

Programme Specification

MSc Electronic Security and Digital Forensics



1. Programme title	MSc Electronic Security and Digital Forensics
2. Awarding institution	Middlesex University
3. Teaching institution	Middlesex University
4. Details of accreditation by professional/statutory/regulatory body	British Computer Society
5. Final qualification	MSc
6. Year of validation Year of amendment	
7. Language of study	English
8. Mode of study	FT/PT

9. Criteria for admission to the programme

The principal criteria for admission are that entrants are capable of working at postgraduate level and are able to succeed at, and benefit from, the programme. The following would normally be considered appropriate entry qualifications:

- An Honours Degree in a discipline related to the programme, such as relevant numerate subjects or those providing a significant exposure to Information Technology, or
- An Honours Degree together with employment or professional experience in a field relevant to the programme and at an appropriate level in the field.

International students whose first language is not English or who have not been taught in the English medium throughout must achieve an IELTS score of 6.5 or TOEFL 575 (paper based) 231 (computer based).

University policies supporting students with disabilities apply, as described in the Guide and Regulations, 'Information for Students with Disabilities'.

10. Aims of the programme

The programme aims to:

- Give students a sound theoretical and practical understanding of principles and

concepts in electronic security and digital forensics.

- Equip students with relevant theoretical and practical understanding of tools, techniques, procedures and skills necessary to effectively carry out effective digital forensic investigations especially relating to computer incidents and computer misuse.

- Equip students with knowledge of legal and professional issues relevant to computer-related crime, digital evidence and digital forensic investigations.

- Give students a broad understanding of regulatory compliance and the detection, investigation and prevention of **financial crime** in corporate environments

- Equip students with relevant knowledge of principles and concepts in information security management.

- Develop critical, analytical and intellectual abilities of students by nurturing creative and independent thinking, and the ability to communicate clearly and coherently.

11. Programme outcomes

A. Knowledge and understanding

On completion of this programme the successful student will have knowledge and understanding of:

Tools and techniques necessary for carrying out digital forensic investigations.

The nature, collection, handling and analysis of digital evidence in a forensic investigation.

Regulatory compliance and the detection, investigation, and prevention of financial crime in corporate environments

Electronic crime investigation frameworks, guidelines and procedures.

Legal and professional issues related to computer-related crime, digital evidence

Teaching/learning methods

. Students gain knowledge and understanding and develop cognitive skills and abilities through self directed, resource based learning, small group discussions, small group and individual exercises, lab sessions, demonstration software, on-line examples and the research project.

Weekly seminar sessions supported by the Local Study Centre Tutor(s) provide the opportunity to address questions, queries and problems.

Throughout their studies students are encouraged to undertake independent study

<p>and digital forensic investigations. Principles and concepts of information security management</p>	<p>both to supplement and consolidate what is being learnt and to broaden their individual knowledge and understanding of the subject. Critical evaluation and selection of methods, tools and solutions engage the students in relating theory to practice</p> <p>Assessment Methods</p> <p>Students' knowledge and understanding is assessed by: Individual coursework, presentations, the unseen examination and the project thesis assess students' knowledge and understanding.</p>
<p>B. Cognitive (thinking) skills</p> <p>On completion of this programme the successful student will be able to:</p> <ol style="list-style-type: none"> 1. Apply relevant tools and techniques to carry out a digital forensic investigation. 2. Investigate, collect and analyse and present relevant digital evidence from computing devices including mobile platforms. 3. Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating and preventing financial crime. 4. Advise on relevant legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations. 5. Manage information security procedures and processes. 6. Analyse information security problems and implement effective solutions as an individual or in cooperation with others. 	<p>Teaching/learning methods</p> <p>Students develop practical abilities through the teaching and learning programme outlined above. These abilities are also nurtured through small group discussions, small group and individual exercises, laboratory sessions, demonstration software, on-line problem-solving examples and the research project.</p> <p>Assessment methods</p> <p>Students' practical abilities are principally assessed through coursework reports and the thesis report, with examination questions addressing aspects of practical abilities as appropriate to the subject material.</p>
<p>C. Practical skills</p>	<p>Teaching/learning methods</p>

<p>On completion of the programme the successful student will be able to:</p> <ol style="list-style-type: none"> 1. Select and use a variety of modes of discourse for effective communication according to the needs of the intended audience. 2. Perform effectively as a member of a team in complex and diverse working environments. 3. Demonstrate a critical understanding of, and the ability to deploy effectively, a wide range of learning methods resources and technologies, including, but not limited to, Information and Communication Technologies. 4. Manage their own learning and development autonomously, demonstrating time management and organisational skills at a professional level. 5. Demonstrate self-direction and originality in learning and problem-solving in familiar and unfamiliar situations. 6. Appreciate the need for continuing professional development in recognition of the need for lifelong learning. 	<p>Students learn transferable skills through the teaching and learning programme outlined above. Although not all the skills are explicitly taught, they are nurtured and developed throughout the programme, which is structured and delivered in such a way as to promote this process.</p>
	<p>Assessment methods</p>
	<p>Students' practical skills are assessed by</p> <ul style="list-style-type: none"> • Outcome 1 is assessed through coursework and examination, presentations and the project report. • Outcome 2 is assessed through coursework. • Outcome 3 is assessed primarily through examinations. • Outcome 4 is assessed through coursework • Outcomes 5 and 6 are assessed primarily through the research project report. • Outcomes 6 and 7 are assessed through individual coursework involving critical analysis and giving advice.
<p>D. Graduate skills</p>	<p>Teaching/learning methods</p>
<p>On completion of this programme the successful student will be well equipped for a career in the rapidly expanding fields of Digital Forensics and IT Security Management.</p>	<p>Students acquire graduate skills through the teaching and learning programme outlined above.</p>
	<p>Assessment methods</p>
	<p>. Students' graduate skills are assessed by individual and/or group coursework, and unseen examinations.</p>

<p>Students must take all of the following:</p> <p>BIS4600: Legal and Professional Aspects of Digital Forensics</p> <p>BIS4610: Information Security Management</p> <p>BIS4620: Digital Investigation and Evidence Management</p> <p>BIS4630: Corporate Compliance and Financial Crime Prevention.</p> <p>BIS4992: Postgraduate Computing Project</p>		<p>Students may not commence BIS4992 until they have obtained 120 credits, i.e. they must pass all taught modules.</p>
---	--	--

12.3 Non-compensatable modules (note statement in 12.2 regarding FHEQ levels)

Module level	Module code
Level 7	BIS4992

13. Curriculum map

See attached.

14. Information about assessment regulations

- Information on how the University formal assessment regulations work, including details of how award classifications are determined, can be found in the University Regulations at <http://www.mdx.ac.uk/regulations/gradecriteriaguide.aspx>
- Practical aspects of the programme are often assessed via coursework that may be carried out using specialist software and may include lab tests.
- Theoretical material is assessed by coursework and examinations.

Grades are awarded on the standard University scale of 1–20, with Grade 1 being the highest. To pass a module all components, both coursework and examination, must be passed individually with a minimum grade of 16. Failure in one of the components will result in the failure of the module.

15. Placement opportunities, requirements and support (if applicable)

16. Future careers (if applicable)

All programmes in the School of Science and Technology – their curricula and learning outcomes – have been designed with an emphasis on currency and the relevance to future employment.

- The majority of graduates are employed in IT posts relevant to the subject.
- Over 20% of students pursue further postgraduate study or research.

The employer links with the School are encouraged in a number of ways e.g. by inviting practitioners from industry as guest speakers in lectures; through links with companies where students are employed as part of their Industrial placement and through alumni both in the UK and overseas

Campus Careers Offices can be found on each campus for advice, support and guidance – or go to <http://www.mdx.ac.uk/campus/support/careers/index.asp>

17. Particular support for learning (if applicable)

The School's Teaching and Learning Strategy is compliant with those of the University, in seeking to develop learner autonomy and resource-based learning.

In support of the students learning experience:

- All new students go through an induction programme and some have early diagnostic numeric and literacy testing before starting their programme. Learning Resources (LR) provide workshops for those students needing additional support in these areas.
- Students are allocated a personal email account, secure networked computer storage and dial-up facilities
- New students are provided with a hard copy of the schools Subject Handbook at enrolment (electronic copies for all students can also be found at UniHub).
- Soft copies of all module handbooks can be found online. Web-based learning materials are provided to further support learning
- Extensive library facilities are available on all campuses. This is available as learning resources through the My Learning Portlet system
- High-quality specialist network, software, digital and wireless laboratories equipped with industry standard software, hardware and tools as appropriate, for formal teaching as well as self-study. Middlesex University is a Cisco Local Academy and a Xilinx University partner
- Access to campus based teaching and learning support drop in sessions, arranged by the school to provide assistance and guidance
- Tutorial sessions for each module organised for groups of up to 20 students are provided for additional teaching support
- Formative feedback is given on completion of student coursework
- Past exam papers with solutions and marking schemes for all modules are available for students in module handbooks and at UniHub
- Research activities of academic staff feed into the teaching programme, which can provide individual students with ad-hoc opportunities to work with academics on some aspect of research

Middlesex University encourages and supports students with disabilities. Some practical aspects of Science and Technology programmes may present challenges to students with particular disabilities. You are encouraged to visit our campuses at any time to evaluate facilities and talk in confidence about your needs. If we know your individual needs we'll be able to provide for them more easily. For further information contact the Disability Support Service (email:

disability@mdx.ac.uk)

18. JACS code (or other relevant coding system)

G500

19. Relevant QAA subject benchmark group(s)

Computing

20. Reference points

21. Other information

The following reference points were used in designing the programme:

- QAA Framework for Higher Education Qualifications in England, Wales and Northern Ireland
- QAA Computing subject benchmark statement
- Towards Benchmarking Standards for Taught Masters Degrees in Computing (sponsored by CPHC), May 2004
- QAA/CLQE guidelines for programme specifications
- QAA Code of Practice for the assurance of academic quality and standards in HE
- University Policy, Regulations and Guidelines

Middlesex University and School of Science and Technology Teaching Learning and Assessment policies and strategies.

Appendix 2: Curriculum Map for MSc Electronic Security & Digital Forensics

This section shows the highest level at which programme outcomes are to be achieved by all graduates, and maps programme learning outcomes against the modules in which they are assessed.

Programme learning outcomes

Knowledge and understanding		Practical skills	
A1	Knowledge and understanding of tools and techniques necessary for carrying out digital forensic investigations.	C1	Select and use a variety of modes of discourse for effective communication according to the needs of the intended audience.
A2	Knowledge and understanding of the nature, collection, handling and analysis of digital evidence in a forensic investigation.	C2	Perform effectively as a member of a team in complex and diverse working environments.
A3	Knowledge of regulatory compliance and the detection, investigation, and prevention of financial crime in corporate environments.	C3	Demonstrate a critical understanding of, and the ability to deploy effectively, a wide range of learning methods resources and technologies, including, but not limited to, information and communication technologies.
A4	Knowledge and understanding of electronic crime investigation frameworks, guidelines and procedures.	C4	Manage their own learning and development autonomously, demonstrating time management and organisational skills at a professional level.
A5	Knowledge and understanding of legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations.	C5	Demonstrate self-direction and originality in learning and problem-solving in familiar and unfamiliar situations.

A6	Knowledge and understanding of principles and concepts of information security management.	C6	Appreciate the need for continuing professional development in recognition of the need for lifelong learning.
Practical Abilities			
B1	Apply relevant tools and techniques to carry out a digital forensic investigation.		
B2	Investigate, collect, handle, analyse and present relevant digital evidence from computing devices including mobile platforms.		
B3	Advise on managing compliance in corporate environments and implementing tools and techniques for detecting, investigating and preventing financial crime.		
B4	Advise on relevant legal and professional issues related to computer-related crime, digital evidence and digital forensic investigations		
B5	Manage information security procedures and processes.		
B6	Analyse information security problems and implement effective solutions as an individual or in cooperation with others.		

Programme outcomes																			
A1	A2	A3	A4	A5	A6		B1	B2	B3	B4	B5	B6		C1	C2	C3	C4	C5	C6

Module Title	Module Code and Level	Programme outcomes																	
		A1	A2	A3	A4	A5	A6	B1	B2	B3	B4	B5	B6	C1	C2	C3	C4	C5	C6
Legal and Professional Aspects of Digital Forensics	BIS4600		✓		✓	✓					✓			✓					✓
Information Security Management	BIS4610						✓					✓	✓			✓	✓		✓
Digital Investigation and Evidence Management	BIS4620	✓	✓		✓			✓	✓					✓		✓	✓	✓	
Corporate Compliance and Financial Crime Prevention	BIS4630		✓	✓	✓			✓		✓				✓	✓	✓	✓		✓
Postgraduate Computing Project	BIS4992													✓		✓	✓	✓	✓

