computer Fundamentals Course by Anita Goel
6. Fundamentals of Computers by Rajaraman V

Suggested Co-Curricular Activities

1. Making of hardware as project.
2. Workshop on Assembly and Disassembly of Computer.
SEMESTER-II

COURSE 3: FUNDAMENTALS OF COMPUTER

List of Experiments:

1. Identification of Input Devices
2. Identification of Output Devices
3. Creation of Folders.
4. Components of Computer and Printers
5. Dissemble of computer.
6. Computer Assembly
7. Creation of a word file and name as Network Devices.
8. Creation of a table and data entry.
9. Power Point presentation with 10 slides.
10. Power Point with various smart arts in it.
SEMESTER-II
COURSE 4: NETWORKING AND SECURITY

Theoryuros: 3 3 hrs/week

Learning Objectives: The students will be able to understand the fundamentals of computers & networks.

Learning Outcomes: On successful completion of the course the student will be able to:
1. Install various operating systems, and configuration
2. Demonstrate on various protocols
3. Troubleshoot laptops and mobile devices
4. Demonstrate network types
5. Understand OSI Model
6. Troubleshoot Computer Networks

UNIT I: Operating Systems
Operating System: Terms, Characteristics and Types; Windows Installation, Storage Device Setup Procedures, Custom Installation Options, Boot Sequence and Registry Files, Windows Configuration and Management, Administrative Tools, Secure System Configurations, Anti-virus installations and configuration.

UNIT II: Applied Computer Networking

UNIT III: Laptops and Mobile Devices

UNIT IV: Network Security

UNIT V: Troubleshooting Computer Networks
SUGGESTED READINGS

1. Introduction to IT essentials version 6 by CISCO
2. Network Forensics: Tracking Hackers Through Cyberspace by Sherri Davidoff
3. Network Forensics by Ric Messier
4. Learning Network Forensics by Samir Datt
5. Introduction to Security and Network Forensics by Willian J. Buchanan

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Creation of a model of various topologies.
2. Making a model of Internet.
3. Demonstration by making a model of various networking devices.
SEMESTER-II

COURSE 4: NETWORKING AND SECURITY

Practical Credits: 1  2 hrs/week

List of Experiments:

1. Installation of Windows
2. Comparison between various operating system.
3. Installation of Virtual Machine
4. Demonstration of components of Laptops and Mobile Devices
5. Troubleshooting Computer Network
6. Working with Nessus and NMAP tools
7. Network packet analysis through Wireshark
8. Experiments on Open Source SIEM tools
9. Experiments on assessing network vulnerabilities
10. Experiments on Detection of DoS/DDoS attacks
SEMMESTER-III

COURSE 5: CYBER SECURITY

Learning Objectives: The students will be able to understand the securing the virtual space.

Learning Outcomes: On successful completion of the course the student will be able to:
1. Understand the concept of Cyber security, issues and challenges associated with it.
2. Understand the cybercrimes, their nature, legal remedies and reporting the crimes through available platforms and procedures.
3. Appreciate various privacy and security concerns on online social media and understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of social media platforms.
4. Understand the basic concepts related to E-Commerce and digital payments. They will become familiar with various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds.

UNIT I: Cyber Space

UNIT II: Cyber Crimes

UNIT III: Cyber Security

UNIT IV: Social Media and Security
Social networks: Introduction and Overview, Opportunities, Pitfalls; Social media: Types, Platforms, Monitoring, Hashtag, Viral content, Marketing, Privacy, Challenges, Security issues, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices, Case studies.
UNIT V: E-Commerce and Digital Payments


SUGGESTED READINGS


SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visiting of Cyber Crime Stations
2. Visiting of Cyber Crimes Tracking Network System
3. Visiting of National Crime Records Bureau
SEMESTER-III

COURSE 5: CYBER SECURITY

Practical Credits: 1  2 hrs/week

List of Experiments:

1. VM Ware installations
2. Configuring security settings in Mobile Wallets and UPIs
3. Applying patches, fixing vulnerability (experiments)
4. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).
5. Setting and configuring two factor authentication in the Mobile phone.
7. Managing Application permissions in Mobile phone.
8. Installation and configuration of computer Anti-virus.
9. Installation and configuration of Computer Host Firewall.
10. Wi-Fi security management in computer and mobile.
11. Basic checklist, privacy and security settings for popular social media platforms.
12. Reporting and redressal mechanism for violations and misuse of social media platforms.
SEMESTER-III

COURSE 6: NETWORK FORENSICS

Theory                                                        Credit: 3

Learning Objectives: The students will be able to understand networks and how to investigate.

Learning Outcomes: After studying this course the students will know-

1. Overview of Wireless Network Forensics
2. Packet Analysis
3. Different Malware Analysis techniques and their behavior.
4. Ransomware Analysis

UNIT I: Network Architecture & Internet - 1

UNIT II: Network Architecture & Internet- 2

UNIT III: Packet Switching

UNIT IV: Network Traffic- Capturing & Analysis

UNIT V: Malware Analysis and Ransomware Analysis
SUGGESTED READINGS:
4. Social Media & Network Forensics, CDAC

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Preparation of models of switches and routers
2. Preparation of model of topologies.
SEMESTER-III

COURSE 6: NETWORK FORENSICS

Practical Credits: 1 2 hrs/week

Network Forensics Practical

1. Network capturing using Wireshark.
2. Malware detection using tools.
3. Extraction of media files from network miner.
4. Examination of the working of router.
5. Configuration of intrusion detection system through Snort (Linux)
6. Examination of the Internet (TCP/IP) protocol stack and the OSI model.
7. Packet tracing.
8. Troubleshooting the given network.
9. Demonstration of simple network configuration with a router that connects two local area network segment using cisco packet tracer.
10. Comparison of networking tools.
SEMESTER-III

COURSE 7: CYBER LAW & INTELLECTUAL PROPERTY RIGHTS

Learning Objectives: The students will be able to understand the legal norms of cyber world.

Learning Outcomes: After studying this course the students will know-
1. Overview of Indian Legal System
2. Information Technology Act, 2000 and its Amendments (till date)
3. Outline of Electronic Governance
4. Incident Response Team Development
5. Explain and Evaluate Emerging Legal and Ethical Issues in E-commerce

UNIT 1: Information Technology (IT) Act
Objectives of IT Act, Digital Signature & Electronic Signature, Authentication of electronic records (Section-3, IT ACT), legal recognition of electronic records and digital signature (Section-4 and 5, IT Act), Certifying Authorities and Controller, Offences as per IT Act (Section-65 to Section-78), Special provision in Indian Evidence Act regarding admissibility of electronic records (Section-65B of IEA, 1872). Features of the IT Act, 2000 as amended in 2008, Applicability & Non-applicability of IT Act, Importance of IT Act, Amendments to ITA, 2000.

UNIT 2: Government Initiation

UNIT 3: Indian Penal Code & Indian Evidence Act

UNIT 4: Intellectual Property Rights
Concept of IPR, IPR Infringements, Civil & Criminal Liabilities in IPR, IPR & Criminal Jurisprudence, Copyrights, Multimedia and Copyright issues, Software Piracy, Trademarks, Trademarks in Internet, Functions and types of Trademarks- Letter Mark, Symbol Mark, Brand, Label and Ticket, Color Combination, Numerals, Containers, Shape of goods, Packaging, Device; Copyright and Trademark cases Patents – Basics, Conditions of Patentability, Indian Patent Act, Infringement, Defenses.

UNIT 5: E- Governance & E- Contract
SUGGESTED READINGS:

a. The Information Technology Act, 2000 Bare Act with Short Notes, Universal Law Publishing Co., New Delhi
c. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi
g. Elias. M. Awad, ”Electronic Commerce”, Prentice-Hall of India Pvt Ltd.

SUGGESTED CO-CURRICULAR ACTIVITIES:

1. Court Visit
2. Cyber Cell Visit

SEMESTER-III

COURSE 7: CYBER LAW & INTELLECTUAL PROPERTY RIGHTS

<table>
<thead>
<tr>
<th>Practical</th>
<th>Credits: 1</th>
<th>2 hrs/week</th>
</tr>
</thead>
</table>

List of Experiments

1. 5 case studies on cyber terrorism.
2. 5 case studies on e-commerce frauds.
3. 5 case studies on credit card frauds.
4. Case study on hacking, phishing & vishing.
5. Research on various government websites for cyber awareness.
8. Comparative analysis on Indian laws and international laws for cybercrime.
9. Preparation of statistical data of last 2 years of cybercrimes.
10. Preparation statistical data of last 2 years for cybercrimes in various countries.
SEMESTER-III

COURSE 8: ADVANCED CYBER FORENSICS

| Theory | Credits: 3 | 3 hrs/week |

**Learning Objectives:** The students will be able to understand advancements in cyber forensics.

**Learning Outcomes:** After studying this course the students will know-
1. File System Analysis
2. Overview of Cryptography
3. Encryption and Decryption
4. Overview of Memory Forensics
5. Anti-forensic Techniques
6. Hypervisor Files and Formats
7. Forensic Analysis of a Virtual Machine
8. Overview of Cloud Forensics
9. Analysis of Cloud Applications

**UNIT I: Windows Forensics**


**UNIT II: Cryptography**

Cryptographic System: Definition and Classification, Secret Key, Cryptography, Cryptanalysis and Attacks, Encryption and their types, Encryption algorithms, brute force attack, Decryption and their types, HDD and Artifacts Encryption and Decryption Techniques.

**UNIT III: Memory Forensics**

History of Memory Forensics, x86/x64 architecture, Data structures, Volatility Framework & plugins Memory acquisition, File Formats – PE/ELF/Mach-O, Processes and process injection, Command execution and User activity, Networking, sockets, DNS and Internet history, shell bags, paged memory and advanced registry artifacts, Related tools-Bulk Extractor and YARA, Timelining memory, Recovering and tracking user activity, Recovering attacker activity from memory, Introduction to Anti-forensics, tools and techniques.

**UNIT IV: Virtual Machine Forensics**

Hypervisors: Types, Files and Formats. Virtual Machines: Descriptions, Use and implementation in Forensic Analysis, Use of VMware to establish working version of suspect’s machine, Networking and virtual networks within Virtual Machine, Forensic Analysis of a Virtual Machine (Imaging of a VM, Identification and Extraction of supporting VM files in the host system, VM Snapshots, Mounting Image, Searching for evidence)
UNIT V: Cloud Forensics

Introduction to Cloud Computing, Challenges faced by Law enforcement and government agencies, Cloud Storage Forensic Framework (Evidence, Source Identification, Collection of Evidence and preservation, Examination and analysis of collected data) Cloud Storage Forensic Analysis.
Dropbox analysis: Data remnants on user machines, Evidence source identification and analysis, Collection of evidence from cloud storage services, Examination and analysis of collected data.
Google Drive: Forensic analysis of Cloud storage and data remnants, Evidence, source identification and analysis - Collection of evidence from cloud storage services, Examination and analysis of collected data, Issues in cloud forensics.

SUGGESTED READINGS
1. Window Forensic Analysis (DVD Toolkit) by Harlan Carver
2. File System Forensic Analysis by Brain Carrier
3. Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey
5. Cryptography: An Introduction (3rd Edition) by Nigel Smart
6. Cryptography and Data Security by Dorothy Elizabeth Rob, ling Denning
7. The Art of Memory Forensics (Detecting Malware and Threats in Windows, Linux, andMac Memory) Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters

SUGGESTED CO-CURRICULAR ACTIVITIES
1. Visit to a cyber cell.
2. Preparation of model on statistical representation of various tools.
SEMESTER-III

COURSE 8: ADVANCED CYBER FORENSICS

List of Experiments

1. Creation of Forensic Image using FTK Imager/Encase Imager
2. Data Acquisition: - acquisition using: - USB Write Blocker + FTK Imager
3. Forensics Case Study: Solve the Case study (image file) provide in lab using Encase Investigator or Autopsy.
6. Recovering and inspecting deleted files.
7. Creating a backup using icloud.
8. Creating a backup using itunes.
9. Extractions of data from ibackup.
10. Recovery of data using bulk extracto
SEMINSTER-IV

COURSE 9: CYBER TOOLS & TECHNIQUES

Theory

Credits: 3

3 hrs/week

Learning Objectives: The students will be able to understand various tools and techniques used.

Learning Outcomes: After studying this course the students will know-

1. Digital Data Acquisition & Examination
2. Tools used in detection of Alteration in Biometrics
3. Tools & Techniques used in Biometric Authentication.
4. Image Manipulation & Video Alteration detection tools.
5. Cyber Crimes & Social Media Data Analysis.

UNIT I: Computer Artifacts

UNIT II: Fundamentals of Biometrics

UNIT III: Data Recovery
Introduction, Phases of Digital Forensics, Tools used for Imaging – FTK, cmd values. Introduction to Write-Blockers— Hardware & Software, Types of Data Extraction Tools – Hardware & Software, Comparative analysis of data & metadata, Analysis of Image metadata, EXIF metadata & different video codec forms with tools used for detection of altering.

UNIT IV: In-Depth Forensic Analysis
Forensic Analysis of OS Artifacts, Internet Artifacts, File System Artifacts, Registry Artifacts, Application Artifacts, Usage of Slack space, Report Writing, Mobile Forensic- Identification, Collection and Preservation of mobile evidence, multimedia evidence, social media analysis, Data retrieval, E-mail investigation, tracking and analysis from mobile phones, IP tracking, renamed file, ghosting, compressed files.
UNIT V: Forensic Tools & Techniques

SUGGESTED READINGS
1. Digital Forensics with Open Source Tools by C. Altheide & H. Carvey.
3. Biometrics for Network Security by Paul Reid
6. Lab Mobile Forensics by Rohit Tamma.
7. CYBER LAW-The Indian Perspective by Pawan Duggal.
8. 7 Years of Indian Cyber Laws by Rohas Nagpal.

CO-CURRICULAR ACTIVITIES
1. Visit cyber cell.
2. Visit IT organization
SEMESTER-IV

COURSE 9: CYBER TOOLS & TECHNIQUES

List of Experiments

1. Extracting the data from the digital device using Celebrite UFED.
2. Extracting the data from hard disk using Encase software.
3. Performing logical extraction in the given device.
4. Performing physical extraction using appropriate tool.
5. Network Scanning using Nmap & Zenmap
6. Network analysis using Wireshark
7. Creating a cellphone dump/data extraction with - MSAB-XRY / Oxygen Forensics / CellebriteUFED4PC
8. Creating Image file with hash values using FTK.
9. Image metadata & EXIF metadata Analysis
10. RAM Acquisition & Analysis
SEMESTER-IV

COURSE 10: DIGITAL FORENSICS

Theory Credits: 3 3 hrs/week

Learning Objectives: The students will be able to understand the importance of digital forensics.

Learning Outcomes: On successful completion of the course the student will be able to:
1. Understand the role of investigator and lab requirements in Digital Forensics.
2. Understand Data Acquisition methods, tools and storage formats of digital evidence.
3. Collect, Preserve and Seize various digital evidences.
4. Validate and test evidences using various methods.

UNIT I: Computer Forensics and Investigations

UNIT II: Data Acquisition
Storage Formats for Digital Evidence, Acquisition Methods, Contingency Planning for Image Acquisitions, Validating Data Acquisition, RAID Data Acquisition, Acquisition Tools, Remote Network Acquisition Tools.

UNIT III: Identifying, Processing Crime and Incident Scenes

UNIT IV: Validating and Testing Forensics
Forensic Analysis of Software and Validation: Data Analysis, Hiding techniques, Carving, Compression; Graphics file: Recognition, Location, Recovery, Live Memory Forensics (RAM)

UNIT V: Introduction to Email Investigation
E-mail Investigations, Role of E-mail in Investigations, Role of Client and Server in E-mail, E-mail Crimes and Violations, E-mail Servers, Special E-mail Forensics Tools.
SUGGESTED READINGS

1. Guide to computer forensics and investigation 3\textsuperscript{rd} or 4\textsuperscript{th} edition by Amelia Philips, Bill Nelson and Christopher Steuart.
2. https://www.intaforensics.com/2012/01/20/understanding-the-computer-forensics-process/

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visit to Cyber Cell.
2. Visit to Cyber Crime Scene.
SEMESTER-IV

COURSE 10: DIGITAL FORENSICS

Practical Credit: 1 2 hrs/week

List of experiments:

1. Disk Imaging (2 types)
2. FTK Imager
3. Cyber check suite and other forensic tools from CDAC
4. Forensic Imaging of Virtual Machines
5. Live Acquisition
6. Live Incident Response
7. Live Memory Forensics (Volatility framework)
8. Scalpel, Autopsy
9. Network Minor
10. Comparison of various software.
SEMESTER-IV
COURSE 11: DATA RECOVERY FORENSICS

Theory
Credits: 3
3 hrs/week

Learning Objectives: The students will be able to understand process to recover the data.

Learning Outcomes: After studying this course the students will know-
1. Overview of networks
2. To understand concept of data recovery and tools related to it.
3. To recover the data authentically.

UNIT-I Collection of Evidence

UNIT-II E-Mail Investigation

UNIT-III Cyber Forensic Investigation
Digital Investigations and Evidence: Digital crime scene investigation process, General Guidelines for Investigation, Data Analysis, Essential and Non-Essential Data, Hard Disk Technology (Hard disk Geometry and Internals), Hard disk data Acquisition: General Acquisition Procedure, Data Acquisition layers. Dead versus Live Acquisition, Blockers Digital Media Forensics.

UNIT-IV Data Recovery

UNIT-V Security Issues
SUGGESTED READINGS:
1. File System Forensic Analysis by Brian Carrier, Publisher: Addison-Wesley Professional
3. Cyber Crime by Dr. R C Mishra, Publisher: Authorspress
4. Forensic Science in Crime Investigation by Dr. Rukmani Krishnamurthy.
11. Firewalls and Internet Security: Repelling the Wily Hacker by Addison.
12. Law Relating to Computers Internet & E-Commerce by Nandan Kamath

SUGGESTED CO-CURRICULAR ACTIVITIES
1. Visit cyber cell.
2. Visit IT organization.
SEMESTER-IV

COURSE 11: DATA RECOVERY FORENSICS

Practical Credits: 1 2 hrs/week

List of Experiments

1. Network Analysis
2. Detail Analysis of E-mail, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-MailRecovery
3. Working on EnCase Software for various peripheral devices.
4. Imaging of disk using various tools.
5. Recovering the data from pen drives.
6. Recovering the data from hard drives.
7. Recovering the data from memory cards.
8. Comparative analysis of software
9. Recovering deleted files.
10. Creating a report of investigation.
SEMESTER-V

COURSE 12: MOBILE FORENSICS

Theory Credits: 3 3 hrs/week

Learning Objectives: The students will be able to understand the importance of mobile forensics.

Learning Outcomes: After studying this course the students will know-
1. Basics and important terminology of the mobile devices.
2. Different types of acquisition methods on various platforms.
3. Internal working structure of the various mobile platforms.
4. Data recovery techniques and Data extraction techniques on various mobile platforms.
5. Different forensic tools that are used for various mobile platforms.

UNIT I: Mobile Forensics – I

UNIT II: Mobile Forensics – II
Potential evidence stored on mobile phones, Rules of evidence (Admissible, Authentic, Complete, Reliable, and Believable). Good forensic practices- Securing, Preserving, Documenting the evidence. Windows OS based mobile Phone Forensics- Windows Phone OS, Data acquisition. BlackBerry Forensics- Data acquisition.

UNIT III: Android Forensics - I
The Android models- The Linux kernel layer, Libraries, Dalvik virtual machine, the application framework layer, the applications layer. Android security - Secure kernel, the permission models, Application sandbox, Secure inter process communication, Application signing. Android file hierarchy. Android file system- Viewing and analysis.

UNIT IV: Android Forensics–II

UNIT V: iOS Forensics
Internals of iOS Devices, iPhone models, iPhone hardware, iPad models, File system, The HFS Plus file system, Disk Layout, iPhone operating system, Data Acquisition via a custom ram disk, Acquisition via jail breaking, Data Acquisition from iOS backups, iTunes backup, iCloud backup.
SUGGESTED READINGS

2. Practical Mobile Forensic by Satish Bommisetti, Rohit Tamma and Heather Mahali kunder
7. https://link.springer.com/chapter/10.1007/978-3-642-39891-9_15

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visit to cyber cell regarding mobile phones as evidence.
2. Visit to cybercrime scene.
List of Experiments:

1. Installation of Android Studio
2. Working on Open-source android forensic tool kit (OSAF-TK)
3. Santoku Linux
4. Andriller and other tools
5. Extraction of mobile data using Oxygen forensic suit
6. Physical Extraction of Data from mobile device using UFED Touch
7. Analyzing data of android mobile using MOBILedit
10. Comparison of open-source software and closed source software.
SEMESTER-V

COURSE 13: MULTIMEDIA FORENSICS & SPEAKER IDENTIFICATION

Learning Objectives: The students will learn about multimedia and can identify the speaker.

Learning Outcomes: After studying this course the students will know-
1. Overview of Multimedia Forensics
2. Image Enhancement Techniques
3. Video Frame Analysis
4. DVR Examination
5. Voice Production Process
6. Automatic Speaker Identification System

UNIT I: Fundamentals of Multimedia

UNIT II: Multimedia Forensics

UNIT III: Image and Video Forensics

UNIT IV: Audio Forensics
Sound: Attributes (Tone, Intensity, Frequency, Wavelength, Pitch), Channels (One-Mic, Stage, Location, Video Mic), Effects (Amplitude, Delay, Time/pitch, Reverse, Invert), Types (Analog/Digital), Digitization (Sampling, Quantization, Encoding), Formats (Uncompressed, Lossy Compressed, Lossless), Acoustic Parameters, Fourier Analysis, Frequency and Time Domain Representation of Speech Signal, Fast Fourier Transform;
Digital Audio: Methods of tampering, Forensic authentication, Enhancement; Microphone Forensics, Software; Forensic Audio Analysis.

UNIT V: Speaker Identification
Speaker identification: Introduction, Need, Scope, Human Vocal Tract, Production & Description of Speech Sound, Speech Signal Processing and Pattern Recognition;
Forensic phonetics and phonetic transcription, Methods of speaker identification: auditory and spectrographic analysis, Spectrographic cues for Vowels and Consonants, Automatic Speaker Identification System, Collection of voice samples: methods and challenges.

**SUGGESTED READINGS**

1. Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T S Ho, Shujun Li
   3. Fundamentals of Speaker Recognition by Homayoon Beigi
   4. Fundamentals of Speaker Recognition Law Enforcement and Counter-Terrorism by Amy Neistein, Hemant A. Patil
   5. Forensic Comparison of Voice, Speech and Speakers by Jonas Lindh

**SUGGESTED CO-CURRICULAR ACTIVITIES**

1. Visit cyber cell
2. Preparation of model on voice structure.
SEMESTER-V

COURSE 13: MULTIMEDIA FORENSICS & SPEAKER IDENTIFICATION

Practical Credits: 1 2 hrs/week

List of Experiments:

1. Collection of multimedia samples
2. Physical examination of Audio recording media
3. Examination of questioned recorder
4. Photo microscopic examination in case of analogue exhibits / speech signals.
5. Comparisons of audio recordings in terms of their contents.
6. Physical examination of Camcorder/VCR/Mobile phones.
7. Segregation of voice using Audacity.
8. Image analysis.
10. Comparison of Praat software and Audacity Software.
SEMESTER-V
COURSE 14: ETHICAL HACKING

Theory Credits: 3 3 hrs/week

Learning Objectives: The students will be able to understand about ethical hacking.

Learning Outcomes: After studying this course the students will know-
1. Impacts of Hacking
2. Information Security Models
3. Information Security Program
4. Business Perspective
5. Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable, and Integration)

UNIT I: Ethical Hacking

UNIT II: Network Protection System and Hacking Web Servers
Routers, Firewall & Honeypots, IDS & IPS, Web Filtering, Vulnerability, Penetration Testing, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, E-mail Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.

UNIT III: Penetration Testing

UNIT IV: Programming for Security Professionals

UNIT V: Prevention of Hacking

SUGGESTED READINGS
1. Preventing Web Attacks with Apache by Ryan C. Barnett
3. HackNotes(tm) Web Security Pocket Suggestive readings by Mike Shema
5. Improving Web Application Security: Threats and Countermeasures by Microsoft Corporation
6. Hacking the Code: ASP.NET Web Application Security by Mark Burnett
9. Advances in digital forensics VI by Kam Pui chow, Sujeet Shenoi
10. Malware forensic by Cameron Malin
11. Windows registry forensic by Harlan Carvey,
12. Digital forensic for network internet and cloud computing clint garrison
List of Experiments

1. Firewalls intrusion Detection and Honeypots
2. Malware – Keylogger, Trojans, Keylogger countermeasures
3. Password guessing and Password Cracking.
5. Penetration Testing and justification of penetration testing through risk analysis
6. Windows Hacking – NT LAN Manager, Secure 1 password recovery
7. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.
8. Understanding DoS Attack Tools- Jolt2, Bubonic, Land and LaTierra, Targa, Nemesy Blast,

10. E-mail header and URL analysis.
SEMESTER-V

COURSE 14: INTRODUCTION TO PROGRAMMING

Learning Objectives: The students will learn about languages.

Learning Outcomes: After studying this course the students will know-
1. Introduction to C language
2. Introduction to Oops
3. Introduction to Java
4. Introduction to Python
5. Python programming

UNIT I: Programming
Programming Languages: Introduction, Description, Types, Concepts (Class, Object, Arrays, structures, Constructors, Copy Constructor, Destructors, Inheritance, Exception Handling).

UNIT II: C & C++
C++: Overview, Basics, Variables, Constants, Input/Output, Functions, Strings.

UNIT III: Java
Java: Introduction, History, Features, Class, Objects, Data Types, Variables, Constants, Java Vs C++; Java Polymorphism: Method over loading, Method Overriding, Super keyword, Final Keyword, Java Abstraction, Java Encapsulation, Multithreading.

UNIT IV: Python Programming- I
Python: Introduction, Use, Applications, Implementation, Merits, Demerits; Data Structures, Data Types, String; Modules: Function Parameters, Variable Arguments.

UNIT V: Python Programming-I
Mutability and Higher-Order Functions, Strings, Tuples, Lists and Dictionaries, Lists and Mutability, Functions as Objects, Testing, Debugging, Handling Exceptions and Assertions.

SUGGESTED READINGS
3. Python Essential SUGGESTED READINGS by David Beazley.
4. Java the complete SUGGESTED READINGS, 7th edition by Herbert Schild.

SUGGESTED CO-CURRICULAR ACTIVITIES
1. Poster presentation on various types of programs.
2. Debate session on programming.
List of Experiments:

1. Execution of Basic C programs.
2. Execution of basic Python programs containing OOPs concepts.
3. Execution of programs using Tuples, Lists and Dictionaries.
4. C++ program to find the sum of individual digits of a positive integer
5. C++ program to generate the first n terms of the sequence
6. C++ program to generate all the prime numbers between 1 and n, where n is a value supplied by the user
7. C++ program to find the factorial of a given integer
8. C++ program to find the GCD of two given integers
10. C++ program to implement call by value and call by Suggested Reading parameters passing.
SEMESTER-V

COURSE 15: CRYPTOGRAPHY AND STEGANOGRAPHY

Learning Objectives: The students will learn about cryptography and steganography.

Learning Outcomes: After studying this course the students will know:

1. Classification of Cryptographic System
2. Forensic importance of various Cryptographic Algorithms
3. Importance of Digital Watermarks
4. Steganography Techniques
5. Development & Analysis of Secret Message Techniques
6. Steganalysis Algorithms

UNIT I: Basics of Cryptography
Cryptography: Introduction, Concept (plain text and cipher text), Techniques (Substitution, Transposition, Encryption and Decryption), Symmetric and Asymmetric Key Cryptography, Key range and Key size, Types of Attacks.

UNIT II: Ciphers
Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.

UNIT III: Validation & Management
Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512); Message authentication codes: Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

UNIT IV – Digital Watermarking

UNIT V – Steganography & Steganalysis

**SUGGESTED READINGS**


**SUGGESTED CO-CURRICULAR ACTIVITIES**

Visit IT company for steganalysis.
SEMESTER-V

COURSE 15: CRYPTOGRAPHY AND STEGANOGRAPHY

Practical Credits: 1 2 hrs/week

List of Experiments:

1. Caesar Cipher algorithm for encryption and decryption messages.

2. Usage of one-time pad technique to encrypt and decrypt messages.

3. Least Significant Bit (LSB) Method: Use the LSB method to embed secret messages within an image or audio file.

4. Hiding secret messages within the white spaces or in-between words of a plain text message.

5. Image steganography- Hiding secret messages within an image.

6. Installation of Kali Linux or Parrot Security Operating System in Virtual Box

7. Steganalysis of digital images.

8. Comparative analysis of steganography tools.

9. Comparative analysis of cryptography tools.

10. Decryption of codes with various tools.
SEMMESTER-V

COURSE 15: DRONE FORENSICS

| Theory | Credits: 3 | 3 hrs/week |

**Learning Objectives:** The students will be able to understand about drone forensics.

**Learning Outcomes:** After studying this course the students will know-

1. UAVs in Forensic Examination
2. Classification of Drones.
3. Analysis of Data stored/hidden in Drones.
4. Tools required in Drone forensics domain.
5. Application, Threats & Anti-Forensic Techniques
6. Laws with respect to Drones in India

**UNIT I: Drone Forensics**
Unmanned Aerial Vehicle (UAV): Introduction, History, Technology, Criminal Use; Drones: Description, History, Classification, Parts of Drones & Storage Devices, Data Retrieval, Methodology for acquisition-Analysis, Detection methods of unidentified Drones. Drones - National Security, Threats, Smuggling, Usage of Drones- mapping and surveying of topographies, agriculture, security and surveillance, aerial photography and videography, navigation, infrastructure solutions for roads and highways including transportation management in high density urban zones, construction support, telecom services, LiDAR in mining, watershed management and monitoring emergency/ disaster situations, Kisan Drones.

**UNIT II: Drone Data Analysis**
Analysis of Flight history, Geo-location mapping, Unique-Id extraction, Image Data Analysis, Date & Time stamp Analysis, EXIF metadata Analysis, SSID Authentication, Registry Entries, File System Data Analysis, Analysis of footage recorded.

**UNIT III: Tools & Techniques**

**UNIT IV: Anti-Forensic Techniques**
Anti-Forensic Techniques: Artifact Wiping (Tools-Eraser & BC Wipe), Data Hiding (Relocation of Data, Altering File Extensions), Signature Analysis of Files, Steganography, Trial Obfuscation (Modification of Data, Timestamps altering), Attack on Computer Forensic Tools & Processes (DoS attacks).

**UNIT V: Legal Aspects**
Registration & Licensing of Drones in India, Restrictions in usage of Drones, Green, Yellow & Red Zones, Introduction of Laws related to UAVs in India- Drone Rules, 2021

**SUGGESTED READINGS**

1. The Big Book of Drones – Ralph DeFrangesco, Stephanie DeFrangesco (2022)
3. The Drone Rules, Gazette of India, Ministry of Civil Aviation (2021)

**SUGGESTED CO-CURRICULAR ACTIVITY**

Preparation of a model of drone.
SEMESTER-V

COURSE 15: DRONE FORENSICS

Practical Credits: 1 2 hrs/week

List of Experiments

1. Examination of the structure of drone.
2. Extraction the data from the memory of drone.
3. Keeping surveillance on particular area with the help of drone and study the data.
4. Capturing bird eye view photo from drone.
5. Recording the entire crime scene with the help of drone.
6. Analyzing the footage extracted from drone.
7. Comparison of footage extracted from drone and footage extracted from camera.
8. Case study on drone forensics.
10. Assembly of the drone.
SEMESTER-VII

COURSE 16: OPERATING SYSTEMS

Theory Credits: 3 3 hrs/week

Learning Objectives: The students will learn about cryptography and steganography.

Learning Outcomes: After studying this course the students will know-
1. Operating Systems overview
2. Operating Systems structure
3. Process Management
4. Concurrency & Synchronization
5. Deadlocks
6. Memory Management

UNIT 1: Fundamentals
Operating system: Introduction, Goals, Functions, Evolution (Mainframe, Multiprogram Batch System, Time Sharing, Desktop System, Multi-Processor, Distributed, Real Time, Hand held, Embedded), Types (Network OS, Mobile OS, Server OS, Client OS and Cloud OS), Future; Concept of Virtual Machine.

UNIT 2: Structure
System Calls: Introduction, Implementation, Types, API-System Call- OS Relationship.

UNIT 3: Process Management
Processes: Definition, Relationship, States, Transitions, Control Block, Context switching.
Threads: Concept of multithreads, Benefits, Types, Process Scheduling, Scheduling criteria, Scheduling algorithms.

UNIT 4: Basic Memory Management
Definition: Logical and Physical address map; Memory allocation: Contiguous Memory allocation, Fixed and variable partition, Internal and External fragmentation and Compaction; Paging: Principle of operation, Page allocation, Disadvantages; Virtual Memory - Basics.

UNIT 5: File Systems & Shell Scripting
Windows File System: FAT, NTFS, ExFAT; Linux: ext., ext2, ext3, ext4; Apple file system (APFS).
Introduction to Shell scripting, writing a script, shell commands, decision making, arithmetic operation, loop, conditional execution and executing a shell script in Linux environment.
**SUGGESTED READINGS**

2. Operating System Concepts by Abraham Silberschatz & Peter Galvin

**SUGGESTED CO-CURRICULAR ACTIVITIES**

1) Preparation of model on operating systems.
2) PowerPoint Presentation on “Types of Operating Systems”.

SEMESTER-VII

COURSE 16: OPERATING SYSTEMS

List of Experiments:
1. Installation of OS
2. Installation of Kali Linux
3. Basics of UNIX.
4. UNIX editors such as vi, ed, ex and EMACS.
5. Shell script to accept ‘n’ integers and count +ves, -ves and zeroes respectively.
7. Shell script to accept many characters and count individual vowels, digits, spaces, special characters and consonants.
8. Shell script to accept student name and marks in 3 subjects through command line arguments. Find the total marks and grade (depending on the total marks).
9. Menu driven shell script for the following a) Rename a file (check for the existence of the source file). b) Display the current working directory. c) List the users logged in.
10. Shell script to accept many filenames through command line. Do the following for each filename a) If it is an ordinary file, display its content and also check whether it has executed permission. b) If it is a directory, display the number of files in it. c) If the file/directory does not exist, display a message.
LEARNING OBJECTIVES: The students will learn about social media forensics.

LEARNING OUTCOMES: After studying this course the students will be able-
1) To understand the definition of social media and its basic features.
2) To explore the characteristics of social media.
3) To get an overview of basic kinds of social media.
4) To understand the working of a social media site and also its evolution and development since its inception.
5) To gain knowledge about the impact of social media on individuals as well as the broader society.

UNIT I: Social Media -I
Social Media: Introduction, Evolution and Development, Definition, Features (User Interface, Personalization, Information Sharing, Realtime Updates on News Feed Simple Web Forms, Search Functionality), Characteristics (Openness, Community, Connectedness, Involvement, Conversation)

UNIT II: Social Media - II

UNIT III: Social Footprint & Platforms
Social Footprint: Description, Identities across different social network, Identifying fraudulent entities in online social network, Tracking.
Social Media Platforms: WhatsApp, Instagram, Facebook, Tinder, Twitter, Telegram, Snapchat, Messenger, Gmail, Yahoo, WeChat etc.

UNIT IV: Social Media- Crimes
Social Media-Crimes: Definition, Types (Cyberbullying, Online Grooming, Online Threats, Cyberstalking, Hacking, Fraud, Buying illegal things, Vacation Robberies, Fake Online Friendship, Spam, Phishing, Hate crime, Abuse and Extremism via online social media, Fake News & content on social media.

UNIT V: Social Media Forensics
SUGGESTED READINGS:


3. Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics

4. Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.

5. Understanding Social Networks: Theories, Concepts by Charles Kadushin

6. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

SUGGESTED CO-CURRICULAR ACTIVITIES-

1) Case Study

2) Debate
SEMESTER-VII

COURSE 17: SOCIAL MEDIA FORENSICS

PracticalCredits: 1 2 hrs/week

List of Experiments:

1. Manually visit social media account pages and gather information.
2. Analyze the Facebook app.
3. Data recovery function testing for digital forensic tools.
4. Checking vulnerabilities in various social media applications.
5. Examination and analysis of directories of social media applications.
6. Examination of WhatsApp messages.
7. Examination of Facebook messages.
8. Detection of spam.
9. Data extraction using Bulk Extractor.
10. Scrapping of data from social media API
SEMESTER-VII

COURSE 18: REVERSE ENGINEERING AND MALWARE ANALYSIS

Learning Objectives: The students will learn reverse engineering and malware analysis.

Learning Outcomes: After studying this course the students will know-
1. Architecture of x86 & x64
2. Working with Assemblers
3. Binary Obfuscation Techniques
4. Malware and types.
5. Malware Analysis

UNIT I: Reverse Engineering -I
Introduction to x86 and x64 Architecture: Register Set and Data Types, Data Movement, Canonical Address, Function invocation.

UNIT II: Reverse Engineering -II

UNIT III: Malware Analysis
Malware: Introduction, Definition, Types (Virus, Worm, Trojan, Backdoor, Ransomware).

UNIT IV: Basic and Advanced Static Malware Analysis
Advanced Static Techniques: x86 Disassembly, Architecture, Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, Stack, Conditionals, Branching, Analyzing. Malicious Windows Programs: Windows API, Windows Registry, Networking APIs, Kernel vs User Mode, Native API.

UNIT V- Basic and Advanced Dynamic Malware Analysis

SUGGESTED READING:
2. Mastering Reverse Engineering, Reginald Wong
3. Practical Reverse Engineering by Bruce Dang, Alexandre Gazet, Elias Bachaalany
4. Reversing: Secrets of Reverse Engineering by Eldad Eilam
5. Implementing Reverse Engineering: The Real Practice of X86 Internals by Jitender Narula

SUGGESTED CO-CURRICULAR ACTIVITIES

Organize Events on following topics

1. Analyze and implement user needs and consider them during the selection, integration, and administration of computer-based systems.
2. Evaluate and analyze of computer networks, security policies, security controls and threats using a range of techniques.
SEMESTER-VII

COURSE 18: REVERSE ENGINEERING AND MALWARE ANALYSIS

<table>
<thead>
<tr>
<th>B.Sc.</th>
<th>Semester: VII</th>
<th>Credits: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course: 18</td>
<td>REVERSE ENGINEERING AND MALWARE ANALYSIS LAB</td>
<td>Hrs/Wk: 2</td>
</tr>
</tbody>
</table>

List of Experiments

1. Analysis of HTML script.
2. MS office macro analysis.
3. Analysis of PDF file samples.
4. Installation of tools- Flare VM
5. Installation of additional tools.
6. Dynamic Analysis of Malware Sample 1
7. Network Analysis of Malware Sample 1
8. Static Analysis of Malware Sample 2
9. Reverse Engineering Malware sample 3
SEMESTER-VII
COURSE 19: INCIDENT RESPONSE

Learning Objectives: The students will learn respond action against any incident.

Learning Outcomes: After studying this course the students will know-
1. Processing Crime and incident scenes
2. Details related to Incident Response and Handling Process
3. Knowing about Incident Response Team Development
4. Hands-On with various Incident Response Investigation tools
5. Various features of Security information and event management

UNIT 1: Cyber Crimes, Threats & Attacks
Cyber-crimes: Definition, Types; General crimes Vs cyber crimes; Electronic Evidence: Introduction, Types, Searching, Collection, Handling and Storage.
Internet crimes: Dark web, Tor, Deep web, Credit card and ATM frauds, White collar crime; Cyber Criminals versus Cybersecurity Specialists; Threats; Attack; Digital Foot printing & Social engineering, Information gathering Methodologies.

UNIT 2: Security Principle
Cybersecurity Cube: Three Dimensions; CIA Triad: Confidentiality (The Principle of Confidentiality, Protecting Data Privacy, Controlling Access-Laws and Liability Integrity)
Principle of Data Integrity, Need for Data Integrity Checks, Availability, The Principle of Availability, Ensuring Availability.

UNIT 3: Incident Response
Incident Response: Definitions, Need, Goals, Challenges; Incident Response Framework: Incident Response Charter, CSIRT, Testing Framework; Forensic Analysis; Investigation tools and Digital Incident Response Kit (for IR role); Malware Analysis for Incident Response; Leveraging Threat Intelligence.

UNIT 4: Incident Response Process

UNIT 5: Investigation
Evidence Acquisition: Collection of Network Evidence, Acquiring Host- Based Evidence, Forensic Imaging; Analyzing Evidence: Analysis of Network Evidence, System Memory, System Storage, Log Files; Report Writing; Tools.
SUGGESTED READINGS
1. Incident Response & Computer Forensics, Third Edition by Jason T. Luttgens and Matthew Pepe
2. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response, by Leighton Johnson
3. Ethical Hacking and Penetration Testing Guide by Baloch, R.
4. Hacking for Dummies by Beaver, K.

SUGGESTED CO-CURRICULAR ACTIVITY
Make model of NIST Incident Response Life cycle.
LIST OF EXPERIMENTS
1. Live Response Collection with cedarpelta tool.
2. Acquiring the data from Windows Operating system by Cyber Defense Institute Incident Response Collector.
3. Artifact collection from Windows & Linus OS by Fast IR Collector.
5. Collection of the forensic evidence with the help of IREC tool.
7. Calculate the MD5 Hash of the extracted VBA macro and make a copy.
8. Identify the mails through packet captures.
10. Create a report for incident response.
SEMESTER-VII

COURSE 20: FORENSIC ROBOTICS

Theory                                                        Credits: 3

Learning Objectives: The students will learn about robots and forensic significance of robots.

Learning Outcomes: After studying this course the students will know-
1. To comprehend how a robot's fundamental parts work.
2. To examine how various End of Effectors and Sensors are used.
3. To share information regarding Robot Kinematics and Programming
4. To understand economics and robot safety issues

Unit I: Robotics
Robot: Definition, Concept of Robotics (Degree of Freedom, Joints, Robot Coordinates, Reference Frames, Programming Modes), Classification, Components, Characteristics, Workplace, Languages, Application, Advantages, Disadvantages.

Unit II: Spatial Descriptions and Transformation

Unit III: Manipulator Forward Kinematics
Link description, link connection, Denavit – Hartenberg parameters, Manipulator Inverse Kinematics: Solvability, algebraic and geometric approaches, Degeneracy and Dexterity, Robotic Forensic services in India.

Unit IV: Jacobians
Velocities, Static Forces, and Manipulator Dynamics analysis: Velocity analysis, the linear and rotational velocity of rigid bodies, velocity propagation, Jacobians, velocity transformation and inverse velocity, force transformation and inverse force, examples Robot Controller Design: P, PI, PD, PID and AI control in Robotics, Robotic solutions for crimes.

Unit V: Robot Operating System (ROS) Forensics

SUGGESTED READINGS
1. Software engineering for experimental robotics by Davide Brugali.
3. Introduction to robotics: mechanics and control by Craig, J. J.
4. Robotics technology and flexible automation by Deb, S., & Deb, S.
5. Robotics for engineers by Yoram Koren.
6. Robotics: Control, sensing, vision and intelligence by Fu, K. S., González, R. C., Lee, C. S. G.,


SUGGESTED CO-CURRICULAR ACTIVITIES

1. Model of Robot.
2. PowerPoint presentation on components of Robots.
SEMESTER-VII

COURSE 20: FORENSIC ROBOTICS

Practical Credits: 1 2 hrs/week

List of Experiments

1. Collection of storage device from the various robots.
2. Extraction of data from the storage device.
3. Analysis of recovered data.
4. Report of the data extracted from the robots.
5. Parts of robots.
7. Statistical data of robotic investigation done nationally.
8. Comparison of statistical data.
SEMESTER-VIII

COURSE 21: ANDROID AND iOS FORENSICS

| Theory | Credits: 3 | 3 hrs/week |

**Learning Objectives:** The students will learn in depth about mobile operating systems.

**Learning Outcomes:** After studying this course the students will know-

1. Setting up the development environment.
2. Reversing and Auditing Android Apps.
4. iOS Application Security.
5. Various Android & iOS tools.

**UNIT 1: Android Devices**

**UNIT 2: Android Data Extraction Techniques**
Manual, Logical, Physical Data Extraction; Android Data Analysis and Recovery; Android App Analysis, Malware, Techniques to reverse engineer an android application; Android Malware.

**UNIT 3: iOS Devices**
iOS Architecture; iOS Security; Jailbreaking; Operating modes of iOS devices; password protection and potential bypass; Logical acquisition; File system acquisition.

**UNIT 4: Data Acquisition from iOS Backup**
iTune backup; Extracting unencrypted backups; handling encrypted backup files; working with iCloud backups.

**UNIT 5: iOS Data Analysis and Recovery**
Interpreting iOS time stamps; working with SQLite databases; Key artifacts; Recovering deleted SQLite records. Working with Cellebrite UFED Physical Analyzer, Magnet AXIOM, Belkasoft Evidence Center, Elcomsoft Phone Viewer.

**SUGGESTED READINGS**

1. Lab Mobile Forensic by Satish Bommisetty, Rohit Tamma and Heather Mahalikunder Packet Publishing
SUGGESTED CO- CURRICULAR ACTIVITIES

1. Preparation of model Mobile phones.
2. Awareness program on mobile phone crimes.
LIST OF EXPERIMENTS

1. Mobile Forensics Investigation using Cellebrite UFED
2. Forensic Investigation of Any Mobile Phone with MOBILedit Forensic.
3. Android Mobile Device Forensics with Mobile Phone Examiner Plus.
4. Retrieve Saved Password from RAW Evidence Image
5. Create a Forensic Image of Android Phone using Magnet Acquire
6. Forensics Investigation of Android Phone using Andriller
7. Logical Forensics of an Android Device using AFLogical
8. SANTOKU Linux- Overview of Mobile Forensics Operating System
SEMESTER-VIII

COURSE 22: VULNERABILITY ASSESSMENT OF APPLICATION SECURITY

| Theory | Credits: 3 | 3 hrs/week |

Learning Objectives: The students will learn vulnerability assessment.

Learning Outcomes: After studying this course the students will know-

1. Proxies and non-proxy-aware clients
2. Setting up Vulnerable web applications
3. Identifying XSS, XML, SSTI, SSRF, and CSRF vulnerabilities
4. Executing an out-of-band command injection
5. Exploiting crypto vulnerabilities
6. Discovering Blind SQL injection

UNIT I: Burp Suite Configuration
Burp Suite and its features, Android and iOS setting - Burp Suite, Setting up proxy listeners, working with non-proxy-aware clients, creating target scopes in Burp Suite, Working with target, Browser add-ons and proxy setting management, Setting system-wide proxy for non-proxy-aware clients, Bug bounty vs client-initiated pentest, Types and features, Crawling, Auditor/Scanner, Insertion points. Stages of an application pentest.

UNIT II: Application Penetration Test & Identification of Vulnerabilities
Setup of vulnerable web applications, Reconnaissance and file discovery: Using Burp for content and file discovery. Testing for authentication via Burp, SQL injection flaws detection, Detecting OS command injection, Detecting XSS vulnerabilities, Detecting XML-related issues such as XXE, Detecting SSTI, Detecting SSRF, Detecting CSRF, Detecting Insecure Direct Object References, detecting security misconfigurations, detecting insecure deserialization, Detecting OAuth-related issues, Detecting broken authentication.

UNIT III: Detection and Exploitation of Vulnerabilities - 1
Data exfiltration via a blind Boolean-based SQL injection, Executing OS commands using an SQL injection, executing an out-of-band command injection, stealing session credentials using XSS, taking control of the user's browser using XSS, extracting server files using XXE vulnerabilities, Performing out-of-data extraction using XXE and Burp Suite collaborator, Exploiting SSTI vulnerabilities to execute server commands.

UNIT IV: Exploitation of Vulnerabilities Using Burp Suite - 2
Using SSRF/XSPA to perform internal port scans. Using SSRF/XSPA to extract data from internal machines, extracting data using Insecure Direct Object SUGGESTED READINGS(IDOR) Flaws. Exploiting security misconfigurations, Directory listings, Default credentials, Untrusted HTTP methods. Using insecure deserialization to execute OS commands, exploiting crypto vulnerabilities, Brute forcing HTTP basic authentication, Brute forcing forms, Bypassing file upload restrictions.
UNIT V: Burp Suite Extensions and Breaking the Authentication
Setting up the development environment, writing a Burp Suite extension: Burp Suite's API, Modifying the user-agent using an extension. Extension execution, performing information gathering, Port scanning, Discovery of Authentication method. Exploitation and Exfiltration of Data from a Large Shipping Corporation: Discovery of Blind SQL injection: Automatic scan, SQL Map detection, Intruder detection.

SUGGESTED READING

2. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more by Gus Khawaja

SUGGESTED CO-CURRICULAR ACTIVITIES

Organization of events on following topics

1. Basics of Infra Security (Data Encryption, Ransomware etc.)
2. Tools and techniques for VAPT (Network, Mobile and WEB)
3. Security appliances (Firewall, Proxy, Web proxy, IPS)
4. Email Security and data calcification.
LIST OF EXPERIMENTS

1. Detecting STI
2. Setting up Android with Burp suit.
3. Setting up iOS with Burp suit.
4. Execution of OS commands using an SQL injection.
5. Identifying the vulnerability.
6. Evaluating the security performance of third-party solutions
7. Performing vulnerability assessment
8. Detecting and prioritizing network threats
9. Analyzing networking devices for compromised passwords
10. Reviewing the system’s strength against common attacks
SEMMER-VIII

COURSE 23: CLOUD SECURITY AND FORENSICS

Theory  |  Credits: 3  |  3 hrs/week

**Learning Objectives:** The students will learn securing the cloud storage.

**Learning Outcomes:** After studying this course the students will know-
2. Various models in cloud computing.
3. Access management
5. Privacy in cloud computing & IoT

**UNIT 1: Cloud Computing**

**UNIT 2: Cloud Identity and Access Management.**

**UNIT 3: Cloud Security**

**UNIT 4: Cloud Forensics**

**UNIT 5: Privacy in Cloud Computing and IoT**

**SUGGESTED READINGS**
1. Cloud Forensics by Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie
2. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems by Vijay Prakash, Alex Williams, Lalit Garg, Claudio Savaglio and Seema Bawa. (Research Paper)
3. Cloud Storage Forensics by Darren Quick, Ben Martini
4. Cybercrime and cloud Forensics: Applications for Investigations Processes Keyun Ruan
SEMESTER-VIII

COURSE 23: CLOUD SECURITY AND FORENSICS

Practical Credits: 1 2 hrs/week

List of Experiments

1. Collection of data remotely from the guest OS layer of cloud using Encase Tool.
2. Collection of data remotely from the guest OS layer of cloud using FTK.
3. Open stack cloud computing platform to acquire Api’s logs, Virtual disk and guest firewall logs using FORST Tool.
5. Collecting data remotely from the guest OS layer of cloud using open-source Tool.
6. Collecting data remotely from the guest OS layer of cloud using proprietary Tool.
7. Comparison of data collected from open source and closed tool.
8. Analysis of data of various types of tools.
### SEMESTER-VIII

#### COURSE 24: ARTIFICIAL INTELLIGENCE IN FORENSICS

<table>
<thead>
<tr>
<th>Theory</th>
<th>Credits: 3</th>
<th>3 hrs/week</th>
</tr>
</thead>
</table>

**Learning Objectives:** The students will learn the importance of artificial intelligence in forensics.

**Learning Outcomes:** After studying this course the students will know-
1. To understand concept of Artificial Intelligence, Machine Learning and Deep Learning
2. To learn various Machine Learning and Deep Learning techniques
3. To create models to understand applications of AI.

**UNIT-I Artificial Intelligence (AI)**
Introduction, History, Components, Foundation, Sub-areas, Application, Current Trends, Future; Intelligent Systems: Introduction, Categorization; Development of Artificial Languages.
Intelligent Agents: Rational Agents, Mapping from Sequences to Actions, Properties of Environments, Structure of Intelligent Agents, Types of Agents: Simple Reflex Agents, Goal Based Agents, Utility Based Agents.

**UNIT-II Machine Learning (ML) & Python**

**UNIT-III Neural Networks**
Biological Brain; Artificial Neural Network (ANN): Introduction, Applications of ANN & Deep Learning; Recurrent Neural Networks (RNN): RNN Architecture, Applications, Building & Fitting RNN Models, Evaluation of Model Performance; Long Short-Term Memory Networks (LSTM): LSTM Network Architecture, Concept, Building LSTMs.

**UNIT-IV Computer Vision**
Introduction, Object Detection and Image Segmentation, Detecting and Recognizing Faces, Tracking Objects, Pattern Recognition; Natural Language Processing (NLP): Introduction, Language as Data, Building Custom Corpus, Text Vectorization & Transformation, Classification for Text Analysis, Clustering for text Similarity, Context Aware Text Analysis, Text Visualization.
UNIT-V Machine Learning in Cyber Security
Malware Detection & Classification, Anomaly Detection, Pen Testing using ML, Social Engineering, ML based Intrusion Detection.

SUGGESTED READINGS

1. Mathematics for Machine Learning 1st Edition by Marc Peter Deisenroth
5. Deep Learning with Keras: Implementing deep learning models and neural networks with the power of Python by Antonio Gulli, Sujit Pal
7. Learning OpenCV 4 Computer Vision with Python 3: Get to grips with tools, techniques, and algorithms for computer vision and machine learning, 3rd Edition by Joseph Howse and Joe Minichino
SEMESTER-VIII

COURSE 24: ARTIFICIAL INTELLIGENCE IN FORENSICS

Practical Credits: 1 2 hrs/week

List of experiments:
1. Image analysis using a tool
2. Using HIDS, analyze the malware.
3. Program to conduct game search.
4. Program to conduct uniformed and informed search.
5. Install anaconda python.
6. Use anaconda jupyter notebook and analyze it.
7. Install power BI Example and get the data
8. Perform plotting of data and check the filters of Power BI Example.
9. Customize Power BI.
10. Compare R vs Python.
Learning Objectives: The students will learn about threats and solutions.
Learning Outcomes: After studying this course the students will know how -
1. To identify malware kinds using analysis techniques
2. To learn fundamental and sophisticated malware analysis methods
3. To hone the methods for analyzing malware on Android for use in Lab applications.

UNIT I: Malware Analysis

UNIT II: Analysis and Detection of Malware
Malware Detection Tools: Solar winds, Security Event Manager, logRhythm, NextGen, SIEM Platform, Splunk enterprise security, Crowdstrike Falcon, McAfee Enterprise security manager, Micro Focus ArcSight ESM; SIM (Security Information Management), SEM (Security Event Management) and SIEM (SIM (Security Information & Event Management).

UNIT III: Analysis of Threats in Documents

UNIT IV: Common Vulnerabilities & Exposures (CVE)
Definition, Scope, Goals, Determination, Merits, Limitations; Difference between vulnerability & exposures, CVE Numbering Authorities (CNA), CVE identifiers, CVSS (Common Vulnerability Scoring System).

UNIT V: Data Collection
Volatile Data: Collection, Preservation, identifying users logged into the system; Non-Volatile Data: Collection, Inspect Prefetch files, Examine the file system, Remote registry analysis, Web browsing activities, Cookies files.

SUGGESTED READINGS
2. Computer viruses: from theory to applications by Filiol, Eric.
5. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware by Monnappa K A.
10. Computer Viruses and Malware by ErciFiliol.
LIST OF EXPERIMENTS

1. Study of different types of vulnerabilities for hacking a websites/ web application.
2. Setting up a Protected Malware Analysis Environment.
3. Identifying Covert Malware and working with Santoku.
4. Malware analysis using ML.
5. Using HIDS, analyze the malware.
6. Analysis of malware using NIPS.
7. Usage of firewall for specific website
8. Performing patch management.
9. Sniffing & their tools.
10. Physical security through windows backdoor