Sam Houston State University

Department of Computer Science
DF 390: Digital Forensics Tools
Syllabus
Fall 2007

General Information

Instructor: Dr. Peter A. Cooper
Office: AB1 214
Phone: 294 1569
Email: cooper@shsu.edu,

Course Title: Digital Forensics Tools

Course Description

This course explores tools for the recovery of information on protected or damaged hardware for the purpose of providing evidence of misuse or abuse of systems. Topics also include the chain of evidence, protocols for data recovery, cryptographic analysis, password recovery, the bypassing of specific target operating systems and obtaining data from digital devices that have been damaged or destroyed. Prerequisite: DF 291. Credit 3.

Course goals

At the end of this course the ideal student should be able to

- Effectively perform live response forensics on Windows, Linux and Macintosh computers
- Conduct network-based forensics examination of Windows and Linux systems
- Acquire forensically sound drive duplications
- Acquire duplications of USB, flash memory and other mobile devices
- Conduct forensic analysis of on-line services
- Apply data recovery techniques to obtain data from various damaged media

Grading Criteria

- Four Tests @ 100 pts each
- Four practical assignments @ 100 pts each
- 1 final exam at 200 pts

Course Schedule

1. **Live Windows Forensics**
2. **Live Unix Forensics**
3. **Live Mac Forensics**
4. **Network-Based Analysis for Windows Systems**
5. **Network Based Analysis of Unix Systems**
6. **Test 1**
7. **Duplication Tools**
8. **Web Activity Analysis**
9. **Email Activity Analysis**
10. **Test 2**
11. **Analyzing Files of Unknown Origin**
12. **Mobile Device Acquisition**
13. **Building a Live CD**
14. **Test 3**
15. **Password Recovery**
16. **Cryptanalysis Tools**
17. **Recovering damaged data**
18. **Recovering data from damaged media**
19. **Test 4**
20. **Final exam**

Attendance Requirements
Student attendance is mandatory for all class sessions. Absence from any and each class period will result in a 5% reduction in overall grade. Documented medical related absences are exempt from this policy. Students may submit 1 extra credit assignment in lieu of a single undocumented absence. Students with documented medical related absences will be expected to initiate the process of completing any make-up work.

Tests
There are four test and a final exam. Each test covers the material for that section of the course. The final exam is a practical exam that requires application of the techniques discussed in class to solve a set of forensics problems. Students are required to take all four tests and the final in order to obtain a grade in the class.

Academic dishonesty
All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain complete honesty and integrity in the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The University and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including, but not limited to, cheating on an examination or other academic work which is to be submitted, plagiarism, collusion and the abuse of resource materials.

Classroom Conduct
Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Cellular telephones and pagers must be turned off before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a directive to leave class. Students who are especially disruptive also may be reported to the Dean of Students for disciplinary action in accordance with university policy.

Visitors in the Classroom
Unannounced visitors to class must present a current, official SHSU identification card to be permitted in the classroom. They must not present a disruption to the class by their attendance. If the visitor is not a registered student, it is at the instructor's discretion whether or not the visitor will be allowed to remain in the classroom.

Americans with Disabilities Act
Students with disabilities covered by the Americans with disabilities Act should go to the Counseling Center and Services for Students with Disabilities (SSD) in a timely manner to obtain the documentation required. Students are responsible for initiating the process of documenting the need for an accommodation under the ADA act.

Religious Observance
University policy allows for student to observe religious holy days without penalty. If you intend to miss class as a result of the observance of a religious holy day or as a result of the necessary traveling time required for religious observance, such an absence will not be penalized. As a courtesy, it would be appreciated if you notify the instructor in advance in writing, of the dates and times of class sessions that are to be missed. Students absent from class as a result of religious observance are required to submit any due assignments immediately on their return to the classroom. Makeup tests and quizzes will also be provided on return to the class.

Course Text
Jones, K.J., Bejtlick, R., & Rose, C.W. Real Digital Forensics: Computer Security and Incident Response. Addison Wesley ISBN 0-321-24069-3

Office Hours
- I am available online most times, most days unless specifically in another class.
- I can be reached via email (cooper@shsu.edu) or via instant messenger (AIM), at peter.cooper@mac.com)
- I am also available by cell phone 936.662.6525