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

DFOR 710 – 001 - Spring 2024
Memory Forensics
George Mason University

Syllabus

Administrative Information:

Instructor: **Jared Greenhilll**
Email: jgreenhi@gmu.edu
Office hours: By appointment, please email me.
Classes: Monday's @ 4.30 pm – 7.10 pm Engineering Building Room 1505

Course Description:

DFOR 710-001 – Memory Forensics (3:3:0)
Prerequisites: DFOR 500 (Intro to Forensic Tech & Analysis), DFOR 510 (Digital Forensic Analysis) DFOR 761 (Malware Reverse Engineering) 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+). 8+GB ram is recommended.
    - Base OS can be Windows, Linux or OSX
- An understanding of TCP/IP fundamentals
- Hex editor (ex. 010, Winhex) familiarity
- 100GB storage capacity via PC or external media to store class materials

Tools Leveraged during the course:

- Volatility (https://www.volatilityfoundation.org)
- Ubuntu (https://ubuntu.com/desktop)
- Python (https://python.org)
- Bulk Extractor (https://github.com/simsong/bulk_extractor)
- Surge Collect Pro (https://www.volexity.com/products-overview/surge/)

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

Optional Tools:

- IDA Pro Free Edition (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 (7th Edition) (Developer Reference); by Mark Russinovich (Author), David Solomon (Author), Alex Ionescu; Microsoft Press; ISBN # 978-0735684188**.** 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. Windows registry
9. Command execution and User activity
10. Networking; sockets, DNS and Internet history
11. File system artifacts including $MFT, shellbags, paged memory and advanced registry artifacts
12. Related tools – Bulk Extractor and YARA
13. Timelining memory
14. Recovering and tracking user activity
15. Recovering attacker activity from memory
16. Advanced Actor Intrusions
17. Creation of presentation material & individual presentations in a group setting

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

Technology

Since we will be in a computer based [virtual] 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 solid understanding of both memory and forensic artifacts, 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. Intrusion and malware investigations will be prioritized, with a focus on incident response and proactive defense. Almost all lectures with be complimented with in class practical labs. Learning is a hands-on process; this is critical to both our individual skills and class growth. Holistically my personal goal is that students will take their new skills directly to their job and/or use them to find gainful employment.

Grading

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

Detail of the grading brake down is as follows.

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. They will likely be quiz or graded lab formats.

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.

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.

Final/Group Project/Presentation

The final project will consist of a technical challenge in which student groups must analyze and investigate a memory sample in class in a team format. Results will be submitted the evening of the final. On the last day of class, groups will give a final presentation with a PowerPoint slide deck to be turned in after. The presentation is expected to be both professional in technical acumen and overall delivery. Groups will present their findings to the class in a group presentation format. Each student is required to

present a portion of the groups findings. 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 2022 Memory Forensics Schedule:

Lecture	Date	Topic	Reading Assignments (To be Read/Performed before class!!!	Assignments Info
Week 1	Jan 22	The focus for this week is a Class introduction and overview, introduction and history of Memory Forensics. Why is Memory Forensics important? Introductions, class intro, syllabus.	Read "The Art of Memory Forensics" Chapters 1 & 2. Read and understand the Review materials – "DFOR 710_Week1_Review.pdf"	
Week 2	Jan 29	Week 2 provides an Introduction and usage of the Volatility Framework, we discuss and perform a hands-on memory acquisition. Additional topics include using Volatility profiles, memory identification/verification, memory formats and related disk based artifacts. Review of Ch.1 & Ch.2 slides and concepts as needed. **Lab**: Memory acquisition with FTK imager and Volexity's Surge Collect. Verification testing with Volatility.	"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.	
Week 3	Feb 5	Week 3 starts with an Introduction into processes and moves into scanning for objects in memory. Additional topics include pool scanning and Windows process structures. **Lab**: Investigating an unlinked process	"The Art of Memory Forensics" Chapters 5 & 6.	Quiz 1 issued
Week 4	Feb 12	Week 4 highlights include process memory, code injection, packing and compression and the PEB. Specifically; hunting malicious processes in memory. The portable executable (PE) file format is discussed. **Lab**: Analyzing Injected Code	"The Art of Memory Forensics" Chapters 7 & 8.	Quiz 1 Due

Week 5	Feb 19	Week 5 focuses on Windows event logs. Log criticality, parsing and analysis will be covered. **Lab**: Parsing and examining Windows Event logs in memory.	"The Art of Memory Forensics" Chapter 9.	
Week 6	Feb 26	Topics for this week are focused on the Windows Registry. We will cover analyzing Windows Registry keys, values and meanings in memory. Additional analysis of persistence mechanism discovery and user and file execution artifacts will be discussed. **Lab**: Determining the most recently added service on a machine.	The Art of Memory Forensics" Chapter 10.	
Week 7	Mar 4	Spring Break – No Class!		Midterm issued (Take home)
Week 8	Mar 11	**This class will be likely given remotely.** We will have a Guest Lecture on relevant discussions in Memory Forensics/Digital Forensics and Incident Response (DFIR) space. This class will likely be remote.		Midterm Due
Week 9	Mar 18	This week highlights networking artifacts in Windows 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.	"The Art of Memory Forensics" Chapter 11.	
Week 10	Mar 25	Week 8 focuses on Windows Services and the Windows GUI Subsystem. Topics include session space, Windows stations, desktops, message hooks, user handles, event hooks and the Windows clipboard.	"The Art of Memory Forensics" Chapter 12,14,15.	

		Lab 1: Determining the most recently added service on a host. **Lab 2**: Finding malicious USB insertion monitoring and investigating sessions and screenshots.		
Week 11	Apr 1	**This class will be delivered remotely.** This week takes a deep dive into disk based artifacts in memory. Specifically, the NTFS Master File Table ($MFT) and leveraging the $MFT in memory based investigations and extracting files from the Windows cache manager. **Lab 1**: Translating strings with Volatility. **Lab 2**: Recovering attacker scripts from the $MFT in memory.	"The Art of Memory Forensics" Chapters 16 & 17.	
Week 12	Apr 8	The week focuses on timelining and event reconstruction and tracking user activity. We'll begin analysis on a compromised host. Students will determine the initial infection vector and attempt to understand the extent of compromise. **Lab**: Investigating a compromised host – Sample001.bin	"The Art of Memory Forensics" Chapters 18.	Final Groups Announced!
Week 13	Apr 15	No lecture Given. This class will continue analysis related to week 12 and solve the exercise. **Lab**: Continue investigating compromised host – Sample001.bin		
Week 14	Apr 22	Class Final, lab format, each group is provided with a unique memory sample with questions to be answered. Answers due at the end of class.		Final Exam given in class.

Week 15	April 29	Final Class of the semester. Presentations are delivered by each of the groups.	No reading assignment.	Final Exam PowerPoints & presentations 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 GMU 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 if. 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.

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.