

# ANNEXURE B



**HSNC UNIVERSITY, MUMBAI  
(2024-2025)**

**Ordinances and Regulations**

**With Respect to**

**Choice Based Credit System (CBCS)**

**For the Programme Under**

**The Faculty of Science & Technology**

**Curriculum – Part II Information Technology**

**Postgraduate Programme**

**2024-2025**

**Syllabus for M.Sc. I.T Part II**

**(With effect from the academic year 2024-2025)**

### Department of M.Sc. I.T Board of Studies

(i) The Board of Studies shall consist of the following members, namely: —

- (a) One head of the Department from amongst the Schools, Centers and Constituent Colleges, of the University in the relevant subject of the University nominated by the Vice Chancellor in consultation with the Dean concerned; -

Sr. No.	Name	Designation	Contact Details
1.	Dr. Rakhi O.Gupta	Chairperson HOD Dept. of IT, KC College, HSNC University	9619914191 <a href="mailto:rakhi.gupta@kccollege.edu.in">rakhi.gupta@kccollege.edu.in</a>

- (b) Two to five teachers each having minimum five years teaching experience amongst the full time teachers of the Departments, Schools, Centers and Constituent Colleges of the University in the relevant subject nominated by the Vice-Chancellor in consultation with the Dean of the respective faculty; -

Sr No.	Name	Designation	Contact Details
1.	Ms. Pragati V.Thawani	Co-chairperson Dept. of IT, KC College, HSNC University	9960782000 <a href="mailto:pragati.thawani@kccollege.edu.in">pragati.thawani@kccollege.edu.in</a>
2.	Ms. Sandhya Bhavsar	Assistant Professor Dept. of IT,KC College,HSNC University	8446677643 <a href="mailto:sandhya.bhavsar@kccollege.edu.in">sandhya.bhavsar@kccollege.edu.in</a>
3.	Ms. Neha Patel	Assistant Professor Dept. of IT,KC College,HSNC University	9820609142 <a href="mailto:Neha.patel@kccollege.edu.in">Neha.patel@kccollege.edu.in</a>
4.	Ms. Nashrah Gowalker	Assistant Professor Dept. of IT,KC College,HSNC University	9664774108 <a href="mailto:nashrah.gowalker@kccollege.edu.in">nashrah.gowalker@kccollege.edu.in</a>

- (c) One Professor / Associate Professor from other Universities or professor / Associate Professor from colleges managed by Parent Body; nominated by Parent Body; --

Sr. No.	Name	Designation	Contact Details
1.	<b>Dr. R. Kamatchi</b>	<b>Director, ISME School of Management Studies and Entrepreneurship, Lower Parel.</b>	<b>9224450454</b> <a href="mailto:rkamatchiiver@gmail.com">rkamatchiiver@gmail.com</a>
2.	<b>Dr. Ajay Patil</b>	<b>Professor, School of Computer Sciences, KNMU, Jalgaon.</b>	<b>9423975215</b> <a href="mailto:ajaypatil.nmu@gmail.com">ajaypatil.nmu@gmail.com</a>

- (d) Four external experts from Industry / Research / eminent scholar in the field relevant to the subject nominated by the Parent Body;

Sr. No.	Name	Designation	Contact Details
1.	<b>Dr. Hiren Dand</b>	<b>Head of Department (IT) Mulund College of Commerce.</b>	<b>9821140717</b> <a href="mailto:Hiren.dand@mccmulund.ac.in">Hiren.dand@mccmulund.ac.in</a>
2.	<b>Mr. Asif K. Rampurawala</b>	<b>Vice Principal, Vidyalkar School Of Information Technology</b>	<b>9820765273</b> <a href="mailto:asif.rampurawala@vsit.edu.in">asif.rampurawala@vsit.edu.in</a>
3.	<b>Mr. Kaushal Shah</b>	<b>PI Industries</b>	<b>9869069203</b> <a href="mailto:Kaushal.shah@kccollege.edu.in">Kaushal.shah@kccollege.edu.in</a>
4.	<b>Mr. Prabhav Daga</b>	<b>Pagadi Group of Companies</b>	<b>9321031131</b> <a href="mailto:prabhav@skiller.com">prabhav@skiller.com</a>
5.	<b>Ms Kirti Bhatt</b>	<b>Lecturer / Industry Expert</b>	<b>9869856998</b> <a href="mailto:Kirti.bhatt@kccollege.edu.in">Kirti.bhatt@kccollege.edu.in</a>

- (e) Top rankers of the Final Year Graduate and Final Year Post Graduate examination of previous year of the concerned subject as invitee members for discussions on framing or revision of syllabus of that subject or group of subjects for one year nominated by Vice Chancellor.

Sr. No.	Name	Contact Details
1.	<b>Ms Sameera Momin</b>	<b>9833011248</b> <a href="mailto:Smomin15600@gmail.com">Smomin15600@gmail.com</a>

## Part-II

### The Scheme of Teaching and Examination:

The performance of the learners shall be evaluated in two components: Internal Assessment with 40% marks by way of continuous evaluation and by Semester End Examination with 60%marks by conducting the theory examination.

### Teaching Hours –

Unit (1 to 3)	Total Lectures	Credit	Total Marks
Theory	45	3	60
Practical	30	1	40

### Evaluation Pattern – 100 Marks

### Theory Assessment– 60 Marks

Q-No.	Particulars	Marks
Q-1	All Units	15 Marks
Q-2	Unit-I	15 Marks
Q-3	Unit-II	15 Marks
Q-4	Unit-III	15 Marks

### Internal Assessment– 15 Marks

Sr. No.	Particulars	Marks
1	Self-Learning Evaluation – Active participation in routine class instructional deliveries Overall Performance – Attendance Record	15 Marks

### Practical Assessment– 25 Marks (50 Marks converted into 25 Marks)

Sr. No	Evaluation type	Marks
1	Two Best Practical	20
	a. Evaluation of One Program	
	b. Evaluation of Second Program	20
2	Journal	05
3	Viva	05

## Preamble

The M.Sc. Information Technology program is started with an aim to make the students employable after

Post-Graduation and impart industry oriented training.

**1. Course Objective:** The main objectives of the course are:

- To think analytically, creatively and critically in developing robust, extensible and highly maintainable technological solutions to simple and complex problems related to human, technology and environmental factors.
- To apply their knowledge and skills to be employed and excel in IT professional careers and/or to continue their education in IT and/or related post graduate programs.
- To be capable of managing complex IT projects with consideration of various factors.
- To work effectively as a part of a team to achieve a common stated goal.
- To adhere to the highest standards of ethics, including relevant industry and organizational codes of conduct.
- To develop an aptitude to engage in continuing educational and professional development.
- To build on the basics and the core concepts learnt during relevant undergraduate program.

The new syllabus is aimed to achieve the following objectives. The syllabus spanning two years covers the industry endorsed relevant courses. The students will be ready for the jobs available in different fields like:

- Networking
- Security
- Machine Learning
- Artificial Intelligence
- Big Data
- Image Processing
- Cloud Computing and Applications
- AI Chat Bot
- And many others

**2. Process adopted for curriculum designing:** The department has conducted multiple meetings with academic partners, industry partners. After discussion with them, the changes in the syllabus were introduced with the view that students need to learn the core concepts in detail.



3. **Salient features, how it has been made more relevant:** After discussion and interaction with the industry partners and understanding the requirement of the industries certain changes in the syllabus are introduced. Upcoming Technologies like AI, Big Data, etc. have been added keeping the upcoming trends in the field of Information Technology.
4. **Learning Outcomes:** It is expected to improvise the soft skill as well as hardware skills for the students.
5. **Input from stakeholders:** (Which sections have been modified) with relevant introduction: There are modifications suggested by the Industry person to make changes in the syllabus provided by University of Mumbai and add a few more topic to the already developed syllabus

**PROGRAMME OUTCOMES (PO)-**

Program Outcomes (POs)	
On successful completion of the M.Sc. Information Technology program	
PO1	<b>Advanced Disciplinary and Interdisciplinary Knowledge:</b> Demonstrate a comprehensive understanding of the core and advanced concepts in the specific field of science (e.g., Physics, Chemistry, Mathematical sciences, Life sciences, , Computers and Information Technology etc). Apply the knowledge from related disciplines to address complex scientific challenges
PO2	<b>Research Proficiency:</b> Develop the ability to design and conduct experiments, analyze data, and interpret results using modern scientific methods and tools
PO3	<b>Critical Thinking, Problem Solving, Data Analysis and Interpretation:</b> Employ logical reasoning and innovative approaches to solve complex scientific problems. Use quantitative and qualitative methods, including statistical and computational tools, to draw valid conclusions
PO4	<b>Use of Technology, Laboratory and Technical Skills:</b> Gain proficiency in handling advanced laboratory equipment and techniques specific to the field of study. Effectively use modern software, tools, and technologies relevant to the discipline
PO5	<b>Use of Technology, Laboratory and Technical Skills:</b> Gain proficiency in handling advanced laboratory equipment and techniques specific to the field of study. Effectively use modern software, tools, and technologies relevant to the discipline
PO6	<b>Ethics and Professionalism:</b> Uphold ethical principles in research and professional practices, ensuring honesty, integrity, and accountability.
PO7	<b>Environmental and Social Responsibility:</b> Demonstrate awareness of the environmental, societal, and global impacts of scientific endeavors
PO8	<b>Independent Learning ability and Preparation for Higher Studies:</b> Cultivate an attitude of continuous learning to adapt to advancements in science and technology. Be prepared to pursue doctoral programs or other advanced studies in the chosen field.
PO9	<b>Carrier development:</b> This program brings together the graduates who wish to enhance their skills and gives them an opportunity to develop their careers in a particular direction. The programme provides in-depth knowledge of particular subject and arouses interest of the students towards research in that particular field.
PO10	<b>Employability and entrepreneurship:</b> The masters of Science program provides the candidate with understanding, general proficiency, and methodical abilities on an advanced level required in industry, consultancy, education, entrepreneurship or public administration etc



**PG Structure and Titles as per NEP Semester III & IV**

**Program Name: M.Sc. Subject: IT**

**List of Papers**

(Theory: 15 Lecture hours= 1 Credit & Practical: 30 Lecture hours= 1

Credit; Change no. of hours accordingly wherever applicable)

**MAJOR/MINOR COURSE**

YEAR	Sem	Track	Theory / Practical	Paper Code	Course Title	No of Credits	No of Lecture Hours	Total Credits
2	III	I	Theory		Artificial Neural Networks	3	45	8+4=12 (Major)
			Practical		Artificial Neural Networks Practical	1	30	
			Theory		Programming Computer Vision	3	45	
			Practical		Programming Computer Vision Practical	1	30	
			Theory		Natural Language Processing	3	45	
			Practical		Natural Language Processing Practical	1	30	
		II	Theory	BIT604B	Statistical Thinking and Data Analysis	3	45	8+4=12 (Major)
			Practical	BIT604D	Statistical Thinking and Data Analysis Practical	1	30	
			Theory	BIT605B	Data Science Implementation	3	45	
			Practical	BIT605D	Data Science Implementation Practical	1	30	





		<b>Theory</b>	BIT606B	<b>Web Data Analytics</b>	<b>3</b>	<b>45</b>	
		<b>Practical</b>	BIT606D	<b>Web Data Analytics Practical</b>	<b>1</b>	<b>30</b>	
<b>III</b>		<b>Theory</b>		<b>Digital Forensics, Incident Response &amp; Malware Analysis</b>	<b>3</b>	<b>45</b>	<b>8+4=12 (Major)</b>
		<b>Practical</b>		<b>Digital Forensics, Incident Response &amp; Malware Analysis Practical</b>	<b>1</b>	<b>30</b>	
		<b>Theory</b>		<b>Vulnerability Assessment and Penetration Testing</b>	<b>3</b>	<b>45</b>	
		<b>Practical</b>		<b>Vulnerability Assessment and Penetration Testing Practical</b>	<b>1</b>	<b>30</b>	
		<b>Theory</b>		<b>Cyber Law</b>	<b>3</b>	<b>45</b>	
		<b>Practical</b>		<b>Cyber Law Practical</b>	<b>1</b>	<b>30</b>	
		<b>Theory</b>	BIT621B	<b>SAP Analytics</b>	<b>3</b>	<b>45</b>	<b>Mi(4)</b>
		<b>Practical</b>	BIT621D	<b>SAP Analytics Practical</b>	<b>1</b>	<b>30</b>	



**Seminar/Research Project**

<b>Year</b>	<b>Sem.</b>	<b>Paper</b>	<b>Paper Code</b>	<b>Course Title</b>	<b>No of Credits</b>	<b>No of Lectures Hours</b>	<b>Total Credits</b>
2	III			<b>Seminar/Research Project</b>	4		
	IV			<b>Seminar/Research Project</b>	8		



**Part-2 Semester III Detailed Syllabus**

**Track 1 – Artificial Intelligence**

**Artificial Neural Networks**

**Course Objectives**

- The aim of this course is to provide students a thorough understanding of neural networks and associated ideas.
- It covers special networks, third-generation neural networks, fuzzy systems, training algorithms, and basic ideas.
- Students will learn both theoretical concepts and useful abilities in creating, putting into practice, and utilizing neural network models through lectures and hands-on activities.

**Course Outcomes**

- Describe different neural network architectures and their uses, such as recurrent networks and feed-forward networks with multiple layers and layers.
- Use supervised learning networks, such as radial basis function networks, back propagation networks, and perceptron networks, and evaluate them. Implement and assess unsupervised learning networks, such as counter-propagation networks, competitive nets, and self-organizing feature maps.
- Gain knowledge of fuzzy systems, including fuzzy logic and fuzzy sets, and their applications in neural networks and other domains.

Unit	Details	No of lectures
1	<p><b>Fundamentals of Neural Networks:</b> What is Neural Network, Basics of neuroscience Evolution of Neural Networks, Basic Models, McCulloch Pitts Neuron, Linear Separability, Hebb Network. Model of Artificial Neuron, Learning rules and various activation functions.</p> <p><b>Neural Network Architecture:</b> The brain metaphor, Single layer Feed-Forward networks. Multilayer Feed-forward networks. Recurrent Networks.</p>	15
2	<p><b>ANN training algorithms</b> Supervised learning. Reinforcement learning. Unsupervised learning. Deep Learning, Geometry of Binary Threshold Neurons and their Networks</p> <p><b>Supervised Learning Network</b> Perceptron Networks, Adaptive Linear Neuron, Multiple Adaptive Linear Neurons, Back propagation Network, Radial Basis Function, Time Delay Network, Functional Link Networks, Tree Neural Network.</p> <p><b>Unsupervised Learning Networks</b> Fixed weight competitive nets, Kohonen Self-organizing feature maps, learning vectors quantization, counter propagation networks, adaptive resonance theory networks.</p>	15
3	<p><b>Special Networks</b> Simulated annealing, Boltzmann machine, Gaussian Machine, Cauchy Machine, Probabilistic neural net, cognition network, neo-cognition network, cellular neural network, optical neural network.</p> <p><b>Third Generation Neural Networks</b> Spiking Neural networks, convolution neural networks, deep learning neural networks, extreme learning machine model, Radial Basis Functions, Attractor Neural Networks</p> <p><b>Fuzzy Systems:</b> Fuzzy Logic, Classical Sets and Fuzzy sets.</p>	15



**Reference Books**

1. Neural Networks, A Classroom Approach, Satish Kumar, second edition, McGraw Hill
2. Artificial Neural Networks, Robert Schalkoff, Mc Graw Hill
3. Bishop, C. M. Neural Networks for Pattern Recognition. Oxford University Press. 1995.
4. Neural Networks, Fuzzy Logic and Genetic Algorithms, by S. Rajasekaran and G.A. Vijayalakshmi Pai.
5. Introduction to Neural Networks using MATLAB, S Sivanandam, S Sumathi, McGraw Hill.

**SLE Topics**

Geometry of Binary Threshold Neurons and their Networks, Radial Basis Function, Time Delay Network, Functional Link Networks, Tree Neural Network, Probabilistic neural net, cognition network, neo-cognition network, cellular neural network, optical neural network.

**Online Resources**

<https://www.classcentral.com/course/swavam-fuzzy-logic-and-neural-networks-13036>  
<https://www.careers360.com/university/indian-institute-of-technology-ropar/deep-learning-certification-course>  
<https://www.coursera.org/learn/neural-networks-deep-learning>  
<https://nptel.ac.in/courses/117105084>  
<https://www.udemy.com/share/101WmO3@rdagK-O7DOcPjhDTlyq5Nifzgo3hctnWGO5uPoGepIFpabFo78hPNOEbeOTMkHd/>

**Practical List**

Practical	Content
1	Show the functioning of Artificial Neural Networks (Implement all the Hidden Layer Functions)
2	Demonstrate that non separable two input perceptron cannot be classified using $P = [-0.8 \ -0.8 \ 0.3 \ 1.0 \ 0.7; \ -0.8 \ 0.8 \ -0.4 \ -1.0 \ -0.7]$ ; and Target $T = [1 \ 0 \ 1 \ 0 \ 1]$
3	Use perceptron learning rule to find final weights of a neural network using fixed input vectors and a fixed target vector
4	Prediction using neural network.
5	Implement Radial Basis Function.
6	Implement Least Mean Square Algorithm.
7	Implement Support Vector Machine Algorithm.
8	Create and train a feed forward back propagation network with a supplied Input P and Target T.
9	Design a Hopfield network consisting of two neurons with two stable Equilibrium points.
10	Perform defuzzification using the following methods <ul style="list-style-type: none"> <li>• Centroid</li> </ul>



	<ul style="list-style-type: none"> <li>• Bisector</li> <li>• Middle of Maximum</li> <li>• Smallest of Maximum</li> <li>• Largest of Maximum</li> </ul>
--	--

**Track 1 – Artificial Intelligence**

**Programming Computer Vision**

**Course Objectives**

- Learn the fundamental handling, processing, and enhancement techniques for pictures and videos using the SimpleCV framework.
- Examine cutting-edge methods for picture analysis, such as pose estimates, camera models, augmented reality, and image searching and retrieval.
- Gain expertise in graphical user interfaces, video processing, file handling, camera manipulation, and computer vision projects.
- Discover how machine learning is used in computer vision, including object detection, multiple view geometry, image grouping, classification, and 3D reconstruction.

**Course Outcomes:**

- Understand the core principles and applications of computer vision.
- Distinguish between easy and hard problems in computer vision and understand the limitations and potential of current technologies.
- Acquire skills in manipulating images and videos using the SimpleCV framework and other tools such as PIL, NumPy, and Matplotlib.
- Employ machine learning algorithms for image clustering, classification, and recognition tasks, including the use of K-Nearest Neighbors, Support Vector Machines, and Optical Character Recognition.
- Build practical applications that incorporate machine learning and computer vision techniques, such as augmented reality demos, image search engines, and automated image classification systems

Unit	Details	No. of Lectures
<b>1</b>	<p><b>Foundations of Computer Vision and SimpleCV</b></p> <p><b>Introduction to Computer Vision</b>                      Why Learn Computer Vision?, What is Computer Vision? Easy vs. Hard Problems, Vision Systems Overview, SimpleCV Framework Introduction</p> <p><b>Working with Images and Videos</b>                      Getting to Know the SimpleCV Framework: Installation, SimpleCV Shell</p>	<b>15</b>



	<p>Image Sources: Cameras, Image Sets, Video, The Xbox Kinect, Networked Cameras, Using Existing Images, Basic Image Handling and Processing: PIL, Matplotlib, NumPy, SciPy, Advanced Features: Image Manipulations (Scaling, Cropping, Slicing), Geometric Transformations, Photometric Image Formation</p> <p><b>Enhancing Images and Features Extraction</b>                  Foreground/Background Segmentation, Feature Extractors, Edge and Hue Histograms, Morphology: Dilation, Erosion, Other Morphological Operations, Image Filters and Improvements: De-noising Techniques</p>	
<p>2</p>	<p><b>Image Analysis and Augmented Reality</b>  <b>Advanced Image Handling</b>                  Camera Models: Pin-hole Camera Model, Camera Calibration, Pose Estimation and Augmented Reality: Planes, Markers, Building AR Applications, Filtering Images: Channel Mixing, Color Space Manipulation, Highlighting Edges</p> <p><b>Image Searching and Retrieval</b>                  Content-based Image Retrieval: Visual Words, Indexing, Database Searching, Ranking Results</p> <p>Image Morphology and Binarization in Detail                  Practical Applications: SpinCam, Warp, and Measurement Tools</p> <p><b>Implementing Computer Vision Projects</b>                  Handling Files, Cameras, and GUIs: I/O Scripts, Project Concept, Object-oriented Design</p> <p>Processing Video: Basics of Video Handling in OpenCV                  Tracking and Motion: Optical Flow, Haar-like Features</p>	<p>15</p>
<p>3</p>	<p><b>Machine Learning in Computer Vision</b>  <b>Image Clustering and Classification</b>                  Clustering Images: K-means, Hierarchical, Spectral Clustering                  Classifying Image Content: K-Nearest Neighbors, Bayes Classifier, Support Vector Machines, Optical Character Recognition</p> <p><b>Multiple View Geometry and 3D Reconstruction</b>                  Epipolar Geometry, Cameras and 3D Structure, Multiple View Reconstruction, Stereo Images</p> <p>Using Hue Peaks, Binary Masking for Effects like Motion Blur, Chroma Key (Green Screen)</p> <p><b>Advanced Computer Vision Applications</b>                  OpenCV for Machine Learning: The OpenCV Python Interface, Basics and Advanced Techniques</p> <p>Barcode and Object Recognition: Template Matching, Barcode Scanner, Mustacheinator</p> <p>Practical Machine Learning Applications: Creating Modules, Barcode Scanning, Facial Feature Recognition</p>	<p>15</p>



**Reference Books:**

1. Practical Computer Vision with SimpleCV Kurt Demaagd, Anthony Oliver, Nathan Oostendorp, and Katherine Scott O'REILLY
2. Programming Computer Vision with Python Jan Erik Solem Creative Commons
3. OpenCV Computer Vision with Python Joseph Howse PACKT

**SLE Topics**

Topic
Bitmaps and Pixels, Image Scaling , Image Cropping , Image Slicing , Geometric primitives and transformations, Photometric image formation
Image Morphology, Binarization , Dilation and Erosion , Examples : The SpinCam , Warp and Measurement
Histograms, Using Hue Peaks , Binary Masking , Examples: Creating a Motion Blur Effect , Chroma Key (Green Screen)
Bitmap Template Matching , Keypoint Template Matching, Optical Flow , Haar-like Features , Barcode , Examples: Barcode Scanner , Mustacheinator

Online Resources
<a href="https://youtu.be/qMfM7X53tFQ">https://youtu.be/qMfM7X53tFQ</a>

**Practical List**

Practical	Content
1	Basic Image Processing using PIL. a. Convert images to another format b. Create thumbnails c. Copy and paste regions Resize and rotate
2	Place a 3D model in a scene using OpenGL.
3	Loading 3D models and displaying them.
4	Write a simple image search engine.
5	Apply the dense SIFT descriptor to images of hand gestures to build a simple Hand gesture recognition system.
6	A simple OCR problem of recognizing numbers in images of printed sudokus.
7	Basic Feature Detection using SimpleCV. a. Finding Blobs of a Specific Color b. Find the line features in an image
8	Find circular features in an image
9	Extract the information from a barcode.
10	Track objects between frames using Optical Flow.



**Track 1 – Artificial Intelligence**  
**Natural Language Processing**

**Course Objective:**

- This course is intended as a theoretical and methodological introduction to the most widely used and effective current techniques, strategies and toolkits for natural language processing, with a primary focus on those available in the Python programming language.
- To familiarize the concepts and techniques of Natural language Processing for analyzing words based on Morphology and CORPUS.

**Course Outcomes**

- Students will be able to understand the wide spectrum of problem statements, tasks, and solution approaches within NLP.
- Students will be able to implement and evaluate different NLP applications.
- Evaluate various algorithms and approaches for the given task, dataset, and stage of the NLP product.
- Students will be able to extract information from text automatically using concepts and methods from natural language processing (NLP).
- Develop speech-based applications that use speech analysis.
- Analyze the syntax, semantics, and pragmatics of a statement written in a natural language.
- Develop a conversational agent that uses natural language understanding and generation.

Unit	Details	No. of Lectures
1	<p><b>Classical Approaches to Natural Language Processing:</b>            The Classical Toolkit, Text Preprocessing, Lexical Analysis, Syntactic Parsing, Semantic Analysis, Natural Language Generation</p> <p><b>A Quick Tour of Traditional NLP:</b> Corpora, Tokens, and Types, Unigrams, Bigrams, Trigrams and N-grams, Lemmas and Stems, Categorizing Sentences and Documents, Categorizing Words.</p> <p><b>NLP applications:</b> Speech to Text(STT), Text to Speech(TTS), Story Understanding, NL Generation, QA system, Machine Translation, Text Summarization, Text classification, Sentiment Analysis, Grammar/Spell Checkers</p>	15
2	<p><b>Word Senses:</b> Defining Word Senses, Relations Between Senses, Word Sense Disambiguation, Alternate WSD algorithms and Tasks</p> <p><b>Segmentation:</b> word level, Sentence level. Survey of English and Indian Languages Morphology, Morphological parsing FSA and FST, Porter stemmer, Machine Learning approaches.</p> <p><b>Information Extraction :</b> Noun Phrase Chunking, Chunking with Regular Expressions, WordNet: Senses and Synonyms, lexical relations, Semantic Similarity.</p>	15





3	<p><b>Part-of-Speech tagging (POS):</b> survey of POS tagsets, Rule based approaches (ENGTOWL), Stochastic approaches (Probabilistic, N-gram and HMM), TBL morphology, unknown word handling.</p> <p><b>Sequence Labeling for Parts of Speech and Named Entities:</b> English Word Classes, Named Entities and Named Entity Tagging, Tagged Corpora: Representing Tagged Tokens, Reading Tagged Corpora, Exploring Tagged Corpora, The Default Tagger, The Regular Expression Tagger, The Lookup Tagger</p> <p><b>NL parsing basics and approaches:</b> TopDown, BottomUp, Indian Language Parsing in Paninian Karaka Theory, CFG parsing using Earley’s and CYK algorithms, Probabilistic parsing, Treebanks.</p>	15
---	--	----

**Reference Books:**


1. Handbook of Natural Language Processing ,Indurkha.N. &Damerau F.J
2. Speech and Language Processing Martin, J. H &Jurafsky, D Pearson Education India
3. Foundations of Statistical Natural Language Processing , Manning, Christopher and Heinrich, Schutze , MIT Press
4. Natural Language Processing with PyTorch ,Delip Rao and Brian McMahan, O’REILLY
5. Natural Language Processing with Python Steven Bird, Ewan Klein, and Edward Loper , O’REILLY

<b>Self-Learning topics</b>
NLP applications: Speech to Text(STT), Text to Speech(TTS), Story Understanding, NL Generation, QA system, Machine Translation, Text Summarization, Text classification, Sentiment Analysis, Grammar/Spell Checkers
WordNet: Senses and Synonyms, lexical relations, Semantic Similarity, Writing Your Own Grammars, Treebanks and Grammars
The Problem of Sentiment Analysis: Document-Level Sentiment Classification, Sentence-Level Subjectivity and Sentiment Classification, Feature-Based Sentiment Analysis

<b>Online Resources</b>
<a href="https://onlinecourses.nptel.ac.in/noc21_cs102/preview">https://onlinecourses.nptel.ac.in/noc21_cs102/preview</a> . <a href="https://www.fast.ai/posts/2019-07-08-fastai-nlp.html">https://www.fast.ai/posts/2019-07-08-fastai-nlp.html</a> <a href="https://onlinecourses.nptel.ac.in/noc19_cs56/preview">https://onlinecourses.nptel.ac.in/noc19_cs56/preview</a>

## Practical List

Practical	Content
1	<ol style="list-style-type: none"> <li>Install NLTK</li> <li>Convert the given text to speech</li> <li>Convert audio file Speech to Text.</li> </ol>
2	<ol style="list-style-type: none"> <li>Study of various Corpus – Brown, Inaugural, Reuters, udhr with various methods like fields, raw, words, sents, categories,</li> <li>Create and use your own corpora (plaintext, categorical)</li> <li>Study Conditional frequency distributions</li> <li>Study of tagged corpora with methods like tagged_sents, tagged_words.</li> <li>Write a program to find the most frequent noun tags.</li> <li>Map Words to Properties Using Python Dictionaries</li> <li>Study DefaultTagger, Regular expression tagger, UnigramTagger</li> <li>Find different words from a given plain text without any space by comparing this text with a given corpus of words. Also find the score of words.</li> </ol>
3	<ol style="list-style-type: none"> <li>Study of Wordnet Dictionary with methods as synsets, definitions, examples, antonyms.</li> <li>Study lemmas, hyponyms, hypernyms, entailments,</li> <li>Write a program using python to find synonym and antonym of word "active" using Wordnet</li> <li>Compare two nouns</li> <li>Handling stopword. Using nltk Adding or Removing Stop Words in NLTK's Default Stop Word List</li> <li>Using Gensim Adding and Removing Stop Words in Default Gensim Stop Words List Using Spacy Adding and Removing Stop Words in Default Spacy Stop Words List</li> </ol>
4	<p>Text Tokenization</p> <ol style="list-style-type: none"> <li>Tokenization using Python's split() function</li> <li>Tokenization using Regular Expressions (RegEx)</li> <li>Tokenization using NLTK</li> <li>Tokenization using the spaCy library</li> <li>Tokenization using Keras</li> <li>Tokenization using Gensim</li> </ol>
5	<p>Important NLP Libraries for Indian Languages and perform:</p> <ol style="list-style-type: none"> <li>wordtokenization in Hindi</li> <li>Generate similar sentences from a given Hindi text input</li> <li>Identify the Indian language of a text</li> </ol>
6	<p>Illustrate part of speech tagging.</p> <ol style="list-style-type: none"> <li>Part of speech Tagging and chunking of user defined text.</li> <li>Named Entity recognition of user defined text.</li> </ol> <p>Named Entity recognition with diagram using NLTK corpus – treebank</p>
7	<ol style="list-style-type: none"> <li>Define grammar using nltk. Analyze a sentence using the same.</li> <li>Accept the input string with Regular expression of FA: <math>101+</math></li> <li>Accept the input string with Regular expression of FA: <math>(a+b)^*bba</math></li> <li>Implementation of Deductive Chart Parsing using context free grammar and a given sentence.</li> </ol>
8	<ol style="list-style-type: none"> <li>Study PorterStemmer, LancasterStemmer, Regexp Stemmer, Snowball Stemmer</li> <li>Study WordNet Lemmatizer</li> </ol>
9	<p>Speech Tagging:</p> <ol style="list-style-type: none"> <li>Speech tagging using spacy</li> <li>Speech tagging using nltk</li> </ol> <p>Statistical parsing: Usage of Give and Gave in the Penn Treebank sample</p>

	a. Probabilistic parser Malt parsing b. Parse a sentence and draw a tree using malt parsing.	
<b>10</b>	a. Multiword Expressions in NLP b. Normalized Web Distance and Word Similarity c. Word Sense Disambiguation	

## Track 2 – Data Science

### Statistical Thinking and Data Analysis

#### Course Objectives

- Provide students with an understanding of measures of central tendency and dispersion to effectively summarize and interpret data.
- Assist students in understanding experimental design for carrying out controlled studies and regression analysis for modelling relationships between variables.
- Give students the information and abilities they need to evaluate time series data and forecast using the right statistical techniques.

#### Course Outcomes

- Students will gain proficiency in calculating and interpreting measures of central tendency (mean, median, and mode) and dispersion (range, mean deviation, standard deviation).
- Students will understand the concept of random variables and various probability distributions such as binomial, Poisson, geometric, negative binomial, exponential, normal, and log-normal distributions.
- They will understand correlation coefficients and their significance in regression analysis.
- ANOVA techniques will also be covered, allowing students to analyze variance in different scenarios.

Unit	Details	No of lectures
1	<b>Introduction to Research and Statistical Analysis</b> Nature and objectives of research, Study and formulation of research problem, Scope and formulation of hypothesis Preparation and presentation of research and project proposals Selection of thrust research <b>Measures of central tendency and dispersion</b> (Mean, Median, Mode, Range, Mean deviation, Standard deviation)	<b>15</b>



<b>2</b>	<p><b>Probability Distributions and Hypothesis Testing</b>                  Random Variables and Probability Distribution: Definition, Distributions, Functions, Mathematical Expectation, Binomial, Poisson, Geometric, Negative binomial, Exponential, Normal, and log-normal Distributions.  <b>Hypothesis Testing:</b> Tests of significance based on normal distribution, Analysis of variance technique (ANOVA)</p>	<b>15</b>
<b>3</b>	<p>Regression Analysis, Experimental Design, Time Series, and Forecasting  <b>Linear Regression and Correlation:</b> Linear regression, Least square principle and fitted models, Karl Pearson’s correlation coefficient, Rank correlation, Lines of regression.  <b>Design of Experiments:</b> Completely randomized design, Random block design, Latin square design, and Statistical Analysis.  <b>Time series and forecasting:</b> Components of time series, Analysis of time series, Measurement of trend, Measurement of seasonal variations, Forecasting method</p>	<b>15</b>

**Reference Book:**

1. Introduction to Statistics and Data Analysis : With Exercises, Solutions and Applications in R by Christian Heumann, Michael Schomaker, Shalabh (auth.)

**SLE Topics**

**Non-Parametric Statistics:** Explore and understand non-parametric statistical tests, such as the Wilcoxon signed-rank test, Mann-Whitney U test, Kruskal-Wallis test, and Spearman's rank correlation coefficient. Learn when and how to apply these tests when the assumptions for parametric tests are not met.

**Data Visualization Techniques:** Dive into various data visualization methods, such as bar charts, histograms, scatter plots, box plots, and heatmaps. Understand how to choose the appropriate visualization method to effectively communicate insights from your data.

**Sampling Methods:** Learn about different sampling techniques, such as simple random sampling, stratified sampling, and cluster sampling. Understand the advantages and limitations of each method and how to apply them in real-world research scenarios.

**Power and Sample Size Calculations:** Study the concepts of statistical power and sample size determination. Discover how to calculate the required sample size for hypothesis testing or regression analysis to ensure sufficient statistical power.

**Time Series Analysis in R/Python:** Explore time series data analysis using programming languages like R or Python. Learn how to identify trends, seasonal patterns, and perform forecasting using popular libraries like pandas, numpy, and statsmodels.



## Online Resources

<https://youtu.be/4SJ7bEILPjk>

## Practical List

Practical	Content
1.	Measures of Central Tendency and Dispersion a. Calculate the mean, median, and mode of the following dataset: [12, 18, 20, 22, 25]. b. Compute the range, mean deviation, and standard deviation for the same dataset. c. Compare the measures of central tendency and dispersion for two different datasets
2.	Calculate the binomial probability for a given experiment with a known probability of success
3.	State the null and alternative hypotheses for a given data set
4.	Perform a hypothesis test using the z-test based on a sample mean and population standard deviation. Interpret the results of a hypothesis test and make conclusions based on the obtained p-value
5.	Conduct a simple linear regression analysis using a provided dataset
6.	Calculate the correlation coefficient between two variables and interpret its value
7.	Design an experiment using the Latin square design for testing three different treatments.
8.	Analyze a given time series data to identify trends and seasonal variations.
9.	Apply a suitable forecasting method (e.g., moving averages) to predict future values in the time series
10.	Perform an ANOVA test to compare the means of multiple groups. Interpret the results of the ANOVA test and perform post-hoc tests if necessary.



**Track 2 – Data Science**  
**Data Science Implementation**

**Course Objectives**

- Learn about different storage tools and their applications in data science, including datalakes, data vaults, hubs, links, and satellites.
- Gain insight into audit, balance, and control layers and their significance in ensuring data integrity and quality.
- Understand the concepts of data lakes, data swamps, and their implications for data storage and retrieval.

**Course Outcomes**

- Proficiency in utilizing Spark for data processing, including Spark Core, Spark SQL, Spark Streaming, and MLlib.
- Understanding of operational management layers and their role in data processing and streamlining.
- Knowledge of various analysis techniques including univariate, bivariate, and multivariate analysis, as well as regression and clustering techniques.

Unit	Details	No of lectures
1	<p><b>Data Science Technology Stack:</b> Rapid Information Factory Ecosystem Data Science Storage Tools, Schema-on-Write and Schema-on-Read , Data Lake, Data Vault, Hubs , Links, Satellites, Data Warehouse Bus Matrix, Data Science Processing Tools</p> <p><b>Spark :</b> Spark Core, Spark SQL, Spark Streaming, MLlib Machine Learning Library, GraphX, Mesos, Akka, Cassandra</p> <p><b>Kafka :</b> Kafka Core , Kafka Streams , Kafka Connect, Elastic Search , R, Scala , Python, MQTT (MQ Telemetry Transport)</p> <p><b>Layered Framework:</b> Definition of Data Science Framework, Cross Industry Standard Process for Data Mining (CRISP-DM), Homogeneous Ontology for Recursive Uniform Schema, The Top Layers of a Layered Framework.</p>	15
2	<p><b>Business Layer:</b> Business Layer, Engineering a Practical Business Layer</p> <p><b>Utility Layer:</b> Basic Utility Design, Engineering a Practical Utility Layer</p> <p><b>Three Management Layers:</b> Operational Management Layer, Processing-Stream Definition and Management, Audit, Balance, and Control Layer, Balance, Control, Yoke Solution, Cause-and-Effect, Analysis System, Functional Layer, Data Science Process.</p>	15
3	<p><b>Retrieve Superstep:</b> Data Lakes, Data Swamps, Training the Trainer Model, Understanding the Business Dynamics of the Data Lake, Actionable Business Knowledge from Data Lakes, Engineering a Practical Retrieve Superstep, Connecting to Other Data Sources,</p> <p><b>Assess Superstep:</b> Assess Superstep, Errors, Analysis of Data, Practical</p>	15



<p>Actions, Engineering a Practical Assess Superstep Process Superstep: Data Vault, Time-Person-Object-Location-Event Data Vault,  <b>Data Science Process:</b> Transform Superstep, Building a Data Warehouse, Transforming with Data Science, Hypothesis Testing, Overfitting and Underfitting, Precision-Recall, Cross-Validation Test. Univariate Analysis, Bivariate Analysis, Multivariate Analysis, Linear Regression, Logistic Regression, Clustering Techniques</p>	
--	--

**Reference book:**

1. Practical Data Science Andreas François Vermeulen APressFor Tableau Practicals Tableau by Ryan Sleeper.  
<https://www.pdfdrive.com/practical-tableau-100-tips-tutorials-and-strategies-from-a-tableau-zen-master-d188034960.html>

**SLE Topics**

<p>Data Science Technologies          Horus &amp; CRISP – DM          Different Processes of Data Science</p>
---

**Online Resources**

<p><a href="https://youtu.be/XohgKT13FKY">https://youtu.be/XohgKT13FKY</a></p>
--

**Practical List**

Practical	Content
1	Create a data model using Cassandra
2	Conversion from different formats to HORUS
3	CSV to HORUS , XML to HORUS , JSON to HORUS , MySQL to HORUS
4	Pictures of HORUS , Video to HORUS , Audio to HORUS
5	Utilities , Fixer Utilities
6	Data Binding and Bucketing
7	Aggregating of Data
8	Outlier Detection



**Track 2 – Data Science**  
**Web Data Analytics**

**Course Objectives:**

- Implement web search concepts and methods to return documents automatically based on user queries.
- Design and implement a crawler application to collect and index documents from the web.
- Design computational methods to classify documents by topic.

**Course Outcomes:**

After completion of the course, the learners will be able:

- Understand the concepts and techniques of web mining, including sequential pattern mining and rule generation.
- Gain knowledge of information retrieval models, text preprocessing, and web search techniques.
- Learn about opinion mining and sentiment classification in web information retrieval.
- Explore social network analysis, link analysis, and the implementation of webpage crawlers.
- Understand web usage mining, including the discovery and analysis of web usage patterns, and the use of recommender systems and query log mining.
- Develop deep understanding of mining techniques exclusively for the Internet
- Understand and develop analytics for social media data.
- Design and implementation of various web analytical tool to understand complex unstructured data on the Internet for aiding individuals and Businesses to grow their business

Unit	Content	No. of Lectures:45
1	<b>Web mining and search engines:</b> Introduction, Web Content Mining, Web Usage Mining, Web Structure Mining, Introduction to Modern Search Engines, Working of a Search Engine, PageRank Algorithm, Precision and Recall <b>Web Data Preprocessing:</b> Data Processing prerequisites, Attributes and Data types, Statistical descriptions of data, Distance and similarity measures, Need for Preprocessing, Handling Missing data, Data Cleaning, Data Integration, Data Reduction, Data Transformation and Data Discretization.	15
2	<b>Introduction to Information Retrieval (IR) systems:</b> Definition and goals of information retrieval, Components of an IR system, Challenges and applications of IR <b>Retrieval Models:</b> Boolean model: Boolean operators, query processing, Vector space model: TF-IDF, cosine similarity, query-document matching, Probabilistic model: Bayesian retrieval, relevance feedback <b>Web Information Retrieval:</b> Web search architecture and challenges, Crawling and indexing web pages, Link analysis and PageRank algorithm	15
3	<b>Web Mining-</b> Data Mining, Basic Concepts, Difference, Mining Sequential Patterns on Prefix Span, Generating Rules from Sequential Patterns. Evaluation measures Text and Web Page Preprocessing, Inverted Index and Its Compression, latent semantic indexing, Web Search, Web Spamming	15





	<p><b>Opinion Mining and Web Usage Mining:</b> Web Information Retrieval, Sentiment Classification, Feature based Opinion Mining and summarization, Comparative Sentence and Relation Mining, Opinion Search and Opinion Spam. Web Usage Mining.</p> <p><b>Webpage crawlers and usage mining:</b> Basic Crawler Algorithm, Implementation Issues, Universal Crawlers, Focused Crawlers, Topical Crawlers, Crawler Ethics and Conflicts, Data modelling and webpage usage mining., Discovery and analysis of web usage patterns, Recommender systems and collaborative filtering, query log mining</p>	
--	---	--

**Reference Books:**

1. Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data by Bing Liu (Springer Publications) 2017 publication
2. Data Mining: Concepts and Techniques, Second Edition Jiawei Han, Micheline Kamber (Elsevier Publications),2017
3. Web Mining: Applications and Techniques by Anthony Scime,2010
4. Mining the Web: Discovering Knowledge from Hypertext Data by Soumen Chakrabarti 2010

**Self-Learning topics.**

<b>Topic</b>
Use distance metrics to compute the similarity of pairs of documents. Create a system to collect and analyze streaming data.
Use link analysis to rank web search results. Evaluate the performance of web search systems.
Analyze text to determine the reliability of the information including potential bias.

**Practical List**

<b>Practical</b>	<b>Content</b>
1.	Perform Spam Classifier
2.	Apriori Algorithm implementation in case study.
3.	Develop a basic crawler for the web search for user defined keywords.
4.	Sentiment analysis for reviews by customers and visualize the same.
5.	Develop a focused crawler for local search.
6.	Web Crawling and Indexing a) Develop a web crawler to fetch and index web pages. b) Handle challenges such as robots.txt, dynamic content, and crawling delays.
7.	Link Analysis and PageRank a) Implement the PageRank algorithm to rank web pages based on link analysis. b) Apply the PageRank algorithm to a small web graph and analyze the results.
8.	Demonstrate Text Mining and Webpage Pre-processing using meta information from the web pages (Local/Online).
9.	Scrape an online Social Media Site for Data. Use python to scrape information from twitter.
10.	Page Rank for link analysis using python Create a small set of pages namely page1, page2, page3 and page4 apply random walk on the same



**Track 3 Cyber Security**

**Digital Forensics, Incident Response & Malware Analysis**

**Course Objectives**

- Learn about different types of cybercrimes and the forensic process involved in investigating them.
- Learn about the phases of cyber security incident management and how to handle incidents effectively.
- Familiarize with threat modelling processes, attack trees, and risk mitigation techniques.

**Course Outcomes**

- Proficiency in using forensic tools and hardware for data collection and analysis.
- Knowledge of forensic reporting standards and techniques for documenting forensic findings.
- Proficiency in collecting malware samples and correlating threat intelligence to understand emerging threats.

Unit	Details	No. of Lectures
1	<p><b>An Introduction to Digital Forensics</b>                      Forensics Fundamentals ; Computer Forensics and Law Enforcement- Indian Cyber Forensic - Forensics Services, Professional Forensics Methodology- Types of Forensics Technology Forensics system and Services : Forensics on - Internet Usage – Intrusion - Firewall and Storage Area Network; Occurrence of Cyber-crimes- Cyber Detectives- Fighting Cyber Crimes- Forensic Process, Legal aspects Laws and regulations Rules of evidence Digital forensic fundamentals A brief history The digital forensic process Identification Preservation Collection Proper evidence handling Chain of custody Examination Analysis Presentation Digital forensic lab Physical security Tools Hardware, Data Backup and Recovery , Data-Recovery Solution, Hiding and Recovering Hidden data, Evidence Collection and Data Seizure</p> <p><b>An Introduction to Incident Response</b>                      The incident response process the role of digital forensics The incident response framework The incident response charter CSIRT CSIRT core team Technical support personnel Organizational support personnel External resources The incident response plan Incident classification The incident response playbook Escalation procedures Maintaining the incident response capability</p> <p><b>Data Backup and Recovery</b>                      Data-Recovery Solution, Hiding and Recovering Hidden data,</p>	15



	<p>Evidence Collection and Data Seizure. Digital Repositories - Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects</p> <p>Containment, Eradication, and Recovery: Choosing a Containment Strategy, Evidence Gathering and Handling, Identifying the Attacking Hosts, Eradication and Recovery. Post- Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.</p>	
<p>2</p>	<p><b>Cyber security Incident Management</b></p> <p>The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist. Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post-Incident Activity. Handling an Incident: Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization&amp; Incident Notification. Coordination and Information Sharing: Coordination: Coordination Relationships, Sharing Agreements and Reporting Requirements. Information Sharing Techniques: Ad Hoc, Partially Automated, Security Considerations. Granular Information Sharing: Business Impact Information, Technical Information. Containment, Eradication, and Recovery: Choosing a Containment Strategy, Evidence Gathering and Handling, Identifying the Attacking Hosts, Eradication and Recovery. Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.</p> <p><b>The Forensics Process</b></p> <p>Network Evidence Collection ,Preparation Network diagram Configuration Logs and log management Network device evidence Security information and event management system Evidence collection ,Acquiring Host-Based Evidence ,Digital Repositories - Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects , Preparation Evidence volatility Evidence acquisition Evidence collection procedures Memory acquisition Local acquisition Virtual machines Non-volatile data ,Understanding Forensic Imaging ,Overview of forensic imaging Preparing a stage drive Imaging Dead imaging ,Network Evidence Analysis</p> <p>Analyzing packet captures Command-line tools Analyzing network log files DNS blacklists SIEM ELK Stack.</p> <p><b>Analyzing System Memory</b></p> <p>Memory evidence overview Memory analysis Memory analysis methodology Network connections methodology Tools Redline Volatility Installing Volatility Identifying the image ,Analyzing System Storage ,Forensic platforms Searches timeline Analysis Registry analysis Basic Steps of Forensic Analysis in Windows and Linux – Forensic Scenario – Email Analysis – File Signature Analysis – Hash Analysis – Forensic Examination of log files</p> <p><b>Forensic Reporting</b></p> <p>Documentation overview What to document Types of documentation Sources Audience Incident tracking Fast incident response Written reports Executive summary Incident reportForensic report, Case study</p>	<p>15</p>



	Report Preparation Processing a complete Forensic case – Preparing Forensic Report ,Working with cloud vendors, obtaining evidence, reviewing logs and APIs, Introduction to Mobile Forensic – Android Device – Analysis- Android Malware – iOSForensic Analysis – SIM Forensic Analysis.	
3	<p><b>Malware Analysis</b>                  Malware Analysis: Introduction, What is Malware Analysis? The Goals of Malware Analysis. Malware Analysis Techniques. Basic Static Analysis, Basic Dynamic Analysis, Advanced Static Analysis, Advanced Dynamic Analysis, Malware taxonomy - Malware threats - Malware analysis methodologies - Legal considerations - Identifying and protecting against malware - Malware hiding places - Collecting malware from live system -Identifying malware in dead system Malware Analysis Environment : Virtual machine - Real systems, Types of Malware, General Rules for Malware Analysis, Malware Functionality,</p> <p><b>Threat Intelligence</b>                  Open Source and Competitive Intelligence, Privacy, Snooping on People Through Open Sources, Web Browsing, Privacy Regulations, Piracy, Copyright Infringement, TrademarkInfringement, Dark Web, Deep Web, Web Scraping to gather Hidden Data, Correlating OSINT, Threat intelligence overview Threat intelligence types Threat intelligence methodology Threat intelligence direction Cyber kill chain Threat intelligence sources Internally developed sources Commercial sourcing Open source Threat intelligence platforms MISP threat sharing Using threat intelligence .</p> <p><b>Threat Modeling</b>                  Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defense in Depth and Principle of Least Privilege.</p>	15

**Reference Books**

1. Digital forensics and incident response by Gerard Johansen
2. Enterprise Security Architecture: A Business-Driven Approach by John Sherwood, Andrew Clark, David Lynas
3. Practical Packet Analysis by Chris Sanders
4. The Art of Memory Forensics by Michael Hale Ligh, Andrew Case, Jamie Levy and Aaron Walters
5. Open Source Intelligence Techniques (2019) by Michael Bazzell
6. Investigating Windows Systems by Harlan Carvey
7. Practical Malware Analysis by Michael Sikorski & Andrew Honig
8. Intelligence Driven Incident Response by Scott Roberts & Rebekah Brown
9. Blue Team Field Manual by Alan White & Ben Clark
10. File System Forensic Analysis by Brian Carrier
11. Real Digital Forensics: Computer Security and Incident Response by Keith Jones, Richard Bejtlich, Curtis Rose
12. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey
13. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons
14. Warren G. Kruse II and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002.
15. The Practice of Network Security Monitoring – Understanding Incident Detection and Response by by Richard Bejtlich



16. Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code by Michael Ligh, Steven Adair, BlakeHartstein, Matthew Richard
17. K. Dunham and S. Abu-Nimeh, Mobile Malware Attacks and Defense. Washington, DC, United States: Syngress Media

### SLE Topics

Tools for malware analysis, ApateDNS, Autoruns, BinDiff, BinNavi, Deep Freeze, Pestudio, Volatility, Remnux Dynamic analysis Process Explorer, Cuckoo sandbox, IDAPro, ProcMon, CFF Explorer, ProcExplore, BinText, FileAlyzer, OllyDbg ,Autopsy Redline Yara and Loki, Insight VM ,Test Disk Suite, Diamond model.

Overview of different software packages – Encase-Autopsy-Magnet – Wireshark - Mobile Forensic Tools – SQLite ,Wireshark Xplico and Cap Analysis ,pslist psscan pstree DLLlist Handles svscan netscan and sockets LDR modules psxview Dlldumpmemdump procdump ReCALL imageinfo pslistEvent logs Sockets Malfind ,Autopsy ,FTK Imager Winmem Remote acquisition Winmem F-Response ,Security onion Packet capture tcpdump WinPcap and RawCap Wireshark m,Proactive threat intelligence Reactive threat intelligence ,A real Forensic case study.

Forensic platforms Opening a case Navigating Autopsy Examining a Case Web Artifacts Email Attached Devices Deleted Files Keyword Searches timeline Analysis Registry analysis, SANS six-part methodology.

Live imaging Imaging with Linux, Downloaders and Launchers, Backdoors, Reverse Shell, RATs, Botnets, RATs and Botnets Compared, Credential Stealers, INA Interception, Hash Dumping, Keystroke Logging, Persistence Mechanisms, Trojanized System, Binaries, DLL Load- Order Hijacking, Privilege Escalation Using SeDebugPrivilege, Covering Its Tracks-User- Mode Rootkits, IAT Hooking, Inline Hooking, Tools for malware analysis



### Online Resources

<https://youtu.be/7DPRWpal4U0>

### Practical List

Practical	Content
1.	Demonstrate usage of Intezer Analyse for practical use case or scenario (as defined by faculty)
2.	Demonstrate usage of Alienvault OSSIM for practical use case or scenario (as defined by faculty)
3.	Create a model Windows Artifact Forensics Report for practical use case or scenario (as defined by faculty)
4.	Demonstrate usage of photorec for practical use case or scenario (as defined by faculty)
5.	Demonstrate usage of Zenmap for practical use case or scenario (as defined by faculty)
6.	Demonstrate usage of Mobile Security Framework (MobSF) for practical use case or scenario (as defined by faculty)
7.	Create a model Incident Response Report for practical use case or scenario (as defined by faculty)
8.	Create a model OSINT Report for practical use case or scenario (as defined by faculty)
9.	Create a model Malware Analysis Report for practical use case or scenario (as defined by faculty)



## Track 3 Cyber Security

### Vulnerability Assessment and Penetration Testing

#### Course Objectives

- Understand the fundamentals of Vulnerability Assessment and Penetration Testing(VAPT) including its benefits and methodology.
- Understand the reconnaissance phase including vulnerability discovery methodologies and fuzzing techniques.
- Understand the basics of SCADA and DCS architecture, protocols, and security challenges.

#### Course Outcomes

- Ability to conduct vulnerability assessments and analyze the reasons for vulnerability existence.
- Knowledge of archiving and documentation practices to maintain the integrity of penetration testing results.
- Ability to identify and mitigate security risks in SCADA and DCS environments.

Unit	Details	No. of lectures
1	<p><b>Basics of Vulnerability Assessment &amp; Penetration Testing</b></p> <p><b>Vulnerability Assessment and Penetration Testing (VAPT):</b> Introduction, Benefits, Methodology, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application Vulnerabilities &amp; Types, Working of Vulnerability Assessment Tool, OWASP, OWASP Top10</p> <p><b>Penetration Testing Overview:</b> What is Penetration Testing? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning &amp; Preparation, Reconnaissance, Discovery, Analyzing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, and Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing, White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing,</p>	15



	<p><b>Social Engineering</b>  Social Engineering: Social Engineering, Overview, Definition(s) of Social Engineering. The Social Engineering Life Cycle: Foot printing, Establishing Trust, Psychological Manipulation, The Exit. Social Engineering Attack Cycle: Research, Developing Rapport and Trust, Exploiting Trust Factor, Exploiting Trust Factor, Recruit &amp; Cloak, Evolve/Regress. The Weapons of a Social Engineer: Shoulder Surfing, Dumpster Diving, Role playing, Trojan horses, Phishing, Surfing Organization Websites &amp; Online forums, Reverse Social Engineering. Different Types of Social Engineering: Physical Social Engineering, Remote Social Engineering, Computer-based Social Engineering, Social Engineering by Email, Phishing, Nigerian or advance-fee fraud scam, Popup windows</p>	
2	<p><b>Penetration Testing Process</b>  <b>Pre-Engagement Interactions</b>  Passive Information Gathering (Web Presence, Corporate Data, WHOIS and DNS Enumeration, Additional Internet Resources), Active Information Gathering (DNS Interrogation, E-mail Accounts, Perimeter Network Identification, Network Surveying)  <b>Reconnaissance</b>  Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing. Automation and Data Generation, Environment Variable and Argument Fuzzing, Web Application and Server Fuzzing, File Format Fuzzing, Network Protocol Fuzzing, Web Browser Fuzzing, In-Memory Fuzzing, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection.  <b>Vulnerability Identification</b>  Port Scanning, Target Verification, UDP Scanning, TCP Scanning, Perimeter Avoidance Scanning, System Identification, Active OS Fingerprinting, Passive OS Fingerprinting, Services Identification, Banner Grabbing, Enumerating Unknown Services, Vulnerability Analysis  <b>Vulnerability Verification</b>  Exploit Codes – Finding and Running (Internet Sites &amp; Automated Tools), Exploit Codes – Creating Your Own (Fuzzing, Code Review &amp; Reverse Engineering), WebHacking (SQL Injection, Cross-Site Scripting &amp; Web Application Vulnerabilities). Project Management -- Executing Process Phase, Monitoring and Control Process  <b>Exploitation</b>  System Enumeration (Internal Vulnerabilities, Sensitive Data), Network Packet Sniffing, Social Engineering (Baiting, Phishing, Pretexting), Wireless Attacks (Wi-Fi Protected Access Attack, WEP Attack &amp; similar)  <b>Post-Exploitation</b>  Maintaining Access (Shells and Reverse Shells, Encrypted</p>	15





	<p>Tunnels, Other Encryption and Tunnel Methods), Covering Your Tracks (Manipulating Log Data,Hiding Files)</p> <p><b>Reporting</b> What Should You Report? (Out of Scope Issues, Findings, Solutions, Manuscript Preparation), Initial Report (Peer Reviews, Fact Checking, Metrics), Final Report (Peer Reviews, Documentation)</p> <p><b>Archiving</b> Should You Keep Data from a Pentest? (Legal Issues, E-mail,Findings and Reports),Securing Documentation (Access Controls, Archival Methods, Archival Locations, Destruction Policies), Archiving Lab Data, Creating and Using System Images (VMs), Creating a “Clean Shop”, Creating a Risk Management Register, Prioritization of Risks and Responses, Creating a Knowledge Database, Sanitization of Findings</p>	
<p>3</p>	<p><b>SCADA &amp; DCS Security</b> Scada Basics- Scada and ICS Architecture, PLC and HMI Basics,RTOS - real timeoperating systems Scada Related Protocols <b>Advanced Linux Exploitation</b> Linux heap management, constructs, and environment, , Defeating Linux exploit mitigationcontrols, Triggering patched vulnerabilities, Writing zero day exploits and day one exploits, Handling modern exploit mitigation controls.</p> <p><b>Windows Kernel Debugging and Exploitation</b> Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, Analysing Kernelvulnerabilities and Kernel vulnerability types, Kernel exploitation techniques.</p> <p><b>Windows Heap Overflows and Client-Side Exploitation</b> Windows heap management, constructs, and environment, Browser- based and client-side exploitation, Remedial heap spraying, , Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls</p> <p><b>Android Exploitation</b> Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis.</p> <p><b>iOS exploitation</b> Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debuggingand Exploitation</p>	<p>15</p>

**SLE Topics**

<p>Methodologies (Overview) Project Management Body of Knowledge Information System Security Assessment Framework Open Source Security Testing Methodology Manual</p> <p>Vulnerability Assessment Using Acunetix SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication &amp; Session</p>
--



Management, Insecure Direct Object References, Failure to Restrict URL, Remote Code Execution  
 Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Understanding C++, vtable/vtable behavior  
 Analysis- Stuxnet, Duqu  
 Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists  
 Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, WinDbg,  
 Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC DA/HAD, SCADA protocol fuzzing Finding Vulnerabilities in HMI software- Buffer Overflows, Shellcode Previous attacks Hardware Testing- Jtag  
 SCADA RTOS firmware reversing

GNU/Radio for Exploiting Radio

Frequencies,

Project Management Knowledge Database, Project Assessments, Team Assessments, Training Proposals  
 Environment Variable and Argument Fuzzing:  
 Automation Web Application and Server Fuzzing:  
 Automation  
 File Format Fuzzing: Automation on  
 UNIX, File Format Fuzzing:  
 Automation on Windows,  
 Network Protocol Fuzzing: Automation on  
 UNIX, Network Protocol Fuzzing:  
 Automation on Windows, Web Browser  
 Fuzzing: Automation,  
 In-Memory Fuzzing: Automation. - Fuzzing Frameworks

## Reference books

1. Penetration Testing A hands on Introduction to hacking by Georgia Weidman
2. ETHICAL HACKING AND PENETRATION TESTING GUIDE by RAFAY BALOCH
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm
4. "Linux Basics for Hackers" by OccupyTheWeb
5. Professional Penetration Testing Creating and Operating a Formal Hacking Lab by Thomas Wilhelm
6. "The Basics of Hacking & Penetration Testing" by PatrickEngelbreton
7. "The Hacker PlayBook 2" and "The Hacker PlayBook 3" by Peter Kim
8. "Red Team Field Manual" by Ben Clark



9. “Metasploit: The Penetration Tester’s Guide” by David Kennedy, Devon Kearns, Jim O’Gorman and Mati Aharoni
10. “Black Hat Python” by Justin Seitz
11. “The Web Application Hacker’s Handbook” by Dafydd Stuttard and Marcus Pinto
12. Gray Hat Hacking: The Ethical Hacker's Handbook, Latest Edition by Allen Harper, Daniel Regalado, et al.
13. Hacking: The Art of Exploitation, 2nd Edition by Jon Erickson
14. The Database Hacker's Handbook: Defending Database Servers by David Litchfield , Chris Anley, et al.
15. The Browser Hacker's Handbook by Wade Alcorn , Christian Frichot , et al.
16. The Mobile Application Hacker's Handbook by Dominic Chell , Tyrone Erasmus , et al
  
17. iOS Hacker's Handbook by Charlie Miller , Dion Blazakis , et al.
18. The Mobile Application Hacker's Handbook by Dominic Chell , Tyrone Erasmus , et al.
19. The Mac Hacker’s Handbook by Charlie Miller and Dino Dai Zovi
20. The Antivirus Hacker's Handbook by Joxean Koret and Elias Bachaalany

**Practical List**

Practical	Content
1.	Create a model Penetration Testing Report for practical use case or scenario (as defined by faculty)
2.	Create a model Vulnerability Analysis Report for practical use case or scenario (as defined by faculty)
3.	Create a model Bug Bounty Report for practical use case or scenario (as defined by faculty)
4.	Demonstrate usage of Acunetix for practical use case or scenario (as defined by faculty) Demonstrate usage of Metasploit for practical use case or scenario (as defined by faculty)
5.	Demonstrate usage of Burp Suite for practical use case or scenario (as defined by faculty)
6.	Create a Script to use Shodan to find vulnerable hosts for practical use case or scenario (as defined by faculty)
7.	Demonstrate SQL Injection for practical use case or scenario (as defined by faculty)
8.	Create a Script to use Exploit-DB to find exploits for practical use case or scenario (as defined by faculty)
9.	XSS for practical use case or scenario (as defined by faculty)



**Track 3 Cyber Security**

**Cyber Law**

**Course Outcome**

- Gain knowledge of the Personal Data Protection Law (PDPA) including its impact on related Acts.
- Explore the concept of digital/electronic signatures and their legal validity.
- Understand the concept of Sensitive Personal Data or Information (SPDI) and reasonable security practices in India.

**Course Objectives**

- Understanding of penalties, offences, and recent amendments to the IT Act.
- Knowledge of intellectual property rights, domain names, and trademark disputes in cyberspace.
- Ability to identify sensitive personal data and implement reasonable security practices.

Unit	Details	No. of Lectures
I	<p><b>Evolution of the IT Act, Genesis and Necessity</b></p> <p>Salient features of the IT Act, 2000; various authorities under IT Act and their powers. ; Penalties &amp; Offences, amendments, Personal Data Protection Law (PDPA) {Both Act and Bill}</p> <p><b>Impact on other related Acts (Amendments) :</b></p> <p>Amendments to Indian Penal Code, Amendments to Indian Evidence Act, Amendments to Bankers Book Evidence Act, Amendments to Reserve Bank of India Act.</p>	
II	<p><b>Cyber Space Jurisdiction</b></p> <p>Jurisdiction issues under IT Act, 2000, Traditional Principals of jurisdiction terrestrial Jurisdiction ,Case Laws on Cyber Space Jurisdiction</p> <p><b>E-commerce and Laws in India</b></p> <p>Digital/ Electronic Signature in Indian Laws ,E-Commerce; Issues and provisions in Indian Law ,E-Governance; concept and practicality in India ,E-Taxation issues in Cyberspace ,E-Contracts and its validity in India ,Cyber Tribunal &amp; Appellate Tribunal , Cyber Regulations</p> <p><b>Intellectual Property Rights, Domain Names and Trademark Disputes</b></p> <p>Concept of Trademark/ in Internet Era Cyber squatting Reverse Hijacking ,Jurisdiction in Trademark Disputes, Copyright in the</p>	



	Digital Medium Copyright in Computer Programmes ,Copyright and WIPO Treaties ,Concept of Patent Right ,Relevant Provisions of Patent Act 1970 .	
III	<p><b>Sensitive Personal Data or Information (SPDI) in Cyber Law</b>                  SPDI Definition and Reasonable Security Practices in India ,Reasonable Security Practices – International perspective ,Cloud Computing &amp; Law</p> <p><b>Cyber Law : International Perspective</b>                  EDI : Concept and legal Issues,UNCITRAL Model Law,Electronic Signature Law’s of Major Countries ,Cryptography Laws ,Cyber Law’s of Major Countries ,EU Convention on Cyber Crime</p> <p>Features of :GDPR-EU, California Privacy Act, Sarbanes-Oxley Act of 2002, The Health Insurance Portability and Accountability Act of Computer Fraud and Abuse Act (CFAA), NIST guidelines, FIPS (Federal Information Processing Standards),The Federal Information Security Management Act (FISMA)</p>	

**Reference Books**

1. "Cyberlaw: Text and Cases" by Gerald R. Ferrera, Stanley E. Stroup, and Thomas K. Jewett
2. "Cyber Law in India" by Rohas Nagpal
3. "Cyber Law: Maximizing Safety and Minimizing Risk in Classrooms" by Aimée M. Bissonette and Douglas J. Amyx
4. "Understanding Cyber Law: Emerging Legal Issues" by Jyoti Rattan and Sonia Sharma
5. "The Law of Cybercrimes and Their Investigations" by Ahmed Al-Ammari
6. "Cyber Law: The Law of the Internet and Information Technology" by Jonathan Rosenoer
7. "Internet Law: Cases & Problems" by James F. Alexander and Michael D. Scott

**SLE TOPICS**

- |  |
|--|
| <ul style="list-style-type: none"> <li>• Case Laws on Cyber Space Jurisdiction</li> <li>• Cyber Regulations</li> </ul> |
|--|

**Online Resources**

<a href="https://youtu.be/OYsY5B9pqYU">https://youtu.be/OYsY5B9pqYU</a>
---

**Practical List**

**A case study report of 50 pages related to the topic assigned by the subject incharge has to submitted and evaluated**

<b>Case Study</b>	<b>Content</b>
1	United States v. Aaron Swartz (2013):
2	Google Inc. v. Oracle America Inc. (2021)
3	Apple Inc. v. Samsung Electronics Co. (2018)
4	Facebook, Inc. v. Duguid (2020)
5	Equifax Data Breach (2017):
6	Carpenter v. United States (2018):
7	European Union Court of Justice (CJEU) Decision on "Right to be Forgotten" (2014):



**Minor**

**SAP Analytics**

**Course Objectives**

- To provide a comprehensive understanding of SAP ERP systems and the ABAP programming language.
- To equip students with hands-on experience in setting up and using ABAP development tools and SAP GUI.
- To develop students' skills in writing ABAP programs using fundamental programming constructs.
- To enable students to create and manage database tables and objects using ABAP Dictionary.
- To introduce students to ABAP reporting techniques and object-oriented programming concepts.
- To foster the ability to enhance, debug, and optimize SAP applications, with an introduction to S/4HANA.

**Course Outcomes**

- Describe the SAP ERP architecture and ABAP programming fundamentals.
- Explain the use of ABAP development tools and SAP GUI.
- Develop ABAP programs using data types, variables, and control structures.
- Design and manage database tables using ABAP Dictionary.
- Create and assess reports and object-oriented programs in ABAP.
- Optimize SAP applications through debugging, enhancements, and S/4HANA integration.

Unit	Details	No. of Lectures
I	<p><b>Introduction to SAP and ABAP:</b> Overview of SAP ERP system, Introduction to ABAP programming language, Understanding SAP architecture</p> <p><b>ABAP Development Environment :</b> Setting up ABAP development environment, Using ABAP workbench tools, Basics of SAP GUI (Graphical User Interface)</p> <p><b>ABAP Basics:</b> Data types and data objects, Variables, constants, and literals, Operators and expressions</p> <p><b>Control Structures:</b> Conditional statements (IF, CASE), Looping statements (DO, WHILE, FOR)</p>	
II	<p><b>ABAP Dictionary:</b> Creating and managing database tables, Data elements and domains, Table types and table maintenance</p> <p><b>Modularization Techniques:</b> Subroutines and functions, Includes and macros, Exception handling</p> <p><b>ABAP Reports:</b> Classical reports, Interactive reports, ALV (ABAP List Viewer) reports</p> <p><b>ABAP Object-Oriented Programming (OOP):</b> Classes and objects, Inheritance and polymorphism, Interfaces and abstract classes</p>	



III	<p><b>Data Retrieval Techniques:</b>Open SQL queries,Database joins,Select options and ranges</p> <p><b>Enhancements and Modifications:</b>User exits and customer enhancements,BADI (Business Add-In) and BAPI (Business Application Programming Interface),Implicit and explicit enhancements</p> <p><b>Debugging and Performance Optimization:</b>ABAP debugging techniques,Performance tuning strategies,Runtime analysis tools</p> <p><b>Introduction to S/4HANA:</b> What is S/4HANA? Overview of S/4HANA and its evolution from ECC,Key Differences: Differences between ECC and S/4HANA, including the HANA database and simplified data model.</p>
-----	---

**Reference Books:**

**For Unit 1**

1. "SAP Analytics Cloud: Getting Started" by Abassin Sidiq
2. "SAP Analytics Cloud For Dummies" by Aaron C. Q. Lee, Rachael Landry, and Jared Hanson
3. "SAP BusinessObjects BI 4.0: The Complete Reference" by Cindi Howson and Elizabeth Newbould
4. "SAP BW/4HANA: An Introduction" by Krishna Kumar Sivalingam and Surya Gummadi
5. "SAP BusinessObjects Web Intelligence: The Comprehensive Guide" by Jim Brogden, Mac Holden, and Heather Sinkwitz
6. "Crystal Reports 2020: The Complete Reference" by George Peck

**For Unit 2**

1. "SAP Analytics Cloud: An Introduction" by Matthias Wild, Xavier Hacking, and Antoine Chabert
2. "Implementing SAP Analytics Cloud" by Ryan Goodman and Vivek Aiyar
3. "SAP Lumira Essentials" by Dmitry Anoshin
4. "SAP Lumira: Beginner's Guide" by Dante Amato
5. "Predictive Analysis with SAP: The Comprehensive Guide" by Tyron McGurgan, Abassin Sidiq, and Andreas Forster
6. "SAP Predictive Analytics: Data Science and Predictive Analysis" by John MacGregor and Allen Krass





**For Unit 3**

1. "SAP Analytics for Office: The Comprehensive Guide" by Nicolas Mainusch and Anne-Christine Clauer
2. "SAP Analytics for Office: Mastering Business Intelligence Analysis" by Tyron McGurgan and Abassin Sidiq
3. SAP BW/4HANA: Data Warehousing with SAP BW/4HANA" by Dominik Schrank and Jens Rohlf
4. "SAP Data Services: The Comprehensive Guide" by Christian Savelli and Joe Pandit
5. "SAP Security: Administration, Authorization, and Auditing" by Mario Linkies, Massimo Manara, and Daniel Platten
6. "SAP BW/4HANA: Administration and Performance Optimization" by Frank Riesner and Sebastian Wenke

**Practical List**

<b>Practical</b>	<b>Content</b>
<b>1</b>	<b>Create a Simple ABAP Program:</b>  Write an ABAP program that displays "Hello, SAP World!" on the screen using the WRITE statement
<b>2</b>	<b>Define and Use Data Types:</b>  Create an ABAP program that declares a variable of type CHAR and another of type NUM. Initialize them with values and display them
<b>3</b>	<b>Conditional Statements:</b>  Write an ABAP program that uses an IF statement to check if a number is positive, negative, or zero, and displays the result.
<b>4</b>	<b>Looping Statements:</b>  Develop an ABAP program that uses a FOR loop to print numbers from 1 to 10
<b>5</b>	<b>Setup ABAP Development Environment:</b>  Explain the steps to set up the ABAP development environment in SAP GUI, including accessing the ABAP Workbench.
<b>6</b>	<b>Create a Database Table:</b>  Define a database table in the ABAP Dictionary with fields for ID, NAME, and AGE. Include data elements and domains for these fields.
<b>7</b>	<b>Write a Subroutine:</b>  Create an ABAP program that includes a subroutine to calculate the factorial of a given number. Call this subroutine from the main program
<b>8</b>	<b>Interactive Report:</b>  Develop an interactive report that displays a list of customers and allows the user to select a customer to see their details in a secondary list
<b>9</b>	<b>ALV Report:</b>



	<p>Create an ALV (ABAP List Viewer) report that displays employee data from a custom table. Use ALV to provide sorting and filtering capabilities.</p>
10	<p><b>Class Definition and Instantiation:</b></p> <p>Define a simple ABAP class with attributes for Name and Age. Include methods to set and get these attributes. Instantiate the class and demonstrate its usage</p>
11	<p><b>Open SQL Query:</b></p> <p>Write an ABAP program that retrieves and displays all records from a custom table using an Open SQL SELECT statement.</p>
12	<p><b>Database Join:</b></p> <p>Develop an ABAP program that performs a join between two tables and displays the results. Ensure that the join is based on a common key.</p>
13	<p><b>Implement a BADI:</b></p> <p>Demonstrate how to implement a BADI (Business Add-In) by creating a custom enhancement spot and implementing the associated BADI.</p>
14	<p><b>Debugging ABAP Code:</b></p> <p>Describe and execute a debugging session for an ABAP program that is not producing the expected output. Use breakpoints and watchpoints to identify the issue.</p>
15	<p><b>Debugging ABAP Code:</b></p> <p>Describe and execute a debugging session for an ABAP program that is not producing the expected output. Use breakpoints and watchpoints to identify the issue.</p>



**PG Structure and Titles as per NEP Semester IV**

**Program Name: M.Sc. Subject: IT**

**List of Papers**

(Theory: 15 Lecture hours= 1 Credit & Practical: 30 Lecture hours= 1

Credit;Change no. of hours accordingly wherever applicable)

**MAJOR/MINOR COURSE**

YEAR	Sem	Track	Theory / Practical	Paper Code	Course Title	No of Credits	No of Lectures Hours	Total Credits
2	IV	I	Theory		Deep Learning	3	45	8+4=12 (Major)
			Practical		Deep Learning Practical	1	30	
			Theory		Artificial Intelligence in Bio Informatics	3	45	
			Practical		Artificial Intelligence in Bio Informatics Practical	1	30	
			Theory		Robotic Process Automation	3	45	
			Practical		Robotic Process Automation Practical	1	30	
		II	Theory		Applied Big Data Analytics	3	45	8+4=12 (Major)
			Practical		Applied Big Data Analytics Practical	1	30	
			Theory		Data Management and Data Warehousing	3	45	
			Practical		Data Management and Data Warehousing Practical	1	30	
Theory			Programming with Hadoop and Spark	3	45			



		<b>Practical</b>	<b>Programming with Hadoop and Spark Practical</b>	<b>1</b>	<b>30</b>	
	<b>III</b>	<b>Theory</b>	<b>Cyber Forensics</b>	<b>3</b>	<b>45</b>	<b>8+4=12 (Major)</b>
		<b>Practical</b>	<b>Cyber Forensics Practical</b>	<b>1</b>	<b>30</b>	
		<b>Theory</b>	<b>Security in Cloud &amp;Other emerging Technologies</b>	<b>3</b>	<b>45</b>	
		<b>Practical</b>	<b>Security in Cloud &amp;Other emerging Technologies Practical</b>	<b>1</b>	<b>30</b>	
		<b>Theory</b>	<b>Security Operations</b>	<b>3</b>	<b>45</b>	
		<b>Practical</b>	<b>Security Operations Practical</b>	<b>1</b>	<b>30</b>	
			<b>Project/Research Paper</b>			<b>8</b>



Part-2 SEM IV Detailed Syllabus

Track 1 Artificial Intelligence

**Deep Learning**

**Course Objectives**

- Understand fundamental concepts of linear algebra including scalars, vectors, matrices, and tensors.
- Understand eigen decompositions and their application in Principal Component Analysis (PCA).
- Explore hidden units, architecture design, and optimization challenges in deep networks.
- Explore sequence modelling techniques such as recurrent neural networks (RNNs) and bidirectional RNNs.

**Course Outcomes**

- Proficiency in performing matrix operations and understanding their implications.
- Capability to apply regularization techniques effectively in deep learning projects.
- Knowledge of advanced neural network architectures and techniques for handling sequential and structured data.

Unit	Details	Lectures
1	<p><b>Applied Math and Machine Learning Basics:</b> Linear Algebra: Scalars, Vectors, Matrices and Tensors , Multiplying Matrices and Vectors, Identity and Inverse Matrices, Linear Dependence and Span, norms, special matrices and vectors, eigen decompositions. Principle Component Analysis</p> <p><b>Numerical Computation:</b> Overflow and under flow, poor conditioning, Gradient Based Optimization, Constraint optimization, History of Deep Learning, Deep Learning Success Stories</p>	15
2	<p><b>Deep feedforward Networks :</b>Example :Learning XOR , Gradient based Learning , Hidden Units , Architecture Design, Back-Propagation</p> <p><b>Regularization for Deep Learning :</b>Parameter Norm Penalties , Regularization and Under-Constrained Problems , Data Augmentation , Noise Robustness , Semi-Supervised Learning , Multi-Task Learning , Early Stopping , Dropout</p> <p><b>Optimization for Training Deep Learning :</b>How learning differs from Pure Optimization , Challenges in Neural Network Optimization , Basic Algorithm , Parameter Initialization Strategies , Algorithms with Adaptive Learning Rates , Approximate Second-Order Methods</p>	15



<b>3</b>	<p><b>Convolutional Network</b> :The convolution Operation , Pooling , Variants Of the Basic Convolution Function ,Structured Outputs , Data Types</p> <p><b>Sequence Modelling: Recurrent</b> Neural Network, Bidirectional RNNs , Encoder-Decoder Sequence to Sequence Architecture , Echo State Networks</p> <p><b>Autoencoders:</b> Undercomplete Autoencoders, Regularized Autoencoders, Stochastic Encoder and decoder, Denoising Autoencoders, Contractive Autoencoders, Application of Autoencoders.</p> <p><b>Linear Factor Models:</b> Probabilistic PCA and Factor Analysis, Independent Component Analysis (ICA), Slow Feature Analysis, Sparse Coding</p>	<b>15</b>
----------	--	-----------

**Reference books:**

1. Deep Learning - Ian Goodfellow, Yoshua Bengio, Aaron Courville - An MIT Press book - 1st - 2016
2. Fundamentals of Deep Learning - Nikhil Buduma - O'Reilly - 1st - 2017
3. Deep Learning: Methods and Applications - Deng & Yu - Now Publishers - 1st - 2013
4. Deep Learning CookBook - Douwe Osinga - O'Reilly - 1st - 2017

**SLE Topics**

History of Deep Learning, Deep Learning Success Stories  
 Shallow Neural Networks; Deep Neural Networks; Recurrent Neural Networks  
 Deep Recurrent Networks, Bidirectional RNNs  
 Autoencoders: Undercomplete Autoencoders , Regularized Autoencoders ,  
 Stochastic Encoder and decoder , Denoising Autoencoders , Contractive Autoencoders ,  
 Application of Autoencoders

**Online References:**

[https://onlinecourses.nptel.ac.in/noc21\\_cs76/preview](https://onlinecourses.nptel.ac.in/noc21_cs76/preview)

<https://in.mathworks.com/videos/deep-learning-with-matlab-transfer-learning-in-10-lines-of-matlab-code-1487714838381.html>

Practical Videos for Deep Learning: <https://www.youtube.com/watch?v=A-cklvzvKOU&t=314s>



## Practical List

Practical	Content
1	Demonstrate the following: a. scalar b. vectors c. matrix d. Performing matrix multiplication and finding eigen vectors and eigen values using Tensorflow.
2	A) Design a simple neural network with 1 input node and 1 output node. Calculate the net input (yin) and apply the binary activation function. B) Implement a neural network using both binary and bipolar sigmoidal activation functions with 2 input and 1 output node. Also, include bias
3	Consider the following feed-forward neural network. Diagram here: $x_1=0.2$ , $x_2=0.5$ , $w_{11}=0.3$ , $w_{12}=0.2$ , $w_{21}=-0.1$ , $w_{22}=0.5$ $y_1=?$ , $y_2=?$ Find the net input $y_{in1}$ and $y_{in2}$ apply bipolar activation function and display the output of $y_1$ and $y_2$ .
4	Solving XOR problem using a deep feed-forward network
5	Deep neural network for performing binary classification
6	A) deep feedforward network with 2 hidden layers for performing multiclass classification and predicting the class. B) deep feedforward network with 2 hidden layers for performing multiclass classification and predicting the probability class
7	A) Hebb network to implement logical AND function. Delta rule network to implement logical OR function with bipolar inputs and targets
8	Deep feedforward network with 2 hidden layers for performing linear regression and predicting values.
9	Regularization to avoid over-fitting in binary classification

### Track 1 Artificial Intelligence

#### Artificial Intelligence in Bio Informatics

##### Course Objectives:

- This course introduces the concepts and state-of-the-art research in bioinformatics, data mining and AI especially for medical application.

##### Course Outcomes: Upon completion of the course, the learners will be able to:

- Understand the concepts of molecular biology, DNA analysis with respect to data processing.
- Analyze biological sequences and score matrices with respect to data processing.
- Implement data mining algorithms on microarray, gene expression, feature selection for proteomic and genomic data.
- Understand ethics in using bioinformatics.
- Apply AI in medical field for development of contributive solutions.
- Investigate state-of-the-art research and developments in bioinformatics.



Unit	Details	No. of Lectures
1	<p><b>Introduction to Bioinformatics and Data Mining;</b> Molecular Biology background: Analysing DNA; Bioinformatics perspective of how individuals of a species differ and how different species differ; Bioinformatics challenges and opportunities</p> <p><b>Biological Sequence Analysis:</b> DNA sequence analysis; DNA databases; Protein structure and function; Protein sequence databases; Sequence alignment; Sequence comparison, Sequence similarity search; Longest common subsequence problem; Scoring matrices for similarity search PAM, BLOSUM, etc</p>	15
2	<p><b>Mining Biological Data</b> Protein structural classification; Protein structural prediction; Modeling text retrieval in biomedicine; Mining from microarray and gene expressions; Feature selection for proteomic and genomic data mining</p> <p><b>Ethics in Bioinformatics</b> Ethical and social challenges of electronic health information; Public access to anatomic images; Evidencebased medicine; Outcome measures and practice guidelines for using data mining in medicine; Computer assisted medical and patient education.</p>	15
3	<p><b>AI in Medical Informatics</b> Infectious disease informatics and outbreak detection; Identification of biological Relationships from text documents; Medical expert systems; Telemedicine and tele surgery; Internet grateful med (IGM).</p> <p><b>Case Studies</b> and recent research in application of artificial intelligence in bioinformatics.</p>	15

**Reference Text Books:**

1. S. Rastogi, N. Mendiratta and P. Rastogi, Bioinformatics: Methods and Applications: Genomics, Proteomics and Drug Discovery, PHI.
2. Z. Ghosh, B. Mallick, Bioinformatics: Principles and Applications, Oxford University Press.
3. J. Chen and S. Lonardi, Biological Data Mining, Chapman and Hall/CRC.
4. V. Buffalo, Bioinformatics Data Skills, O'Reilly Publishing.
5. H. Zengyou, Data Mining for Bioinformatics Applications, Woodhead Publishing.
6. L. Low, Bioinformatics: A Practical Handbook of Next Generation Sequencing and its Applications, World Scientific Publishing.
7. M. Model, Bioinformatics Programming Using Python, O'Reilly Publishing

**SLE Topics**

**Ethics in Bioinformatics**

Ethical and social challenges of electronic health information.

**Case Studies**

Recent research in application of artificial intelligence in bioinformatics.



**Online References:**

<https://www.youtube.com/watch?v=2zLn-RngMU4>  
<https://nptel.ac.in/courses/102103044>

**Practical List**

Practical	Content
1	Practical based on Data Pre-processing and Cleaning
2	Practical based on Sequence Analysis
3	Practical based on Predictive Modeling
4	Practical based on CNN, RNN and LSTM
5	Practical based on Network Analysis
6	Practical based on Systems Biology
7	Practical based on Text Mining
8	Practical based on Literature Analysis
9	Practical based on Biological Data Visualization

**Track 1 Artificial Intelligence****Robotic Process Automation****Course Objectives**

- Understand the scope and techniques of robotic process automation (RPA).
- Gain proficiency in using UiPath Studio for creating automation workflows.
- Explore controls and actions on controls including mouse and keyboard activities.
- Understand the process of deploying and maintaining UiPath bots, including publishing and using orchestration servers.

**Course Outcomes**

- Proficiency in recording and playing back automation tasks using UiPath Studio.
- Capability to integrate UiPath with different applications using plugins and extensions.
- Understanding of OCR (Optical Character Recognition) usage and handling typical failure points
- Understanding of deployment strategies and maintenance procedures for UiPath bots in production environments.



Unit	Details	No of Lectures
1	<p><b>Robotic Process Automation:</b> Scope and techniques of automation, About UiPath.</p> <p><b>Record and Play:</b> UiPath Stack, Downloading and installing UiPath Studio, Learning UiPath Studio, Task Recorder, Step-by-step examples using the recorder.</p> <p><b>Sequence, Flowchart, and Control Flow:</b> Sequencing the workflow, Flowchart, State Machine, Activities, Control flow, various types of loops and decision making.</p>	15
2	<p><b>Data Manipulation:</b> Variables and scope, Collections, Arguments – Purpose and use, Data table usage with examples, Clipboard management, File operation with step-by-step example, CSV/Excel to datatable and vice versa.</p> <p><b>Controls and Act on controls</b> – Finding and attaching windows, mouse and keyboard activities, Working with UiExplorer, Handling events , Screen Scraping, When to use OCR, Types of OCR available, How to use OCR, Avoiding typical failure points</p> <p><b>Tame that Application with Plugins and Extensions:</b> Terminal plugin, Java plugin, Citrix automation, Mail plugin, PDF plugin, Web integration, Excel and Word plugins, Credential management, Extensions – Chrome and Firefox,</p>	15
3	<p><b>Handling User Events and Assistant Bots:</b> What are assistant bots?, Monitoring system event triggers, Hotkey trigger, Mouse trigger, System trigger , Launching an assistant bot on a keyboard event.</p> <p><b>Exception Handling, Debugging &amp; Logging:</b> Exception handling, Common exceptions and ways to handle them, Logging and taking screenshots, Debugging techniques, Collecting crash dumps.</p> <p><b>Managing and Maintaining the Code &amp; Deploying and Maintaining the Bot:</b> Project organization, Nesting workflows, Reusability of workflows, Commenting techniques, State Machine, Publishing using publish utility, Overview of Orchestration Server, Using Orchestration Server to control bots.</p>	15



**SLE TOPICS**

How RPA works?, Step-by-step example using Sequence and Flowchart, Step-by- step example using Sequence and Control flow, ROI for RPA, RPA Implementation in Enterprise. Case Study Introduction Henn Na Hotel in Tokyo Japan.

Finding the control, Techniques for waiting for a control, Web integration, SAP Automation, Extensions Java and Silverlight, Monitoring Email, Example of monitoring a copying event and blocking it.

When to use Flowcharts, State Machines, or Sequences. Using Orchestration Server to deploy bots, License management, Publishing and managing updates.

**Reference Books:**

1. Learning Robotic Process Automation, Alok Mani Tripathi, Packt, first edition, 2018
2. Robotic Process Automation Tools, Process Automation and their benefits: Understanding RPA and Intelligent Automation, Srikanth Merianda, Create space Independent Publishing, first edition, 2018.
3. The Simple Implementation Guide to Robotic Process Automation (Rpa): How to Best Implement Rpa in an Organization, Kelly Wibben meyer, iUniverse, first edition, 2018.

**Online Sources**

1. <https://www.udemy.com/course/uipath-robotic-process-automation/>
2. <https://www.uipath.com/resources/all>
3. <https://docs.uipath.com/activities/other/latest>
4. <https://forum.uipath.com/t/uipath-documentation/16123>
5. <https://www.uipath.com/learning/video-tutorials>

**Practical List**

Practical	Content
1.	Perform the following : a. Create a simple sequence based project. b. Create a flowchart-based project
2.	Create an UiPath Robot which can empty a folder in Gmail solely on basis of recording.
3.	Automate UiPath Number Calculation (Subtraction, Multiplication, and Division of numbers).
4.	Create an automation UiPath project using different types of variables (number, date time, Boolean, generic, array, and data table).
5.	Perform the following : a. Create an automation UiPath Project using decision statements. b. Create an automation UiPath Project using looping statements.



6.	<p>Perform the following :</p> <ol style="list-style-type: none"> <li>Automate any process using basic recording.</li> <li>Automate any process using desktop recording.</li> <li>Automate any process using web recording.</li> </ol>
7.	<p>Consider an array of names. We have to find out how many of them start with the letter "a". Create an automation where the number of names starting with "a" is counted and the result is displayed.</p>
8.	<p>Perform the following</p> <ol style="list-style-type: none"> <li>Create an application automating the read, write and append operation on excel file.</li> <li>Automate the process to extract data from an excel file into a data table and vice versa.</li> </ol>
9.	<p>Perform the following</p> <ol style="list-style-type: none"> <li>Implement the attach window activity.</li> <li>Mouse (click, double click and hover)</li> <li>Type into.</li> <li>Type Secure</li> </ol>
10.	<p>Perform the following</p> <ol style="list-style-type: none"> <li>Automate the process of send mail event (on any email).</li> <li>Automate the process of launching an assistant bot on a keyboard event.</li> </ol>
11.	<p>Perform the following</p> <ol style="list-style-type: none"> <li>Automate the process of logging and taking screenshots in UiPath.</li> <li>Automate any process using State Machine in UiPath.</li> </ol>

**Track 1 Artificial Intelligence**

**Applied Big Data Analytics**

**Objective of the course:**

- This course covers the concept of big data analytics, algorithms, applications and frameworks.

**Course Outcomes:**

- Students will do the detailed study of big data analytics and able to apply in practical problems.
- Student must be Able to understand the building blocks of Big Data.
- Student must be able to articulate the programming aspects (map Reduce etc.
- Student must be able to understand the specialized aspects of big data with the help of different big data applications
- Student must be able to represent the analytical aspects of Big Data.
- Student must be know the recent research trends related to Hadoop File System, MapReduce and Google File System etc.
- Ability to apply analytics techniques to analyze and interpret the data.



- Ability to perform descriptive, predictive and prescriptive analytics.

Unit	Details	No. of Lectures
1	<p><b>Introduction to Big Data Analytics:</b> What is Analytics? What is Big Data? Characteristics of Big Data , Analytics Flow for Big Data, Big Data Stack</p> <p><b>Domain Specific Examples of Big Data:</b> Web ,Financial, Healthcare ,Internet of Things , Environment Logistics &amp; Transportation Industry Retail</p> <p><b>Big Data Patterns:</b> Analytics Architecture Components &amp; Design Styles, MapReduce Patterns. Setting up Big DataStack: Hortonworks Data Platform (HDP) , Cloudera CDH Stack , Amazon Elastic MapReduce (EMR) Azure HDInsight.</p> <p><b>Data Acquisition and Analysis :</b> Data Acquisition Considerations, Publish - Subscribe Messaging Frameworks, Big Data Collection Systems, Messaging Queues, Custom Connectors, Steps of Data Analysis, Descriptive Analysis, Predictive Analysis, Predictive Analysis Methods.</p>	15
2	<p><b>Big Data Storage:</b> HDFS Architecture, HDFS Usage Examples</p> <p><b>Real-time Analysis:</b> Stream Processing, In-Memory Processing, Real-time data collection system Real-time data streaming tools and technologies and data processing</p> <p><b>Interactive Querying:</b> Spark SQL, Hive, Amazon Redshift, Google BigQuery</p> <p><b>Serving Databases &amp; Web Frameworks:</b> Relational (SQL) Databases, Non-Relational (NoSQL) Databases, Python Web Application Framework – Django , Real-time Sensor Data Analysis , Real-time Twitter Sentiment Analysis,Django application.</p>	15
3	<p><b>Analytics Algorithms:</b> Frameworks, Supervised Learning, Unsupervised Learning, Collaborative Filtering Clustering, Classification &amp; Regression, Recommendation Systems</p> <p><b>Data Visualization:</b> Frameworks &amp; Libraries, Visualization Examples.</p> <p><b>Genome Data Analysis</b> (Implementation), Recommendation Systems, Alternating Least Squares (ALS) , Singular Value Decomposition (SVD), Classifying Handwritten Digits.</p> <p><b>Descriptive, Predictive and Prescriptive analytics:</b> Description and implementation, Why should real-time data analytics solutions offer exhaustive data and a personalized approach?</p>	15



**REFERENCE BOOKS**

1. Data Analytics Practical Guide, Arthur Zhang
2. Big Data Analytics : A Hands on Approach, Anshdeep Bagha and Vijay Madiseti
3. Big Data in Practice, Bernard Marr

**SLE TOPICS**

Setting up Big Data Stack: Hortonworks Data Platform (HDP) , Cloudera CDH Stack , Amazon Elastic MapReduce (EMR) Azure HDInsight
The Effects of Predictive Analytics on Real Estate, The National Association of Realtors (NAR) and Its Use of Predictive Analytics, The Revolution of Predictive Analysis across a Variety of Industries
Case Studies : Real-time Sensor Data Analysis , Real-Time Parking Sensor Data Analysis for Smart Parking System , Real-time Twitter Sentiment Analysis, Windowed Analysis of Tweets , Django application for viewing weather data, Batch Analysis of News Articles,
Case Study: Genome Data Analysis (Implementation), Recommendation Systems, Alternating Least Squares (ALS) , Singular Value Decomposition (SVD), Classifying Handwritten Digits

**Practical list**

Practical	Content
1.	Processing data generated by social media platform(raw data fetching)
2	Write a Python / R program to pick the content for Bill Boards from the givendata
3	Write a Python program to process the balance sheet to ensure that only gooddata is processing.
4	Collecting and ingesting data from various sources into the big data storage using Data Access Connectors.
5	Implement an application that stores big data in Mongo DB and manipulate using R and Python.
6	Analyzing Instagram App Reviews
7	Data visualization using pygal / Creating data model using Cassandra
8	Pig Latin scripts to sort, group, join, project, and filter your data
9	Real time Analysis using Apache Storm
10	Writing interactive Query using BigQuery



Track 2 Data Science

**Data Management and Data Warehousing**

**Course Objectives:**

- Understand the concept and framework of data warehousing and differentiate between OLAP and OLTP.
- Gain knowledge of data mining techniques and their applications in knowledge discovery.
- Acquire skills in data preprocessing, including handling missing data, cleaning, integration, and transformation.
- Apply association rules mining algorithms such as APRIORI and FP-Growth to discover frequent item sets.

**Course Outcomes**

- Explain the purpose and components of a data warehouse and differentiate it from transactional databases.
- Perform OLAP operations on a multidimensional data model to analyze and query data.
- Implement data preprocessing techniques to address missing data and prepare the data for mining.
- Apply association rules mining algorithms to discover patterns and relationships in large datasets.

Unit	Content	No. of Lectures
1	<p><b>Introduction to Data Mining:</b> Need of Data Mining, What Can Data Mining Do and Not Do? Data Mining Applications, Data Mining Process, Data Mining Techniques</p> <p><b>Data Preprocessing:</b> Need for Data Preprocessing, Data Preprocessing Methods, Data cleaning, Data integration, Data transformation, Data reduction</p> <p><b>Classification:</b> Types of Classification, Working of Classification, Guidelines for Size and Quality of the Training Dataset, Introduction to the Decision Tree Classifier, Naïve Bayes Method.</p> <p><b>Data warehouse:</b> The Need for an Operational Data Store (ODS) , Operational Data Store , Data warehouse , Data Marts</p>	15

<p style="text-align: center;"><b>2</b></p>	<p><b>Data Warehouse Schema:</b> Introduction to Data Warehouse Schema , Star Schema, Snowflake Schema ,Fact Constellation Schema (Galaxy Schema) , Comparative Study of Data Warehouse with OLTP and ODS Data warehouses versus OLTP: similarities and distinction Comparison among Star, Snowflake and Fact Constellation Schema</p> <p><b>Cluster Analysis:</b> Applications of Cluster Analysis , Desired Features of Clustering, Distance Metrics, Major Clustering Methods/Algorithms,Partitioning Clustering, Hierarchical Clustering Algorithms</p> <p><b>Association Rule Mining:</b> Defining Association Rule Mining, Representations of Items for Association Mining, The Metrics to Evaluate the Strength of Association Rules , The NaïveAlgorithm for Finding Association Rules, Approaches for TransactionDatabase Storage, The Apriori Algorithm, , Closed and Maximal Itemsets , The Apriori–TID Algorithm</p>	<p style="text-align: center;"><b>15</b></p>
---	--	--





3	<p><b>Web mining and search engines:</b> Introduction ,Web Content Mining , Web Usage Mining , Web Structure Mining, Introduction to Modern Search Engines, Working of a Search Engine, PageRank Algorithm , Precision and Recall</p> <p><b>NoSQL:</b> The Rise of Relational Databases, Major Issues with Relational Databases, Challenges from the Internet Boom, Possible Solutions to Handle Huge Amount of Data, The Emergence of Technologies for Cluster Environment, Birth of NoSQL, Defining NoSQL from the Characteristics it Shares, Data Models of NoSQL, Future of NoSQL, Recent applications of data mining methods; Decision support system (DSS) and its components, Knowledge discovery from data, Difference between NoSQL and Relational Data Models (RDBMS)</p>	15
---	---	----

**Reference Books:**

- 1 . Data Warehousing: Design, Development And Best Practices by Soumendra Mohanty (Author), Tata McGraw Hill Education (Publisher).
2. Jiawei Han, Michelin Kamber, “Data Mining-Concepts and techniques”, Morgan Kaufmann Publishers, Elsevier, 3rd Edition.
3. Alex Berson, Stephen J.Smith, “Data warehousing Data mining and OLAP”, Tata McGraw- Hill, 2nd Edition.
- 4.

**Additional Reference(s):**

1. Arum K Pujari, “Data Mining Techniques”, 3rd Edition, Universities Press, 2005
2. PualrajPonnaiah, Wiley, “Data Warehousing Fundamentals”, Student Edition, 2004.
3. Ralph Kimball, Wiley, “The Data warehouse Life Cycle Toolkit”, Student Edition, 2006.

**SLE topics**

SLE Topic
Understanding Metrics to Assess the Quality of Classifiers : The boy who cried wolf , True positive , True negative , False positive ,False negative , Confusion matrix ,Precision , Recall , F-Measure
Implementing Clustering with Weka and R: Handling Missing Values, Results Analysis after Applying Clustering, Classification of Unlabeled Data, Clustering in R using Simple k-Means
Comparative Study of Data Warehouse with OLTP and ODS Data warehouses versus OLTP: similarities and distinction, Comparison among Star, Snowflake and Fact Constellation Schema
Recent applications of data mining methods; Decision support system (DSS) and its components, Knowledge discovery from data, Difference between NoSQL and Relational Data Models (RDBMS)



Online Resources
<a href="http://nptel.ac.in/courses/106106093/35">http://nptel.ac.in/courses/106106093/35</a> 2. <a href="http://nptel.ac.in/syllabus/syllabus_pdf/106106105.pdf">http://nptel.ac.in/syllabus/syllabus_pdf/106106105.pdf</a> 3. <a href="http://nptel.ac.in/video.php?subjectId=106106093">http://nptel.ac.in/video.php?subjectId=106106093</a> 4. <a href="http://textofvideo.nptel.iitm.ac.in/video.php?courseId=106106093&amp;p=4">http://textofvideo.nptel.iitm.ac.in/video.php?courseId=106106093&amp;p=4</a>

**Practical list:**

Practical	Content
1	Implementing Classification using decision tree in Weka used iris dataset
2	Write a code using R language to read the dataset iris, display all the data and plot the graph of complete data set
3	Understanding Weka, read iris dataset in Weka and show the analysis and histogram of dataset and also remove 1 column from the dataset and again display the data in graph.
4	Implementing Classification in R (Decision Tree)
5	Write a code using R language to read the dataset diabetes, display all the data and plot the graph of complete data set
6	Implementing Clustering with R (K-means Clustering).
7	Implementing Classification in Weka (Naïve Bayes).
8	Implementing Classification in python (Decision Tree)
9	Implementing Classification in Weka (Naïve Bayes) used whether nominal dataset
10	Implementing Classification in Weka (Decision Tree) used iris dataset
11	Implementing Classification in python (Naïve Bayes)



**Track 2 Data Science**

**Programming with Hadoop and Spark**

**Course Objective**

- Understand the fundamentals of Big Data, including its characteristics and challenges.
- Develop practical skills in setting up a Hadoop environment and performing basic operations.
- Understand advanced concepts and optimization techniques in MapReduce.
- Dive deeper into Spark SQL, DataFrames, and Datasets for advanced data processing.

**Course Outcomes**

- Proficiency in explaining the architecture and components of the Hadoop ecosystem.
- Capability to set up Spark in standalone and cluster mode and develop Spark applications.
- Competence in building Spark applications for data processing and analysis.
- Competence in designing and implementing end-to-end Big Data solutions using Hadoop and Spark, including data collection, processing, analysis, and visualization, with considerations for performance optimization and scalability.

Unit	Details	No. of Lectures
1	<p><b>Introduction to Big Data and Hadoop Ecosystem</b>                      Big Data Fundamentals Understanding Big Data: Characteristics and Challenges                      Overview of Big Data Technologies Introduction to Distributed Systems Hadoop                      Ecosystem and Architecture, Overview of the Hadoop Ecosystem, Hadoop                      Distributed File System (HDFS): Concepts, Architecture, and DataFlow, Introduction                      to YARN (Yet Another Resource Negotiator) Working with Hadoop, Setting up a                      Hadoop Environment, Basic HDFS Operations: File System Shell Commands                      Introduction to MapReduce: Concepts and Workflow, Hands-On Exercise:                      Implementing a Simple MapReduce Program, Writing and Running a Basic                      MapReduce Java Program, Analyzing MapReduce Job Logs</p>	15
2	<p><b>Advanced Hadoop Features and Introduction to Spark</b>                      Advanced Hadoop Processing, Understanding Advanced MapReduce                      Concepts, Optimizing MapReduce Jobs, Data Ingestion into HDFS: Flume and                      Sqoop Introduction to Apache Spark, Spark vs. Hadoop: Understanding the                      Differences Spark Ecosystem and Components: Spark Core, Spark SQL, Spark                      Streaming, MLlib, GraphX, Setting Up Spark: Standalone and Cluster Mode                      Basics of Spark Programming</p>	15



	Understanding RDDs (Resilient Distributed Datasets), Transformations and Actions in Spark, Developing Spark Applications Using Spark Shell, Hands-On Exercise: Building a Spark Application, Creating a Spark Application to Process Data, Analyzing Data with Spark SQL	
3	<p><b>Advanced Spark Programming and Data Processing</b></p> <p>Advanced Spark Data Processing, Deep Dive into Spark SQL: Data Frames and Datasets, Data Aggregation and Analysis, Introduction to Data Frames Operations and SQL Queries Streaming Data Processing with Spark , Understanding Spark Streaming: Concepts and Architecture, Processing Real-Time Data Streams, Window Operations and Stateful Stream Processing Machine Learning with Spark MLlib, Overview of Machine Learning Concepts, Introduction to MLlib: Machine Learning Library in Spark, Building a Simple Machine Learning Model with Spark</p> <p><b>Hands-On Project:</b></p> <p>End-to-End Big Data Solution, Designing and Implementing a Complete Data Processing Pipeline Using Hadoop and Spark, Real-World Data Collection, Processing, Analysis, and Visualization, Performance Optimization and Scalability Considerations</p>	15

**REFERENCE BOOKS**

1. Big Data Analytics with Hadoop 3, Pakt
2. Big Data Analytics with Spark, Apress

**Self-Learning Topic (Unit Wise)**

Topic
Scientific Computing and Big Data Analysis with Python and Hadoop : Installing standard Python, Installing Anaconda , Using Conda
Statistical big data with r and Hadoop: Install R on workstations and connect to the data in Hadoop Install R on a shared server and connect to Hadoop, Utilize Revolution R Open Execute R inside of MapReduce using RMR2 Summary and outlook for pure open source options
Monitoring Spark Application: jobs launched by application, stages in Job, Environment, Spark Streaming Application, Spark SQL Queries Built-in Functions, UDFs and UDAFs , Interactive Analysis with Spark SQL JDBC Server, An Example of MLib Application, Spark ML, An example of Spark ML Application

**Online Resources**

[http://nptel.ac.in/syllabus/syllabus\\_pdf/106106105.pdf](http://nptel.ac.in/syllabus/syllabus_pdf/106106105.pdf) 3.

**Practical List**

01.	PySpark Data Reading and Display Example.
02.	Combining Data Frames with PySpark.
03.	Collect, filter, map, MapReduce example using PySpark.
04.	Creating a spark session using the configuration and Data frame creation.
05.	PySpark Word Count and Data Manipulation Example.
06.	Real-Time Word Count with PySpark Streaming.
07.	Creating a temporary view of data frame to use sql query with Spark session.
08.	Creating User defined function with spark session.
09.	PySpark using ml lib library working with linear regression.
10.	PySpark using ml lib library working with logistics regression.
11.	PySpark using ml lib library working with Naive Bayes.
12.	PySpark using ml lib library working with k mean clustering.
13.	Case Study



### Track 3 Cyber Security

## Cyber Forensics

### Course Objective

- Understand the present scenario of cyber forensics and its importance in investigation processes.
- Develop skills in acquiring and duplicating data, recovering deleted files and partitions, and using forensic tools like Access Data FTK and Encase.
- Learn about different types of audits, including remote, onsite, and human interaction audits.
- Learn about other frameworks relevant to cybersecurity, risk management, and IT governance

### Course Outcome

- Capability to perform data acquisition, duplication, and recovery of deleted files and partitions.
- Competence in analyzing steganography, image files, and cracking application passwords in forensic investigations.
- Proficiency in planning, initiating, and conducting audits, including document review and evidence verification.
- Proficiency in evaluating and selecting appropriate frameworks based on organizational needs and industry standards.

Unit	Details	No. of Lectures
1	<b>Introduction to Cyber Forensics</b> The present Scenario, The Investigation Process, Computers – Searching and Seizing, Electronic Evidence, Procedures to be followed by the first responder. Setting up a lab for Computer Forensics, Hard Disks and File Systems, Forensics on Windows Machine, Acquire and Duplicate Data Recovery of deleted files and partitions, Using Access Data FTK and Encase for Forensics Investigation, Forensics analysis of Steganography and Image files, Cracking Application passwords.	15



<p style="text-align: center;"><b>2</b></p>	<p><b>Auditing</b>  <b>ISO 19011:2018</b> : Plan, Do, Check, Act Cycle ,Overview of Management Systems &amp; Certification Body , Accredited certification vs Unaccredited Certification/body, Overview of Clauses &amp; Annex A Guidelines; Auditing terms and definitions; Types of Audit - Remote, Onsite, Human Interaction, Non-Human Interaction; Types of Audit - First Party, Second Party, Third Party; Types of Audit - Stage 1 Audit, Stage 2 Audit; Audit sequence (Input, Activity, Output);Audit process (Audit Criteria, Audit Evidence, Evaluation, Audit Findings, Audit Conclusion);Audit resources; Audit responsibilities (Lead Auditor, Audit Team Member, Auditee Top Management, Guides, Management Representative, Technical Experts);Audit evidence triangle (Document Review, Interview, Observation);Audit programme &amp; activities; Audit scope, objectives and criteria; Principles of auditing; Typical audit activities; Planning the Audit; Initiating the audit; Document review; Auditing programming; Audit plan and sampling;</p>	<p style="text-align: center;"><b>15</b></p>
---	---	--



	Audit work documents; Opening meeting; Communication, attributes and question types; Verifying information and recording evidence; Nonconformities; Simulated internal audit; Documenting nonconformities; Preparing audit conclusions; Presenting nonconformities; Closing meeting; Audit report contents; Closing an Audit;SSAE	
3	<p><b>Introduction to Frameworks</b></p> <p>Study of features of : ISO 27001:2013 , ISO 27701:2019, , ISO 22301:2019, ISO 31000:2018</p> <p>Study of features of: NIST 800-53,14,26,12 Cybersecurity Framework, SOC1 SOC2 SOC3 Study of features of :CCISv7, COSO, features of ITILv4, CMMI, Cloud Control Matrix (CCM)v4’, features of COBIT5, COBIT 2019, Compare and contrast of different ISO frameworks , Compare and contrast of different Cloud frameworks</p>	15

**Reference Books:**

1. EC-Council CHFIv10 Study Guide, EC-Council, 2018
2. The official CHFI Exam 312-49 study Guide, Dave Kleiman, SYNGRESS, 2007
3. Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing, 2020 4) Cyber Security and Cyber Laws Nilakshi Jain (Author), Ramesh Menon (Author) Publisher : Wiley (1 October 2020); ISBN-13 : 978-9390395750

**Self-Learning topics**

<b>Topic</b>
The present Scenario, The Investigation Process, Electronic Evidence
Hard Disks and File Systems
ISO 27701:2019, ISO 22301:2019
NIST 800-,14,26,12,SOC1 SOC2 SOC3
Study of features of :CCISv7, COSO,CMMI, Cloud Control Matrix (CCM)v4’, COBIT 2019, Compare and contrast of different ISO frameworks , Compare and contrast of different Cloud frameworks

**Online Resources**

<https://youtu.be/5hjsrWiXTqY>



**Practical List:**

<b>Practical</b>	<b>Content</b>
<b>1</b>	File System Analysis Using Autopsy
<b>2</b>	File System Analysis Using The Sleuth Kit (TSK)
<b>3</b>	Identifying and Extracting Malware
<b>4</b>	Getting an Image Ready for Examination
<b>5</b>	Viewing an Image on a Windows, Linux and Mac Forensic Workstations
<b>6</b>	Using Xplico for Network Forensics
<b>7</b>	Imaging using DCFLDD and XXD
<b>8</b>	Using Bulk Extractor
<b>9</b>	Mock Stage 1 Audit (Document Review) per ISO 19011 & ISO 27001 for Fictitious Organization
<b>10</b>	Mock Stage 2 Audit per ISO 19011 & ISO 27001 for Fictitious Organization



Track 2 Cyber Security

**Security in Cloud & other Emerging Technologies**

**Course Objectives**

- Learn about cloud security concepts, including cryptography, access control, and network security.
- Understand cloud reference architecture, including categories (SAAS, IAAS, PAAS) and deployment models (Public, Private, Hybrid, Community).
- Explore data security concepts in cloud environments, including data lifecycle management, encryption, and data classification.
- Gain knowledge of hardware and network security configurations, incident management, and emerging technologies' impact on cloud security.

**Course Outcomes**

- Competence in understanding and implementing various cloud reference architecture categories and deployment models.
- Capability to implement data security measures such as encryption, data classification, and data lifecycle management in cloud environments.
- Skill in understanding and applying security concepts to emerging technologies and analyzing case studies related to cloud security.

Unit	Details	No. of Lectures
1	<p><b>Cloud Architecture : Concept and Design</b>  <b>Understanding Cloud concepts:</b> Glossary of definitions, Roles of Service: Customer ,Provider ,Broker and partner                      Characteristics of :Multitenancy, Elasticity, Scalability, Resource Pooling                      Block, Technologies: Virtualization, Storage, Networking, Databases and orchestration  <b>Security Concept in Cloud Computing:</b> Cryptography and key management, Access Control, Data Sanitization and operations. , Network Security, Virtualization Security: Hypervisor Security and Container Security.</p> <p><b>Overview of design principles of secure cloud computing :</b> Secure Data Lifecycle , Disaster Recovery , Business Continuity Planning , Cost Benefit Analysis , Portability and inter-operability , Vendor Locking , Security Considerations for SAAS, IAAS, PAAS</p> <p><b>Evaluating Cloud Service providers :</b> Verification against criteria (eg: ISO27001, PCIDSS) , Product Certifications (e.g.: Common criteria(cc) , FIPS140-2)</p> <p><b>Overview cloud reference architecture :</b> Categories: SAAS, IAAS, PAAS , Deployment models: Public, Private, Hybrid, Community</p>	15



<p>2</p>	<p><b>Cloud Platform and Infrastructure security</b> :Infrastructure Components:Physical environments, Management , Plane (Scheduling, Orchestration, Maintenance ) , Secure Data Centre Design: Logical, Physical and environmental , Risk analysis and assessment, Virtualization Risks, Vulnerabilities, Threats, Attacks, Counter measures , Disaster recovery and business continuity : a)Business Requirements (e.g., Recovery Time Objective (RTO) , Recovery Point Objective (RPO), Recovery Service Level(RSL)) b)Strategy and Planning of DR and BC</p> <p><b>Cloud data security</b> : Data Lifecycle, Data Dispersion, Storage types, Data Classification, Data Discovery(Structured and Unstructured data) Encryption and Key management, Data Loss prevention, Hashing, Masking, Tokenization, Obfuscation, Anonymization Data Rights, Provisioning, Access Models , Data Retention ,Deletion, Archiving , Event sources, Identity Attribution , Logging, Storage and Analysis of Data Events Chain of Custody and Non-repudiation</p>	<p>15</p>
<p>3</p>	<p><b>Cloud Application Security:</b> Secure SDLC process , Common Cloud Vulnerabilities, Phases and Methodologies, Software Configuration Management and Versioning, Security Testing, Overview of secure Components e.g., Web Application Firewall (WAF), Database Activity Monitoring (DAM), Extensible Markup Language (XML) firewalls, Application Programming Interface (API) gateway. Identity and Access Management (IAM) Solutions e.g.(Federated Identity, Identity Providers, Single Sign-On (SSO), Multi-factor Authentication, Cloud Access Security Broker (CASB))</p> <p><b>Cloud Security operations</b> : Hardware Security Configuration(BIOS, TPM, Controllers),Virtualization Tools(Network, Storage, CPU, Memory),Guest OS , Access Control(Secure KVM,RDP,SSH),Secure Network Configuration(VLAN, TLS, DHCP, DNS, VPN), Network Security Controls(IDS,IPS),Network Security Groups, OS Hardening through baselines, backup and restore , Management of Change, Continuity, Security,Incident,Problem,Release,Deployment,Configuration,Availability,Capacity, Service Level</p> <p><b>Impact of Emerging Technologies</b> : (AI/ML/DL/Data Science) Application of Security concepts to therespected technologies a)Developer/Defender b)Attacker ,Case Studies</p> <p>Discussion on the following Technologies (IoT/Automation/Quantum Computing/BlockChain/SpaceTechnologies/ICS(IndustrialControlSystems)/Co ntainerization/VR/AR/IR/3D Printing/Drones)</p>	<p>15</p>

**Reference books:**

1. Official (ISC) <sup>2</sup> CCSP Study Guide, Second Edition  
<https://cyberstartupobservatory.com/cyber-security-next-generation-challenges-threatsand-defense/>
2. Cybersecurity Issues in Emerging Technologies By Leandros Maglaras, Ioanna Kantzavelou ISBN 9780367626174 October 15, 2021 Forthcoming by CRC Press



3. Space Security: Emerging Technologies and Trends (First)Publisher : K W Publishers
4. Pvt Ltd; First edition (15 January 2017) ISBN-13 : 978-9386288356

**SLE TOPICS**

<b>Topic</b>
Glossary of definitions, Roles of Service: Customer ,Provider ,Broker and partner Characteristics of :Multitenancy, Elasticity, Scalability, Resource Pooling Block, Technologies: Virtualization, Storage, Networking, Databases and orchestration
Access Control, Data Sanitization and operations. ,Network Security
Business Continuity Planning ,Portability and inter-operability Security Considerations for SAAS,IAAS,PAAS
Product Certifications(e.g.: Common criteria(cc) , FIPS140-2)
Categories: SAAS, IAAS,PAAS , Deployment models: Public, Private, Hybrid, Community
Physical environments, Management , Plane (Scheduling, Orchestration, Maintenance Business Requirements (e.g., Recovery Time Objective (RTO) , Recovery Point Objective (RPO), Recovery Service Level (RSL))
Data Lifecycle, Data Dispersion, Storage types, Data Classification, Data Discovery(Structured and Unstructured data), Hashing, Event sources
Secure SDLC process, Phases and Methodologies, Software Configuration Management and Versioning, Security Testing, Solutions e.g.(Federated Identity, Identity Providers, Single Sign-On (SSO), Multi-factor Authentication, Cloud Access Security Broker (CASB))
backup and restore , Management of Change, Continuity, Security, Incident ,Problem, Release, Deployment ,Configuration, Availability, Capacity, Service Level
Discussion on the following Technologies (IoT/Automation/Quantum Computing/BlockChain/SpaceTechnologies/ICS(IndustrialControlSystems)/Contain erization/VR/AR/IR/3D Printing/Drones)

<b>Online Resources</b>
<a href="https://www.japcc.org/cybersecurity-challenges-with-emerging-technologies/">https://www.japcc.org/cybersecurity-challenges-with-emerging-technologies/</a>
<a href="http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_sys temic_risk_2020.pdf">http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_sys temic_risk_2020.pdf</a>

**Practical List:**

<b>Practical</b>	<b>Content</b>
<b>1</b>	Design and implement security monitoring.
<b>2</b>	Design and implement security alerting.
<b>3</b>	Design and implement logging solution.
<b>4</b>	Design and implement secure network infrastructure.
<b>5</b>	Design and implement host-based security.
<b>6</b>	Design and implement key management and use.
<b>7</b>	Design and implement data encryption solution for data at rest
<b>8</b>	Design and implement data encryption solution for data in transit.
<b>9</b>	Designing a cloud setup
<b>10</b>	Understanding cloud privacy policy



**Track 3 Cyber Security**  
**Security Operations**

**Course Objective**

- Understand the CIA Triad (Confidentiality, Integrity, and Availability) and common cybersecurity threats.
- Learn about the structure and components of a SOC, including people, processes, and technology.
- Understand the identification and handling of suspicious files and the role of perception and memory in investigation.
- Understand the concept of Operational Security (OPSEC) and its application in threat modelling.

**Course Outcomes**

- Ability to identify and analyze common cybersecurity threats and vulnerabilities.
- Skill in implementing network security monitoring and continuous security monitoring concepts.
- Gain knowledge of improving Security Operations Centers (SOCs) through automation, orchestration, and human capital.

Unit	Details	No. of Lectures
1	<p><b>CIA Triad</b> : Who is a Threat Actor and Types of Threats &amp; Threat Actors, Patch Tuesday, Exploit Wednesday, Zero day attacks , Common Vulnerabilities and Exposures (CVE) , Common Vulnerability Scoring system (CVSS)</p> <p><b>Introduction to the Blue Team Mission:</b> What is a SOC? What is the mission?, Why are we being attacked? , Modern defense mindset, The challenges of SOC work</p> <p><b>SOC Overview</b> : The people, process, and technology of a SOC, Aligning the SOC with your organization , SOC functional component overview, Tiered vs. tierless SOC's , Important operational documents</p> <p><b>Overview of Defensible Network Concepts</b> : Network security monitoring (NSM) concepts , NSM event collection , NSM by network layer , Continuous security monitoring (CSM) concepts , CSM event collection ,</p> <p><b>Introduction to Events, Alerts, Anomalies, and Incidents</b> : Event collection , Alert collection , Signatures vs. anomalies , Alert incident creation , Event creation, attributes, correlation, and sharing , What is Alert Triage, How to prioritize alert.</p> <p><b>Incident Management Systems</b> : SOC data organization tools , Incident management systems options and features , Case creation, alerts, observables, playbooks, and workflow , Incident categorization</p> <p><b>Threat Intelligence Platforms:</b> What is cyber threat intelligence? ,</p>	15



	Threat data vs. information vs. intelligence , Threat intel platform and workflow	
2	<p><b>SIEM</b> :Benefits of data centralization , SIEM options and features , SIEM searching, visualizations, and dashboards , Use cases and use case databases , Advanced tools, including SIEM 2.0 , How SOAR works and benefits the SOC ,Options and features , Data flow between SOAR and the SIEM</p> <p><b>Opportunistic vs. targeted attackers</b> : Hactivists, insiders, organized crime, governments , Motivation by attacker group , Case studies of different attack groups , Attacker group naming convention</p> <p><b>Endpoint Attack Tactics</b> :Initial exploitation , Service-side vs client-side exploits , Post-exploitation tactics, tools, and explanations - execution, persistence, discovery, privilege escalation, credential access, lateral movement, collection, exfiltration</p> <p><b>Endpoint Defense In-Depth</b> :Software inventory and Whitelisting , Vulnerability scanning and patching , Host intrusion prevention and detection systems , File integrity monitoring , Windows privileges and permissions , Endpoint detection and response tools (EDR) , Data loss prevention(DLP) , User and entity behavior analytics (UEBA)</p> <p><b>Overview of how Windows Logging Works (PRAC)</b> : Channels, eventIDs, and sources , XML format and event templates ,Log collection path</p> <p><b>Log Collection, Parsing, and Normalization:</b> Logging pipeline and collection methods, Parsing logs , The role of parsing and log enrichment , Log storage , classification and retention lifecycle</p> <p><b>Identifying and Handling Suspicious Files</b> :Safely handling suspicious files , Dangerous files types , Exploits vs. program "features" ,Exploits vs. Payloads ,Executables, scripts, office docs, RTFs, PDFs, and miscellaneous exploits , Detecting malicious scripts</p> <p><b>Perception, Memory, and Investigation</b> :The role of perceptionand memory in observation and analysis , Introduction to decomposition and externalization</p>	15
3	<p><b>Overview of Mental Models for Information Security</b> :Cyber kill chain , Defense-in-depth , NIST cybersecurity framework ,Incident response cycle , Threat intelligence levels and models , Diamond model , The OODA loop , Attack modeling, graph/list thinking, attack trees, Pyramid of pain , MITRE ATT&amp;CK</p> <p><b>Structured Analysis Techniques</b> :System 1 vs. System 2 thinking , Datadriven vs. concept-driven analysis , Confirmation bias avoidance , Link analysis, event matrices</p> <p><b>Overview OPSEC</b> : OPSEC vs. your threat model , Traffic light protocoland intel sharing</p> <p><b>Intrusion Discovery</b> :Choosing an appropriate response , Reacting to opportunistic/targeted attacks</p> <p><b>Incident Closing and Quality Review:</b> Steps for closing incidents</p> <p><b>Overview of Improving Life in the SOC</b> :Improvement through SOC human capital theory , The future of SOCs, including AI-Assisted SOCs, machine learning, and training models</p>	15



<p><b>Analytic Features and Enrichment:</b> High-feature vs. low-feature logs  <b>New Analytic Design, Testing, and Sharing :</b>Introduction to false positives/negatives , Verification of false positives/negatives with threat intel                  Regular expressions , Common matching and rule logic options  <b>Tuning and False Positive Reduction :</b>Using policy to raise fidelity                  Automation and fast lanes  <b>Automation and Orchestration:</b> The definition of automation vs. orchestration, What is SOAR? , Features of SOAR , Common SOAR use cases  <b>Containing Identified Intrusions</b>                  Overview of Isolation options across network layers - physical, link, network, transport, application DNS firewalls, HTTP blocking and containment, SMTP, Web Application Firewalls</p>
--

**Reference books:**

1. The Modern Security Operations Center by Joseph Muniz, Aamir Lakhani, Omar Santos, Moses Frost ,Released April 2021 ,Publisher(s): Addison-Wesley Professional, ISBN: 9780135619773
2. Cisco CyberOps Associate CBROPS 200-201 by Omar Santos / Ron Taylor Released March 2021 Publisher(s): Pearson IT Certification ISBN: 0137333455
3. Security Operations Center: Building, Operating and Maintaining your SOC by Joey Muniz, Gary McIntyre, Nadhem AlFardan Released November 2015 Publisher(s): Cisco Press ISBN: 9780134052083

**SLE TOPICS**

<b>Topic</b>
Why are we being attacked? , Modern defense mindset
The people, process, and technology of a SOC, Tiered vs. tierless SOCs , Important operational documents
Event creation, attributes, correlation, and sharing
SOC data organization tools
Benefits of data
Hackers, insiders, organized crime, governments , Motivation by attacker group , Case studies of different attack groups , Attacker group naming convention
Software inventory and Whitelisting ,Windows privileges and permissions Data loss prevention(DLP) ,





Channels, event IDs, and sources , XML format and event templates ,Log collection path
Syslog log format , Syslog daemons , Syslog network protocol , Log collection path , Systemd journal , Application logging , Service vs. system logs
Dangerous files types , Exploits vs. program "features" ,Exploits vs. Payloads
Cyber kill chain , Defense-in-depth , NIST cybersecurity framework ,
Data-driven vs. concept-driven analysis , Confirmation bias avoidance ,
Choosing an appropriate response , Reacting to opportunistic/targeted attacks
High-feature vs. low-feature logs
Regular expressions
definition of automation vs. orchestration
Firewalls

**Online Resources**

<a href="https://youtu.be/OYsY5B9pqYU">https://youtu.be/OYsY5B9pqYU</a>
---

**Practical List:**

Practical	Content
1	Recovering Deleted Partitions
2	Analyze traffic for FTP password cracking attempts
3	Forensic Analysis of Storage to Acquire the Email Attachments



<b>4</b>	USB Device Enumeration using Windows PowerShell
<b>5</b>	Database Forensics Using SQL Server Management Studio
<b>6</b>	Logical / Physical Acquisition of Android Devices
<b>7</b>	Collecting Windows /Linux Logs using scripts
<b>8</b>	Implement packet transmission analysis
<b>9</b>	Analyze traffic for SMB password cracking attempts
<b>10</b>	Analyze traffic for sniffing attempts/ Analyze traffic to detect malware activity

Reference tools :
OSSIM OSSEC Sagan Splunk Free Snort Elasticsearch MozDef ELK Stack Wazuh Apache Metron