CFRS 780

Cloud Forensics • Spring 2018 Garfinkel

Spring 2018
Mon 7:20-10:00pm
Fairfax Campus
Nguyen Engineering Bld. ????

Instructor: Simson L. Garfinkel, Ph.D.
E-Mail: sgarfin2@gmu.edu
Phone: 202-649-0029
Office Hours: by appointment

Overview

"Explores digital forensics as applied to cloud computing. We will explore how to perform digital forensics on a cloud-based system, and how to leverage cloud computing for performing massive digital forensics at scale. Class sessions consist of a 1-hour lecture and discussion followed by a 75-minute lab. Homework consists of reading and commenting on papers, and a final project.

Learning Outcomes:

At the end of this class, you will be able to:

- Create and manage virtual machines using Amazon Web Services.
- Acquire data from systems running in the cloud, including virtual machines, virtualized services, databases and log files.
- Analyze data in the cloud using Apache Spark
- Read and discuss scientific papers about digital forensics.
- Design, execute, and present a digital forensics research project.

Materials

Assigned papers

Open source software

An Amazon Web Services account (please create yours before the first day of class.)

Milestones

Mon Jan 22
First Day of class

Mon April 30
Last day of class.
In class presentations.
Projects due.

Requirements

Students must have a working knowledge the Unix command line. Students must have *either* a laptop or a USB stick to hold private key material that they will use to access Amazon Web Services. Students must create an Amazon Web Services Educate! Account (https://aws.amazon.com/education/awseducate/) prior to the first day of class. To do so, students will need to have a valid credit card.

Materials and Student Deliverables

Required Readings are due on the date for which they are appear on the syllabus so that they can be discussed in class. Students are responsible for the content of these readings. Readings will be made available on Blackboard. **This course expects you to spend 1-2 hours of preparation time for each hour of class time.**

Discussions take place in class from 7:20-8:30. Students are expected to participate.

Labs take place from 8:45-10:00. Students will typically be given one class period to start the lab and one class period to continue the lab. Students that are well-prepared and well-organized may be able to complete the lab work in class alone; other students will need to invest their own time after class.

Each student is expected to make two *Presentations* during this course. 1) Each student will present a current cloud forensics problem and discuss how they will research the problem. This presentation should be 5-10 minutes in length. 2) Each student will present their final project, in which they present a solution to the problem at they previously identified. This presentation will be 10-15 minutes in length. Depending on the size of the class and the project, final projects may be performed by individuals or teams.

Grading

The grade shall be based on labs, final project, and classroom participation.

Grading will be consistent with the GMU Graduate Grading Policy[1], with a 100% of all possible credit being equivalent to 4.0 quality points and a grade of A+.

Student Deliverables and Weight:

Student Deliverable	Assigned	Due	Weight
Lab 1 (2 weeks) AWS VM Lab	Jan 22	Feb 5	10%
Lab 2: (1 week) AWS Disk Imaging and Analysis	Feb 5	Feb 12	10%
Lab 3 (1 week) S3 and HDFS	Feb 12	Feb 19	10%
Lab 4 (2 weeks) Spark and SparkSQL	Feb 19	Mar 5	10%
Lab 5: (2 weeks) Finding cloud artifacts with bulk_extractor	Mar 5	Mar 19	10%
Presentation #1: Final Project Proposal			5%
Presentation #2: Final Project		Apr 28	10%
Final Project Paper		TBD	15%
Class Participation First Half			10%
Class Participation Second Half			10%

Problem Sets (Labs & Homework)

Problem sets are research-oriented tasks that begin in class and may be completed at home. These tasks will typically take between 1 and 4 hours to complete, depending on the skill of the student. Students are to submit a PDF file that is structured as a laboratory report clearly indicating what they did and what they discovered. Each report should include the sections: **Executive Summary; Apparatus and Procedures; Results; Conclusions**. A standard rubric will be used to grade the lab report.

Late labs will only be accepted in exceptional circumstances.

Online Materials and Communications

All materials will be accessible through Blackboard, and Blackboard will be used to collect all student assignments. All class announcements will be sent through Blackboard. You are responsible for either having announcements delivered to a mailbox that you check, or monitoring Blackboard for information. You can access Blackboard at https://mymasonportal.gmu.edu/.

[1] http://catalog.gmu.edu/content.php?catoid=15&navoid=1172#gradgrading

According to university policy, students and faculty are to use their GMU.EDU email addresses for all course-related communications, as some commercial email systems may be filtered out by the GMU.EDU system.

Attendance Policy

“AP.1.6 Attendance Policies: Students are expected to attend the class periods of the courses for which they register. In-class participation is important not only to the individual student, but also to the class as a whole. Because class participation may be a factor in grading, instructors may use absence, tardiness, or early departure as de facto evidence of nonparticipation. Students who miss an exam with an acceptable excuse may be penalized according to the individual instructor’s grading policy, as stated in the course syllabus.” (2017-2018 University Catalog, p. 78, https://catalog.gmu.edu/pdf/2017-2018.pdf)

Students are expected to attend each class, to complete all preparatory work (including assigned reading), and to participate actively in lectures, discussions and exercises. Students are expected to contact the Instructor in advance for planned absences, and after class as soon as possible in the event of a medical or personal emergency. Work-related absences can be accommodated if the Instructor is notified in advance.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Academic Integrity and the Honor Code

The Mason Honor Code: Student members of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work (https://oai.gmu.edu/mason-honor-code/).

Academic integrity on the part of students is an important part of professional performance. The policy for labs, homework, tests and final projects is simple: no assistance may be obtained from any person, by any means including conversation, copying written work, phone conversations, or any electronic communication, unless specifically approved in advance by the instructor. Open book exams include: use of all books, notes, and on-line sources that do not involve interaction with a person.

Accommodations for Disabilities

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with Office for Disability Services (SUB I, Rm. 2500; 993-2474; http://ods.gmu.edu) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.