

Course title: Malware Analysis

Course number:	ISCG7408	Level:	7	Credits:	15
Main programme:	BCS				
Pre-requisites:	For BCS: 6407 For GDCMP: 6407				
Co-requisites:	None				
Restrictions:					
Compulsory/elective:	BCS Elective GDCMP Elective				

Learning time: 150 hours

(Lecturer) Contact hours	Non-contact hours	Total hours
39 (13 weeks)	111	150

Level descriptor: The student is able to carry out processes that:

- require a wide range of specialised technical or scholastic skills
- involve a wide choice of standard and non-standard procedures
- are employed in a variety of routine and non-routine contexts employing a broad knowledge base with substantial depth in some areas
- require analytical interpretation of a wide range of data
- involve the determination of appropriate methods and procedures in response to a range of concrete problems with theoretical and applied elements of cyber-security
- are a self-directed and directed activity
- require taking responsibility for the nature, quantity and quality of outcomes
- require responsibility for the achievement of group outcomes to Analyse, Integrate, Estimate, Compare, Contrast, Differentiate, Investigate, Demonstrate and Evaluate problems and solutions in cyber-security at a fundamental level.

Course aim: To give students an insight into the fundamental concepts of malware analysis, the knowledge needed to understand the security risks of malware infections and the mitigation mechanisms required to be implemented and managed for securing IT infrastructure.

Learning outcomes:

	Learning outcomes
1.	Programming language knowledge necessary to analyse malware
2.	Static and Dynamic analysis of malware
3.	Understanding malware functionality and how malware enables the underground economy
4.	Reverse engineering and obfuscation techniques used in modern malware
5.	Shellcode analysis
6.	Rootkit analysis