UG Cyber Forensics (4 Years Honors)

CBCS - 2020-21

B.Sc.
CYBER FORENSICS

Syllabus and Model Question Papers

TABLE OF CONTENTS

Note: BOS is to provide final soft copy in PDF and word formats and four copies of hard copies in bounded form to the office of Dean Academic affairs.

1. Resolutions of the Board of Studies

Meeting held on: 22/01/2021.Time: 10:00 AM
At: Adikavi Nannaya University, NTR Convention Centre, Rajamahendravaram.

Agenda: Revision of Syllabus of B.Sc. Cyber Forensics , as per the guidelines and model curriculumprovided by APSCHE for implementation from 2020-21 admitted batches.

Members present:

BOS-Chairman: Dr. D. Kalyani, Asst. Professor, ANUR Members: Mr. E. Mohan, Principal, Aditya Degree College.

Resolutions:

The Board of Studies members of B.Sc. Cyber Forensics thoroughly discussed on Cyber Forensics course structure, framing of syllabus, eligibility of students, qualifications of teachers and career prospects of the students.

The following were the resolutions made in the meeting. It was resolved

1. It was resolved to adopt revised common programme structure as per the guidelines issued by APSCHE.
2. Resolved to adopt regulations and scheme of examinations and marks/grading system of the universityUG-Programmes.
3. Resolved to prepare model question Courses in the given prescribed format.
4. Resolved to prepare a list of equipment/software required for each Lab/Practicals.
5. Resolved to give the eligibility criteria for students for joining the course.
6. Resolved to give the eligibility criteria for faculty for teaching the course.
7. Resolved to prepare a list of Course setter/Course evaluators/project evaluators in a given format

2. DETAILS OF COURSE TITLES & CREDITS

Sem	Course no.	Course Name	Course type (T/L/P)	Hrs./ Week (Science:4+2)	Credits (Science: 4+1)	Max. Marks Cont/ Internal /MidAssessment	Max. Marks Sem-end Exam
I	1	Fundamentals of Computer	T	4	4	25	75
		Fundamentals of Computer Lab	L	2	1		50
II	2	Networking and Security	T	4	4	25	75
		Networking and Security Lab	L	2	1		50
III	3	Cyber Security	T	4	4	25	75
		Cyber Security Lab	L	2	1		50
IV	4	Digital Forensics	T	4	4	25	75
		Digital Forensics Lab	L	2	1		50
	5	Mobile Forensics	T	4	4	25	75
		Mobile Forensics Lab	L	2	1		50

Note: *Course type code: T: Theory, L: Lab, P:Practical.

a. Proposed combination subjects: Cyber Forensics& Chemistry

b. Student eligibility for joining in the course:
Intermediate Examination (10+2) with Botany or Zoology or Mathematics and Chemistry
OR
12th Standard (ICSE/CBSE with Science group)

c. Faculty eligibility for teaching the course:M.Sc. in Cyber Forensics with minimum 60% or above in Cyber Forensics subjects (Minimumqualification); Ph.D. is desirable.

d. List of Proposed Skill enhancement courses with syllabus, if any

e. Any newly proposed Skill development/Life skill courses with draft syllabus and required resources

f. Required instruments/software/ computers for the course:
(Lab/Practical course-wise required i.e., for a batch of 15 students)

Sem. No.	Lab/Practical Name	Names of Instruments/Software/ computers required with specifications	Brand Name	Qty Required
1	Fundamentals of Computer Lab	Computers	Dell/Lenovo/Acer/ HP	15
2	Networking & Security Lab	Computers	Dell/Lenovo/Acer/HP	15
3	Cyber Security Lab	Kali Linux OS	Offensive Security	15
4	Digital Forensics Lab	1) Forensic Universal Bridge (T356789iu) 2) Forensic Imager TX1 3) EnCase Portable Tool 4) AMPED Five Software 5) Magnet Axiom Software 6) Disk Forensic Software 7) Faraday Bags	Tableau Tableau EnCase AMPED AXIOM EnCase	Each 2
	Mobile Forensics Lab	1) Paraben's Electronic Evidence Examiner (E3:Universal) 2) UFED 4PC Ultimate 3) MOBILedit Forensic	Paraben Cellebrite MOBILedit	Each 2

g. List of Suitable levels of positions eligible in the Govt./Pvt. organizations

Suitable levels of positions for these graduates either in industry/govt. organization like, technical assistants/ scientists/ school teachers., clearly define them, with reliable justification

S.No	Position	Company/ Govt. organization	Remarks	Additional skills required, if any
1	Scientific Assistant	CFSL/State FSL/Regional FSL/CDTI	Upgrade their skills and get promoted	Communication skills Language skills Computational skills
2	Crime Scene Officer	Clues Team/ Crime Spot	”	”
3	Lab Assistant	CFSL/State FSL/CDTI	”	”
4	Cyber Crime analyst	CFSL/State FSL	”	”
5	Record Assistant	State or District Crime Records Bureau	”	”
6	Lab Technician	Chemical Examiner’s Laboratory	”	”
7	Forensic Faculty	Police Academies		
8	Forensic Faculty	Central Detective Training Institutes		
9	Cyber Expert	Cyber Security		
10	Cyber Security Expert	IT Companies		
11	Forensic Consultant	Forensic Consultancies		
12	Document Expert	Banks		

h. List of Govt. organizations / Pvt. companies for employment opportunities or internships or projects

S.No	Company/ Govt organization	Position type	Level of Position
1	Central / State FSLs	Intern/Project Assistant	Basic (can be upgraded)
2	FPB/NCRB	Intern/Project Assistant	Basic (can be upgraded)

i. Any specific instructions to the teacher /Course setters/Exam-Chief Superintendent:

Course setter may strictly follow the syllabus and blue print of question Course while setting the Course.Course evaluators may strictly follow the scheme of evaluation.

3. Program objectives, outcomes, co-curricular and assessment methods

B.Sc.	Cyber Forensics

1. Aim and objectives of UG program in Subject:

a. Students will understand history of forensic science, development and its role in criminalinvestigation.
b. Application of a computer to everyday tasks using standard procedures
c. Need to effectively protect and process various physical evidences at SoC
d. Documents and finger impressions can be used for the identification of culprit.
e. How to protect ourselves from various kinds of cyber attacks
f. Importance of biological evidences encountered in crime scene investigation.
g. Applications of Chemistry and Ballistics for criminal investigation
h. Investigation techniques, requirement and analyzing of digital evidences are covered.
i. Mobile devices and its analysis in solving the crimes.

2. Learning outcomes of Cyber Forensics:
After successful completion of B.Sc. Forensic Science, students will be able to answer the importanceof Cyber Forensicsin solving the crimes through the scientific investigation of crime scene and analysis of various physical evidence including digital evidence.

3. Recommended Skill enhancement courses: (Titles of the courses given below and details of the syllabusfor 4 credits (i.e., 2 units for theory and Lab/Practical) for 5 hrs class-cum-lab work.

4. Recommended Co-curricular activities: (Co-curricular Activities should not promote copying from textbook or from others' work and shall encourage self/independent and group learning)

A. Measurable:
1. Assignments on: Crime Scene Management, Questioned Documents & Finger Impressions
2. Student seminars (Individual presentation of Courses) on topics relating to: Cyber Security,Digital Forensics, Mobile Forensics
3. Quiz Programmes on: Forensic Biology & DNA Fingerprinting, Chemistry & Toxicology
4. Individual Field Studies/projects: Crime Scene Management
5. Group discussion on: Digital Forensics, Mobile Forensics

6. Group/Team Projects on: Crime Scene Management, Questioned Documents & Finger Impressions, Forensic Biology & DNA Fingerprinting, Chemistry & Toxicology, Cyber Security, Digital Forensics, Mobile Forensics

B General

1. Collection of news reports and maintaining a record of Course-cuttings relating to topicscovered in syllabus
2. Group Discussions on: Crime Scene Management, Digital Forensics, Mobile Forensics
3. Watching TV discussions and preparing summary points recording personal observationsetc., under guidance from the Lecturers
4. Any similar activities with imaginative thinking.

5. Recommended Continuous Assessment methods: Workshops, Conferences & Course presentations tobe conducted regularly.

DETAILS OF COURSE WISE SYLLABUS

4. Details of course-wise Syllabus

B. Sc.	Semester: I	Credits: 4
Course: 1	**Fundamentals of Computer**	Hrs/Wk: 4

Aim and objectives of Course: The objective of the course is to give basic competency in application of a computer to everyday tasks using standard procedures.

Learning outcomes of Course: After studying this Course the students will know-

- Demonstrate on Computer and its components
- To identify Basic input and output devices
- Demonstrate on Types of printers and its configuration
- The Assembling and Dissembling of computer
- To identify Preventive Maintenance and Troubleshooting process

UNIT I:

Basic Computer Knowledge Computer organizations, types of computers, Components of computer, Input Devices Key board, mouse, touch pad and other pointing Devices, Desktop Icons and control panel objects, Operating system types, Creating Files and Folders, Exploring the folders, files, and programs, Editing a document file.

UNIT II:

Introduction to Computer Networks: Computer networks, Intranet, Surfing the Internet, ISPs and connection types, Search, Email, Virtual communities, Social Networks, Tools on the web.

UNIT III:

Components of Computer and Printers Introduction to the Computer Hardware, Power Supplies, Motherboards, Internal PC Components, External Ports and Cables, Input and Output Devices, Select Computer Components, Safe Lab 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, Optimizing Printer Performance, Sharing Printers, Print Servers, Maintaining and Troubleshooting Printers, Troubleshooting Printer Issues, Common Problems and Solution

UNIT IV:

Computer Assembly: Assemble the Computer, Computer Disassembly, Install the Motherboard, Install Drives, Install Cables, Install the Adapter Cards, Install the Adapter Cards, BIOS Beep Codes and Setup, BIOS and UEFI Configuration, Upgrade and Configure a Computer, Storage Devices, Peripheral Devices

UNIT V:

Preventive Maintenance and Troubleshooting, Preventive Maintenance and the Troubleshooting Process, PC Preventive Maintenance, Benefits of Preventive Maintenance, Preventive Maintenance Tasks, Clean the Case and Internal Components, Inspect Internal Components, Identify the Problem, Probable Cause, Test the Theory to Determine, Plan of Action to Resolve the Problem and Implement the Solution.

REFERENCE BOOKS:

1. Introduction to IT essentials Version 6 by CISCO
2. Fundamentals of Computers by Balagurusamy, McGraw Hill by: Balagurusamy
3. Fundamentals of computers by Rajaraman
4. Computer Fundamentals Courseback by Anita Goel
5. Computer Fundamentals 6th Ed by P.K. Sinha
6. Fundamentals of Computers by Rajaraman V

Suggested Co-Curricular Activities: NA.

B. Sc.	Semester: I	Credits: 1
Course: 1	**Fundamentals of Computer Lab**	Hrs/Wk: 2

List of Experiments:

1. Basic Computer Knowledge
2. Introduction to Computer Networks
3. Components of Computer and Printers
4. Computer Assembly
5. Preventive Maintenance and Troubleshooting

B.Sc.	Semester: II	Credits: 4
Course: 2	**Networking and Security**	Hrs/Wk: 4

Learning Objective: Networking and Security concerns with gathering, monitoring and analyzing of network activities to uncover the source of attacks, viruses, intrusions or security breaches that occur on a network or in network traffic.

Outcomes: After studying this course the students will know-

- Installation of various operating systems, and configuration
- Demonstrate on various protocols
- Troubleshooting of laptops and mobile devices
- Demonstrate on network and network types
- Understanding of OSI Model
- Troubleshooting Computer Networks

UNIT I:

Operating Systems and Installation: Windows Installation, Operating System Terms and Characteristics, Types of Operating Systems and Operating Systems Upgrade, Operating System Installation, Storage Device Setup Procedures, Custom Installation Options, Boot Sequence and Registry Files, Multiboot Procedures, Disk Management Utility, Windows Configuration and Management, Windows Desktop, Tools and Applications, Control Panel Utilities, Administrative Tools, Secure System Configurations, Disk Defragmenter and Disk Error- Checking Tool, Command Line Tools, Client-Side Virtualization, Common Preventive Maintenance Techniques for Operating Systems, access control considerations, Anti-virus installations and configuration, Desktop level windows/linux builtin firewall configurations, enabling logging options in operating systems (event log in windows and syslog in linux).

UNIT II:

Applied Computer Networking: Computer Networks, Types of Networks, OSI Reference Models, Wired and Wireless Ethernet Standards, Physical Components of a Network, Hubs, Bridges, Switches, Rourters, Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS), Cables and Connectors, Basic Networking Concepts and Technologies, IP Addresses, IPv4 vs. IPv6, Static Addressing, Dynamic Addressing, Transport Layer Protocols, TCP, UDP, Port Numbers, Computer to Network Connection, Wireless and Wired Router Configurations, Network Sharing, Remote Connections, ISP Connection Technologies, Internet Technologies, Networked Host Services, Common Preventive Maintenance Techniques Used for Networks, Basic Troubleshooting Process for Networks, secret communication, convert communication and applications of secret/covert communication.

UNIT III:

Laptops and Mobile Devices: Laptops and Mobile Devices, Laptop Components, Laptop Displays, Laptop Configuration, Wireless Configuration, Laptop Hardware and Component Installation and Configuration, Replacing Hardware Devices, Mobile Device Hardware, Common Preventive Maintenance for Laptops and Mobile Devices, Basic Troubleshooting Process for Laptops and Mobile Devices, Mobile, Linux, and OS X Operating Systems, Mobile Operating Systems, Methods for Securing Mobile Device, Mobile Device Synchronization, Configuring Email, Linux and OS X Operating Systems, Basic Troubleshooting Process for Mobile, Linux, and OS X O/S, Common Problems and Solutions for Mobile, Linux, and OS X O/S. Trouble shooting of network issues.

UNIT IV:

Network Security: Introduction to Security, Security vulnerabilities, Security Threats & attacks such as Denial of Service/Distributed Denial of Service (DDoS), Side channel attacks, DNS reflection & amplification attacks and others, Security Procedures, best practices, 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: Apply Troubleshooting Process to Networks, Apply Troubleshooting Process to Security, Identify and Troubleshooting LAN problems, Cyber warfare and Network Attacks, Mitigating Cyber Attacks, Troubleshoot Security Problems, Security Assessment, Testing and Evaluation, Security information and event management.

REFERENCE BOOKS:

1. Introduction to IT essentials version 6 by CISCO
2. https://www.webopedia.com/TERM/N/network.html
3. Network Forensics: Tracking Hackers Through Cyberspace by Sherri Davidoff, PearsonIndia by Sherri Davidoff
4. https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model
5. Network Forensics by Ric Messier
6. Learning Network Forensics by Samir Datt
7. Introduction to Security and Network Forensics by Willian J. Buchanan
8. Hands-On Network Forensics by Salman Arthur

Suggested Co-Curricular Activities: NA

B.Sc.	Semester: II	Credits: 1
Course: 2	**Networking and Security Lab**	Hrs/Wk: 2

List of Experiments:

1. Operating Systems and Installation
2. Applied Computer Networking
3. Laptops and Mobile Devices
4. Network Security
5. Troubleshooting Computer Network
6. Working with Nessus and NMAP tools
7. Network packet analysis through Wireshark,
8. Configuration of intrusion detection system through Snort (Linux)
9. Experiments on Open Source SIEM tools
10. Experiments on assessing network vulnerabilities
11. Experiments on Detection of DoS/DDoS attacks

B.Sc.	Semester: III	Credits: 4
Course: 3	**Cyber Security**	Hrs/Wk: 4

Learning Objective: Cyber Security is one of the immense rising area in the world, which guide us how to defend how to protect ourselves from various kinds of cyber-attacks.

Outcomes: After studying this course the students will know-

- To Create Solutions in Incident Handling
- Demonstrate the methods and techniques, best practices to protect against variouskind of cyber- attacks.
- Describes Indian IT Act 2008
- Demonstrate CIA Traid and Security measures.
- Understand Secure Software Design and Secure Practices
- Impact of Cyber security risk in an Ethical, Social, and Professional Manner
- Compare and contrast the three basic cryptographic functions.
- Describe how cryptographic functions can be used to strengthen security of data and

UNIT I :

Need of Cyber Security- Introduction to Cyber Security -The Cyber World, Security Vulnerabilities, issues & threats, trends in cyber- attack trends, Cybersecurity Domains Overview of the Cybersecurity Domains, Examples of Cybersecurity Domains, The Growth of the Cyber Domains, Cybersecurity Criminals versus Cyber security Specialists, Cybersecurity Criminals, Who Are the Cyber Criminals? Cyber Criminal Motives, Intentions techniques, Cybersecurity Specialists, Why Become a Cybersecurity Specialist? Thwarting Cyber Criminals Digital Forensic and Cyber Crime-Understanding Cyber Crime. Indian IT Act 2008 and amendment, sections, provisions, rules and guidelines, categories of cybercrimes i.e., unauthorized access and hacking

UNIT II:

E-mail related crimes, Internet relay, chat relating crimes, sale of illegal articles, online gambling, phishing, Intellectual property crimes, web defacement, unauthorized network scanning/probing, malware related attacks, financial frauds, social media related attacks such as cyber stalking, fake news, propaganda, Computer hardware/Software: Hardware- Storage related simple problems, OCR, OMR, BAR Code, QR Codes etc., Memory Hierarchies : Basics of Semiconductor Memories, Circuits, Address Decoding, Access Time, Examples of Integrated Circuit ROMs, PROMs, EPROMs, EEPROM, Components of CPU, Register, Accumulator, Software System-application Software and their Examples in real life. Operating System and their usage. Multitasking –Multiprogramming- Multiprocessing Operating System.

UNIT III:

Foot printing & Social engineering, Information gathering methodologies, Competitive Intelligence, DNS Enumerations, Social Engineering attacks, Analysis of Deep web/ dark web analysis, investigations and case studies such as silk road, Working with Windows and DOS Systems, Understanding File Systems, Exploring Microsoft File Structures, Examining NTFS Disks, Understanding Whole Disk Encryption, Understanding the Windows Registry, Understanding Microsoft Startup Tasks, Understanding MS-DOS Startup Tasks, Understanding Virtual Machines. Examining UNIX and Linux Disk Structures and Boot Processes,

Understanding Other Disk Structures, Free space Management Bit-Vector Linked List Grouping Counting Efficiency Performance Recovery Physical Damage, Physical Damage Recovery Logical Damage, Logical Damage Recovery.

UNIT IV:

Ethical Hacking terminology, various tools & techniques to hack/compromise system/server and learning how to apply counter measures to protect against hacker attempts: Five stages of hacking, Vulnerability Research, Legal implication of hacking, Impact of hacking, System Hacking, Password cracking techniques, Key loggers, Escalating privileges, Hiding Files, Steganography, The Cybersecurity Cube, Three Dimensions of the Cybersecurity Cube, The Principles of Security, Cybersecurity Safeguards, CIA Triad, Confidentiality, The Principle of Confidentiality, Protecting Data Privacy, Controlling Access-Laws and Liability Integrity Principle of Data Integrity, Need for Data Integrity Integrity Checks, Availability, The Principle of Availability, Ensuring Availability

UNIT V:

States of Data: Data at Rest, Types of Data Storage, Challenges of Protecting, Stored Data, Data In-Transit, Methods of Transmitting Data, Challenges of Protecting, Stored Data, Data In-Transit, Methods of Transmitting Data, Challenges of Protecting Data In-Transit, Data in Process, Forms of Data Processing and Computation, Challenges of Protecting Data In- Process, Cybersecurity Countermeasures

REFERENCE BOOKS:

1. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students andPractitioners,2nd Edition, Springer's, 2010
2. Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures forEthical Hackers & IT Security Experts, Ali Jahangiri, 2009
3. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series:Computer Forensics), 2010
4. Hacking Exposed™ Computer Forensics Second Edition- Aaron Philipp David CowenChris Davis (2010)
5. http://cybercrime.planetindia.net/email_crimes.htm
6. https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/
7. https://www.upguard.com/blog/cybersecurity-important
8. Comptia Cyber Security Analyst Certification by Fernando J Mayme
9. Computer Evidence: Collection and Preservation, Second Edition Christopher L. T. Brown
10. https://www.geeksforgeeks.org/cryptography-and-its-types/
11. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Courseback) by … Michael Sikorski
12. Cryptography and Network Security by Atul Kahate
13. Cyber Security, Cyber Crime and Cyber Forensics by Raghu T. Santanam (Editor), M. Sethu madhavan (Editor)

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

B.Sc.	Semester: III	Credits: 1
Course: 3	**Cyber Security Lab**	Hrs/Wk: 2

List of Experiments:

1. Write Blocking
2. Study of HTML
3. Fake Email & other scams
4. VM Ware Installations
5. Understanding Kali linux for ethical hacking experiments
6. Key - Loggers & Key Scramblers
7. Information gathering
8. Detection of vulnerability (vulnerability assessment)
9. Testing by exploiting the vulnerability
10. Applying patches, fixing vulnerability (experiments)
11. Steganography
12. Email Tracing
13. Bit locker
14. Dumpit
15. FTK

B.Sc.	Semester: IV	Credits: 4
Course: 4	**Digital Forensics**	Hrs/Wk: 4

Learning objectives: Basic investigation techniques, requirement and analysing of digital evidences are covered.

Outcomes: After studying this course the students will know-

- The role of investigator and lab requirements in Digital Forensics.
- Data Acquisition methods, tools and storage formats of digital evidence.
- Collecting, Preserving and Seizing of various digital evidences.
- Validating and Testing of evidences using various methods.
- The techniques in developing standard methods of network forensics.

UNIT I:

Computer Forensics and Investigations: Understanding Computer Forensics, Preparing for Computer Investigations, Taking A Systematic Approach, Procedure for Corporate High- Tech Investigations, Understanding Data Recovery Workstations and Software Office and Laboratory: Understanding Forensics Lab Certification Requirements Determining the Physical Requirements for a Computer, Forensics Lab Selecting a Basic Forensic Workstation

UNIT II:

Data Acquisition: Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Contingency Planning for Image Acquisitions, Using Acquisition Tools, Validating Data Acquisition, Performing RAID Data Acquisition, Using Remote Network Acquisition Tools, Using Other Forensics Acquisition Tools

UNIT III:

Processing Crime and Incident Scenes: Identifying Digital Evidence, Collecting the Evidence in Private-Sector Incident Scenes, Processing law Enforcement Crime Scenes, preparing for a Search, Securing a Computer Incident or Crime Scene, Seizing Digital evidence at the crime Scene, Storing Digital evidence, Obtaining a Digital Hash, Current Computer Forensics Tools, Evaluating Computer Forensics Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools.

UNIT IV:

Validating and Testing Forensics Software Computer Forensics Analysis and Validation, Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisition, data carving, Recovering Graphics and Network Forensics, Recognizing a Graphics File, Understanding Data Compression, Locating and Recovering Graphics Files, live Memory forensics (RAM), Understanding Copyright Issues with Graphics, Network Forensic, social media forensics.

UNIT V:

Developing Standard Procedure for Network Forensics, Using Network Tools, Examining Honeynet Project, E-mail Investigations, Cell Phone and Mobile Device Forensics, Exploring the Role of E- mail in Investigations, Exploring the Role of Client and Server in E-mail, Investigating E-mail Crimes and Violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Understanding Mobile Device Forensics, Understanding Acquisition Procedure for Cell Phones and Mobile Devices

REFERENCE BOOKS:

1. Guide to computer forensics and investigation 3rd or 4th edition by Amelia Philips, Bill Nelsonand 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: NA

B.Sc.	Semester: IV	Credits: 1
Course: 4	**Digital Forensics Lab**	Hrs/Wk: 2

List of experiments:

1. Disk Imaging (2types)
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

B.Sc.	Semester: IV	Credits: 4
Course: 5	**Mobile Forensics**	Hrs/Wk: 4

Learning objectives: Introduction to various platforms of mobile devices and its analysis in a forensically manner.

Outcomes: After studying this course the students will know-

- Basics and important terminology of the mobile devices.
- Different types of acquisition methods on various platforms.
- Internal working structure of the various mobile platforms.
- Data recovery techniques and Data extraction techniques on various mobileplatforms.
- Different forensic tools that are used for various mobile platforms.

UNIT I:

Introduction to Mobile Forensics – I - Mobile Phone Basics**,** components Inside Mobile devices, Crimes using mobile phones, SIM Card, SIM Security, Mobile forensics, Mobile forensic & its challenges, Mobile phone evidence Extraction process. The evidence intake phase, The identification phase, The preparation phase, The isolation phase, The processing phase, The verification phase, The document and reporting phase, The presentation phase.

UNIT II:

Introduction to Mobile Forensics – II - Potential evidence stored on mobile phones - Rules of evidence, Admissible, Authentic, Complete, Reliable, and Believable. Good forensic practices- Securing the evidence, preserving the evidence, documenting the evidence, documenting all changes. Windows OS based mobile Phone Forensics- Windows Phone OS, Windows Phone file system, Data acquisition. BlackBerry Forensics- BlackBerry OS, Data acquisition, BlackBerry analysis

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 file systems on an Android device, Extended File System –EXT, File system analysis, App analysis, detection of malware activities, identification of malicious applications, live memory forensics.

UNIT IV:

Android Forensics–II: Android Forensic Setup and Pre-Data Extraction Techniques, A forensic environment setup, Screen lock bypassing techniques, Gaining root access. Android Data Extraction Techniques - Imaging an Android Phone, Data extraction techniques. Android Data Recovery Techniques, Data recovery. Android App Analysis and Overview of Forensic Tools- Android app analysis, Reverse engineering Android apps, Forensic tools overview, Cellebrite – UFED, MOBIL edit, and Autopsy

UNIT V:

Understanding the 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.

Reference Books:

1. Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma and Heather Mahalikunder Packet Publishing
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
8. https://en.wikipedia.org/wiki/List_of_Android_smartphones
9. subscription.packtpub.com/book/application_development/9781783288311/10
10. https://study.com/academy/lesson/data-extraction-techniques-for-android-devices- manual-logical-physical.html#:~:text=Gaining%20root%20access%20to%20the,%2Doff%2C%20and% 20micro%20read.

Suggested Co-Curricular Activities: NA

B.Sc.	Semester: IV	Credits: 1
Course: 5	**Mobile Forensics Lab**	Hrs/Wk: 2

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

5. BLUE PRINT OF MODEL QUESTION COURSE (Sem-End. Examinations)

MODEL QUESTION COURSE - THEORY
Semester: I
Course: ….., Title of the Course

Time: 3 Hours. Max Marks: 75

SECTION – A

Answer any 5 questions. Each question carries 5 marks **5 X 5 = 25M**
(Total 8 questions, questions 1-5 from Units 1-5 & questions 6-8 from any of the units)

1. Unit -I
2. Unit-II
3. Unit-III
4. Unit-IV
5. Unit-V
6. From any Unit
7. From any Unit
8. From any Unit

SECTION – B

Answer all the questions. Each question carries 10 marks. **5 X 10 = 50M**
(Each question (both 'A' or 'B') from each Unit.

9. A.
or
B
10. A.
or
B
11. A.
or
B
12. A.
or
B
13. A.
or

6. MODEL QUESTION COURSES FOR THEORY

MODEL QUESTION COURSE (Sem-end. Exam)

UG - DEGREE EXAMINATIONS
Semester – I
Course: Fundamentals of Computer

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following. **5X5=25M**

1. What is Computer Hardware?
2. Write about Computer organizations.
3. Write about Operating system.
4. Write about Computer Assembly.
5. Write about BIOS and UEFI Configuration
6. Define internet & intranet
7. What is Troubleshooting
8. What is ISP.

Section – B

Answer FIVE **questions.** **5X10=50M**

9. (a) Write about Internal PC Components.
(OR)
(b) Explain types of Memory.

10. (a) Explain types of Operating system.
(OR)
(b) Explain files and folders on computer

11. (a) Explain Procedures to Protect Equipment and Data.
(OR)
(b) Explain Installing and Configuring Printers.

12. (a) Explain Maintaining and Troubleshooting Printers.
(OR)
(b) Classify Computer networks and Explain.

13. (a) Explain Preventive Maintenance Tasks.
(OR)
(b) Explain Plan of Action to Resolve the Problem and Implement the Solution.

MODEL QUESTION COURSE (Sem-end. Exam)

UG - DEGREE EXAMINATIONS
Semester – II
Course :Networking and Security

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following. **5X5=25M**

1. What is Operating System?
2. Write about Routers.
3. Write about Mobile Device Synchronization.
4. Write about Security vulnerabilities.
5. Write about Cyber warfare
6. Define Network Security
7. What is IPv4?
8. What is Command Line Tool.

Section – B

Answer FIVE **questions.** **5X10=50M**

9. (a) Explain Installation of various operating systems.
   (OR)
   (b) Explain various internet protocols.

10. (a) Explain IP Addresses & IPv4 vs. IPv6.
    (OR)
    (b) Explain IDS & IPS.

11. (a) Explain Basic Troubleshooting Process for Mobile Linux.
    (OR)
    (b) Explain Laptop Hardware and Component Installation.

12. (a) Explain Denial of Service & Distributed Denial of Service (DDoS).
    (OR)
    (b) Classify network layers and explain role of each layer.

13. (a) Explain Security information and Event management.
    (OR)
    (b) Explain Troubleshooting Process to Security.

MODEL QUESTION COURSE (Sem-end. Exam)

UG - DEGREE EXAMINATIONS
Semester – III
Course : Cyber Security

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following. **5X5=25M**

1. What is Cyber Space?
2. Write about Internet relay.
3. Write about Social engineering.
4. Write about Vulnerability Research.
5. Write about Data at Rest
6. Define Cyber Security.
7. What is Principle of Data Integrity
8. What is Whole Disk Encryption.

Section – B

Answer **FIVE** questions. **5X10=50M**

9. (a) Explain Cybersecurity Criminals versus Cybersecurity Specialists.
(OR)
(b) Explain Need of Cyber Security with case any two case studies.

10. (a) Explain Memory Hierarchies.
(OR)
(b) Explain Operating System and their usage

11. (a) Explain components of Windows Registry.
(OR)
(b) Explain MS-DOS Startup Tasks.

12. (a) Explain Five stages of hacking.
(OR)
(b) Explain Cybersecurity Cube.

13. (a) Explain various States of Data.
(OR)
(b) Explain Methods of Transmitting Data.

MODEL QUESTION COURSE (Sem-end. Exam)

UG - DEGREE EXAMINATIONS
Semester – IV
Course :Digital Forensics

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following. **5X5=25M**

1. What is Cyber Forensics?
2. Write about Digital Evidence.
3. Write about Collecting the Digital Evidence.
4. Write about Network Forensics.
5. Write about Role of Client and Server in E-mail
6. Define Honeynet Project
7. What is Memory forensics
8. What is RAID.

Section – B

Answer FIVE **questions** **5X10=50M**

9 (a) Explain Certification Requirements for Digital Forensic Lab.
(OR)
(b) Explain Procedure for Corporate High-Tech Investigations.

10. (a) Explain Image Acquisitions.
(OR)
(b) Explain Network Acquisition Tools

11. (a) Explain how to obtain a Digital Hash.
(OR)
(b) Describe Computer Forensics Hardware Tools.

12. (a) Explain Copyright Issues with Graphics.
(OR)
(b) Explain process of Remote Acquisition.

13. (a) Explain Role of E-mail in Investigations.
(OR)
(b) Explain live Memory forensics (RAM).

MODEL QUESTION COURSE (Sem-end. Exam)

UG - DEGREE EXAMINATIONS
Semester – IV
Course : Mobile Forensics

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following. **5X5=25M**

1. What is a SIM Card?
2. Write about Rules of evidence
3. Write about Android models.
4. Write about Android Forensic Setup
5. Write about iPhone models
6. Define HFS
7. What is iCloud backup
8. Write about UFED.

Section – B

Answer FIVE **questions[** **5X10=50]**

9. **a)** Explain Mobile phone evidence Extraction process.

(OR)

(b) Explain components Inside Mobile devices.

10. (a) Explain Windows OS based mobile Phone Forensics.

(OR)

(b) Explain BlackBerry Forensics

11. (a) Explain the Linux kernel layer.

(OR)

(b) Explain Dalvik virtual machine.

12. (a) Explain Imaging an Android Phone.

(OR)

(b) Explain Android Data Recovery Techniques.

13. (a) Explain Internals of iOS Devices.

(OR)

(b) Explain acquisition via jail breaking.