MODULE HANDBOOK DESCRIPTION

Module designation	Digital Forensics	
Code	FBD0011	
Semester(s) in which the module is taught	5 / third year	
Person responsible for the module	A.Sjamsjiar Rachman, ST., MT.	
Language	Indonesian	
Relation to curriculum	Compulsory for Computer System	
Teaching methods	Lectures, case based method, collaborative learning.	
Workload (incl. contact hours, self-study hours)	Contact minutes every week, each week of the 16 weeks/semester: • Lectures: 2 x 50 minutes • Exercises and Assignments: 2 x 60 minutes • Self-study/Case Study: 2 x 60 minutes. Total study hours = 5 hours 40 minutes/week.	
Credit points	2 SKS (~ 3.2 ECTS)	
Required and recommended prerequisites for joining the module	-	
Module objectives/intended learning outcomes	1. Students are able to apply professional practices for reporting of findings from digital forensic investigations. 2. Students are able to deconstructing a systemic understanding of underpinning concepts and best practices in relation to digital forensic investigations.	PLO3
	3. Students are able to critically evaluate methodology options and course of actions to undertake digital forensic investigations given a case scenario.	PLO4
	4. Students are able to evaluate challenges faced by digital forensic investigators resulting from advances in technology and widespread use of digital devices.	PLO9

Content	This module will aim to familiarise students with core concepts (e.g. Locard's exchange principle, and legal admissibility of digital evidence) and best practices (e.g. the ACPO Good Practice Guide for Digital Evidence, Contemporaneous Notes taking, and the SWGDE guidelines) underpinning digital forensic investigations. It introduces methodologies that guide the digital investigative process (i.e., collection, interpretation, analysis and reporting), and key techniques that can be applied for interpretation and analysis of digital evidence in the context of digital forensics in general (e.g., hashing, and file carving), computer forensics (e.g., windows registry analysis and metadata analysis), and multimedia forensics (e.g., multimedia source analysis for device identification, and multimedia content analysis for forgery detection).
Examination forms	- Written case study
Study and examination requirements	The final grade in the module is composed of: a. Case I assessment: 25% b. Case II assessment: 25% c. Case III assessment: 25% d. Case IV assessment: 25% Students must have a final grade of 65% or higher to pass
Reading list	1. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press; 3 edition. ISBN 978-0123742681. 2. Altheide, C. and Carvey, H. (2011). Digital Forensics with Open Source Tools. Syngress. ISBN 978-1597495868. 3. Ho, A. T. S. and Li, S (2015). Handbook of Digital Forensics of Multimedia Data and Devices. Wiley-IEEE Press. ISBN 978-1118640500.