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

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. 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:


**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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>20%</td>
</tr>
<tr>
<td>Quizzes</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm</td>
<td>25%</td>
</tr>
<tr>
<td>Hands-on Exercises</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Grade</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>92-100</td>
</tr>
<tr>
<td>A-</td>
<td>90-91</td>
</tr>
<tr>
<td>B+</td>
<td>87-89</td>
</tr>
<tr>
<td>B</td>
<td>83-86</td>
</tr>
<tr>
<td>B-</td>
<td>80-82</td>
</tr>
<tr>
<td>C</td>
<td>70-79</td>
</tr>
<tr>
<td>F</td>
<td>0-69</td>
</tr>
</tbody>
</table>
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/](http://universitypolicy.gmu.edu/)
Important Dates

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last day to drop with no tuition penalty</td>
<td>January 26</td>
</tr>
<tr>
<td>Last day to drop with a 33% tuition penalty</td>
<td>February 2</td>
</tr>
<tr>
<td>Last day to drop with a 67% tuition penalty</td>
<td>February 19</td>
</tr>
<tr>
<td>Spring Break</td>
<td>March 7-13</td>
</tr>
<tr>
<td>Final Exams</td>
<td>May 4-11</td>
</tr>
</tbody>
</table>

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  


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  


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  

ETSI. “Mobile technologies GSM.”  
http://www.webcitation.org/5yRQiyd8W

ETSI. “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:  

<table>
<thead>
<tr>
<th>Week 4</th>
<th>Network Service Provider Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom material</td>
<td>Carriers.pptx</td>
</tr>
</tbody>
</table>

| 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 |

<table>
<thead>
<tr>
<th>Week 5</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom material</td>
<td>Procedures.pptx</td>
</tr>
</tbody>
</table>

| | 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 |

| 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**
- **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

## Week 8
### Comparison and Contrast of Current Industry Toolsets
#### 3/14 to 3/20
- **Reading assignment**
- **Classroom material**
  - Forensic_Tools.pptx
  - Chip-off_Forensics.pptx
- **Assignment**
  - Assignment #6 – Recommendations
  - Due by 11:59PM on March 20
### Week 9: Acquisition I

**3/21 to 3/27**

**Reading assignment**


**Classroom material**

- UFED_Acquisition.pptx
- DS_Acquisition.pptx
- BitPim_Acquisition.pptx

**Assignment**

Assignment # 7 – Forensic Tools Recommendations
Due by 11:59PM on March 27

---

### Week 10: Acquisition II

**3/28 to 4/03**

**Reading assignment**


**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)
Due by 11:59PM on April 3

---

### Week 11: Legal Interception of Data

**04/04 to 4/10**

**Reading assignment**


**Classroom material**

- Legal_Interception.pptx

The hands-on lab will be conducted on George Mason University’s Fairfax campus on April 9th from 8:00AM to 5:00PM.
The location of the classroom will be announced
**Week 12**  
4/11 to 4/17

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

**Reading assignment**  


**Classroom material**  
NSP-data.pptx

Tower_Info.pptx

Geolocating.pptx

EXIF_Data.pptx

**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**  
4/18 to 4/24

**Interpreting Recovered Data**

**Reading assignment**  

**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**  
4/25 to 5/01

**Mobile Malware**

**Reading assignment**  


http://www.pcworld.com/businesscenter/article/216842/coming_soon_a_new_way_to_hack_into_your_smartphone.html


Classroom material
Malware on Exploits.pptx
Malware on Mobile Platforms.pptx

Assignment
Project
Due by 11:59PM on May 1

Week 15 Final Exam
05/02 to 05/08

The final exam is to be completed by 11:59PM on May 08.