UNIVERSITY OF LONDON | INTERNATIONAL PROGRAMMES

Royal Holloway University of London

University of London International Academy
MSc/PG Dip in Information Security
Lead College – Royal Holloway

Digital Forensics IYM015 (Option)

Aims

This module complements other modules by examining the subject from the criminal angle and presenting a study of computer crime and the computer criminal. We will discuss its history, causes, development and repression through studies of surveys, types of crime, legal measures, and system and human vulnerabilities. We will also examine the effects of computer crime through the experiences of victims and law enforcement and look at the motives and attitudes of hackers and other computer criminals.

Pre-requisites

None

Essential Reading

- Real Digital Forensics (K.Jones, R. Bejtlich C.W.Rose)

Included as study material once registered on the course.

Assessment

This module is assessed by a two hour unseen written examination.

Learning Outcomes

On completion of the module students should be able to:

- follow trends in computer crime
- relate computer security methodologies to criminal methods
- detect criminal activity in a computerised environment
- apply the criminal and civil law to computer criminality
- understand how viruses, logic bombs and hacking are used by criminals
- appreciate the views of business, governments, and the media to instances of computer crime.

Syllabus

***Unit 1*- Administrative matters**

• Overview of module and topics covered
• Exercises, tutorials, and formative feedback

***Unit 2* - An introduction to forensic science**

• Legal background
• Forensic science
• A.C.P.O. Guidelines

Unit 3 **- Forensic evidence collection and processing**

- Types of evidence
- Chain of evidence
- Phases of a (digital) forensic examination

Unit 4 **- The Microsoft Windows kernel architecture**

- Operating system principles and functions
- Major subsystems, information and control flows through the MicrosoftWindow operating system kernel
- Windows Device Driver Model and driver layering
- Configuration database mechanisms and life-cycle

Unit 5 **- Microsoft Windows security architecture**

- Components constituting the Microsoft Windows security architecture
- Access control mechanisms
- Auditing mechanisms
- Introduction to Virtualisation and surrounding security issues

Unit 6 **- Introduction to Live Forensics**

- The Microsoft Windows NT kernel architecture
- MS Windows device driver architecture
- I/O processing
- Registry database
- The security architecture of Microsoft Windows NT
- Auditing subsystem: Event log

Unit 7 **- Microsoft Windows Storage Architecture**

- Fixed disk storage abstractions
- Dynamic file systems and major subsystems involved in storage management
- Interactions with the virtual memory architecture
- Abstract file system architecture
- Partition and volume management

Unit 8 **- The File Allocation Table File System**

- Development and extensions of the basic File Allocation Table mechanism are described
- FAT file system organisation is discussed in depth
- Directory structures and attributes
- The exFAT extension mechanism

Unit 9 **- The Microsoft NTFS File System**

- Key features and attributes of NTFS
- Data structures and limitations
- File and directory attributes and their storage loci
- File system recovery and self-healing mechanisms
- File and volume encryption

Unit 10 **- Linux Kernel Architecture**

- Development and timeline for Unix derivatives
- The Linux 2.6 kernel series
- A high-level review of kernel components and concepts
- Configuration and management virtual file systems

Unit 11 **- Linux and Unix Security and Audit Architecture**

- Privilege separation
- Access control mechanisms
- Linux Security Modules and the SELinux Architecture
- The Linux auditing infrastructure

Unit 12 **- Introduction to Live Forensics II**

- In-system and external data acquisition
- Memory analysis techniques including *carving* of known and unknown data structures
- Counter-forensic techniques, particularly for evading or manipulating memory dumps
- Live acquisition techniques: Physical RAM persistence effects Cryptographic Applications