Subject Description Form

Subject Code	EIE4114 (for 42480 and 42470)
Subject Title	Digital Forensics for Crime Investigation
Credit Value	3
Level	4
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	1. To provide students with basic concepts about digital forensic techniques for crime investigation 2. To appreciate how different forensic techniques are used for information security
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand different approaches for digital forensics 2. Use different techniques for forensic investigation Category B: Attributes for all-roundedness 3. Present ideas and findings effectively
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Digital and Computational Forensics Context Introduction to digital and computational forensics; Historical aspects in digital and computational forensics; Introduction to techniques for multimedia manipulation; different classes of techniques for forensics: basic idea, framework and applications. 2. Forensics based on Intrinsic/Extrinsic Data Models of digital data capturing device; idea of the use of intrinsic data in digital forensic investigation; introduction to forensics techniques using intrinsic data; applications in source device identification, device linking and integrity verification. Introduction to techniques for multimedia content protection and authentication; attacks modelling. 3. Machine Learning Forensics Different types of ML-based Forensics; Extractive Forensics; Inductive forensics; deductive forensics. Example use cases in ML-based Forensics. 4. Digital Evidence Models of digital evidence; event analytics: surveillance, monitoring, forensic and security; file carving: idea, different classes of techniques; software tools for file carving. 5. Robustness of Forensic Techniques Robustness and security of forensic techniques; adversary model; case studies of reliabilities of forensic techniques. **Laboratory Experiments:** Practical Works: 1. Evaluation of forensic techniques based on intrinsic data. 2. Evaluation of forensic techniques based on extrinsic data. 3. Forensic analysis of digital evidence.

Teaching/Learning Methodology

Teaching and Learning Method	Intended Subject Learning Outcome	Remarks
Lectures	1, 2	Fundamental principles and key concepts of the subject are delivered to students.
Tutorials	1, 2	Supplementary to lectures; Students will be able to clarify concepts and to have a deeper understanding of the lecture material; Problems and application examples are given and discussed.
Laboratory sessions	2, 3	Students will evaluate different kinds of forensic techniques.
Mini-project	1, 2, 3	Students are required to study a problem in forensic application. Students will need to submit a written report and make a presentation.

Assessment Methods in Alignment with Intended Subject Learning Outcomes

Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)		
		1	2	3
1. Continuous Assessment (total 50%)				
• Tests	14%	√	√	
• Laboratory sessions	19%		√	√
• Mini-project	17%		√	√
2. Examination	50%	√	√	
Total	100%			

The continuous assessment consists of tests, laboratory exercises and a mini-project.

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

Specific Assessment Methods/Tasks	Remark
Tests and examination	end-of chapter type problems used to evaluate students' ability in applying concepts and skills learnt in the classroom; students need to think critically in order to come with a solution for a problem.
Laboratory sessions, mini-project	oral examination will be conducted to evaluate student's technical knowledge and communication skills.

Student Study Effort Expected	**Class contact (time-tabled):**	
	• Lecture	21 Hours
	• Tutorial/Laboratory/Practice Classes	18 Hours
	Other student study effort:	
	• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination	36 Hours
	• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing	30 Hours
	Total student study effort:	**105 Hours**
Reading List and References	**Reference Books:** 1. JoakimKavrestad, "*Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*", Springer, 2020. 2. Darren R. Hayes, "*A Practical Guide to Digital Forensics Investigations*", Pearson IT Certification, 2020. 3. Nihad A Hassan, "*Digital Forensics Basics: A Practical Guide using Windows OS*", Apress 2019. 4. Anders Flaglien, Inger Marie Sunde, AusraDilijonaite, Jeff Hamm, Hens Petter Sandvik, PetterBjelland, Katrin Franke, Stefan Axelsson, "*Digital Forensics: an academic introduction*", John Wiley & Sons, 2018. 5. Husrev Taha Sencar and Nasir Memon (editors), *"Digital Image Forensics"*, Springer, 2013. 6. Frank Y. Shih, *"Multimedia Security Watermarking, Steganography and Forensics"*, CRC Press, 2013. 7. Li Chang-Tsun, "*Emerging Digital Forensics Applications for Crime Protection, Prevention and Security",* IGI Global 2013, doi:10.4018/978-1-4666-4006-1, 2013. 8. Li Chang-Tsun and Anthony T.S. Ho, *"Crime Prevention Technologies and Applications for Advancing Criminal Investigation",* IGI Global 2012, doi:10.4018/978-1-4666-1758-2, 2012.	
Last Updated	November 2021	
Prepared by	Dr Wen Chen and Dr Bonnie Law	