

## **CGS 5131, Computer Forensics I**

S. Lang, Fall 2006

**Syllabus**

August 22, 2006

**Instructor:** Dr. S. Lang (203 CSB, 407-823-2474, [lang@cs.ucf.edu](mailto:lang@cs.ucf.edu))

**Office Hours:** Monday and Wednesday, 2 – 4 pm

**Recommended Text:** File System Forensic Analysis, by Brian Carrier, Addison-Wesley, 2005, ISBN 0-32-126817-2

### **Other References:**

- (1) Computer Forensics, by Kruse and Heiser, Addison-Wesley, 2002
- (2) Guide to Computer Forensics and Investigations, by Nelson, Phillips, Enfinger, and Steuart, Thomson Course Technology, 2004
- (3) Hacking Exposed Computer Forensics, by Davis, Cowen, and Philipp, McGraw-Hill/Osborne, 2005
- (4) Real Digital Forensics, by Jones, Bejtlich, and Rose, Addison-Wesley, 2006

### **Topics:**

#### Part A. Fundamentals:

1. Overview of computer forensics  
The forensics process, disk imaging, forensics tools
2. Hardware and OS fundamentals  
Disk geometry, partitions, Windows and Linux file systems
3. File signatures, string searching  
File types, regular expressions, grep, egrep, and fgrep commands
4. Data hiding techniques  
Deleted file recovery, recycle bin, alternate data streams, cryptography, steganography, anti-forensics tools

#### Part B. Investigative Techniques:

5. Windows registry files
6. Email analysis
7. Internet activity analysis
8. Live system forensics and incident response
9. Static and dynamic analysis of executable file
10. Documentation and reports

#### Part C. Legal Issues:

11. The justice system
12. Cyberlaw and case studies

### **Course Work:**

- Homework assignments, including exams on floppy disk, USB thumb drive, and hard disk using FTK and other open source tools (50%)
- Midterm exam (20%)
- Final exam (30%)

### **Grading Policy:**

- Homework assignments are to be submitted to the WebCT site by the due dates; no late assignments are accepted unless prior arrangements are made
- Exams are given online on WebCT, each open for a period of 5 days
- Homework (and exams) represent individual work, no “team” work or plagiarism will be tolerated
- Grades are based on the straight-percentage scale, i.e., A (90% or up), B (80 – 89.99%), C (70 – 79.99%), D (60 – 69.99%), and F (below 60%); plus/minus grades will be used sparsely (if at all)

**Academic Integrity and Student Conduct:** Please read and understand student rights and responsibilities including conduct rules clearly stated in UCF’s **golden rules**, available at [http://www.goldenrule.sdes.ucf.edu/2e\\_Rules.html](http://www.goldenrule.sdes.ucf.edu/2e_Rules.html)

**Course Website:** [www.cs.ucf.edu/courses/cgs5131/fall2006](http://www.cs.ucf.edu/courses/cgs5131/fall2006) and also on WebCT (under construction)