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

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.

**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**

- Last day to drop with no tuition penalty: January 29
- Last day to drop with a 33% tuition penalty: February 11
- Last day to drop with a 67% tuition penalty: February 21
- Spring Break: March 10-16
- Final Exams: May 7-14
The full calendar maintained by the University Registrar can be found online at:
http://registrar.gmu.edu/calendars/2013fall/

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
1/24


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
1/31

Appendix C. pp. 82-92.


Classroom material  Usage_and_Data.pptx

Assignments  Assignment #1 – Current Events
Due on January 31 by 7:00PM

Week 3  Carrier Technologies
2/7

Section 2.1. pp. 6-8.

ETSI. “Mobile technologies GSM.”
http://www.webcitation.org/5yRQiYd8W

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:

Classroom material  Carriers.pptx
Assignment Assignment #2 – Data Contained on Mobile Devices
Due on February 7 by 7:00PM

Quiz Quiz 1 (Material from weeks 1 and 2)

Week 4
2/14

Network Service Provider Infrastructure


Classroom material Infrastructure.pptx

Assignment Assignment #3 – Carrier Technology
Due on February 14 by 7:00PM

Week 5
2/21

Procedures


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 on February 21 by 7:00PM

Quiz Quiz 2 (Material from weeks 3 and 4)

Week 6
2/28

Impediments to Cell Phone Forensics

Classroom material  | Impediments.pptx
--- | ---
Assignment  | Assignment #5 – Procedures  
| Due on February 28 by 7:00PM

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

Spring Break  
3/14

**Week 8**  
Comparison and Contrast of Current Industry Toolsets  
3/21


Classroom material  | Forensic_Tools.pptx  
| Chip-off_Forensics.pptx

Hands-on Exercises/Acquisitions to be conducted

Assignment  | Assignment #6 – Recommendations  
| Due on March 21 by 7:00PM

**Week 9**  
Acquisition I  
3/28

Reading assignment

Classroom material  | UFED_Acquisition.pptx  
| DS_Acquisition.pptx  
| BitPim_Acquisition.pptx

Hands-on Exercises/Acquisitions to be conducted

Assignment  | Assignment #7 – Forensic Tools Recommendations  
| Due on March 28 by 7:00PM

**Week 10**  
Acquisition II  
4/4

| Section 2.3. pp. 11-12.
### Week 11
#### Legal Interception of Data

4/11

**Reading assignment**


**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

4/18

**Reading assignment**


**Classroom material**

NSP-data.pptx

Tower_Info.pptx

Geolocating.pptx

EXIF_Data.pptx

Other Fun Stuff – Analyzing EXIF Data

**Assignment**

Assignment #8 – FISA
Due April 18 by 7:00PM

**Quiz**

Quiz 4 (Material from weeks 10 and 11)
Week 13  4/25  Interpreting Recovered Data


Classroom material  Mapped_CDR.pptx

Cell_Site_Analysis.pptx

Hands-on Exercises/Acquisitions to be conducted

Assignment  Assignment #9 – Cell Tower Assignment (.pptx)
Due on April 25 by 7:00PM

Week 14  5/2  Mobile Malware


Classroom material  Malware on Exploits.pptx

Malware on Mobile Platforms.pptx

Assignment  Project
Due by May 2 by 7:00PM

Week 15  5/9  Final Exam