UNDERGRADUATE PROGRAM IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING
FACULTY OF INTELLIGENT ELECTRICAL AND INFORMATICS TECHNOLOGY

Module name	**Digital Forensics**	
Module level	Undergraduate	
Code	EC184903	
Courses (if applicable)	Digital Forensics	
Semester	Elective	
Contact person	Dr. Adhi Dharma	
Lecturer	Dr. Adhi Dharma	
Language	Indonesia	
Relation to curriculum	Undergraduate degree program, elective semester. {semester}	
Type of teaching, contact hours	Lecture, < 60 students, 170 Minutes * SKS	
Workload	1. Lectures: 3 x 50 = 150 minutes (2.5 hours) per week. 2. Exercises and Assignments: 3 x 60 = 180 minutes (3 hours) per week. 3. Private study: 3 x 60 = 180 minutes (3 hours) per week.	
Credit points	3 credit points (sks).	
Requirements according to the examination regulations	A student must have attended at least 75% of the lectures to sit in the exams.	
Mandatory prerequisites	• Operating Systems • Database Management Systems • Computer Networks and Laboratory	
Learning outcomes and their corresponding PLOs	CLO-1 Students are able to explain the origins of forensic science	PLO-3 PLO-4
	CLO-2 Students are able to explain the difference between scientific conclusions and legal decision-making	PLO-3 PLO-4
	CLO-3 Students are able to explain the role of digital forensics and the relationship of digital forensics to traditional forensic science, traditional science and the appropriate use of scientific methods	PLO-3 PLO-4
	CLO-4 Students are able to outline a range of situations where digital forensics may be applicable	PLO-5 PLO-6
	CLO-5 Students are able to identify and explain at least three current issues in the practice of digital forensic investigations.	PLO-5 PLO-6

Content	In this course, students will learn about Digital Forensics Science and the systematic process of obtaining, authenticating, and analyzing digital evidence. Technical and managerial topics will be explored, giving students practical and theoretical experience using forensic equipment and software. Additional topics of EDiscovery, Data Retention, Data Disposal, Litigation, Internal Investigation, Regulation Compliance and Incident Response will be discussed in the context of Digital Forensics. Students will also have the opportunity to work with open source forensic software programs.
Study and examination requirements and forms of examination	• In-class exercises • Quiz 1 and 2 • Assignment 1, 2, 3 • Mid-term examination • Final examination
Media employed	LCD, whiteboard, websites (myITS Classroom).
Assessments and Evaluation	CO-1: Question no 1 in midterm exam (10%) CO-2: Question no 2 in midterm exam (15%) CO-3: Question no 3 in midterm exam (15%), quiz 1 (5%) CO-4: Assignment 1 (5%), question no 4 in midterm exam (15%), Quiz 2 (5%) CO-5: Question no 1 in final exam (15%), question no 2 in final exam (15%)
Reading List	10. BUNDLE: Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning; 4 edition 2010. 11. Network Forensics: Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham Prentice Hall, 2012. 12. Guide to Computer Forensics and Investigations (4th edition). By B. Nelson, A. Phillips, F. Enfinger, C. Steuart. ISBN 0-619-21706-5, Thomson, 2009. 13. Computer Forensics: Hard Disk and Operating Systems, EC Council, September 17, 2009. 14. File System Forensic Analysis. By Brian Carrier. Addison-Wesley Professional, March 27, 2005.