Digital Forensics
ITP 375 (3 Units)

USC Viterbi School of Engineering

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	Howard Williamson
Contacting the Instructor	howardwi@usc.edu
Office Hours	By Appointment
Lab Assistants	Ashley Sheward & Jonathan Holtmann
Lecture/Lab	9:00 – 10:15 (PST) Tuesday & Thursday

Textbook (Not Required)

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
Lectures 1 & 2

Week 2 – Computer Hardware
- Understanding computer components
- Digital Media
- Hard disk basics

Reading
Chapter 2
Lectures 3 & 4

Assignment/Lab
Lab 1: Chain of Custody

Week 3 –Forensic Tools
- Forensic hardware
- Hardware write/blockers
- Hard drive acquisitions
- Processing the scene

Reading
Chapters 3, 4
Lectures 5 & 6

Assignment/Lab
Lab 2: Acquisition & Authentication with FTK Imager

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

Reading
Chapter 6 (pgs 132-135)

Lectures 7 & 8

Assignment/Lab

Lab 3: Acquisition & Authentication with Kali Linux

Week 5 – Hash/Signature Analysis & Timestamps

- EnCase Introduction
- File Signatures
- Hash Analysis

Reading

Chapter 9

Lecture 9

Assignment/Lab

Lab 4: Files, Signature & Hash Analysis

Week 6 – Partition Analysis

- Partitions & Volumes

Reading

Chapter 6 (pgs 135—150)

Lecture 10

Assignment/Lab

Lab 5: Partition Analysis

Week 7 – Windows Artifacts and Forensic Reports

- Operating Systems
- Partitions and Volumes
- Windows Folder Structure
- Page File
- Print Spool
- Unallocated Clusters
- Slack Space
- Link Files
- Creating a forensic report
- Proper report writing
- Explaining forensics to the uneducated

Reading

Chapter 6 (pgs 150-160)

Lecture 11

ITP Report Writing Guidelines

Assignment/Lab

Lab 6: Signature Analysis

Case 1 Assigned

Week 8 – Midterm (Handed out Tuesday)

Reading

All previous materials

Week 9 – Midterm (Uploaded by Friday)

Week 10 – Windows Registry

- Introduction to the Windows Registry
- Registry Hives
- Registry Artifacts

Reading

Lecture 12

AccessData Registry Cheatsheet

Assignment/Lab

Lab 7: Windows Registry

Week 11 – Searching & GREP

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

Reading

Lecture 13

Assignment/Lab

Lab 8: GREP Lab

Week 12 – Internet, Email & USB Device Tracking

- Viewing e-mail
- Webmail
- POP
- IMAP
- USB Artifacts

Reading

Chapter 11

Lectures 14 & 15

Week 13 – Tracking User Activity

- UserAssist
- Timestamps

Reading

Chapter 12

Lectures 16 & 17

Assignment/Lab

Final Case 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