

**Jerash University**

**Faculty of Computer Science and Information Technology**

**Computer Sciences Department**

**Semester**: Fall Semester 2018/2019

|  |  |
| --- | --- |
| **Course symbol and number:** 1003472 | **Course Name:** تحليل الادلة الجنائية |
| **Teaching Language:** English | **Prerequisites:** . **1003460** |
| **Credits:** 3 hours**.** | **Course Level:** 3 |

|  |
| --- |
| **Course Description** |
| Examination of techniques and tools used to investigate, search, collect, analyze, and report on network based breaches and events.  Although many concepts of network forensics are similar to those of any other digital forensic investigation, the network in of itself presents many nuances that require special attention. This course will teach digital forensics and incident response to network-based evidence. This course will also acclimate the student to the basic tools and techniques of the trade. |

|  |
| --- |
| **Course Objectives** |
| •This course is designed to build on the material learned foundational forensic courses and apply those concepts to a network environment. This course places a strong emphasis on digital forensic procedures, digital forensic tools, and legal issues relating to digital forensics in a network environment. This course uses advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators. |

|  |
| --- |
| **Learning Outcomes** |
| This course is designed to build on the material learned foundational forensic courses and apply those concepts to a network environment. This course places a strong emphasis on digital forensic procedures, digital forensic tools, and legal issues relating to digital forensics in a network environment. This course uses advanced forensic tools and hands on exercises to emphasize the procedures that students will utilize in the field as forensic investigators. |

|  |  |
| --- | --- |
|  | **Text Book(s)** |
| **Title** | Network Forensics- Tracking Hackers Through Cyberspace. ISBN: 0132564718 |
| **Author(s)** | Davidoff |
| **Publisher** | 2012 |
| **Year** | 2012 |
| **Edition** | Fourth |

|  |  |
| --- | --- |
|  | **References** |
| **Books** | Brunty, J., Helenek, K. (2012). Social Media Investigation for Law Enforcement. ISBN: 1455731358 |
| **Internet links** | http://www.jpu.edu.jo/lms |
| **Course link** | [Click here](http://www.jpu.edu.jo/lms) |

|  |  |
| --- | --- |
|  | **Instructors** |
| **Instructor** |  |
| **Office Location** | الطابق السادس - 611 |
| **Office Phone** | 666 |
| **E-mail** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics Covered** | | | |
| **Topics** | **Chapters in Text** | **Week number** | **Teaching hours** |
| Introduction. Host security and network security. Basic cryptography and cryptanalysis. Steganography. Traffic types. | Mirkovic et al. Chapters 1-4 | 1-3 | 2 |
| Basic traffic analysis. Pcap vs. NetFlow vs. Headers. | SiLK Analysts' | 4, 5, 6 | 5 |
| Approaches for Traffic and Data Anonymization. | CAIDA traffic | 7 | 4 |
| Network Statistics and Visualization | SiLK's RAVE docs CAIDA +Internet Motion Sensor sites | 8 | 2 |
| Network Analysis Experiences | Mirkovic et al.Chapter 7, Appendix C | 9 | 3 |
| Mathematical Traffic Models | Skitter/  Archipelago  topology of  Internet | 10 | 2 |
| Multiresolution Analysis I | **MRA in Matlab** | 11 | 3 |
| Multiresolution Analysis II | MRA in Matlab | 12 | 2 |
| Sidechannel Analysis | Mirkovic,  Backscatter  Cryptanalysis  Lounge site | 13 | 2 |
| Connecting the dots: relating to the host | Conficker (or recent malware) reports | 14 | 2 |
| Basic host forensics | Knoppix tools  TCT tools | 15 | 2 |
|  | Handout |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Evaluation** |  |
| **Assessment Tool** | **Expected Due Date** | **Weight** |
| Programming assignments and LMS |  | 20 % |
| First Exam |  | 20 % |
| Second Exam |  | 20 % |
| Final Exam | According to the University final examination schedule | 40 % |

|  |  |
| --- | --- |
|  | **Policy** |
| **Attendance** | Attendance is very important for the course. In accordance with university policy, students missing more than the allowed absence rate of total classes are subject to failure. Penalties may be assessed without regard to the student's performance. Attendance will be recorded at the beginning or end of each class. |
| **Exams** | All exams will be CLOSE-BOOK; necessary algorithms/equations/relations will be supplied as convenient. |

|  |
| --- |
| **Class Schedule & Room** |

|  |  |  |
| --- | --- | --- |
| **Office Hours** | | |
| Sun: 11 – 12.30  Mon: 11 - 12:30  Tues: 11- 12.30  Wed: 11 – 12:30 | | |
|  | \* Or by an appointment through email |  |

|  |  |
| --- | --- |
|  | **Teaching Assistant** |
| To announced later on. |  |

|  |  |
| --- | --- |
|  | **Prerequisites** |
| **Prerequisites by course** |  |