TCOM/CFRS 660 - Network Forensics
Department of Electrical and Computer Engineering
George Mason University
Fall, 2009

Syllabus
revised 2009-07-24

Administrative Information

Instructor:
Dr. Aleksandar Lazarevich
Email: alazarev@gmu.edu subject=GMU-TCOM/CFRS 660 Sec_002_Your_name
Phone: 703-393-2247
Office hours: By appointment

Teaching Assistant
TBD

Day/time of class: Monday 4:30-7:10 pm

Location: Manassas/Prince William Campus – Bull Run Hall, Room 252

Class section: 002

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 and working knowledge of a computer language
Textbooks

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


References from the Web include the following sites:
- www.house.gov
- www.cert.org
- www.cisco.com
- www.ethereal.com
- www.perl.org
- www.foundstone.com

Grading

Raw scores may be adjusted to calculate final grades. Grades will be assessed on the following components:

Homeworks (4@10% each) 40%
Mid-term exam 30%
Final exam 30%

These components are outlined in the following sections.

Homeworks:
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.

Reports will due in Weeks 5, 9, 12, and 14.
Late reports will be assessed a penalty of 25% of the assignment grade for each week or part thereof it is late.

Mid-term exams
The mid-term exam will be conducted during class time in Week 8 and will cover material discussed in Weeks 1-7.
The mid-term exam will be take home and will be posted on blackboard

**Final exam**

The final exam will be held the week after the final class in the same room used for classes and will cover material from the weeks 9-15. The final exam will be take home and will be posted on blackboard

### Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading Assignments</th>
<th>Projects Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>08/31/2009</td>
<td>Introduction and review of Network Protocols</td>
<td>Notes &amp; TCOM 500/509 Material</td>
<td></td>
</tr>
<tr>
<td>Week 2</td>
<td>9/7/2009</td>
<td>Labor Day No class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>09/14/2009</td>
<td>Federal laws pertaining to the interception of digital evidence will be presented as they pertain to network forensics</td>
<td>Notes <a href="http://www.house.gov">www.house.gov</a> <a href="http://www.cybercrime.gov">www.cybercrime.gov</a></td>
<td></td>
</tr>
<tr>
<td>Week 4</td>
<td>09/21/2009</td>
<td>Incident Response Windows</td>
<td>Jones Chapters 1</td>
<td></td>
</tr>
<tr>
<td>Week 5</td>
<td>09/28/2009</td>
<td>Incident Response Unix/Linux</td>
<td>Jones Chapter 2</td>
<td>Project 1</td>
</tr>
<tr>
<td>Week 6</td>
<td>10/5/2009</td>
<td>Data Collection</td>
<td>Jones Chapter 3</td>
<td></td>
</tr>
<tr>
<td>Week 7</td>
<td>10/13/2009</td>
<td>Building a Response Tools</td>
<td>Jones Chapter 16</td>
<td></td>
</tr>
<tr>
<td>Week 8</td>
<td>10/20/2009</td>
<td>Midterm</td>
<td>In Class</td>
<td></td>
</tr>
<tr>
<td>Week 9</td>
<td>10/27/2009</td>
<td>Using Linux for Analyzing Files</td>
<td>Jones Chapter 13</td>
<td>Project 2</td>
</tr>
<tr>
<td>Week 10</td>
<td>11/3/2009</td>
<td>Hands-on Analysis of a File Linux</td>
<td>Jones Chapter 14</td>
<td></td>
</tr>
<tr>
<td>Week 11</td>
<td>11/10/2009</td>
<td>Hands-on Analysis of a File Windows</td>
<td>Jones Chapter 15</td>
<td></td>
</tr>
<tr>
<td>Week 12</td>
<td>11/17/2009</td>
<td>Analyzing Network Traffic</td>
<td>Jones Chapter 4 &amp; Orebaugh</td>
<td>Project 3</td>
</tr>
<tr>
<td>Week 13</td>
<td>11/24/2009</td>
<td>Analyzing Network Traffic</td>
<td>Jones Chapter 5 &amp; Orebaugh</td>
<td></td>
</tr>
<tr>
<td>Week 14</td>
<td>12/1/2009</td>
<td>Routers/Firewalls</td>
<td>Handout</td>
<td>Project 4</td>
</tr>
<tr>
<td>Week 15</td>
<td>12/8/2009</td>
<td>Wrap-up More on Logs</td>
<td>Anson Chapter 15</td>
<td></td>
</tr>
<tr>
<td>Week 16</td>
<td>12/15/2008</td>
<td>Final Exam</td>
<td>In Class</td>
<td></td>
</tr>
</tbody>
</table>

*This schedule is subject to revision before and throughout the course.*

Call 703–993–1000 for recorded information on campus closings (e.g. due to weather).

### Important Dates

- **Last day to add classes**: Tuesday Sep 15
- **Last day to drop with no tuition liability**: Tuesday Sep 15
- **Last day to drop**: Friday Oct 2
Attendance Policy
Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications
Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Honor Code
Students are required to be familiar and comply with the requirements of the GMU Honor Code[1]. The Honor Code will be strictly enforced in this course.

All assessable work is to be completed by the individual student.

Students must NOT collaborate on the project reports or presentation without explicit prior permission from the Instructor.