GMU CFRS 764: Mac Forensics Syllabus

Instructor: Simson L. Garfinkel

Email: sgarfin2@gmu.edu

Class Meetings: Wednesday, 7:20 pm – 10:00pm, Innovation Hall - Room 233

Office Hours: By appointment

Required Materials: *(The following items are required Week 2)*

- 1TB+ USB 3.0 drive (Spinning or SSD) - Example
- iCloud Account - https://www.icloud.com
- Apple Developer Account – https://developer.apple.com/
- (you do not need a paid membership or subscription)
- MacOS X Installers - (You should download installers for macOS Mojave 10.14.1 from https://developer.apple.com/download/ and optionally OS X Yosemite 10.10.3 from https://developer.apple.com/download/more/.)

Required Textbooks:

OSX Incident Response, by Jaron Bradley, Elsevier Syngress, 2018, ISBN 978-0-12-804456-8

The Art of Memory Forensics, Michael Ligh, Andrew Case, Jamie Levy and Aaron Walters, Wiley, 2014, 978-1-118-82509-9

Additional written materials will be provided by the instructor and disseminated via Blackboard

Optional:

Mac Computer (Lab computers will be available)

Description: Presents students with the concepts, tools, and techniques used for forensic analysis of the Macintosh based computers. Classes will consist of lectures on forensic practice and research, followed by exercises conducted in a lab environment.

Teaching Objectives: Students will learn how Macs are different than computers running Windows and Linux and be able to analyze them accordingly, including both stored data (HD/SSD/USB/SD) and memory acquisition and analysis. Students will learn to research and present a current topic in Mac digital forensics. Students will learn how to engage with digital forensics as an *experimental science*, by performing and reporting digital forensics experiments during classroom labs.

Student Presentations: Students will be responsible for making two presentations.

Presentation #1: Literature Review—10 minutes

Each student will present the contents of an academic paper about Mac forensics. Students will identify the paper that they wish to present (a list of possible papers will be provided, but students may also suggest their own). Three days before the presentation the student will send slides to the professor for grading; the slides will be returned within 48 hours.

Presentation #2: Group Research Presentation—15 minutes.

The second presentation may be based on a set of research papers, the application of an open source digital forensics tool to a Mac system, or original research that the student performs. Both presentation topics and student slides must be approved in advance.

Tentative Course Schedule

Overview Week 1 – ***Jan 23, 2019***
Course Overview/Administrative Items; History
Overview of course presented, syllabus reviewed, administrative items discussed. Topic of discussion will include the history of MacOS, Mac forensics history, and current issues.

Week 2 – ***Jan 30, 2019***
Mac Hardware, Disk Partitioning and Mac Filesystems
Deep-dive into Mac hardware understanding use scenarios. Storage in the Mac world.

Week 3 – ***Feb 6, 2019***
Understanding Live and Dead Imaging. Time Machine.
Setting up and configuring a Mac to conduct forensic analysis. Live and dead imaging of storage systems. Verifying and safely mounting forensic images as they pertain to the Mac environment. Making use of Time Machine.

Week 4 – ***Feb 13, 2019***
Loading, Validating and using Mac Images. File System Artifacts. Communications.
Viewing the file system. File recovery. Sqlite3. Plists. Spotlight! Most Recently Used (MRU) lists. Apple Mail, including a crazy SQLite3 database, attachments, metadata, and mail accounts. Decoding the AddressBook. iMessage. Honestly, whatever we have time for.

Week 5 – ***Feb 20, 2019***
Understanding the MacOS Boot Sequence, Processes, and Time
How MacOS starts running. Examining processes on a running system. How time is set, maintained and displayed.

Week 6 – ***Feb 27, 2019***
Unallocated Space Analysis & Exam Prep
Extracting and identifying artifacts from unallocated space with bulk_extractor, Volatility, and other tools.

Week 7 ***– March 6, 2019***
Mid-Term Exam
Mid-Term Exam will be administered in class.

Spring Break! ***– March 11 — March 17***

Week 8 ***– March 20, 2019***
Users Directory Artifacts Analysis
Identifying user generated artifacts and analyzing these evidentiary items. Specific attention to Keychains, Bluetooth, Bash history, Printer configurations, firewall settings, sharing settings, and application preferences. Privacy, permissions settings, and location services.

Week 9 ***– March 27, 2019***
System and Global Artifacts Analysis
Identify and analyzing artifacts generated in the system and global directories. Special attention to Wifi and network settings, log files, the Unix logfile system, the new Apple logging system, log parsing, and log recovery.

Week 10 ***– April 3, 2019***
Containers and MacOS System Protection. Odds and Ends.
Deep dive into Apple's developing systems for program isolation. If we have time, we'll discuss Photos and Maps.

Week 11 ***– April 10, 2019***
Encryption
Symmetric and asymmetric encryption, including AES, RSA, Elliptic Curves, TLS, PKI, S/MIME, PGP, FDE, and many other acronyms that everyone forensicator should know.

Week 12 ***– April 17, 2019***
iOS, iTunes, and iCloud Contributions
How MacOS interoperates with iOS and iCloud. Decoding iTunes backups.

Weeks 13 ***– April 24, 2019***
Recent Research in Mac Forensics
Students will look at where the Mac industry is going and the forensic challenges associated with this evolution. Presumably some students will present their final projects this week.

Week 14 ***– May 1, 2019 (last day of class)***
Final presentations and Exam Prep

Week 15 ***– May 8 – May 15 — Final Exams!***
Final Exam
Final Exam will be administered in class.

Reference Material:
Forensic Focus http://www.forensicfocus.com/

Apple Support http://www.apple.com/support

Apple Developer Connection http://developer.apple.com/ Fixit Guide Series http://www.ifixit.com/Guide

MacOSXHints http://www.macosxhints.com/

Grading

First (solo) presentation slides advance submission: 2%
First (solo) presentation slides: 5%
First presentation 5%
Second (group) presentation slides advance submission: 2%
Second (group) presentation slides: 10%
Second (group) presentation: 10%
Midterm: 30%
Final 30%
Online Participation (forums) 6%

Up to five extra credit points may be randomly distributed during the course of the semester, like power pellets in the ancient Ms. Pac Man game. Don't count on them!

Canceled Classes - Weather related or otherwise
We will follow GMU's decisions regarding weather related cancellations. If unforeseen issues arise and the instructor is unable to attend class, efforts will be made to communicate a change the venue to online or to cancel as early as possible.

Student Support Resources
George Mason University has a number of academic support and other resources to facilitate student success. Please reference the links below and reach out if any questions arise.

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 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.