

# CFRS 660

## Network Forensics

### Fall 2017

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

**Instructor:** Bob Osgood

[rosgood@gmu.edu](mailto:rosgood@gmu.edu)

Engr 3255 Office Hours Thursday 2:00 PM – 4:00 PM  
Saturday 8:00 AM – 9:00 AM (CFRS 660 Students Only)  
And also by appointment

**Classes Meet:**

In Class Section
<b>Day: Saturday</b>
<b>Time: 9:00 AM – 11:45 AM</b>
<b>Where: Engr 5358</b>

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

**Course Goals:** At the conclusion of this course, the student will have learned the laws applicable to presenting network digital evidence in a court of law. 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.

**Prerequisites:** TCP/IP and Network Routing (TCOM 535 and TCOM 515)

**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.

Mason Calendar: <http://registrar.gmu.edu/calendars/>

First day of class: Saturday, 9/2/107

No class: Saturday, 11/25/2017 (Thanksgiving Break)

Final: Saturday, 12/16/2017

**Prerequisites:** TCOM 535 and working knowledge of a computer language and operating systems (Windows & Linux)

**Cross Listed:** TCOM 660

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

<b>Week</b>	<b>Topic</b>	<b>Reading Assignments</b>	<b>Projects Due</b>
1	L-1 Introduction and review of Network Protocols Application to Network Intercepts	Notes from Blackboard Chappell Ch 1 & 2 Bejtlich Ch 2	
2	L-2 Tapping an Ethernet Network		
3	L-3 Federal laws pertaining to the interception of digital evidence will be presented.	Notes and pdf's from Blackboard <a href="http://www.house.gov">www.house.gov</a> <a href="http://www.cybercrime.gov">www.cybercrime.gov</a>	
4	L-4 Incident Response Windows	ABJP Ch 1	Project 1- Due 9/23/2017
5	L-5 Incident Response Unix/Linux	JBR Ch 2	
6	L-6 Collecting Network Based Evidence	Chappell Ch 3 & 4 Bejtlich Ch 1	
7	L-7 Building Response Tools	JBR Ch 16	Project 2 – Due 10/14/2017
8	Midterm – In Class - 2 Hour Timed Exam – Open Book & Notes		
9	L-8 Unknown Code Analysis	ABJP Ch 10	
10	Network Analysis and NetFlow	Davidoff and Ham Ch 4&5	
11	L-10-13 Analyzing Network Traffic	Chappell Ch 28 & 29	Project 3 – Due 11/11/2017
12	L-10-13 Analyzing Network Traffic	Chappell Ch 30 & 31 Bejtlich 6 & 7	
13	L-10-13 Analyzing Network Traffic	Bejtlich Ch 7	
14	L-10-13 Analyzing Network Traffic	Bejtlich Ch 7	
14	L-12 Routers/Firewalls	Notes from Blackboard Liu – Cisco Router & Switch Forensics	Project 4 – 12/9/2017
15	Final Exam - In Class - 2 Hour Timed Exam – Open Book, Notes, and Computer		

**Grading:**      **Mid-term:**              **30% (Open Book, Notes, and Computer)**  
**4 Projects:**              **40%**  
**Final:**                      **30% (Open Book, Notes, and Computer)**

**Projects:**      There will be four projects assigned during the semester. All projects must be typed, Times Roman 12 point, double spaced, with one inch margins. Each project will have a **maximum** length not including diagrams and bibliography. Each project is worth 10% of the total grade.

**Exams:**      The format of exams will be a combination of multiple choice, fill-in, and short answer questions. Expect approximately 50 – 70 questions per exam. 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 have a duration of 2 hours and be open book, notes, and computer.

**Online Lectures:** In certain situations, we will have class online via Blackboard Collaborate. You will be contacted by email ahead of time should a class be held online. Online classes will be recorded and saved for later review.

**Mason Calendar:** <http://registrar.gmu.edu/calendar.html>

The above link will provide you with Mason's important dates and deadlines.

**Course Material:** All course material is available on Mason Blackboard.

How do you 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-660

How do I get to the online lectures?

- Follow instructions to login into Blackboard
- Click on **Tools**
- Click on **Blackboard Collaborate Ultra**
- You should see the current session listed
- Previously recorded sessions are accessed via the **Previously Recorded Tab**

**External USB Drive Required (500 GB or higher)**

An External USB drive is required in order to maintain your software and virtual machines.

**Thumb Drive or SD card (32 GB or higher)**

A Thumb Drive/SD card 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) (place on your external drive and/or laptop)**

Software that you should have loaded on your personal computer include

- Wireshark                      [www.wireshark.org](http://www.wireshark.org)
- Network Miner                [sourceforge.net/projects/networkminer/](http://sourceforge.net/projects/networkminer/)
- Microsoft Message Analyzer <https://www.microsoft.com/>
- Netwitness Investigator      EMC
- SNORT (offline mode only) [www.snort.org](http://www.snort.org)

-Xplico	<a href="http://www.xplico.org">www.xplico.org</a>
-Process Monitor	Technet
-Process Explorer	Technet
-TCPView	Technet
-PEID	Technet
-Dependency Walker	Technet
-Mandiant RedLine	Fireeye (Mandiant)
-Autopsy	<a href="http://www.autopsy.com/">http://www.autopsy.com/</a>
-FTK Imager	<a href="http://accessdata.com/">http://accessdata.com/</a>

These tools are available on Blackboard or if you wish the latest and greatest, you can just Google for the tool.

**VM's** – VM's of Kali and Ubuntu are 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. BlackLight, EnCase, FTK, Nuix, Axiom, and Truxton as well as 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 required text. For the purpose of exam preparation, the Blackboard notes are stressed; however, they are notes. Please verify the accuracy of the notes.

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

**Required:** Wireshark Network Analysis 2<sup>nd</sup> Ed, Laura Chappell, Chappell University, [www.wiresharkbook.com](http://www.wiresharkbook.com), 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 2<sup>nd</sup> 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:** Mastering Windows Network Forensics and Investigation; Anson and Bunting; Sybex; ISBN #9780470097625

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

**Optional:** Incident Response & Computer Forensics, Second and Third Editions; Kevin Mandia, Chris Prorise, & Matt Pepe; McGraw Hill; ISBN #007222696X (2<sup>nd</sup> Ed), #9780071798686 (3<sup>rd</sup> 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: <http://technet.microsoft.com/en-us/default.aspx>

Sourceforge.net: <http://sourceforge.net>

Perl: [www.perl.org](http://www.perl.org)

Python: [www.python.org](http://www.python.org)

Foundstone: [www.foundstone.com](http://www.foundstone.com)

FireEye: [www.mandiant.com](http://www.mandiant.com)

**Microsoft Downloads:**

This course uses Microsoft software available at no charge through the Microsoft DreamSpark program. You should have received notification of your access to this program when you first registered for a course in the Volgenau School of Engineering. If you can't find that notification email, please read the DreamSpark FAQ on <http://labs.vse.gmu.edu> for instructions on activating your account or resetting your password.

**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, Mason Virtual Computing Lab (<http://www.vcl.gmu.edu>), or you can obtain Visio through **Microsoft Downloads**.

**VSE 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, <http://labs.vse.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.

**Virtual Computing Lab:**

Software for this course has been installed on the Mason Virtual Computing Lab (VCL), run by Mason's ITS. The VCL allows you to run remote sessions through your own computer. You can initiate a VCL session through <http://www.vcl.gmu.edu> and that site also has a link for instructions on its use. Please remember to save all of your work on a drive separate from the virtual machine as the entire virtual machine disappears after you exit.

## **Software downloads:**

The Volgenau School subscribes to Microsoft's DreamSpark and VMWare's Academic programs which offer free software downloads to our students. All students in VSE eligible courses receive an invitation to each of those programs at the beginning of their first semester in which they are registered for an eligible course. If you can't find that notification email, please read the relevant Student FAQ on <http://labs.vse.gmu.edu> for instructions on activating your account or resetting your password. Microsoft does not make Mac versions of most of its software products. If you have a Mac, you will have to use Boot Camp, VMWare Fusion, or a Virtual Machine product and then install Windows. Volgenau School students may obtain a renewable one year license for VMWare Fusion through a program sponsored by the Volgenau School. Information on that program is in a FAQ on <http://labs.vse.gmu.edu>. There are also some hints for Mac users on getting Microsoft Windows in the Macintosh Tips FAQ. Other software downloads, including anti-virus software and SSH clients, can be found on the Mason ITS site at <http://itservices.gmu.edu/downloads/index.cfm>.

Mason VMWare link is below

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

## **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.**

**Note: ALL STUDENTS MUST HAVE GMU CREDENTIALS (EMAIL ACCOUNT) AND HAVE ACCESS TO <https://mymasonportal.gmu.edu> !!**

**Note: All Email Correspondence Will Take Place From Your GMU Account to [rosgood@gmu.edu](mailto: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 Blackboard. Project 3 must be physically handed in.**