Dr. HOMI BHABHA STATE UNIVERSITY, MUMBAI

Faculty of Science and Technology

Syllabi for One-Year Postgraduate Diploma Programmes in

1. Forensic Science and Related Laws
2. Digital & Cyber Forensics and Related Laws
3. Cyber Security and Related Laws

As per National Education Policy (NEP) – 2020 Guidelines

SEMESTER-WISE SYLLABUS

(Theory and Practical)

Semester I and II

To Be Implemented From Academic Year

2024-25

Preamble

India is a rising economic power among the G-20 nations and rising as world leader in multiple sectors. Being a fastest-growing economy, the country also faces many challenges. The need of hour is to address such challenges to safeguard and strengthen our nation's interest. One of the challenges is changing crime landscape and dynamics both in physical and digital world, crime is relentlessly improvising and rapidly evolving; the crime rate is directly proportional to the economic growth of the country. It calls for equally competent minds to provide them with quality education and impart skill-based curriculum, to raise human resource in Forensic Science, Cyber and allied domains. Aiming towards the dream of a crimeless society, victim centric, speedy justice and high conviction, not only promises well-being to the people but also fosters the progress and strengthening of the nation. Maharashtra being a progressive state of country, to achieve the goal of creation of highly specialized and skillful human resources, the Government of Maharashtra realizing the urgency of such skilled manpower to address the future challenges, government set up the state-of-art institutions dedicated to higher education in Forensic Science and allied domains. The courses in the programme are well structured and designed by seeking guidance and inputs from various experts in the field of Forensic Science. The seven subjects incorporated in the degree are chosen from the major domains of Forensic Science. To provide various public and private sectors with experts who are efficient, able and competent is the goal of the Institution. The Department of Higher and Technical Education, Government of Maharashtra has started three Institutes of Forensic Science at Mumbai, Aurangabad and Nagpur. Dr. Homi Bhabha State University through its constituent institute namely the Institute of Forensic Science, Mumbai offers one-year Postgraduate Diploma (PGD) Programmes in Forensic Science and Related Laws (PGD-FSRL), Digital & Cyber Forensics and Related Laws (PGD-DCFRL) and Cyber Security and Related Laws (PGD-CSRL) and adapted the framework directed by Ministry of Education as per NEP 2020. It encompasses a holistic, flexible and over all development of the learner.

Accordingly, the curriculum designed with the advice of the experts in the field and in compliance with NEP 2020 which ensures the learners are equipped with adequate skills and knowledge to provide expertise in the respective fields after successful completion of the programme. The new NEP 2020 curriculum also encourages them to develop critical thinking and analytical skills, new ideas and strategies for effective crime solving along with holistic development of the learner.

INTRODUCTION

These programmes are designed to provide a comprehensive and in-depth understanding of the fascinating world of Forensic Science and related subjects. Through a rigorous academic curriculum and hands-on research experience, the aim is to nurture the intellectual curiosity and scientific acumen of the students, preparing them for successful careers in various sectors of forensic sciences. These PGD programmes are structured to equip students with a strong theoretical foundation, practical skills, and critical thinking abilities necessary to address the challenges and opportunities in the diverse fields of forensics. These programmes shall necessarily provide an opportunity for working professionals for skill enhancement in their field of work. Whether the passion lies in research, industry, education, or beyond, this program aims to provide the knowledge and skills necessary to excel in the chosen path of the learners. The ultimate goal of the institute is to encourage and support holistic development of the students; to ensure all the students reach their maximum potential inspiring them towards a society which is grounded in equality and flourished with ideas of innovation and creation.

ABBREVIATIONS

1. B.Sc. – Bachelor of Science
2. M.Sc. – Master of Science
3. DSC – Discipline Specific Core
4. DSE – Discipline Specific Elective
5. NHEQF – National Higher Education Qualification Framework
6. CBCS – Choice Based Credit System
7. HEIs – Higher Education Institutes
8. NCrF – National Credit Framework
9. NCVET – National Council for Vocational Education and Training
10. NEP – National Education Policy
11. NSEQF – National School Education Qualification Framework
12. NIOS – National Institute of Open Schooling
13. NSQF – National Skill Qualifications Framework
14. UGC – University Grants Commission
15. OJT – On Job Training/ Internship/ Apprenticeship
16. FP – Field projects
17. RM – Research Methodology

PROGRAMME STRUCTURE & DISTRIBUTION OF CREDITS

Each of the PG Diploma programme are divided into two semesters with a total **44** credits. During each of the programme students must take **9** theory courses, a total of **2** practical lab courses, and **1** On-job training, spread over two semesters. Each theory course shall consist of four units. Lab course (practical paper) shall consist of a minimum of ten experiments based on the theory papers. In Semester-I, there are five theory papers which includes 03 Mandatory courses and 01 Minor Research Methodology course, and 01 lab course (practical paper) based on the core subjects, whereas 01 elective Major theory paper to be selected by the students from amongst the two papers given in the list. Similarly, Semester-II, there are four theory papers that includes 03 Mandatory theory courses, and 01 lab course (practical paper) based on the core subjects, whereas one elective Major theory paper to be selected by the students from amongst the two papers given in the list. Additionally, the student must earn 04 credits of On Job Training (OJT) / Field Project (FP) during summer break. A student earns 22 (twenty-two) credits per semester and a total of 44 (eighty-eight) credits in two semesters.

After completing any of these one-year PG Diploma programmes, students are not eligible for admission to M.Sc. (Forensic Science) programme offered by the Institute of Forensic Science, Mumbai.

ELIGIBILITY

For all the offered Postgraduate Diploma programmes, the eligibility is Any Graduate. Successful completion of 3-year graduation degree in any subject of any faculty.

INTAKE CAPACITY

The total intake for the one-year Postgraduate Diploma Programmes in each of the offered programmes shall be 20 seats. The seats shall be filled strictly on the basis of merit (Graduation) and prevailing state reservation policies.

DURATION OF THE PROGRAMME

The duration of all the Postgraduate Diploma Programmes is 1 year (2 semesters).

CHOICE OF ELECTIVE COURSES

The student must select any one of the electives in each semester. The student is not allowed to change the selected elective after 15 days from the commencement of respective semester. For each elective, there shall be a minimum of 25% of the intake/ on roll students. If inadequate

students have opted for any specific elective in such circumstances whether to run or not such electives shall be sole discretion of the Director/ Principal of the Institute/ College.

Batch size for practical:

The guidelines by the University Grants Commission (Minimum Standards of Instruction for the Grant of the Master's Degree through Formal Education) Regulations, 2003 has given the directives in this regards but as per the availability of infrastructure, the batch size for practical sessions may differ. As per the availability of the laboratory infrastructure, the batch size shall be decided. There shall be not more than 10 students in a batch for all Postgraduate laboratory courses. The batch size may vary as per the guidelines of Dr. Homi Bhabha State University, Mumbai from time to time.

EXAMINATION AND EVALUATION

As suggested in NEP 2020, continuous internal evaluation is proposed. Total evaluation is proposed in a 60:40 ratio for external: internal evaluation. There will be no internal evaluation for lab courses. Each course carries a defined number of credits. The credits are based on the course structure, including the teaching mode and the number of contact hours for lecture, tutorial, and practical classes. One hour of theory/tutorial teaching per week equals one credit, and two hours of laboratory/ demonstration classes per week equals one credit. Credits are considered based on the number of contact hours, course content, teaching methodology and allotted maximum marks.

While calculating the grading, one credit is equal to 25 marks in a semester. Thus, 4 credit courses will receive 100 marks and 2 credit courses will receive 50 marks. The proportion of marks earned in a course and the credits given to that course will be used to calculate the Semester Grade Point Average (SGPA) or Cumulative Grade Point Average (CGPA).

General Education credit refers to a unit by which the course work is measured. It determines the number of hours of instructions required per week. One credit is equivalent to one hour of teaching [lecture or tutorial] or two hours of practical work/ field work per week. Accordingly, one Credit would mean equivalent to 15 hrs. of theory or 30 hrs. of workshop/ lab/ Internship/ OJT/ FP/ CEP/ CC work per semester.

For the ease of calculation, the break-up of credit with respect to general education component is as in the table below:

Theory **1 Credit = 15 hours**	**Practical** **1 Credit = 30 hours**	**Experiential learning including relevant experience and professional levels acquired** **1 Credit = 30 hours**

Credits will be used to quantify the relative value of the subjects. The result will be declared based on Semester Grade Point Average (SGPA), or Cumulative Grade Point Average (CGPA) earned.

Choice-Based Credit System (CBCS) is followed for the programme which allows students to tailor their educational journey according to their interests and career aspirations. As per NEP 2020, continuous evaluation through class tests, presentations and tutorials will be conducted. The total evaluation will be in the ratio of 60:40 ratio for External : Internal evaluation. There will be no internal evaluation for lab courses.

- The student will have to have minimum of 75% attendance in each head of evaluation.
- Candidates are expected to pass separately in theory (Internal and external), and practical examination. Minimum marks for passing in the subject would be 40 % in each separate head of evaluation for Theory (Internal), Theory (External) and practical examination.
- 60% External Assessment and 40% Internal Assessment only for theory-based papers (No internal assessment for practical/ project/ OJT/ RP)

Internal Assessment:

Internal assessment to be conducted by department teachers (Continuous Evaluation). Internal assessment marks should be submitted to the University one month prior to the final examination.

Sr. No.	Credits	Total Marks	Internal	External
1.	4	100	40	60

No internal assessment for practical/ project/ OJT/ RP.

The distribution of 40 marks for evaluation of internal assessment will be as follows:

1. 20 marks – One written test (Objective type) to be conducted.

2. 20 marks – Student will be evaluated on Seminar/presentation/ literature Survey & evaluation/ Assignment / Project work/ Output from group -collaboration work (For project work, there should not be more than 3 students per group). Abstract or report must be submitted by the student to the Department. Department must maintain documented proofs of the above-mentioned evaluation method.

Setting of Question Papers for External Theory Courses:

The following are the guidelines for paper setting of a 4 credits theory courses of 60 marks. The duration of the external theory exam shall be 2.5 hrs.

Que. No.	Unit	Sub-questions	Marks allotted to each sub-question	Total Marks
1	I	5	5	15
2	II	5	5	15
3	III	5	5	15
4	IV	5	5	15
			Grand Total	**60**

All questions are compulsory.
Student shall attempt 3 sub-questions out of 5 sub-questions from each question.

Practical Examination:

- ✓ For certification, minimum ten experiments shall be reported in the journal of each practical course.
- ✓ Practical evaluation for Major/ Minor (DSC/DSE) papers will carry 25 marks per credit.
- ✓ Practical examination will be conducted at the end of each semester. The student must be present with the duly certified journal, failing which they will not be allowed for the practical examination. In case of loss of a journal, a report must be obtained from the head/coordinator failing which the student will not be allowed to appear for the practical examination.
- ✓ Each lab course shall have an external examination for 50 marks of 4 Hrs duration. The distribution of marks shall be – Two experiments for a maximum of 20 marks each, Viva-voce for maximum of 05 marks and maximum of 05 marks for the certified journal.
- ✓ Projects, industrial training, industrial / field visits will be conducted and assessed as per the need in the curriculum.

On-job Training (OJT)/ Field Project (FP):

Every student is required to take up On Job Training (OJT)/ Field Project (FP) that shall be from the relevant discipline approved by the university. OJT/ FP has to be completed during the summer vacation period and the report of the same needs to be submitted to the Institute at the end of the Sem-II.

OJT/ FP shall be evaluated at the end of Sem-II. For evaluation there shall be a minimum of two examiners, one preferably external.

Transfer of Admissions, Attendance, Results, Grievances/ Redressal and ATKT rules:

Transfer of Admissions, Attendance, Results, Grievances/ redressal/ revaluation and ATKT rules shall be as made applicable by the Dr. Homi Bhabha State University, Mumbai from time to time.

Modification to the Regulations:

Notwithstanding the foregoing, any amendments / modifications issued or notified by the Dr. Homi Bhabha State University, Mumbai/ Department of Higher and Technical Education, Government of Maharashtra/ University Grants Commission/ Higher Education Commission of India and its verticals such as National Higher Education Regulatory Council, General Education Council or the State Government, from time to time, shall be deemed to have been incorporated into these Regulations and shall constitute an integral part of these Regulations.

Ad-hoc BoS in Forensic Science
Credit Distribution of PGD FSRL

Yr	Lvl	Sem	Major		Minor	OE	VSC, SEC (VSEC)	AEC, VEC, IKS All Mandatory	OJT, FP, CEP, CC, RP	Cum. Cr. / Sem	Cum. Cr. / Degree
			Mandatory	Electives							
1	6.0	I	DSC1-1 DFFSDC101T Fundamentals of Forensic Science (4)	DSE1-1 DFFSDE101T Introduction to Forensic Physics & Forensic Psychology (4) **OR** DSE1-1 DFFSDE102T Special Law-I (4)	DSC2-1 DFFSRM101T Research Methodology (4)	—	—	—	—	**22**	**44** **PG Diploma in Forensic Science and Related Laws (44)**
			DSC1-2 DFFSDC102T Introduction to Forensic Biology (4)								
			DSC1-3 DFFSDC103T Criminal Law-I (4)								
			DSC1-4 DFFSLB104P Lab Course – I (2)								
		II	DSC1-5 DFFSDC201T Fingerprints & Questioned Documents (4)	DSE2-1 DFFSDE201T Digital Forensics (4) **OR** DSE2-1 DFFSDE202T Special Law-II (4)	—	—	—	—	OJT/ RP/ FP DFFSOJ201P / DFFSFP201P (4)	**22**	
			DSC1-6 DFFSDC202T Introduction to Forensic Chemistry (4)								
			DSC1-7 DFFSDC203T Criminal Law-II (4)								
			DSC1-8 DFFSLB204P Lab Course – II (2)								
Cum. Cr.			**28**	**8**	**4**	—	—	—	**4**	**44**	
Award of PG Diploma in Forensic Science and Related Laws with 44 credits											

Postgraduate Diploma in Forensic Science and Related Laws

Teaching and Examination Scheme – Semester I

Course	Course Code	Course Title	Credits	Teaching Scheme				Examination Scheme						
								Theory				Practical		
				Lectures per Week	Practical per Week	Total Periods	Duration in Hours	Max. Marks (Theory)	Max. Marks (Internal)	Total Marks	Minimum Passing Marks*	Max. Marks	Total Marks	Minimum Passing Marks*
DSC1-1	DFFSDC101T	Fundamentals of Forensic Science	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-2	DFFSDC102T	Introduction to Forensic Biology	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-3	DFFSDC103T	Criminal Law-I	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-4	DFFSLB104P	Lab Course – I	2	-	1	4	4	-	-	-	-	50	50	20
DSE1-1	DFFSDE101T	Introduction to Forensic Physics & Forensic Psychology	4	4	-	4	4	60	40	100	40	-	-	-
DSE1-1	DFFSDE102T	Special Law-I	4	4	-	4	4	60	40	100	40	-	-	-
DSC2-1	DFFSRM101T	Research Methodology	4	4	-	4	4	60	40	100	40	-	-	-
		Total	**22**	20	1	24	24	300	200	**500**	-	50	**50**	-

Teaching and Examination Scheme – Semester II

DSC1-5	DFFSDC201T	Fingerprints & Questioned Documents	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-6	DFFSDC202T	Introduction to Forensic Chemistry	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-7	DFFSDC203T	Criminal Law-II	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-8	DFFSLB204P	Lab Course – II	2	-	1	4	4	-	-	-	-	50	50	20
DSE2-1	DFFSDE201T	Digital Forensics	4	4	-	4	4	60	40	100	40	-	-	-
DSE2-1	DFFSDE202T	Special Law-II	4	4	-	4	4	60	40	100	40	-	-	-
OJT-1 / FP-1	DFFSOJ201P / DFFSFP201P	On Job Training / Field Project	4	-	1	8	8	-	-	-	-	100	100	40
		Total	**22**	16	2	28	28	240	160	**400**	-	150	**150**	-

*Candidates shall pass separately in each head of assessment (i.e. Theory (External), Theory (Internal) and Practical examination) with minimum 40% marks.

SEMESTER – I

Mandatory	
Course DSC1-1: DFFSDC101T	**Course Title: Fundamentals of Forensic Science**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand the history, need and scope of forensic science
2. To understand the basic principles of forensic science
3. To understand the organizational set up of forensic science laboratories in India
4. To understand the concept of crime scene, crime scene processing and management
5. To apply the concepts and process of crime scene reconstruction

Course Contents: Introduction to Forensic Science; Evolution and Structure of Forensic Science in India; Crime Scene Investigation and Evidence Management; Principles and Methods of Crime Scene Reconstruction		**Reqd. Hrs.**
Unit I – Introduction to Forensic Science		**15 Hrs.**
	• Definition, Nature, Need and Scope of Forensic Science • Historical development of Forensic Science: Global perspective • Key contributions in the history of Forensic Science • Principles of Forensic Science • Forensic Scientist: Education, Training, Ethical considerations, Role and Responsibilities	
Unit II – Evolution and Structure of Forensic Science in India		**15 Hrs.**
	• Forensic Science in pre independent India • Forensic Science in Independent India • Organizational structure and role of Forensic Science Laboratories • Various branches of Forensic Science • Emerging Trends in Forensic Science	
Unit III – Crime Scene Investigation and Evidence Management		**15 Hrs.**
	• Definition and importance of a Crime Scene • Types of Crime Scene • Process of Crime Scene Investigation and Management • Crime Scene Documentation • Evidence and its types • Occupational health and safety for Forensic Scientist	

Unit IV – Principles and Methods of Crime Scene Reconstruction		15 Hrs.
	• Importance and Principles of Crime Scene Reconstruction • Methods of Crime Scene Reconstruction • Steps involved in Crime Scene Reconstruction • Scene Specific Reconstruction • Report writing and Expert testimony	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Apply forensic science principles in investigations 2. Understand the role and working of forensic science laboratories in India 3. Identify, preserve and document crime scene 4. Identify, collect and preserve various evidences on crime scene 5. Perform crime scene reconstruction

Suggested Readings:

1. Lee, H. C., Palmbach, T., Miller, M. T. (2001). Henry Lee's Crime Scene Handbook, Netherlands: Elsevier Science.
2. James, S. H., Nordby Ph.D., J. J., Bell, S., Williams, L. J. (2014). Forensic Science: An Introduction to Scientific and Investigative Techniques, Fourth Edition. United States: Taylor & Francis.
3. Saferstein, R. (2018). Criminalistics: An Introduction to Forensic Science, 12th Edition.
4. Sharma, B. R. (2021). Forensic Science in Criminal Investigation & Trials, India: Universal/ Lexis Nexis.
5. Crime Scene Management with Special Emphasis on National level Crime Cases: Dr. Rukmani Krishnamurthy
6. Ratan Deepak & Zaidi Mohd. Hasan (2008) – Forensic Science in India and the World, Alia Law Agency, Alahabad-211 001
7. B S Nabar Forensic Science In Crime Investigation 3rd Edn. Reprint 2023, Asia Law House, Hyderabad
8. Nanda, B. B., Tewari, R. K. (2001). Forensic Science in India: A Vision for the Twenty-first Century. India: Select Publishers.
9. V. N. Sehgal, N. Surinder (2012) Forensic Science and its related issues, Selective and Scientific Books, Delhi
10. Houck, M. M., Siegel, J. A. (2015). Fundamentals of Forensic Science. Netherlands: Elsevier Science.

11. Fisher, B. A., Tilstone, W. J., Woytowicz, C. (2009). Introduction to Criminalistics: The Foundation of Forensic Science. United Kingdom: Elsevier Science.
12. A laboratory manual for the introduction to the Crime Lab, L.J. Kaplan, 2001, Williamstown, Massachusetts.
13. Crime Scene to Court: The Essentials of Forensic Science. (2020). United Kingdom: Royal Society of Chemistry.
14. Jones, P., Williams, R. E. (2009). Crime Scene Processing and Laboratory Workbook. United Kingdom: Taylor & Francis.
15. Gardner, R. M., Krouskup, D. (2018). Practical Crime Scene Processing and Investigation, Third Edition. United States: Taylor & Francis.
16. Nordby J, Deed Reckoning; The Art of Forensic Detection, CRC Press LLC (2000).
17. Lyman, M. D. (2002). Criminal Investigation: The Art and the Science. UK: Prentice Hall.
18. Chisum, W. J., Turvey, B. E. (2011). Crime Reconstruction. Netherlands: Elsevier Science

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-1 (Major Mandatory)	Fundamentals of Forensic Science	DFFSDC101T	4	16	40	24	60	2.5 Hrs.

Course DSC1-2: DFFSDC102T	Course Title: Introduction to Forensic Biology
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand the nature and scope of forensic biology and various biological evidences.
2. To understand forensic serology and examine blood and other fluids.
3. To understand the examination and significance of hair and fibers.
4. To understand the examination and significance of pollens and diatoms.
5. To understand the role of insects in forensic entomology.
6. To understand role of forensic anthropology and odontology in identification.
7. To understand the process and significance of forensic DNA analysis in identification.

Course Contents: Overview of Forensic Biology; Forensic Serology and other Body Fluids in Forensic Science; Forensic Examination of Hair, Fiber, Forensic Palynology and Entomology; Forensic Anthropology and DNA Analysis		**Reqd. Hrs.**
Unit I – Overview of Forensic Biology		**15 Hrs.**
	Introduction to Forensic Biology Various services of Forensic Biology Nature and types of biological evidence Collection and preservation of biological evidence Significance of biological evidence	
Unit II – Forensic Serology and other Body Fluids in Forensic Science		**15 Hrs.**
	Introduction to blood and major body fluids Blood spatter analysis and its significance Presumptive tests of blood, semen, saliva, urine, sweat and other body fluids Confirmatory tests of blood, semen, saliva, urine, and other body fluids	
Unit III – Forensic Examination of Hair, Fiber, Forensic Palynology and Entomology		**15 Hrs.**
	Forensic Hair and Fiber examination: Structure of hair, Human versus non-human hair, Identification and comparison of hair, Significance. Types of fibers and methods of identification and comparison. Forensic Palynology and Forensic Limnology: Structure of pollen grain, Extraction and Examination methods, Forensic significance. Structure of diatoms, Extraction and Examination methods, Forensic significance	

	Forensic Entomology: Insects involved in decomposition, Insects life cycle, Collection and examination of insects, Estimation of Post Mortem Interval (PMI). Introduction to wildlife forensics	
Unit IV – Forensic Anthropology and DNA Analysis		**15 Hrs.**
	Forensic Anthropology: Introduction to human skeleton, Skeletal anatomy, Difference between human and animal skeletons, Gender, Stature and ethnicity estimation from skull, pelvis and long bones. Forensic Odontology: Dental anatomy, Development of dentition, Dental profiling, Bite-mark analysis. Forensic DNA analysis: DNA: Types, structure and significance, DNA extraction and amplification via Polymerase Chain Reaction (PCR), Detection methods, Forensic DNA profiling techniques using various markers; Disaster Victim Identification	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Identify, collect and preserve biological evidence from crime scene 2. Identify, collect, preserve and examine blood and other body fluids 3. Reconstruct events based on blood spatter analysis 4. Identify and examine pollens and establish links 5. Identify Antemortem and Post Mortem drowning based on examination of diatoms 6. Estimate Post Mortem Interval (PMI) based on life cycle of insects 7. Estimate age, gender, stature and ethnicity through skeletal remains 8. Estimate age, gender, and ethnicity through dental remains 9. Perform separation, isolation and analysis of DNA in personal identification 10. Apply anthropology, odontology and DNA in personal identification in mass disasters.

Suggested Readings:

1. Gupta, P. K. (2005). Cell and Molecular Biology. India: Rastogi Publications.
2. Houck, M. M., Siegel, J. A. (2015). Fundamentals of Forensic Science. Netherlands: Elsevier Science.
3. Fisher, B. A., Tilstone, W. J., Woytowicz, C. (2009). Introduction to Criminalistics: The Foundation of Forensic Science. United Kingdom: Elsevier Science.
4. Saferstein, R. (2018). Criminalistics: An Introduction to Forensic Science, 12th Edition.

5. James, S. H., Nordby Ph.D., J. J., Bell, S., Williams, L. J. (2014). Forensic Science: An Introduction to Scientific and Investigative Techniques, Fourth Edition. United States: Taylor & Francis.
6. Bevel, T., Gardner, R. M. (2008). Bloodstain Pattern Analysis with an Introduction to Crime Scene Reconstruction. United Kingdom: Taylor & Francis.
7. James, S. H., Kish, P. E., Sutton, T. P. (2005). Principles of Bloodstain Pattern Analysis: Theory and Practice. United Kingdom: Taylor & Francis.
8. Gunn, A. (2019). Essential Forensic Biology. United Kingdom: Wiley.
9. Li, R. (2015). Forensic Biology. United Kingdom: Taylor & Francis.
10. Houck, M. M (2015), Forensic Biology. Netherlands: Elsevier Science.
11. James L. Castner, Jason H. Byrd (2000), Forensic Entomology: The Utility of Arthropods in Legal Investigations. United States: CRC Press.
12. Huffman, J. E., Wallace, J. R. (2012). Wildlife Forensics: Methods and Applications, Germany, Wiley
13. David R. Senn, Paul G. Stimson (2010), Forensic Dentistry. United Kingdom: CRC Press.
14. David R. Senn, Richard A. Weems (2013), Manual of Forensic Odontology. United Kingdom: CRC Press.
15. Christensen, A. M., Passalacqua, N. V., Bartelink, E. J. (2013). Forensic Anthropology: Current Methods and Practice. Netherlands: Elsevier Science.
16. Byers, S. N., Juarez, C. A. (2023). Introduction to Forensic Anthropology. Taylor & Francis.
17. Butler, J. M. (2014). Advanced Topics in Forensic DNA Typing: Interpretation. Netherlands: Elsevier Science.
18. Butler, J. M. (2009). Fundamentals of Forensic DNA Typing. Netherlands: Elsevier Science.
19. Elkins, K. M. (2012). Forensic DNA Biology: A Laboratory Manual. Netherlands: Elsevier Science

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-2 (Major Mandatory)	Introduction to Forensic Biology	DFFSDC102T	4	16	40	24	60	2.5 Hrs.

Course DSC1-3: DFFSDC103T	Course Title: Criminal Law-I	
Course Credits: 4	**Total contact hours: 60 Hrs.**	
Course Contents: 1. This course is designed to understand the meaning of crime and the essential principles of criminal liability. 2. It further aims to empower students to understand the fundamentals of criminal law with special reference to Bharatiya Nyaya Sanhita 2023. 3. The students will be equipped to understand various concepts and types of punishments under Bharatiya Nyaya Sanhita 2023. 4. The students will be prepared to analyze the ingredients of various offences and study the punishments prescribed thereto.		**Reqd. Hrs.**
Unit I – Introduction to Crime & Criminal Law		**15 Hrs.**
	• **Concept of crime**- History of crime, Essential elements of crime, Stages of Crime, Definitions of crime, Various Causes of crime commission • **Bhartiya Nyaya Sanhita 2023-** Historical development of Bharatiya Nyaya Sanhita 2023, Salient Features of Bharatiya Nyaya Sanhita 2023 • Bharatiya Nyaya Sanhita vis a vis Indian Penal Code 1860 • **Types of Punishments under Bhartiya Nyay Sanhita 2023-** a) Death (b) Imprisonment for life (c) Imprisonment, which is of two descriptions, namely: (1) Rigorous, that is, with hard labour; (2) Simple (d) Forfeiture of property (e) Fine (f) Community Service	
Unit II – Important Provisions under Bhartiya Nyaya Sanhita 2023		**15 Hrs.**
	• Definitions (Sec. 2), General Exceptions (Sec. 14- 44) • Offences against Women and Child- Sexual Offences (Sec. 63-79), Offences against Child (Sec. 93-99) • **Offences Against Body-** Offences affecting life (Sec. 100-110), Organized crime (Sec. 111-113), Hurt (Sec.115-125), Criminal Force and Assault (Sec. 128-136) Kidnapping, Abduction, slavery and Forced labour (Sec. 137-146)’	
Unit III – Offences against State and Society		**15 Hrs.**
	• Offences against State (Sec. 147-158) • Offence Relating to False evidence and against public justice (Sec. 227-269)	

	• Offences affecting the public health, safety, convenience, decency and morals (Sec. 270-297)	
Unit IV – Offences against Property		**15 Hrs.**
	• Theft (Sec. 202-208) • Robbery and Dacoity (Sec. 309-313) • Criminal Misappropriation of property (Sec. 314-315) • Criminal Breach of Trust (Sec. 316) • Receiving of Stolen Property (Sec. 317), Cheating (Sec. 318-319) • Offences relating to documents and to property marks (Sec. 335-350)	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Identify the various components of criminal culpability and an offence. 2. Appreciate the fundamentals of Criminal Jurisprudence and the various kinds of punishment. 3. Understand various crimes from the point of view of the requirements of substantive criminal law.

Suggested Readings:

1. J. K. Verma- Bharatiya Nyaya Sanhita, 2023 (Offences and Penalties): A Commentary (2024)
2. Taxmann's Editorial Board-Bharatiya Nyaya Sanhita 2023 (2024)
3. Anjana Prakash & Anuj Prakaash- Concise Commentary on the Bharatiya Nyaya Sanhita 2023 (2024)
4. Ratanlal Dhirajlal- Indian Penal Code
5. Prof. T. Bhattacharyya the Indian Penal code
6. K. D. Gaur -Criminal Lavr. Cases and Materials
7. Justice Hidaytullah -Indian penal Code
8. P.S. Achutan Pillai - Criminal Law

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-3 (Major Mandatory)	Criminal Law-I	DFFSDC103T	4	16	40	24	60	2.5 Hrs.

Course DSC1-4: DFFSLB104P	Course Title: Lab Course – I
Course Credits: 2	**Total contact hours: 60 Hrs.**

Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)

1.	Perform the general protocols of crime scene investigation. (4)
2.	Documentation of crime scene.
3.	Perform collection and preservation of evidences.
4.	Reconstruction of crime scene: Homicide.
5.	Reconstruction of crime scene: Arson.
6.	Preliminary examination of blood.
7.	Blood grouping.
8.	Perform blood spatter analysis.
9.	To identify angle of impact and directionality.
10.	Preliminary examination of pollen.
11.	Preliminary examination of diatom.
12.	Preliminary examination of hair.
13.	Preliminary examination of fibers.
14.	Estimation of gender from bones.
15.	Estimation of stature from bones.
16.	Estimation of age from bones.
17.	Estimation of age from dental records.
18.	Extraction of DNA from different biological samples.

Learning objectives -After completion of the course, the learner shall be able to,

1. To identify the crime scene and implement essential procedures for thorough crime scene processing.
2. To systematically collect and preserve different types of evidence for subsequent analytical testing.
3. To reconstruct various crime scenes through methodical examination and analysis.
4. To perform both preliminary and confirmatory assays for the detection of blood.
5. To analyze and classify various blood spatter patterns, determining their directionality.
6. To differentiate between human and animal hair through microscopic and comparative analysis.
7. To identify type of pollens and establish links to specific locations.

8. To extract and identify diatoms to aid in the determination of ante-mortem and post-mortem drowning.
9. To ascertain the type and origin of various fibers, establishing connections between evidence and sources.
10. To determine gender, stature, and age through the morphological analysis of skeletal remains.
11. To estimate age from dental records through forensic odontology.
12. To extract DNA from various biological samples, including blood, for DNA profiling.

Suggested Readings:

1. WORKING PROCEDURE MANUAL: FORENSIC BIOLOGY (2019), DIRECTORATE OF FORENSIC SCIENCE SERVICES, MINISTRY OF HOME AFFAIRS, GOI
2. Bevel, T., Gardner, R. M. (2008). Bloodstain Pattern Analysis with an Introduction to Crime Scene Reconstruction. United Kingdom: Taylor & Francis.
3. Elkins, K. M. (2012). Forensic DNA Biology: A Laboratory Manual. Netherlands: Elsevier Science.
4. Christensen, A. M., Passalacqua, N. V. (2018). A Laboratory Manual for Forensic Anthropology. Netherlands: Elsevier Science.
5. Kubic, T., Petraco, N. (2018). Forensic Science Laboratory Manual and Workbook. United Kingdom: Taylor & Francis.
6. Mirakovits, K., Londino-Smolar, G. (2021). The Basics of Investigating Forensic Science: A Laboratory Manual. United Kingdom: Taylor & Francis.
7. McClintock, J. T. (2008). Forensic DNA Analysis: A Laboratory Manual. United Kingdom: Taylor & Francis.

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-4 (Major Mandatory)	Lab Course – I	DFFSLB104P	2	-	-	20	50	4 Hrs.

Electives (Any One)	
Course DSE1-1: DFFSDE101T	**Course Title: Introduction to Forensic Physics & Forensic Psychology**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand forensic ballistics and its role in criminal investigation
2. To understand the collection and examination of various pattern and impression evidence
3. Understand the role and significance of psychology in criminal investigations & legal proceedings
4. To understand various psychological principles, tools and instruments used in forensic psychology

Course Contents: Introduction to Ballistics; Pattern and Impression Evidence; Forensic Psychology, Investigative Techniques in Forensic Psychology		**Reqd. Hrs.**
Unit I – Introduction to Ballistics		**15 Hrs.**
	• Ballistics: Classification of firearms and their mechanism. • Internal, external and terminal ballistics • Collection of firearms and related evidences • Examination of firearms and related evidences	
Unit II – Pattern and Impression evidence		**15 Hrs.**
	• Pattern and Impression evidence: Tool marks, Tread and Footwear impressions, Serial number restoration • Collection of pattern and impression evidence • Examination and comparison of pattern and impression evidence	
Unit III – Forensic Psychology		**15 Hrs.**
	• Forensic Psychology – Definition, History, Importance & Scope • Ethics for a Forensic Psychologist • Psychological and Forensic testing, Assessment and Evaluation. • Criminal Behavior – Social, Psychological, Biological factors • Detection of Deception – Study, Deception medium, Expertise, Baseline familiarity • Training to detect deception, Limitations and future challenges	

Unit IV – Investigative Techniques in Forensic Psychology		15 Hrs.
	• Polygraph • Narcoanalysis • Psychological Autopsy • BEOS – Brain Electrical Oscillation Signature Profiling • Forensic Hypnosis • Case study discussion – Polygraph, Narcoanalysis, Psychological Autopsy, BEOS, Forensic Hypnosis	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Identify firearms and collect all related evidences 2. Examine and compare firearms and all related evidences 3. Understand the role, responsibilities and significance of forensic psychology 4. Apply and interpret various investigative tools in forensic psychology

Suggested Readings:

1. Saferstein, R. (2018). Criminalistics: An Introduction to Forensic Science, 12th Edition.
2. James, S. H., Nordby Ph.D., J. J., Bell, S., Williams, L. J. (2014). Forensic Science: An Introduction to Scientific and Investigative Techniques, Fourth Edition. United States: Taylor & Francis.
3. Houck, M. M., Siegel, J. A. (2015). Fundamentals of Forensic Science. Netherlands: Elsevier Science
4. Fisher, B. A. J., Fisher, D. R. (2022). Techniques of Crime Scene Investigation. United States: Taylor & Francis.
5. Sharma, B. R. (2017). Firearms in Criminal Investigation and Trials: An Integrative Approach. India: LexisNexis.
6. Heard, B. J. (2011). Handbook of Firearms and Ballistics: Examining and Interpreting Forensic Evidence. Germany: Wiley.
7. Kumar, K. (2015). Forensic Ballistics Criminal Justice. India: Easterm Book Company.
8. Bodziak, W. J. (2017). Forensic Footwear Evidence. United Kingdom: CRC Press.
9. Bodziak, W. J. (2008). Tire Tread and Tire Track Evidence: Recovery and Forensic Examination. United Kingdom: Taylor & Francis.
10. Baldwin, D., Birkett, J., Facey, O., Rabey, G. (2013). The Forensic Examination and Interpretation of Tool Marks. Germany: Wiley.
11. Working procedures Laboratory Manual (Physics Division), DFSL, Mumbai.

12. Veeraraghavan V (2009), Handbook Of Forensic Psychology. (2009). India: Selective & Scientific Books.
13. Kleiner M (2002), Handbook of Polygraph Testing. United Kingdom: Academic Press.
14. Crighton D, et al (2021). Forensic Psychology. United Kingdom: Wiley.
15. Urbina, S. (2014). Essentials of Psychological Testing. United Kingdom: Wiley.
16. Walker, L. E., Shapiro, D., Akl, S. (2020). Introduction to Forensic Psychology: Clinical and Social Psychological Perspectives. Germany: Springer International Publishing.
17. Howitt, D. (2021). Introduction to Forensic and Criminal Psychology. United Kingdom: Pearson Education.
18. Bartol, C. R., Bartol, A. M. (2021). Introduction to Forensic Psychology: Research and Application. United States: SAGE Publications.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Major Elective)	Introduction to Forensic Physics & Forensic Psychology	DFFSDE101T	4	16	40	24	60	2.5 Hrs.

Course DSE1-1: DFFSDE102T	Course Title: Special Law-I
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. The Course is designed to provide the students with a conceptual and practical understanding of meaning, purpose and application of special criminal minor Acts to Forensic science.
2. It will help the students think about need and necessity of special enactments on specific subjects while dealing with respective issues such as environmental cases, mentally ill persons, food adulteration and motor accident cases.
3. The course will effectively impart learning on conceptual understanding, legal framework, procedural aspects and application of forensic specific aspects in legal proceedings.

Course Contents: Topics and sub-topics		**Reqd. Hrs.**
Unit I –		**15 Hrs.**
	• Meaning and Definition of Environment, Environmental Pollution, Its kinds (Natural and Artificial – Air, Water, Noise, Soil), causes and effects. • Environment Protection under the Constitution of India • The Environmental Protection Act, 1986 (Definitions, Measures taken for protection and conservation of natural resources, Authorities, offences and penalties and important judicial decisions) • The Wildlife Protection Act, 1972 (Important Definitions, Authorities under the Act, Wildlife Advisory Board, Hunting, Protection of Specified plants, Sanctuaries and National Parks, Central Zoo Authority and Recognition of Zoos, Trade or commerce in Wild Animals, animal articles and trophies, Forfeiture of Property Derived from Illegal Hunting and Trade, Offences and Penalties, important judicial decisions	
Unit II –		**15 Hrs.**
	• Mental Healthcare Act 2017 (Preliminary, Definitions, Central Mental Health Authority, State Mental Health Authority, Rights of Persons with Mental Illness, Mental Health Establishments, Mental Health Review Boards, Admission, Treatment and Discharge, Responsibilities of Other Agencies, Offences and Penalties)	

	• Medical Termination of Pregnancy Act 1971- Object behind enactment, Definitions, when pregnancies may be terminated by registered medical practitioners, Place where pregnancy may be terminated, Protection of privacy of a woman. • Pre Conception and Prenatal Diagnostic Technique Act, 1994- Object behind enactment, Definitions, Regulation of genetic counselling centres, genetic laboratories and genetic clinics, Regulation of pre-natal diagnostic techniques, Central Supervisory Board, Registration of Genetic Counselling Centres, Genetic Laboratories and Genetic Clinics, Offences and Penalties	
Unit III –		**15 Hrs.**
	• The Food Safety and Standards Act, 2006 (Preliminary, Food safety and Standard Authority of India, General principles of Food safety, General provisions as to articles of food, Analysis of Food, Enforcement provisions, Offences and Penalties) • The Drugs and Cosmetics Act, 1940 (Preliminary, Definitions, Authorities, Import of Drugs and Cosmetics, Provisions as to manufacture, sale and purchase of drugs, miscellaneous provisions)	
Unit IV –		**15 Hrs.**
	• The Standards of Weights and Measures Act 1976 (Preliminary, Definition, Establishment of standards of weights and measures, Physical representation of standard units, Standards of Weights and Measures, Offences and their trial) • The Motor Vehicles (Amendment) Act, 2019 **(**Preliminary, Licensing of drivers of motor vehicles, Registration of motor vehicles, Control of traffic, Insurance of motor vehicles against third party risks, Offences, penalties and procedure)	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understanding of various concept related environment pollution. 2. Familiarize with the mentally ill persons and their rights in the light of Mental healthcare Act 2017. It will enhance knowledge related to women's issues such as termination of pregnancy and female foeticide. 3. Understand the specific legislations pertaining to Food safety and Drugs and cosmetics

in India.

4. Develop a basic understanding of offences and penalties under Motor vehicles amended Act of 2019.

Suggested Readings:

1. Environmental Law and Policy in India, Shyam Divan and Armin Rosencranz, Oxford University Press, New Delhi
2. Environmental Law in India, P. Leelakrishnan, LexisNexis, New Delhi.
3. Environment and Wildlife Laws in India, Majumdar, Nandy, Mukherjee, LexisNexis.
4. The Arms Act 1959 (Bare Act) Professional Book Publishers, Delhi.
5. Explosive Substances Act 1908 (Bare Act) Professional Book Publishers, Delhi.
6. Mental Healthcare Act 2017 (Bare Act) Professional Book Publishers, Delhi
7. The Indian Cyber Law by Suresh T. Vishwanathan- Bharat Law House New Delhi
8. Guide to Cyber and E- Commerce Laws by P.M. Bukshi and R.K. Suri- Bharat Law House, New Delhi
9. The Regulation of Cyberspace by Andrew Murray, 2006- Routledge –Cavendish
10. Mental Healthcare Act 2017 (Bare Act) Professional Book Publishers, Delhi.
11. H. N. Tiwari, Environmental Law, Allahabad Law Agency
12. Dr. S. B. N. Prakash- Mental Health and Law. Lawyer'sLawBook.2008.
13. S.K. Verma. Legal Framework for Health Care in India Lexis Nexis Butterworths 2002
14. Kannan K. Medicine and Law. Oxford University Press–2014.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Elective)	Special Law-I	DFFSDE102T	4	16	40	24	60	2.5 Hrs.

Minor	
Course DSC2-1: DFFSRM101T	**Course Title: Research Methodology**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand research and its significance
2. To learn research design and formulation of hypothesis
3. To learn data sampling and data collection techniques
4. To learn various statistical tools involved in analyzing data
5. To understand data interpretation and various types of scientific report writing
6. To understand various tools available for data discovering and management
7. To understand the ethics in scientific publishing

Course Contents: Introduction to Research and Research Methodology; Hypothesis, Sampling and Acquisition of Data; Processing and Interpretation of Data; Report Writing		**Reqd. Hrs.**
Unit I – Introduction to Research and Research Methodology		**15 Hrs.**
	Research-Definition and Objectives Types of Research Research Design: Definition, need and types of research design Literature review process	
Unit II – Hypothesis, Sampling and Acquisition of Data		**15 Hrs.**
	Types of Hypotheses Formulation of Hypothesis and Hypothesis Testing Sampling procedure and different types of sampling methods Types of data and collection methods	
Unit III – Processing and Interpretation of Data		**15 Hrs.**
	Various statistical tools used for data analysis Tabulation and Graphical representation of data Interpretation of data	
Unit IV – Report Writing		**15 Hrs.**
	Types of scientific reports Various search tools and Reference management software's used in scientific research Steps involved in scientific writing Ethics in scientific publishing	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Cultivate scientific and research temper 2. Formulate hypothesis and design research plan 3. Collect data and apply various statistical tools to test hypothesis 4. Interpret data and based on it write scientific reports 5. Apply various tools for data discovering and management 6. Apply ethics in scientific writing

Suggested Readings:

1. Kothari, C. R. (2004). Research Methodology: Methods and Techniques. India: New Age International (P) Limited.
2. Baykoucheva, S. (2015). Managing Scientific Information and Research Data. United Kingdom: Elsevier Science.
3. D. K. Bhattacharyya (2006), Research Methodology. India: Excel Books.
4. Thomas, C. G. (2021). Research Methodology and Scientific Writing. Germany: Springer International Publishing.
5. Nagar P (2021), Research Methodology Made Easy: A Handbook on Research Methodology. India. Exceller Books.
6. Kumar, R. (2010). Research Methodology: A Step-by-Step Guide for Beginners. United Kingdom: SAGE Publications.
7. Körner, A. M. (2008). Guide to Publishing a Scientific Paper. United Kingdom: Taylor & Francis.
8. Ellison, C. (2010). McGraw-Hill's Concise Guide to Writing Research Papers. United Kingdom: McGraw-Hill Education.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC2-1 (Minor)	Research Methodology	DFFSRM101T	4	16	40	24	60	2.5 Hrs.

SEMESTER – II

Mandatory	
Course DSC1-5: DFFSDC201T	**Course Title: Fingerprints & Questioned Documents**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand the history and development of fingerprint examination
2. To understand the anatomy of friction ridge skin
3. To learn various types of fingerprint patterns and classification systems
4. Compare fingerprint patterns
5. To understand various fingerprint development techniques
6. To understand the need and scope of questioned document examination
7. To learn the principles of handwriting and signature examination
8. To learn various forgeries and examination of questioned documents

Course Contents: Introduction to Fingerprints; Development and Collection of Fingerprints; Overview of Questioned Document Examination; Examination of Handwriting, Signature and other documents		**Reqd. Hrs.**
Unit I – Introduction to Fingerprints		**15 Hrs.**
	• History and development of fingerprint examination • Anatomy and morphology of friction ridges • Types of fingerprints (latent, patent and plastic) and types of fingerprint patterns • Fingerprint Classification Systems • Comparison of fingerprints	
Unit II – Development and Collection of Fingerprints		**15 Hrs.**
	• Physical methods for fingerprint development • Chemical Methods for fingerprint development • Collection of prints at the crime scene • Digital fingerprint analysis technique-AFIS	
Unit III – Overview of Questioned Document Examination		**15 Hrs.**
	• Overview of Questioned Document Examination: Scope, need and Questioned Document Examiner roles and responsibilities • Classification of documents • Different types of forgeries related to documents	

	• Currency notes and security document examination • Handling, care and preservation of documents	
Unit IV – Examination of Handwriting, Signature and other documents		**15 Hrs.**
	• Principles of handwriting examination and factors affecting handwriting • Collection of handwriting exemplars and comparison • Signature analysis: Principle, collection and comparison • Examination of charred, indented, secret writing, typewritten, printed and photocopied documents.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Identify various types of fingerprints and classify them 2. Develop fingerprints and compare them 3. Identify and compare handwriting and signature specimens. 4. Identify and decipher various forgeries under questioned document examination

Suggested Readings:

1. Lee and Gaensslen's Advances in Fingerprint Technology, Third Edition. (2012). United Kingdom: Taylor & Francis.
2. Bleay, S. M., Croxton, R. S., De Puit, M. (2018). Fingerprint Development Techniques: Theory and Application. Germany: Wiley.
3. Hawthorne, M., Plotkin, S., Douglas, B. (2021). Fingerprints: Analysis and Understanding the Science. United Kingdom: Taylor & Francis.
4. S.A. Cole, Suspect Identities: A History of Fingerprint and Criminal Identification. Harvard Univ. Press, May 2001
5. Justice, U. S. D. (2014). The Fingerprint: Sourcebook. United States: CreateSpace Independent Publishing Platform.
6. Daluz, H. M. (2014). Fundamentals of Fingerprint Analysis. United States: Taylor & Francis.
7. Champod, C., Lennard, C. J., Margot, P., Stoilovic, M. (2017). Fingerprints and Other Ridge Skin Impressions. United Kingdom: Taylor & Francis.
8. Saxena, B. L. (1963). Law and Technique Relating to Identification of Handwriting, Disputed Documents, and Detection of Forgeries. India: Central Law Agency.
9. Harralson, H. H., Miller, L. S. (2021). Huber and Headrick's Handwriting Identification:

Facts and Fundamentals, Second Edition. United Kingdom: Taylor & Francis Limited (Sales).

10. Osborn, A. S. (2014). Questioned Documents: A Study of Questioned Documents with an Outline of Methods by Which the Facts May Be Discovered and Shown - Primary Source Editi. United States: Bibliolife DBA of Bibilio Bazaar II LLC.
11. Morris, R. N. (2020). Forensic Handwriting Identification: Fundamental Concepts and Principles. Netherlands: Elsevier Science.
12. Kelly J (2006), Scientific Examination of Questioned Documents. United Kingdom: Taylor & Francis.
13. Hilton, O. (1992). Scientific Examination of Questioned Documents, Revised Edition. United States: CRC-Press. Sulner, H.F.: Disputed Document, 1966 Oceana Publications Inc., New York.
14. Ellen, D., Day, S., Davies, C. (2018). Scientific Examination of Documents: Methods and Techniques, Fourth Edition. United Kingdom: Taylor & Francis.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-5 (Major Mandatory)	Fingerprints & Questioned Documents	DFFSDC201T	4	16	40	24	60	2.5 Hrs.

Course DSC1-6: DFFSDC202T	Course Title: Introduction to Forensic Chemistry
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To learn about various illicit drugs, alcohol and adulterated petroleum products
2. To understand collection, packaging and examination about arson and explosive related evidence
3. To understand the collection, examination and significance of ink, glass, paint and soil evidence
4. To understand various injuries, decomposition stages, process of autopsy and collection and preservation of various viscera samples
5. To understand various poisons, their metabolism and mode of action

Course Contents: Introduction to the examination of drugs of abuse, alcohol, petroleum products, arson and explosives; Examination of Ink, Glass, Paint and Soil; Autopsy, identification and medicolegal significance of injuries; Forensic Toxicology		**Reqd. Hrs.**
Unit I – Introduction to the examination of drugs of abuse, alcohol, petroleum products, arson and explosives		**15 Hrs.**
	• Introduction & scope of Forensic Chemistry • Drugs of abuse: Introduction and classification • Alcoholic beverages: Collection, preservation and analysis • Petroleum products: Collection, preservation and analysis • Arson and explosive residue: Collection, preservation and analysis	
Unit II – Examination of Ink, Glass, Paint and Soil		**15 Hrs.**
	• Introduction, definition and significance of: Ink, glass, Paint and Soil evidence • Classification and examination of Ink • Classification and examination of Glass • Classification and examination of paints • Classification and examination of soil	
Unit III – Autopsy, identification and medicolegal significance of injuries		**15 Hrs.**
	• Classification, evaluation and interpretation of injuries • Post-mortem changes and their significance • Autopsy: Definition and classification	

	• Collection and preservation of visceral samples	
Unit IV – Forensic Toxicology		**15 Hrs.**
	• Introduction & scope of Forensic Toxicology • Classification of poisons • Routes of administration & modes of action of poison • Factors influencing toxicity and individual variability • Interpretation of toxicological findings and cause of death determination	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Identify and test various illicit drugs, alcohol poisoning and adulterated petroleum products 2. Collect and examine arson and explosive related evidence 3. Identify and compare ink, glass, paint and soil evidence 4. Identify and classify various types of injuries 5. Estimate PMI and other conditions through decomposition stage 6. Understand the process of autopsy and collect and preserve various viscera samples 7. Identify various poisoning cases

Suggested Readings:

1. Saferstein, R. (2018). Criminalistics: An Introduction to Forensic Science, 12th Edition.
2. James, S. H., Nordby Ph.D., J. J., Bell, S., Williams, L. J. (2014). Forensic Science: An Introduction to Scientific and Investigative Techniques, Fourth Edition. United States: Taylor & Francis.
3. Houck, M. M., Siegel, J. A. (2015). Fundamentals of Forensic Science. Netherlands: Elsevier Science
4. Chang, R., Overby, J. (2011). General Chemistry: The Essential Concepts. United Kingdom: McGraw-Hill.
5. Nguyen K, et al (2019) Forensic Analysis of Fire Debris and Explosives. Germany: Springer International Publishing.
6. Forensic Investigation of Explosions, Second Edition. (2011). United Kingdom: Taylor & Francis.
7. "Working Procedure Manual on Chemistry", Directorate of Forensic Science MHA Govt. of India, 2005.

8. “Laboratory Procedure Manual: Petroleum Products”, Directorate of Forensic Science, MHA, Govt. of India, 2005.
9. Bureau of Indian Standard Specifications related to Alcohols and Petroleum Products.
10. “Working Procedure Manual- Chemistry, Explosives and Narcotics”, BPR&D, 2000.
11. Houck M.M (2015), Forensic Chemistry. Netherlands: Elsevier Science.
12. Khan, J. I., Kennedy, T. J., Christian, D. R., Christian, D. R. (2011). Basic Principles of Forensic Chemistry. Netherlands: Humana Press.
13. Elkins, K. M. (2018). Introduction to Forensic Chemistry. United Kingdom: Taylor & Francis.
14. Forensic Chemistry Handbook. (2011). United States: Wiley.
15. Levine Barry (2021), Principles of Forensic Toxicology. Switzerland: Springer International Publishing.
16. Lappas, N. T., Lappas, C. M. (2021). Forensic Toxicology: Principles and Concepts. Netherlands: Elsevier Science.
17. Clarke's Analytical Forensic Toxicology. (2013). United Kingdom: Pharmaceutical Press.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-6 (Major Mandatory)	Introduction to Forensic Chemistry	DFFSDC202T	4	16	40	24	60	2.5 Hrs.

Course DSC1-7: DFFSDC203T	Course Title: Criminal Law-II
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. This course is specifically designed to assist students in understanding the importance of the Bharatiya Nagarik Suraksha Sanhita 2023 which is one of the essential criminal enactments in India prescribing the procedure for administering criminal justice.
2. The course will acquaint the student with the organization of the functionaries under the Code, their power and functions at various stages and the procedure according to which these powers and functions are to be exercised.
3. The course is aimed at driving home the students how the pretrial, trial and the subsequent process are geared up to make the administration of criminal justice effective.
4. The Course is designed to provide the students with a conceptual and practical understanding of meaning, purpose and application of rules of evidence in relation to relevancy of facts and proof in the court of law during the trial.
5. It will help the students think about the process of adducing evidence, principles of admissibility and exclusion of evidences in a trial.

Course Contents: Introduction to Bharatiya Nagarik Suraksha Sanhita 2023; Investigation and Trial of Criminal Cases; Introduction to Bharatiya Sakshya Adhiniyam, 2023; Types of Evidences & Examination of witnesses.		**Reqd. Hrs.**
Unit I – Introduction to Bharatiya Nagarik Suraksha Sanhita 2023		**15 Hrs.**
	• **Introduction**- Historical Background, Objectives behind enactment Salient Features of Bharatiya Nagarik Suraksha Sanhita, 2023 Bharatiya Nagarik Suraksha Sanhita 2023 vis a vis Code of Criminal Procedure 1973 • **Definitions** (Sec.2) • **Criminal Courts in India**- Constitution of criminal courts (Sec. 6-17) Public prosecutors & Directorate of Prosecution (Sec. 18-20) Powers of Criminal Courts (Sec. 21-29)	
Unit II – Investigation and Trial of Criminal Cases		**15 Hrs.**
	• **Procedure of Investigation-** Arrest of persons- (Sec. 35-62) Processes to compel appearance- Summons (Sec. 63-71), Warrant Sec. 72-83), Processes to compel the production of things (Sec. 94-124) Information to the police and their powers to investigate Sec. 173-196)	

	• **Procedure of Trial-** Framing of Charge (Sec. 234-237) Trial before a court of session (Sec. 248-260), Trial of warrant-cases by magistrate (Sec. 261-273), Trial of summons-cases by magistrates Sec. 274- 282), Summary Trial (Sec. 283-288) Evidence in inquiries and trials (Sec. 307-337) Provisions as to accused persons with mental illness (Sec. 367-378) Provisions as to bail and bonds (Sec. 479-498)	
Unit III – Introduction to Bharatiya Sakshya Adhiniyam, 2023		**15 Hrs.**
	• **Introduction-** Historical Background, Objectives behind enactment Salient Features of Bharatiya Sakshya Adhiniyam, 2023 Bharatiya Sakshya Adhiniyam, 2023 vis a vis Indian Evidence Act 1872 • **Definitions** (Sec. 2) • **Dying Declaration-** Statements by persons who cannot be called as witnesses (Sec. 26) • **Opinion of Expert-** Opinions of third persons when relevant (Sec. 39-45)	
Unit IV – Types of Evidences & Examination of witnesses		**15 Hrs.**
	• **Types of Evidence-** Oral evidence (Sec. 54-55) Documentary Evidence (Sec. 56-73) Burden of proof (Sec. 104-120) • **Examination of witnesses-** Witnesses (Sec. 124-139) Examination of Witnesses (Sec. 140-168)	

Course Outcomes – After completion of the course, the learner shall be able to,
1. After completion of this course student will be able to: 2. Identify the stages in investigation and procedure of trial in criminal cases. 3. Explain the powers, functions, and duties of police and criminal courts. 4. Analyze the concept and nature of different types of evidences. 5. Identify and apply the rules relating to relevance and admissibility of evidence in courts. 6. Understand the standard of burden of proof followed in civil and criminal cases and analyze the role played by the witnesses and evidentiary value attached to ocular evidence vis-à-vis scientific evidence.

7. Understand the procedure of examination of witnesses and different categories of witnesses involved in a suit or proceeding and examine the applicability and admissibility of forensic science in civil and criminal cases along with the admissibility of expert's opinion.

Suggested Readings:

2. J. K. Verma- Bharatiya Nagarik Suraksha Sanhita, 2023 (Criminal Procedure) : A Commentary 1st Edition (2024)
3. Jaswant Dhawan- The Bharatiya Nagarik Suraksha Sanhita, 2023 (2024)
4. J. K. Verma- Bharatiya Sakshya Adhiniyam, 2023 (Evidence): A Commentary 1st Edition (2024)
5. Saurabh Kansal, Vageshwari Deswal, Shruti Goyal - Taxmann Bharatiya Sakshya Adhiniyam 2023 Law & Practice (2024)
6. Kush Kalra-The Bhartiya Sakshya Adhiniyam, 2023 (Repeal and Replace the Indian Evidence Act, 1872) (2024)
7. Commercial Law Publishers- Bharatiya Sakshya Adhiniyam (Evidence) alongwith Comparative Study of Indian Evidence Act, 1872
8. Ratanlal & Dhirajlal- Criminal procedure Code, Universal, Delhi.
9. Chandrashekaran Pillai, Kelkar Lectures on Criminal Procedure Code, Eastern, Lucknow.
10. Shailedra Malik, The Code Of Criminal Procedure Code, Eighteen edition, 2011, Allahabad law Agency.
11. K. I. Vibhute, Durga Das Basu Criminal Procedure Code, (1999), Universal, Delhi
12. S.C. Sarkar, Sarkar the Code of Criminal Procedure, Lexis Nexis,
13. K.D. Gaur, Textbook on Criminal Procedure Code, Universal Law Publisher.
14. S. N. Mishra, The Code of Criminal Procedure, Central Law Publication.
15. Ratanlal & Dhirajlal- The Law of Evidence
16. Batuklal- The Law of Evidence.
17. Sarkar- The Law of Evidence.

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-7 (Major Mandatory)	Criminal Law-II	DFFSDC203T	4	16	40	24	60	2.5 Hrs.

Course DSC1-8: DFFSLB204P	Course Title: Lab Course – II
Course Credits: 2	**Total contact hours: 60 Hrs.**

Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)

1.	Development of fingerprints by chemical methods.
2.	Development of fingerprints by physical methods.
3.	Fingerprint identification and comparison.
4.	Analysis of handwriting.
5.	Evaluating the effect of various factors on handwriting.
6.	Comparison of glass samples.
7.	Analysis of ink samples
8.	Analysis of soil samples
9.	Analysis of paint samples
10.	Analysis of petroleum products
11.	Analysis of alcoholic beverages.
12.	Analysis of viscera (simulated sample) for pesticides by TLC.
13.	Identification of adulteration of vegetable in oils by color test.
14.	Extraction of poison from biological and non-biological samples.
15.	Preliminary and confirmatory tests for poisons.

Learning objectives -After completion of the course, the learner shall be able to,

1. To apply different development techniques used in fingerprints depending on the surface conditions.
2. To identify and compare fingerprints using three levels of comparison
3. To analyze handwriting characteristics and determine their source through comparative analysis.
4. To examine and identify and compare glass, soil, ink and paint samples using various techniques
5. To examine adulteration of various alcoholic beverages, petroleum products and vegetable oils using various techniques
6. To extract poisons from samples and conduct both preliminary and confirmatory tests.

Suggested Readings:

1. WORKING PROCEDURE MANUAL: CHEMISTRY (2021), DIRECTORATE OF FORENSIC SCIENCE SERVICES, MINISTRY OF HOME AFFAIRS, GOI © NEW DELHI
2. WORKING PROCEDURE MANUAL: TOXICOLOGY (2021), DIRECTORATE OF FORENSIC SCIENCE SERVICES, MINISTRY OF HOME AFFAIRS, GOI © NEW DELHI
3. Hawthorne, M. (2017). Fingerprints: Analysis and understanding. Ukraine: CRC Press.
4. Kubic, T., Petraco, N. (2018). Forensic Science Laboratory Manual and Workbook. United Kingdom: Taylor & Francis.
5. Mirakovits, K., Londino-Smolar, G. (2021). The Basics of Investigating Forensic Science: A Laboratory Manual. United Kingdom: Taylor & Francis.
6. The Forensic Laboratory Handbook: Procedures and Practice. (2006). United Kingdom: Humana Press.
7. Lawrence Kobilinsky (2011), Forensic Chemistry Handbook. United States: Wiley.
8. Erickson, E. (2013). Criminalistics Laboratory Manual: The Basics of Forensic Investigation. United Kingdom: Taylor & Francis.

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-8 (Major Mandatory)	Lab Course – II	DFFSLB204P	2	-	-	20	50	4 Hrs.

Electives (Any One)	
Course DSE2-1: DFFSDE201T	**Course Title: Digital Forensics**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To Understand the basics of computer system
2. To understand the basics of digital forensics
3. To understand the methods of data recovery
4. To understand the basis of cyber investigation

Course Contents: Cybercrime and Digital Forensics; Forensic Analysis: Networks, Mobile Devices, and social media; Forensic Photography: Techniques and Challenges; Forensic Video and Speaker Identification		**Reqd. Hrs.**
Unit I – Cybercrime and Digital Forensics		**15 Hrs.**
	• Understanding cybercrime and its classifications • Digital Forensics process and methodologies • Digital evidence handling and preservation • Disk imaging and cloning • Data recovery and reconstruction	
Unit II – Forensic Analysis: Networks, Mobile Devices, and social media		**15 Hrs.**
	• Investigating network intrusions and cyber attacks • Mobile device forensics (smartphones, tablets, etc.) • Web browser analysis, Email investigations and tracing • Social media investigations	
Unit III – Forensic Photography: Techniques and Challenges		**15 Hrs.**
	• Principles, history and development of photography • Photography on challenging surfaces • Forensic photography- photogrammetry, filtered photography, macro photography • Introduction to image forensics • Challenges in image forensics	
Unit IV – Forensic Video and Speaker Identification		**15 Hrs.**
	• Introduction to video forensics • Anatomy of vocal tract • Introduction to forensic speaker identification	

	• Methods of speaker identification • Challenges in Forensic Audio and Video Analysis	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand the working of computer systems 2. Understand the concept of software 3. Understand the overview of digital forensics 4. Understand the methods of data recovery 5. Understand the methods of cyber investigation

Suggested Readings:

1. Cybercrime: Susan Banor
2. Cybercrime investigation: Robert More
3. Computer Forensics: Principles and Practices: Linda Volonino, Reynaldo
4. Digital Evidence and Computer Crime, 2nd ed.: Eoghan Casey
5. Computer Security Basics by Rick Lehtines
6. Cyber Forensic by Mareculla Menendez
7. Network and System Security by John Vacca
8. Security Policies and Implementation Issue by Robert Jahnson
9. Photography, John Freeman, Collins and Brown.
10. A concise history of photography, Helmut Gernsheim, Dove publications.
11. Optics in Photography, Rodolf Kingslake, Spie optical engineering press.
12. Basic Photography, Michael Langford, Focal Press.
13. Magic: Stage illusions, special effects and trick photography, Albert A Hopkins, Diver
14. Color Theory, Patti Mollica, Walter Foster Publishing.
15. Digital Audio Forensics Fundamentals, James Zjalic, 2020, Focal Press, ISBN: 9781000205718
16. Principles of Forensic Audio Analysis by Robert C. Maher
17. Photo Forensics, Hany Farid · 2019, MIT Press
18. Digital Image Forensics: There is More to a Picture Than Meets the Eye, Husrev Taha Sencar, Nasir Memon · 2012, Springer
19. Forensic Speaker Identification, Phil Rose · 2002, Taylor & Francis
20. Forensic Voice Identification, Harry Francis Hollien · 2002, Academic Press

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSE2-1 (Major Elective)	Digital Forensics	DFFSDE201T	4	16	40	24	60	2.5 Hrs.

Course DSE2-1: DFFSDE202T	Course Title: Special Law-II
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. In depth understanding of environment concepts and laws relating to Air Act, Water Act, Biodiversity Act and The Wildlife (Protection) Act, 1972.
2. Aims to impart the principles and the Laws relating to Arms and Explosives.
3. To impart the students a basic understanding of the areas of health and drugs related laws like Mental Healthcare Act, 2017, Medical Termination of Pregnancy Act, 1971 and Pre Conception and Prenatal Diagnostic Technique Act, 1994, Narcotic Drugs and Psychotropic Substance Act, The Drug and Magic Remedies (Prevention of Objectionable Advertisement) Act, 1954, Transplantation of Human Organs Act, 1994, Drugs and cosmetics Act, 194
4. Impart the student's basic understanding of the areas Cyber and data protection related laws, like The Digital Personal Data Protection Bill 2022, Right to Privacy Bill and freedom of Expression in India and Specific Provisions of Information Technology Act 2000 relating to cyber-crimes.

Course Contents: Topics and sub-topics		**Reqd. Hrs.**
Unit I –		**15 Hrs.**
	• Water (Prevention and Control of Pollution) Act, 1974- Preliminary, The Central and State Boards for Prevention and Control Of Water Pollution, Powers And Functions of Boards, Prevention And Control Of Water Pollution, Penalties And Procedure, Central Water Laboratory, State Water Laboratory., Analysts, Reports of analyst • Air (Prevention and Control of Pollution) Act,1981- Central and State Boards for The Prevention and Control of Air Pollution, Powers and Functions of Boards, Prevention and Control of Air Pollution, Penalties and Procedure • The Noise Pollution (Regulation and Control) Rules, 2000 • Hazardous Waste (Management, Handling and Transboundary Movement) Rules 2016 with its Amendments	
Unit II –		**15 Hrs.**
	• The Arms Act 1959 (Preliminary, Definition of arms, Prohibited Arms, firearms, Types of firearms, Acquisition, Possession, Manufacture,	

	Sale, Import, Export and Transport of Arms and Ammunition, Provisions Relating To Licenses, Powers And Procedure, Offences and penalties, Miscellaneous) • The Explosive Substances Act 1908 (Preliminary, Definitions, Licensing Procedure, Power to make rules conferring powers of inspection, search, seizure, detention and removal, Notice and inquiry of accidents, Punishment for certain offences) of Pregnancy Act 1971	
Unit III –		**15 Hrs.**
	• Poisons Act 1919 • The Narcotic Drugs and Psychotropic Substances Act, 1985 (Object, Definitions, Authorities and officers, Prohibition control and regulation under Act, Offences and Penalties, Special Courts and its Procedure) • The Prevention of Illicit Trafficking in NDPS Act,1988	
Unit IV –		**15 Hrs.**
	• Introduction to Cyber Crime, Types of Cyber Crimes • The Information Technology Act 2000 with recent Amendments • Preliminary, Definitions, Attribution, Acknowledgment and Dispatch of Electronic Records, Secure Electronic Records and Secure Digital Signatures, Electronic Governance, Regulation of Certifying Authorities, Digital Signature Certificates, Offences and Penalties. • Overview of Digital Personal Data Protection Act, 2023	

Course Outcomes – After completion of the course, the learner shall be able to,
1. After completion of this course student will be able to: 2. To have in depth understanding of various statutes and provisions in respect of environmental law. 3. Familiarize with the basic principles and the Laws relating to Arms and Explosives. 4. Understand the specific legislations pertaining to Poison and Drug law. 5. To develop a basic scientific understanding of cyber-crime and cyber law.

Suggested Readings:

1. P. Leelakrishnan, The Environmental Law in India, Butterworths–India
2. Cyber Crime Law Practice and Procedure-Kataria Srinivas.
3. Cyber Law & Crimes, Asia Law House Hyderabad

4. Sarkar's Criminal Minor Acts by S. K. Sinha Ray,LexisNexis New Delhi
5. An Introduction to Cyber Crime and cyber Law By Prof R.K.Chaubey
6. Cyber-crime: law & policy perspective, by Manikyam K Sita, Hind Law House (Pune).
7. Law relating to Information Technology by Dr. V. N. Shukla Shyam Diwan & Armin Rosencranz, Environmental Law and Policy in India, Oxford University Press.
8. S.C. Shastri, Environmental Law, Eastern Book Company.
9. Gurdip Singh, Environmental Law in India, MacMillan Publisher.
10. Environmental &Pollution Laws in India by Justice T S Doabia, LexisNexis
11. Krishan Keshav, Lawand Environment, Singhal Law Publications
12. Environment, Energy and Climate Change Author: Nawneet Vibhaw, Lexis Nexis
13. Shantakumar's Introduction to Environmental Law, Wadhwa and Company
14. H. M. Seervai, Constitutional Law of India, Law and Justice Publishing Company
15. International Trade Law by Indira Carr, Peter Stone, 4th edition, 2010,
16. Page 103 to 136 Online Dispute Resolution: Challenges for Contemporary Justice by Gabrielle Kaufmann Kohler, Thomas Schultz, 2004, pages 5 to 58, 67 to 81, 108 to 120, 131.
17. The Arms Act 1959 (Bare Act) Professional Book Publishers, Delhi.
18. Explosive Substances Act 1908 (Bare Act) Professional Book Publishers, Delhi.
19. Sarkar's Criminal Minor Acts by S. K. Sinha Ray, LexisNexis New Delhi
20. Puneet Bhasin- Practical Guide to the Digital Personal Data Protection Act, 2023- Law and Compliances OakBridge (2024)

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE2-1 (Major Elective)	Special Law-II	DFFSDE202T	4	16	40	24	60	2.5 Hrs.

On Job Training	
Course OJT-1: DFFSOJ201P / DFFSFP201P	**Course Title: On Job Training / Field Project**
Course Credits: 4	**Total contact hours: 120 Hrs. (During Summer Vacation)**

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
OJT-1/ FP-1 (OJT/ FP)	On Job Training/ Field Project	DFFSOJ201P / DFFSFP201P	4	-	-	40	100	6 Hrs.

Ad-hoc BoS in Forensic Science
Credit Distribution of PGD DCFRL

Yr	Lvl	Sem	Major		Minor	OE	VSC, SEC (VSEC)	AEC, VEC, IKS All Mandatory	OJT, FP, CEP, CC, RP	Cum. Cr. / Sem	Cum. Cr. / Degree
			Mandatory	Electives							
1	6.0	I	DSC1-1 DDFSDC101T Cyber Forensics – I (4)	DSE1-1 DDFSDE101T Introduction to Digital Devices and Networking (4) **OR** DSE1-1 DDFSDE102T Regulation of Cyberspace (4)	DSC2-1 DDFSRM101T Research Methodology (4)	—	—	—	—	22	**44** **PG Diploma in Digital & Cyber Forensic and Related Laws (44)**
			DSC1-2 DDFSDC102T Cyber Security (4)								
			DSC1-3 DDFSDC103T Cyber Law – I (4)								
			DSC1-4 DDFSLB104P Lab Course – I (2)								
		II	DSC1-5 DDFSDC201T Cyber Forensics – II (4)	DSE2-1 DDFSDE201T Cyber Crime Investigation (4) **OR** DSE2-1 DDFSDE202T Cyber Law: International Perspective and Future Challenges (4)	—	—	—	—	OJT/ RP/ FP DDFSOJ201P / DDFSFP201P (4)	22	
			DSC1-6 DDFSDC202T Mobile Forensics (4)								
			DSC1-7 DDFSDC203T Cyber Law – II (4)								
			DSC1-8 DDFSLB204P Lab Course – II (2)								
Cum. Cr.			**28**	**8**	**4**	—	—	—	**4**	**44**	
Award of PG Diploma in Digital & Cyber Forensic and Related Laws with 44 credits.											

Postgraduate Diploma in Digital & Cyber Forensics and Related Laws

Teaching and Examination Scheme – Semester I

Course	Course Code	Course Title	Credits	Teaching Scheme				Examination Scheme						
								Theory				Practical		
				Lectures per Week	Practical per Week	Total Periods	Duration in Hours	Max. Marks (Theory)	Max. Marks (Internal)	Total Marks	Minimum Passing Marks*	Max. Marks	Total Marks	Minimum Passing Marks*
DSC1-1	DDFSDC101T	Cyber Forensics – I	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-2	DDFSDC102T	Cyber Security	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-3	DDFSDC103T	Cyber Law – I	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-4	DDFSLB104P	Lab Course – I	2	-	1	4	4	-	-	-	-	50	50	20
DSE1-1	DDFSDE101T	Introduction to Digital Devices and Networking	4	4	-	4	4	60	40	100	40	-	-	-
DSE1-1	DDFSDE102T	Regulation of Cyberspace	4	4	-	4	4	60	40	100	40	-	-	-
DSC2-1	DDFSRM101T	Research Methodology	4	4	-	4	4	60	40	100	40	-	-	-
		Total	**22**	20	1	24	24	300	200	**500**	-	50	**50**	-

Teaching and Examination Scheme – Semester II

DSC1-5	DDFSDC201T	Cyber Forensics – II	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-6	DDFSDC202T	Mobile Forensics	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-7	DDFSDC203T	Cyber Law – II	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-8	DDFSLB204P	Lab Course – II	2	-	1	4	4	-	-	-	-	50	50	20
DSE2-1	DDFSDE201T	Cyber Crime Investigation	4	4	-	4	4	60	40	100	40	-	-	-
DSE2-1	DDFSDE202T	Cyber Law: International Perspective and Future Challenges	4	4	-	4	4	60	40	100	40	-	-	-
OJT-1 / FP-1	DDFSOJ201P / DDFSFP201P	On Job Training / Field Project	4	-	1	8	8	-	-	-	-	100	100	40
		Total	**22**	16	2	28	28	240	160	**400**	-	150	**150**	-

*Candidates shall pass separately in each head of assessment (i.e. Theory (External), Theory (Internal) and Practical examination) with minimum 40% marks.

SEMESTER – I

Mandatory	
Course DSC1-1: DDFSDC101T	**Course Title: Cyber Forensics-I**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To provide a foundational understanding of cyber forensics,
2. To equip with the skills & knowledge needed to effectively respond to cybersecurity incidents.
3. To provide specialized knowledge in conducting forensic analysis on Windows systems.
4. To develop the skills necessary to perform forensic analysis on volatile memory (RAM).

Course Contents: Introduction to Cyber Forensic; Incident Response; Windows Forensics; Memory Forensics	**Reqd. Hrs.**
Unit I – Introduction to Cyber Forensics	**15 Hrs.**
• Definition and origin of the term "forensic", Nature, need and scope of forensic science, Principles, and laws of forensic science. • Cyber Forensics: A Brief About Cyber Forensics, Digital Forensics Categories • Forensics Investigation Process: Incident, Identification, Seizure, Imaging, Hashing, Analysis, Reporting, Preservation • Forensic Protocol for Evidence Acquisition • Digital Evidence: Write Blockers, Forensic Triage, Chain of Custody • Digital Forensics Standards, Guidelines and Best Practices- Handling the Digital Crime Scene - Digital Evidence Examination Guidelines –ACPO, SWGDE, DFRWS, ISO 27037 • Cyber-crimes mechanisms: Types of Cyber-crimes, Notable Data Breaches • Challenges in Cyber Forensics • Skills Required to Become a Cyber Forensic Expert, Proficiency of a Cyber Forensic Expert • Cyber Forensic Tools	
Unit II – Incident Response	**15 Hrs.**
• Introduction to Incident Response Process ➢ What is the Computer Security Incident? ➢ What are the goals of Incident Response?	

	➢ Who is involved in the 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 III – Windows Forensics		**15 Hrs.**
	• Volatile Data Collection: Live Response, Locard's Exchange Principle, Order of Volatility, When to Perform Live Response, What Data to Collect. • Memory Dump, System Time, Logged on Users, Open Files, Network Information (Cached NetBIOS Name Table), Network Connections, Process Information, Process-to-Port Mapping, Process Memory, Network Status, Clipboard Contents, Service / Driver Information, Command History, Mapped Drives, Shares • Non-Volatile Data Collection: Disk Imaging (External Storage such as USB and Native Hard Disk), Registry Dump, Event Logs, Devices and Other Information, Files Extraction, Write-Blocking port • Registry Analysis • Browser Usage • Hibernation File Analysis • Crash Dump Analysis • File System Analysis • File Metadata and Timestamp Analysis • Event Viewer Log Analysis • Timeline Creation	
Unit IV – Memory Forensics		**15 Hrs.**
	• System overview • x86/x64 architecture • Data structures • Volatility Framework & plug-in	

	• Memory acquisition • Processes, Handles and Tokens • Windows registry • Networking; sockets, DNS and Internet history • Disk Artifacts in memory • Event Reconstruction • Timelining memory	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Have solid foundation in the principles and practices of cyber forensics. 2. Effectively manage and respond to cybersecurity incidents. 3. Acquire specialized skills to perform forensic analysis on Windows systems. 4. Develop expertise in analyzing volatile memory for forensic purposes.

Suggested Readings:

1. Practical Cyber Forensics by Niranjan Reddy, A Press publication
2. Digital Forensics Basics by Nihad A. Hassan
3. Practical Windows forensic Packt publisher
4. Computer Forensics, Computer Crime Investigation by John R, Vacca, Firewall Media, New Delhi.
5. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
6. http://dfs.nic.in/pdfs/Computer_Forensics_WPM_Final.pdf
7. https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf
8. http://dfs.nic.in/pdfs/Computer_Forensics_WPM_Final.pdf
9. http://dfs.nic.in/pdfs/crime%20scene%20manual%20full_organized.pdf
10. https://keralapolice.gov.in/storage/pages/custom/ckFiles/file/7GafuMCjLbFgjBNh8aXz8WhLv2Zqtfczvbi7Uv6m.pdf
11. https://police.mizoram.gov.in/wp-content/uploads/2023/01/SOP-Cyber-Crime-Investigation-v1.0.pdf
12. https://www.in.gov/isp/files/Evidence-Collection.pdf
13. https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf
14. https://cbi.gov.in/assets/files/media/pc_20201222_1.pdf

15. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.
16. Real Digital Forensics by Keith J. Jones, Richard Bejitlich, Curtis W. Rose, Addison Wesley Pearson Education
17. Forensic Compiling, A Practitioners Guide by Tony Sammes and Brain Jenkinson, Springer International edition.
18. Computer Evidence Collection &Presentation by Chrostopher L.T. Brown, Firewall Media.
19. Homeland Security, Techniques& Technologies by Jesus Mena, Firewall Media.
20. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M. Slade, TMH 2005
21. Windows Forensics by Chad Steel, Wiley India Edition
22. John Sammons, “The Basics of Digital Forensics, The Primer for Getting Started in Digital Forensics”, Syngress, 2012.
23. Cory Altheide and Harlan Carvey, “Digital Forensics with Open-Source Tools”, Elsevier, 2011.
24. Bill Nelson, Amelia Philips, Chris Steuart, “Guide to Computer Forensics and Investigations”, 5th Edition, CENGAGE Learning, 2015.
25. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGraw Hill, 2006.
26. Peter Stephenson, “Investigating Computer Crime: A Handbook for Corporate Investigations”, Sept 1999.
27. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001.
28. Skoudis. E., Perlman. R. Counter Hack: “A Step-by-Step Guide to Computer Attacks and Effective Defenses”. Prentice Hall Professional Technical Reference. 2001.
29. Norbert Zaenglein, “Disk Detective: Secret You Must Know to Recover Information from a Computer”, Paladin Press, 2000.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-1 (Major Mandatory)	Cyber Forensics-I	DDFSDC101T	4	16	40	24	60	2.5 Hrs.

Course DSC1-2: DDFSDC102T	Course Title: Cyber Security
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Understand the fundamental concepts of cyber security and its importance in today's digital world.
2. Acquire advanced search techniques using Google for data gathering and reconnaissance purposes.
3. Explore various techniques and methodologies used by hackers for foot printing and scanning networks.
4. Gain insights into the concept of denial-of-service (DoS) attacks, examples of such attacks, and precautionary measures to mitigate their impact.
5. Learn about vulnerability assessment, its importance, the process involved and case studies.

Course Contents: Introduction to Security; Basics of Cryptography and Wireless Security; Vulnerability Assessment and Pen Testing; SQL Security and Attacks: Basics, XSS	**Reqd. Hrs.**
Unit I – Introduction to Security	**15 Hrs.**
• Introduction to Security: security triangle. Various terms. Methodologies of various hackers. • Networking Basics: Topologies. Addressing schemes. NAT, protocols related to networking. • Data Gathering with Google: advanced search techniques. • Foot Printing& Scanning: advantages & techniques & types • Windows Security: types of password attacks, different monitoring techniques • Linux security: directory structure. Data locations etc.	
Unit II – Basics of Cryptography and Wireless Security	**15 Hrs.**
• Theory of Proxy Server: Advantages, types, possible misuses • Malware and Trojans: introduction, types, and detection • Denial of Service: Concept, Examples, precaution • Sniffers and Tools: introduction, process of sniffing, countermeasures • Steganography and Steganalysis: concept, advantages, and detection	

	• Basics of Cryptography: concept, types • Wireless Security and Attacks: components of wireless network. Security standards, types of attacks, guidelines for securing the wireless networks.	
Unit III – Vulnerability Assessment and Pen Testing		**15 Hrs.**
	• Firewall, IDS and IPS: concept, types of firewalls, IDS, IPS advantages, configuration guidelines. • Theory of Vulnerability Assessment: importance of vulnerability assessment. Process of vulnerability assessment, guidelines, case studies. • Introduction to Penetration Testing: concept, importance, guidelines, types, example. • Session Hijacking: introduction, mechanism, countermeasures.	
Unit IV – SQL Security and Attacks: Basics, XSS		**15 Hrs.**
	• Introduction to Web Server: importance of websites and servers, working of webserver, possible vulnerabilities in web server and application, hardening web server • SQL Security and Attacks: basics of DBMS, DDL & DML Statements, server & client-side validation, working of SQLi, Types of SQLi, countermeasures • Cross Site Scripting: introduction to JavaScript, working of XSS, types, countermeasures. • Reverse Engineering: concept, disassembling & decompiling, advantages.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Demonstrate a foundational understanding of cyber security principles and their significance in protecting digital assets. 2. Utilize advanced search techniques on Google for data gathering and reconnaissance in a cyber-security context. 3. Conduct foot printing and scanning activities using various methodologies to assess network vulnerabilities. 4. Employ precautionary measures to mitigate the impact of denial-of-service (DoS) attacks on systems and networks. 5. Conduct vulnerability assessments and identify potential weaknesses in a system or network.

Suggested Readings:

1. Certified Information (Security Expert, Main Book, Inn buss Knowledge Solutions (P)
2. Certified Ethical Hacker Manual
3. www.hackthissite.org
4. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
5. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws, Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.
6. Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
7. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-2 (Major Mandatory)	Cyber Security	DDFSDC102T	4	16	40	24	60	2.5 Hrs.

Course DSC1-3: DDFSDC103T	Course Title: Cyber Law-I
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. The main objective of this course is to familiarize important aspects of Information Technology Law in the context of cyber forensics.
2. To familiarize the students about cybercrime, its different types and laws related to it
3. To analyze the digital evidence under Information Technology Law.
4. To understand the jurisdiction and Investigation of cybercrimes.

Course Contents: Cyber Forensic and Computer Crimes; Cyber Crimes and its Categories; Information Technology Act, 2000; Cyber Space Jurisdiction and Investigation of Cyber Crimes		**Reqd. Hrs.**
Unit I – Cyber Forensic and Computer Crimes		**15 Hrs.**
	Introduction: Meaning, Nature and Scope of Cyber Crime and relevance with Conventional Crimes, Historical Genesis and Evolution of Cyber Crimes Characteristics, causes of cybercrimes and measures to combat cybercrimes, Classifications of cybercrimes, cybercrimes against individuals, Institutions and state, Hacking and Cracking, Digital Forgery and Cyber Stalking/Harassment.	
Unit II – Cyber Crimes and its Categories		**15 Hrs.**
	Online based Cyber Crimes, Financial Crimes, ATM and Card Crimes Software & Hardware Piracy Money Laundering, Computer Fraud, Cheating Cyber Pornography and Obscenity, Identity theft Cyber Terrorism, Cyber Defamation, Virus Attack and Social Networking Crimes.	
Unit III – Information Technology Act, 2000		**15 Hrs.**
	Salient features of Information Technology Act, 2000 Definitions, Digital Signatures, Authorities and Digital Signature Certificates Electronic Evidence and Electronic Signature under Bharatiya Sakshya Adhiniyam 2023 Electronic Governance, Security Procedures, Electronic Contracts, Offences and Penalties Under IT Act Establishment of Authorities under IT Act and their functions, powers, etc.	

	Controller, Certifying Authorities, Cyber Regulation, Appellate Tribunal, Adjudicating officer	
Unit IV – Cyber Space Jurisdiction and Investigation of Cyber Crimes		**15 Hrs.**
	Territorial Jurisdiction, Extra Territorial Jurisdiction and personal jurisdiction in cyber space Investigation of Cyber Crimes, Introduction to cybercrime investigation Cyber forensics, Investigation tools, Digital evidence, collection of evidence, Admissibility of Electronic records, Problems and challenges in investigation. Cybercrimes prevention measures, Data safety and future challenges	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understanding concepts of cyber space and cyber world. 2. Understand the various facets of cybercrimes. 3. Understand the concepts of digital and electronic signature. 4. Understand the cyber offences and penalties under IT Law

Suggested Readings:

1. Kamlesh N. & Murali D. Tiwari (Ed), *IT and Indian Legal System*, Macmillan India Ltd, New Delhi
2. K. L. James, *The Internet: A User's Guide* (2003), Prentice Hall of India, New Delhi
3. Chris Reed, *Internet Law-Text and Materials*, 2nd Edition, 2005, Universal Law Publishing Co., New Delhi
4. Vakul Sharma, *Handbook of Cyber Laws*, Macmillan India Ltd, New Delhi
5. S. V. Joga Rao, *Computer Contract & IT Laws* (in 2 Volumes), 2005 Prolific Law Publications, New Delhi
6. T. Ramappa, *Legal Issues in Electronic Commerce*, Macmillan India Ltd, New Delhi
7. Indian Law Institute, *Legal Dimensions of Cyber Space*, New Delhi
8. Pankaj Jain & Sangeet Rai Pandey, *Copyright and Trademark Laws relating to Computers*, Eastern Book Co, New Delhi
9. Farouq Ahmed, *Cyber Law in India*
10. S. V. Joga Rao, *Law of Cyber Crimes and Information Technology Law*, 2007, Wadhwa & Co, Nagpur
11. Rodney D. Ryder, Guide to Cyber Laws, 2nd Edit, Wadhwa and Company, Nagpur

12. Dr. Keval Ukey: Cyber Forensics, A Legal Perspective of Data Protection and E-Commerce, A-22/1, Akash Vihar, Shahid Chandrashekhar Azad Marg, Nangloi-Najafgarh Road, New Delhi, 2018

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-3 (Major Mandatory)	Cyber Law- I	DDFSDC103T	4	16	40	24	60	2.5 Hrs.

Course DSC1-4: DDFSLB104P	Course Title: Lab Course – I
Course Credits: 2	**Total contact hours: 60 Hrs.**
Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)	
1.	Perform the general protocols of crime scene investigation (SOP)
2.	Chain of custody
3.	Incident Response
4.	Identification and seizure of evidence from the crime scene
5.	Preparing windows and Linux system for investigation
6.	Study of toolkits: FRAT, Win Hex, OS Forensics, CAINE8 OS
7.	Study of various digital forensic tools (FTK, Encase, Autopsy etc.) and its uses
8.	Create a forensic Image of secondary Storage media using FTK and other tools
9.	Disk image analysis using Autopsy
10.	Windows forensic
11.	Study of Windows Registry
12.	Event Log Analysis
13.	Basic network analysis
14.	Network configuration
15.	Data gathering with Google
16.	Website cloning techniques
17.	Windows hardening
18.	Linux hardening
19.	Using proxy server.
20.	Demonstration of DDoS
21.	Sniffing the traffic
22.	Data hiding techniques
23.	Wireless network configuration and security
24.	Firewall configuration
25.	IDS/IPS configuration
26.	Web server configuration
27.	SQL injection
28.	XSS

Course Outcomes -After completion of the course, the learner shall be able to,
1. Equips students with practical skills in crime scene investigation, focusing on the correct implementation of SOPs, chain of custody, and incident response. 2. Learn to identify, seize, and preserve physical and digital evidence, and prepare Windows and Linux systems for forensic analysis. 3. Use the forensic toolkits such as FRAT, Win Hex, and OS Forensics, along with digital forensic tools like FTK, Encase, and Autopsy for forensic imaging and disk analysis. 4. Gain expertise in Windows forensics, network security, and basic network analysis. 5. Delves into advanced topics like data gathering, website cloning, system hardening, and securing web servers against vulnerabilities such as SQL injection and XSS, with an emphasis on reverse engineering and cyber defense techniques.

Suggested Readings:

1. Practical Cyber Forensics by Niranjan Reddy, Après publication
2. Practical Windows forensic Packt publisher
3. Practical Digital Forensics. Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD and Memory by A. Bhardwaj, K. Kaushik BPB Publication
4. Cory Altheide and Harlan Carvey, "Digital Forensics with Open Source Tools", Elsevier, 201
5. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
6. Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-4 (Major Mandatory)	Lab Course – I	DDFSLB104P	2	-	-	20	50	4 Hrs.

Electives (Any One)		
Course DSE1-1: DDFSDE101T	**Course Title: Introduction to Digital Devices and Networking**	
Course Credits: 4	**Total contact hours: 60 Hrs.**	
Course Objectives 1. Study fundamentals of computers, various types of software and hardware devices, operating system, filesystems, computer 2. Network and internet related technology.		
Course Contents: Computer Basics–I, Computer Basics–II; Networking Basics – I; Networking Basics – II		**Reqd. Hrs.**
Unit I – Computer Basics – I		**15 Hrs.**
1.1	**Understanding Computer Hardware:** Looking Inside the Machine**,** Components of a Digital Computer, The Role of the Motherboard, The Roles of the Processor and Memory**,** The Role of Storage Media, Why This Matters to the Investigator**,** The Language of the Machine, Wandering Through a World of Numbers, Who's on Which Base?	
1.2	**Understanding the Binary Numbering System:** Converting Between Binary and Decimal**,** Converting Between Binary and Hexadecimal, Converting Text to Binary, Encoding Nontext Files, Why This Matters to the Investigator	
Unit II – Computer Basics – II		**15 Hrs.**
2.1	**Understanding Computer Operating Systems:** Understanding the Role of the Operating System Software**,** Differentiating Between Multitasking and Multiprocessing Types**,** Multitasking, Multiprocessing**,** Differentiating Between Proprietary and Open-Source Operating Systems	
2.2	**An Overview of Commonly Used Operating Systems :** Understanding DOS**,** Windows1.*x*Through3.*x*, Windows9*x* (95, 95b, 95c, 98, 98SE, and ME), WindowsNT, Windows2000, Windows XP, Linux/ UNIX, Other Operating Systems **Understanding File Systems:** FAT12, FAT16, VFAT, FAT32, NTFS, Other File Systems	
Unit III – Networking Basics – I		**15 Hrs.**
3.1	**Understanding How Computers Communicate on a Network:** Sending Bits and Bytes Across a Network, Digital and Analog Signaling Methods,	

	How Multiplexing Works, Directional Factors, Timing Factors, Signal Interference, Packets, Segments, Datagrams, and Frames, Access Control Methods, Network Types and Topologies, Why This Matters to the Investigator	
3.2	**Understanding Networking Models and Standards:** The OSI Networking Model, The DoD Networking Model, The Physical/Data Link Layer Standards, Why This Matters to the Investigator	
Unit IV – Networking Basics – II		**15 Hrs.**
4.1	**Understanding Network Hardware:** The Role of the NIC, The Role of the Network Media, The Roles of Network Connectivity Devices, Why This Matters to the Investigator **Understanding Network Software**	
4.2	**Understanding Client/Server Computing:** Server Software, Client Software, Network File Systems and File Sharing Protocols, A Matter of (Networking) Protocol, A Matter of (Networking) Protocol **Understanding the TCP/IP Protocols Used on the Internet:** The Need for Standardized Protocols, A Brief History of TCP/IP, The Internet Protocol and IP Addressing, How Routing Works, The Transport Layer Protocols, The MAC Address, Name Resolution, TCP/IP Utilities, Network Monitoring Tools, Why This Matters to the Investigator	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Describe about fundamentals of computers, 2. Various types of software and hardware devices, operating system 3. File Systems, computer network and internet related technology

Suggested Readings:

1. Computer Forensics – Computer Crime Scene Investigation, Second Edition, John R. Vacca, Charles River Media Inc., ISBN 1-58450-389-0
2. Scene of the Cybercrime – Computer Forensics Handbook, Debra Littlejohn Shinder, Ed Tittel, Syngress Publishing Inc., 2002, ISBN 1-931836-65-5
3. Handbook of Digital Forensics and Investigation, Edited by Eoghan Casay, Elsevier Academic Press, ISBN 13: 978-0-12-374267-4
4. Computer Forensics for Dummies
5. Cyber Crime Investigations by Anthony Ryes

6. Computer Forensics: A Field Manual for Cancelling, Examining, and Preserving
7. Evidence of Computer Crimes by Albert J. Marcella
8. Cyber Crime Investigator's Field Guide by Bruce Middleton
9. Digital Forensics: Digital Evidence in Criminal Investigation by Angus M. Marshall
10. Digital Forensics for Network, Internet and Cloud Computing by Clint P. Garrison
11. A Practical Guide to Computer Forensics Investigations by Dr. Darren R. Heyes
12. Computer Fundamentals by Pradeep K. Sinha & Priti Sinha
13. Computer Fundamentals by Larry Long
14. Computer System Architecture, M. Morris Mano, PHI Publications
15. Computer Organization and Architecture Designing for Performance, Eight Edition, William Stallings, Pearson Publication

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Major Elective)	Introduction to Digital Devices and Networking	DDFSDE101T	4	16	40	24	60	2.5 Hrs.

Course DSE1-1: DDFSDE102T	Course Title: Regulation of Cyberspace
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To provide a foundational understanding of cyberspace, its unique characteristics, and the legal challenges it presents.
2. To explore the differences between real space and cyberspace, along with the concept of digital identity.
3. To address various legal issues, including jurisdiction, privacy, and security concerns, while also examining contemporary technologies like AI, IoT, and blockchain.
4. To study the need for and methods of international regulation of cyberspace, with a focus on legal frameworks in different regions.
5. To cover data protection, emphasizing the importance of privacy and the international legal standards for safeguarding data in the digital realm.

Course Contents: General Introduction to Cyberspace; Legal Challenges of cyberspace; International Regulation of Cyberspace; Data Protection in Cyberspace		**Reqd. Hrs.**
Unit I – General Introduction to Cyberspace		**15 Hrs.**
	• Overview of Cyberspace- • Meaning and definition of cyberspace • Real space and cyberspace • Concept of Digital Identity in cyber world • Legal Assumptions in Cyber World (a) World Unbounded (b) Global Enforcement (c) Corporeal Property Unfounded (d) Virtual Relationship (e) Digital Records	
Unit II – Legal Challenges of cyberspace		**15 Hrs.**
	• **General Legal Issues in Cyberspace-** Domain Name Issues in cyberspace Jurisdiction Issues in cyberspace Data protection and Privacy issues in cyberspace Authentication issues in cyberspace State Behaviour in cyberspace	

	• **Contemporary Issues in Cyberspace-** 1. **Artificial Intelligence-** Deep fake attacks, AI phishing attacks, Denial of service (DoS) attacks, AI-powered ransom ware, Advanced persistent threats, Budapest Convention on Cybercrime, AI & International Humanitarian Law **Legal Challenges-** Ethical and Legal Responsibility, Complex Accountability, Autonomous Decision-making, Privacy and Data Protection, Cyber security and State Responsibility 2. **IOT (Internet of things)-** Overview of Concept of IoT, Application of IoT Issues - Internet walls, Cloud attacks, Botnet problems, Security issues **Legal Challenges-** Data protection, Data ownership, Security, Jurisdiction, Product liability & consumer protection, Formation & validity of e-contracts 3. **BIGDATA-** What is Big Data? Characteristics & application of BIGDATA **Legal challenge-** Compliance with data protection laws and regulations, data licensing issues, Intellectual property ownership and competition law issues 4. **Block chain & smart contract technology-** What is Block-chain Technology? **Legal Challenges-** Jurisdictional Issues, Regulatory Compliance, Privacy & Data protection, Intellectual Property, Determination of Liability, Enforceability of Smart Contract, Insurance Regulation, Jurisdictional challenges, Dispute Resolution, Decentralized Autonomous Organizations (DAOs) 5. **Crypto-currency-** History of Block Chain and Crypto-currency, Overview of the Most Common Crypto-currencies **Legal Challenges-** Anonymity of transacting parties, Problems related to lack of proper authority, Absence of well-defined Laws, Tax Evasion, Money laundering etc., phishing attacks, loss of data, Insecurity of trading & purchase platforms etc.	
Unit III – International Regulation of Cyberspace		**15 Hrs.**
	• Need of Regulation	

	• How Cyberspace can be Regulated • Legal and Self-Regulatory Framework • Filtering Devices and Rating Systems • Regulation of Internet Content • UNCITRAL Model Law • Global scenario- 1. United States- Communications Decency Act 1996(CDA), COPA, CIPA and Other Related Legislations 2. European Union- The Council of Europe's (CoE) Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law 2024	
Unit IV – Data Protection in Cyberspace		**15 Hrs.**
	• Concept of Data in cyberspace • Right to privacy and personal data in cyberspace • Need and necessity of data protection in cyberspace • International Legal framework of data protection- General Data Protection Regulations (GDPR), 2016 • Legal Framework for Regulation of Cyberspace Content in India- Digital Personal Data Protection Act, 2023.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. To understand the meaning and nature of cyberspace. 2. To study the difference between Real Space and Cyberspace. 3. To analyze contemporary legal challenges in Cyber World. 4. To examine the International legal framework available for regulation of cyberspace. 5. To study legal implications of data protection in cyberspace.

Suggested Readings:

1. Rodney D Ryder- Guide to Cyber Laws 3rd Edition (2007)
2. Janine Kremling, Amanda M. Sharp Parker- Cyberspace, Cybersecurity, and Cybercrime
3. David Skillicorn- C*yberspace, Data Analytics, and Policing* (2022)
4. Evon Abu-Taieh, Issam H. Al Hadid, Abdelkrim El Mouatasim- Cyberspace (2020)
5. Krishan Kumar Goyal, Amit Garg, Saurabh Singhal- Cyber Security & Data Privacy (2021)
6. Alan Davidson- Privacy and data protection in cyberspace, The Law of Electronic

Commerce by Cambridge University press (2009)

7. Duggal Pawan, Mobile Law, Universal Law Publishing Co. Pvt. Ltd. 2nd Edition

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Major Elective)	Regulation of Cyberspace	DDFSDE102T	4	16	40	24	60	2.5 Hrs.

Minor	
Course DSC2-1: DDFSRM101T	**Course Title: Research Methodology**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand research and its significance
2. To learn research design and formulation of hypothesis
3. To learn data sampling and data collection techniques
4. To learn various statistical tools involved in analyzing data
5. To understand data interpretation and various types of scientific report writing
6. To understand various tools available for data discovering and management
7. To understand the ethics in scientific publishing

Course Contents: Introduction to Research and Research Methodology; Hypothesis, Sampling and Acquisition of Data; Processing and Interpretation of Data; Report Writing		**Reqd. Hrs.**
Unit I – Introduction to Research and Research Methodology		**15 Hrs.**
	Research-Definition and Objectives Types of Research Research Design: Definition, need and types of research design Literature review process	
Unit II – Hypothesis, Sampling and Acquisition of Data		**15 Hrs.**
	Types of Hypotheses Formulation of Hypothesis and Hypothesis Testing Sampling procedure and different types of sampling methods Types of data and collection methods	
Unit III – Processing and Interpretation of Data		**15 Hrs.**
	Various statistical tools used for data analysis Tabulation and Graphical representation of data Interpretation of data	
Unit IV – Report Writing		**15 Hrs.**
	Types of scientific reports Various search tools and Reference management software's used in scientific research Steps involved in scientific writing Ethics in scientific publishing	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Cultivate scientific and research temper 2. Formulate hypothesis and design research plan 3. Collect data and apply various statistical tools to test hypothesis 4. Interpret data and based on it write scientific reports 5. Apply various tools for data discovering and management 6. Apply ethics in scientific writing

Suggested Readings:

1. Kothari, C. R. (2004). Research Methodology: Methods and Techniques. India: New Age International (P) Limited.
2. Baykoucheva, S. (2015). Managing Scientific Information and Research Data. United Kingdom: Elsevier Science.
3. D. K. Bhattacharyya (2006), Research Methodology. India: Excel Books.
4. Thomas, C. G. (2021). Research Methodology and Scientific Writing. Germany: Springer International Publishing.
5. Nagar P (2021), Research Methodology Made Easy: A Handbook on Research Methodology. India. Exceller Books.
6. Kumar, R. (2010). Research Methodology: A Step-by-Step Guide for Beginners. United Kingdom: SAGE Publications.
7. Körner, A. M. (2008). Guide to Publishing a Scientific Paper. United Kingdom: Taylor & Francis.
8. Ellison, C. (2010). McGraw-Hill's Concise Guide to Writing Research Papers. United Kingdom: McGraw-Hill Education.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC2-1 (Minor)	Research Methodology	DDFSRM101T	4	16	40	24	60	2.5 Hrs.

SEMESTER – II

Mandatory	
Course DSC1-5: DDFSDC201T	**Course Title: Cyber Forensics- II**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To introduce Virtualization and its technologies
2. To provide the skills and knowledge necessary to implement, provisioning and administer server and desktop virtualization.
3. Gain insights into cloud forensics, including challenges, methodologies, and the forensic analysis of cloud-based evidence.
4. Understand the principles and methodologies of OSINT (Open-Source Intelligence) and its applications in cyber security and digital investigations.
5. Gain knowledge of the emerging trends and future directions in OSINT, including advancements in tools, techniques, and data sources.
6. Develop proficiency in using OSINT tools and techniques for planning, collecting, analyzing, and disseminating intelligence.

Course Contents: Virtual Machine Forensics; Cloud Forensics; Email Investigation; Gathering Evidence from OSINT Sources	**Reqd. Hrs.**
Unit I – Virtual Machine Forensics	**15 Hrs.**

• Types of Hypervisors
• Hypervisor Files and Formats
• Use and Implementation of Virtual Machines in Forensic Analysis
• Use of VMware to establish working version of suspect's machine
• Networking and virtual networks within Virtual Machine
• Forensic Analysis of a Virtual Machine
  ➢ Imaging of a VM
  ➢ Identification and Extraction of supporting VM files in the host system
  ➢ VMSnapshots
  ➢ MountingImage
• Searching for evidence	

Unit II – Cloud Forensics	**15 Hrs.**
• Introduction to Cloud computing • Challenges faced by Law enforcement and government agencies • Cloud Storage Forensic Framework	

	➢ Evidence Source Identification and preservation in the cloud storage ➢ Collection of Evidence from cloud storage services ➢ Examination and analysis of collected data ✓ Cloud Storage Forensic Analysis ✓ Evidence Source Identification and Preservation ✓ Collection of evidence from cloud storage devices ✓ Examination and analysis of collected data • Dropbox analysis: • Google Drive analysis • Issues in cloud forensics Case Studies	
Unit III – Email Investigation		**15 Hrs.**
3.1	• Working of Email, Types of email, configurations – IMAP / POP., Various parts of an email. Components of an email header. Email header analysis. Differences between emails headers of various service providers. Identifying spoofed email, phishing email. Step action guide on email tracking and tracing. Requesting details from intermediaries. • Collection of email as evidence – single email, multiple emails, entire mailbox etc. • Presentation of email as evidence in court. • Restoring deleted emails from web and app. • Challenges such as proxy and VPN.	
3.2	• Attack Simulation Techniques and Tools--Web Application: The App Checklist, Manual Testing, Automated Testing, Commercial Tools	
Unit IV – Gathering Evidence from OSINT Sources		**15 Hrs.**
	• Goals of OSINT Collection • OSINF Categories, Benefits and Challenges of OSINT • OSINT Methodology and Process (planning, collection, analysis, and dissemination), Legal and Ethical Considerations in OSINT (privacy, data protection, and ethical guidelines) • OSINT Tools and Techniques (search engines, social media, online communities) • OSINT Data Sources and Research Skills (web resources, government databases, academic sources)	

	• Web Scraping and Data Extraction for OSINT (automated data collection) • Social Media Intelligence and Analysis (monitoring, sentiment analysis, network analysis), Geospatial OSINT and Mapping (geo location, satellite imagery, GIS tools),Dark Web and Deep Web Investigations (TOR, hidden services, onion sites),OSINT for Cyber Threat Intelligence (monitoring threat actors, identifying vulnerabilities),Image and Video Analysis in OSINT (reverse image search, deep fake detection) • OSINT in Social Engineering and Fraud Investigations • OSINT in Business Intelligence and Competitive Analysis • OSINT for Digital Forensics and Incident Response • Emerging Trends and Future Directions in OSINT	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Practice various methods of virtualization and perform desktop and server virtualization. 2. Analyze and investigate Live and Dead virtualization environment. 3. Perform forensic analysis of cloud-based evidence and conduct cloud forensics investigations in compliance with legal and ethical considerations. 4. Apply OSINT methodologies and techniques for collecting, analyzing, and disseminating intelligence in cyber security and digital investigations. 5. Utilize various OSINT tools, including search engines, social media monitoring, web scraping, and geospatial mapping tools. 6. Assess and address legal and ethical considerations related to OSINT, ensuring privacy, data protection, and adherence to ethical guidelines

Suggested Readings:

1. Virtualization and Forensics by Diane Barrett, Greg Kipper
2. Virtualization Security Protecting virtualized environment By Dave Shackleford
3. "Cloud Forensics: A Guide for Incident Responders" by Darren Quick, Ben Martini, and Raymond Choo
4. "Cloud Computing Forensics: Challenges and Solutions" by George Grispos, et al.
5. "Investigating Cloud Computing: Forensics and Governance" by Anthony Reyes, et al.

6. "Cloud Storage Forensics" by Darren Quick, Ben Martini, and Raymond Choo
7. "Automating Open-Source Intelligence: Algorithms for OSINT" by Robert Layton, et al.
8. "Digital Forensics: Threatscape and Best Practices" by John Sammons
9. "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics" by John Sammons
10. OSINT Playbook: A Guide to Open-Source Intelligence Gathering for Threat Intelligence" by Armstrong, Wilkinson, and Swetnam
11. "Introduction to Open-Source Intelligence in the Digital Age" by Babak Akhgar, David Radcliffe, and Andrew Staniforth
12. "Open-Source Intelligence Investigation: From Strategy to Implementation" by Babak Akhgar, et al.
13. Practical Open-Source Intelligence for Cyber Intelligence" by Kevin Cardwell
14. Dr. Keval Ukey: Cyber Forensics, A Legal Perspective of Data Protection and E-Commerce, A-22/1, Akash Vihar, Shahid Chandrashekhar Azad Marg, Nangloi-Najafgarh Road, New Delhi, 2018

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-5 (Major Mandatory)	Cyber Forensics-II	DDFSDC201T	4	16	40	24	60	2.5 Hrs.

Course DSC1-6: DDFSDC202T	Course Title: Mobile Forensics
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Gain foundational knowledge of cellular network components, mobile devices, and the hardware and software characteristics that distinguish mobile operating systems from desktop systems.
2. Explore the importance of mobile forensics, including the challenges faced in the field, and understand the processes and practical approaches for extracting evidence from mobile devices.
3. Delve into the architecture and file system of Android devices, learn data extraction and recovery techniques, and set up forensic environments for Android data analysis.
4. Study the internal structures of iOS, Windows Phone, and BlackBerry devices, focusing on file systems, data acquisition, analysis, and recovery methods unique to each platform.
5. Develop skills in identifying and analyzing mobile malware, using various tools and techniques for static and dynamic analysis, and understand the security vulnerabilities and threats specific to mobile applications.

Course Contents: Introduction to Mobile Forensics; Android Forensics; iOS Forensics and Windows Phone, BlackBerry Forensics; Mobile Malware		**Reqd. Hrs.**
Unit I – Introduction to Mobile Forensics		**15 Hrs.**
1.1	Basics of Mobile phone & communications: Components of Cellular Network, Different Mobile Devices, Hardware Characteristics of Mobile Devices, Software Characteristics of Mobile Devices, Mobile Operating Systems: Classification of Mobile Operating Systems (WebOS, Symbian OS, Android OS, RIM BlackBerry OS, Windows Phone 7, Apple iOS), difference between desktop operating system and mobile operating system	
1.2	Introduction to Mobile Forensics, the need for mobile forensics, Understanding mobile forensics, Challenges in mobile forensics The mobile phone evidence extraction process, Practical mobile forensic approaches: Mobile forensic tool leveling system, Data acquisition methods. Potential evidence stored on mobile phones. Rules of evidence	
Unit II – Android Forensics		**15 Hrs.**

2.1	Android Forensics: Understanding Android, The evolution of Android, The Android architecture, The Linux kernel layer, The Hardware Abstraction Layer Libraries, Dalvik Virtual Machine (DVM), ART164, The Java API framework layer, the system apps layer, Android file hierarchy, Android file system Android Forensic Setup and Pre-Data Extraction Techniques: Setting up a forensic environment for Android, Connecting an Android device to a workstation, Screen lock bypassing techniques, Using ADB to bypass the screen lock	
2.2	Android Data Extraction Techniques: Understanding data extraction techniques, Manual data extraction, Logical data extraction, Physical data extraction. Android Data Recovery Techniques and Tools, Analyzing and extracting data from Android image files using the Autopsy tool, Understanding techniques to recover deleted files from the SD card and the internal memory.	
Unit III – iOS Forensics and Windows Phone, BlackBerry Forensics		**15 Hrs.**
3.1	**Windows Phone Forensics:** Windows Phone OS, Windows Phone file system **BlackBerry Forensics:** BlackBerry OS, BlackBerry analysis	
3.2	**iOS Forensics:** Understanding the Internals of iOS Devices, iPhone models and hardware, iPad models and hardware, The HFS Plus and APFS filesystems, The iPhone OS, Data Acquisition from iOS Devices, Operating modes of iOS devices, Password protection and potential bypasses, Logical acquisition, Filesystem acquisition, iOS Data Analysis and Recovery Overview of iOS Forensic Tools and its features Difference between Android and iOS	
Unit IV – Mobile Malware		**15 Hrs.**
	Introduction to Mobile Malware Analyzing Mobile Malware Overview of App Analysis tools APK File Structure. AndroidManifest XML File Reversing to Get Source Code of the Application – Decompiling with dex2jar	

	Reversing and Re-compiling with APKTool APK Teardown in a Nutshell on Your Android Device Static vs. Dynamic Analysis Static Analysis of Android Application Dynamic Analysis of Android Application MobSF – Mobile – Security – Framework. Malware Analysis Automated Security Assessments Intercept Traffic Intent Sniffing Fuzzing using Burp – Password Brute-Force. Username Enumeration OWASP top 10 vulnerabilities for mobiles	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand Basics and important terminology of the mobile devices. 2. Understand Internal working structure of the various mobile platforms. 3. Practice Different types of acquisition methods on various platforms. 4. Practice Data recovery techniques and Data extraction techniques on various mobile platforms. 5. Practice Different forensic tools that are used for various mobile platforms

Suggested Readings:

1. Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd., 2014, ISBN 978-1-78328-831-1
2. Learning iOS Forensics, Mattia Epifani, Pasquale Stirparo, Packt Publishing Ltd, 2015, ISBN 978-1-78355-351-8 iPhone and iOS Forensics Investigation, Analysis and Mobile Security for Apple
3. iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempka, Publisher Synergy Mobile phone security and forensics: A practical approach *by* Iosif I. Androulidakis, Springer publications, 2012
4. iPhone, iPad, and iOS Devices by Andrew Hoog, Katie Strzempka, Publisher Synergy Mobile phone security and forensics: A practical approach *by* Iosif I. Androulidakis, Springer publications, 2012
5. Learning Android Forensics Analyze Android Devices with The Latest Forensic Tools and Techniques 2nd Ed. by Oleg Skulkin, Donnie Tindall, Rohit Tamma, Packt Publishing Ltd ,2018

6. Mobile Malware Attacks and Defense, Ken Dunham, Syngress Publishing, Inc., ISBN978-1-59749-298-0
7. Wireless Crime and Forensic Investigation, Gregory Kipper, Auer Bach Publications
8. https://codered.eccouncil.org/course/mobile-penetration-testing-of-android-applications?logged=false
9. CYBERCRIME INVESTIGATION HANDBOOK FOR POLICE OFFICERShttps://ssb.gov.in/WriteReadData/LINKS/5%20days36c9f227-7ceb-4b60-bada-f52beeb7e196.pdf
10. ASCL Cyber Crime Investigation Manual https://police.mizoram.gov.in/wp-content/uploads/2023/01/SOP-Cyber-Crime-Investigation-v1.0.pdf

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-6 (Major Mandatory)	Mobile Forensics	DDFSDC202T	4	16	40	24	60	2.5 Hrs.

Course DSC1-7: DDFSDC203T	Course Title: Cyber Law-II
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To familiarize important aspects of national and international provisions of E-Commerce and E-Governance
2. TO understand the basics of Intellectual property rights and related legal aspects
3. TO understand the concepts of trademark and Domain name
4. To understand the basics of Copyrights, patents and designs and related legal aspects

Course Contents: E-Commerce and E-Governance; Information Technology and Intellectual Property; Intellectual Property Rights in Digital Medium		**Reqd. Hrs.**
Unit I – E-Commerce and E-Governance		**15 Hrs.**
	• International Organizations and Their Roles, ICANN etc. • UDRP Dispute Resolution Policy • WTO and TRIPS • UNICITRAL Model LAW • E- Commerce and E- Governance in India	
Unit II – Information Technology and Intellectual Property		**15 Hrs.**
	• Jurisprudence of Concept of Intellectual Property • Salient features of Indian Patent Act, 1970 • Salient features of Indian Copyright Act, 1957 • Salient features of Indian Trademark Act, 1999 • Salient features of The Design Act, 2000.	
Unit III – Intellectual Property Rights in Digital Medium–I		**15 Hrs.**
	• Meaning, Nature, Scope and types of Intellectual Property in India • Concept of Trademark/Domain Name • Domain Names and Trademark Disputes • Cyber Squatting and Reverse Hijacking • Law relating to Semiconductor, Layout and Design.	
Unit IV – Intellectual Property Rights in Digital Medium–II		**15 Hrs.**
	• Concept of Copyright and Patent in Cyberspace • Software Piracy and Musical Piracy • Copyright and WIPO Treaties • Protection of Software and Hardware.	

	• Geographical Indication, Plant varieties and Bio Piracy	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understanding concepts of E- Commerce and E- Governance. 2. Understand the various facets of Intellectual property rights. 3. Understand the concepts of trademark and Domain name. 4. Understand the cyber offences and penalties under IT Law. 5. Understand the Intellectual Property Rights in digital medium.

Suggested Readings:

1. Kamlesh N. & Murali D. Tiwari (Ed), *IT and Indian Legal System*, Macmillan India Ltd, New Delhi
2. K. L. James, *The Internet: A User's Guide* (2003), Prentice Hall of India, New Delhi
3. Chris Reed, *Internet Law-Text and Materials*,2nd Edition,2005, Universal Law Publishing Co., New Delhi
4. Vakul Sharma, *Handbook of Cyber Laws*, Macmillan India Ltd, New Delhi
5. S.V. JogaRao, *Computer Contract & IT Laws* (in2Volumes),2005 Prolific Law Publications, New Delhi
6. T. Ramappa, *Legal Issues in Electronic Commerce*, Macmillan India Ltd, New Delhi
7. Indian Law Institute, *Legal Dimensions of Cyber Space*, New Delhi
8. Pankaj Jain & Sangeet Rai Pandey, *Copyright and Trademark Laws relating to Computers*, Eastern Book Co, New Delhi Farouq Ahmed, *Cyber Law in India*
9. S. V. Joga Rao, *Law of Cyber Crimes and Information Technology Law*,2007, Wadhwa & Co, Nagpur
10. Rodney D. Ryder, Guide to Cyber Laws, 2ndEdit, Wadhwa and Company, Nagpur
11. Dr. Keval Ukey: Cyber Forensics, A Legal Perspective of Data Protection and E-Commerce, A-22/1, Akash Vihar, Shahid Chandrashekhar Azad Marg, Nangloi-Najafgarh Road, New Delhi, 2018

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-7 (Major Mandatory)	Cyber Law-II	DDFSDC203T	4	16	40	24	60	2.5 Hrs.

Course DSC1-8: DDFSLB204P	Course Title: Lab Course – II
Course Credits: 2	**Total contact hours: 60 Hrs.**
Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)	
1.	Installation of VMWare virtual machine.
2.	Installation of Virtual Box virtual machine.
3.	Installation of windows operating system on virtual machine
4.	Installation of Linux operating system on virtual machine
5.	Creating virtual network
6.	Configuration of windows web server
7.	Configuration on Linux server
8.	Analysis of traces of Virtual Machine using – Registry Analysis
9.	Analysis of VMWare traces on the system
10.	Analysis of external device
11.	Analysis of prefetch file
12.	Data Carving
13.	Investigating Dead Virtual Environments
14.	Recovering cached and internet artifacts
15.	Facebook profile data acquisition and documentation.
16.	Study of E-mail Headers.
17.	Forensic investigation on a cloud storage service, analyzing files, access logs, and metadata.
18.	Dropbox analysis
19.	Google Drive analysis
20.	Installation of Android Studio
21.	Working on Open-source android forensic tool kit (OSAF-TK/ Santuko Linux/Andriller and other tools)
22.	Extraction of mobile data using mobile forensic tools
23.	Physical Extraction of Data from mobile device using mobile forensic tools
24.	Analyzing data of android mobile using mobile forensic tools (MOBILedit/autopsy forensic tool etc.)
25.	Extraction of .apk file from mobile device using ADB
26.	Reversing engineering an Android application using tools (dex2jar/ JDGUI/

	APKtool/ Androguardetc)
27.	Collect OSINT data using various online sources, such as search engines, social media platforms, and specialized databases.
28.	Apply web scraping techniques to automate the collection of OSINT data from websites.
29.	Conduct sentiment analysis on social media data to extract insights and detect trends.
30.	Perform geospatial OSINT analysis, including geo location of IP addresses and mapping of OSINT data.
31.	Explore dark web and deep web investigations, accessing hidden services and analyzing Tor network activity.
32.	Investigate a case involving OSINT for cyber threat intelligence, monitoring threat actors and identifying potential vulnerabilities.
33.	Conduct an OSINT investigation for digital forensics and incident response, gathering intelligence to support the investigation process.
34.	Stay updated with emerging trends in OSINT tools and techniques by exploring new tools and experimenting with innovative methodologies

Course Outcomes -After completion of the course, the learner shall be able to,

1. Install and configure VMWare and VirtualBox virtual machines with Windows and Linux operating systems and create virtual networks to simulate real-world environments.
2. Set up and configure both Windows and Linux servers, focusing on web server functionalities and security measures.
3. Conduct forensic investigations on virtual machines, including registry analysis, trace analysis, external device analysis, and prefetch file analysis.
4. Perform data carving and recover cached and internet artifacts from virtual environments, enhancing skills in digital forensics.
5. Investigate cloud storage services like Dropbox and Google Drive, and extract and analyze data from Android devices using mobile forensic tools.
6. Reverse engineer Android applications, collect and analyze OSINT data using various techniques, and conduct investigations on the dark and deep web for cyber threat intelligence.

Suggested Readings:

1. Practical Digital Forensics. Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD and Memory by A. Bhardwaj, K. Kaushik BPB Publication
2. Practical Open-Source Intelligence for Cyber Intelligence" by Kevin Cardwell
3. Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd., 2014, ISBN 978-1-78328-831-1

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-8 (Major Mandatory)	Lab Course – II	DDFSLB204P	2	-	-	20	50	4 Hrs.

Electives (Any One)	
Course DSE2-1: DDFSDE201T	**Course Title: Cyber Crime Investigation**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Present an overview of types of cybercrime.
2. Analyses the different crimes that pertain to use of Emails, various Social Media platforms, dark Web.
3. Identify strategies to track, document and use Emails, Social Media platforms, and the dark web, data as evidence

Course Contents: Introduction to location / cloud-based investigations; Introduction to Website Investigations; Social Network Crime Investigations, Investigation of Fin-Tech fraud; Dark Web Investigations		**Reqd. Hrs.**
Unit I – Introduction to Location/ Cloud-based Investigations		**15 Hrs.**
	Introduction to Location Based Services., Types of Location Based Services. Triangulation and GPS Techniques to pinpoint the actual location of the criminals., By using CDR and Cell ID. By using Triangulation techniques. By using GPS tagging on photographs. By using Google Photos. Etc. By using WhatsApp, Facebook, Viber etc. Types of cloud service providers (Android / Apple / Blackberry etc.) Tracking of missing / stolen mobile phones or tablets, gathering data created using various Google services, requesting details from Google via legal approach Introduction to Location Based Services. Retrieval of data from Google / iCloud /Microsoft cloud services. Tracing missing/stolen mobile By Using IMEI No. Tracing missing/stolen mobile By Using MAC No.	
Unit II – Introduction to Website Investigations		**15 Hrs.**
	(Handling complaints related to website crimes, identifying a fake website, Identification of IP address of the website, Gathering information related to a website ownership, Collection of evidence (Live, archival), Website defacement investigation, PR Infringement Issues, Responsibilities of intermediaries, Acquaints Website Investigation. Deleted Website Investigation., Website specific content removal. Data and document forgery, Notice process to WSP-ESP- ISP-MSP Challenges involved - PROXY or VPN involvement in website investigation. Relevant Sections of IT Act & IPC laws for FIR registration.	

	Standard Operating Procedures for investigating website related crimes.	
Unit III – Social Network Crime Investigations, Investigation of Fin-Tech Fraud		**15 Hrs.**
	Introduction to social media (Facebook, Tweeter, Instagram, Snapchat, LinkedIn, YouTube, WhatsApp, Telegram, etc.), Possible crimes on social media. Some frequent modus operandi, Investigation Procedure for social media related Crimes, Social Media monitoring and intelligence platforms *Matrimonial/Dating/ Adultery Related Investigations* *Other Social Media Apps/ Websites Related Investigations* *Advisory content for Cyber Safety Awareness* *Investigation of Fin-Tech fraud*: Various kinds of Fin-Tech options available in India, Common misconceptions, investigating e-wallets Investigating ATM related frauds, Investigating OTP related frauds, Investigating Payment gateways, Investigating identity theft related cases Database forensics, Job frauds, Gambling, Betting, Financial transactions for illegal activities, Load fraud.	
Unit IV – Dark Web Investigations		**15 Hrs.**
	Introduction of Deep & Dark Net., Surface Internet vs. Deep Internet., Indexed Website vs. Non-Indexed Websites. Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links. Modus operandi of cyber-crimes committed using Dark Web. Working principle of BlockChain. Concepts of Crypto currencies and mechanism behind it. Wallet Tracking, Public Key vs. Private Key (With respects to Crypto Currencies), Introduction to track crypto currencies. Challenges in investigations.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understanding the methods of cyber investigation 2. Articulate an overview of types of cybercrime. 3. Analyze the different crimes that pertain to use of Emails, various Social Media platforms, and the dark web. 4. Identify strategies to track, document and use Emails and Social Media platforms as evidence.

Suggested Readings:

1. Tommie W. Singleton, Aaron J. Singleton (2010): Fraud Auditing and Forensic Accounting.
2. Mark Nigrini (2011): Forensic Analytics: Methods and Techniques for Forensic Accounting.
3. Jo Kranacher, Richard Riley, Joseph T. Wells (2010) Forensic Accounting and Fraud Examination.
4. Steven L. Skalak, Thomas W. Golden, Mona M. Clayton (2011): A Guideto Forensic Accounting Investigation.
5. Cybercrime Investigation Handbook for Police Officers https://ssb.gov.in/WriteReadData/LINKS/5%20days36c9f227-7ceb-4b60-bada-f52beeb7e196.pdf
6. ASCL Cyber Crime Investigation Manual https://police.mizoram.gov.in/wp-content/uploads/2023/01/SOP-Cyber-Crime-Investigation-v1.0.pdf
7. Dr. Keval Ukey: Cyber Forensics, A Legal Perspective of Data Protection and E-Commerce, A-22/1, Akash Vihar, Shahid Chandrashekhar Azad Marg, Nangloi-Najafgarh Road, New Delhi, 2018

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSE2-1 (Major Elective)	Cyber Crime Investigation	DDFSDE201T	4	16	40	24	60	2.5 Hrs.

Course DSE2-1: DDFSDE202T	Course Title: Cyber Law: International Perspective and Future Challenges
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives

1. Understand Foundations of International Law and Cyber Legislation
2. Analyze Global Frameworks for Human Rights and Cybersecurity.
3. Evaluating Legal Challenges in Cryptocurrency and Digital Finance.
4. Assessing Legal and Ethical Issues in Social Media and Data Privacy.
5. Develop Insights into Emerging Cyber Legal Issues.

Course Contents: Foundations of International Law and Cyber Legislation; Global Frameworks for Human Rights, Trade, and Cybersecurity; Cryptocurrency, Blockchain, and Legal Challenges in Digital Finance and Gaming; Legal and Ethical Dimensions of Social Media, Data Privacy, and Artificial Intelligence		**Reqd. Hrs.**
Unit I – Foundations of International Law and Cyber Legislation		**15 Hrs.**
	International Law: Meaning, Definition and Concept. Sources of International Law. State, Sovereignty and Jurisdiction. International Bodies: United Nations, UNGA and ICJ. Reciprocal Arrangements and Investigations of Cyber Crimes. Human Rights and Cyber Laws.	
Unit II – Global Frameworks for Human Rights, Trade, and Cybersecurity		**15 Hrs.**
	International Conventions on Human Rights: UDHR, ICCPR, ICESCR, ICERD, CEDAW, CRC and CRPD, etc. UDRP Dispute Resolution Policy. UNCITRAL Model of Law. WTO and TRIPS. WIPO Treaties. Budapest Convention on Cybercrime. Cyber Crimes and Legal Framework in other Countries	
Unit III – Cryptocurrency, Blockchain, and Legal Challenges in Digital Finance and Gaming		**15 Hrs.**
	Concept of Cryptocurrency. Internet and Mobile Association of India Vs. Reserve Bank of India:	

	Recognition of Cryptocurrency in India? E-Rupee: Block Chain and Currency. Block Chain Technology and Governing Law: Paradox? Online Gaming, related Cyber Crimes and Need for Legislation Governing Online Gaming.	
Unit IV – Legal and Ethical Dimensions of Social Media, Data Privacy, and Artificial Intelligence		**15 Hrs.**
	Social Media Applications and E-Contracts. Misuse of Social Media and Cyber Crimes. Social Media and Data Privacy. Facebook – Cambridge Analytica Data Breach: A Case Study. Framework Convention on Artificial Intelligence & Human Rights, Democracy and Rule of Law: Treaty by Council of Europe *vis-à-vis* European Union Artificial Intelligence Act.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand the intersection of cyber law with international law and human rights, including concepts, sources of international law, state sovereignty, jurisdiction, and the role of international bodies like the UN, UNGA, and ICJ, as well as reciprocal arrangements for cybercrime investigations. 2. Explore international conventions and legal frameworks relevant to cyber law, including human rights treaties (UDHR, ICCPR, ICESCR, etc.), UDRP Dispute Resolution Policy, UNCITRAL Model Law, WTO and TRIPS, WIPO treaties, the Budapest Convention on Cybercrime, and cybercrime laws in various countries. 3. Learn about cryptocurrency, blockchain technology, and their related laws, including the concept of cryptocurrency, legal recognition in India (Internet and Mobile Association of India vs. RBI), E-Rupee, the paradox of blockchain governing law, and the cybercrimes and legal needs related to online gaming. 4. Examine social media, mobile applications, and related laws, including e-contracts, misuse of social media, data privacy issues, case studies like the Facebook-Cambridge Analytica data breach, and the global perspective on AI challenges through frameworks like the Council of Europe's Framework Convention on AI and the European Union AI Act

Suggested Readings:

1. S. K. Kapoor – "International Law and Human Rights".
2. V. K. Ahuja – "Public International Law", (2023).
3. Dr. S. R. Myneni – "Information Technology Law", (2023).
4. Dr. Keval Ukey – "Cyber Forensics, a legal perspective of Data Protection and E-Commerce".
5. Convention on Artificial Intelligence & Human Rights, Democracy and Rule of Law: Treaty by Council of Europe vis-à-vis European Union Artificial Intelligence Act.
6. Relevant and Latest Case Laws.

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSE2-1 (Major Elective)	Cyber Law: International Perspective and Future Challenges	DDFSDE202T	4	16	40	24	60	2.5 Hrs.

On Job Training	
Course OJT-1/ FP-1: DDFSOJ201P / DDFSFP201P	**Course Title: On Job Training / Field Project**
Course Credits: 4	**Total contact hours: 120 Hrs. (During Summer Vacation)**

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
OJT-1/ FP-1 (OJT/ FP)	On Job Training/ Field Project	DDFSOJ201P / DDFSFP201P	4	-	-	40	100	6 Hrs.

Ad-hoc BoS in Forensic Science
Credit Distribution of PGD CSRL

Yr	Lvl	Sem	Major		Minor	OE	VSC, SEC (VSEC)	AEC, VEC, IKS All Mandatory	OJT, FP, CEP, CC, RP	Cum. Cr. / Sem	Cum. Cr. / Degree
			Mandatory	Electives							
1	6.0	I	DSC1-1 DCFSDC101T Cyber Security (4)	DSE1-1 DCFSDE101T Introduction to Digital Forensics (4) **OR** DSE1-1 DCFSDE102T Regulation of Cyberspace (4)	DSC2-1 DCFSRM101T Research Methodology (4)	—	—	—	—	22	44 PG Diploma in Cyber Security and Related Laws (44)
			DSC1-2 DCFSDC102T Web Application Security (4)								
			DSC1-3 DCFSDC103T Cyber Law & Practice in India (4)								
			DSC1-4 DCFSLB104P Lab Course – I (2)								
		II	DSC1-5 DCFSDC201T Penetration Testing for Website (4)	DSE2-1 DCFSDE201T Network and Security (4) **OR** DSE2-1 DCFSDE202T Cyber Law: International Perspective and Future Challenges (4)	—	—	—	—	OJT/ RP/ FP DCFSOJ201P / DCFSFP201P (4)	22	
			DSC1-6 DCFSDC202T Dark Web (4)								
			DSC1-7 DCFSDC203T Intellectual Property Rights in Cyberspace (4)								
			DSC1-8 DCFSLB204P Lab Course – II (2)								
Cum. Cr.			**28**	**8**	**4**	—	—	—	**4**	**44**	
Award of PG Diploma in Cyber Security and Related Laws with 44 credits.											

Postgraduate Diploma in Cyber Security and Related Laws

Teaching and Examination Scheme – Semester I

Course	Course Code	Course Title	Credits	Teaching Scheme				Examination Scheme						
								Theory				Practical		
				Lectures per Week	Practical per Week	Total Periods	Duration in Hours	Max. Marks (Theory)	Max. Marks (Internal)	Total Marks	Minimum Passing Marks*	Max. Marks	Total Marks	Minimum Passing Marks*
DSC1-1	DCFSDC101T	Cyber Security	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-2	DCFSDC102T	Web Application Security	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-3	DCFSDC103T	Cyber Law & Practice in India	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-4	DCFSLB104P	Lab Course – I	2	-	1	4	4	-	-	-	-	50	50	20
DSE1-1	DCFSDE101T	Introduction to Digital Forensics	4	4	-	4	4	60	40	100	40	-	-	-
DSE1-1	DCFSDE102T	Regulation of Cyberspace	4	4	-	4	4	60	40	100	40	-	-	-
DSC2-1	DCFSRM101T	Research Methodology	4	4	-	4	4	60	40	100	40	-	-	-
		Total	**22**	20	1	24	24	300	200	**500**	-	50	**50**	-

Teaching and Examination Scheme – Semester II

DSC1-5	DCFSDC201T	Penetration Testing for Website	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-6	DCFSDC202T	Dark Web	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-7	DCFSDC203T	Intellectual Property Rights in Cyberspace	4	4	-	4	4	60	40	100	40	-	-	-
DSC1-8	DCFSLB204P	Lab Course – II	2	-	1	4	4	-	-	-	-	50	50	20
DSE2-1	DCFSDE201T	Network and Security	4	4	-	4	4	60	40	100	40	-	-	-
DSE2-1	DCFSDE202T	Cyber Law: International Perspective and Future Challenges	4	4	-	4	4	60	40	100	40	-	-	-
OJT-1 / FP-1	DCFSOJ201P / DCFSFP201P	On Job Training / Field Project	4	-	1	8	8	-	-	-	-	100	100	40
		Total	**22**	16	2	28	28	240	160	**400**	-	150	**150**	-

*Candidates shall pass separately in each head of assessment (i.e. Theory (External), Theory (Internal) and Practical examination) with minimum 40% marks.

SEMESTER – I

Mandatory		
Course DSC1-1: DCFSDC101T	**Course Title: Cyber Security**	
Course Credits: 4	**Total contact hours: 60 Hrs.**	
Course Objectives: 1. Understand Cyber Security Fundamentals 2. Analyze Attacker Techniques and Motivations 3. Examine Exploitation Techniques 4. Study Malicious Code and Defense Mechanisms 5. Develop Skills in Cyber Defense and Analysis		
Course Contents: Cyber Security Fundamentals; Attacker Techniques and Motivations; Exploitation; Malicious Code, Defense and Analysis Technique		**Reqd. Hrs.**
Unit I – Cyber Security Fundamentals		**15 Hrs.**
	Network and Security Concepts (Information Assurance Fundamentals, Basic Cryptography, Symmetric Encryption Public Key Encryption, The Domain Name System (DNS), Firewalls, Virtualization) Microsoft Windows Security Principles (Windows Tokens, Windows Program Execution the Windows Firewall)	
Unit II – Attacker Techniques and Motivations		**15 Hrs.**
	How Hackers Cover Their Tracks (Antiforensics): How and Why Attackers Use Proxies, Tunneling Techniques, Fraud Techniques, Rogue Antivirus, Click Fraud, Threat Infrastructure:	
Unit III – Exploitation		**15 Hrs.**
	Techniques to Gain a Foothold: Shellcode, Integer Overflow Vulnerabilities, Stack-Based Buffer Overflows, Format String Vulnerabilities, SQL Injection, Malicious PDF Files, Race Conditions, Web Exploit Tools, DoS Conditions Brute Force and Dictionary Attacks, Misdirection, Reconnaissance, and Disruption Methods	
Unit IV – Malicious Code, Defense and Analysis Technique		**15 Hrs.**
	Self-Replicating Malicious Code: Evading Detection and Elevating Privileges: Obfuscation, Virtual Machine Obfuscation, Persistent Software Techniques, Rootkits, Spyware, Attacks against Privileged User Accounts and Escalation of Privileges, Token Kidnapping, Stealing Information and Exploitation: Form Grabbing, Man-in-the-Middle	

	Attacks, DLL Injection, Browser Helper Objects Memory Forensics, Honeypots, Malicious Code Naming Automated Malicious Code Analysis Systems, Intrusion Detection Systems	

Course Outcomes – After completion of the course, the learner shall be able to,

1. Understand core network and security concepts, including cryptography, DNS, firewalls, and virtualization.
2. Comprehend Microsoft Windows security principles, such as tokens, program execution, and the Windows Firewall.
3. Analyze attacker techniques and motivations, including antiforensics, proxies, tunneling, and fraud techniques.
4. Explore exploitation techniques like shellcode, buffer overflows, SQL injection, web exploit tools, and DoS attacks.
5. Examine malicious code, defense, and analysis techniques, including evading detection, privilege escalation, memory forensics, and intrusion detection systems.

Suggested Readings:

1. Cyber Security Essentials
2. Cyber Security_ Analytics, Technology and Automation
3. The Basics of Cyber Warfare_ Understanding the Fundamentals of Cyber Warfare in Theory and Practice

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-1 (Major Mandatory)	Cyber Security	DCFSDC101T	4	16	40	24	60	2.5 Hrs.

Course DSC1-2: DCFSDC102T	Course Title: Web Application Security
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Understand Web Application Security Principles
2. Analyze Authentication and Authorization Mechanisms
3. Study Browser Security Principles
4. Examine Database and File Security
5. Apply Defense-in-Depth Strategies

Course Contents: Comprehensive Web Application Security: Principles, Threats, and Defense Strategies; Authentication and Authorization: Principles, Best Practices, and Session Management; Browser Security Principles: Same-Origin Policy, XSS, and CSRF; Database and File Security: Principles, Vulnerabilities, and Protection Strategies		**Reqd. Hrs.**
Unit I – Comprehensive Web Application Security: Principles, Threats, and Defense Strategies		**15 Hrs.**
	The Wide World of Web Application Security: Misplaced Priorities and the Need for a New Focus. Network Security versus Application Security: The Parable of the Wizard and the Magic Fruit Trees Real-World Parallels. Thinking like a Defender The OWASP Top Ten List. (Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Cross-Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards) Secure Features, Not Just Security Features	
	Security Fundamentals: Input Validation (Blacklist Validation, Whitelist Validation, More Validation Practices) The Defense-in-Depth Approach (Attack Surface Reduction: Attack Surface Reduction Rules of Thumb) Classifying and Prioritizing threats (STRIDE, IIMF, CIA, CWE, DREAD, CVSS)	
Unit II – Authentication and Authorization: Principles, Best Practices, and Session Management		**15 Hrs.**
	Authentication	

	Access Control Overview, Authentication Fundamentals (Proving Your Identity), Two-Factor and Three-Factor Authentication, Web Application Authentication (Password-Based Authentication Systems, Built-In HTTP Authentication, Single Sign-On Authentication, Custom Authentication Systems, Validating Credentials) Securing Password-Based Authentication (Attacks Against Passwords, The Importance of Password Complexity, Password Best Practices) Secure Authentication Best Practices (When and Where to Perform Authentication, Securing Web Authentication Mechanisms)	
	Authorization Access Control Continued (Authorization, Session Management Authorization Fundamentals, Authorization Goals, Detailed Authorization Check Process, Types of Permissions Authorization Layers, Controls by Layer, Custom Authorization Mechanisms, Client-Side Attack, TOCTTOU Exploit, Web Authorization Best Practices, Attacks Against Authorization) Session Management Fundamentals (What is session, How to Manage Session State? Why Do We Need Session Management? Attacks Against Sessions, SSL and HTTPS, Jetty: Session Predictability in the Real World, Attacks Against Session State) Securing Web Application Session Management (Session Management Best Practices)	
Unit III – Browser Security Principles: Same-Origin Policy, XSS, and CSRF		**15 Hrs.**
	Browser Security Principles: The Same - Origin Policy Defining the Same-Origin Policy (An Important Distinction: Client-Side vs. Server-Side, A World Without the Same-Origin Policy) Exceptions to the Same-Origin Policy (HTML <script> Element JSON and JSONP, iframes and JavaScript document.domain, Adobe Flash Player Cross-Domain Policy File, Microsoft Silverlight, XML Http Request (Ajax) and Cross-Origin Resource Sharing, XDomainRequest) Final Thoughts on the Same-Origin Policy	
	Browser Security Principles: Cross - Site Scripting and Cross - Site Request Forgery	

	Cross-Site Scripting (Cross-Site Scripting Explained, Reflected XSS, POST-Based Reflected XSS, Stored XSS, Local XSS, Another Variation: HTML Injection, XSS Defense: Encoding Output, XSS Defense: Sanitizing Input, XSS Defense: Using a Reduced Markup Language, XSS Defense-in-Depth: HTTP Only, XSS Defense-in-Depth: Content Security Policy (CSP), Final Thoughts on Cross-Site Scripting) Cross-Site Request Forgery (Cross-Site Request Forgery Explained, TTP GET and the Concept of Safe Methods, Ineffective CSRF Defense: Relying on POST, Ineffective CSRF Defense: Checking the Referrer Header Ineffective CSRF Defense: URL Rewriting, Better CSRF Defense: Shared Secrets, Better CSRF Defense: Double-Submitted Cookies, Prevent XSS, Reauthentication, What Being "Logged In" Means, Final Thoughts on Cross-Site Request Forgery)	
Unit IV – Database and File Security: Principles, Vulnerabilities, and Protection Strategies		**15 Hrs.**
	Database Security Principles Structured Query Language (SQL) Injection (SQL Injection Effects and Confidentiality-Integrity-Availability the Dangers of Detailed Errors, Blind SQL Injection: No Errors Required, Solving the Problem: Validating Input, Regular Expressions, Solving the Problem: Escaping Input) Setting Database Permissions (Single Account Security, Separate Accounts for Separate Roles) Stored Procedure Security (The Stored-Procedures-Only Approach: Reducing Permissions Even Further, SQL Injection in Stored Procedures) Insecure Direct Object References (No Technical Knowledge Required, Insecure Direct Object References and Confidentiality-Integrity-Availability, Solving the Problem: Pre- or Post-Request Authorization Checks, Final Thoughts on Insecure Direct Object References)	
	File Security Principles Keeping Your Source Code Secret (Static Content and Dynamic Content, Revealing Source Code Interpreted versus Compiled Code, Backup File Leaks, Include-File Leaks, Keep Secrets Out of Static Files, Exposing Sensitive Functionality) Security Through Obscurity	

	Forceful Browsing (Forceful Browsing and Insecure Direct Object References, Directory Enumeration, Redirect Workflow Manipulation) Directory Traversal (etc/passwd, More Directory Traversal Vulnerabilities, Canonicalization)	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand web application security fundamentals, including key concepts, common threats, and best practices for securing web applications. 2. Learn authentication and authorization mechanisms to ensure secure user access and data protection. 3. Explore browser security principles, focusing on the same-origin policy, cross-site scripting (XSS), and cross-site request forgery (CSRF). 4. Examine database security principles, including techniques to protect data integrity, confidentiality, and availability. 5. Understand file security principles, including methods for securing file storage and access control.

Suggested Readings:

1. Web Application Security – A Beginner Guide by Bryan Sullivan, Vincent Liu.
2. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, Andrew Hoffman
3. Grokking Web Application Security, Malcolm McDonald

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-2 (Major Mandatory)	Web Application Security	DCFSDC102T	4	16	40	24	60	2.5 Hrs.

Course DSC1-3: DCFSDC103T	Course Title: Cyber Law & Practice in India
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To provide a comprehensive understanding of the legal framework governing information technology in India, with a focus on the Information Technology Act of 2000 and its subsequent amendments.
2. To explore the evolution, necessity, and key features of the Act, as well as the National Cyber Security Policy of 2013.
3. To cover the concepts of digital and electronic signatures, including their authentication, legal recognition, and the regulation of certifying authorities.
4. To gain insight into the offenses and penalties outlined in the Act and the procedures for adjudication.
5. To delve into the processes and challenges of cybercrime investigation in India, including the roles of various agencies, crime scene investigation procedures, and international collaboration in cybercrime cases.

Course Contents: General Introduction; Digital Signature and Electronic Signature; Offences and Penalties; Cybercrime Investigation		**Reqd. Hrs.**
Unit I – General Introduction		**15 Hrs.**
	• Evolution of the Information Technology Act 2000- Genesis and Necessity • Background and Legislative History of Information Technology Act, 2000 • Electronic Evidence and Electronic Signature under Bharatiya Sakshya Adhiniyam 2023 • Concept of E-Commerce, E-Governance and E-Contracts • Salient features of the Information Technology Act, 2000 • Important Definitions under Information Technology Act, 2000 • Information Technology (Amendment) Act, 2008 • National Cyber Security Policy, 2013	
Unit II – Digital Signature and Electronic Signature		**15 Hrs.**
	• Authentication of electronic record & electronic Signature • Legal recognition of electronic records & electronic signature • Secure electronic records and secure electronic signature	

	• Regulation of certifying authorities- Appointment and Functions of Controller and other officers • Appointment of Licensed Certifying Authorities • Power and procedure to issue electronic signature certificate	
Unit III – Offences and Penalties		**15 Hrs.**
	• Penalties, compensation and adjudication • Offences and penalties under Information Technology Act 2000 • Changes introduced by Information Technology (Amendment) Act 2008.	
Unit IV – Cybercrime Investigation		**15 Hrs.**
	• Agencies appointed for investigation of cybercrime in India • Indian Computer Emergency Response Team (**CERT-In**)- The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**CERT-In Rules**) • Reporting of Cybercrime- Filing of FIR with Cyber Police station • Guidelines for International Investigations- Budapest Convention on Cybercrime Mutual Legal Assistance Treaty (MLAT) & Letter Rogatory • Crime Scene Investigation-Search & Seizure • Steps in Crime scene investigation- a) Panchnama b) Chain of custody and Digital evidence collection form c) Preparation of charge sheet	

Course Outcomes – After completion of the course, the learner shall be able to,
1. To understand need, necessity and evolution of Information Technology Act 2000. 2. To learn about different types of cyber offences provided under Information Technology Act 2000. 3. To examine the role of various agencies of the criminal justice system in investigation of cyber offences. 4. To gain a comprehensive understanding of the regulatory framework under the Information Technology Act 2000. 5. To analyze legal implications of electronic signature.

Suggested Readings:

1. Dr. S. R. Myneni – "Information Technology Law", (2023).
2. Prashant Mali – "Cyber Law and Cyber Crimes Simplified", (2018).
3. Dr. Chintan Pathak – "Landmark Judgments on Cyber Crimes and Cyber Laws".
4. K. M. Muralidharan – "Law of Crimes in India".
5. Talat Fatima – "Cyber Crimes", (2023).
6. Vakul Sharma – "Information Technology Law and Practice: Cyber Laws and Laws relating E-Commerce", (2023).
7. Information Technology Act, 2000.
8. Kamlesh N. and Murali D. Tiwari – "IT and Indian Legal System".
9. K. M. Murlidharan- Law of cybercrime in India (2023)
10. Pavan Duggal, Cyber Law- An exhaustive section wise Commentary on the Information Technology Act 3rd Edition (2023)
11. Santosh Kumar & Gagandeep Kaur- Cyber Crimes & Laws 3rd Edition (2024)
12. Relevant and Latest Case Laws.

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-3 (Major Mandatory)	Cyber Law & Practice in India	DCFSDC103T	4	16	40	24	60	2.5 Hrs.

Course DSC1-4: DCFSLB104P	Course Title: Lab Course – I
Course Credits: 2	**Total contact hours: 60 Hrs.**

Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)

1.	Checklist for reporting cybercrime at Cybercrime Police Station.
2.	Checklist for reporting cybercrime online.
3.	Reporting phishing emails.
4.	Demonstration of email phishing attack and preventive measures.
5.	Reporting and redressal mechanism for violations and misuse of social media platforms.
6.	Installation and configuration of Computer Host Firewall
7.	Wi-Fi security management in computer and mobile.
8.	Report Writing for High-Tech Investigations
9.	Configuring windows firewall.
10.	Configuring Iptables in Linux.
11.	Configuring Webserver and DVWA.
12.	Email tracing
13.	Using SQL injections using sqlmap
14.	Arp poisoning and identification
15.	Advanced google search
16.	Advanced bing search
17.	Advanced yahoo search
18.	Findmyhash
19.	OpenVas
20.	nikto

Learning objectives -After completion of the course, the learner shall be able to,

1. Develop comprehensive checklists for reporting cybercrimes at Cybercrime Police Stations and online, including steps for reporting phishing emails and the reporting and redressal mechanisms for violations and misuse of social media platforms.
2. Understand the demonstration of email phishing attacks and implement preventive measures to protect against such attacks.
3. Learn the installation, configuration, and management of computer host firewalls and Wi-Fi security for both computer and mobile devices.
4. Master report writing for high-tech investigations, including detailed procedures and

proper documentation.

5. Gain hands-on experience configuring security measures such as Windows Firewall, Linux iptables, web servers, and DVWA (Damn Vulnerable Web Application).
6. Acquire skills in email tracing, SQL injections using sqlmap, ARP poisoning, and identification techniques.
7. Enhance advanced search techniques using Google, Bing, and Yahoo, along with practical usage of security tools like Findmyhash, OpenVAS, and Nikto for comprehensive vulnerability assessments.

Suggested Readings:

1. Cyber Security Essentials
2. Cyber Security Analytics, Technology and Automation
3. The Basics of Cyber Warfare - Understanding the Fundamentals of Cyber Warfare in Theory and Practice
4. Web Application Security A Beginners Guide, Bryan Sullivan Vincent Liu
5. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, Andrew Hoffman
6. Grokking Web Application Security, Malcolm McDonald

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC1-4 (Major Mandatory)	Lab Course – I	DCFSLB104P	2	-	-	20	50	4 Hrs.

Electives (Any One)		
Course DSE1-1: DCFSDE101T	**Course Title: Introduction to Digital Forensics**	
Course Credits: 4	**Total contact hours: 60 Hrs.**	
Course Objectives 1. Understand Digital Forensics Fundamentals 2. Analyze OS-Specific Forensic Techniques 3. Investigate Application Data 4. Apply Investigative Techniques to E-mail and Social Media 5. Address Cloud Forensics Challenges		
Course Contents: Basics of Digital Forensics; OS Specific Investigation; Investigating applications; Investigative techniques		**Reqd. Hrs.**
Unit I – Basics of Digital Forensics		**15 Hrs.**
	Digital Investigation Foundation: Digital Investigation and Evidence, Digital Crime Scene Investigation Process, Data Analysis, Overview of Tool kits Volume Analysis: Introduction, Background, Analysis Basics File System Analysis: What is File System, File System Category, Content Category, Metadata Category, Filename Category, Application Category, Application-Level Search Techniques, Specific File Systems	
Unit II – OS Specific Investigation		**15 Hrs.**
	Working With Windows and CLi systems: Understanding File System, Exploring Microsoft Structure, Examining NTFS Disk, Understanding Registry, Startup tasks, Virtual Machines Event Logs, Prefetch Files, Shortcut files Examining Linux File structures, Using Linux Forensics Tools	
Unit III – Investigating applications		**15 Hrs.**
	What is application data? Where is application data stored? Web browsers, E-mail Clients, Instant Message	
Unit IV – Investigative techniques		**15 Hrs.**
	Exploring the Role of E-mail in Investigations, Exploring the Roles of the Client and Server in E-mail, Investigating E-mail Crimes and Violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Applying Digital Forensics Methods to Social Media Communications. CLOUD FORENSICS: An Overview of Cloud Computing, Legal Challenges in Cloud Forensics, Technical Challenges in Cloud Forensics, Acquisitions in	

	the Cloud, Conducting a Cloud Investigation, Tools for Cloud Forensics.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand the foundations of digital investigation, including the digital crime scene process, data analysis, and overview of forensic toolkits. 2. Learn volume and file system analysis, covering file system categories, application-level search techniques, and specific file systems. 3. Investigate OS-specific artifacts, including Windows and Linux file systems, registry, startup tasks, event logs, and forensic tools. 4. Explore application data, its storage locations, and investigation techniques for web browsers, email clients, and instant messaging. 5. Examine email and cloud forensics, including the role of email in investigations, cloud computing challenges, and specialized forensic tools and methods.

Suggested Readings:

1. File System Forensic Analysis, by Brian Carrier
2. Guide to Computer Forensics and Investigations 6th Edition, by Bill Nelson/Amelia Phillips/Christopher Steuart
3. Incident Response & Computer Forensics 3rd Edition, by Jason T. Luttgens, Matthew Pepe, Kevin Mandia

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Major Elective)	Introduction to Digital Forensics	DCFSDE101T	4	16	40	24	60	2.5 Hrs.

Course DSE1-1: DCFSDE102T	Course Title: Regulation of Cyberspace
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To provide a foundational understanding of cyberspace, its unique characteristics, and the legal challenges it presents.
2. To explore the differences between real space and cyberspace, along with the concept of digital identity.
3. To address various legal issues, including jurisdiction, privacy, and security concerns, while also examining contemporary technologies like AI, IoT, and blockchain.
4. To study the need for and methods of international regulation of cyberspace, with a focus on legal frameworks in different regions.
5. To cover data protection, emphasizing the importance of privacy and the international legal standards for safeguarding data in the digital realm.

Course Contents: General Introduction to Cyberspace; Legal Challenges of cyberspace; International Regulation of Cyberspace; Data Protection in Cyberspace		**Reqd. Hrs.**
Unit I – General Introduction to Cyberspace		**15 Hrs.**
	• Overview of Cyberspace- • Meaning and definition of cyberspace • Real space and cyberspace • Concept of Digital Identity in cyber world • Legal Assumptions in Cyber World (a) World Unbounded (b) Global Enforcement (c) Corporeal Property Unfounded (d) Virtual Relationship (e) Digital Records	
Unit II – Legal Challenges of cyberspace		**15 Hrs.**
	• **General Legal Issues in Cyberspace-** Domain Name Issues in cyberspace Jurisdiction Issues in cyberspace Data protection and Privacy issues in cyberspace Authentication issues in cyberspace State Behaviour in cyberspace	

	• **Contemporary Issues in Cyberspace-** 1. **Artificial Intelligence-** Deep fake attacks, AI phishing attacks, Denial of service (DoS) attacks, AI-powered ransom ware, Advanced persistent threats, Budapest Convention on Cybercrime, AI & International Humanitarian Law **Legal Challenges-** Ethical and Legal Responsibility, Complex Accountability, Autonomous Decision-making, Privacy and Data Protection, Cyber security and State Responsibility 2. **IOT (Internet of things)-** Overview of Concept of IoT, Application of IoT Issues - Internet walls, Cloud attacks, Botnet problems, Security issues **Legal Challenges-** Data protection, Data ownership, Security, Jurisdiction, Product liability & consumer protection, Formation & validity of e-contracts 3. **BIGDATA-** What is Big Data? Characteristics & application of BIGDATA **Legal challenge-** Compliance with data protection laws and regulations, data licensing issues, Intellectual property ownership and competition law issues 4. **Block chain & smart contract technology-** What is Block-chain Technology? **Legal Challenges-** Jurisdictional Issues, Regulatory Compliance, Privacy & Data protection, Intellectual Property, Determination of Liability, Enforceability of Smart Contract, Insurance Regulation, Jurisdictional challenges, Dispute Resolution, Decentralized Autonomous Organisations (DAOs) 5. **Crypto-currency-** History of Block Chain and Crypto-currency, Overview of the Most Common Crypto-currencies **Legal Challenges-** Anonymity of transacting parties, Problems related to lack of proper authority, Absence of well-defined Laws, Tax Evasion, Money laundering etc., phishing attacks, loss of data, Insecurity of trading & purchase platforms etc.	
Unit III – International Regulation of Cyberspace		**15 Hrs.**
	• Need of Regulation	

	• How Cyberspace can be Regulated • Legal and Self-Regulatory Framework • Filtering Devices and Rating Systems • Regulation of Internet Content • UNCITRAL Model Law • Global scenario- 1. United States- Communications Decency Act 1996(CDA), COPA, CIPA and Other Related Legislations 2. European Union- The Council of Europe's (CoE) Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law 2024	
Unit IV – Data Protection in Cyberspace		**15 Hrs.**
	• Concept of Data in cyberspace • Right to privacy and personal data in cyberspace • Need and necessity of data protection in cyberspace • International Legal framework of data protection- General Data Protection Regulations (GDPR), 2016 • Legal Framework for Regulation of Cyberspace Content in India- Digital Personal Data Protection Act, 2023.	

Course Outcomes – After completion of the course, the learner shall be able to,
1. To understand the meaning and nature of cyberspace. 2. To study the difference between Real Space and Cyberspace. 3. To analyze contemporary legal challenges in Cyber World. 4. To examine the International legal framework available for regulation of cyberspace. 5. To study legal implications of data protection in cyberspace.

Suggested Readings:

1. Rodney D Ryder- Guide to Cyber Laws 3rd Edition (2007)
2. Janine Kremling, Amanda M. Sharp Parker- Cyberspace, Cybersecurity, and Cybercrime
3. David Skillicorn- C*yberspace, Data Analytics, and Policing* (2022)
4. Evon Abu-Taieh, Issam H. Al Hadid, Abdelkrim El Mouatasim- Cyberspace (2020)
5. Krishan Kumar Goyal, Amit Garg, Saurabh Singhal- Cyber Security & Data Privacy (2021)
6. Alan Davidson- Privacy and data protection in cyberspace, The Law of Electronic

Commerce by Cambridge University press (2009)

7. Duggal Pawan, Mobile Law, Universal Law Publishing Co. Pvt. Ltd. 2nd Edition

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-1 (Elective)	Regulation of Cyberspace	DCFSDE102T	4	16	40	24	60	2.5 Hrs.

Minor	
Course DSC2-1: DCFSRM101T	**Course Title: Research Methodology**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To understand research and its significance
2. To learn research design and formulation of hypothesis
3. To learn data sampling and data collection techniques
4. To learn various statistical tools involved in analyzing data
5. To understand data interpretation and various types of scientific report writing
6. To understand various tools available for data discovering and management
7. To understand the ethics in scientific publishing

Course Contents: Introduction to Research and Research Methodology; Hypothesis, Sampling and Acquisition of Data; Processing and Interpretation of Data; Report Writing		**Reqd. Hrs.**
Unit I – Introduction to Research and Research Methodology		**15 Hrs.**
	Research-Definition and Objectives Types of Research Research Design: Definition, need and types of research design Literature review process	
Unit II – Hypothesis, Sampling and Acquisition of Data		**15 Hrs.**
	Types of Hypotheses Formulation of Hypothesis and Hypothesis Testing Sampling procedure and different types of sampling methods Types of data and collection methods	
Unit III – Processing and Interpretation of Data		**15 Hrs.**
	Various statistical tools used for data analysis Tabulation and Graphical representation of data Interpretation of data	
Unit IV – Report Writing		**15 Hrs.**
	Types of scientific reports Various search tools and Reference management software's used in scientific research Steps involved in scientific writing Ethics in scientific publishing	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Cultivate scientific and research temper 2. Formulate hypothesis and design research plan 3. Collect data and apply various statistical tools to test hypothesis 4. Interpret data and based on it write scientific reports 5. Apply various tools for data discovering and management 6. Apply ethics in scientific writing

Suggested Readings:

1. Kothari, C. R. (2004). Research Methodology: Methods and Techniques. India: New Age International (P) Limited.
2. Baykoucheva, S. (2015). Managing Scientific Information and Research Data. United Kingdom: Elsevier Science.
3. D. K. Bhattacharyya (2006), Research Methodology. India: Excel Books.
4. Thomas, C. G. (2021). Research Methodology and Scientific Writing. Germany: Springer International Publishing.
5. Nagar P (2021), Research Methodology Made Easy: A Handbook on Research Methodology. India. Exceller Books.
6. Kumar, R. (2010). Research Methodology: A Step-by-Step Guide for Beginners. United Kingdom: SAGE Publications.
7. Körner, A. M. (2008). Guide to Publishing a Scientific Paper. United Kingdom: Taylor & Francis.
8. Ellison, C. (2010). McGraw-Hill's Concise Guide to Writing Research Papers. United Kingdom: McGraw-Hill Education.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSC2-1 (Minor)	Research Methodology	DCFSRM101T	4	16	40	24	60	2.5 Hrs.

SEMESTER – II

Mandatory	
Course DSC1-5: DCFSDC201T	**Course Title: Penetration Testing for Website**
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Understand Penetration Testing Methodologies.
2. Analyze Web Application Security Fundamentals.
3. Implement Attack Simulation Techniques.
4. Document and Present Security Findings.
5. Apply Remediation Strategies and Best Practices.

Course Contents: Penetration Testing and Security in Web Applications: Concepts and Methodologies; Web Application Security: Discovery, Fingerprinting, and Vulnerability Analysis; Simulating Web Server and Application Attacks: Techniques, Tools, & Testing; Reporting & Remediation in Web Security: Documentation, Presentation, and Best Practices		**Reqd. Hrs.**
Unit I – Penetration Testing and Security in Web Applications: Concepts and Methodologies		**15 Hrs.**
	Penetration Testing Web Applications: The Case for Pen Testing, The Mindset, The Goal, Methodology, The Business. Web Applications--Some Basics: Application Aspects, Data Aspects, Emerging Web Application Models.	
Unit II – Web Application Security: Discovery, Fingerprinting, and Vulnerability Analysis		**15 Hrs.**
	Discovery: Logistics, OS Fingerprinting, Web Server Fingerprinting, Application Fingerprinting, Information Harvesting, Web Services. Vulnerability Analysis: OWASP and the Top Ten Threats, WASC, A1--Unvalidated Input, A2--Broken Access Control, A3--Broken Authentication and Session Management, A4--Cross-Site Scripting (XSS) Flaws, A5--Buffer Overflows, A6--Injection Flaws, A7--Improper Error Handling, A8--Insecure Storage, A9--Denial of Service (DoS), A10--Insecure Configuration Management, Other Areas.	
Unit III – Simulating Web Server and Application Attacks: Techniques, Tools, and Testing		**15 Hrs.**
	Attack Simulation Techniques and Tools--Web Server: Identifying Threats, Tools, Commercial Tools.	

	Attack Simulation Techniques and Tools--Web Application: The App Checklist, Manual Testing, Automated Testing, Commercial Tools.	
Unit IV – Reporting and Remediation in Web Security: Documentation, Presentation, and Best Practices		**15 Hrs.**
	Documentation and Presentation: Results Verification, Document Structure, Presentation Techniques. Remediation: Edge-Level Protection, Some Best Practices, Code Audit	

Course Outcomes – After completion of the course, the learner shall be able to,

1. Understand the fundamentals of penetration testing for web applications, including the rationale, mindset, goals, methodology, and business aspects of pen testing.
2. Learn discovery techniques for identifying web application components, including logistics, OS, web server, and application fingerprinting, as well as information harvesting and web services.
3. Analyze web application vulnerabilities, focusing on OWASP's Top Ten Threats, including unvalidated input, broken access control, authentication and session management flaws, XSS, buffer overflows, injection flaws, error handling, insecure storage, DoS, and insecure configuration management.
4. Explore attack simulation techniques and tools for both web servers and web applications, including threat identification, manual and automated testing, and the use of commercial tools.
5. Develop skills in documentation and presentation of penetration testing results, including verification, document structure, presentation techniques, and remediation best practices such as edge-level protection and code audits.

Suggested Readings:

1. Professional Pen Testing for Web Applications, by Andres Andreu
2. The Basics of Hacking and Penetration Testing, by Dr. Patrick Engebretson

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-5 (Major Mandatory)	Penetration Testing for Website	DCFSDC201T	4	16	40	24	60	2.5 Hrs.

Course DSC1-6: DCFSDC202T	Course Title: Dark Web
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. Understand the Dark Web and Cybersecurity Context
2. Explore and Analyze the Tor Network.
3. Investigating Malware and Its Criminal Implications.
4. Examine Cybercriminal Activities and Evolution of the Web.
5. Apply Techniques for Dark Web Investigation and Forensics.

Course Contents: Introduction; Working with Dark web; Activities in Dark web; Investigation		**Reqd. Hrs.**
Unit I – Introduction		**15 Hrs.**
	Introduction to Cybersecurity & Dark Web: Introduction, Cybersecurity and Cybercrime, Cybersecurity, Cybercrime, Web and Its Levels, Web Levels, Dark Net, Malicious Activities in the Dark Web, Malware Analysis, The Dark Web in the Context of Emerging Crime Threats. Threat Landscape in Dark Net: Emerging Crime Threats in Dark Net, Dark Net Black Markets, Illegal Goods and Services Offered on the Dark Net.	
Unit II – Working with Dark web		**15 Hrs.**
	Malicious Dark Net - Tor Network: Introduction to Tor, Usage, Working Pattern of Tor Challenges of the Tor Network, Deep Web and Tor, Tor's Hidden Services, The Users of Tor. Malware: Introduction, Learning Outcomes, Classification of Malware, Criminal Business Model of Malware, Malware Analysis, Malware Detection Techniques.	
Unit III – Activities in Dark web		**15 Hrs.**
	Cybercriminal Activities in Dark Net: Introduction, Cybercrime and Its Categories, Cybercriminal Activities through the Dark Net, Data Exfiltration, Monetization of Cybercrime, Malware-as-a-Service and Money Laundering. Evolution of the Web & its hidden Data: Introduction, Terminologies and Explanations Origins of the Internet, Internet Characteristics, Evolution of the Hidden Web, Deep Web Information Retrieval Process.	

Unit IV – Investigation		15 Hrs.
	Dark Web Content Analyzing Techniques: Introduction, Surface Web versus Deep Web Traditional Web Crawlers Mechanism, Surfacing Deep Web Content, Analysis of Deep Web Sites. Dark Web Forensics: Introduction, Introduction to Forensics, Crypto Market and Cryptocurrencies in the Dark Web, Forensic Investigation Scope and Models, Forensic Toolkit, Anti-Forensics Analysis. Open-Source Intelligence: Introduction, What Is Open-Source Intelligence? Open-Source Intelligence Monitoring Tools, Data Gathering, Summary of the Chapter	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Comprehensive Understanding of Dark Web Dynamics 2. Proficiency in Tor Network Operation 3. Expertise in Malware Analysis and Detection 4. Insight into Cybercriminal Activities and Web Evolution 5. Competence in Dark Web Forensics and Open-Source Intelligence.

Suggested Readings:

1. Dark Web Investigation
2. Inside the Dark Web, Erdal Ozkaya and Rafiqul Islam
3. Tor and the deep web

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-6 (Major Mandatory)	Dark Web	DCFSDC202T	4	16	40	24	60	2.5 Hrs.

Course DSC1-7: DCFSDC203T	Course Title: Intellectual Property Rights in Cyberspace
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives:

1. To introduce students to the fundamental concepts of Intellectual Property Rights (IPR) and their significance in both traditional and digital contexts.
2. To explore the various types of intellectual property, including copyrights, patents, trademarks, and trade secrets, and understand their role in protecting innovation and creativity.
3. To provide an overview of the international intellectual property regime, focusing on key organizations like WIPO and agreements such as TRIPS.
4. In the context of cyberspace, to examine the unique challenges posed by copyright issues, including the rights associated with digital content and the complexities of enforcement.
5. To study the impact of cyberspace on trademarks and patents, addressing topics such as domain name disputes, cybersquatting, and the legal implications of online trademark use.

Course Contents: Introduction to Intellectual Property Rights; International Intellectual Property Regime; Copyright issue in cyber space; Trademarks and Patents in Cyberspace	**Reqd. Hrs.**
Unit I – Introduction to Intellectual Property Rights	**15 Hrs.**
• Meaning of property • Origin, Nature, Meaning of Intellectual Property Rights • Concept of Property vis-à-vis Intellectual Property • Kinds of Intellectual property rights- Copy Right, Patent, Trademark, Trade Secret and trade dress, Design, Layout Design, Geographical Indication, Plant Varieties and Traditional Knowledge • Intellectual Property Rights as Human Right	
Unit II – International Intellectual Property Regime	**15 Hrs.**
• World Intellectual Property Organisation (WIPO) • Functions of WIPO • WTO & GATT Agreement • Major Conventions on IP – Berne Convention – Paris Convention – TRIPS agreement	

	• ICANN • UDRP	
Unit III – Copyright issue in cyberspace		**15 Hrs.**
	• Copyright in Digital medium, Copyright in digital goods, Upload of content, transmission of content, Access of content, Use of content, Copyright in joint works. • Copyright as a bundle of rights, Right of Reproduction, Public performance and Display rights, Distribution Rights, Derivative Works • Software – Copyrights vs. Patents debate • Copyright issues- Authorship and Assignment Issues • Commissioned Work and Work for Hire • Idea/Expression dichotomy • Jurisdiction Issues in copyright • Copyright Infringement in cyberspace and Remedies	
Unit IV – Trademarks and Patents in Cyberspace		**15 Hrs.**
	• Types of Marks, Concurrent use in cyberspace, Trademark and unfair competition in cyberspace, Online Infringement. • Internet Domain Names: What is domain name, registering a domain name, Domain name and the legal system, Domain name disputes, Domain Names Dispute Resolution Policies (UDRP), the NSI plan, proposed Domain Name System, ICANN Policy. • Cybersquatting & Typo squatting, protest Website. • Linking: Type of linking, Liability for hyper linking, Legal implications. • Framing: Application to Copyright and Trademark law, Legal issues. • Metatags: Metatags and Key word dispute, legal issues. • Selling of trademark	

Course Outcomes – After completion of the course, the learner shall be able to,
1. To understand the basic concepts relating to Intellectual Property Rights. 2. To explore international organizations working in the field of Intellectual Property Rights. 3. To evaluate the historical development and evolution of copyright protection for computer software.

4. To analyze the types of trademark infringement and dilution that occur in cyberspace.
5. To explore trademark issues related to e-commerce, online branding, and digital marketing strategies.
6. To explore domain name disputes and the procedures for resolving them under the Uniform Domain Name Dispute-Resolution Policy (UDRP)

Suggested Readings:

1. S.R Myneni- Intellectual Property Rights In Information Technology (Cyber Space) First Edition (2021)
2. Subhasis Saha- Challenges to Intellectual Property Rights in cyberspace (2012)
3. Sanchi Gupta- Interface between cybercrime and Intellectual Property Rights
4. Akash Kamal Mishra- Intellectual Property Rights in cyberspace (2020)
5. Prof (Dr) Tabrez Ahmad, Prof (Dr) Azimkhan B Pathan and Dr Gagandeep Kaur- Emerging dimensions of Cyber Law and IPR Issues & Challenges in 21st Century (2022)
6. G Peter Albert- Intellectual Property Law in Cyberspace (1999)
7. P. Narayanan – "Intellectual Property Law", (2023)
8. V K Unni- Trademarks and the emerging concepts of Cyber property rights (2002)
9. Dr. S. R. Myneni – "Information Technology Law", (2023).
10. Relevant and Latest Case Laws.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE1-7 (Major Mandatory)	Intellectual Property Rights in Cyberspace	DCFSDC203T	4	16	40	24	60	2.5 Hrs.

Course DSC1-8: DCFSLB204P	Course Title: Lab Course – II
Course Credits: 2	**Total contact hours: 60 Hrs.**

Course Contents: (Provide 18-20 experiments, minimum 12 experiments to be conducted)

1.	Information gathering about domain.
2.	Nmap.
3.	fing
4.	Vulnerability scanning using Nessus
5.	Vulnerability Scanning with Armitage
6.	Metasploit
7.	Social Engineering toolkit
8.	Netcat.
9.	Socat.
10.	Aircrack
11.	Using Kismet
12.	Using BurpSuite
13.	OWASP ZAP
14.	Using WebGoat
15.	John the ripper
16.	Live OS for password bypass
17.	Using wareshark
18.	Tcpdump

Learning objectives -After completion of the course, the learner shall be able to,

1. Acquire skills in information gathering about domains using tools like Nmap and Fing for network scanning and reconnaissance.
2. Conduct vulnerability scanning using Nessus and Armitage to identify security weaknesses, and leverage Metasploit for penetration testing.
3. Utilize advanced penetration testing tools such as the Social Engineering Toolkit, Netcat, Socat, Aircrack, and Kismet for various attack simulations and network security assessments.
4. Employ web application security tools like BurpSuite, OWASP ZAP, and WebGoat to identify and exploit web vulnerabilities.

5. Implement password cracking techniques using tools like John the Ripper, live operating systems for password bypass, and packet analysis with Wireshark and Tcpdump for network traffic monitoring and analysis

Suggested Readings:

1. Professional Pen Testing for Web Applications, by Andres Andreu
2. The Basics of Hacking and Penetration Testing, by Dr. Patrick Engebretson
3. Dark Web Investigation
4. Inside the Dark Web, Erdal Ozkaya and Rafiqul Islam
5. Tor and the deep web

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
DSC1-8 (Major Mandatory)	Lab Course – II	DCFSLB204P	2	-	-	20	50	4 Hrs.

Electives (Any One)		
Course DSE2-1: DCFSDE201T	**Course Title: Network and Security**	
Course Credits: 4	**Total contact hours: 60 Hrs.**	
Course Objectives: 1. Comprehend Network Security Fundamentals 2. Analyze Network Attacks and Countermeasures. 3. Utilize Advanced Network Exploitation Tools and Techniques. 4. Explore Wireless Security Threats and Techniques. 5. Develop Network Security and Penetration Testing Skills.		
Course Contents: Introduction to Network Security; Network Attacks Part 1; Advanced Network Exploitation and Security Assessment Techniques; Comprehensive Wireless Security: Threats, Attacks, and Countermeasures		**Reqd. Hrs.**
Unit I – Introduction to Network Security		**15 Hrs.**
	Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP/IP Model, TCP Vs. UDP, Routers, Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based) and setup.	
Unit II – Network Attacks Part 1		**15 Hrs.**
	Sniffing concepts, Sniffing Techniques: MAC Attack, DHCP attack, ARP poisoning, Spoofing, DNS poisoning. Wireshark, packet analysis, display and capture filters, Ettercap, sniffing counter measures, sniffing protection tools. Denial of service (DOS)/Distributed Denial of service (DDOS): Concepts, DOS/DDOS Technique, Botnets, DDOS, DOS/DDOS attacking tools, DOS/DDOS counter Measures, DOS/DDOS protection tools. Vulnerability scanning tools: Concepts, Scanning Techniques, Tools: Nessus, OpenVAS, Sparta, Nexpose, Nmap. Network Scanning Report Generation,	

	Striping, Router attacks, VPN pentesting, VOIP pentesting, Enumeration techniques: SMTP, SNMP, IPsec, VOIP, RPC, Telnet, FTP, TFTP, SMP, IPV6 and BGP.	
Unit III – Advanced Network Exploitation and Security Assessment Techniques		**15 Hrs.**
	Network Exploitation OS Detection in network, Scanning: Nmap, open ports, filtered ports, service detection, Metasploit framework, interface of Metasploit framework, network vulnerability assessment, evade anti viruses and firewalls, Metasploit scripting, exploits, vulnerabilities, payloads, custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploits delivery, burp-suite, End Point Security.	
Unit IV – Comprehensive Wireless Security: Threats, Attacks, and Countermeasures		**15 Hrs.**
	Wireless concept, wireless encryption, wireless threats, wireless hacking methodology, wireless hacking and security tools, Bluetooth hacking, countermeasures to wireless threats, Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentications, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework	

Course Outcomes – After completion of the course, the learner shall be able to,
1. Understand network security fundamentals, including types of networks, IP addressing, subnets, DHCP, ports, DNS, proxy servers, VPNs, OSI and TCP/IP models, networking devices, and various network layer attacks and defenses like firewalls, IDS, and IPS. 2. Learn about different network attacks, including sniffing, spoofing, ARP poisoning, DNS poisoning, DoS/DDoS attacks, and the use of tools like Wireshark, Ettercap, Nessus, OpenVAS, and Nmap, as well as countermeasures and protection tools. 3. Explore network exploitation techniques, including OS detection, network scanning, the use of Metasploit framework, network vulnerability assessment, evading security measures, and the use of tools like Burp Suite and the Social Engineering Toolkit. 4. Examine wireless network security, including wireless encryption, threats, hacking methodologies, Bluetooth hacking, countermeasures, various attacks on WEP, WPA, WPA2, and the use of tools for wireless security and exploitation.

Suggested Readings:

1. Computer Networks by Tanenbaum; Prentice Hall of India, New Delhi
2. Data Communications and Networking by Forouzan, (Edition 2nd and 4th); Tata McGraw Hill Education Pvt Ltd , New Delhi
3. Data and Computer Communication by William Stallings; Pearson Education, New Delhi
4. Information Security: The Complete Reference, Second Edition by Mark Rhodes-Ousley
5. Principles of Information Security by Whitman
6. Cryptography and Network Security: Principles and Practice by William Stallings
7. Cryptography Theory & Practice by Douglas Stinson
8. Understanding Cryptography: A Textbook for Students and Practitioners by Paar
9. Information Security by Pankaj Sharma
10. Charles P. Pfleeger, Shari Lawerance Pfleeger, "Analyzing Computer Security"
11. V.K. Pachghare, "Cryptography and information Security".

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE2-1 (Major Elective)	Network and Security	DCFSDE201T	4	16	40	24	60	2.5 Hrs.

Course DSE2-1: DCFSDE202T	Course Title: Cyber Law: International Perspective and Future Challenges
Course Credits: 4	**Total contact hours: 60 Hrs.**

Course Objectives

1. Understand Foundations of International Law and Cyber Legislation
2. Analyze Global Frameworks for Human Rights and Cybersecurity.
3. Evaluating Legal Challenges in Cryptocurrency and Digital Finance.
4. Assessing Legal and Ethical Issues in Social Media and Data Privacy.
5. Develop Insights into Emerging Cyber Legal Issues.

Course Contents: Foundations of International Law and Cyber Legislation; Global Frameworks for Human Rights, Trade, and Cybersecurity; Cryptocurrency, Blockchain, and Legal Challenges in Digital Finance and Gaming; Legal and Ethical Dimensions of Social Media, Data Privacy, and Artificial Intelligence		**Reqd. Hrs.**
Unit I – Foundations of International Law and Cyber Legislation		**15 Hrs.**
	International Law: Meaning, Definition and Concept. Sources of International Law. State, Sovereignty and Jurisdiction. International Bodies: United Nations, UNGA and ICJ. Reciprocal Arrangements and Investigations of Cyber Crimes. Human Rights and Cyber Laws.	
Unit II – Global Frameworks for Human Rights, Trade, and Cybersecurity		**15 Hrs.**
	International Conventions on Human Rights: UDHR, ICCPR, ICESCR, ICERD, CEDAW, CRC and CRPD, etc. UDRP Dispute Resolution Policy. UNCITRAL Model of Law. WTO and TRIPS. WIPO Treaties. Budapest Convention on Cybercrime. Cyber Crimes and Legal Framework in other Countries	
Unit III – Cryptocurrency, Blockchain, and Legal Challenges in Digital Finance and Gaming		**15 Hrs.**
	Concept of Cryptocurrency. Internet and Mobile Association of India Vs. Reserve Bank of India:	

	Recognition of Cryptocurrency in India? E-Rupee: Block Chain and Currency. Block Chain Technology and Governing Law: Paradox? Online Gaming, related Cyber Crimes and Need for Legislation Governing Online Gaming.	
Unit IV – Legal and Ethical Dimensions of Social Media, Data Privacy, and Artificial Intelligence		**15 Hrs.**
	Social Media Applications and E-Contracts. Misuse of Social Media and Cyber Crimes. Social Media and Data Privacy. Facebook – Cambridge Analytica Data Breach: A Case Study. Framework Convention on Artificial Intelligence & Human Rights, Democracy and Rule of Law: Treaty by Council of Europe *vis-à-vis* European Union Artificial Intelligence Act.	

Course Outcomes – After completion of the course, the learner shall be able to,

1. Understand the intersection of cyber law with international law and human rights, including concepts, sources of international law, state sovereignty, jurisdiction, and the role of international bodies like the UN, UNGA, and ICJ, as well as reciprocal arrangements for cybercrime investigations.
2. Explore international conventions and legal frameworks relevant to cyber law, including human rights treaties (UDHR, ICCPR, ICESCR, etc.), UDRP Dispute Resolution Policy, UNCITRAL Model Law, WTO and TRIPS, WIPO treaties, the Budapest Convention on Cybercrime, and cybercrime laws in various countries.
3. Learn about cryptocurrency, blockchain technology, and their related laws, including the concept of cryptocurrency, legal recognition in India (Internet and Mobile Association of India vs. RBI), E-Rupee, the paradox of blockchain governing law, and the cybercrimes and legal needs related to online gaming.
4. Examine social media, mobile applications, and related laws, including e-contracts, misuse of social media, data privacy issues, case studies like the Facebook-Cambridge Analytica data breach, and the global perspective on AI challenges through frameworks like the Council of Europe's Framework Convention on AI and the European Union AI Act

Suggested Readings:

1. S. K. Kapoor – "International Law and Human Rights".
2. V. K. Ahuja – "Public International Law", (2023).
3. Dr. S. R. Myneni – "Information Technology Law", (2023).
4. Dr. Keval Ukey – "Cyber Forensics, a legal perspective of Data Protection and E-Commerce".
5. Convention on Artificial Intelligence & Human Rights, Democracy and Rule of Law: Treaty by Council of Europe vis-à-vis European Union Artificial Intelligence Act.
6. Relevant and Latest Case Laws.

Course Type	**Course Name**	**Course Code**	**Course Credit**	**Assessment**				**Duration of Exam**
				Internal Marks		**External Marks**		
				(Min.)	**(Max.)**	**(Min.)**	**(Max.)**	
DSE2-1 (Major Elective)	Cyber Law: International Perspective and Future Challenges	DCFSDE202T	4	16	40	24	60	2.5 Hrs.

On Job Training	
Course OJT-1/ FP-1: DCFSOJ201P / DCFSFP201P	**Course Title: On Job Training / Field Project**
Course Credits: 4	**Total contact hours: 120 Hrs. (During Summer Vacation)**

Course Type	Course Name	Course Code	Course Credit	Assessment				Duration of Exam
				Internal Marks		External Marks		
				(Min.)	(Max.)	(Min.)	(Max.)	
OJT-1/ FP-1 (OJT/ FP)	On Job Training/ Field Project	DCFSOJ201P / DCFSFP201P	4	-	-	40	100	6 Hrs.