



PgC - 30 ECTS	ECTS	Compulsory / Elective	Teaching	Assessment
Cyber Security	6	C	Online Classroom	Final Exam (50%), Individual Assignment (20%), Individual Class Presentation (30%)
Advanced Computer Forensics	6	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
Introduction to Financial Crime and Fraud	4	C	Online Classroom	Final Exam (50%), Individual Essay (20%), Individual Class Presentation (30%)
Information Security Management System	4	C	Online Classroom	Final Exam (50%), Group Project (20%), Group Class Presentation (30%)
Cyber Security Risk Assessment and Management	4	C	Online Classroom	Final Exam (50%), Individual Essay/Report (30%), Individual Class Presentation (20%)
PgC Independent Research	6	C	Online Classroom	Dissertation Content (80%), Presentation (20%)

PgD - 30 ECTS	ECTS	Compulsory / Elective	Teaching	Assessment
Advanced Web and Open Source Intelligence	4	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Class Presentation (30%)
Digital Multimedia Forensics	4	C	Online Classroom	Final Exam (50%), Group Project (20%), Individual Essay/Report (10%), Group Class Presentation (20%)
Cryptography	4	C	Online Classroom	Final Exam (50%), Individual Coding Project (20%), Individual Class Presentation (30%)
Penetration Testing	4	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
Cyber Threat Intelligence	4	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
Security and Privacy in Cloud Computing	4	C	Online Classroom	Final Exam (50%), Individual Assignment (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
PgD Independent Research	6	C	Online Classroom	Dissertation Content (80%), Presentation (20%)

Master's - 30 ECTS	ECTS	Compulsory / Elective	Teaching	Assessment
Advanced Network Forensics and Analysis	6	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
Advanced Mobile Forensics and Cell Site Analysis	6	C	Online Classroom	Final Exam (50%), Individual Project (20%), Individual Essay/Report (20%), Individual Class Presentation (10%)
Master's Independent Research and Final Dissertation	18	C	Online Classroom	Dissertation Content (80%), Presentation (20%)



- c) Mitigate cyber threats such as phishing, malware, ransomware, SQLI, XSS.
- d) Investigate and analyse current threat intelligence to determine who was behind the cyber-attack.
- e) Perform a forensic acquisition and analysis of digital evidence
- f) Create a report that involves the findings of an investigation.

Skills. The learner will be able to:

- a) Practice risk assessment and management techniques.
- b) Develop an information security framework for businesses and organizations.
- c) Perform penetration testing on IT assets such as web sites, computers, and networks.
- d) Investigate cyber-crime and incidents.
- e) Demonstrate evidence and intelligence about cyber-attacks.

15. **Teaching, learning and assessment procedures:** Online sessions delivered through our Institutional platform (MS Teams), access to study material on MS Teams and our Digital Library for independent study. Assessments are online.

16. **Type of Assessment:** Research Assignment (including elements of report writing, critical analysis of case studies, presentations, group work as appropriate), Dissertations and Case Study + Individual Presentation.

(Teaching and learning methodologies available in the Course outlines)

17. **Registration Method:** Online on EFI Admissions Portal

18. **Next Intake:** September every Academic Year

19. **Pass Rate:** > 40% (EFI grading system)

20. **Grading system**

Learning Outcome Score	Percentage Equivalent	Description	Honours Degree Classification	Other Award Classification	Qualitative Description
10	100	Pass	First	High Distinction	Student has achieved the learning outcome with no issues noted
7 - 9	70 - 99	Pass	First	Distinction	Student has achieved the learning outcome with minimal and/or negligible issues
6	60 - 69	Pass	Upper Second	Merit	Student has achieved the learning outcome with minor but non-negligible issues
5	50 - 59	Pass	Lower Second	Pass	Student has achieved the learning outcome with non-negligible issues
4	40 - 49	Pass	Third	Pass	Student has achieved the learning outcome with significant non-negligible issues
1 - 3	1 - 39	Fail	Fail	Fail	Student has NOT achieved the learning outcome with significant issues noted
0	0	Fail	Fail	Fail	Student did not answer question

21. **Registration:** admissions process, a step-by-step-guide and other information are available on our website - <https://www.eufor.eu/education/admission/>

22. Identity Malta's VISA requirement for third-country nationals:

<https://www.identitymalta.com/unit/central-visa-unit/>

23. Contact Details: available on our website (<https://www.eufor.eu/contact-us/>)

24. Address: Malta Life Sciences Park, Sir Temi Zammit Buildings – SGN 3000, San Gwann



Cyber Security

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Discuss an organization's/IT-based company's security procedures in action.
- b) Collaborate on an evaluation of an organization's or company's current cybersecurity plans and practices.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Connect key cybersecurity terms and concepts.
- b) Discuss how cybersecurity affects the security of a business.
- c) Analyse the most common threats, attacks, and vulnerabilities.
- d) Contrast cyber attackers and their motivations.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Recommend the best cybersecurity practices to maintain confidentiality, integrity, and availability of computer systems.
- b) Create policies and procedures to control cybersecurity threats.
- c) Discuss information security concerns in a professional context with cybersecurity experts and practitioners.

Module-Specific Learner Skills

The learner will be able to:

- a) Illustrate their knowledge of cybersecurity threats and controls in an IT-based setting.
- b) Implement and follow the best cybersecurity practices/policies, in order to safeguard the computerized system.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Match the relevant best practices for a computerized environment with online cybersecurity resources.

Advanced Computer Forensics

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Acquire complex digital evidence.
- b) Analyse complex digital evidence, RAW searches and virtualization.
- c) Create the final report and present it to the Court.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain the method and processes for determining whether or not a case is admissible in court.
- b) Recognize when digital forensics may be useful and how to conduct an investigation.
- c) Demonstrate existing and developing digital forensics technology and tools for analyzing the case.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Handle evidence on the scene
- b) Create and maintain an on-site digital forensics capability.
- c) Gather digital evidence (physical, network, and live acquisition).
- d) Analyse and export the findings of the gathered data from the target environment.
- e) Write a report to provide details of the incident, such as what happened (what we know), which process, tools, and methods were used during the investigation, and what evidence was found.

Module-Specific Learner Skills

The learner will be able to:

- a) Examine a computer-based environment for obtaining any type of digital evidence.
- b) Solve a range of digital forensics case studies.
- c) Able to present DF findings in a courtroom setting.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Use specialized digital forensics software/tools/procedures.
- b) Use a computer and editing software to create a report.



Introduction to Financial Crime and Fraud

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Interpret the rules governing financial crime.
- b) Advise about the risk of financial crimes
- c) Carry out risk assessments based on business environment red flags
- d) Monitor for gaps and discrepancies in various financial crimes
- e) Develop strategies for managing financial crime risks.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Define types of financial crimes
- b) Explain how the risk of financial crime affects your business.
- c) Recognize various types of fraud in the financial sector
- d) Draw accurate conclusions on case studies of various financial crimes
- e) Identify red flags that indicate financial crimes including behavioral red flags
- f) Explain key concepts in fraud identification, deterrence, and detection.
- g) Relate the most important risks and preventative measures for financial crime.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Demonstrate an understanding of the various financial crimes
- b) Examine financial crime trends.
- c) Use fraud investigation process from planning to reporting
- d) Apply the type of financial crime and red flag to the various case studies
- e) Relate various key concepts in fraud investigation process and different techniques used to investigate the fraud.
- f) Plan the risk of financial crimes based on the red flags identified
- g) Develop a comprehensive and efficient fraud response program for the business.

Module-Specific Learner Skills

The learner will be able to:

- a) Independently recognize behavioral red flags
- b) Analyse and make a report of fraud and investigation activities.
- c) Evaluate the gathering of evidence for a court case or for a client.
- d) Proactively identify and report on new fraud patterns and make recommendations to mitigate the risks.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Analyze the public, private or court documents to see whether there are any criminal records.



Information Security Management System

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Create, update, and disseminate current information security policies, standards, and recommendations.
- b) Be in charge of a risk management program that ensures the company owns, controls, or processes information with integrity, confidentiality, and availability.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain systemic understanding of the need of a processes approach to cyber security and the function of security risk management.
- b) Identify gaps in an Information Security management system.
- c) Design solutions to real-world secure systems challenges.
- d) Establish a link between cyber resilience and business continuity planning and management.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Analyse an organization's security and data protection requirements.
- b) Apply and critically evaluate current security by design concepts.
- c) Make suggestions for improvements to a current security issue and offer solutions.
- d) Comply with regulatory requirements by implementing current IT-security standards.

Module-Specific Learner Skills

The learner will be able to:

- a) Evaluate potential computer system risks and devise mitigation strategies.
- b) Design, execute, and monitor security policies and procedures for the company.
- c) Establish, update, and document information security policies and procedures across the organization.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Make a series of digital documents such as standards, procedures and policies, which will be used for auditing purposes.

Cyber security Risk Assessment and Management

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Develop a risk assessment.
- b) Prioritize risk remediation measures, as a consequence of the risk assessment.
- c) Examine risk management models to see whether they can be implemented in the company.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Classify the components of risk assessment and the data required to conduct a thorough risk evaluation.
- b) Identify and clearly describe the various forms of information system threats and vulnerabilities.
- c) Describe best practices in risk management, including risk assessment and risk treatment domains.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Implement efficient security policies and procedures at a company.
- b) Relate an organization's business requirements to security safeguards that have been applied.
- c) Evaluate a wide range of safeguards in order to select and justify acceptable risk-reduction countermeasures.

Module-Specific Learner Skills

The learner will be able to:

- a) Create a security policy.
- b) Monitor and review the risks.
- c) Prioritize risk remediation measures, as a consequence of the risk assessment.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Adopt online risk management and methodologies in order to reduce/control the risks.



PgC Independent Research

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Demonstrate administrative design for original content of research
- b) Undertake further studies with a fair degree of autonomy including searching for and studying existing research papers on relevant field and appropriately citing the source

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Use theories and principles in chosen field of research
- b) Apply methods and tools available to accomplish their research goal.

Skills

At the end of the module/unit the learner will have acquired the following skills:

Applying knowledge and understanding

The learner will be able to:

- a) Communicate ideas, problems and solutions using a range of techniques involving qualitative and quantitative information in a written report suitable for a professional in the field
- b) Evaluate own learning and identifies learning needs

Judgment Skills and Critical Abilities

The learner will be able to:

- a) Critically evaluate and interpret the results of the personal analysis
- b) Analyse, identify key issues, carry out an independent investigation using multiple information sources and apply critical judgement to construct logical arguments

Module-Specific Communication Skills

The learner will be able to:

- a) Explain in a clear and simple way the chosen procedure and the reached conclusions.
- b) Write a report in a correct and clear way, relevant and understandable to professionals in the field
- c) Submit his/her findings before the set deadline and answer any question that may rise about the research in a professional and confident manner

Module-Specific Learner Skills

The learner will be able to:

- a) Conduct a research on chosen field using cross-disciplinary knowledge acquired in the previous months

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Write a 15-20 (3750-5000 words) pages long paper using IT instruments
- b) Use the internet to find information

Advanced Web and Open Source Intelligence

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Advise businesses and government agencies about the various types of Web and Open Source Intelligence Tools.
- b) Carry out a Web and Open-Source process and investigation
- c) Be responsible for various types of data available including sourcing from the dark web
- d) Establish a secure data collection platform.
- e) Carry out OSINT investigations for a wide range of clients.
- f) Examine the customers' collection requirements.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Apply the various types of Web and Open Source Intelligence Tools
- b) Sequence a Web and Open Source process and investigation
- c) Discover the various types of data available including sourcing from the dark web
- d) Analyse online resources for tracking people and organizations on a global scale, including public record databases and a powerful people search tool.
- e) Discuss current challenges and trends in social media and open source research

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Demonstrate the application of various types of Web and Open Source Intelligence Tools.
- b) Apply a Web and Open Source process and investigation
- c) Discover more about the ethical issues surrounding the use of OSINT methods in law enforcement and research.
- d) Demonstrate the various types of data available including sourcing from the dark web
- e) Use open source platforms such as social media, search engines, and the dark web to access, explore, and gather intelligence.
- f) Evaluate the usefulness and accuracy of internet sources and data.

Module-Specific Learner Skills

The learner will be able to:

- a) Create tools and methods for gathering and managing data from both online and offline sources.
- b) Investigate and locate relevant information from a variety of sources using cutting-edge technology and innovative research approaches.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Perform advanced browsing.
- b) Structure collected data.
- c) Use a wide range of web Intelligence Open Source tools.



Digital Multimedia Forensics

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Acquire images and videos that might be related to a cyber crime.
- b) Identify and solve technical and quality issues.
- c) Perform an analysis assessment.
- d) Enhance, process and analyse the material.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain theory and the procedural aspects of the discipline, specifically referring to the advanced image/audio processing,
- b) Describe the problems and the challenges found in the acquisition of videos, audio and pictures from different sources.
- c) Describe how to operate to enhance images, audio and videos

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Extract the hash codes from digital images and audio files.
- b) Enhance and reconstruct not clear features in image, audio and video.
- c) Use different types of file formats and test their search methodologies.
- d) Evaluate the authenticity of pictures acquired with digital devices.

Module-Specific Learner Skills

The learner will be able to:

- a) Check a digital forensic image/audio
- b) Perform a digital forensic analysis.
- c) Document all the steps of a digital forensic analysis.
- d) Evaluate the documentation and the devices submitted for the forensic analysis.
- e) Ask the appropriate question to authorities and clients.
- f) Evaluate the digital forensic analysis carried out by other experts.
- g) Choose the appropriate hardware and software instrumentation for the job.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Write a report using computer and editing software.
- b) Manage digital image and video evidence to preserve its quality and its value as evidence
- c) Operate with specific image and video forensics software such as FotoForensics, Video Cleaner and Forevid



Cryptography

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Design security protocol implementation software.
- b) Handle professional cryptology issues with both professionals and the general public.
- c) Carry out tasks under supervision, conduct a modest research or development project in cryptology.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Summarize historical ciphers and determine their flaws.
- b) Describe the concepts of today's cryptography algorithms and the mathematical theory that underpins them.
- c) Explain the use of public-key cryptography methods and their applications.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Apply security strategies to solve real-world security issues in real-world systems.
- b) Demonstrate how to use public-key cryptography methods and applications.
- c) Evaluate the security of authentication and key exchange, e-mail, and wireless communication

Module-Specific Learner Skills

The learner will be able to:

- a) Examine the professional and scientific ethical issues in cryptography.
- b) Assess the current cryptology ideas, techniques, and interpretations, and work independently on theoretical and practical challenges.
- c) Analyse and apply the critical analysis of numerous literary sources to the structuring and formulation of scientific principles in cryptology.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Investigate cyber security techniques and ways of keeping our data secure in the digital environment.



Penetration Testing

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Collaborate in performing vulnerability assessment and penetrating testing in order to identify software flaws on both the server and client sides, with a special focus on network applications.
- b) Advice on system security and recommendations for addressing security flaws.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Identify flaws in network hardware and software.
- b) Explain hacking techniques and tools used on computer networks, web applications, mobile devices, servers, and clients.
- c) Define ethical hacking terminologies such as attack vectors, OWASP top 10, vulnerabilities and exploits, APT, malware, threats.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Apply information about target systems, use and understand basic network reconnaissance techniques.
- b) Take part in discovering security flaws in networks and web services in an organized manner.
- c) Apply specific solutions to discovered security flaws

Module-Specific Learner Skills

The learner will be able to:

- a) Perform penetration testing and security assessments regardless of the size of the business.
- b) Defend a computerized network and its systems against cyber-attacks.
- c) Collaborate in groups to do research and express sensible, well-thought-out arguments using acceptable approaches

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Verify the status of vulnerabilities and apply fixes using publicly available resources.



Cyber Threat Intelligence

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Carry-out an investigation and analysis of the Intelligence-Driven Incident Response method.
- b) Perform a cyber-attack event analysis and document the behavior of the adversary.
- c) Represent the Diamond Model and MITRE ATT&CK framework to create a threat model for a cyber incident.
- d) Be able to assess an organization's attack surface, determining how it corresponds to cyber threats, and developing effective CTI policies.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain Cyber Threat Intelligence (CTI), its main attributes, value and advantages.
- b) Determine how threat actors carry out their cyberspace actions to achieve their objectives.
- c) Connect CTI at tactical, operational, and strategic levels to detect sophisticated threats and critical functions defenses.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Discover how cyber intelligence, digital forensics and penetration testing can work together.
- b) Relate the relationship between a threat actor's motivation, access, and capabilities and their aims.
- c) Analyse a cyber threat actor's tactics, techniques and procedures (TTPs) in detail.
- d) Make suggestions for modifications to information system security design, implementation, policy, and practices using cyber intelligence.

Module-Specific Learner Skills

The learner will be able to:

- a) Create a Cyber Threat Intelligence report on a threat actor that is aimed at top decision makers.
- b) Be able to collect threat intelligence from a variety of online sources, analyzing it, and reporting on it.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Categorise various online information about a company's threats.
- b) To gather and use cyber threat intelligence from a variety of online sources, with a focus on open source intelligence (OSINT).

Security and Privacy in Cloud Computing

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Create safe defense mechanisms for cloud applications that include the infrastructure, platform, application, data, and privacy security domains.
- b) Advise on accomplishing intended goals and discuss complicated concerns linked to cloud security.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain data privacy and its relation to cloud computing.
- b) Identify the risks associated with the various cloud service provider offerings (CSPs).
- c) Recognize the most effective approaches to cloud security.
- d) Explain how specialized knowledge and skills can be used to secure a wide range of cloud computing business applications.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Analyse cloud and cloud application security risks and threats in light of government rules and industry best practices.
- b) Create a plan on how to minimize risk and dangers in a cloud system/service
- c) implement security techniques (i.e. spacing and capitalisation) for safeguarding cloud applications.
- d) Apply security techniques for safeguarding cloud applications in order to reduce risk and dangers in a cloud system/service.
- e) Analyse and deploy cloud technologies for governance, compliance, operational auditing, and risk auditing.

Module-Specific Learner Skills

The learner will be able to:

- a) Protect cloud systems at scale by applying key infrastructure ideas.
- b) Correlate a company's needs with secure cloud infrastructure in a variety of industries.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Examine how knowledge gleaned from diverse online sources may be used to solve cloud computing-related business difficulties.
- b) Examine and assess the present cloud services and in-cloud apps for security.



PgD Independent Research

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Demonstrate administrative design for original content of research
- b) Be responsible for work and study contexts that require problems to be solved
- c) Undertake further studies with a relevant degree of autonomy including searching for and studying existing research papers on relevant field and appropriately citing the source

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Provide details of theoretical and practical knowledge involving understanding of theories and principles in chosen field of research
- b) Understanding methods and tools available including most recent innovation in the field

Skills

At the end of the module/unit the learner will have acquired the following skills:

Applying knowledge and understanding

The learner will be able to:

- a) Communicate ideas, problems and solutions using a range of techniques involving qualitative and quantitative information in a written report suitable for a professional in the field
- b) Evaluate own learning and identifies learning needs
- c) Devise and sustain arguments to solve problems

Judgment Skills and Critical Abilities

The learner will be able to:

- a) Gather and critically evaluate and interpret the results of the personal analysis and of the analysis of other experts involved in the research
- b) Investigate and analyse, identify key issues, carry out an independent investigation using multiple information sources and apply critical judgement to construct logical arguments

Module-Specific Communication Skills

The learner will be able to:

- a) Communicate to colleagues and co-workers personal ideas regarding procedural choices, made or to be made.
- b) Write a report in a correct and clear way, relevant and understandable to professionals in the field being able to write a conclusion of his/her research
- c) Submit his/her findings before the set deadline and answer any question that may rise about the research in a professional and confident manner

Module-Specific Learner Skills

The learner will be able to:

- a) Conduct a detailed research on chosen field using cross-disciplinary knowledge acquired throughout the year
- b) Develop in-depth study, be it experimental, conducted alone or in a team.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Write a 20-30 (5000-7500 words) pages long paper using IT instruments
- b) Use the internet to find information

Advanced Network Forensics and Analysis

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Monitor malicious activity and find network problems.
- b) Guide a business to protect themselves against network attacks.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Explain how attackers use man-in-the-middle technologies to intercept communications that appear to be secure.
- b) Identify possibilities to gather new evidence, based on the current systems and platforms inside a network architecture.
- c) Determine how computer crimes affect digital network forensics.
- d) Use industry best practices, when doing digital network forensics.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Analyse network traffic using standard network protocols to look for patterns of behaviour or particular acts that need to be looked into further.
- b) Take apart files derived from network packet captures and proxy cache files, enabling for additional malware research and final data loss findings.
- c) Investigate and evaluate methods of data concealment and scrambling.

Module-Specific Learner Skills

The learner will be able to:

- a) Implement digital evidence gathering, preservation, and analysis tools.
- b) Discover a wide range of computer and network vulnerabilities.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Monitor network traffic and analyse log files.
- b) Able to use various online tools for responding to network incidents.



Advanced Mobile Forensics and Cell Site Analysis

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Perform a complex forensic acquisition of a mobile device.
- b) Perform a forensic acquisition of Call Detail Record (CDR) and check the real cell tower coverage.
- c) Correlate mobile extraction and Cell Site Analysis (CSA) analysis for a trustworthy report.
- d) Deal with data analysis and correlation in complex investigation cases.

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Determine how the evidence came to be on the mobile device.
- b) Explain how data is stored on smartphone components, as well as how encrypted data can be viewed.
- c) Describe file systems and locate information that isn't readily available to the general public on mobile devices.

Skills

At the end of the module/unit the learner will have acquired the following skills: Applying knowledge and understanding. The learner will be able to:

- a) Perform a complex forensic acquisition and analysis of a mobile device.
- b) Retrieve lost information by examining SQLite databases and raw data dumps from devices.
- c) Manage smartphone encryption and manually retrieve lock codes by bypassing, cracking, and/or decoding them.
- d) Perform a complex forensic analysis of CDR files and Base Transceiver Station (BTS) data.
- e) Create a report that involves multiple sources of data.

Module-Specific Learner Skills

The learner will be able to:

- a) Analyse a digital forensic image.
- B Perform a digital forensic analysis.
- c) Document all the steps of a digital forensic analysis.
- d) Evaluate the documentation and objects submitted for the forensic analysis.
- e) Ask appropriate information to authorities and clients.
- f) Evaluate the digital forensic analysis carried out by other experts.
- g) Choose the appropriate hardware and software instrumentation for the activity.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Write a report using computer and editing software.
- b) Operate with specific digital, mobile and cell site analysis forensic software.



Master's Independent Research and Final Dissertation

Competences

At the end of the module/unit the learner will have acquired the responsibility and autonomy to:

- a) Demonstrate administrative design for original content of research
- b) Be responsible for work and study contexts that are unpredictable and require that complex problems are solved
- c) Undertake further studies with a high degree of autonomy including searching for and studying existing research papers on relevant field and appropriately citing the source

Knowledge

At the end of the module/unit the learner will have gained knowledge and understanding to:

- a) Analyse cross-disciplinary knowledge that includes some aspects that will be at the forefront of this field
- b) Use theories and principles in chosen field of research
- c) Apply methods and tools available including most recent innovation in the field
- d) Create a genuine work using specialized anti-plagiarism software (pedagogical approach).

Skills

At the end of the module/unit the learner will have acquired the following skills:

Applying knowledge and understanding

The learner will be able to:

- a) Apply cross-disciplinary knowledge and understanding acquired throughout the programme in a professional manner
- b) Communicate ideas, problems and solutions using a range of techniques involving qualitative and quantitative information in a written report suitable for a professional in the field
- c) Devise and sustain arguments to solve problems
- d) Continuously evaluates own learning and identifies learning needs

Judgment Skills and Critical Abilities

The learner will be able to:

- a) Gather and critically investigate relevant data to inform judgements that include reflection on social, scientific and/or ethical issues
- b) Critically evaluate and interpret the results of the personal analysis and of the analysis of other experts involved in the research
- c) Investigate and analyse, including the ability to formulate problems clearly, identify key issues, carry out a substantial independent investigation using multiple information sources and apply critical judgement to construct logical arguments

Module-Specific Communication Skills

The learner will be able to:

- a) Communicate to colleagues and co-workers personal ideas regarding procedural choices, made or to be made.
- b) Explain in a clear and simple way the chosen procedure and the reached conclusions.
- c) Write a report/essay/thesis in a correct and clear way, relevant and understandable to professionals in the field
- d) Present his/her findings professionally to a panel and confidently discuss any questions raised

Module-Specific Learner Skills

The learner will be able to:

- a) Conduct in-depth study and research on chosen field using cross-disciplinary knowledge acquired throughout the programme
- b) Develop projects of innovative research or in-depth study, be it experimental, conducted alone or in a team.

Module-Specific Digital Skills and Competences

The learner will be able to:

- a) Write a 30-40 (7500-10000 words) pages long dissertation using IT instruments
- b) Use the internet to find information
- c) Write a genuine dissertation with the support of anti-plagiarism software

**Master's in Cyber Security, Digital Forensics and
Crime Analysis**

Post Graduate Certificate					Percentage of Total Contact Hours		Hours of Total Learning			
Module	ECTS	MQF/EQF Level	Compulsory/Elective	Total learning hours	Contact Hours Delivered Online	Contact Hours Delivered Face-to-Face	Total Contact Hours	Supervised Placement and Practice Hours	Self-Study Hours	Assessment Hours
Cyber Security	6	7	Compulsory	150	100%	0%	30	0	114	6
Advanced Computer Forensics	6	7	Compulsory	150	100%	0%	30	0	114	6
Introduction to Financial Crime and Fraud	4	7	Compulsory	100	100%	0%	20	0	76	4
Information Security Management System	4	7	Compulsory	100	100%	0%	20	0	76	4
Cyber Security Risk Assessment and Management	4	7	Compulsory	100	100%	0%	20	0	76	4
PgC Independent Research	6	7	Compulsory	150	100%	0%	30	0	90	30
Post Graduate Diploma					Percentage of Total Contact Hours		Hours of Total Learning			
Module	ECTS	MQF/EQF Level	Compulsory/Elective	Total learning hours	Contact Hours Delivered Online	Contact Hours Delivered Face-to-Face	Total Contact Hours	Supervised Placement and Practice Hours	Self-Study Hours	Assessment Hours
Advanced Web and Open-Source Intelligence	4	7	Compulsory	100	100%	0%	20	0	76	4
Digital Multimedia Forensics	4	7	Compulsory	100	100%	0%	20	0	76	4
Cryptography	4	7	Compulsory	100	100%	0%	20	0	76	4
Penetration Testing	4	7	Compulsory	100	100%	0%	20	0	76	4
Cyber Threat Intelligence	4	7	Compulsory	100	100%	0%	20	0	76	4
Security and Privacy in Cloud Computing	4	7	Compulsory	100	100%	0%	20	0	76	4
PgD Independent Research	6	7	Compulsory	150	100%	0%	30	0	90	30
Master's					Percentage of Total Contact Hours		Hours of Total Learning			
Module	ECTS	MQF/EQF Level	Compulsory/Elective	Total learning hours	Contact Hours Delivered Online	Contact Hours Delivered Face-to-Face	Total Contact Hours	Supervised Placement and Practice Hours	Self-Study Hours	Assessment Hours
Advanced Network Forensics and Analysis	6	7	Compulsory	150	100%	0%	30	0	114	6
Advanced Mobile Forensics and Cell Site Analysis	6	7	Compulsory	150	100%	0%	30	0	114	6
Master's Independent Research and Final Dissertation	18	7	Compulsory	450	100%	0%	90	0	300	60