Digital Forensics
ITP 375 (3 Units)

Fall 2015

Objective

In 2013, worldwide cybercrime profits exceeded the worldwide drug trade profits. 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 led 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.

Concepts

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

ITP 125 or Instructor Approval

Instructor	Jennifer Kassar
Contacting the Instructor	jkassar@usc.edu
Office Hours	Tuesday / Thursdays 6:30-7PM OHE 406 Wednesday 1:30-4:30PM OHE 530C
Lab Assistants	Kevin Keer & Yiwei Song
Lecture/Lab	5-6:30PM Tuesday & Thursday OHE 406

Required Textbooks

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

Website

All course material will be on Blackboard (http://blackboard.usc.edu).

Grading

Grading will be based on percentages earned in assignments. Students will have structured labs throughout the semester, to be conducted during the scheduled lab time.

Lab Assignments	60%
Midterm Exam	15%
Final Exam	25%
Total	100%

Grading Scale

The following shows the grading scale to be used to determine the letter grade.

93% and above	A
90% - 92%	A-
87% - 89%	B+
83% - 86%	B
80% - 82%	B-
77% - 79%	C+
73% - 76%	C
70% - 72%	C-
67% - 69%	D+
64% - 66%	D
63% and below	F

Policies

No make-up exams (except for documented medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.

The labs will be posted on Blackboard under the "Assignments" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link.

It is your responsibility to submit your assignments on or before the due date. Assignments turned in one day late will have 20% of the total points deducted from the graded score. Assignments turned in two days late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted and you will receive a 0.

All assignments will be digitally submitted through Blackboard except where specified. Do not email them to the lecturer or lab assistant.

Incomplete and Missing Grades

Excerpts for this section have been taken from the University Grading Handbook, located at

http://www.usc.edu/dept/ARR/grades/gradinghandbook/index.html. Please see the link for more details on this and any other grading concerns.

A grade of Missing Grade (MG) "should only be assigned in unique or unusual situations… for those cases in which a student does not complete work for the course before the semester ends. All missing grades must be resolved by the instructor through the Correction of Grade Process. One calendar year is allowed to resolve a MG. If an MG is not resolved [within] one year the grade is changed to [Unofficial Withdrawal] UW and will be calculated into the grade point average a zero grade points.

A grade of Incomplete (IN) "is assigned when work is no completed because of documented illness or other 'emergency' **occurring after the twelfth week** of the semester (or 12th week equivalency for any course scheduled for less than 15 weeks)."

Academic Integrity

USC seeks to maintain an optimal learning environment. General principles of academic honesty include the concept of respect for the intellectual property of others, the expectation that individual work will be submitted unless otherwise allowed by an instructor, and the obligations both to protect one's own academic work from misuse by others as well as to avoid using another's work as one's own. All students are expected to understand and abide by these principles. *Scampus,* the Student Guidebook, contains the Student Conduct Code in Section 11.00, while the recommended sanctions are located in Appendix A: http://www.usc.edu/dept/publications/SCAMPUS/gov/. Students will be referred to the Office of Student Judicial Affairs and Community Standards for further review, should there be any suspicion of academic dishonesty. The Review process can be found at: http://www.usc.edu/student-affairs/SJACS/.

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 your course instructor (or TA) as early in the semester as possible. DSP is located in STU 301 and is open from 8:30am to 5:00pm, Monday through Friday. Website and contact information for DSP http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html (213) 740-0776 (Phone), (213) 740-6948 (TDD only), (213) 740-8216 (FAX) ability@usc.edu

Emergency Preparedness/Course Continuity in a Crisis

In case of emergency, when travel to campus is difficult, if not impossible, USC executive leadership will announce a digital way for instructors to teach students in their residence halls or homes using a combination of the Blackboard LMS (Learning Management System), teleconferencing, and other technologies. Instructors should be prepared to assign students a "Plan B" project that can be completed 'at a distance.' For additional information about maintaining your classes in an emergency, please access: http://cst.usc.edu/services/emergencyprep.html

Digital Forensics
ITP 375 (3 Units)

Course Outline
Note: Schedule subject to change

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

Reading
> Chapters 3, 4

Assignment/Lab
> **Lab 1:** Hard drive acquisition

Week 4 – Files and File Systems
- Windows file systems
- FAT32
- NTFS
- Forensic file images

Reading
> Chapter 6

Assignment/Lab
> **Lab 2:** Case Preparation

Week 5 – Forensic Software
- Overview of different software packages

- EnCase Introduction
Reading
    Instructor Handouts
Assignment/Lab
    Lab 3: EnCase Introduction

Week 6 – Bookmarking and Searching
- Creating basic search queries
- Hex, Decimal, and Binary
- ASCII
- Unicode

Reading
    Instructor Handouts
Assignment/Lab
    Lab 4: Searching evidence

Week 7 – GREP
- Understanding GREP
- Building Regular Expressions
- Creating GREP keywords
- Viewing and managing keywords and cases

Reading
    Instructor Handouts
Assignment/Lab
    Lab 5: GREP Lab
    Case 1 Assigned

Week 8 – Forensic Reports
- Creating a forensic report
- Proper report writing
- Explaining forensics to the uneducated

Reading
    Instructor Handouts

Week 9 – Midterm

Week 10 – Email Analysis
- Viewing e-mail
- Webmail
- POP
- IMAP

Reading
    Chapter 11

Assignment/Lab
> **Lab 6**: Email analysis lab

Week 11 – File Signature Analysis
- File signatures
- File extensions
- Differences between
- Identifying differences

Reading
> Instructor Handouts

Assignment/Lab
> **Lab 7:** Detecting File Manipulation

Week 12 – Hash Analysis
- Understanding hash algorithms
- Hashing files
- Hash libraries

Reading
> Instructor Notes

Assignment/Lab
> **Lab 8**: Hash Analysis Lab

Week 13 – Other Windows Artifacts
- Common windows artifacts
- Recycle bin
- My Documents
- Recent files
- Installed programs
- Windows XP vs. Windows 7

Reading
> Chapter 12

Assignment/Lab
> **Case 2 Assigned**

Week 14 – Work on Forensic Case II

Week 15 – Conclusion
- Review for the final exam
- Conclusion to the course

Final Exam to Be Held According to the Schedule of Classes