Date of last update: 3/23/2017

Digital Forensics and Hacking Investigation

CIS 104 (CRN: 44662)
Spring, 2017
*Online class with **two on-campus meetings from 4:00- 5:50PM on 4/13/2017 and 6/29/2017 in ATC203***
Office hours: via Internet video, via e-mail & in person (see below for details)

COURSE DESCRIPTION

This is a "synchronous", "hybrid" online course in which you will be given weekly laboratory assignments and quizzes to complete**. You should probably work more quickly than the schedule that is specified for this course, but will not receive credit if you work more slowly than the schedule**. The course is an introduction to computer cyber crime and hacking investigation 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. Also, 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.

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:

in person at ATC 203b on the De Anza campus from **3:00-3:50 PM** on 4/13/2017 and 6/29/2017.

via web video: from 4:00 to 6:00 every Thursday from 4/20/2017 through 6/22/2017 on CCCConfer as follows:

The **cccconfer.org** website is a videoconferencing site and you need a computer with microphone and speakers, plus, if you wish, a webcam. Or, you can use an iPhone, iPad, or Android device if you download the mobile app "Blackboard Collaborate."

cccconfer office hours: Go to cccconfer.org and select the "**Office Hours / Student**" button, then scroll to find the entry for "Len Fisk Office Hour". Then hit the "**GO**" button. Or, simply use this link: : http://cccconfer.org/GoToMeeting?SeriesID=61e8e505-60b0-419b-aff6-79ad5b9c4c0b. The participant passcode is **198591**. I will be using a webcam and encourage you to do so also, but there is no requirement that you use video (there is a text box). If you do not have Internet capability, you can always call 888-886-3951 to participate by voice.

via e-mail: I can be reached virtually any time via e-mail (see below for address). **Please send e-mail only to the address shown, and use CIS102 in the subject line to ensure that I will get the mail in a timely manner.**

E-mail address: **mailto:fisklen@fhda.edu**

Website: I will post up-to-date information regarding this course at Jones & Bartlett's site for this course. In particular, I will post updates and changes to this syllabus at that site which, like the campus "Catalyst" system, is Moodle-based. You will be accessing this site via https://www.jblcourses.com/ . Various other links may be added at this class site, and assignments will be uploaded to it as well. It will be the center point for communications about the course. Effectively, the only fee for a "textbook" will also be included in the fee to buy access to this site.

ATTENDANCE POLICY

Students are required to attend all class meetings every Thursday, 6:00-7:50 PM in AT 205.

Drop Policy: By **midnight**, **Wednesday of THE SECOND WEEK OF THE COURSE (4/19/2017)** you must purchase the text and the lab access, and have logged into the Jones and Bartlett site that provides the Moodle "main office" for the class and the critically important virtual laboratory. **By midnight on Friday of the second week (4/21/2017), you will also have completed and turned in (to J&B Moodle) all of the Week 1 Lab assignment posted on the website** (we will ignore the "challenge" assignments). (This due day is two days later than I will expect for all remaining Lab assignments, which will be due at midnight Wednesday of each week.) **Failure to do so may result in a DROP.**

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 the ability to use computer forensics tools and hacking investigation tools to accomplish data recovery and do information gathering, computer data preservation and conduct computer cybercrime investigations.

REQUIRED COURSE MATERIALS

Textbook: System Forensics, Investigation, and Response, 2nd Edition, with special virtual lab access, by Chuck Easttom.

Purchasing text and lab materials: You can purchase access to the virtual labs required for the course at the De Anza bookstore. If you would prefer a hard-copy version of the textbook, the bookstore will have a number of copies for purchase. Please note that access to the virtual lab is unique for each person and cannot be shared: i.e., the code you purchase will belong to you and to you alone.

The bookstore will sell you a packet with either

- **e-book plus lab access**: System Forensics, Investigation, and Response, 2nd Edition, by Chuck Easttom**,** or
- **hard copy text plus lab access:** System Forensics, Investigation, and Response, 2nd Edition, by Chuck Easttom, or
- **Lab Access alone** (with no text) (assuming you already have a copy of the 2nd Edition of the text: this option is NOT recommended unless you already own a copy of the text).

Any of these three options will provide you with the access code you need for individual access to the Jones & Bartlett virtual lab site (plus the e-book if you have chosen that option). **Please note that the specific code needed to access the virtual laboratory MUST be purchased, otherwise you cannot participate in the class.**

To redeem your access code to the JBL Virtual Security Cloud Lab, do the following:

1. Go to www.jblcourses.com
2. Click on "**Redeem an Access Code**" on upper right side of screen
3. Enter the **8-digit** lab access code you received and the **four digit** code for this specific course – **6075**. Then click **Submit**.
4. Once your access code has been validated, click on the blue **New User Sign Up** link underneath the yellow submit button. You must do the new user "sign-up" before you can enter a username and password.
5. In the **New User** Box type in
    a. **Username** - must contain alphabetical letters, numbers, a hyphen, underscore, period, or @ sign (DON'T FORGET THIS, AS IT ALLOWS YOU INTO THE LAB!).
    b. **Password** – must contain at least 8 characters, and include one digit, one lower case letter, one upper case letter, and one non-alphanumeric symbol such as"#". For instance, ABCabc1# sign (AGAIN, DON'T FORGET THIS, AS IT ALLOWS YOU INTO THE LAB!).
    c. **First Name/Last Name** in appropriate box
    d. **Email**
    e. Click **submit**
    f. You have successfully entered a link to your course on the next screen.
    g. Click on the course name to enter the course.

If your code doesn't work or you are unable register please contact our tech support specific for the virtual labs and lecture presentations at 1-866-601-4525 or www.jblcourses.com/techsupport.

J&B Moodle and Virtual Lab Site: As noted above, the J&B site will be used for completing all class assignments. The J&B site also provides an interesting feature that 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).

REQUIRED COMPUTER COMPONENTS AND AVAILABILITY

You will need a **broadband Internet connection** (not dial up!) if you wish to work at home.

Hardware Requirements: A PC computer is required to run the Jones and Bartlett software to access the labs for this course. If you do not own a PC, you may use the De Anza lab computers in ATC 203. In addition, some students may wish to install some of the tools that are installed in the Jones & Bartlett virtual environment on their own machines, although this is not required.

Software: (1) You will need a **Firefox** web browser (preferably) to access the Moodle and virtual laboratory sites. The Jones and Bartlett access codes will allow access to the Jones & Bartlett virtual environment that accompanies the Hacker Techniques, Tools, and Incident Handling e-book, and all of the software used will be located on their servers. One exception is the necessary installation of the (free) **Citrix ICA Client**, which you will be prompted to do when you first access the virtual lab from the J&B Moodle site. (2) You will also need Microsoft **PowerPoint**, or a free MS PowerPoint Reader (download from https://www.microsoft.com/en-us/download/details.aspx?id=13). (3) To post Extra Credit assignments, and to post your weekly laboratory assignments, you will need both MS **Word** and **PowerPoint**, or a tool that produces output compatible with Word and PowerPoint (.DOC AND .PPT), like Apache Open Office (students have reported problems with recording audio for presentations with non-Microsoft tools)..

Computers in the De Anza Labs: If you do not have a broadband-connected computer with the proper software, you can use our CIS lab computers. For CIS computer lab hours, see **http://www.deanza.edu/buscs/lab/hours.html**. (Please note that the ATC lab computers are not equipped with speakers, so you will need to provide headphones if you plan to listen to the lectures there.)

WAYS TO EARN POINTS TOWARD A GRADE

This course will require weekly, hands-on lab assignments in which you will be using forensic software. You will take 10 quizzes and a final exam. 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
Quizzes	10	10	100
Final	1	100	100
Extra Credit/Security News	5	10	50
Total points possible:			350

SUBMITTING WEEKLY LABORATORY ASSIGNMENTS

This course uses a virtual laboratory environment provided by Jones and Bartlett to accompany the System Forensics, Investigation, and Response textbook, and all of the labs will require access to this environment. All course information, including assignments, course deadlines, etc. will be made available to you online via the Jones and Bartlett course web site. When you enter the Jones and Bartlett online course site, you will find the assignments that you will be asked to complete, listed within each class week 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 J&B Moodle site. Each week's lab assignment will entail using the virtual environment and doing a number of screen captures, which you will use to document your actions there. You will then paste the captured screen images into your narrative, answering the questions and describing what you did, and post the resulting document to satisfy the assignment at the class Moodle site.

Each Lab will have both a "due date" and a "drop dead" date associated with it. The "drop dead" date represents the date beyond which no labs will be accepted for scoring. Your job is simply to stay ahead of the "due dates" (and most importantly, the "drop dead" dates). Similarly, your completion of the Lab by uploading the report document will trigger the opportunity to take the unit quiz and the assure the availability of materials in the subsequent units. You will have the opportunity to amend your Lab Report after you uploaded your initial version and before the "drop dead" date.

Late Work

Work 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 working day (24 hours) the assignment is late. This will continue until 5 days have elapsed, 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 you. Quizzes must be completed before the date specified in Moodle, and **cannot be taken beyond the deadline**. Please note that there are dependencies among Lab Reports and Quizzes: the former being required as pre-requisites to the latter. If you fail to submit a lab by the "drop dead date", or fail to take a quiz, you will be blocked from continuing the course. **It is better to submit a partial Lab or a poorly executed quiz than to submit none at all: at least you can continue in the course this way.**

Extra Credit Assignments:

Various extra credit assignments will be made available via the J&B site, and will be on topics that you choose and seek approval for before doing. Like all of the other assigned work, it will be turned in via the Jones & Bartlett site. Unlike lab work, **extra credit work will be prepared as a PowerPoint, with an audio recording of your voice presentation, which I will post for the full class to access**. (Even older versions of PowerPoint permit the recording of your voice for presentation: 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 in no more than 10-minutes time 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.** If you have a topic that you think would be an interesting Extra Credit presentation (there are many at this moment, considering the importance that hacking has had in the current change of governments), just send me a proposal, detailing what you wish to present, in specific terms, and I will reply with a judgment (most often "go for it!"). You then prepare the presentation and post it on Moodle.

The Sequence of Events for Finishing Each Unit of the Curriculum:

Initially, you will find that the Moodle page looks rather empty. The reason is that the successive portions of the course only become visible and available to you as you finish each unit/week in the sequence. There will be 10 units associated with specific chapters in the text and specific Laboratory exercises, as shown in the table below:

Unit Sequence Table:

Unit/Week	"Drop-Dead" Dates	Lecture / LabTopic	Reading
Unit 1/ Wk. 1	Unit Lab and Quiz done by midnight 4/21 & 4/25, respectively	**Intro, syllabus, Applying the Daubert Standard to Forensic Evidence**	**Chpt 1&2**
Unit 2/ Wk. 2	Unit Lab and Quiz done by midnight 4/26 & 5/2, respectively	**Documenting a Workstation Configuration Using Common Forensic Tools**	**Chpt 3,14&15**
Unit 3/ Wk. 3	Unit Lab and Quiz done by midnight 5/3 & 5/9, respectively	**Uncovering New Digital Evidence Using Bootable Forensic Utilities**	**Chpt 4**
Unit 4/ Wk. 4	Unit Lab and Quiz done by midnight 5/10 & 5/16, respectively	**Creating a Forensic System Case File for Analyzing Forensic Evidence**	**Chpt 5&6**
Unit 5/ Wk. 5	Unit Lab and Quiz done by midnight 5/17 & 5/23, respectively	**Analyzing Images to Identify Suspicious or Modified Files**	**Chpt 7**
Unit 6/ Wk. 6	Unit Lab and Quiz done by midnight 5/24 & 5/30, respectively	**Recognizing the Use of Steganography in Image Files**	**Chpt 8**
Unit 7/ Wk. 7	Unit Lab and Quiz done by midnight 5/31 & 6/6, respectively	**Automating E-mail Evidence Discovery Using P2 Commander**	**Chpt 9**
Unit 8/ Wk. 8	Unit Lab and Quiz done by midnight 6/7 & 6/13, respectively	**Decoding an FTP Protocol Session for Forensic Evidence**	**Chpt 10&11**
Unit 9/ Wk. 9	Unit Lab and Quiz done by midnight 6/14 & 6/20, respectively	**Identifying and Documenting Evidence from a Forensic Investigation**	**Chpt 12**
Unit 10/ Wk. 10	Unit Lab and Quiz done by midnight 6/21 & 6/27, respectively	**Conducting an Incident Response Investigation for a Suspicious Login**	**Chpt. 13**
Wk. 12	**6/29**	**FINAL - (120 min) 6:15-8:05 PM, 6/29, ATC 203)**	**All Chapters**

For each unit, the materials must be accessed and completed in the required order, and must be completed before the listed "drop-dead" date. The Laboratory for any specific unit/week must be completed before the unit/week mastery quiz appears on Moodle and you are allowed to take it. (The grading of each of the labs may take several workdays before a score is posted.)

TESTING/GRADING POLICIES/FINAL GRADES

To pass this course, you must complete ALL assignments plus ALL Exams with the minimum scores shown below**.** Weekly deadlines for all assignment will be posted via Moodle.

Exam Grading Scale:

A+	96%-100%
A	93% -100%
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	28.57%
Quizzes	28.57%
Final Exam	28.57%
Extra Credit	14.28%
	=====
Total =	100%

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.

Disruptive Classroom behavior

Disruptive classroom behavior may include (but is not limited to) the following: talking when it does not relate to the discussion topic, sleeping, reading other material (e.g. newspapers, magazines, textbooks, from other classes), eating or drinking, monopolizing discussion time, refusing to participate in classroom activities, leaving cell phones and pagers on, riding unicycles on desks, texting, making rude biological noises, and engaging in any other activity not related to the classroom activity. Students who engage in disruptive behavior will be approached by the instructor. If the disruptive behavior continues, students may be asked to leave the classroom and/or eventually be dropped from the course.

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 Jones and Bartlett virtual laboratory, please contact Jones and Bartlett Technical Support directly at msupport@jblearning.com or, if the problem stems from a client software glitch in your personal computer, complete your course work using the computers in the CIS lab.

SCHEDULE/CALENDAR

Unit/ Week	Date	Topic	News/Extra Credit Present?	Reading	Test (1)/ Quiz (5)	Due
1	4/9-4/15/2017	Intro, syllabus, Applying the Daubert Standard to Forensic Evidence	No	Chpt 1&2		
2	4/16-4/22/2017	Documenting a Workstation Configuration Using Common Forensic Tools	Yes	Chpt 3,14&15	Quiz 1	Lab 1, midnight 4/21/17
3	4/23-4/29/2017	Uncovering New Digital Evidence Using Bootable Forensic Utilities	Yes	Chpt 4	Quiz 2	Lab 2, midnight 4/26/17

4	4/30-5/6/2017	Creating a Forensic System Case File for Analyzing Forensic Evidence	Yes	Chpt 5&6	Quiz 3	Lab 3, midnight 5/3/17
5	5/7-5/13/2017	Analyzing Images to Identify Suspicious or Modified Files	Yes	Chpt 7	Quiz 4	Lab 4, midnight 5/10/17
6	5/14-5/20/2017	Recognizing the Use of Steganography in Image Files	Yes	Chpt 8	Quiz 5	Lab 5, midnight 5/17/17
7	5/21-5/27/2017	Automating E-mail Evidence Discovery Using P2 Commander	Yes	Chpt 9	Quiz 6	Lab 6, midnight 5/24/17
8	5/28-6/3/2017	Decoding an FTP Protocol Session for Forensic Evidence	Yes	Chpt 10& 11	Quiz 7	Lab 7, midnight 5/31/17
9	6/4-6/10/2017	Identifying and Documenting Evidence from a Forensic Investigation		Chpt 12	Quiz 8	Lab 8, midnight 6/7/17
10	6/11-6/17/2017	Conducting an Incident Response Investigation for a Suspicious Login	Yes	Chpt. 13	Quiz 9	Lab 9, midnight 6/14/17
11	6/18-6/24/2017	Study for Final			Quiz 10	Lab 10, midnight 6/21/17
12	6/29/2017	FINAL - (120 min) 6:15-8:15 PM	No	Chapters 1-15	FINAL	