George Mason University  
CFRS 762 – Mobile Device Forensics  
CRN 77355, Sec 001  
Fall 2012, August 31-December 14, 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.


**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

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last day to drop with no tuition penalty</td>
<td>September 4</td>
</tr>
<tr>
<td>Last day to drop with a 33% tuition penalty</td>
<td>September 18</td>
</tr>
<tr>
<td>Last day to drop with a 67% tuition penalty</td>
<td>September 28</td>
</tr>
<tr>
<td>Thanksgiving Break</td>
<td>November 21-25</td>
</tr>
<tr>
<td>Final Exams</td>
<td>December 11-19</td>
</tr>
</tbody>
</table>
Course Outline

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

**Week 1  Introduction to Cell phone forensics**
8/31


Classroom material  Introduction.pptx

“The Growth of Mobile: Stats and figures that will shock you!”
[http://www.youtube.com/watch?v=0aUQLIPdtg8](http://www.youtube.com/watch?v=0aUQLIPdtg8)

**Week 2  Mobile Device Usage and Data Artifacts**
9/7


Classroom material  Usage_and_Data.pptx

Assignments  Assignment #1 – Current Events
Due on September 7 by 5:45PM

Assignment #2 – Current Mobile Device Forensics
Due on September 7 by 5:45PM

**Week 3  Carrier Technologies**
9/14


ETSI. “Mobile technologies GSM.”
[http://www.webcitation.org/5yRQjyd8W](http://www.webcitation.org/5yRQjyd8W)

ETSI. “Cellular History”

TelecomSpace. “CDMA”

Classroom material  Carriers.pptx

Assignment  Assignment #3 – Data Contained on Mobile Devices
Due on September 14 by 5:45PM
<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>Section</th>
<th>Reading Assignment</th>
</tr>
</thead>
</table>

**Assignment**
- **Week 4**
  - Assignment #4 – Carrier Technology
  - Due on September 21 by 5:45PM

- **Week 5**
  - Assignment #5 – Infrastructure
  - Due on September 28 by 5:45PM

**Quiz**
- **Week 4**
  - Quiz 1 (Material from weeks 1 and 2)
- **Week 6**
  - Quiz 2 (Material from weeks 3 and 4)
Week 7 10/12
Mid-term

Week 8 10/19
Comparison and Contrast of Current Industry Toolsets
Reading assignment

Classroom material
Forensic_Tools.pptx
Hands-on Exercises/Acquisitions to be conducted

Assignment
Assignment #6 – Procedures
Due on October 5 by 5:45PM

Assignment #7 –Recommendations
Due on October 19 by 5:45PM

Week 9 10/26
Acquisition I
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 October 26 by 5:45PM

Week 10 11/2
Acquisition II
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

Hands-on Exercises/Acquisitions to be conducted

<table>
<thead>
<tr>
<th>Week 11</th>
<th>Legal Interception of Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Classroom material</td>
</tr>
</tbody>
</table>

Hands-on Exercises/Acquisitions to be conducted

<table>
<thead>
<tr>
<th>Week 12</th>
<th>Call Detail Records (CDRs) and other Data from Network Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Classroom material</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assignment</td>
</tr>
<tr>
<td></td>
<td>Assignment</td>
</tr>
<tr>
<td></td>
<td>Quiz</td>
</tr>
</tbody>
</table>

**Thanksgiving Break**
11/23

<table>
<thead>
<tr>
<th>Week 13</th>
<th>Interpreting Recovered Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Classroom material</td>
</tr>
</tbody>
</table>

Hands-on Exercises/Acquisitions to be conducted
Assignment

Assignment #10 – Cell Tower Assignment (.pptx)
Due on November 30 by 5:45PM

Week 14
12/7

Mobile Malware

Reading assignment


into Your Smartphone." http://www.pcworld.com/businesscenter/article/216842/coming_soon_a_new_way_to_hack_into_your_smartphone.html


Architecture.”
http://developers.sun.com/mobility/midp/articles/permissions/

Classroom material

Malware on Exploits.pptx

Malware on Mobile Platforms.pptx

Assignment

Assignment #11
Due on December 7 by 5:45PM

Quiz

Quiz 5 (Material from weeks 12 and 13)

Week 15
12/14

Final Exam