

South Plains College
Semester: Spring 2020
Revised 1/6/2020

Instructor Contact Information:

Name: Ben Walton
Office Location: LC120A – Lubbock Center
Email: bwalton@southplainscollege.edu
Office Phone: 806-716-4602
Office Hours: See Blackboard
Blackboard: <http://southplainscollege.blackboard.com/>
Remind: See Blackboard (required)

Course Sections:

Section: ITSY2343.271 Computer System Forensics
Format: Hybrid
Campus: Lubbock Center
Lecture: Online
Lab: LC113: Tue/Thu
9:00-10:40AM

COURSE DESCRIPTION:

In-depth study of system forensics including methodologies used for analysis of computer security breaches. Gather and evaluate evidence to perform postmortem analysis of a security breach.

Credit: 3 Lecture: 3 Lab: 2

COURSE OUTCOME:

- Identification of computer investigation issues
- Identification of legal issues associated with computer investigations
- Collection and documentation of evidence and digital evidence
- Evaluation of network traffic
- Evaluation of recovered data

Course Competencies:

There are seven general areas in which a digital forensics examiner must be competent:

1. Search Warrants
2. Evidence Control
3. Data Image Acquisition
4. Data Image Examination

5. Data Recovery
6. Data Analysis
7. Documentation & Reports

This list of competencies is also the typical sequence of work that a digital forensics examiner performs. As you progress through the Course, you will learn about each of the general areas of competency. You will also acquire the knowledge and develop the skills to be able to demonstrate proficiency in these areas. Each area of competency contains knowledge-based and skill-based competencies.

SEARCH WARRANTS

There are several types of possible permissions that may be granted to search a computer or other electronic device. You will learn how to work with the various types of permissions. You will also learn the importance of knowing the scope of an investigation.

EVIDENCE CONTROL

Digital forensics examiners must utilize the chain of custody procedures for their law enforcement agency or corporate entity. You will work with authentic evidence bags and tape. You will also work with check in & check out procedures.

DATA IMAGE ACQUISITION

Digital forensics examiners do not merely copy a suspect's hard drive, memory card or USB drive. Instead, a forensic copy must be made. This is a bit-by-bit copy of the evidence. Only by making a forensic copy can deleted files be recovered and other evidence gathered.

You will acquire forensic images from several different types of hard drives, memory cards and USB drives. Each memory storage device contains evidence. You will use a forensic duplicator to acquire images from the devices.

DATA IMAGE EXAMINATION

The Trainer teaches decimal, binary & hexadecimal number systems. You will use a hexadecimal editor program to work with ASCII and Unicode data. You will also learn how to work with the various Windows file systems (FAT12, FAT16, FAT32 and NTFS).

You will learn to identify graphic file types and file compression methods. You will also use software and hardware write-blockers (bridges) to make working copies of evidence images.

DATA RECOVERY

You will use several forensic software programs to recover deleted and hidden files & partitions, web activity & e-mail. You will also use password recovery software to crack Windows passwords, open encrypted files. You will also learn how to identify data hidden within a file.

DATA ANALYSIS

After files are recovered, they must be analyzed to determine if they are relevant to the case. You will explore how to interpret recovered data and put it in a logical and useful format. You will use forensic software to conduct data searches for keywords and hexadecimal codes.

DOCUMENTATION & REPORTS

Throughout the Course, you will document your work and produce reports of your evidence examination work, including reports produced by forensic software.

MATERIALS NEEDED:

- MindTap (electronic textbook, lab, and materials): ISBN 9781337568999
 1. Guide to Computer Forensics & Investigations, 6th Ed.
 2. Lab Manual for Guide to Computer Forensics & Investigations, 6th Ed.
- USB Thumb/Flash/Jump Drive
- Computer/Laptop and reliable Internet connection

Course Evaluation: Students will be evaluated by assignments, exams, and projects.

Category	Percentage
Attendance	10%
Quizzes/Assignments/Labs	35%
Exams	40%
Final Exam	15%

Attendance Policy: Students are expected to attend all classes in order to be successful in a course. The student may be administratively withdrawn from the course when absences become excessive as defined in the course syllabus.

Class attendance, even online, is extremely important in order to meet the objectives of this course. A student is responsible for initiating his or her own withdrawal, if that becomes necessary. If a student is administratively withdrawn from the class by the professor, the grade appearing on the transcript will be at the professor’s discretion, an ‘X’ or ‘F’.

Administrative withdrawal may occur if the student has missed six (6) class periods for MWF classes, four (4) class periods for MW/TR classes, two (2) class periods for hybrid classes or if the professor decides absences are excessive due to non-participation or incomplete coursework. When enrolled in an online course, students must login to Blackboard two times per week. Two weeks of non-participation in an online course may also result in an administrative drop.

See the General Catalog Attendance Policy for additional information.

Plagiarism and Cheating: Students are expected to do their own work on all projects, quizzes, assignments, examinations, and papers. Failure to comply with this policy will result in an F for the assignment and can result in an F for the course if circumstances warrant.

Plagiarism violations include, but are not limited to, the following:

1. Turning in a paper that has been purchased, borrowed, or downloaded from another student, an online term paper site, or a mail order term paper mill.
2. Cutting and pasting together information from books, articles, other papers, or online sites without providing proper documentation.
3. Using direct quotations (three or more words) from a source without showing them to be direct quotations and citing them.
4. Missing in-text citations.

Cheating violations include, but are not limited to, the following:

1. Obtaining an examination by stealing or collusion.
2. Discovering the content of an examination before it is given.
3. Using an unauthorized source of information (notes, textbook, text messaging, internet, apps) during an examination, quiz, or homework assignment.
4. Entering an office or building to obtain unfair advantage.
5. Taking an examination for another.
6. Altering grade records.
7. Copying another's work during an examination or on a homework assignment.
8. Rewriting another student's work in Peer Editing so that the writing is no longer the original student's work.
9. Taking pictures of a test, test answers, or someone else's paper.

Drop Policy: You may be dropped with an X or F for any of the following reasons:

1. Attendance
 - a. You do not follow the guidelines of the attendance policy listed above.
2. Participation, completion of homework, exams, and team project
 - a. You have missed several homework assignments.
 - b. You have missed two or more exams.
 - c. You have not participated with your assigned team.
3. Academic Integrity
 - a. Cheating, plagiarism, or sharing your work with others as listed above.

Student Code of Conduct Policy: Any successful learning experience requires mutual respect on the part of the student and the instructor. Neither instructor nor student should be subject to others' behavior that is rude, disruptive, intimidating, aggressive, or demeaning. Student conduct that disrupts the learning process or is deemed disrespectful or threatening shall not be tolerated and may lead to disciplinary action and/or removal from class.

Diversity Statement: In this class, the teacher will establish and support an environment that values and nurtures individual and group differences and encourages engagement and interaction. Understanding and respecting multiple experiences and perspectives will serve to challenge and stimulate all of us to learn about others, about the larger world and about ourselves. By promoting diversity and intellectual exchange, we will not only mirror society as it is, but also model society as it should and can be.

Disability Statement: Students with disabilities, including but not limited to physical, psychiatric, or learning disabilities, who wish to request accommodations in this class should notify the Disability Services Office early in the semester so that the appropriate arrangements may be made. In accordance with federal law, a student requesting accommodations must provide acceptable documentation of his/her disability to the Disability Services Office. For more information, call or visit the Disability Services Office at Levelland (Student Health & Wellness Office) 806-716-2577, Reese Center (Building 8) 806-716-4675, or Plainview Center (Main Office) 806-716-4302 or 806-296-9611.

Nondiscrimination Policy: South Plains College does not discriminate on the basis of race, color, national origin, sex, disability or age in its programs and activities. The following person has been designated to handle inquiries regarding the non-discrimination policies: Vice President for Student

Affairs, South Plains College, 1401 College Avenue, Box 5, Levelland, TX 79336. Phone number 806-716-2360.

Title IX Pregnancy Accommodations Statement If you are pregnant, or have given birth within six months, Under Title IX you have a right to reasonable accommodations to help continue your education. To [activate](#) accommodations you must submit a Title IX pregnancy accommodations request, along with specific medical documentation, to the Director of Health and Wellness. Once approved, notification will be sent to the student and instructors. It is the student's responsibility to work with the instructor to arrange accommodations. Contact the Director of Health and Wellness at 806-716-2362 or [email cgilster@southplainscollege.edu](mailto:cgilster@southplainscollege.edu) for assistance.

Campus Concealed Carry: Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in South Plains College buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and South Plains College policy, license holders may not carry a concealed handgun in restricted locations. For a list of locations and Frequently Asked Questions, please refer to the Campus Carry page at: <http://www.southplainscollege.edu/campuscarry.php>

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all South Plains College campuses. Report violations to the College Police Department at 806-716-2396 or 9-1-1.

IMPORTANT INFORMATION BELOW

Communication: This is a hybrid class and all communication for this class will be conducted through the Remind App (See Blackboard) with SPC email as a backup. All students will be required to check their Remind App and SPC student email accounts regularly for course updates and announcements. All replies to emails will be sent to the student's SPC email address. Please include your name, course name, and section number in all email communication.

Additional Textbook Information: The access code with electronic textbooks is available at the SPC bookstore. You can also purchase the MindTap access code directly from Cengage. Please see more detailed information on Blackboard – How to access your MindTap Course.

Instructional and Outside Course Time Estimation:

- Reading and Study Time: 2 hours x 16 modules/chapters = 32 hours
- Assignment Time: 2 per chapter x 16 chapters x 1 hour = 32 hours
- Activity Time: 48 total assignments x 1 hour each = 48 hours
- Exam Time: 4 exams x 1 hour = 4 hours

Total Estimated Minimum Course Time = 116 hours

Total Estimated Minimum Time per Week = 7.5 hours per week

Reading Assignments: Mandatory, assigned reading is a requirement for this course. Without reading the book and going through the voluntary tutorials, you may fall behind and become lost as we move through the semester. Going through the book, following the tutorials and doing the simulations will greatly help you pass the quizzes, assignments, labs and exams.

Assignments: Assignments will be available through MindTap and Blackboard. The course calendar outlining due dates and availability times is available in Blackboard. There may also be homework assignments and projects assigned periodically throughout the semester. No late work is accepted! You are expected to complete all homework assignments within the due dates indicated. Missing homework assignments may result in an administrative drop.

It is important for you to start your homework early in the week. Do not wait until the night it is due to report problems. If you report problems the night of an assignment, the instructor is not obligated to re-open those for you. Start your homework early in the week and complete it with time to spare!

Exams: There will be four exams given, one after every four chapters/modules. Exams will be given using the MindTap courseware. The exam will be open for several days and no make-up exams will be given.

Gradebook: The gradebook will be updated automatically each time you complete an assignment or exam. The gradebook and your current average will be available in MindTap/Blackboard.

Counseling: If at any point in the semester you find yourself having trouble with stress or feel depressed please stop in and see a counselor. Counseling services are available at all campuses. The number for the counseling office is 806-716-2366. Below is a link to SPC's personal

counseling services.

<https://www.southplainscollege.edu/health/mentalhealthresources.php>

Note: The instructor reserves the right to modify the course syllabus and policies, as well as notify students of any changes, at any point during the semester.