CSCI 393 Computer Forensics - Spring 2018

Course Information

Lectures:

MWF 9:00 - 9:50 AM, Freedom 322

Professor:

Dr. Yana Kortsarts
Office: Freedom Hall 313
Phone: (610) - 499 - 4367
e-mail: ykortsarts@widener.edu
homepage: **http://cs.widener.edu/~yanako**

Office Hours:

Place: Freedom Hall 313
Time:

- Monday: 12:00 - 1:00 PM, 3:45 - 4:00 PM, 5:00 - 5:30 PM
- Wednesday: 12:00 - 1:00 PM, 3:45 - 5:00 PM
- Thursday: 6:00 - 7:00 PM - Virtual Office Hours by Skype connect to **office_hours_for_students**
- Friday: 1:00 - 3:00 PM, 4:00 - 5:00 PM

Additional office hours and extra help are ALWAYS available!
Please see me in class, call me or email me. I am available at other times outside of the listed office hours to help you. JUST ASK.
To make an appointment, please, send an e-mail ykortsarts@widener.edu

Recommended Text - NOT REQUIRED:

- Access Data Forensics (will be provided)
- File System Forensics Analysis, Brian Carrier, Pearson Education, Inc, ISBN 0-32-126817-2

Course Description

Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law. This course will introduce students to the fundamentals of computer forensics and cyber-crime scene analysis, evidence acquisition and data decryption. Student will learn investigative and analytical techniques to acquire and protect potential legal evidence. The various laws and regulations dealing with computer forensic analysis will be discussed. Students will be introduced to the emerging international standards for computer forensic analysis, as well as a formal methodology for conducting computer forensic investigations.

Tentative Course Topics:

- Digital Investigation Foundations
  - Digital Crime Scene Investigation Process

        - Data Analysis
        - Overview of the toolkits
    - File Systems Analysis
        - File System Category
        - Specific File Systems Overview
    - Working with FTK Imager
    - Registry Viewer Introduction
    - Working with FTK
    - Processing the Case
    - Regular Expressions
    - Overview of Cryptography Topic Related to the Course
        - Understanding of the challenges faced when encountering encrypted data during forensic examinations.
        - Typical Encryption Schemes Used in Today's Software applications
        - Encryption File System
        - Working with PRTK Password Recovery Toolkit
    - Case Reporting

Student Learning Outcomes

Upon successful completion of this course, students will be able to:

- Demonstrate understanding of fundamentals of computer forensics and cyber-crime scene analysis, evidence acquisition and data decryption.
- Demonstrate understanding of the investigative and analytical techniques to acquire and protect potential legal evidence.
- Apply introductory descriptive analytics techniques to perform the data analysis
- Perform forensic computer examinations using Access Data Forensic Toolkit (FTK), FTK Imager, Password Recovery Toolkit (PRTK) and Registry Viewer

Corresponding Computer Science/Computer Information Systems Outcomes

- Outcome 3. Students demonstrate independent learning, recognize the limitations of their computer science knowledge and are prepared for continued learning in computer science.
- Outcome 4. Demonstrate an understanding of ethical issues and professional responsibilities related to computing and the impact technology has on society

Corresponding A&S Goals

- Goal 2: A liberally educated graduate thinks critically.
    - 2.a. Makes claims and draws conclusions that require the analysis and evaluation of evidence.
- Goal 4: A liberally education graduate has developed a wide range of intellectual perspectives and methodologies.
    - 4.a. Evaluates the workings of the natural and physical world using theories and models that can be tested by experiments and observations.

Corresponding Widener University Institutional Learning Objectives (ILOs)

- ILO 1. Students will demonstrate the knowledge, skills, and scholarship appropriate to their major field of study.
- ILO 2. Students will be able to think critically and communicate effectively.

Policies

Attendance Policy

The University's policy will be applied. Students who miss class are always responsible for obtaining class assignments. All assignments and class materials are available through this website.

In this course ATTENDANCE IS REQUIRED. Class Participation and Attendance is 25% of the final grade.

Academic Fraud

The Science Division strictly enforces the University's policy on cheating and other forms of academic fraud.

Student Academic Grievance Procedure

If a student has a grievance concerning a class in which he/she is enrolled, he/she will first try to resolve the problem with the instructor of the class. If it is impossible to resolve the matter at this level, then the grievance must be placed in writing and appealed in the following order:

- Division or Program Head
- Dean of Arts and Sciences (Arts and Sciences Academic Council)
- Provost of the University
- University Academic Council

All student grievances will first be referred to the class instructor before they are treated at the level of the Division Head.

Please see Widener's Undergraduate Catalog for:
Standards for Academic Integrity, Appeal Procedures for Student Academic Grievances, and Attendance Policy

Please see Widener's Policies on Attendance in the student handbook on-line:
Student Handbook

Learning Accommodations

In accordance with the Americans with Disabilities Act, any student has the right to request reasonable accommodation of a disability. Accommodations can be requested through Academic Support Services, Disabilities Services (520 E. 14th St., 610-499-1266). Disabilities Services is the office that authorizes all accommodations on campus. Please note that you will need to present documentation of your disability to Disabilities Services. It is important to make this request as soon as possible so that we will have time to make any necessary arrangements

Electronic Devices in the Classroom

- NO CELL PHONES. Cell phones must be turned off for the duration of the lecture and lab.
- All electronic devices except cell phones are permitted

Evaluation Criteria (Grading)

Your grade for this course is divided into three categories: In Class Quizzes and Lab Assignments, In Class Practice and Participation, Homework. The breakdown is as follows:

Final Grade

In Class Quizzes and Lab Assignments	70%
In Class Practice, Participation and Attendance	25%
Homework	5%
Total	100%

Final Grade Table

A:	95 - 100
A-:	90 - 94
B+:	87 - 89
B:	83 - 86
B-:	80 - 82
C+:	77 - 79
C:	73 - 76
C-:	70 - 72
D+:	67 - 69
D:	60 - 66
F:	59 - 0

- **Course and Reading Material**

All information in this document is subject to change throughout the semester. Check the course website and your Widener e-mail regularly, any changes will be indicated on the course website and sent by e-mail. Students will be notified about any change at least one week in advance.
