Macintosh, OSX, & iOS Forensics

ITP 445 (3 Units)

Fall 2015

USC Viterbi School of Engineering

Objective/Concepts

Upon completing this course, students will:

- Understand the fundamentals of computer forensics for OS X and iOS systems
- Understand the relationship between IT, IS, and Forensics
- Learn industry standard best practices utilizing industry standard tools for incident response, acquisition, investigation, and presentation of findings regarding Apple hardware, software, and mobile devices
- Be able to visually identify Apple hardware/mobile devices and recommend acquisition methodologies while understanding the different types of information available from different acquisition tools and methods

Prerequisites

ITP 375 (Introduction to Digital Forensics)

Instructor	Pierson Clair
Contacting the Instructor	pclair@usc.edu
Office Hours	OHE 542 after class (and by appointment)
Lab Assistants	n/a
Lecture	Monday 6PM – 7:50PM – OHE 542
Lab	Monday 5PM – 6PM – OHE 542

Textbooks/Required Materials

Due to the fast paced changes in forensics, AppleExaminer.com, ForensicFocus.com and ForensicsWiki.org along with instructor handouts/posts will serve as digital textbooks for the first half of the semester.

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory - **ISBN-10:** 1118825098 - **ISBN-13:** 978-1118825099

A 1TB USB 3.0 bus powered hard drive is highly recommended

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.

Lab Assignments 3 @ 5% each	15%	(Wireshark, Basic OS Triage, Log File Analysis)
Case Practical 1 – IP Tracking	10%	
Case Practical 2 – Social Media	10%	
Case Practical 3 – iPhone Fun	10%	
Midterm Exam	10%	
Final Exam	10%	
Final Project/White Paper	25%	
Participation/Professionalism	10%	
Total	100%	

Grading Scale

The following is 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 will be offered nor will there be any changes made to the Final Exam schedule or assignment due dates (except for documented medical or family emergencies).
- It is your responsibility to submit your assignments on or before the due date. **It is not the responsibility of the lab assistant or the instructor.** Do **not** turn in anything to your lab assistant!
- Assignments are due on the date listed in the syllabus at the beginning of class unless otherwise changed by announcement in class or via e-mail. Any assignment turned in late will incur a 25% penalty for the first 24-hour period that it is late, an additional 50% off for the second 24-hour period that it is late, and will not be accepted after 48-hours. All assignments must be turned in either in person to the instructor or via Blackboard. Do not e-mail assignments. All case reports must be submitted in paper form with your accompanying notes and on Blackboard (report only).
- Grades will be posted on Blackboard and it is your responsibility to ensure that the grades

online are accurate and to follow your progress in the class.

- You are expected to be in class, on time, and distraction free. While I usually won't take attendance, this class is small enough that I will know if you are present or if you miss class. As this class meets once a week and as it is lecture and lab any student who misses more than two classes is in danger of failing the course. Please see me immediately if you have missed that number of class meetings.

Professionalism/Participation

While attendance is not mandatory, it is highly suggested as this is a lecture and lab based class. If you are not in class, it is not the TA nor the instructor's responsibility to teach you the material that you missed. Attendance is mandatory for guest lectures. Guest lectures are tentatively noted in the syllabus and will be announced in class.

To promote class discussion, each student will be required to submit an article for class discussion starting September 8th. Articles shall be posted with a hyperlink to the article and a 1 paragraph summary to the USC Forensics Blog at http://uscdigitalforensics.blogspot.com/ if you have not used this blog before, please submit your google user name (which is not your USC e-mail address) to the instructor. Please take care not to duplicate stories that have been submitted that week.

News stories should directly pertain to material covered in this class and may relate to: Apple, Mac OSX, iOS, iPhone, iPad, Mac malware/spyware/viruses/security, unique software or hardware which could impede or aid a forensic acquisition or examination.

- Post a link on the blog by 4PM before class.
- Please submit a story that is no more than one week old.
- If the story is behind a pay-wall or subscription-wall or requires a login, please submit a PDF copy along with the link.
- Be prepared to give a short three-minute summary of the article and any surrounding background details to start the discussion.
- You are welcome to post press releases, however they do not count as your article. Anything from http://www.prnewswire.com/ is definitely a press release.
- There will be no article requirement on November 24.

The Professionalism/Participation grade is a combination grade based upon class participation, overall quality of work, and factors that are important in the forensic investigation line of work.

Assignments: Unless otherwise announced, all assignments are due at the start of class on the day they are due. Please turn in a copy on Blackboard and bring a hard copy to class.

Extra Credit: Procure an iPhone 4 or older, complete a physical acquisition using MPE+ and then investigate the phone. Extra Credit available for completing the physical and for the report.

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

Macintosh, OSX, & iOS Forensics

ITP 445 (3 Units)

Course Outline

Note: Schedule subject to change

Week 1 (August 25) – Introduction/Review

- Review of Forensic Methodologies & Legal Requirements
- Differences between Apple's OSX and Microsoft Windows

Reading

Review intro slides

Week 2 (September 1) – No Class – Labor Day

Week 3 (September 8) – Introduction to Apple Hardware

- Apple Desktop, Laptop, Server/SAN, Network, and Connected Home Hardware
- PowerPC & Intel Processor/Hardware Architecture
- 32bit v 64bit
- Acquisition Methodologies
- Partitions/HFS+/GUID/MBR
- Wireshark Network Packet Analysis
-

Reading

TBA

Assignment/Lab

Assign: Wireshark Lab

Week 4 (September 15) – Field Trip to JMC/Apple OS Operating Systems/Artifacts

- Field Trip to JMC (meet in front of JMC at 5:55PM at the main entrance adjacent to the IM field) to tour USC Video facilities and discuss large scale network acquisition methodologies
- System 6, 7, 8, 9
- Early Versions of OS X
- 10.5/Leopard
- 10.6/Snow Leopard
- 10.7/Lion
- 10.8/Mountain Lion
- 10.9/Mavericks
- Introduction to BlackLight
- User Accounts
- Built-in Firewall
- Access & Network Controls

- Sharing

Reading

http://appleexaminer.com/MacsAndOS/OperSys/OperSys.html
http://appleexaminer.com/MacsAndOS/Analysis/Analysis.html

Assignment/Lab

Due: Wireshark Lab
Assign: Basic OS Information Lab

Week 5 (September 22) – Forensic Tools Introduction

- Macquisition Demo
- EWMounter Demo
- Introduction to BlackLight

Assignment/Lab

Assign: Case Practical 1

Week 6 (September 29) – Lab & Case Work

- Lab & Case Work Time

Reading

n/a

Assignment/Lab

Due: Basic OS Information Lab

Week 7 (October 6) – Introduction of Apple Software & Artifacts/Midterm Review

- Acquisition of Fusion & Hybid Drives
- Apple Password/User Authentication Security
- Initial Triage
- Time Stamps/PLists/Connected Devices (USB, Firewire, Network)/Print Spool/FileVault & FileVault 2 Encryption
- SQL/SQLite/kexts/inodes

Reading

http://appleexaminer.com/MacsAndOS/AppleApps/AppleApps.html

Assignment/Lab

Assign: Log File Analysis Lab

Week 8 (October 13) – Midterm

Assignment/Lab

Due: Case Practical 1
Assign: White Paper Assignment

Week 9 (October 20) – Introduction to iOS (iPhone/iPad)

- Versions of iOS
- Apple Applications
- Contacts, SMS/MMS, Calendar
- Encryption & Security
- Jailbreaking
- Recovery of Deleted Content
- iOS Backup Files

Reading

http://appleexaminer.com/iPhoneiPad/IDG_iPhone/IDG_iPhone.html
http://appleexaminer.com/iPhoneiPad/iOSAnalysisTools/iOSAnalysisTools.html

Assignment/Lab

Due: Log File Analysis Lab
Assign: Case Practical 2

Week 10 (October 27) – iOS Acquisition & Guest Lecture

- Blacklight, MPE+, Zdiarski, EnCase 7, Cellebrite, Elcomsoft
- Physical v Logical Acquisition
- Firmware Modes; Normal, Recovery, DFU
- Passcode Cracking

Reading

TBA

Assignment/Lab

Assign: Case Practical 3

Week 11 (November 3) – iOS & Apple OSX Third Party Apps

- Case Work Time

Reading

TBA

Week 12 (November 10) – Memory Analysis

- Mac Memory Analysis

Reading

The Art of Memory Forensics chapters 1-4 & 28-31 (start on this early)

Assignment/Lab

Due: Case Practical 2

Week 13 (November 17 – Case & Lab work

- White Paper Work Time

Week 14 (November 24 Thanksgiving week – Case & Lab work) –

Reading

TBA

Assignment/Lab

Due: Case Practical 3

Due: iPhone Physical Image Extra Credit

Week 15 (December 2) – 2nd Exam

- White Paper Work Time

Assignment/Lab

Extra Credit iPhone Case Report Due

Final Exam Day - White Paper Presentations

- The White Paper assignment will allow students to gain a deeper technical understanding into a specific part of either the Mountain Lion, Mavericks, or Yosemite Operating Systems or a commonly installed Mac application from a forensic perspective. Alternatively an iOS 7 or 8 OS component or application may be selected. Topic selections must be approved by the instructor. Students may work individually or in pairs. If students elect to work in pairs, the work will be expected to be double an individual's effort. The white paper will be presented in class with individuals having 8 minutes to present their research and groups having 16 minutes to present their research. If pursued individually, the paper should be 3 pages, 1.5 spaced with graphics, charts, or other media placed on appendix pages or 6 pages for groups. The white papers will have the option to be submitted to appleexaminer.com for presentation to the forensic community. This project will be graded based primarily on the quality of the research and understanding of your topic.

Date, Time, and Place

According to the final exam schedule on the Schedule of Classes