CFRS 780 Sec 001
Advanced Topics in Computer Forensics – Counter Forensics
George Mason University
Fall, 2012

Syllabus

revised 2012-09-03

Administrative Information

Instructor:	**Tahir Khan**
Email:	tkhan9@gmu.edu subject=GMU-TCOM/CFRS 780-001 Your name
Phone:	703-582-8257
Office hours:	By appointment
Teaching Assistant:	TBD
Classes:	Friday, Innovation Hall/323, 6:00 pm – 8:45 pm

Course Description

CFRS 780 - Advanced Topics in Computer Forensics – Counter 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. Teaches advanced topics from recent developments and applications in various areas of computer forensics. The advanced topics are chosen in such a way that they do not duplicate existing CFRS courses. Active participation of the students is encouraged in the form of writing and presenting papers in various research areas of the advanced topic. The course is designed to enhance the professional engineering community's understanding of breakthrough developments in specific areas of computer forensics.

Textbooks

(Optional) Digital Forensics with Open Source Tools - ISBN: 1597495867

Potential topics

1. Digital Media wiping
2. Stegonography
3. Rootkits
4. Encryption
5. Metadata manipulation
6. S.M.A.R.T. manipulation
7. Audit/Log manipulation
8. Timestomping
9. Slack space manipulation
10. Secure Digest Collision generation
11. Memory manipulation
12. Misleading evidence
13. Forensic tool vulnerabilities
14. Obfuscation
15. Polymorphism
16. Anonymizing
17. Flushable devices
18. Network manipulation

Grading

Grades will be assessed on the following components:

Research Papers (4@20% each)	80%
Class Presentation/Participation	20%

These components are outlined in the following sections.

Research Papers

Each student will prepare four research papers in APA format address a technique or tool used in counter/anti-forensics. They will be 6-10 pages in length with no less than 4 references. No more than 25% of the paper may be quotes. Papers will be randomly chosen for discussion in class.

Papers will due in Weeks 5, 8 11, and 15. Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of it is late.

Presentation

Each student will select one of their research papers to present to the class in a one hour presentation that will include leading a discussion and a question and answer session. A soft copy of the PowerPoint (.ppt) file will be submitted prior to the presentation.

Participation

Throughout the semester there will be hands on exercises and labs to demonstrate the various tools and techniques covered in class. Students are expected to participate in the exercises. While the exercises are not graded, participation is a factor in the overall grade.

Schedule

Week	Date	Topic	Reading Assignments	Projects Due
Week 1	8/31/2012	Introduction and overview of counter forensics		
Week 2	9/7/2012	Review of network forensics In class Lab Packet manipulation/Tunneling	Read up on basic networking	
Week 3	9/14/2012	Counter forensic tools/techniques In class lab Hiding data in memory	Read up on memory allocation/storage and processes	
Week 4	9/21/2012	Review of digital media forensics In class Lab Hiding data from the User	Read up on OS File systems (NTFS)	
Week 5	9/28/2012	Counter forensic techniques/tools In class Lab Hiding data	Read up on File headers	Paper 1 due

Week 6	10/5/2012	Counter forensic techniques/tools In class Lab Artifact wiping	Read up on OS file systems (NTFS) and slack space.	
Week 7	10/12/2012	Counter forensic techniques/tools In class Lab Trail obfuscation	Read up on MAC times, NTFS MFT	
Week 8	10/19/2012	Counter forensic techniques/tools In class Lab Trail obfuscation	Read up on hashing/PE File format	Paper 2 due
Week 9	10/26/2012	Student Presentations and paper discussions		
Week 10	11/2/2012	Student Presentations and paper discussions		
Week 11	11/9/2012	Student Presentations and paper discussions		Paper 3 due
Week 12	11/16/2012	Student Presentations and paper discussions		
Week 13	11/23/2012	Thanksgiving		
Week 14	11/30/2012	Student Presentations and paper discussions		
Week 15	12/7/2012	Student Presentations and paper discussions		Paper 4 due
Week 16	12/14/2012	Student Presentations and paper discussions		

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, September 4th
Last day to drop with no tuition liability Tuesday, September 4th
Last day to drop (33% penalty) Tuesday, September 18th
Last day to drop (67% penalty) Friday, September 28th
From http://registrar.gmu.edu/calendars/2012Fall.html
See that Web page for more information.

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 [http://honorcode.gmu.edu/]
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.