## Subject: Cyber Forensics

w.e.f. AY 2023-24

### COURSE STRUCTURE

<table>
<thead>
<tr>
<th>Year</th>
<th>Semester</th>
<th>Course</th>
<th>Title of the Course</th>
<th>No. of Hrs /Week</th>
<th>No. of Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>II</td>
<td>1</td>
<td>Fundamentals of Computer</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fundamentals of Computer Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>III</td>
<td>2</td>
<td>Cyber Security</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Security Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>IV</td>
<td>3</td>
<td>Cyber Tools &amp; Techniques</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cyber Tools &amp; Techniques Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Digital Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Digital Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>V</td>
<td>5</td>
<td>Mobile Forensics</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mobile Forensics Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>Multimedia Forensics &amp; Speaker Identification</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multimedia Forensics &amp; Speaker Identification Practical Course</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
SEMESTER-II

COURSE 1: FUNDAMENTALS OF COMPUTER

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

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

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

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

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

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

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

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

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

Suggested Co-Curricular Activities

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

COURSE 1: FUNDAMENTALS OF COMPUTER

List of Experiments:

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


**UNIT II: Cyber Crimes**


**UNIT III: Cyber Security**


**UNIT IV: Social Media and Security**

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


SUGGESTED READINGS


SUGGESTED CO-CURRICULAR ACTIVITIES

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

COURSE 2: CYBER SECURITY

List of Experiments:

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

COURSE 3: CYBER TOOLS & TECHNIQUES

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

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

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

UNIT I: Computer Artifacts

UNIT II: Fundamentals of Biometrics

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

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

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

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

COURSE 3: CYBER TOOLS & TECHNIQUES

List of Experiments

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

COURSE 4: DIGITAL FORENSICS

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

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

UNIT I: Computer Forensics and Investigations

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

UNIT III: Identifying, Processing Crime and Incident Scenes

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

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

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

SUGGESTED CO-CURRICULAR ACTIVITIES

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

COURSE 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

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

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

UNIT IV: Android Forensics–II

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

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

SUGGESTED CO-CURRICULAR ACTIVITIES

1. Visit to cyber cell regarding mobile phones as evidence.
2. Visit to cybercrime scene.
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
10. Comparison of open-source software and closed source software.
SEMESTER-V

COURSE 6: MULTIMEDIA FORENSICS & SPEAKER IDENTIFICATION

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

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

UNIT I: Fundamentals of Multimedia

UNIT II: Multimedia Forensics

UNIT III: Image and Video Forensics

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

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

**SUGGESTED READINGS**

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

**SUGGESTED CO-CURRICULAR ACTIVITIES**

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

COURSE 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.
10. Comparison of Praat software and Audacity Software.