TCOM/CFRS 664 Sec 001 – Incident Response and Corporate Forensics
Department of Electrical and Computer Engineering
George Mason University
Fall 2015

Syllabus

revised 2015-08-14

Administrative Information

Instructor: **Dr. Aleksandar Lazarevich**
Email: alazarev@gmu.edu subject=GMU-TCOM/CFRS 664-001 Your name
Phone: 703-393-2247
Office hours: By appointment
Teaching Assistant: Sarah Kabli (skabli@gmu.edu)
Classes: Mondays, Engineering Building 4457, 7:20 pm –10:00 pm

Course Description

TCOM 664 - Incident Response Forensics (3:3:0)
Prerequisites: TCOM 509 and TCOM 529. This course addresses incident detection, response, and those aspects of computer forensics pertinent to the investigation of trade secret theft, economic espionage, copyright infringement, piracy, and fraud. Procedures for gathering, preserving, and analyzing forensic evidence are discussed in detail and are applied to both computer and network incident response forensics.

Textbooks

- Computer Security Incident Handling Guide, NIST Publication SP800-61 Revision 1 (Draft), Grace, Kent, Kim, September 2007, http://csrc.nist.gov/publications/nistpubs/index.html
- Guide to Integrating Forensic Techniques into Incident Response, NIST Publication SP800-86, Kent, Chevalier, Grance, Dang, August 2006, http://csrc.nist.gov/publications/nistpubs/index.html
- Guide to Computer Forensics and Investigations, Edition: 5th, Nelson, Phillips, and Steuart; 2015; Cengage; ISBN: 1285060032, Publisher's Web page: http://www.cengage.com/search/productOverview.do?Ntt=1285060032||467566138592255847626494261168144905O&N=16&Ntk=APG%7C%7CP_EPI&Ntx=mode+matchallpartial
- RTFM; Red Team Field Manual, Edition 1, BenClark, 2013, ISBN: 9781494295509, https://watchthestack.files.wordpress.com/2015/03/rtfm-red-team-field-manual.pdf
- (Optional) Blue Team Handbook: Incident ResponseEdition; *A Condensed Field Guide for the Cyber Security Incident Responder*,Version2, 2013, ISBN: 9781500734756,

Grading

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

Homeworks (4@15% each)	60%
Mid-term exam	20%
Final exam	20%

These components are outlined in the following sections.

Homework

The use of an eBook may not give you access to the student resource DVD so verify with publisher. Purchasing a used book may require you to purchase the DVD separately. You may use either the software provided or go to the software manufacturer's site and download the current trialware. You may use alternative software to do the homework if you wish.

- **Homework 1 -** In a 3-4 page paper, describe how you would prepare and maintain an incident response plan. Explain what the plan should contain, who should participate in the writing and validating, how it will be kept current, etc. Ensure you include who will respond and escalation criteria and procedures.
- **Homework 2 –** Using the Nelson Book, Prepare a 3-5 page response to Hands on Project Project 4-3 on pages 177-178.
- **Homework 3 –** Using the Nelson Book, Perform Hands-on project 5-4 on pages 249-250 and Write a 3-4 page paper describing your observations
- **Homework 4 –** Using the Nelson Book, Perform Hands-on projects 8-1 through 8-3 on pages 353-356

Reports will due in Weeks 5, 8, 12, and 14. Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of it is late.

Mid-term exams

The mid-term exam will be conducted on-line starting after class on Week 8, ending week 9 end of class time, and will cover material discussed in Weeks 1-9. No collaboration or web searching is authorized.

Final exam

The final exam will be a practicum where you will be issued files and folders to evaluate. You will need your own computer (any windows computer/laptop will do) with which to perform the investigation or you may use the machines in the open lab ENGR 1506. You will not be able to use your work computer since most will not allow you to install software. The final exam will be "take home". No collaboration is authorized.

Schedule

Week	Date	Topic	Reading Assignments	Projects Due
Week 1	8/29/2016	Introduction Incident Response	SP800-61 Chapt 2-8,	
Week 2	9/5/2016	Labor day – No class		
Week 3	9/12/2016	Forensic Investigations & Evidence Collection	Nelson Chapt 1 – 4	
Week 4	9/19/2016	No Class		
Week 5	9/26/2016	Windows	Nelson Chapt 5	Homework 1 due
Week 6	10/3/2016	Tools	Nelson Chapt 6,	
Week 7	10/10/2016	Macintosh, Linux	Nelson Chapt 7	Homework 2 due
Week 8	10/17/2016	Class on Tuesday, Forensic Analysis	Nelson Chapt 9	Mid-Term published/released
Week 9	10/24/2016	Mid-term (no-line) No lecture	Covers Weeks 1-9	Mid-term Due on-line
Week 10	10/31/2016	Graphics Files	Nelson Chapt 8	
Week 11	11/7/2016	Live Acquisition	Nelson Chapt 10	
Week 12	11/14/2016	Forensic Integration	SP 800-86 Chapt. 2-8	Homework 3 due
Week 13	11/21/2016	Email	Nelson Chapt 11	
Week 14	11/28/2016	Mobile Device & Cloud Investigations	Nelson Chapt 12-13	Release final exam
Week 15	12/5/2016	Law, ethics and testimony	Nelson Chapt 14-16	
Week 16	12/12/2016	Final exam	Covers weeks 10-15	Final exam

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	Tue. September 6
Last day drop with no tuition liability	Tue. September 6
Last day to drop (33% penalty)	Tue. September 20
Last day to drop (67% penalty)	Fri. September 30

From http://registrar.gmu.edu/wp-content/uploads/3YrCalendar-2016-18-approved-11.4.15.pdf
See that Web page for more information.
Religious holiday calendar http://ulife.gmu.edu/calendar/religious-holiday-calendar/?_ga=1.106512451.1901005430.1470254435

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.

Helpful In formation

Lab Info: http://labs.vse.gmu.edu/uploads/FacultyFAQ/StudentWelcome.pdf and http://labs.vse.gmu.edu/uploads/FacultyFAQ/SyllabiTexts.pdf

University email policy: Per university policy 1315 (http://universitypolicy.gmu.edu/policies/employees-electronic-communications/), you must use university email for all Mason-related email. Failure to do so puts us at risk of a violation of FERPA and could expose your entire personal email communications to legal discovery actions in the event of any legal actions that involve you.

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 exams.

In order to be able to fully exchange information and insure complete candor in discussions, the policy of non-attribution will be STRICTLY enforced.

[1] Available at http://catalog.gmu.edu/content.php?catoid=5&navoid=410#Honor and related GMU Web pages.