# F21FO Digital Forensics

## COURSE DETAILS

<table>
<thead>
<tr>
<th>Course Code:</th>
<th>F21FO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Course Title:</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td>SCQF Level:</td>
<td>11</td>
</tr>
<tr>
<td>SCAF Credits:</td>
<td>15</td>
</tr>
<tr>
<td>Available as Elective:</td>
<td>No</td>
</tr>
</tbody>
</table>

## DELIVERY LEVEL

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

Additional Information:

## COURSE AIMS

- Impart a deep understanding of common attack scenarios to students.
- Improve students’ critical analysis skills in computer security and allow them to identify incidents artefacts in a systematic way.
- Provide the student with in-depth understanding of digital forensics concepts and methodologies.
- 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.

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

- Critically review the security of Windows and Linux systems.
- Identify suspicious activities and combine them into attack scenarios.
- Assess the security of an IT infrastructure.

## LEARNING OUTCOMES – PERSONAL ABILITIES

At the end of this course, the students will:

- 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.

At the end of this course, the students will be able to:
F21FO Digital Forensics

- Show initiative, creativity and team working skills in shared digital forensics investigation environments.

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

- Build on initial skills and knowledge by independent research using online resources.

SYLLABUS

- Legal aspects: investigation limitations (territorial and jurisdictional), inchoate offences.
- 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></td>
<td>Assessment</td>
<td>Semester 2</td>
<td></td>
</tr>
<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></td>
<td>Reassessment</td>
<td>Semester 3</td>
<td></td>
</tr>
</tbody>
</table>