LEEDS BECKETT UNIVERSITY

Course information for applicants

This information applies to the course as it will be delivered to students starting the course in 2027/28.
Information provided here was confirmed on 24/08/2026

General information

Programme code
CSDFM

Target award
If you complete this course successfully you will be eligible for the award of:
MEng Cyber Security and Digital Forensics

Delivery mode
✓ On campus
☐ Distance learning

Where you will study
The majority of teaching will be at Headingley campus but on occasion may be at City campus.

Professional accreditation or recognition

Professional body
British Computer Society (BCS) - The Chartered Institute for IT

Summary of the accreditation or recognition
A graduate meets some or all of the educational requirements for registration with BCS as a Chartered IT Professional (CITP). BCS will not accredit until graduates have exited the award.

Awarding body
Leeds Beckett University

Regulator
Office for Students

Level of qualification
Level 7 of the Framework for Higher Education Qualifications

Course duration

If you are made an offer of a place on the course, your offer letter will include the start date.

This course can be studied:
4 years full-time (September start only)
5 years full-time with a placement year (September start only)

Work placement

If you opt to undertake a full year placement and this is completed successfully you will have the words 'with placement year' added to the award title including for any contained awards that you are eligible for.

Placement Delivery

Students are responsible for obtaining their own placement, with assistance from the University.

Location

Placement location will vary dependant on the opportunity.

Approval

Whilst students source their own placements, they will need to meet requirements which will be outlined before module enrolment.

Entry requirements

Admissions criteria are available on the online prospectus entry for this course.

If you have previous relevant qualifications or experience, you could be exempt from certain parts of your course. Recognition of prior learning (RPL) allows you to start your course at a point appropriate to the learning and skills that you may have developed in a professional, vocational or community setting.

Find out more here: https://www.leedsbeckett.ac.uk/student-information/course-information/recognition-of-prior-learning
If you have questions about entry requirements and admissions, contact AdmissionsEnquiries@leedsbeckett.ac.uk

Course fees

Course fees and a breakdown of any additional costs is included on the online prospectus entry for this course.

If you have questions about fees for this course, contact Fees@leedsbeckett.ac.uk

Timetable

You will receive your full timetable for the year during induction week.

What you will study

Course aims

The aim of the course is to provide cyber security and digital forensics skills for students wanting to embark on a career in either of these fields, but who wish to have a deeper understanding of the underpinnings of both disciplines than is usually covered in a single honours course. Students who undertake the course will develop a critical understanding and application of the two subject areas and be in a position to perform digital forensic acquisition and analysis, and implement cyber security mechanisms into any business they obtain employment with at a higher masters' level of competency.

With an increase in the use of digital devices within every walk of life this means that there is not a single crime that a digital device cannot be linked to. There is an ever-growing demand for digital forensic techniques as the number of digital devices and the volume of data that can be stored rapidly increases. Cyber-attacks are rising: the impact on companies both is terms of the financial implications and security breaches is significant and of concern. Companies and institutions are bound by the General Data Protection Regulation (GDPR), which requires that data be kept secure and accurate. Companies and institutions are only too aware of the legal implications of security breaches and leaked data and are therefore implementing more rigid and pronounced cyber security and management policies.

With the ever increasing use of digital devices and the risks posed by them, and an increase in recent years of cybercrime, it is commonly understood that the skill sets required for cyber security and digital forensics are essentially the same, and are complementary where they differ (or any differences are complementary). Students with the dual skill set are not only ultimately in the position to undertake a more rigorous digital forensic analysis, but also to implement more robust security mechanisms. Fundamental to this is the understanding of computer systems and the broader computing field which is addressed throughout the levels of the course.

Students on the MEng Cyber Security and Digital Forensics course will learn how to test the security of computer systems and networks and be able to analyse the systems for evidence of breaches following evidential standards. Students will learn through practical applications on our bespoke Hacktivity system designed and created, in house, to replicate real world business systems and potential attacks. Students will gain expertise in the use of digital forensic techniques and analysis through appropriate tools, commercially used in industry (Encase, XRY / Cellebrite) and open-source variants (Autopsy, FTK Imager), across a wide range of digital devices. Students will also work with employers, lawyers and experts to gain experience of preparing work for use by courts and customers and subsequently presenting it.

Progression through to the master's stage (level 7) of the MEng Cyber Security and Digital Forensics course will involve gaining specialism in the more challenging areas of digital forensics such as multimedia forensic investigations and deep fakes. In security areas students will gain knowledge and expertise in software security exploitation development and the analysis and implementation of security mechanisms to defend and analyse systems. The award will develop students' knowledge in research practices and advanced scholarship which are utilised through practical based projects at both Level 6 and Level 7 of the award.

The two subject areas have many facets, and therefore the numbers of optional modules within the award are limited. This allows the teaching team to cover the two subject areas to the depth expected of a graduate with such a degree.

The programme will provide a mix of academic and practical content; provide students with the theoretical knowledge to excel in their field and the practical experience to be able to physically implement their skills. The course will allow students who are unsure as to which field to focus on, to become proficient in both to a masters' level of understanding; creating additional career paths.

The course aims to prepare students for a career in the cyber security and/or digital forensics industry working with small consultancies or large organisations, including the police. However, the course will also prepare students for a career in the IT sector including software development, web design, IT network management and database administration within business, voluntary or public sectors.

Teaching and learning activities

For each module students will normally receive a weekly lecture followed by a tutorial or practical lab based session(s). In addition, some modules may be supported by optional drop-in workshop sessions. The course is supplemented with a programme of guest speakers and/or industry led seminars. This structure is preferred within such a vocational award where students are learning specialised material for a specific career.

This is a very hands-on subject area where theory alone would be unlikely to allow a student to achieve successful employment in this area. Practical exercises allow for students to implement their theoretical learning and see how it relates to industry. Practical solutions are achieved through the replication of exercises such as compromised computer systems and digital devices that students must analyse – similar to that as found in industry. Many of these examples are available through open-source community projects but are also built in-house when suitable external material is not available.

The use of a team project at Level 5 allows students to develop communication skills with their peers, this will include where possible, mixing with other cultures and individuals that they may not have originally chosen to work with as they are outside of their direct friendship group. Any issues that arise within group work such as difficulties with other group members are carefully managed through distanced support of the group where possible, to encourage the students to deal with the issues themselves. Where distance support is not possible tutors will directly resolve the issue working with the group to rectify and identify solutions. Team working is developed further still at Level 7 where the students will be expected to produce a commercially viable product as part of a small group.

An independent project will be undertaken at Level 6 to ensure that the students are able to proficiently manage and build a product that has underpinning academic research and appropriate methodological understanding; culminating in a Showcase ready piece of work.

Students are encouraged to debate within a variety of learning environments, including in-class and through the VLE discussion boards and additional chat applications where appropriate – this helps to develop respectful appreciation of their peers. Through encouraging students to use industry forums and scholarly research, students interact with a range of cultures and thinking that they are required to draw upon and evaluate within several modules.

The use of an induction session begins the process of welcoming students to the University and the course. Students are introduced to the support mechanisms in place, school and university wide, and begin to develop relationships with their peers. Students are placed into small teaching /tutorial groups that they will remain with for the first year of their study. Each group has an assigned Academic Adviser who will support the students through the academic year as a main point of contact. Course Tutorials will be delivered during the first academic year to support learning

and understanding of university systems and working practices such as: academic honesty, referencing, placement and employability. Each student will have a one-to-one meeting with their Academic Adviser at least once a semester in order to discuss progress and help with settling into university life.

Course structure

This information is correct for students progressing through the course within standard timescales. If you have to repeat study or take time out during your course, you may be taught alternative modules which meet the overall course learning outcomes.

The option modules listed may vary. Those listed here are likely to be offered in a typical year.

Level 4

Compulsory modules

Module title	Credits	Semester/teaching period
Fundamentals of Digital Forensics	20	S1 / Year 1
Computer Communications	20	S1 / Year 1
Computer Programming	20	S1 / Year 1
Ethical Hacking and Penetration Testing	20	S2 / Year 1
Fundamentals of Databases	20	S2 / Year 1
Object Oriented Programming	20	S2 / Year 1
Total number of credits of compulsory modules:	120	

Level 5

Compulsory modules

Module title	Credits	Semester/teaching period
Digital Forensic Processing	20	S1 / Year 2
Cyber Security Landscapes	20	S1 / Year 2
Web and Network Security	20	S2 / Year 2
Digital Forensics Analysis	20	S2 / Year 2
Team Project	20	S2 / Year 2
Total number of credits of compulsory modules:	100	

Option modules

Module title	Credits	Semester/teaching period
Database Systems	20	S1 / Year 2
Web Application and Technologies	20	S1 / Year 2
Software Systems Development	20	S1 / Year 2
Total number of credits of elective modules a student must enrol on:	20	

Placement year (if chosen)

Compulsory modules

Module title	**Credits**	**Semester/ teaching period**
Placement Module	120	Min 40 weeks

Level 6

Compulsory modules

Module title	Credits	Semester/teaching period
Production Project	40	S1 & 2 / Year 3
Mobile Forensics Investigation	20	S2 / Year 3
Systems Security	20	S2 / Year 3
Total number of credits of compulsory modules:	80	

Option modules

Module title	Credits	Semester/teaching period
Forensic Investigative Techniques	20	S1 / Year 3
Incident Response and Investigation	20	S1 / Year 3
Advanced Database Systems	20	S1 / Year 3
Advanced Web Engineering	20	S1 / Year 3
Advanced Software Engineering	20	S1 / Year 3
Total number of credits of elective modules a student must enrol on:	40	

Level 7

Compulsory modules

Module title	Credits	Semester/teaching period
Forensic Multimedia Processing	20	S1 / Year 4
Reverse Engineering and Malware Analysis	20	S1 / Year 4
Research Practice	20	S1 / Year 4
Software Security and Exploitation	20	S2 / Year 4
Project	40	S2 / Year 4
Total number of credits of compulsory modules:	120	

Assessment and feedback

The balance of assessment may change depending on which option modules you choose.

Level 4

Level 4 is assessed by a broadly even mix of coursework and practical assessments.

Level 5

Level 5 is assessed by a broadly even mix of coursework and practical assessments.

Placement year

Level 5 placement is assessed by presentation and a report.

Level 6

Level 6 is assessed by a broadly even mix of coursework and practical assessments.

Level 7

This course is assessed by a broadly even mix of coursework and examinations. There is a major independent study module which is assessed by a dissertation.

Workload

You can expect to spend a total of 100 hours learning per 10 credits.

Typically, a student on this course can expect to divide their time like this:

Overall workload	Level 4	Level 5	Placement year (if chosen)	Level 6	Level 7
Teaching, learning and assessment	270 hours	219 hours		207 hours	165 hours
Independent study	930 hours	981 hours		993 hours	1035 hours
Placement study			1200 hours		