Course Name	*Malware Analysis*		تحليل البرمجيات الضارة	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911633	CS 633	3 (3-0-6)	0911622
Course Track	☐ Program Core ☒ Electives			

Course Description

The increasingly networked nature of the world has also enabled the spread of various types of malicious software, from a simple adware to more sophisticated Cyber-weaponry. This course will provide the students with the knowledge and skills to detect, analyze, understand, control, and eradicate malware which is an increasingly important issue in information security. This course provides students with an understanding of the issues and techniques used in malware detection and classification. This course will introduce students to the detailed process of malware analysis, packing and unpacking of malwares, static and dynamic analysis of malware, and the malicious activities and techniques. The course also focusses on how to overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques. The course will equip the students with the skills needed to use advanced tools and methodologies that perform malware analysis.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Analyze** modern malware samples using both static and dynamic analysis techniques. [B]
2. **Explain** executable formats, Windows internals and API, and analysis techniques. [A]
3. **Identify** specific coding constructs in disassembly. [B]
4. **Apply** techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. [E]
5. **Use** industry standard tools to perform Malware Analysis on existing Operating Systems. [E]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Christopher C. Elisan, "*Advanced Malware Analysis*", 1st Edition, McGraw-Hill/Osborne, 2015. ISBN-13: 978-0071819749.					
References	1. Michael Sikorski, Andrew Honig "*Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software*", 1st Edition, No Starch Press, 2012. ISBN-13: 978-1593272906. 2. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard, "*Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*", 1st Edition, Wiley Publishers, 2011. ISBN-13: 978-0470613030.					