Course Syllabus

University of Maryland - Shady Grove Campus
CCJS 318I: Introduction to Cyber Security and Digital Investigations
Spring, 2024 - Section ESG1

Course Information

Day/Time: Wednesday, 2 PM – 4:30 PM

Location: Shady Grove Campus, Building III, Room 4212

Course description: The majority of modern investigations conducted by law enforcement agencies (criminal investigations) and within private sector companies (HR investigations, internal/insider threat investigations, theft/fraud, and others) contain digital evidence and/or cyber security component. This course will introduce students to the field of cyber security, with focus on how cyber security and digital investigation techniques are used by investigators in government, law enforcement, and private sector roles. The course will cover topics such as cyber security roles and responsibilities in a typical organization, identifying and collecting digital evidence and digital records for investigations, methods for conducting investigations using technical data, interview techniques in digital investigations, and other related topics. This course will also provide an introduction to more advanced topics such as digital forensics, eDiscovery, and open-source intelligence.

Required reading:

- Reading assignments will consist of research papers, scholarly journal articles, and online resources. They will be posted on ELMS from week-to-week.

Instructor Contact Information

John Conroy, M.S., CFCE, CCI, CCCE

- Office hours: Office hours are provided by appointment (typically before and/or after class). Students may make an appointment at any time during class or via e-mail.
- E-mail: jwconroy@umd.edu
- Phone Number: 240-753-2099

Michael Yu, B.S., CFCE, CCCE

- Office hours: Office hours are provided by appointment (typically before and/or after class). Students may make an appointment at any time during class or via e-mail.
- E-mail: mikeyu41@gmail.com
- Phone Number: 240-773-6969

Grading

Grading Scale		
A		90 – 100 points
B		80 - 89 points
C		70 – 79 points
D		60 – 69 points
F		0 - 60 points

Grading Criteria	
Class Participation	15% of final grade
Mid-Term Exam	25% of final grade
Case Studies	35% of final grade
Final Exam	25% of final grade

Course Format/Hybrid

This course is presented in hybrid format. Some classes will be presented in person at the USG Campus and some classes will be delivered via Zoom. All classes will be delivered on Wednesdays between 2 PM and 4:30 PM. Students are expected to attend all classes during the time period they are delivered and in the venue the class is delivered that week.

For virtual classes via Zoom, students are required to have their cameras on for the duration of the class. Students not complying with this requirement will be considered non-participative.

The following classes will be presented **in-person**, at **Shady Grove Campus, Building III, Room 4212:**

- 01/24/24
- 02/07/24
- 02/28/24
- 03/13/24 (Mid-Term Exam)
- 03/27/24
- 04/10/24
- 04/24/24
- 05/08/24 (Final Exam)

The following classes will be presented **virtually,** via **Zoom**. You can access these classes via ELMS during the class meeting time:

- 01/31/24
- 02/14/24
- 02/21/24
- 03/06/24
- 04/03/24
- 04/17/24
- 05/01/24

Learning Outcomes

At the conclusion of this course, students will be able to:

- Understand the role of digital evidence and cyber security in modern investigations conducted by law enforcement and private sector companies.

- Identify and describe the key responsibilities of cyber security professionals in various organizational settings.

- Explain the concepts of cyber attackers and cyber defenders and their impact to the security of organizations and government agencies.

- Gain familiarity with basic investigation methods and techniques applicable to both traditional and digital investigations.

- Analyze the importance of interview and interrogation techniques in digital investigations, including the use of witness statements and confessions as evidence.

- Apply investigative methods to digital and cyber investigations, considering unique considerations and challenges in the digital realm.

- Examine cyber attack tactics, techniques, and procedures (TTPs), including reconnaissance, scanning, exploitation, and covering tracks.

- Understand specific cyber threats such as ransomware attacks, blockchain, and cryptocurrency investigations, and advanced persistent threats (APTs).

- Gain familiarity with open-source intelligence techniques, insider threat investigations, digital forensics, and emerging trends in the cyber investigations field.

Class Participation / Attendance Policy

Students are expected to participate in class. There will be various opportunities throughout the course to participate. Students will earn class participation points by attending class on time and participating in class discussions and asking/responding to questions in class. For each class that a student attends on time and actively participates, the student will receive 3 class participation points. Missed classes, late arrivals, and failure to participate will result in reduction of points. An unexcused absence will result in the loss of class participation points for that day. It is not possible to participate in class if you are not present in class. Students are asked not to use cell phones or be distracting to others during class. Students are permitted to use laptop computers in class for note-taking purposes and use relating to class. Students who use cell phones and computers in class for any other reasons than those permitted by this syllabus will be penalized class participation points. A student's final class participation grade will be calculated at the end of the semester and will account for 10% of the student's final grade for the course.

Please note that this course follows the university's "Excused Absence Policy" as outlined on https://www.ugst.umd.edu/courserelatedpolicies.html and https://www.president.umd.edu/sites/president.umd.edu/files/files/documents/policies/V-100G.pdf

Students are expected to take full responsibility for their own academic work and progress. Students, to progress satisfactorily, must meet all of the requirements of each course for which they are registered. Students are expected to attend classes regularly. Consistent attendance offers students the most effective opportunity to gain command of course concepts and materials. Excused absences must be requested promptly and must be supported by appropriate documentation.

Excused absences do not alter the academic requirements for the course. Students are responsible for information and material missed on the day of absence. Students are within reason entitled to receive any materials provided to the class during the absence. Students are responsible for making provision to determine what course material they have missed and for completing required exercises in a timely manner.

Events that justify an excused absence include:

- Religious observances
- Mandatory military obligation
- Illness of the student or illness of an immediate family member
- Participation in university activities at the request of university authorities
- Compelling circumstances beyond the student's control (e.g., death in the family, required court appearance)

Excused absences do not alter the academic requirements for the course. Students are responsible for information and material missed on the day of absence. Students are, within reason, entitled to receive any materials provided to the class during the absence. Students are responsible for making provision to determine what course material they have missed and for completing required exercises in a timely manner. Students with excused absences will be entitled to a makeup exam at a mutually-agreed upon time between the professor and the student. However, students are reminded that except for emergencies, such arrangements must be made prior to the exam or assignment in which the student will miss due to an excused absence.

Course Related Policies

Students are strongly encouraged to review the University's course-related policies and their rights related to various topics including: Academic Integrity, Code of Student Conduct, Sexual Misconduct, Discrimination, Accessibility, Attendance/Absences/Missed Assignments, Student Rights, Official UMD Communication, Mid-Term Grades, Complaints About Course Final Grades, Copyright and Intellectual Property, Final Exams, Course Evaluations, and Campus Resources. **Students should view these policies at the following URL.**

http://www.ugst.umd.edu/courserelatedpolicies.html

Please note that this course will follow the University's "course related policies" detailed above and these are incorporated into this syllabus herein by reference.

Inclement weather policy / Emergency evacuation

In case of inclement weather, contact the Shady Grove campus hotline 301-738-6012. If class is cancelled for any reason, I will contact all students as soon as I am aware of the cancellation via e-mail and/or Elms/Canvass. Students may also sign up to receive electronic notification via www.shadygrove.umd.edu/weather/ . In case of emergency, follow the emergency procedures discussed the first day of class and as posted in the building.

Students are strongly encouraged to sign up for the Shady Grove Campus Alert System (which is separate from the UMD College Park Alert System), at http://shadygrove.umd.edu/ (Click "USG Alerts" on the lower right-hand corner and sign up with one or multiple phone numbers and e-mail addresses.

Mid-Term and Final Exams

Students will be required to take a mid-term exam on **03/13/24 from 2:00 PM to 4:30 PM** and a final exam on **05/08/2024 from 2:00 PM to 4:30 PM.** The mid-term and final exams will consist of multiple choice and true/false questions. Unless prior permission is given, all students are required to take the examination on the day it is administered. **Before the mid-term and final exams an extensive exam review will be conducted. Students are strongly encouraged to attend these sessions.** Make-up examinations will only be authorized for reasons consistent with University of Maryland policy. If prior permission is not obtained, students will receive a zero ("0") for that examination. If a make-up exam is granted, the make-up exam will consist of different questions than those originally offered. Both the mid-term and final exams will each account for 25% each of the student's final grade in the course. The mid-term exam will be taken in class and will be **closed book.** The final exam will be taken in class and will be **closed book.** The final exam will be cumulative, covering material that may have also been covered in the mid-term.

Case Studies

Throughout the course, students will be assigned a total of 5 case studies. Each case study will focus on a specific cyber incident or investigation (either real or fictional), with instructions on how to prepare the report/paper/ deliverable for that case study. The actual deliverable/work product may vary from case study to case study. For example, the scenario in one case study may be that you are asked to draft a report summarizing your findings from the case study. In another case study, you may be asked to answer direct questions in Quiz format from the case study. In another, you may be asked to draft PowerPoint slides and present to the instructors via Zoom.

Academic Integrity

You should be familiar with UMD's Academic Integrity Policy, which applies in this course:
https://president.umd.edu/sites/president.umd.edu/files/files/documents/policies/III-100A.pdf

UMD maintains a commitment to the principles of truth and academic honesty. Accordingly, the Code of Academic Integrity is designed to ensure that the principle of academic honesty is upheld. While all members of the University share this responsibility, the Code of Academic Integrity is designed so that special responsibility for upholding the principle of academic honesty lies with you as a student.

To promote academic honesty on campus you will be asked by your course instructors to write by hand and sign the following pledge on every examination, paper or other academic exercise. Writing this pledge will serve as a reminder of your commitment to academic integrity.

I pledge on my honor that I have not given or received any unauthorized assistance on this examination.

Failure to sign the pledge is not a violation of the Code of Academic Integrity, but neither is it a defense in case of violation of this Code. Students who do not sign the pledge will be given the opportunity to do so. Refusal to sign must be explained to the instructor. Signing or non-signing of the pledge will not be considered in grading or judicial procedures. Material submitted electronically should contain the pledge, submission implies signing the pledge. On examinations, no assistance is authorized unless given by or expressly allowed by the instructor. On other assignments, the pledge means that the assignment has been done without academic dishonesty, as defined below.

The pledge is a reminder that you as a University of Maryland student carry the primary responsibility for academic integrity. The meaningfulness of your degree depends on it. Academic dishonesty is a corrosive force in the academic life of a university. It jeopardizes the quality of education and depreciates the genuine achievements of others. All members of the University community-students, faculty, and staff share the responsibility and authority to challenge and make known acts of apparent academic dishonesty.
Code of Academic Integrity defines five major types of Academic Dishonesty:

- CHEATING: fraud, deceit, or dishonesty in any academic course or exercise in an attempt to gain an unfair advantage and/or using or attempting to use unauthorized materials, information, or study aids in any academic course or exercise.

- FABRICATION: unauthorized falsification or invention of any information or citation in an academic course or exercise.

- FACILITATING ACADEMIC DISHONESTY: knowingly helping or attempting to help another to violate any provision of this Code.

- PLAGIARISM: representing the words or ideas of another as one's own in any academic course or exercise.

- SELF-PLAGIARISM: the reuse of substantial identical or nearly identical portions of one's own work in multiple courses without prior permission from the current instructor or from each of the instructors if the work is being submitted for multiple courses in the same semester.

The Office of Student Conduct will contact you if you have been reported for a violation of the Code of Academic Integrity. Your course instructor may or may not mention the report to you. The instructor may not grade or record the grade of an assignment that is related to the report. Information about the resolution options are outlined in the University of Maryland Code of Academic Integrity. Note that the normal sanction for a violation is the grade of "XF" for the course.

To promote academic honesty on campus you will be asked by your course instructors to type, agree to, or write by hand and sign the following pledge on every examination, paper or other academic exercise. Writing this pledge will serve as a reminder of your commitment to academic integrity: ***I pledge on my honor that I have not given or received any unauthorized assistance on this examination.***

Use of Generative AI Technologies (such as ChatGPT)

You may not use Generative AI technologies to generate content for any work you submit in the course. This includes your case studies, responses to questions, responses on the mid-term and final exams, and any other course material. Please note that many products incorporate generative AI into them. Grammerly, includes features that generated responses from ChatGPT so if you paste your work into Grammerly, it may incorporate Generative AI responses into its output. It is your responsibility to ensure that the work submitted is your own and that it is in compliance with this course's and UMD's academic integrity expectations. Note that the instructor for this course will employ technology designed to detect instances of plagiarism and use of generative AI technologies. Anybody who is suspected as having used generative AI in any assignment will be referred to the Office of Student Conduct.

Accessibility / Students Requiring Special Accommodations

This course follows the University's policy on Course Accessibility / Special Accommodations outlined here: VI-1.00(D) University of Maryland Disability & Accessibility Policy and Procedures

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The University of Maryland provides reasonable accommodations to qualified individuals. Reasonable accommodations shall be made in a timely manner and on an individualized and flexible basis.

Discrimination against individuals on the grounds of disability is prohibited. The University also strictly prohibits retaliation against persons arising in connection with the assertion of rights under this Policy.

Accessibility & Disability Service (ADS) facilitates reasonable accommodations to qualified individuals. For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301.314.7682, or adsfrontdesk@umd.edu. More information is available at counseling.umd.edu/ads/.

After receiving an Accommodations Letter from ADS, as a student you are expected to meet with each course instructor, to provide them with a copy of the Accommodations Letter and to obtain their signature on the Acknowledgement of Student Request form. You and your instructors will discuss a plan for how the accommodations will be implemented in the course throughout the semester. Specific details regarding the implementation of certain ADS approved accommodations agreed upon between you as the student and the individual course instructor must be documented on a Detailed Implementation Plan, signed by you and the instructor, and submitted to ADS. You as the student are responsible for submitting the signed copy of the Detailed Implementation Plan to ADS and retaining a copy for your records. For further assistance, contact adsfrontdesk@umd.edu or 301-314-7682.

Course Evaluations

Your participation in CourseEvalUM course evaluations is both your right and responsibility as a student. Your feedback is confidential and important to the improvement of teaching and learning at the University of Maryland as well as to the tenure, promotion, and retention of its instructors. You can go directly to the website (www.courseevalum.umd.edu) to complete your evaluations.

Copyright and Intellectual Property

Class lectures and other course materials are copyrighted and may not be reproduced for anything other than your personal use without the permission of the course instructor. Course materials are the property of the course instructor – do not sell them, do not post them on a website. Be aware that copyright infringements may be referred to the Office of Student Conduct. As a student, you own the work that you create as part of your University academic and research activities. Full details and a few limitations are found within the policy.

The lectures delivered in course and the course materials that are created/distributed in this course are protected by federal copyright law. Students are permitted to take notes and will be given access to class PowerPoint slides and other course material via ELMS. Access or license to course material (including presentations, lectures, written documentation, etc.) does not constitute waiver of intellectual property rights/copyright and does not transfer ownership of said material to the student. Students may not reproduce or distribute the lectures, slides, presentation material, articles, or other course material without explicit written consent from the instructor. Any student who wishes to record the all or part of this course must receive prior permission and written consent from the instructor. Recording any conversation without the express permission of all parties involved in the State of Maryland is violation of Maryland Criminal Law.

Classes / Topics

Class 1	01/24/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • Introduction and Course Overview • Syllabus Review • Introduction to the Cyber Security/Cyber Investigations Field • Basic Networking and the Internet • Introduction to Cyber Attacks/Cyber Defense
		Reading Assignments for Next Class: • To be assigned on ELMS.
Class 2	01/31/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Basic Investigations Methods
		Reading Assignments for Next Class: • To be assigned on ELMS.
Class 3	02/07/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • Introduction to Interview and Interrogation Techniques • Witness Statements/Testimonial Evidence • Statements and Confessions as Evidence **Case Studies Assigned:** • Case Study 1
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.
Class 4	02/14/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Applying Investigative Methods to Digital/Cyber Investigations • Unique Considerations in Cyber Investigations • Digital Evidence
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.

Class 5	02/21/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Managing a Cyber Investigative/Digital Forensics Unit • Cyber Incident Management • Cyber Threat Intelligence **Case Studies Due** • Case Study 1 Due **Case Studies Assigned** • Case Study 2 Assigned
For next class:		**Reading Assignments for Next Class:** ● To be assigned on ELMS.
Class 6	02/28/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • Introduction to Cyber Attack Tactics, Techniques, and Procedures (TTPs) • Cyber Attack TTPs: Reconnaissance • Cyber Attack TTPs: Scanning
		Reading Assignments for Next Class: To be assigned on ELMS.
Class 7	03/06/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Cyber Attack TTPs: Exploitation • Cyber Attack TTPs: Persistence • Cyber Attack TTPs: Covering Tracks **Case Studies Due** • Case Study 2 Due **Case Studies Assigned** • Case Study 3 Assigned
For next class:		**Review all course materials for Mid-Term Exam.**

Class 8	03/13/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Exams:** • **Mid-Term Exam**
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.
Class 9	03/27/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • **Ransomware Attacks and Investigations** • **Blockchain and Cryptocurrency Investigations**
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.
Class 10	04/03/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Advanced Persistent Threat (APT) Attacks • Cyber Espionage and Cyber Warfare • Malware Analysis/Reverse Engineering **Case Studies Due** • Case Study 3 Due **Case Studies Assigned** • Case Study 4 Assigned
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.
Class 11	04/10/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • **Cyber Incident Response (Part 1)** • **Cyber Vulnerability Assessments**
For next class:		**Reading Assignments for Next Class:** • To be assigned on ELMS.

Class 12	04/17/24	**Location:** *This class will be virtually, via Zoom @ 2 PM ET. Zoom meeting details will be posted on ELMS.* **Topics:** • Advanced Persistent Threat (APT) Attacks • Cyber Espionage and Cyber Warfare • Malware Analysis/Reverse Engineering **Case Studies Due** • Case Study 4 Due **Case Studies Assigned** • Case Study 5 Assigned
Class 13	04/24/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Topics:** • Introduction to Open-Source Intelligence • Introduction to Insider Threat Investigations
Class 14	05/08/24	**Location:** *This class will be held in-person at the Shady Grove Campus* **Exams:** • **FINAL EXAM**