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

UG Program (4 years Honors) Structure (CBCS)

2020-21 A. Y., onwards

BACHLOR OF SCIENCE

(3rd and 4th year detailed design will be followed as per APSCHE GUIDELINES)

Subjects/ Semesters		I		II		III		IV		V		VI			
		H/W	C	H/W	C	H/W	C	H/W	C	H/W	C	H/W	C		
Languages												THIRD PHASE of APPRENTICESHIP Entire 5th / 6th Semester		FIRST and SECOND PHASES (2 spells) of APPRENTICESHIP between 1st and 2nd year and between 2nd and 3rd year (two summer vacations).	
English		4	3	4	3	4	3								
Language (H/T/S)		4	3	4	3	4	3								
Life Skill Courses		2	2	2	2	2+2	2+2								
Skill Development Courses		2	2	2+2	2+2	2	2								
Core Papers															
M-1	C1 to C5	4+2	4+1	4+2	4+1	4+2	4+1	4+2 4+2	4+1 4+1						
M-2	C1 to C5	4+2	4+1	4+2	4+1	4+2	4+1	4+2 4+2	4+1 4+1						
M-3	C1 to C5	4+2	4+1	4+2	4+1	4+2	4+1	4+2 4+2	4+1 4+1						
M-1	SEC (C6,C7)									4+2 4+2	4+1 4+1				
M-2	SEC (C6,C7)									4+2 4+2	4+1 4+1				
M-3	SEC (C6,C7)									4+2 4+2	4+1 4+1				
Hrs/ W (Academic Credits)		30	25	32	27	32	27	36	30	36	30	0	12	4	4
Project Work															
Extension Activities (Non Academic Credits)															
NCC/NSS/Sports/Extra Curricular									2						
Yoga							1		1						
Extra Credits															
Hrs/W (Total Credits)		30	25	32	27	32	28	36	33	36	30	0	12	4	4

M= Major; C= Core; SEC: Skill Enhancement Courses

Marks & Credits distribution: UG-Sciences

Sl. No	Course type	No. of courses	Each course teaching Hrs/wk	Credit for each course	Total credits	Each course evaluation			Total marks
						Conti-Assess	Univ-exam	Total	
1	English	3	4	3	9	25	75	100	300
2	S.Lang	3	4	3	9	25	75	100	300
3	LS	4	2	2	8	0	50	50	200
4	SD	4	2	2	8	0	50	50	200
5	Core/SE -I	5+2	4+2	4+1	35	25	75+50	150	1050
	Core/SE -II	5+2	4+2	4+1	35	25	75+50	150	1050
	Core/SE -III	5+2	4+2	4+1	35	25	75+50	150	1050
6	Summer-Intern	2		4	8		100	200	200
7	Internship/ Apprentice/ on the job training	1		12	12		200	200	200
		38			**159**				**4550**
8	**Extension Activities (Non AcademicCredits)**								
	NCC/NSS/Sports/ Extra Curricular			2	2				
	Yoga	2		1	2				
	Extra Credits								
	Total	**40**			**142**				

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 /Mid Assessment	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 ForensicsLab	L	2	1		50
	5	Mobile Forensics	T	4	4	25	75
		Mobile ForensicsLab	L	2	1		50
V	6A	Cyber Law	T	4	4	25	75
		Cyber Law Lab	L	2	1		50
	7A	Advanced Cyber Forensics	T	4	4	25	75
		Advanced Cyber Forensics Lab	L	2	1		50
	OR						
	6B	Machine Learning for Digital Forensics	T	4	4	25	75
		Machine Learning for Digital Forensics Lab	L	2	1		50
	7B	Multimedia Forensics & Speaker Identification	T	4	4	25	75
		Multimedia Forensics & Speaker Identification Lab	L	2	1		50
	OR						
	6C	Social Media Forensics	T	4	4	25	75
		Social Media Forensics Lab	L	2	1		50
	7C	Network Forensics	T	4	4	25	75
		Network Forensics Lab	L	2	1		50
	OR						
	6D	Reverse Engineering & Malware Analysis	T	4	4	25	75
		Reverse Engineering & Malware Analysis Lab	L	2	1		50
	7D	Vulnerability Assessment and Penetration Testing	T	4	4	25	75
		Vulnerability Assessment and Penetration Testing Lab	L	2	1		50

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

Note 1: For Semester–V, for the domain subject **Cyber Forensics**, any one of the three pairs of SECs shall be chosen as courses 6 and 7, i.e., 6A & 7A or 6B & 7B or 6C & 7C or 6D&7D. The pair shall not be broken (ABC allotment is random, not on any priority basis).

Note 2: One of the main objectives of Skill Enhancement Courses (SEC) is to inculcate field skills related to the domain subject in students. The syllabus of SEC will be partially skill oriented. Hence, teachers shall also impart practical training to students on the field skills embedded in the syllabus citing related real field situations.

Note 3: To insert assessment methodology for Internship/ on the Job Training/Apprenticeship under the revised CBCS as per APSCHE Guidelines.

- **First internship (After 1st Year Examinations):** Community Service Project. To inculcate social responsibility and compassionate commitment among the students, the summer vacation in the intervening 1st and 2nd years of study shall be for Community Service Project (the detailed guidelines are enclosed).
- **Credit For Course: 04**

- **Second Internship (After 2nd Year Examinations):** Apprenticeship / Internship / on the job training / In-house Project / Off-site Project. To make the students employable, this shall be undertaken by the students in the intervening summer vacation between the 2nd and 3rd years (the detailed guidelines are enclosed).
- **Credit For Course: 04**

- **Third internship/Project work (6th Semester Period):**
  During the entire 6th Semester, the student shall undergo Apprenticeship / Internship / On the Job Training. This is to ensure that the students develop hands on technical skills which will be of great help in facing the world of work (the detailed guidelines are enclosed).
  Credit For Course:12

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 ChemistryOR
12th Standard (ICSE/CBSE with Science group)

c. Faculty eligibility for teaching the course:M.Sc. in Cyber Forensics with minimum 60% or abovein 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 requiredresources

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 andSolutions 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 Evidencein Private-Sector Incident Scenes, Processing law Enforcement Crime Scenes, preparing fora 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 Crimesand Violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Understanding Mobile Device Forensics, Understanding Acquisition Procedure for Cell Phones andMobile 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 processingphase, 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)

B. Sc - DEGREE EXAMINATIONS
Semester – I
Course 1: Fundamentals of Computer

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following Questions. **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 **ALL** the following 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)
B. Sc - DEGREE EXAMINATIONS
Semester – II
Course 2 :Networking and Security

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following questions. **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 **ALL** the following 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)

B. Sc - DEGREE EXAMINATIONS
Semester – III
Course 3: Cyber Security

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following Questions. **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 **ALL** the following 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)

B. Sc - DEGREE EXAMINATIONS
Semester – IV
Course 4:Digital Forensics

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following questions. **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 **ALL** the following 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)
B. Sc - DEGREE EXAMINATIONS
Semester – IV
Course 5 : Mobile Forensics

Time: 3hrs Max Marks: 75

Section – A

Answer any **FIVE** of the following Questions. **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 **ALL** the following Questions **5X10=50M**

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.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 6A	Cyber Law	Hrs/Wk: 4

Learning Outcomes:

1. Overview of Indian Legal System
2. Overview of Cyber Space
3. Information Technology Act, 2000 and its Amendments (till date)
4. Outline of Electronic Governance
5. Copyright infringements
6. Incident Response Team Development
7. Identify, Interpret and Evaluate Laws, Government Regulations and International Legal Systems Pertinent to Ecommerce
8. Explain and Evaluate Emerging Legal and Ethical Issues in Ecommerce
9. Analyze Ethical Problems That Arise in The E-Commerce Context Through the Examination of Case Studies

Syllabus: *(Total Hours: 90 including Teaching, Lab, Field Training and unit tests etc.)*

UNIT I: Cyber crimes and related offences and penalties: Introduction to Cybercrimes, Classification of cybercrimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; Spamming, Phishing, Privacy and National Security in Cyberspace, Cyber Defamation and hate speech, computer vandalism etc.
Provisions in Indian Laws in dealing with Cyber Crimes and its critical analysis, Information Technology Act, 2000, Penalties under IT Act, Offences under IT Act, Offences and Analysis related with Digital Signature and Electronic Signature under IT Act, Statutory Provisions, Establishment of Authorities under IT Act and their functions, powers. Cyber crimes under IPC.

UNIT II: Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the IT Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability– Powers of Police under the IT Act – Impact of the IT Act on other Laws .
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).

UNIT III: Cr.P.C and Indian Evidence Act - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases

UNIT IV: Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases
Patents - Understanding Patents - European Law on Computer related Patents, Legal process on Computer related Patents - Indian process Patents – Case Law, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases

UNIT V: E-commerce and related laws: History, Overview of developments in Information Technology and Defining E-Commerce, Understanding Ethical, Social and Political issues in E-Commerce: A model for Organizing the issues, Basic Ethical Concepts, Analyzing Ethical Dilemmas, Candidate Ethical principles Privacy and Information Rights: Information collected at E-Commerce Websites, The Concept of Privacy, Legal protections Intellectual Property Rights: Types of Intellectual Property protection, Governance. UNCITRAL model law in electronic commerce.

REFERENCES:

1. The Information Technology Act, 2000 Bare Act with Short Notes, Universal Law Publishing Co., New Delhi
2. Justice Yatindra Singh: Cyber Laws, Universal Law Publishing Co., New Delhi
3. Farouq Ahmed, Cyber Law in India, New Era publications, New Delhi
4. S.R.Myneni: Information Technology Law(Cyber Laws), Asia Law House, Hyderabad.
5. Chris Reed, Internet Law-Text and Materials, Cambridge University Press.
6. Pawan Duggal: Cyber Law- the Indian perspective Universal Law Publishing Co., NewDelhi
7. Elias. M. Awad, " Electronic Commerce", Prentice-Hall of India Pvt Ltd.

Co-curricular Activities:

1. Court Visit
2. Cyber Cell Visit

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 6A	Cyber Law	Hrs/Wk: 2

Cyber Law Practicals:

1. Do a case study at least 5 cyber terrorism cases.
2. Do a case study on e-commerce frauds.
3. Prepare a report for various laws of cyber crime.
4. Do a comparative analysis on Indian laws and international laws for cybercrime

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 7A	Advanced Cyber Forensics	Hrs/Wk: 4

Learning Outcomes: Overview of Windows Forensics

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 - Volatile data collection, Non-volatile data collection, 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, Classification of Cryptographic System, 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, shellbags, 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 - Types of Hypervisors, Hypervisor Files and Formats, Use and Implementation of Virtual Machines 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 and preservation, Collection of Evidence, 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.

Case Studies.

REFERENCE:

1. Window Forensic Analysis (DVD Toolkit) by Harlan Carver
2. File System Forensic Analysis by Brain Carrier
3. Windows Registry Forensics
4. Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey
5. Cryptography and Network Security: United States Edition by William Stallings
6. Cryptography: An Introduction (3rd Edition) by Nigel Smart
7. An Introduction to Cryptography
8. Cryptography and Data Security by Dorothy Elizabeth Rob, ling Denning
9. The Art of Memory Forensics (Detecting Malware and Threats in Windows, Linux, and Mac Memory) Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters
10. Advances in Memory Forensics by Fabio Pagani
11. Virtualization and Forensics A Digital Forensic Investigator's Guide to Virtual Environments by Diane Barrett
12. http://atkison.cs.ua.edu/papers/ACMSE11_JF.pdf
13. https://stars.library.ucf.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2790&context=etd
14. https://odr.chalmers.se/bitstream/20.500.12380/300023/1/CSE%2019-10%20CPL%20Andersson.pdf
15. Cloud Forensics by Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie
16. Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data Paperback by Terrence V. Lillard
17. Data Collection Techniques for Forensic Investigation in Cloud by Thankaraja Raja Sree and Somasundaram Mary Saira Bhanu
18. https://www.researchgate.net/publication/235712413_Cloud_Forensics_A_MetaStudy_of_Challenges_Approaches_and_OpenProblems
19. Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems by Vijay Prakash, Alex Williams, Lalit Garg, Claudio Savaglio and Seema Bawa. (Research Paper)

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 7A	Advanced Cyber Forensics	Hrs/Wk: 2

Advanced Cyber Forensics Practical:

1. Create a backup using icloud.
2. Create a backup using itunes.
3. Extractions of data from ibackup.
4. Recovery of data using bulk extractor.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 6B	Machine Learning for Digital Forensics	Hrs/Wk: 4

Learning Outcomes:

- Understanding the important role of machine learning
- Analyzing large amounts of diverse datasets in order to reveal any criminal behavior
- Understanding various machine learning algorithms and techniques that can be useful in the process of extracting and analyzing digital evidence

UNIT I: Introduction to Machine Learning

Brief Introduction to Machine Learning Well Posed Learning Problems, Motivation to Machine Learning, Applications of Machine Learning, Designing a Learning System, Perspective and Issues in Machine Learning, Concept Learning; Types of Machine Learning - Supervised Learning, Unsupervised Learning, Reinforcement Learning.

Applications of Machine Learning in Natural Language Processing, Image & Video Processing and Analysis, Computer Vision, Financial Data Processing and Social Network Analysis

Data analysis using machine learning for forensic expert, social media and machine learning, malware analysis using ML, HIDS, NIPS based analysis

UNIT II: Dimensionality Reduction

Subset Selection, Shrinkage Methods, Principle Components Regression; Linear Classification, Logistic Regression, Linear Discriminant Analysis; Optimization, Classification-Separating Hyperplanes Classification.

UNIT III: Supervised and Unsupervised Learning

Naïve Bayes Classification: Fitting Multivariate Bernoulli Distribution, Gaussian Distribution and Multinomial Distribution, K-Nearest Neighbors, Decision Trees.

Support Vector Machines: Hard Margin and Soft Margin, Kernels and Kernel Trick, Evaluation Measures for Classification, Ensemble Models, k-means and Hierarchical Agglomerative Clustering, Evaluation Measures for Clustering

UNIT IV: Artificial Neural Network

Artificial Neural Networks (Early models, Back Propagation, Initialization, Training & Validation), Parameter Estimation (Maximum Likelihood Estimation, Bayesian Parameter Estimation), Decision Trees, Evaluation Measures, Hypothesis Testing, Ensemble Methods,Graphical ModeL

UNIT V:Clustering

Clustering, Gaussian Mixture Models, Spectral Clustering; Ensemble Methods; Learning Theory, Reinforcement Learning

SUGGESTED READINGS:

1. Tom Mitchell, Machine Learning, TMH
2. C. Bishop, Pattern Recognition and Machine Learning, Springer
3. R. O. Duda, P. E. Hart and D. G. Stork, Pattern Classification and Scene Analysis, Wiley
4. Kishan Mehrotra, Chilukuri Mohan and Sanjay Ranka, Elements of Artificial Neural Networks, Penram International
5. Rajjan Shinghal, Pattern Recognition, Techniques and Applications, OXFORD
6. Athem Ealpaydin, Introduction to Machine Learning, PHI
7. Andries P. Engelbrecht, Computational Intelligence - An Introduction, Wiley Publication
8. Prince , Computer Vision: Models, Learning, and Inference, Cambridge University Press, Theodoridis and Koutroumbas

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 6B	Machine Learning for Digital Forensics	Hrs/Wk: 2

Machine Learning for Digital Forensics Practical:

1. Malware analysis using ML.
2. Using HIDS analysis the malware.
3. Analysis of malware using NIPS.
4. To perform image analysis using a tool.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 7B	Multimedia Forensic & Speaker Identification	Hrs/Wk: 4

Learning Outcomes:

1. Overview of Multimedia Forensic
2. Image Enhancement Techniques
3. Video Frame Analysis
4. DVR Examination
5. Voice Production Process
6. Automatic Speaker Identification System

UNIT I: Foundation to Multimedia Forensics

Introduction to digital signals: audio, image and video, Digitization process: sampling and quantization, Image Enhancement Techniques: Spatial and frequency domain, Image Compression Techniques: Introduction and techniques, Image description and representation techniques, Pattern clustering and classification.

UNIT II: Introduction to Multimedia Forensics

Introduction and scope of Multimedia Forensics, Basics of Multimedia Devices for capturing image and video, audio, Standard and best practices in Multimedia Forensics, Admissibility of multimedia evidence to the court of law along with various acts.

UNIT III: Image and Video Forensics

Introduction and scope, Standards for video transmission, Active and passive image/video forensics, Blind and non-blind image/video forensics, Methods of source camera identification, Methods for tampering of digital image/video, Forensic authentication of digital image/video, Enhancement of digital image/video, Specific Frame Analysis, Scope & it's Forensic Application in the Field of Security, DVR Examination.

UNIT IV: Audio Forensics

Introduction and scope, Analog to Digital Conversion- Sampling and Quantization, Acoustic Parameters of Sound, Fourier Analysis, Frequency and Time Domain Representation of Speech Signal, Fast Fourier Transform, Methods of tampering for digital audio, Forensic authentication of digital audio, Microphone Forensics, Enhancement of digital audio.

UNIT V: Speaker Identification

Introduction and scope of speaker identification, Human vocal tract and production and description of speech sound, Voice Production Theory, 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.

REFERENCES

1. Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T S Ho, Shujun Li
2. Multimedia Forensics and Security Foundations, Innovations, and Applications by Aboul Ella Hassanien, Mohamed Mostafa Fouad
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

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 7B	Multimedia Forensic & Speaker Identification	Hrs/Wk: 2

Multimedia Forensic & Speaker Identification Practical:

1. Collection of multimedia samples
2. Segregation of voice using Audacity.
3. Image analysis.
4. Analysis of voice.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 6C	Social Media Forensics	Hrs/Wk: 4

Learning Outcomes:

1. Overview of Social Media Forensics
2. Cyber Crimes related to social media
3. Open Street Map
4. Open-Source tools for social media analytics

UNIT I: What is Online Social Networks, data collection from social networks, challenges, opportunities, and drawbacks in online social network, Cybercrimes related to social media and its awareness, scrapping of data from social media API's.

UNIT II: Information privacy disclosure, revelation and its effects in OSM and online social networks, Privacy issues related to location-based services on OSM.

UNIT III: Tracking social footprint / identities across different social network, Identifying fraudulent entities in online social networks, Effective and usable privacy setting and policies on OSM, Policing & OSM.

UNIT IV: Detection and characterization of spam, phishing, frauds, hate crime, abuse and extremism via online social media, Data Collection & Analysis, Fake News & content on socialmedia.

UNIT V: Social Media Forensics: Case Studies Open-Source tools or social media analytics, Safety on social media. Legal Issues in world social media, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

REFERENCES:

1. Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
2. Social Network Analysis: Methods and Application by Katherine Faust and Stanley Wasserman.
3. Understanding Social Networks: Theories, Concepts by Charles Kadushin
4. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 6C	Social Media Forensics	Hrs/Wk: 2

Social Media Forensics Practical

1. Analyse the Facebook app

2. Detection of spam.

3. Data extraction using Bulk Extractor.

4. Scrapping of data from social media APIs.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 7C	Network Forensics	Hrs/Wk: 4

Learning Outcomes: Overview of networks

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

UNIT I: BASICS OF NETWORK ARCHITECTURE & INTERNET - Part 1

Network Forensics: Overview, Securing a Network, Scope, Standard Operating Procedure of Network Data, Introduction to Networks: ARPANET Protocols, Network, Need of Networks.
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: LAN, MAN, WA (with applications). Wireless Network: Wireless LAN, MAN,WAN

UNIT II: BASICS OF NETWORK ARCHITECTURE & INTERNET Part 2

Network Communication: Introduction, Types of network communication
Network Components: Twisted Pair Cable, Shielded Twisted Pair, Unshielded Twisted Pair, Unshielded Twisted Pair, Coaxial cable, Fiber Optic Cables Standard categories of cables. Network Interface Card-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, Lifi
ISO/OSI Model in Communication Networks: Features of OSI Model, Functions of layers- Physical, Data Link, Network, Transport, Session, Presentation, Application. Merits of OSI TCP/IP Reference Model: Overview, Different TCP/IP Protocols, Merits/ Demerits
Packet Routing: Packet in Internet, Processing packet at source machine, router

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: NetworkMiner, Xplico.

UNIT V: MALWARE ANALYSIS AND RANSOMWARE ANALYSIS

Introductory Malware Analysis: Malware, viruses, and worms, Importance of Malware Analysis, Essential Skills and Tools for Malware Analysis, Dependency walker, PEview, W32dasm, OllyDbg, Wireshark, Convertshell Code. Trends in Malware Evolution: Botnets, Encryption and Obfuscation, Automatic Self Updates, Metamorphic network behaviour, Blending Network Activity. Ransomware Analysis: Patterns of Ransomeware, Cruptolocker, Moscellaneous Ransomeware, RSO Cryptosystem, AES Cryptosystem, Cryptographich Techniqyes as Hacking tools, Tor Network, Digital Cash and Bitcoin.

REFERENCES:

1. Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensics analysis 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 network forensics. *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.
6. Mohanta, A., Velmurugan, K., & Hahad, M. (2018). *Preventing Ransomware: Understand, prevent, and remediate ransomware attacks*. Packt Publishing Ltd.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 7C	Network Forensics	Hrs/Wk: 2

Network Forensics Practical

1. Network capturing using Wireshark.
2. Malware detection using tools.
3. Extraction of media files from network miner.
4. Examine the working of router.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 6D	Reverse Engineering and Malware Analysis	Hrs/Wk: 4

Aim and Objectives of Course: Understanding Reverse Engineering, Typical Malware Behaviour, Working with the Payload. Also covering the Low-Level Language, Binary Obfuscation Techniques, Anti-emulation tricks, and Anti-dumping tricks.

Learning Outcomes

1. Overview of Tools like Autoruns and The Process Explorer
2. Design a payload
3. Working with Assemblers
4. Binary Obfuscation Techniques
5. Passing code execution via SHE
6. Reversing Various File Types

UNIT I: Preparing to Reverse Engineer

What is Reverse engineering, Reverse engineering as a process, Tools, The operating system environment, Typical malware behaviour: Persistence, Malware delivery, Software piracy, Payload - the evil within, Tools: Autoruns, The Process explorer.

UNIT II: The Low-Level Language

Binary numbers, x86: Registers, Memory addressing: Endianness. Basic instructions, Bitwise algebra, Control flow, Stack manipulation, Tools – builder and debugger: Popular assemblers: MASM, NASM, FASM, x86: Debuggers, WinDbg, Ollydebug, x64dbg.

Hello World: Installation of FASM, Dealing with common errors when building, Dissecting the program. After Hello: Calling APIs, Common Windows API libraries, Short list of common, API functions, Debugging

UNIT III: Static and Dynamic Reversing

Assessment and static analysis: Static analysis, File types and header analysis: Extracting useful information from file, Other information: PE executables. Deadlisting: IDA (Interactive Disassembler), Decompilers: ILSpy – C# Decompiler. Dynamic analysis, Analysis environments, Information gathering tools, Disassemblers, Debuggers, Decompilers, Network tools, Editing tools, Attack tools, Automation tools, Software forensic tools, Automated dynamic analysis, Online service sites.

UNIT IV: Sandboxing and Binary Obfuscation Techniques

Emulation of Windows and Linux under an x86 host, Analysis in unfamiliar environments: Linux ARM guest in QEMU, MBR debugging with Bochs. Binary Obfuscation Techniques: Data assembly on the stack, Encrypted data identification, Assembly of data in other memory regions,Decrypting with x86dbg, Other obfuscation techniques, Packing and Encryption: A quick review on how native executables are loaded by the OS, Packers, crypters, obfuscators, protectors and SFX, Unpacking, Dumping processes from memory, How about an executable in its unpacked state? Other file-types.

UNIT V- Anti-analysis Tricks

Anti-debugging tricks, Debugger information from NtQueryInformationProcess, Timing tricks. Passing code execution via SHE, Anti-VM tricks, Anti-emulation tricks, Anti-dumping tricks. Practical Reverse Engineering of a Windows Executable, Initial static analysis, Debugging, Reversing Various File Types: Analysis of HTML scripts, MS Office macro analysis, PDF file analysis, SWF file analysis: SWFTools, FLASM, Flare, XXXSWF, JPEXS SWF decompiler.

SUGGESTED READING:

1. Mastering Reverse Engineering, Reginald Wong
2. Practical Reverse Engineering by Bruce Dang, Alexandre Gazet, Elias Bachaalany
3. Reversing: Secrets of Reverse Engineering by Eldad Eilam
4. Implementing Reverse Engineering: The Real Practice of X86 Internals by Jitender Narula
5. Ghidra Software Reverse Engineering for Beginners: Analyze, identify, and avoid malicious code and potential threats in your networks and systems by A. P. David

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 6D	Reverse Engineering and Malware Analysis	Hrs/Wk: 2

Reverse Engineering and Malware Analysis Practical

1. Network capturing using Wireshark.
2. Analysis of HTML script.
3. Perform MS office macro analysis.
4. Do analyse the given PDF file samples.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 4
Course: 7D	Vulnerability Assessment of Application Security	Hrs/Wk: 4

Aim and Objectives of Course: Understanding Vulnerability Assessment, Differences between a bug bounty and a client-initiated pentest, Detecting SQL Injection flaws. Also covering the Extracting data using Insecure Direct Object Reference (IDOR) Flaws, Discovering Authentication methods.

Learning Outcomes

1. Working with 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: Configuring Burp Suite

Setting up proxy listeners, Working with non-proxy-aware clients, Creating target scopes in Burp Suite, Working with target, Additional browser add-ons that can be used to manage proxy Settings, Setting system-wide proxy for non-proxy-aware clients, Setting up Android and iOS to work with Burp Suite, Differences between a bug bounty and a client-initiated pentest, Why Burp Suite?: Types and features, Crawling. Why Burp Suite Scanner?: Auditor/Scanner, Understanding the insertion points. Detailed Stages of an application pentest, Features of Burp Suite.

UNIT II: Preparing for an Application Penetration Test and Identifying Vulnerabilities

Setup of vulnerable web applications, Reconnaissance, and file discovery: Using Burp for content and file discovery. Testing for authentication via Burp, Detecting SQL injection flaws, 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: Detecting and Exploiting 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: Exploiting 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 Reference (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: Writing 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. Executing the extension, Performing information gathering, Port scanning, Discovering Authentication method. Exploiting and Exfiltrating Data from a Large Shipping Corporation: Discovering Blind SQL injection: Automatic scan, SQLMap detection, Intruder detection.

SUGGESTED READING:

1. Hands-on Penetration Testing for Web Applications: Run Web Security Testing on Modern Applications 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 by Carlos A. Lozano, Dhruv Shah, et al.

B.Sc.	Semester: V (Skill Enhancement Course- Elective)	Credits: 1
Course: 7D	Vulnerability Assessment of Application Security	Hrs/Wk: 2

Vulnerability Assessment of Application Security Practical

1. Detecting STI
2. Setting up Android with Burp suit.
3. Setting up iOS with Burp suit.
4. Execute OS commands using an SQL injection.

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 6A : Cyber Law

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What are ethical, social and political issues in e-commerce.
2. Classify cyber crime.
3. Give reason for Commission of cyber crime.
4. What are the various cyber crimes under IPC.
5. Define national security in cyberspace.
6. UNCITRAL model law in e commerce.
7. What is the advantage of ecommerce.
8. Explain data protection and privacy.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) What are the various types of e-commerce frauds.

(OR)

(b) Comment on penalties under IT Act.

10. (a) What are the various provisions in Indian law dealing with cybercrimes?

(OR)

(b) Write a short note on copyright, patent & trademark.

11. (a) Write a short note on child pornography, cyber stalking, denial of service attacks, software piracy & phishing.

(OR)

(b) What are the various offenses under IT act.

12. (a) Define E-Commerce.

(OR)

(b) Comment on role of certifying authorities.

13. (a) What do you understand by cybercrime?

(OR)

(b) Write a short note on cyber terrorism.

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6

Time: 3 hrs Max. Marks: 50

1. Do a case study at least 5 cyber terrorism cases. 8 M

2. Do a case study on e-commerce frauds. 8 M

3. Prepare a report for various laws of cyber crime. 12 M

4. Do a comparative analysis on Indian laws and international laws for cybercrime. 12 M

Record + Viva-voce 6+4 = 10 M

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 7A : Advanced Cyber Forensics

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is window forensics?
2. What is cryptography?
3. What is memory forensics?
4. What is virtual machines forensic?
5. What is cloud forensics?
6. Define registry analysis.
7. Comment on history of memory forensics.
8. What are various file formats

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) What are the different types of hypervisors?

(OR)

(b) What are the procedures for collection of evidences from cloud storage services.

10. (a) Write about forensic analysis of VM files in the host system.

(OR)

(b) What is encryption and define their types

11. (a) Classify cryptographic system.

(OR)

(b) How can you collect evidences in linux and mac operating system?

12. (a) Examination and collection of data in cloud storage.

(OR)

(b) Explain about bulk extractor.

13. (a) What are the various memory forensic techniques?

(OR)

(b) How can you recover user activity?

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 7A

Time: 3 hrs Max. Marks: 50

1. Create a backup using icloud. 8 M
2. Create a backup using itunes. 8 M
3. Extractions of data from ibackup. 12 M
4. Recovery of data using bulk extractor. 12 M

Record + Viva-voce 6+4 = 10

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 6B : Machine Learning for DigitalForensics

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is machine learning?
2. What is supervised learning?
3. Define artificial neural network?
4. What do you understand by clustering?
5. What is logistic regression?
6. What are the applications of machine learning?
7. What are shrinkage methods?
8. Write about Naïve Bayes classification.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) Write about gaussian mixtures models.

(OR)

(b) What is unsupervised learning?

10. (a) Analyse the malware using ML, HIDS, NIPS.

(OR)

(b) Explain reinforcement learning.

11. (a) What are kernel and kernel trick?

(OR)

(b) What are separating hyperplane classification?

12. (a) Explain reinforcement learning.

(OR)

(b) Differentiate hard margin and soft margin.

13. (a) Write about gaussian mixtures models?

(OR)

(b) What is social networking analysis?

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6B

Time: 3 hrs Max. Marks: 50

1. Malware analysis using ML. 8 M

2. Using HIDS analyse the malware. 8 M

3. Analysis of malware using NIPS. 12 M

4. To perform image analysis using a tool. 12 M

Record + Viva-voce 6+4 = 10

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 7B : Multimedia Forensics &Speaker Identification

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is Multimedia Forensics?
2. What is Image forensics?
3. What is the Digital Signals?
4. What is Audio Forensics?
5. What is Video Forensics?
6. What are the applications of multimedia forensics?
7. What is speaker reorganization?
8. Draw the diagram of human vocal tract.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) Write about automatic speaker identification system?
   (OR)
   (b) What is image authentication

10. (a) What are the various acts for the admissibility of multimedia forensics?
    (OR)
    (b) What is passive authentication?

11. (a) What is Digital Signature & Digital Watermarking?
    (OR)
    (b)Write about automatic speaker identification system?

12. (a) Explain spatial domain and frequency domain image analysis.
    (OR)
    (b) Write about image authentication?

13. (a) Explain audio authentication?
    (OR)
    (b) Explain DSP along with sampling and quantization.

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6B

Time: 3 hrs Max. Marks: 50

1. Collection of multimedia samples 8 M
2. Segregation of voice using Audacity. 8 M
3. Image analysis. 12 M
4. Analysis of voice. 12 M

Record + Viva-voce 6+4 = 10 M

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 6C : Social Media Forensics

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is Social Media Forensics?
2. What is Online Social Network?
3. What is information privacy disclosure?
4. What is Spam?
5. What is social footprint?
6. What are various fishing frauds?
7. Discuss in detail fake news?
8. Write 3 cases studies on social media forensics.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) How can you detect spam?

(OR)

(b) Comment on cyber crimes related to social media and its awareness.

10. (a) Explain effects in OSM and online social networks.

(OR)

(b) How can you scrape data from social media?

11. (a) How can you identify fraudulent identities?

(OR)

(b) Write effective and usable privacy settings about osm?.

12. (a) How can you detect spam, phishing, hate crime, abuse and extremism via online social media?

(OR)

(b) What is Spam? Describe in detail.

13. (a) What are the various legal issues in world social media?

(OR)

(b) Write a short note on intermediary guidelines on digital media ethics code rules 2021.

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6C

Time: 3 hrs Max. Marks: 50

1. Analyse the Facebook app 8 M

2. Detection of spam. 8 M

3. Data extraction using Bulk Extractor. 12 M

4. Scrapping of data from social media APIs. 12 M

Record + Viva-voce 6+4 = 10 M

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 7C : Network Forensics

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is Network Forensics?
2. What is Arpanet?
3. What is LAN & WAN?
4. What is network capturing?
5. What is malware?
6. How can you secure network?
7. What are the types of network communication?
8. Write about Mac address, gateway & wireless access point.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) How can you create a dump file?

   (OR)

   (b) What are the importance of malware analysis.

10. (a) What is FTP analysis?

    (OR)

    (b)What is encryption and define their types?

11. (a) What are the various types of topologies comment.

    (OR)

    (b)Explain different network components.

12. (a) Write about functions of physical layer, data link layer, network layer & transport layer?

    (OR)

    (b) Explain about Wireshark tool.

13. (a) Differentiate malware viruses and WORMS.

    (OR)

    (b) Discuss in detail LAN, MAN & WAN

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6C

Time: 3 hrs Max. Marks: 50

1. Network capturing using Wireshark. 8 M

2. Malware detection using tools. 8 M

3. Extraction of media files from network miner. 12 M

4. Examine the working of router. 12 M

Record + Viva-voce 6+4 = 10 M

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 6D : Reverse Engineering &Malware Analysis

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is reverse engineering?
2. What are binary numbers?
3. What is static analysis?
4. What is Sand boxing?
5. What is malware?
6. Explain about reverse engineering tools?
7. Explain about FLASM?
8. What are various binary obfuscation techniques.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) What are anti emulation tricks?

(OR)

(b) Comments about decompiler.

10. (a) How can you reverse various file types?.

(OR)

(b) What are network tools, editing tools, attack tools, automation tools and software for accepting?

11. (a) What is common windows API library?

(OR)

(b) Explain in detail about Wireshark tool?

12. (a) Differentiate malware viruses and WORMS.

(OR)

(b) How native executables are loaded by the OS, Packers ,Crypters, Protectors and sfx.

13. (a) How can you analyse an unfamiliar environment?

(OR)

(b)What are various online service sites?

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 6D

Time: 3 hrs Max. Marks: 50

1. Network capturing using Wireshark. 8 M

2. Analysis of HTML script. 8 M

3. Perform MS office macro analysis. 12 M

4. Do analyse the given PDF file samples. 12 M

Record + Viva-voce 6+4 = 10 M

MODEL QUESTION COURSE (Sem-end. Exam)
B. Sc - DEGREE EXAMINATIONS
Semester – V (Skill Enhancement Course- Elective)
Course 7D : Vulnerability Assessmentand Penetration Testing

Time: 3hrs **Max Marks: 75**

Section – A

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

1. What is vulnerability assessment?
2. What is application security?
3. What is web application?
4. What is data exfiltration?
5. What is IDOR?
6. How to setup vulnerable web applications?
7. How can you work with non-proxy aware clients?
8. How can data exfiltration can be done.

Section – B

Answer **ALL** the following Questions **5X10=50M**

9. (a) Using what you can perform internal port scan?
   (OR)
   (b) How can you set up development environment

10. (a) What is exploiting and exfiltrating data from a large shipping corporation?
    (OR)
    (b) What is insecure direct object reference flaws?

11. (a) How can you detect broken authentication?
    (OR)
    (b) How can you set up Android to work with Burpsuit?

12. (a) Difference between a bug bounty and a client-initiated pen test open?
    (OR)
    (b)How can you take a control of users browser using XSS?

13. (a) What are various HTTP untrusted methods?
    (OR)
    (b) How can you discover blind SQL injection.

Suggested Question Paper Model for Practical Examination

Semester – V/ Course – 7D

Time: 3 hrs Max. Marks: 50

1. Detecting STI. 8 M
2. Setting up Android with Burp suit. 8 M
3. Setting up iOS with Burp suit. 12 M
4. Execute OS commands using an SQL injection. 12 M

Record + Viva-voce 6+4 = 10 M