

George Mason University
CFRS 762 – Mobile Device Forensics
CRN 16900, Sec 001
Spring 2013, January 25-Mary 10, F 6:00-8:45PM
ENGR 4457

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.

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 class:

- At least one USB flash drive
- Laptops with VMware, VM Fusion, or VMplayer

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. (2007, May). "Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology." Special Publication 800-101. National Institute of Standards and Technology. Gaithersburg, MD. <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.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

Attendance is mandatory. A number of classes 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.

Important Dates

Last day to drop with no tuition penalty	January 29
Last day to drop with a 33% tuition penalty	February 12
Last day to drop with a 67% tuition penalty	February 22
Thanksgiving Break	March 11-17
Final Exams	May 8-14

Course Outline

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

Week 1 Introduction to Cell phone forensics

1/25

Reading assignment Casey, E. (2010). "Chapter 10: Mobile Network Investigations." *Handbook of Digital Forensics and Investigations*. pp. 537-542.

Classroom material Introduction.pptx

"The Growth of Mobile: Stats and figures that will shock you!"
<http://www.youtube.com/watch?v=0aUQLPdtg8>

Week 2 Mobile Device Usage and Data Artifacts

2/1

Reading assignment Jansen, W. and Ayers, R. (2007). Guidelines on Cell Phone Forensics. Appendix C. pp. 82-92.

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 on February 1 by 5:45PM

Assignment #2 – Current Mobile Device Forensics
 Due on February 1 by 5:45PM

Week 3 **Carrier Technologies**
2/8

Reading assignment Jansen, W. and Ayers, R. (2007). Guidelines on Cell Phone Forensics. Section 2.1. pp. 6-8.

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>

Classroom material Carriers.pptx

Assignment Assignment #3 – Data Contained on Mobile Devices
Due on February 8 by 5:45PM

Quiz Quiz 1 (Material from weeks 1 and 2)

Week 4 **Network Service Provider Infrastructure**
2/15

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 #4 – Carrier Technology
Due on February 15 by 5:45PM

Week 5 **Procedures**
2/22

Reading assignment	Jansen, W. and Ayers, R. (2007). Guidelines on Cell Phone Forensics. Sections 3 – 7.2. pp. 13-61. 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=fMPUCrvuo Hands-on demonstrations with phones and tools Paraben Device Seizure Instructions
Assignment	Assignment #5 – Infrastructure Due on February 22 by 5:45PM
Quiz	Quiz 2 (Material from weeks 3 and 4)

Week 6 **Impediments to Cell Phone Forensics**
3/1

Reading assignment	Jansen, W., Delaitre, A., and Moenner, L. (2008). "Overcoming Impediments to Cell Phone Forensics." Proceedings of the 41 st 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 #6 – Procedures Due on March 1 by 5:45PM

Week 7 **Mid-term**
3/8

Spring Break
3/15

Week 8 **Comparison and Contrast of Current Industry Toolsets**
3/22

Reading assignment Ayers, R., Jansen, W., Moenner, L., and Delaitre, A. (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. NISTIR 7387.

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

Hands-on Exercises/Acquisitions to be conducted

Assignment Assignment #7 –Recommendations
Due on March 22 by 5:45PM

Week 9 **Acquisition I**
3/29

Reading assignment

Classroom material UFED_Acquisition.pptx

DS_Acquisition.pptx

BitPim_Acquisition.pptx

Hands-on Exercises/Acquisitions to be conducted

Assignment Assignment # 8 – Forensic Tools Recommendations
Due on March 29 by 5:45PM

Week 10 Acquisition II

4/5

- Reading assignment Jansen, W. and Ayers, R. (2007). Guidelines on Cell Phone Forensics. Section 2.3. pp. 11-12.
- 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=ffMPUCPrvu0>
- Hands-on Exercises/Acquisitions to be conducted
- Quiz Quiz 3 (Material from weeks 8 and 9)

Week 11 Legal Interception of Data

4/12

- Reading assignment Casey, E. (2010). “Chapter 10: Mobile Network Investigations.” *Handbook of Digital Forensics and Investigations*. pp. 542-556.
- Classroom material Legal_Interception.pptx
- Hands-on Exercises/Acquisitions to be conducted

Week 12 Call Detail Records (CDRs) and other Data from Network Service Providers

4/19

Reading assignment Jansen, W. and Ayers, R. (2007). Guidelines on Cell Phone Forensics. Sections 7.3. pp. 61-64.

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

Hands-on Exercises/Acquisitions to be conducted

Assignment Assignment #9 – FISA
Due April 19 by 5:45PM

Quiz Quiz 4 (Material from weeks 10 and 11)

Week 13 Interpreting Recovered Data

4/26

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

Hands-on Exercises/Acquisitions to be conducted

Assignment Assignment #10 – Cell Tower Assignment (.pptx)
Due on April 26 by 5:45PM

Week 14 Mobile Malware

5/3

Reading assignment	<p>Android Developers. (2011, June 7). "Security Permissions." http://developer.android.com/guide/topics/security/security.html</p> <p>(Anonymous). (2011, March 20). "Breaking out of Android Sandbox." http://pfalcon-oe.blogspot.com/2011/03/breaking-out-of-android-sandbox.html</p> <p>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</p> <p>Morgan, B. (2002, November 15). "J2ME Security: Now and in the Future." http://www.informit.com/articles/article.aspx?p=30029</p> <p>Knudsen, J. (2003, February). "Understanding MIDP 2.0's Security Architecture." http://developers.sun.com/mobility/midp/articles/permissions/</p>
Classroom material	<p>Malware on Exploits.pptx</p> <p>Malware on Mobile Platforms.pptx</p>
Assignment	<p>Assignment #11</p> <p>Due on May 3 by 5:45PM</p>
Quiz	<p>Quiz 5 (Material from weeks 12 and 13)</p>

Week 15 Final Exam

5/10