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

Required Materials: None – Material will be provided by the instructor and disseminated via Blackboard

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

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 it evidentiary value, and locate/analyze artifacts of interest. Hands-on exercises 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 iOS systems with an emphasis on hands- on exercises using currently available open-source and commercial tools.

Overview Week 1 ***- 23 January 2013***
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 ***- 30 January 2013***
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 ***- 06 February 2013***
Recognizing the Hardware and Understanding Live and Dead Imaging (Part 1)
Topics of discussion will include recognizing the HW and 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 4 ***- 13 February 2013***
Recognizing the Hardware and Understanding Live and Dead Imaging (Part 2)
Topics of discussion will include recognizing the HW and 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 ***- 20 February 2013***
Mac Incident Response & Imaging Practical
Students will be challenged with hands-on collection and analysis of Mac data.

Week 6 ***- 27 February 2013***
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 ***- 06 March 2013***
Mid-Term Exam
Mid-Term Exam will be given.

Spring Break - No Class ***- 13 March 2013***

Week 8 ***- 20 March 2013***
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 ***- 27 March 2013***
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 ***- 03 April 2013***
System Artifacts Analysis
Student will learn how to properly identify and analyze system generated artifacts.

Week 11 ***- 10 April 2013***
Application Artifacts Analysis (Part 1)
Students will learn how to identify application generated artifacts and properly identify and analyze these evidentiary items.

Week 12 ***- 17 April 2013***
Application Artifacts Analysis (Part 2)
Students will learn how to identify application generated artifacts and properly identify and analyze these evidentiary items.

Week 13 ***- 24 April 2013***
Unallocated Space Analysis
Students will learn how to properly identify unallocated space, analyze unallocated space, and identify artifacts of evidentiary interest.

Weeks 14 ***- 1 May 2013***
The Future of Mac Forensics
Students will look at where the Mac industry going and the forensic challenges associated with this evolution

Week 15 ***- 8 May 2013***
Final Exam
Final Exam will be given.

Reference Material:

References include:
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
Mid-term: 30% 4 Projects: 40% Final: 30%