ANDHRA PRADESH STATE COUNCIL OF HIGHER EDUCATION

MINOR

Subject: Cyber Forensics

w.e.f. AY 2023-24

COURSE STRUCTURE

Year	Semester	Course	Title of the Course	No. of Hrs /Week	No. of Credits
I	II	1	Fundamentals of Computer	3	3
			Fundamentals of Computer Practical Course	2	1
II	III	2	Cyber Security	3	3
			Cyber Security Practical Course	2	1
	IV	3	Cyber Tools & Techniques	3	3
			Cyber Tools & Techniques Practical Course	2	1
		4	Digital Forensics	3	3
			Digital Forensics Practical Course	2	1
III	V	5	Mobile Forensics	3	3
			Mobile Forensics Practical Course	2	1
		6	Multimedia Forensics & Speaker Identification	3	3
			Multimedia Forensics & Speaker Identification Practical Course	2	1

SEMESTER-II

COURSE 1: 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 1: 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-III

COURSE 2: 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 2: 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-IV

COURSE 3: 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 3: 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 4: 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 4: 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-V

COURSE 5: 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

1. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma and HeatherMahali kunder
2. https://www.electronics-notes.com/articles/connectivity/cellular-mobile- phone/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/windows- phone-forensics/
6. 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 5: 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 6: 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 spectrographic analysis, Spectrographic cues for Vowels and Consonants, Automatic Speaker Identification System, Collection of voice samples: methods and challenges.

SUGGESTED READINGS

1. Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T S Ho, 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 6: 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.