NHẬP MÔN ĐIỀU TRA SỐ (INTRODUCTION TO DIGITAL FORENSICS)
Đề cương chi tiết (Course Syllabus)

1. General Information

Course name: Nhập môn điều tra số (Introduction to Digital Forensics)

Course code: SEC1416_CLC

Course type: Selective

Number of credits: 3

2. Objectives

Knowledge:

The aim of this course is to provide students with fundamental knowledge of digital forensics, including investigation procedures, data acquisition, forensic analysis, evidence validation, and forensic reporting.

Skills:

On successful completion of this course a student will be able to:
- Apply forensic investigation procedures to collect, analyze, and interpret digital evidence;
- Use forensic tools for data acquisition, validation, and forensic analysis;
- Create forensic reports for legal proceedings.

Attitude:

Students are required to attend the classes and complete assignments/projects.

3. Abstracts

This course provides fundamental knowledge of digital forensics, focusing on forensic investigation procedures, data acquisition, forensic analysis, validation, and report writing. It explores techniques for collecting, analyzing, and interpreting digital evidence from diverse sources, including operating systems, mobile devices, networks, and online services. The course also covers forensic tools, data recovery techniques, addressing data-hiding methods, and best practices for documenting findings in reports for legal proceedings.

4. Teaching and learning methods

Lectures:	24h
Exercises:	5h
Projects :	8h
Labs:	8h
Individual reading:	0h

5. Prerequisites: Fundamentals of Information Security - SEC1401_CLC

6. Learning outcomes

After completing this course, the student is able to:
[CLO1]: Understand and explain fundamental concepts of digital forensics, including forensic investigation procedures, data acquisition methods, and evidence validation
[CLO2]: Collect, analyze, and interpret digital evidence from various sources, including operating systems, mobile devices, networks, and online services using forensic tools and techniques
[CLO3]: Create forensic reports suitable for legal proceedings

7. Assignment criteria

Learning outcomes	**Assignment criteria**
[CLO1]: Understand and explain fundamental concepts of digital forensics, including forensic investigation procedures, data acquisition methods, and evidence validation	Chapter 1, Chapter 2
[CLO2]: Collect, analyze, and interpret digital evidence from various sources, including operating systems, mobile devices, networks, and online services using forensic tools and techniques	Chapter 3, Chapter 4
[CLO3]: Create forensic reports suitable for legal proceedings	Chapter 4

8. Outlines

Chapter 1: Understanding the Digital Forensics Profession and Investigations
1.1. An Overview of Digital Forensic
1.2. Preparing for Digital Investigations
1.3. Procedures for Private-Sector High-Tech Investigation
1.4. Conducting an Investigation
1.5. Current Digital Forensics Tools

Chapter 2: Data Acquisition
2.1. Understanding Storage Formats for Digital Evidence
2.2. Determining the Best Acquisition Method
2.3. Contingency Planning for Image Acquisitions
2.4. Using Acquisition Tools
2.5. Validating Data Acquisitions

Chapter 3: Digital Forensics Analysis and Validation
3.1. Determining What Data to Collect and Analyze
3.2. Validating Forensic Data
3.3. Operating System Forensics
3.4. Mobile Device Forensics
3.5. Network and Online Services Forensics
3.6. Data Recovery Techniques
3.7. Addressing Data-Hiding Techniques

Chapter 4: Report Writing for High-Tech Investigations
4.1. Understanding the Importance of Reports
4.2. Guidelines for Writing Reports
4.3. Generating Report Findings with Forensics Software Tools

9. Required Textbooks

[1] Bill Nelson, Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations*, 7th Edition, Course Technology, Cengage Learning, 2022.

10. Suggested Textbooks

[2] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science*, Computers, and the Internet, 3rd Edition, Academic Press, 2011.
[3] Eoghan Casey, *Handbook of Digital Forensics and Investigation*, Academic Press, 2010.

11. Schedule

Main contents	Duration	Specific contents
Chapter 1: Understanding the Digital Forensics Profession and Investigations	4h lecture	1.1. An Overview of Digital Forensic 1.2. Preparing for Digital Investigations 1.3. Procedures for Private-Sector High-Tech Investigation 1.4. Conducting an Investigation 1.5. Current Digital Forensics Tools
Chapter 2: Data Acquisition	6h lecture 2h exercise 4h lab 3h project	2.1. Understanding Storage Formats for Digital Evidence 2.2. Determining the Best Acquisition Method 2.3. Contingency Planning for Image Acquisitions 2.4. Using Acquisition Tools 2.5. Validating Data Acquisitions
Chapter 3: Digital Forensics Analysis and Validation	8h lecture 3h exercise 4h lab 3h project	3.1. Determining What Data to Collect and Analyze 3.2. Validating Forensic Data 3.3. Operating System Forensics 3.4. Mobile Device Forensics 3.5. Network and Online Services Forensics 3.6. Data Recovery Techniques 3.7. Addressing Data-Hiding Techniques
Chapter 4: Report Writing for High-Tech Investigations	6h lecture 2h project	4.1. Understanding the Importance of Reports 4.2. Guidelines for Writing Reports 4.3. Generating Report Findings with Forensics Software Tools

12. Grading Policy
Attendance: 10%
Mid-term exam/exercises: 10%

Course projects:	30%
Final examination:	50%