DFOR 772-001
Forensic Artifact Extraction
Spring 2023

Instructor: Dr. Eric Eppley
Email:eeppley@gmu.edu

Office Hours: Immediately after class (Tuesdays 7:30PM, or by appointment)

Classes Meet: Tuesdays 4:30 PM - 7:10 PM, In Person or Synchronous Virtual via Blackboard classroom link

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 guides 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.

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.

Recommended Prerequisites: DFOR 510 and DFOR 661

Grading:	Homework/Hands-on Projects (10/11):	30%
	Labs:	15%
	Midterm:	25%
Final Project:		30%

Homework: There will be eleven homework projects and one final project assigned during the semester. Homework projects are started in class and completed outside of class. Homework projects are equally weighted and are due at 8am EST on Tuesdays. Project due dates are firm, as I will grade and discuss the projects in the subsequent class meeting. Your lowest homework project grade will be dropped.

Midterm Exam: The format of the midterm exam will be a combination of multiple choice, fill-in the blank, and short answer questions. The exam will have a duration of 90 minutes and will be closed book and closed notes.

Completeness: You are expected to complete all assignments on time. Incomplete, late, or missing work will negatively affect your final grade.

Online Lectures: If class is cancelled for weather or similar reasons, we will have an online version of the class. Details will be provided on Blackboard as necessary.

Attendance Policy: You are expected to be in each class, to participate, and to work on class-related tasks only. Unexcused absences or other issues will negatively affect your final grade.

Mason Calendar: https://registrar.gmu.edu/calendars/spring_2023/

The above link will provide you will Mason’s important dates and deadlines.

Code Storage: A USB thumb drive or cloud storage is recommended to hold your code and data. The drive/space does not need to be large.

Personal Computer: You may use your own computer for homework and projects, or you may use the open computer lab. The classroom lab computers are not normally available outside of class time.

Required Reading and Optional Material:

Required Texts (Kindle versions of both are available):

Chan, J. "Learn Python in One Day and Learn It Well" 2nd Edition, 2017.
ISBN-10: 1546488332
ISBN-13: 978-1546488330

Miller, P. & Bryce, C. "Learning Python for Forensics", 2016.
ISBN-10: 1783285230
ISBN-13: 978-1783285235

Additional References (optional):

Carrier, B. "File System Forensic Analysis" (Chapters 8-17)
ISBN-10: 0321268172
ISBN-13: 978-0321268174

Carvey, J. "Windows Forensic Analysis" (Chapters 3-7)
ISBN-10: 1597497274
ISBN-13: 978-1597497275

O'Connor, T.J., "Violent Python" (Chapters 3-4)
ISBN-10: 1597499579
ISBN-13: 978-1597499576

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

How do I get on Blackboard?

-Go to: https://mymasonportal.gmu.edu/webapps/portal/frameset.jsp
-Login with your Mason Credentials
-Click on the Courses tab
-Click on the DFOR-772-001 (Spring 2022) course

How do I get to the online lectures (if necessary)?

-Follow instructions to login into Blackboard
-Click on **Tools**
-Click on **Blackboard Collaborate**
-You should see the current session listed
-Previously recorded sessions are accessed via the **Previously Recorded** Tab

In order for Blackboard to work properly, what do I need loaded on my computer?

-JAVA
-Quicktime
-Flash

Communication: All students must have a GMU email account and access to blackboard.gmu.edu. Please only use GMU email and BlackBoard for class-related communications. I will use one, the other, or both to communicate class-related information.

Name and pronoun use: *If you wish, please share your name and gender pronouns with me and indicate how best to address you in class and via email. I use [he/his] for myself and you may address me as "Dr./Prof. Eppley" in email and verbally.*

GMU Notice: 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.

Fall 2022 Note 1: While there are currently no Covid-19-related university-wide policies that affect teaching and learning, you may find it useful to direct students to the Safe Return to Campus page so they can keep track of any updates and changes.

Moreover, individual faculty may require their students to show a green Mason Covid Health Check notification when they attend an in-person class meeting. You may use the following language in your syllabus. For an editable document with this language and a QR code that will give students quick access to the MCHC site (perhaps for posting outside your classroom door each day), click here.

To support your safety and the safety of everyone in this class, all students are required to complete the Mason COVID Health Check before each class meeting; I [Prof. X] may [will] ask you to show that you have received a "green" notification to participate in class. If you suspect that you are sick, please stay home and contact the faculty member [me] [Prof.. X] about options for making up the missed class.

Fall 2022 Note 2: Mason's Anti-Racism and Inclusive Excellence Implementation Teams continue to work to support our goals for the Mason community. Outreach to and resources for faculty will be a key part of upcoming projects. In the meantime, Stearns Center encourages faculty to continue to commit to anti-racist, inclusive, and equitable practices; if you would like to acknowledge your commitment on your syllabus, please see some recommended language under the University Policies section of this page.

Office of Disability Services: *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 http://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*

Covid-19 Note: Students who have a Covid-related disability should contact the Disability Services office; DS will contact faculty using standard protocols about any students who require accommodations.

Final Instructor Note: I will make every effort not to adjust this syllabus, but I may do so if in the best interests of students and the learning objectives of the course.