Mobile Forensics (CS 480 & CS 580) Fall 2019

August 22, 2019

Course Description

This course examines digital forensics of mobile devices such as smart phones and tablets from the perspective of law enforcement. Mobile device characteristics that make forensics examinations difficult are discussed. Various forensics tools are critically examined with an eye toward improved tool development. The course will introduce a few forensics tools geared towards mobile devices but will not focus on teaching the students on how to use the tools. The focus will be on creating an understanding of the underlying system in order to be able to actually **build** and **extend** such forensic tools. Hence the course will cover basics of currently used Mobile Operating Systems (Android and iOS) with a focus on "targeted data extraction." The course will also introduce malware forensics for mobile devices.

Goal: At the end of the course the students should have a solid understanding of different mobile operating systems and the challenges they create for forensic analysts. They should be able to explain the inner workings of different forensic tools and would also be able to extend their functionalities with the current state of the art.

Instructor & TA Info

Dr. Tathagata Mukherjee
Class Room: OKT N327
Class Hours: TR 16:20 - 17:40 Hrs. OKT N327
Email: tathagata.mukherjee@uah.edu
Office: OKT N347
Office Hours: TR 15:00 Hrs - 16:00 Hrs or By Appointment
Course Resource: Canvas
TA: Mr. Krishna Chaitanya Choudary Anumolu
Email: ka0049@uah.edu
TA Office Hours: TBA

Pre-Requisites

The required courses for taking this course are CS 413 or CS 513 or CPE 323. Broadly the pre-requisites for this course ensure that the student has taken Computer Architecture in some form and has an understanding of file systems. Additionally a good understanding of operating systems and computer networking models is a plus but is not required. The student will benefit if she is able to read and understand programs in at least one high level language.

Please email the instructor if you are not sure whether you have the required background to take the course. Note instructor will NOT be able to waive pre-requisites.

Books

1. Suggested Text Book: File System Forensic Analysis. (We will not follow the textbook by chapter as it is not a book on mobile forensics).
2. Suggested Reference: Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations (A good reference).
3. Lecture Notes will be the main source of the material.

Assignments and Projects

Four group projects (three small projects and one term project) will be assigned along the lectures and they need to be done in groups of at most **4 people, not less than 2** and turned. Projects will ask you to explore aspects of the materials taught in class and write small programs to test them. Each project will require a final report to be turned in from the group. All members a group will be expected to address **at least** one aspect of the project and the report **should clearly indicate** who was responsible for which part. **Grades will be individual based on the performance of the student as gleaned from the report**. So each section of the report must indicate name of student responsible for the same. There will be one midterm exam, one final exam and one term project. The term project will be a culmination of the class projects. The weight distribution will be as follows:

1. Class Attendance & Participation 5 %
2. Projects (4) 40 %
3. Midterm 30 %
4. Final 25 %

The grade assignment will be as follows:

1. Over 90 %: A
2. Between 85 % and 90 %: A-
3. Between 80 % and 85 %: B+
4. Between 70 % and 79 %: B
5. Between 65 % and 69 %: B-
6. Between 60 % and 64 %: C+
7. Between 55 % and 59 %: C
8. Between 50 % and 55 %: C-
9. Less than 50: F

Tentative Schedule

1. First set of lectures **before midterm** will cover the basic introduction to mobile forensics and mobile operating systems with stress on their privacy and data protection aspects. We will also cover basics of networking on mobile platforms. These lectures will go over the idea of TCP/IP and the different networking layers. We hope to introduce trageted data extraction before the midterm. The midterm will cover these topics. **After the midterm** we will dive into targeted data extraction (both manual and automated) We will introduce one common mobile forensic tool and then build our own targeted data extraction tools and finally we will cover malware forensics.
2. Project 1 Posting: Mid September
3. Project 2 Posting: Mid October
4. Midterm (End of October in class)
5. Project 3 & 4 (Term Project) Posting: November Start
6. **Finals Tuesday December 10, 2019 15:00 Hrs - 17:30 Hrs OKT N327**

Expectation from Students

Attendance is expected for this class. Unless you obtain prior consent of the instructor, missing classes will be used as basis for attendance grading. In case that it is necessary to skip a class, students are responsible to make up missed materials. Participation in in-class discussions and activities is also expected.

All submitted assignments and projects must be done by the author(s). **It is a violation of the Academic Honor Code to submit other's work and the instructor of this course takes these violations very seriously and will most likely FAIL the student for the entire class in case of honor code violations. So please be careful.**

Changes to Syllabus

There might be small changes to the syllabus as we proceed. The instructor will determine, based on the student's progress, how much to cover in the time frame of the semester. Stress will be on ensuring that the students understand the concepts taught in class and are able to apply them for solving real life problems, not on speed. The changes to the syllabus will be posted on canvas and will also be discussed in class.

Disclaimer

This course will cover certain techniques to break down known systems in order to demonstrate their vulnerabilities. However it is illegal to practice these techniques on others' systems without explicit written consent as is done by white hat hackers. With great power comes great responsibility and so the students will be liable for their behavior and the resulting consequences if the tools learned in class are used unethically or unlawfully.

CS Department Policies and Procedures

This document should be handed out with the syllabus and discussed on the first day of classes

Responsibilities of Teacher

1. Provide a detailed syllabus. This syllabus should list office hours, course objectives, textbooks, references, prerequisites, and grading policy/method of assessment.

2. Come to class well prepared, on time, and make full use of the class time.

3. Provide timely and adequate feedback on grades. Return graded material promptly.

4. Conduct final exam at the time designated in the class schedule. Never post grades.

5. Not assign **new** work (i.e. not listed on syllabus) that is due in last two weeks of classes.

6. Avoid leaving the examination room without a proctor. Provide paper for exams. Make reasonable use of the assigned textbook.
7. Check students have proper prerequisites. Instructor does not waive assigned prerequisites.
8. Report all incidences of academic misconduct to the Department and VP for Student Affairs

Responsibilities of Student

1. Come to class with the proper prerequisites, well prepared, on time, and make full use of the class time.
2. Provide adequate notice of anticipated absences and take full responsibility for finding out about missed work, announcements, and assignments.
3. Submit assessment material on time and submit only your own work. (see integrity)
4. Do not allow other students to copy your work.
5. Read and understand the syllabus and follow announced policies.

Integrity

We expect CS instructors and students to conduct themselves in a professional manner. Students are subject to all the provisions in the UAH Code of Student Conduct, which is available free from the Office of Admissions and Records. Information on plagiarism and other forms of misconduct is presented in the Student Handbook Article III. Departments are obliged to report all student misconduct to the Office of Student Affairs.

Complaint Procedure

If you have difficulties or complaints related to this course, your first action should be to discuss them with your instructor. If such a discussion would be uncomfortable for you or fails to resolve your difficulties, you should ask for a meeting with the Chair of the Computer Science Department in Technology Hall N-300, info@cs.uah.edu, telephone 824-6088. If you are still unsatisfied, you should discuss the matter with Dr. Debra Moriarity, Associate Dean of the College of Science, moriard@email.uah.edu. Dr. Moriarity's office is CS 207 Materials Science Building.

Students with Disabilities

Your instructor would like to hear from anyone who has a disability that may require a modification of seating, testing, or other class procedures. Please see instructor after class or during office hours to discuss appropriate modifications. You should also contact Student Development Services in UC 113 (Ph. 824 6203) for further assistance.

Student Computer Account

Students enrolled in any CS course are entitled to an account on the departmental computer network. Use of such an account is subject to departmental and university policies. To apply for an account, and see the current policies, go to the departmental web site at http://www.cs.uah.edu/account/

Examination Policy

In response to past student complaints about problems during examinations, the Computer Science Department has developed the following guidelines for in-class examinations in all courses.

1. Come to the exam prepared to complete it without a break. If you think you will need a break, please inform the proctor before the exam if possible.

2. Do not communicate with other students. Talk only to the instructor.

3. Whenever you leave the exam room turn in your exam.

4. Use only the paper provided by the instructor for all writing.

5. If assigned a specific seat, remain in that seat.

6. Unless specifically permitted by the instructor, use no books or other reference materials. Do not bring calculators, computers, pocket-organizers, cell phones, pagers, or other electronic devices to the exam.