Appendix I

Examination scheme leading to Post Graduate Diploma in Digital and Cyber Forensics and Related Law Scheme of Teaching and examination under semester pattern Credit Based system

SEMESTER-I

Sr. No.	SUBJECT CODE	Theory/Practical	Teaching Scheme (Hrs/week)				Examination Scheme					
			Theory	*Practical*	*Total*	*Credits*	*Exam Duration*	Marks Max			Minimum Passing Marks	
								External Marks	Internal Marks	*Total* Marks	Th	Pr
1	PGDC 1T1	ComputerForensics –I	4		4	4	3	80	20	100	40	
2	PGDC 1T2	Cyber Security–I	4		4	4	3	80	20	100	40	
3	PGDC 1T3	MobileForensics–I	4		4	4	3	80	20	100	40	
4	PGDC 1T4	CyberLaw–I	4		4	4	3	80	20	100	40	
5	PGDC 1P1	Practical–I		8	8	4	6	80	20	100		40
		Grand total	**20**	**32#**	**48#**	**20**	**24**	**400**	**100**	**500**	**160**	**40**

Note:**# for four batches**

1 Minimum passing marks in Theory [External +Internal] combined will be 40 %.

2 Minimum passing in Practical [External ~~&~~ Internal] combined will be 40%

Appendix II

SEMESTER-II

Sr. No.	SUBJECT CODE	Theory/Practical	Teaching Scheme (Hrs/week)				Examination Scheme					
			Theory	*Practical*	*Total*	*Credits*	*Exam Duration*	Marks Max			Minimum Passing Marks	
								External Marks	Internal Marks	*Total* Marks	Th	Pr
1	PGDC 2T1	ComputerForensics–II	4		4	4	3	80	20	100	40	
2	PGDC 2T2	Cyber Security–II	4		4	4	3	80	20	100	40	
3	PGDC 2T3	MobileForensics–II	4		4	4	3	80	20	100	40	
4	PGDC 2T4	CyberLaw–II	4		4	4	3	80	20	100	40	
5	PGDC 2P1	Project		8	8	4	6	80	20	100		40
		Grand Total	**20**	**32#**	**48#**	**20**	**24**	**400**	**100**	**500**	**160**	**40**

Note:**# for four batches**

1 Minimum passing marks in Theory [External +Internal] combined will be 40 %.

2 Minimum passing in Practical [External & Internal] combined will be 40%

DIRECTION NO. ...... OF 2022

RASHTRASANT TUKDOJI MAHARAJ NAGPUR UNIVERSITY NAGPUR

FACULTY OF SCIENCE AND TECHNOLOGY

Credit Based Semester pattern

Syllabus for Post Graduate Diploma in Digital and Cyber Forensics and Related Law

(WitheffectfromtheAcademicYear2022-23)

Appendix-IV

General Rules and Regulations

A) Pattern of Question Paper

1. There will be four units in each paper.
2. Each of the four units having equal weightage of 20 marks.
3. Question paper will consist of five questions.

   i. First four questions will be one from each unit and will carry 15 marks. Each question will have internal choice.

   ii. Fifth question will be from all four units one from each unit and will carry 5 marks

4. Maximum marks of each paper will be 80 and 20 internal.
5. Examination of Each paper will be of 3 hours duration.

B) Instructions for teaching

i. The students shall be required to participate in educational/Industrial tour during course.
ii. Each theory paper is supposed to cover minimum15 clock hours per unit) of teaching.
iii. One credit course of theory will be of one clock hour of 25 marks; hence four credit course of theory will be of four clock hours per week of 100 marks running for 15 weeks.
iv. Practical and project work will be given 4 credits each and will consist of eight hours of laboratory exercise of 100 marks running for 15 weeks.

C)Grade Point Average (GPA) and Cumulative Grade Point Average (CGPA)

On clearing a paper, based on cumulative score (out of 100) in that paper, a student will be given grade point average (GPA) (Maximum of 10 and minimum of 4) for that paper on the following basis.

Sr. No.	CGPA	Grade	%
1	9.00 -10.00	O	90 - 100%
2	8.00 to 8.99	A+	80- 89%
3	7.00 to 7.99	A	70- 79%
4	6.00 to 6.99	B+	.60- 69%
5	5.50 to 5.99	B	55- 59%
6	5.00 to 5.49	C	·50- 54%
7	4.00 to 4.99	P	40 - 49%
8	Below 4.00	F	Below 40%

On clearing all the papers in a semester, a student will be allotted a**Semester Grade Point Average (SGPA)** for that particular semester. As the pattern given above does not have differential weighs for papers, the SGPA of a student for a particular semester will be the average of the GPA's for all the papers.

3) A student will be allotted a **Cumulative Grade Point Average (CGPA)** after clearing all the two semesters. Again as there is no differentialweight system for semesters, the CGPA of a student will be the average ofthe two SGPA's of that student.
The CGPA can be converted to the usual / conventional divisions in the following way.
a. A student failed to score minimum 40% marks in each head of passing and in aggregate shall be given F grade.
b. Student with F grade in a course would be granted credit for that course but not the grade for that course.

Post Graduate Diploma in Digital and Cyber Forensics and Related Law To be implemented from Academic Year2022-2023

Scheme of Assessment

Theory

Assessment Type	Allocation ofMarks	Total Marks
Internal Assessment	1. Periodical Class Test 10Marks 2. Attendance andParticipation 05Mark 3. OverallConduct 05Marks	20 Marks
Semester End Examination	Question Paper Pattern- Each paper will have five questions. Break-up of each question shall be as follows: **Q.1 to Q.4**: One or two long questions from each unit. ……………………………… 15 Marks each. (With Internal Choice) **Q.5**: Short notes/Short answer type: a), b), c) and d) (one from each unit) ………… 05 Marks each (Compulsory, Without Internal Choice)	80 Marks
	Total	**100Marks**

Paper	Allocation ofMarks	Total Marks
V	Practical Assesment For a semester I 1. Long experiment 40 Marks 2. Short experiment 20 Marks 3. Practical Record 10 Marks 4. Viva 10 Marks 5. Internal Assessment 20 Marks	100
V	Project - (for Semester-II) 1) Project Report 60 Marks 2) Presentation 10 Marks 3) Viva-Voice 10 Marks 4) Internal 20 Marks	100

Practical

Note- Every student shall submit three copies of the project report (typed and properly bound) for the Second Semester to the University at least one month prior to the commencement of the final practical examination through the Head of the Department/ Centre / the Principal of the college concerned along with the certificate signed by the supervisor and declaration by the candidate towards original work which is not submitted to any university or organization for the award of the degree. The scheme/ guidelines for the students and supervisors regarding Project Work Report are given in Appendix.

Semester I

Course Title: Computer Forensics - I

Course Code: PGDC1T1 Semester I, Paper-I

Level: PG

Course Objective (CO): This course will cover:

- Fundamentals of Computers
- Basics of Computer Network
- Operating system overviews

Student Learning Objectives: After completion of this course student will know about

- Evolution of Computer
- Components of Computer
- Types of Memory
- Types of operating system and its functions
- Windows and Linux
- Types of network and network topologies
- OSI and TCP/IP

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC1T1: Paper I

Computer Forensics - I

Unit I: Computer Basics– I

15 Lectures

Understanding Computer Hardware: Looking Inside the Machine, Components of a Digital Computer, The Role of the Motherboard, The Roles of the Processor and Memory, The Role of Storage Media, Why This Matters to the Investigator, The Language of the Machine, Wandering through a World of Numbers, Who's on Which Base?

Understanding the Binary Numbering System: Conversion of Binary number into Decimal number, Conversion of Binary number into and Hexadecimal number, Converting Text to Binary, Encoding Non text Files, BCD, ASCII, EBCDIC encoding, Why This Matters to the Investigator?

Unit II: Computer Basics – II

15 Lectures

Understanding Computer Operating Systems: Understanding the Role of the Operating System, Multitasking, Multiprocessing, Difference Between Multitasking and Multiprocessing Operating System, Difference Between Proprietary and Open-Source Operating Systems

An Overview of Commonly Used Operating Systems: Understanding of DOS, Windows, Linux/UNIX and various Mobile Operating Systems

Understanding File Systems: FAT12, FAT16, VFAT, FAT32, NTFS and Other File Systems

Unit III: Networking Basics– I

15 Lectures

Understanding How Computers Communicate on a Network : Sending Bits and Bytes Across a Network, Digital and Analog Signaling Methods, How Multiplexing Works, Signal Interference, Packets, Segments, Datagram, and Frames, Access Control Methods.

Networking Concepts: What is a Network?, Types of Networks, Network Topologies, Networking Devices and Cables, Concept of Ports and Services, Types of IP Addresses, ISO - OSI Model, TCP/IP Model, Client Server Model.

Unit IV: Networking Basics– II

15 Lectures

Networking Protocols: ARP, RARP, ICMP, FTP, Telnet, SMTP, SNMP, HTTP, POP, etc.

Understanding Network Hardware: The Role of the NIC, the Role of the Network Media, and the Roles of Network Connectivity Devices, Why This Matters to the Investigator?

Understanding Client/Server Computing: Server Software, Client Software, Network File Systems and File Sharing Protocols, a Matter of (Networking) Protocol

Course Title: Cyber Security – I

Course Code: PGDC1T2 Semester I, Paper-II

Level: PG

Course Objective (CO): This course will cover:

- Basics of Security
- Basics of Network Security

Student Learning Objectives: After completion of this course student will know about

- Security
- Operating System Security (Windows and Linux)
- Security attacks
- Virtualization
- Foot Printing
- Google Hacking
- Steganography
- Cryptography

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC1T2: Paper II

Cyber Security– I

Unit I: Basics of Security– I 15 Lectures

Introduction to Security: What is Information Security? , Problems faced by the Corporate World, Why Corporate needs Information Security?, The CIA Triad, Hacking – Legal or Not?, Type of Ethical Hackers, Hackers vs. Crackers, Classification of Hackers, Phases of Hacking, Basic Terminologies

Virtualization: Introduction to virtualization, Advantages of Virtualization, Virtual Box, Vmware Workstation

Linux: Introduction, Installation, Basic Linux Commands, Installing Linux application

Unit II: Basics of Security – II 15 Lectures

Footprinting: Footprinting /Information Gathering, Types of Footprinting, Information Gathering Principle, Steps to Information Gathering, Domain Registry, Gathering Target Information , Parallel Domain, MX Entry, Trace Route, Archive Pages, Crawling and Mirroring of Websites ?, Banner Grabbing, Preventive techniques.

Google Hacking: Introduction to Google, Working of Google – Outline, Working of Google – Crawling, Indexing & Searching, Using Cache and Google as Proxy, Directory Listing and Locating Directory Listings along with specific folders, Google Hacking and what it is about, The basics of Google Hacking: Advanced Search in Google, Advance Search Operators: site:, filetype:, inurl:, intitle:, cache:, info:, Wildcard and Quotes, Understanding and Viewing Robots.txt for important Files, Prevention Techniques: Robot.txt, Metatag and Google Official Remove, Hiding Detailed Error Messages, Disabling Directory Browsing , Tools: Wikto, GoogleHacks

Unit III: Basic Network Security– I 15 Lectures

Scanning: Definition of Scanning, Types of Scanning, Difference between Port and Network Scanning, Objectives and Benefits of Scanning, TCP three way hands shake, Classification of scanning, Fragments, UDP, ICMP, Reverse Ident, List & Idle, RPC, Window Scan, Ping Sweep, Concept of War Dialer (History), OS Fingerprinting and Types – Active & Passive, Concealing file extensions, Anonymizers, Scanning Tools: T1Shopper.com, Yougetsignal, Advanced Port Scanner v1.3 (Radmin – Advanced Port Scanner), Whatsup Port Scanner, NetScanner, Mi-Tec Network Scanner

System Hacking: Win7 and Linux: System Hacking: Introduction to System Hacking, System Hacking Techniques, Steps to Crack Passwords, Password Attack Classification – Dictionary, Brute Force and Hybrid, LM Hash and Sam File, Password Recovery through Elcomsoft, SysKey, Hiding Files, Ophcrack, Hiren Boot, NTFS Stream Countermeasures, Password Cracking Countermeasures.

Unit IV: Basic Network Security – II 15 Lectures

Cryptography: Concept of Cryptography, Advantages and uses of Cryptography, PKI (Public Key Infrastructure), Algorithm's of encryption – RSA, MD5, SHA, SSL, PGP, SSH, GAK , Concept of Digital Signature, Encryption Cracking Techniques, Disk Encryption.

Steganography: What is Steganography?, Types of Steganography, Steganography Tools

Steganalysis: What is Steganalysis?, Types of Steganalysis, Identification of Steganographic Files

Steganalysis meets Cryptanalysis: Password Guessing, Cracking Steganography Programs

Course Title: Mobile Forensics – I

Course Code: PGDC1T3 Semester I, Paper-III

Level: PG

Course Objective (CO): This course will cover:

- Mobile Phone Basics
- Mobile Forensic
- Android Forensic

Student Learning Objectives: After completion of this course student will know about

- Basics of Mobile Phone
- Potential evidence stored on mobile phones
- Mobile phone evidence extraction process

Pedagogy: The course shall be taught in active-learning mode. incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC1T3: Paper III

Mobile Forensics – I

Unit I: Introduction to Mobile Forensics– I 15 Lectures

Mobile Phone Basics

Inside Mobile devices: Cell Phone Crimes, SIM Card, SIM Security

Mobile Forensics: Mobile Forensic and 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 documentation and reporting phase, The presentation phase

Practical mobile forensic approaches: Mobile operating system overview, Mobile forensic tool leveling system, Data acquisition methods

Unit II: Introduction to Mobile Forensics– II 15 Lectures

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 Phone Forensic: Windows Phone OS, Windows Phone file system

Unit III: Android Forensics – I 15 Lectures

The Android model: The Linux kernel layer, Libraries, Dalvik Virtual Machine, The application framework layer, the application layer

Android security: Secure kernel, the permission model, Application sandbox, Secure inter process communication, Application signing

Android file hierarchy

Android file system: Android file system analysis, Extended File System– EXT

Unit IV: Android Forensics – II 15 Lectures

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, Overview of Forensic Tools, Forensics tools overview, Cellebrite – UFED, MOBILedit, and Autopsy

Course Title: Cyber Law– I

Course Code: PGDC1T4 Semester I, Paper-IV

Level: PG

Course Objective (CO): This course will cover:

- Cyber Crimes
- Information Technology Act 2000
- Procedural Law relating to Cyber Crimes
- E - contracts, E - Banking, E - Commerce

Student Learning Objectives: After completion of this course student will know about

- Types of Cyber Crime
- Provisions in Indian Laws in dealing with cyber crime
- E - contracts, E - Banking, E - Commerce
- Cyber Crime Investigation Process
- Agencies for Cyber Crime investigation

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC1T4: Paper IV

Cyber Law– I

Unit I: Introduction to cyber crime

15 Lectures

Defining Crime
Concept of Cyber Crime
Distinction between Cyber Crimes & conventional crime
Various types of cyber crime

- Hacking
- Obscenity & Pornography
- Cyber Stalking
- Identity Theft
- Cyber Fraud
- Cyber Defamation
- Cyber Terrorism
- Breach of Confidentiality and Privacy
- Offences of/by Companies

Liability of Intermediaries including 2011 guidelines

Unit II: Regulatory Framework of Information Technology Act 2000

15 Lectures

- Evolution of the Information Technology Act 2000- Genesis and Necessity
- Salient features of the Information Technology Act 2000
- Various authorities under Information Technology Act 2000
- Offences and penalties under Information Technology Act 2000
- IT Amendment Act 2008

Unit III: E contracts, E- Banking, E-Commerce and Related Issues

15 Lectures

- **E contracts and related issues**

  Types of Electronic Contracts

  i) Employment Contracts

  ii) Consultant Agreements

Indian Law on Shrink Wrap Contracts

Drafting of Cyber Contracts

- **E-Commerce and related Issues**

  Online business

  Definition of E-commerce

  Types of E-commerce

  Important Issues in Global E-commerce

  i. Issues relating to Access (to infrastructure; to contents; universal access; Digital Divide and Universal Divide)

  ii. Trust, Privacy

  iii. Security

  iv. Consumer Protection

  v. Content Regulation; Uniformity in Legal Standards pertaining to internet

- **E-Banking and related Issues**

  Electronic Money

  Regulating e-transactions

  Role of RBI and Legal issues

  Transnational Transactions of E-Cash

  Credit Card and Internet

  Laws relating to Internet credit cards

  Secure Electronic Transactions

Unit IV: Procedural Law relating to Cyber Crimes 15 Lectures

- Investigation of Cyber Crimes
- Compoundable Offences
- Agencies for investigation in India, their powers and their constitution as per Indian Laws
- Investigation of malicious applications
- Procedures followed by First Responders
- Law of Evidence in Cyber Crimes (Electronic Evidence)
- Admissibility and relevancy of Electronic Evidence
- Search and Seizure Procedures of Digital Evidence
- Evidence issues including legal aspects of Cyber Forensics

PGDC1P1: Paper V

PRACTICAL

Max. Marks: 100

Note: Atleast 80% of the practical listed below should be completed.

1. Using Google Search in Information Collection.
2. Study of Network Related Commands (DOS)
3. Study of Network related Commands(Linux)
4. Practical based on Website Watcher and Web data Extractor tools
5. Disk Imaging, Deleted Data Recovery, Keyword Search, File Signature analysis, report generation using EnCase.
6. Disk Imaging, Deleted Data Recovery, Keyword Search, File Signature analysis, report generation using FTK.
7. Windows Log Analysis
8. Mobile/ Smart Phone Forensic (Using Mobiledit, UFED, etc.) (Any 2 tools)
9. Network Scanning tools (NMAP, AngryIP Scanner, Zenmap, etc) (Any 2 Tools)
10. Packet Sniffing using Wireshark.
11. Study of SQL Injection attacks
12. Memory Forensic using Volatility Framework.
13. Demonstration of Steganography Tools
14. Data Hiding Using Alternate Data Streams in NTFS.
15. Timeline Analysis of Computer Files based on File creation, Modification and Last Access time.
16. Password Guessing and Password Cracking.
17. Linux Log Analysis
18. Study of Wireless Network and Attacks
19. Firewall Configuration
20. Study of IDS/IPS

Semester – II

Course Title: Computer Forensics – II

Course Code: PGDC2T1 Semester II, Paper-I

Level: PG

Course Objective (CO): This course will cover:

- Computer Forensic Fundamentals
- Data Recovery
- Operating System Investigation

Student Learning Objectives: After completion of this course student will know about

- Basics of Computer Forensic
- Data Recovery
- Operating System Investigation – Windows and Unix

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC2T1: Paper I

Computer Forensics – II

Unit I: Computer Forensics Technology – I 15 Lectures

Computer Forensic Fundamentals: Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensic Services

Types of Computer Forensic Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement, Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensic Techniques

Types of Computer Forensics Systems:

Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems, Homeland Security Systems

Unit II: Computer Forensics Technology – II 15 Lectures

Data Recovery: Data Recovery Defined, Data Backup and Recovery, the Role of Backup in Data Recovery, the Data- Recovery Solution, Hiding and Recovering Hidden Data

Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options, Obstacles, Types of Evidence, the Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination, Reconstructing the Attack

Unit III: Operating System Investigation – I 15 Lectures

Window, Windows Everywhere, NTFS Overview, Forensic Analysis of NTFS MF, Metadata, Artifacts of User Activities, Deletion and Destruction of Data, Windows Internet and Communications Activities, Windows Process Memory, Bit locker and EFS, RAIDs and Dynamic Disks

Unit IV: Operating System Investigation – II 15 Lectures

Introduction to Unix, Boot Process, Forensic Duplication Consideration, File Systems, User Accounts, System Configuration, Artifacts of User Activities, Internet Communications, Firefox, Cache, Saved Sessions, E- Mail Analysis, Chat Analysis, Memory and Swap Space

Course Title: Cyber Security – II

Course Code: PGDC2T2 Semester II, Paper-II

Level: PG

Course Objective (CO): This course will cover:

- Advanced Network Security
- Database Security

Student Learning Objectives: After completion of this course student will know about

- Social Engineering
- Identity Theft
- Cross-Site Scripting
- Sniffing
- SQL Injection
- Session Hijacking
- SQL Security

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

Kapur

PGDC2T2: Paper II

Cyber Security – II

Unit I: Advanced Network Security – I 15 Lectures

Social Engineering: What is Social Engineering?, Techniques of Social Engineering: Attempt Using Phone, E-mail, Traditional Mail, In person, Dumpster Diving, Insider Accomplice, Extortion and Blackmail, Websites, Shoulder surfing, Third Person Approach, Technical Support, Computer based Social Engineering, Social Networking Sites – Impersonation platform/medium ?, Social Engineering Prevention Methods: Policies, Techniques to prevent Social Engineering Methods, Identifying Phishing Emails, Anti-Phishing Toolbar

Identity Theft: Introduction of Identity Theft, Identity Theft Occurrence, Impact of Identity Theft Fraud, Types of Identity Theft, Dumpster Diving, Change of ID, E-Mail Theft, Smishing, Vishing, Data Breach, Overlays, ATM Schemers / Hand-held Skimmers, Shoulder Surfing, Preventive Techniques

Unit II: Advanced Network Security – II 15 Lectures

Cross Site Scripting: Introduction Cross Site Scripting, Ways of Launching Cross-Site Scripting Attacks, Working Process of Cross-Site Scripting Attacks, When.will be an attack successful, Programming Languages Utilized in XSS Attacks, Types of XSS Attacks, Steps of XSS Attack, Not Fixing CSS/XSS Holes Compromises, Methodology of XSS, How to protect Against XSS

Sniffing: Sniffing Concepts, Sniffing Threats in Network, Working of Sniffers, Types of Sniffing, Protocols Vulnerable for Sniffing, Sniffing Tools: Wireshark, Tcpdump, Cain & able, NwInvestigator, Sniffing Prevention Techniques: Wiretapping , Hardware Protocol Analyzers, Port mirroring, MAC Flooding

Unit III: Database and Other Security – I 15 Lectures

SQL Injection Concepts:

Basics of SQL, Web Application Working, Introduction to Server Side Technologies, HTTP GET and POST Method Basics

Testing for SQL Injection: Identifying SQL Injection, Techniques to identify SQL Injection, Pentesting methodologies for SQL Injection

Types of SQL Injection:

Types of SQL Injection, Simple SQL Injection Attack, Union SQL Injection Example, SQL Injection Error Based ?

Blind SQL Injection: What is Blind SQL Injection?, Symptoms of Blind SQL Injection, Information extraction via Blind SQL injection, Exploitation techniques (MySQL)

SQL Injection Tools: BSQL Hacker, Marathon Tool, SQL Power Injector, Havij, SQLPoizon

Preventive measures for SQL Injection

Unit IV: Database and Other Security – II 15 Lectures

DDoS: Concept: Denial of Service, Working of Distributed Denial of Service Attacks, Symptoms of a DoS Attack, Impact DDoS/DoS Attack, Difference of DDoS & DoS, DoS / DDoS Attack Techniques, Types of DOS Attack, Smurf Attack, Buffer Overflow Attack, Ping of Death Attack, Tear Drop Attack, SYN Attack, Concept of Reflected DOS, Permanent Denial of Service Attack, Mitigate the DoS / DDoS Attack

Botnets: Introduction to Botnet, Botnet Propagation Technique, Detection Techniques, How to defend against Botnet

Session Hijacking: What is Session Hijacking?, Types of Session Hijacking , Techniques for Session Hijacking, Phases of Session Hijacking: Tracking the session, Desynchronizing the connection, Session Sniffing, Predictable Session Token, Difference between Spoofing and Session Hijacking, Session Hijacking Tools, Prevention Methods

Course Title: Mobile Forensics – II

Course Code: PGDC2T3 Semester II, Paper-III

Level: PG

Course Objective (CO): This course will cover:

- iOS Forensics
- Mobile Malware Analysis

Student Learning Objectives: After completion of this course student will know about

- Difference between Android and iOS
- iOS Data Analysis and Recovery
- Analyzing Mobile Malware

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC2T3: Paper III

Mobile Forensics – II

Unit I: iOS Forensics – I 15 Lectures

Understanding the Internet of iOS Devices: iPhone models, iPhone hardware, iPad models, iPad hardware, File system, The HFS plus file system, Disk layout, iPhone operating system

Data Acquisition from iOS Devices: Operating modes of iOS devices, Physical acquisition

Difference between Android and iOS

Unit II: iOS Forensics – II 15 Lectures

iOS Data Analysis and Recovery : Timestamps, SQLite databases, Property lists, Other important files, Recovering deleted SQLite records

Overview of iOS Forensic Tools and its features : Elcomsoft iOS Forensic Toolkit, Oxygen Forensic Suite 2014, Cellebrite UFED Physical Analyzer, Paraben iRecovery Stick

Unit III: Mobile Malware Analysis – I 15 Lectures

Introduction to Mobile Malware, Types of Mobile Malware, Taxonomy of Mobile Malware, APK file structure.

Phishing, Smishing, Vishing, Mobile Sandbox.

Steps you can take to protect yourself

Unit IV: Mobile Malware Analysis – II 15 Lectures

Android Malware Threats, Hoaxes, and Taxonomy

Analyzing Mobile Malware : Learning about Dynamic Analysis, Static Analysis, Android app analysis, Analysis Technique, Android manifest, intents, services, API calls and permissions, Reverse engineering Android apps

Overview of App Analysis tools: apktool, androguard, dex2jar, MobSF etc.

Course Title: Cyber Law– II

Course Code: PGDC2T4 Semester II, Paper-IV

Level: PG

Course Objective (CO): This course will cover:

- Intellectual Property Rights in Digital Medium
- Emerging Trends in Cyber Space

Student Learning Objectives: After completion of this course student will know about

- IPR International Organizations and Their Roles
- Domain Names and Trademark Disputes
- Concept of Copyright and Patent in Cyberspace
- Trademarks in Cyber Space
- Quantum Computing, Artificial Intelligence, IOT (Internet of things). BIGDATA, Block chain technology

Pedagogy: The course shall be taught in active-learning mode, incorporating lectures along with relevant case studies and sections, with the help of chalk and board method, PowerPoint presentations, e-lectures, case study method, general discussions, MOOCs, demonstrations and interactions.

PGDC2T4: Paper IV

Cyber Law– II

Unit I: Introduction to Intellectual Property Rights 15 Lectures

- Concept of Property vis-à-vis Intellectual Property
- Types of Intellectual Property
- Origin and Development- An Overview
- Intellectual Property Rights as Human Right
- Role of International organizations- WTO, TRIPS, WIPO, ICANN, UDRP etc.

Unit II: Copyright and Information Technology 15 Lectures

- Copyright issue in cyber space
- Software – Copyrights vs. Patents debate
- Authorship and Assignment Issues
- Commissioned Work and Work for Hire
- Idea/Expression dichotomy
- Copyright in Internet
- Jurisdiction Issues and Copyright
- Infringement and Remedies
- Multimedia and Copyright issues
- Software Piracy

Unit III: Trademarks and Patents in Cyber Space 15 Lectures

Trademark issues in cyberspace

- Understanding Trademarks
- Trademark Law in India
- Infringement and Passing Off
- Domain name registration
- Domain Name Disputes & WIPO

Patent issues in cyberspace

- Understanding Patents
- European Position on Computer related Patents
- Legal position of U.S. on Computer related Patents
- Indian Position on Computer related Patents
- SEP and FRAND

Unit IV: Emerging and Contemporary issues in Cyber Space 15 Lectures

- Data Protection- data privacy :emerging technologies
- Quantum Computing
- Artificial Intelligence
- IOT (Internet of things)
- BIGDATA
- Block chain technology

- GDPR, HIPAA and proposed PDPA 2018

PGDC2P1: Paper V

PROJECT WORK

Max. Marks: 100

The student in consultation with their project guide/project supervisor shall do the literature search/literature review/pilot study/preliminary work on a topic related to the syllabus mutually decided by them/allotted to them. The following aspects shall be covered before finalizing the topic by the project guide/supervisor:

Introduction to Research, Identification and criteria of selecting a research problem, Formulation of objectives, research plan and its components, Literature Search, Literature review, Sampling procedure. Plagiarism- Types, steps to avoid plagiarism, plagiarism detection tools and Referencing styles.

The student is expected to carry out the detailed sample analysis/experimental work/ Critical analysis/ Analytical study/ exploratory research/comparative study/Critical review/Comprehensive review.

The evaluation of the student will be carried out jointly by internal and the external examiner during the project work examination.

The evaluation shall be based upon the following parameters:

Report	*: 60 Marks*
Presentation	*: 10 Marks*
Viva-voce	*: 10 Marks*
Internal Assessment	*: 20 Marks*

Every student is required to carry out Project Work on a related research topic of the subject /course. It must be an original work. On the basis of this work, student must submit the Project Report (typed and properly bound) in two copies at least one month prior to commencement of the final Practical Examination of Semester II along with the declaration by the candidate that the work is original and not submitted to any University or Organization for award of the degree and certified by the supervisor and forwarded through Head of the Department/Course-coordinator/Director of the Institute or the Principal of the College.

Reference and Text Books:

PGDC1T1: Computer Forensics –I
PGDC2T1: Computer Forensics - II

Sr. No.	Suggested Readings
1	Computer Forensics – Computer Crime Scene Investigation, Second Edition, John R. Vacca, Charles River Media Inc., ISBN 1-58450-389-0
2	Scene of the Cybercrime – Computer Forensics Handbook, Debra Littlejohn Shinder, Ed Tittel, Syngress Publishing Inc., 2002, ISBN 1-931836-65-5
3	Handbook of Digital Forensics and Investigation, Edited by Eoghan Casay, Elsevier Academic Press, ISBN 13 : 978-0-12-374267-4

Sr. No.	Additional Suggested Readings
1	Computer Forensics for Dummies
2	Cyber Crime Investigations by Anthony Ryes
3	Computer Forensics : A Field Manual for Cancelling, Examining, and Preserving Evidence of Computer Crimes by Albert J. Marcella
4	Cyber Crime Investigator's Field Guide by Bruce Middleton
5	Digital Forensics : Digital Evidence in Criminal Investigation by Angus M. Marshall
6	Digital Forensics for Network, Internet and Cloud Computing by Clint P. Garrison
7	A Practical Guide to Computer Forensics Investigations by Dr. Darren R. Heyes

PGDC1T2: Cyber Security– I
PGDC2T2: Cyber Security - II

Sr. No.	Suggested Readings
1	Certified Information (Security Expert, Main Book, Innobuss Knowledge Solutions (P) Ltd.

Sr. No.	Additional Suggested Readings
1	Certified Ethical Hacker Manual
2	www.hackthissite.org

PGDC1T3: Mobile Forensics– I

PGDC2T3: Mobile Forensics - II

Sr. No.	Suggested Readings
1	Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd., 2014,ISBN 978-1-78328-831-1
2	Learning iOS Forensics, Mattia Epifani, Pasquale Stirparo,Packt Publishing Ltd, 2015 ISBN 978-1-78355-351-8
3	Guide to Computer Forensics and Investigations, Fourth Edition, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning,2010,ISBN-13: 978-1-435-49883-9 ,ISBN-10: 1-435-49883-6
4	Wireless Crime and Forensic Investigation, Gregory Kipper,Auerbach Publications
5	Mobile Malware Attacks and Defense, Ken Dunham, Syngress Publishing, Inc.,ISBN 978-1-59749-298-0

Sr. No.	Additional Suggested Readings
1	Digital Evidence and Computer Crime, Third Edition Eoghan Casey.Published by Elsevier Inc
2	Andriod Forensic, Investigation, and Security by Andrew Hogg, Publisher Synergy
3	iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempka ,Publisher Synergy
4	Mobile phone security and forensics: A practical approach *by* Iosif I. Androulidakis, Springer publications, 2012
5	The basics of digital forensics : the primer for getting started in digital forensics, John Sammons., Syngress publisher ,2012

PGDC1T4: Cyber Law– I

PGD2T4: Cyber Law – II

Sr. No.	Suggested Readings
1	Cyber Law in India by Farooq Ahmad- Pioneer Books
2	Information Technology Law and Practice by Vakul Sharma- Universal Law Publishing Co. Pvt. Ltd.
3	The Indian Cyber Law by Suresh T. Vishwanathan- Bharat Law House New Delhi
4	Guide to Cyber and E- Commerce Laws by P.M. Bukshi and R.K. Suri- Bharat Law House, New Delhi

5	Guide to Cyber Laws by Rodney D. Ryder- Wadhwa and Company, Nagpur
6	The Information technology Act, 2000- Bare Act- Professional Book Publishers, New Delhi.
7	Computer Crime and Computer Forensics by Dr. R. K. Tewari, P. K. Sastry, K. V. Ravikumar – Select publisher
8	Cyber Laws and Crimes by barkha and V Rama Mohan- Asia Law House 3 rd edition
9	Cyber Laws and IT Protection by Harish Chander