TCOM/CFRS 510 Sec 001 – Digital Forensics Analysis
Department of Electrical and Computer Engineering
George Mason University
Fall 2012

Syllabus (19 Aug 2012)

Class time/location: Monday 7:20 pm – 10:00 pm / Prince William Campus: Bull Run Hall, room 252

Administrative Information

Instructor: Eric J. Eifert, Special Agent USAF
Adjunct Professor
E-mail: eeifert2@gmu.edu
Phone: 703-966-9998
Office Hours: By Appointment

Course Description

TCOM/CFRS 510 Sec 001 – Digital Forensics Analysis
Explains Computer Forensics crime scene procedures, beginning with initial walk-through and evaluation; identification and collection of potential evidence; preparation of intrusion investigation; aspects of working with investigators and attorneys; reverse engineering with file identification and profiling; application of critical thinking in determination of significance of artifacts; and analysis and reporting of evidence.

Credits: 3
Prerequisite(s): Graduate standing or permission of instructor

Text book

Title: Digital Evidence and Computer Crime, 3rd edition
Author: Eoghan Casey
Publisher: Academic Press
ISBN: 9780123742681
Pages: 807

Lab book

Title: Guide to Computer Forensics and Investigations Lab Manual
Author: Andrew Blitz and Christopher Steuart
Publisher: Course Technology
ISBN: 9781435498853
Pages: 224

Grading

Homework assignments, individual presentation, mid-term exam, and group presentations will be evaluated to create the final grade. All group members will receive the same grade.

Homework (4 assignments): 20%
Individual Presentation #1: 10%
Midterm Exam: 25%
Individual Presentation #2: 20%
Final Exam: 25%

Schedule

Week	Date	Topic	Reading Assignment / Lab	Projects Assigned / Due
Week 1	27-Aug-12	Foundations of Digital Forensics	Chapter 1	Assigned: Homework #1 - Introduction to Digital Forensic Tools
Labor Day	3-Sep-12	No Class this week		
Week 2	10-Sep-12	Language of Computer Science Investigation	Chapter 2 / Lab 1 and 2	Due: Individual presentation topics (Computer forensics in the news)
Week3	17-Sep-12	Digital Evidence in the Courtroom	Chapter 3 / Lab 3	Due: Homework #1
Week 4	24-Sep-12	Cybercrime Law: A United States Perspective	Chapter 4 / Lab 4	Due: Individual Presentation #1
Week 5	1-Oct-12	Conducting Digital Investigations	Chapter 6 / Lab 5	
Week 6	**Tuesday 9-Oct-12**	Handling a Digital Crime Scene	Chapter 7 / Lab 6	Assigned: Homework #2 - Cryptographic Hash Functions
Week 7	15-Oct-12	Investigative Reconstruction with Digital Evidence	Chapter 8 / Lab 7	
Week 8	22-Oct-12	MIDTERM EXAM		Due: Homework #2 Assigned: Individual Presentation #2 topics
Week 9	29-Oct-12	Computer Basics for Digital Investigators	Chapter 15 / Lab 8	Due: Individual Presentation #2 topics
Week 10	5-Nov-12	Applying Forensic Science to Computers	Chapter 16 / Lab 9	In class Project (Homework #3): Crime Scene Collection
Week 11	12-Nov-12	Digital Evidence on Windows Systems	Chapter 17 / Lab 10	Due: Crime Scene Collection report (Homework #3)
Week 12	19-Nov-12	modus Operandi, Motive, and Technology	Chapter 9 / Lab 11 and 12	Assigned: Homework #4 - Forensic Examination of Hard Drive Image
Week 13	26-Nov-12	Violent Crime and Digital Evidence & Digital Evidence as Alibi	Chapter 10 & 11 / Lab 13	
Week 14	3-Dec-12	Sex Offenders on the Internet	Chapter 12 / Lab 14	Due: Homework #4 and Individual Presentation #2
Reading Day	10-Dec-12	No class this week		
Week 15	17-Dec-12	Final Exam		Final Exam

Blackboard Learn

We will be utilizing the new Blackboard Learn capability to post material, manage assignments, chat and other activities. You can access the Blackboard at: http://myMason.gmu.edu.

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 e-mail or telephone. E-mail is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. E-mail 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.

Honor Code

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

Accommodations for Disabilities

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with *Office for Disability Services* (SUB I, Rm. 4205; 993-2474;http://ods.gmu.edu) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.

"A better title for Digital Evidence and Computer Crime might be the Comprehensive Guide to Everything You Need to Know About Digital Forensics. One is hard pressed to find another book overflowing with so many valuable details and real-world examples."--Ben Rothke on Slashdot.org (Sept 2011). "The third edition of this comprehensive textbook on forensic science and the Internet is thoroughly updated to reflect the great leaps forward in technology in the six years since the previous printing. The work is divided into five sections covering digital forensics Traditional computer crime investigations focused on the forensic analysis of powereddown computer components, usually known as " dead-box " forensics. However, computer forensic examinations extend beyond the traditional forms of computer hardware to include other forms of digital evidence, defined as information that is either transferred or stored via a computer (Casey, 2011). Digital evidence may be found on mobile phones, global positioning systems (GPS) devices, cameras, and networks, to name a few. ...Â Recognizing this growth in digital evidence, an umbrella term, digital forensics, refers to the analysis of digital evidence, which includes network forensics, computer forensics, and mobile-device forensics, and malware forensics (Casey, 2011).