Module:	**Network Forensics**
Lecturer:	Prof. Dr. rer. nat. Clemens H. Cap
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basics in computer science and mathematics to the extent which is characteristic for a third term student in computer science
Goals / Skill:	The student will learn about the threats and attacks against networks. He or she will study techniques for detecting intrusion, for defending networks and for gathering evidence from an attack on a company network. The **focus** of the module is on understanding the concepts and mechanisms of network security. The **goal** is to enable the student to defend a network and to derive important information from an ongoing attack.
Detailed Content:	- Network intrusion detection. - Building a network monitoring station. - Capturing and analysing network traffic. - Extracting forensic evidence from network traffic.
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations, Lab Exercises by the students.
Literature:	W. Buchanan: Introduction to Security and Network Forensics. Auerbach Publications, 2011. C. Sanders: Practical Packet Analysis. Pollock. 2011. S. Davidoff, J. Ham: Network Forensics. Prentics Hall. 2012
Assigned Tutorials:	Tutorial 1: OpenSSL • Getting familiar with the OpenSSL software package for data encryption and decryption Tutorial 2: RSA & PGP • Getting familiar with RSA encryption and decryption as well as PGP for signing, encrypting and decrypting texts, e-mails, files and directories
Suggested Reading before the start of the summer school:	A text on computer security could be helpful. For example: Ross Anderson: Security Engineering. Wiley, 2008.