CYB 529 – Advanced Cyber Forensics Spring 2020

Instructor	Bhrigu Celly	**E-Mail**	bcelly@csudh.edu
Classroom	TBD	**Class Time**	TBD
Office	TBD	**Office Hours**	TBD
Phone	(310) 243-3398	**URL**	*http://csc.csudh.edu*

COURSE DESCRIPTION:
The course provides advanced case examples in digital forensics. It provides understanding of everyday issues in a real investigations such as technical, logistical, and legal challenges**.** IT also presents advanced methodologies and machine learning applied in digital investigations. Machine Learning is a rapidly growing field with an intersection of mathematics and statistics. There have been several advancements in technology from recommendation systems to prediction to serving personalized setting on shopping sites. This course provides a broad introduction to major ideas in machine learning with focus of application in forensics when used with digital assets and communication systems. This focuses on practical aspects of machine learning vs theoretical concepts. There will be several projects and assignments to showcase techniques and how to apply them to new problems. This also will teach how to measure performance and how to compare algorithms.

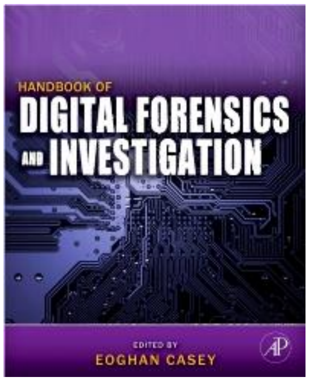
The format of this course includes lectures and hands-on assignments. Students will also complete a project and present it as part of the course. The course contains a project that will include a presentation at the end of the quarter. Students will randomly be asked questions about presentation of their peers during the presentation sessions. Attendance is mandatory.

- Project: 20%
- Presentation: 10%
- Assignments: 10%
- Final Exam: 25%
- Midterm Exam: 20%
- Participation / Class Contribution: 15%
- Total: 100%

PRE-REQUISITE: : Foundations in Cyber Forensics, Foundations in Information Security, Programming Language (java or python), Statistics and Algebra.

TEXTBOOKS [Required]:

1. **Handbook of Digital Forensics and Investigation, 1st Edition**



Author: E Casey

Imprint: Academic Press

Print Book ISBN : 9780123742674

eBook ISBN : 9780080921471

2. Hands on Machine Learning with skit learn and tensorflow, Aurelien Geron
3. Concise Computer Vision an Introduction into Theory and Algorithms. Reinhard
4. Current research papers

COURSE GOALS:

- Provides cutting edge advanced methodologies proven in practice for predicting and conducting digital investigations of all kinds.
- Learn the latest techniques in machine learning as they apply to forensics and data communication.
- Demonstrates how to locate and interpret and find patterns in a wide variety of digital evidence, and how it can be useful in investigations.
- Presents tools in the context of the investigative process, see the use of machine learning and its working with digital forensics and data communication including skit-learn, keras, tensorflow, EnCase, FTK, ProDiscover, Mobiledit software, Paraben Device Seizure Software, MPE+ Mobile Phone-Access Data Software, Foremost, XACT,

Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms.

- The course provides advanced case examples in machine learning with digital forensics, and presents a practical understanding of the technical, logistical, and legal challenges that arise in real investigation predictions**.**

COURSE OUTCOMES:

- To understand how to conduct advanced digital investigations in both criminal and civil contexts.
- To understand how to use machine learning on data acquired on computers, networks, and embedded systems (including cellular telephones and other mobile devices).
- To understand the advanced machine learning investigative techniques methodology which this provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery and Intrusion Investigation.
- To become familiar to the advanced tools in machine learning and digital forensics
- To understand machine learning in digital forensics investigations involving networks and data communication (including enterprise environments and mobile telecommunications technology.

STUDENT ACADEMIC APPEALS PROCESS

Authority and responsibility for assigning grades to students rests with the faculty. However, in those instances where students believe that miscommunication, error, or unfairness of any kind may have adversely affected the instructor’s assessment of their academic performance, the student has a right to appeal by the procedure listed in the Undergraduate Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

AMERICANS WITH DISABILITIES ACT

CSUDH adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with temporary and permanent disabilities. If you have a disability that may adversely affect your work in this class, I encourage you to register with Disabled Student Services (DSS) and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: no accommodation can be made until you register with the DSS. For information call (310) 243-3660 or to use the Telecommunications Device for the Deaf, call (310) 243-2028.

COMPUTER INFORMATION LITERACY EXPECTATIONS

It is expected that students will:

1. *Use Microsoft Word for word processing unless otherwise approved by the instructor,*
2. *Be familiar with using email as a communication tool and check your official campus email account at least every other day;*
3. *Be able to access websites and online course materials which may require Flash and other plug-ins;*
4. *Use the library databases to find articles, journals, books, databases and other materials;*
5. *Be able to create an effective PowerPoint presentation;*
6. *Be able to record audio (ideally video) to share with the instructor via the web; and*
7. *Have regular access to a computer and internet access for the term of this course.*
8. *Be able to program in python*

ACADEMIC INTEGRITY

Academic integrity is of central importance in this and every other course at CSUDH. You are obliged to consult the appropriate sections of the University Catalog and obey all rules and regulations imposed by the University relevant to its lawful missions, processes, and functions. ***All work turned in by a student for a grade must be the students' own work.*** Plagiarism and cheating (e.g. stealing or copying the work of others and turning it in as your own) will not be tolerated, and will be dealt with according to University policy. The consequences for being caught plagiarizing or cheating range from a minimum of a zero grade for the work you plagiarized or cheated on, to being dropped from the course.

COURSE POLICIES:

- Deliverables (Class Assignments, Projects) submitted late are not accepted.
- Deliverables (Class Assignment, Projects) not submitted before the end of the final class will earn 0%.
- Any exceptional, non-academic circumstances need to be discussed with the instructor as soon as they arise, prior to the due date of the deliverable. At the time of the discussion, NO make-up work will be assigned.

The instructor reserves the right not to award credit for deliverables that are incomplete. Partial credit is awarded at the instructor's discretion, and only for work that merits such an award. Assignments that are incomplete or incongruous with the specifications may be returned to the student.

MIDTERM & FINAL EXAM:

Midterm exam is during the 8th week of the class and the date for the final exam is based on the final examination schedule printed in the campus Class Schedule. All projects are due no later than the last week of the semester.

No makeup or early exams will be administered.

GRADES:

The following grading scale will be used:

Score	Grade	Score	Grade

94-100	A	91-93	A-
88-90	B+	84-87	B
81-83	B-	78-80	C+
74-77	C	71-73	C-
68-70	D+	64-67	D
0-63	F		

- Project: 20%
- Presentation: 10%
- Assignments: 10%
- Final Exam: 25%
- Midterm Exam: 20%
- Participation / Class Contribution: 15%
- Total: 100%

TOPIC OUTLINE (Will be conducted according the following. However, the schedule of the topics schedule or timetable may be varying slightly)
Course Outline:

Day	TOPICS
Week 1	**Introduction to Problem Structure and Setup** History of forensics and machine learning Digital Forensics and Intelligent Forensics Overview of various applications, Big Data introduction Basic concepts Bias, Overfitting, Prediction, Training Generalization, Models Issues with learning Classification and Regression Machine Learning Pipeline
Week 2	**Supervised Learning** Introduction to Supervised Learning and algorithms Naïve Base Classifier, Decision Trees, Random Forest Decision Trees Generation Algorithms Linear and Non-Linear Regression, Multiple Regression Logistic Regression, Stochastic Gradient Descent Regularization ,Support Vector Machines
Week 3	**Supervised Learning 2** Singular Vector Decomposition Dimensionality reduction, Principle Component Decomposition K Nearest Neighbor, Ensemble Classifiers Stacking, Boosting, Bagging, Boosting Trees Newer Boosting Algorithms AdaBoost, Gradient Boost, XGBoost Frameworks – skitt-learn, numpy and pandas
Week 4	**Supervised Learning - Deep Learning** History of neural networks Overview of various applications What is deep learning Classification, Regression, Logistic Regression Gradient Decent, Forward Propagation Parameters vs hyperparameters Parameter tuning, Deep neural networks
Week 5	**Supervised Learning - Deep Learning 2 – CNN and RNN** **Convolution Neural Networks** Introduction Edge Detection, Filters, Image Operations Padding Simple CNN

	Recurrent Neural Network (RNN) Introduction Propagation through time Different type of networks Bidirectional RNN
Week 6	**Supervised Learning - Deep Learning 3 – LSTM, GAN** Introduction GRU, Style Transfer Encoders , Decoders Adversarial Networks Frameworks – tensorflow and keras
Week 7	**Unsupervised Learning** Structured and Unstructured data Clustering, Evolutionary Algorithms Expectation Maximation K Means, DBScan Clustering Latent Dirichlet Algorithms Canopy Clustering Spectral Clustering
Week 8	**Model Deployment** Pre-Processing Model Deployment Workflow Pre-requisites Steps to follow Digital Intelligence Architecture ***Process, Pipeline and Model Evaluation*** AOC/ROC, RMSE MSE Multi variable classification using AOC/ROC curves
Week 9	***Computer Vision 1- Forensic Image Analysis*** Light, Electromagnet Spectrum, Colors and Color scales Image Understanding, Camera Basics and Lenses Color Mixing, Image Data, Image formats Basics of Image Operations and Analysis Morphing, Warping, Matting and Blending, Panoramic Imaging
Week 10	**Computer Vision 2- Forensic Image Analysis** Image Segmentation using CNN Tone Mapping Object Detection Models Object detection and classification basics

	Image shading and Shadow Detection with Removal Contouring and region identification, Grouping Video coding standards, Time Series and DTW
Week 11	**Computer Vision Forensic Applications and Models** Car License Plate detection using CNN Object Detection in Surveillance and autonomous cars navigation with CNN & FCNN Digital image reconstruction with GAN Objectionable content detection using CNN and optical flow Facial Reconstruction from Skeletal remains using GAN Reconstruction of shredded ripped documents
Week 12	**Natural Language Processing, Pattern Recognition and Multimedia Document Analysis** Introduction to NLP Stemming and Lemmatization Word Embeddings, Word Vectors, 1- hot encoding GLOVE, Word2Vec, seq2seq Correction Analysis, Keyword searches Counter-Forensics, Adversary aware systems Behavioral Pattern detection and prediction using NLP Evidence analysis and Conversation monitoring using NLP NLTK, DeepQA and Beautiful Soup
Week 13	**Web, Smart and Network Connected Devices** Location sensing Malware abnormality detection with LSTM Weblog intrusion detection using NLP Feature Selection for IDS Intendent response with NLP Botnet detection Profiling internet pirates, cyberstalking and online auction fraud
Week 14	**Social Networks, Phones, PDA and Voice Signals** **Social Network Analysis** Connection Strength Hidden Group detection Organization Structure Detection Voice Sentiment analysis Scaling with AWS, GCP and Azure
Week 15	Project Presentations

GO TOROS!