

Course Syllabus

1. **Program of Study** Bachelor of Science (Computer Science)
Faculty/Institute/College Mahidol University International College
 Mahidol University

- Course Code** ICCS 438 **Course Title** Introduction to Computer Forensics

2. **Number of Credits** **4 (Lectures/lab) (3 - 2)**

3. **Prerequisite(s)** ICCS 315, ICCS 316

4. **Type of Course** Elective

5. **Trimester / Academic Year** Trimester III / Year 2005 - 2006

6. **Course Description**
 A practical approach to the investigation of computerized incidents; core computer science theories and practical skills for computer forensic investigations; the role of technology in investigating computer-based crime; dealing with investigative bodies at a rudimentary level

7. **Course Objective(s)**
 By the end of the course students should be able to:
 - Describe and explain the current practice of computer forensics
 - Explain and apply the process of forensic investigation
 - Appropriately select tools for specific forensic investigations
 - Identify frauds using proper techniques
 - Detect computer intrusions

8. Course Outline

Week	Topic			Instructor	
	Lecture	Hour	Lab		Hour
1	Introduction	3	Lab.#1: Evidence Acquisition	2	Dr. Udom Silparcha
2	Current Practice: Electronic Evidence, Forensic Tools, Emerging Procedure and Standards	3		2	
3	History of Computer Forensics, its Role in Law Enforcement, Principle of evidence	3	Lab.#2:Data and File Formats	2	
4	Forensic Examination, Resources and Tools, Competencies and Certification	3		2	

Week	Topic				Instructor
	Lecture	Hour	Lab	Hour	
5	Auditing and Fraud Detection, Defining Fraudulent Activity	3	Lab.#3: Encryption, Signatures	2	Dr. Udom Silparcha
6	Fraud Detection Techniques, Visual Analysis Techniques, Building a Fraud Analysis Model	3	Lab.#4: Fraud Detection lab.	2	
7	Case Studies: “Little Nicky” Scarfo, “El Gritton”	3	Case discussion and review	2	
8	Case Studies: Melissa, the World Trade Center Bombing (1993), Operation Bojinka, Other Cases	3	Case discussion and review	2	
9	Intrusion Detection System, Network Security	3	Lab.#5: Network Tracing, E-mail Tracing	2	
10	Intrusion Forensics	3	Lab.#6: Hacker Tracing	2	
11	Research Directions and Future Developments	3	Class review	2	
	Total	33		22	

9. Teaching Method(s)

Lectures, in-class practical exercises, discussion, and self-study

10. Teaching Media

Text and teaching materials, Powerpoint, and handouts, computer software and tools assisting Computer Forensics

11. Measurement and Evaluation of Student Achievement

Assessment made from stated criteria: students with 85% obtain grade A

12. Course Evaluation

1. Participation	5%	3. Mid-term exam	30%
2. Assignments (×6)	30%	4. Final exam	40%

13. Reference(s)

Mohay, G., et al., 2003. Computer and Intrusion Forensics. Artech House Publishers, Norwood, MA.

Caloyannides, M.A., 2001. Computer Forensics and Privacy. Artech House Publishers, Norwood, MA.

14. Instructor(s)

Dr. Udom Silparcha

15. Course Coordinator

Dr. Udom Silparcha