CFRS 780
Forensic Artifact Extraction
Spring 2014

Instructor: Jim Jones
Nguyen Engineering Bldg., Room 3241
jjonesu@gmu.edu
(o) 703-993-5599
(c) 703-955-1033

Office Hours: Thursday 1:00 PM – 4:00 PM
or by appointment

Classes Meet: Tuesdays 4:30 PM - 7:10 PM
Nguyen Room 4457

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.

Prerequisites: CFRS 500, CFRS 661

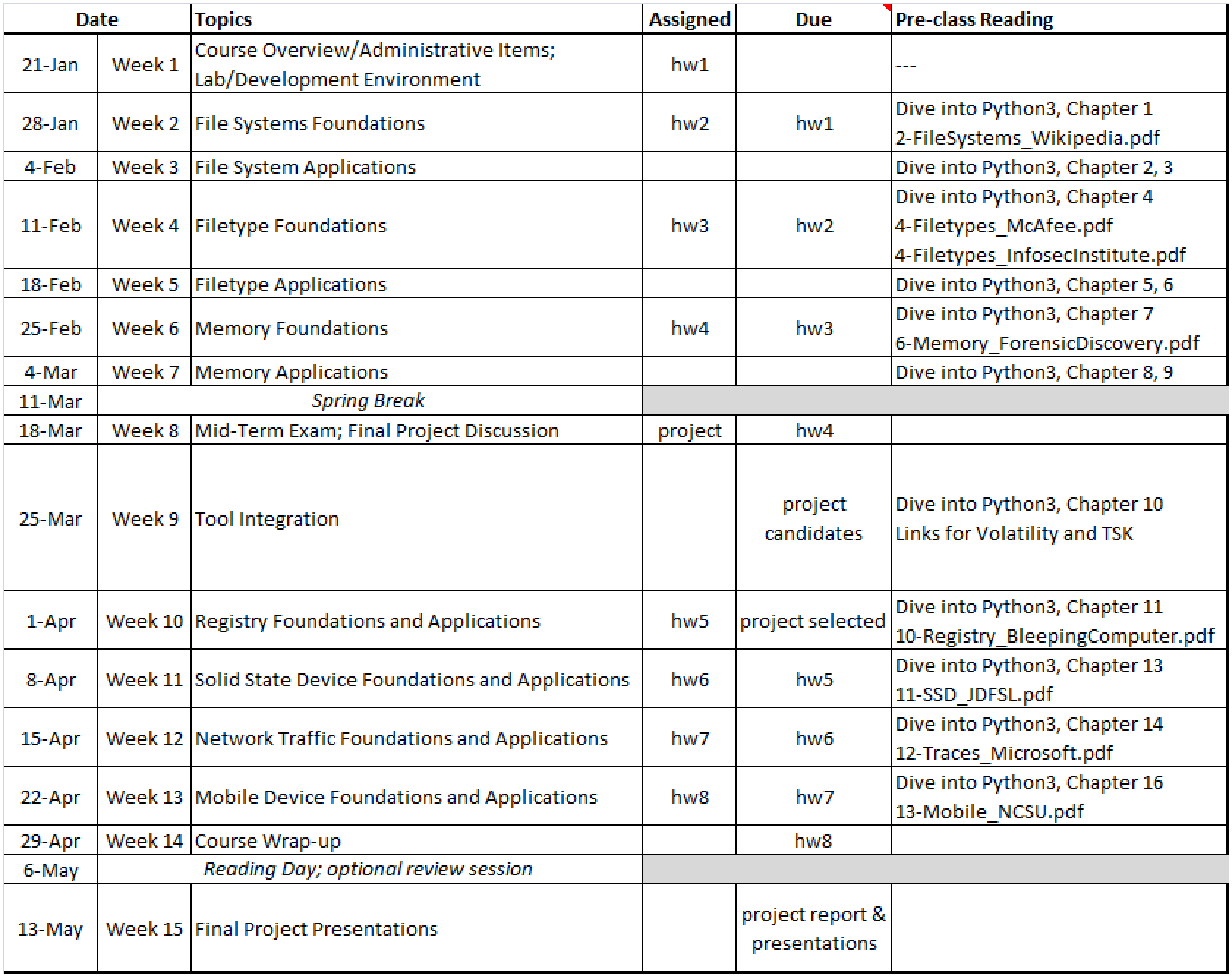
Grading:	Homework/Hands-on Projects (8):	35%
	Midterm:	30%
	Final Project:	35%

Homework: There will be eight homework projects assigned during the semester. Projects are equally weighted and are due at 8am EST on Mondays. Project due dates are firm, as I will grade and discuss the projects in the subsequent class meeting.

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

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

Course Schedule:



Date		Topics	Assigned	Due	Pre-class Reading
21-Jan	Week 1	Course Overview/Administrative Items; Lab/Development Environment	hw1		---
28-Jan	Week 2	File Systems Foundations	hw2	hw1	Dive into Python3, Chapter 1 2-FileSystems_Wikipedia.pdf
4-Feb	Week 3	File System Applications			Dive into Python3, Chapter 2, 3
11-Feb	Week 4	Filetype Foundations	hw3	hw2	Dive into Python3, Chapter 4 4-Filetypes_McAfee.pdf 4-Filetypes_InfosecInstitute.pdf
18-Feb	Week 5	Filetype Applications			Dive into Python3, Chapter 5, 6
25-Feb	Week 6	Memory Foundations	hw4	hw3	Dive into Python3, Chapter 7 6-Memory_ForensicDiscovery.pdf
4-Mar	Week 7	Memory Applications			Dive into Python3, Chapter 8, 9
11-Mar	*Spring Break*				
18-Mar	Week 8	Mid-Term Exam; Final Project Discussion	project	hw4	
25-Mar	Week 9	Tool Integration		project candidates	Dive into Python3, Chapter 10 Links for Volatility and TSK
1-Apr	Week 10	Registry Foundations and Applications	hw5	project selected	Dive into Python3, Chapter 11 10-Registry_BleepingComputer.pdf
8-Apr	Week 11	Solid State Device Foundations and Applications	hw6	hw5	Dive into Python3, Chapter 13 11-SSD_JDFSL.pdf
15-Apr	Week 12	Network Traffic Foundations and Applications	hw7	hw6	Dive into Python3, Chapter 14 12-Traces_Microsoft.pdf
22-Apr	Week 13	Mobile Device Foundations and Applications	hw8	hw7	Dive into Python3, Chapter 16 13-Mobile_NCSU.pdf
29-Apr	Week 14	Course Wrap-up		hw8	
6-May	*Reading Day; optional review session*				
13-May	Week 15	Final Project Presentations		project report & presentations	

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.

Thumb Drive: A USB thumb drive is recommended to hold your scripts. The drive 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:

Title:	Python In A Day
Author:	Wagstaff, R.
Publisher:	CreateSpace Independent Publishing Platform (March 27, 2013)
ISBN-10:	1490475575
ISBN-13:	978-1490475578

Title:	Dive Into Python 3
Author:	Pilgrim, M.
Publisher:	Apress; 2 edition (October 23, 2009)
ISBN-10:	1430224150
ISBN-13:	978-1430224150

Additional per-topic readings will be assigned and provided by the instructor.

Additional References (optional):

Title:	File System Forensic Analysis (Chapters 8-17)
Author:	Carrier, B.
Publisher:	Addison-Wesley Professional; 1 edition (March 27, 2005)
ISBN-10:	0321268172
ISBN-13:	978-0321268174

Title:	Windows Forensic Analysis (Chapters 3-7)
Author:	Carvey, H.
Publisher:	Syngress; 3 edition (February 10, 2012)
ISBN-10:	1597497274
ISBN-13:	978-1597497275

Title:	Violent Python (Chapters 3-4)
Author:	O'Connor, T.J.
Publisher:	Syngress; 1 edition (November 22, 2012)
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-780-001 (Spring 2014) 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.