TCOM/CFRS 661–Digital Media Forensics
Department of Electrical and Computer Engineering
George Mason University
Spring, 2013

Syllabus

revised 2013-015-12

Administrative Information

Instructor: **Dr. Aleksandar Lazarevich**
Email: alazarev@gmu.edu subject=GMU-TCOM/CFRS 661-B01/02 Your name
Phone: 703-393-2247
Office hours: By appointment
Teaching Assistant: To Be Assigned
Classes: Monday, ENG 5358 (Engineering Building, Room 5358), 7:20 pm - 10:00 pm

Course Description

TCOM/CFRS 661 - Digital Media Forensics (3:3:0)
Prerequisites: TCOM 548 and TCOM 556 or TCOM 562; a working knowledge of computer operating systems (e.g. CS 471 or equivalent) or permission from instructor. This course deals with the collection, preservation, and analysis of digital media such that the 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 seizure, preservation, and analysis of digital media will be examined in this course.

Textbooks

- File System Forensic Analysis, Brian Carrier, Addison-Wesley, 2005, ISBN:0-321-26817-2 http://www.digital-evidence.org/
- Computer Forensics: Investigating Hard Disks, File and Operating Systems, EC-Council, Cengage Press, 2010 , ISBN:1-4354-8350-2, http://www.cengage.com/search/productOverview.do;jsessionid=1hhqMtpGSNyNy2HyhzJc5rC9y77yRRfkyW2zZGWNJddTGhtMY33t!-1930700699?N=+16&Ntk=P_Isbn13&Ntt=9781435483507
- Computer Forensics: Investigating Data and Image Files (Volume 3 of 5), EC-Council, Cengage Press, 2010 , ISBN: 1-4354-8351-0, http://www.cengage.com/search/productOverview.do?N=+14+11&Ntk=P_Isbn13&Ntt=9781435483514
- Computer Forensics Investigating Wireless Networks and Devices (Volume 5 of 5), EC-Council, Cengage Press, 2010 , ISBN: 1-4354-8353-7, http://www.cengage.com/search/productOverview.do?N=+14+11&Ntk=P_Isbn13&Ntt=9781435483538.

Grading

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

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

These components are outlined in the following sections.

Homework

All material necessary for the homework projects is available at the web site, http://www.cengage.com/community/eccouncil link for the appropriate book. The use of an eBook may not give you access to the student resource site so verify with publisher. Purchasing a used book may require you to purchase access to the student resources separately. The online access code is in your texts. Use the correct code for each text. 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 -** Complete the hands on project on pages 2-19 through 2-29 of the text, Computer Forensics: Investigating Data and Image Files (Volume 3 of 5) and write a 3-5 page report describing your findings.
- **Homework 2 -** Complete the hands on project on pages 3-22 through 3-25 of the text, Computer Forensics: Investigating Data and Image Files (Volume 3 of 5) and write a 3-5 page report describing your findings.
- **Homework 3 –** Complete the hands on project on pages 5-28 through 3-31 of the text, Computer Forensics: Investigating Hard Disks, File and Operating Systems and write a 3-5 page report describing your findings.
- **Homework 4 -** Complete the hands on project on pages 6-32 through 6-39 of the text, Computer Forensics: Investigating Hard Disks, File and Operating Systems and write a 3-5 page report describing your findings.

Homework will due in Weeks 4, 7, 11, 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 take home and will cover material discussed in Weeks 1-8. The mid-term exam will be released the week before it is due. No collaboration is authorized.

Final exam

The final exam will be a practicum where you will be issued a hard drive image. You will need a computer (any windows computer/laptop will do) with which to perform the investigation. You may also use the computers in the open lab 1506 ENGR. 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. The submission will be in the form of an expert witness report so completeness is paramount.

Schedule

Week	Date	Topic	Reading Assignments	Projects Due
Week 1	1/28/2013	Introduction/Legal Issues	Notes supplement	
Week 2	2/4/2013	Data Acquisition and duplication	EC-Council Data book Chapt. 1&2	
Week 3	2/11/2013	Forensic Investigations	EC-Council Data book Chapt. 3&4	
Week 4	2/18/2013	File systems	EC-Council Hard Disk book Chapt. 1	Homework 1 due
Week 5	2/25/2013	Hard Drives & Digital Media	Carrier Chapt 5 & 8 & EC-Council Hard Disk book Chapt. 2 and Carrier Chapt 9 & 10	
Week 6	3/4/2013	Boot Processes	EC-Council Hard Disk book Chapt. 3 and Carrier Chapt 11	
Week 7	3/11/2013*	Spring Break/ No class		Homework 2 due
Week 8	3/18/2013	Windows Forensics	EC-Council Hard Disk book Chapt. 4&5	Mid-term released in blackboard
Week 9	3/25/2013	Mid-term	Covers Weeks 1-8	Mid-term due
Week 10	4/1/2013	Linux Forensics	EC-Council Hard Disk book Chapt. 6	
Week 11	4/8/2013	Application Password Crackers	EC-Council Hard Disk book Chapt. 7	Homework 3 due
Week 12	4/15/2013	Practicum discussion Investigating Wireless Attacks	EC-Council Wireless book Chapt. 1 and Nelson Chapt. 6	
Week 13	4/22/2013	Blackberry Forensics Final exam Published	EC-Council Wireless book Chapt. 2 and Carrier Chapt 14 & 15	Practum/Final released
Week 14	4/29/2013	iPod & iPhone Forensics &Android Final exam may be turned in	EC-Council Wireless book Chapt.3 & 4 and Carrier Chapt 7	Final exam may be turned in Homework 4 due
Week 15	5/6/2013	Cloud Forensics Final exam may be turned in		Final exam may be turned in
Week 16	5/13/2013	Final exam Due	Covers weeks 9-15	Final exam Due

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. JAN. 29
Last day to drop with no tuition liability	Tue. JAN. 29
Last day to drop (33% penalty)	Tue. FEB 12
Last day to drop (67% penalty)	Fri. FEB 22

From http://registrar.gmu.edu/calendars/2013Spring.html
See that Web page for more information.
Religious holiday calendar http://ulife.gmu.edu/religious_calendar.php

Attendance Policy

Students are expected to attend each class, whether on-line or in person, 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 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.