DFOR 510
Digital Forensics Analysis
Spring 2024

Read this document in its entirety. You are responsible for its contents!

Instructor: Bob Osgood
rosgood@gmu.edu
703-993-5443
Engr 3800 Office Hours Thursday 2:00 PM – 5:00 PM Eastern Time
And, by appointment.

Classes Meet: Thursday 7:20 PM – 10:00 PM
ENGR 5358

The semester for this class is from **1/18/2024 to 5/2/2024**.

Course Description: Explains digital forensics procedures, beginning with initial walk-through and evaluation; identification and collection of potential evidence; preparation of intrusion investigation; static (non-decompilation) and dynamic analysis; application of critical thinking in determination of significance of artifacts; and analysis and reporting of evidence. Covers Python from a digital forensics perspective. This course is your gateway into DFOR. Many of the topics covered in the course are expanded into full courses themselves. There is a deliverable in this course every four days. Please don't get behind. Deliverable links will appear before the due date then disappear when the deadline passes. The syllabus lists deliverable dates.

Everything you need for this class is located on Blackboard. Every lecture is located in a folder in the Course Content section of this class.

You are going to need a decent computer for this class and have Internet access capable of supporting Blackboard. At a bare minimum, a computer with 16GB of memory, at least an I7 processor, and 500 GB hard drive/SSD is required. More is better.

Course Goals: At the conclusion of this course, the student will have learned at an entry level many of various aspects of DFOR as well as be able to use Python to automate DFOR processes.

Honor Code: - The Mason Honor Code is in effect https://oai.gmu.edu/full-honor-code-document/
Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

The material provided in this course is proprietary. Uploading this material anywhere without the express permission of the instructor is strictly prohibited and a violation of the Mason Honor Code.

Course Schedule: (**Subject to Change**)

DELIVERABLE DUE DATES ARE NOT WHEN YOU START WORKING ON THE MATERIAL. IT'S WHEN YOU NEED TO COMPLETE THE MATERIAL AND TURN IT IN.

Week	Topic	Deliverable	Deliverable Due
0	Course Begins – Get Busy	Familiarize Yourself With the Blackboard Site	
1	The DFOR Story Begins		1/18/2024
2	Python 1	See Blackboard Quiz Lecture 1	1/25/2024
3	Hard Drives & File Systems		2/1/2024
4	Python 2	See Blackboard Quiz Lecture 3	2/8/2024
5	Graphic File Images	GI Project – Blackboard	2/15/2024
6	Python 3	Codebat is Due See Blackboard for additional work	2/22/2024
7	Midterm – Blackboard	Blackboard Midterm Course Content Link	2/29/2024
	Spring Recess 3/4-10/2024		
8	VM & Cloud Forensics		3/14/2024
9	Python 4	VMDK Project	3/21/2024
10	Live Response Acquisition	Programming Assignment – Hashing	3/28/2024
11	Python 5	Live Acquisition Project	4/4/2024
12	Unknown Code Analysis -Static Analysis	Programming Assignment Base64	4/11/2024
13	Python 6	Quiz	4/18/2024
14	Unknown Code Analysis – Dynamic Analysis	Programming Assignment Base Conversion Quiz	4/25/2023
15	Final – In Class on Blackboard	Blackboard Final Course Content Link	5/2/2024

Grading:

Quizzes & Assignments:	**30%**
Mid-term:	**20% (Open Book, Notes, and Computer)**
3 Python Projects:	**30%**
Final:	**20% (Open Book, Notes, and Computer)**

I do not use the grading algorithm incorporated in Blackboard. So, please do not ask me questions concerning the way Blackboard grades. Projects will be graded by the GTA. Consult

with the GTA for any questions you may have regarding project grades. I will grade the quizzes and exams, not Blackboard. So, please refrain from grade questions until I have graded the quiz/test.

Projects: There will be three Python projects assigned during the semester as well as other assignments. All non-code projects must be typed, Times Roman 12 point, double spaced, with one-inch margins. All Python projects must be developed in PyCharm using the naming convention identified in the individual projects.

Exams: The format of exams will be a combination of multiple choice, fill-in, and short answer questions. Expect approximately 50 questions per exam. The Final Exam is not cumulative per se; however, knowledge of the material covered in the first half of the semester is integrated into material covered in the second half of the course. The exams will be timed and be open book, notes, and computer.

Course Material: All course material is available on Mason Blackboard.

Software That You Will Need (Free Stuff) (place on your external drive and/or laptop)

Working version of Windows 10/11 either as iron or a VM
FTK Imager (https://www.exterro.com/ftk-imager)
PyCharm Community Version (https://www.jetbrains.com/pycharm/)
Redline (https://www.fireeye.com/services/freeware/redline.html)
HexEdit (https://sourceforge.net/projects/hexedit/)
HxD (https://download.cnet.com/HxD-Hex-Editor/3000-2352_4-10891068.html)

Other tools that will be demonstrated in class:

Procom
Process Explorer
TCPView
RegShot
WireShark
PE Studio
PEView
DIE
Dependency Walker

Required Reading and Reference Material: All reading is incorporated in Blackboard

Va. Cyber Range (VaCR)

You will receive an email from the Va CR. Please log in and confirm your account. The VaCR will provide a Windows and Linux VM that will be available for use during the semester. It's also not a bad idea to have an Ubuntu VM at your disposal just in case. This is a cyber range; certain network features are restricted on these VM's. Port 443 is open. APT (Linux) also now works.

VSE Labs:

All software required for this course is installed on computers in the open student lab in ENGR 1506. Lab hours can be found on the Labs web site, http://labs.vse.gmu.edu . Please remember to save your work to an external drive as any data stored on those computers will not persist after a reboot.

Software downloads:

The Volgenau School subscribes to Microsoft’s DreamSpark and VMWare’s Academic programs which offer free software downloads to our students. All students in VSE eligible courses receive an invitation to each of those programs at the beginning of their first semester in which they are registered for an eligible course.
If you can't find that notification email, please read the relevant Student FAQ on http://labs.vse.gmu.edu for instructions on activating your account or resetting your password. Microsoft does not make Mac versions of most of its software products. Make sure that you have allocated enough memory to your VM. Volgenau School students may obtain a renewable one-year license for VMWare Fusion through a program sponsored by the Volgenau School. Information on that program is in a FAQ on http://labs.vse.gmu.edu.

https://e5.onthehub.com/WebStore/Security/Signin.aspx?ws=0784610b-cd9b-e011-969d-0030487d8897

Student Welcome - This link provides up-to-date information on IT services:

http://labs.vse.gmu.edu/uploads/FacultyFAQ/StudentWelcome.pdf

http://itservices.gmu.edu/downloads/index.cfm.

Microsoft tools may be available for you at:

https://azureforeducation.microsoft.com/devtools

Disability Services:

Students with disabilities who seek accommodations in a course must be registered with the Mason Office of Disability Services (ODS) and inform the instructor, in writing, at the beginning of the semester. See https://diversity.gmu.edu/ada/student-accommodations or call 703-993-2474 to access the ODS.

Note: ALL STUDENTS MUST HAVE GMU CREDENTIALS (EMAIL ACCOUNT) AND HAVE ACCESS TO https://mymasonportal.gmu.edu !!

Note: All Email Correspondence Will Take Place from Your GMU Account to rosgood@gmu.edu!!!
If you email me from an account other than a Mason account (gmu.edu), I may not respond.

Note: All Students Are Responsible for All of the Material in This Course

Good Luck and Have a Great Semester!!!

If you start running into problems during the semester, please come and see me. The earlier the better. Do not wait until the week of the final to raise a challenge.