Course Name	*Incident Response with Digital Forensics*		الاستجابة للحوادث مع التحليل الجنائي الرقمي	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911632	CS 632	3 (3-0-6)	0914611, 0914612
Course Track	☐ Program Core ☒ Electives			

Course Description

Every organization, which uses computers to support their operations, are facing attacks. This course will equip the students to detect any attempt made to attack an organization and take appropriate actions to either stop that attack or take appropriate actions to mitigate its effect. The course starts with brief discussion on Intrusion Detection/Prevention systems (IDPS) architecture and all its components, and IDPS tools. After that, digital forensics process will be discussed in detail with focus on different tools to retrieve and analyze forensic data. Focus is then shifted to applying IDPS and concepts of forensics to handle security incidents in organizations. The course will discuss different elements in detail including incident response policy and incident team structure. The course will discuss the concepts for detecting and analyzing the incidents including attack vectors, incident analysis, containment and eradication strategy, handling, eradication and recovery and evidence retention. The coordination and information sharing between different teams will also be discussed to provide the flavor of actual working in organizations.

Course Outcomes

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

1. **Explain** the detailed working of the forensics process. [A]
2. **Explain** all the components and workings of an Intrusion Detection / Prevention Systems. [A]
3. **Describe** the incident response process in Digital Forensics and Intrusion Detection / Prevention Systems. [A]
4. **Analyze** the logs obtained from monitoring the behavior of observed systems during attack. [B, E]
5. **Decide** and **Plan** the incident response for analyzed attacks. [C, D]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Ric Messier, "*Network Forensics*", 1st Edition, Wiley, 2017, ISBN-13: 978-1119328285.					
References	1. Jason T. Luttgens, Mathew Pepe and Kevin Mandia, "*Incident Response & Computer Forensics*", 3rd Edition, Mc-Graw Hill Education, 2014. ISBN-13: 978-0071798686. 2. Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone**,** "*Computer Security, Incident Handling Guide*", SP 800-61 R2, NIST US Dept. of Commerce, 2012. 3. Don Franke, "*Cyber Security Basics: protect your organization by applying the fundamentals*", 1st Edition, CreateSpace Independent Publishing Platform, 2016. ISBN-13: 978-1522952190.					