Date of last update: 12/7/2023

Digital Forensics and Hacking Investigation

CIS D104.63Z (CRN: 34925) – Online Course Winter 2024

Class begins January 8, 2024. Final is on March 28, 2024

Office hours: via Zoom, and via e-mail (see below for details)

COURSE DESCRIPTION

This is an "asynchronous" online course in which you will be given 15 laboratory assignments, 10 quizzes and a midterm and final to complete. You are encouraged to work more quickly than the schedule that is specified for this course but will not receive credit if you work more slowly. You will have from 1 to 2 Labs to complete each week.

The course is an introduction to computer cyber-crime investigation and forensics processes. Topics include computer forensics tools, hacking investigation tools, data recovery, information gathering techniques, computer data preservation techniques, and computer cybercrime investigation techniques. System administrators, security professionals, IT staff, and law enforcement personnel would benefit from taking this course. This course can help prepare students to pass computer forensics certification examinations, such as the EC-Council Computer Hacking Forensic Investigator (CHFI) or the Certified Forensic Computer Examiner (CFCE) credential.

The lab environment is provided by InfoSecLearning.com and offers a large and varied collection of virtual digital security labs that many professionals use to polish their skills in a variety of security areas. There are now 15 labs for this course. I have provided many opportunities to earn extra credit points so that you need not worry about earning a poor grade if you are willing to do some extra work. As always, I record new lectures and videos for the quarter.

The Canvas class will not be available to you until the class start date early (12:01 AM) on January 6, 2023, and until you have (1) watched the two videos about the syllabus and the labs that are visible links when you first visit the course in Canvas and (2) completed the "student contract" in which you verify that you have read and understand the content of this syllabus with regard to the way the class will work.

PREREQUISITE SKILLS

Advisory: EWRT 200 and READ 200 (or LART 200), or ESL 261, 262 and 263; CIS 108.

INSTRUCTOR INFORMATION:

Instructor: Leonard (Len) Fisk

Office Hours:

via the Zoom conference tool on the class Canvas page: from 4:00 to 5:00 every Tuesday and Thursday from 1/9/2024 through 3/28/2024

via e-mail: I can be reached virtually any time via e-mail (see below for address).
E-mail address: fisklen@fhda.edu

Website: I will post up-to-date information regarding this course at the Canvas page for this course. Various other links may be added at this class site, and assignments and tests will be done at this location as well. It will be the center point for communications about the course.

ATTENDANCE POLICY

Drop Policy: By midnight on Friday of the second week (1/19/2024), you will have completed and turned in (to Canvas) the Unit 01 Lab assignment posted on the website. You will also have completed the Student Contract quiz on Canvas by that date. Failure to do either of these things may result in a DROP. You will have a 5-day reprieve on handing in Labs and will receive apoints penalty for handing it in during the 5 day period following the due date: that means the "deadline" date

beyond which you cannot hand in Lab 1 will be at 11:59 PM (midnight) on 1/24. The "due" date is midnight on 1/19. No Lab will receive credit if handed in after the "deadline" date.

Students who wish to drop this class must follow the De Anza College drop procedures. The Drop calendar deadlines can be found at https://www.deanza.edu/calendar. Do not assume you will be automatically dropped from this course. If you intend to drop the course, you must drop yourself!

OBJECTIVES

Upon completion of this course, you will be able to use a personal computer and understand the following personal computer objectives. By the close of the course, the student will have/be able to

1. Explore the forensics profession
2. Analyze examples of computer crime
3. Investigate forensic methods and labs
4. Learn how to collect, seize, and protect evidence
5. Explore e-mail forensics
6. Analyze Windows forensics
7. Examine mobile forensics

STUDENT LEARNING OUTCOMES FOR THIS COURSE:

Demonstrate data recovery and cybercrime forensics investigation techniques.

REQUIRED COURSE MATERIALS

Purchasing the Textbook: The textbook is *Learn Computer Forensics 2nd Edition by William Oettinger, PACKT Publishing, 2022 (ISBN: 978-1803238302).* You can buy the textbook either online or from the student bookstore. (Amazon sells the Kindle version for $29.99. The new paperback version is $44.99, used is low $40's.

Purchasing Access to the Lab: The easiest way to purchase Lab access is online, directly from infoseclearning.com. (This will cost approximately $88.) You can purchase access to InfoSecLearning's Digital Forensics Fundamentals by getting into our course (CIS 104) on Canvas (after 12:01 AM on Jan 6, 2023) and going to any of the fifteen links to labs *(you must complete the Student Contract and watch the two videos on the syllabus and "how to do the labs" that are in Canvas to open access to these labs)* which are labeled with the text "**Lab** *nn:* **Access:** *Title of specific lab"*. Once you click on the link to the virtual lab, InfoSecLearning will automatically begin to create an account for you and take your credit/debit card information. You will only authenticate this one time. After this you will simply click the link in Canvas and will be taken directly into the lab you wish to access. You must always be logged into Canvas and access our class site within Canvas access the labs. **(Note: DO NOT go directly to InfoSecLearning's web site to do this purchase. Go there by using the laboratory links in Canvas.** This will ensure that your link will is uncomplicated and that you will never be confused about which lab is required.**)**

Once you have access to the virtual laboratory via any of the 15 **"Lab 0***n* **Access:** *…***"** links found on the Canvas site for CIS 104 you will be given access for the length of your subscription (6 months). I have arranged for the canvas page for this class to remain active for that period of time so that you can return to the labs after the quarter has ended.

Linking the Virtual Lab to this Particular Course: (Unless you carry out this additional step, the labs you complete will not send me verification of your completion of extra credit exercises.) If you wish to earn extra credit for the "capture the flag" exercises in any lab, you must link the your flag capture information to me. I have posted a PDF in the very first segment of our Canvas site that offers instruction about how to do this, using my e-mail address (fisklen@fhda.edu) to link your flag capture history to this class so I can access them. Select the "**Digital Forensics Fundamentals**" as the course and then click on the "link instructor" button. The resulting screen will ask for an email address, which you can provide as **fisklen@fhda.edu**. If you then push the "ADD" button, I will be allowed to see your flag captures to include them in your grades.

RELATED ACCESS ISSUES

If you encounter difficulties in accessing the lab, or if the virtual labs are not working correctly, you can email

InfoSecLearning at info@infoseclearning.com. If you do have access to the labs and encounter a technical problem with the labs, you can simply click on the "hamburger" (3 horizontal bars on top of one another in a circle) symbol in the blue bar at the upper right corner of the instruction pane, which will pull down a menu. The bottom item on the menu is "Help Desk".

Canvas and the Virtual Lab Site: As noted above, Canvas will be used for completing all class assignments. This site also allows you to create discussion forums and to reach other students to form study groups, etc., as well as a chat-room to use in addition to regular e-mail. I am available at most times during the week via regular e-mail (I have my iPhone nearby at almost all times).

Hardware Requirements: A desktop or laptop computer is recommended to run the labs for this course. The critical feature is the full keyboard, but if you have a tablet, I suspect that a Blue Tooth keyboard will also work.

Software: The software required for this class is: (1**) a web browser** (Chrome is officially required, but Firefox will work well also).

You will also need **MS Word** or a tool that produces output compatible with Word (i.e., it can read/write DOC or .DOCX files), like Apache Open Office or LibreOffice. I have found that minimalist tools like Google Docs and WordPad are not capable of retaining the formatting I have added to the report templates.

If you wish to earn extra credit by doing "voice over" PowerPoint presentation(s), you will need a copy of **Microsoft PowerPoint** on a computer with a microphone to record the audio. If you have a student email account at De Anza, you do have free online access to Office 365, which has both Word and PowerPoint and the Computer Labs in ATC 203 are equipped with this software.

WAYS TO EARN POINTS TOWARD YOUR GRADE

This course will require 15 hands-on lab assignments in which you will be using security software. You will be able to earn up to 2.5 extra credit points for any or all of the 15 labs by doing the "capture the flag" challenges in each lab. There are 10 quizzes, one for each unit. Finally, in addition to these graded activities, you have the opportunity to earn additional "extra credit" points by researching and presenting additional information about tools and various forensic and recovery issues currently being discussed in the press and on the web to the class. The maximum possible points are summarized in the table shown below.

Source	number	points	total
Laboratory Assignments	**15**	**15**	**225**
Extra Credit Flag Captures in required Labs	*15*	*2.5*	*37.5*
Unit Quizzes	**10**	**10**	**100**
Midterm	**1**	**50**	**50**
Extra Credit Forensic Tools/News Presentations	*5*	*10*	*50*
Final	**1**	**100**	**100**
Total points possible: (**475 points required**)			**562.5**

SUBMITTING WEEKLY LABORATORY ASSIGNMENTS

This course uses a virtual laboratory environment provided by InfoSecLearning to accompany the text, and all of the labs will require access to this environment, which is linked via the Canvas class site. All course information, including assignments, course deadlines, etc. will be made available to you online via the Canvas course web site. When you enter the Canvas online course site, you will find the assignments that you will be asked to complete, listed within each Unit of the quarter. The actual course schedule and due dates for exams and assignments may be subject to change and will be posted in the schedule in this course syllabus on the Canvas site for this class. Each week's lab assignment will entail using the virtual environment and doing a number of screen captures and

written answers, which you will use to document your actions there in the laboratory report "template" which you will download from Canvas. You will then paste the captured screen images into your narrative, answer the questions describing what you did, and post the resulting document to satisfy the assignment at the link that reads "*Lab0n (Required or Extra Credit) Report Turn-in*". You will find a video that details how to prepare the lab reports on Canvas.

LATE WORK

Lab reports will be accepted after the due date according to the following rules: Ten percent (10%) of the maximum possible points will be subtracted for each day (24 hours) the assignment is late. This will continue until 5 days have passed, when the points total will drop to zero, and no credit will be earned. If you have clear and compelling reasons for not getting an assignment in on time, **please let me know on or before the day it is due**, and I will arrange an extension for compelling cases.

EXTRA CREDIT WORK

Lab Extra Credit: In each of the 15 lab exercises, you will find that there are "flags" (actually 6 digit numbers) that you can "capture" by simply typing the number into the provided space in the lab instructions at the left side of the screen. Each time you capture a flag, you will earn an extra .5 credit points. Every lab will have 2.5 possible "capture the flag" points.

To earn credit for the "capture-the-flag" extra credits, you must have linked the virtual lab environment to my e-mail as explained in the "How to link your extra credit flag capture scores to your grades" PDF shown in the Canvas class site.

Audio-augmented PowerPoint presentations for Extra Credit: Unlike the lab extra credits, this form of Extra Credit will be prepared as a PowerPoint presentation, with an embedded audio recording of your voice doing the presentation, which I will post for the full class to access. (Even older versions of PowerPoint permit the recording of your voice for presentations: all you need is a laptop with a built-in microphone, or an external microphone with either USB or audio jack.) You will upload a PowerPoint presentation that has been augmented with your own voice recording, explaining each slide, with no more than 10-minutes time being taken for the full presentation. **Extra Credit work will be posted on topics that are truly substantive and that target specific security issues pertinent to this course.** These Extra Credit topics will include: (1) The demonstration of, and/or installation of, and/or use of, and/or analysis of, major tools used in forensics (like Autopsy, Wireshark, Kali Linux, etc.), or (2) The reporting and technical analysis of major events in digital forensics (for example, the January Sixth Committee made extensive use of cell phones in their investigation – why?) and related issues in the current eye.

Any Extra Credit presentations **will require the prior approval of Professor Fisk** and will be posted to the Canvas site to earn extra credit points. (If it is accepted for credit, Dr. Fisk will make your report available to the full class.) I will accept a maximum of only 5 Extra Credit presentation submissions per week (first come-first served), and any one student cannot submit any more than one per week. I will accept a maximum of 5 Presentation Extra Credits from any one person.

THE SCHEDULE FOR COMPLETING EACH UNIT

Initially, you may find that the Canvas page looks rather empty. The reason is that You must (1) view both of the videos I have supplied in the initial block of the Canvas page (one video about the syllabus and one about how to do the labs) and (2) complete the Student Contract, which simply summarizes the rules we will operate under for the course. Once you've done these things, the rest of the course will become visible. There will be 10 units associated with specific chapters in the text and specific Laboratory exercises, as shown in the table below:

		Text Chapt				lab(s) due	lab(s) deadline	quiz deadline
1	8-Jan	13 & 1	Ethics of Expert Witness Testimony & Types of Investigations	1/19 (midnight)	Lab 1: Introduction to File Systems	1/19 (midnight)	1/24 (midnight)	1/25 (midnight)
2	15-Jan	2 & 3	The Forensic Analysis Process & Acquiring Evidence	1/26 (midnight)	Lab 8: FAT File System Lab 9: The NTFS File System	1/26 (midnight) 1/28 (midnight)	1/31 (midnight) 2/2 (midnight)	2/1 (midnight)
3	22-Jan	11	Network Basics	2/2 (midnight)	Lab 5: The Imaging Process	2/2 (midnight)	2/7 (midnight)	2/8 (midnight)
4	29-Jan	4 & 5	Computer System Components & Investigation Process	2/9 (midnight)	Lab 3: Hashing Data Sets Lab 13: Log Analysis	2/9 (midnight) 2/11 (midnight)	2/14 (midnight) 2/16 (midnight)	2/15 (midnight)
5	5-Feb	6	Windows Artifact Analysis	2/16 (midnight)	Lab 2: Common Windows Artifacts	2/16 (midnight)	2/21 (midnight)	2/22 (midnight)
5x	8-Feb	all prior	Midterm: 70 MC in 70 minutes					
6	12-Feb	7	RAM Memory Analysis	2/23 (midnight)	Lab 14: Memory Analysis Lab 11: Communication Artifacts	2/23 (midnight) 2/25 (midnight)	2/28 (midnight) 3/1 (mdnight)	2/29 (midnight)
7	19-Feb	8	E-Mail Analysis	3/1 (midnight)	Lab 10: Browser Artifact Analysis	3/1 (midnight)	3/6 (midnight)	3/7 (midnight)
8	26-Feb	9	Internet (Web) Artifacts	3/8 (midnight)	Lab 7: Intro. to Autopsy Lab 6: Intro. to Single Purpose Tools	3/8 (midnight) 3/10 (midnight)	3/13 (midnight) 3/15 (midnight)	3/14 (midnight)
9	4-Mar	10	Online Investigations	3/15 (midnight)	Lab 4: Linux Drive Letter Assignments	3/15 (midnight)	3/20 (midnight)	3/21 (midnight)
10	11-Mar	12	Writing Forensic Reports	3/22 (midnight)	Lab 12: User Profiles & Registry Lab 15: Forensic Case Capstone	3/22 (midnight) 3/24 (midnight)	3/27 (midnight) 3/29 (midnight)	3/28 (midnight)
	28-Mar	1 - 13	Final: 130 MC in 130 minutes		Final will be open to take from 4:00PM to 11:59 PM on March 28			

The Lab report of the <u>first unit</u> *should* be completed and uploaded to the class Canvas site before midnight of Friday, 1/19/2023, and *must* be completed (and uploaded) before <u>midnight, Wednesday, 1/24/2023</u> for you to receive credit.

In general, the sequence you should follow for each unit is as follows:

1. Read the chapter(s) for the unit and watch the lecture, with audio narrative for the unit;
2. **Do the virtual lab(s) for the unit and post each lab report to Canvas <u>as a single DOC (MS Word format) document</u>**;
3. Complete the Quiz for that Unit.

TESTING/GRADING POLICIES/FINAL GRADES

To pass this course, you must complete the assignments and Exam with the minimum scores shown below**.** Weekly deadlines for all assignments will be posted via Canvas.

Grading Scale:

A+	96%-100%
A	93% -95%
A-	90%-92%
B+	87%-89%
B	83%-86%
B-	80%-82%
C+	77%-79%
C	70%-76%
D+	67%-69%
D	63%-66%
F	0%-62%

In the end I will simply total all of your points (regular plus extra credit) and divide by 475. I will convert the resulting number to a percentage (of 475) and look it up on the table shown above. If, for example, you earn 311 points of the 475 required points available to you, this would be tallied as 65%, which would earn you a D. Similarly, earning 452 points would yield 95%, which would earn you an A.

ACADEMIC INTEGRITY:

Students who submit work of others as their own or cheat on exams or other assignments will receive a failing grade in the course and will be reported to college authorities.

Note to students with disabilities

If you have a disability-related need for reasonable academic accommodations or services in this course, provide your instructor with a Test Accommodation Verification Form (also known as a TAV form) from Disability Support Services (DSS) or the Educational Diagnostic Center (EDC). Students are expected to provide five-day notice of the need for accommodation. Students with disabilities can obtain a TAV form from their DSS counselor (864-8753 DSS main number) or EDC advisor (864-8839 EDC main number).

TECHNICAL DIFFICULTIES

If you have technical problems with the InfoSecLearning virtual laboratory, please contact them directly at info@infoseclearning.com.