DFOR 772
Forensic Artifact Extraction
Spring 2025

Please read this document in its entirety. You are responsible for its contents.

Instructor: Jim Jones
jjonesu@gmu.edu
703-993-5599 (office); 703-955-1033 (mobile)
https://ece.gmu.edu/profiles/jjonesu
Office Hours: Monday 2-4pm (Arlington: Vernon Smith Hall 1305)
Wednesday 2-4pm (Fairfax: ENGR 3253)
and by appointment

Classes Meet: ENGR 4457 (Fairfax campus), Tuesday 4:30 PM – 7:10 PM, January 21, 2025 – May 5, 2025

(NOTE: We will use the final exam period (Tue 5/13 4:30 PM -7:15 PM) for final project presentations.)

Course Description: Presents tools and techniques for the extraction and processing of digital artifacts from various media and formats. Foundations are presented and examples are developed for Windows, Linux, Mac, and media filesystems, files, RAM, Windows Registry, solid state devices, network traffic, and mobile devices. Emphasis on applications and hands-on exercises.

Course Goals: This course will present students with the foundations of potential forms of digital evidence, including the formats, structure, and creation of artifacts within those forms. The course builds upon that foundation by posing artifact extraction tasks within each of those forms, and guiding students through the development and implementation of solutions to those tasks. Students will acquire the skills to develop their own artifact extraction tools to enable new capabilities or to validate the results of existing tools.

Course Structure: This course meets in person once per week for 2 hours and 45 minutes in a lab classroom. Each class consists of lecture, which will address the necessary technical foundations and programming elements, followed by a hands-on lab exercise. The lab exercises will reinforce the technical foundations to support the weekly homework assignments. The homework assignments are each one element of an integrated digital forensics tool written in Python. Each homework will add a capability to this tool; at the end of the semester, each student will have developed a tool with 12 distinct capabilities related to 12 distinct lecture topics. The last two lectures (classes 13 and 14) have labs but no homeworks so that students may focus the last few weeks of the semester on their projects. The projects are to develop a capability of each student's choosing and integrate the capability with their class tool or with a publicly available tool, e.g., Autopsy, Binary Ninja, EnCase, etc. Project submissions will consist of code, an explanatory writeup and users guide, and short presentation with demonstration.

Honor Code: - The Mason Honor Code is in effect https://academicstandards.gmu.edu/. 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 unless otherwise noted. 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**)

DUE DATES ARE FIRM (11:59PM EST/EDT on the dates noted)

Date/Class		**Topics**	**Assigned**	**Due**
21-Jan	Class 1	Course Intro; Lab/Development Environment	hw1	27-Jan
28-Jan	Class 2	File Systems: FAT32 (portable media)	hw2	3-Feb
4-Feb	Class 3	File Systems: NTFS (Windows)	hw3	10-Feb
11-Feb	Class 4	File Systems: EXT4 (Linux)	hw4	17-Feb
18-Feb	Class 5	File Systems: APFS (MacOS)	hw5	24-Feb
25-Feb	Class 6	Embedded device storage	hw6	3-Mar
4-Mar	Class 7	Memory (Windows); project discussion	hw7	17-Mar
11-Mar	*Spring Break*			
18-Mar	Class 8	Memory (Linux)	hw8	24-Mar
25-Mar	Class 9	Memory (MacOS)	hw9	31-Mar
1-Apr	Class 10	Firmware	hw10	7-Apr
8-Apr	Class 11	Filetypes and structures	hw11	14-Apr
15-Apr	Class 12	Network traffic (pcap)	hw12	21-Apr
22-Apr	Class 13	iOS/Android	project milestone 1	28-Apr
29-Apr	Class 14	Windows Registry	final project	12-May
6-May	*Reading Day*			
13-May	Class 15	Final Project Presentations		

Grading:

14 labs:	35%
12 homeworks:	35%
Project:	30%

Schema:

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

Labs: Each class will include a lab exercise, designed to reinforce the technical foundations presented in the lecture portion of the class. Lab exercises are expected to be completed in class and submitted prior to the end of class, although I will accept lab submissions up to two days after class to allow for occasional unexpected challenges completing the lab in class. The 14 labs are equally weighted and combined are worth 35% of your final grade.

Homeworks: Classes 1-12 each have an associated homework assignment, due at 11:59 PM EST/EDT the day before the next class meeting. Each homework assignment will build on that class's lecture and lab, and will consist of developing a digital forensic capability in Python, testing it, and integrating it with the Python tool that each student develops throughout the semester. The 12 homework assignments are equally weighted and combined are worth 35% of your final grade.

Project: Each student will select and complete a final project. The project will develop a digital forensics capability in Python and will incorporate that capability into their tool developed during the course of the semester, or integrate it with a publicly available platform like Autopsy, Binary Ninja, EnCase, etc. Project submissions will consist of code, an explanatory writeup and users guide, and short presentation with demonstration. The project is worth 30% of your final grade.

Exams: There are no exams in this class.

Course Material: There is no assigned textbook for this class. All course material will be available on Canvas.

Va. Cyber Range (VaCR):

You will receive an email from the VaCR. 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 a 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.

These links provide 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 (Canvas)

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. Please do not wait until the week of the final to raise an issue or 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.