Syllabus

Course: CFRS 764: Mac Forensics

Instructor: Ryan L. Chapin

Email: rchapin@gmu.edu

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

Office Hours: By appointment only

Required Materials: ***You will not need the following items until Week 2***
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 ***- 22 January 2014***
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 ***- 29 January 2014***
Mac Analysis - Setup
Topics of discussion will include setting up and configuring a Mac to conduct forensic analysis to include file system makeup and the tools to be used.

Week 3 ***- 05 February 2014***
Recognizing the Hardware
Topics of discussion will include recognizing the Apple HW and understanding use scenarios.

Week 4 ***- 12 February 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 ***- 19 February 2014***
Mac Incident Response & Imaging
Students will be challenged with hands-on collection and imaging of Mac data.

Week 6 ***- 26 February 2014***
Validating and Loading an Image
Students will learn how to and the necessity of properly validating ~~of~~ an image and the loading and parsing of an image.

Week 7 ***- 05 March 2014***
Mid-Term Exam
Mid-Term Exam will be given.

Spring Break ***- 12 March 2014***

Week 8 ***- 19 March 2014***
Users Directory Artifacts Analysis (Part 1)
Students will learn how to identify user generated artifacts and properly identify and analyze these evidentiary items.

Week 9 ***- 26 March 2014***
Users Directory Artifacts Analysis (Part 2)
Students will learn how to identify user generated artifacts and properly identify and analyze these evidentiary items.

Week 10 ***- 02 April 2014***
System Artifacts Analysis
Student will learn how to properly identify and analyze system generated artifacts.

Week 11 ***- 09 April 2014***
Application Artifacts Analysis (Part 1)

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

Week 12 ***- 16 April 2014***
Application Artifacts Analysis (Part 2)
Students will learn how to identify application generated artifacts and properly identify and analyze these evidentiary items.

Week 13 ***- 23 April 2014***
Unallocated Space Analysis
Students will learn how to properly identify unallocated space, analyze unallocated space, and identify artifacts of evidentiary interest.

Weeks 14 ***- 30 April 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 15 ***- 07 May 2013***
Final Exam
Final Exam will be given 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%

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/