USC SCHOOL OF ENGINEERING

Advanced Digital Forensics
ITP 475 (4 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 as an advanced course in computer forensics. The course assumes that students have either satisfied the prerequisite of ITP 375 – Digital Forensics, or instructor approval. Students will engage in advanced topics in computer forensics, culminating in a final project involving a mock trial.
Objective	Upon completing this course, students will: - Have advanced knowledge in the latest tools and techniques for computer forensics - Engage in a mock trial - Research upcoming topics in digital forensics - Complete a variety of case studies in digital forensics
Prerequisites/ Recommended Preparation	ITP 375 or department approval
Instructor	Joseph Greenfield
Contacting the Instructor	joseph.greenfield@usc.edu | 213-740-4604
Lecture/Lab	5:00 – 6:50, Tuesday & Thursday, OHE 406
Required Textbooks	Incident Response and Computer Forensics, Second Edition ISBN: 007222696X
Recommended Textbook	Hacking Exposed Computer Forensics, Second Edition ISBN: 0071626778
Web Site	All course material will be on Blackboard at blackboard.usc.edu
Grading	Grading will be based on percentages earned in assignments. The scheduled class time will involve a combination of lectures and structured labs. Students are expected to spend time at home completing the assignments. Labs 50% Midterm 15% Final (Mock Trial) 35% 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.

Security and Computer Forensics

ITP 475 (4 Units)

Course Outline

Week 1 – Digital Forensics Review

- Investigative Process
- Analysis methodologies
- Tools and techniques

Reading:

Week 2 – Lab Setup and Network Overview

- Setting up the investigative software
- Establishing remote connection to server

Reading:
Lab 1: Review (Windows standalone) case

Week 3 – Unix/Linux Forensics

- *nix operating systems
- *nix file systems
- Artifacts and investigative leads

Reading:
Lab 2: Linux case

Week 4 – Filesharing and Peer-to-Peer

- Popular file sharing protocols and applications
- Filesharing logs
- Network logs

Reading:

Week 5 – Mobile Device Forensics

- Mobile device discussions
- Introduction to common handheld devices
- Mobile device project introduced

Reading:
Lab 3: Filesharing case

Week 6 – Advanced file system analysis

- FAT
- NTFS
- Partially deleted headers
- Parsing NTFS and FAT entries

Reading:

Week 7 – Viruses, Malware, and other nastiness

- The "virus defense"
- Detecting malware
- Rootkit analysis

Reading:
Lab 4: The malware defense

Week 8 – Advanced E-mail and Internet analysis

- Web cache, history, bookmarks, etc.
- Mail header analysis
- E-mail server analysis
- Building timelines

Reading:
Lab 5: E-mail case

Week 9 – MIDTERM

Week 10– Network forensics

- Networking 101
  - Topologies and designs
  - Protocols
  - Enterprise setups
- Introduction to network forensics
- Decrypting Logs!

Week 11 – Incident Response

- Preparing for disaster
- Policies and actions

Reading:
Lab 6: Enterprise Case

Week 12 – Live system and network analysis

- Malware analysis
- Network sniffing
- Network isolation
- Live and network acquisitions

Reading:
Lab 7: Live analysis case

Week 13 – Court and Deposition

- The game of court
- Court documents
- Interacting with attorneys

Reading:

Week 14 – Law enforcement and forensics

- Role of digital forensics in law enforcement
- Guest speakers from various agencies

Reading:

Week 15 – Preparing for the final case

Reading:

Week 15 – Mock Trial

- Time and location TBA

Reading: