

George Mason University

CFRS- 762 Mobile Device Forensics

CRN 20768 SEC DL1

3.0 Credit Hours

Spring 2019 - January 22, 2019 – May 15, 2019

Mondays 7:20pm - 10:15pm (except where noted) - Synchronous Online Blackboard Ultra

Saturday lab February 23rd 9am-noon and 1pm-4pm In-Person - Room TBD

Instructor:

Jessica Hyde

jhyde@gmu.edu

Office hours: Available upon request

Prerequisites:

CFRS 500, CFRS 661

Required Textbook:

Bair, J. (2018). *Seeking the truth from mobile evidence: Basic fundamentals, intermediate and advanced overview of current mobile forensic investigations*. London: Academic Press.

Recommended Textbook:

Mahalik, H., Tamma, R., & Bommisetty, S. (2016). *Practical Mobile Forensics: A hands-on guide to mastering mobile forensics for the iOS, Android, and Windows Phone platforms*. Birmingham: Packt Publishing.

Optional Textbook:

Reiber, L. (2016). *Mobile forensic investigations: A guide to evidence collection, analysis, and presentation*. New York, NY: McGraw Hill Education. ISBN: 978-0-07-184363-8

Required Materials:

You must have a personal laptop computer for the hands-on lab capable of using the forensic tools that will be made available on Blackboard prior to the Saturday in-person class meeting. Additionally, you must have a headset or mic capable of both listening to and responding to the synchronous remote lectures on Monday evenings using Blackboard Collaborate. Download links for required software will be provided by the instructor and disseminated via Blackboard.

Course Description:

This course will familiarize students with mobile forensics. We will focus on data types, storage, acquisition, and analysis of data from mobile devices. Students will utilize industry best practices for acquisition, analysis, and presentation of data from mobile devices. This class will be a mixture of lecture and hands-on acquisition and analysis.

Course Schedule: *Subject to Change*

Week	Date	Topic	Reading	Homework
1	Jan 21	No Class - MLK, University closed	N/A	N/A
2	Jan 28	Lesson 1: Mobile Phone Networks, Data Sources, and Data Presentation	Req: Bair Ch 5, Ch 7 Opt: Reiber Ch 1, 14	Homework 1 Distributed
3	Feb 4	Lesson 2: Mobile Forensics vs Computer Forensics and Mobile Forensic Image Types	Req: Bair Ch 1 Rec: Mahalik Ch 1 Opt: Reiber Ch 2, 6 (p 119 -133)	Homework 2 distributed Project discussed
4	Feb 11	Lesson 3: Mobile Data preservation	Req: Bair Ch 2, 3, 4 Opt: Reiber Ch 3, Ch 4, 7, 8	Homework 1 due
5	Feb 18	No Class (lecture/lab in person Feb 23)		
6	Feb 23 In-person Location TBD	Lesson 4: Acquisition with Manual Methods - Lab 1 and Lesson 5: Acquisitions via Commercial Means-Lab 2	Req: Bair Ch 8 -11, 13 Opt: Reiber Ch 5, Ch 6 (p 142 - 152)	Lab 1 and 2
7	Feb 25	No Class (lecture/lab in person Sep 22nd)		
8	Mar 4	Lesson 6: Advanced Acquisitions – Flasher Boxes, JTAG, Chip-Off (R)	Req: Bair Ch 19, 20-24, 26-28, 30 Opt: Reiber Ch 6 (p 133 - 142)	Homework 3 distributed
9	Mar 11	Spring Break (No Class)		
10	Mar 18	Midterm		
11	Mar 25	Lesson 7: Mobile Analysis – SIM	Req: Bair Ch 6 Opt: Reiber Ch 9	Homework 2 due
12	Apr 1	Lesson 8: Mobile Analysis – Android	Rec: Mahalik Ch 10 Opt: Reiber Ch 13	
13	Apr 8	Lesson 9: Mobile Analysis – iOS (R)	Rec: Mahalik Ch 6 Opt: Reiber Ch 11	
14	Apr 15	Lesson 10: Mobile Analysis - Blackberry and Windows	Rec: Mahalik Ch 12 Opt: Reiber Ch 10	Homework 3 due
15	Apr 22	Lesson 11: Mobile Analysis – Feature Phones, Raw Binaries, and Time Stamps	Req: Bair Ch 15	
16	Apr 29	Lesson 12: Mobile Analysis - 3rd Party Applications	Req: Bair Ch 17 Rec: Mahalik Ch 11, 13 Opt: Reiber Ch 12	
17	May 6	Lesson 13: SQLite, Internet of Things, and Challenges to Mobile Forensics	Req: Bair Ch14	Project Due
18	May 13	Final (7:30pm - 10:15pm)		

Grading:

<u>Weights</u>		<u>Letter Grades</u>
Homework	15 % (three assignments at 5 points each)	A+ 98-100
Labs	10 % (two labs at 5 points each)	A 92-98
Project	25 %	A- 90-91
Midterm	25 %	B+ 87-89
Final	25 %	B 83-86
		B- 80-82
		C 70-79
		F 0-69

The Midterm and Final exams are cumulative and will be timed online exams.

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions, and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter. Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice. Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using e-mail or telephone. E-mail is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. E-mail messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account. **Students must utilize their GMU email account to contact the instructor.**

Honor Code

Students are required to be familiar and comply with the requirements of the GMU Honor Code. The Honor Code will be strictly enforced in this course.

Accommodations for Disabilities

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with Office for Disability Services (SUB I, Rm. 4205; 993-2474; <http://ods.gmu.edu>) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.