USC Viterbi
School of Engineering
Information Technology Program

ITP 445: Macintosh, OSX, & iOS Forensics

Units: 3
Fall 2019
Monday 6-9PM

Class Location: OHE 542

Instructor: Pierson Clair
Office: OHE 412
Office Hours: See Blackboard (and always by appointment)
Contact Info: pclair@usc.edu

Teaching Assistant: TBD
Office: n/a
Office Hours: n/a
Contact Info: Blackboard

IT Help: Viterbi Information Technology
Hours of Service: Monday-Friday 8AM – 9PM
Contact Info: Phone: 213-740-0517; Email: engrhelp@usc.edu

Program Mission: The goal of the Digital Forensics and Cyber Security 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 and intrusions. Students will study various areas of cyber investigations, including digital evidence gathering, reporting, examinations, and court presentations. Students will study cyber security tenants of risk analysis, remediation, as well as penetration testing and network security design.

Advice from Former Students:
Preethi says start sooner on everything… you'll thank her later! Always bring your take home drive to class that way you always have your evidence to work on. Get your at home environment setup early in the semester!

Course Description

- This course is designed as an advanced course in computer forensics focusing on Mac OS X, 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.

Learning Objectives

- 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

Prerequisite(s): ITP 375 (Introduction to Digital Forensics) [or INF 528]

Course Notes

Course is letter graded, with any and all materials available on Blackboard (blackboard.usc.edu). Labs will be conducted in the security lab (OHE 542) during assigned class or lab time.

Technological Proficiency and Hardware/Software Required

For any upper-division course (300-level and above), it is assumed that you have refined your technical abilities in the prerequiste classes, including basic Python scripting.

Required Readings and Supplementary Materials

Due to the fast paced changes in Mac and iOS 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 or SSD is highly recommended to work on assignments outside of class.

Description and Assessment of Assignments

The assignments will be a combination of in-class and out-of-class laboratory exercises. They will typically involve some form of procedural work (we will provide instructions), with some reflection on the work performed including researching processes and procedures performed. All laboratory exercises will be

graded on a point-scale, typically between 5 and 10 points. This class will also include a large research project to be completed during the second half of the semester.

Grading Breakdown

Lab Assignments 3 @ 5% each	15%(Wireshark,BasicOSTriage, 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

Course final grades will be determined using the following scale

A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Grading Policies

The lab assistants, graders, and instructors will do their best to return assignments graded to students within two weeks of submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading rubric is posted. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in the class. Do not rely upon an expectation of a guaranteed minimum final grade in this class regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

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.

Assignment Policies

The labs will be posted on Blackboard under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments, and you must make sure that you have fully submitted the assignment (usually a two step process).

Unless otherwise noted, all lab assignments and case reports are due at the beginning of class on the date noted in the syllabus, unless otherwise modified by Blackboard announcement and/or email from the instructor. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours particularly on the date the assignment is due.

If you join the class after the semester has started, you will have two weeks from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours 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 no credit for the assignment.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due, without expressing an emergency such as being kidnapped and taken to Mexico, it will probably not be granted.

Certain assignments will require a paper submission, and you may be asked to submit them to the main ITP office. There have been previous allegations of student rudeness to the ITP Staff. If the staff complains about you being rude, you will have 25% automatically deducted from your assignment. Don't be rude.

The instructor and lab assistants reserve the right to not answer certain questions about the lab/case assignments. This is normally due to the nature of the question being directly related to the learning objectives of the lab/case. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

All lab assignments have been tested by the instructor and/or lab assignments. Due to the nature of certain software packages and configurations in the lab, the assignments may or may not work as intended. You are encouraged to ask questions if something appears to not work correctly. However, there are certain instances where things are intended to not work correctly and the instructor and lab assistant will indicate as such. When in doubt, do a little research.

Unless otherwise announced, all assignments are due at the start of class on the day they are due. For cases, please turn in a copy on Blackboard and bring a hard copy to class with your investigative notes stapled to the report.

Exam Policies

Please review the schedule of classes for the Final Exam schedule. Should you have a scheduling conflict with the final exam, you must contact the instructor and coordinate an alternative time by the end of Week 3. Any requests made after Week 3 are not guaranteed to be accommodated.

Per USC policy, Final Exams must be scheduled during the assigned final examination schedule. It is your responsibility to arrange your travel after the scheduled date of the final exam.

All students are required to participate in the final exam and/or project. Failure to take the final exam and/or submit a final project will result in an automatic failure in the class.

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. Missing your alarm is not an emergency. A documented medical event (car accident with documentation), family emergency (death in the family), or alien abduction can be considered emergencies.

Contacting the Instructor, Lab Assistants or Graders

When emailing the lab assistants, graders or instructor, please be sure to include your full name, student ID, class name and number, and class section (day and time) in the email.

Emails sent to the lab assistants or graders will be responded to within two business days. The instructor will endeavor to respond to emails within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the grader and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

Questions about lab assignments should be submitted through the class discussion board (typically Piazza). This will have a faster response rate. Do not post code or answers on Piazza.

The instructor will post his/her regular office hours on blackboard. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you. We do have other responsibilities outside of the class.

Attendance Policy

You are expected to be in class, on time, and distraction free. 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 the instructor immediately if you have missed two or more class meetings.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in the class, and punctuality is vital to success in your professional careers. The lab assistants will be taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor. Should you miss a class with a lab assignment, contact the lab assistants to determine available times to come to the lab and finish your assignment.

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

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating what was discovered by writing professional quality 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 properly communicate your lab and assignment findings.

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 also 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.

News Assignment

To promote class discussion, each student will be required to submit an article for class discussion starting week two. Articles shall be posted with a hyperlink to the article and a one-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.

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 to the proper week on the blog at least one hour before class.
- Please submit a story that is no more than one week old.
- Please take care not to duplicate stories that have been submitted that week.
- 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 two-minute summary of the article and any surrounding background details to start the discussion.
- Press releases including anything from prweb.com are not valid news content
- Make you you validate the veracity of your news story
    - Example: Content from TheHackerNews is frequently inaccurate
- Groups will be posted to Blackboard once enrollment has settled.
- Each proper posting contributes to your participation grade
- If you are in need of news sources, please visit http://feedly.com/pclair

Additional University policies follow the course schedule.

ITP 445 - Course Schedule

Subject to Change Throughout The Semester

For some readings, you may need to copy and paste the link together, if it runs onto a second line

Week 1 (August 26) – Introduction

- Course Introduction & Pierson's Rules For Life
- Forensic Review & Metadata Analysis
- Mac Hardware Triage & Acquisition
- Wireshark
- Lab Computer Setup

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

- Forensic Review Slides
- Report Writing Guidelines & Watch Video Lecture
- Assign: Wireshark Lab
- Send Pierson your gmail address for news assignment

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

Week 2 (September 9) – Lab Computer Setup, Introduction to Apple Hardware, Operating Systems & Artifacts

- Log Files
- Time
- Apple Password/User Authentication Security
- 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
- Partitions/HFS+/GUID/MBR
- System 6, 7, 8, 9, Early Versions of OS X/Mac OS X 10.5 – macOS Sierra 10.12
- System Preferences: User Accounts, Built-in Firewall, Access & Network Controls, Sharing
- kexts/inodes

Reading

- Sarah's Log File Lectures (posted on BlackBoard)

Assignment/Lab

- Due: Wireshark Lab
- Assign: Log File Analysis Lab

Week 4 (September 16) – Forensic Tools Introduction & In Class Lab

- Forensic Methodologies
- MacQuisition Demo
- EWMounter Demo
- Introduction to BlackLight
- Initial Case Triage
- Basic OS Information Lab

Reading

- n/a

Assignment/Lab

- Assign: Basic OS Information Lab

Week 5 (September 23) – Introduction of Apple Software & Artifacts

- Acquisition of Fusion & Hybid Drives – Core Storage
- SQL/SQLite

Assignment/Lab

- Due: Log File Analysis Lab
- Assign: Case Practical 1

Week 6 (September 30) – Mac Live Incident Response & Malware - Lab & Case Work

- State of Mac Security & The Ultimate Case Investigation
- Detecting Mac Malware and auto-runs
- How processes start
- Live Response at the Terminal
- Lab & Case Work Time

Reading

- n/a

Assignment/Lab

- Due: Basic OS Information Lab

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

- Midterm Review
- Case & Lab Work Time
- Guest Lecture

Reading

- As assigned

Assignment/Lab

- n/a

Week 8 (October 14) – Midterm

- Midterm

Assignment/Lab

- Due: Case Practical 1

Week 9 (October 21) – 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
- Assign: White Paper Assignment

Week 10 (October 28) – 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 4) – iOS & Apple OSX Third Party Apps

- Case Work Time

Reading

- As assigned

Week 12 (November 11) – 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 18) – Case & Lab work

- White Paper & Case Work Time

Week 14 (November 25 Thanksgiving week – Case & Lab work) –

- White Paper Work Time

Reading

- TBA

Assignment/Lab

- Due: Case Practical 3

Week 15 (December 2) – 2nd Exam

- White Paper Work Time

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 High Sierra (macOS 10.13) or Mojave (macOS 10.14) Operating Systems or a commonly installed Mac application from a forensic perspective. Alternatively an iOS 11 or iOS 12 Operating System 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: According to the final exam schedule on the Schedule of Classes
Normal Classroom

Statement on Academic Conduct and Support Systems

Academic Conduct:

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 that can include expulsion. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" 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.

Support Systems:

Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. engemannshc.usc.edu/counseling

National Suicide Prevention Lifeline – 1 (800) 273-8255
Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. www.suicidepreventionlifeline.org

Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender-based harm. engemannshc.usc.edu/rsvp

Sexual Assault Resource Center
For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: sarc.usc.edu

Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086
Works with faculty, staff, visitors, applicants, and students around issues of protected class. equity.usc.edu

Bias Assessment Response and Support
Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. studentaffairs.usc.edu/bias-assessment-response-support

The Office of Disability Services and Programs
Provides certification for students with disabilities and helps arrange relevant accommodations. dsp.usc.edu

Student Support and Advocacy – (213) 821-4710
Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. studentaffairs.usc.edu/ssa

Diversity at USC
Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. diversity.usc.edu

USC Emergency Information
Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. emergency.usc.edu

USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.
Provides overall safety to USC community. dps.usc.edu