Undergraduate

Program

Course Title Fundamental of Digital Forensics Mahidol University International College

Course Code EGCI 494 Division Science

TQF 3 Course Specifications

Section 1 General Information

1. Course code and course

title

Thai EGCI 494 นิติวิทยาเชิงเลขขั้นพื้นฐาน

English EGCI 494 Fundamental of Digital Forensics

2. Number of credits 4 Credits

3. Program and type of subject

3.1 Program Bachelor of Engineering (Computer Engineering)

3.2 Type of Subject Major Course (Required Major)

4. Course Coordinator and Course Lecturer

4.1 Course Coordinator Asst. Prof. Lalita Narupiyakul, Ph.D.

4.2 Course Lecturer Assoc. Prof. Suratose Tritilanunt, Ph.D.

5. Trimester/ Year of Study

5.1 Trimester Third trimester / for 3rd year Computer Engineering

5.2 Course Capacity Approximately 25 students

6. Pre-requisite None

7. Co-requisites None

8. Venue of Study Mahidol University, Salaya campus

9. Date of Latest Revision

Date 2nd Month March Year 2023

Section 2 Goals and Objectives

1. Course Goals

To develop student in the basic principle of digital forensic techniques and tools. The concept of data collection and investigation from operating system such as Windows and Unix will be explained in the classroom. Students will learn the fundamental of computer files system storage. Principle techniques of collecting and analyzing network traffic will be discussed and exercised via lab experiments and class assignments. These lab exercises will help students clearly understand this course and be able to use their skill and knowledge to solve simple engineering problems.

2. Objectives of Course Development/Revision

2.1 Course Objectives

1. Explain basic principle of digital forensic techniques and tools.
2. Explain concept of data collection and investigation processes.
3. Explain fundamental of computer files system storage.
4. Collecting and analyzing network traffic.

2.2 Course-level Learning Outcomes: CLOs

By the end of the course, students will be able to (CLOs)

1. CLO1 Analyze digital forensic problems that exists in network system
2. CLO2 Show ability to work as team by presenting knowledge resulting from studies or experiments in a written report systematically.

Section 3 Course Management

1. Course Description

(Thai) แนะนำพื้นฐานนิติวิทยาเชิงเลข การเก็บรวบรวมข้อมูลและการสืบสวนข้อมูลจากระบบปฏิบัติการเช่นวินโดวส์และยูนิกซ์ หน่วยเก็บระบบแฟ้มข้อมูลคอมพิวเตอร์ การเก็บรวบรวมและวิเคราะห์การจราจรเครือข่าย การวิเคราะห์และตรวจสอบความสมเหตุสมผล เครื่องมือนิติวิทยาเชิงเลข

(English) Introduction to basic of digital forensics. Data Collection and Investigation from Operating System such as Windows and Unix. Computer files system storage. Collecting and analyzing network traffic. Data analysis and validation. Digital Forensic Tools.

2. Credit hours per trimester

Lecture (Hour(s))	Laboratory/field trip/internship (Hour(s))	Self-study (Hour(s))
48 hours (4 hours x 12 weeks)	-	96 hours (8 hours x 12 weeks)

3. Number of hours that the lecturer provides individual counseling and guidance.

1 hours/week

Section 4 Development of Students' Learning Outcome

1. Short summary on the knowledge or skills that the course intends to develop in students (CLOs)

By the end of the course, students will be able to

1. CLO1 Analyze digital forensic problems that exists in network system
2. CLO2 Show ability to work as team by presenting knowledge resulting from studies or experiments in a written report systematically.

2. Teaching methods for developing the knowledge or skills specified in item 1 and evaluation methods of the course learning outcomes

Course Code	Teaching methods	Evaluation Methods
CLO1	Interactive Lecture, Individual Assignment	Written Examination, Individual Evaluation
CLO2	Lab Exercise, Class Assignment	Lab Examination , Lab Exercise

Undergraduate

Program

Course Title Fundamental of Digital Forensics Mahidol University International College

Course Code EGCI 494 Division Science

Section 5 Teaching and Evaluation Plans

1. Teaching plan

Week	Topic	Number of Hours		Teaching Activities/ Media	Lecturer
		Lecture Hours	Lab/Field Trip/Internship Hours		
1	Principle of Digital Forensics	4	0	Interactive Lecture, Individual Assignment	Interactive Lecture, Quiz1, Individual Assignment, Lab Exercise
2	Documentation and Chain of Custody	4	0		
3	File System Gathering Process and Procedure	4	0		
4	File System Gathering and Analyzing Tools	4	0		
5-6	Windows Registry and Logs analysis	8	0	Interactive Lecture, Lab Exercise	
7	Examination	2	0		Midterm
7-8	Network Traffic Evidence Gathering and Analyzing Tools	6	0	Interactive Lecture, Lab Exercise, Individual Assignment	Quiz2, Individual Assignment
9-11	Cyber-attacks and Network Forensics	12	0		
12	Case study and Project presentation	4	0	Group project presentation	Project presentation
13	Examination	2	0		Final Exam
	Total	48	0		

2. Plan for Assessing Course Learning Outcomes

2.1 Assessing and Evaluating Learning Achievement

a. Formative Assessment

The assessment tools such as homework, quizzes and exam are used to evaluate student's understanding by their ability to explain network architecture and protocol, as well as principle of network and information security. For the design and troubleshoot parts, students should be able to show how to search and examine any network vulnerabilities by using lab exercises provided in the classroom. These assessments are made through their homework, quizzes and exams.

b. Summative Assessment

(1) Tools and Percentage Weight in Assessment and Evaluation

Learning Outcomes	Assessment Methods	Assessment Ratio (Percentage)	
CLO1 Analyze digital forensic problems that exists in network system.	Quiz	10	80
	Lab Exercise	10	
	Midterm Exam	30	
	Final Exam	30	
CLO2 Show ability to work as team by presenting knowledge resulting from studies or experiments in a written report systematically.	Homework	10	20
	Project presentation	10	
Total			100

(2) Grading System

Grade	Achievement	Final Score (% range)	GPA
A	Excellent	90-100	4.0
B+	Very Good	85-89	3.5
B	Good	80-84	3.0
C+	Fairly Good	75-79	2.5
C	Fair	70-74	2.0
D+	Poor	65-69	1.5
D	Very Poor	60-64	1.0
F	Fail	Less than 60	0.0

(3) Re-examination

N/A - (Not applicable with MUIC)

3. Student Appeals

The student wishing to appeal according to grading result must submit a written and signed appeal form personally to the academic affair unit. It is prohibited to assign another person to appeal on one's behalf. The written appeal form is then sent to the program director and chair of department. The final decision is transferred for approval by the faculty committee. The result of appeal then is informed to the student.

Section 6 Teaching Materials and Resources

1. Textbooks and/or other documents/materials

    1) Darren R. Hayes, “Practical Guide to Digital Forensics Investigations”, Pearson IT Certification; 2nd edition, (October 16, 2020).
    2) Nipun Jaswal, “Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools”, Packt Publishing, (March 30, 2019).
    3) Nik Alleyne, “Learning by Practicing - Hack & Detect: Leveraging the Cyber Kill Chain for Practical Hacking and its Detection via Network Forensics”, December 10, 2018.

2. Recommended textbooks and/or other documents/materials

    1) Websites – To be Announced in class

3. Other Resources (If any)

Section 7 Evaluation and Improvement of Course Management

1. **Strategies for effective course evaluation by students**

   1.1 Evaluation of peers by students

   1.2 Student evaluation

      1.2.1 Course content

      1.2.2 Course management

      1.2.3 Suggestions

      1.2.4 Overall opinions

2. **Evaluation strategies in teaching methods**

   2.1 Student evaluation

   2.2 Presentation

3. **Improvement of teaching methods**

   Use evaluation from 1 and 2 for course improvement

4. **Evaluation of students' learning outcome**

   Analysis of students' learning outcomes using scores from each CLOs for evaluation.

5. **Review and improvement for better outcome**

   Review the course before trimester starts, before each teaching period and review course contents every 3 years.

Appendix

Alignment between Courses and General Education courses

Relations between the course and the program

Table 1 Relations between the course and the PLOs

Computer Networks and Information Security	*PLOs*					
	PLO1	*PLO2*	*PLO3*	*PLO4*	*PLO5*	*PLO6*
EGCI 494			R		R	

Table 2 Relations between CLOs and PLOs

EGCI 494	*PLOs*					
	PLO1	*PLO2*	*PLO3*	*PLO4*	*PLO5*	*PLO6*
CLO1 Analyze digital forensic problems that exists in network system.			x			
CLO2 Show ability to work as team by presenting knowledge resulting from studies or experiments in a written report systematically.					x	

Table 3 PLOs that the course is responsible for

PLOs	*SubPLOs*
PLO3: Evaluate the computer requirements and identify the appropriate knowledge and tools for effective problem solving in computer	3.1 Analyze problems that exists in computer system
PLO5: Perform good communication skills with various groups of people and demonstrate self and team responsibility.	5.2 Present knowledge resulting from studies or experiments in a written report systematically