# CSC 471: Modern Malware Analysis

Dr. Si Chen

Spring 2025

| | |
|---|---|
| **Office:** | *(25 University Ave. Room 131)* |
| **Department Phone:** | *(610-436-6998)* |
| **E-mail:** | `schen@wcupa.edu` |
| **Office Hours:** | Tuesday 10:00 AM - 12:00 PM |
| | Wednesday 11:00 AM - 12:00 PM |
| | Thursday 10:00 AM - 12:00 PM |
| **Course Mode of Instruction:** | In-person (Face-to-Face) |
| **Time and Location:** | *(T/Th 12:30-13:45 PM, Mitchell Hall 203)* |

## Catalog Information and Course Description

**Official Course Name and Number: CSC 471: Modern Malware Analysis**

Malware, a term used to describe various types of malicious software, poses a significant threat to both personal privacy and computer security. This can include viruses, adware, spyware, browser hijacking software, and fake security software. When installed on a computer, these programs can relay personal information to third parties without user consent, and may also contain worms and viruses that cause significant damage. As a result, the ability to detect, analyze, understand, control, and eradicate malware is becoming a crucial issue in both economic and national security.

This course aims to provide students with a comprehensive understanding of modern malware analysis techniques through lectures and hands-on interactive analysis of real-world samples. This includes exploring various recent attacks to develop a foundation and well-rounded view of cybersecurity research. Participants will also read and discuss research papers, and conduct an independent project on a topic related to cyber risk and malware analysis.

Upon completion of the course, students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis methods. This knowledge will enable them to effectively detect, understand, and mitigate the impact of malware threats.

**Enrollment Requirements:**
Prerequisites:

- CSC 302

- (CSC 231 or CSC 242)

As a 400-level course, this offering is intended for advanced students (primarily juniors and seniors). Although no reverse-engineering background is required, it is recommended that students possess:

- Basic programming concepts
- C programming language (pointers, arrays, loops, function calls)
- Unix/Linux basics (shell, gdb)
- Intel x86 assembly language and architecture
- Web programming concepts (HTML, HTTP, TCP, networking)

*Credits:* 3

### General Education or Additional Baccalaureate Requirement Status

This course is **not** an approved General Education or Additional Baccalaureate Requirement course.

## Required and Recommended Materials

### Required Textbook

None. All essential readings and materials will be posted or distributed as needed.

### Reference Books

- Monnappa K A, *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*, ISBN 978-1788392501
- Michael Sikorski, Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, 1st Edition, ISBN 978-1593272906

### Other Required Materials

- A computer capable of running VirtualBox or similar virtualization software
- Secure Remote Access (SSH or RDP) to Dr. Si Chen's Badger server (credentials to be provided)

## Course Student Learning Outcomes and Alignment

**Upon completion of this course, students will be able to:**

1. Perform static/dynamic analysis of system malware (Lab 1, Lab 3, Lab 5).
    - *Relates to Program SLO 1 (Analyze a complex computing problem).*

2. Build anti-malware systems (Lab 2, Lab 4).
   - *Relates to Program SLO 2 (Design, implement, and evaluate a solution).*
3. Work effectively as a team and use forensics tools (e.g., Volatility) to analyze kernel-level rootkits (Final Project).
   - *Relates to Program SLO 5 (Function effectively as a member or leader).*
4. Understand how to mitigate certain types of real-world malware attacks (Lab 1, Lab 2, Lab 4).
   - *Relates to Program SLO 1, 2.*
5. Communicate effectively about malware analysis methods, results, and ethical considerations (Final Project, Presentation).
   - *Relates to Program SLO 3 (Communicate effectively) and 4 (Recognize professional responsibilities).*

**Mapping to Program SLOs:**

- SLO 1: Analyze a complex computing problem
- SLO 2: Design, implement, and evaluate a computing-based solution
- SLO 3: Communicate effectively
- SLO 4: Recognize professional responsibilities
- SLO 5: Function effectively as a team member/leader

## Assignments/Activities Aligned to Course Outcomes

- **Lab Assignments (50% total)**:
  - Lab 1: "Hello World" DLL injection
  - Lab 2: Heuristic malware detection system
  - Lab 3: Stack analysis in Linux
  - Lab 4: Dynamic Heuristic Analysis Tool
  - Lab 5: Stuxnet
- **Group Project (25%)**: A team-based in-depth project to analyze kernel-level rootkits or other advanced malware, culminating in a written report.
- **Group Presentation (15%)**: Presentation on a selected research paper or specialized malware case study.
- **Attendance (10%)**: Regular participation and engagement are crucial.

## Course Evaluation Policy and Grading Scale

**Evaluation Breakdown:**

| Assignments | % of Grade | Details |
|---|---|---|
| Attendance/Participation | 10% | Attendance & engagement |
| 5 Malware Analysis Labs | 50% | (Labs 1 through 5) |
| Group Presentation | 15% | 1 Presentation (paper/topic) |
| Group Project | 25% | 1 Project (team-based) |

**Letter Grade Scale:** A [90–100], B [80–89], C [70–79], D [60–69], F [0–59]

**Nature and Timing of Evaluations:**

- You will receive feedback on each lab prior to the next lab's due date.
- At least one major grade (Lab or exam/quiz) will be posted in D2L before the final course withdrawal deadline, so you can make an informed decision.
- We will follow the official WCU final exam schedule. (If no exam is held, we will use that time for final project presentations or wrap-up as appropriate.)

**Retention of Evaluations:**

- In accordance with WCU policy, all final evaluations will be retained for at least one full semester.

## Tentative Course Schedule

*(Compliant with the academic calendar; no assignments will be due beyond the last day of the term.)*

| Week | Topic | Planned Activities/Assignments |
|---|---|---|
| 1 | Introduction, Overview, Syllabus | – |
| 2 | Basic Concepts, DLL Injection (1) | – |
| 3 | DLL Injection (2), Static Analysis, PE Format | Lab 1 assigned |
| 4 | PE Format, Static Analysis (Case Study) | Lab 2 assigned |
| 5 | Assembly, Disassembly Primer, IAT, EAT | – |
| 6 | Stack Fundamentals | – |
| 7 | Stack Frames | Lab 3 assigned |
| 8 | Dynamic Analysis | – |
| 9 | Hooks | Lab 4 assigned |
| 10 | IAT, IAT Hooks | – |
| 11 | Anti-virus, Dynamic Heuristic Analysis | – |
| 12 | API Hook, Stealth Process (Rootkit) | – |
| 13 | Kernel Mode Rootkit | Lab 5 assigned |
| 14 | Kernel Forensics | Final Project Work |
| 15 | Group Presentations | Group Presentation Due |

# Course Policies

## Attendance Policy (Undergraduate Student Attendance Policy)

Students are advised to carefully read and comply with the Undergraduate Student Attendance Policy in the WCU Catalog. Please note that the responsibility for meeting academic requirements rests with the student. This policy does not excuse students from completing required academic work. If you must miss class for an official university-sanctioned event, we will make every effort to provide a fair alternative or allow you to make up missed work.

## Late Assignments Policy

Late assignments will be accepted for **no penalty** if a valid excuse is **communicated to the instructor before the deadline**. Otherwise, **no credit** will be given for unexcused late submissions.

## Course Mode and Pre-Course Assignment Policy

This course is offered **in-person (face-to-face)**. We will **not** assign any coursework *prior* to the first official day of class, in accordance with WCU's Pre-Course Assignment Policy.

## Academic Integrity and Honesty

The Computer Science Department has adopted the following policies regarding academic dishonesty:

- First offense (assignment): Zero on that assignment. Second offense (assignment): F in the course.
- First offense (test/exam): F in the course.
- Cheating includes but is not limited to plagiarism, copying work without giving credit, submitting work prepared by another person, using unauthorized materials during exams, or taking an exam in someone else's name.

## ADA Policy and Accommodations for Disabilities

If you have a disability that requires accommodations under the Americans with Disabilities Act (ADA), please bring me your letter of accommodations and meet with me as soon as possible. Contact the Office of Services for Students with Disabilities at 610-436-3217 for more information, or visit: **wcupa.edu/ussss/ossd**.

## Electronic Mail Policy

Students are required to maintain access to their official WCU e-mail accounts and are responsible for all course-related communications sent there.

### Excused Absences Policy for University-Sanctioned Events

When you have an officially sanctioned event (e.g., athletics, band, required military service), notify me in advance with documentation. We will coordinate fair alternatives for missed work.

### Reporting Incidents of Sexual Violence (Title IX)

WCU faculty are mandatory reporters of any incidents of sexual violence shared by students. The only exceptions are incidents shared as part of a classroom discussion, assignment, or approved research. Further details are outlined in the Undergraduate Catalog.

### Emergency Preparedness

All students are encouraged to sign up for **WCU ALERT**, the official West Chester University emergency text message system: **wcupa.edu/wcualert/**.

### Final Examination Policy

We will follow the official WCU Final Exam schedule for Spring 2025. The official date/time of the final exam or project presentations will be announced in class and on D2L. No final exam may be given outside of the scheduled final examination time.

### APSCUF

I am a member of APSCUF, the Association of Pennsylvania State College and University Faculties. APSCUF strives for excellence in teaching, scholarship, and service.

### Other University-Wide Policies

Please refer to the official **Undergraduate Catalog** and relevant WCU policies (e.g., University-Excused Absences Policy, Distance Education Course Policy, etc.) for any topics not explicitly covered here.