CFRS/TCOM 660
Network Forensics
Fall 2012

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

Instructor: Bob Osgood
rosgood@gmu.edu
Engr 3255 Office Hours Monday 2:00 PM – 4:00 PM
Wednesday 2:00 PM – 5:00 PM

Classes Meet:

In Class Section	Distance Learning Section
Day: Monday	**Day: Wednesday**
Time: 4:30 PM – 7:10 PM	**Time: 7:20 PM – 10:00 PM**
Where: Engr 1505	**Where: Online (Blackboard Collaborate)**

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 analysis of audit trails, the recordation of running processes, 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 analyze logs, decipher network traffic, and report this information in a suitable format.

Prerequisites: TCOM 509/529 and working knowledge of a computer language

Cross Listed: TCOM 660

Course Schedule: (Subject to Change)

Abbreviations: DL – Distance Learning Class
BM - Brick and Mortar Class

Week	Date	Topic	Reading Assignments	Projects Due
1	8/27/2012 BM 8/28/2012 DL	L-1 Introduction and review of Network Protocols Application to Network Intercepts	Notes from Blackboard	
2	9/3/2012 BM	Labor Day - No Class		
3	9/5/2012 DL 9/10/2012 BM	L-2 Federal laws pertaining to the interception of digital evidence will be presented.	Notes from Blackboard www.house.gov www.cybercrime.gov	
4	9/12/2012 DL 9/17/2012 BM	L-3 Incident Response Windows	Jones Ch 1/Carvey Ch 1	
5	9/19/2012 DL 9/24/2012 BM	L-4 Incident Response Unix/Linux	Jones Ch 2	Project 1
6	9/26/2012 DL	L-5 Collecting Network Based Evidence	Jones Ch 3	

	10/1/2012 BM			
7	10/3/2012 DL 10/9/2012 BM	L-6 Building Response Tools – Class Meets on Tuesday	Jones Ch 16	
8	10/10/2012 DL 10/15/2012 BM	Midterm – On campus for both DL and B&M class	In Class Both DL and BM	
9	10/17/2012 DL 10/22/2012 BM	L-7 Email Analysis	Notes	Project 2
10	10/24/2012 DL 10/29/2012 BM	L-8 Unknown Code Analysis	Jones Chs 13, 14,15/Carvey Ch 6	
11	10/31/2012 DL 11/05/2012 BM	L-9 Windows Memory Analysis and Persistence	Carvey Ch 3/Ch 4	
12	11/07/2012 DL 11/12/2012 BM	L-10 Analyzing Network Traffic	Jones Ch 4 & Orebaugh	Project 3
13	11/14/2012 DL 11/19/2012 BM	L-11 Analyzing Network Traffic	Jones Chapter 5 & Orebaugh	
14	11/21/2012 DL	Thanksgiving Recess – No Class		
15	11/26/2012 BM 11/28/2012 DL	L-12 Routers/Firewalls	Handout/Liu	
16	12/3/2012 BM 12/5/2012 DL	L-13 Logs	Carvey Ch 5	Project 4
17	12/10/2012 BM 12/12/2012 DL	Reading Day – No Class Final Exam DL Class – On Campus		
18	12/17/2012 BM	Final Exam B&M – In Class	In Class	

Grading: **Mid-term:** **30%** **DL students are required to come to campus to take exams.**
4 Projects: **40%**
Final: **30%** **DL students are required to come to campus to take exams.**

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.

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 TCOM-660-1/CFRS-660-01(Fall 2012) course

I'm DL student. How do I get to the online lectures?

-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 right, what do I need loaded on my computer (This is especially true for DL students)

-JAVA
-Quicktime
-Flash

Software That You Will Need (Free Stuff)

Software that you should have loaded on your personal computer include (This is especially true for DL students)

-Wireshark	www.wireshark.org
-Network Miner	sourceforge.net/projects/networkminer/
-SNORT (offline mode only)	www.snort.org
-Process Monitor	Technet
-Process Explorer	Technet
-TCPView	Technet
-PEID	Technet
-Dependency Walker	Technet

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

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.

DL Students are always welcome to sit in on the Monday class and come to campus to use the open lab ENGR 1506

Required Reading and Reference Material:

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

Required: Real Digital Forensics; Jones, Bejtlich, and Rose; Addison Wesley; ISBN #0321240693

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 Edition; Kevin Mandia, Chris Prosise, & Matt Pepe; McGraw
Hill; ISBN #007222696X

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

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

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
Python: www.python.org
Foundstone: www.foundstone.com
Mandiant: www.mandiant.com

The Mason MSDN Academy link below is where you can get Visio

http://msdn05.e-academy.com/elms/Storefront/Home.aspx?campus=gmu_bsit

Mason VMWare link is below

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

Note: ALL STUDENTS MUST HAVE A GMU EMAIL ACCOUNT AND HAVE ACCESS TO BLACKBOARD.GMU.EDU!!!

ALL COMMUNICATION WILL BE THROGH GMU EMAIL AND NOT BLACKBOARD EMAIL OR ANYOTHER EMAIL ACCOUNT!!!

ALL PROJECTS WILL BE TURNED IN DURING CLASS. NO BLACKBOARD SUBMISSIONS FOR THE B&M CLASS.

THE DL CLASS WILL SUBMIT PROJECTS 1, 2, AND 4 BY EMAIL. PROJECT 3 MUST BE HAND DELIVERED TO ENGINEERING ROOM 3255 or ENGR 3300