CFRS 771 Sec 001
Advanced Topics in Computer Forensics – Digital Profiling
George Mason University
Fall 2015

ADMINISTRATIVE INFORMATION

Instructor: *Chad M.S. Steel*
Phone: *610-639-3884*
E-mail: *csteel@gmu.edu*
Office Hours: *Mondays (after class) or upon request*

COURSE DESCRIPTION

CFRS 771 - Advanced Topics in Computer Forensics – Digital Profiling
This course details the application of criminal profiling to digital forensic evidence and computer crime. The course covers typologies of cyber criminals, ranging from hacktivists to organized crime to state actors. Additionally, the course reviews how the results of digital forensics can be used to profile individuals to better facilitate investigative interviews and prosecutions. Finally, the course applies cyberprofiling to the identification of criminal behavior for insider threats and fraud.

COURSE FORMAT:

Incorporates case studies, recent academic papers, and current trends in criminal behavior. The class will be a combination of exercises, lectures, case studies, discussion, and student presentations. Students will utilize the lessons learned in evaluating offender behavior in a series of online exercises. Each class will be conducted as follows:

- Student Presentation (starting Week 5)
- Discussion of Readings.
- Interactive Lecture on Key Principles.
- Case Study.

STUDENT OUTCOMES:

- Students will be able to articulate the various aspects of criminal profiling, including inductive and deductive profiles, modus operandi and signatures, and victimology.

- Students will be able to identify targets for digital forensic profiling, including mobile devices, log files, Internet activity, GPS devices, and non-traditional digital forensic sources.

- Students will understand how to analyze forensic data for the purposes of digital profiling and create specific tools to facilitate the creation of a digital profile.

- Students will exhibit an understanding of how digital evidence can provide behavioral clues that can be used in search warrants, interviews, and subsequent analyses.

- Students will demonstrate an understanding of how behavioral digital evidence can be used to show intent for prosecutorial purposes and combat current defense strategies.

- Students will be familiar with how to profile the different types of individuals that commit computer crime (and computer facilitated crime), including:
    - Hacktivists
    - Cyberterrorists
    - Organized Crime/Digitally Facilitated Fraud
    - Digital Stalkers
    - Child Pornographers
    - Data Thieves
    - Cyberespionage Actors

- Students will analyze case studies of computer crime and provide an analysis of the specifics of the digital behavior related to the crime and motivations of the criminals.

REQUIRED/SUPPLEMENTAL/RECOMMENDED TEXTS AND/OR READINGS:

Brenner, Susan W., Brian Carrier, and Jef Henninger. "Trojan Horse Defense in Cybercrime Cases, The." *Santa Clara Computer & High Tech. LJ* 21 (2004): 1.

Claycomb, William R., Carly L. Huth, Lori Flynn, David M. McIntire, Todd B. Lewellen, and CERT Insider Threat Center. "Chronological examination of insider threat sabotage: Preliminary observations." *J Wirel Mobile Netw Ubiquitous Comput Dependable Appl* 3, no. 4 (2012): 4-20.\

Décary-Hétu, David, Benoit Dupont, and Francis Fortin. "Policing the Hackers by Hacking Them: Studying Online Deviants in IRC Chat Rooms." *Networks and Network Analysis for Defence and Security*. Springer International Publishing, 2014. 63-82.

Denning, Dorothy E. "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy." *Networks and netwars: The future of terror, crime, and militancy* (2001): 239-288.

Drachen, Anders, Rafet Sifa, and Christian Thurau. "The name in the game: Patterns in character names and gamer tags." *Entertainment Computing* 5.1 (2014): 21-32.

Frank, L., and Ryan E. Hohimer. "Modeling human behavior to anticipate insider attacks." *Journal of Strategic Security* 4.2 (2011): 3.

Gordon, Sarah. "Virus Writers: The End of The Innocence?." In *Proc. International Virus Bulletin Conference*. 2000.

Herley, Cormac. "Why do Nigerian Scammers Say They are from Nigeria?." In *Proceedings of the Workshop on the Economics of Information Security*. 2012.

Internet Crime Complaint Center. "Internet Crimes Report – 2013". *Tech Report* (2014): 1:31.

Lanning, Kenneth V. "Cyber ''pedophiles'': A behavioral perspective." *The APSAC Advisor* 11.4 (1998): 12-18.

Lickiewicz, Jakub. "Cyber CrIme Psychology–Proposal of an Offender Psychological Profile." (2011).

Mentor, The Hacker Manifesto, 1986.

Palo Alto Networks. "419 Evolution", *Tech Report* (2014): 1-46.

Pierre Lai, Kam-Pui Chow, Xiao-Xi Fan and Vivien Chan. "An Empirical Study Profiling Internet Pirates." *Advances in Digital Forensics IX IFIP Advances in Information and Communication Technology Volume 410, 2013, pp 257-272*

Rogers, Marcus K., and Kathryn C. Seigfried-Spellar. "USING INTERNET ARTIFACTS TO PROFILE A CHILD PORNOGRAPHY SUSPECT." *Journal of Digital Forensics, Security and Law* 9.1 (2014): 57-66.

Rosoff, Heather, Jinshu Cui, and Richard John. "Behavioral Experiments Exploring Victims' Response to Cyber-based Financial Fraud and Identity Theft Scenario Simulations." *Symposium on Usable Privacy and Security (SOUPS)*. 2014.

Sofo, Francesco, et al. "Investigating the relationship between consumers' style of thinking and online victimization in scamming." *JDCTA* 4.7 (2010): 38-49.

Steel, Chad. "Idiographic Digital Profiling: Behavioural Analysis Based on Digital Forensics." *Journal of Digital Forensics, Security, and the Law.* 2014.

Whitty, Monica T., and Tom Buchanan. "The online romance scam: A serious cybercrime." *CyberPsychology, Behavior, and Social Networking* 15.3 (2012): 181-183.

Wolak, J., Finkelhor, D., and Mitchell, K. (2012). Trends in Arrests for Child Pornography Possession: The Third National Juvenile Online Victimization Study (NJOV-3). Durham, NH: Crimes against Children Research Center.

OPTIONAL, FOR REFERENCE: Turvey, Brent E., ed. *Criminal profiling: An introduction to behavioral evidence analysis*. Academic press, 2011. (Partial)

COURSE REQUIREMENTS, EVALUATION CRITERIA, AND GRADING SCALE:

1. Class Discussions: Each student must participate actively in discussions to receive class credit. Participation includes coming to class, providing feedback on the presentations of classmates, and asking insightful questions. Students will receive feedback mid-class on where they are with their discussion grade, and provided guidance on improving it if needed. Participation should be throughout the class – asking 20 questions the day before finals does not qualify.

2. Case Study and Profile: Each student is responsible for presenting a case study and creating a digital profile on a particular computer criminal. The case study should be approximately 30 minutes in length, and will be presented at the end of each class session (starting on week 5). The written profile is due at the time of the case study. The case study and profile are detailed in a separate handout.

3. Digital Profiling Exercises: Students will complete 6 exercises (three team exercises and three individual exercises) that demonstrate the thought process of digital criminals. The grading will be two-fold – the first part of the grade depends on the success of the students/teams in the exercises. The second part of the grade depends on the presentation of the student's strategy used and how that impacted their success/failure. The digital profiling exercises will be detailed in a separate handout.

Grading Policy

Attendance and Class Participation	20%
Case Study and Profile	40%
Exercises (first triad)	20%
Exercises (second triad)	20%
TOTAL: points	**100**

Grading Scale

A = 93-100%
A- = 90-92%
B+ = 88-89%
B = 83-87%
B- = 80-82%

C = 70-79%
F = Below 70%

Grades will be curved as follows:

- The highest numerical grade will be assumed to have received "100%"
- All students grades will be raised by the difference between the highest grade and 100%.
- Any attempts to game the system (e.g. all students not doing a paper) will result in the curve being suspended and all students receiving their directly calculated grade.

Schedule

This schedule is subject to revision before and throughout the course.

Week	Date	Topic	Reading Assignments	Comments
1	8/31	Why Study Digital Profiling?	Mentor	
2	9/14	Building a Profile	Steel, IC3 Report	Case Study Choices Due
3	9/21	Insider Threat	Claycomb, Frank	
4	9/28	Behavioral Principles	Drachen	Case Studies Begin
5	10/5	Online Child Exploitation	Lanning, Wolak	
*6	10/13	Digital Victimology	Herley, Palo Alto Networks, Soto	
7	10/19	Fraud and Identity Theft	Whitty, Rosoff	Final Day for First Triathlon – Group Presentations
8	10/26	Evidence Analysis	Rogers	
9	11/2	Hackers, Pirates and Hacktivists	Denning	
10	11/9	MO, Ritual, and Signature	Lickiewicz	
11	11/16	Case and Offender Linkage	Décary-Hétu	
12	11/23	Using Profile Information in Search Warrants and Court	Brenner	

13	11/30	Advanced Topics/Makeup Day		Final Day for Second Triathlon
14	12/7	Final Thoughts – Lessons Learned from Second Triathlon		

***Note: Class meets Tuesday**

Call 703-993-1000 for recorded information on campus closings (*e.g.* due to weather).
Important Dates

Last day to add classes 8 Sep
Last day to drop with no tuition liability 8 Sep
Last day to drop (33% penalty) 15Sep
Last day to drop (67% penalty) 2 Oct

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 as soon as feasible if they miss any class without notice due to an emergency.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method. 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.

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.

Corroboration is encouraged – students may consult each other and work collaboratively on any and all class endeavors.