ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION

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

w.e.f. AY 2023-24

COURSE STRUCTURE

Year	Semester	Course	Title of the Course	No. of Hrs /Week	No. of Credits
I	I	1	Introduction to Classical Biology	3+2	4
		2	Introduction to Applied Biology	3+2	4
	II	3	Fundamentals of Computer	3	3
			Fundamentals of Computer Practical Course	2	1
		4	Networking & Security	3	3
			Networking & Security Practical Course	2	1
II	III	5	Cyber Security	3	3
			Cyber Security Practical Course	2	1
		6	Network Forensics	3	3
			Network Forensics Practical Course	2	1
		7	Cyber Law & Intellectual Property Rights	3	3
			Cyber Law & Intellectual Property Rights Practical Course	2	1
		8	Advanced Cyber Forensics	3	3
			Advanced Cyber Forensics Practical Course	2	1
	IV	9	Cyber Tools & Techniques	3	3
			Cyber Tools & Techniques Practical Course	2	1
		10	Digital Forensics	3	3
			Digital Forensics Practical Course	2	1
		11	Data Recovery Forensics	3	3
			Data Recovery Forensics Practical Course	2	1

Year	Semester	Course	Title of the Course	No. of Hrs /Week	No. of Credits
III	V	12	Mobile Forensics	3	3
			Mobile Forensics Practical Course	2	1
		13	Multimedia Forensics & Speaker Identification	3	3
			Multimedia Forensics & Speaker Identification Practical Course	2	1
		14	Ethical Hacking (OR) Introduction to Programming	3	3
			Ethical Hacking (OR) Introduction to Programming Practical Course	2	1
		15	Cryptography & Steganography (OR) Drone Forensics	3	3
			Cryptography & Steganography (OR) Drone Forensics Practical Course	2	1
	VI	Semester Internship/Apprenticeship with 12 Credits			
IV	VII	16	Operating Systems	3	3
			Operating Systems Practical Course	2	1
		17	Social Media Forensics	3	3
			Social Media Forensics Practical Course	2	1
		18	Reverse Engineering & Malware Analysis	3	3
			Reverse Engineering & Malware Analysis Practical Course	2	1
		SEC			
		19	Incident Response	3	3
			Incident Response Practical Course	2	1
		20	Forensic Robotics	3	3
			Forensic Robotics Practical Course	2	1
	VIII	21	Android & IOS Forensics	3	3
			Android & IOS Forensics Practical Course	2	1
		22	Vulnerability Assessment & Penetration Testing	3	3
			Vulnerability Assessment & Penetration Testing Practical Course	2	1

Year	Semester	Course	Title of the Course	No. of Hrs /Week	No. of Credits
		23	Cloud Security & Forensics	3	3
			Cloud Security & Forensics Practical Course	2	1
		SEC			
		24	Artificial Intelligence in Forensics	3	3
			Artificial Intelligence in Forensics Practical Course	2	1
		25	Cyber Threats & Solutions	3	3
			Cyber Threats & Solutions Practical Course	2	1

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 theireconomic 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.

1.1. Systematics – Definition and concept, Taxonomy – Definition and hierarchy.

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 structureof 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

4.1. Cell theory, Ultrastructure of prokaryotic and eukaryotic cell, cell cycle.

4.2. Chromosomes and heredity – Structure of chromosomes, concept of gene.

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

1. Sharma O.P., 1993. Plant taxonomy. 2nd Edition. McGraw Hill publishers.
2. Pandey B.P., 2001. The textbook of botany Angiosperms. 4th edition. S. Chand publishers,New Delhi, India.
3. Jordan E.L., Verma P.S., 2018. Chordate Zoology. S. Chand publishers, New Delhi, India.
4. Rastogi, S.C., 2019. Essentials of animal physiology. 4th Edition. New Age International Publishers.
5. Verma P.S., Agarwal V.K., 2006. Cell biology, genetics, Molecular Biology, Evolution and Ecology. S. Chand publishers, New Delhi, India.
6. Sathyanarayana U., Chakrapani, U., 2013. Biochemistry. 4th Edition. Elsevier publishers.
7. Jain J.L., Sunjay Jain, Nitin Jain, 2000. Fundamentals of Biochemistry. S. Chand publishers,New Delhi, India.
8. Karen Timberlake, William Timberlake, 2019. Basic chemistry. 5th Edition. Pearsonpublishers.
9. Subrata Sen Gupta, 2014. Organic chemistry. 1st Edition. Oxford publishers.

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

12. Hands-on experience of various equipment – Microscopes, Centrifuge, pH Meter,Electronic Weighing Balance, Laminar Air Flow

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 complexbiological 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

2.1. Biomolecules I – Carbohydrates, Lipids.
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

3.1. History, scope, and significance of biotechnology. Applications of biotechnology in Plant, Animal, Industrial and Pharmaceutical sciences.
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.
3.4. Transgenic plants – Stress tolerant plants (biotic stress – BT cotton, abiotic stress – salt tolerance). Transgenic animals – Animal and disease models.

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.

5.2. Measures of dispersion – range, standard deviation and variance. Probability and tests of significance.

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

1. Gerard J., Tortora, Berdell R. Funke, Christine L. Case., 2016. Microbiology: An Introduction. 11th Edition. Pearson publications, London, England.
2. Micale, J. Pelczar Jr., E.C.S. Chan., Noel R. Kraig., 2002. Pelczar Microbiology. 5th Edition. McGraw Education, New York, USA.
3. Sathyanarayana U., Chakrapani, U., 2013. Biochemistry. 4th Edition. Elsevier publishers.
4. Jain J.L., Sunjay Jain, Nitin Jain, 2000. Fundamentals of Biochemistry. S. Chand publishers,New Delhi, India.
5. R.C. Dubey, 2014. Advanced Biotechnology. S. Chand Publishers, New Delhi, India.
6. Colin Ratledge, Bjorn, Kristiansen, 2008. Basic Biotechnology. 3rd Edition. Cambridge Publishers.
7. U. Sathyanarayana, 2005. Biotechnology. 1st Edition. Books and Allied Publishers pvt. ltd., Kolkata.
8. Upadhyay, Upadhyay and Nath. 2016. Biophysical Chemistry, Principles and Techniques. Himalaya Publishing House.
9. Arthur M. Lesk. Introduction to Bioinformatics. 5th Edition. Oxford publishers.
10. AP Kulkarni, 2020. Basics of Biostatistics. 2nd Edition. CBS publishers.

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 wastesand 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

Theory Credits: 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. 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.

7Suggested 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
5. Computer Fundamentals 6th Ed by P.K. Sinha
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

Practical | Credits: 1 | 2 hrs/week

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

Theory Credits: 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

OSI Models, Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS), IP Addresses, IPv4 vs. IPv6, Static Addressing, Dynamic Addressing, Transport Layer Protocols, TCP, UDP, Port Numbers, Wireless and Wired Router Configurations, Network Sharing, Common Preventive Maintenance Techniques used for Networks, Troubleshooting process for Networks, Communication: secret and covert communication and applications of secret/covert communication.

UNIT III: Laptops and Mobile Devices

Laptop: Components, Configuration, Hardware and Component Installation, Configuration Replacing Hardware Device replacement, Preventive Maintenance, Troubleshooting Process; Mobile Device: Components and Configuration, Operating Systems, Synchronization Preventive Maintenance, Basic Troubleshooting Process, Methods for Securing, Common Problems and Solutions.

UNIT IV: Network Security

Security: Introduction, Vulnerabilities, Threats & Attacks (Denial of Service/Distributed Denial of Service, Side channel, DNS reflection & amplification); Procedures, Intrusion detection and response, Securing Web Access, Protecting Data, Protection Against Malicious Software, Security Techniques, Protecting Physical Equipment, Common Preventive Maintenance Techniques for Security, Basic Troubleshooting Process for Security.

UNIT V: Troubleshooting Computer Networks

Identification and Troubleshooting Process; Networks, Security, LAN, Cyber warfare and Network Attacks, Mitigating Cyber Attacks; Security Assessment, Testing and Evaluation, Security information and event management.

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
6. Hands-On Network Forensics by Salman Arthur

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

SEMESTER-III

COURSE 5: CYBER SECURITY

Theory Credits: 3 3 hrs/week

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

Cyberspace: Definition, Architecture and Regulation; Overview of Web-technology; Internet: Advent of internet, World Wide Web, Internet infrastructure for data transfer and governance.

UNIT II: Cyber Crimes

History & Development, Classification of cybercrimes- Cyber Terrorism, Cyber Threats, Cyber Stalking, Pornography, Child Pornography, Hacking, Viruses, Worms, Trojans, Malware, Scareware, Adware, Command and Control, Botnet, Cyber Trespass, Cyber Theft, Cyber Fraud, Password Cracking, Malware, Hunk Mail, Steganography, Cyber Terrorism, Cyber Warfare, Phishing. Impact of cybercrimes- Effect of cybercrimes on society, Cybercrimes against people, property, business and nation. Evaluation of cybercrimes, Definition of cyber criminals, Trends in cybercrime across India & the world.

UNIT III: Cyber Security

Cybersecurity: Need and Importance, Overview, Cybersecurity Domains and Growth, The Cybersecurity Cube - Three Dimensions, CIA Triad, Confidentiality, The Principle of Confidentiality, Protecting Data Privacy, Controlling Access-Laws and Liability; Data Integrity: Principle, Need and Integrity Checks, Availability, The Principle of Availability, Ensuring Availability.

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

E- Commerce: Definition, Components, Security Elements, Threats, Security best practices. Digital payments: Introduction, Components, Modes (Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments), Frauds and Preventive measures. RBI guidelines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act, 2007.

SUGGESTED READINGS

1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) 3
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.

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.
6. Security patch management and updates in Computer and Mobiles.
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.
13. Windows memory acquisition using Dumpit Tool.

SEMESTER-III

COURSE 6: NETWORK FORENSICS

Theory Credits: 3 3 hrs/week

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. Ransom ware Analysis

UNIT I: Network Architecture & Internet - 1

Network: Definition; Securing a Network, Standard Operating Procedure of Network Data, ARPANET Protocols. Classification by Network Geography: Types of Topologies- RING, STAR, BUS, MESH (features, advantages, disadvantages). Classification by Component: Peer to Peer, Client/ Server

Types of Networks: PAN, LAN, MAN, WAN, VPN (with applications). Wireless Network: Wireless LAN, MAN, WAN. Network Forensics: Introduction, Need & Scope, Forensic Significance.

UNIT II: Network Architecture & Internet- 2

Network Communication: Introduction, Types. Network Components: Twisted Pair Cable, Shielded Twisted Pair, Unshielded Twisted Pair, Coaxial cable, Fiber Optic Cables; Standard categories of cables. Network Devices: HUB, Switch, Router. Router: Working of Router, Router Logs, Routing, Routing Table.

UNIT III: Packet Switching

Basic Terms: MAC Address, ARP, NAT, Gateway, Wireless Access Point,

ISO/OSI Model in Communication Networks: Features, Functions of layers (Physical, Data Link, Network, Transport, Session) Application, Merits. TCP/IP Model: Overview, Different TCP/IP Protocols, Merits/ Demerits. Packet Routing: Packet in Internet, Processing packet at source machine.

UNIT IV: Network Traffic- Capturing & Analysis

Basics: NeSA (features, creating a dump file, Preliminary Settings, loading a dump file, Session Filtering) Wireshark: Overview, features, Running the application, FTP Analysis, SMTP Analysis, SSL Decryption. Extraction of Media Files from Network Traffic: Network Miner, Xplico.

UNIT V: Malware Analysis and Ransomware Analysis

Malware Analysis: Introduction (Malware, viruses, and worms), Importance, Essential Skills and Tools; Dependency walker, PEview, W32dasm, OllyDbg, Wireshark, Convert shell Code. Trends in Malware Evolution: Botnets, Encryption and Obfuscation, Automatic Self Updates, Metamorphic network behavior, Blending Network Activity.

Ransomware Analysis: Patterns of Ransomware, Crypto locker, Miscellaneous Ransomware, RSO Cryptosystem, AES Cryptosystem, Cryptographic Techniques as Hacking tools, Tor Network, Digital Cash and Bitcoin.

SUGGESTED READINGS:

1. Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensicsanalysis using Wireshark. *International Journal of Security and Networks*, *10*(2), 91-106.
2. Meghanathan, N., Allam, S. R., & Moore, L. A. (2010). Tools and techniques for networkforensics. *arXiv preprint arXiv:1004.0570*.
3. Davidoff, S., & Ham, J. (2012). *Network forensics: tracking hackers through cyberspace* (Vol. 2014). Upper Saddle River: Prentice Hall.
4. Social Media & Network Forensics, CDAC
5. Monnappa, K. A. (2018). *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing Ltd.

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

Theory Credits: 3 3 hrs/week

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

Cyber security initiatives by Government of India- National Cyber Security Policy, National Cyber Security Coordination Centre, National Critical Information Infrastructure Protection Centre, Cyber Swachhta Kendra, International Cooperation, Promoting research and development, Sectoral and state CERTs, Security Testing.

UNIT 3: Indian Penal Code & Indian Evidence Act

IPC- Sections 63, 63B, 292, 292 A, 293, 294, 379, 382, 411, 419, 420, 463, 464, 468, 469, 499, 500, 503, 506, 507, 509.

IEA- Sections 47A, 65A, 65B, 67A, 81A, 85A, 85B, 85C, 88A, 90A, 131.

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

E- Governance- Goals and stages of E- Governance, Types of interactions in E- Governance, Government Initiatives, Advantages & Disadvantages, Challenges & law. E- Contract- Introduction, Contract, Definition, Parties, Recognition of E- contract, Essentials & Types of E-Contract.

SUGGESTED READINGS:

a. The Information Technology Act, 2000 Bare Act with Short Notes, Universal Law Publishing Co., New Delhi
b. Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi
c. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi
d. S.R.Myneni: Information Technology Law(Cyber Laws), Asia Law House, Hyderabad.
e. Chris Reed, Internet Law-Text and Materials, Cambridge University Press.
f. Pawan Duggal: Cyber Law- the Indian perspective Universal Law Publishing Co., NewDelhi
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

Practical Credits: 1 2 hrs/week

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.
6. Report preparation for various laws of cyber-crime in India.
7. Report preparation for various international laws of cyber-crime.
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

Data Collection: Volatile & Non- volatile data. Registry Analysis, Browser Usage, Hibernate File Analysis, Crash Dump Analysis, File System Analysis, File Metadata and Timestamp Analysis, Event Viewer Log Analysis, MFT analysis, Timeline Creation, Evidence Collection in Linux and Mac Operating system.

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
4. Cryptography and Network Security: United States Edition by William Stallings
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

Practical | Credits: 1 | 2 hrs/week

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.
4. Capture and analysis of network packets using Wireshark (Fundamentals).
5. Using Sys internal tools for Network Tracking and Process Monitoring: - Check Sys internal tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk - Monitor Virtual Memory - Monitor Cache Memory.
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

SEMESTER-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.
6. Laws pertaining to the admissibility of Electronic Evidence.

UNIT I: Computer Artifacts

Definition, Cardinal Rules, Introduction to Digital forensics, Handling Forensic software and hardware – TX1, TD2u, Data Acquisition, Imaging: types of formats and authentication: Tools & processes, Windows Systems-FAT12, FAT16, FAT32 and NTFS, UNIX file Systems, MAC file systems, Computer Artifacts, Internet Artifacts, OS Artifacts and their forensic applications, Memory hierarchy, Types of memory, Storage devices, System software.

UNIT II: Fundamentals of Biometrics

Introduction – Benefits of biometric security, Verification and identification, Basic working of biometric matching, Accuracy – False match rate, False non-match rate, Failure to enroll rate, Derived metrics – Layered biometric solutions. Fundamentals of Gait Analysis, Motion Analysis Systems & theirdetection tools, Competing voice Scan (facial) technologies – Strength and weakness, Facial Character Recognition systems and their development tools.

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

Introduction to Forensic Tools - Encase, FTK, Photorec, Sleuth kits, Autopsy, Magnet Axiom & Examine, Oxygen Forensics, Cellebrite UFED4PC, MSAB-XRY, Metasploit, SQL Injection, SQ-lite, Bulk Extractor, Elocmsoft, Praat, Pro-Discover, Disk-Digger, Disk-driller, Recuva, Nessus, Nikto, Nmap, Zenmap, Burpsuit, Kali-Linux, cedarpelta, CDIIR tool, Penorma, Wingman, RAM analysis tools, Vulnerability Assessment Tools.

SUGGESTED READINGS

1. Digital Forensics with Open Source Tools by C. Altheide& H. Carvey.
2. Biometrics – Identity Verification in a Networked World by Samir Nanavati, Michael Thieme, RajNanavati.
3. Biometrics for Network Security by Paul Reid
4. Dreamtech Biometrics- The Ul by John D. Woodward, Jr. Wiley.
5. Security in Computing by Charles P. Fleeger.
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.
9. Doctrine of IT Act of India, Government of India Publication (2000)

CO-CURRICULAR ACTIVITIES

1. Visit cyber cell.
2. Visit IT organization

SEMESTER-IV

COURSE 9: CYBER TOOLS & TECHNIQUES

Practical | Credits: 1 | 2 hrs/week

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

Computer Forensics: Introduction, Investigation Process, Systematic Approach. Data Recovery Workstations and Software. Investigator's Office and Laboratory: Forensics Lab Certification Requirements, Physical Requirements for a Computer Forensics Lab, Basic Forensic Workstation.

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

Digital Evidence: Search, Collection, Preparation, Isolation, Storage, Process, Verification, Documentation, Report, Archiving.

Computer Forensics Tools: EvaluatingNeeds, Hardware & Software Tools.

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 3rd or 4th edition by Amelia Philips, BillNelsonand Christopher Steuart.
2. https://www.intaforensics.com/2012/01/20/understanding-the-computer-forensics-process/
3. https://www.coursehero.com/file/p3ip151/Understanding-Data-Recovery-Workstations-and-Software-Investigations-are/
4. study.com/academy/lesson/raid-acquisitions-in-digital-forensics-definition-process.html
5. https://prezi.com/ebwye4gtrmyj/chapter-9-computer-forensics-analysis-validation/
6. https://www.thebalancesmb.com/copyright-definition-2948254
7. https://www.ques10.com/p/24610/explain-a-standard-procedure-for-network-forensics/?
8. https://www.makeuseof.com/tag/technology-explained-how-does-an-email-server-work/

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visit to Cyber Cell.
2. Visit to Cyber Crime Scene.

SEMESTER-IV

COURSE 10: DIGITAL FORENSICS

Practical | Credits: 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

Evidence: Definition, Importance, Rules, Types, Investigation Process. Data Backup: Recovery, Obstacles, Role; Data and Evidence Recovery: Formatted Partition Recovery, Procedures and Ethics.

UNIT-II E-Mail Investigation

E-Mail Investigation, E-Mail Tracking, IP Tracking, E- Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences from e-mail, technical issues – Security Technologies: Certification and key Distribution, Cryptographic Applications, Digital Signature Protocols for Transactions, SSL-Secure Socket Layer, SET- Secure Electronic Transaction. Security Issues– Types of Attacks (Active and Passive) Stealing Passwords, Social Engineering, Bugs and Backdoors, Illegal accessing, Authentication Failures, Protocol Failures, Information Leakage, Viruses and Worms, Denial-of-Service, etc.

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

Data recovery, deleted files/folders Recovery, Deleted Partitions, Data Formatted Partition Data, Add Data, Report Data Findings. Analyze True Back Image, Encase Image, Raw Disk Dumps, Virtual disk images and RAM, Dumps, Investigations on Report Analysis, cyber-Laws in Secure Analysis, Extract unallocated and disk slack areas, Data carving of slack areas, Hash Files, File Signature.

UNIT-V Security Issues

Firewalls, Packet Filters, Application-Level Filtering, Circuit Level Gateways, Dynamic Packet Filters, Distributed Firewalls; Digging for Worms, Packet Filtering, implementing policies (Default allow, Default Deny) on proxy; Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Threats, Picking a Security Policy, Strategies for a Secure Network, The Ethics of Computer Security, Security Threats, and levels, Security Plan (RFC 2196)

SUGGESTED READINGS:

1. File System Forensic Analysis by Brian Carrier, Publisher: Addison-Wesley Professional
2. Cyber Law & Crimes (IT Act 2000 & Computer Crime Analysis) by Barkha & Ram Mohan.
3. Cyber Crime by Dr. R C Mishra, Publisher: Authorspress
4. Forensic Science in Crime Investigation by Dr. Rukmani Krishnamurthy.
5. Handbook of Scurity, Cryptography & Digital Signature by S.M. Bhaskar & P. Ramachandran.
6. Forensic Science – From the Crime Scene to the Crime Lab by Richard Saferstein.
7. E-Commerce: The Cutting Edge of Business by Kamlesh K. Bajaj &Debjani Nag.
8. Cyber Law and E .Commerce by David Baumer, J C Poindexter.
9. E- Commerce Strategy , Technologies and Applications by David Whiteley.
10. E- Security, Electronic Authentication and Information Systems Security by Sundeep Oberoi.
11. Firewalls and Internet Security: Repelling the Wily Hacker by Addison.
12. Law Relating to Computers Internet & E-Commerce by NandanKamath
13. Information Technology Law& Practice, by Vakul Sharma.
14. E-government: the science of the possible by J. Satyanarayana.

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

Mobile Phone: Basics**,** Components, Associated Crimes, SIM Card, SIM Security,

Mobile forensics: Challenges, Evidence Extraction process- phase wise.

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

Android Forensic Setup and Pre-Data Extraction Techniques, Screen lock by passing techniques, Gaining root access. Android Data Extraction Techniques - Imaging an Android Phone. Data recovery Techniques. Android App Analysis and Overview of Forensic Tools- Android app analysis, Reverse engineering Android apps, Forensic tools overview, Cellebrite – UFED, MOBILedit and Autopsy.

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 Bommisetty, Rohit Tamma and HeatherMahali kunder
3. https://www.electronics-notes.com/articles/connectivity/cellular-mobile- phone/how-cellphone-works-inside-components.php
4. https://pavanduggalonmobilelaw.wordpress.com/kinds-of-mobile-crimes/
5. https://resources.infosecinstitute.com/windows-phone-digital-forensics/
6. https://www.gillware.com/phone-data-recovery-services/windows- phone-forensics/
7. https://link.springer.com/chapter/10.1007/978-3-642-39891-9_15
7. https://www.nist.gov/system/files/documents/forensics/5-Punja-nist-2014-bb-forensics- FULL.pdf

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visit to cyber cell regarding mobile phones as evidence.
2. Visit to cybercrime scene.

SEMESTER-V

COURSE 12: MOBILE FORENSICS

Practical | Credits: 1 | 2 hrs/week

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
8. Analyzing android device using autopsy forensic tool.
9. Comparison of software -Mobiledit & Autopsy.
10. Comparison of open-source software and closed source software.

SEMESTER-V

COURSE 13: MULTIMEDIA FORENSICS & SPEAKER IDENTIFICATION

Theory Credits: 3 3 hrs/week

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

Multimedia: Introduction, Definition, History, Need, Development Platforms (MS DOS, Windows, Linux), Elements (Text, Graphics, Bitmap Images, Vector Graphics, Audio, Video, Animation), Hardware/ Software Requirements.

UNIT II: Multimedia Forensics

Multimedia Forensics: Introduction, Scope, History, Standards, Practice; Multimedia Authentication: Active Image Authentication, Passive Image Authentication, Video Authentication, Audio Authentication; Basics of Multimedia Devices for capturing image, video and audio; Forensic Analysis: Audio Evidences, Image Evidences, Video Evidences, CCTV Footages; Statistical Interpretation of Forensic Analysis; Legal Admissibility of multimedia evidence. Metadata analysis of Audio / Video/image file, evidence handling, Case studies.

UNIT III: Image and Video Forensics

Image/ Video Forensics: Introduction, Scope, Standards, Active and Passive Forensics, Blind and Non-Blind Forensics; Methods: Source Camera Identification and Tampering; Enhancement of digital image/video, Specific Frame Analysis, Forensic Applications; DVR Examination.

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 spectrographicanalysis, 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, ShujunLi
2. Multimedia Forensics and Security Foundations, Innovations, and Applications by AboulElla Hassanien, Mohamed Mostafa Fouad
3. Fundamentals of Speaker Recognition by Homayoon Beigi
4. Fundamentals of Speaker Recognition Law Enforcement and Counter-Terrorism by AmyNeistein, 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.
9. Analysis of voice.
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

Hacking: Definition, Types, Phases, Passive & Active Reconnaissance, Hacktivism; Ethical Hacking: Introduction, Need, Scope, Limitations, Techniques; Ethical Hacker; Technical Foundations of Hacking: The Attacker's Process, The Ethical Hacker's Process; Security Fundamental, Security testing.

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

Principles and Concepts, PT workflows and Examples, Blind tests, Synthetic Transactions, Interface Testing and Fuzzing, SDLC Phases, and Security mandates.

UNIT IV: Programming for Security Professionals

Web Application Vulnerabilities, Buffer Overflow Attacks, Session Hijacking, Code Injection Attacks- Cross Site Scripting (CSS) Attacks, Required Lab goals; Attack Target-gathering information, Finding Critical Bugs in Servers.

UNIT V: Prevention of Hacking

Prevention: DoS Attacks, Session Hijacking, Hacking Web Servers, Hacking Web Applications, SQL injection attacks, Social Engineering. Surveillance Techniques and Countermeasures. Investigating range of security issues relating to operating systems, PC systems, threats - vulnerabilities and securitymechanisms.

SUGGESTED READINGS

1. Preventing Web Attacks with Apache by Ryan C. Barnett
2. Innocent Code : A Security Wake-Up Call for Web Programmers by Sverre H. Huseby
3. HackNotes(tm) Web Security Pocket Suggesive readingsby Mike Shema

4. Testing Web Security: Assessing the Security of Web Sites and Applications by Steven Splaine
5. Improving Web Application Security: Threats and Countermeasures by Microsoft Corporation
6. Hacking the Code: ASP.NET Web Application Security by Mark Burnett
7. How to Break Software Security by James A. Whittaker and Herbert H. Thompson
8. Exploiting Software: How to Break Code by Greg Hoglund and Gary McGraw
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
13. Steven DeFino, Barry Kaufman, Nick Valenteen, "Official Certified Ethical Hacker ReviewGuide", CENGAGE Learning, 2009-11-01.
14. Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking andPenetration Testing Made Easy", Syngress Basics Series – Elsevier, August 4, 2011.

SEMESTER-V

COURSE 14: ETHICAL HACKING

Practical Credits: 1 2 hrs/week

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,

9. Understanding DoS Attack Tools- Panther2, Crazy Pinger, Some trouble, UDP Flood, FSMax.

10. E-mail header and URL analysis.

SEMESTER-V

COURSE 14: INTRODUCTION TO PROGRAMMING

Theory Credits: 3 3 hrs/week

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: Introduction, History, Fundamentals, Structure, Elements, Data Types, Variables, Constants, Emulators, Array, Function, Strings.
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

1. Programming in 'C' by Stephen G, Kochan.
2. Pythton Object oriented programming – Fourth edition by Steven F.Lott, Dusty Phillips, PacktPublication.
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.

SEMESTER-V

COURSE 14: INTRODUCTION TO PROGRAMMING

Practical Credits: 1 2 hrs/week

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
9. C++ program that uses a recursive function for solving Towers of Hanoi problem.
10. C++program to implement call by value and call by Suggested Reading parameters passing.

SEMESTER-V

COURSE 15: CRYPTOGRAPHY AND STEGANOGRAPHY

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. 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

Security: Introduction, Concept, Need, Approaches, Principles, Services, Mechanism, Types of Security attacks, Network Security Model.

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.

Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.

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.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public Key Infrastructure.

UNIT IV – Digital Watermarking

History & Basics, Designing, Importance, Data Hiding, Detection & Analysis of Digital Watermarks, Media Specific Digital Watermarking: Image Watermarking, Video Watermarking, Audio Watermarking, Watermarking for CG-models, Watermarking for Binary Images, Watermarking for 3D Contents.

UNIT V – Steganography & Steganalysis

Steganography: Terminology, History, Concept and methods, Properties, Importance, Applications.

Steganographic Security, Practical Steganographic Methods; Steganalysis: Forensic Steganalysis, Algorithms, Analysis, Blind Steganalysis of JPEG images using Calibration, Blind Steganalysis in the Spatial Domain.

SUGGESTED READINGS

1. Cryptography and Network Security by W. Stallings [Prentice Hall]
2. Cryptography and Network Security: Principles and Practices by William Stallings.
3. Cryptography and Network Security by C K Shyamala, N Harini and Dr. T R Padmanabhan.
4. Digital Watermarking and Steganography, 2nd Edition, by Cox, Miller, Bloom, Fridrich, and Kalker,2008
5. Cryptography and Network Security: Principles and Practice by A William Stallings.
6. Applied Cryptography: Protocols, Algorithms, and Source Code in C by Bruce Schneier,[Wiley].

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 withinan 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.

SEMESTER-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

File System Data Carving Tools, EXIF Optimal sensor metadata Analysis Tools, Video-Footage Analysis Tools, Imaging Tools, FTK, VIP 2.0, XRY Drone, XAMN, MD-DRONE, DJI Assistant-2, DatCon, DJI GO 4 App, CsvView, Cellebrite (UFED4PC), AvsPmod, AviSynth, VirtualDub, open- source tools.

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

and the Drone (Amendment) Rules, 2021. Laws for Nano, Micro, Small, Medium, Large Drones. Drone Registration & Operation Guidelines. Remote Pilot Licensing guidelines, Drone-Traffic Management.

SUGGESTED READINGS

1. The Big Book of Drones – Ralph DeFrangesco, Stephanie DeFrangesco (2022)
2. Drone Forensics: The Impact and Challenges - Atkinson, Carr, Shaw and Zargari (2020)
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.
9. Disassembly of the drone.
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

OS Components: Process Management, Memory Management - Main & Secondary, File Systems Management, Input/Output Management, Networking, Protection System, Command- Interpreter System.

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

System Structure: Introduction, MS DOS System Structure, UNIX System Structure, Layered Structure.

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

1. Operating Systems: Principles and Practice, by Thomas Anderson, Michael Dahlin, Recursive Books, 2012.
2. Operating System Concepts by Abraham Silberschatz & Peter Galvin
3. Operating Systems: Internals and Design Principles by Wiliam Stallings
4. Operating System: A Concept-Based Approach by D M Dhamdhere.

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

Practical | Credits: 1 | 2 hrs/week

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.
6.Summation of +ves and -ves.
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.

SEMESTER-VII

COURSE 17: SOCIAL MEDIA FORENSICS

Theory Credits: 3 3 hrs/week

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

Social Media: Kinds (Blogs, Social Networking Sites, Wikis, Micro Blogging, Forums, Media Sharing Sites, Podcasts, Videocasts and Virtual World), Working, Applications, Security Issues, Impact (Positive/Negative), Emerging Trends.

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

Social Media Forensics: Introduction, Data, Need, Scope, Investigation Process (Collection, Examination & Analysis), Tools (Open source & Proprietary). Legal issues in world social media, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Case Studies.

SUGGESTED READINGS:

1. Social network sites: Definition, history and scholarship by Boyd, D. M., & Ellison, N. B. (2008). Journal of Computer-Mediated Communication, 13, 210-230.
2. Reconsidering research on learning from media by Clark, R. E. (1983). Review of Educational Research, 53(4), 445–459.
3. Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
4. Social Network Analysis: Methods and Application by Katherine Faust and StanleyWasserman.
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

Practical Credits: 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

Theory Credits: 3 3 hrs/week

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

Windows Kernel: Windows Fundamental, Survey of Obfuscation techniques, Piracy and Copy Protection, Deep Web and Dark Net, Anti Reversing Techniques.

UNIT III: Malware Analysis

Malware: Introduction, Definition, Types (Virus, Worm, Trojan, Backdoor, Ransomware).
Malware Analysis: Introduction, Need, Goals, Techniques (Static & Dynamic). Virtual Machines for Malware Analysis.

UNIT IV: Basic and Advanced Static Malware Analysis

Basic Static Techniques: Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executable File Format, Linked Libraries and Functions, PE File Header and Sections.
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

Basic Dynamic Analysis: Executing Malware Analysis in safe environment, Monitoring with Process Monitor, Viewing Processes with Process Explorer, Comparing Registry Snapshots with Regshot, Faking a Network, Packet Sniffing with Wireshark.
Advanced Dynamic Analysis: Debugging- Source Level vs Assembly Level Debuggers, Kernel vs User mode Debugging, Using Debugger – OllyDbg/IDA Pro, Exceptions, Modifying execution with Debugger, Malware Behavior: Reverse Shell, RAT, Botnet, Process Injection, Hook Injection, APC Injection.

SUGGESTED READING:

1. Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig, 1st Edition
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
6. Ghidra Software Reverse Engineering for Beginners: Analyze, identify, and avoid maliciouscode and potential threats in your networks and systems by A. P. David.

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

Practical Credits: 1 2 hrs/week

B.Sc.	Semester: VII	Credits: 1
Course: 18	REVERSE ENGINEERING AND MALWARE ANALYSIS LAB	Hrs/Wk: 2

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

Theory Credits: 3 3 hrs/week

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

Incident Response and Handling Process: Identification, Incident Recording, Initial Response, Communicating the Incident, Containment, formulating a Response Strategy, Incident Classification, Incident Investigation, Data Collection, Forensic Analysis, Evidence Protection, Notify External Agencies, Eradication, System Recovery, Incident Documentation, Incident Damage and Cause assessment, Review and Update of Response Policies.

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 MatthewPepe
2. Computer Incident Response and Forensics Team Management: Conducting a SuccessfulIncident 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.

SEMESTER-VII

COURSE 19: INCIDENT RESPONSE

Practical | Credits: 1 | 2 hrs/week

LIST OF EXPERIMENTS

1. Live Response Collection with cedarpelta tool.
2. Acquiring the data from Windows Operating system by Cyber Defense Institute Incident ResponseCollector.
3. Artifact collection from Windows & Linus OS by Fast IR Collector.
4. Creating fast report of the incident on the Windows system with Panorama tool.
5. Collection of the forensic evidence with the help of IREC tool.
6. Collection and analysis of forensic artifacts by DG Wingman Tool.
7. Calculate the MD5 Hash of the extracted VBA macro and make a copy.
8. Identify the mails through packet captures.
9. Usage of Net Flow for incident response.
10. Create a report for incident response.

SEMESTER-VII

COURSE 20: FORENSIC ROBOTICS

Theory Credits: 3 3 hrs/week

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

Robotic Mechanisms, Matrix Representation, Description of Position and Orientation, Frames and Displacement mappings, Homogeneous transforms, Transformation of free vectors, examples.

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

Robot Operating System (ROS) Forensics: Introduction, Definition, Concept, Version of ROS; Data Distributed Service (DDS); ROS2: Definition, Security Features, Vulnerabilities, ROS Digital Investigation and Forensic Works, Forensic Analysis of hacked ROS System.

SUGGESTED READINGS

1. Software engineering for experimental robotics by Davide Brugali.
2. Robotics. ACM Computing Surveys by Lewis, F. L., Fitzgerald, M., & Liu, K.
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.,
7. https://www.researchgate.net/publication/338800343. An Overview of Robot Operating System Forensics
8. https://sci-hub.se/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.77
9. https://cyforce.in/robot-forensics.html.
10. https://dps.mn.gov/blog/Pages/20200113-robotics-in-forensic-testing.aspx

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.
6. Statistical data of robotic investigation done internationally.
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.
3. Traffic Analysis for Android Devices.
4. iOS Application Security.
5. Various Android & iOS tools.

UNIT 1: Android Devices

Android: Introduction, Evolution, Architecture, Security, File Hierarchy, Android File System, Forensic Setup; Pre-data extraction, Screen lock bypassing techniques.

UNIT 2: Android Data Extraction Techniques

Manual, Logical, Physical Data Extraction; Android Data Analysis and Recovery; Android AppAnalysis, 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 andpotential bypass; Logical acquisition; File system acquisition.

UNIT 4: Data Acquisition from iOS Backup

iTune backup; Extracting unencrypted backups; handling encrypted backup files; working with iCloudbackups.

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
2. https://www.electronics-notes.com/articles/connectivity/cellular-mobilephone/how-cellphone-works-inside-components.php
3. https://pavanduggalonmobilelaw.wordpress.com/kinds-of-mobile-crimes/
4. https://resources.infosecinstitute.com/windows-phone-digital-forensics/
5. https://www.gillware.com/phone-data-recovery-services/windowsphone-forensics/

SUGGESTED CO- CURRICULAR ACTIVITIES

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

SEMESTER-VIII

COURSE 21: ANDROID AND iOS FORENSICS

Practical | Credits: 1 | 2 hrs/week

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
9. Mobile Forensics Investigation using Wondershare Recoverit.
10. Mobile Forensics Investigation using EaseUS Recovery Wizard.

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

1. Hands-on Penetration Testing for Web Applications: Run Web Security Testing on ModernApplications Using Nmap, Burp Suite and Wireshark by Richa Gupta
2. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit,and more by Gus Khawaja
3. Hands-On Application Penetration Testing with Burp Suite: Use Burp Suite and its features byCarlos A. Lozano, Dhruv Shah, et al.

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.

SEMESTER-VIII

COURSE 22: VULNERABILITY ASSESSMENT OF APPLICATION SECURITY

Practical Credits: 1 2 hrs/week

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

SEMESTER-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-

1. Fundamentals of Cloud Computing.
2. Various models in cloud computing.
3. Access management
4. Framework of cloud forensics.
5. Privacy in cloud computing & IoT

UNIT 1: Cloud Computing

Cloud: Introduction, Definition, Types; Cloud Computing: Introduction, Characteristics, Need, Security Design & Architecture; Cloud Computing Model: Cloud Computing Service Models, Multi Tenancy Model, Cloud Security Reference Model, Cloud Computing Deploying Models.

UNIT 2: Cloud Identity and Access Management.

Identity Provision: Authentication; Key management for access control: Authorization; Infrastructure and Virtualization Security; Hypervisor Architecture Concerns.

UNIT 3: Cloud Security

Cloud Security: Security boundary, Security service boundary, Security Mapping, Securing Data, Brokered Cloud Storage Access, Storage Location and tenancy, Encryption, Auditing and compliance, Establishing identity and presence, Identity protocol standard.

UNIT 4: Cloud Forensics

Cloud Forensic Framework: Introduction, Dimensions, Usages, Challenges, Tools; Cloud Crime; Digital Forensic Investigation and Cloud Computing.

UNIT 5: Privacy in Cloud Computing and IoT

Privacy in Cloud Computing: Introduction, Paradigm and privacy, Challenges; Privacy in IoT: Introduction, IoT Governance, Security, Issues, Challenges, Solutions.

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 Problemsby 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 usingFORST Tool.
4. Analyzing cloud data and metadata using UFED Cloud analyzer.
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

Theory Credits: 3 3 hrs/week

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

Machine Learning: Definition, Applications, Types, Issues and Challenges; Supervised Learning: Basics, Prediction, Classification, Datasets, Feature Selection, Feature Normalization, Data Cleaning, Training, Testing & Validation Sets, Models, Hyperparameters, Measuring Performance, Accuracy and Loss Underfitting & Overfitting; Unsupervised Learning: Basics, Models; Mathematics for ML: Vectors, Matrices, Linear Equations, Variance, Probability, Handling and Representing Data.

Python: Setting up Environment, Basic Python Commands, Python Scripts, Conditions, Loops, List, Dictionary, User Defined Functions, Anaconda, Working with NumPy, Pandas and Matplotlib.

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
2. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 2nd Edition by Aurélien Géron
3. Python Machine Learning: Machine Learning and Deep Learning with Python, scikit- learn, and TensorFlow 2, 3rd Edition by Sebastian Raschka and Vahid Mirjalili
4. Hands-On Neural Networks with Keras: Design and create neural networks using deep learning and artificial intelligence principles 1st Edition by Niloy Purkait
5. Deep Learning with Keras: Implementing deep learning models and neural networks with the power of Python by Antonio Gulli, Sujit Pal
6. Lab Machine Learning for Computer Vision 1st Edition by Valliappa Lakshmanan, Martin Görner and Ryan Gillard
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 Howseand Joe Minichino
8. Natural Language Processing in Action: Understanding, analyzing, and generating text with Python 1st Edition by Hobson Lane, Hannes Hapke and Cole Howard.
9. Machine Learning for Cybersecurity Cookbook: Over 80 recipes on how to implement machine learning algorithms for building security systems using Python by Emmanuel Tsukerman.
10. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem by Soma Halder (Author), Sinan Özdemir.

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.

SEMESTER-VIII

COURSE 25: CYBER THREATS AND SOLUTIONS

Theory Credits: 3 3 hrs/week

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

Malware: Introduction, Definition & Classification; Malware Analysis: Introduction, Definition, Scope, Types of Attacks, History of Attacks, Analysis; Static Malware: Definition, Analysis; Dynamic Malware: Definition, Analysis; Virus vs Worms vs Malware. Case studies.

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

Malicious Macro; Document Exploit: Definition, Major Exploits, Detection, Prevention; PDF Malware: Introduction, Analysis; Word Malware: Introduction, Analysis; Loopholes of Malicious Document attacks; Malicious Scripts; Windows malware.

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

1. Lab malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorskiand Andrew Honig.
2. Computer viruses: from theory to applications by Filiol, Eric.
3. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by MichaelDavis, Sean Bodmer, Aaron Lemasters.

4. Windows Malware Analysis Essentials by Victor Marak.
5. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigateWindows malware by Monnappa K A.
6. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code byMichael Hale Ligh, Steven Adair, Blake Hartstein and Matthew Richard.
7. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle.
8. Malware Forensics Field Guide for Windows Systems by Cameron H. Malin, Eoghan Casey, James
   M. Aquilina and Curtis W. Rose.
9. Advanced Malware Analysis by Tata McGraw Hill.
10. Computer Viruses and Malware by ErciFiliol.
11. Computer Viruses: from theory to applications, Springer,2005.

SEMESTER-VIII

COURSE 25: CYBER THREATS AND SOLUTIONS

Practical Credits: 1 2 hrs/week

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