Instructor: Brian Hussey
e-mail: bhussey@gmu.edu
CFRS 500 - 001
Fairfax Campus, Engineering Hall (Engr 5358)
Introduction to Technologies of Forensic Value
Fall 2012
Aug 28, 2012 - Dec 11, 2012
Tuesdays 4:30pm - 7:10pm

Syllabus:

This course will introduce concepts and techniques involved with the analysis of digital media. Topic selection will vary across several different sub-disciplines; to include network intrusions, cyber-terrorism, malware analysis, network log analysis, and memory analysis. However, the specific focus will be on hard drive analysis, forensic artifacts found in Windows Operating systems and methodologies for recovering and deciphering them. The majority of the lessons will be in the context of investigating a network intrusion.

By the end of this class, students will have a basic understanding of the underlying concepts of computer forensic investigations and they will have a basic framework for conducting the full lifecycle of a forensic investigation, from acquisition to technical analysis and reporting.

Hybrid Course Format:
This course will be taught in both an in-class lecture format and an online format. Students will be notified via their George Mason e-mail accounts when a class will be taught online. Please check these accounts frequently. An announcement will also be made on Blackboard.

Online classes will use the **Colaboration** tool on Blackboard. Students are expected to be logged in during class time, however, sessions will be saved for students to review later on Blackboard. All labs and assignments will still be required to be uploaded to Blackboard regardless of the class format.

Currently two classes are scheduled to be taught online:
Module 1: Tuesday 8/28/12
Module 3: Tuesday 8/11/12

The instructor reserves the right to change class format as his schedule requires.

- **Computer**

All students will be required to have access to a computer with a Windows Operating System installed (XP or newer). Students must have administrative rights on this computer. The professor suggests, if possible, for students to bring Windows-based laptop computers to each class as we will do labs in class that students can follow along with. However, if the student does not have access to a laptop computer, they may use the computers provided in class.

Books

This class will use the following textbooks:

- Casey, E. (ed). (2009) Handbook of Digital Forensics and Investigation. ISBN:13:978-0-12-374267-4.
- Bunting, S. (2008). EnCE: The Official EnCE: EnCase Certified Examiner Study Guide. ISBN: 13:978-0-470-18145-4
- The professor may provide additional reading material from various sources that the students will be expected to read prior to class.

Materials

Class materials will be posted to Blackboard; they will often be posted in a compressed (.rar or .zip) format. It is the responsibility of the student to come to every class with all of the required materials, in an uncompressed format. The materials can be saved on a laptop, thumb drive, or CD/DVD, but they must be easily accessible for in-class labs.

Assessment

- **25% - Mid term Exam**

The 8th class session will be a mid-term exam. It will be composed of multiple choice, true/false, and essay questions. It will contain questions that are cumulative from the first half of the semester. This exam will account for 25% of the student's grade in this course. The test will be closed book, however, each student will be allowed to bring in 1 page (8.5x11) of hand-written notes to use as reference. (The student may write on both sides of the page)

- **25% - Final Exam**

The 15th class session will be a final exam. It will be composed of multiple choice, true/false, and essay questions. It will be contain questions that are cumulative from the entire class, (However, the majority of questions will be based on the second half of the course). This exam will account for 25% of the student's grade in this course. The test will be closed book, however, each student will be allowed to bring in 1 page (8.5x11) of hand-written notes to use as reference. (The student may write on both sides of the page)

- **15% - Evidence Acquisition Project**

During the first half of the semester, the professor will provide a "mock acquisition" office setting containing a variety of pieces of digital evidence. The students will form groups and deploy to the scene. Students should bring a camera and take pictures of all digital (and relevant non-digital) evidence. Then each student will write a detailed report of the process they would take to acquire the evidence. The report will include details about what hardware and software that they would use to acquire the evidence, the notes they would take and the pictures they took when deployed to the scene. The student should also explain why they chose to use the methods they describe in their report. This project is due by session # 7.

- **20% - Forensics Research White Paper**

Each student will choose a topic relevant to the world of computer forensics. The topic must be approved by the professor prior to proceeding with research or writing. This topic should challenge the student to conduct in-depth technical research in their area of interest and ability. The research should be presented in an 8-12 page formally written white paper. Students are expected to provide both sound technical research and grammatically correct, professionally written papers. Standard margins and 12-point Times New Roman font is expected. Students will be expected to have their topics approved by the professor prior to the mid-term exam and the paper will be due by Session #13.

- **15% - Student Participation / Labs**

Most classes will involve labs. Students are expected to complete the labs and post them to Blackboard. Students are also expected to actively participate in class discussions, ask questions, and provide input based on their own experience. Performance on the labs will be combined with observed class participation to account for the final 15% of the course grade.

➢ Session Descriptions

Session 1 – Course introduction, introduction to the field of computer forensics, sources and types of evidence

- Handbook of Digital Forensics and Investigation -Chapter 1: Introduction
- EnCE The Official EnCase Certified Examiner Book - Chapter 1: Computer Hardware

Session 2 - Forensic acquisitions of various forms of media, hashes, write-blocking, and chain of custody

- EnCE The Official EnCase Certified Examiner Book –
    - Chapter 3: First Response
    - Chapter 4: Acquiring Digital Evidence

Session 3 – Introduction to file systems. Concepts of sectors, clusters, and slack space. Timestamps and timeline analysis. User accounts and file / action attribution

- EnCE The Official EnCase Certified Examiner Book - Chapter 2: File Systems
- Handbook of Digital Forensics and Investigation - Chapter 5: Windows Forensic Analysis (Pages 209 - 229)

Session 4 – Windows system forensic artifacts: Link files, temp files, Recycle bin, prefetch files, Pagefile, hiberfil.sys

- EnCE The Official EnCase Certified Examiner Book - Chapter 9: Windows Operating System Artifacts

Session 5 - Windows System Forensic Artifacts Con't & File Signature

- Handbook of Digital Forensics and Investigation -Chapter 8: File Signature and Hash Analysis

Session 6 – Windows System Logs & Registry analysis

- Handbook of Digital Forensics and Investigation -Chapter 5: Windows Forensic Analysis Pages (230 - 300)
- EnCE The Official EnCase Certified Examiner Book - Chapter 10: Advanced EnCase Pages (486 - 496)

Session 7 – Internet activity and e-mail analysis

- Handbook of Digital Forensics and Investigation -Chapter 3: Electronic Discovery
- EnCE The Official EnCase Certified Examiner Book - Chapter 10: Advanced EnCase (Pages 514 - 531)

Session 8 – Mid-term exam

Session 9 – Introduction to malware, rootkits and network intrusions methodologies

- Handbook of Digital Investigations - Chapter 4: Intrusion Investigation

Session 10 – Network data analysis, ports and TCP/IP

- Handbook of Digital Forensics and Investigations - Chapter 9: Network Investigations

Session 11 – Mobile Device Forensics

- Handbook of Digital Forensics and Investigations - Chapter 10: Mobile Network Investigations

Session 12 - Cybercrime, cyberterror, and cyber-espionage. Attack vectors and steganography

- Stuxnet Article (Supplied on Blackboard)
- Additional Reading TBD

Session 13 – Dynamic Malware analysis

- Sysinternals Analysis of Stuxnet (Supplied on Blackboard)

Session 14 – Memory Acquisition and Analysis

- Reading TBD

Session 15 – Final exam

Attendance Policy:

GMU Policy: Students are expected to attend the class periods of the courses for which they register. In-class participation is important not only to the individual student, but also to the class as a whole. Because class participation may be a factor in grading, instructors may use absence, tardiness, or early departure as de facto evidence of nonparticipation. Students who miss an exam with an acceptable excuse may be penalized according to the individual instructor's grading policy, as stated in the course syllabus.

Students are expected to make prior arrangements with Instructor in writing (e-mail is preferable) 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. Absences from final exams will not be excused except for sickness on the day of the exam or other cause approved by the student's academic dean or director. The effect of an unexcused absence from an undergraduate final exam shall be determined by the weighted value of the exam as stated in the course syllabus provided by the instructor. If absence from a graduate final exam is unexcused, the grade for the course is entered as F. See the Additional Grade Notations in the Grading System section for information on being absent with permission.

CFRS 500 Practice: Excused absences may be granted on days that are not scheduled for an exam or project. To achieve credit for the absence from class, the student will be required to read all of assigned reading for that week, review the instructor's slides for that week (available on blackboard), and complete any labs scheduled for that week (available on blackboard). The student will e-mail the professor a synopsis of the reading and slides. The e-mail should display that the student has attained an understanding of that week's course content as well as the completed lab sheets (complete with screenshots verifying the lab was completed).

Honor Code: All students matriculating in this course are subject to the George Mason University Honor Code. Plagiarism, cheating and theft of intellectual property is strictly prohibited and will result in failing the class.

The instructor reserves the right to make changes to this syllabus throughout the course of the class as he deems necessary.