Mobile Forensics (CS 480 & CS 580) Fall 2020

August 23, 2020

Instructor Info

Dr. Tathagata Mukherjee
Class Room: OKT N327 and Zoom
Class Hours: TR 16:20 - 17:40 Hrs. OKT N327 and Zoom
Email: tathagata.mukherjee@uah.edu
Office: OKT N347
Office Hours: Mondays: 3:00-4:00pm Wednesdays: 1:30pm-2:30pm using Zoom (links will be posted)
Course Resource: Canvas

Course Description

From Catalog: This course examines digital forensics of mobile devices such as smart phones and tablets in a law enforcement context. Mobile device characteristics that make forensics examinations difficult are discussed. Various forensic tools are critically examined with an eye toward improved tool development.

This course examines digital forensics of mobile devices such as USB drives, external portable drives, IoT, smart phones and tablets from the perspective of law enforcement and incidence response. Mobile device characteristics that make forensics examinations difficult and unique will be discussed and differences with standard digital forensics will also be 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 file systems forensics, network forensics and "targeted data extraction." The course will also introduce malware forensics for mobile devices and in-memory forensics.

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.

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, First Edition by Brian Carrier. (We will not follow the textbook by chapter as it is not a book on mobile forensics).
2. Suggested Reference: Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, Second Edition, Reiber, Lee. I would encourage you to get the second book as the main reference. I will provide slides for file system forensics as well as additional reading materials.
3. Lecture Notes will be the main source of the material.

Assignments and Projects

We will have one group term project, two homeworks, two individual projects, one midterm and one final. The exams will be open book and open notes and open Internet.

1. Homework 20 %
2. Projects 20 %
3. Term Project 20%
4. Midterm and Final 40 %

Grading Policies

I will use a traditional grading scale: A (90 and above), B (80 and above), C (70 and above), D (60 and above) and F (less than 60).

I strive to return all graded work within one and a half week of the due date.

Late work is accepted up to 5 days late, with a 20 % penalty per 24 hours. If you will miss a test or a test deadline, you must notify me in advance with a valid excuse, in order to be allowed to make up the test.

Expectation from Students

This class is a synchronous ONLINE class (with option for asynchronous learning) and the instructor will hold regular lecture hours as per UAH schedule via Zoom (links posted). All the lectures can either be attended online through Zoom. The lectures will also be recorded and the recordings posted on Canvas. Attendance is optional for this class in Fall 2020. In case you decide to skip a lecture, you are responsible for making up the missed materials. Participation in in-class discussions and activities is expected but not required. 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.

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.