Advanced Digital Forensics

ITP 475 (4 Units)

USC Viterbi School of Engineering

Spring 2018

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, advanced artifact analysis, memory analysis, 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, 3rd Edition. Carvey
ISBN: 0071626778
NOTE: 4th edition covers Windows 8. I would prefer you get the 3rd edition if possible.
You will also need last semester's textbook *Hacking Exposed Computer Forensics 2nd ed.*

Recommended Textbooks

Incident Response & Computer Forensics, Third Edition. Luttgens, Pepe, Mandia.
ISBN: 0071798684
File System Forensic Analysis. Carrier.
ISBN: 0321268172

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% (sum total of all labs)
Cases	50% (every case weighted equally)
Quizzes	10% (sum total of all quizzes)
Final Case (Moot Court)	20%
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 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 submitted with both hard copies and electronic submissions.

It is your responsibility to submit your assignments on or before the due date. Assignments turned in up to 24 hours late will have 25% deducted. Assignments turned in up to 48 hours late will have 50% deducted. Assignments will not be accepted after 48 hours past the due date.

You will be given weekly quizzes every Friday. The quizzes will be variable multiple choice and fill in the blank style questions, deployed through blackboard and will be open book and open note. Any and all topics covered in ITP 375 and 475 to that point in the semester is fair game for the quizzes. The quizzes are designed to assist in your preparation of interviews and the moot court, and as such will have a reduced time limit as the semester progresses.

Starting the week after Spring Break, there will be oral quiz questions asked in class.

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

Advanced Digital Forensics

ITP 475 (4 Units)

Course Outline

Note: Schedule subject to change

	Tuesday	Thursday	Lab/Case
Week 1	**January 10** Introduction	**January 12** 375 Review	Case 1 Chapters 1 & 2
Week 2	**January 17** FAT Filesystems	**January 19** Parsing FAT Filesystems	Lab 1: Parsing FAT Instructor Notes
Week 3	**January 24** NTFS Filesystems	**January 26** Parsing NTFS Filesystems	Lab 2: Parsing NTFS Ch. 4 (MFT)
Week 4	**January 31** BitTorrent	**February 2** BitTorrent	Lab 3: BitTorrent; Case 2 Reading: Instructor Notes
Week 5	**February 7** Prefetch & Superfetch	**February 9** Shortcuts & Jumplists	Lab 3: Tracking Activity Ch. 4 (Prefetch, Jumplists)
Week 6	**February 14** Malware Detection	**February 16** Malware Analysis	Lab 4: Malware Analysis Ch. 6
Week 7	**February 21** Memory Capture	**February 23** Memory Analysis	Lab 5: Volatility; Case 3 Instructor Notes
Week 8	**February 28** Advanced Registry	**March 2** Thumbnail Cache	Lab 6: Thumbnail Cache Ch. 5
Week 9	**March 7** Advanced Recycle Bin	**March 9** E-Discovery Guest Lecture	Lab 7: Recycle Bin; Case 4 Ch. 4 (Recycle Bin)
	Spring Break		
Week 10	**March 21** Volume Shadow Copy	**March 23** ESE Databases	Lab 8: Windows Search; Case 5 Ch. 3
Week 11	**March 28** Incident Response	**March 30** Incident Response	 Ch. 7 & 8
Week 12	**April 4** Moot Court Case	**April 6** Moot Court Case	Case 6: Moot Court
Week 13	**April 11** Moot Court Case	**April 13** Moot Court Case	
Week 14	**April 18** Moot Court Case	**April 20** Moot Court Case	
Week 15	**April 25** Moot Court Case	**April 27** Moot Court Case	**Tentative Moot Court Date** **April 28, 1:30 PM**