USC
SCHOOL OF
ENGINEERING

Digital Forensics
ITP 375 (3 Units)

Description

In 2007, the FBI reported that over 200 major companies reported a loss of over 60 million dollars due to computer crime. Computers are becoming more of a threat today than ever before. From cyber-terrorism to identity theft, the digital age has brought about a change in the way that crime is being committed. The usage of computers in crime has lead to the emerging field of computer forensics. This course is designed to give students the tools and techniques for investigating crime involving digital evidence.

This course is designed as an introductory course in computer forensics. Students will first understand the need for computer forensics. Students will learn best practices for general incidence response. The course will then focus on the tools and techniques to perform a full computer forensic investigation.

Objective

Upon completing this course, students will:
- Understand the fundamentals of computer forensics
- Understand the legal aspects of forensics
- Understand the relationship between IT and forensics
- Learn best practices for incidence response

Prerequisites/ Recommended Preparation

ITP 125 or Department Approval

Instructor

Joseph Greenfield

Contacting the Instructor

joseph.greenfield@usc.edu | 213-740-4604

Lecture/Lab

Tuesday & Thursday, 3:30 – 4:50, OHE 406

Required Textbooks

Hacking Exposed: Computer Forensics, Second Edition. Davis, Philipp, and Cowen
ISBN: 0071626778

Web Site

All course material will be on Blackboard at blackboard.usc.edu

Grading

Students will have structured labs throughout the semester, to be conducted during the scheduled lab time. Students will also have a few labs to be completed at home. The grade breakdown is as follows:

Labs	60%
Midterm	15%
Final Exam	25%
Total	100%

Grading Scale

The following is the grading scale to be used for the final grades at the end of the semester

93% and above	A
90% – 93%	A-
87% – 90%	B+
83% – 87%	B
80% – 83%	B-
77% – 80%	C+
73% - 77%	C
70% – 73%	C-
67% – 70%	D+
63% – 67%	D
60% – 63%	D-
Below 60%	F

Policies

- Projects turned in after the deadline will automatically have 5% deducted per day. Projects will not be accepted after 1 week beyond the project’s deadline
- No make-up exams (except for medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.
- It is your responsibility to submit your project on or before the due date. **It is not the responsibility of the lab assistant.** Do **not** turn in anything to your lab assistant!
- All projects will be digitally submitted through blackboard except where specifically specified. Always keep a backup copy of your labs

Academic Integrity

The use of unauthorized material, communication with fellow students during an examination, attempting to benefit from the work of another student, and similar behavior that defeats the intent of an examination or other class work is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behaviour resulting from the nervous tension accompanying examinations. When the professor determines that a violation has occurred, appropriate action, as determined by the instructor, will be taken.

Although working together is encouraged, all work claimed as yours must in fact be your own effort. Students who plagiarize the work of other students will receive zero points and possibly be referred to Student Judicial Affairs and Community Standards (SJACS).

All students should read, understand, and abide by the University Student Conduct Code listed in SCampus, and available at: http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html

Students with Disabilities

Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each

	semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to your TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m. - 5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776.

Fundamentals of Computer Forensics

ITP 375 (3 Units)

Course Outline

Week 1 – Introduction to Computer Forensics

- Course overview
- Understanding the need for computer forensics
- Defining computer forensics

Reading: Chapter 1

Week 2 – Computer Hardware

- Understanding computer components
- Digital Media
- Hard disk basics

Reading: Chapter 2

Week 3 – The Forensic Toolkit

- Forensic hardware
- Hardware write/blockers
- Hard drive acquisitions
- Processing the scene

Reading: Chapters 3 & 4
Lab 1: Hard drive acquisition

Week 4 – Files and File Systems

- Windows file systems
- FAT32
- NTFS
- Forensic file images

Reading: Chapter 6
Lab 2: Preparing the case

Week 5 – Forensic software

- Overview of different software packages
- EnCase
- Autopsy

Reading: Instructor Handouts
Lab 3: EnCase introduction

Week 6 – Bookmarking and Searching

- Creating basic search queries
- Hex, Decimal, and Binary
- ASCII
- Unicode

Reading: Instructor Handouts
Lab 4: Searching evidence for common keywords

Week 7 – GREP

- Understanding GREP
- Building Regular Expressions
- Creating GREP keywords
- Viewing and managing keywords and cases

Reading: Instructor Handouts
Lab 5: GREP lab

Week 8 – Forensic Reports

- Creating a forensic report
- Proper report writing
- Explaining forensics to the uneducated

Reading: Instructor Handouts

Week 9 – MIDTERM

Week 10 – E-mail Analysis

- Viewing e-mail
- Webmail
- POP
- IMAP

Reading: Chapter 11
Lab 6: E-mail analysis lab

Week 11 – File Signature Analysis

- File signatures
- File extensions
- Differences between
- Identifying differences

Reading: Instructor Handouts
Lab 7: Detecting File Manipulation

Week 12 – Hash Analysis

- Understanding hash algorithms
- Hashing files
- Hash libraries

Reading: Instructor notes
Lab 8: Hash analysis lab

Week 13 – Other Windows Artifacts

- Common windows artifacts
- Recycle bin
- My Documents
- Recent files
- Installed programs

Reading: Chapter 12
Lab 9: Basic Computer Forensics Lab

Week 14 – A real forensic case

- Processing a complete forensic case
- Preparing a forensic report

Reading: Chapter 14

Week 15 – Conclusion

- Review for the final exam
- Conclusion to the course