MACS H6015: Digital Forensics

Short Title:	Digital Forensics APPROVED
Full Title:	Digital Forensics

Module Code:	MACS H6015

ECTS credits:	10

NFQ Level:	9

Module Delivered in	2 programme(s)

Module Contributor:	Christina Thorpe

Module Description:	The purpose of this module is to provide students with the knowledge and skills to perform a digital forensic investigation. Throughout the module, the students will learn about: (1) The various different types of digital crime and investigations (private, corporate, and public). (2) The role of an investigator. (3) A methodology for performing a digital forensics investigation. (4) Many common open source and commercial tools used for imaging and analysis. (5) Low level file system forensics (FAT and NTFS). (6) Students will gain extensive experience using FTK tools.

Learning Outcomes:

On successful completion of this module the learner will be able to

1. Appraise the fundamental legal considerations when dealing with digital forensics evidence and demonstrate how to apply appropriate measures to maintain evidence integrity.
2. Evaluate computer filesystems and demonstrate how to apply the low level filesystem knowledge to manually decode digital evidence.
3. Research how to apply the digital forensic methodology, skills, and techniques to investigate an incident involving digital evidence.
4. Demonstrate how to write a digital forensics report using a realistic professional template and style.

Module Content & Assessment

Indicative Content
Introduction to Digital Forensics Introduced the key concepts of the Digital Forensics profession and investigations. The role of an investigator. The types of evidence. The fundamental legal considerations. Digital forensics methodology. The investigators lab. Types of investigations: public, private, criminal.
Data Acquisition The tools and techniques used to acquire digital evidence in a forensically sound manner. A description of the low level technical details involved in acquisition. The legal considerations. The chain of evidence. The various tools: dd, ftp imager, etc. Verifying the image using hash functions. Using write blockers: hardware and software.
The FAT Filesystem The evolution of the FAT filesystem, FAT12, FAT16, FAT32. The structure of FAT. The contents of each component. Saving and deleting a file in FAT. Manual decoding the boot sector fields, the timestamps in the root directory, and the FAT chaining in FAT12. Long file names.
The NTFS Filesystem The history of NTFS. The structure of NTFS. Details of each component: The boot sector, MFT, records, attributes, system attributes. Alternate Data Streams. Manual decoding of fields in the boot block. 2's compliment.
Mobile Devices Types of devices and hardware platforms; operating systems and their environments and tools; Systems logs; vulnerabilities; Analysis Reports For Complex Cases; Case Studies; Data Hiding Techniques; Dealing with Encryption and Passwords; Log Analysis; Testing and Verification Methodology; Metadata; Communication Forensics.
Analysis Techniques and Methodologies Overview of open source tools and commercial products for analysis digital systems. Comparison of different suites of tools on various systems. Effective keyword searching. Regular expressions. Data carving. Case management. Exporting. Password cracking. Places to look for evidence. Developing a methodology.
Network Forensics Introduction to network forensics; evidence acquisition; packet analysis; protocol analysis; practical exercises dealing with packet capture files; investigation methodology; introduction to various network forensic tools.
Email Tracing Why it is important. How email is abused. Email fundamentals. Important services. Email protocols. Spoofing SMTP. SMTP headers. SMTP server logs. UNIX sendmail. Techniques for identifying spoofed mail. Timestamps and timezones.
Writing a Forensics Report Best practices. Note taking. Legal considerations. Formats. Content. Styles.

Indicative Assessment Breakdown	%
Course Work Assessment %	100.00%

Course Work Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
In-class test	A class test to evaluate the theory delivered in the first 6 weeks of the semester.	1,2	35.00	Week 7
Practical/Skills Evaluation	Practical evaluation of forensic investigation skills.	3	35.00	Week 12
Written Report	Write a report for a forensic investigation conducted on a disk image.	4	30.00	Sem 1 End

No Final Exam Assessment %

Indicative Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

ITB reserves the right to alter the nature and timings of assessment

Indicative Module Workload & Resources

Indicative Workload: Full Time	
Frequency	**Indicative Average Weekly Learner Workload**
Every Week	30.00
Every Week	30.00
Every Week	140.00

Resources

Recommended Book Resources

Brian Carrier 2005, *File System Forensic Analysis*, Addison-Wesley Professional

Bill Nelson, Christopher Steuart, Amelia Philips 2015, *Guide to Computer Forensics and Investigations*, 5th Ed.

Sherri Davidoff, Jonathan Ham 2012, *Network Forensics: Tracking Hackers Through Cyberspace*

This module does not have any article/paper resources

Other Resources

Internet based resource: *1*
http://www.securityfocus.com/

Internet based resource: *2*
http://www.knoppix-std.org/

Internet based resource: *3*
http://www.e-fense.com/

Internet based resource: *4*
http://www.f-secure.com/

Internet based resource: *5*
http://www.owasp.org/

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_KMACS_R	Master of Science in Computing in Applied Cyber Security	1	Mandatory
BN_KMACS_M	Master of Science in Computing in Applied Cyber Security (Research)	1	Group Elective 1