Advanced Digital Forensics

ITP 475 (4 Units)

Spring 2013

Objective

Upon completing this course, students will:

- Be able to investigate Windows workstations and servers
- Understand how the Windows operating system works for the purposes of collecting evidence
- Understand Windows file systems, FAT and NTFS
- Research upcoming topics in digital forensics
- Complete a variety of case studies in digital forensics

Concepts

This course is designed as an advanced course in computer forensics, focusing on Windows systems. It is estimated that Windows comprises over 85% of the operating systems used worldwide. This course focuses on advanced topics in Windows operating system analysis, including advanced file system analysis, web and email, as well as a comprehensive final case involving a moot court exercise.

Prerequisites

ITP 375 or Department Approval

Instructor

Joseph Greenfield

Contacting the Instructor

joseph.greenfield@usc.edu
213-740-4542

Office Hours

Listed on the ITP Website (itp.usc.edu)

Lab Assistants

Listed on Blackboard under Contacts

Lecture/Lab

Tuesday & Thursday, 5:00 – 7:00, OHE 406

Required Textbooks

Windows Forensic Analysis, DVD Toolkit, 2nd Edition. Carvey
ISBN: 0-07-1626778

Website

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

Grading

The following percentage breakdown will be used in determining the grade for the course.

Labs	20%
Cases	40%
Final Case	40%
Total	100%

Grading Scale

This section must include a breakdown of the final letter grade in terms of the above grading scale. It must indicate the total percentage or points required to earn each letter grade. Here's an example:

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 and cases will be posted on Blackboard under the "Assignments" section. Each lab will include instructions, a due date, and a link for electronic submission where applicable. Labs must be submitted using this link. Cases must be printed and submitted in class.

It is your responsibility to submit your assignments on or before the due date. For every 24 hours late, the assignment will have 5% of the total points deducted from the graded score. After seven 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

Course Outline

Note: Schedule subject to change

Week 1 – Digital Forensics Review

- Investigative Process
- Analysis Methodologies
- Tools and techniques

Reading

Instructor Notes

Week 2 – Lab Setup and Network Overview

- Setting up the investigative software
- More forensic review

Assignment/Lab

Case 1: Windows review (windows standalone) case

Week 3 – FAT32 Filesystems

- History and background on FAT
- Allocation Tables
- Directory Entries
- Bitmaps
- Deleted files and unallocated space

Reading

Chapter 5

Assignment/Lab

Lab 1: FAT analysis

Week 4 – NTFS File Systems

- History & background of NTFS
- Master File Table (MFT)
- MFT Entries
- Deleted Entries
- Unallocated space

Assignment/Lab

Lab 2: NTFS analysis

Week 5 – Filesharing and Peer-to-Peer

- Popular file sharing protocols and applications
- Filesharing logs

- Network logs
- Advanced BitTorrent Analysis

Reading

Instructor Notes

Assignment/Lab

Lab 3: BitTorrent Lab

Case 2: BitTorrent Case

Week 6 – Executable File Analysis

- Static Analysis
- Dynamic Analysis
- Virtualization

Reading

Chapter 6

Assignment/Lab

Lab 4: VMWare and Forensic Analysis

Week 7 – Viruses, Rootkits and Rootkit Detection

- The “virus defense”
- Malware
- Rootkits
- Rootkit analysis

Reading

Chapter 7

Assignment/Lab

Lab 5: Rootkit analysis

Case 3: Compromised system forensics

Week 8 – Email and Internet Analysis

- Web cache, history, bookmarks
- Mail header analysis
- Email server analysis
- Building timelines

Assignment/Lab

Case 4: Employee investigation

Week 9 – Windows Registry

- Registry locations
- Windows registry keys and values
- Useful registry keys
- Automated tools for registry analysis

Reading

Chapter 4

Assignment/Lab

Lab 6: Registry Analysis

Week 10 – Incident Response and Live Analysis

- Live analysis of systems
- Collecting volatile data
- Analyzing Log Files

Reading

Chapters 1 & 2

Assignment/Lab

Final Case Assigned

Week 11 – Memory Analysis

- Dumping physical memory
- Analyzing physical memory

Reading

Chapter 3

Assignment/Lab

Lab 7: Live analysis & memory analysis

Week 12 – Court and Deposition

- Courts and Trials
- Court documents
- Interacting with attornys

Week 13 – Law Enforcement and Forensics

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

Reading

Chapter or Website

Assignment/Lab

Description or listing of assignment

Week 14 – Preparing for the Moot Court

Week 15 – Moot Court