COURSE STRUCTURE

Name of Course: DIGITAL FORENSICS

Course Code: DCS2112

Credit Hours: 4

Prerequisite/co-requisite: DCS2110 Cybersecurity Fundamentals

Summary:

This module introduces students to the various types of computer related crimes, techniques of gathering electronic evidence, and the recovery of deleted, damaged or encrypted data. Students will also use forensic tools to perform forensic investigation. Besides the tools and techniques of investigation, students will be taught the forensic investigation methodology and the proper handling of evidence.

Course Learning Outcomes:

Upon completing this course, the students will be able to:

CLO1: Understand the fundamental principles of digital investigation in the context of computer forensic. (C2, PLO1)

CLO2: Explain the digital forensics investigation by applying appropriate methods, procedures, tools and techniques. (P3, PLO3)

Course Format:

Total Student Learning Time (SLT) (L = Lecture; T = Tutorial; P = Practical; EL = E-Learning) :

Learning Hours				**Independent Learning (hr)**	**Total Student Learning Time (hr)**
L	T	P	EL		
28	0	14	14	104	160

Teaching and Delivery Methods/ Teaching Methodology:

Lectures, Tutorial and Practical/Laboratory work delivered in a combination of blended & independent learning

E-Learning provided by INTI makes learning more accessible and convenient for the students. The blended model utilized by INTI is the integration of E-learning via INTI's Learning Management System and the conventional lecturer-led classroom activities. INTI students are required to access to the online learning materials (additional notes, reading materials, online assessments, discussion forums and etc.), so as to acquire a complete learning process. This also promotes self-directed learning in encouraging INTI students to be independent learners.

Syllabus:

Lecture	Course Content Outline	CLO*
1 - 4	**Fundamentals of Digital Forensic:** Concept of Digital Forensics, What is Computer Forensic, Examining data, Steps involved a forensic examination in a digital environment.	1
5 - 8	**Cybercrime, Cyber Aided Crime and Digital Evidence:** Types of cyber crime, how digital envidence can be used in criminal investigations**.**	1,2
9 - 12	**Storage and Host Forensics:** Related terminologies, how to collect evidences from storage media and host based, how to preserve the evidences.	1,2
13 - 16	**Email and Web Forensics:** Related terminologies, how to collect evidences from email and websites, how to preserve the evidences.	1,2
17 - 20	**Mobile and network forensics:** Related terminologies, how to collect evidences from mobile and network based, how to preserve the evidences.	1,2
21 - 24	**Malware forensics**: Malware detection in memory, Ways to find key artifacts, how to correctly intepret it to detect suspicious instructions.	1,2
25 - 28	**Documenting and Managing the crime scene:** Actions involved to carry out on computer to collect evidence, , securing digital evidence in a forensic sound manner, concept of write blocker, live investigations**.**	1,2
	FINAL EXAMINATION	

Student Evaluation:

Continuous Assessment		Percentage (%)	CLO
1	Mid Term Test	20	1
2	Assignment (2)	40	2
Total		**60%**	
Final Assessment		**Percentage (%)**	
Final Examination		40	1
Total		**100%**	

Final exam format:
Duration: 2 hours
The students will be required to answer all:
Section A: MCQ (40 marks)
Section B: Structured written questions (60 marks)

Grading Scale:
A+ (90-100), A (80-89), A- (75-79), B+ (70-74), B (65-69), B- (60-64), C+ (55-59), C (50-54), C- (45-49), D (40-44), F (0-39), Resit Pass, RP (50-100), Resit Fail, RF (0-49)

IMPORTANT NOTE:
Students are required to "**PASS**" BOTH continuous and final assessment in order to pass the subject.

Additional Information: Problem Solving and Scientific Skills;

Main Reference(s) Supporting Course:

1. William Oettinger (2022), Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence, 2nd Edition 2nd ed. Edition. ISBN 978-1803238302
2. Darren R. Hayes (2020) Practical Guide to Digital Forensics Investigations, A 2nd Edition, Kindle Edition, Pearson IT Certification; 2nd edition. ISBN 978-0789759917

Additional References:

1. Joakim Kavrestad (2020), Fundamentals of Digital Forensics, Springer International Publishing. 2nd Edition. ISBN-13: 978-3030389536
2. Nihad A. Hassan (2019), Digital Forensics Basics: A Practical Guide Using Windows OS, Apress; 1st edition. ISBN-13: 978-1484238370
3. Abdul Rahman (2019), Computer Forensics: A Practical Guide 2019. ISBN-13: 978-1087067322

LABORATORY WORK:

No	Practical Work
1	Digital Forensics Investigation Process and Procedure
2	Imaging and Analysing Delected Content
3	Digital Evidence: What data can you retrieve?
4	Examining and Extracting Hidden Data
5	Email and Web Forensics
6	Evidence Trials