Course Name: Digital Forensics **Course Code: ITEC435**

General Information						
Course Code	**ITEC435**	**Level/Year**	8^{th} / 4^{nd}	**Required (R) / Selected Elective (SE)**		**SE**
Credit Hours	**Theory**	**2**	**Lab**	**1**	**Total**	**3**
Prerequisites	ITEC331	**Course Coordinator**		Ms. Ahmed Unnisa Begu		
Corequisites		**Track Leader**		**Dr. Rahma Salman**		

Course Description

This course introduces the fundamental concepts of computer forensics and its applications in digital investigations. Students will learn the principles and techniques necessary for effective digital crime scene investigations, including the use of specialized software tools essential for conducting forensic analysis. The curriculum covers the various phases of the digital investigation process, from initial system preservation to event reconstruction, and emphasizes the creation and implementation of an incident response plan. Practical lab exercises will enable students to conduct live investigations, focusing on evidence acquisition, examination, analysis, and preservation. Additionally, the course explores state-of-the-art techniques in digital investigation analysis, such as file carving, multimedia forensics, and memory analysis. Topics on mobile device forensics, anti-forensics, counter anti-forensics, and log analysis will also be included to enhance students' investigative skills and prepare them for real-world challenges in the field.

Course Objectives : On completion of the course, the student will be able to:

- To provide an understanding of digital forensics principles and their applications in investigations.
- To explore the stages of the digital forensics process, from evidence identification to presentation.
- To examine the legal frameworks governing cybercrime and digital evidence collection.
- To develop skills in effective methods for collecting and preserving digital evidence.
- To analyze the unique challenges associated with mobile and embedded forensics.
- To become familiar with advanced tools and technologies used in digital forensic investigations.
- To identify and implement best practices for maintaining the integrity of digital evidence.
- To assess emerging trends and future directions in the field of digital forensics

Course Contents

List of Topics	Weeks
UNIT 1: Introduction to Digital Forensics	1,2
UNIT 2: The Digital Forensics Process	3, 4,
UNIT 3: Cybercrime Law under digital forensic	5, 6, 7
UNIT 4: Digital Forensic Readiness	8, 9, 10
UNIT 5: Computer Forensics	11, 12, 13
UNIT 6: Mobile and Embedded Forensics	14,, 15, 16

Textbook

- Digital Forensics By André Årnes (1st Edition, 2018), ISBN: 9781119262381

- Digital Forensics - Explained, Second Edition, Edited by Greg Gogolin, PhD, CISSP, by CRC Press 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742 ISBN: 9780367502812 (hbk), ISBN: 9780367503437 (pbk), ISBN: 9781003049357 (ebk)

Reference Materials

- Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications, Third Edition, ISSN 1868-0941 ISSN 1868-095X (electronic) Texts in Computer Science, ISBN 978-3-031-53648-9 ISBN 978-3-031-53649-6 (eBook), https://doi.org/10.1007/978-3-031-53649-6, 1st and 2nd editions: © Springer Nature Switzerland AG 2018, 2020, 3rd edition: © The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer, Nature Switzerland AG 2024

Course Learning Outcomes

CLO	Description	Mapped PI
CLO#01	**Understand** the fundamental concepts of digital forensics and crime scene investigation procedures. **Identify** key methodologies and tools for effectively collecting and analyzing digital evidence.	PI 1.1, PI 1.3
CLO#02	**Comprehend** the digital forensics process and its importance, along with the principles that guide forensic practices. Explore the five phases of digital forensics for a comprehensive overview of investigations.	PI 2.2
CLO#03	**Explain** the cybercrime law under the lens of digital forensics, highlighting substantive digital offenses, evidence collection methods, and the vital role of international cooperation in investigations..	PI 4.1, PI 4.3
CLO#04	**Analyze** digital forensic readiness as the organization's preparedness to manage digital evidence during security incidents, highlighting the differences between law enforcement and enterprise approaches. Evaluate the significance of frameworks, personnel roles, and technology usage in forensic labs.	PI 2.3
CLO#05	**Justify** the importance of digital evidence in uncovering insights from electronic devices, involving evidence collection through tools and methods like live data acquisition and forensic imaging, followed by a detailed examination of disk and file structures.	PI 3.1 PI 3.3, PI 5.1, PI 5.3
CLO#06	**Apply** security principles and best practices in digital forensics to safeguard data and system integrity by using response tools for incident response and forensic analysis**.**	PI 6.1, PI 6.3

CLO-PI-SO Mapping

	SO-1	SO-2	SO-3	SO-4	SO-5	SO-6
CLO#01	PI 1.1, PI 1.3	-	-	-	-	-
CLO#02	-	PI 2.2	-	-	-	-
CLO#03	-	-	-	PI4.1,PI 4.3	-	
CLO#04	-	PI 2.3	-	-	-	-
CLO#05	-	-	PI 3.1, PI 3.3	-	PI 5.1, PI 5.3	-
CLO#06	-		-	-	-	PI 6.1,PI 6.3