GMU DFOR 764: Mac Forensics 2022 Syllabus

Instructor: Kristi Horton

Email: khorton3@gmu.edu

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

Office Hours: By appointment

Description: This is a seminar-style course that presents students with the concepts, tools, and techniques used for forensic analysis of the Macintosh based computers. Classes will consist of lectures on the Macintosh operating system, forensic practice and research, followed by exercises conducted in a lab environment.

Required Materials:

The following items are required Week 2:

- SSD USB 3.0/USB-C drive, 500GB or more.
  (You can partition this and install multiple bootable operating systems.)
- 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 Catalina 10.15.2 and optionally macOS Mojave 10.14.1 from https://developer.apple.com/download/ and OS X Yosemite 10.10.3 from https://developer.apple.com/download/more/.)
- Disk images of Tracy's home computer from the 2012 National Gallery DC Scenario at digitalcorpora.org:
  - http://downloads.digitalcorpora.org/corpora/scenarios/2012-ngdc/tracy-home/tracy-home-2012-07-16-final.E01
  - http://downloads.digitalcorpora.org/corpora/scenarios/2012-ngdc/tracy-home/tracy-home-2012-07-16-final.E02

Required Textbooks:

OSX Incident Response, by Jaron Bradley, Elsevier Syngress, 2016, 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)

Learning Outcomes

After completing the course, students should be able to:

- Describe ways in which Macs are different from computers running Windows and Linux. Explain the Mac boot sequence, the kinds of code running on Mac systems, the kernel, Unix subsystem, and GUI layer.
- Monitor a running Macintosh computer using tools built into the Macintosh operating system, including Activity Monitor,
- Identify the hardware, software, and network configurations of a Macintosh computer under analysis.

- Identify, review and analyze Mac log files.
- Perform disk images of both unencrypted and encrypted file systems. Analyze disk images using a variety of tools and techniques.
- Perform memory acquisitions and analyze memory dumps using Volatility.
- Research a current topic in Mac forensics using the Internet and by performing digital forensics experiments, and write up the results of their work.
- Opine knowingly on the MacOS security model.

Student Deliverables

- 14 Lectures; attendance at every class, unless excused in advance.
- 12 Readings — Do the readings and we will discuss them in class (participation is 10% of grade)
- 4 Labs — Done in class
- Midterm & Final
- Two student presentations

Student Presentations

Presentation #1: Problem Identification (Literature Review) —10 minutes

Each student will present the contents of a paper or substantial blog post about Mac forensics. Topics must be approved in advance. **Three days before the presentation** the student will send slides to the instructor for grading; comments on slides will be provided within 48 hours.

Presentation #2: Group Research Presentation—15 minutes.

This group project is based on original research done in the class, either reporting the application of an open source digital forensics tool to a Mac system, or original research regarding some aspect the Mac operating system or a popular application program. Groups, presentation topics, and student slides must be approved in advance.

Course Schedule

Week 1 – *Jan 26, 2022*

Course Overview/Administrative Items; History; Encryption

Overview of course and syllabus reviewed. Administrative items. What's different about the Mac. History of Mac and Mac Forensics. Booting MacOS (magic keys!). Apple's macOS Security Guide. Current issues and research. Symmetric and asymmetric encryption, including AES, RSA, Elliptic Curves, TLS, PKI, S/MIME, PGP, FDE, and many other acronyms that every forensicator should know.

Readings: Apple macOS Security—Overview for IT | March 2018
Bradley Chapter 1, "Introduction"
Bradley Chapter 2, "Incident response basics"

Lab: Installing MacOS in VMs and Lab System testing

Week 2 – *Feb 2, 2022*

Live System Analysis: Stored Data, Log files and File Structures

We go exploring in the Mac filesystem to see what we can find. Sqlite3. Plists. Spotlight! Most Recently Used (MRU) lists. Apple Mail, including its crazy SQLite3 database, attachments, metadata, and mail accounts. Decoding the AddressBook. Messages. Honestly, whatever we have time for.

Readings Due: Bradley Chapter 3, "Bash Commands"

Lab 1 start: Mac command line and SQL

Week 3 – *Feb 9, 2022*

Live System Analysis: The Storage Layer, Disk Partitioning and Mac File systems

We see how the storage layer really works. HFS, HFS+, APFS, FileVault.

Readings Due: Bradley Chapter 4, "File System"

Lab 1 end: Mac command line and SQL

Week 4 – *Feb 16, 2022*

Disk imaging and working with disk images.

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. Loading, validating and using Mac Images. Viewing the file system. File recovery. Making use of Time Machine.

Readings Due: Recon Lab User's Manual

Lab 2 start: ReconLab and Open Source tools — Find the malware

Week 5 – *Feb 23, 2022*

Live System Analysis: Processes, Network Connections, and other stuff

MacOS boot sequence. Secure Boot. Examining processes on a running system. How time is set, maintained and displayed. Commands for examining a running system.

Readings Due: Bradley Chapter 5, "System Startup and Scheduling"

Lab 2 end: ReconLab and Open Source tools — Find the malware

Week 6 – *March 2, 2022*
Memory Analysis: Memory Capture and Volatility.

Capturing Mac memory. Analyzing Mac memory with Volatility. 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. Loading, Validating and using Mac Images. Viewing the file system. File recovery. Making use of Time Machine.

Readings Due: Bradley Chapter 7, "Memory analysis"
Ligh et al, Chapter 28, "Mac Acquisition and Internals"
Ligh et al, Chapter 29, "Mac Memory Overview"

Lab 3 start: Volatility

Week 7 – *March 9, 2022*
Persistence and Malware

Lab 3 end: Volatility

Mid-Term Exam will be take-home and will be due on March 10th.

Spring Break! ***– March 13 — March 20***

Week 8 – *March 23, 2022*
User 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.

Readings Due: Bradley Chapter 6, "Browser Analysis"
Ligh et al. Chapter 31, "Tracking User Activity"

Lab 4 start: Debugging and Reverse Engineering

Week 9 – *March 30, 2022*
Using dtrace

Analyzing running programs with dtrace and other tools.

Lab 4 end: Debugging and Reverse Engineering

Week 10 – *April 6, 2022*

Readings Due: ***Physical Decrypted Images from Macs with the T2 Chip***

Week 11 – *April 13, 2022*
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.

Lab: Work on final project

Week 12 – *April 20, 2022*
iOS, iTunes, and iCloud Contributions

How MacOS interoperates with iOS and iCloud. Decoding iTunes backups.

Weeks 13 – *April 27, 2022*
Recent Research in Mac Forensics

Where the Mac industry is going and the forensic challenges associated with this evolution. Presumably some students will present their final projects this week.

Lab: Work on final project

Week 14 – *May 4, 2022 (last day of class)*
Final presentations and Exam Prep

Lab time: Present final projects

Week 15 – *May 11 - 18 — Final Exams!*
Final Exam

Final Exam will be administered in class on May 11, 2022

Reference Material:

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

Apple Developer Connection http://developer.apple.com/

iFixit Guide Series http://www.ifixit.com/Guide

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

MacOSXHints http://www.macosxhints.com/

Grading

First (solo) presentation topic approval:	1%
First (solo) presentation slides advance submission:	2½%
First (solo) presentation **and** slides:	9 %
Second (group) presentation topic and group approval:	1 %
Second (group) presentation slides advance submission:	2½%
Second (group) presentation **and** slides:	9 %
Total for presentations:	25 %
Lab #1:	10 %
Lab #2:	5 %
Lab #3:	10 %
Lab #4:	10 %
Total for labs:	35 %
Presentations:	25 %
Labs:	35 %
Class participation:	10 %
Midterm:	15 %
Final	15 %
Grand Total:	100 %

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.

Course materials are not to be distributed or posted by students without the written consent of the instructor.

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.