UNIVERSITY OF ILLINOIS AT SPRINGFIELD

CSC470: Incident Response

Credit Hours: 4.0
Spring 2015

Instructor: Frank C Fuchs
Office: UHB 3102
Office Hours: By Appointment
Phone: (217) 206-8535
Email: ffuch2@uis.edu

Course Description

Blended - Online & Classroom.
This is a hands-on virtual lab course. The course consists of labs utilizing real workplace scenarios. Learn how digital forensic professionals focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

Course topics include methods for analyzing digital crime, tool kits that can be taken to the scenes of computer-related crime, forensic analysis and solutions for other types of digital media such as USB memory and Palm devices. Restricted to graduating students required to take an on campus course.
Contact csc@uis.edu. Requires Departmental Approval

Course Objectives/Learning Outcomes

- Understand the process of responding to a network intrusion
- Explain the different types of network-based evidence
- Compare open-source tools with industry standard commercial software
- Identify what computer forensics tools and techniques can reveal and recover
- Describe the basic steps in a network-based intrusion
- Understand some common forensic analysis techniques
- Learn how to reconstruct basic web browsing activity
- Learn how to reconstruct e-mail activity
- Conduct a forensic recovery of electronic media
- Report the results of a forensic examination

Reasonable accommodations are available for students who have a documented disability. A documented disability can include: physical, psychological, chronic health, vision, hearing, learning, traumatic brain injury, Asperger's Syndrome and/or autism, cognitive, and A.D./H.D.D. Please notify the instructor during the first week of class of any accommodations needed for the course. While O.D.S. does accept late applications, accommodations are not retroactive. All accommodations must be approved through the Office of Disability Services (ODS) (217-206-6666), HRB 80.

Course Content

The following topics are a guideline only and are subject to change.

Topics

- Chapter 1: Windows Live Response
- Chapter 3: Collecting Network-Based Evidence
- Chapter 4: Analyzing Network-Based Evidence
- Chapter 6,7,8: Acquiring a Forensic Duplication
- Chapter 9: Common Forensic Analysis Techniques
- Chapter 10: Web Browsing Activity Reconstruction
- Chapter 11: E-Mail Activity Reconstruction
- Chapter 12: Windows Registry Reconstruction
- Chapter 19-20: Forensic Duplication and Analysis
- Chapter 21: Tracing E-Mail and Domain Name Ownership

Required Text

Real Digital Forensics: *Computer Security and Incident Response*
Keith J, Jones, Richard Bejtlich, and Curtis W. Rose
Pearson Education, Inc. 2006
ISBN: 0-321-24069-3

Additional recommended reading:

Best Practices for Seizing Electronic Evidence v.3 by the U.S. Department of Homeland Security, United States Secret Service (available on the course Blackboard).

Grading

The final grade will be based on:
40% Chapter Quizzes
40% Laboratory Reports
10% Participation
10% Mid-Term Quiz

Delivery Method

A Blackboard course space will be available for course material, quizzes, and labs. Laboratories will be performed on the UIS virtual servers using EnCase Forensic Suite by Guidance Software, Inc

UIS Academic Integrity Policy

I support the UIS policy on Academic Integrity, which states, in part:

"Academic integrity is at the heart of the university's commitment to academic excellence. The UIS community strives to communicate and support clear standards of integrity, so that undergraduate and graduate students can internalize those standards and carry them forward in their personal and professional lives. Living a life with integrity prepares students to assume leadership roles in their communities as well as in their chosen profession. Alumni can be proud of their education and the

larger society will benefit from the University's contribution to the development of ethical leaders. Violations of academic integrity demean the violator, degrade the learning process, deflate the meaning of grades, discredit the accomplishments of past and present students, and tarnish the reputation of the university for all its members."

Academic sanctions range from a warning to expulsion from the university, depending on the severity of your violation and your history of violations. Whatever the sanction, I will file a report of academic dishonesty to the Office of the Provost.

You are responsible for understanding and complying with the UIS Academic Integrity Policy available at http://www.uis.edu/campussenate/academicintegrity.htm