Macintosh, OSX, & iOS Forensics

ITP 445 (3 Units)

Fall 2017

USC Viterbi School of Engineering

Objective/Concepts

- This course is designed as an advanced course in computer forensics focusing on Mac OSX, macOS, iOS, and other devices in the Apple ecosystem. The course assumes that students have either satisfied the prerequisite of ITP 375 – Digital Forensics, or have received instructor approval. Students will engage in forensic acquisition and analysis of the above family of devices.
- The goal of the Digital Forensics program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. This is accomplished through utilizing industry standard tools and techniques to investigate labs and cases based upon real-world investigations.
- ITP 445 & ITP 447 are built differently than ITP 375, ITP 475, and INF 528. You'll apply knowledge you've learned in these courses along with applying knowledge from ITP 125 and other ITP classes to logically solve puzzles. You are expected to manage your time properly taking into account that assignments are staggered but may be due at the same time. These classes contain ambiguity and are built to help you bridge from an academic setting to a business environment.

Upon completing this course, students will:

- Understand the fundamentals of computer forensics for Mac OS X, macOS, and iOS systems. Discussions will also include tvOS and watchOS.
- 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) [or INF 528]

Instructor	Pierson Clair
Contacting the Instructor	pclair@usc.edu
Office Hours	See Blackboard (and by appointment) If you will be attending office hours, please e-mail me in advance.
Lab Assistants	n/a
Lecture/Lab	Monday 5PM – 7:50PM – 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 majority of the semester.

Optional textbook: 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 if you would like to work on assignments outside of class.

Website

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

Richard and Vanessa say: Sometimes the simplest answer is the most obvious answer and the accurate answer. That doesn't mean that there might not be more… but don't go on a long wild goose chase unless there is something that points to it.

To succeed in this class: Read the assignment fully, if you have questions ask them before the assignment is due. I'm happy to proof any assignment more than 72 hours before it is due.

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%	
2nd 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/Blackboard announcement. 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 12th. 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.
- Press releases do not count as your article. Anything from http://www.prnewswire.com/ is definitely a press release.
- There will be no article requirement during Thanksgiving week.

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. Other options will be made available in the second half of the semester.

Writing Skills

The goal of the Digital Forensics program at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. A significant portion of the digital forensics curriculum involves communicating what was discovered by writing professional quality digital forensic reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. It is expected that the reports will be written with correct spelling, grammar and language nuances of the American English language. A component of each report grade will be based on writing style, grammar and word choice. These reports must be accessible to technical and non-technical readers alike.

Please take care to review the Digital Forensic Report Writing Guidelines available on Blackboard. If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

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

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Section 11, *Behavior Violating University Standards* https://policy.usc.edu/scampus-part-b/. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct/.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the *Office of Equity and Diversity* http://equity.usc.edu/ or to the *Department of Public Safety* http://capsnet.usc.edu/department/department-public-safety/online-forms/contact-us. This is important for the safety whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. *The Center for Women and Men* http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage sarc@usc.edu describes reporting options and other resources.

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 22) – Introduction/Review & Introduction to Apple Hardware, Apple OS Operating Systems/Artifacts

- Review of Forensic Methodologies & Legal Requirements (on your own, slides on Blackboard)
- Differences between Apple's OSX and Microsoft Windows
- 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
- 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
- 10.10/Yosemite
- 10.11/El Capitan
- 10.12/macOS Sierra
- System Preferences: User Accounts, Built-in Firewall, Access & Network Controls, Sharing

Reading

- Review intro slides
- http://www.macrumors.com/roundup/macos-sierra/
- http://www.macworld.com/article/3083346/os-x/macos-sierra-faq-what-you-need-to-know-about-the-new-mac-operating-system.html
- http://www.macworld.com/article/3087556/os-x/8-hidden-features-of-macos-sierra.html
- https://lawfareblog.com/apple-blackhat-reopening-going-dark-debate

Assignment/Lab

Assign: Wireshark Lab (and don't forget to send Pierson your gmail address)

Week 2 (August 29) – Forensic Tools Introduction & Lab Computer Setup

- Log Files
- MacQuisition Demo
- EWMounter Demo
- Introduction to BlackLight

Reading

As assigned

Assignment/Lab

Due: Wireshark Lab
Assign: Log File Analysis Lab

Week 3 (September 5) – No Class – Labor Day

Week 4 (September 12) – In Class Lab

- Basic OS Information Lab

Reading

n/a

Assignment/Lab

Assign: Basic OS Information Lab

Week 5 (September 19) – Introduction of Apple Software & Artifacts

- Acquisition of Fusion & Hybid Drives – Core Storage
- 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

Assignment/Lab

Due: Log File Analysis Lab
Assign: Case Practical 1

Week 6 (September 26) – Mac Live Incident Response & Malware - Lab & Case Work

- Detecting Mac Malware and auto-runs
- How processes start
- Lab & Case Work Time

Reading

n/a

Assignment/Lab

Due: Basic OS Information Lab

Week 7 (October 3) – Midterm Review & Guest Lecture

- Midterm Review
- Case & Lab Work Time

Reading

As assigned

Assignment/Lab

n/a

Week 8 (October 10) – Midterm

Assignment/Lab

Due: Case Practical 1
Assign: White Paper Assignment

Week 9 (October 17) – 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

As assigned

Assignment/Lab

Assign: Case Practical 2

Week 10 (October 24) – 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 (October 31) – iOS & Apple OSX Third Party Apps

- Case Work Time

Reading

As assigned

Week 12 (November 7)– Memory Analysis

- Mac Memory Analysis

Recommended Reading

The Art of Memory Forensics chapters 1-4 & 28-31

Assignment/Lab

Due: Case Practical 2

Week 13 (November 14) – Case & Lab work

- White Paper Work Time

Week 14 (November 21 Thanksgiving week – Case & Lab work) –

Reading

TBA

Assignment/Lab

Due: Case Practical 3

Due: iPhone Physical Image Extra Credit

Week 15 (November 28) – 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 Mavericks or Yosemite Operating Systems or a commonly installed Mac application from a forensic perspective. Alternatively an iOS 9 or 10 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. 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