DEREE COLLEGE SYLLABUS FOR:

ITC 4344 DIGITAL FORENSICS **3/0/3**
(Fall 2020) **UK LEVEL: 6**
UK CREDITS: 15

PREREQUISITES:	ITC 1070 Information Technology Fundamentals ITC 2024 Computer Networks & Cybersecurity Fundamentals ITC 2193 Operating System Concepts
COREQUISITES:	None.
CATALOG DESCRIPTION:	Computer crime and the forensic investigation process; principles and practices; digital evidence on computer systems, hardware storage, the Internet, mobile devices. Computer forensics on data analysis; operating systems forensics; assisting cryptographic techniques; event timing; forensic disk imaging; data recovery; file reconstruction. Rules of evidence and standards; principles of evidential management; the expert witness; standards and ethics.
RATIONALE:	The purpose of this module is to introduce the students to the principles of digital forensics in computers, wireless and wireline networks. The students are exposed to techniques and tools that allow the discovery, collection, preservation and analysis of evidence with the purpose of understanding the weaknesses that made the attacks possible.
LEARNING OUTCOMES:	As a result of taking this course, the student should be able to: 1. Investigate and assess security breaches and network attacks by using digital forensics tools and techniques. 2. Discover, collect, preserve and interpret digital evidence. 3. Critically discuss the ethical and legal aspects of digital forensics.
METHOD OF TEACHING AND LEARNING:	In congruence with the teaching and learning strategy of the college, the following tools are used: • Classroom lectures, laboratory practical sessions using various simulations tools and progress meetings. • Office hours held by the instructor to provide further assistance to students. • Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources.
ASSESSMENT:	**Summative**: 1st assessment: Midterm Exam — Short essay questions and case problems. **30%** 2nd assessment: Portfolio of student work and oral assessment **10%** Final assessment: Individual Project — Investigation, collection and analysis of digital evidence, ethical and legal considerations of a real-world scenario. **60%** **Formative:** Take-home short problems **0%**

	The formative assessments aim to prepare students for the summative assessments and expose them to teamwork. The 1st summative assessment tests the LOs 1 and 2. The 2nd summative assessment tests the LOs 1-3. The final summative assessment tests the LOs 1-3. *The final grade for this module will be determined by averaging all summative assessment grades, based on predetermined weights for each assessment. If students pass the **final summative assessment,** which tests all Learning Outcomes for this module, and the average grade for the module is 40 or above, students are not required to resit any failed assessments.*
INDICATIVE READING:	**REQUIRED READING:** 1. Arnes, A., (2018). Digital Forensics. Wiley **RECOMMENDED READING:** 1. Johansen, G., (2020). Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats (2nd Edition). Packt 2. Hassan, N., (2019). Digital Forensics Basics: A Practical Guide Using Windows OS. Apress. 3. Parasram, Sh., (2017). Digital Forensics with Kali Linux: Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools. Packt. 4. Sachowski, J., (2018). Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise. CRC Press. 5. Holt, Th., et all, (2017). Cybercrime and Digital Forensics: An Introduction (2nd Edition). Routledge. 6. Miller, Pr., & Bryce, Ch. (2017). Python Digital Forensics Cookbook: Effective Python recipes for digital investigations. Packt. 7. Kavrestad, J. (2018). Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. Springer.
INDICATIVE MATERIAL: *(e.g. audiovisual, digital material, etc.)*	**REQUIRED MATERIAL:** N/A **RECOMMENDED MATERIAL:** N/A
COMMUNICATION REQUIREMENTS:	Daily access to the course's site on the College's Blackboard CMS and the acg email. Communication using proper written and oral English. Use of word processor, spreadsheet and presentation SW for documentation and presentation of assignments.
SOFTWARE REQUIREMENTS:	MS-Office Kali Linux (latest version) Cisco Packet Tracer Wireshark VMware Pro SANS SIFT ProDiscover Forensic Volatility Framework Magnet RAM capture The Sleuth Kit (+Autopsy) CAINE

	Xplico FTK Imager X-Ways Forensics Crowdstrike PALADIN EDGE/LTS EnCase
WWW RESOURCES:	• https://www.sans.org/blog/?focus-area=digital-forensics • https://securityaffairs.co/wordpress/ • http://www.forensicfocus.com/ • https://www.infosecurity-magazine.com/digital-forensics/ • https://digitalforensicsmagazine.com/blogs/ • https://ridethelightning.senseient.com/
INDICATIVE CONTENT:	1. Digital Forensics Science 2. Digital Forensics Process 3. Cybercrime Law 4. Digital Forensic Readiness 5. Computer Forensics 6. Mobile and Embedded Forensics 7. Internet Forensics