

CSEC320 Computer Forensic and Incident Response Syllabus for Spring 2024

Corin Pitcher

28 Mar 2024

Overview

Introduction to the topics of computer forensic, computer crimes, response to security incidents, Cybercrime investigation and prosecution. Students will learn how an organization can setup a security response team, prepare for security incidents and manage these incidents.

Instructor Information

- **Instructor** Dr. Corin Pitcher
- ~~835, CDM Building, 243 S. Wabash Avenue~~ **Zoom meetings only this quarter**
- **Email** cpitcher@cs.depaul.edu
- **Tel** ~~+1 312 362 5248~~ **use email/Discord/Zoom this quarter**
- **Instructor Homepage**
<https://fpl.cs.depaul.edu/cpitcher/>
- **Course Homepage**
<https://fpl.cs.depaul.edu/cpitcher/courses/csec320/>
(for lectures slides, assignments, reading schedules, examples, learning outcomes)
- **LMS Homepage**
<https://d2l.depaul.edu>
(for grades and video recordings)

- **Discord Server** see Course Homepage
- **Lecture Videos** See Panopto via D2L

Prerequisites

If you are not sure that you have satisfied the prerequisites, speak to the instructor before the second lecture.

Prerequisite Courses

- **Host Based Security** (CSEC378) OR
- **Computer Systems II** (CSC374)

Prerequisite Skills

- You must be familiar with the Linux command-line environment and SSH before this course.

System Requirements

This course requires you to create multiple virtual machines on your own computer(s) for practice and coursework. You must have a computer that is capable of installing virtual machine software such as VMware, VirtualBox, Parallels, QEMU/KVM, or Proxmox. You will need at least 16GB of physical RAM and to assign 8GB of RAM to your VM. You will need at least 128GB of free disk space to assign to your VM (this can be on an external hard drive or SSD if necessary).

Textbooks

There are two required textbooks:

- File System Forensic Analysis
by Brian Carrier, 1st Edition.
Published by Addison-Wesley.
<https://www.amazon.com/System-Forensic-Analysis-Brian-Carrier/dp/0321268172/>

- Digital Forensics with Kali Linux: Enhance your investigation skills by performing network and memory forensics with Kali Linux 2022.x by Shiva V. N. Parasram, 3rd Edition. Published by Packt. <https://www.amazon.com/Digital-Forensics-Kali-Linux-investigation-dp-1837635153/>

Attendance and Participation

This class is asynchronous. There are lecture videos to watch each week, and it is expected that students try running/developing all of the examples from lectures and more themselves. Students are encouraged, but not required, to participate in the class Discord server or in office hours via Zoom to ask questions.

Students are expected to subscribe to the class Discord server, and read all messages within 24 hours normally (48 hours at the latest).

Assessment

The course grade will be based on:

Item	Weight
Homework assignments	60%
Midterm exam	20%
Final exam	20%

- The exams are multiple choice.
- The final exam is comprehensive, i.e., requires knowledge of the material covered in the entire course.

Exams

OL student exams must be proctored following the rules described at <https://www.cdm.depaul.edu/onlinelearning/Pages/Exams.aspx>.

OL students should register for the exams as soon as possible on D2L.

NOTE It is not possible to take exams online. Nor is it possible to proctor your own exam at home.

Classroom Instruction

This class will have 30 hours of combined lecture video and tutorial/office hours instruction.

Policies I

Changes to Syllabus

This syllabus is subject to change as necessary during the quarter. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L, and sent via Discord.

Attendance

1. Students are expected to ~~attend the class or~~ watch the recorded lectures for each week during that week, i.e., watch lectures for Week 1 during Week 1.
2. Students are expected to subscribe to the class Discord server, and read messages in a timely fashion.
3. The midterm exam and final exam dates are posted on the schedule on the [course homepage](#). You must attend the midterm and final exams if you are in the in-class section, and you must follow the CDM OL exam policies if you are in the OL section. A medical note will be required for an absence. Business trips or vacations are not valid reasons for missing the exam.
4. Online Learning students must ensure that they can take the proctored exams within the window specified on COL before the drop date. Please register for the exam as soon as possible.
5. **Lecture slides are a supplement to lectures only.** The slides are not intended to be read in lieu of listening to the lecture.

Homework

1. Students must keep backup copies of all submitted homework.
2. **Late homework submissions will not be accepted at all to ensure timely grading and because each assignment may be discussed in class.**

3. Submitted work must be worked on individually. You must not use or look at anyone else's solution, and you must clearly acknowledge any code that you obtain from other sources (such as books, magazines, or the Internet). If you are in any doubt, contact the instructor well before the submission date for advice. You may use as much code as you like (without acknowledgement) from the examples discussed in class. **Plagiarism will result in penalties up to and including failing the course. Submitting homework assignments copied from the Internet will result in a plagiarism report on your record.**

Expectations

1. Many tools will be used. Students are expected to learn these tools without the level of guidance that would be available for 100 and 200 level classes.
2. The course requires that students actively engage the material on your own. Students should not only read the notes and examples, but also perform their own similar experiments to reinforce the material.
3. Students must keep up with the assigned textbook reading.
4. All electronic interactions are an extension of the classroom and should be treated as such. While disagreement can be part of the discourse, online communication should remain respectful and appropriate rather than demeaning and/or unprofessional.

Policies II

Retro-Active Withdrawal

CDM understands certain extenuating circumstances can hinder one's ability for academic success and completion of course work. Please see <http://www.cdm.depaul.edu/Current%20Students/Pages/Enrollment-Policies.aspx> for additional information.

Absence Notifications

In order to petition for an excused absence, students who miss class due to illness or significant personal circumstances should complete the Absence

Notification process through the Dean of Students office. The form can be accessed at <http://studentaffairs.depaul.edu/dos/academicprocesses.html>. Students must submit supporting documentation alongside the form. The professor reserves the sole right whether to offer an excused absence and/or academic accommodations for an excused absence.

Academic Integrity and Plagiarism

This course will be subject to the university's academic integrity policy. More information can be found at <http://academicintegrity.depaul.edu/>. If you have any questions be sure to consult with your professor.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at: <http://cdm.depaul.edu/enrollment>

Incomplete Grades

An incomplete grade is defined in the Student Handbook as follows (note that the policy in the undergraduate student handbook applies to both undergraduate and graduate students): A temporary grade indicating that the student has a satisfactory record in work completed, but for unusual or unforeseeable circumstances not encountered by other students in the class and acceptable to the instructor is prevented from completing the course requirements by the end of the term. Please see <http://www.cdm.depaul.edu/Current%20Students/Pages/Grading-Policies.aspx> for additional information.

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential. To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at: csd@depaul.edu

- Lewis Center 1420, 25 East Jackson Blvd.
- Phone number: 312 362 8002
- Fax: 312 362 6544
- TTY: 773 325 7296

Dean of Students' Office

The Dean of Students' Office (DOS) helps students navigate the college experience, particularly during difficulty situations such as personal, financial, medical, and/or family crises. For a list of support services and advocacy information, please visit <http://studentaffairs.depaul.edu/dos/>.

Online Course Evaluations

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100% participation is our goal, students are sent periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in CampusConnect.