



It is hereby inform to all concerned that, the syllabus prepared by the Ad-hoc Board in Forensic Science and recommended by the Dean, Faculty of Science & Technology the Hon'ble Vice-Chancellor has accepted the following syllabi in his emergency powers under section 12(7) of the Maharashtra Public Universities Act, 2016 on behalf of the Academic Council as appended herewith for University and Affiliated Colleges.

Sr.No.	Syllabus (under Choice Based Credit System)
1.	M.Sc. Forensic Cyber semester Ist to IVth.
2.	M.Sc. Forensic Toxicology semester Ist to IVth.
3.	M.Sc. Applied Physics and Ballistics semester Ist to IVth.
4.	PG Diploma in Digital and Cyber Forensic & Related Law semester Ist and IInd
5.	PG Diploma in Forensic Science & Related Law semester Ist and IInd
6.	Service Course

All concerned are requested to note the contents of this circular and bring notice to the students, teachers and staff for their information and necessary action.

REF.NO. SU/SCI/2021/4692-700
Date:- 06-12-2021.

Date:- 06-12-2021.

```

      *
      *
      *
foo  *
      *
* * * * *
      *

```

Deputy Registrar,
Academic Section.

- 1] **The Principal of all affiliated concerned Colleges,**
Dr. Babasaheb Ambedkar Marathwada University,
- 2] **Head of the Department, Department of Forensic Science,**
Dr. Babasaheb Ambedkar Marathwada University, Aurangabad.
- 3] **The Director, University Network & Information Centre, UNIC,**
with a request to upload this Circular on University Website.

- 1] The Director, Board of Examinations & Evaluation, Dr.BAMU, A'bad.
- 2] The Section Officer, [M.Sc.Unit] Examination Branch, Dr.BAMU, A'bad.
- 3] The Programmer [Computer Unit-1] Examinations, Dr.BAMU, A'bad.
- 4] The Programmer [Computer Unit-2] Examinations, Dr.BAMU, A'bad.
- 5] The In-charge, [E-Suvidha Kendra], Rajarshi Shahu Maharaj Pariksha Bhavan, Dr.BAMU, A'bad.
- 6] The Public Relation Officer, Dr.BAMU, A'bad.

**DR. BABASAHEB AMBEDKAR MARATHWADA
UNIVERSITY, AURANGABAD**



STRUCTURE AND CURRICULAM FOR

**Post Graduate Diploma in Digital and Cyber
Forensic & Related Law**

Effective from Academic

Year 2021-22

1

Handwritten signature and date 29/11/21
**Dean
Faculty of Science & Technology
Dr. Babasaheb Ambedkar Marathwada
University, Aurangabad**

Handwritten signature

Structure and Curriculum for P G Diploma in Digital and Cyber Forensics & Related Law

Preamble :-

The course of P G Diploma in Digital and Cyber Forensic & Related Law is divided in two semesters with total 40 credits. There shall be four theory papers & one theory based practical papers each semester and two mini projects distributed across the two semesters. These papers will be compulsory for all the admitted students.

Eligibility: Bachelor Degree in Science (excluding life sciences), Law (with computer knowledge)

Engineering, IT, Computer Sciences, BCS, BCA, MCM, MCA, B.COM (Comp. Application).

Intake Capacity :- 40 Seats to be filled as per following criterion.

- I) Thirty-two seats (80%) shall be reserved for the eligible candidates those have obtained the Bachelor's degree from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. These seats will go as per the reservation criteria of Govt. of Maharashtra.
- II) Four seats (10%) shall be reserved for the eligible candidate who has obtained their Bachelors' degree from an University within the State of Maharashtra other than Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Two seats will be for open and the other two will go as per the reservation criteria of Govt. of Maharashtra.
- III) Four seats (10%) shall be reserved for the eligible candidates who has obtained their Bachelors' degree from the any recognized university outside the state of Maharashtra and will be filled on the basis of merit.

Note: 1. The marks obtained by candidate from criteria II & III shall not be less than the marks of the last candidate admitted in respective category from criteria I above. If a candidate with such marks are not available then these seats will be filled up by candidate pertaining to criteria I.

- 2. If any seat remains vacant then it will be allotted to candidate pertaining to criteria I) above further vacant seat/s if any will be allocated to waitlist candidate belonging to criteria II or then to criteria III.*
- 3. Prevailing reservation policies of Maharashtra state and Dr. Babasaheb Ambedkar Marathwada University will be applicable.*
- 4. Admissions will be strictly on the basis of merit. If required, the Institution(s) offering this Post Graduate Diploma program may conduct a separate entrance examination at their level and may give the proportionate weightage.*

Choice Based Credit System (CBCS):-

The choice-based credit system has been adopted for PG Diploma course. This provides flexibility to make the system more responsive to the changing needs of our students, the professionals and society. Students will have to earn 40 credits for the award of P G Diploma in Forensic Science & Related Law.

Credit-to- contact hour Mapping:-

One contact hour per week is assigned 1 credit for theory and 0.5 credits for laboratory courses/ research project. Thus, a 4-credit theory paper corresponds to 4 contact hours per week and a 2-credit practical paper/research project corresponds to 4 contact hours per week.

Attendance:-

Students must have minimum of 75% attendance in each theory, practical and project paper for appearing examination otherwise he/she will not be strictly allowed for appearing the University examination. However, students having 65 % attendance may request Head of the concerned Institution for the condonation of attendance on medical ground.

Evaluation Methods:-

The assessment will be based on continuous internal assessment (CIA) and semester end examination (SEE).

There shall be Continuous Internal Assessment for each theory paper. In semester I and II, 20% (i.e., 10) marks shall be for CIA and 80% (i.e., 40) marks for SEE. Marks obtained by the student in all heads viz. CIA and SEE shall be added while declaring the final result.

Continuous Internal Assessment (CIA):-

The internal marks shall be assigned on the basis of tutorials/ home assignment /seminar presentation and weekly tests/preliminary examination to be conducted by the concerned Institution. These marks shall be communicated to the University before commencement of semester end examination.

Semester End Examination (SEE) :

- The semester end examination for each theory and practical paper shall be conducted by the University at the end of each semester.
- Duration of theory examination shall be of two hour for a paper of 40 marks. Practical examinations shall be of three-hour duration.
- The respective departments are advised to arrange maximum number of experiments from the list of experiments provided with the syllabus or experiments based on theory syllabus. However, a minimum of 06 experiments shall be reported in the journal for the purpose of certification for each practical paper.
- Students without certified journal shall not be allowed to appear for the practical examination.

Results Grievances / Redressal and ATKT rules :-

Result Grievances / redressal / revaluation and ATKT rules shall be as made applicable by the University from time to time.

Earning Credits:-

At the end of every semester, a letter grade will be awarded in each course for which a student had registered. A student's performance will be determined by the number of credits that he/she earned by the weighted Grade Point Average (GPA). The SGPA (Semester Grade Point Average) will be awarded after completion of respective semester and the CGPA (Cumulative Grade Point Average) will be awarded at the end of the 2nd semester by the University.

Grading System:-

A ten-point rating scale shall be used for the evaluation of the performance of the students to provide letter grade for each course and overall grade for the PG Diploma Programme. Grade points are based on the total number of marks obtained by him / her in all heads of the examination of the course. The grade points and their equivalent range of marks are shown in the following Table.

Table: Ten-point grade and grade description

Marks Obtained (%)	Grade Point	Letter Grade	Description
90-100	9.00- 10	O	Outstanding
80-89	8.00-8.90	A ⁺⁺	Exceptional
70-79	7.00-7.90	A ⁺	Excellent
60-69	6.00-6.90	A	Very Good
55-59	5.50-5.90	B ⁺	Good
50-54	5.00-5.40	B	Fair
45-49	4.50-4.90	C ⁺⁺	Average (Above)
41-44	4.1-4.49	C	Average
40	4.0	P	Pass
< 40	0.0	F	Fail (Unsatisfactory
	0.0	AB	Absent

- Nonappearance in any examination / assessment shall be treated as the students have secured zero marks in that subject examination / assessment.
- Minimum P grade (4.00 grade points) shall be the limit to clear / pass the course / subject. A student with F grade will be considered as 'failed' in the concerned course and he / she have to clear the course by appearing in the next successive semester examinations.
- Every student shall be awarded grade points out of maximum 10 points in each subject (based on 10-point scale). Based on the grade points obtained in each subject, Semester Grade Point Average (SGPA) and then Cumulative Grade Point Average (CGPA) shall be computed. Results will be announced at the end of each semester and CGPA will be given on the completion of PG Diploma program.

Computation of SGPA (Semester Grade Point Average) and CGPA (Cumulative Grade Point Average)

Grade in each paper will be calculated based on the summation of marks obtained in internal and semester end examination.

The computation of SGPA and CGPA will be as below

- Semester Grade Point Average (SGPA) is the weighted average points obtained by the students in a semester and will be computed as follows

$$\text{SGPA} = \frac{\text{Sum (Course Credit X Number of Grade Points in concern Course Gained by the Student)}}{\text{Sum (Course Credit)}}$$

The SGPA will be mentioned on the mark sheet at the end of every semester.

- The Cumulative Grade Point Average (CGPA) will be used to describe the overall performance of a student in all semester of the course and will be computed as under.

$$\text{CGPA} = \frac{\text{Sum (All four Semester SGPA)}}{\text{Total Number of Semester}}$$

The SGPA and CGPA shall be rounded off to the second place of decimal.

Grade Card:-

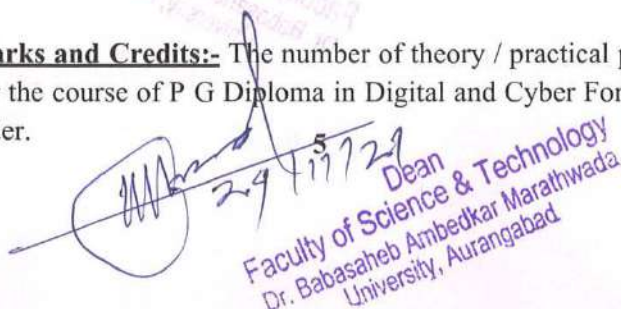
Results will be declared and the grade card (containing the grades obtained by the student along with SGPA) will be issued by the university after completion of every semester. The grade card will be consisting of following details.

- Title of the courses along with code opted by the student.
- Credits associated with the course.
- Grades and grade points secured by the student.
- Total credits earned by the student in a particular semester.
- Total credits earned by the students till that semester.
- SGPA of the student.
- CGPA of the student (at the end of the 2nd semester).

Cumulative Grade Card:-

The grade card sheet showing details grades secured by the student in each paper in all semester along with overall CGPA will be issued by the University at the end of 2nd semester.

Distribution of Marks and Credits:- The number of theory / practical papers and marks / credit allotted for the course of P G Diploma in Digital and Cyber Forensics & Related Law shall be as under.



Year	Semester	No. of papers			Total Marks				Total Credits			
		Theory	Practical	Project	Theory	Practical	Project	Total	Theory	Practical	Project	Total
One year	Sem.-I	4	1	1	400	100	100	600	16	2	2	20
	Sem.-II	4	1	1	400	100	100	600	16	2	2	20
TOTAL		8	2	2	800	200	200	1200	32	4	4	40

Course Structure of P G Diploma in Digital and Cyber Forensics & Related Law:-

SEMESTER – I					Marks		
Paper No.	Paper Code	Title	No. of Credits	Hrs. /week	Internal (CIA)	External (SEE)	Total
I	PGDC1T1	Basics of Computer and Cyber Forensics	4	4	20	80	100
II	PGDC1T2	Computer Security	4	4	20	80	100
III	PGDC1T3	Cyber Law	4	4	20	80	100
IV	PGDC1T4	Fundamentals of Cyber Crime	4	4	20	80	100
V	PGDC1P1	Practical based on PGDC1T1 & PGDC1T2	2	4	--	100	100
VI	PGDC1P2	Mini Project-I (Synopsis & Literature review)	2	4	20	80	100
TOTAL			20	24	100	500	600
SEMESTER – II					Marks		
Paper No.	Paper Code	Title	No. of Credits	Hrs. /week	Internal (CIA)	External (SEE)	Total
VII	PGDC2T1	Computer Crime Scene Investigation	4	4	20	80	100
VIII	PGDC2T2	Digital Forensics and Incident Response	4	4	20	80	100
IX	PGDC2T3	Intellectual Property Rights in Cyber Space	4	4	20	80	100
X	PGDC2T4	Crime Investigations, Trials and Related Laws	4	4	20	80	100
XI	PGDC2P1	Practical based on PGDC2T1 & PGDC2T2	2	4	--	100	100
XII	PGDC2P2	Mini Project-II (Based on Mini Project I)	2	4	20	80	100
TOTAL			20	24	100	500	600

[Handwritten signature]
29/11/21

Dean
Faculty of Science & Technology
Dr. Babasaheb Ambedkar Marathwada University, Aurangabad

Dean
Faculty of Science & Technology
Dr. Babasaheb Ambedkar Marathwada University, Aurangabad

Paper No	Code	Title	Marks	Credits
I	PGDC1T1	BASIC OF COMPUTER FORENSICS	100	4

Unit I

Computer Forensics Fundamentals: Introduction to Computer Forensics , Use of Computer Forensics in Law Enforcement ,Computer Forensics Assistance to Human Resources/ Employment Proceedings, Computer Forensics Services Benefits of Professional Forensics Methodology, Steps Taken by Computer Forensics Specialists, Who Can Use Computer Forensic Evidence?

Unit II

Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analyzing malicious software. Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems

Unit III

Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems ,Router Forensics. Cyber forensics tools and case studies. Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.

Unit IV

Data Recovery: Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution, Hiding and Recovering Hidden Data

REFERENCES:

1. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, John R. Vacca, Charles River Media, 2005.
2. Cyber Forensics - Concepts and Approaches, Ravi Kumar & B Jain, 2006, icfai university press
3. Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl, 2010, Second Edition, Springer's.
4. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri, First edition, 2009 .
5. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics), 2010

Paper No	Code	Title	Marks	Credits
II	PGDC1T2	COMPUTER SECURITY	100	4

Unit I

What Is Computer Security- Values of Assets, The Vulnerability–Threat–Control Paradigm. Threats- Confidentiality, Integrity, Availability, Types of Threats, Types of Attackers. Harm- Risk and Common Sense, Method–Opportunity–Motive. Vulnerabilities, Controls.

Authentication-Identification Versus Authentication, Authentication Based on Phrases and Facts: Something You Know, Authentication Based on Biometrics: Something You Are, Authentication Based on Tokens: Something You Have, Access Control- Access Policies, Implementing Access Control, Procedure-Oriented Access Control, Role-Based Access Control.

Unit II

Program Security: Secure programs, Non-malicious program errors, Viruses and other malicious code, Targeted malicious code, Controls against program threats

Web Security: Sources of Attacks: Internal, External. Types of attacks: Denial of Service (DOS), TCP/IP insecurity, Eavesdropping, Sniffing/Snooping/Wiretapping.

Tools of use: Ethereal, Wireshark, Etherpeek, Packet Spoofing, Replay, Message Integrity, Phreaking

Unit III

Database Security: Introduction to Database, Basics of SQL, Security requirements, Reliability and integrity, Sensitive data, Interface, Multilevel database, Proposals for multilevel security.

Operating System Security: Protected objects and methods of protection, Memory address protection, Control of access to general objects, File protection mechanism.

Authentication: Authentication basics, Password, Challenge-response, Biometrics.

Unit IV

Security in Networks: Threats in networks, Network security control, Firewalls, Intrusion detection systems, Secure e-mail, Networks and cryptography, Example protocols: PEM, SSL, IPsec

IDS: Network based Intrusion Detection and Prevention Systems, Host based Intrusion Prevention System

Network Forensics: Scientific Overview, Principles of network forensics, Attack Traceback and attributes, Critical Needs Analysis.

TEXTBOOKS:

1. Web application vulnerabilities: detect, exploit, prevent, By Michael Cross, Steven Palme

REFERENCES:

1. Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, fifth edition, 2015 Pearson Education.

Paper No	Code	Title	Marks	Credits
III	PGDCIT3	Cyber Laws	100	4

Unit I

Fundamentals of Cyber Law : Introduction on cyber space , Jurisprudence of Cyber Law , Scope of Cyber Law, Cyber law in India with special reference to Information Technology Act, 2000(as amended) and Information Technology Act, 2008

Unit II

E- Governance and E – Commerce: Electronic Governance, Procedures in India, Essentials & System of Digital Signatures , The Role and Function of Certifying Authorities ,Subscriber and controller, Digital contracts ,UNCITRAL Model law on Electronic Commerce ,Cryptography – Encryption and decryption.

Unit III

Legal Recognition of Electronic Records: Electronic record as per IT Act, Securing Electronic records and secure digital signatures , Admissibility of electronic record (Section 65 A and Section 65 B of IEA), Conditions of admissibility of electronic record, Supreme Court Judgments on admissibility of electronic record, Authentication of electronic records.

Unit IV

Cyber Offences and Penalties: Penalty and compensation for damage to computer, computer system, etc., Compensation for failure to protect data, Penalty for failure to furnish information, return, etc., with special reference to Information Technology Act.

Paper No	Code	Title	Marks	Credits
IV	PGDC1T4	Fundamentals of Cyber Crime	100	4

Unit I

Cyber Crime: Historical perspective to Cyber Crime, Meaning & definitions of Cyber Crimes , Convention V/s Cyber Crimes, Misuse of Technology, factors leading to increase in Cyber Crimes, Tools and Techniques Used to Commit Cyber Crimes, Threats to national security.

Unit II

Classification of Cyber Crimes: Cyber Criminals, Relevant Cyber Crimes other than IT Act, 2000, Cyber Crime in Modern Society, Different Kinds of Cyber Crime, measures for prevention of cyber crimes, Impact of cyber warfare on privacy, identity theft, Social Networking Sites vis-à-vis Human Rights.

Unit III

Cyber Crimes & e-commerce : Impact of cyber crime on Businesses, Concept of e-Commerce and Types of e-Commerce, 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 debit card/credit card/virtual card frauds.

Unit IV

Cyber Crime and Criminal Justice: Concept of Cognizable and Non-Cognizable Offences, bailable & non-bailable offences, compoundable and non-compoundable offences, Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography, Identity Theft & Fraud, Cyber terrorism and Cyber Defamation, Concepts of Arrest.

Paper No	Code	Title	Marks	Credits
V	PGDC1P1	Practical based on PGDC1T1 & PGDC1T2	100	2

List of Experiments

(Minimum 6 Experiments)

1. Working of Image Master Solo
2. Working of Drive Locker
3. Working of cloning software for hard disk using workstation.
4. Working of data recovery softwares like Minitool, EaseUS, etc.
5. Working of packet capturing and analysis tools.
6. Working of Intrusion Detection Software
7. Working of database security tools like Nmap, Scuba, etc.
8. Working of malware analysis software.
9. Virtual Box installation
10. Demonstration and handling of workstation computer

Paper No	Code	Title	Marks	Credits
VI	PGDC1P2	Mini Project –I	100	2

Minimum six activities out of the following list have to be conducted from the list

S/R	Topic	Number
1	Seminar	02
2	Bok review	02
3	Case Study	05
4	Field visit	02
5	Review of research paper	05
6	Project	01

-----END OF SEMESTER-I-----

Semester II

Paper No	Code	Title	Marks	Credits
VII	PGDC2T1	COMPUTER CRIME SCENE INVESTIGATION	100	4

Unit I

Computer Investigation Process : Introduction to Computer Investigation, Investigating Computer Crime, Policy and Procedure Development , Before Starting the Investigation, Legal Considerations, Investigating Methodology, Evaluating the Case, Collecting the Evidence, Examining and Collecting Evidence, Securing the Computer Evidence, Processing Location Assessment, Write Protection, Evidence Assessment, Evidence Examination, Analysis of Extracted Data

Unit II

Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Investigating Web attacks, Investigating network Traffic ,Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events.

Unit III

Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene, Computer Evidence Processing Steps, Legal Aspects of Collecting and Preserving Computer Forensic Evidence.

Unit IV

Computer Forensics Analysis: Discovery of Electronic Evidence, Identification of Data, Reconstructing Past Events.

Networks: Network Forensics Scenario, A Technical Approach, Destruction of Email, Damaging Computer Evidence, Tools Needed for Intrusion Response to the Destruction of Data, System Testing.

REFERENCES:

1. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition, John R. Vacca, Charles River Media, 2005.
2. Cyber Forensics - Concepts and Approaches, Ravi Kumar & B Jain, 2006, icfai university press
3. Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl, 2010, Second Edition, Springer's.
4. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri, First edition, 2009 .
5. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics), 2010

Paper No	Code	Title	Marks	Credits
VIII	PGDC2T2	Digital Forensics and Incident Response	100	4

Unit I

Introduction to Incident handling: Computer Security Incident, Types of incidents, Why necessary, Goals, Purpose, Organizational Roles. Incident Response Methodology.

Preparing for incident Response- Identifying Risk, Preparing Individual Hosts, Preparing Network ,Establishing Appropriate Policies & Procedures, Creating Response Toolkit, Establishing an Incident Response Team.

Unit II

After detection of Incident- Overview of IR phases, documenting steps, Establishing an incident notification procedure, Recording Details After Initial Detection, Conducting Interviews, Formulating a Response Strategy.

Initial Response: Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system.

Forensic Duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive

Unit III

Storage And Evidence Handling : File Systems for window, linux and Mac OS, Forensic Analysis of File Systems - Storage Fundamentals-Storage Layer, Hard Drives.

Evidence Handling: Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure.

Unit IV

Network Forensics: Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud. Systems Investigation and Ethical Issues.

Data Analysis Techniques - Investigating Live Systems (Windows & Unix) - Investigating Hacker Tools - Ethical Issues – Cybercrime. Report Writing Guidelines, A Template for Digital and Cyber Forensics report.

Reference Books:

1. Kevin Mandia, Chris Prosise, "Incident Response and computer forensics", Tata McGrawHill, 2006.
2. Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999.
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001.
4. Skoudis. E., Perlman. R. Counter Hack: "A Step-by-Step Guide to Computer Attacks and Effective Defenses", .Prentice Hall Professional Technical Reference. 2001.
5. Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information From a Computer", Paladin Press, 2000.
6. Bill Nelson, Amelia Philips and Christopher Steuart, "Guide to computer forensics and investigations", course technology, Cengage Learning; 4th edition, ISBN: 1-435-49883-6, 2009.

Paper No	Code	Title	Marks	Credits
IX	PGDC2T3	Intellectual Property Rights in Cyber Space	100	4

Unit I

Cyber Space: Fundamentals, various definitions, Interface of Technology and Law, Jurisprudence and Jurisdiction in Cyber Space, extra-territorial jurisdiction: Challenges, Cyber Jurisdiction: An Indian Context, Enforcement agencies and correctional measures.

Unit II

Intellectual Property Rights : Concept of IPR, Important international conventions and Treaties, Paris Industrial Property Convention, Berne Convention, WIPO copyright Treaty, ROME Convention for protection of Performers, producers and broadcasting organization, TRIPS Agreement on Trade related aspects of IPR, Brussels satellite convention, IPR infringements, Civil and Criminal liabilities under IPR.

Unit III

IPR in Cyber Space: Intellectual Property Rights– Copyrights, Copyrights v/s Patents debate, Authorship and Assignment Issues, Copyright in Internet- Multimedia and Copyright issues, Software Piracy, Trademarks - Trademarks in Internet – Copyright and Trademark cases, Trade mark law and Domain name dispute with case laws, Software and Business Method Patents, Data Privacy in cyber space.

Unit IV

Patent Law: Basics of Patent Law, Conditions of Patentability, Product Patent and Process Patent, WIPO Patent Co-operation Treaty, Geneva convention on Patent Law, Software and Business Method Patents, Indian Patent Act, Infringement, Defenses

Paper No	Code	Title	Marks	Credits
X	PGDC2T4	Cyber Crime Investigations and Related Laws	100	4

Unit I

Concept of Digital 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, 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, Cyber Espionage.

Unit II

Procedural aspects of Cyber Crime: How to Combat Digital Crime by State Enforcement Agency, IT Act-Penalties & Offences, Investigations and Adjudication. Indian penal law – An overview with relevant sections(IPC and IT Act)/ rules highlighted, Procedure of Filing cyber crime complaint.

Unit III

Cyber Crime and Criminal Procedure Code: An overview with relevant sections/ rules highlighted, Search and seizure provisions under Cr.P.C., power of police to arrest and Warrant of arrest under Cr.P.C., Provisions relating to preventive actions of the police, Power of police for investigation in cognizable and non cognizable cases.

Unit IV

Courtroom presentation of digital evidence: Hierarchy of Criminal Courts, concept of digital/electronic evidence, Courtroom presentation and evidence rules: An emphasis on the preliminary considerations for the prosecutor when reviewing the scope of the investigation to date, Integrity, Discovery, and Disclosure of Digital Evidence, Presentation of Digital Evidence, Reliability of Digital Evidence, Evidentiary value of cyber forensic experts, Investigator and forensic examiners and also evidentiary issues like authentication and hearsay in digital evidence context.

Paper No	Code	Title	Marks	Credits
XI	PGDC2P1	Practical based on PGDC2T1 & PGDC2T2	100	2

List of Experiments

(Minimum 6 Experiments)

1. F-RAT Installation and Registry analysis
2. Working in Windows and Linux Environment
3. Use of Internet – Visiting websites with given URL, searching information using search engine.
4. Dos Commands and 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 and Hosting 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 No	Code	Title	Marks	Credits
XII	PGDC2P2	Mini Project-II	100	2

Minimum six activities out of the following list have to be conducted from the list

S/R	Topic	Number
1	Seminar	02
2	Bok review	02
3	Case Study	05
4	Field visit	02
5	Review of research paper	05
6	Project	01

-----END OF THE SYLLABUS-----

[Handwritten signature]

[Handwritten signature]
29/12/29

Dean
Faculty of Science & Technology
Dr. Babasaheb Ambedkar Marathwada
University, Aurangabad