Ch. Charan Singh University, Meerut

Proceedings

Of

Board of Studies (Law) held on

20 July, 2022

Course Curriculum
of
Post Graduate Diploma
In
Cyber Crime and Laws
(PGD-CCL)

Ch. Charan Singh University Meerut

Board of Studies in Subject-Law

A meeting of the Board of Studies university campus and affiliated colleges (Law) is scheduled on 20.07.2022 at 5:00 P.M. online at Zoom App.

The following are the member of the meeting:

1. Dr. Anjali Mittal (Dean), CCS University, Meerut
2. Dr. I.M. Khan (Convener), Head, Associate Professor, NREC College, Khurja
3. Sh. K.K. Gupta (Member), Associate Professor, Meerut College, Meerut
4. Dr. Vaishali Gupta (Member), Associate Professor, NREC College, Khurja
5. Dr. Reema Agarwal (Member), Associate Professor, MMH College, Ghaziabad
6. Dr. Kameshwar Prasad (Member), Associate Professor, Meerut College, Meerut
7. Prof. SC Gupta (Member), HNB Garhwal University (Pauri Campus)
8. Prof. KPS Mahalwar (Member), (Retd.), M.D.University, Rohtak
9. Prof. RK Gupta (Member), (Retd.), Kurushetra University, Kurushetra
10. Prof. AS Bhatnagar (Member), (Retd), Principal, VSSD College, Kanpur
11. Prof. SS Jaswal (Member), NLU Shimla
12. Dr. Vivek Kumar Special invitee (Coordinator) Institute of legal studies, CCS University (Campus), Meerut.
13. Dr. Anurag Singh, Special invitee, Meerut College, Meerut.

Dr. I.M. Khan(Convener)

Board of Studies (University Campus and Affiliated Colleges) (Law)
Resolution

A meeting of the Board of Studies in law convened today on 20.07.2022 at 5:00 P.M. online at Zoom App. The following resolution has been passed unanimously that –

1. A one-year P.G. Diploma in Cyber Crime and Laws will be commenced from the academic session 2022-23.
2. The Syllabus and Ordinance of P.G. Diploma in Cyber Crime and Laws is attached herewith.
3. The teaching faculty and fee structure for the P.G. Diploma in Cyber Crime and Laws shall be in accordance with the Ch. Charan Singh University norms.

Dr. Anjali Mittal Dean	Dr. I.M. Khan Convener	K.K. Gupta Member	Dr. Vaishali Gupta Member
Dr. Reema Agarwal Member	Dr. Kameshwar Prasad Member	Prof. SC Gupta Member	Prof. KPS Mahalwar Member
Prof. RK Gupta Member	Prof. AS Bhatnagar Member	Prof. SS Jaswal Member	Dr. Vivek Kumar Special Invitee

Dr. Anurag Singh
Special Invitee

CONTENTS

----------x----------x----------x----------

Post Graduate Diploma in Cyber Crime and Laws

(One Year Programme)

OVERVIEW OF THE COURSE:

With the development of communication and information technology, the invention of Computer and internet has huge contribution for the growth of humans and made their life easier. It is being using for various purposes starting from the individual to large organizations across the globe. Internet is a virtual medium of information and communication which has no boundaries, no geographical mass, or gravity.

Frequently use of internet and cyber activities gave birth to **"Cyber Crime"**. Cyber-crimes are illegal acts where the computer is used either as a tool or a target or both. The massive growth in electronic commerce (e-commerce) and online trading has led to an unusual erupt in incidents of Cyber-crime. We can define Cyber-crime as the criminal activities committed using computers or computer network and are usually take place over the Cyberspace.

"Cyberspace" is a very broad term and includes computers, networks, software, and data storage devices such as hard disks, USB, Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. The increased dependence of individuals and organizations on cyberspace has resulted in many illegal activities which are known as Cyber-Crimes. This cyberspace is controlled, governed and regulated by the "Cyber Laws".

"Cyber Laws" play a very important role in this new epoch of technology and take control over the crimes committed through the internet or the cyberspace or through the uses of computer resources. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law. We can define "Cyber law" as the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e., the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world.

Along with the progression in technology it is similarly important to be aware of cyber-crime and other related issues thereof. The cyber safety depends on the knowledge of the technology and the care taken while using internet and that of the defensive measures adopted by user and servers' systems. Cyber law portrays the legal issues associated with the use of communications technology, mainly "cyberspace", i.e., the Internet. Cyber law basically deals with almost all aspects of transaction and activities concerning Internet, World Wide Web and Cyberspace. It is well known that each action and each reaction in Cyberspace has some legal and Cyber legal views.

OBJECTIVES OF THE COURSE:

The course enables the scholars to get a vibrant knowledge about the Cyber Crime and Cyber Laws with the following objectives:

1. The manner in which the crime is committed in the cyber world.

2. To enable the scholars to evaluate and interpret the case laws with depth knowledge of IT Act and other Laws associated with the cyberspace.

3. The method and way in which these crimes are being investigated.

4. Evidence collection, handling and examination of the evidences.

5. Presenting the facts and findings of the Cyber Crime case.

6. To identify the emerging challenges in cyberspace in today's scenario.

7. To provide the knowledge of legal frame work of and Intellectual Property issues, Right to Privacy, Data Security and Data Protection.

8. To provide fundamental knowledge of Information Technology and computer structural design of its hardware, software and networking to understand various aspect of working of a computer in cyberspace.

9. To provide the knowledge and awareness of relationship between E-commerce and cyberspace.

10. To provide and cover the special tools and technology in-order to prevent and protect from different types of Cyber-attacks.

EMPLOYMENT OPPORTUNITIES:

In the present era of digitization the Cyber experts and professionals are in huge demand in Communication and Information Technology to prevent, protect and resolve the cyber crimes in public and private organizations as well as in various departments of government i.e.

1. Police;
2. Revenue;
3. Law firms;
4. Armed forces;
5. Corporate Sectors;
6. Educational Institutions;
7. RAW and Intelligence units;
8. Banks and financial institutions;
9. Electronic and print media houses and
10. In many other fields of different organizations.

DURATION OF THE COURSE:

The total duration of the course shall be **One Year**. There will be **2 Semesters** of six months each in an Academic Session.

Semester – I (July to December)

Semester – II (January to June)

Ordinances for P.G. Diploma in Cyber Crime & Laws

Admissions: -

1 The P.G. Diploma in Cyber Crime and Laws course in the university and Law colleges is a self-finance course with intake of 40 seats.

2 P.G. Diploma in Cyber Crime & Cyber Laws programme in the campus of the university and law colleges is a full-time programme consisting of two semesters spread over one academic year.

3 Every candidate, who has passed graduate exam in any stream from a recognized university with at least 45% of marks, shall be eligible for admission to P.G. Diploma in Cyber Crime and Laws programme.

4 The admission shall be given either on the basis of merit prepared in accordance with the marks secured by a candidate in qualifying courses or the merit position secured in entrance examination conducted by the university.

5 The rules of reservation will apply in admission as per rules made by state Government time to time.

6 Students selected for admission, shall be required to take admission by the last date given to them for admission. After that their place shall be allotted to the next waiting candidate.

7 At the time of admission following documents would be required in original for verification along with photostat copies to be deposited by the candidate seeking admission.

i. Marks Sheet of graduation degree or provisional degree and all other previous marks sheets.
ii. Caste certificate is case of reserved categories.
iii. Character certificate not more than six months old.
iv. Transfer Certificate from the last attended institution.
v. Migration Certificate (For candidates from other universities)
vi. In case of employed persons, a no objection certificate from the employer as well as an affidavit by the candidate that he will fulfill the required attendance shall be necessary.

8 If there are two or more candidates with the same marks/rank in the combined entrance test/merit list. Admission will be made on the following basis:

1 The candidate securing higher marks in the graduation will be preferred for admission.
2 If two or more candidates have the same marks in the graduation degree examinations, the older in age shall be preferred.

NOTE: - ALL ADMISSIONS ARE PROVISIONAL SUBJECT TO VERIFICATION OF DOCUMENTS ON THE BASIS OF WHICH ADMISSION IS SOUGHT. NO PERSON CAN CLAIM ADMISSIONS AS A MATTER OF RIGHT, WHICH CAN BE REFUSED AT THE DISCRETION OF THE CONCERNED AITHORITY WITHOUT ASSIGNING ANY REASON.

Course of study: -

This is a two semester, Ten papers course with Project and Dissertation.

Examination: -

No student shall be eligible to appear in the exam if he/she fails to put in 75% in attendance.

Evaluation:

It will be treated as P.G. course for the purpose of evaluation and Remuneration.

Rules for Promotion: -

1 P.G. Diploma in Cyber Crime and Laws is a one-year course & a student is required to complete his diploma within a maximum time of two year from the date of admission.

2 A student can appear for back paper only in two papers / courses. However, a student failing in more than two papers will have to appear in the corresponding semester as an ex-student in all the papers, which he has failed.

3 No candidate shall be considered to have passed in any paper in P.G. Diploma in Cyber Crime and Laws unless he/she has secured at least 40% in each individual course and 50% in aggregate of all the courses.

4 There shall be First Division on securing 60% marks and second Division on securing above 50% and below 60 of marks.

5 At the time of completion of diploma, a student shall be given a grace of three (03) marks either to pass an individual paper or in making up the aggregate or for the attainment of first division.

Semester - 1

At the end of First Semester-

1. Theory Exam: There shall be 4 written exams of 100 marks each.
2. Assignment, Presentation and Viva-Voce: 100 marks.

Paper No	Paper Name	Code	Max. Marks
Paper – I	Cyber Crimes and Torts	**DL-1001**	100
Paper – II	Laws relating to Information Technology for Cyberspace	**DL-1002**	100
Paper – III	Basics of Computers and System Architecture	**DL-1003**	100
Paper – IV	Laws relating to E-Commerce and Cyberspace	**DL-1004**	100
Paper – V	Assignment, Presentation and Viva-Voce	**DL-1005**	100
	Total		**500**

Semester - 2

At the end of Second Semester-

1. Theory Exam: There shall be 4 written exams of 100 marks each.
2. Project Work and Viva-Voce: 100 marks.

Paper No	Paper Name	Code	Max. Marks
Paper – I	Intellectual Property Rights and Protection in Cyberspace	**DL-2001**	100
Paper – II	Computer Networking and Security	**DL-2002**	100
Paper – III	Cloud and Virtual Technology	**DL-2003**	100
Paper – IV	Mobile and Digital Forensics	**DL-2004**	100
Paper – V	Project Work and Viva-Voce	**DL-2005**	100
	Total		**500**

The pass-marks shall be 40% in each paper and 50% in the aggregate of all the papers prescribed for the First and Second Semesters. First Division will

be assigned at 60% marks and above and Second Division on securing above 50% and below 60% of marks.

FIRST SEMESTER

SYLLABUS

Semester – 1

Post Graduate Diploma in Cyber Crime and Laws

Paper – I: Cyber Crimes and Torts
Code - DL- 1001

Unit – I:

Cyber Crime – History, overview and evolution of Cyber Crime, Identifying thief, Phishing etc. different types of cyber-attacks i.e., DNS attack, SQL attacks, etc., Cyber warfare, Banking Malware, Phone hijacking, Android hack etc.

Unit – II:

Classifications of Cyber Crime:

Cyber Crime against individuals – Email spoofing, Spamming, Cyber defamation, IRC Crime (Internet Relay Chat), Net extortion, Hacking, Indecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc.

Cybercrime against organization – Unauthorized access of computer, Password Sniffing, Denial-of-service (DOS) attack, Backdoors and Malwares and its types, E-mail Bombing, Salami Attack, Software Piracy, Industrial Espionage, Intruder attacks. Security policies violations, Crimes related to social media, ATM, Online and Banking Frauds. Intellectual Property Frauds. Cyber Crimes against Women and Children.

Unit – III:

A global perspective on cybercrimes, Phases of cyber-attack– Reconnaissance, Passive Attacks, Active Attacks, Scanning, Gaining Access, Maintaining Access, Lateral movement and Covering Tracks. Detection Avoidance, Types of Attack vectors, Zero-day attack, Overview of Network based attacks.

Unit – IV:

Cyber Crime and cloud computing, Different types of tools used in cybercrime, Password Cracking – Online attacks, Offline attacks, Remote attacks, Random Passwords, Strong and weak passwords. Viruses and its types. Ransomware and Cryptocurrencies. DoS and DDoS attacks and their types. Cybercriminal syndicates and nation state groups.

Recommended Book:

1. "All in One CISSP", Shon Harris , McGraw Hill.

2. "Cybercrime and Society", Majid Yar, Sage Publications.

3. "Cyber Crime: Issues, Threats and Management", Atul Jain.

4. "Principles of Information Security", Michael E Whiteman and Herbert J Mattord; Vikas Publishing House, New Delhi.

5. "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Nina Godbole and Sunit Belapore, Wiley Publications.

Semester – 1

Post Graduate Diploma in Cyber Crime and Laws

Paper – II: Laws relating to Information Technology and Cyberspace
Code: - DL- 1002

Unit - I: Introduction to Cyberspace, Cybercrime and Cyber Law

The World Wide Web, Web Centric Business, e-Business Architecture, Models of e-Business, e-Commerce, Threats to virtual world., Applicability, Non-applicability, Definitions, Amendments and Limitations. Cyber Crimes- Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Social Media-Online Safety for women and children, Misuse of Private information.

Unit - II: Regulatory Framework of IT Act 2000

Information Technology Act 2000, Digital Signature, E-Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. (Rules announced under the Act), Network and Network Security, Access and Unauthorized Access, Data Security, E Contracts and E Forms.

Unit - III: Offences and Penalties

Information Technology (Amendment) Act 2008 – Objective, Applicability and Jurisdiction; Various cyber-crimes under Sections 43 (a) to (j), 43A, 65, 66, 66A to 66F, 67, 67A, 67B, 70, 70A, 70B, 80 etc. along with respective penalties, punishment and fines, Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Unit - IV: Indian Evidence Act

Classification – civil, criminal cases. Essential elements of criminal law. Constitution and hierarchy of criminal courts. Criminal Procedure Code. Cognizable and non-cognizable offences. Bailable and non-bailable offences. Sentences which the court of Chief Judicial Magistrate may pass. Indian Evidence Act – Evidence and rules of relevancy in brief. Expert witness. Cross examination and re-examination of witnesses. Sections 32, 45, 46, 47, 57, 58, 60, 73, 135, 136, 137, 138, 141. Section 293 in the code of criminal procedure. Secondary Evidence- Section 65-B.

Recommended Book:

1. The Patent Act, 1970.
2. The Copyright Act, 1957.
3. The Indian Evidence Act, 1872.
4. "Cyber Law – The Indian Perspective", Pavan Duggal; Saakshar Law Publications.
5. "Computers, Internet and New Technology Laws", Karnika Seth, Lexis Nexis Buttersworth Wadhwa.

Semester – 1

Post Graduate Diploma in Cyber Crime and Laws

Paper – III: Basics of Computers and System Architecture
Code: - DL- 1003

Unit – I: Basics of Computers

Overview and working of computers, Generation and Classification of computers, Basics of computer hardware and software, Booting process in a computer, Computer memory and its classification, other peripherals devices and cards.

Unit – II: Understanding computer Architecture

System Architecture – Multitasking, Multiprocessing, Multiprogramming, Processor. Digital Architecture of CPU – Input Unit, Output Unit and Storage Unit. Number System – Binary, Decimal, Octal and Hexadecimal. ASCII codes. Types of Storage Media – Hard Drive, SSD, Optical Devices, Holographic Storage, Smart cards. File Systems- Types and components.

Unit – III: Basics of Operating System

Introduction- Operating system and Function, Batch, Interactive, Time-sharing and Real-Time systems, CPU Scheduling – Scheduling concept, algorithms and Performance criteria, memory management. File sharing, File System Implementation. Overview of Linux Operating System.

Unit – IV: Basics of Networking

Basic Computer Network Components – Server, client, routers, Shared Printers and other peripherals, Network Interface Card. Network Devices – hubs, Switches, routers, repeaters. OSI model and TCP/IP model. Basic HTTP, World Wide Web, Web Browsers, Web Servers, Domain Names, URL and DNS. IP addressing – types and classes. Types of Networks – LAN, MAN and WAN. Working of Wi-Fi and Bluetooth. Overview of cloud computing.

Recommended Book:

1. "Computer Fundamentals", Anita Goel; Pearson Publications.
2. "Modern Operating Systems", Andrew S.Tanenbaum; Addison Wesley.
3. "Computer Architecture and Organization", John P.Hayes; McGraw-Hill.
4. "Data Communication and Networking", Beherouz. A Forouzan; TMH.
5. "Fundamentals of Computers", V. Rajaraman and Niharika Adabala; PHI Learning Pvt. Ltd.

Semester – 1

Post Graduate Diploma in Cyber Crime and Laws

Paper – IV: Laws relating to E-Commerce and Cyberspace
Code: - DL- 1004

Unit – I: Introduction to International Standards and Audit Methodology

Audit Life Cycle Initiation – Commencement, Discovery Stage, Maturation Stage, Predictive Stage. PDCA – Cycle Plan, Do, Check, Act. Types of Audit - Internal, External - Mandatory and – Statutory. ISMS 27001 ISO Standards. SOX and HIPPA– International Compliance – Introduction and Applicability. Oversight and Introduction. Common Risk Infrastructure.

Unit – II: Risk Management

Introduction. Method and Principles. Classes or Types of Risk. Process, Mitigation - Potential risk treatments - Risk management plan. Limitation, Implementation,. Types of risk management for projects-For natural disasters of information technology - In petroleum and natural gas. Business Continuity and Planning

Unit – III: Financial Fraud

Investigate allegations of fraud. Investigate internal & external theft. Investigate allegations of bribes & kickbacks, Investigate inventory theft. Company Backgrounds, Due Diligence, Economic Espionage, Financial Fraud, Mergers/Acquisitions. Structured Data Forensics of Financial Records.

Unit – IV: Analysis, Evidence and Testimony

Review internal controls to safeguard assets, Conduct small business asset protection survey & make recommendations for preserving company assets. Fraud auditing services. Uncover financial statement fraud. Conduct white-collar crime investigations. Asset record reconstruction. Provide anti-money laundering and/or fraud training. Consult on civil and/or criminal litigation matters, including asset forfeiture issues. Assist legal counsel with plea negotiations involving drug trafficking, public corruption, money laundering, & currency structuring.

Recommended Book:

1. Chris Jackson; “Network Security Auditing”, CISCO Systems Inc.
2. “IT Audit, Control and Security”, Roobert Moeller; John Wiley & Sons.
3. “Cyber-Risk Management”, A. Refsdal, B. Solhaug, K. Stolen; Springer.
4. “Information Security and Auditing in the Digital Age: A Practical and Managerial Perspective”, Amjad Umar; NGE Solutions Inc.
5. “Information Technology Control & Audit”, Sandra Senft, Frederick Gallegos & Aleksendra Davis; CRC Press, Taylor & Francis.

Semester – 1

Post Graduate Diploma in Cyber Crime and Laws

Paper – V: Assignment, Presentation and Viva-Voce
Code: - DL- 1005

The faculty shall provide an assignment on the basis of first semester course curriculum to the students including some Cyber-Crime cases under IT Act and other relevant laws and the students shall prepare their assignment file individually and will show it to the internal and external examiners appointed by the university during the presentation and viva-voce exam and the examiners shall assess the assignment and award the marks.

The division of 100 marks will be as follows: assignment - 40 marks, Presentation - 30 marks and Viva-Voce - 30 marks.

SECOND SEMESTER

Semester – 2

Post Graduate Diploma in Cyber Crime and Laws

Paper – I: Intellectual Property Rights and Protection in Cyberspace
Code: - DL-2001

Unit – I

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 Institutions.

Unit – II

Commercialization of Intellectual Property Rights by Licensing. Determining Financial Value of Intellectual Property Rights. Negotiating Payments Terms in Intellectual Property Transaction. Intellectual Property Rights in the Cyber World.

Unit – III

Introduction to Copyright- International Protection of Copyright and Related rights- An Overview (International Convention/Treaties on Copyright). Indian Copyright Law- The Copyright Act, 1957 with its amendments, Copyright works, Ownership, transfer and duration of Copyright, Renewal and Termination of Copyright, Infringement of copyrights and remedies.

Unit – IV

History and Perspective of Privacy Laws. Global Privacy Issue. Legal Tools – The Constitution. Statutes & State Protection.

Recommended Book:

1. "Law and practice of intellectual property in India", Vikas Vashishth.
2. "Law Relating to Intellectual Property", Sreenivasulu N.S; Patridge Publishing.
3. "Information Technology: Law and Practice", Vakul Sharma; Universal Law Publishing Co.
4. The Copyright Act, 1957.
5. The Patent Act, 1970.

Semester – 2

Post Graduate Diploma in Cyber Crime and Laws

Paper – II : Computer Networking and Security
Code :- DL-2002

Unit – I : Introduction to Cyber Security

Introduction to Cyber Security. Confidentiality, Integrity and Availability – Triad. Attacks: Threats, Vulnerabilities and Risk. Risk Management, Risk Assessment and Analysis. Information Classification, Policies, Standards, Procedure and Guidelines. Controls: Physical, Logical and Administrative; Security Frameworks, Defence in-depth: Layers of Security. Identification and Authentication– Factors. Authorization and Access Controls- Models, Methods and Types of Access Control.

Unit – II : Basics of Cryptography

Definitions and Concepts, Symmetric and Asymmetric Cryptosystems, Classical Encryption Techniques – Substitution Techniques, Transposition Techniques, Block Ciphers and Stream Ciphers, Hybrid Encryption Techniques, One-Time Pad. E-mail security, Internet and Web Security. Steganography and its detection, Data Encryption Standard (DES), Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange.

Unit – III : Network and Wireless Attacks

Network Sniffing, Wireshark, packet analysis, display and capture filters, Ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Setup network IDS/IPS, Router attacks, Man-in-the-middle Attack, Nmap, open ports, filtered ports, service detection, network vulnerability assessment, Evade anti viruses and firewalls, Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots.

Unit – IV : Network Security

IP security architecture, Security protocols, IPSec, Web Security – Firewalls, IDS, IDPS – Types and Technologies. Trusted systems – Electronic payment protocols. Network Security Applications, Authentication Mechanisms: Passwords, Cryptographic authentication protocol, Kerberos, X.509 LDAP Directory. Digital Signatures. Web Security: SSL Encryption, TLS, SET. Intrusion detection. Securing online payments (OTP).

Recommended Book:

1. "Cryptography and Network Security", Atul Kahate; McGraw Hill.
2. "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Nina Godbole and Sunit Belapore; Wiley Publications.
3. "Cryptography and Network Security: Principles and Practices", William Stallings; Prentice Hall Publication Inc.
4. "Computer Security Art and Science", Matt Bishop; Pearson/PHI.
5. "Principles of Information Security", Michael E Whiteman and Herbert J Mattord; Vikas Publishing House, New Delhi, 2003.

Semester – 2

Post Graduate Diploma in Cyber Crime and Laws

Paper – III : Cloud and Virtual Technology
Code :- DL-2003

Unit – I : Introduction to Cloud Computing

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs. private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit – II : Cloud Application Architecture

Technologies and the processes required when deploying web services; Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.

Unit – III : Cloud Services Management

Reliability, availability and security of services deployed from the cloud. Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Unit – IV : Cloud Security and Forensics

Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO). Cloud Security Architecture, Identity and Access Management, Encryption and Key Management. Data Collection, Live Forensics, Evidence Segregation, virtualized environments and proactive measures. Organizational Dimension- Internal staffing, External Dependency Chains, Service Level Agreement, Multiple Jurisdictions and Tenancy. Investigative tools in the virtualized environment. Analysis- correlation, reconstruction, time synchronization, logs, metadata, timelines. Cloud Forensic Challenges.

Recommended Book:

1. “Cloud Computing”, Thomas Earl; Pearson.

2. “Cloud Computing: A Hands-on Approach”, Arshdeep Bagha and Vijay Madisetti.

3. “Cloud Computing: Principles and Paradigms”, Rajkumar Buyya, James Broberg, Andrzej M. Goscinski; Wiley Publications.

4. “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”, Ronald L. Krutz, Russell Dean Vines; Wiley-India.

5. “Digital Forensics for Network, Internet and Cloud Computing: A Forensic Evidence Guide for moving Targets and Data”, Terrence V. Lillard; Syngress Publications.

Semester – 2

Post Graduate Diploma in Cyber Crime and Laws
Paper – IV : Mobile and Digital Forensics
Code :- DL-2004

Unit – I : Introduction to Mobile Technologies

Asynchronous Transfer Mode (ATM), Wireless Application Protocol (WAP). Cellular technologies including Advanced Mobile Phone System (AMPS), Imode, Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) including features and relative strengths. Functions of Subscriber Identity Module (SIM), International Mobile Equipment Identity (IMEI), Bluetooth and Mobile Payment Gateways. Understanding of the mobile phone operating systems – Android, iOS, Windows. Basics of Rooting \ Jail breaking.

Unit – II : Introduction to Mobile Eco-System Security
Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm. Mobile phones including SIM cloning and other Bluetooth vulnerabilities. Attacks - Denial of Service (DOS), Packet Spoofing & Masquerading, Eavesdropping etc. Wireless Public Key Infrastructure. Securing WLAN, WEP Decryption script, Understanding of SQLite Databases. Voice, SMS and Identification Data Interception in GSM. SMS security issues – Availability, Confidentiality and Integrity issues.

Unit – III : Introduction to Mobile Forensics

Mobile Forensic, Types of Evidence present in mobile phones - Files present in SIM card, phone memory dump, and evidences in memory card. Mobile phone evidence extraction process, Data Acquisition Methods. Good Forensic Practices, Mobile Forensic Investigation Toolkit. Tracking of mobile phone location. Analysis of mobile data like SMS, call logs, contacts, media files, recordings and important mobile application data (IM Chats like whatsapp, telegram, iMessage, Email clients, Calendar, Reminder and Note apps). Challenges to Mobile forensics. CDR and IPDR analysis.

Unit – IV : Introduction to Network Forensics

Monitoring of computer network and activities, Live Packet Capturing and Analysis. Searching and collection of evidences from the network. Network Intrusion Detection and Analysis. Event Log Aggregation – role of logs in forensic analysis, tools and techniques. Investigating network attacks. Evidence collection from Routers & CCTV DVRs. Forensic analysis of online browsing activity and related artifacts.

Recommended Book:

1. "Cryptography and Network Security", Atul Kahate; McGraw Hill.
2. "Data Communication and Networking", Beherouz. A Forouzan; TMH.
3. "Network Forensics – Tracking Hackers through Cyberspace", Sherri Davidoff and Jonathan Ham; Pearson Publications.
4. "Learning Network Forensics – Identify and Safeguard your Networks against both Internal and External Threats, hackers and malware attacks", Samir Datt; PACKT Publishing.
5. "Practical Mobile Forensics – Dive into mobile Forensics on iOS, Android, Windows and Blackberry Devices with action-packed, practical guide", Satish Bommisetty, Rohit Tamma and Heather Mahalik; PACKT Publishing.

Semester – 2

Post Graduate Diploma in Cyber Crime and Laws

Paper – V: Project Work and Viva-Voce
Code: - DL-2005

The faculty shall provide a topic on the basis of first and second semester course curriculum to the students including some Cyber-Crime cases under IT Act and other relevant laws and the student shall prepare his/her project work individually under the supervision of the faculty within 45 days from the last written examination. It will be evaluated by the internal and external examiner appointed by the university. The project work will carry 100 marks.