

## CS 4677 Course Syllabus

1. **Catalog Description:** CS4677 Computer Forensics (3-3). This course is intended to provide students with an understanding of the fundamentals of computer forensics as it might be used in the context of DoN/DoD information assurance and information operations activities. Students will examine how information is stored in computer systems and how it may be deliberately hidden and subverted. The course will establish a sound foundation based upon methods for information extraction as used for evidential purposes. It will cover practical forensic examination and analysis. The course will also examine techniques of computer evidence recovery and the successful presentation of such evidence within legal contexts. Laboratory activities will introduce students to the use of common forensic tools, the principle of original integrity, disk examination, logging and preparation of evidence. **PREREQUISITES:** CS3010 or CS3030, CS3600 and CS3670, or the consent of the instructor.

2. **Academic Objectives:** An understanding of the application of basic forensic techniques

3. **Skills:** Upon completion of this course, the student is expected to be able to collect digital evidence and conduct forensic analysis of compromised computer systems

4. **Course Outline** (not necessarily limited to the following)

1. Forensics and Incident response background
2. Live system collection and analysis
  - a. Windows
  - b. Unix
3. Network evidence collection and analysis
  - a. Windows
  - b. Unix
4. Forensic duplication tools and techniques
5. File systems
6. Disk image analysis techniques
7. Web browser forensics
8. Email forensics
9. Windows registry forensics

10. Malware analysis

11. Mobile Phone Forensics

6. **Grading:** Homework/Labs = 100%

7. **Course Work:** We will cover a wide variety of topics from very technical to very non-technical. Lab assignments will reinforce concepts covered in lecture and the text while occasional homework assignments will explore topics outside those explicitly covered in the lecture.

8. **Collaboration Policy:** Homework is to be done individually. For labs, you may work with a partner unless otherwise specified.

9. **Late Submissions:** These are accepted, but unless you have arranged in advance (more than 48 hours) for an extension you lose 10% per day up to a maximum of %50. You can always get at least half credit up to the end of the quarter.

10. **Plagiarism:** If you refer to material from external sources (other than the slides or lecture) please be sure to cite it. Also, please don't turn in work you didn't do yourself. If there is evidence that an assignment has been improperly copied, everyone who submitted the copied text will receive a 0 for that assignment (even the people who actually did the work, since I have no way of knowing who that was), and your program officer will be notified. Please don't let this happen; it is super depressing.

11. **Instructor Information:**

