Subject	Digital Forensics			
	Type	**Semester**	**ECTS**	**Code**
		5	5	
Course Lecturer				
Aims and Objectives	Digital forensic is a hybrid science which offers professionals a systematic approach to perform comprehensive investigation in order to solve computer crimes. The needs for computer forensic experts are growing in corporations, law firms, insurance agencies, and law enforcement. Organizations are now realizing that evidence retrieved from computers and other digital media are becoming more relevant to convicting hackers and criminals. Though this digital evidence can be powerful, but if it is not retrieved through proper investigative procedure, it can be easily damaged and ruled inadmissible in a court of law. The course covers both the principles and practice of digital forensics. Societal and legal impact of computer activity: computer crime, intellectual property, privacy issues, legal codes; risks, vulnerabilities, and countermeasures; methods and standards for extraction, preservation, and deposition of legal evidence in a court of law. This course provides hands-on experience in different computer forensics situations that are applicable to the real world. Students will learn different aspects of digital evidence: ways to uncover illegal or illicit activities left on disk and recovering files from intentionally damaged media with computer forensics tools and techniques.			
Learning Outcomes	Upon completion of this module, participants will be capable to: Describe fundamental computer forensics concepts and procedures. Explain how to recover hidden data for forensic analysis from Windows and Linux/Unix file systems Apply digital forensic tools to discover, collect, preserve and analyze Windows and Linux/Unix digital evidence. Explain how steganography tools work and how to use them to detect and possibly recover hidden information. Document and report digital evidence to court.			
Course Content	**Course Plan**			**Week**
	Introduction to Digital Forensics: structuring, computer crimes, evidence, extraction, preservation.			1
	Criminal Justice system for forensic: legal aspect audit/investigative situations, Investigation Procedures and response.			2
	The Principles of Digital Evidence: Overview of general principles.			3
	Examination of digital evidence at crime scene: data recovery, identifying hidden data, Encryption/Decryption, Steganography.			4
	Live Data Forensics: computer Forensic tools FTK, Autopsy, Axiom Forensics, Belkasoft			5
	Computer Forensic Analyzing Methodologies: crime scene analyzing methodologies and Laboratory analyzing methodologies.			6
	Mobile Network Forensic: Introduction, Mobile Network Technology, Investigations, Examination of smartphones.			7
	Audio and Video Forensics: Analyzing and Interpretation of different file formats.			8
	Network Forensic: Collecting and analyzing network-based evidence, tracking Hackers Through Cyberspace, reconstructing web browsing.			9
	Software Reverse Engineering: defend against software targets for viruses, worms and other malware.			10
	Computer Forensic challenges: human, technology and legal future challenges.			11
	The future of digital forensics: quantum technology and artificial intelligence in use of computer forensics.			12
	Preparation for Exam			
	Exam period			

Teaching/Learning Methods	**Teaching/Learning Activity**			**Weight (%)**
	1. Lectures			50%
	2. Seminars			10%
	3. Practice			25%
	4. Case studies			10%
	5. Role play			-
	6. Problem-based learning			5%
	7. Study visits			-
	8. Work placement			-
Assessment Methods	**Assessment Activity**	**Number**	**Week**	**Weight (%)**
	1. Quiz	2	7,11	%
	2. Group work/project	1	3,..,12	25%
	3. Mid-term exam	1	7	15%
	4. Final exam	1	17	50%
	5. Attendance			10%
Course resources	**Resources**			**Number**
	1. Class (e.g)			1
	2. Laboratory (e.g)			1
	3. Moodle			
	4. Software			1
	5. Projector			1
ECTS Workload	**Activity**		**Weekly hrs**	**Total workload**
	1. Lectures		2	30
	2. Seminars		1	15
	3. Laboratory		1	15
	4. Practice in the industry			6
	5. Independent learning		3/4	55
	6. Exams			4

Literature/References	PowePoint Slides for each lecture Excercises Network Forensics: Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham Prentice Hall, 2012 Guide to Computer Forensics and Investigations (4 th edition). By B. Nelson, A. Phillips, F. Enfinger, C. Steuart. ISBN 0-619-21706-5, Thomson, 2009. Computer Forensics: Hard Disk and Operating Systems, EC Council, September 17, 2009 • Computer Forensics Investigation Procedures and response, EC-Council Press, 2010 • EnCase Computer Forensics., 2014 File System Forensic Analysis. By Brian Carrier. Addison-Wesley Professional, March 27, 2005. NIST Computer Forensic Tool Testing Program (www.cftt.nist.gov/) omputer Forensics: Investigating Data and Image Files (Ec-Council Press Series: Computer Forensics) by EC-Council (Paperback - Sep 16, 2009)
Contact	