DFOR 660 (aka TCOM 660)
Network Forensics
Fall 2024

Read this document in its entirety. You are responsible for its contents!

Instructor: Bob Osgood
rosgood@gmu.edu
703-993-5443
Engr 3800 Office Hours Thursday 2:00 PM – 5:00 PM
and by appointment

Classes Meet:

Day: Saturday
Time Lecture: 10:00 AM – 12:45 AM Engr 5358

Course Description: This course deals with the collection, preservation, and analysis of network-based digital evidence such that this evidence can be successfully presented in a court of law (civil, criminal, and organizational). The relevant federal laws and court decisions will be examined as well as private sector applications. The capture/intercept of digital evidence, NetFlow, volatile/non-volatile data, and the collection and analysis of data and the reporting of such information will be examined.

Course Goals: At the conclusion of this course, the student will have learned the tools, techniques, and laws applicable to presenting network digital evidence. The student will be able to successfully intercept network traffic, collect and analyze volatile data, decipher network traffic, and report this information in a suitable format.

Honor Code: - The Mason Honor Code is in effect https://oai.gmu.edu/wp-content/uploads/2022/08/George-Mason-University-Honor-Code-2022-2023-draft-1.pdf

Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

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.

Mason Calendar: https://registrar.gmu.edu/calendars/fall_2024/

First day of class: **Saturday, 8/31/2024**
Midterm**, 10/12/2024 In Class**
Fall Break**, Saturday, 11/30/2024**
Final: **Saturday, 12/14/2024 In class**

Recommended Prerequisites: TCOM 535 (knowledge of TCP/IP) and working knowledge of a computer language and operating systems (Windows & Linux)

Cross Listed: TCOM 660

Course Schedule: (**Subject to Change**)

Week	Topic	Reading Assignments	Projects Due
1 8/31	Introduction and review of Network Protocols - Application to Network Intercepts	CANVAS Lecture-Networking	
2 9/7	Tapping an Ethernet Network	CANVAS Lecture Tapping an Ethernet Network	LAB IN-CLASS
3 9/14	Federal laws and cases pertaining to the interception of digital evidence will be presented.	CANVAS Lecture Legal Stuff	
4 9/21	Live Collection Windows	CANVAS Lecture Live Collection Windows	Project 1-Due CoB
5 9/28	Live Collection Unix/Linux	CANVAS Lecture Live Collection Unix/Linux	
6 10/5	Building Response Tools – Linux Focus	CANVAS Lecture Building Response Tools Linux Focus	
7 10/12	Midterm – In Class - Timed Exam – Open Book & Notes		Project 2 Due CoB
8 10/19	Collecting Network Based Evidence	CANVAS Lecture - Collecting NBE	
9 10/26	Network Analysis and NetFlow	CANVAS Lecture – Network Analysis …	LAB IN-CLASS
10 11/2	Analyzing Network Traffic		Project 3 – Due CoB
11 11/9	Analyzing Network Traffic	CANVAS Lecture Analyzing Network Traffic	
12 11/16	Analyzing Network Traffic	CANVAS Lecture Analyzing Network Traffic	
13 11/23	Analyzing Network Traffic/Routers and Firewalls	CANVAS Lecture Analyzing Network Traffic & Routers and Firewalls	
11/30	Fall Break		
14 12/7	Routers and Firewalls	Routers and Firewalls – Lab	LAB IN-CLASS JC G010 Project 4 – Due CoB

15 12/14	Final Exam – In Class - Timed Exam – Open Book, Notes, and Computer		

CoB means close of business – end of the day (11:59PM).

Grading:

Mid-term/Quizzes:	**25% (Open Book, Notes, and Computer).**
Final:	**25% (Open Book, Notes, and Computer).**
4 Projects:	**40%**
Labs:	**10%**
Total:	**100%**

Grades will be posted on Canvas, but the Canvas grading algorithm will not be used.

Final grades will be posted to both Canvas and Patriot Web using the standard grading format used by Mason for graduate studies A(+-), B(+-), C, F.

Quizzes: Expect a quiz at the beginning of every class. The quiz will be one question based on the material from the prior class. The quiz will be on Canvas in the module for that week's lecture and will close at 10:05 AM.

Projects: There will be four projects assigned during the semester. Projects must be typed, Times Roman 12 point, double spaced, with one-inch margins. Each project is worth 10% of the total grade. Project 3 is a BASH script that needs to be physically turned in on a thumb drive in an evidence bag with a completed chain of custody form.

Labs: There are three in-class labs in this course worth a **total** of 10 points. There may also be questions on the midterm and final concerning the labs.

Exams: The format of exams will be a combination of multiple choice, fill-in, and short answer questions. Expect approximately 40 – 60 questions per exam. The exams are comingled with labs meaning you need to complete the labs in order to answer questions on the exams. The Final Exam is not cumulative per se; however, knowledge of the material covered in the first half of the semester is integrated into material covered in the second half of the course. The exams will be in class and be timed open book, notes, and computer (no search engines).

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

How do you get on Canvas?

-Go to: https://canvas.gmu.edu
-Login with your Mason Credentials
-Click on the DFOR-660

Thumb Drive (32 GB or higher) – Cost about $10.00.

A Thumb Drive is required for Project 3. This Thumb Drive will be returned to you after Project 3 is graded.

Software That You Will Need (Free Stuff)

Software that you should have loaded on your personal computer/VM include:

-Wireshark	www.wireshark.org (Windows, Mac, or Ubuntu)
-Network Miner	https://www.netresec.com/?page=NetworkMiner (Windows)
-Netwitness Investigator	https://www.netwitness.com/en-us/contact-us/netwitness-investigator-freeware/ (Windows)
-SNORT (offline mode only)	www.snort.org (Ubuntu or Windows)
-Arkime/Moloch	https://arkime.com/ (Ubuntu)
-Argus	https://openargus.org (Linux)

Be careful of weaponize sites. Know who you are downloading from.

VM's – VM of Ubuntu (**23.x** version) is required.

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. Truxton, Wireshark, and other tools are installed on these machines.

Required Reading and Reference Material:

Multiple books and sources are used to create this course. No one book is used exclusively. Of these, two are technically required text, but the Canvas site is self-contained meaning everything you need for this class can be found within Canvas.

Required: The Practice of Network Security Monitoring, Richard Bejtlich, No Starch Press, ISBN: 978-1-59327-509-9 (**Bejtlich**)

Required: Wireshark Network Analysis 2nd Ed, Laura Chappell, Chappell University, https://www.chappell-university.com/books, ISBN 978-1-893939-94-3 (**Chappell**)

Optional: Network Forensics, Davidoff and Ham, Prentice Hall, ISBN 978-0-13-256471-7

Optional: Mastering Windows Network Forensics and Investigation 2nd Edition; Anson, Bunting, Johnson, and Pearson; Sybex, 2012; ISBN: 978-1-118-16382-5 (**ABJP**)

Optional: Windows Forensic Analysis, Harlan Carvey, Syngress, ISBN #9781597494229

Optional: Real Digital Forensics; Jones, Bejtlich, and Rose; Addison Wesley; ISBN #0321240693 (**JBR**)

Optional: Wireshark & Ethereal Packet Sniffing; Orebaugh, Ramirez, and Beale; Syngress; ISBN #1597490733

Optional: Incident Response & Computer Forensics, Second and Third Editions; Kevin Mandia, Matt Pepe, and Jason Luttgens; McGraw Hill; ISBN #007222696X (2nd Ed), #9780071798686 (3rd Ed)

Optional: Web Security; Mike Shema; Osborne; ISBN #0072227842

Optional: Cisco Router and Switch Forensics; Dale Liu; Syngress; ISBN #9781597494182 (**Liu**)

Optional: Practical Malware Analysis; Sikorski and Hinig; No Starch Press; ISBN # 9781593272906

References from the Web include the following sites:

U. S. Congress: http://www.house.gov
Cert: http://www.cert.org
Cisco: http://www.cisco.com
TechNet: https://docs.microsoft.com/en-us/
Sourceforge.net: http://sourceforge.net
CCIPS https://cybercrime.gov

Lab resources and other important information can be found at https://labs.cec.gmu.edu. Software for personal laptops can be found at https://labs.vse.gmu.edu/index.php/FAQ/FAQ

Visio:

Visio is a Microsoft Office product that you should all be familiar with.

Visio can be purchased @ the Mason Computer Store @ a reduced price, you can use the free Visio viewer (with limited functionality), you can use any of the open Mason computer labs since they all have Visio, or you can obtain Visio through **Microsoft Downloads**. You can also buy Visio on Amazon for about $100.00. There are also free tools that can read/manipulate Visio files. https://clickup.com/blog/microsoft-visio-alternatives/ is a site that list such tools. I do not recommend any tool per se except for Visio.

CEC Labs:

All software required for this course is installed on computers in the open student lab in ENGR 1506. Lab hours can be found on the Labs web site, https://labs.cec.gmu.edu . Please remember to save your work to an external drive as any data stored on those computers will not persist after a reboot.

Student Welcome - This link provides up-to-date information on IT services:

http://itservices.gmu.edu/downloads/index.cfm.

Microsoft tools may be available for you at:

https://azureforeducation.microsoft.com/devtools

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 https://ds.gmu.edu/ or call 703-993-2474 to access the ODS.

Note: ALL STUDENTS MUST HAVE GMU CREDENTIALS (EMAIL ACCOUNT) AND HAVE ACCESS TO CANVAS.

Note: All Email Correspondence Will Take Place From Your GMU Account to rosgood@gmu.edu!!!

Note: All Students Are Responsible for All of the Material in This Course

Projects 1, 2, and 4 will be delivered by you through Canvas. Project 3 must be physically handed in.

Good Luck and Have a Great Semester!!!

Student Contract

As a student in this class:

1. This course is extremely comprehensive, but no individual topic is overwhelming per se. You need to be prepared, keep up with the course material, and learn how to apply what is being taught.

2. Be ready for class. Review the information for the class in Canvas prior to attending class and be prepared to discuss, participate, and get involved.

3. Make sure that you have all of the required VM's, and tools properly installed prior to any use for class labs or projects.

4. The instructor and graduate teaching assistant (GTA) will provide assistance in this course, however, neither is your IT support team. You are responsible for maintaining your own computer systems, virtual machines, and software installs.

If you start running into problems during the semester, please come and see me. The earlier the better. Do not wait until the week of the final to raise a challenge.