CS694 Mobile Forensics and Security

Department of Computer Science
Metropolitan College
Boston University

Spring 2024 Syllabus

Instructor Information

Name: Yuting Zhang
Office: 1010 Commonwealth Ave., Rm 322
Phone: 617-358-5683
Email: danazh at bu dot edu
URL: http://people.bu.edu/danazh

Course Information

Lecture time and location

Thursday 6:00-8:45, CAS 214

Recommended Reference Books

Bommisetty, S., Tamma, R., Mahalik, H. (2020). Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices, PACKT Publishing, 4th Edition.

Tiepolo, G. (2022). iOS Forensics for Investigators. PACKT Publishing. 1st Edition

Other References and Readings

Tamma, R. & Tindall. D. (2018). Learning Android Forensics. PACKT Publishing, 2nd Edition.

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

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, 265-275. https://www.sciencedirect.com/science/article/abs/pii/S0167739X18315644

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys (CSUR)*, *51*(3), 1-31. Retrieved from: https://dl.acm.org/doi/pdf/10.1145/3177847

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. Retrieved 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

Mobile Device Forensic Tool Specification, Test 4 Assertions and Test Cases. National Institute of Standards and Technology (NIST). Version 3.1. Retrieved from: https://www.nist.gov/system/files/documents/2021/02/24/Mobile%20Device%20Forensic%20Tool%20Test%20Specification%20V%203.1.pdf

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

Android Security, Retrieved from https://source.android.com/security

Course Materials

Please check the blackboard for all course materials. (https://onlinecampus.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 security mechanisms used in iPhone and Android platforms

6. Explain and compare the jailbreaking process for iPhone and rooting process for android phones
7. Explain and compare various data acquisition and analysis techniques used in mobile forensics.
8. Conduct the logical acquisition and physical acquisition to extract data from mobile devices such as iPhone and Android phones.
9. 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.
10. 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
    - 5 Labs
    - 3 General Discussion + 3 Project-related Discussion
    - Semester-long Project
- Quizzes and Exams

Course Schedule

Module # Class Date	Topics	Assignments
1 01/18, 01/25, 02/01	Introduction to Mobile Forensics and Security Introduction to Mobile Ecosystem Systems	Lab1 (01/25 - 02/08) Project Proposal (01/18 - 02/08) Discussion 1 (01/18 - 02/01)

2 02/08 02/15	Introduction to iOS devices iOS forensics and analysis	Online Quiz 1 for Module 1 (02/08 - 02/15) Lab2 (02/08 - 02/22) Discussion 2 (02/08-02/15)
3 02/22 02/29	Internals of iOS Devices iOS Security	Lab3 (02/22 - 03/07) Discussion 3 (02/29 - 03/07)
4 03/07 03/21	Intro to Android Devices Android Acquisition and Analysis	Online Quiz 2 for Module 2 & 3 (03/07-03/14) Lab 4 (03/14 - 03/28) Project Midterm Report Due (03/21) Discussion 4 (03/21-03/28)
03/14	Spring break	
5 03/28, 04/04	Internals of Android Devices Android Security	Lab5 (03/28-04/11) Discussion 5 (04/04-04/18)
6 04/11, 04/18	Windows Phone & BlackBerry Android Application and Malware Analysis Cloud and IoT Forensics Review	Online Quiz 3 for Module 4 & 5 (04/11 - 04/18)
04/25	Final Project Presentation	Final project & Discussion 6 Due (05/02)
05/09	Final Exam	

Course Policies

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 broken down as shown below. All percentages are approximate and the instructor reserves the right to make necessary changes.

- 5% on class participation
- 9% on 3 quizzes
- 9% on 3 general discussion and 3% on 3 project related discussion
- 25% on 5 hands-on lab exercises
- 21% Project (3% on Proposal, 6% on Progress Report, 12% on Final presentation and Report)
- 28% 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.

Assignment Late Policy

The late assignments will be penalized within a week with **3 points per 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 CS694_<student's BU use 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 **points**.

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* https://www.bu.edu/academics/policies/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."