



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Wales Institute of Science and Art

Applied Computing

Digital Forensics Analysis (ACCA7031)

MILESTONE - Academic Year 2023-24 (Sep 2023) - Sem 1

Lecturer: Dr. Nitheesh Murugan Kaliyamurthy

Contact: n.kaliyamurthy@uwtsd.ac.uk;

To establish concepts relating to essential procedures and corresponding techniques involved in computer forensics process, in correlation to real-world scenarios. Gain understanding of the process of finding evidence related to a digital crime to find the culprits and initiate legal action against them. Understand the methodological procedures and techniques using up-to-date tools that will allow them to facilitate assessments and technical approaches that are necessary to analyse and mitigate risks, threats, vulnerabilities and attacks relating to cyber incidents which could occur across various industries.

Week	Unit(s) Covered	Concepts	Labs
Week 1 (06/10/2023)	Introduction: Cybercrime, Digital Forensics, Cyber Laws	Module Delivery, Assessments, Challenges, Technology in Crime, Typology, Principles of Digital Forensics, Law Enforcement, Security vs Privacy.	Lab Environment and Setup
Week 2 (13/10/2023)	Digital Forensics - Incident Response - Investigative Process	History of Forensics, Evolution of DF, Roles, Challenges, Principles, Regulations, Incident Response Process and Framework	Hands-on Activity 1
Week 3 (20/10/2023)	Digital Forensic Capabilities	Network Evidence (Configurations, Firewalls, Proxys, Packet Captures), Volatile and Non-Volatile Evidences, Mobile Evidences, Cloud, Antiforensic Challenges	Hands-on Activity 2
Week 4 (27/10/2023)	Digital Forensic Evidences	Types, Considerations, Acquisition, Data Preservation, Imaging Tools, Uncovering Digital Evidence, Readiness	Hands-on Activity 3
Week 5 (03/11/2023)	Analyzing Digital Evidences	Analyse Network Evidence, System Memory, Storage, Logs, etc	Hands-on Activity 4
Week 6 (10/11/2023)	Reporting	Documentation, Incident Tracking and Report writing	Hands-on Activity 5

Week 7 (17/11/2023)	Reading/Mid-Assessment Week	Complete all the labs - Work with your Team to compete the Tasks for Coursework	
Week 8 (24/11/2023)	Collect, Analyse, Report	Work on Task 3 and 4 stated in your Coursework	Implement the Hands-on experience reflecting in your Coursework
Week 9 (01/12/2023)			
Week 10 (08/12/2023)	Threat Intelligence	Threat Intelligence, Indicators, MITRE ATT&CK, Hunt Planning and Reporting - Summary	
Week 11 (15/12/2023)		Continue to work with your Task 3, 4 in your Coursework	
Assessment			
	Outcome	Deadline	
Coursework (100%)	provide a systematic understanding of a wide range of current research and technological advances in digital and cyber security incidents and defensive techniques; perform computer forensics, to assess, investigate and analyse digital and cyber security crimes of an organisation with	12/01/2024	Coursework
Readings			
Book	Essential Sachowski, J. (2021). Digital Forensics and Investigations. 2nd Edition. CRC Press.		
Book	Chuck, W. (2021). Penetration Testing Fundamentals. 2nd Edition. Pearson IT Certification.		
Book	Blunden, B. (2014). The Rootkit arsenal: escape and evasion in the dark corners of the system. 2nd Edition. Burlington, Ma Jones & Bartlett Learning.		
Book	Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Analyzing computer security: a threat / vulnerability / countermeasure approach. 3rd Edition. Prentice Hall.		
Book	Johansen, G. (2021). Digital Forensics and Incident Response: An intelligent way to respond to attacks. 2nd Edition. Packt Publishing Limited.		
Book	Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2019). Cybercrime and Digital Forensics: An Introduction. 3rd Edition. Routledge.		
Resources	OWASP Foundation. (n.d.). Open Web Application Security Project (OWASP). [online] Available at: https://owasp.org/ .		
Resources	EC-Council. (n.d.). Computer Hacking Forensic Investigator (CHFI). Retrieved from https://www.eccouncil.org/programs/computer-hacking-forensic-investigator/		
Resources	https://codered.eccouncil.org/?utm_source=aspen&utm_medium=header&utm_campaign=navigation&logged=false		
Resources	tryhackme.com		