Academic Syllabus

Course Name: Digital Forensics
Course Number: CS 477
Course Credits: 4
Prerequisite: C or higher in CS 344 and CS 370

Course Description:

This course will introduce the concept of digital forensics, its role and importance, and tools and techniques for collecting and curating digital evidence. It will also discuss the role of evidence in the justice system and some legal aspects as they pertain to digital forensics. It will introduce tools and techniques for computer and network forensics.

Course Content:

- Digital forensics concepts:
  - What is forensics?
  - Branches and applications of digital forensics.
  - Overview of forensics principles: scientific method, evidence principles, documentation, reporting & testimony.
- Sociological Aspects of Digital Forensics
  - Structure of legal system - Disputes/adversarial, Civil vs. criminal justice systems
  - Evidence - Standards for scientific evidence, Forensic sciences
  - Decision-makers - Judges, Juries.
- Legal Aspects of Digital Forensics
  - Bill of Rights; requirement of warrant; expectations of privacy; exceptions
  - Rules of evidence, chain of custody, best evidence rule etc.
  - Privacy laws, cyber crime laws, electronic communication laws
- Computer Forensics
  - What is computer forensics?
  - Hardware fundamentals; files system analysis; recovering deleted files/evidence; analysis of windows systems
- Network Forensics
  - Network-based evidence sources; evidence-gathering techniques; packet/flow/protocol analysis; network intrusion detection analysis
- Additional related topics, time permitting
  - Fraud Investigations
  - Digital Archives
  - Incident Management and Response - Preparation; Detection and Analysis; Containment, Eradication, and Recovery; Post-Incident Activity
Course Specific Measurable Student Learning Outcomes:

At the completion of this course, students will be able to:

1. Understand the need for digital forensics, as well as relevant legal structure and laws
2. Describe basic evidence gathering and curating techniques for computer and networks forensics
3. Apply tools and techniques to acquire and curate forensics evidence from computers and networks
4. Assess the value of different pieces of forensics evidence

Evaluation of Student Performance:

- Homeworks/Quizzes/Participation/Hands-on Labs (approx. 30%)
- Programming Assignments/Problems (approx. 40%)
- Exams (approx. 30%)

Learning Resources:

The instructor will typically provide students with lecture notes, links to online resources and/or textbooks such as the following...

- Brian Carrier, File System Forensic Analysis, Addison Wesley.
- Cichonski et. al, National Institute of Standards and Technology Special Publication 800-61, Rev. 2, Computer Security Incident Handling Guide.

Statement Regarding Students with Disabilities:

Accommodations for students with disabilities are determined and approved by Disability Access Services (DAS). If you, as a student, believe you are eligible for accommodations but have not obtained approval please contact DAS immediately at 541-737-4098 or at http://ds.oregonstate.edu. DAS notifies students and faculty members of approved academic accommodations and coordinates implementation of those accommodations. While not required, students and faculty members are encouraged to discuss details of the implementation of individual accommodations.
Statement of Expectations for Student Conduct:

http://studentlife.oregonstate.edu/code