Dr. BABASAHEB AMBEDKAR MARATHWADA UNIVERSITY, AURANGABAD

CIRCULAR NO.SU/Sci. & Tech./Colleges./NEP/23/2023

It is hereby inform to all concerned that, the syllabi prepared by the Board of Studies & Ad-hoc Boards and recommended by the Dean, Faculty of Science & Technology, the Hon'ble Vice-Chancellor has accepted **the following curriculum of All Post Graduate Degree Courses as per Norms of National Education Policy – 2020 under the Faculty of Science & Technology run to the Affiliated Colleges, Dr.Babasaheb Ambedkar Marathwada University** in his emergency powers under section 12(7) of the Maharashtra Public Universities Act, 2016 on behalf of the Academic Council as appended herewith.

Sr.No.	Syllabi of Affiliated BAMU, Aurangabad.	Semester
1.	M.Sc. Biotechnology	Ist and IInd Semester
2.	M.Sc.Forensic Science.	Ist and IInd Semester
3.	M.Sc Forensic Cyber.	Ist and IInd Semester
4.	One Year PG Diploma in Forensic Sci. & Realated Law	Ist and IInd Semester
5.	One Year PG Diploma in Digital and Cyber Forensic and Related Law.	Ist and IInd Semester
6.	M.Sc.Forensic Applied Physics and Ballistics	Ist Semester
7	M.Sc.Forensic Toxicology.	Ist Semester

This is effective from the Academic Year 2023-24 and onwards.

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

University Campus,
Aurangabad-431 004.
REF.NO.SU/NEP/2023/10092-100
Date:- 16.08.2023.

★★★★★

Deputy Registrar,
Academic Section

Copy forwarded with compliments to :-

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

Copy to :-

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.
7] The Record Keeper, Dr.BAMU,A'bad.

Dr. BABASAHEB AMBEDKAR MARATHWADA UNIVERSITY, AURANGABAD

NAAC Reaccredited with 'A' Grade

Faculty of Science and Technology

1 Year P.G. Diploma Programme

Digital and Cyber Forensic and Related Law

Course Structure and Curriculum for Affiliated Colleges
(Outcome-Based Credit System)

As per National Education Policy 2020
(Effective from Academic Year -2023-24)

Table of Contents

Table of Contents

Preamble

The extent and nature of cybercrime have increased tremendously in the last few decades. The changing modus operandi of crime has become more challenging for law enforcement agencies. The program has been designed keeping in mind to give a brief idea of law and digital forensics to the students, which can make them suitable for the industry/law enforcement agencies. Dr. Babasaheb Ambedkar Marathwada University, Aurangabad is committed to providing a comprehensive syllabus for PGD in Digital and Cyber Forensics and Related Law in line with the objectives and philosophies of National Education Policy 2020.

Course Structure

The Course Structure as per the Government Resolution of the Department of Higher and Technical Education, Government of Maharashtra Dated 16/05/2023 is as follows:

Credits Distribution Structure for One Year PG Diploma Program

Faculty of Science & Technology

Year / level	Sem.	Major subject		RM	OJT /FP	RP	Credits	Degree
		DSC Core Mandatory	DSE (Elective)					
First year 6.0	I	3(4) +2=14	4	4			22	PG Diploma (After 3 years degree)
	II	3(4) +2=14	4		4 Complete during summer break		22	
Cum. Cr. For PG Diploma		28	08	4	4		44	

Abbreviations

Major: A course, which should compulsorily be studied by the student as a requirement of core or major subject is termed as a core course.

DSE: Generally, a course that can be chosen from a pool of courses that may be very specific or specialized or advanced, or supportive to the discipline/subject of study or which provides an extended scope or which enables exposure to some other discipline/subject/domain or nurtures the candidates' proficiency/skill is called as an elective course.

OJT: On-Job Training: Internship/Apprenticeship

FP: Field Project

RP: Research Project

Vision

The vision of the curriculum is as follows:

- To produce graduates with the highest skill and professional ethics competitive to the global forensic demands.

Mission

The mission of the curriculum is as follows:

- To facilitate the updated domain knowledge and skills at par with the global forensic scenario
- To inculcate professional ethics, teamwork, leadership, and value system among students
- To provide research skills among students for further learning and finding innovative solutions

Program Educational Objectives

The educational objective of the PG program in Forensic Science is as follows:

- **PEO1:** To develop scientific and technical competency among graduates leading to a successful career in forensic sciences and allied disciplines
- **PEO2:** To develop analytical and problem-solving skills among students to solve complex issues/problems related to forensic analysis in crime investigation
- **PEO3:** To inculcate professionalism, ethics, teamwork, communication, and leadership quality in the students
- **PEO4:** To make the students responsive toward the environment and society
- **PEO5:** To inculcate the practices of lifelong learning in the direction to have a successful career and responsive citizen of the globe

Program Outcomes and Program Specific Outcomes

The university is committed to implementing a student-centric curriculum throughout its programs. Program outcomes, program-specific outcomes, and course outcomes have been defined as per Bloom's taxonomy. These are as follows:

Program Outcomes (POs): Program outcomes describe what skills, knowledge, and behaviors students acquire as they progress through the program. The program outcomes are as follows:

PO1: Basic and Discipline-specific knowledge: Apply the knowledge of basic and applied sciences, engineering, social sciences, and arts to various forensic problems.

PO2: Problem Analysis: Identify and analyze forensic problems using standard methods based on a scientific approach.

PO3: Modern tool usage: Understand, select, and apply appropriate techniques, resources, and modern scientific techniques with an understanding of their merits and limitations.

PO4: Design/ Develop research-based solutions: Design novel solutions for regular or complex problems based on research outcomes.

PO5: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of forensic practices.

PO6: Effective Communication: Speak, read, write, and listen clearly in person and through electronic media in English and in one Indian language, and make meaning of the world by connecting people, ideas, books, media, and technology.

PO7: Forensic practices for society and criminal Justice setup: Understand and analyze the impact of forensic solutions to society and criminal justice setup.

PO8: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in a multidisciplinary setting.

PO9: lifelong learning: Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of Technological change.

Program-Specific Outcomes (PSOs): Program Specific Outcomes are statements that describe what the graduates of a specific program should be able to do. The PSOs of the PGD in Digital and Cyber Forensics and Related Laws are as follows:

- **PSO1:** Understand the basic and advanced techniques in digital forensics and law
- **PSO2:** Analyze the cases/practical scenarios raising in cybercrime using basic and state-of-the-art techniques of digital forensics.
- **PSO3:** Interpret the court orders and observations for various forensic cases
- **PSO4:** Evaluate the results of various techniques and make decisions on simple or complex problems of the digital domain.

Eligibility

A candidate who has passed the following: B.Sc. in any discipline (three-year program) except life sciences/ LLB (supported by computer courses) / Engineering/ IT/ Computer Science/BCS/BCA/MCM/MCA/B. Com (Computer Applications) or equivalent degree from a recognized university with 45% marks will be eligible for getting admission to PG Diploma in Digital and Cyber Forensics and Related Law.

Duration

As per the guidelines of the Government of Maharashtra and the university, the PG Diploma Program will be of one-year duration. However, the students need to pass the minimum credits within four years from the date of admission.

Medium of Instruction

Presently, the medium of instruction is English. However, any change in this will be as per the guidelines of the university and the government of Maharashtra.

Attendance

Students must have a minimum of 75 % attendance in each theory and practical course for appearing in the Semester End Examination (SEE), otherwise he/she will not be strictly allowed for appearing for the SEE. However, students having 65 % attendance may request the Head of the concerned Institution for the condonation of attendance on medical grounds.

Assessment Scheme/Scheme of Examination

The assessment scheme is as follows:

- Each course has been assigned marks equivalent to 25 marks/credit. Thus, each theory course is 75/100 marks while the practical/Laboratory course is 25/50 marks. Moreover, On-Job-Training shall be 100 marks.
- Continuous Internal assessment (CIA) will be for 40% while Semester End Examination (SEE) will be for 60%.
- It shall be mandatory for the students to pass individually for both SEE and CIA for each course to complete the program successfully.
- Passing percentage for both theory and practical shall be 40%.
- The CIA may be in terms of class tests, group, and individual assignments, and presentation. Two tests on completion of 40%, and 100% syllabus, each of 20 marks will be conducted and the average result will be reported. Presentation of 10 marks

and assignments of 10 marks will also be conducted to get an aggregate of 40% weightage.

- Changes in the examination scheme are possible as per the guidelines issued by the university from time to time.

Curriculum and Structure as per NEP 2020

As per the Government Resolution of the Department of Higher and Technical Education, Government of Maharashtra, the course structure of the PG program in Forensic Science is as follows:

Credit distribution and structure of the one-year program in PGD Digital and Cyber Forensics and Related Law

PG Diploma (First Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Theory	Practical	Theory	Practical	
Major Mandatory DSC	DFL/MJ/500T	Introduction to Computer and Cyber Forensics	3	-	3	-	3
	DFL/MJ/501T	Computer Security	3	-	3	-	3
	DFL/MJ/502T	Cyber Laws	3	-	3	-	3
	DFL/MJ/500P	Practical based on DFL/MJ/500T	-	2	-	1	1
	DFL/MJ/501P	Practical based on DFL/MJ/501T	-	2	-	1	1
	DFL/MJ/502P	Practical based on DFL/MJ/502T	-	2	-	1	1
	DFL/MJ/503P	Skill/Practical based activity	-	4	-	2	2
DSE (Choose any one of the courses: theory and practical together makes a complete course)	DFL/DSE/504T	Cybercrime, e-commerce, and criminal justice	3	-	3	-	3
	DFL/DSE/504P	Practical based on DFL/DSE/504T	-	2	-	1	1
	DFL/DSE/505T	Cyber Psychology-I	3	-	3	-	3
	DFL/DSE/505P	Practical based on DFL/DSE/505T	-	2	-	1	1
	DFL/DSE/506T	A course from SWAYAM or another Digital Platform	3	-	3	-	3
	DFL/DSE/506P	Practical based on DFL/DSE/506T	-	2	-	1	1
RM	DFL/RM/509	Research Methodology	4	-	4	-	4
			16	**12**	**16**	**06**	**22**

PG Diploma (Second Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Theory	Practical	Theory	Practical	
Major Mandatory DSC	DFL/MJ/550T	Computer Crime Scene Investigation	3	-	3	-	3
	DFL/MJ/551T	Digital Forensics and Incident Response	3	-	3	-	3
	DFL/MJ/552T	Intellectual Property Rights in Cyber Space	3	-	3	-	3
	DFL/MJ/550P	Practical based on DFL/MJ/550T	-	2	-	1	1
	DFL/MJ/551P	Practical based on DFL/MJ/551T	-	2	-	1	1
	DFL/MJ/552P	Practical based on DFL/MJ/552T	-	2	-	1	1
	DFL/MJ/553	Skill/Practical based activity	-	4	-	2	2
DSE (Choose any one of the courses: theory and practical together makes a complete course)	DFL/DSE/554T	Crime Investigation, Trials, and Laws	3	-	3	-	3
	DFL/DSE/554T	Practical based on DFL/DSE/554T	-	2	-	1	1
	DFL/DSE/555T	Cyber Psychology-II	3	-	3	-	3
	DFL/DSE/555P	Practical based on DFL/DSE/555P	-	2	-	1	1
	DFL/DSE/556T	Course based on SWAYAM or other Digital platforms	3	-	3	-	3
	DFL/DSE/556P	Practical based on DFL/DSE/556P	-	2	-	1	1
OJT/FP	DFL/OJT/FP/559	OJT/FT	-	8	-	4	4
			12	**20**	**12**	**10**	**22**

Detailed Curriculum of Semester-I

Discipline-Specific Core Courses

DFL/MJ/500T	Introduction to Computer and Cyber Forensics	Credit:03	Contact Hours:45	Marks:75

Course Overview

The course covers basic concepts of computer and cyber forensics.

Course Objectives

The course has the following objectives:

- Students will gain an idea of computer and cyber forensics
- Students will learn computer and cyber forensic tools
- Students will have an understanding of data recovery and related concepts
- Students will learn various types of computer forensics systems

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Define and explain concepts of computer and cyber forensics
- CO2: Apply various computer and cyber forensics fundamentals in the real crime scenario
- CO3: Analyze various physical evidence and its involvement in crime
- CO4: Compare properties of various evidence of computer related crime

Unit	Course Content	Contact Hours
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?	09
Unit-II	**Introduction to Cyber Forensics** • Information Security Investigations, Corporate	09

	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.	**09**
Unit-IV	**Computer and Cyber Forensics tools** • Computer and Cyber forensics tools and case studies. Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking	**09**
Unit-V	**Data Recovery** • Data Recovery Defined, Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-	**09**

	Recovery Solution, Hiding and Recovering Hidden Data	

Suggested Readings/Reference Books:

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,ChristofPaar, 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

***

DFL/MJ/500P	Practical based on DFL/MJ/500T	Credit:01	Contact Hours:30	Marks:25

Course Overview

This is a laboratory course based on Introduction to Computer and Cyber Forensics (DFL/MJ/500T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical

(Minimum of 10 practical has to be performed for successful completion of the course)

1. To make a forensic copy using Image Master Solo
2. To verify the original and forensic copy using various hash algorithms
3. To create a forensic image using FTK imager
4. To create a forensic image using EnCase imager
5. To create a forensic image using Forensic Explorer imager
6. To understand the workings of Drive Locker
7. To understand the workings of cloning software for hard disk using the workstation.
8. To perform data recovery from the physical drive of the given media using software like Minitool.
9. To perform data recovery from the physical drive of the given media using software like EaseUs.
10. To perform data recovery from the logical drive of the given media using software like Minitool
11. To perform data recovery from the logical drive of the given media using software like EaseUs.
12. To analyze and inspect recovered data using various tools
13. To perform a case study using computer and cyber forensics tools
14. To perform a case study on a hacked/compromised system

***

DFL/MJ/501T	Computer Security	Credit:03	Contact Hours:45	Marks:75

Course Overview

The course covers basic concepts of computer security

Course Objectives

The course has the following objectives:

- Students will gain a basic idea of computer security
- Students will learn concepts of program and web security
- Students will have an understanding of database and operating system security
- Students will learn concepts of network security and network forensics

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Define and explain concepts of computer security
- CO2: Apply various tools to explore and analyze the threat analysis of various components of computer systems and network
- CO3: Analyze various compromised system
- CO4: Compare the performance of various tools on vulnerability analysis

Unit	Course Content	Contact Hours
Unit-I	**Computer Security** • Computer Security definition and 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.	09

Unit-II	**Program and Web Security** • 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	**09**
Unit-III	**Database and Operating System Security** • 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.	**09**
Unit-IV	**Network Security** • Security in Networks: Threats in networks, Network security control, Firewalls, Intrusion detection systems, Secure e-mail, Networks, and cryptography, Example protocols: PEM, SSL, IPsec	**09**

	• IDS: Network-based Intrusion Detection and Prevention Systems, Host-based Intrusion Prevention System	
Unit-V	**Network Forensics** • Network Forensics: Scientific Overview, Principles of network forensics, Attack Traceback and attributes, Critical Needs Analysis.	**09**

Suggested Readings/Reference Books:

1. Web application vulnerabilities: detect, exploit, prevent, By Michael Cross, Steven Palme.
2. Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, fifth edition, 2015 Pearson Education.

***

DFL/MJ/501P	Practical based on DFL/MJ/501T	Credit:01	Contact Hours:30	Marks:25

Course Overview

This is a laboratory course based on Computer Security (DFL/MJ/501T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical

(Minimum of 10 practical has to be performed for successful completion of the course)

1. Working with packet capturing and analysis tools.
2. Working on Intrusion Detection Software
3. Working with database security tools like Nmap, Scuba, etc.
4. Working on malware analysis software.
5. Virtual Box installation
6. Demonstration and handling of workstation computer
7. To analyze e-mail for its origin
8. To perform case study on Denial-of-Service attack
9. To perform threat analysis of a given network
10. To capture and analyse network packets using various software
11. To crack password of a locked system using Brute-force algorithm
12. To perform case study on security issues on the recently attacked systems

***

DRL/MJ/502T	Cyber Laws	Credit:03	Contact Hours:45	Marks:75

Course Overview

The course covers the cyber laws in India especially as per the provisions of the Information Technology Act.

Course Objectives

The course has the following objectives:

- Students will gain an idea of Cyber laws in India
- Students will learn about e-governance and e-commerce
- Students will have an understanding of the admissibility of electronic records
- Students will learn about cyber offenses and the penalties

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Define and explain the provisions of cyber law in India
- CO2: Understand the procedure of e-governance in India
- CO3: Describe cyber offenses and their penalty
- CO4: Compare punishment over the severity of the crime

Unit	Course Content	Contact Hours
Unit-I	**Introduction to Cyber Laws** • Introduction to cyberspace, 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	09
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.	09
Unit-III	**Legal Recognition of Electronic Records**	09

	• 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 offenses and penalty** • Penalty and compensation for damage to the 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.	**09**
Unit-V	**Impact of IT Act on other related act** • Amendments to Indian Penal Code • Amendments to Indian Evidence Act • Amendments to the Reserve Bank of India Act	**09**

Suggested Readings/Reference Books:

1. Commentary on The Information Technology Act by J N Barowalia, Abhishek Barowalia
2. The Information Technology Act, 2000, Bare Act with short notes, Universal's New Delhi, 2022
3. Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce, Vakul Sharma and Seema Sharma 2021
4. Bharat's The Indian Cybar Law with The Information Technology Act 2000 by Suresh T Viswanathan Edition 2022

***

DRL/MJ/502P	Practical based on FRL/DSE/502T	Credit:01	Contact Hours:30	Marks:25

Course Overview

This is a laboratory course based on Cyber Laws (DRL/DSE/502T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 6 practical has to be covered in the semester for successful completion of the course.

List of Practical

(Minimum of 6 practical has to be performed for successful completion of the course)

1. Perform a case study on the status of the Examiner of Electronic Records in India
2. Perform a case study on the admissibility of electronic records compiling the various Supreme courts judgments
3. Perform a case study on e-governance policy in India
4. Perform a case study on the status of cyber infrastructure in India
5. Perform a comparative study of cyber laws of India and other countries
6. Perform a case study on the judgment on IT Act (Case can be taken from any of the Civil/High/Supreme Courts) **(minimum three different cyber offences).** While performing the study consider the following:
    a. Nature of crime
    b. Modus operandi
    c. Mens rea
    d. Factors that take the offender to commit the crime
    e. Provisions of punishment under the law for that crime
    f. The punishment given to the offender

***

DFL/MJ/503P	Skill/Practical-Based Activity	Credit:02	Contact Hours:60	Marks:50

Course Overview

The course has been designed to let the students acquire skills in his/her area of interest. As the aim of the course is to develop skills, the students can choose any one of the activities, which can be conducted under the guidance of a teacher. In the end, students have to prepare a report on the acquired skill listing the practical work carried out throughout the semester.

List of activities

- Data recovery using various tools
- Vulnerability analysis and intrusion detection
- Forensic analysis of network packets
- Any other skill-based activities chosen by the students as per their interests

***

Discipline-Specific Elective Courses

DFL/DSE/504T	Cybercrime, e-commerce, and Criminal Justice	Credit:03	Contact Hours:45	Marks:75

Course Overview

The course covers basic concepts of computer and cyber forensics.

Course Objectives

The course has the following objectives:

- Students will gain an idea of computer and cyber forensics
- Students will learn computer and cyber forensic tools
- Students will have an understanding of data recovery and related concepts
- Students will learn various types of computer forensics systems

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Define and explain concepts of computer and cyber forensics
- CO2: Apply various computer and cyber forensics fundamentals in the real crime scenario
- CO3: Analyze various physical evidence and its involvement in crime
- CO4: Compare properties of various evidence of computer-related crime

Unit	Course Content	Contact Hours
Unit-I	**Cyber Crime** • Historical perspective on Cyber Crime, Meaning & definitions of Cyber Crimes, Convention V/s Cyber Crimes, Misuse of Technology, factors leading to an increase in Cyber Crimes, Tools and Techniques Used to Commit Cyber Crimes, and Threats to national security.	09
Unit-II	**Classification of cyber crimes** • 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	09

	prevention of cybercrimes, Impact of cyber warfare on privacy, identity theft, Social Networking Sites vis-à-vis Human Rights.	
Unit-III	**Cyber crime and e-commerce-I** • 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.	**09**
Unit-IV	**Cyber crime and e-commerce-II** • 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.	**09**
Unit-V	**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.	**09**

Suggested Readings/Reference Books:

1. An Introduction to Cyber Crime and Cyber law by R.K. Chaubey, 2021
2. Cyber Law Simplified by Vivek Sood, Tata McGraw Hill.
3. Computer Forensics and Cyber Crime by Marjie T. Britz, Pearson

***

DFL/DSE/504P	Practical based on DFL/DSE/504T	Credit:01	Contact Hours:30	Marks:25

Course Overview

This is a laboratory course based on Cybercrime, e-commerce, and criminal justice (DFL/DSE/504T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 6 practical has to be covered in the semester for successful completion of the course.

List of Practical

(Minimum of 6 practical has to be performed for successful completion of the course)

1. Perform a case study to analyze factors leading to an increase in cyber crime
2. Perform a case study to analyze the women related crime in cyberspace
3. Perform a comprehensive analysis of a particular type of cyber crime committed in the last five years across the States of India using NCRB Data. **(Minimum three)**
4. Perform a case study highlighting the legal issues in e-banking/internet/mobile banking
5. Perform a case study on a particular cybercrime where judgment has been pronounced (Case can be taken from any of the Civil/High/Supreme Courts) **(minimum three different types of cyber crime).** While performing the study consider the following:
    a. Nature of crime
    b. Modus operandi
    c. Mens rea
    d. Factors that take the offender to commit the crime
    e. Provisions of punishment under the law for that crime
    f. The Punishment given to the offender

***

DRL/DSE/505T	Cyber Psychology-I	Credit:03	Contact Hours:45	Marks:75

Course Overview

The course covers cyberpsychology. Cyberpsychology is the study of persons in the context of human–technology interaction. As a developing field, cyberpsychology research encompasses a host of psychological phenomena associated with or affected by emerging technologies.

Course Objectives

The course has the following objectives:

- Students will gain an idea of psychology
- Students will learn concepts of cyberpsychology
- Students will have an understanding of the personality types in cyberspace
- Students will learn about psychotherapy in cyberspace

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Define and explain the concepts of psychology and cyberpsychology
- CO2: Understand the psychology of internet users
- CO3: Describe the context of technology use
- CO4: Compare personality types in cyberspace

Unit	Course Content	Contact Hours
Unit-I	**Introduction to Psychology** • History and Approaches in Psychology; Biological Basis of Behavior; Sensation and Perception; Cognition-Learning, Memory, Motivation, Emotion; Personality.	09
Unit-II	**Introduction to Cyberpsychology** • Concept and Meaning of Cyberpsychology; Historical Developments of Cyberspace; • Transfer and Interference of Online Learning Behavior; Defining Cyber Culture; Biological and Technological Bases of Cyber Culture; Models and Metaphors in Cyber Culture; Psychology of Internet.	09

Unit-III	**Personality types in cyberspace** • Classification of Personality Types; Narcissistic-Schizoid, Paranoid, Depressive, Manicmasochistic, Obsessive/Compulsive, Psychopathic, Histrionic, Schizotypal; Anti-social Personality Disorder; Gaming Disorder.	**09**
Unit-IV	**Context of technology use** • Evolving Relationship with Digital Technology; Subjective Understanding of Technology; Life Stages, Life Orientations, and Context References	**09**
Unit-V	**Psychotherapy in cyberspace** • Counseling via e-mail- real-time chat-audio-video conferencing-therapeutic virtual environments-Accessibility Cost- Empathy- It's Thinking and Learning- Personality Feelings- Rapport-Task Performance; Online and Computer-Mediated Psychotherapy; • Disorder support group-internet Addiction Disorder (IAD)- Diagnostic Criteria.	**09**

Suggested Readings/Reference Books:

1. Attrill, A. (2015), Cyberpsychology, Oxford University Press: Oxford.
2. Turkle, Sh. (1984), The Second Self: Computers and the Human Spirit. Touchstone Book, N.Y. (pp. 30-32 & 326-332)
3. Norman, L.K. (2008), Cyberpsychology: An Introduction to Human-Computer Interaction, Cambridge University Press

***

DRL/DSE/505P	Practical based on FRL/DSE/505T	Credit:01	Contact Hours:30	Marks:25

Course Overview

This is a laboratory course based on Cyber psychology-I (DRL/DSE/505T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 6 practical has to be covered in the semester for successful completion of the course.

List of Practical

(Minimum of 6 practical has to be performed for successful completion of the course)

1. To carry out Minnesota Multiphasic Personality Inventory-2/A (MMPI-2/A)
2. To measure Mobile Phone Addiction Scale
3. To perform Mental Status Examination
4. Taking Case History
5. Coping Responses Inventory for Adult/Children
6. Perform Alienation Scale
7. Perform Rorschach Inkblot Test
8. Perform Miller Forensic Assessment of Symptoms Test
9. Case Study on cybercrime and human behavior

***

DRL/DSE/506T	Courses on SWAYAM and other digital platforms	Credit:03	Contact Hours:45	Marks:75

Course Overview

- There is a provision that the student can select the course from SWAYAM or another digital platform. The student can select a course of 3/4 credits. The other guidelines will be issued by the university from time to time

***

DRL/DSE/506P	Practical Based on FRL/DSE/506T	Credit:01	Contact Hours:30	Marks:25

Course Overview

- The practical will depend on the structure of course available on platform. In case there is only theory course of 4 credits, the students will be free to opt the same.

***

Research Methodology

DRL/RM/549	Research Methodology	Credit:04	Contact Hours:60	Marks:100

Course Overview

- The course gives an overview of research methodology, research writing, and selection of research problems.

Course Objectives

The course has the following objectives:

- Students will gain an idea of research and describe the research process and research methodology
- Students will learn qualitative research and methods used to execute and validate qualitative research
- Students will have an understanding of how to apply the basic aspects of the research process in order to plan and execute a research project.
- Students will able to present, review and publish scientific articles

Course Outcomes

After the completion of the course, the students will be able to do the following:

- CO1: Understand and explain the research process
- CO2: Perform systematic literature survey, formulation of a research topic, study design, analysis and interpretation of data.
- CO3: Design a research approach for a specific research issue of their choice
- CO4: Create a research document for the implementation of the research project

Part-I (30 Contact Hours)

Unit	Course Content	Contact Hours
Unit-I	**Fundamentals of Research** • Introduction to research methodology, definition and basic concepts of research, objectives of research, motivation behind a research, types of research, research process: defining research problem, review the literature, formulation of hypothesis, research design, collection and analysis of data, interpretation and writing a report. Criteria for good research, measuring research impact and quality: JCR report,	10

	impact factor and citation index, ethics and scientific conduct, Ethics in human and animal studies.	
Unit-II	**Writing and Presenting Research** • Components of research paper: the IMRAD system, title, authors and addresses, abstract, acknowledgments, references, tables, and illustration; preparation for publication, submission of manuscript, publication processes; presentation of research: oral and poster presentations, presentation and submission of research proposals to the funding agencies.	**10**
Unit-III	**Funding Agency and Plagiarism** • A brief idea about funding agencies for research and development: UGC, CSIR, DFSS, DST, ICMR, BPR&D, DBT, BARTI. • Plagiarism: definition, types, consequences, UGC regulations.	**10**

Part II (30 Contact Hours)

Presentations, case studies, Assignments, and Tutorials based on Units I to III **(30 Hrs.)**

Students are expected to do the followings

1. Select a broad area of research
2. Read the basic concepts/fundaments of the broad topic
3. Identify 10 SCOPUS / WEB OF SCIENCE Indexed Journals related to the broad topic
4. Search and download 20 research articles from the above research Journals
5. Do systematic review of above 20 research articles
6. While doing review of each of above mentioned 20 research articles, students are expected to prepare notes on following points
    - What are the objectives of the research article?
    - What methodology has been adopted?
    - What are prominent results?
    - How these results of relevant to the latest development of the subject?
    - What is novelty of research article?
    - What are prominent shortcomings of this research a presented in this research article?

- What are your plans to address those shortcomings?

7. Draft the fine-tuned title of research project
8. Draft hypothesis
9. Draft Objectives and Methodology
10. Draft expected outcome of the research project

At the end of the assignment, students are expected to prepare a report having following points

1. Fine-tuned title of Research Project
2. Fundamental aspects of the fine-tuned research topic
3. Hypothesis
4. Objectives
5. Methodology
6. Detailed Experimental plan
7. Expected outcome
8. References

References:

1. Research Methodology by Dr. S. L. Gupta, Hitesh Gupta; International Book House Pvt Ltd **(2013),** ISBN-10: 8191064278, ISBN-13: 978-8191064278
2. Basic Research Methods-Gerard Guthrie SAGE Publications, India, Pvt Ltd, New Delhi **(2010),** ISBN-10: 8132104579, ISBN-13: 978-8132104575
3. Research Methodology-methods and techniques By C. R. Kothari, New Age International Publishers **(2011)** ISBN 978-81-224-1522-3
4. Principles of Research Methodology- Phyllis G. Supino, Jeffrey S. Borer; Springer, Verlag New York **(2012),** ISBN-ebook: 1461433592, ISBN (Hardcover): 978-1461433590
5. Research Design Qualitative, Quantitative. and Mixed Methods Approaches- John W. Creswell; SAGE Publications Ltd, UK **(2011),** ISBN-9780857023452
6. Research Methodology -A Step-by-Step Guide for Beginners- Ranjit Kumar; Sage Publications Ltd**(2010)**, ISBN- 1849203016.
7. Scientific Writing and Communication- Angelika Hofmann; Oxford University Press, US **(2010),** ISBN-13-: 978-0 199947560, ISBN-10: 01 99947562
8. Writing Science: How to Write Papers That Get Cited and Proposals That Get Funded- Joshua Schimel, Oxford University Press, **(2011)**, ISBN: 9780199760237
9. Handbook of Scientific Proposal Writing- A.YavuzOruc; CRC Press, Taylor & Francis group **(2011)**, ISBN: 9781439869185

***