# F20FO Digital Forensics

## COURSE DETAILS

| Course Code: | F20FO |
| SCQF Level: | 10 |
| SCAF Credits: | 15 |
| Available as Elective: | No |

## DELIVERY LEVEL

<table>
<thead>
<tr>
<th>Undergraduate:</th>
<th>Yes</th>
<th>Postgraduate Taught:</th>
<th>No</th>
<th>Postgraduate Research:</th>
<th>No</th>
</tr>
</thead>
</table>

Additional Information:

## COURSE AIMS

- Provide the student with in-depth understanding of digital forensics concepts and methodologies
- Impart a deep understanding of common attack scenarios to students
- Improve students' analysis skills and allow them to identify incidents artefacts in a systematic way
- Give practical experience of finding clues and discovering attack scenarios in common operating systems and applications

## LEARNING OUTCOMES – SUBJECT MASTERY

At the end of this course, the students will be able to:

- Understand the technical and legal aspects of the digital forensics process
- Identify and explain the role of different types of digital artefacts
- Review the security of Windows and Linux systems
- Assess the security of an IT infrastructure
- Identify suspicious activities and combine them into attack scenarios
- Understand appropriateness and effectiveness of different techniques and research methodologies for digital forensics processes

## LEARNING OUTCOMES – PERSONAL ABILITIES

At the end of this course, the students will:
F20FO Digital Forensics

- Develop a set of ethical and legal best practices needed for a digital forensics career
- Be able to critically appraise the security of an IT infrastructure

- Practice in ways that demonstrate a clear awareness of own and others' roles and responsibilities

- Use a range of digital forensics software to support and enhance their analyses
- Make formal presentations about digital forensics topics to informed audiences

SYLLABUS

- Legal aspects: investigation limitations (territorial and jurisdictional)
- Search and seizure: consent, warrant, evidence seizure
- Analysis: things to consider, analysis Process, evidence guidelines, order of evidence importance
- Forensic toolkits: hardware features, software features, common software tools
- Windows OS artefacts: event log, registry, prefetch, volume shadow copies, shell bags, jumplists, boot, services
- Linux OS artefacts: "etc" folder, logs, home folder, nautilus, accounts and login history, grub, services
- Malware persistence mechanisms: auto-startup, cron jobs
- Malware analysis
- Reverse Engineering
- Storage Media: types overview, file Systems overview
- Common applications' artefacts: web browsers, chat clients, servers (Apache, mysql), cross-platform applications

COURSE RELATIONSHIPS

N/A

LOCATION AND ASSESSMENT METHODS

<table>
<thead>
<tr>
<th>Edi</th>
<th>SBC</th>
<th>Ork</th>
<th>Dub</th>
<th>Malay</th>
<th>IDL</th>
<th>COLL</th>
<th>ALP</th>
<th>OTH</th>
<th>Method</th>
<th>Weight</th>
<th>Exam Mins</th>
<th>Type</th>
<th>Diet</th>
<th>Synoptic Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Coursework</td>
<td>100</td>
<td>Assessment</td>
<td>Semester 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>