CMSC 654: Memory and Malware Forensics
Syllabus

Instructor:	Dr. Irfan Ahmed
Office Location:	ERB 2323
Office hours:	Monday 3:30 pm to 5:30 pm
	or by appointment.
Email:	iahmed3@vcu.edu
Slack:	We will use Slack for frequent communication.

Overview:
Semester course; 3 lecture hours. 3 credits. This course provides a strong foundation in *memory and malware forensics*, using the Volatility memory forensics framework, an open source toolkit written in Python. Memory forensics involves deep investigation of the contents of volatile computer memory (RAM), which can reveal hidden malware processes, network connections, clipboard contents, evidence of malware, and a wealth of other important evidence. The course ultimately requires you to develop significant skills in operating systems internals (Mac, Windows, Linux), since memory forensics concentrates on the data structures used internally by operating systems (and some userspace applications).

Course Prerequisites:
CMSC 312 - Introduction to Operating Systems, and significant programming experience. You will need to learn some Python, but no previous Python experience is expected.

Class Meeting:
Engineering Building East 1224
Monday and Wednesday
2:00 pm - 3:15pm

Textbook:

- "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory", by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters (Wiley, 2014).

Additional reading material may be assigned in class.

Reference Books:

- "Operating Systems: Internals and Design Principles", by William Stallings (Prentice Hall; ninth edition, 2018)

Grading:

Midterm Examination	15%
Final Examination	15%
Lab Assignments	40%
Research Paper Presentation	10%
Project and Semester Paper	20%

Grading Scale:
The following grading scale is used. I never curve. Grading in college courses is objective and based directly on your performance. Please don't ask me to change your grade on an assignment unless you clearly deserve it and can demonstrate that this is the case.

A	**90-100**	**B**	**80-89**	**C**	**70-79**
D	**60-69**	**F**	**0-59**		

Tests:
There will be one midterm and one final. The final examination is based on the material covered after the midterm. Any missed test will receive a grade of zero unless arrangements are made with me.

Midterm Exam Date: Wednesday, Oct 27, 2021
Final Exam Date: Wednesday, December 15, 2021

Lab Assignments: There will be a number of laboratory assignments in this course. You should consider the due date for each assignment to be a hard deadline. When the due date arrives, turn in what you have. I do give partial credit, but **late submissions are not accepted.** Submission procedures will be discussed in class.

Research Paper Presentation:
You will do a 25 minutes presentation on a recent research paper on memory forensics. I will provide a list of papers.

Presentation slides due: Tuesday, November 9, 2021
Class Presentation: Tuesday, November 10 & 15, 2021

Project and Semester Paper: There will also be a significant, semester-long project, involving creating a case study on analysis of a cybercrime using memory forensics. You will recreate the cybercrime incident on virtual machines, acquire their memory, and perform memory analysis using Volatility. You will get bonus marks if you create your own plugin that new functionality, which current Volatility plugins do not have.

In the end, you will write a six-page DFRWS-style paper describing your research. Teams of up to two students may work on the semester-long project together.

Proposal: ***(Four Marks) –*** *include Name and student IDs of your group members*

Initially you will submit a ***2-page proposal*** for the project that I will review and approve. It should clearly describe the case study including cybercrime to investigate, and how you recreate the environment to obtain relevant memory dumps, and some preliminary analysis steps using Volatility to start working on the case.

Project Deliverables: I expect two deliverables:
1) PowerPoint slides with screenshots on the entire case study ***(15 Marks)***
2) a DFRWS-style paper ***(5 Marks)***

Five bonus marks if you create a new Volatility plugin with new functionality to help with the case study. You can also participate on the Volatility plugin contest, https://www.volatilityfoundation.org/2021. The contest submission deadline is December 31, 2021. Last year's contest projects: https://volatility-labs.blogspot.com/2020/11/the-2020-volatility-plugin-contest-results.html

Important Dates:
Proposal Deadline: Monday October 18, 2021
Project Submission Deadline: Wednesday December 1, 2021 by Noon (before the class)
Project Presentation and Demo: Wednesday December 1, 2021

Class Materials: The lecture slides will be available via blackboard. Be sure to check the blackboard site frequently.

Major Topics Include:

- Introduction to Memory Forensics
- Memory acquisition
- Basic memory forensics
- Processes
- Memory allocation
- Windows GUI subsystem and registry
- Network forensics
- Malware detection
- Deeper kernel forensics (if time permits)
- Application forensics (if time permits)

Tentative Timeline:

Date	**Milestone**
Monday October 18, 2021	Class Project: *Proposal*
Monday, Oct 25, 2021	Exam: *Review before Midterm*
Wednesday, Oct 27, 2021	Exam: *Midterm*
Tuesday, November 9, 2021	Research Paper: *Slides Submission*
Tuesday, November 10 & 15, 2021	Research Paper: *Presentations*
Wednesday December 1, 2021 (by noon before class)	Class Project: *Final Submission*
Wednesday December 1 & 6, 2021	Class Project: *Presentation and Demo*
Monday, December 13, 2021	Exam: *Review before Final Exam*
Wednesday, December 15, 2021	Exam: *Final*

Learning objectives/outcomes

Upon completion of this course, students will:

- Have a firm understanding of state-of-the-art techniques in memory forensics
- Understand physical memory acquisition
- Have a deep understanding of Volatility, a state-of-the-art memory forensics framework
- Be aware of open research problems in memory forensics

Technology Support
Engineering & VCU Resources:

- **Personal Computer Requirement**: For our current system requirements and recommendations, see: https://egr.vcu.edu/admissions/accepted/computer-recommendations/
- **Remote Access to Public Lab computers**: To provide remote access, we use the Citrix App2Go environment to provide full and exclusive control over "the next available" computer in the lab. See this link for more details: https://wiki.vcu.edu/x/Oa0tBg
- **VCU provides a lot of software available for students to download to their personal computers.** For a list of software and the specifics for each, see: https://ts.vcu.edu/software-center/. In particular, Microsoft Office is available free to students.
- **VCU is transitioning to Canvas.** See the Canvas Student Guide at this link: https://community.canvaslms.com/t5/Student-Guide/tkb-p/student
- **For IT help in the College of Engineering**, see our Wikipedia for "student" help at: https://wiki.vcu.edu/display/EGRITHELP
- **VCU's Technology Services (TS) provides support for "central IT" services**. If you have a technical issue with any of the following services, please submit a ticket with VCU Technology Services at https://itsupport.vcu.edu/ or call (804) 828-2227. VCU TS maintains and supports these services and will be able to provide assistance to you.
    - VCU Cisco VPN
    - 2Factor or Dual Authentication (DUO)

  - Blackboard/Canvas
  - Gmail or other Google Apps
  - Zoom videoconferencing
  - VCU App2Go (Application server)
  - Resetting VCU password
- **For IT issues related to College of Engineering teaching and research, email egrfixit@vcu.edu**
- **For loaner Chromebooks for emergency purposes:** See this link for more details: https://vcutsmpc.getconnect2.com/