Instructor: Brian Hussey
e-mail: bhussey@gmu.edu
CFRS 500 - 001
Fairfax Campus, Nguyen Engineering Building (Engr 1505)
Introduction to Forensic Technology and Analysis
Spring 2014
January 21 – May 14
Thursdays 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. The lecture may be pre-recorded or live, depending on the professor's availability. If the lecture is provided live, then students are expected to be logged in during class time. Sessions will also be saved for students to review later on Blackboard. Pre-recorded sessions may be viewed at any point during the scheduled week of class. All labs and blog entries will still be required to be uploaded to Blackboard regardless of the class format.

No classes are currently scheduled to be taught online, but this is subject to change based on the Professor's availability.

- **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.

- **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**

- **15% - Blogs & Labs**

Most classes will involve labs. Students are expected to complete the labs and post them to Blackboard. Additionally, most classes will require reading from an online source and posting to a class blog on Blackboard. Each blog entry should answer the questions presented in the syllabus below. There may also be time for open class discussion on the topic, time permitting. Students are expected to actively participate in class discussions, ask questions, and provide input based on their own experience/ideas. Performance on the labs will be combined with the blog entries to account for 15% of the course grade.

- **25% - Midterm 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)

- **10% - 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. <u>This project is due by session # 7.</u>

- **25% - Forensic Investigation Group Project**

Students will form small groups of 3-4 people. The group will work together to plan a crime that will be solved via a computer forensic investigation. Students will create a VMware system using either Windows XP or Windows 7. It will be the responsibility of each group to gain access to a Windows OS to use for this project.

George Mason students do have access to a Microsoft MSDN via this website: http://msdn05.e-academy.com/gmu_bsit. Students will have to establish their own account to use it.

Students will execute their crime using the VM. Students should ensure that their crime creates forensic artifacts discussed in this class. After the crime is committed and forensic artifacts created, the students will make a forensic image of the system. They will then use the techniques taught in this class to conduct forensic analysis on the VM. Students will create a forensic analysis report documenting their findings. Screenshots must be included in this report to verify their findings. The final product will include both a written report and a 10 minute oral presentation describing the crime and how they solved it using computer forensics.

The following specific steps will be taken to successfully complete this project:

1. Create a group of 3 – 4 students. Get together and create a detailed, written plan that documents what kind of crime they will use the computer. Any kind of crime is acceptable as long as (of course) it is completely fabricated and NOTHING ILLEGAL ACTUALLY OCCURS!

2. Use the VM for everyday user activity; this will create noise that will make the investigation more realistic.
    a. Create a minimum of 3 user profiles on the system.
    b. Set up email that is saved on the computer directly and is not web-based. Students can use Outlook Express, download Thunderbird, or another format that the group prefers.
    c. Surf the Internet for various topics. The group must use Internet Explorer, but they can use other browsers as well, if they choose. Download various files from the Internet and save them in various locations on the hard drive.
    d. Download a number of programs and run them.
    e. Plug USB drives into the system, copy files to them, open the files on both the USB drive and on the host system.
    f. Delete some files by placing them in the Recycle Bin, delete other files permanently.
    g. Conduct these activities over a MINIMUM of one week, longer the better.

3. Now that the system is properly set up, it is time to execute the crime of your choosing.
    a. The crime should involve analysis of e-mail, Internet, registry, timeline, prefetch files, link files, and as many more forensic artifacts as possible. Your grade will be dependent on how many forensic artifacts are recovered and analyzed, keep this in mind when planning and executing your crime.

4. After the crime is committed, the team will forensically acquire the system using FTK imager Lite. It should be a live image. Acquisition of RAM is also highly encouraged.

5. The group will now conduct forensic analysis on the image. You can use the tools provided in this class or any other tool that you prefer. Remember to examine as many forensic artifacts as possible. I highly suggest examining every item discussed in this class.

6. Create your forensic analysis report. The final package should include the following:
    a. The detailed written crime plan created in step 1.

b. A page showing the specific responsibilities that each group member conducted as part of this project.
c. Forensic Analysis Report (**All findings should include a screenshot**)
    i. Executive Summary
    ii. Media Acquisition
        1. This should include the type of acquisition conducted, the scene of the acquisition, and the type of system acquired.
        2. Include size, MD5 hash, and time of acquisition.
        3. Include basic system information, such as Operating System, user accounts, hard drive size, file system, etc.
    iii. Timeline of Events
    iv. Details of Analysis
        1. This section should include all the various items forensically examined.
        2. Reporting of findings should be fact based. Ie: "The Internet Explorer Index.dat file was parsed to show Internet History. Analysis of this file showed that the user profile "Jim" visited www.xbadsite.xx.com 127 times from June 2, 2013 8:27:13am and 8:27:15am".
        3. It is acceptable to make expert opinions based on fact. Mark all opinions as an Analyst's Comment and format them in italics. Ie: *(ANALYST'S COMMENT: The system visited 127 pornographic sites in the span of 2 seconds but never visited one before or after those two seconds. The analyst believes that this activity was not the intent of the user because it was very anomalous behavior and occurred faster than an individual could purposefully conduct the actions. This is more indicative of an automated event or malicious code.)*
        4. This report should show all technical analysis and examination of forensic artifacts and it should include an explanation / interpretation of events.
    v. List of all software tools used during analysis of this case.

7. In addition to the report package, a 10 minute oral presentation must be prepared. It will be given on the class directly prior to the Final exam. A PowerPoint presentation must be prepared to guide the presentation. The presentation should describe the crime, the forensic analysis, and the group's findings.

➢ Session Descriptions

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

- Reading: http://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/
- Blog / Discussion Questions:
    - What mistakes did the Computer Forensic Examiner make in the Casey Anthony case?
    - Was it the fault of the examiner or the fault of the forensic tools?
    - How could the examiner have mitigated the damage created by the situation?

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

- LABS 1 & 2
- Reading: http://digital-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/
    - Why not pull the plug on a computer prior to forensic acquisition?
    - What are the pros and cons of live acquisition vs. dead acquisition?

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

- LAB 3
- Reading: http://archive.wired.com/techbiz/people/magazine/17-01/ff_max_butler?currentPage=all
    - What do you think about Max Butler's takeover of the cyber criminal underground market?
    - Was Max Butler a victim of circumstances or was he a true criminal mastermind? (Or somewhere in the middle)

Session 4 – Internet activity and e-mail analysis

- LABS 4 & 5
- Reading: http://www.magnetforensics.com/how-private-is-internet-explorers-inprivate-browsing-first-define-private/ & http://www.magnetforensics.com/how-does-chromes-incognito-mode-affect-digital-forensics/
    - What kind of Internet evidence can still be recovered when private Internet browsing options are enabled? How do you find them?
    - Which private browser would you recommend, IE or Chrome?

Session 5 – Windows system forensic artifacts: Link files, temp files, Recycle bin, prefetch files, Pagefile, hiberfil.sys

- LABS 6 & 7
- Reading: http://www.pcadvisor.co.uk/features/internet/3414409/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring/
    - What is Hacktivism?
    - What makes Hactivism different from hacking for profit?
    - Can hacking be justified if the cause is truly honorable?

Session 6 - Windows System Forensic Artifacts Con't & File Signature

- **LABS 8, 9, & 10**
- Blog Entry: Answer the question – If you had three professional certifications (computer forensic related) to complement your education, which would they be and why?

Session 7 – Windows System Logs & Registry analysis
- **LABS 11 & 12**
- Reading: Go study for the midterm.

Session 8 – Mid-term exam

Session 9 – Introduction to malware, rootkits and network intrusions methodologies
- Meet with group to develop final project plans

Session 10 – Network data analysis, ports and TCP/IP & Windows 8 Forensics
- **LAB 13**
- Reading: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
    - Mandiant's report asserts that China has carried on a long term cyber campaign against the United States. Do you feel this is an act of war, simple cybercrime, or just the next evolution of espionage?
    - What should the U.S. response be?
    - Are you surprised at the specificity in Mandiant's report? How do you think they came to their conclusions?

Session 11 - Cybercrime, cyberterror, and cyber-espionage. Attack vectors and steganography
- **LABS 14**
- Reading http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/
    - Should Stuxnet be classified as a computer program (malware) or as a weapon?
    - The international cooperation in the analysis of Stuxnet was unprecedented. Why do you think this is?
    - Stuxnet was the first known malware designed to cause physical damage on a large scale, is this the next evolution of cyberwar?

Session 12 – Volatile Memory Analysis
- Reading: http://www.washingtonpost.com/blogs/the-switch/wp/2013/07/29/rip-barnaby-jack-the-hacker-who-wanted-to-save-your-life/
    - Barnaby Jack designed famous hacks, such as ATM Jackpotting and biomedical device hacks, how do you feel about a single person having that much power?
    - What other devices, previously thought of as untouchable, do you think could be vulnerable to attack?

Session 13 – Dynamic Malware analysis
- **LABS 15**
- Group meetings for final presentation preparation.

Session 14 – Student Oral presentations of Group Projects

Session 15 – Final exam

Late Assignment Policy:
In general, late assignments will not be accepted and will be recorded as a 0% grade. All assignments are expected to be uploaded to Blackboard by midnight of the due date. In the event that unforeseen circumstances prevent a student from being able to turn in their assignment, the professor may grant permission for late submission. However, the student's grade will be significantly decreased, the exact amount subtracted from the student's score will depend on the amount of days late the assignment is.

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.