Knight Foundation School of Computing and Information Sciences

Course Title: Principles and Practices of Digital Forensics Science **Date:** 1/15/2021

Course Number: CIS 4203

Number of Credits: 3

Subject Area: Foundations	**Subject Area Coordinator:** Xudong He **email:** hex@cis.fiu.edu
Catalog Description: This course introduces the principles of digital forensic investigations and best practices involved in the use of software and hardware tools for preserving and analyzing a crime scene.	
Textbook: Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications Textbook by Joakim Kävrestad, Springer Nature, 2019	
References: System Forensics, Investigation, and Response by Chuck Easttom Jones & Bartlett Learning, 2017.	
Prerequisites Courses: MAC-XXXX and COP-XXXX (passed at least one college level math course and one basic college level programming course)	
Corequisite Courses: COP-2XXX or EEL-2880 (must have either passed/enrolled-in a 2000 college level programming course)	

Type: Elective for CS Majors.

Prerequisites Topics:

1. Solve algebraic equations
2. Selection statements
3. Data collection and Analysis
4. Understanding of Windows, Linux and other OS

Course Outcomes:

This course is designed to present the students with an overview of Forensic Sciences with specific focus on Digital Forensics. The course will highlight the current tools and the best practices in this field and showcase its importance in analyzing and solving crime scenes. Students will learn the various stages involved in the digital forensic investigation and the different tools including the ones provided and built using AI/ML techniques that are used in each of the stages including data collection, preservation, orchestration of a crime scene using log data, storage requirements for the collected data, evidence maintenance and archiving etc. Students will also get to understand various case-studies providing them with the various directions to compute and analyze the situation and use computational tools to remediate the situation. The students will get to learn different techniques and procedures

that enable them to perform a digital investigation and become a skilled workforce in the computational front of Digital Forensics investigations.

1. Identify need for software tools and techniques for forensics studies and real-time applications in digital forensics
2. Understand phases of forensic analysis and the computational aspects involved in each phase
3. Understand the integration of software tools for the various platforms ranging from Mainframes to IoT devices.
4. Modern techniques covering BigData storage, Hadoop and Spark processing for real-time analysis of streams of forensic data and use of traditional and modern databases to preserve and store the digital evidence
5. Discuss case studies and identify new ways to solve them including AI/ML based approaches while understanding the trade-offs and requirement.
6. Compare existing tools for digital forensics and propose novel algorithmic tools for computationally mitigating cyber-risk and remediating flaws.
7. Hands-on experience on identifying and solving digital crime.

Knight Foundation School of Computing and Information Sciences
CIS 4203
Principles and Practices of Digital Forensics Science

Relationship between Course Outcomes and Program Outcomes

BS in CS: Program Outcomes	Course Outcomes
a) Demonstrate proficiency in the foundation areas of Computer Science including mathematics, discrete structures, logic and the theory of algorithms	1, 2, 3, 4
b) Demonstrate proficiency in various areas of Computer Science including data structures and algorithms, concepts of programming languages and computer systems.	
c) Demonstrate proficiency in problem solving and application of software engineering techniques	5, 6, 7
d) Demonstrate mastery of at least one modern programming language and proficiency in at least one other.	
e) Demonstrate understanding of the social and ethical concerns of the practicing computer scientist.	1, 2, 3, 4, 5, 6, 7
f) Demonstrate the ability to work cooperatively in teams.	5, 7
g) Demonstrate effective communication skills.	

Assessment Plan for the Course & how Data in the Course are used to assess Program Outcomes

Student and Instructor Course Outcome Surveys are administered at the conclusion of each offering, and are evaluated as described in the School's Assessment Plan: http://www.cis.fiu.edu/programs/undergrad/cs/assessment/

Knight Foundation School of Computing and Information Sciences
CIS 4203
Principles and Practices of Digital Forensics Science

Outline

Topic	Number of Lecture Hours	Outcome
1. Introduction and Concepts 1.1. Introduction to Digital Forensics 1.2. Types of Digital Forensics 1.3. Process involved in Digital Forensics 1.4. Applications of Digital Forensics in current life	7	1, 2
2. Forensic Software and Hardware 2.1. Forensic Ballistics and Photography 2.2. Face, Iris and Fingerprint Recognition 2.3. Audio Video Analysis, 2.4. Windows and Linux System Forensics 2.5. Network Forensics	8	2, 3, 4
3. Operating System and Core for Cyber Security 3.1. File System Architecture, File creation, File deletion and Journaling 3.2. Other Disk structures 3.3. Windows, Linux and IOS boot process 3.4. File system acquisition and recovery	5	2, 4, 6
4. Cyber Crime Investigations 4.1. Investigation Tools 4.2. Digital Evidence Collection 4.3. Evidence Preservation 4.4. Deepfakes identification 4.5. E-Mail Investigation, E-Mail Tracking, IP Tracking, Email Recovery	7	4, 5, 7
5. Integration of AI/ML techniques for Digital Forensics 5.1. Encryption and Decryption Methods 5.2. Search and Seizure of Computers 5.3. Recovering Deleted Evidence 5.4. Password Cracking 5.5. Drone Digital Forensics 5.6. Integration of AI/ML techniques 5.7. Social media crime, Online defacement crime, Email investigation	8	5, 6, 7

Knight Foundation School of Computing and Information Sciences
CIS 4203
Principles and Practices of Digital Forensics Science

Learning Outcomes:

Introduction to Digital Forensics

1. Describe with examples the basic terminology of forensic Sciences and analysis.
2. Describe the Process involved in Digital Forensics
3. Relate practical examples to the digital forensic techniques.

Forensic Software and Hardware:

1. Explain the development of algorithms and the corresponding software applications.
2. Develop platforms that can be used for the forensic software analysis.
3. Describe how hardware integration can be developed for
    a. Forensic Ballistics and Photography
    b. Face, Iris and Fingerprint Recognition
    c. Audio Video Analysis,
    d. Windows and Linux System Forensics
4. Application of the above for Network Forensics

Operating System and Core for Cyber Security

1. Explain the importance of File System Architecture, File creation, File deletion and Journaling
2. Understand the differences between various operating systema and how they handle forensic files
3. Tools that will be used for storing/preserving/archiving the forensic information. (Windows, Linux and IOS boot process)

Cyber Crime Investigations

1. Understand the existing state-of-the-art in Investigation Tool, Digital Evidence Collection, Evidence Preservation etc.
2. E-Mail Investigation, E-Mail Tracking, IP Tracking, Email Recovery

Hands on Case Studies

1. Encryption and Decryption Methods
2. Search and Seizure of Computers
3. Recovering Deleted Evidence
4. Password Cracking
5. Drone Digital Forensics
6. Integration of AI/ML techniques
7. Social media crime, Online defacement crime, Email investigation

Knight Foundation School of Computing and Information Sciences
CIS 4203
Principles and Practices of Digital Forensics Science

Oral and Written Communication

No significant coverage

Written Reports		Oral Presentations	
Number Required	Approx. Number of pages	Number Required	Approx. Time for each
1	10	1	30 minutes

Social and Ethical Implications of Computing Topics

No significant coverage

Topic	Class time	student performance measures

Assessments *

Midterm Examination – 30%

Final Examination – 50%

Projects/Assignments – 20%

* The University Grading Policy will be used

Knight Foundation School of Computing and Information Sciences
CIS 4203
Principles and Practices of Digital Forensics Science

Approximate number of credit hours devoted to fundamental CS topics

Fundamental CS Area	Core Hours	Advanced Hours
Algorithms:	0.5	
Software Design:	3	
Computer Organization and Architecture:	5	
Data Structures:	0.5	
Concepts of Programming Languages		

Theoretical Contents

Topic	Class time
Principles and Practices of Digital Forensics Investigation	40 hours

Problem Analysis Experiences

Solution Design Experiences
