CS694 Mobile Forensics

Department of Computer Science
Metropolitan College
Boston University

Syllabus (General Information)

Instructor Information

Name: Yuting Zhang
Office: Fuller 263 (808 Commonwealth Ave., Rm 263)
Phone: 617-358-5683
Email: danazh at bu dot edu
URL: http://people.bu.edu/danazh

Course Information

Required Text Books

Epifani, M. & and Stirparo, P (2015). Learning iOS Forensics. PACKT Publishing. (ISBN-13: 978-1783553518)

Tamma, R. & Tindall. D. (2015). Learning Android Forensics. PACKT Publishing. (ISBN-13: 978-1782174578)

Reference Books

Reiber, L.(2016). Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation. Feb 2016.

Bommisetty, S., Tamma, R., Mahalik, H. (2014). Practical Mobile Forensics. July 21, 2014 (2nd Edition is also available now)

Hoog, A. (2011). Android Forensics: Investigation, Analysis and Mobile Security for Google Android. 1st Edition. Syngress.

Hoog, A. & Strzempka, K. (2011). iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices. Syngress.

Other Readings

Barmpatsalou, K., Damopoulos, D., Kambourakis, G. & Katos V, (2013). A Critical Review of 7 Years of Mobile Device Forensics. Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response. Volume 10 Issue 4. Retrived from: http://dx.doi.org/10.1016/j.diin.2013.10.003

Ayers, R., Brothers, S. & Jansen W. (2014). Guidelines on Mobile Device Forensics. National Institute of Standards and Technology (NIST) Special Publication 800-101 Revision 1. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Apple Inc., iOS Security. Retrieved from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Course Materials

Please check blackboard for all course materials. (https://learn.bu.edu/)

Description (for catalog)

Overview of mobile forensics investigation techniques and tools. Topics include mobile forensics procedures and principles, related legal issues, mobile platform internals, bypassing passcode, rooting or jailbreaking process, logical and physical acquisition, data recovery and analysis, and reporting. Provide in-depth coverage of both iOS and Android platforms. Laboratory and hands-on exercises using current tools are provided and required. 4 credits.

Objectives

By the end of the course, the students shall be able to:

1. Describe basic principles of digital forensics and identify the unique challenges involved in mobile forensics.
2. Describe mobile ecosystem security mechanisms and risks
3. Explain and apply the procedures of the validation, preservation, acquisition, examination, analysis and reporting of digital information from a mobile device.
4. Explain and compare the internals of iPhone and android platforms such as hardware, OS architectures and file systems.
5. Explain and compare the jailbreaking process for iPhone and rooting process for android phones
6. Explain and compare various data acquisition and analysis techniques used in mobile forensics.
7. Conduct the logical acquisition and physical acquisition to extract data from mobile device such as iPhone and android phones.
8. Analyze the extracted data to identify and examine important case data such as contacts, call logs, SMS, images, audio and video files, web history, passwords, and application data.
9. Apply industry best practices to evidence collection and analysis with hands-on exercises using current tools.

Students are responsible for ALL the materials covered including any topics not in the textbooks. Reading before and after class is required and essential to succeed in this course.

Course Requirements

- Class participation

- Reading and study
- Assignments (Labs, written homework)
- Quizzes and Exams.

Course Content

Topics *(to be updated)*

Module #	Topics	Readings	Assignments
1	Digital Forensics Review Introduction to Mobile Forensics	Module 1 Notes Barmpatsalou et al. Ayers et al., Chapters 3-4 Epifani & Stirparo, Chapter 1 Tamma & Tindall, Chapter 1, Page 1-11	HW1 Lab1 Discussion 1 Quiz 1
2	Introduction to Mobile Ecosystem Systems Internals of iOS Devices iOS Security	Module 2 Notes Ayers et al., Chapter 2 Epifani & Stirparo, Chapters 2 & 3 (Page 49-52)	HW2 Lab2 Discussion 2 Quiz 2
3	Acquisition from iOS Devices iOS Data Analysis	Ayers et al., Chapters 5-7 Epifani & Stirparo, Chapter 3-6	HW3 Lab3 Discussion 3 Quiz 3
4	Internals of Android Devices Android Security	Tamma & Tindall, Chapters 1-2	HW4 Lab4 Discussion 4 Quiz 4
5	Data Acquisition from Android Devices Android Data Analysis	Tamma & Tindall, Chapters 2, 4-8	HW5 Lab5 Discussion5 Quiz 5

6	Windows Phone Security and Forensics BlackBerry Security and Forensics	Bommisetty, Tamma & Mahalik, Chapters 12-13	HW6 Discussion 6 Quiz 6
7	Review/ Final Exam		

Course Polices

Grading Policy

The grade that a student receives in this class will be based on class participation, assignments, quizzes and final exam. The grade is breakdown as shown below. All percentages are approximate and the instructor reserves the right to make necessary changes.

- 6% on class participation
- 15% on quizzes
- 24% on written homework
- 25% on hands-on lab exercises
- 30% on final exam

Letter grade/numerical grade conversion is shown below:

A (95-100) A- (90-94)
B+ (85-89) B (80-84) B- (79-77)
C+ (74-76) C (70-73) C- (65-70)
D (60-65) F (0 – 59)

Attendance Policy

Attendance is expected at all class meetings. You are responsible for all materials discussed in class. In general, no makeup quizzes and exams will be given unless an extremely good, verifiable reason is given in advance. Please respect your classmates by silencing your cell phones and other electronic devices before class begins.

Assignment Late Policy

The late assignments will be penalized within a week with **3% of your grade each day**. No assignments will be accepted one week after the deadline. It is the students' responsibility to keep secure backups of all assignments.

Assignment Format

All assignments should be named as CSXXX_<student's bu user name>_HW<number>.doc. Please include file name and page number in the header of the document. The incorrect file name and format will be penalized with 3**% of your grade**.

Academic Integrity

Academic conducts in general and MET College rule in particular require that **all references and uses of the work of others must be clearly cited**. All instances of plagiarism must be reported to the College for action. *For the full text of the academic conduct code, please check* http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/.

Here is the brief description about plagiarism in the document: “Plagiarism. Representing the work of another as one’s own. Plagiarism includes but is not limited to the following: copying

the answers of another student on an examination, copying or restating the work or ideas of another person or persons in any oral or written work (printed or electronic) without citing the appropriate source, and collaborating with someone else in an academic endeavor without acknowledging his or her contribution. Plagiarism can consist of acts of commission appropriating the words or ideas of another-or omission failing to acknowledge/document/credit the source or creator of words or ideas (see below for a detailed definition of plagiarism). It also includes colluding with someone else in an academic endeavor without acknowledging his or her contribution, using audio or video footage that comes from another source (including work done by another student) without permission and acknowledgement of that source."