ITSY 2343
Section 001 (LC113)
Computer System Forensics

Spring 2019

Instructor:	Ben Walton		
Phone:	716- 4602	**Location:**	Lubbock Center 120A
Office Hours:	See Additional Handout		
Class Time:	Section 001: TR (9:00AM – 10:40AM)	**Location:**	Section 001: LCC 113
Email:	bwalton@southplainscollege.edu		
Blackboard:	http://southplainscollege.blackboard.com/		

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.

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:

- Textbook:
  1. Guide to Computer Forensics & Investigations, 5th Ed.
     (ISBN-13: 9781285060033)
  2. Lab Manual for Guide to Computer Forensics & Investigations, 5th Ed.
     (ISBN-13: 9781285079080)
- USB Thumb/Flash/Jump Drive
- Binder 3 Ring, 2”-3”
- Composition Notebook

ATTENDANCE:

Students are expected to attend all class meetings. Two late arrivals to class will be considered an absence. Two consecutive absences, four total absences, or three late/missed assignments will be cause for the student to be dropped from this class. Missed assignments can/will be treated as absences. This drop will be initiated by the instructor.

It is the responsibility of each student to monitor his or her progress in the course and to request conference time with the instructor if there are questions or problems. Your questions and any discussions regarding course material are encouraged at all times.

THE INSTRUCTOR RESERVES THE RIGHT TO CHANGE ANY PORTION OF THIS SYLLABUS AT ANY TIME.

HOMEWORK:

If you are absent from a class, you are still required to turn in any homework on the date it is due. You must come see me, consult the website, or ask a classmate for missed work. NO late homework will be accepted. All homework is to be uploaded by the time and date it is due.

CHEATING POLICY:

Cheating will result in a zero on the assignment at the very least if not a
zero for the class.

GRADING POLICY: Final grades will be calculated as follows:

Attendance	10%
Review Questions	10%
Labs	10%
Quizzes	10%
Exams (4)	30%
Final Exam	30%

Each exam is announced and reviewed prior to the test. There are NO make-up exams.

Numeric grades will be given on all tests and assignments based on the following scale:

90-100	= A
80-89	= B
70-79	= C
60-69	= D
Below 60	= F

ADDITIONAL INFORMATION: Smoking is not allowed in any SPC facility. Food or drinks will be allowed in designated areas only and not permitted in classrooms, laboratories, library, shops, elevators, etc. Cellular phones should be turned off during class time. Copying or removing copyright materials from the computer labs is in violation of the law and is strictly prohibited. Your cooperation is certainly appreciated and will benefit the overall learning environment.

SCANS:

SCANS competencies incorporated within the structure and content of this class include:
C1,C3,C5,C6,C7,C8,C9,C10,C14,C15,C16,C17,C18,C19,C20

SCANS foundation skills incorporated within the scope of instruction and performance of this class include:
F1,F2,F3,F4,F5,F6,F7,F8,F9,F10,F12,F13,F14,F15,F16,F17

SCANS COMPETENCIES

C-1 TIME-Selects goal relevant activities, ranks them, allocates time, and prepares and follows schedules.

C-2 MONEY-Uses or prepares budgets, makes forecasts, keeps records, and makes adjustments to meet objectives.

C-3 MATERIALS & FACILITIES-Acquires, stores, allocates, and uses materials or space efficiently.

C-4 HUMAN RESOURCES-Assesses skills and distributes work accordingly, evaluates performances and provides feedback.

INFORMATION-Acquires and Uses Information

C-5 Acquires and evaluates information

C-6 Organizes and maintains information.

C-7 Interprets and communicates information.

C-8 Uses computers to Process information.

INTERPERSONAL-Works With Others

C-9 Participates as members of a team and contributes to group effort.

C-10 Teaches others new skills.

C-11 Serves clients/customers-works to satisfy customer's expectations.

C-12 Exercises leadership-communicates ideas to justify position, persuades and convinces others, responsibly challenges existing procedures and policies.

C-13 Negotiates-Works toward agreements involving exchanges of resources resolves divergent interest.

C-14 Works with Diversity-Works well with men and women from diverse backgrounds.

SYSTEMS-Understands Complex Interrelationships

C-15 Understands Systems-Knows how social, organizational, and technological systems work and operates effectively with them.

C-16 Monitors and Correct Performance-Distinguishes trends, predicts impacts on system operations, diagnoses systems performance and corrects malfunctions.

C-17 improves or Designs Systems-Suggest modifications to existing systems and develops new or alternative systems to improve performance.

TECHNOLOGY-Works with a variety of technologies

C-18 Selects Technology-Chooses procedures, tools, or equipment including computers and related technologies.

C-19 Applies Technology to Task-Understands overall intent and proper procedures for setup and operation of equipment.

C-20 Maintains and Troubleshoots Equipment-prevents, identifies, or solves problems with equipment, including computers and other technologies.

FOUNDATION SKILLS

BASIC SKILLS-Reads, writes, performs arithmetic and mathematical operations, listens and speaks

F-1 Reading-locates, understands, and interprets written information in prose and in documents such as manuals, graphs, and schedules.

F-2 Writing-Communicates thoughts, ideas, information and messages in writing, and creates documents such as letters, directions, manuals, reports, graphs, and flow charts.

F-3 Arithmetic-Performs basic computations, uses basic numerical concepts such as whole numbers, etc.

F-4 Mathematics-Approaches practical problems by choosing appropriately from a variety of mathematical techniques.

F-5 Listening-Receives, attends to, interprets, and responds to verbal messages and other cues.

F-6 Speaking-Organizes ideas and communicates orally.

THINKING SKILLS-Thinks creatively, makes decisions, solves problems, visualizes, and knows how to learn and reason

F-7 Creative Thinking-Generates new ideas.

F-8 Decision-Making-specifies goals and constraints, generates alternatives, considers risks, and evaluates and chooses best alternative.

F-9 Problem Solving-Recognizes problems and devises and implements plan of action.

F-10 Seeing Things in the Mind's Eye-Organizes and processes symbols, pictures, graphs, objects, and other information.

F-11 Knowing How to Learn-Uses efficient learning techniques to acquire and apply new knowledge and skills.

F-12 Reasoning-Discovers a rule or principle underlying the relationship between two or more objects and applies it when solving a problem.

PERSONAL QUALITIES-Displays responsibility, self-esteem, sociability, self-management, integrity and honesty

F-13 Responsibility-Exerts a high level of effort and preservers toward goal attainment.

F-14 Self-Esteem-Believes in own self-worth and maintains a positive view of self.

F-15 Sociability-Demonstrates understanding, friendliness, adaptability, empathy, and politeness in group settings.

F-16 Self-Management-Assesses self accurately, sets personal goals, monitors progress, and exhibits self-control.

F-17 Integrity/Honesty-Chooses ethical courses of action.

CAMPUS GUIDELINES

CHILDREN ON CAMPUS

Many of the students attending classes at South Plains College are also parents who value the opportunity to participate in higher education. Sometimes students are faced with the decision of whether to remain at home with their children, bring children with them to class, or be absent from class. The following guidelines address concerns for the safety of children on campus and provide for an environment conducive to learning:

1. **Students are not allowed to bring children to class** and will be asked to leave in the interest of providing an environment conducive for **all** students enrolled in the class. Students are responsible for adherence to the attendance requirements set forth by the instructor in the course syllabus.
2. **Children may not be left unattended.** In order to provide for the safety of children on campus, parents or other guardians are responsible for supervising children while utilizing services or conducting business on campus.
3. **Disruptive children will not be allowed to interfere with college business.** Parents or other guardians are responsible for supervising and controlling the behavior of children they have brought on campus.

AMERICANS WITH DISABILITIES ACT 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 Center 806-716-2577, Reese Center (also covers ATC) Building 8: 806-716-4675, Plainview Center Main Office: 806-716-4302 or 806-296-9611, or the Health and Wellness main number at 806-716-2529.

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.

(*Developed by the Title III summer 2001 participants as part of the training opportunity, May-June 2001, South Plains College).

GENERAL SAFETY ON CAMPUS

South Plains College recognizes the importance of safety on campus. The protection of persons and property is a responsibility which we all share. Personal safety begins with the individual. The following guidelines are intended to assist you in protecting yourself and to encourage practices that contribute to a safe environment for our campus community.

- Never leave your personal property unsecured or unattended.
- Look around and be aware of your surroundings when you enter and exit a building.
- Whenever possible, avoid walking alone, particularly after dark. Walk to your vehicle with other class members or request that the Security Guard walk you to your car.
- When approaching your vehicle, keep your keys in your hand; look under your car and in the back seat and floorboard. Lock the doors as soon as you are inside your car.

FOOD AND DRINK IN CLASSROOMS

It is the policy of South Plains College not to permit food or drink in the classrooms or laboratories.

In case of emergency, contact the following numbers but DO NOT leave a voice mail message:
716-2338 - Levelland Campus 716-4677 – Lubbock Center 716-2923 - Reese Center (mobile 893-5705)