CFRS 772
Forensic Artifact Extraction
Spring 2019

Instructor: Jim Jones
Nguyen Engineering Bldg., Room 3241
(e) jjonesu@gmu.edu
(o) 703-993-5599
(c) 703-955-1033
https://ece.gmu.edu/people/full-time-faculty/jim-jones
https://dfdarg.wordpress.com/

Office Hours: Mondays and Wednesdays 3:00 PM – 4:00 PM or by appointment (adjustments noted as necessary at: https://ece.gmu.edu/people/full-time-faculty/jim-jones)

Classes Meet: Tuesdays 4:30 PM - 7:10 PM, Nguyen Room 1505

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.

Honor Code: - The Mason Honor Code is in effect http://oai.gmu.edu/honor-code/masons-honor-code/
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: CFRS 500, CFRS 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.

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: http://registrar.gmu.edu/calendar.html

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.

Lab Computers: In class we will be using lab computers. Please make sure that your computer is working properly prior to the start of class. If your machine is not working, please let me know and switch to another computer.

Open Computer Lab: The open computer lab is located in Engr 1506. Python is installed on these computers.

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 CFRS-772-001 (Spring 2015) 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.

Office of Disability Services: Students with disabilities who seek accommodations in a course must be registered with the GMU Office of Disability Services (ODS) and inform the instructor, in writing, at the beginning of the semester. See http://www2.gmu.edu/dpt/unilife/ods/ or call 703-993-2474 to access the ODS.

Final 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.