EE4222: DIGITAL FORENSICS

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Digital Forensics

Subject Code
EE - Electrical Engineering
Course Number
4222

Academic Unit
Electrical Engineering (EE)

College/School
College of Engineering (EG)

Course Duration
One Semester

Credit Units
3

Level
B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
CS2311 Computer Programming and EE2004 Microcomputer

Precursors
EE3009 Data Communications and Networking

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract
The aim of this course is to provide students with an understanding of the concepts of Forensic Science and the basic principles of application of computer science and engineering methods to a legal proceeding. The interdisciplinary

investigation covers diverse topics from fields of Law, Ethics, Electronic Engineering, Computer Science and Information System Management. This course also intends to provide future digital system administrators and computer security practitioners with the fundamental knowledge in the post-incident reaction.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Acquaintance with the nature of digital forensic evidence and forms of Internet-based fraud.		x	x	
2	Acquaintance with the basics of hard drive geometry and analysis of common file systems including FAT, NTFS and Unix file systems.		x	x	
3	Analysis of forensic evidence from storage systems such as hard drives.		x	x	
4	Investigation and interpretation of network events which contribute to an ethics component as well as to a legal component.		x	x	
5	Application of basic theories to practical work.		x	x	

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Teaching and Learning Activities (TLAs)

	TLAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Explain key concepts in digital Forensics	1, 2, 3, 4, 5	3 hrs/wk
2	Project/Experiments	Conduct experiments/ projects on basic digital forensics	1, 2, 3, 4, 5	3 hrs/wk (3 weeks)

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Tests (min:2)	1, 2, 3, 4, 5	42	
2	#Assignments and lab exercises (min: 3)	1, 2, 3, 4, 5	18	

Continuous Assessment (%)
60

Examination (%)
40

Examination Duration (Hours)
2

Additional Information for ATs
To pass the course, students are required to achieve at least 30% in course work and 30% in the examination. Also, 75% laboratory attendance rate must be obtained.

#may include homework, tutorial exercise, project/mini-project, presentation

Assessment Rubrics (AR)

Assessment Task
Examination

Criterion
Achievements in CILOs

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
Coursework

Criterion
Achievements in CILOs

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)

Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

Introduction to Digital Forensics and Methodologies
Digital device; digital crime; digital investigation; URL obscuring; registrar impersonation phishing attacks; Email tracing.

Legal Issues and Evidence Collection
Nature of computer evidence; best evidence rule; acquisition of evidence; Fourth Amendment; Privacy Protection Act; ethical and legal requirements for evidence collection; reaction to evidence volatility; forensic duplication; solid state disks forensics.

Hard Drive Evidence and File System Analysis
Hard drive geometry; MBR structure; partition table entry; GUID; Apple partitions; File Allocation Table; FAT principle; USB storage device; NTFS file system; MFT entry; NTFS analysis; Unix file systems; journaling file systems; timestamp analysis; allocation sequence causality.

Investigation and Interpretation of Network Events
Internet artefacts; cookies and caches; browsers; Unix intrusion; network protocols; link layer forensics; ATM; ARP attacks; ISMP Smurf Attack; Mitnick Attack; DNS cache poisoning; routing changes; TCP/IP related evidences.

Snorts, Malware and Ethics
Snort architecture; computer viruses; snort rules; snort utilization; anti-virus techniques; worms; malicious mobile code; promiscuous sniffing backdoors; Trojan horses; Linux kernel manipulations; Windows kernel manipulations; buffer overflow attack; pointer subterfuge; format string vulnerability; program analysis; hacking damage; moral issues in digital age.

Reading List

Compulsory Readings

	Title
1	Lecture notes
2	J. Sammons: The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, ISBN-10: 1597496618 (Syngress Publishing, February 2012).

Additional Readings

	Title
1	Nil