TECHNICAL COLLEGE
OF THE LOWCOUNTRY

Technical College of the Lowcountry
921 Ribaut Road, PO Box 1288
Beaufort, SC 29901

Dr. Kenneth Flick
Business Technologies Division
843-441-0362
kflick@tcl.edu

IST 269
DIGITAL FORENSICS

COURSE DESCRIPTION

Prerequisite(s): CPT 242 or instructor approval.
This course will examine the advanced technical aspects of digital computer evidence detection, collection, identification and preservation. Emphasis will be placed on specific tools and methods for extracting deleted or destroyed computer r Lec. 3 Lab. 0 Cr. 3

Guide to Computer Forensics and Investigations

Nelson, Philips, Stewart, 2016

ISBN: 13: 978-1-337-38361-4

Supplemental Study Guide for CySA+ Cybersecurity Analyst Certification

Student should register for Cengage Unlimited.

Online Students should have access to a computer running Windows 7 or later with internet access. If you are taking this as an online course, you should have web access and be able to send in homework via email

To access the class web site:

Go to: elearning.tcl.edu or www.tcl.edu

Click on the Blackboard logo (you might need to scroll down on the web page)

Enter your login and password

Username (first name, last name-no caps and no spaces; Example Ken Flick would be kenflick)

Password: (first initial of last name and last three numbers of social security number; Example of 123-45-6789 for Ken Flick would be f789)

Click on class IST 269

If you cannot get to the site, please call the helpdesk 525- 8344 or email them at helpdesk@tcl.edu.

COURSE GOALS

The following list of course goals will be addressed in the course. These goals are directly related to the performance objectives (Addendum A). (*designates a CRUCIAL goal)

1. understand an overview of digital forensics
. 2. understand the history of digital forensics
3. understand preparing for digital investigations
4. identify duties of the lab manager and staff
5. identify the physical requirements for a digital forensics lab
6. select workstations for the forensics lab
7. select hardware peripherals
8. select operating systems and software inventories
9. describe storage formats for digital evidence
10. describe the best acquisition method
11. describe acquisition tools
12. determining digital evidence
13. determining evidence in private sector incident scenes
14. processing law enforcement crime scenes
15. preparing for a search
16. securing a computer incident or crime scene
17. seizing digital evidence at the crime scene
18. storing digital evidence
19. explore file systems
20. explore Microsoft file structures
21. explore NTFS disks
22. perform whole disk encryption
23. evaluate virtual machines
24. evaluate digital forensics tool needs
25. examine linux file structures
26. examine linux forensic tools
27. recognize a graphics file
28. recognize data compression
29. locate and recover graphic files
30. identify unknown file formats
31. determine what data to collect and analyze
32. validate forensic data
32. address data-hiding techniques
33. review virtual machine forensics
34. perform live acquisitions in windows
35. perform a networks forensics overview
36. explore e-mail investigations
37. understand e-mail servers
38. use special e-mail forensic tools
39. apply digital forensics to social media
40. understand mobile device forensics
41. understand acquisition procedures for mobile devices

42. understand cloud computing
43. discuss legal challenges in cloud forensics
44. discuss technical challenges in cloud forensics
45. understand the importance of reports
46. generate report findings with forensics software tools
47. prepare for CySA+ Cybersecurity Analyst Certification

STUDENT CONTRIBUTIONS

Each student will spend at least 6 hours per week preparing for class and preparing assignments to turn in weekly. Attendance is critical in this class if this information is new to you.

Each week students will turn in a list of assignments as specified on the class website and also take chapter tests as each chapter in the book is completed. They will also take a final exam to demonstrate their knowledge of the material.

Students will use a python developer environment on a TCL computer or they will set up the development environment on their own computers. Students will be expected to write python programs and demonstrate them.

Student Attendance Policy : See student handbook within course catalog.

ADA STATEMENT

The Technical College of the Lowcountry provides access, equal opportunity and reasonable accommodation in its services, programs, activities, education and employment for individuals with disabilities. To request disability accommodation, contact the counselor for students with disabilities at (843) 525-8228 during the first ten business days of the academic term.

ACADEMIC MISCONDUCT

There is no tolerance at TCL for academic dishonesty and misconduct. The College expects all students to conduct themselves with dignity and to maintain high standards of responsible citizenship.

It is the student's responsibility to address any questions regarding what might constitute academic misconduct to the course instructor for further clarification.

The College adheres to the Student Code for the South Carolina Technical College System. Copies of the Student Code and Grievance Procedure are provided in the TCL Student Handbook, the Division Office, and the Learning Resources Center.

ATTENDANCE

The College's statement of policy indicates that students must attend ninety percent of total class hours or they will be in violation of the attendance policy.

"Students not physically attending class during the first ten calendar days from the start of the semester must be dropped from the class for NOT ATTENDING.

" Students taking an online/internet class must sign in and communicate with the instructor within the first ten calendar days from the start of the semester to indicate attendance in the class. Students not attending class during the first ten calendar days from the start of the semester must be dropped from the class for NOT ATTENDING.

"Reinstatement requires the signature of the division dean.

"In the event it becomes necessary for a student to withdraw from the course OR if a student stops attending class, it is the student's responsibility to initiate and complete the necessary paperwork. Withdrawing from class may have consequences associated with financial aid and time to completion.

" When a student exceeds the allowed absences; the student is in violation of the attendance policy. The instructor MUST withdrawal the student with a grade of "W", "WP", or "WF" depending on the date the student exceeded the allowed absences and the student's progress up to the last date of attendance

or under extenuating circumstances and at the discretion of the faculty member teaching the class, allow the student to continue in the class and make-up the work. This exception must be documented at the time the allowed absences are exceeded.

" Absences are counted from the first day of class. There are no "excused" absences. All absences are counted, regardless of the reason for the absence.

"A student must take the final exam or be excused from the final exam in order to earn a non-withdrawal grade.

" A copy of TCL's STATEMENT OF POLICY NUMBER: 3-1-307 CLASS ATTENDANCE (WITHDRAWAL) is on file in the Division Office and in the Learning Resources Center.

ONLINE ATTENDANCE PROCEDURE

For all online courses, students must complete an assignment designated by the instructor during the first week of classes. The instructor will drop the student from the course if the initial assignment is not completed.

Instructors will withdraw students from the class when 90% attendance is not maintained. Attendance in

an online course is defined by regular course access and by timely completion of assignments as required by the instructor. Each student will be expected to access the web class at least once a week and complete 90% of assignments on time. Additional access is encouraged and may be necessary for successful completion of classes.

Failure to log in and complete assignments will result in the student being withdrawn from the course. The instructor will assign a grade of “W,” “WP,” or “WF” based upon the student’s academic standing as the last date of attendance, which is the last login. Students are responsible for any financial matters associated with an administrative withdrawal. If a fails to email the instructor (using the my.tcl.edu email account) requesting to be dropped from the course and has not submitted the initial assignment required during the first week of class, the instructor will assign a “Never Attended” code in the student information system (web-advisor) no later than ten calendar days after the first day of the class. Students who are dropped as a result of never attending the course are still responsible for all fees associated with the course.

HAZARDOUS WEATHER

In case weather conditions are so severe that operation of the College may clearly pose a hardship on students and staff traveling to the College, notification of closing will be made through the following radio and television stations: WYKZ 98.7, WGCO 98.3, WGZO 103.1, WFXH 106.1, WWVV 106.9, WLOW 107.9, WGZR 104.9, WFXH 1130 AM, WLVH 101.1, WSOK 1230 AM, WAEV 97.3, WTOC TV, WTGS TV, WJWJ TV, and WSAV TV. Students, faculty and staff are highly encouraged to opt in to the Emergency Text Message Alert System. www.tcl.edu/textalert.asp

Emergency Text Message Alert

Students, faculty and staff are highly encouraged to opt in to the Emergency Text Message Alert System. Participants receive immediate notification of emergency events and weather cancelations via text messaging on their cell phones. Participants can also opt in to receive non-emergency news and announcements. Go to www.tcl.edu. On the homepage, click on "emergency TextAlert at TCL" and fill out the form or go to www.tcl.edu/textalert.asp

BROADCAST LEARNING FORMAT: This class is being taught in a broadcast learning format. Images and word of class participants may be transmitted live or on a delayed basis to other locations. Classes may be rebroadcast due to extenuating circumstance.

COURSE EVALUATION

Each week's assignments are worth 100 points and averaged over the semester. chapter tests are also worth 100 points and averaged at the end of the semester. The final will be 100 points.

Tests: 50%

Final Project: 45%

COURSE SCHEDULE

The class can be taken online or as a web-enhanced class that meets 1.5 hours per week.
We will cover the information in the order of the content goals as listed.

Syllabus Safety Addendum

Purpose

The purpose of this safety addendum is to provide each student with safety guidelines during an incident, emergency, or disaster at TCL. In addition, it provides students guidelines for lockdown procedures, evacuation procedures, and active shooter.

Definition

An incident is any event, potential or actual, that may impact normal operations but has no immediate health or life threatening consideration or serious effect on the overall functional capacity of the College. An event of this nature should be reported to the Office of the Vice President for Administrative Services. Also notify the off-site campus administrator if applicable.

An emergency is any incident, potential or actual, which may endanger life or health or which affects an entire building or buildings, and will disrupt the overall operations of the College. Outside emergency services will probably be required, as well as major efforts from campus support services. Major policy considerations and decisions will usually be required from the college administration during times of crises. An emergency should be reported immediately by directly using **911** if life or health/injury considerations exist and then to the Office of the President or Vice President for Administrative Services as quickly as possible. Also notify the off-site campus administrator if applicable.

A disaster is any event or occurrence that has taken place and has seriously impaired or halted the operations of the College. In some cases, mass personnel casualties and severe property damage may be sustained. A coordinated effort of all campus-wide resources is required to effectively control the situation. Outside emergency services will be essential. In all cases of disaster, an Emergency Control Center will be activated, and the appropriate support and

operational plans will be executed. The disaster should be immediately reported, first by calling **911** and then to the Office of the President or Vice President for Administrative Services. Also notify the off-site campus administrator if applicable.

Types of Emergencies

- Hurricane
- Tornado
- Fire
- Biochemical or Radiation Spill
- Explosion/Bomb
- Downed Aircraft (crash which directly impacts campus operations)
- Utility Failures
- Violent or criminal behavior
- Psychological Crisis

Procedures

Active Shooter
Run/hide/fight (http://www.fbi.gov/about-us/cirg/active-shooter-and-mass-casualty-incidents/run-hide-fight-video)

Building Evacuation
1. Building evacuations occur when an alarm sounds and/or upon notification by Security or the Emergency Director.

2. When the building evacuation alarm is activated during an emergency, individuals should exit according to the building evacuation plan and alert others to do the same.

3. Once outside, individuals should proceed to a clear area that is at least 500 feet away from the affected building. Streets, fire lanes, hydrant areas and walkways should be kept clear for emergency vehicles and personnel.

4. Individuals should not return to an evacuated building unless told to do so by Security or the Emergency Director.

5. Individuals should assist persons with disabilities in exiting the building. Elevators are reserved for disabled persons

Campus Evacuation
1. A uniformed Security Guard, the Emergency Director, or an Emergency Resource Team member will announce evacuation of all or part of the campus grounds.

2. All persons (students and staff) are to immediately vacate the campus, or in the case of a partial evacuation relocate to another part of the campus grounds as directed.

Lockdown
1. Clear the halls
2. Report to the nearest classroom/office
3. Assist those needing special assistance
4. Ensure classroom/office doors are closed and locked
5. Turn off lights
6. Stay away from doors and windows (out of the line of sight)
7. BE QUIET and follow instructor's directions
8. Silence cell phones
9. Wait for the "All Clear" before leaving

Updated 1/28/19