DR. BABASAHEB AMBEDKAR MARATHWADA
UNIVERSITY,
AURANAGABAD

Revised Syllabus

Of

Post Graduate Diploma in Digital and cyber Forensic and Related Law

Effective from Academic Year
2012-2013 onwards

P.G Diploma in digital and cyber Forensic and Related Law

P. G Diploma in digital and cyber Forensic and Related Law shall be conferred on a Candidate who satisfies the following Condition:

R- He must have Passed Bachelor degree such as, B.Sc. IT / Computer Science / Bioinformatics; B. Sc. with Statistics / Mathematics / Electronics as a special subject at final year (Honours); BCS / BCA, Engineering degree (B.E. / B. Tech) in Computer Science / Information Technology / Electronics / Telecommunication / Electronics and Telecommunication.

R-Examination pattern for Theory and Practical

The course of study for **P.G Diploma in digital and cyber Forensic and Related Law** is of one year (fulltime) The Course will have 4 theory papers, each of 100 Marks. There will be Practical of 100 marks and Report on field visits & Project Work of 100 Marks.

1) Theory examination of 3 hrs duration would be conducted at the end of Academic year
2) Practical examination will be at the end of Academic year and will be of 6 hrs Duration.
3) The students have to submit report on Field Visit and Project work at the end of Academic year.

R-Structure of class and Practical Examination

Maximum number of students in a class of Theory shall be 40. Maximum Number of Students in a batch for Practical shall consist of 12 students.

R-Standard of Passing and Award of Division.

a) A candidate who secures minimum 40% of the marks in each subject/ Paper will be declared to have passed the examination.

b) A candidate who secures 50% or more but less than 60% in each subject/paper shall be awarded a Second Division.

c) A candidate who secures a minimum 50% mark in each paper and an aggregate of 60% and above marks on the whole shall be declared to have passed the examination in First Division.

d) A candidate who secures a minimum of 40% marks in each paper and an aggregate of 70% and above marks on the whole shall be declared to have passed the Examinations with Distinctions.

Course Structure for
P.G Diploma in Digital and Cyber Forensic Science and Related Law

Paper No	Paper code	**Title of paper**	Lecturers per week (1 hr Duration)	Maximum Mark
I	PGDC1	CYBERSPACE TECHNOLOGY & INFORMATION SECURITY	4	100
II	PGDC2	COMPUTER , DIGITAL FORENSIC ,CYBER CRIMES & DIGITAL EVIDENCE	4	100
III	PGDC3	**CYBER LAW AND IT SECURITY**	4	100
IV	PGDC4	CYBER CRIME & FORENSIC EVIDENCE	4	100
V	PGDC5	PRACTICAL TRAINING	4 per Batch	100
VI	PGDC6	REPORT ON FIELD VISIT AND PROJECT	4 Per Batch	100

Paper – I
CYBERSPACE TECHNOLOGY & INFORMATION SECURITY (cyber)

Marks- 100 **(Credits 4)**

Unit I :- **Emergence of Cyberspace:** Defining Cyberspace, Evolution of Computer, history of computers, Generations of Computers Technology .A look at evolving Ethics in Information age with special reference to free Music , flash mobs. Brief Historical perspective , Non-Technical overview of Computer/Mobile devices and the Internet. Areas of Application Computers and its components Advantages and Disadvantages of Computer Application Software and System Software ,Memory Hierarchy and Cache Memory.

Unit –II :- A glance of computer/mobile application as they are used in the cyberspace, automating and increasing workforce's productivity and mobility. The world of network from the very basis LAN and WAN to a global infrastructure the evolving internet. Networking technology, topologies and their application, OSI Model, TCP/IP and Related Protocols Related Terms (Terminologies) Impact of cyberspace on the society especially social behavior, governance, learning & education, healthcare and business including entertainment social networking.

Unit-III :- Both hardware and software Concepts. Communication medias and medium, Access to the cyberspace would deal with copper wires, co-axial cables and wireless networks as a mean of communication to the Cyberspace. How the telecom cable / broadcast and other spectrum policies affect the market mechanisms influencing the net citizen's ability to use it. Introduction to Internet Application Areas of Internet Working of Internet its Advantages and Disadvantages Search Engines, Chat, E-mails and WWW Internetworking Devices Internet Service Provider, Practical working model of e-commerce , Overall working of net-banking and online purchase, recent Authentication techniques & methods, Introduction to cyber forensic and mobile forensic .

Unit IV :- **Investigations:** Approach of Digital and Cyber services in Forensic Services. The Cyber laws its significance with the present day problem. Court testimonial in Digital and Cyber cases. Stegnography, **classification of stegnography (linguistic,digital,technical)**Reversing stegnographic process Counter or anti forensics Anti forensics: A View from the Edge Cloaking Techniques (Data Hide and Seek), Renaming and Manipulating File System, Data Hiding on NTFS with Alternate data Stream.

Unit V :- Computer Security: Information Security Overview , Information Security Services Types of Attacks , Goals for Security ,Security model Network Security:, Overview of Security threats ,Hacking Techniques Password Cracking, Insecure Network connections , Malicious Code , Email security: PGP and SMIME , Web Security: web authentication, SSL and SET , Database Security , Operating System Security , E-commerce Security

Paper – II
COMPUTER, DIGITAL FORENSIC, CYBER CRIMES & DIGITAL EVIDENCE (cyber)

Marks- 100 (Credits 4)

Unit 1 :- Computers and the Internet: Computer components, Computer media, the internet, the World Wide Web, and Types of Computers, Types of Operating Systems, Digital devices like laptops, watches ,Cell phones , handling devices etc. **The Cyber Crimes:** Tampering with Computer Source Documents, Hacking with Computer System, different type of hacking and hackers
Unit II :- Cyber Forensic and Computer Crimes: Distinction between Conventional Crime & Cyber Crime, Reasons for Cyber Crime. Modus operand of Cyber Criminal . Computer crime prevention measures, Types of Cyber Crimes: Phishing ip spoofing etc Crimes targeting Computers: Unauthorized Access Packet Sniffing Malicious Codes including Trojans, Viruses, Logic Bombs, etc Investigating the crime scene by first responders . Electronic devices with their potential evidence value, Evidence Collection Packing, Transportation and storage of Evidence collected. Precaution in the investigation/examination of Digital evidences as they can be altered, damaged or destroyed by improper handling or examination losing evidence value. Steps in cyber forensic, Computer ethics.

Unit III :- Speaker Identification: Use of Auditory analysis, Acoustic analysis, Computer technique to recognize , identify and discriminate between human voices, Voice characteristic for future verifications and identification , computer Recognition of Voice and Speech . Principles of Forensic speaker identification Characterizing forensic speaker identification: Principles of Generation of speech and its uniqueness Speaker recognition Speaker identification and verification Forensic significance: Phonemic structure.

Unit IV:- Image processing techniques: Digital photography: processing pipeline and sensor charters tic, sensor identification, Anomaly to detection: Statistics of natural images inconsistency in lighting and chromatic aberration, duplication detection. Image and video processing: re-sampling algorithms (rotation scaling) and their identification via linear dependency patterns among adjust cent pixels, compression history identification, Super resolution. Document printer / scanner Identification with focus on steganography, water marking, and finger printing algorithms for hiding, recovering, detecting and distorting embedding signals in invariant properties. ___

Unit V :- Technical concern to the cyber crimes and techniques for solving those crimes. Unauthorized access, Web spoofing, Hacking and web defacement Denial of service attack Malicious code Financial crime: - including online fraud, counter feinting etc. Social engineering attacks ,Identity theft Cyber stalking Pornography Harassment Murder and death threats Gambling Spamming , Sell to controlled items – tobacco wines etc , Commercial espionage Commercial extortion , Data manipulation Software/ hardware piracy , Money laundering Threat or Disruptions to Health and Safety, Shutdown or Essential Services and Extortions. Espionage and Terrorism. Other including the One’s involving Mobile Devices Data collection and Analysis techniques .

Paper III
Cyber Law and IT Security (law)

Unit I Fundamentals of Cyber Law , Jurisprudence of Cyber Law
Overview of Computer and Web Technology, included in paper 1 Introduction to Indian Cyber Law. Cyber Law-A Time line. Governance of Internet & Other relevant details outlined.**(LAW related)** , Publishing of Information which is Obscene in Electronic From, motives behind cyber crimes , Offences: Breach of Confidentiality & Privacy, Offences: Related to Digital Signature Certificate, Technology of Digital Signature, Creating a Digital Signature, Verifying a Digital Signature, Digital Signature.

Overview of General Laws and Procedures in India,Information Technology Act 2000. Overview of IT Act 2000 along with rules with relevant sections and rules highlighted along with amendments to other laws. Jurisprudence: - A case digest with 125 to 150 typical cases, sets a present context in different categories of legal issues. Here we briefly focus on initiatives of internet policy marking at international levels by individual inter-government organizations, which are considerable feats, pointing to an emerging international framework .As an illustrative example of policy making, we could discuss the TRIPP Agreement and the WTO, ICANN and UNICITRAL in the area of intellectual property , Domain names and Model E-commerce law.

Unit II Domain Name

Disputes and Trademark Law, Concept of Domain Names, New Concepts in Trademark Jurisprudence , cyber squatting , Reverse Hijacking , Meta Tags, framing , spamming , Jurisdiction in Trademark dispute ,Cyber Regulations Appellate Tribunal, Establishment & Composition of appellate Tribunal Powers of Adjudicating officer to Award Compensation, Powers of Adjudicating officer to Impose Penalty.

Unit III Digital Signature:

Technology of Digital Signature, Creating a Digital Signature, Verifying a Digital Signature, Digital Signature and Law, E-governance and IT Act 2000, Legal Recognition of electronic Records. Legal recognition of Digital Signature use of electronic records and digital signatures in Government and its agencies, Certifying authorities, need of certifying authority and Power, Digital Signature Certifications Generation, Suspension and Revocation of Digital Signature Certificate

Unit IV: Cyber crime and Digital Evidence - Indian Perspective

Penalties and Offences under the IT Act ,
Offences under the Indian Penal Code ,
Investigation and adjudication issues ,
Digital Evidence

Unit V : Intellectual Property Issues and Cyberspace , The Indian Perspective

Overview of Intellectual Property related Legislation, Copyright law & Cyberspace
Trademark law & Cyberspace , Law relating to Semiconductor Layout & Design
Jurisprudence and latest initiatives, Jurisprudence and zoning Online contracts-contrasting/comparing click wrap agreements with others. Privacy issues and along with Negligence, Protection of personal data , Torts in cyberspace along with negligence, Strict liability, immunities and privileges. Security and Evidence in e-commerce with respect to Digital Signatures, encryption and Digital Certificate. Taxation issues in Cyberspace taxes related to internet (e-commerce), tax evasion and the problems of Taxation on the net, International taxation, US & European views

Paper – IV
CYBER CRIMES, DIGITAL FORENSIC & EVIDENCE (law)

Marks- 100 (Credits 4)

Unit I : Contextualizing Digital Crimes: Undertaking cyber crime A- sample of at least 25/30 , cases in different category, in compassing crime against or / and supported by the computer and the network. This concern , Unauthorized access , Web spoofing, Hacking and web defacement , Denial of service attack, Malicious code, Financial crime: - including online fraud, counter feinting etc. Social engineering attacks, Password cracking , Steganography ,Identity theft , Cyber stalking, Pornography, Harassment, Murder and death threats , Gambling , Spamming, Sell to controlled items – tobacco wines etc, Commercial espionage
Commercial extortion, Data manipulation, Software/ hardware piracy, Money laundering, Threat or Disruptions to Health and Safety, Shutdown or Essential Services and Extortions. Espionage and Terrorism. Other including the One's involving Mobile Devices.

Unit II Case study rule and Procedures , Profiling the need to Combat Digital Crime by State Enforcement as well as Comparing/Contrasting Cyber Crime with Conventional Crime, IT Act-Penalties & Offences, Investigations and Adjudication. Indian penal law – An overview with relevant sections/ rules highlighted. Criminal Procedures Code- An overview with relevant sections / rules highlighted , Evidence Act – An overview with relevant sections/rules highlights.

Critical evaluation of rules & procedures:- Are these enough/ more to address digital crimes? Are there more challenges? A Critical Evaluation by Participants who can workout the Ideal model rules and Procedures. Identify areas not covered by IT Act and classify those addressed by other laws and issues that await attention.

Focus on some other typical issues: Obscenity & Pornography on the Internet Freedom of Speech & Expression Defamation & Hate Speech included.

Unit III Reporting the incident on desire of victim:

A FIR and in few cases a remand order. Other process including how the accused with a different profile needs to handled than normal Criminals, accessing their motives, degree of empathy, sympathy & anger expressed based on the nature of crime, age of the accused & degree of offence to be considered.

Unit IV Courtroom presentation of digital evidence: A Brief Summary covering the "Search and Seizure issues" Integrity Discovery and Disclosure of Digital Evidence courtroom Reparation and Evidence Rules and Presentation Digital Evidence.

Courtroom presentation and evidence rule would focus on the preliminary considerations for the prosecutor when reviewing the scope of the investigation to date, effective pre-trail communication between prosecutor, investigator and forensic examiners and also evidentiary issues like authentication and hearsay in digital evidence context

Unit V –Commerce and e-Banking: Anti-trust cases along with emerging checks on the Market place with open source, co-evolution, interoperability and standards becoming the order of the day instead of Competition. Converging business models for service with Information appliances like iPods. Legal issues related to e-banking (internet banking) and us of credit/debit cards on the net like buying Indian railway or cinema tickets

Paper-V
Practical training (cyber)

Marks- 100 **(Credits 3)**

1.	Finding results of different logic gates and their combinations
2.	Working with windows file (creation, modification, deletion, attributes) folder (creation, nesting, attributes)
3.	Working with Linux- file (Creation, modification, deletion, attributes), folder (Creation, nesting attributes).
4.	Working with external storage devices using windows- Reading and writing data on floppy, CD,DVD, USB thumbdrive
5.	Working with external storage devices using Linux-reading writing data on floppy, CD, DVD, USB, thumb drive.
6.	Understanding LAN-client/server, user creation, password protection.
7.	Use of internet- visiting websites with given URL, searching in formation using search engine.
8.	Use of E-mail, creating e-mail, sending and receiving e-mails with attachments.
9.	Networking commands- like ping, IP Config, etc with various switches.
10.	Tracing E-mail, finding senders IP address, of received email, tracing route of email received using tool available on internet, e.g. Visual Trace Route etc.
11	Demonstration of various concealment techniques and recovery software/hardware’s
12	Demonstration of various Cyber forensic Software’s (encase, FTK, helix , paraben etc)
13	Demonstration of various Cyber forensic Hardware (Forensic work station , write protect, disk imaging etc)

Paper-VI
Report on Field Visit and Project work (cyber)

Marks- 100 **(Credits 3)**