



## Applied Reverse Engineering (HACS408E)

**Term:** Fall 2025

**Instructors:** Chase Kanipe, Luke Mains

**Pronouns:** he/him, he/him

**Email:** [ckanipe@umd.edu](mailto:ckanipe@umd.edu), [lmains@umd.edu](mailto:lmains@umd.edu)

**Office Hours:**

- Chase: Monday Evenings 6:00-7:00
- Luke: Friday Evenings 6:00-7:30

**Credits:** 3

**Course Dates:** Sep 03, 2025 - Dec 17, 2025

**Course Times:** Wednesday 5:00 pm - 7:45 pm

**Classroom:** PHY 4311B

## Course Description

This course will introduce students to the tools and techniques required to analyze the security properties of various systems. Topics covered will include assembly language, executable file formats, operating system internals, and the static/dynamic analysis of compiled binaries. Students will apply these concepts to real-world scenarios like malware analysis and vulnerability analysis with interactive labs, at-home assignments, and a final project.

## Learning Outcomes

After successfully completing this course you will be able to:

- **Use a variety of popular reverse engineering tools**, including:
  - Binary Ninja
  - Debuggers (GNU Debugger, Windbg)
  - Wireshark
  - Shell scripting and command line utilities
- **Understand binary file formats how to approach unknown binary data**
  - Triage, extract and analyze unknown binary files
  - Executable file formats such as ELF and PE
- **Operating systems concepts**
  - Windows and Linux operating system APIs
  - Reversing programs written for both Windows and Linux
- **Reverse engineer a variety of binary executables**, including:
  - Programs written in a variety of languages (C, C++, Java, Go)
  - Malicious programs (including how to handle anti reversing techniques)
- **Understand and interpret network packets**
  - Passively sniff and record local network traffic
  - View the structure of packets for standard protocols such as TCP, UDP, HTTP(S), QUIC, etc.
  - Analyze web traffic to find indicators of malicious activity
- **Present reverse engineering projects to a technical audience**
- **Understand how attackers gain access to computer systems**
  - Exploit buffer overflow vulnerabilities in computer programs
  - Understand standard mitigations such as stack canaries and ASLR
- **Learn to apply reversing techniques to other problem domains**
  - Embedded devices and firmware analysis
  - Reverse engineer android applications

- Understand the challenges associated with modern languages such as Go or Rust
- **Document and organize artifacts recovered from reverse engineering into a technical report.**

## Required Resources

- Course Website: <https://hacs408e.umd.edu>
- All software used in this class will be free and/or open source. Students will be provided a Windows and Linux VM hosted on ACES infrastructure which will be accessed remotely.. Alternatively, students can run their own virtual machine using VMWare or Virtualbox or another hypervisor. The following software will be used in this class:
  - Standard Windows / Linux Command line Tools
  - Binary Ninja
  - Gnu Debugger / Windbg
  - Wireshark

## Course Structure

Since this is an applied course, it will be very focused on labs modeled after real-world reverse engineering tasks. Students are expected to attend class and attempt the labs, which are used to introduce the skills necessary to complete the homeworks. The in-person nature of this class will push you to take an active role in the learning process. You will do this by engaging and collaborating with other students and the instructor on a regular basis both, in live sessions, as well as through group work and activities.

## Tips for Success in this Course

1. **Participate.** I invite you to engage deeply, ask questions, and talk about the course content with your classmates. You can learn a great deal from discussing ideas and perspectives with your peers and professor. Participation can also help you articulate your thoughts and develop critical thinking skills.
2. **Manage your time.** Students are often very busy, and I understand that you have obligations outside of this class. However, students do best when they plan adequate time that is devoted to course work. Block your schedule and set aside plenty of time to complete assignments including extra time to handle any technology related problems.
3. **Login regularly.** I recommend that you log in to ELMS-Canvas several times a week to view announcements, discussion posts and replies to your posts. You may need to log in multiple times a day when group submissions are due.
4. **Do not fall behind.** This class moves at a quick pace and each week builds on the previous content. If you feel you are starting to fall behind, check in with the instructor as soon as possible so we can troubleshoot together. It will be hard to keep up with the course content if you fall behind in the pre-work or post-work.
5. **Use ELMS-Canvas notification settings.** Pro tip! Canvas ELMS-Canvas can ensure you receive timely notifications in your email or via text. Be sure to enable announcements to be sent instantly or daily.
6. **Ask for help if needed.** If you need help with ELMS-Canvas or other technology, IT Support. If you are struggling with a course concept, reach out to the instructors and your classmates for support.

## Policies and Resources for Undergraduate Courses

It is our shared responsibility to know and abide by the University of Maryland's policies that relate to all courses, which include topics like:

- Academic integrity
- Student and instructor conduct
- Accessibility and accommodations
- Attendance and excused absences
- Grades and appeals
- Copyright and intellectual property

Please visit [www.ugst.umd.edu/courserelatedpolicies.html](http://www.ugst.umd.edu/courserelatedpolicies.html) for the Office of Undergraduate Studies' full list of campus-wide policies and follow up with me if you have questions.

## Course Guidelines

### Names/Pronouns and Self-Identifications:

The University of Maryland recognizes the importance of a diverse student body, and we are committed to fostering inclusive and equitable classroom environments. I invite you, if you wish, to tell us how you want to be referred to in this class, both in terms of your name and your pronouns (he/him, she/her, they/them, etc.). Keep in mind that the pronouns someone uses are not necessarily indicative of their gender identity. Visit [trans.umd.edu](http://trans.umd.edu) to learn more.

Additionally, it is your choice whether to disclose how you identify in terms of your gender, race, class, sexuality, religion, and dis/ability, among all aspects of your identity (e.g., should it come up in classroom conversation about our experiences and perspectives) and should be self-identified, not presumed or imposed. I will do my best to address and refer to all students accordingly, and I ask you to do the same for all of your fellow Terps.

### Communication with Instructor:

If you need to reach out to the instructors, please email us at [ckanipe@umd.edu](mailto:ckanipe@umd.edu), and [lmains@umd.edu](mailto:lmains@umd.edu). Please DO NOT email us with questions that are easily found in the syllabus or on ELMS (i.e. When is this assignment due? How much is it worth? etc.) but please DO reach out about personal, academic, and intellectual concerns/questions. While we will do our best to respond to emails within 24 hours, you will more likely receive email responses from us after 5:00 pm EST, weekdays or the next day.

ELMS: We will send IMPORTANT announcements via ELMS messaging. You must make sure that your email & announcement notifications (including changes in assignments and/or due dates) are enabled in ELMS so you do not miss any messages. You are responsible for checking your email and Canvas/ELMS inbox with regular frequency.

## Communication with Peers:

You will be given access to the class discord server through ELMS. This is meant to be a space for you to connect with your peers, ask questions, and plan for your midterm presentation. With a diversity of perspectives and experience, we may find ourselves in disagreement and/or debate with one another. As such, it is important that we agree to conduct ourselves in a professional manner and that we work together to foster and preserve a virtual classroom environment in which we can respectfully discuss and deliberate controversial questions. I encourage you to confidently exercise your right to free speech—bearing in mind, of course, that you will be expected to craft and defend arguments that support your position. Keep in mind, that free speech has its limit and this course is NOT the space for hate speech, harassment, and derogatory language. I will make every reasonable attempt to create an atmosphere in which each student feels comfortable voicing their argument without fear of being personally attacked, mocked, demeaned, or devalued.

Any behavior (including harassment, sexual harassment, and racially and/or culturally derogatory language) that threatens this atmosphere will not be tolerated. Please alert me immediately if you feel threatened, dismissed, or silenced at any point during our semester together and/or if your engagement in discussion has been in some way hindered by the learning environment.

## Major Assignments

### Homework Assignments

- There will be a homework assignment associated with almost every topic covered in class. Assignments will be grouped together and due approximately every two weeks. Please see the schedule below (and on the class webpage) for exact due dates. Every assignment will require understanding the tools and techniques described in the associated week's lecture. Students must complete a write-up of their results, explaining their analysis methods and possibly answering some questions. You must submit a pdf copy of the report to ELMS with working images.
- There will be **10 Homework Assignments** out of the 14 weeks of actual lectures. Each homework will be announced and can be found in the corresponding week tab of the class website, or in ELMS.

### Quizzes

- There will be 3 small quizzes spread throughout the semester. Each quiz will be announced the week before and will take place during the first 15-30 minutes of class a week from the announcement.
- Quizzes may include questions from all course content covered, not just the information since the last quiz. However these will likely be biased towards more recent lectures.

### Participation & Engagement

- During live sessions, students will work on multiple labs and are expected to submit documents with their answers to the questions for each lab at the end of class. If you miss class, you can still complete the labs and submit them after. Please let both of the instructors know if you will not be able to make it to class.
- Labs are graded but not harshly. As long as you try to answer the questions as best you can, you'll get full points.

### Team Presentation

- At the midpoint of the semester, students will be split into groups of 4 and given a password protected zip file containing a live malware sample to analyze. DO NOT run this program on your personal laptop. Each group will present two weeks from the announcement with an analysis of the software. The goal is not necessarily to gain a complete understanding of the malware in two weeks, but to conduct open

source research, demonstrate reverse engineering techniques learned in class, and present your findings to a technical audience of your peers.

### Final Project

- In lieu of a final exam students will be given a final project to complete. Previously this has been a challenging executable to reverse engineer but it may not be the same year to year. A final report will be due by 11:59 pm the Sunday before finals week.

## Grading Structure

Assignment	Percentage % (Distributed evenly across assignments)
Homework	40%
In-class Participation (Labs)	10%
Quizzes	10%
Team Presentation	20%
Final Project	20%
Total	100%

## Academic Integrity







For this course, some of your assignments will be collected via Turnitin on our course ELMS page. I have chosen to use this tool because it can help you improve your scholarly writing and help me verify the integrity of student work. For information about Turnitin, how it works, and the feedback reports you may have access to, visit [Turnitin Originality Checker for Students](#)

The University's Code of Academic Integrity is designed to ensure that the principles of academic honesty and integrity are upheld. In accordance with this code, the University of Maryland does not tolerate academic dishonesty. Please ensure that you fully understand this code and its implications because all acts of academic dishonesty will be dealt with in accordance with the provisions of this code. All students are expected to adhere to this Code. It is your responsibility to read it and know what it says, so you can start your professional life on the right path. **As future professionals, your commitment to high ethical standards and honesty begins with your time at the University of Maryland.**

It is important to note that course assistance websites, such as CourseHero, or AI-generated content are not permitted sources unless the instructor explicitly gives permission. Material taken or copied from these sites can be deemed unauthorized material and a violation of academic integrity. These sites offer information that might be inaccurate or biased and most importantly, relying on restricted sources will hamper your learning process, particularly the critical thinking steps necessary for college-level assignments.

Additionally, students may naturally choose to use online forums for course-wide discussions (e.g., Group lists or chats) to discuss concepts in the course. However, collaboration on graded assignments is strictly prohibited unless otherwise stated. Examples of prohibited collaboration include: asking classmates for answers on

quizzes or exams, asking for access codes to clicker polls, etc. Please visit the [Office of Undergraduate Studies' full list of campus-wide policies](#) and reach out if you have questions.

	 <b>OPEN NOTES</b>	 <b>USE BOOK</b>	 <b>LEARN ONLINE</b>	 <b>GATHER CONTENT With AI</b>	 <b>ASK FRIENDS</b>	 <b>WORK IN GROUPS</b>
In-Class Labs	✓	✓	✓	✓	✓	✓
Homework Assignments	✓	✓	✓	✓	---	---
Quizzes	✓	✓	✓	---	---	---
Team Project	✓	✓	✓	✓	✓	✓

## Grades

All assessment scores will be posted on the course ELMS page. If you would like to review any of your grades (including the final project), or have questions about how something was scored, please email the instructors to schedule a time for us to meet and discuss. We are happy to discuss any of your grades with you, and if we have made a mistake we will immediately correct it. Any formal grade disputes must be submitted in writing and within one week of receiving the grade.

Final letter grades are assigned based on the percentage of total assessment points earned. To be fair to everyone I have to establish clear standards and apply them consistently, so please understand that being close to a cutoff is not the same as making the cut (89.99  $\neq$  90.00). It would be unethical to make exceptions for some and not others.

Final Grade Cutoffs									
+	97.00%	+	87.00%	+	77.00%	+	67.00%	+	
A	94.00%	B	84.00%	C	74.00%	D	64.00%	F	<60.0%
-	90.00%	-	80.00%	-	70.00%	-	60.00%	-	

Your overall course grade will be calculated by multiplying the percentage of points for your assignments times the percentage value of the assignment type, summed together. For example, if you scored 120 out of 144 points on your homework assignments, then  $120/144 * 50 = 41.667$  would be how much your homework grade contributes to your overall course grade because the homework category is worth 50 percent of your total grade.

## Course Outline

Date	Week #	Topic	In Class	At Home
03 Sep 2025	1	File Identification and Extraction	Labs	HW 1
10 Sep 2025	2	Code Analysis	Labs	
17 Sep 2025	3	Binary Analysis I	Labs	HW 2
24 Sep 2025	4	Binary Analysis II	Labs, Quiz	
01 Oct 2025	5	Cryptography, Protocols	Labs	HW 3
08 Oct 2025	6	Malware I	Labs	
15 Oct 2025	7	Malware II	Labs, Quiz	
22 Oct 2025	8	Group Presentation	Group Presentation	
29 Oct 2025	9	Vulnerability Analysis I	Labs	HW 4
05 Nov 2025	10	Vulnerability Analysis II	Labs, Quiz	
12 Nov 2025	11	Kernel, Rootkits	Labs	HW 5
19 Nov 2025	12	Firmware, Memory Forensics	Labs	
26 Nov 2025		— Fall Break (no class) —	—	
03 Dec 2025	13	Mobile	Labs	
10 Dec 2025	14	CTF		CTF Writeup
17 Dec 2025		— Finals Week (no class) —		

**Note:** This is a tentative schedule, and subject to change as necessary – monitor the course ELMS page for current deadlines. In the unlikely event of a prolonged university closing, or an extended absence from the university, adjustments to the course schedule, deadlines, and assignments will be made based on the duration of the closing and the specific dates missed.

## Resources & Accommodations

### Accessibility and Disability Services

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 [Accessibility & Disability Service \(ADS\)](#) provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements.

For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at [adsfrontdesk@umd.edu](mailto:adsfrontdesk@umd.edu). Information about [sharing your accommodations with instructors](#), [note taking assistance](#) and more is available from the [Counseling Center](#).

### **Student Resources and Services**

Taking personal responsibility for your own learning means acknowledging when your performance does not match your goals and doing something about it. I hope you will come talk to me so that I can help you find the right approach to success in this course, and I encourage you to visit [UMD's Student Academic Support Services website](#) to learn more about the wide range of campus resources available to you.

In particular, everyone can use some help sharpening their communication skills (and improving their grade) by visiting [UMD's Writing Center](#) and schedule an appointment with the campus Writing Center.

You should also know there are a wide range of resources to support you with whatever you might need ([UMD's Student Resources and Services website](#) may help). If you feel it would be helpful to have someone to talk to, visit [UMD's Counseling Center](#) or [one of the many other mental health resources on campus](#).

### **Notice of Mandatory Reporting**

Notice of mandatory reporting of sexual assault, sexual harassment, interpersonal violence, and stalking: As a faculty member, I am designated as a "Responsible University Employee," and I must report all disclosures of sexual assault, sexual harassment, interpersonal violence, and stalking to UMD's Title IX Coordinator per University Policy on Sexual Harassment and Other Sexual Misconduct.

If you wish to speak with someone confidentially, please contact one of UMD's confidential resources, such as [CARE to Stop Violence](#) (located on the Ground Floor of the Health Center) at 301-741-3442 or the [Counseling Center](#) (located at the Shoemaker Building) at 301-314-7651.

You may also seek assistance or supportive measures from UMD's Title IX Coordinator, Angela Nastase, by calling 301-405-1142, or emailing [titleIXcoordinator@umd.edu](mailto:titleIXcoordinator@umd.edu).

To view further information on the above, please visit the [Office of Civil Rights and Sexual Misconduct's](#) website at [ocrsm.umd.edu](http://ocrsm.umd.edu).

### **Basic Needs Security**

If you have difficulty affording groceries or accessing sufficient food to eat every day, or lack a safe and stable place to live, please visit [UMD's Division of Student Affairs website](#) for information about resources the campus offers you and let me know if I can help in any way.

### **Veteran Resources**

UMD provides some additional support to our student veterans. You can access those resources at the office of [Veteran Student life](#) and the [Counseling Center](#). Veterans and active duty military personnel with special circumstances (e.g., upcoming deployments, drill requirements, disabilities) are welcome and encouraged to communicate these, in advance if possible, to the instructor.

### **Participation**

- Given the interactive style of this class, attendance will be crucial to note-taking and thus your performance in this class. Attendance is particularly important also because class discussion will be a critical component for your learning.
- Each student is expected to make substantive contributions to the learning experience, and attendance is expected for every session.



- Students with a legitimate reason to miss a live session should communicate in advance with the instructor, except in the case of an emergency.
- Students who miss a live session are responsible for learning what they miss from that session.
- Additionally, students must complete all readings and assignments in a timely manner in order to fully participate in class.

## **Course Evaluation**

Please submit a course evaluation through Student Feedback on Course Experiences in order to help faculty and administrators improve teaching and learning at Maryland. All information submitted to Course Experiences is confidential. Campus will notify you when Student Feedback on Course Experiences is open for you to complete your evaluations at the end of the semester. Please go directly to the [Student Feedback on Course Experiences](#) to complete your evaluations. By completing all of your evaluations each semester, you will have the privilege of accessing through Testudo the evaluation reports for the thousands of courses for which 70% or more students submitted their evaluations.

## **Copyright Notice**

Course materials are copyrighted and may not be reproduced for anything other than personal use without written permission.