De Montfort University

Course Template

1. Basic information

- Course Name: Forensic Computing
- Course Code: CC501A
- Level (UG, PG): Undergraduate
- Academic Period: 2014
- Faculty: Faculty of Technology
- Department: Computer Engineering and Cyber security
- PMB COMP
- Offered at: DM - DMU Leicester
- Type (single, joint.): SI
- Highest Award : Bachelor of Science (Honours)
- All possible exit awards : Bachelor of Science; Certificate of Higher Education; Diploma of Higher Education; Institutional Undergraduate Credit
- Award notes :

Professional Body Recognition

- Accreditation by Professional/Statutory body:

No

- Exemption by Professional/Statutory body:

No

- Details

- Modes of attendance: Main MOA: Full-Time
  Other MOA: Part-Time; Year Out/On Placement
- Mode Notes:

- Course leader: Peter Norris

2. Entry Requirements and Profile

Award BSc (Hons) Standard Entry Requirements Candidates must normally offer the following (or an equivalent) - 5 passes at GCE/GCSE level including Mathematics and English with - A-level: 260 points with at least 2 subjects passed at A2 or AVCE Applicant profile BSc(Hons) Forensic Computing should attract applicants who like puzzles, are methodical and enjoy grappling with detail. They should be logical and have good language skills. Evidence of ability to work systematically on a problem until it is resolved is a valuable indication of success in this field. Specific prior experience in either computing and/or law is not needed.

3. Course Description

Characteristics and Aims

Prospectus entry Why this programme? BSc(Hons) Forensic Computing is concerned with the detection, preservation, analysis and presentation of digital evidence equips graduates to meet the challenge of combating computer crime pays attention to computer security

has been developed in consultation with regional electronic crime law enforcement specialists

The programme
The opportunities for criminals to use digital electronics are countless: mobile phones hold details of criminal contacts; the Internet is used to distribute child pornography; sophisticated fraud is carried out by identity theft. The combination of ready availability, simplicity of use, mobility, phenomenally high performance and ridiculously low price offers the criminal imagination enormous possibilities.

A society where digital crime is limited solely by the criminal imagination is an unpleasant prospect. That we are not living through this depressing scenario is due in part to the efforts of existing Forensic Computing specialists - individuals who prevent crime by ensuring the security of computer systems or who support law enforcement by skilled handling of digital evidence.

The course is built around three major strands:
- technical (what is possible)
- professional (what is permissible)
- practice (what is appropriate)

The technical strand develops understanding of digital computers. From this understanding flows the ability to work with computers, either avoiding being the target of cyber crime, or handling potential evidence after an incident. Topics studied include:
- data storage, data representation, data communication,
- computer processes, operating systems, security,
- the Internet, protocols, client / server programming

The professional strand establishes the context in which the Forensic Computing specialist performs. The strand deliberately balances the possibilities that the technical strand opens up, with the professional responsibilities of handling digital evidence. Topics studied include:
- ethics and its relation to the law and computing,
- computer law, legal processes, digital evidence
- regulatory framework of digital investigation

The practice strand creates specific scenarios to be investigated. These case studies bring together the technical and professional strands, together with additional teaching appropriate to the particular case study. Topics studied include:
- using appropriate tools from the forensic computing toolkit
- evidence analysis
- presentation of evidence

Industrial Placement
The third year placement is compulsory. Some student placements will be overtly forensic computing in nature. Other placements will be within the broad computing industry but with no obvious forensic content. In both cases, the placement year provides invaluable experience, experience either of the investigation of computer incidents, or of the general working environment where much unethical activity could take place.

Teaching, Learning and Assessment Strategies

The professional and technical skills will be taught as distinct themes of modules throughout the course. They will be fused together in each year of the course by one or more case studies. Wherever appropriate, the material and / or context for these case studies will be drawn directly from Leics Police.
A conventional mix of timetabled contact to introduce concepts, unstaffed student activity to take ownership of concepts, and small group staffed activity to make timely formative interventions, will be used.
Informal contact between tutors in the relatively small course team should ensure the correct sequencing of material within the professional, technical and case study themes.

4. Outcomes

Generic outcome headings	What a student should know and be able to do upon completion of the course
• **Knowledge & understanding**	1a) Can explain the characteristics of data. 1b) Can explain the process of code execution in digital computer. 1c) Can explain the requirements of digital evidence. 1d) Can explain the security threats to a computer system.
• **Cognitive skills**	2a) Can identify and maintain a position of professional integrity. 2b) Can formulate an appropriate investigative response to a computer incident. 2c) Can reason about digital evidence.
• **Subject specific skills**	3a) Can perform a forensic investigation of computer equipment. 3b) Can identify potential digital evidence. 3c) Can preserve material that might be used as digital evidence. 3d) Can analyse material that might be used as digital evidence. 3e) Can present digital evidence. 3f) Can select and apply appropriate investigative tools. 3g) Can analyse the exposure of a computer system to malevolent use.
• **Key Skills**	4a) Can collaborate effectively with other specialists in multidisciplinary teams. 4b) Can maintain professional competence via CPD. 4c) Can present complex concepts with clarity.

5. Structure and Regulations

Relationship Details

Module	Credits	Level	Take/Pass	Semester	Locations
CTEC1401	**30.00**	**1**	**Must Take**	**Y**	**DM**
CTEC1412	**30.00**	**1**	**Must Take**	**Y**	**DM**
CTEC1801	**30.00**	**1**	**Must Take**	**Y**	**DM**
CTEC1901	**30.00**	**1**	**Neither**	**Y**	**DM**
CTEC2121	**30.00**	**2**	**Must Take**	**Y**	**DM**
CTEC2122	**30.00**	**2**	**Must Take**	**Y**	**DM**
CTEC2701	**30.00**	**2**	**Must Take**	**Y**	**DM**
LAWG2003	**30.00**	**2**	**Must Take**	**Y**	**DM**
SAND2802	**0.00**	**2**	**Neither**	**Y**	**DM**
CTEC3110	**15.00**	**3**	**Neither**	**Y**	**DM**
CTEC3426	**15.00**	**3**	**Neither**	**Y**	**DM**
CTEC3427	**30.00**	**3**	**Must Take**	**Y**	**DM**
CTEC3428	**30.00**	**3**	**Must Take**	**Y**	**DM**
IMAT3406	**15.00**	**3**	**Neither**	**Y**	**DM**
IMAT3429	**15.00**	**3**	**Neither**	**Y**	**DM**
IMAT3451	**30.00**	**3**	**Must Take**	**Y**	**DM**

Structure

Structure notes

1 Structure Notes

The course structure is recorded on the spreadsheet, constructed annually for timetabling

Course Specific Differences or Regulations

1 Placement must be passed to progress to BSc Hons Forensic Computing final year.
A student who fails placement but otherwise has sufficient credits may progress to BSc Computer Studies.

The requirements to progress into the sandwich are determined by Faculty Policy which requires that normally student must have passed a minimum of 60 credits at level 2.

Numbers at sites, including partner institutions

1

Relevant QAA Subject Benchmarking statement(s)

1 This programme has been informed by the QAA Subject Benchmark Statement in Computing.

6. Quality Assurance Information

QA of Workbased Learning

Liaison with Collaborative Partners

Procedures for Maintaining Standards

The Programme is managed by a programme leader together with a programme team. They are guided by the prevailing academic regulations and modular scheme handbooks produced by Registry.

An external examiner is attached to the programme who acts as a critical friend. He/She attends the assessment board and scrutinises student work and marking to ensure that standards have been maintained at an apposite level.

Each year the programme leader completes a Programme Enhancement Plan which is approved by the Programme Board/Subject Authority Board and Faculty Academic Committee.

The student voice is heard via student representatives on the Programme Board and the Staff Student Consultative Committee. Feedback from students is gathered by end of module questionnaires and programme questionnaires.

The programme is subject to a periodic review in line with University requirements.

Course Handbook Descriptor