Department of Business Information Technology (BIT)
King Abdullah II School for IT
The University of Jordan
M S C . W E B I N T E L L I G N E N C E
Course Name: **Digital Forensics (1904740)**

Instructor name: Dr. Ja'far Alqatawna
Office number: _____
Office hours:_____
E-mail address: J.Alqatawna@ju.edu.jo

Course Description:
While there is remarkable dependency on online and web applications, there is also a rapid increase in number of cyber and digital crimes. In such situation it is inevitable to have professionals equipped with the necessary knowledge and skills to discover what possible damage or digital crime has been done on computing devices and applications, when it was done, and how it was done. The aim of this course is to cover method and techniques used when investigating digital data. It will discuss technical issues in acquiring computer related evidence. The course will cover several topics such as: Incident Response in various operating systems, Web Activity Reconstruction, Email Activity Reconstruction, Windows Registry Reconstruction, Forensic tools and Network forensics.

Course Objectives:
- Develop a working knowledge of digital forensics principles, methodologies and techniques.
- Develop an understanding of best practices for collecting and preserving digital evidences.
- Develop a working knowledge of OS and file forensics.
- Develop a working knowledge of Network and Web forensics.

Learning Outcomes:
Upon successful completion of this course, students will be able to:
- Demonstrate a working knowledge of digital evidences.
- Understand the role and responsibilities of computer forensic investigator.
- Collect and analyze data from various sources.
- Design/implement/use various forensics tools.

Recommended reading materials

Guide to Computer Forensics and Investigations.
Bill Nelson; Amelia Phillips; Christopher Steuart, ISBN-10: 1-4354-9883-6, ISBN-13: 978-1-4354-9883-9.

Investigation, and Response (2014). Easttom, System Forensics,
Computer Forensics: Cybercriminals, Laws, and Evidence (2014). Maras,

Selected papers covering related topics will be provided to students during the course.

Topics:

1:Computer Forensics and Investigation Processes.
2: Understanding Computing Investigations.
3: The Investigator's Office and Laboratory.
4: Data Acquisitions.
5: Processing Crime and Incident Scenes.
6: Working with Windows and DOS Systems.
7: Current Computer Forensics Tools.
8: Macintosh and Linux Boot Processes and File Systems.
9: Computer Forensics Analysis.
10: Recovering Graphics Files.
11: Virtual Machines, Network Forensics, and Live Acquisitions.
12: E-mail Investigations.
13: Cell Phone and Mobile Device Forensics.
14: Report Writing for High-Tech Investigations.
15: Expert Testimony in High-Tech Investigations.
16: Ethics and High-Tech Investigations

Grading:

The total grades of this course are assigned as follows

1. 2 Hour exam 30%
2. Final Exam 40%
3. Class Participations and HWs 10%
4. Research paper & presentation 20 %

Attendance

Students are expected to attend class; there is no system of permitted absences. The instructor in each class determines the effect of absences on a student's grade in that class." Students may not normally receive credit for a course if they do not attend the class meetings.

Project and term paper:

Each Student is expected to participate in several tasks covering various topics in web and secure software development. Each student will also submit and present a term paper that forms a basis for a publishable research paper.

GOOD LUCK!