

RASHTRASANT TUKADOJI MAHARAJ NAGPUR UNIVERSITY, NAGPUR



P.G. DIPLOMA IN DIGITAL AND CYBER FORENSIC AND RELATED LAW

SCHEME OF EXAMINATION AND SYLLABUS

RASHTRASANT TUKADOJI MAHARAJ NAGPUR UNIVERSITY, NAGPUR
Syllabus for P.G. Diploma in Digital and Cyber Forensic and Related law

O -----:- Title of the Course: - P.G. Diploma in Digital and Cyber Forensic and related law

O -----:- Eligibility:. Bachelor Degree in Science excluding life science , Law with computer knowledge Engineering, IT, Computer Sciences, BCS, BCA, MCM, MCA, B.COM (Comp. Application)

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

R ----- :- Fee Structure: - As Per the State Government Rules

R -----:- Intake Capacity - 40

R -----:- 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 ----- :- Standard of Passing:-

- a. Candidate who secures minimum 35% in each subject/paper be declared to have passed the examination.
- b. A candidate who fails to secure 35% in a subject/Paper will be allowed to reappear in that subject/paper c. Candidate can carry forward at his/her option the marks in the subject/paper in which he/she has passed, in such a case student is entitled for award of class.
- c. Candidate who secures a minimum of 35% 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.
- d. Candidate who secures a minimum of 35% 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

Visit at Forensic Science Laboratory/other Laboratories

**Syllabus for P.G. Diploma in Digital and Cyber Forensic and
Related law Course Structure**

PAPER	TITLE OF PAPER	MARKS	LECTURES (1 hr. duration)
I	Basic of Computer and Internet Security	100	90
II	Advance Computers Security Techniques	100	90
III	Cyber Crimes and Investigation Procedures	100	90
IV	Cyberspace and Regulation under Law	100	90
V	Practical Training	100	90
VI	Project Work	100	90

Syllabus for

P.G. Diploma in Forensic Science and Related Law (PGDF)

Paper I: Basic of Computer and Internet Security

Paper II: Advance Computers Security Techniques

Paper III: Cyber Crimes and Investigation Procedures

Paper IV: Cyberspace and Regulation under Law

Paper V: Practical Training

Paper VI: Project Work

Paper I: Basic of Computer and Internet Security (Total 100 marks)

Unit I: Fundamentals of Computers	15 lectures
<ul style="list-style-type: none">• History Of computers• Areas of Application• Computers and its components• Advantages and Disadvantages of Computer• Application Software and System Software• The Memory Hierarchy and Cache Memory	
Unit II: Operating System and File System	15 lectures
<ul style="list-style-type: none">• Introduction to Operating System• Operating System Objectives and Functions• Study of Operating System<ul style="list-style-type: none">▪ Windows▪ Linux▪ Android• Introduction to File system<ul style="list-style-type: none">▪ FAT▪ NTFS▪ EXT	
Unit III: Basics of Networks	15 lectures
<ul style="list-style-type: none">• An Introduction to Networking• Network Topologies• Networking Standards and the OSI Model• Transmission Basics and Networking Media• Introduction to TCP/IP Protocols• Network Hardware• WANs and Remote Connectivity• Wireless Networking• Network Operating Systems	
Unit IV: Concept of Internet	15 lectures
<ul style="list-style-type: none">• Introduction to Internet• Application Areas of Internet• Working of Internet its Advantages and Disadvantages• Search Engines• Chat• E-mails and WWW• Internet Service Provider	

Paper II Advance Computers Security Techniques (Total 100 marks)

Unit I: Concealment Techniques	15 lectures
<ul style="list-style-type: none">• Spoofing• Hijacked session attacks• Polymorphism• Steganography• Reversing steganographic 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 II: Forensic speaker identification	15 lectures
<ul style="list-style-type: none">• Forensic-phonetic parameters:<ul style="list-style-type: none">▪ Acoustic vs. auditory parameters▪ Linguistic vs. non-linguistic parameters• Principles of Forensic speaker identification• Characterizing forensic speaker identification:<ul style="list-style-type: none">▪ Principles of Generation of speech and its uniqueness▪ Speaker recognition▪ Speaker identification and verification• Forensic significance: Phonemic structure	
Unit III: Image processing techniques	15 lectures
<ul style="list-style-type: none">• Image Processing Fundamentals:<ul style="list-style-type: none">▪ Digital Image Processing and Computer Graphics▪ Various Image Enhancement Techniques• Image Enhancement in the Spatial Domain:<ul style="list-style-type: none">▪ Gray level transformations▪ Histogram processing,▪ Arithmetic and logic operations,• Spatial filtering:<ul style="list-style-type: none">▪ Introduction▪ Smoothing and sharpening filters• Image Enhancement in the Frequency Domain:<ul style="list-style-type: none">▪ Frequency domain filters:<ul style="list-style-type: none">▪ Smoothing and Sharpening filters▪ Homomorphic filtering	
Unit IV: Computer Security	15 lectures

- Computer Security:
 - Information Security Overview
 - Information Security Services
 - Types of Attacks
 - Goals for Security
- 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 III: Cyber Crimes and Investigation Procedures (Total 100 marks)

Unit I: Introduction to Computer Forensics	15 lectures
<ul style="list-style-type: none"> • Introduction to Computer/Cyber Forensic • Cyber Forensic Steps <ul style="list-style-type: none"> ▪ Identification ▪ Seizure ▪ Acquisition ▪ Authentication ▪ Presentation ▪ Preservation) • Qualities and skills of Computer forensics Expert. • Goal of the Forensic Investigation • Why Investigate <ul style="list-style-type: none"> ▪ Internet usage exceeds norm ▪ Using email inappropriately ▪ Use of Internet, email, or PC in a non–work–related manner ▪ Theft of information ▪ Violation of security policies or procedures ▪ Intellectual property infractions ▪ Electronic tampering • Establishing a Basis or Justification to Investigate • Determine the Impact of Incident • Auditing V/s Cyber Forensic Investigations 	
Unit II: Cyber Crimes	15 lectures
<ul style="list-style-type: none"> • Types of Cyber Crimes <ul style="list-style-type: none"> ▪ Crimes targeting Computers: <ul style="list-style-type: none"> ○ Unauthorised Access ○ Packet Sniffing ○ Malicious Codes <ul style="list-style-type: none"> – Trojans – Viruses – Logic Bombs, etc ▪ Online based Cyber Crimes: <ul style="list-style-type: none"> ○ Phishing and its variants ○ Web Spoofing and E-mail Spoofing ○ Cyber Stalking ○ Web defacement ▪ Financial crimes, ATM and Card Crimes <ul style="list-style-type: none"> ○ Spamming Commercial espionage and Commercial Extortion ○ online Software and Hardware Piracy ○ Money Laundering Fraud & Cheating ○ Other Cyber Crimes 	
Unit III: Incident Response	15 lectures
<ul style="list-style-type: none"> • Introduction to Incident Response Process <ul style="list-style-type: none"> • What is Computer Security Incident? • What are the goals of Incident Response? 	

- Who is involved in Incident Response Process?
- Incident Response Methodology
- Formulate a Response Strategy
- Investigate the Incident
- Preparing for Incident Response
- Overview of Pre-incident Preparation
- Identifying Risk
- After Detection of an Incident.

Unit IV: Cyber Forensic Tools and Utilities

15 lectures

- Introduction
- Disk Imaging and Forensic tools (Any 2)
- Memory Forensic Tools (Any 2)
- Data Recovery Tools (Any 2)
- Network Forensic tools (Any 2)
- Mobile Forensic Tools (Any 2)

Paper IV- Cyberspace and Regulation under Law (Total Marks 100)

Unit I: Information Technology Act	15 lectures
<ul style="list-style-type: none">• Provisions in Indian Laws in dealing with Cyber Crimes and its critical analysis• Information Technology Act, 2000.• Penalties Under IT Act• Offences Under IT Act<ul style="list-style-type: none">▪ Offences Related with Digital Signature and Electronic Signature Under IT Act• Statutory Provisions Establishment of Authorities under IT Act and their functions, powers, etc<ul style="list-style-type: none">▪ Controller▪ Certifying Authorities▪ Cyber Regulation Appellate Tribunal▪ Adjudicating officer	
Unit II: International Framework of E-Commerce	15 lectures
<ul style="list-style-type: none">• International Organizations and Their Roles<ul style="list-style-type: none">○ ICANN○ URDP○ WTO○ TRIPS○ UNICITRAL Model Law• Evolution of IT Act - Genesis and Necessity• Digital/ Electronic Signature- Analysis in the background of Indian Laws• E-Commerce - Issues and provisions in Indian Law• E-Governance - concept and practicality in India• E-Taxation issues in Cyberspace	
Unit III: Domain Names and Trademark Disputes	15 lectures
<ul style="list-style-type: none">• Concept of Trademark/Domain Name• Cybersquatting• Reverse Hijacking• Jurisdiction in Trademark Disputes	
Unit IV: Concept of Copyright and Patent in Cyberspace	15 lectures
<ul style="list-style-type: none">• Copyright in the Digital Medium• Copyright in Computer Programmes• Copyright and WIPO Treaties• Concept of Patent Right• Relevant Provisions of Patent Act 1970	

Paper V - Practical Training (Total 100 marks)

90 Lectures

1. Finding results of different logic gates & their combinations.
2. Working in Windows and Linux Environment
3. Use of Internet – Visiting websites with given URL, searching information using search engine.
4. Networking commands – like ping, IPConfig, etc. with various switches.
5. 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.
6. Study of Encase software and its uses
7. Study of WinHex software and its uses.
8. Domain Name Registration
9. Creation and verification of Digital Signature, Study of Digital Certificate
10. Study of various commands in Linux like Encryption and Decryption, message digest etc.
11. Steganography using steganography tools (like Invisible Secret etc)
12. Concealment Techniques (Cloaking Techniques (Data Hide and Seek), Renaming Files, Manipulating File System, Data Hiding on NTFS

Paper VI

PROJECT WORK

(Total Marks100)

The project should be based on any topic based on the subjects related to the syllabus. The project report submitted by the student will be evaluated jointly by internal and the external examiner during the practical examination. The distribution of marks will be as follows:

- | | |
|--------------------------|----------------|
| 1) Project Report | 60marks |
| 2) Presentation | 20marks |
| 3) Viva-Voice | 20marks |

Recommended List of Books:

1. Cyber Law in India by Farooq Ahmad- Pioneer Books
2. Information Technology Law and Practice by Vakul Sharma- Universal Law Publishing Co. Pvt. Ltd.
3. The Indian Cyber Law by Suresh T. Vishwanathan- Bharat Law House New Delhi
4. Guide to Cyber and E- Commerce Laws by P.M. Bukshi and R.K. Suri- Bharat Law House, New Delhi
5. Guide to Cyber Laws by Rodney D. Ryder- Wadhwa and 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 Guide to Computer Forensics by Richard Nolan et al.- Carnegie Mellon, 2005.
9. Digital Evidence and Computer Crime, 2nd ed. By Eoghan Casey- Academic 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](http://www.garykessler.net.library/forensicsurl.html)
14. Introduction to Forensic Science in Crime Investigation By Dr.(Smt) Rukmani