DFOR 771 Sec 001
Advanced Topics in Computer Forensics – Digital Profiling
George Mason University
Spring 2022

ADMINISTRATIVE INFORMATION

Instructor: *Chad M.S. Steel*
E-mail: *csteel@gmu.edu*
Office Hours: *Tuesdays (virtual after class) or upon request*

COURSE DESCRIPTION

DFOR 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. This class is primarily in-person, however synchronous online classes may be held throughout the semester. 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(s).
- Discussion of Readings.
- Interactive Lecture on Key Principles.
- Case Studies.

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
    - Identity and 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:

Al Mutawa, Noora, Joanne Bryce, Virginia NL Franqueira, Andrew Marrington, and Janet C. Read. "Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes." *Digital Investigation:*28 (2019): 70-82.

Bednar-Schadle, Teresa. "Misinterpretation of Digital Evidence: Recommendations to Improve Data Integrity." PhD diss., Utica College, 2018

Fortin, Francis, and Jean Proulx. "Sexual interests of child sexual exploitation material (CSEM) consumers: Four patterns of severity over time." International journal of offender therapy and comparative criminology 63, no. 1 (2019): 55-76.

Hinchliffe, Alexander. "Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime." *Computer Fraud & Security* 2017, no. 5 (2017): 5-9.

Internet Crime Complaint Center. "Internet Crimes Report – 2020". *Tech Report* (2020).

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

Maasberg, Michele, John Warren, and Nicole L. Beebe. "The dark side of the insider: detecting the insider threat through examination of dark triad personality traits." In *2015 48th Hawaii International Conference on System Sciences*, pp. 3518-3526. IEEE, 2015.

McGovern, Virginia, and Francis Fortin. "The Anonymous collective: Operations and gender differences." Women & Criminal Justice 30, no. 2 (2020): 91-105.

National Crime Agency, "Pathways into Cybercrime", 2017.

Stachl, C., Au, Q., Schoedel, R., Buschek, D., Völkel, S., Schuwerk, T., ... & Bühner, M. (2019). Behavioral patterns in smartphone usage predict big five personality traits

White, Ryan, Puneet V. Kakkar, and Vicki Chou. "Prosecuting darknet marketplaces: challenges and approaches." US Att'ys Bull. 67 (2019): 65.

COURSE REQUIREMENTS, EVALUATION CRITERIA, AND GRADING SCALE:

1. Class Discussions: Each student must participate actively in discussions to receive class credit. Participation includes attending the synchronous lectures, 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 be provided guidance on improving it if needed. Participation should be throughout the semester – asking 20 questions the final day of class 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 20 minutes in length, and will be presented at the start of each class session. The case study/profile is detailed in a separate handout.

3. Digital Profiling Exercises: Students will complete 4 team 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	40%

TOTAL: 100 points

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 an exercise) 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	1/25	Why Study Digital Profiling?	IC3 Report	
2	2/1	Building a Profile	Bednar-Schadle	Case Study Choices Due
3	2/8	Personality and Criminality	Stachl et al.	
4	2/15	Behavioral Principles	Lickiewicz	Case Studies Begin
5	2/22	Insider Threat	Maasberg	
6	3/1	Digital Victimology	Hinchcliffe	
7	3/8	Interviewing	N/A	N/A

8	3/15	SPRING RECESS - INDEPENDENT WORK ON PROJECTS - NO CLASS		
9	3/22	Online Child Exploitation	Fortin & Proulx	
10	3/29	Economics of Cybercrime	National Crime Agency	
11	4/5	MO, Ritual, and Signature	Mutawa	
12	4/12	Networks, Ideology, and International Criminality	McGovern & Fortin	
13	4/19	Attribution, Defenses, and Court Concerns	White	
14	4/26	Advanced Topics/Makeup Day		
15	5/3	Advanced Topics/Makeup Day		

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

Last day to add classes 31 Jan
Last day to drop with no tuition liability 14 Feb

Attendance Policy

Students are expected to attend each in person and/or synchronous, online 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.

The material provided in the course is proprietary. Uploading this material anywhere without the express permission of the instructor is strictly prohibited and a violation of the Mason Honor Code.