1. **Title of the module**

COMP8230 (CO823) Introduction to Digital Forensics

1. **Division or partner institution which will be responsible for management of the module**

Division of Computing, Engineering, Mathematical Sciences (CEMS)

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 7

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Autumn or Spring

1. **Prerequisite and co-requisite modules**

None

1. **The courses of study to which the module contributes**

Portfolio of Taught Postgraduate Courses in Computing, with and without Industrial Placement

1. **The intended subject specific learning outcomes.  
   On successfully completing the module students will be able to:**
   1. Demonstrate a systemic understanding of underpinning concepts and best practices in relation to digital forensic investigations.
   2. Select and apply techniques and methods most suitable for collection and interpretation of data of evidential value for a Court of Law in a forensically sound manner.
   3. Critically evaluate methodology options and course of actions to undertake digital forensic investigations given a case scenario.
   4. Demonstrate the ability to analyse uncovered digital evidence to answer typical investigative questions such as what, when, where, who, and how.
   5. Apply and critically evaluate professional practices for reporting of findings from digital forensic investigations.
   6. Critically evaluate challenges faced by digital forensic investigators resulting from advances in technology and widespread use of digital devices.
2. **The intended generic learning outcomes.  
   On successfully completing the module students will be:**

9.1 Demonstrate the ability for critical thinking, reasoning and reflection.

9.2 Produce a specification of the operation of a complex system based on an understanding of the component parts.

9.3 Undertake critical appraisal of a candidate system design and reflect upon its merits.

9.4 Study independently and make appropriate use of relevant resources learning in order to advance their knowledge and understanding.

9.5 Demonstrate personal and interpersonal skills, and work as a member of a team.

9.6 Learn effectively and critically for the purpose of continuing professional development.

9.7 Manage time and resources within a potentially complex problem domain.

9.8 Master the use of general IT facilities including information retrieval skills.

1. **A synopsis of the curriculum**

This module will aim to familiarise students with core concepts (e.g., Locard’s exchange principle, and legal admissibility of digital evidence) and best practices (e.g., the ACPO Good Practice Guide for Digital Evidence, Contemporaneous Notes taking, and the SWGDE guidelines) underpinning digital forensic investigations. It introduces methodologies that guide the digital investigative process (i.e., collection, interpretation, analysis and reporting), and key techniques that can be applied for interpretation and analysis of digital evidence in the context of digital forensics in general (e.g., hashing, and file carving), computer forensics (e.g., windows registry analysis and metadata analysis), and multimedia forensics (e.g., multimedia source analysis for device identification, and multimedia content analysis for forgery detection).

The module also discusses challenges faced by digital forensics due to the increasing volume and diversity of data sources involved in investigations.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press; 3 edition. ISBN 978-0123742681.

[Altheide](https://www.amazon.co.uk/Cory-Altheide/e/B004MD0240/ref=dp_byline_cont_book_1), C. and [Carvey](https://www.amazon.co.uk/s/ref=dp_byline_sr_book_2?ie=UTF8&field-author=Harlan+Carvey&text=Harlan+Carvey&sort=relevancerank&search-alias=books-uk), H. (2011). Digital Forensics with Open Source Tools.  Syngress. ISBN 978-1597495868.

Ho, A. T. S. and Li, S (2015). *Handbook of Digital Forensics of Multimedia Data and Devices*. Wiley-IEEE Press. ISBN 978-1118640500

<http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf>

<https://www.swgde.org/documents/published>

1. **Learning and teaching methods**

Total contact hours: 30

Private study hours: 120

Total study hours: 150

1. **Assessment methods**
   1. Main assessment methods

2 hour written exam (50%)

Problem Solving Exercises (20% and approximately 10 hrs)

Mock Digital Forensics Investigation (30% and approximately 20 hrs)

* 1. Reassessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section 12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | *8.1* | *8.2* | *8.3* | *8.4* | *8.5* | *8.6* | *9.1* | *9.2* | *9.3* | *9.4* | *9.5* | *9.6* | *9.7* | *9.8* |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Lectures | x | x | x | x | x | x | x | x | x | x |  |  | x | x |
| Private study | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Problem Solving Exercises |  | x |  | x |  |  | x |  | x | x | x | x | x | x |
| Mock DF investigation |  | x | x | x | x |  | x |  | x | x | x | x | x | x |
| Examination | x | x | x | x |  | x | x | x | x |  |  |  |  |  |

1. **Inclusive module design**

The Divsion recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

The topics addressed by this module relate to a field that is of international importance, given the global role of computers in today's technological innovation. The topics covered by this module are international in nature, being identical worldwide and independent of traditional spoken language.

**DIVISION USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of the delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
|  |  |  |  |  |
|  |  |  |  |  |