TCOM/CFRS 661–Digital Media Forensics
Department of Electrical and Computer Engineering
George Mason University
Fall, 2014

Syllabus

revised 2014-08-17

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), 4:30 pm - 7:10 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/
- System Forensics, Investigation, and Response, 2nd Edition, Chuck Easton, Jones & Bartlett Learning, 2014 , ISBN:978-1-284-03105,
- Lab Manual and Virtual Lab access to accompany System Forensics, Investigation, and Response, 2nd Edition, Version 2.0, Jones & Bartlett Learning, 2014 , ISBN: 978-1-284-073935 (available from the publisher @ www.shopjblearning.com
- Optional- Hard copy of Lab Manual: Lab Manual and Virtual Lab access to accompany System Forensics, Investigation, and Response, 2nd Edition, Version 2.0, Jones & Bartlett Learning, 2014 , ISBN:978-1-284-03753-1

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 1 is available on blackboard in the appropriate folder. Homeworks 2-4 require access to the Virtual Security Cloud Lab that may be purchased at www.shopjblearning.com . The lab access includes an electronic copy of the lab manual but if you wish a hard copy, it is available at the university bookstore. Alternative software is available to experiment with. For all homework, I expect you to tell me what you did,what you saw and what it means.

- **Homework 1 - U**sing either dd from a live boot cd or ftk imager to acquire the image of the pagefile.sys on your PC, copy the image to another location. Use Mount Image Pro to mount the image of pagefile.sys and exam the contents. Use R-Drive image to capture a portion of your document directory. Write a 3+ page report describing your procedures, observations and analysis of your findings (the contents of what you examined). Include screenshots where appropriate.
- **Homework 2 -** Complete Lab # 1 in the VSCL and fill out the assessment worksheet as well as a 3+ page report describing your procedures, observations and analysis of your findings. Include screenshots where appropriate.
- **Homework 3 –** Complete Lab # 4 in the VSCL and fill out the assessment worksheet as well as a 3+ page report describing your procedures, observations and analysis of your findings. Include screenshots where appropriate.
- **Homework 4 -** Complete Lab # 9 in the VSCL and fill out the assessment worksheet as well as a 3+ page report describing your procedures, observations and analysis of your findings. Include screenshots where appropriate.

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 1-9. 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 download 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	8/25/2014	Introduction/Legal Issues	Notes supplement, Easttom Chapter 1 &2	
Week 2	9/1/2014	Labor day – No class		
Week 3	9/8/2014	Data Acquisition and duplication	Easttom Chapter 3	
Week 4	9/15/201	Forensic Investigations	Easttom Chapter 4 & 5	Homework 1 due
Week 5	9/22/2014	File systems	Carrier Chapt 5 & 8	
Week 6	9/29/2014	Hard Drives Digital Media	Carrier Chapt 9 & 10 and Easttom Chapter 6	
Week 7	10/6/2014	Boot Processes Linux and Mac Forensics	Easttom Chapter 9 and 10	Homework 2 due
Week 8	10/14/2014	Class on Tuesday, Windows Forensics	Carrier Chapt 11 and Easttom Chapter 8	
Week 9	10/20/2014	Windows Forensics	Easttom Chapter 8	Mid-term released in blackboard
Week 10	10/27/2014	Mid-term (no class)	Covers Weeks 1-9	Mid-term due
Week 11	11/3/2014	Application Password Crackers	Carrier Chapt 7, and Eastomm Chapter 7	Homework 3 due
Week 12	11/10/2014	Investigating Wireless Attacks	Easttom Chapter 12	
Week 13	11/17/2014	Practicum discussion Blackberry Forensics	Easttom Chapter 11 & 15	
Week 14	11/24/2014	iPod & iPhone Forensics &Android Final exam Published	Carrier Chapt 14 & 15	Homework 4 due Practum/Final released
Week 15	12/1/2014	Cloud Forensics Final exam may be turned in	Easttom Chapter 14	Final exam may be turned in
Week 16	12/8/2014	Reading Day, Final exam may be turned in		Final exam may be turned in
Week 17	12/15/2014	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 or drop with no tuition liability — Tue. September 2
Last day to drop (33% penalty) — Tue. September 16
Last day to drop (67% penalty) — Fri. September 26
From http://registrar.gmu.edu/calendars/2013fall/
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.