CFRS 780 Sec B01
Advanced Topics in Computer Forensics – Anti Forensics
George Mason University
Summer, 2013

Syllabus

revised March 2, 2013

Administrative Information

Instructor:	**Tahir Khan**
Email:	tkhan9@gmu.edu subject=GMU-TCOM/CFRS 780-B01 Your name
Phone:	703-582-8257
Office hours:	By appointment
Teaching Assistant:	TBD
Classes:	Engineering building, Room 5358. Tues/Thurs - 19:20-22:00

Course Description

CFRS 780 - Advanced Topics in Computer Forensics – Anti 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

None

Potential topics

1. Digital Media wiping
2. Steganography
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. Memory manipulation
11. Misleading evidence
12. Forensic tool vulnerabilities
13. Obfuscation
14. Polymorphism
15. Anonymizing
16. Network manipulation

Grading

Grades will be assessed on the following components:

(10%) Research paper on CCLeaner
(15%) Research paper review on a current anti-forensic technique
(10%) Homework – (VM usage)
(10%) In-class labs
(15%) Research paper on a current security application
(30%) Final paper and forensic report
(10%) Presentation on final paper

Research Papers	40%
Homework (In class/Take Home)	20%
Final Paper	30%
Class Presentation	10%

Research Papers

Each student will prepare 3 research papers in APA format. The papers shall be approximately 3-5 pages in length with no less than 4 references. No more than 25% of the paper may be quotes. Papers may be randomly chosen for discussion in class.

The papers will address/cover the following:

- A paper on a public privacy software application (CCLeaner)
  - The paper will address artifacts left behind on disk and in memory
  - Utilization of an older copy of CCleaner is acceptable.
- A review on a published paper that covers an anti-forensic technique. The paper must be published within in the last two years. In your summary include the implications of their findings and future direction.
- A research paper on a software application that has privacy or anti-forensic capabilities:
  - E.g. Opera, Chrome, IE, Truecrypt, Bitlocker, Word encryption
  - The student must use tools like Process Monitor, regshot, wireshark to determine what artifacts are left behind (if any)
  - Utilization of an older copy of software is acceptable

Late papers will be assessed a penalty of 25% of the assignment grade for each week or part thereof it is late.

Final Project

The final project will consist of a forensic report on an assigned virtual machine. The report must detail actions performed on the VM, please be aware the image/disk may not contain any obvious artifacts and try and focus on the anti-forensic techniques used. The package will contain a memory snapshot, a pcap file and a disk image. The VM can be booted up and live analysis may be performed. This VM will be obtained from the pool of

student VMs and the goal is to see what anti-forensic techniques were performed on the VM compared to what was found. The student shall not receive a copy of the actions performed on the virtual machine until the presentation has been performed.

Presentation

The final presentation will be an in-class presentation of findings obtained from the forensic analysis of the virtual machine. Please present the findings in a professional manner and expect questions. A soft copy of the PowerPoint (.ppt) file must 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. Please be aware, in-class labs are part of the overall grade.

Schedule

	Date	Topic	Reading Assignments	Assignments Due
Class 1	6/4/2013	Introduction and overview of anti-forensics		
Class 2	6/6/2013	Review of network forensics In class labs Packet manipulation/Tunneling Encryption (SSL) Protocol misuse/manipulation Attacking the tools/process Network based logs	Read up on basic networking	
Class 3	6/11/2013			
Class 4	6/13/2013	Review of memory forensics In class labs Router forensics Memory dumping Virtual Memory/Pagefile/Hiberfile Encryption Alternative memory Other applications Malware and memory Syscall proxing Avoiding the disk	Read up on memory allocation/storage and processes	Paper 1 due
Class 5	6/18/2013			
Class 6	6/20/2013	Review of disk forensics Slack Space Disk Encryption / External Disks Bad blocks/Misreporting drive size S.M.A.R.T. Data Destruction Duplicate disks Mobile disk forensics	Read up disk based forensics, OS file systems (NTFS) and slack space.	

Class 7	6/25/2013	Review of file system forensics Basic attributes File extension manipulation Headers/Magic Numbers Alternate data streams Prefetch manipulation	Read up on MAC times, file formats	Paper 2 due
Class 8	6/27/2013	File system tunneling Steganography Encryption Timestomping Registry time modification File stuffing / splitting		
Class 9	7/2/2013	Malware / IR Obfuscation Polymorphism Analyzing autoruns Malicious websites / websites (DF) DNS poisioning	Read up on javascript obfuscation	Take home VM
Class 10	7/4/2013	University closed on Thursday, July 4, in observance of Independence Day.		
Class 11	7/9/2013	Application forensics Third party tools Word/Excel/PPT Toolbars		
Class 12	7/11/2013	Browser Forensics Crash reports InPrivate/Incognito Proxy Servers Live-CD's TOR		Paper 3 due
Class 13	7/16/2013	Review of logfiles DrWatson files/logs Trail obfuscation Log manipulation	Review various logs and log formats	
Class 14	7/18/2013	Tracing deletes in a corporate environment		
Class 15	7/23/2013	Student Presentations		
Class 16	7/25/2013	Review		Final paper 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

See:
http://studentaccounts.gmu.edu/dates.html#summer
http://summer.gmu.edu/dates/

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.