CFRS 780 Sec 003
Advanced Topics in Computer Forensics – Digital Profiling
George Mason University
Spring, 2014

ADMINISTRATIVE INFORMATION

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

COURSE DESCRIPTION

CFRS 780 - Advanced Topics in Computer Forensics – Digital Profiling
Prerequisites: CFRS500, CFRS661 or equivalent. At least one programming class or prior background in development, or permission from instructor.
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 develop a tool to be used in digital profiling, write a fully referenced paper on either their tool (or a current research area), and present a 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:

Allison, Stuart FH, Amie M. Schuck, and Kim Michelle Lersch. "Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics." *Journal of Criminal Justice* 33, no. 1 (2005): 19-29.

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.

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.

Goodman, Marc D. "Why the police don't care about computer crime." *Harv. JL & Tech.* 10 (1996): 465.

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.

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*

Lanning, Kenneth V. "SEX OFFENDER CONTINUUM."

Marrington, Andrew Daniel. "Computer profiling for forensic purposes." (2009).

Mentor, The Hacker Manifesto, 1986.

Rogers, Marc. "The role of criminal profiling in the computer forensics process."*Computers & Security* 22, no. 4 (2003): 292-298.

Schultz, E. Eugene. "A framework for understanding and predicting insider attacks." *Computers & Security* 21, no. 6 (2002): 526-531.

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

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.

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: Each student is responsible for presenting a case study 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 4). The case study is detailed in a separate handout.

3. Tool Development and Paper: Each student will develop a tool and present a paper on that tool covering a specific area of interest in digital profiling. Tool design and selection are up to the student, as is the platform used. The tool may use a prototype interface or be text-based, and should provide information useful in doing a digital profile. Examples of possible tools:

- A tool that extracts search terms from Internet history and histograms/categorizes them.
- An Internet history tool that does histograms of usage patterns and categorizes them.
- An online time analysis that looks at the times a user logs on/off to the computer and/or particular services and graphs them.

- A tool that extracts GPS coordinates from all EXIF information and plots geographically.
- A geographic distribution tool that geolocates websites visited.
- A directory analysis tool that highlights unusual directory structures (by name/depth/etc).
- A connected devices tool that extracts, cleans, and categories all USB connected devices.
- A sentiment analysis tool that identifies documents/emails written by the subject and classifies them.
- An email/chat analysis tool that plots conversations in a meaningful way for psychological analysis.

The tool must first be described and approved in a proposal (due week 3). The proposal should describe the overall functioning of the tool, limitations, what it will be written in, and how it will be tested (on what data). Further details will be provided on the proposal and report format in a separate handout.

The student must demonstrate the tool on the final two days of class in a 20 – 30 minute demonstration and submit a single-spaced paper, 10 point font, default margins, between 6 and 10 pages with references describing the tool, the reasoning behind it, similar tools (or research), and the results of testing the tool. The paper must be fully referenced using any standardized format (IEEE, ACM, APA, etc). Since Word has built-in spelling and grammar checking, these types of errors are not expected.

Grading Policy

Attendance and Class Participation	20%
Case Study	30%
Tool Construction/Demo	30%
Research Paper	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	1/27	Why Study Digital Profiling?	Turvey (Chapters 1-3,5) Goodman	
2	2/3	Building a Digital Profile Behavioral Analysis Principles	Rogers	
3	2/10	Digital Victimology	Herley	Proposals Due
4	2/17	Criminal Motivation, MO, and Signature	Turvey (Chapters 13 and 14)	Case Studies Begin
5	2/24	Sources of Digital Profile Information/Constructing a Digital Profile	Marrington	
6	3/3	Case and Offender Linkage	Turvey (Chapter 14)	
7	3/10	Spring Break	Turvey (Chapter 15)	
8	3/17	Fraud and Identity Theft	Allison	
9	3/24	Online Child Exploitation	Lanning, Wolak	
10	3/31	Insider Threat	Schultz, Claycomb	
11	4/7	Hackers, Pirates and Hacktivists	Mentor, Denning Lai	
12	4/14	Virus Writers and Cyberterrorists	Gordon	
13	4/21	Using Profile Information in Search Warrants and Court	Brenner	

14	4/28	TBD – Advanced Topics		
15	5/5	Final Presentations		Final Papers Due

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

Last day to add classes 29 Jan
Last day to drop with no tuition liability 29 Jan
Last day to drop (33% penalty) 11 Feb
Last day to drop (67% penalty) 21 Feb

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.