INFORMATION SECURITY GROUP

Course Specification 2013-14

Course Code:	IY5609	**Course Value:**	0.5	**Status:**	Option
Course Title:	Digital Forensics			**Availability**	Spring term
Prerequisites:	IY5511, IY5512			**Recommended:**	IY5605
Co-ordinator:	Stephen Wolthusen				
Course Staff	Stephen Wolthusen and John Austen				
Aims:	The objective of this module is to provide the foundations and theoretical underpinnings for an understanding of the way in which data that can subsequently be used as evidence is generated, stored, and transmitted. Based on this, methods for the collection and analysis of digital evidence are covered which will not alter the underlying data or potentially trigger destructive mechanisms and which can be reproduced reliably.				
Learning Outcomes:	After completing this course, students will have • gained an understanding of audit and indirect activity records retained by operating systems, particularly in file systems, and on how to retrieve such information • understanding of selected network protocols and the collection and derivation of evidence leading to the reconstruction of system and user activity based on network trace information • learned about infiltration and anti-forensics techniques used particularly by malicious software • gained an overview of steganographic and particularly steganalytical methods for different types of media • obtained understanding of retention characteristics of storage systems and non-standard devices such as mobile/smart phones, cloud computing, and vehicular systems				
Course Content:	Introduction to forensic science, steps from collecting data to preserving evidence, and a framework for digital forensic evidence collection and processing Fundamentals of host forensics for Microsoft Windows, including kernel architecture, device driver architecture, registry, auditing, and security architecture, file system handling, and reconstruction of file and directory structures on the FAT and NTFS file system families Fundamentals of host forensics for Unix derivatives using the Linux operating system as an exemplar, including kernel and device driver architecture, security and audit mechanisms, file systems and pseudo file systems, and the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars Foundations of network forensics from data capturing and collection to network file systems and supplementary protocols as well as selected application-layer protocols and techniques used for identifying and reverse-engineering protocols used on networks Introduction to malware including anti-forensics and propagation techniques Introduction to steganographic techniques for images, video, textual data, and audio as well as steganalytical techniques for selected media types and approaches to traitor tracing. A survey of non-standard storage mechanisms from retention characteristics to mobile and smart phones and vehicular systems as well as network-based search and storage mechanisms.				
Teaching & Learning Methods:	Lectures and selected self-directed laboratory sessions to reinforce material covered in lectures				
Key Bibliography:	K.J. Jones, R. Bejtlich, C. W. Rose: Real Digital Forensics. Addison-Wesley, 2006 B. Carrier: File System Forensic Analysis. Addison-Wesley, 2005 D. P. Bovet, M. Cesati: Understanding the Linux Kernel, 3rd ed. O'Reilly, 2006 M. Russinovich, D.A. Soiomon, A. Ionescu: Windows Internals, 5th ed. Microsoft Press, 2008				
Formative Assessment & Feedback:	Formative feedback will be given twice during the module in the form of exercise sheets which will be marked and used as the basis for feedback.				
Summative Assessment:	**Exam** (100%) 2 hours. **Coursework:** None. **Deadlines:** None.				