Mobile Device Security & Forensics

ITP 447 (3 Units)

Spring 2017

USC Viterbi School of Engineering

Objective/Concepts

- This course is designed as an advanced course in computer forensics focusing on mobile devices and other devices not classifiable as laptops, desktops, or servers. 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 mobile computing devices, specifically Android, BlackBerry and Windows Phone devices. Students will also gain an understanding of mobile device identification features and a general understanding of spectrum and frequency allocation in the United States.
- 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 are built to help you bridge from an academic setting to a business environment.

Upon completing this course, students will:

- Understand what data is able to be acquire from mobile devices and be able to acquire and investigate data from mobile devices using forensically sound and industry standard tools
- Understand the relationship between mobile and desktop devices in relationship to a criminal and corporate investigations
- Be able to analyze mobile devices, their backup files, and artifacts for forensic evidence

Prerequisites

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

Instructor	Pierson Clair
Contacting the Instructor	pclair@usc.edu
Office Hours	OHE 530C Monday 4PM-4:50PM (and by appointment) If you will be attending office hours, please e-mail me in advance.
Lab Assistants	Chris Holmes
Lecture/Lab	Monday 5PM – 7:50PM – OHE 542

Textbooks/Required Materials

Due to the fast paced changes in forensics, ForensicsWiki.org along with instructor handouts/posts will serve as digital textbooks.

I would highly recommend you consider:
Practical Mobile Forensics, Second Edition, Mahalik, Bommisetty & Tamma, ISBN-13: 978-1786464200

If you would like an additional resource, please consider:
Learning Android Forensics, Tamma & Tindall, ISBN-13: 978-1782174578

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).

Grading

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

Lab Assignments 2 @ 10% each	20% (BlackBerry & Android)
Lab Assignment 1 @ 5%	5% (Windows Phone)
Case Practical 1 – BlackBerry	10%
Case Practical 2 – Android	10%
Case Practical 3 - Combined	10%
Internet of Things Presentation	5%
End of Semester Case Presentation	5%
Midterm Exam	10%
Research Project	15%
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. The purpose of office hours is not to teach content if you missed class.
- Please take care to read and understand the Report Writing Basics PDF that appears on Blackboard before you write your reports.
- Lecture slides will be posted on Blackboard, however any content covered during a lecture or guest lecture is fair game on exams.

Case Presentation:

During the last week of class, students will each draw a number to correspond with a case that they have completed during the course of the semester. During the time allotted to the final, before and after the test, each student will individually present their case findings to the Professor and a panel allowing for the experience of presenting case results to a client and their executives who may not understand computer forensics or computers. The presentations will last 10 minutes and cover findings.

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 January 23. 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: Windows Phone, Android, BlackBerry malware/spyware/viruses/security, unique software or methodologies relating to these devices that could impede 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.
- Do not submit press releases – this includes content from prweb.com and any other press release housing site

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.

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

Mobile Device Security & Forensics

ITP 447 (3 Units)

Course Outline

Note: Schedule subject to change due to class needs

Don't forget to post news each week!

Week 1 (January 9) – Digital Forensics Review
- Investigative process
- Analysis methodologies
- Tools and techniques
- Case Triage
- Thinking about Investigations
- Report Writing – Read the Report Writing Guide for Homework

Week 2 (January 16) – No School – MLK

Week 3 (January 23) – BlackBerry Devices Introduction & Analysis
- History & Evolution of BlackBerry OS
- BlackBerry devices
- BlackBerry acquisition tools and software
- Imaging and Analyzing BlackBerry Devices
- Analyzing BlackBerry backup files
- BlackBerry Email, Messenger (BBM), Calendar and Sync
- BlackBerry Messenger analysis
- BlackBerry sync logs and analysis

Lab 1: Acquiring and Analyzing a BlackBerry device
Case 1: BlackBerry Investigation

Week 4 (January 30) – Guest Lecture – LA District Attorney

Week 5 (January 23) – Handheld Devices/Communications
- Introduction of handheld devices/History of mobile devices
- Evolution of mobile device forensics
- Carriers, Spectrum, Communication Topology
- SIM Cards
- SQLite Databases
- Forensic Tools Introduction
- Metadata including EXIF and GPS

Week 6 (February 13) – Mobile Device Acquisition
- Software Acquisition
- Hardware Acquisition
    - Chip-Off
    - JTAG
    - ISP
- Backup Files
- Server/Cloud Acquisitions

BlackBerry Lab Due

Week 7 (February 20) – No School – President's Day

BlackBerry Case Due (February 21st Tuesday – 7PM – OHE 406)

Week 8 (February 27) –
- Non-traditional and older device acquisition & analysis
- Lab work time
- Midterm Review

Internet of Things Presentations

Week 9 (March 6) - MIDTERM

Spring Break (March 14) – No School

Week 10 (March 20) – Android Device and OS
- History and evolution of Android
- Android Open Source Project (AOSP)
- Android Market
- Overview of Android Devices (Phones, Tablets, Netbooks, etc.)
- Android ROM and Bootloaders
- Android update mechanism

Lab 2: Android Lab

Week 11 (March 27) – Android Device Acquisition & Analysis
- Procedures for acquiring an Android device
- Imaging an android

- Logical vs. physical acquisition
- Analysis Techniques
- Android File System Forensics

Case 2: Android Case

Week 12 (April 3) – Android Data and App Security
- Data theft from Android devices
- Encrypted android devices
- Corporate mobile security policies and procedures
- Android software development security strategies

Case 3: Combined BlackBerry/Android Case

Week 13 (April 10) – Windows Phones
- Introduction and History of Windows Phone OS
- Legacy and Current OS
- Windows Phone 7
- Analysis techniques
- File system forensics
- Common application forensic analysis

Android Case and Lab due at beginning of class

Week 14 (April 17) – Windows Phones
- Acquisition of Windows Phones
- Windows Phone Analysis

Lab 3 (in class lab): Windows Phone

Week 15 (April 24) – Wrapping up
- Extra Work Time

Lab 3 Due
Case 3 Due

Final exam (Case Presentation & Research Project Presentation) to be held according to the schedule of classes. It is likely May 8 from 4:30 – 6:30PM in OHE 542.