CFRS 763 – Summer 2015 Syllabus
Windows Registry Forensics
George Mason University

Administrative Information

Instructor:	David Loveall
Email:	dloveall@gmu.edu
Office hours:	By appointment
Classes:	T/R, 19:20 – 22:00, Nguyen Engineering Building 1505

Course Description

Presents the concepts, tools, and techniques used for forensic collection, identification, and analysis of the Windows registry; review the structure and layout of the Windows registry and be introduced to the types of artifacts that can be found within; evaluate and interpret data from the Windows registry with emphasis on hand-on exercises. Course will consist of exercises conducted in a lab environment with concurrent lectures (combined total of 3 credits for lab and lecture exercises). *Prerequisites: CFRS 500 and CFRS 661 or permission from instructor.*

Required Skills and Hardware / Software

Students are expected to have an understanding of the following items:

- Working knowledge of Microsoft Windows
- A PC that can run virtual machines supporting Windows 10 (and earlier)
- Knowledge and understanding of digital forensics of offline filesystems

Textbook

Title:	*Windows Registry Forensics*
Authors:	Harlan Carvey
Publisher:	Syngress
Pub. Date:	February 7, 2011
Print ISBN-13:	9978-1597495806

Other Readings

Title:	*Windows Internals, Part 1*
Authors:	Mark Russinovich, David Solomon, Alex Ionescu
Publisher:	Microsoft Press
Pub. Date:	March 25, 2012
Print ISBN-13:	978-0735648739

Title:	*Windows Forensic Analysis Toolkit*
Authors:	Harlan Carvey
Publisher:	Syngress
Pub. Date:	April 10, 2014
Print ISBN-13:	978-0124171572

Topics

Windows registry forensics. Windows specific forensics.

Technology

Because this is a computer classroom, we will frequently be using the internet as a means to enhance our discussions. We will also be using the computers for our in-class lab assignments. Please be respectful of your peers and your instructor and do not engage in activities that are unrelated to the class. Such disruptions show a lack of professionalism.

Goals

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. Analysis and understanding of the context of the registry in the overall operating system will be enhanced through analysis of other Windows specific data stores and structures.

Participation

Throughout the semester there will be hands on exercises and labs to demonstrate the various tools and techniques covered in class. Students are expected to participate in the exercises. In-class assignments are a factor in the overall grade.

Grading

Grades will be assessed on the following components:

40%	Assignments	(Take home assignments)
30%	Midterm	(Multiple choice / short answer test)
30%	Final	(Short paper and presentation)

Assignments

Assignments will be given throughout the course. The material covered will be first discussed in class, and then applied in the homework. Homework may have advanced topics not fully covered in class, but will be discussed in a future class. The advanced problems are for students to go above and beyond. All assignments are due when specified and late submissions will not be accepted. Due to the compressed schedule of the summer course, the assignments will be discussed immediately after they have been submitted. Quizzes may be given throughout the semester to assess comprehension of the material, covering topics discussed in lectures.

The midterm will consist of a multiple choice and short answer test. It will be open book / reference, but **the time to complete will be limited**.

The final will consist of a white paper of approximately four pages and a ten to fifteen minute presentation. Topics will be chosen to avoid overlap with other students, allowing for a month of research.

Important Dates

Please visit http://registrar.gmu.edu/calendars/ and view important dates for the current semester.

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account. Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Academic Integrity

GMU 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. Students are required to be familiar and comply with the requirements of the GMU Honor Code @ http://oai.gmu.edu/the-mason-honor-code/. All assessable work is to be completed by the individual student. Students must NOT collaborate on the project reports or presentation without explicit prior permission from the Instructor.

Disability Accommodations

If you have a learning or physical difference that may affect your academic work, you will need to furnish appropriate documentation to the Office of Disability Services. If you qualify

for accommodation, the ODS staff will give you a form detailing appropriate accommodations for your instructor. In addition to providing your professors with the appropriate form, please take the initiative to discuss accommodation with them at the beginning of the semester and as needed during the term. Because of the range of learning differences, faculty members need to learn from you the most effective ways to assist you. If you have contacted the Office of Disability Services and are waiting to hear from a counselor, please tell me.

Diversity

George Mason University promotes a living and learning environment for outstanding growth and productivity among its students, faculty and staff. Through its curriculum, programs, policies, procedures, services and resources, Mason strives to maintain a quality environment for work, study and personal growth.

An emphasis upon diversity and inclusion throughout the campus community is essential to achieve these goals. Diversity is broadly defined to include such characteristics as, but not limited to, race, ethnicity, gender, religion, age, disability, and sexual orientation. Diversity also entails different viewpoints, philosophies, and perspectives. Attention to these aspects of diversity will help promote a culture of inclusion and belonging, and an environment where diverse opinions, backgrounds and practices have the opportunity to be voiced, heard and respected.

The reflection of Mason's commitment to diversity and inclusion goes beyond policies and procedures to focus on behavior at the individual, group and organizational level. The implementation of this commitment to diversity and inclusion is found in all settings, including individual work units and groups, student organizations and groups, and classroom settings; it is also found with the delivery of services and activities, including, but not limited to, curriculum, teaching, events, advising, research, service, and community outreach.

Acknowledging that the attainment of diversity and inclusion are dynamic and continuous processes, and that the larger societal setting has an evolving socio-cultural understanding of diversity and inclusion, Mason seeks to continuously improve its environment. To this end, the University promotes continuous monitoring and self-assessment regarding diversity. The aim is to incorporate diversity and inclusion within the philosophies and actions of the individual, group and organization, and to make improvements as needed.

Privacy

Students must use their MasonLive email account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.

Schedule

Date		Discussion Topics	Assignment
Week 1	6/2	Introductions, overview and review of the Windows Registry and hive files. Initial hands on exercise for browsing registry.	**Chapter 1**
Week 2	6/4	Tools for registry analysis.	**Chapter 2**
Week 3	6/9	Hands-on exercise extracting and interpreting information from offline registry hives. Intro to programming and scripting for forensic examiners.	**Assignment 1 Issued**
Week 4	6/11	Comparative Windows Registry analysis. Windows Sysinternals tools.	**Assignment 2 Issued**
Week 5	6/16	Unallocated / slack space in Windows Registry hives. Windows PowerShell.	**Assignment 1 Due @ 1920**
Week 6	6/18	Live Windows Registry analysis.	**Chapter 3**
Week 7	6/23	**MIDTERM.** Discussion on final topics.	**Choose topic for Final**
Week 8	6/25	Windows Event Logs. Microsoft Log Parser.	**Assignment 3 Issued**
Week 9	6/30	Windows automatic code execution. Malware detection.	**Assignment 2 Due @ 1920**
Week 10	7/2	Volume Snapshot Service (VSS) / Shadow Copies.	
Week 11	7/7	Active Directory, Domain Policies, Hyper-V, Internet Explorer.	**Assignment 4 Issued**
Week 12	7/9	Windows specific filesystem topics, to include shortcuts, junctions, Access Control Lists, Named / Alternate Data Streams, Recycle Bin / INFO2.	**Assignment 3 Due @ 1920**
Week 13	7/14	Booting offline Windows systems, VHD files. Remote access to Windows. Anti-forensics discussion.	**Chapter 4**
Week 14	7/16	Tracking and reconstructing user activity.	**Assignment 4 Due @ 1920**
Week 15	7/21	Advanced topics / case studies / course review.	
Week 16	7/23	Final Presentations	**Final Paper Due @ 1920**