# COMP H4228: Computer Forensics

| | |
|---|---|
| **Module Title:** | Computer Forensics |
| **Language of Instruction:** | English |

| | |
|---|---|
| **Credits:** | 10 |

| | |
|---|---|
| **NFQ Level:** | 8 |

| | |
|---|---|
| **Module Delivered In** | No Programmes |

| | |
|---|---|
| **Teaching & Learning Strategies:** | Learners will develop understanding and practical skills through lectures, labs and practical workshops. Delivery of theoretical content will promote active engagement and discussion, providing a positive learning experience. Labs and practical workshops will be used extensively to enable learners to apply knowledge and skills to real world problems, enhancing learner engagement. |

| | |
|---|---|
| **Module Aim:** | To provide learners with a high level of expertise in the forensic analysis of computer systems and acquisition of data as part of a forensic investigation. |

| **Learning Outcomes** | |
|---|---|
| *On successful completion of this module the learner should be able to:* | |
| LO1 | Summarise the steps involved in a computer forensic examination. |
| LO2 | Synthesise forensic analysis of computer systems and data storage devices. |
| LO3 | Securely acquire data and preserve the integrity of data from a range of sources. |
| LO4 | Analyse and present findings from an electronic discovery process. |

| **Pre-requisite learning** |
|---|
| ***Module Recommendations***<br>*This is prior learning (or a practical skill) that is recommended before enrolment in this module.* |
| No recommendations listed |
| ***Incompatible Modules***<br>*These are modules which have learning outcomes that are too similar to the learning outcomes of this module.* |
| No incompatible modules listed |
| ***Co-requisite Modules*** |
| No Co-requisite modules listed |
| ***Requirements***<br>*This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed.* |
| Learners should have good knowledge of Operating Systems and be comfortable working in a command line environment (Linux and Windows). |

# COMP H4228: Computer Forensics

## Module Content & Assessment

| Indicative Content |
|---|
| **Forensic Science**<br>Areas and domains of forensic science. The role of computer forensics and incident response process. The principles of computer based electronic evidence, control of a crime scene. |
| **Ethics**<br>Ethical responsibilities of studying computer forensics, data and computer law. New developments in digital crimes based on the latest technology. Professional guidelines, best practice and policies. |
| **File Systems**<br>Detailed analysis of common file systems including FAT family, NTFS, exFAT, ext2, ext3, ext4 and HFS (Mac). Disk structures (traditional and SSD), inodes, metadata and analysis of Windows Registry. |
| **Acquiring Forensic Evidence**<br>Investigative plans and forensic workstations set up for investigation. Quality assured processes for retrieving potential evidence. Electronic discovery process and IT forensic support. |
| **Data Acquisition**<br>Tools and techniques available to acquire data on computer systems. Full volume images, partial volume images and image capture tools. Recovering deleted data, erased data and volatile data. |
| **Network and Internet Forensics**<br>Using network logs to collect evidence of a network intrusion incident or a crime. Internet browser forensics and email forensic investigations, popular internet/email forensic tools. |
| **Mobile and Other Device Forensics**<br>Extraction and analysis of static data from smartphones, tablets, USB sticks and dynamic/volatile dada from other sensor/node devices. Analysis of data using hash tools. |
| **Forensic Analysis**<br>Analysing captured data using tools. Timelines using log2timeline, hash analysis using md5deep, volatile data using Volatility, network data using Wireshark, file carving using Scalpel. |
| **Counter Forensics**<br>Detection of tampered, altered, destroyed and/or deleted files and logs. Trace evidence, disk level analysis and manipulation tools such as timestomp. |
| **Types of Evidence**<br>Chain of custody, evidence identification, evidence preservation, evidence analysis, evidence communication and presentation. |
| **Software and Tools**<br>Analysis of computer forensic tools and applications, not exclusive to the following list, Encase, SANS Investigative Forensic Toolkit (SIFT), TSK and Autopsy and Oxygen Forensics Suite. |

| Assessment Breakdown | % |
|---|---|
| Continuous Assessment | 20.00% |
| Practical | 30.00% |
| End of Module Formal Examination | 50.00% |

**Continuous Assessment**

| *Assessment Type* | *Assessment Description* | *Outcome addressed* | *% of total* | *Assessment Date* |
|---|---|---|---|---|
| Case Studies | Critique a Case Study of an electronic discovery process, reflecting on knowledge and experience gained over the duration of the module. | 4 | 20.00 | n/a |

No Project

**Practical**

| *Assessment Type* | *Assessment Description* | *Outcome addressed* | *% of total* | *Assessment Date* |
|---|---|---|---|---|
| Practical/Skills Evaluation | Analyse and extract relevant data from a device in a professional manner. | 2 | 30.00 | n/a |

**End of Module Formal Examination**

| *Assessment Type* | *Assessment Description* | *Outcome addressed* | *% of total* | *Assessment Date* |
|---|---|---|---|---|
| Formal Exam | Terminal Examination | 1,3,4 | 50.00 | End-of-Semester |

**SETU Carlow Campus reserves the right to alter the nature and timings of assessment**

# COMP H4228: Computer Forensics

## Module Workload

| Workload: Full Time | | |
|---|---|---|
| *Workload Type* | *Frequency* | *Average Weekly Learner Workload* |
| Laboratory | 30 Weeks per Stage | 2.00 |
| Lecture | 30 Weeks per Stage | 1.00 |
| Independent Learning | 30 Weeks per Stage | 3.67 |
| | Total Hours | 200.00 |