Date of last update: 6/3/2021

Digital Forensics and Hacking Investigation

CIS D104.61Z (CRN: 13183) – Online Course Summer 2021

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 to complete over a very short span of time. You are encouraged 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 2 to 3 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.

I have rewritten this course completely this quarter and have changed both the textbook and the virtual laboratory environment. The new text is focused on preparing people for the Certified Cyber Forensics Professional Certification. It is much less expensive than the prior text and does a good job of covering the material required for this course. 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. The quizzes for instructional Units have been eliminated, placing the major emphasis on the labs in the virtual setting. I have also provided many opportunities to earn extra credit points so that you need not worry about earning a poor grade if you are willing to 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 on 6/26/2021, and until you have 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 6/29/2020 through 8/05/2020

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 Wednesday of the second week (7/7/2021), you will also 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 both of these things may result in a DROP. You will have a 2 ½ day reprieve on handing in Labs and will receive a points penalty for handing it in during 2 ½ day period following the due date: that means the "deadline" date beyond which you cannot hand in Lab 1 will be at 11:59 AM (noon) on 7/10. The "due" date is midnight on July 7. 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 *CCFP Certified Cyber Forensics Professional All-in-One Exam Guide, 1st Edition by Chuck Easttom, McGraw-Hill Education*. You can buy the textbook either online or from the student bookstore. (Amazon has it for around $35.)

Purchasing Access to the Lab: The lab should be purchased directly from infoseclearning.com. (This will cost approximately $80.) You can purchase access by getting into our course (CIS 104) on Canvas and going to any of the fifteen links to labs (you must do the Student Contract 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.

Once you have access to the virtual laboratory via any of the 15 "**Lab 0***n* **Access:** ..." links found on the Canvas page for CIS 104 you will be given access for the length of your subscription (about 6 months). I have arranged for the canvas site to remain active for that period of time.

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 lab to this class. As soon as you have purchased access to the labs, go to any of the 15 "*Lab 0n Access: ...*" links found on the Canvas page for CIS 104. When you arrive at the virtual lab on the InfoSecLearning server, find the circle with a "home" symbol

inside it at the right side of the red bar at the top of the screen and click it. The resulting screen will have a button labelled "Link Course to Instructor". Click this button. The subsequent screen has two boxes: (1) a "select course" pull-down, and (2) a box for "Instructor Email". Select the "**Digital Forensics Fundamentals**" as the course and type **fisklen@fhda.edu** for the Instructor email, then click on the "link to Instructor" button. That's all you need to do.

RELATED ACCESS ISSUES

If your code doesn't work or you are unable to register please 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 red bar at the upper left corner of the lab display, 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** (I prefer Chrome, 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. 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.

WAYS TO EARN POINTS TOWARD YOUR GRADE

This course will require 10 hands-on lab assignments in which you will be using security software. You have the opportunity of doing 5 additional labs for extra credit, and will be able to earn up to five extra credit points for any or all of the 15 labs by doing the "capture the flag" challenges in each lab. 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	**10**	**10**	**100**
Extra Credit Flag Captures in required Labs	*10*	*5*	*50*
Extra Credit Lab Assignments	*5*	*10*	*50*
Extra Credit Flag Captures in Extra Credit Labs	5	*5*	25
Extra Credit Forensic Tools/News Presentations	*5*	*10*	*50*
Midterm	**1**	**50**	**50**
Final	**1**	**100**	**100**
Total points possible: (250 points required)			425

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 are 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 ½ day (12 hours) the assignment is late. This will continue until 2 ½ 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

Extra Credit Labs: In 5 of the 10 units that make up the course, you will find that there are two lab assignments rather than just one. The second of these two will be labelled "Extra Credit". It is a laboratory assignment like all the others, except that it is optional, and doing it will earn you extra credit points.

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 credit point. Every lab will have 5 possible "capture the flag" points.

Audio-augmented PowerPoint presentations for Extra Credit: Unlike the lab extra credits, this form of Extra Credit will be prepared as a PowerPoint, with an 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 Credits will involve:

(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 (as I write this, they are seizing all of the computers at Rudy Giuliani's house – 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 SEQUENCE OF EVENTS FOR COMPLETING EACH UNIT

Initially, you may find that the Canvas page looks rather empty. The reason is that You must complete the Student Contract, which simply summarizes the rules we will operate under for the course. Once you are able to answer "Yes" to each of the Student Contract questions, you can proceed and the rest of the course becomes visible. There will be 10 units associated with specific chapters in the text and specific Laboratory exercises, as shown in the table below:

Course Schedule:

Unit	unit start date	topics	Chapt.	Lab(s)	lab(s) due	lab(s) deadline
1	28-Jun	Legal and Ethical Principles: Introduction to Forensics	1	Lab 1: Introduction to File Systems	7/7 (midnight)	7/10 (noon)
2	1-Jul	Legal and Ethical Principles: The Investigative Process	2	Lab 3: Common Locations of Windows Artifacts Lab 2: Hashing Data Sets	7/10 (midnight)	7/13 (noon)
3	5-Jul	Legal and Ethical Principles: Evidence Management	3	Lab 4: Drive Letter Assignments in Linux	7/14 (midnight)	7/17 (noon)
4	8-Jul	Forensic Science: Principles and Methods	4	Lab 5: The Imaging Process Lab 6: Introduction to Single Purpose Forensic Tools	7/17 (midnight)	7/20 (noon)
5	12-Jul	Forensic Science: Forensic Analysis; Digital Forensics: Hardware Forensics	5 & 6	Lab 7: Introduction to Autopsy Forensic Browser	7/21 (midnight)	7/24 (noon)
		Midterm: 30 MC in 30 minutes, 7/22	1 - 6	Midterm will be open to take from 4:00PM to 9:00 PM on 7/22	7/22 (9:00)	7/22 (9:00)
6	15-Jul	Digital Forensics: Hidden Files and Attributes	7	Lab 8: FAT File Systems Lab 9: The NTFS File System	7/24 (midnight)	7/27 (noon)
7	19-Jul	Digital Forensics: Network Forensics and Virtual Systems	8 & 9	Lab 10: Browser Artifact Analysis	7/28 (midnight)	7/31 (noon)
8	22-Jul	Digital Forensics: Mobile Forensics	10	Lab 11: Communication Artifacts Lab 12: User Profiles and the Windows Registry	7/31 (midnight)	8/3 (noon)

9	26-Jul	Application Forensics and Emerging Technologies: Application Forensics	11	Lab 13: Log Analysis	8/4 (midnight)	8/6 (noon)
10	29-Jul	Application Forensics and Emerging Technologies: Malware Forensics	12 & 13	Lab 14: Memory Analysis Lab 15: Forensic Case Capstone	8/6 (noon)	8/6 (noon)
		Final: 60 MC in 60 minutes	1 - 13	Final will be open to take from 4:00PM to 9:00 PM on August 6	8/6 (9:00 PM)	8/6 (9:00 PM)

For each unit, the materials must be accessed and completed in the required order and must be completed before the listed "deadline" date in order to earn credit.

The Lab report of the first unit *should* be completed and uploaded to the class Canvas site before midnight of Wednesday, July 7, and *must* be completed (and uploaded) before noon, Saturday, July 10 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 as a single DOC (MS Word format) document**;

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 assignment 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%

Final Grade Mix:

The following percentages reflect how the final grade will be determined:

Lab Assignments	50.0%
Final Exam	50.0%
Extra Credit	87.5%
	=====
Total =	187.0%

In the end I will simply total all of your points (regular plus extra credit) and divide by 250. I will convert the resulting number to a percentage (of 250) and look it up on the table shown above. If, for example, you earn 195 points of the 375 points available to you, this would be tallied as 78%, which would earn you a C+.

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 give a five day notice of the need for accommodations. 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.