PG Diploma in Cyber Crime and Law 2019-2020

(1-year program)

Salient Features

1. With the advancement of Information Communication Technology and the good amount of knowledge shared through internet has encouraged the techno savoy young generation to indulge in cyber-crime. This Cyber Space and its IT infrastructure are very much vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. As the cyber-crime is borderless and very delegate to handle, it needs special tools and technology in-order to prevent different types of Cyber-attacks and gather digital evidence without any kind of damage. For the admissibility of the evidence in the court, the evidence must be preserved and handled to ensure that it hasn't been changed. Apart from this the rise and evolution of social media has changed the definition of communication and social interaction.

2. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence there is a need for cyber laws. Cyber law touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. Hence, this course will allow the participants to get a vivid knowledge of how crime is committed in the cyber world, the manner in which these crimes are being investigated including evidence collection and examination of the evidences and the laws pertaining to such crimes, handling evidences, maintaining the chain of custody and presenting the facts and findings in the court.

Course Objectives

The course has been designed keeping in mind the following objectives:

1. This course will look at the emerging legal, policy and regulatory issues pertaining to cyberspace and cybercrimes.
2. To cover all the topics from fundamental knowledge of Information Technology and Computer Architecture so that the participant can use to understand various aspects of working of a computer.
3. To identify the emerging Cyberlaws, Cybercrime & Cyber security trends and jurisprudence impacting cyberspace in today's scenario.
4. To enable the participants appreciate, evaluate and interpret the case laws with reference to the IT Act and other Laws associated with the cyberspace.
5. To provide vivid knowledge about different types of Digital Forensics such as Mobile Device Forensics, Network Forensics, Cloud based Forensics etc., including the Standard Operating Procedures for IO's which will be useful in investigating real-time cases pertaining to cybercrime.
6. To provide knowledge related to auditing of computer systems, managing and mitigating risk situations in the organization and techniques for investigating financial frauds.

Overview of Course

Course Name	Course Duration	Eligibility of the Participants	Minimum Qualifications
P G Diploma in Cyber Crime and Law	1 Year	1. **For In-Service Officers**: Forensic Scientists working in various CFSLs/FSLs in Cyber Forensic Division, SI and above working in Cyber Cells in Police Departments. 2. **For Other Students**: Bridging Course of One Week	Graduate in any relevant discipline of Science

1. Academic session starts in August.
2. There are 2 semesters in each Academic Session. Semester 1 (August to November) and Semester 2 (January to April).
3. Examinations are held in the month of May and December.
4. Each semester consists of 17 weeks of teaching.
5. No. of teaching hours per week = **6 hours/day x 5 days/week = 30 hours**
6. Semester 1 consists of 5 theory papers (practical work included) and Semester 2 consists of 4 theory papers (practical work included) along with a dissertation project.
7. Total number of papers in PG Diploma Course = **10 papers (1 year duration)**
8. **The total credit points of 1 year (2 semesters) are 56 credit points.**

SYLLABUS OF P.G. DIPLOMA COURSE IN CYBER CRIME & LAW

Credit Distribution Matrix

Semester I

Paper Code	Paper Name	L*	T*	P**	Total
PGDCCL 101	Fundamentals of Computers & Networking	2	1	1	4
PGDCCL 102	Introduction to Cyber-crime	2	1	1	4
PGDCCL 103	Fundamentals of Computer & Network Security	2	1	1	4
PGDCCL 104	IT Act and other Laws for cyber-crime	3	1	0	4
PGDCCL 105	Auditing, Risk Management and Financial Fraud Investigation	3	1	0	4
	Total (credits)	**12**	**5**	**3**	**20**

Semester II

Paper Code	Paper Name	L*	T*	P**	Total
PGDCCL 201	Digital Forensics	2	1	1	4
PGDCCL 202	Mobile and Network Forensics	2	1	1	4
PGDCCL 203	Cloud and Virtual Technology Security	2	1	1	4
PGDCCL 204	Intellectual Property Rights and Privacy Laws	3	1	0	4
PGDCCL 205	Dissertation (Mini Project)	0	0	20	20
	Total (credits)	**9**	**4**	**23**	**36**

***** Each theory class of 1 hour (1hour of lecture and/or 1 hour of Tutorial respectively) hold 1 credit point.

****** Each practical class of 2 hours holds 1 credit point.

FIRST SEMESTER

Semester-I, Paper I
PG Diploma Cyber Crime and Law
PGDCCL-101 Fundamentals of Computers and Networking
L=2, T=1, P=1 Credits = 4

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.

Reference Books

1. John P. Hayes; “Computer Architecture and Organization”, McGraw-Hill, 1988.
2. V. Rajaraman and Niharika Adabala; “Fundamentals of Computers”, 6th Edition, PHI Learning Pvt. Ltd., 2015.
3. Anita Goel; “Computer Fundamentals”, Pearson Publications, 2010.
4. Beherouz. A Forouzan; “Data Communication and Networking”, 4th Edition, TMH, 2000.
5. Andrew S.Tanenbaum; “Modern Operating Systems”, 2nd edition, Addison Wesley, 2001.
6. Gary Nutt; “Operating Systems: A Modern Perspective”, 2nd edition, Pearson Education, 2001.
7. William Stallings; “Operating Systems: Internals and Design Principles”, 5th Edition, Prentice Hall, 2005.

Semester-I, Paper II
PG Diploma Cyber Crime and Law
PGDCCL-102 Introduction to Cyber-crime
L=2, T=1, P=1 Credits = 4

Unit I

Cyber Crime- Overview, Internal and External Attacks, Attack Vectors. Cybercrimes against Individuals – E-mail spoofing and online frauds, Phishing and its forms, Spamming, Cyber-defamation, Cyberstalking, Cyber Bullying and harassment, Computer Sabotage, Pornographic offenses, Password Sniffing. Keyloggers and Screenloggers**.** Cyber Crimes against Women and Children.

Unit II

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

Cybercrime 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.

Reference Books

1. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
2. Shon Harris, "All in One CISSP, Exam Guide Sixth Edition", McGraw Hill, 2013.
3. Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.
4. William Stallings; "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall Publication Inc., 2007.
5. Atul Jain; "Cyber Crime: Issues, Threats and Management", 2004.
6. Majid Yar; "Cybercrime and Society", Sage Publications, 2006.
7. Michael E Whiteman and Herbert J Mattord; "Principles of Information Security", Vikas Publishing House, New Delhi, 2003.
8. Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.

Semester-I, Paper III
PG Diploma Cyber Crime and Law
PGDCCL-103 Fundamentals of Computer & Network Security
L=2, T=1, P=1 Credits = 4

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).

Reference Books

1. William Stallings; "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall Publication Inc., 2007.
2. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
3. Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.
4. Michael E Whiteman and Herbert J Mattord; "Principles of Information Security", Vikas Publishing House, New Delhi, 2003.
5. Atul Kahate "Cryptography and Network Security" McGraw Hill Education (India), 2008.
6. Alfred J. Menezes, Paul. C. Van Oorschot, and Scott A. Vanstone "Handbook of Applied Cryptography", CRC press, Lib of Congress -2006

Semester-I, Paper IV
PG Diploma Cyber Crime and Law
PGDCCL-104 IT Act and other Laws for Cyber-crime
L=3, T=1, P=0 Credits = 4

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. IT Act 2000 - Objectives, 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 Information and Technology 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.

Reference Books

1. Karnika Seth; "Computers, Internet and New Technology Laws", Lexis Nexis Buttersworth Wadhwa, 2012.
2. Vikas Vashishth.; "Law and practice of intellectual property in India"
3. Jonathan Rosenoer; "Cyber Law: The Law of Internet", Springer- Verlag, New York, 1997.
4. Sreenivasulu N.S; "Law Relating to Intellectual Property", Patridge Publishing, 2013
5. Pavan Duggal; "Cyber Law – The Indian Perspective", Saakshar Law Publications.
6. Harish Chander; "Cyber Laws and IT Protection", PHI Learning Pvt. Ltd, 2012.
7. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
8. Vakul Sharma; "Information Technology: Law and Practice", Universal Law Publishing Co., India, 2011.
9. The Copyright Act, 1957
10. The Patent Act, 1970
11. The Indian Evidence Act, 1872.

Semester-I, Paper V
PG Diploma Cyber Crime and Law
PGDCCL-105 Auditing, Risk Management and Financial Fraud Investigation
L=3, T=1, P=0 Credits = 4

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 – Introduction and Applicability. SOX – International Compliance – Introduction and Applicability. 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. Implementation, Limitation. 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

Reference Books

1. Amjad Umar; "Information Security and Auditing in the Digital Age: A Practical and Managerial Perspective", NGE Solutions Inc., 2004.
2. Chris Jackson; "Network Security Auditing", CISCO Systems Inc., 2010.
3. Roobert Moeller; "IT Audit, Control and Security", John Wiley & Sons, 2010.
4. Sandra Senft, Frederick Gallegos & Aleksendra Davis; "Information Technology Control & Audit", 4th Edition, CRC Press, Taylor & Francis, 2013.
5. A. Refsdal, B. Solhaug, K. Stølen; "Cyber-Risk Management", Springer, 2015.
6. Domenic Antonucci; "The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities", Wiley Finance Series, 2017.
7. Howard Silverstone, Michael Sheetz, Stephen Pedneault and Frank Rudewicz; "Forensic Accounting and Fraud Investigation for Non-Experts", 3rd Edition, John Wiley & Sons, 2012.
8. Tracy L. Coenen; "Expert Fraud Investigation- A Step-by-Step Guide", John Wiley & Sons, 2009.
9. Tommie Singleton and Aaron Singleton; "Fraud Auditing and Forensic Accounting", 4th Edition, Wiley Corporate F&A, 2010.

SECOND SEMESTER

Semester-II, Paper I
PG Diploma Cyber Crime and Law
PGDCCL-201 Digital Forensics
L=2, T=1, P=1 Credits = 4

Unit I – Basics of Digital Forensics

Digital Forensics- Introduction, Objective and Methodology, Rules of Digital Forensics, Good Forensic Practices, Daubert's Standards, Principles of Digital Evidence. Overview of types of Computer Forensics – Network Forensics, Mobile Forensics, Social Media Forensics and E-mail Forensics. Services offered by Digital Forensics. First Responder – Role, Toolkit and Do's and Don'ts

Unit II – Cyber Crime Investigation

Introduction to Cyber Crime Investigation, Procedure for Search and seizure of digital evidences in cyber-crime incident. Forensics Investigation Process- Pre-search consideration, Acquisition, Duplication & Preservation of evidences, Examination and Analysis of evidences, Storing of Evidences, Documentation and Reporting, Maintaining the Chain of Custody. Data Acquisition of live system, Shutdown Systems and Remote systems, servers. E-mail Investigations, Password Cracking. Seizing and preserving mobile devices. Methods of data acquisition of evidence from mobile devices. Data Acquisition and Evidence Gathering from Social Media. Performing Data Acquisition of encrypted systems. Challenges and issues in cyber-crime investigation.

Unit III – Analysis of Digital Evidences

Search and Seizure of Volatile and Non-volatile Digital Evidence, Imaging and Hashing of Digital Evidences, Introduction to Deleted File Recovery, Steganography and Steganalysis, Data Recovery Tools and Procedures, Duplication and Preservation of Digital Evidences, Recover Internet Usage Data, Recover Swap files/Temporary Files/Cache Files. Software and Hardware tools used in cyber-crime investigation – Open Source and Proprietary tools. Importance of Log Analysis in forensic analysis. Understanding Storage Formats for Digital Evidences – Raw Format, Proprietary Formats, Advanced Forensic Formats.

Basics of various email clients like Outlook, Lotus Notes, Thunderbird, and forensically relevant files for the same (in both Windows and MacBook OS).

Unit IV –Windows and Linux Forensics

Windows Systems Artifacts: File Systems, Registry, Event logs, Shortcut files, Executables. Alternate Data Streams (ADS), Hidden files, Slack Space, Disk Encryption, Windows registry, startup tasks, jumplists, Volume Shadow, shellbags, LNK files, Recycle Bin Forensics (INFO, $i, $r files). Forensic Analysis of the Registry – Use of registry viewers, Regedit. Extracting USB related artifacts and examination of protected storages. Linux System Artifact: Ownership and Permissions, Hidden files, User Accounts and Logs. Use of built-in command line tools for forensic investigation – dd, dcfldd, fdisk, mkfs, mount, unmount, md5sum, sha1sum, dmseg.

Forensic Acquisition and analysis of Apple OS macbooks, and their various forensic artefacts (Plists), Function of File Vault, Keychain

Reference Books

1. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
2. Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.
3. Shon Harris; "All in One CISSP Guide, Exam Guide Sixth Edition", McGraw Hill, 2013.
4. LNJN National Institute of Criminology and Forensic Science, "A Forensic Guide for Crime Investigators – Standard Operating Procedures", LNJN NICFS, 2016.
5. Peter Hipson; "Mastering Windows XP Registry", Sybex, 2002.
6. Harlan Carvey; "Windows Forensic Analysis Toolkit", Syngress, 2012.
7. Anthony Reyes, Jack Wiles; "The Best Damn Cybercrime and Digital Forensic Book", Syngress, USA, 2007.
8. Cory Altheide and Halan Carvey; "Digital Forensics with Open Source Tools", Syngress Publication.

Semester-II, Paper II
PG Diploma Cyber Crime and Law
PGDCCL-202 Mobile and Network Forensics
L=2, T=1, P=1 Credits = 4

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 \ Jailbreaking.

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. Seizure and Preservation of mobile phones and PDA. Mobile phone evidence extraction process, Data Acquisition Methods – Physical, Logical and File System\Manual Acquisition. 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.

Reference Books

1. William Stallings; "Network Security Essentials", 3rd Edition, Pearson Education, 2006.
2. Atul Kahate; "Cryptography and Network Security" McGraw Hill Education (India), 2008
3. Beherouz. A Forouzan; "Data Communication and Networking", 4th Edition, TMH, 2000.
4. Sherri Davidoff and Jonathan Ham; "Network Forensics – Tracking Hackers through Cyberspace", Pearson Publications, 2012.
5. Samir Datt; "Learning Network Forensics – Identify and Safeguard your Networks against both Internal and External Threats, hackers and malware attacks", PACKT Publishing, 2016
6. John R. Vacca; "Network and Systems Security", Syngress Publications.
7. Satish Bommisetty, Rohit Tamma and Heather Mahalik, "Practical Mobile Forensics – Dive into mobile Forensics on iOS, Android, Windows and Blackberry Devices with action-packed, practical guide", PACKT Publishing, 2015.
8. Iosif I. Androulidakis, "Mobile Phone Security and Forensics – A Practical Approach", Springer New York Heidelberg, 2012.
9. Jonathan Zdziarski, "iOS Forensic Investigative Methods", 2012.

Semester-II, Paper III
PG Diploma Cyber Crime and Law
PGDCCL-203 Cloud and Virtual Technology Security
L=2, T=1, P=1 Credits = 4

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.

Reference Books

1. Arshdeep Bagha and Vijay Madisetti; "Cloud Computing: A Hands-on Approach", 2014.
2. Thomas Earl; "Cloud Computing", Pearson, 2014.
3. Barrie Sosinsky; "Cloud Computing Bible", Wiley-India, 2010.
4. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski; "Cloud Computing: Principles and Paradigms", Wiley Publications, 2013.
5. Ronald L. Krutz, Russell Dean Vines; "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley-India, 2010.
6. K. Kent, S. Chevalier, T. Grance and H. Dang; "Guide to Integrating Forensic Techniques into Incident Response", Special Publication 800-86, NIST, Gaithersburg, Maryland, 2006.
7. Terrence V. Lillard; "Digital Forensics for Network, Internet and Cloud Computing: A Forensic Evidence Guide for moving Targets and Data", Syngress Publications, 2010.

Semester-II, Paper IV
PG Diploma Cyber Crime and Law
PGDCCL-204 Intellectual Property Rights and Privacy Laws
L=3, T=1, P=0 Credits = 4

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.

Reference Books

1. Vikas Vashishth.; "Law and practice of intellectual property in India"
2. Sreenivasulu N.S; "Law Relating to Intellectual Property", Patridge Publishing, 2013
3. Vakul Sharma; "Information Technology: Law and Practice", Universal Law Publishing Co., India, 2011.
4. The Copyright Act, 1957
5. The Patent Act, 1970

Semester-II, Paper V
PG Diploma Cyber Crime and Law
PGDCCL-205 Dissertation (Mini-Project)
L=0, T=0, P=20 Credits = 20

The students would develop their project individually and get the topic approved by the Director. For the purpose of approval, they have to submit their project titles and proposals with the name of internal or external guides within twenty one days of the commencement of the semester. In case, if the student proposal is rejected, the revised proposal, is required to submit and get it sanctioned within next seven days. Failing to do this, He/she will not be qualified for this subject.

The students have to report to the guide for at least five times during the project lifespan with the progress report duly signed by the internal guide. Moreover they have to submit the progress reports with the final project report at the time of external examination.

The external examiners appointed by the Director shall award the marks out of 20 on the basis of the Presentation, Demonstration, Viva-Voce, and basis of Project Report. The internal guide shall award out of 40 Marks.

Syllabus

Of

Post-Graduate Diploma in Cyber Crime and Law

(2018)

LNJN National Institute of Criminology & Forensic Science

Ministry of Home Affairs, Govt. of India

Delhi