DFOR 500
Intro to Forensic Technology and Analysis

George Mason University – M.S. in Computer Forensics
Spring 2022

Instructor

Kristi Horton
Email: khorton3@gmu.edu
Office Hours: By email, or video/audio conferencing, by appointment only.

Teaching Assistant

Omoche (Cheche) Agada
Email: oagada@gmu.edu
Office Hours:
Tuesday: 2pm - 4pm
Thursday: 5pm - 7pm
GTA office hours will be conducted virtually.

Location and Time

This is an Asynchronous Online course. All course material is located on Blackboard. You work with the material at your own pace **staying in line with the course timeline in order to not fall behind**.

Course Description

DFOR 500 presents an overview of technologies of interest to forensics examiners. It will introduce, software, analysis, and other aspects required for forensic analysis and related examinations. The course puts an emphasis on operating systems, networking, and programming concepts with a forensic focus. These concepts, technologies and workflows will recur as you continue your education and begin/extend your careers in digital forensics. Other DFOR classes will require a solid understanding of what is taught in this course.

Course Goals

This course focuses on ensuring students gain a fundamental understanding of digital forensic concepts. These include Windows and Linux operating and file system constructs, basic scripting, assembly, networking, triage, and mobile forensic concepts. DFOR 500 also serves as a prerequisite for all other DFOR courses.

Course Materials

The material provided in the 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.

Class Schedule

Lecture #	Topic	Source	Relevant Dates
1	DFOR 500 Class Introduction **Due: 8/25/2022**: Read Syllabus, Test out Blackboard Collaborate Ultra in preparation for first Online discussion Group. (1/25 @7:30PM) **DUE: 8/29/2022**: Install Truxton on VA cyber Range Windows 10 VM	Online video content,	8/23 – 8/29
2	Windows Operating System NTFS (Master File Table) MFT Ex-FAT **Due 9/6/2022**: exFAT quiz, **NTFS Quiz**	Online video content, notes, diagram(s)	8/30-9/5
3	Windows Operating System Processes Services Autorun Registry **Due 9/12/2022**: Windows Registry Assessment Test (timed 10 mins), Windows Process & Services Quiz (timed 5 mins)	Online video content, demo, notes, chart	9/6- 9/12
4	Windows Forensic Artifacts Alternate Data Streams (ADS) Most Recently Used (MRU's) ShellBags Prefetch files Event Logs **DUE: 9/19/2022:** ADS Assignment MRU Assignment ShellBags Quiz Prefetch Exercise	Online video content, notes, diagram(s)	9/13 – 9/19
5	The Windows Command Line (CLI) & PowerShell Windows batch file scripting Accessing Windows CLI and PowerShell **DUE 10/3/2022: Deliverables**: Windows Batch Script Creation – batch files will be graded using the VA Cyber Range Windows 10 VM.	Online video content, notes, diagram(s)	9/20 – 9/26
6	Linux Operating System VFS EXT	Online video content, notes, diagram(s)	9/27 – 10/3

7	Linux Operating System Commands Bash Shell	Online video content, notes, diagram(s), exercise	10/4 – 10/10
8	Linux Artifacts Etc./ Var/log Dmesg Shared Libraries **DUE: 10/17/2022: Deliverables**: Linux quiz (matching) **DUE: 10/17/2022: Deliverables**: Linux Mounting exercise – Please use the Linux Virtual Machine Provided in the VA Cyber Range.	Online video content, notes, diagram(s)	10/11 – 10/17
9	Networking Layer 1 (Physical) Layer 2 (MAC) Layer 3 (IP) Layer 4 (Transport) Layer 5 (Application) **Due 10/24/2022**: Networking quiz	Online video content, notes, diagram(s)	10/18 – 10/24
10	Hashing & Triage What is cryptographic hashing? MD5 SHA1 SHA256 Hash Calc Certutil Md5sum **Due: 10/31/2022**: Hashing quiz, Triage quiz	Online video content, notes, diagram(s), notes	10/25 – 10/31
11	Email Header Analysis Who sent the email Where the email came from Server logs **Due 11/7/2022**: Email header analysis quiz	Online video content, notes, diagram(s), python script usage	11/1 – 11/7
12	Mobile Devices Basic Operation LTE IoS Android **Due 11/14/2022**: Mobile Investigations quiz	Online video content, notes, diagram(s), reading assignment	11/8 – 11/14
13	Assembler What is assembler? Basic assembly language skills **Due: 11/21/2022**: Assembler Project	Online video content, notes, diagram(s), reference documents	11/15 – 11/21
14	**Thanksgiving Recess – No Class**		11/22 – 11/27

15	**Final Exam: 11/29/2022 7:30 PM – 10:00 PM**		11/28 – 12/3

Computer and Network Requirements

As DFOR 500 is an on online class, students need to have access to sufficient and stable Internet bandwidth to effectively communicate with Mason Blackboard and the Virginia Cyber Range.

When a student chooses not to use the VA Cyber Range, the computer used needs to be sufficiently robust to be able to handle the software used for this class. At a **minimum**, the following is recommended.

- I-7 processor
- 16 GB Memory
- 250 GB of **free** storage space, SSD highly recommended.
- USB 3 or better

A Linux VM is provided within the VA Cyber Range. If a student does not use the Cyber Range VM provided, then a Kali Linux VM is required to be run on VMWare. VMWare is available through Mason.

Use of the Virginia Cyber Range (VaCR)

Each student will be provisioned a Windows and Linux VM from the Virginia Cyber Range. You access these VM's via Remote Desktop via the VaCR portal. You will receive an email from the VaCR with access instructions. These VM's shall only be accessed via ports 80 or 443.

Online Discussion Group (ODG)

There will be weekly online discussion group meetings to discuss that week's relevant material. Other related questions are also welcome. It is strongly recommended that all students attend the online discussions. These discussion group meetings are only as good as the questions and comments that you bring to the group. **ODG participation is worth 5% of your total grade.** ODG meetings will be held on **Tuesdays at 7:30 PM**. These group meetings will vary in duration based on the level of participation.

Students may join the ODG by going to the course tools section on the course blackboard page and selecting Blackboard Collaborate Ultra. Instructions for participating in a Blackboard Collaborate Ultra session can be found at:
https://its.gmu.edu/knowledge-base/where-can-i-find-help-on-how-to-use-blackboard-collaborate-ultra/

Grading

Weights		Letter Grades and Percentages			
(65%)	Quizzes & Projects	A	92-100	B-	80-82
(5%)	Class Participation	A-	90-91	C	70-79
(30%)	Final Exam	B+	87-89	F	0-69
		B	83-86		

Quizzes, Projects & Assignments

Quizzes, projects and assignments will be given throughout the course. **They are due on the date presented on the syllabus or as instructed by the teacher**. Each assignment will be relevant to the current topics. Upon receipt of all assignments, they will be discussed in class. They will likely be quiz or graded lab formats. Quizzes, Projects and Assignments are worth 65% of your total grade.

Assignments are to be presented in a professional format. 12-point font is preferred. Screenshots should be readable and fit on the page. All document submissions should include the student's name in the document's filename. **Quizzes and assignments cannot be discussed in the online discussion sessions or the message boards until all students have submitted them.**

Assignments are due by 11:59 PM Eastern time on the due date listed in the class schedule section of this document. No quizzes or assignments will be accepted late unless prior approval of the instructor is obtained. The instructor will only approve late submissions for extenuating circumstances.

Class Participation

Class participation through online discussion groups is **worth 5% of your grade**. If a student is unable to participate live in the discussion sessions, he/she may watch/listen to the recorded session and post questions or comments to the class discussion boards**. Instructions on how to access the session recordings can be found at: https://its.gmu.edu/knowledge-base/introduction-to-blackboard-collaborate-ultra/**

Final Exam

There will be a final exam worth 30% of your grade. The exam will be made available through the course website under the final exam link on the date specified in the Class Schedule section of this document.

Disability Services

Students with disabilities who seek accommodations in a course must be registered with the Mason 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.

All correspondence will be through Mason email. No other email service is permitted.