DFOR 510
Digital Forensics Analysis
Spring 2025

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: Friday 4:30 PM – 7:10 PM
ENGR 1505

The semester for this class is from **1/24/2025 to 5/2/2025**.

Course Description: Explains digital forensics procedures, beginning with initial forensics concepts; identification and collection of potential digital evidence; preparation of intrusion investigations; 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 in the MS DFOR program.

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

You are going to need a decent computer for this class and have Internet access capable of supporting Canvas. At a bare minimum, a computer with 16GB of memory, at least an I7 processor, and a 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 the various aspects of DFOR as well as be able to use Python to automate DFOR processes.

Honor Code: - The Mason Honor Code can be found here: https://academicstandards.gmu.edu/wp-content/uploads/2023/08/George-Mason-University-Honor-Code-2023-2025-final-version-SaveasPDF.pdf

Students at George Mason University pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

The material provided with this course is proprietary. Uploading this material anywhere without the express permission of the instructor is 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 Canvas Site	
1	The DFOR Story Begins		1/24/2025
2	Python 1	Quiz Lecture 1	1/31/2025
3	Hard Drives & File Systems		2/7/2025
4	Python 2	Quiz Lecture 3	2/14/2025
5	VM & Cloud Forensics		2/21/2025
6	Python 3	Codebat is Due	2/28/2025
7	Midterm – In Class Canvas	Midterm Canvas Module Link	3/7/2025
	Spring Recess 3/10-16/2025		
8	Live Response Acquisition		3/21/2025
9	Python 4	VMDK Project	3/28/2025
10	Unknown Code Analysis -Static Analysis	Programming Assignment – Hashing	4/4/2025
11	Python 5	Live Acquisition Project	4/11/2025
12	Unknown Code Analysis – Dynamic Analysis	Programming Assignment Base64	4/18/2025
13	Python 6	Quiz	4/25/2025
14	Cryptography	Programming Assignment Base Conversion Quiz	5/2/2025
15	Final – In Class on Canvas	Final Canvas Module Link	5/9/2025

Grading:

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

I do not use the grading algorithm incorporated in Canvas. So, please do not ask me questions concerning the way Canvas 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 Canvas. So, please refrain from grade questions until I have graded the quiz/test.

Projects: There will be three to four 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 Canvas (https://canvas.gmu.edu).

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 (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:

- Procmon
- Process Explorer
- TCPView
- WireShark
- PE Studio
- PEView
- DIE
- Dependency Walker

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

College of Engineering and Computing (CEC) 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, https://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 CEC subscribes to Microsoft's Azure and VMWare's Academic programs which offer free software downloads to our students. All students in CEC 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 https://labs.vse.gmu.edu for instructions on activating your account or resetting your password. Make sure that you have allocated enough memory to your VM.

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

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

https://its.gmu.edu/find-a-service/

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.