USC Viterbi School of Engineering

ITP-375: Digital Forensics and Cybersecurity Investigations

Units: 4
Fall 2024
Day/Time: MW 12pm–1:50pm
Location: RRB101

Instructor: Pierson Clair

Office: N/A
Office Hours/Open Lab:
TBD

Contact Info: pclair@usc.edu

Learning Assistant(s):

TBD

Digital Forensics & Cyber Security Program Open Lab Hours:

TBD

IT Help: Viterbi IT

Hours of Service:
Monday – Friday, 8:30 a.m. – 5:00 p.m.
Contact Info: DRB 205 (213) 740-0517
engrhelp@usc.edu

Piazza Enrollment:

TBD

Course Description

In 2023, the global cost of cybercrime is estimated at 8 trillion USD, and the average cost of a data breach in the US is 4.45 million USD. Computers are more of a threat today than ever before. From cyber-terrorism to identity theft, the digital age has brought about a change in the way that crime is being committed. The usage of computers in crime has led to the emerging field of computer forensics. This course is designed to give students the fundamental tools and techniques for investigating crime involving digital evidence.

This course is designed as an introductory course in computer forensics. Students will first understand the need for computer forensics. Students will learn best practices for general incidence response. The course will then focus on the tools and techniques to perform a full computer forensic investigation and produce a written report of their findings.

Catalogue Description

Forensic science techniques. Digital evidence preservation. Processes and methodologies for digital examinations. Cybercrime investigations. Windows file system analysis. Real-case scenario analysis and reporting.

Learning Objectives

Upon completing this course, students will:

1. Understand the fundamentals of computer forensics.
2. Understand the legal aspects of computer forensics.
3. Understand best practices for evidence preservation and documentation.
4. Understand the relationship between IT and computer forensics.
5. Introduce concepts related to incident response.

Prerequisite(s): ITP-125 or Instructor Approval

Technological Proficiency and Hardware/Software Required

It is assumed that the student has baseline technical knowledge (basic computer usage, basic internet usage). For any upper-division course (300-level and above), it is assumed that you have refined your technical abilities in ITP 125, including basic Python scripting and fundamentals of the Windows operating system, ports and protocols, and networking.

Course Notes

The course is letter graded, with all materials available on Blackboard (blackboard.usc.edu). Labs and case work will be conducted in the classroom (RRB101) during assigned class time and on your own time outside the classroom.

Required Readings and Supplementary Materials

TBD

Grading Breakdown

Assignment	% of grade
Lab Assignments (Qty. 10)	**50**
Case 1	**10**
Case 2	**5**
Case 3 (w/ quizzes)	**5 + 15**
Final Exam	**10**
Participation/Professionalism	**5**
TOTAL	**100**

Grading Scale

The following shows the grading scale to be used to determine the letter grade.

93% and above	A
90% - 92%	A-
87% - 89%	B+
83% - 86%	B
80% - 82%	B-
77% - 79%	C+
73% - 76%	C
70% - 72%	C-
67% - 69%	D+
63% - 66%	D
60% - 62%	D-
59% and below	F

Grading Policies

The lab assistants, graders, and instructors will do their best to return lab assignments graded to students within one week of the submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading rubric is posted. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in class. Do not rely upon an expectation of a guaranteed minimum final grade in this class, regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam, or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

Grades will be posted on Blackboard, and it is your responsibility to ensure that the grades online are accurate and to follow your progress in the class.

Assignment Policies

The labs will be posted on Blackboard under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments, and you must ensure you have fully submitted the assignment (usually a two-step process).

All lab assignments and case reports are due at 11:59:59 PM on Friday during the week listed in the syllabus, unless otherwise modified by Blackboard announcement and/or email from the instructor and/or Lab Assistants. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours, particularly when the assignment is due.

If you join the class after the semester has started, you will have two weeks from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted, and you will receive no credit for the assignment.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due without expressing an emergency, such as being kidnapped and taken to Mexico, it will probably not be granted.

Certain assignments will require a paper submission, and you may be asked to submit them to the main ITP office. There have been previous allegations of student rudeness to the ITP Staff. If the staff complains about you being rude, you will have 25% automatically deducted from your assignment. Don't be rude.

The instructor and lab assistants reserve the right not to answer certain questions about the lab assignment. This is normally due to the nature of the question being directly related to the

learning objectives of the lab. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

All lab assignments have been tested by the instructor and/or lab assignments. Due to the nature of certain software packages and configurations in the lab, the assignments may or may not work as intended. You are encouraged to ask questions if something appears not to work correctly. However, there are certain instances where things are intended not to work correctly, and the instructor and lab assistant will indicate as such. When in doubt, do a little research.

Exam Policies

Please review the schedule of classes for the Final Exam schedule. Should you have a scheduling conflict with the final exam, or, per university policy, you have more than 2 final exams scheduled on the same day, you must contact the instructor and coordinate an alternative time by the end of Week 3. Any requests made after Week 3 are not guaranteed to be accommodated.

Per USC policy, Final Exams must be scheduled during the assigned final examination schedule. It is your responsibility to arrange your travel after the scheduled date of the final exam.

All students are required to participate in the final exam and/or project. Failure to take the final exam and/or submit a final project will result in an automatic failure in the class.

No make-up exams (except for documented medical or family emergencies) will be offered, nor will any changes be made to the Final Exam schedule. Missing your alarm is not an emergency. A documented medical event (car accident with documentation), family emergency (death in the family), or alien abduction can be considered emergencies.

Contacting the Instructor, Lab Assistants, or Graders

When emailing the lab assistants, graders, or instructor, please include your full name, student ID, class name and number, and class section (day and time).

Emails sent to the lab assistants or graders should have a response within two business days. The instructor will endeavor to respond to emails within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the lab assistants and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

Questions about lab assignments should be submitted through the class discussion board (typically Piazza). This will have a faster response rate. Do not post code or answers on Piazza.

The instructor will post their regular office hours on Blackboard. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you. We do have other responsibilities outside of the class.

Attendance Policy

You are expected to be in the classroom on time and distraction-free. As this class meets twice a week and is lecture and lab, any student who misses more than four classes is in danger of failing the course. Please see the instructor immediately if you have missed four or more class meetings. Should you miss more than four class meetings without meeting with the instructor, the instructor may elect to drop you from the class.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in this class, and punctuality is vital to your professional career. The lab assistants will be taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor.

If you are not in class, it is not the TA's or the instructor's responsibility to teach you the material you missed. Attendance is mandatory for guest lectures. Guest lectures are tentatively noted in the syllabus and will be announced in class.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating by writing professional quality case reports. These reports are held to standards expected by professionals in the industry who are writing reports for clients, executives attorneys, judges, juries, congresspeople, senators – individuals who may be very technical or individuals who while intelligent are not technical.

It is expected that the reports will be written with correct spelling, grammar, and language nuances of the American English language. A component of each report grade will be based on writing style, grammar, and word choice. These reports must be accessible to technical and non-technical readers alike.

It is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional career. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center.

Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with university standards, plagiarism of any type will not be tolerated.

Course Content Distribution and Synchronous Session Recordings Policies

USC has policies that prohibit the recording and distributing any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express written permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future and thus infringe on the academic freedom of other students and the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express written permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information that had been distributed to students or in any way had been displayed for use in relation to the class, whether obtained in class, via email, on the internet, or via any other media. (Living our Unifying Values: The USC Student Handbook, page 13)

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct is in contrast to the university's mission to educate students through a broad array of first-rank academic, professional, and extracurricular programs and includes any act of dishonesty in the submission of academic work (either in draft or final form).

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. All students are expected to submit assignments that are original work and prepared specifically for the course/section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences that can include expulsion. Please familiarize yourself with the discussion of plagiarism and academic integrity in the USC Student Handbook: https://policy.usc.edu/studenthandbook

Other forms of academic dishonesty are equally unacceptable. See additional information and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct

For more information about academic integrity, see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Policy on Generative AI

Since creating, analytical, and critical thinking skills are part of the learning outcomes of this course, all assignments should be prepared by the student working individually or as allowed by the instructor in groups. Students may not have another person or entity complete any substantive portion of the assignment. Developing strong competencies in these areas will prepare you for a competitive workplace. Therefore, using AI-generated tools is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

ChatGPT:

ChatGPT and similar programs and platforms represent great promise for the field of information technology, cybersecurity, and just about every other part of our world. Our policy on ChatGPT is as follows: you may use ChatGPT or similar programs for your assignments for this class, but treat them as a research *tool* and not a primary or secondary *source*. This means 1) cite your original source(s), and they can't be ChatGPT or similar tools directly, 2) treat everything those tools tell you to do or information they provide with a strong grain (pound?) of salt, and 3) *never* copy and paste or treat their output as a source or knowledgebase of ultimate authority. We want to emphasize the concept of using them as *tools* since they may guide you to the right answers; however, they can't and don't always do this correctly, and you may not know when they're telling the truth or making something up.

Our team is exceptionally good at recognizing answers from ChatGPT and similar tools. AI-detection tools and real humans will both be used to validate your assignments in this class. If we suspect or determine that your assignments are being produced by AI-based tools or otherwise violate the guidelines above, your submissions will be treated as violations of the university's academic integrity policy and handled as such.

ITP 375 Fall 2024 Weekly Course Schedule | NOTE: Subject to Change

Week	Monday	Wednesday	Lab/Case Assignments
1	**August 26** Introduction I	**August 28** Introduction II	
2	**September 2** Labor Day - NO CLASS	**September 4** Digital Media & Acquisition I: Digital Media	Assign: Lab 1 (Chain of Custody)
3	**September 9** Digital Media & Acquisition II: Acquisition	**September 11** Lab Setup	Due: Lab 1 Assign: Lab 2 (Acquisition)
4	**September 16** File, Hash, & Signature Analysis	**September 18** Introduction to Forensic Tools	Due: Lab 2 Assign: Lab 3 (File Sig Analysis) **Assign: Case 1**
5	**September 23** File Systems I	**September 25** File Systems II	Due: Lab 3 Assign: Lab 4 (File System)
6	**September 30** Tracking User Activity I	**October 2** Investigative Mindset	Due: Lab 4 Assign: Lab 5 (User Activity 1)
7	**October 7** TBD	**October 9** Forensic Report Writing	Due: Lab 5 (due Oct 9) Assign: Lab 6 (User Activity 2)
8	**October 14** Tracking User Activity II	**October 16** In-Class Forensic Work (Case 1)	**Due: Case 1**
9	**October 21** Enterprise Network Artifacts	**October 23** Registry	Due: Lab 6 Assign: Lab 7 (Registry) Assign: **Case 2**
10	**October 28** Logs & Work Time	**October 30** In-Class Forensic Work (Case 2)	Due: Lab 7 Assign: Lab 8 (Event Logs)
11	**November 4** Artifacts of Execution I	**November 6** Case 1 Review	Due: Lab 8 **Due: Case 2**
12	**November 11** Artifacts of Execution II	**November 13** Guest Lecture I	Assign: Lab 9 (Execution) Assign: **Case 3**
13	**November 18** Persistence Mechanisms I	**November 20** Persistence II & Work Time	Due: Lab 9
14	**November 25** Case 2 Review	**November 27** In-Class Forensic Work (Case 3)	Work on Case 3
15	**December 2** Guest Lecture II	**December 4** Conclusion, Exam Review	**Due: Case 3 [Fri 11:59pm]**

Final Exam: As stated in the USC Schedule of Classes at https://classes.usc.edu/term-20241/finals/

Statement on Academic Conduct and Support Systems

Students and Disability Accommodations:

USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline is comprised of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu *ß*
Confidential Lifestyle Redesign services for USC students to support health promoting habits and routines that enhance quality of life and academic performance.