



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

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

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

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

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

University Campus,
Aurangabad-431 004.

REF.NO.SU/NEP/2023/10092-500

Date:- 16.08.2023.

*Deputy Registrar,
Academic Section*

Copy forwarded with compliments to :-

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

Copy to :-

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

BABASAHEB AMBEDKAR MARATHWADA UNIVERSITY, AURANGABAD



NAAC Reaccredited with 'A' Grade

Faculty of Science and Technology

2 Years P.G. Programme in Science (M.Sc.)

Subject: Forensic Cyber

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

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

Table of Contents

Preamble.....	3
Course Structure.....	3
Vision	4
Mission	4
Program Educational Objectives	4
Program Outcomes and Program-Specific Outcomes	5
Eligibility.....	6
Duration	6
Medium of Instruction.....	6
Attendance.....	6
Assessment Scheme/Scheme of Examination	6
Curriculum and Structure as per NEP 2020	8
Detailed Curriculum of Semester-I	12
Discipline-Specific Core Courses	12
Discipline-Specific Core Courses	24
Research Methodology	30
Detailed Curriculum of Semester-II.....	33
Discipline-Specific Core Courses	33
Discipline-Specific Elective Courses	44
On Job Training/ Field Project.....	50

Computer and computer-related crimes have increased tremendously in the last couple of years. Criminals are using various modus operandi to commit such crimes. Master's program in Forensic Cyber (Cyber Forensics) has been aimed to generate quality human resources for the field. Dr. Babasaheb Ambedkar Marathwada University, Aurangabad is committed to providing a comprehensive syllabus for PG programs in Forensic Cyber in line with the objectives and philosophies of National Education Policy 2020.

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

Faculty of Science & Technology

Year / level	Sem.	Major subject		RM	OJT /FP	RP	Credits	Degree
		DSC Core Mandatory	DSE (Elective)					
First year 6.0	I	3(4) +2=14	4	4			22	PG Diploma (After 3 years degree)
	II	3(4) +2=14	4		4 Complete during summer break		22	
Cum. Cr. For PG Diploma		28	08	4	4		44	
Exit option with Post-graduate Diploma (44 credits) after the first year or two semesters with completion of courses equivalent to 44 credits								
Second Year 6.5	III	3(4) +2= 14	4			4	22	PG Degree after 3 years UG or PG Degree after 4 years UG
	IV	3(4) =12	4			6	22	
Cum. Cr. For 1 year PG Degree		26	8			10	44	
Cum. Cr. For 2 years PG Degree		54	16	4	4	10	88	
2 Years -4 sem.PG Degree (88 credits) after three-year UG Degree or 1 Year -2 sem. PG Degree (44 credits) after four-year UG degree								

Abbreviations

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

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

OJT: On-Job Training: Internship/Apprenticeship

FP: Field Project

RP: Research Project

Vision

The vision of the curriculum is as follows:

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

Mission

The mission of the curriculum is as follows:

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

Program Educational Objectives

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

- **PEO1:** To develop scientific and technical competency among graduates leading to a successful career in digital forensics and allied disciplines
- **PEO2:** To develop analytical and problem-solving skills among students to solve complex issues/problems related to forensic analysis in crime investigation
- **PEO3:** To inculcate professionalism, ethics, teamwork, communication, and leadership quality in the students

- **PEO4:** To make the students responsive toward the environment and society
- **PEO5:** To inculcate the practices of lifelong learning in the direction to have a successful career and responsive citizen of the globe

Program Outcomes and Program-Specific Outcomes

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

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

PO1: Basic and Discipline-specific knowledge: Apply the knowledge of computer science and related discipline to various forensic computer-related crimes.

PO2: Problem Analysis: Identify and analyze crime and crime investigation issues using standard methods based on a scientific approach.

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

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

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

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

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

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

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

Program-Specific Outcomes (PSOs): Program Specific Outcomes are statements that describe what the graduates of a specific program should be able to do. The PSOs of the PG Program in Forensic Cyber are as follows:

- **PSO1:** Understand the basic and advanced techniques in various disciplines of forensic cyber.
- **PSO2:** Analyze the forensic samples using basic and state-of-the-art techniques of various disciplines of digital forensics.
- **PSO3:** Evaluate the results of various techniques and make decisions on simple or complex forensic problems.
- **PSO4:** Design and develop research-based solutions to complex forensic problems.

Eligibility

A candidate who has passed B.Sc. (three years) in science as a major from a recognized university with 45% marks will be eligible for getting admission to PG programs. Reservation policy and relaxation of marks will be as per the norms of the university and Government of Maharashtra.

Duration

As per the guidelines of the Government of Maharashtra and the university, the PG Program will be of two-year duration. However, the students need to pass the minimum credits within the four years from the date of admission. Re-entry to the program, if left in between, can be made within five years. Lateral entry and exit will be as per the guidelines issued by the university from time to time.

Medium of Instruction

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

Attendance

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

Assessment Scheme/Scheme of Examination

The assessment scheme is as follows:

- Each course has been assigned marks equivalent to 25 marks/credit. Thus, each theory course is 75/100 marks while the practical/Laboratory course is 25/50 marks. Moreover, research project shall be 100/150 while On-Job-Training shall be 100 marks.

- Continuous Internal assessment (CIA) will be for 40% while Semester End Examination (SEE) will be for 60%.
- It shall be mandatory for the students to pass individually for both SEE and CIA for each course to complete the program successfully.
- Passing percentage for both theory and practical shall be 40%.
- The CIA may be in terms of class tests, group, and individual assignments, and presentation. Two tests on completion of 40%, and 100% syllabus, each of 20 marks will be conducted and the average result will be reported. Presentation of 10 marks and assignments of 10 marks will also be conducted to get an aggregate of 40% weightage.
- Changes in examination scheme is possible as per the guidelines issued by the university from time to time.

Curriculum and Structure as per NEP 2020

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

Credit distribution and structure of two years/one-year program in Forensic Science with multiple entry and exit options

M.Sc. First Year (First Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Th	Pr	Th	Pr	
Major Mandatory DSC	FOC/MJ/500T	Forensic Science	3	-	3	-	14
	FOC/MJ/501T	Criminal Law and Information Risk Management	3		3	-	
	FOC/MJ/502T	Digital Forensics-I	3	-	3	-	
	FOC/MJ/500P	Practical based on FOC/MJ/500T	-	2	-	1	
	FOC/MJ/501P	Practical based on FOC/MJ/501T	-	2	-	1	
	FOC/MJ/502P	Practical based on FOC/MJ/502T	-	2	-	1	
	FOC/MJ/503	Skill/Practical based activity	-	4	-	2	
DSE (Choose anyone from the courses: Theory and Practical together make a complete course)	FOC/DSE/504T	Machine Learning	3	-	3	-	4
	FOC/DSE/504P	Practical based on FOC/DSE/504T	-	2	-	1	
	FOC/DSE/505T	Cloud Security	3	-	3	-	
	FOC/DSE/505P	Practical based on FOR/DSE/505T	-	2	-	1	
RM	FOC/RM/509	Research Methodology and Statistics	4	-	4	-	4
			16	12	16	06	22

41-51

M.Sc. First Year (Second Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Th	Pr	Th	Pr	
Major Mandatory DSC	FOC/MJ/550T	Forensic Application Development and Networking	3	-	3	-	14
	FOC/MJ/551T	Threats to Web Infrastructure, its Defense and Resilience	3	-	3	-	
	FOC/MJ/552T	Digital Forensics-II	3	-	3	-	
	FOC/MJ/550P	Practical based on FOC/MJ/550T	-	2	-	1	
	FOC/MJ/551P	Practical based on FOC/MJ/551T	-	2	-	1	
	FOC/MJ/552P	Practical based on FOC/MJ/552T	-	2	-	1	
	FOC/MJ/553	Skill/Practical based activity	-	4	-	2	
DSE (Choose anyone from the courses: Theory and Practical together makes a complete course)	FOC/DSE/554T	Multimedia Forensics	3	-	3	-	4
	FOC/DSE/554P	Practical based on FOC/DSE/554T	-	2	-	1	
	FOC/DSE/555T	Web Science	3	-	3	-	
	FOC/DSE/555P	Practical based on FOC/DSE/555T	-	2	-	1	
OJT/FP	FOR/OJT/599	OJT/FP	-	8	-	4	4
			12	20	12	10	22

41-51

M.Sc. Second Year (Third Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Th	Pr	Th	Pr	
Major Mandatory DSC	FOC/MJ/600T	Malware Analysis	3	-	3	-	14
	FOC/MJ/601T	Network Security and Forensics	3	-	3	-	
	FOC/MJ/602T	Mobile Security and Forensics	3	-	3	-	
	FOC/MJ/600P	Practical based on FOC/MJ/600T	-	2	-	1	
	FOC/MJ/601P	Practical based on FOC/MJ/601T	-	2	-	1	
	FOC/MJ/602P	Practical based on FOC/MJ/602T	-	2	-	1	
	FOC/MJ/603	Skill/Practical based activity	-	4	-	2	
DSE (Choose anyone from the courses: Theory and Practical together make a complete course)	FOC/DSE/604T	Data Science	3	-	3	-	4
	FOC/DSE/604P	Practical based on FOC/DSE/604T	-	2	-	1	
	FOC/DSE/605T	Ethical Hacking	3	-	3	-	
	FOC/DSE/605P	Practical based on FOC/DSE/605T	-	2	-	1	
RP	FOC/RP/649	Research Project	-	8	-	4	4
			12	20	12	10	22

Uji-51

M.Sc. Second Year (Fourth Semester)

Course Type	Course Code	Course Name	Teaching Scheme (Hrs./week)		Credit Assigned		Total credits
			Th	Pr	Th	Pr	
Major Mandatory DSC	FOC/MJ/650T	Cloud Security and Forensics	3	-	3	-	12
	FOC/MJ/651T	IOT Security and Forensics	3	-	3	-	
	FOC/MJ/652T	Image Processing and Biometrics	3	-	3	-	
	FOC/MJ/650P	Practical based on FOC/MJ/650T	-	2	-	1	
	FOC/MJ/651P	Practical based on FOC/MJ/651T	-	2	-	1	
	FOC/MJ/652P	Practical based on FOC/MJ/652T	-	2	-	1	
DSE (Choose anyone from the courses: Theory and Practical together makes a complete course)	FOC/DSE/653T	Artificial Intelligence	3	-	3	-	4
	FOC/DSE/653P	Practical based on FOC/DSE/653T	-	2	-	1	
	FOC/DSE/654T	Block Chain Technology	3	-	3	-	
	FOC/DSE/654P	Practical based on FOC/DSE/654T	-	2	-	1	
RP	FOC/RP/699	Research Project	-	12	-	6	6
			12	20	12	10	22

4+1-51

Detailed Curriculum of Semester-I

Discipline-Specific Core Courses

FOC/MJ/500T	Forensic Science	Credit:03	Contact Hours:45	Marks:75
-------------	------------------	-----------	------------------	----------

Course Objectives

1. To understand what is forensics.
2. To know the organization and function of forensic laboratory in India.
3. To analyze evidence and chain of custody.
4. To understand the role of medical examiners
5. To learn the concept of cyber forensics.

Course Outcomes

- **CO1:** To understand basics of forensic.
- **CO2:** To understand various types of forensic examination.
- **CO3:** To understand cyber forensic.
- **CO4:** To gain knowledge in details about forensics.

Unit	Content	Contact Hours
Unit-I	Basics of Forensic Science • Basic of Forensic Science: Introduction, Definition, need, signification and scope of Forensic Science. Principles of Forensic Science, multi professional and multi personal aspects of forensic science. Domains in Forensic Science: Forensic Biology, Forensic Medicine, Forensic Toxicology, Forensic Osteology and Odontology, Forensic Physics, Forensic Photography, Ballistics, Fingerprint, Questioned Documents, Forensic Psychology, Forensic Anthropology, Wildlife Forensic, DNA profiling, Computer Forensics etc.,	09 hours
Unit-II	Forensic Scientists and other related Personnel • Functions of Forensic Scientist, Police officers, Prosecution, Judicial Officers and Medico-legal experts etc. Problem of proof in Forensic Science, corpus	

	delicti, modus operandi. Ethical issue in Forensic Science: Definition of ethics, professional standards for the practice of Criminalistics, sanction against expert for unethical conduct.	
Unit-III	Crime scene investigation Definition of crime scene, crimes without scene. Classification of crime scene: indoor & outdoor, primary & secondary, macroscopic & microscopic crime scene. Significance of crime scene, argument and ethics of crime scene.	09 hours
Unit-IV	Physical Evidence Definition of physical evidence, classification of physical evidence, types of physical evidences, sources of physical evidence, signification and value of physical evidence, linkage between crime scene, victim and criminal, study of some special crime scene such as mass disaster, terror attack, geological scene and explosive etc.	09 hours
Unit-V	Introduction to Cyber Forensics Concept of cyber forensics, computer forensics and cyber-crime, cyber forensics and why it is important, the 5 steps in cyber forensics, objective of cyber forensics, benefits of cyber forensics, the different types of cyber forensics, difference between cyber-crime and cyber forensic, cyber-crime and its types in detail. Cyber forensics used.	09 hours

Suggested Readings

1. Henry Lee's Crime Scene Handbook: Henry C Lee
2. Computer Crime and Computer Forensic: Dr. R.K. Tiwari
3. Forensic Science in Criminal Investigation and Trial, 4th edn.: B.R. Sharma
4. Forensic Science: An Introduction to Scientific and Investigative Techniques 3rd ed. : Stuart H. James
5. Criminalistics: An Introduction to Forensic Science, 9th edn.: Richard Saferstein
6. Computer Crime and Computer Forensic: Dr. R.K. Tiwari
7. Criminal Profiling: An Introduction to a Behavioral Evidence Analysis, 3rd edn. : Brent E. Turvey
8. Forensic Science in Criminal Investigation and Trial, 4th edn.: B.R. Sharma
9. Handbook of Forensic Psychology: Dr. Veerraghavan

10. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
11. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal
12. Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
13. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by
14. Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
15. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
16. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
17. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
18. Fundamentals of Network Security by E. Maiwald, McGraw Hill

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

Course Overview

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

List of Practical (Students have to perform at least 10 practical)

1. Collection, preservation, handling, physical evidence method of different Crime
2. To compare physical evidence (Cloth, Thread)
3. Examination of Bomb Blast Scene
4. To compare and calculate diameter of given bangle piece
5. To collect and compare physical evidence of Hit and run crime scene Samples.
6. Collection and Handling of arson scene Samples
7. Packaging and forwarding of physical evidences.
8. Collection of special evidences.
9. Setting and configuring two factor authentication in the Mobile phone.
10. Security patch management and updates in Computer and Mobiles.
11. Managing Application permissions in Mobile phone.
12. Installation and configuration of computer Anti-virus.
13. Installation and configuration of Computer Host Firewall.
14. 7. Wi-Fi security management in computer and mobile.

FOC/MJ/501T	Cyber Law and Information Risk Management	Credit:03	Contact Hours:45	Marks:75
-------------	---	-----------	------------------	----------

Course Objectives

1. To learn Basics of Cyber Law.
2. To understand the Concept of Jurisdiction.
3. To understand the Copyrights
4. To understand the Legal Issues in Cyber Contracts
5. To understand the Trademarks in Internet

Course Outcomes

- **CO1:** To understand Cyber law (IT ACT 2000)
- **CO2:** To gain knowledge for intellectual property Law
- **CO3:** To gain knowledge for various types of IPR-Copyrights, Patent and trademark.
- **CO4:** To study overall cyber law, intellectual property law in this subject

Unit	Content	Contact Hour
Unit-I	Introduction Basics of Law, Understanding Cyber Space, Defining Cyber Laws, Scope and Jurisprudence, Concept of Jurisdiction, Cyber Jurisdiction, Overview of Indian Legal System, Introduction into IT Act 2000, Amendments in IT Act, Cyber Laws of EU- USA- Australia-Britain, other specific Cyber laws.	09 hours
Unit-II	IPR& Copyrights-I Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property Rights, Understanding Patents, Understanding Trademarks,	09 hours
Unit-III	IPR& Copyrights-II Trademarks in Internet, Domain name registration, Software Piracy, Legal Issues in Cyber Contracts, Authorship, Document Forgery. Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO,	09 hours
Unit-IV	IPR& Copyrights-III Copyrights, Jurisdiction Issues and Copyright Infringement, Multimedia and Copyright issues, WIPO, Intellectual Property	09 hours

	Rights, Understanding Patents, Understanding Trademarks, Trademarks in Internet, Domain name registration, Software Piracy, Legal Issues in Cyber Contracts, Authorship, Document Forgery.	
Unit-V	Cyber security Plan cyber security policy, cyber crises management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy.	09 hours

Suggested Readings

1. Information Security and Cyber Laws by Saurabh Sharma
2. Cyber frauds, cybercrimes & law in india by pavan duggal
3. The Internet Law of India : Indian Law Series by Shubham Sinha
4. CyberLaws-
IndianandInternationalPerspectivesonKeytopicsincludingDataSecurity,E-commerce, Cloud Computing and Cyber Crimes by Aparna Viswanathan
5. NIST-Computer Security Incident Handling Guide by Paul Cichonski, TomMillar, Tim, Grance, Karen Scarfone.
6. Good Practice Guide for Incident Management, ENISA
7. Handbook for Computer Security Incident Response Teams (CSIRTs) by Moira J. West-Brown, Don Stikvoort,Klaus-Peter,Kossakowski,GeorgiaKillcrece,RobinRuefle,MarkZajicek
8. Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response by Leighton Johnson
9. Incident Response & Computer Forensics, Third Edition by Jason T.Luttgens, Matthew Pepe, Kevin Mandia.
10. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
11. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
12. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
13. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram.
14. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.
15. Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning

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

Course Overview

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

List of Practical (Students have to perform at least 10 practical)

1. Prepare password policy for computer and mobile devices.
2. List out security controls for computers and implement technical security controls in the personal computer.
3. List out security controls for mobile phones and implement technical security controls in the personal mobile phone.
4. Log into the computer system as an administrator and check the security policies in the system.
5. Perform a case study on the status of the Examiner of Electronic Records in India
6. Perform a case study on the admissibility of electronic records compiling the various Supreme courts judgments
7. Perform a case study on e-governance policy in India
8. Perform a case study on the status of cyber infrastructure in India
9. Perform a comparative study of cyber laws of India and other countries
10. Perform a case study on the judgment on IT Act (Case can be taken from any of the Civil/High/Supreme Courts) (**minimum three different cyber offences**). While performing the study consider the following:
 - a. Nature of crime
 - b. Modus operandi
 - c. Mens rea
 - d. Factors that take the offender to commit the crime
 - e. Provisions of punishment under the law for that crime
 - f. The punishment given to the offender

FOC/MJ/502T	Digital Forensics-I	Credit:03	Contact Hours:45	Marks:75
--------------------	----------------------------	------------------	-------------------------	-----------------

Course Objectives

1. To study Locard's Principle of Exchange
2. To study Branches of Digital Forensics
3. To recover deleted data
4. To describe open-source analysis tools
5. To study EnCase

Course Outcomes

- **CO1:** To understand hardware and software as well as operating system, Setting up Digital Forensics Laboratory
- **CO2:** To understand digital evidence and data recovery Introduction to storage media.
- **CO3:** to gain knowledge, in File types and signature, Data Recovery and Carving tools.
- **CO4:** to Gain knowledge in Creating and managing cases using 7EnCase, FTK and Autopsy, Working with Time line, Keywords, Book marks and Reports.

Unit	Content	Contact Hours
Unit-I	Computer Forensics and Investigations Understanding Computer Forensics, Preparing for Computer Investigations, Taking A Systematic Approach, Procedure for Corporate High-Tech Investigations, Understanding Data Recovery Workstations and Software Office and Laboratory: Understanding Forensics Lab Certification Requirements Determining the Physical Requirements for a Computer, Forensics Lab Selecting a Basic Forensic Workstation	09 hours
Unit-II	Data Acquisition Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Contingency Planning for Image Acquisitions, Using Acquisition Tools, Validating Data Acquisition, Performing RAID Data Acquisition, Using Remote Network Acquisition Tools, Using Other Forensics Acquisition Tools	09 hours

Unit-III	Processing Crime and Incident Scenes Identifying Digital Evidence, Collecting the Evidence in Private-Sector Incident Scenes, Processing law Enforcement Crime Scenes, preparing for a Search, Securing a Computer Incident or Crime Scene, Seizing Digital evidence at the crime Scene, Storing Digital evidence, obtaining a Digital Hash, Current Computer Forensics Tools, Evaluating Computer Forensics Tool Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools.	09 hours
Unit-IV	Social Media Forensics: Case Studies Open-Source tools or social media analytics, Safety on social media. Legal Issues in world social media, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	09 hours
Unit-V	Validating and Testing Forensics Software Computer Forensics Analysis and Validation, Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, Performing Remote Acquisition, data carving, Recovering Graphics and Network Forensics, Recognizing a Graphics File, Understanding Data Compression, Locating and Recovering Graphics Files, live Memory forensics (RAM), Understanding Copyright Issues with Graphics, Network Forensic, social media forensics.	09 hours

Suggested Readings/Reference Books

1. Guide to computer forensics and Investigation: 3rd or 4th edition by Amelia Philips, Bill Nelson and Christopher Steuart.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons
3. Digital Forensics Workbook: Hands-on Activities in Digital Forensics by Michael K Robinson
4. Computer Forensics and Cyber Crime: An Introduction by MarjieT. Britz
5. Digital Forensics with Open-Source Tools by Cory Altheide, HarlanCarvey
6. ForensicComputing-A Practitioner's Guide by Tony Sammes, Brian Jenkinson

7. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher Steuart.
8. Handbook of Digital Forensics and Investigation by Eoghan Casey
9. Digital Forensics Explained by Greg Gogolin
10. File System Forensic Analysis by Brian Carrier
11. EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting
12. ComputerForensicsandDigitalInvestigationwithEnCaseForensicv7bySuzanneWidup
13. Computer Forensics with FTK by Fern and oCarbone
14. Digital Forensics with the Access Data Forensic Toolkit(FTK) by John Sammons
15. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management by Anton A. Chuvakin and Kevin J. Schmidt
16. Social Media Analytics: Effective Tools for Building, Interpreting, and Using Metrics
17. Social Network Analysis: Methods and Application by Katherine Faust and Stanley
18. Wasserman.
19. Understanding Social Networks: Theories, Concepts by Charles Kadushin
20. Social Media Data Extraction and Content Analysis by Shalin Hai-Jew

FOC/MJ/502P	Practical based on FOC/MJ/502T	Credit:01	Contact Hours:30	Marks:25
--------------------	---------------------------------------	------------------	-------------------------	-----------------

Course Overview

This is a laboratory course based on Digital Forensics-I (FOC/MJ/502T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical (Students have to perform at least 10 practical)

1. Create a forensic copy of the given device
2. Create disk image using FTK Imager
3. Create disk image using Encase Imager
4. Create disk image using Forensic Imager
5. Mining of Social Media Information using OSINT
6. Verify original and forensic copy using various hash algorithms
7. Cyber check suite and other forensic tools from CDAC
8. Forensic Imaging of Virtual Machines
9. Live Acquisition of system
10. Live Incident Response
11. Live Memory Forensics (Volatility framework)
12. Working with Scalpel, Autopsy
13. Working with Encase and FTK

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

Course Overview

The course has been designed to let the students acquire skills in his/her area of interest. As the aim of the course is to develop skills, the students can choose any one of the activities, which can be conducted under the guidance of a teacher.

List of activities

- Data recovery from various devices
- Social media mining using OSINT
- Validation and testing of forensic software
- Any other skill-based activities chosen by the students as per their interests

Discipline-Specific Core Courses

FOC/DSE/504T	Machine Learning	Credit:03	Contact Hours:45	Marks:75
---------------------	-------------------------	------------------	-------------------------	-----------------

Course Objectives

1. To Motivate and role of machine learning in computer science and problem solving
2. To appreciate the probability distributions
3. To analyze statistical data.
4. To understand fundamentals of ML.
5. To validate and test the data.

Course Outcomes

- **CO1:** To gain knowledge role of machine learning in computer science and problem solving.
- **CO2:** To understand probability distributions in the context of data, Prior probabilities and Bayes Rule.
- **CO3:** to study PCA and Dimensionality Reduction, KNN, Linear Regression.
- **CO4:** to obtain knowledge Kernels (with SVM), Bayesian Methods, Generative Methods, HMM, EM, PAC learning.

Unit	Content	Direct-teaching learning hours
Unit-I	Introduction to Machine Learning Motivation and role of Machine learning in computer Science and problem-solving Representation (features), linear transformations, Appreciate linear transformations and matrix-vector operations in the context of data and representation.	09 hours
Unit-II	Problem formulations classification and regression, the probability distributions in the context of data, Prior probabilities, and the Bayes Rule.	09 hours
Unit-III	Fundamentals of ML-I PCA and other Dimensionality Reduction techniques Nearest Neighbours and KNN. Linear Regression Decision Tree Classifiers	09 hours

Unit-IV	Fundamentals of ML-II Notion of Generalization and concern of Overfitting Notion of Training, Validation and Testing Connect to generalization and overfitting.	
Unit-V	Selected Algorithms Ensembling and RF, Linear SVM, K Means, Logistic Regression, Naive Bayes, Key Concepts from ML:Kernels (with SVM), Bayesian Methods, Generative Methods, HMM, EM, PAC learning	09 Hours

Suggested Readings

1. The Hundred-Page Machine Learning Book by Andriy Burkov
2. Machine Learning for Absolute Beginners by Oliver Theobald
3. Machine Learning for Hackers by Drew Conway and John Myles White
4. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow by Geron Aurelien

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

Course Overview

This is a laboratory course based on Machine Learning (FOC/DSE/504T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical (Students have to perform at least 10 practical)

1. Perform KNN classification on the given data
2. Perform PCA on the given data
3. Perform K means on the given data
4. Perform Linear regression on the given data
5. Perform Logistic regression on the given data
6. Perform decision tree classification on the given data
7. Perform Naïve Bayes classification on the given data
8. Perform SVM on the given data
9. Perform HMM modeling on the given data
10. Perform Random Forest classification on the given data
11. Apply the EM algorithm to the given data
12. Perform n-cross validation on the given data

FOC/DSE/505T	Cloud Security	Credit:03	Contact Hours:45	Marks:75
--------------	----------------	-----------	------------------	----------

Course Objectives

1. Understand what Cloud is computing
2. Architectural and Technological Influences of Cloud Computing
3. Cloud Computing Roles
4. Risks and Security Concerns

Course Outcomes

- **CO1:** To study Fundamentals of Cloud Computing.
- **CO2:** To understand Security Design and Architecture for Cloud Computing
- **CO3:** To learn Common attack vectors and threats.
- **CO4:** To gain knowledge Secure Isolation of Physical & Logical Infrastructure.

Unit	Content	Direct-teaching learning hours
Unit-I	Fundamentals of Cloud Computing Fundamentals of Cloud Computing and Architectural Characteristics: Understand what is Cloud computing Architectural and Technological Influences of Cloud Computing	09 hours
Unit-II	Cloud Deployment Model Understand the Cloud deployment models a. Public, Private, Community and Hybrid models • Scope of Control a. Software as a Service (SaaS) b. Platform as a Service (PaaS) c. Infrastructure as a Service (IaaS)	09 hours
Unit-III	Security Design and Architecture for Cloud Computing Guiding Security design principles for Cloud Computing Secure Isolation Comprehensive data protection End-to-end access control	09 hours
Unit-IV	Monitoring and auditing Quick look at CSA, NIST and ENISA guidelines for Cloud Security • Common attack vectors and threats	09 hours
Unit-V	Secure Isolation of Physical & Logical Infrastructure: • Isolation o Compute, Network and Storage • Common	09 hours

	attack vectors and threats • Secure Isolation Strategies o Multi tenancy, Virtualization strategies o Inter-tenant network segmentation strategies o Storage isolation strategies	
--	--	--

Suggested Readings

1. CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security 1st Edition by Raj Samani (Author), Brian Honan (Author)
2. Enterprise Cloud Security and Governance: Efficiently set data protection and privacy principles by Zeal Vora
3. Mastering AWS Security: Create and maintain a secure cloud ecosystem
4. Pressman R.S. Software Engineering: A Practitioner's Approach, MGH.
5. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005
6. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004
7. Ian Sommerville, "Software Engineering", Fifth Edition, Pearson Education Asia. by Albert Anthony
8. Microsoft Azure Security Center (IT Best Practices - Microsoft Press) 2nd Edition
9. by Yuri Diogenes (Author), Tom Shinder (Author)
10. Practical Cloud Security: A Guide for Secure Design and Deployment 1st Edition by Chris Dotson (Author) Multi-Cloud Architecture and Governance, by Jeroen Mulder.

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

Course Overview

This is a laboratory course based on Cloud Security (FOC/DSE/505T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical (Students have to perform at least 10 practical)

1. Study NIST model of cloud computing
2. study different types of virtualizations, Host and bare metal hypervisors and implement horizontal scalability
3. Implement IaaS using your resources
4. Simulate identity management in a private cloud
5. Explore Storage as a Service for remote file access using web interface
6. Understand security of web server and data directory
7. create and access VM instances and demonstrate various components such as EC2, S3, Simple DB, DynamoDB
8. Deploy web applications on commercial cloud
9. Understand on demand application delivery and Virtual desktop infrastructure
10. To have a basic understanding of implementation/applications of fog computing
11. Create their private cloud for the institute using the available resources.
12. Apply security concepts to secure a private cloud.
13. Implement efficient load balancing.
14. Compare various virtualization technologies with given resource.
15. Create cloud applications such as messenger, photo editing website, your own social media etc.

Research Methodology

FOC/RM/549	Research Methodology and Statistics	Credit:04	Contact Hours:60	Marks:100
-------------------	--	------------------	-------------------------	------------------

Course Overview

Research is an important aspect for academic growth of an individual. Research means contributing something new in the existing stock of knowledge. In addition to the general component of research, what is important is validation of data and its analysis. Statistics helps to collect, present, analyse and interpret the data collected during the research. Combining both the components, the course has been designed to give the complete idea of a scientific research and its statistical analysis.

Course Objectives

The course has the following objectives:

- To make the students aware the concepts of research
- To facilitate the students to make research plan
- To enable the students to do scientific writings
- To enable students to apply statistical methods in their research
- To enable students to design their research methods

Course Outcomes

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

- CO1: Explain the concepts of research process, writing of research, basics on descriptive statistics, basics of inferential statistics and probability.
- CO2: Execute literature review, select research problem, formulate hypothesis, collect data, analyze the data and test the hypothesis.
- CO3: Draw connections between various ideas presented in a research article/journal and book.
- CO4: Author master dissertation, research paper and present the findings in a conference.
- CO5: Apply statistical tools to calculate central tendency, dispersion and higher statistics.
- CO6: Test the hypothesis for both small and large samples.

Unit	Course Content	Contact Hours
Unit-I	Fundamentals of Research • Introduction to research methodology, definition and basic concepts of research, objectives of research, motivation behind a research, types of research, research process: defining research problem, review the literature, formulation of hypothesis, research	12

	design, collection and analysis of data, interpretation and writing a report. Criteria for good research, measuring research impact and quality: JCR report, impact factor and citation index, ethics and scientific conduct, Ethics in human and animal studies.	
Unit-II	Writing and Presenting Research • Components of research paper: the IMRAD system, title, authors and addresses, abstract, acknowledgements, references, tables and illustration; preparation for publication, submission of manuscript, publication processes; presentation of research: oral and poster presentations, presentation and submission of research proposals to the funding agencies. • A brief idea about funding agencies for research and development: UGC, CSIR, DFSS, DST, ICMR, BPR&D, DBT, BARTI. • Plagiarism: definition, types, consequences, UGC regulations.	12
Unit-III	Basic Concepts of Statistics and Data Analysis • Basic definitions and applications of statistics, sampling: Representative sample, sample size, sampling bias and sampling techniques. Data collection and presentation: Types of data, methods of collection of primary and secondary data. Methods of data presentation-graphical representation by histogram, polygon, ogive curves and pie diagram. Measures of central tendency: mean, median and mode; measures of dispersion: range, mean deviation, standard deviation, variance, quartile, standard error and coefficient of variation; correlation and regression: positive and negative correlation and calculation of Karl-Pearson's coefficient of correlation, skewness and kurtosis.	12

Unit-IV	Probability • Introduction to probability theory, various definitions of probability, Basic terms: random experiments, event, trial, sample space, independent and mutually exclusive events, exhaustive events; conditional probability, addition and multiplication theorem, Bayes' theorem, likelihood ratio and discriminating power. Distribution of data: normal, binomial and Poisson distribution.	12
Unit-V	Test of Hypothesis • Introduction and concepts; test for small and large sample: Z-test, t-test, chi-square test, F-test and ANOVA. • Software related to statistical analysis	12

Suggested Readings/Reference Books:

1. Fundamentals of Statistics (2018), S C Gupta, Himalaya Publishing House
2. Statistics in Biology, (1967) Vol. 1: Bliss, C.I.K. McGraw Hill, New York.
3. Practical Statistics for experimental biologist (1985): Wardlaw, A.C.
4. Statistical Methods in Biology (2000): Bailey, N.T. J. English Univ. Press.
5. Biostatistics - 7th Edition: Daniel
6. Fundamental of Biostatistics: Khan
7. Bio-statistical Methods: Lachin
8. Statistics for Biologist (1974): Campbell R.C. Cambridge
9. Research Methodology Tools and Techniques: H.C Purohit
10. Research Methodology: An Introduction: Wayne Dean Goddard, Stuart Melville
11. Research Methodology For Biological Science : Gurumani N Gurumani
12. Research Methodology- G.R. Basotia and K.K. Sharma.
13. Research Methodology- C.H. Chaudhary, RBSA Publication
14. Research Methodology: An Introduction - Wayne Goddard & Stuart Melville
15. Research Methodology - Ranjit Kumar
16. Research Methodology: Methods & Techniques - Kothari, C.R.

Detailed Curriculum of Semester-II

Discipline-Specific Core Courses

FOC/MJ/550T	Forensic Application Development and Networking Concepts	Credit:03	Contact Hours:45	Marks:75
--------------------	---	------------------	-------------------------	-----------------

Course Objectives

1. To understand Python Basics
2. To understand Basics of Networking
3. To understand Link Layer Devices and Protocols
4. Introduction to Perl programming and Bash Scripting

Course Outcomes

- **CO1:** To Gain Knowledge in Python Basics, Perl programming and Bash Scripting
- **CO2:** To Study Basics of Networking- Protocols, Packets
- **CO3:** To Understand Subnet ,Calculators, Routing, Routing Table
- **CO4:** To Obtain Knowledge in Link Layer Devices and Protocols.

Unit	Content	Contact Hours
Unit-I	UNIT- I Python Basics- Python Setup, debugging, Variables, Strings, Lists, Dictionaries, Networking, Selection, Exception Handling, Function, Iteration, File I/O, Sys Module, OS Module, Comments And Pound Characters, Numbers And Math, Variables And Names, Conditional Statements, Classes and Objects (OOP) Is-A, Has-A, Inheritance and Composition.	09 hours
Unit-II	Introduction to Perl programming and Bash Scripting- Introduction, Data types, Conditional and iteration statements, Array and Lists, Subroutines, Regular Expressions, File Handling, Introduction to Bash Scripting.	09 hours
Unit-III	Basics of Networking- I Protocols, Packets: The IP Header, Protocol Layers, ISO/OSI, Encapsulation, IP: IPv4 Addresses, Reserved IP Addresses, IP/Mask and CIDR, IP/Mask CIDR Example, IP/MASK Host Example,	09 hours
Unit-IV	Basics of Networking- II Network and Broadcast Addresses, IP Examples, Subnet Calculators, Routing, Routing Table, Routing Table Example, Default Route Example, Routing Metrics, Routing Metrics Example, Checking the Routing Table	09 hours
Unit-	Link Layer Devices and Protocols Link Layer Devices, MAC Addresses, IP and MAC Addresses,	09 hours

IV	Broadcast MAC Addresses, Switches: Multi-switch Networks Segmentation, Multi-switch Example, Multi- switch and Router Example, Forwarding Tables, CAM Table Population, ARP, Hubs. TCP and UDP: Ports, Ports Examples, Well-known Ports, TCP and UDP Headers, TCP Header, UDP Header, Netstat Command, TCP Three-way Handshake	
----	--	--

Suggested Readings

1. Violent Python: A Cook book for Hackers, Forensic Analysts, Penetration Testers and Security Engineers Import by TJ O'Connor
2. Learning Perl by Randal L. Schwartz, O'Reilly Media
3. PenetrationTesting:AHands-OnIntroductiontoHacking1stEditionbyGeorgiaWeidman
4. Computer Security Principles and Practice by William Stallings Pearson
5. Forouzan, B. A., &Fegan, S. C. New York: "Data communications and networking",
6. McGraw-Hill Higher Education, 2007.

FOC/MJ/550P	Practical based on FOC/MJ/550T	Credit:01	Contact Hours:30	Marks:25
--------------------	---------------------------------------	------------------	-------------------------	-----------------

Course Overview

This is a laboratory course based on **Forensic Application Development and Networking Concepts** (FOC/MJ/550T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practicals has to be covered in the semester for successful completion of the course.

List of Practical

1. Troubleshooting Computer Network
2. Working with Nessus and NMAP tools
3. Network packet analysis through Wireshark,
4. Configuration of intrusion detection system through Snort (Linux)
5. Experiments on Open Source SIEM tools
6. Experiments on assessing network vulnerabilities
7. Experiments on Detection of DoS/DDoS attacks
8. Study of different types of Network cables
9. Study of Network Devices in Detail.
10. Study of network IP.
11. Connect the computers in Local Area Network.
12. Study of basic network command and Network configuration commands.
13. Configure a Network topology using packet tracer software.
14. Configure a Network using Distance Vector Routing protocol.
15. Configure Network using Link State Vector Routing protocol.
16. Program to implement connection oriented client server communication
17. Program to implement connectionless client server communication
18. Implement the data link layer framing methods such as Bit Stuffing.
19. Implement on a data set of characters the CRC polynomials

FOC/MJ/551T	Threats to Web Infrastructure, its Defense and Resilience	Credit:03	Contact Hours:45	Marks:75
-------------	---	-----------	------------------	----------

Course Objectives

1. To study Vulnerability Assessments
2. To study Footprinting and Scanning
3. To Map a Network
4. To study Fingerprinting with Nmap Port Scanning

Course Outcomes

- **CO1:** Gained knowledge about vulnerabilities.
- **CO2:** Learned about Footprinting and Scanning.
- **CO3:** to study Metasploit.

Unit	Content	Contact Hours
Unit-I	Vulnerability Assessments Introduction to Vulnerability Assessment, Life cycle of Vulnerability Assessment, Vulnerability Scanners, Manual Testing, Vulnerability using W3af and Nikto, Nessus, Architecture, Introduction to Unknown Vulnerability Assessment.	09 hours
Unit-II	Footprinting and Scanning Footprinting: Mapping a Network: Why Map a (Remote) Network, Ping Sweeping : Fping, Nmap Ping Scan, OS Fingerprinting: Fingerprinting with Nmap Port Scanning : Under the Hood of a Port Scanner : TCP Three Way Handshake, Scanning with Nmap : Nmap Scan Types , TCP Connect Scan with Nmap, TCP SYN Scan with Nmap, Version Detection with Nmap, Specifying the Targets :By DNS Name , With an IP Addresses List , By Using CIDR Notation ,By Using Wildcards , Specifying Ranges , Octets Lists , Combining the Previous Methods ,Choosing the Ports to Scan , Nmap Examples, Port Scanning, Service Detection, Vulnerabilities Database Lookup.	09 hours
Unit-III	Scanning with Nmap : Nmap Scan Types , TCP Connect Scan with Nmap, TCP SYN Scan with Nmap, Version Detection with Nmap, Specifying the Targets :By DNS Name , With an IP Addresses List , By Using	09 hours

	CIDR Notation ,By Using Wildcards , Specifying Ranges , Octets Lists , Combining the Previous Methods ,Choosing the Ports to Scan , Nmap Examples, Port Scanning, Service Detection, Vulnerabilities Database Lookup.	
Unit-IV	Metasploit: Introduction, MSFConsole, Identifying a Vulnerable Service, Searching, Configuring an Exploit, Configuring a Payload, Running an Exploit, Meterpreter: Bindand Reverse, Launching Meterpreter, Session, Information Gathering with Meterpreter, System Information, Network Configuration, Routing Information, Current User, Privilege Escalation, Bypassing UAC, Dumping the Password Database, Exploring the Victim System, Uploading and Downloading files, Running an OS Shell.	09 hours
Unit-V	System Information, Network Configuration, Routing Information, Current User, Privilege Escalation, Bypassing UAC, Dumping the Password Database, Exploring the Victim System, Uploading and Downloading files, Running an OS Shell.	09 hours

Suggested Readings

1. Social Engineering: The Art of Human Hacking Kindle Edition by Christopher Hadnagy(Author),PaulWilson(Foreword)
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (byDafyddStuttard, MarcusPinto)
3. Metasploit - The Penetration Tester's Guide Paperback – Import, 15 Jul 2011 by DavidKennedy(Author), Jim O'gorman (Author), Devon Kearns(Author), MatiAharoni(Author)
4. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press, 2015. ISBN : 78-1-4822-3161-8.
5. Dr. Patrick Engebretson, The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing made easy , Syngress publications, Elsevier, 2013. ISBN :978-0-12-411644-3.
6. Andrew Whitaker and Daniel P. Newman, Penetration Testing and Network Defence The practical guide to simulating, detecting an responding to network attacks, Cisco Press, 2010. ISBN: 1-58705-208-3.
7. Vivek Ramachandran, BackTrack 5 Wireless Penetration Testing, Beginners guide Master bleeding edge wireless testing techniques with BackTrack 5, PACKT Publishing, 2011. ISBN 978-1-849515-58-0.
8. Mayor, K.K.Mookey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver, Metasploit Toolkit for Penetration Testing, Exploit Development and Vulnerability Research, Syngress publications, Elsevier, 2007. ISBN : 978-1-59749-074-0

FOC/MJ/551P	Practical based on FOC/MJ/551T	Credit:01	Contact Hours:30	Marks:25
--------------------	---------------------------------------	------------------	-------------------------	-----------------

Course Overview

This is a laboratory course based on **Threats to Web Infrastructure, its Defense and Resilience** (FOC/MJ/551T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practicals has to be covered in the semester for successful completion of the course.

List of Practical

1. To learn about hacking tools and skills.
2. To study about Footprinting and Reconnaissance.
3. To study about Fingerprinting.
4. To study about system Hacking.
5. To study about Wireless Hacking.
6. To learn & study about Sniffing & their tools
7. Study various methods for Taping into the wire.
8. Study the steps for installing Wireshark, the packet-sniffing tool for performing Network analysis.
9. Study of working with captured packets.
10. Study of advanced Wireshark features.
11. Study of security packet analysis.
12. Study of Operating System Fingerprinting.
13. Practical based on Vulnerability Assessments.

FOC/MJ/552T	Digital Forensics-II	Credit:03	Contact Hours:45	Marks:75
-------------	----------------------	-----------	------------------	----------

Course Objectives

1. To understand Live Memory Acquisition
2. To understand Live Memory Analysis
3. To understand Advanced Encase and FTK
4. To study Cryptography and Steganography
5. To understand Manual Techniques

Course Outcomes

- **CO1:** To understand Live Memory Acquisition and live memory analysis.
- **CO2:** To study EnCase and FTK.
- **CO3:** To learn Cryptography and Steganography

Unit	Content	Contact Hours
Unit-I	Live Memory Acquisition Importance of live memory in Digital Forensics, Acquisition of volatile memory using various tools, environment setup for memory acquisition, acquiring RAM dump from Window and Linux Machines. Working with LiME.	09 hours
Unit-III	Live Memory Analysis Introduction to memory analysis tools like Volatility, Rekall, FTK, EnCase and others. Exploring Volatility commands to analyze memory dumps from various versions of Windows OS. Analysing Linux Memory Dumps using various tools.	09 hours
Unit-IV	Advanced Encase and FTK Working with filters and conditions, exploring built in EnScripts, writing custom enscripts, remote acquisition using EnCase, designing custom Reports, export options, working with advanced options of FTK, remote acquisition using FTK.	09 hours
Unit-V	Cryptography and Steganography Introduction to Cryptography, Symmetric and Asymmetric Cryptography, Hash functions, Digital Certificates and Digital Signatures, Handling encrypted evidences, Introduction to	09 hours

	cryptanalysis, Introduction to steganography and steganalysis, Introduction to various Cryptography and Steganography tools.	
	Manual Techniques- Manual techniques used in forensic investigation of a computer, automating manual steps, writing python / powershell / bash / batch scripts to assist manual investigation. Handling basic Anti-forensics using manual techniques.	

Suggested Readings

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons
2. Digital Forensics Workbook: Hands-on Activities in Digital Forensics by Michael K Robinson
3. Computer Forensics and Cyber Crime : An Introduction by Marjie T. Britz
4. Digital with Open Source Tools by Cory Altheide, Harlan Carvey
5. Forensic Computing- A Practitioner's Guide by Tony Sammes, Brian Jenkinson
6. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher Stuart.
7. Handbook of Digital Forensics and Investigation by Eoghan Casey
8. Digital Forensics Explained by Greg Gogolin
9. Windows Forensic Analysis by Harlan Carvey
10. Linux Forensics by Philip Polstra
11. EnCase Computer Forensics-- The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting
12. Computer Forensics and Digital Investigation with EnCase Forensic v7 by Suzanne Widup
13. Computer Forensics with FTK by Fernando Carbone
14. Digital Forensics with the AccessData Forensic Toolkit (FTK) by John Sammons
15. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management by Anton A. Chuvakin and Kevin J. Schmidt
16. Handbook of Digital Forensics of Multimedia Data and Devices Edited by Anthony T.S. Ho and Shujun Li
17. Digital Image Forensics: There is More to a Picture than Meets the Eye Edited by Husrev Tah a Sencar and Nasir Memon
18. Steganography in Digital Media: Principles, Algorithms, and Applications by Jessica Fridrich
19. The Basics of Digital Forensics: The Primer for getting started in Digital Forensics by
20. Sammons
21. Digital Forensics Workbook: Hands-on Activities in Digital Forensics by Michael K
22. Robinson

23. Computer Forensics and Cyber Crime: An Introduction by Marjie T. Britz
24. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey
25. Forensic Computing -A Practitioner's Guide by Tony Sammes, Brian Jenkinson
26. Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips, Christopher Steuart
27. Handbook of Digital Forensics and Investigation by Eoghan Casey
28. Digital Forensics Explained by Greg Gegolin
29. Windows Registry Forensics (WRF) with Volatility Framework: Quick Startup Guide for Beginners by Kapil Soni
30. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Windows Registry by Harlan Carvey File System Forensic Analysis by Brian Carrier
31. EnCase Computer Forensics- The Official EnCE: EnCase Certified Examiner Study Guide by Steve Bunting

FOC/MJ/552P	Practical based on FOC/MJ/552T	Credit:01	Contact Hours:30	Marks:25
--------------------	---------------------------------------	------------------	-----------------------------	-----------------

Course Overview

This is a laboratory course based on **Digital Forensics-II** (FOC/MJ/552T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practicals has to be covered in the semester for successful completion of the course.

List of Practical

1. Live Case Studies
2. Open Source Forensic Tools
3. Disk Forensics and Data Recovery
4. Steganography
5. Key loggers
6. Network monitors
7. Flowchart management
8. UML diagrams
9. E Commerce on websites
10. Practical based on Cryptography and Steganography
11. Practical based on EnCase
12. Practical based on data recovery

FOC/MJ/553	Skill/Practical-Based Activity	Credit:02	Contact Hours:60	Marks:50
-------------------	---------------------------------------	------------------	-----------------------------	-----------------

Course Overview

The course has been designed to let the students acquire skills in his/her area of interest. As the aim of the course is to develop skills, the students can choose any one group of activities, which can be conducted under the guidance of a teacher.

List of activities

- Acquisition of data from the live system
- Analysis of RAM dump from various systems
- Perform steganalysis
- Any other problem identified by the students

Discipline-Specific Elective Courses

FOC/DSE/554T	Multimedia Forensics	Credit:03	Contact Hours:45	Marks:75
---------------------	-----------------------------	------------------	-------------------------	-----------------

Course Objectives

1. To study Foundation to Multimedia Forensics
2. To study the Digitization process
3. Introduction to Multimedia Forensics
4. Image and Video Forensics Introduction and scope
5. Forensic Application in the Field of Security, DVR Examination.

Course Outcomes

- **CO1:** To understand Introduction to digital signals: audio, image and video.
- **CO2:** To learn introduction to Multimedia Forensics.
- **CO3:** To learn admissibility of multimedia evidence to the court of law along with various acts.
- **CO4:** To study Scope & it's Forensic Application in the Field of Security, DVR Examination.

Unit	Content	Direct-teaching learning hours
Unit-I	Foundation to Multimedia Forensics Introduction to digital signals: audio, image and video, Digitization process: sampling and quantization, Image Enhancement Techniques: Spatial and frequency domain,	09 hours
Unit-II	Image Compression, description, and representation Introduction to compression techniques, Image description and representation techniques, Pattern clustering and classification.	09 hours
Unit-III	Introduction to Multimedia Forensics Introduction and scope of Multimedia Forensics, Basics of Multimedia Devices for capturing image and video, audio, Standard and best practices in Multimedia Forensics, Admissibility of multimedia evidence to the court of law along with various acts.	09 hours
Unit-IV	Image and Video Forensics Introduction and scope, Standards for video transmission,	09 hours

	Active and passive image/video forensics, Blind and non-blind image/video forensics, Methods of source camera identification, Methods for tampering of digital image/video.	
Unit-V	Authentication Process Forensic authentication of digital image/video, Enhancement of digital image/video, Specific Frame Analysis, Scope & it's Forensic Application in the Field of Security, DVR Examination.	09 hours

Suggested Readings

- Handbook of Digital Forensics of Multimedia Data and Devices by Anthony T S Ho, Shujun Li
- Multimedia Forensics and Security Foundations, Innovations, and Applications by Aboul Ella Hassanien, Mohamed Mostafa Fouad
- Fundamentals of Speaker Recognition by Homayoon Beigi
- Fundamentals of Speaker Recognition Law Enforcement and Counter-Terrorism by Amy Neistein, Hemant A. Patil
- Forensic Comparison of Voice, Speech and Speakers by Jonas Lindh

FOC/DSE/554P	Practical based on FOC/DSE/554T	Credit:01	Contact Hours:30	Marks:25
---------------------	--	------------------	-------------------------	-----------------

Course Overview

This is a laboratory course based on Multimedia Forensics (FOC/DSE/554T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical

1. Enhancement of distorted/noisy images
2. Enhancement of distorted/noisy video
3. Enhancement of distorted/noisy audio
4. Authentication of image
5. Authentication of video
6. Authentication of audio
7. Source device recognition from image
8. Source device recognition from video
9. Source device recognition from audio
10. Apply various compression techniques to the given image
11. Apply various compression techniques to the given video
12. Apply various compression techniques to the given audio
13. Describe an object in the image using various shape descriptors
14. Describe an object in the image using various texture descriptors
15. Describe an object in the image using various color descriptors
16. Classify various objects in the images

FOC/DSE/555T	Web Science	Credit:03	Contact Hours:45	Marks:75
---------------------	--------------------	------------------	-------------------------	-----------------

Course Objectives

1. Web science in forensics and its importance
2. Introduction to XML
3. Introduction to Ajax

Course Outcomes

- **CO1:** understand web science in forensics and its application.
- **CO2:** Understand XML and Ajax.
- **CO3:** Apply web science for forensic applications

Unit	Content	Contact Hours
Unit-I	Define web science, importance, role, scope, functions. Web science in forensics and its importance.	09 hours
Unit-II	XML- Introduction to XML, Comparing XML with HTML Describing the Structure of XML - Declaration, Elements, Attributes, Comments, CDATA, XML Entity References, Parsers ,Describing Document Type Definitions, Using XSLT with XML :xsl:template Element .	09 hours
Unit-III	xsl:apply-templates Element, xsl:import , xsl:include Element , Element, xsl:element Element, xsl:attribute Element, xsl:value-of Element, using Conditional Statements, Sorting Elements, XSLT functions, Creating Well-formed and Valid Documents.	09 hours
Unit-IV	Introduction to Ajax – AJAX Web Application Model, Working of AJAX Asynchronous Data Transfer with XMLHttpRequest-Creating the XMLHttpRequest Object, XMLHttpRequest Properties, XMLHttpRequest Methods, Using the XMLHttpRequest Object in Different Browsers,	09 hours
Unit-IV	Reading a File Synchronously, Reading a File Asynchronously, Performing Tasks Using the XMLHttpRequest Object, Integrating PHP and AJAX-Sending Data from a Web Application to a Server, Validating a Field Using AJAX and PHP	09 hours

Suggested Readings

- 1) XML: A Beginner's Guide by Steven Holzner
- 2) AJAX for Beginners, Ivan Bayross and Sharanam Shah, SPD
- 3) Web Development with jQuery (WROX) by Richard York
- 4) Learning PHP, MySQL & JavaScript with j Query, CSS & HTML5 – by Robin Nixon, SPD

FOC/DSE/555P	Practical based on FOC/DSE/555T	Credit:01	Contact Hours:30	Marks:25
---------------------	--	------------------	-------------------------	-----------------

Course Overview

This is a laboratory course based on Web Science (FOC/DSE/555T). The course objectives and outcomes of this laboratory course have been added to the theory course. A minimum of 10 practical has to be covered in the semester for successful completion of the course.

List of Practical

1. Representing Data using XML with XSL and Internal DTD **(three)**
2. Retrieving data from server & Sending data to server using AJAX
3. Retrieving data from HTML using PHP
4. Retrieving Employee Details/ Registration Details from the database using Ajax and PHP
5. Adding ,Modifying and Deleting data from Client side to into table in MySql Ajax and PHP
6. Representing Data Using jQuery Selectors/ jQuery Methods to Access HTML Attributes **(Two)**
7. Representing Data using jQuery Manipulators, jQuery Events, jQuery Effects **(Three)**

On Job Training/ Field Project

FOC/OJT/559	On Job Training/Field Project	Credit:04	Contact Hours:120	Marks:100
--------------------	--------------------------------------	------------------	------------------------------	------------------

Course Overview

As per NEP 2020, the student has to carry out on job training (internship/apprenticeship) and field project at least for four weeks during the summer vacations. The student can work in the industry/ academic institutions/ research institutions/ laboratories specified by the university/Institute/colleges. On completion, the student needs to produce the certificate of completion. Detailed guidelines will be issued by the university in due course of time.