#	Lecture	Hours	Preknowledge	Outcomes
1	Course Introduction, digital forensics basics	2	General information about information security.	This lecture will introduce main definitions and terms of digital forensic as well as common methodologies used in the forensic context. Topics discussed include:international standards related to forensic ISO 27001, ISO 20000, ISO / IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031. Also students will get an overview of the local legal aspects of digital forensic and the references for self-education. This lecture should provide a theoretical basis for the forthcoming practical work devoted to the presentation of national laws for computer crime / policies / data protection laws / privacy laws / etc.
2	Description of available forensic tools	2	Windows, Linux and Mac operation systems basics	This lecture is designed to provide students with the basic knowledge of software used for evidences collection and storage. Topics discussed include: description of main digital forensic tools as well as the main steps for their installation and configuration. Also students will be introduced to practical aspects of digital forensic, e.g. report writing &documentation principles. This lecture should provide a theoretical basis for the forthcoming lab devoted to the setting up a forensic workstation.
3	Acquisition basics	2		In this section the student get to know a of forensicly sound acquisition of a device should look like and which kind of tools excists for these acquisitions. The student should also know which main kind of forensically images exists and how to create them.
4	Partition analysis, RAID	2		In this lecture students will get an overview of discstructures in general. By the end of this module/lesson students will be able to: • recall the basics of partitioning schemes, • know about partitions, MBR, GPT, GUID, VBR, • identify components of Master Boot Record,

				• decode the Master Partition Table and Extended Partition Table records.
5	FAT/NTFS file systems, description of applicable tools	2		This lecture will give an overview of datastructure of the file System FAT. It includes the connection between directory entries FAT and data area. The students will get information about the storage of date and time fields and long filenames. By the end of this module/lesson students will be able to: • recall the basics of FAT file system, • explain how FAT is working, • explain and explore the FAT, • describe the changes to the FAT file system when a file is deleted, • identify recovery issues under the FAT file system.
6	NTFS file system and its artifacts	2	Windows operating systems basics Command Line Interface basics Disk structures Numbering Systems	This lecture covers the NTFS file system in-depth. The students will learn about the structure of the file system. They get to know how data is stored and managed by NTFS and how they can analyse the file system to extract evidential data. Theoretical input is suplemented by practical exercises in which the students have to analyse actual NTFS image files.
7	Ext file system and its artifacts	2	Linux operatingsystems basics Command Line Interface basics	This lecture covers the EXT file system. The students will learn about the structure of the file system. They get to know how data is stored and managed by EXT and how they can analyse the file system to extract evidential data. Theoretical input is suplemented by practical exercises in which the students have to analyse actual EXT image files.

			Disk structures Numbering Systems	
8	HFS file system and its artifacts	2	Mac OS Xoperatingsystems basics Command Line Interface basics Disk structures Numbering Systems	This lecture covers the HFS file system. The students will learn about the structure of the file system. They get to know how data is stored and managed by HFS and how they can analyse the file system to extract evidential data. Theoretical input is suplemented by practical exercises in which the students have to analyse actual HFS image files.
9	Windows artifacts (part 1)	2	Windows operation systems basics	This session covers the especially the artifacts which are produced by the Windows Operating System. With these artifacts the students should know which actions and behaviors the user and the system produce during a specified process.
10	Windows artifacts (part 2)	2	Windows operation systems basics	In this session the student get to know which kind od Windows Artefacts exists and how the analyse them. Especially the Windows Events Logs, Firewall Logs and so on.
11	Windows applications artifacts analysis (part 1)	2	Windows operation systems basics	In this session the student get to know how windows application artefacts are located and analysed. In this session the lecture should be to show the student where and how common important windows applications store there informations and how these artefacts can help to provide necesarry informations. These artefacts are for example browser artefacts, skype artefacts, peering programm artefacts and so on
12	Windows applications artifacts analysis (part 2)	2	Windows operation systems basics	In this session the student get to know how windows application artefacts are located and analysed. In this session the lecture should be to show the student where and how common important windows applications store there informations and how these artefacts can help to provide necesarry informations. These artefacts are for

				example browser artefacts, skype artefacts, peering programm artefacts and so on
13	Linux artifacts	2	Linux operating systems basics Command Line Interface basics	In this session the students get to know which evidential data a Linux operating system might contain. In the theoretical parts relevant areas in the Linux operating systems are explained and techniques for analysing the data are shown. The students have to apply those techniques in the practical part of this session. At the end of the session students should be able to extract and analyse evidential data from a Linux operating system.
14	MAC OS artifacts	2	MAC OS X operating systems basics Command Line Interface basics	In this session the students get to know which evidential data a Mac OS X operating system might contain. In the theoretical parts relevant areas in the Mac OS X operating systems are explained and techniques for analysing the data are shown. The students have to apply those techniques in the practical part of this session. At the end of the session students should be able to extract and analyse evidential data from a Mac OS X operating system.
15	Network forensic	2	Network security basics. E.g. advanced network and cloud security course.	This lecture covers the tools, methodology and network evidence types and sources descriptions required for network evidence collection. Within the context of the lecture the relations between operation system and network forensics will be considered. This lecture should provide a theoretical basis for the forthcoming practical work devoted to the using of free tools (Wireshark) for collecting and analyzing of network traffic
16	Live forensic basics	2	Digital Forensics basics Windows, Linux and Mac operation systems basics Command Line	In this session the students will learn how to acquire and extract data from running computer systems. They will learn basic principles and methodologies how to conduct live data forensics. The topics include: Volatile data, acquisition of computer memory, triage techniques, command line tools to acquire volatile data. By the end of the sessions the students should be able to conduct live data forensics.

			Interface basics Networking basics	
17	SSD forensic basics	2	File system basics Disk structures Numbering Systems	This session will explain the students the characteristics when analysing solid state drives. They will be introduced to the structure of SSDs and get to know how techniques like garbage collection, write-amplification and TRIM work. They will also learn which forensic issues and challenges arise when analysing SSDs. By the end of the session the students will be able to carry out an examination of the chip off physical dump.
18	Memory analysis basics	2	Live forensic basics File system basics	In this session the students will learn how to analyse memory dumps that have been acquire using live data forensic techniques. They will get to know the basics of memory structures and will learn how to use tools to extract evidential data out of a raw memory image. The theoretical input will be put into practise in a lab session. In that lab the students will not only have to analyse a given memory dump but also use extracted encryption keys from that dump to open an encrypted container. By the end of the sessions the students will be able to practically extract data of evidential value from a memory image.
	Total lectures:	36		