DFOR 510
Digital Forensics Analysis
Fall 2024

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

Instructor: Jim Jones
jjonesu@gmu.edu
703-993-5599
https://ece.gmu.edu/profiles/jjonesu
Office Hours:
Monday 2-4pm (Arlington: Vernon Smith Hall 1305)
Tuesday 2-4pm (Fairfax: ENGR 3253)
and by appointment

Classes Meet: ONLINE Thursday 7:20 PM – 10:00 PM

The semester for this class is from **Aug 26, 2024 - Dec 18, 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 seven 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 Canvas. 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 Canvas. 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 Canvas Site	8/26/2024-8/29/2024
1	The DFOR Story Begins		8/29/2024
2	Python 1	See Canvas Quiz Lecture 1	9/5/2024
3	Hard Drives & File Systems		9/12/2024
4	Python 2	See Canvas Quiz Lecture 3	9/19/2024
5	Graphic File Images	GI Project – Canvas	9/26/2024
6	Python 3	Codebat is Due See Canvas for additional work	10/3/2024
7	Midterm	Midterm	10/10/2024
8	VM & Cloud Forensics		10/17/2024
9	Python 4	VMDK Project	10/24/2024
10	Live Response Acquisition	Programming Assignment – Hashing	10/31/2024
11	Python 5	Live Acquisition Project	11/7/2024
12	Unknown Code Analysis -Static Analysis	Programming Assignment Base64	11/14/2024
13	Python 6	Quiz	11/21/2024
	Thanksgiving Recess Wed. Nov 27 - Sun. Dec 1		
14	Unknown Code Analysis – Dynamic Analysis	Programming Assignment Base Conversion	12/5/2024
15	Final Exam	Final Exam	TBD (12/11/2024-12/18/2024)

Grading:

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

Schema:

A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C	70-79
F	0-69

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 Canvas.

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 Canvas

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

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 jjonesu@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 contact me. The earlier the better. Do not wait until the week of the final to raise a challenge.

Academic Standards
Academic Standards exist to promote authentic scholarship, support the institution's goal of maintaining high standards of academic excellence, and encourage continued ethical behavior of faculty and students to cultivate an educational community which values integrity and produces graduates who carry this commitment forward into professional practice.

As members of the George Mason University community, we are committed to fostering an environment of trust, respect, and scholarly excellence. Our academic standards are the foundation of this commitment, guiding our behavior and interactions within this academic community. The practices for implementing these standards adapt to modern practices, disciplinary contexts, and technological advancements. Our standards are embodied in our courses, policies, and scholarship, and are upheld in the following principles:

- **Honesty:** Providing accurate information in all academic endeavors, including communications, assignments, and examinations.
- **Acknowledgement:** Giving proper credit for all contributions to one's work. This involves the use of accurate citations and references for any ideas, words, or materials created by others in the style appropriate to the discipline. It also includes acknowledging shared authorship in group projects, co-authored pieces, and project reports.
- **Uniqueness of Work:** Ensuring that all submitted work is the result of one's own effort and is original, including free from self-plagiarism. This principle extends to written assignments, code, presentations, exams, and all other forms of academic work.

Violations of these standards—including but not limited to plagiarism, fabrication, and cheating—are taken seriously and will be addressed in accordance with university policies. The process for reporting, investigating, and adjudicating violations is outlined in the university's procedures. Consequences of violations may include academic sanctions, disciplinary actions, and other measures necessary to uphold the integrity of our academic community.

The principles outlined in these academic standards reflect our collective commitment to upholding the highest standards of honesty, acknowledgement, and uniqueness of work. By adhering to these principles, we ensure the continued excellence and integrity of George Mason University's academic community.

Student responsibility: Students are responsible for understanding how these general expectations regarding academic standards apply to each course, assignment, or exam they participate in; students should ask their instructor for clarification on any aspect that is not clear to them.

Accommodations for Students with Disabilities
Disability Services at George Mason University is committed to upholding the letter and spirit of the laws that ensure equal treatment of people with disabilities. Under the administration of University Life, Disability Services implements and coordinates reasonable accommodations and disability-related services that afford equal access to university programs and activities. Students can begin the registration process with Disability Services at any time during their enrollment at George Mason University. If you are seeking accommodations, please visit https://ds.gmu.edu/ for detailed information about the Disability Services registration process. Disability Services is located in Student Union Building I (SUB I), Suite 2500. Email: ods@gmu.edu. Phone: (703) 993-2474.

Student responsibility: Students are responsible for registering with Disability Services and communicating about their approved accommodations with their instructor *in advance* of any relevant class meeting, assignment, or exam.

FERPA and Use of GMU Email Addresses for Course Communication

The Family Educational Rights and Privacy Act (FERPA) governs the disclosure of education records for eligible students and is an essential aspect of any course. **Students must use their GMU email account** to receive important University information, including communications related to this class. Instructors will not respond to messages sent from or send messages regarding course content to a non-GMU email address.

Student responsibility: Students are responsible for checking their GMU email regularly for course-related information, and/or ensuring that GMU email messages are forwarded to an account they do check.

Title IX Resources and Required Reporting

As a part of George Mason University's commitment to providing a safe and non-discriminatory learning, living, and working environment for all members of the University community, the University does not discriminate on the basis of sex or gender in any of its education or employment programs and activities. Accordingly, **all non-confidential employees, including your faculty member, have a legal requirement to report to the Title IX Coordinator, all relevant details obtained directly or indirectly about any incident of Prohibited Conduct** (such as sexual harassment, sexual assault, gender-based stalking, dating/domestic violence). Upon notifying the Title IX Coordinator of possible Prohibited Conduct, the Title IX Coordinator will assess the report and determine if outreach is required. If outreach is required, the individual the report is about (the "Complainant") will receive a communication, likely in the form of an email, offering that person the option to meet with a representative of the Title IX office.

For more information about non-confidential employees, resources, and Prohibited Conduct, please see University Policy 1202: Sexual and Gender-Based Misconduct and Other Forms of Interpersonal Violence. Questions regarding Title IX can be directed to the Title IX Coordinator via email to TitleIX@gmu.edu, by phone at 703-993-8730, or in person on the Fairfax campus in Aquia 373.

Student opportunity: If you prefer to speak to someone ***confidentially***, please contact one of Mason's confidential employees in Student Support and Advocacy (SSAC), Counseling and Psychological Services (CAPS), Student Health Services (SHS), and/or the Office of the University Ombudsperson.