Mobile Device Security & Forensics  
ITP 447 (3 Units)  
Spring 2015

Objective/Concepts
• This course is designed as an advanced course in computer forensics focusing on mobile devices and other devices not classifiable as desktop or servers. The course assumes that students have either satisfied the prerequisite of ITP 375 – Digital Forensics, or instructor approval. Students will engage in forensic acquisition and analysis of mobile computing devices, specifically Android, BlackBerry and Windows Phone devices.

Upon completing this course, students will:
• Be able to acquire the 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)

Instructor  
Piersen 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 and ForensicsWiki.org along with instructor handouts/posts will serve as digital textbooks.

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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab Assignments 2 @ 10% each</td>
<td>20% (BlackBerry &amp; Android)</td>
</tr>
<tr>
<td>Lab Assignment 1 @ 5%</td>
<td>5% (Windows Phone)</td>
</tr>
<tr>
<td>Case Practical 1 – BlackBerry</td>
<td>15%</td>
</tr>
<tr>
<td>Case Practical 2 – Android</td>
<td>15%</td>
</tr>
<tr>
<td>Case Presentation</td>
<td>5%</td>
</tr>
<tr>
<td>Midterm Exam</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>15%</td>
</tr>
<tr>
<td>Participation/Professionalism</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Grading Scale**

The following is the grading scale to be used to determine the letter grade.

<table>
<thead>
<tr>
<th>Percentage Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>93% and above</td>
<td>A</td>
</tr>
<tr>
<td>90% - 92%</td>
<td>A-</td>
</tr>
<tr>
<td>87% - 89%</td>
<td>B+</td>
</tr>
<tr>
<td>83% - 86%</td>
<td>B</td>
</tr>
<tr>
<td>80% - 82%</td>
<td>B-</td>
</tr>
<tr>
<td>77% - 79%</td>
<td>C+</td>
</tr>
<tr>
<td>73% - 76%</td>
<td>C</td>
</tr>
<tr>
<td>70% - 72%</td>
<td>C-</td>
</tr>
<tr>
<td>67% - 69%</td>
<td>D+</td>
</tr>
<tr>
<td>64% - 66%</td>
<td>D</td>
</tr>
<tr>
<td>63% and below</td>
<td>F</td>
</tr>
</tbody>
</table>
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.
- Please take care to read and understand the Report Writing Basics PDF that appears on BlackBoard before you write your reports.

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 26. 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/](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.

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.

**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/](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/](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](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](mailto: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](http://cst.usc.edu/services/emergencyprep.html)
Mobile Device Security & Forensics

ITP 447 (3 Units)

Course Outline
Note: Schedule subject to change

**Week 1 (January 12)** – Digital Forensics Review
- Investigative process
- Analysis methodologies
- Tools and techniques

**Week 2 (January 19)** – No School – MLK

**Week 3 (January 26)** – Handheld Devices/Communications
- Introduction of handheld devices
- History of mobile devices
- Evolution of mobile device forensics
- Carriers, Spectrum, Communication Topology

**Week 4 (February 2)** – 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

**Lab 1: Acquiring and Analyzing a BlackBerry device**

**Week 5 (February 9)** – BlackBerry Email, Messenger (BBM), Calendar and Sync
- Email analysis of BlackBerry devices
- BlackBerry Messenger analysis
- BlackBerry sync logs and analysis

**Case 1: BlackBerry Investigation**
**Week 6 (February 16)** – No School – President's Day

**Week 7 (February 23)** – BlackBerry Enterprise Server
- BlackBerry devices and enterprise server introduction
- BlackBerry enterprise server sync and logs
- Acquisition and analysis of enterprise server

**Week 8 (March 2)** – Guest Lecture
BlackBerry Lab and Case Due

**Week 9 (March 9)** - MIDTERM

Week 10 (March 16) – Spring Break – No School

**Week 11 (March 23)** – 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 12 (March 30)** – 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 device**

**Week 13 (April 6)** – Android Data and App Security
- Data theft from Android devices
- Encrypted android devices
- Corporate mobile security policies and procedures
- Android software development security strategies
**Week 14 (April 13)** – 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 15 (April 20)** – Windows Phones
- Acquisition of Windows Phones
- Windows Phone Analysis

**Lab 3: Windows Phone**

**Week 16 (April 27)** – Wrapping up
- Extra Work Time
- Final Review

**Lab 3 Due**

Final exam to be held according to the schedule of classes