This syllabus is subject to changes and revisions throughout the course.

CFRS 780 – 001 - Spring 2016
Memory Forensics
George Mason University

Syllabus

Administrative Information:

Instructor:	**Jared Greenhilll**
Email:	jgreenhi@gmu.edu
Office hours:	By appointment, please.
Classes:	Wednesday's – 19.20 – 22.00
Twitter:	@gmumemforensics

Course Description:

CFRS 780-001 – Memory Forensics (3:3:0)
Prerequisites: CFRS 761 (Malware Reverse Engineering) and CFRS 510 (Digital Forensic Analysis), or permission from the instructor. Additionally, students should have a solid understanding of computer operating systems (e.g. CS 471 or equivalent or relevant work experience). This course focuses on memory forensics, specifically the investigation, analysis and acquisition of artifacts that reside in random access memory (RAM). Memory forensics provides an evidentiary goldmine of unique digital artifacts with regards to computer forensics and digital investigations such as intrusions and malware infections.

Required Skills and Related Hardware/Software:

Students **must** have a **working understanding** of the following items:

- Windows and Linux command line knowledge.
- A PC that can run VMWare (v11+). 6+GB ram is recommended.
    - Base OS can be Windows, Linux or OSX.
- Solid understanding of TCP/IP.
- Hex editor (ex. 010, Winhex).
- External storage media to supplement existing PC storage capacity.
    - A 250GB external drive will work fine, the more the merrier.

Tools Leveraged during the course:

- Volatility (Volatiityfoundation.org)
- Ubuntu (Instructor provided VM)
- Python (https://python.org)
- Bulk Extractor (https://github.com/simsong/bulk_extractor)
- Moonsols (win32dd, win64dd, DumpIt) (http://www.moonsols.com/windows-memory-toolkit/)

This syllabus is subject to changes and revisions throughout the course.

Optional Tools:

- IDA Pro (https://www.hex-rays.com)
- Wireshark (https://wireshark.org)
- YARA (https://plusvic.github.io/yara)
- SYSTERNALS Suite (https://technet.microsoft.com/en-us/sysinternals/bb842062)

GMU VMware Downloads:

Students are encouraged to download VMware for the respective operating systems for free:

http://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=57245579-6f24-de11-a497-0030485a8df0&vsro=8&JSEnabled=1

Textbooks:

Required: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory; Michael Hale Ligh, Andrew Case, Jamie Levy and Aaron Walters; Wiley; ISBN 978-1-118-82509-9.

Optional: File System Forensic Analysis, Brian Carrier, Addison-Wesley Professional; ISBN #978-0321268174.

Optional: Windows Internals, Part 1 (6th Edition) (Developer Reference); by Mark Russinovich (Author), David Solomon (Author), Alex Ionescu; Microsoft Press; ISBN #978-0735648739**.** Part I Chapter 1 (Concepts and Tools).

Optional: Windows Internals, Part 2 (6th Edition) (Developer Reference); by Mark Russinovich (Author), David Solomon (Author), Alex Ionescu; Microsoft Press; ISBN #978-0735665873**.** Part II Chapter 10 (Memory Management).

Software repositories and related documentation:

Volatility GitHub:
https://github.com/volatilityfoundation/volatility

Volatility Reference Online:
https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage

Volatility Cheatsheet (2.4):
http://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

This syllabus is subject to changes and revisions throughout the course.

Topics

1. History of Memory Forensics
2. x86/x64 architecture
3. Data structures
4. Volatility Framework & plugins
5. Memory acquisition
6. File Formats – PE/ELF/Mach-O
7. Processes and process injection
8. Volatility plug-in writing
9. Windows registry
10. Command execution and User activity
11. Networking; sockets, DNS and Internet history
12. File system artifacts including $MFT, shellbags, paged memory and advanced registry artifacts
13. Related tools – Bulk Extractor and YARA
14. Timelining memory
15. Recovering and tracking user activity
16. Recovering attacker activity from memory
17. Advanced Actor Intrusions
18. Report writing

Technology

Since we will be in a computer based 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 and may affect your participation grade.

Goal

Over this semester, students will achieve a deep understanding of both memory and forensic artifacts, primarily focusing on the Windows operating system. By the end of the course, students will also be able to triage and parse memory with open-source tools. Finally, an understanding of intrusion and malware investigations will be prioritized, with a focus on incident response and proactive defense. We will heavily supplement lectures with in class practical labs. Learning is a hands on process; this is critical to both our individual skills and class growth.

Grading

Weights	Letter Grades	
(20%) Assignments/Quizzes	A	92-100
(25%) Midterm	A-	90-91
(25%) Group Project	B+	87-89
(30%) Final & Report	B	83-86
	B-	80-82
	C	70-79
	F	0-69

Detail of the grading brake down is as follows:

This syllabus is subject to changes and revisions throughout the course.

Assignments

Quizzes and assignments will be given throughout the course. They are due on the date presented on the syllabus or instructed by the teacher. Each assignment will be relevant to the current topics. Upon receipt of all assignments, they will be discussed in class.

Midterm Test

A midterm test will be an assigned that will test the student's knowledge of the first six weeks of class. This will be a take home test and is expected to be completed by the due date assigned by the teacher.

Final Project

The final project will consist of a technical challenge in which students must analyze and investigate a memory sample. Results will be submitted in a report format and are expected to be both professional in technical acumen and overall delivery.

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 piece of the overall grade. Your opinions and contributions to the classes overall learning are important, this part should be fun! A twitter account was made for this account, feel free to tweet relevant discussions to this account.

Group Project

A group project will be assigned, multiple students will be in each group and research and perform analysis together. The instructor will provide multiple topics to choose from related to memory forensics and digital investigative topics.

Presentation

Groups will present their group projects. Each student is expected to present a portion of the project during this event. While this is not a public speaking course, everyone must be or begin to be comfortable with discussing technical subject matter in front of an audience.

This syllabus is subject to changes and revisions throughout the course.

Spring 2016 Memory Forensics Schedule

Lecture	Date	Topic	Reading Assignments (To be Read/Performed before class!!!)	Assignments Info
Week 1	Jan 20	The focus for this week is a Class introduction and an overview and history of Memory Forensics. We will also review the course syllabus.		
Week 2	Jan 27	Week 2 topics include: OS internals, 32/64bit architecture, paging, addressing, processes, data structures & more.	"The Art of Memory Forensics" Chapters 1 & 2.	
		Lab: Virtual Address Translation		
Week 3	Feb 3	Week 3 provides an introduction and usage of the Volatility Framework, We will discuss and perform a hands on memory acquisition. Additional topics include using Volatility profiles, memory identification/verification, memory formats and related disk based artifacts.	"The art of Memory Forensics" Chapters 3&4. Finish "The Art of Memory Forensics" Chapters 1 & 2 if not completed. If you aren't comfortable with the concepts, re-read and review.	
		Lab: Memory acquisition with FTK imager and Moonsols DumpIt 2.0. Verification testing with Volatility.		
Week 4	Feb 10	Week 4 starts with scanning for objects in memory, Introduction into processes, pool scanning, process structures in Windows, Linux and OSX. DKOM and process enumeration.	"The Art of Memory Forensics" Chapters 5 & 6.	
		Lab: Investigating an unlinked process		
Week 5	Feb 17	Process memory, code injection, packing and compression, PEB. Specifically; hunting malicious processes in memory. Executable file formats (Portable Executable (PE), ELF & Mach-O).	"The Art of Memory Forensics" Chapters 7 & 8.	
		Lab: Analyzing injected code		

This syllabus is subject to changes and revisions throughout the course.

Week 6	Feb 24	This week focuses on Windows event logs, discovering and analyzing Windows registry entries in memory. Additional analysis of persistence mechanism discovery and user and file execution artifacts will be discussed. **Lab1**: Writing a plugin to print network settings from the registry. **Lab2**: Determining the most recently added service on a host.	"The Art of Memory Forensics" Chapters 9 & 10.	Midterm issued (Take home)
Week 7	Mar 2	This week highlights networking artifacts in Windows, Linux and OSX including hidden connections, raw sockets, internet history and DNS cache. We will also discuss Windows based services, and investigating their activity. **Lab**: Examining active connections of a machine.	"The Art of Memory Forensics" Chapters 11 & 12.	
Week 8	Mar 9	Spring Break – Mon. March 7th – Sun. March 13th.	No reading assignment.	Midterm Due Monday March 7th.
Week 9	Mar 16	This week will include a guest speaker – Tentatively Jared Myers from RSA IR. Relevant discussions in DFIR will be made on or around the guest speaker's topic. We will also talk about tools such as Yara and Bulk Extractor. No Lab.	No reading assignment.	Group projects issued.
Week 10	Mar 23	This class focuses on Kernel Forensics. Topics include Windows driver objects and IRPs, Windows device trees, system calls, kernel callbacks and kernel timers. Kernel level rootkits will be discussed.	"The Art of Memory Forensics" Chapters 13.	

		Lab: Examining IRP functions and devices and extracting malicious rootkit code.		
Week 11	Mar 30	This class is the first of two classes on the Windows GUI Subsystem. Topics include session space, Windows stations, desktops, atoms and windows. **Lab**: Finding malicious USB insertion monitoring and investigating sessions and screenshots.	"The Art of Memory Forensics" Chapters 14.	
Week 12	Apr 6	This class is the second of two classes on the Windows GUI Subsystem. Topics include message hooks, user handles, event hooks and the Windows clipboard. **Lab**: Examining GUI hooks and clipboard data in your own created memory sample.	"The Art of Memory Forensics" Chapters 15.	Group Projects due. Final Exam Issued
Week 13	Apr 13	This week takes a deep dive into disk based artifacts in memory. Specifically the NTFS Master File Table ($MFT), leveraging the $MFT in memory based investigations and extracting files from the Windows cache manager. **Lab**: Recovering attacker scripts from the $MFT in memory.	"The Art of Memory Forensics" Chapters 16 & 17.	
Week 14	Apr 20	The second to last class; continued analyzing of disk based artifacts that live in memory. Topics are LINUX/OSX based and cover mounted filesystems, listing files and directories, extracting file system metadata and recovering file contents. Advanced actor case study – instructor presentation about an APT intrusion spanning multiple years stemming from one memory image. **Lab**: Examining files with Linux and OSX.	Reading assignment TBD.	

Week 15	Apr 27	Final class. We'll focus on reconstructing events and tracking user activity. We will also focus on timelining memory to aid in these efforts. **Lab**: Investigating two compromised machines.	"The Art of Memory Forensics" Chapters 18.	Final Exam Due.

This syllabus is subject to changes and revisions throughout the course.

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, and complete and/all preparatory work (including assigned reading!), participate actively in class during lectures, discussions and labs. 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 phone. Email is the preferred method, phone is second. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – Please forward your GMU email to your primary account, and test before the semester begins. Lectures will have corresponding slides, however class will be dynamic and never the same. Please attend class as there is no replacement for not being there. I'm happy to share my phone number on as needed- please reach out to me directly for it.

Academic Integrity and this class

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 if there are any questions or concerns. The principle of academic integrity is taken very seriously and violations are treated as such. 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 my course; class will be conducted with civility and respect for differing ideas, perspectives, traditions and mindsets. Students must be familiar and comply with the requirements of the GMU Honor Code @ http://oai.gmu.edu/the-mason-honor-code-2/. 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.

This syllabus is subject to changes and revisions throughout the course.

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.