CFRS 500
Intro to Forensic Technology and Analysis

George Mason University – M.S. in Computer Forensics
Spring 2019

Instructor

Kristi Horton
Email: khorton3@gmu.edu
Office Hours: By email, or in person, by appointment only.

Teaching Assistant

Sarah Davis
Email: sdavis55@masonlive.gmu.edu
Office Hours: By email, Wednesdays & Fridays 4-6 PM Engineering building Room 3702

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

CFRS 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 CFRS 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. CFRS 500 also serves as a prerequisite for all other CFRS courses.

Class Schedule

Lecture #	Topic	Source	Relevant Dates
1	CFRS 500 Class Introduction	Online video content	1/22/2019-1/25/2019
2	Windows Operating System NTFS	Online video content, notes, diagram(s)	1/28/2019-2/1/2019

	(Master File Table) MFT Ex-FAT **Due 2/1/2019**: NTFS quiz, exFAT test		
3	Windows Operating System Processes Services Autorun Registry **Due 2/8/2019**: Windows Registry Assessment Test (timed 10 mins), Windows Process & Services Quiz (timed 5 mins)	Online video content, demo, notes, chart	2/4/2019 – 2/8/2019
4	Windows Forensic Artifacts Alternate Data Streams (ADS) Most Recently Used (MRU's) ShellBags Prefetch files	Online video content, notes, diagram(s)	2/11/2019 – 2/15/2019
5	The Windows Command Line (CLI) & PowerShell Windows batch file scripting Accessing Windows CLI and PowerShell **Deliverables**: Windows Batch Script Creation	Online video content, notes, diagram(s)	2/18/2019 – 2/22/2019
6	Linux Operating System VFS EXT **Deliverables**: Linux quiz (matching), Linux Mounting exercise	Online video content, notes, diagram(s)	2/25/2019 – 3/1/2019
7	Linux Operating System Commands Bash Shell	Online video content, notes, diagram(s), exercise	3/4/19 – 3/8/19
8	Spring Break		3/11/2019-3/17/2019
9	Linux Artifacts Etc./ Var/log Dmesg Shared Libraries	Online video content, notes, diagram(s)	3/18/2019 – 3/22/2019
10	Networking Layer 1 (Physical) Layer 2 (MAC) Layer 3 (IP)	Online video content, notes, diagram(s)	3/25/19 – 3/29/19
11	Networking Layer 4 (Transport) Layer 5 (Application) **Due 4/5/2019**: Networking quiz, discussion	Online video content, notes, diagram(s), notes	4/1/19 – 4/5/19

12	Hashing & Triage What is cryptographic hashing? MD5 SHA1 SHA256 Hash Calc Certutil Md5sum **Due 4/12/19**: Hashing quiz, Triage quiz	Online video content, notes, diagram(s), notes	4/8/19 – 4/12/19
13	Mobile Devices Basic Operation LTE IoS Android **Due 4/19/19**: Mobile Investigations quiz	Online video content, notes, diagram(s), reading assignment	4/15/2019 – 4//19/19
14	Assembler What is assembler? Basic assembly language skills **Due** : Assembler Project	Online video content, notes, diagram(s), reference documents	4/22/19 – 4/26/19
15	Email Header Analysis Who sent the email Where the email came from Server logs **Due 5/3/19**: Email header analysis quiz	Online video content, notes, diagram(s), python script usage	4/29/2019 – 5/3/2019
	Final Exam		5/8/2019 – 5/10/2019

Computer and Network Requirements

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

Your computer 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

An ubuntu and/or Kali Linux VM is required to be run on VMWare. VMWare is available through Mason here:

http://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=57245579-6f24-de11-a497-0030485a8df0&vsro=8&JSEnabled=1

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 the that week's relevant material. Other related questioned 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 7:20 PM. Students should plan on one hour of discussion/participation, but these group meetings will vary in duration based on the level of participation.

Grading

Weights

(65%)	Quizzes & Projects
(5%)	Class Participation
(30%)	Final Exam

Letter Grades and Percentages

A	92-100	B-	80-82
A-	90-91	C	70-79
B+	87-89	F	0-69
B	83-86		

Quizzes & Projects

Quizzes and assignments will be given throughout the course. They are due on the date presented on the syllabus or 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 and Projects are worth 60% of your total grade.

Class Participation

Class participation through online discussion groups is worth 5% of your grade.

Final Exam

There will be a final exam worth 30% of your grade.

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.