CFRS/TCOM 660  
Network Forensics  
Spring 2013

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 – 5:00 PM  
Tuesday 2:00 PM – 5:00 PM  
and also by appointment

**Classes Meet:**

<table>
<thead>
<tr>
<th>In Class Section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Day:</strong> Tuesday</td>
</tr>
<tr>
<td><strong>Time:</strong> 7:20 PM – 10:00 PM</td>
</tr>
<tr>
<td><strong>Where:</strong> Engr 5358</td>
</tr>
</tbody>
</table>

**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 intercept network traffic, analyze logs, decipher network traffic, and report this information in a suitable format.

**Honor Code:** - The Mason Honor Code is in effect [http://oai.gmu.edu/honor-code/masons-honor-code/](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.

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

**Cross Listed:** TCOM 660

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

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading Assignments</th>
<th>Projects Due</th>
</tr>
</thead>
</table>
| 1    | 1/22/2013 | L-1 Introduction and review of Network Protocols  
Application to Network Intercepts | Notes from Blackboard  
Chappell Ch 1 & 2  
ABJP Ch 2 & 5 |              |
| 2    | 1/29/2013 | L-2 Federal laws pertaining to the interception of digital evidence will be presented. | Notes from Blackboard  
www.house.gov  
www.cybercrime.gov |              |
<p>| 3    | 2/5/2013  | L-3 Incident Response Windows                                          | ABJP Ch 1                                                 |              |
| 4    | 2/12/2013 | L-4 Incident Response Unix/Linux                                       | JBR Ch 2                                                  | Project 1    |
| 5    | 2/19/2013 | L-5 Collecting Network Based Evidence                                  | Chappell Ch 3 &amp; 4                                          |              |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Assignments</th>
<th>Textbook/Notes</th>
<th>Project/Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>2/26/2013</td>
<td>L-6 Building Response Tools</td>
<td>JBR Ch 16</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>3/5/2013</td>
<td>Midterm – In Class - 2 Hour Exam – Open Book &amp; Notes</td>
<td></td>
<td>Project 2</td>
</tr>
<tr>
<td>8</td>
<td>3/12/2013</td>
<td>Spring Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>3/19/2013</td>
<td>L-7 Email Analysis</td>
<td>Notes from Blackboard Chappell Ch 25</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>3/26/2013</td>
<td>L-8 Unknown Code Analysis</td>
<td>ABJP Ch 10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>4/2/2013</td>
<td>L-9 Windows Memory Analysis and Persistence</td>
<td>ABJP Ch 3, 6, 9</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>4/9/2013</td>
<td>L-10 Analyzing Network Traffic</td>
<td>Chappell Ch 28 &amp; 29</td>
<td>Project 3</td>
</tr>
<tr>
<td>13</td>
<td>4/16/2013</td>
<td>L-11 Analyzing Network Traffic</td>
<td>Chappell Ch 30 &amp; 31</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>4/23/2013</td>
<td>L-12 Routers/Firewalls</td>
<td>Notes from Blackboard Liu – Cisco Router &amp; Switch Forensics</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>4/30/2013</td>
<td>L-13 Logs</td>
<td>ABJP Ch 11 - 15</td>
<td>Project 4</td>
</tr>
<tr>
<td>16</td>
<td>5/7/2013</td>
<td>Reading Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>5/14/2013</td>
<td>Final Exam - In Class - 2 Hour Exam – Open Book &amp; Notes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Grading:  
- Mid-term:  30% (Open Book and Notes)
- 4 Projects:  40%
- Final:   30% (Open Book and Notes)

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 and notes.

Online Lectures:  
In certain situations, snow or something else causing a school closure or disruption, 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](http://registrar.gmu.edu/calendar.html)

The above link will provide you will 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](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(Spring 2013) course

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

- JAVA
- Quicktime
- Flash

Software That You Will Need (Free Stuff)

Software that you should have loaded on your personal computer include

- 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
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.

**Open Computer Lab** - The open computer lab is located in Engr 1506. Both EnCase and FTK are installed on these computers as well as the software listed above.

**Required Reading and Reference Material:** Multiple books and sources are used to create this course. Of these, two are required text. For the purpose of exam preparation, the Blackboard notes are stressed.

**Required:** Wireshark Network Analysis 2nd Ed, Laura Chappell, Chappell University, [www.wiresharkbook.com](http://www.wiresharkbook.com), ISBN 978-1-893939-94-3 (Chappell)


**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:** 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:**

- Cert: [http://www.cert.org](http://www.cert.org)
- Cisco: [http://www.cisco.com](http://www.cisco.com)
- Sourceforge.net: [http://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)
The Mason MSDN Academy link below is where you can get Visio


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 THROUGH GMU EMAIL AND NOT BLACKBOARD EMAIL OR ANY OTHER EMAIL ACCOUNT!!!
ALL PROJECTS WILL BE TurnED IN VIA EMAIL EXCEPT For PROJECT 3. NO BLACKBOARD SUBMISSIONS.