Course Title	Incident Response and Forensic Analysis				
Course Code	CYS685				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. If the organization has a mature incident response capability, they will have taken measures to ensure they are prepared to address an incident at each stage of the process. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyze and respond to. The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Detecting these incidents therefore requires additional skills such as forensics, malware analysis and threat detection which help decipher how these threats operate and therefore how they can be prevented and mitigated. Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way. Digital forensics serves as the mechanism for understanding the technical aspects of the incident, potentially identifying the root cause, and discovering unidentified access or other malicious activity				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Understand Incident Response • Managing Cyber Incidents • Define and describe the main phases of incident response • Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident • Identify different kinds of attacks methods to counter their effects • Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up • Explain the principles of evidence collection and the chain of custody • Contact an incident respond analysis • Identify and evaluate key forensic analysis techniques, collect evident data from the incident, Fundamentals of Digital Forensics,				

	Forensic Imaging, Analyzing Evidence, System Memory and System Storage • Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection. • Contact a forensic analysis of the evidence. Examine and analyze the evidence • Writing the Incident Report		
Prerequisites	None	Co-requisites	None
Course Content	Introduction: Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles. Preparation: Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates. Identification: Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC). Containment: Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation. Eradication: Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully. Recovery: Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process. Follow-up: Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement. Digital Forensics Investigation Process: Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures. Technical forensics tools and techniques: Hard disks, removable media and file systems, Windows forensics, duplication/imaging of		

	forensic data, recovering deleted files and hidden or deleted partitions, steganography and image forensics, log analysis, password crackers, network device forensics, packet capture analysis, email tracking, mobile forensics, investigation of attacks, common tools (Autopsy, FTK, etc.) Business case study and lecture: Lecture by invited experts from the cybersecurity industry, including law enforcement. Discussion normally focuses on the practicalities and challenges of incident response and the ways in which forensic analysis contributes to successful cybercrime prosecutions.
Teaching Methodology	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
Bibliography	"*Practical Cyber Forensics*", Niranjan Reddy, Apress "Digital Forensics Basics: A Practical Guide Using Windows OS", Nihad A. Hassan, Apress *Digital Forensics with Kali Linux,* Shiva V. N. Parasram**,** *Packt Publishing* *"Incident Response & Computer Forensics"* by Jason T. Luttgens and Matthew Pepe *"Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response"*, by Leighton Johnson *"The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics"*, by John Sammons *Investigating Windows Systems by Harlan Carvey, Elsevier* *"Digital Forensics with Open Source Tools"*, by Cory Altheide and Harlan Carvey *"Digital Forensics Processing and Procedures"*, by David Lilburn Watson and Andrew Jones
Assessment	Examinations both theory and practice: 50% On-going evaluation through assignments: 50% 100%
Language	English