

Syllabus

Course: CFRS 764: Mac Forensics

Instructor: Ryan L. Chapin

Email: rchapin@gmu.edu

Class Meetings: Tuesday, 4:30 - 7:10, Robinson Hall A - Room 352

Office Hours: By appointment

Required Materials: *(The following items are not required until Week 3)*

250GB+ USB 3.0/FW 800 - [Example](#)

8GB+ USB Flash Drive

iCloud Account - <https://www.icloud.com>

MacOS X License - [Link](#) (Wait until class to download, unless you already have it)

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

Optional:

Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit; ISBN-10:1597492973

Mac Computer: i5 with 8GB of RAM and 500GB HDD (Lab computers will be available)

Description: Presents students with the concepts, tools, and techniques used for forensic analysis of the Macintosh based computers and iOS devices (iPhone, iPad, iPod). Students will learn digital best practices for working with Mac and iOS, be able to successfully recognize the HW and its evidentiary value, and locate/analyze artifacts of interest. Hands-on exercises will be included.

Course will consist of exercises conducted in a lab environment with concurrent lectures

Objectives: This course will present students with the basic tools and techniques used to conduct a Mac and iOS forensic analysis. Students will apply industry best practices to both the collection and subsequent analysis of Mac and iOS systems with an emphasis on hands-on exercises using currently available open-source and commercial tools.

Tentative Course Schedule:

Overview Week 1 - 01 September 2015

Course Overview/Administrative Items; History

Overview of course presented, syllabus reviewed, administrative items discussed. Topic of discussion will include the history of Mac forensics.

Week 2 - 08 September 2015

Recognizing the Hardware

Topics of discussion will include recognizing the Apple HW and understanding use scenarios.

Week 3 - 15 September 2015

Mac Analysis - Setup

Topics of discussion will include recognizing hardware needs, setting up and configuring a Mac to conduct forensic analysis to include file system makeup and the tools to be used.

Week 4 - 22 September 2014

Understanding Live and Dead Imaging

Topics of discussion will include understanding live & dead imaging processes (tools and techniques), automated imaging and acquisition, verifying and safely mounting forensic images as they pertain to the Mac environment.

Week 5 - 29 September 2015

Mac and iOS Incident Response & Imaging

Students will be challenged with hands-on collection and imaging of Mac data.

Week 6 - 06 October 2015

Loading and Validating an Image

Students will learn how to and the necessity of properly validating an image and the loading and parsing of an image. Once the image is parsed, a “quick look” will be conducted to get first impressions of the suspect.

Columbus Day Recess - 13 October 2014

Week 7 - 20 October 2014

Mid-Term Exam

Mid-Term Exam will be administered in class.

Week 8 - 27 October 2014

Users Directory Artifacts Analysis (Part 1 & Part 2)

Students will learn how to identify user generated artifacts and properly analyze these evidentiary items.

Week 9 - 03 November 2014

System and Global Artifacts Analysis (Change for 2015 - Add Global Pt 1 too)

Student will learn how to properly identify and analyze artifacts generated in the system and global directories.

Week 10 - 10 November 2014

Root and Hidden Directories

Students will continue to learn how to identify system and application generated artifacts and properly analyze these evidentiary items.

Week 11 - 17 November 2014

Unallocated Space Analysis

Students will learn how to properly identify unallocated space, analyze unallocated space, and identify artifacts of evidentiary interest.

Week 12 - 24 November 2014

iOS and iCloud Contributions

Students will look at an iOS backup and compare what they have previously learned with the Mac OS. Some time will also be dedicated to identifying iCloud generated artifacts and properly analyzing these evidentiary items.

Weeks 13 - 01 December 2014

The Future of Mac Forensics

Students will look at where the Mac industry is going and the forensic challenges associated with this evolution.

Week 14 - 08 December 2014

Reading Day

Preparations for the Final Exam.

Week 15 - 15 December 2014

Final Exam

Final Exam will be administered in class.

Reference Material:

Apple Examiner <http://www.appleexaminer.com/>

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: Participation: 10% Mid-term: 30% Three Projects: 30% Final: 30%

Canceled Classes - Weather related or otherwise: We will mirror the University regarding weather related cancellations. If unforeseen issues arise and the instructor is unable to attend class, efforts will be made to communicate a change in venue (online) or cancelation no fewer than 24 hours in advance of the next class.

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.

Office of Disability Services: <http://ods.gmu.edu/>

University Policies: <http://universitypolicy.gmu.edu/>