George Mason University
CFRS 762 – Mobile Device Forensics
CRN 73287, Sec 001
Fall 2015, August 31 – December 12

Instructor

Michael Robinson
mrobinsv@gmu.edu
Office Hours: Available upon request

Description

This course will familiarize students with mobile devices and technology used by carriers. Students will identify data that can be retrieved from mobile devices, such as cell phones, smart phones, and GPS devices. Recovered and analyzed data will include address books, call logs, text messages, video files, audio files, and Internet history. Students will correlate data with records from Network Service Providers, e.g., call phone service carriers. Students will apply industry best practices to evidence collection and analysis with hands-on exercises using current tools.

This course will be taught in a hybrid format with online and in-person components. This will include:

- Course material (e.g., presentations, quizzes, assignments, and exams) will be made available via Blackboard.
- During the first week of class, a time will be set up for weekly conference calls between the students and the professor. This will allow students to dialogue with each other and the professor to ensure the delivery of the course content is clear.
- The mandatory hands-on lab, where students will acquire data from various phones using state of the art commercial tools, will be conducted in-person on Saturday, November 14 from 8:00AM to 5:00PM. The location of the classroom will be announced on Blackboard.

Learning Objectives

Upon completing the course, students will be able to:

- Produce a forensic report that includes the steps in the collection, handling, and preservation of digital evidence from mobile devices, such as cell phones.
- Construct a forensic acquisition plan for mobile devices that will account for various scenarios and the limitations of cell phone technology.
- Validate data obtained from the forensic acquisition of mobile devices with current tools.
- Analyze data retrieved from mobile devices with current tools.
- Assess the differences between cellular network architectures and identify their impact on forensic data.
- Analyze data provided from network service providers and cross-reference the results with data obtained from mobile devices.

Required Materials

Students are to bring the following materials to the hands-on lab:

- At least one USB flash drive (formatted with the FAT32 file system)

The following texts will be used for the class:

Casey, E. (ed.) (2010). *Handbook of Digital Forensics and Investigations*. Elsevier Academic Press. Burlington, MA.

Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. National Institute of Standards and Technology. Gaithersburg, MD. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Jansen, W. and Delaitre, A. (2009, October). "Mobile Forensic Reference Materials: A Methodology and Reification." National Institute of Standards and Technology Interagency Report (NISTIR) 7617. National Institute of Standards and Technology. Gaithersburg, MD. http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf

Jansen, W., Delaitre, A., and Moenner, L. (2008, January). "Overcoming Impediments to Cell Phone Forensics." National Institute of Standards and Technology. Gaithersburg, MD. http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Impediments-formatted-final-post.pdf

Graded Material

Each assignment, quiz, project, and exam will be graded on a 0-100 point scale.

The final average is calculated by the following weights.

Assignments	20%
Quizzes	20%
Midterm	25%
Hands-on Exercises	15%
Final Exam	20%
Total	100%

The following criteria will be used for the assignment of letter grades

A	92-100
A-	90-91
B+	87-89
B	83-86
B-	80-82
C	70-79
F	0-69

The course will adhere to the university's policies on grading.

Assignment Due Dates

All assignments are to be submitted by the due dates listed in the syllabus. Work will not be accepted late. Assignments are to be submitted via Blackboard.

Class Attendance

While the course will be taught primarily online, attendance for the conference calls and hands-on lab is mandatory. The lab will involve the hands-on use of forensics tools, which will be used in the classroom. In the event that a student cannot attend class due to an emergency or crisis, the student is to contact the instructor as soon as possible.

Responsible Use of Computing Policy

Use of computer equipment, including Internet connections within the classroom will be conducted in accordance with the University's Responsible Use of Computing (RUC) Policy. This applies to all academic and operational departments and offices at all university locations owned or leased. The policies and procedures provided herein apply to all Mason faculty, staff, students, visitors, and contractors.

The university provides and maintains general computing services, including web and Internet resources, and telecommunication technology to support the education, research, and work of its faculty, staff, and students. At the same time, Mason wishes to protect all users' rights to an open exchange of ideas and information. This policy sets forth the responsibilities of each member of the Mason community in preserving the security, confidentiality, availability, and integrity of Mason computing resources. To accomplish these ends, this policy supports investigations of complaints involving Mason computing abuse, including sexual harassment, honor code, federal, state, applicable industry, and local law violations.

University faculty and staff members, as state employees, are subject to the Freedom of Information Act, §2.2-3700, et seq., of the Code of Virginia, and all applicable state and federal rules and regulations. While this policy endeavors to maintain user confidentiality, it cannot create, nor should faculty or staff members presume, any expectation of privacy.

Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities. It is the responsibility of all users of Mason computing resources to read and follow this policy and all applicable laws and procedures (user sign-on agreement).

For more information regarding the RUC Policy, consult the student handbook.

University Policies

This course will be taught in compliance with George Mason University policies, which can be found online at http://universitypolicy.gmu.edu/

Important Dates

Last day to drop with no tuition penalty	September 8
Last day to drop with a 33% tuition penalty	September 15
Last day to drop with a 67% tuition penalty	October 2
Thanksgiving Break	November 25-29
Final Exams	December 14-21

The full calendar maintained by the University Registrar can be found online at:
http://registrar.gmu.edu/calendars/2015fall/

Office of Disability Services

The Office of Disability Services (ODS) is available to serve all students with disabilities, including those with cognitive (e.g., learning, psychological, and closed head injury), sensory, mobility, and other physical impairments.

The Office of Disability Services serves qualified students with disabilities to ensure equal access to the university's programs and services. A qualified student with a disability is a student with a disability, who meets the academic and technical standards required for admission or participation in the university's educational program and services. As defined in the Americans with Disabilities Act (ADA), and section 504 of the Rehabilitation Act of 1973, a person has a disability if he/she:

- Has a physical or mental impairment which substantially limits one or more major life activities, or
- Has a record of such impairment, or
- Is regarded as having such impairment

Students requesting assistance should contact the Office of Disability Services at http://ods.gmu.edu/

Course Outline

The following is the course outline. It is subject to revision.

Week 1 8/31 to 9/5	**Introduction to Cell phone forensics**	
	Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 537-542. Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 48-50.
	Classroom material	Introduction.pptx "The Growth of Mobile: Stats and figures that will shock you!" http://www.youtube.com/watch?v=0aUQLIPdtg8
Week 2 9/6 to 9/12	**Mobile Device Usage and Data Artifacts**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 3-7. Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 529-532.
	Classroom material	Usage_and_Data.pptx
	Assignments	Assignment #1 – Current Events Due by 11:59PM on September 12
Week 3 9/13 to 9/19	**Carrier Technologies**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 10-14. ETSI. "Mobile technologies GSM." http://www.webcitation.org/5yRQjyd8W ETSI. "Cellular History." http://www.etsi.org/WebSite/Technologies/Cellularhistory.aspx TelecomSpace. "CDMA" http://www.telecomspace.com/cdma.html Antipolis, S. (2012, June 1.) "New SIM card format for slimmer, smaller phones." Retrieved from the ETSI website: http://www.etsi.org/news-events/news/398-news-release-1-june-2012

		Jansen, W. and Ayers, R. (2007, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 7-10.
	Classroom material	Carriers.pptx
	Assignment	Assignment #2 – Data Contained on Mobile Devices Due by 11:59PM on September 19
	Quiz	Quiz 1 (Material from weeks 1 and 2)
Week 4 9/20 to 9/26	**Network Service Provider Infrastructure**	
	Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 517-526.
	Classroom material	Infrastructure.pptx
	Assignment	Assignment #3 – Carrier Technology Due by 11:59PM on September 26
Week 5 9/27 to 10/3	**Procedures**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 27-47.
		Ayers, R., Wayne, J., Cilleros, N., and Daniellou, R. (2005). Cell Phone Forensic Tools: An Overview and Analysis. p. 5.
	Classroom material	Procedures.pptx
		Cellebrite Demonstration http://www.youtube.com/watch?v=kET-F_3xuD8
		SIM Card Seizure Demonstration http://www.youtube.com/watch?v=fFMPUCrvuo
		Hands-on demonstrations with phones and tools
		Paraben Device Seizure Instructions
	Assignment	Assignment #4 – Infrastructure Due by 11:59PM on October 3
	Quiz	Quiz 2 (Material from weeks 3 and 4)

Week 6 10/4 to 10/10	**Impediments to Cell Phone Forensics**		
	Reading assignment	Jansen, W., Delaitre, A., and Moenner, L. (2008). "Overcoming Impediments to Cell Phone Forensics." Proceedings of the 41st Hawaii International Conference on System Sciences. National Institute of Standards and Technology. http://www.forensicswiki.org/images/9/9c/JensenCellPhones.pdf
	Classroom material	Impediments.pptx
	Assignment	Assignment #5 – Procedures Due by 11:59PM on October 10
Week 7 10/11 to 10/17	**Mid-term**	The mid-term is to be completed by 11:59PM on October 17.
Week 8 10/18 to 10/24	**Comparison and Contrast of Current Industry Toolsets**	
	Reading assignment	Ayers, R., Jansen, W., Moenner, L., and Delaitre, A. (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. NISTIR 7387. Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 15-26. Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 410-412.
	Classroom material	Forensic_Tools.pptx Chip-off_Forensics.pptx
	Assignment	Assignment #6 –Recommendations Due by 11:59PM on October 24
Week 9 10/25 to 10/31	**Acquisition I**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 50-52.
	Classroom material	UFED_Acquisition.pptx DS_Acquisition.pptx BitPim_Acquisition.pptx

	Assignment	Assignment # 7 – Forensic Tools Recommendations Due by 11:59PM on October 31
Week 10 11/1 to 11/7	**Acquisition II**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 27-47.
	Classroom material	Kindle.pptx SIM Acquisition.pptx TomTom-GPS.pptx "Bourne SIM clone" http://www.youtube.com/watch?v=3_eYMfggkq0 "Paraben's SIM Card Seizure software demo" http://www.youtube.com/watch?v=fFMPUCPrvuo
	Quiz	Quiz 3 (Material from weeks 8 and 9)
Week 11 11/8 to 11/14	**Legal Interception of Data**	
	Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 542-556.
	Classroom material	Legal_Interception.pptx The hands-on lab will be conducted on George Mason University's Fairfax campus on November 14th from 8:00AM to 5:00PM. The location of the classroom will be announced
Week 12 11/15 to 11/21	**Call Detail Records (CDRs) and other Data from Network Service Providers**	
	Reading assignment	Jansen, W. and Ayers, R. (2014, May). "Guidelines on Cell Phone Forensics." Special Publication 800-101. Revision 1. pp. 52-55. Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 527-528.
	Classroom material	NSP-data.pptx Tower_Info.pptx Geolocating.pptx EXIF_Data.pptx

		Other Fun Stuff – Analyzing EXIF Data
	Assignment	Assignment #8 – FISA Due by 11:59PM on November 21
	Quiz	Quiz 4 (Material from weeks 10 and 11)
	Thanksgiving Break	
11/22 to 11/28		
Week 13	**Interpreting Recovered Data**	
11/29 to 12/5	Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 517-526.
	Classroom material	Mapped_CDR.pptx
		Cell_Site_Analysis.pptx
	Assignment	Assignment #9 – Cell Tower Assignment (.pptx) Due by 11:59PM on December 5
Week 14	**Mobile Malware**	
12/6 to 12/12	Reading assignment	Android Developers. (2011, June 7). "Security Permissions." http://developer.android.com/guide/topics/security/security.html
		(Anonymous). (2011, March 20). "Breaking out of Android Sandbox." http://pfalcon-oe.blogspot.com/2011/03/breaking-out-of-android-sandbox.html
		McMillan, R. (2011, January 17). "Coming Soon: A New Way to Hack into Your Smartphone." http://www.pcworld.com/businesscenter/article/216842/coming_soon_a_new_way_to_hack_into_your_smartphone.html
		Morgan, B. (2002, November 15). "J2ME Security: Now and in the Future." http://www.informit.com/articles/article.aspx?p=30029
		Knudsen, J. (2003, February). "Understanding MIDP 2.0's Security Architecture." http://developers.sun.com/mobility/midp/articles/permissions/

	Classroom material	Malware on Exploits.pptx
		Malware on Mobile Platforms.pptx
	Assignment	Project Due by 11:59PM on December 12
Week 15 12/14 to 12/19	**Final Exam**	The final exam is to be completed by 11:59PM on December 19.