

**George Mason University**  
**CFRS 762 – Mobile Device Forensics**  
**CRN 17828, DL1**  
**Spring 2016, January 19 – May 11**

### **Instructor**

Michael Robinson  
[mrobinsv@gmu.edu](mailto: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. The class will be using Blackboard's Collaborate to hold these weekly video conference calls. 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, April 9 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](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	January 26
Last day to drop with a 33% tuition penalty	February 2
Last day to drop with a 67% tuition penalty	February 19
Spring Break	March 7-13
Final Exams	May 4-11

The full calendar maintained by the University Registrar can be found online at:  
<https://registrar.gmu.edu/calendars/spring-2016/>

### **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 Introduction to Cell phone forensics

1/19

to

1/24

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 Mobile Device Usage and Data Artifacts

1/25

to

1/31

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 January 31

### Week 3 Carrier Technologies

2/01

to

2/07

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/technologies-clusters/technologies/past-work/cellular-history>

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 February 7
Quiz	Quiz 1 (Material from weeks 1 and 2) Due by 11:59PM on February 7
<b>Week 4</b> 2/08 to 2/14	<b>Network Service Provider Infrastructure</b>
Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." <i>Handbook of Digital Forensics and Investigations</i> . pp. 517-526.
Classroom material	Infrastructure.pptx
Assignment	Assignment #3 – Carrier Technology Due by 11:59PM on February 14
<b>Week 5</b> 2/15 to 2/21	<b>Procedures</b>
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 <a href="http://www.youtube.com/watch?v=kET-F_3xuD8">http://www.youtube.com/watch?v=kET-F_3xuD8</a>  SIM Card Seizure Demonstration <a href="http://www.youtube.com/watch?v=fFMPUCrvuo">http://www.youtube.com/watch?v=fFMPUCrvuo</a>  Hands-on demonstrations with phones and tools  Paraben Device Seizure Instructions
Assignment	Assignment #4 – Infrastructure Due by 11:59PM on February 21
Quiz	Quiz 2 (Material from weeks 3 and 4) Due by 11:59PM on February 21

**Week 6 Impediments to Cell Phone Forensics**

2/22

to

2/28

Reading assignment Jansen, W., Delaitre, A., and Moenner, L. (2008). "Overcoming Impediments to Cell Phone Forensics." Proceedings of the 41<sup>st</sup> 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 February 28

**Week 7 Mid-term**

2/29

to

3/06

The mid-term is to be completed by 11:59PM on March 6.

**Spring Break**

3/07

to

3/13

No class – no conference calls

**Week 8 Comparison and Contrast of Current Industry Toolsets**

3/14

to

3/20

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 March 20

<b>Week 9</b> 3/21 to 3/27	<b>Acquisition I</b>	
	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 March 27
<b>Week 10</b> 3/28 to 4/03	<b>Acquisition II</b>	
	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" <a href="http://www.youtube.com/watch?v=3_eYMfggkq0">http://www.youtube.com/watch?v=3_eYMfggkq0</a>  "Paraben's SIM Card Seizure software demo" <a href="http://www.youtube.com/watch?v=fFMPUCPrvu0">http://www.youtube.com/watch?v=fFMPUCPrvu0</a>
	Quiz	Quiz 3 (Material from weeks 8 and 9) Due by 11:59PM on April 3
<b>Week 11</b> 04/04 to 4/10	<b>Legal Interception of Data</b>	
	Reading assignment	Casey, E. (2010). "Chapter 10: Mobile Network Investigations." <i>Handbook of Digital Forensics and Investigations</i> . pp. 542-556.
	Classroom material	Legal_Interception.pptx  The hands-on lab will be conducted on George Mason University's Fairfax campus on April 9 <sup>th</sup> from 8:00AM to 5:00PM. The location of the classroom will be announced



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

4/11

to

4/17

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 April 17

Quiz Quiz 4 (Material from weeks 10 and 11)  
Due by 11:59PM on April 17

**Week 13 Interpreting Recovered Data**

4/18

to

4/24

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 April 24

**Week 14 Mobile Malware**

4/25

to

5/01

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](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 May 1
<b>Week 15</b> 05/02 to 05/08	<b>Final Exam</b>  The final exam is to be completed by 11:59PM on May 08.