UNIVERSITY OF MUMBAI
No.UG/465 of 2009

CIRCULAR: -

The Directors/Heads of the recognized Science Institutions concerned and the Principals of the affiliated Colleges in Science and Law are hereby informed that the recommendation made by the Ad-hoc Committee relating to Forensic Science at its meeting held on 9th September, 2009 has been accepted by the Academic Council at its meeting held on 17th September, 2009 **vide** item No.4.22 and subsequently approved by the Management Council at its meeting held on 25th September, 2009 vide item No.21 and that, in accordance therewith, the P.G. Diploma in Digital and Cyber Forensic Science and related Law has been introduced from the academic year 2009-2010.

Further that in exercise of the powers conferred upon the Management Council under Section 54(1) and 55(1) of the Maharashtra Universities Act, 1994, it has made **Ordinances 5896, 5897 and Regulations 8201, 8202, 8203, 8204 and 8205** including the Scheme of Examination and Syllabus relating to the P.G. Diploma in Digital and Cyber Forensic Science and related Law is as per Appendix and that the same has been brought into force with effect from the academic year 2009-2010.

MUMBAI-400 032
12th December, 2009

PRIN. K. VENKATARAMANI
REGISTRAR

To,

The Directors/Heads of the recognized Science Institutions concerned and the Principals of the affiliated Colleges in Science and Law.

A.C./4.22/17.09.2009
M.C./21/25.09.2009

****

No. UG/465-A of 2009, MUMBAI-400 032 12th December, 2009

Copy forwarded with compliments for information to :

1) The Deans, Faculty of Science and Law,
2) The Convener of the Ad-hoc Committee of Forensic Science.
2) The Controller of Examinations.
3) The Co-ordinator, University Computerization Center.

12/12/09
(D. H. KATE)

Enclosure to Item No. 4.22
17/9/2009

UNIVERSITY OF MUMBAI

Ordinances, Regulations,

Scheme of Examinations & Syllabus

for

P.G.Diploma in Digital and Cyber Forensics and related law

(Introduced from the academic year 2009-2010)

UNIVERSITY OF MUMBAI

O 5896 Title of the Course: -Post Graduate Diploma in Digital and Cyber Forensic And related Law

O 5897 Eligibility: Bachelor Degree in Science, Psychology, Law, Engineering, IT, Computer Sciences, Medical Sciences

R 5201 Duration of the Course: - One Year (Part Time.)

R 5202 Fee Structure: - As per The state Government Rules

R 5203 Intake Capacity -40 (reservation as per state Govt.Rule)

R 5204 Teacher Qualifications: - As per the U.G.C./ State Government Norms and Experts from Forensic Science Field and Related Industry with minimum 3 years of experience.

R 5205 Standard of Passing: -

a. Candidate who secures minimum 50% in each subject/ paper be declared to have passed the examination.

b. Candidate who secures a minimum of 50% marks in each paper and an aggregate of 60% and above marks on the whole shall be declared to have passed the examinations in the First Class.

c. Candidate who secures a minimum of 50% marks in each paper and an aggregate of 70% and above marks on the whole shall be declared to have passed the examinations with Distinction.

Medium of Instruction: English

Field Visits at Forensic Science Laboratory

Syllabus

Syllabus for P.G. Diploma in Digital and Cyber Forensics and related law
Effective from the academic year 2009 - 2010

Course Structure

PAPER	TITLE OF PAPER	MARKS	LECTURES (1 hr. duration	NO. OF CREDITS
I	Jurisprudence, Information and Cyberspace Technology	100	90	6
II	Cyber law and IT Security	100	90	6
III	Basic of Computer and Digital Forensics	100	90	6
IV	Cyber Crimes, Digital Forensics and its Evidences	100	90	6
V	Practical I: Practical Training	100	90	3
VI	Report on Field Visit and Project Work	100	90	3
				Total 30 credits

Syllabus for P.G. Diploma in Digital and Cyber Forensics and related law

Paper I: Jurisprudence, Information and Cyberspace Technology

Paper II: Cyber law and IT Security

Paper III: Basic of Computer and Digital Forensics

Paper IV: Cyber Crimes, Digital Forensics and its Evidences

Paper V: Practical I: Practical Training

Paper VI: Report on at least Field Visits and Project Work

Paper – I: JURISPRUDENCE, INFORMATION & CYBERSPACE TECHNOLOGY

Each Unit will have 25 marks and 18 lectures of 1 hr each.

Unit-1:-

Emergence of Cyberspace
Defining Cyber space.
Evolution of Computer Technology & Cyber Law- A time Line.
Governance of Internet & other relevant details outlined.
A look at evolving ethics in information age with special reference to free music, flash mobs.

Unit -2:-

A brief historical perspective, non-technical overview of computer/mobile devices and the internet. Both hardware and software concepts
A glance of Computer/mobile applications as they are used in the cyber space, 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.
The impact of cyber space on society especially social behavior, governance, learning & education, health care and business including entertainment social networking.
Information Technology Act 2000
Overview of IT Act 2000 along with rules with relevant sections and rules highlighted along with amendments to other laws.
Access to the Cyber Space would deal with copper wires, co-axial cables and wireless networks as a means of communication to the cyber space. How the telecom cable/broadcast and other spectrum policies affect the market mechanisms influencing the net citizen's ability to use it.

Unit-3

Jurisprudence and latest initiatives:-

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, ICAAN and INICITRAL in the area of Intellectual Property, Domain Names and model e-commerce law.

Unit-4

E-Commerce and e-Banking:-

Jurisdiction and zoning

Online contracts-contrasting/comparing click wrap agreements with others.

Privacy issues and along with negligence, protection of personal data.

Torts in cyber space 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 Cyber spaces- Taxes related to the Internet (e-commerce), tax evasion and the problems of taxation on the net, International taxation, US & European views

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 usc credit/debit cards on the net like buying Indian railway or cinema tickets.

PAPER II: CYBER LAW AND IT SECURITY

Each Unit will have 25 marks and 18 lectures of 1 hr each.

Unit 1:

IT Act and Encryption

Genesis, Object and Scope of the Act, Encryption, Symmetric Cryptography, Asymmetric Cryptography, RSA Algorithm, Public Key Encryption

Unit 2:

Digital Signature

Technology of Digital Signature, Creating a Digital Signature, Verifying a Digital Signature, Digital Signature and the 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 3:

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 4:

The Cyber Crimes

Tampering with Computer Source Documents, Hacking with Computer System, Publishing of Information which is Obscene in Electronic Form, Offences : Breach of Confidentiality

& Privacy , Offences : Related to Digital Signature Certificate

PAPER III: BASIC OF COMPUTER AND DIGITAL FORENSIC

Each Unit will have 25 marks and 18 lectures of 1 hr each.

Unit 1:

Computers and the Internet

Computer components, computer media, the Internet, the World Wide Web, and TCP/IP protocol,

Types of computers, Types of operating Systems, Digital devices like laptops, watches, cell phones, handling devices etc.

Unit 2:

Investigations

Approach of digital and cyber services in Forensic services .The cyber Laws its significance with the present day problem. Court testimonials in Digital and cyber cases.

Unit 3:

Speaker Identification

Use of Auditory analysis, acoustic analysis, computer techniques to recognize, identify and discriminate between human voices, voice characteristics for future verification and identification, computer recognition of voice and speech

Unit 4: **Image processing techniques**

Digital photography: processing pipeline and sensor characteristics, sensor identification. Anomaly detection: statistics of natural images, inconsistencies in lighting

and chromatic aberration, duplication detection .Image and video processing: re-sampling algorithms (rotation, scaling) and their identification via linear dependency patterns among adjacent pixels,

compression history identification, super-resolution. Document printer/scanner identification.

with focus on Steganography, watermarking, and fingerprinting: algorithms for hiding, recovering, detecting and distorting embedded signals, invariant properties

Paper -IV: CYBER CRIMES, DIGITAL FORENSIC & ITS EVIDENCES

Each Unit will have 25 marks and 18 lectures of 1 hr each.

Unit-1 (18 hrs)

Contextualising Digital Crimes:-

Undertaking Cyber Crimes- A sample of at least 25/30 cases in different categories, encompassing crimes against or/and supported by the computer and the network. This concern

Unauthorized access
Web Spoofing
Hacking and web defacement
Denial of service Attacks
Malicious Code
Financial Crimes – including online fraud, counterfeiting etc.
Social engineering Attacks
Password Cracking
Setganography
Identity theft
Cyber stalking
Pornography
Harassment
Murder and death threats
Gambling
Spamming
Sale of controlled items –tobacco wines etc.
Commercial espionage
Commercial extortion
Data manipulation
Software/hardware piracy
Money laundering
Threat or disruptions to health and safety, shut down or essential servies and extortions.
Espionage and terrorism
Others including, the ones involving mobile devices.

Unit- 2

Case studies rules and Procedues

Profiling the need to combat Digital crime by state Enforcement as well as comparing/contrasting cyber crimes with conventional crimes.
Information Technology Act-Penalties & offences, investigations and adjudication.
Indian Penal Law- An overview with relevant sections/rules highlighted.
Criminal Procedure code- An overview with relevant sections/rules highlighted.

Evidence Act –An overview with relevant sections/rules highlighted.

Critical Evaluation of Rules & Procedures:-

Are these enough/more to address digital crimes? Are there more challenges? A critical evaluation by participants who can work out 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 -3

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 be 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.

Investigating the crime scene by first responders

Introduction.

Electronic devices with their potential evidence profile

Securing the Scene & its Evaluation

Documenting the Scene

Evidence Collection

Packaging, Transportation and storage of Evidence collected.

Precautions in the investigation/examination of digital evidence

A brief summary as to the special precautions to be taken to document, collect, preserve and examine the fragile natured evidence, with due diligence. Fragile as it can be altered, damaged or destroyed by improper handling or examination losing evidence value.

Unit-4

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-trial communication between prosecutor, investigator and forensic examiners and also evidentiary issues like authentication and hearsay in digital evidence context.

Presentation of Digital Evidence would include educating the audience, what needs to be proved/disproved?, Expert witness/Scientific method evidence, recurring issues in computer crime trials with respect to identity, knowledge, chronology of events, Jury instructions, jury selection, presenting complicated technical issues.

List of Books:

1. Cyber Law in India by Farooq Ahmad- Pioneer Books
2. Infromation 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 Compney, Nagpur
6. The Information technology Act, 2000- Bare Act- Professional Book Publishers, New Delhi.
7. Computer Forensics: Principles and Practices by Linda Volonino, Reynaldo Anzaldua and Jana Godwin -Pearson Prentice-Hall 2007.
8. First Responder's Gude to Computer Forensics by Richard Nolan et al.- Carnegi Mellon, 2005.
9. Digital Evidence and Computer Crime, 2nd ed. By Eoghan Casey- Acdemic Press, 2004.
10. The Regulation of Cyberspace by Andrew Murray, 2006- Routledge -Cavendish.
11. Scene of the Cybercrime: Computer Forensics Handbook by Syngress.
12. Security and Incident Response by Keith J. Jones, Richard Bejtlich and Curtis W. Rose
13. List of Websites for more information is available on : Http://www.garykessler.net.library/forensicsurl.html

Paper -V: Practical Training

1. Finding results of different logic gates & 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 & Writing data on Floppy, CD, DVD, USB Thumbdrive.
5. Working with external storage devices using Linux - Reading & Writing data on Floppy, CD, DVD, USB Thumbdrive.
6. Understanding LAN - Client / Server, User creation, password protection.
7. Use of Internet - Visiting websites with given URL, searching information using search engine.
8. Use of E - mail - Creating e - mail ID, sending & receiving e - mails with attachments.
9. Networking commands - like ping, IPConfig, etc. with various switches.
10. Tracing E - mail - Finding senders IP Address of received e - mail, tracing route of e - mail received using tools available on internet e.g. Visual Trace Route etc.

Paper -VI: Report on Field Visit and Project Work

— ××× —