CFRS 780 – Windows Registry Forensics

Department of Electrical and Computer Engineering

Computer Forensics Program

George Mason University

Summer 2013

Instructor:	Jonathan P. Fowler, EnCE, ACE
E-Mail Address:	jfowler9@gmu.edu
Office Location:	TCOM Adjunct Faculty Offices
Office Hours:	By request only
Class Time:	M/W/F, 7:00-10:05 p.m.
Location:	Nguyen Engineering Bldg., Room 5358

NOTE: All students MUST have a GMU e-mail account and have access to blackboard.gmu.edu. Students must use their MasonLIVE e-mail account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.

Course Description (from GMU catalog):

This course will present students with concepts, tools, and techniques used for a forensic analysis of the Windows registry. Students will first review the structure and layout of the Windows registry and then be introduced to the types of artifacts that can be found within the registry itself. Students will also learn how to evaluate and interpret data from the Windows registry in order to identify specific user activity on the computer. Changes in the Windows registry between different versions of Windows will also be discussed. Hands-on exercises included.

Prerequisites:

CFRS 500, CFRS 661.

Course Objectives:

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

Grading:

Because the majority of forensic examinations conducted result in written reports being generated, grading will be assessed on the following components:

Homework/Hands-on Projects:	35%
Mid-Term Examination:	30%
Final Examination:	30%
Attendance/Class Participation:	5%
TOTAL:	**100%**

Course Material:

The text for the course is listed below. Additional electronic material may be posted through the class Blackboard site – if so, I will send an e-mail to the class informing everyone:

- Windows Registry Forensics, Carvey, Harla, 2011, Elsevier, Inc.

Course Schedule (subject to change):

Date	Topic(s)	Assignments Due
05/20/13	***Course Overview/Administrative Items; Windows Registry Overview***	
05/22/13	***Registry Hives - Overview***	
05/24/13	NO CLASS - HOLIDAY	
05/27/13	***Registry Hives – SAM, Security, NTuser***	Homework Assignment #1
05/29/13	***Registry Hives – System, Software***	
05/31/13	***Basic Registry Analysis – Commercial and Open Source Registry Analysis Tools***	
06/03/13	***Basic Registry Analysis – Post-Mortem Registry Analysis/Review***	
06/05/13	***MID-TERM EXAMINATION***	
06/07/13	***Advanced Registry Analysis – Comparative Registry Analysis***	
06/10/13	***Advanced Registry Analysis – Unallocated/Slack Space in Registry Hives***	Homework Assignment #2
06/12/13	***Advanced Registry Analysis – Malware/APT Analyses***	

06/14/13	***Case Studies – Removable Devices***	
06/17/13	***Case Studies – Tracking/Reconstructing User Activity***	Homework Assignment #3
06/19/13	***FINAL EXAMINATION***	

Academic Integrity:

George Mason University is an Honor Code University; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely.

What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else's work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions.

When in doubt (of any kind) please ask for guidance and clarification.

Disability Policy:

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 the Office for Disability Services (located in SUB1, Room 4205, 703-995-2474, http://ods.gmu.edu) to determine the accommodations you need; and, (2) talk with me to discuss your accommodation needs.