BOR 6342
Cybersecurity and the Constitution

Course Description

This course examines the scope of cybercrime and its impact on today's system of criminal justice. Topics to be studied include: cybercrime and the Bill of Rights, computer-based economic crime, electronic commerce, ethical challenges, and the Computer Fraud and Abuse Act. Included will be an analysis of the legal considerations facing law enforcement and cybersecurity professionals who deal with the problems of discovering, investigating, and prosecuting cybercrime.

Course Bibliography and Required Readings

Digital Evidence and Computer Crime (3rd edition)
Author: Casey, Eoghan
Date: 2011

ISBN (hard cover): 978-0-12-374268-1
There is no electronic version at this time. Relatively inexpensive copies may be acquired from online booksellers.

Prerequisites

There are no prerequisites for this course.

Technical Skills Required for This Course

AS with all online courses, students must be able to operate a computer and have the necessary technical skills to navigate around a web page. Additional technical skills are not a prerequisite for this course, however your computer must meet certain minimum requirements to operate Blackboard.

Time Spent on this Course

Students can expect to spend a minimum of 6 hours per week to complete all readings and assignments. The lessons themselves take as long as it requires the student to read the materials and watch or listen to media presentations.

Course Objectives/Learning Outcomes

Objective 1: Gain knowledge about the way in which cybersecurity, and the computer itself, has affected - and has been affected by - the criminal justice system, law enforcement professionals, and the community-at-large.

Objective 2: Become conversant with terminology of the world of “cyberspace, “with emphasis on terms and concepts pertinent to the application of computerization within the criminal justice system.

Objective 3: Be able to discuss the impact that specific security issues related to cybertecbnology have had on the criminal justice system in particular, and upon modem society in general, in the context of past, present, and future developments.

Objective 4: Be able to identify and analyze provisions of the United States Constitution, with special emphasis on The Bill of Rights, which underlie the basis upon which the criminal justice system must deal with “cybercrime, “and those who commit such criminal acts.

Objective 5: Be able to distinguish the particular attributes of a computer-based economic system which tend to facilitate fraud and other criminal acts by those with criminal intent.

Objective 6: Be able to compare and contrast and, more significantly, understand those efforts undertaken by the Legislative and Executive branches of both state and federal government to thwart crimes facilitated by or, in some instances, only made possible by the use of computers.

Objective 7: Be able to trace the history of development of the law enforcement community’s efforts at policing the unlawful use of computers.

Objective 8: Be able to identify the ethical challenges to be considered by those within the Law enforcement field who are working to thwart cybertech crime.

Objective 9: Be able to anticipate changes in laws and legal procedures that may likely occur as the criminal justice system attempts to forestall further incursions by deviants into the world of cybertech security.

One consistent skill which you will need in any future career is that of effective writing and the ability to clearly communicate your thoughts. Therefore, you will be assigned discussion boards that evaluate your ability to write clearly. Your instructor will grade your assignment on technical skills, such as clear organization, spelling and grammar usage, as well as a subjective assessment of whether or not you are able to think critically and analyze both sides of a legal or social issue.

Grading Policies

This course uses three major writing assignments, several short writing assignments, and weekly discussions to measure the student's comprehension of the presented materials.

There is an extensive amount of reading assigned that will drive student responses to discussion questions and writing assignments. Staying current with course is important. The subject matter in and of itself is particularly intense so staying on top of the subject matter and utilizing outside sources to better understand the information is imperative. Additionally, where possible, videos are utilized to enhance student learning.

Assignment	**Percent of Grade**	**Due**
Participation in the Discussion Board	100%	Initial Post: Fridays by 11:59pm Secondary Post: Sundays by 11:59pm

Angelo State University employs a letter grade system. Grades in this course are determined on a percentage scale:

A = 90 – 100 %
B = 80 – 89 %
C = 70 – 79 %
F = 59 % and below.

Discussions

This course employs eight (8) Discussion assignments. The Discussions account for 100% of the course grade. The professor will post discussion questions each week and you will be required to write an initial post of no less than 300-500 words and make at least two responses toward each of the discussions as a minimum. These postings should be made thoughtfully and you should be able to provide evidence for your conclusions through the reading materials or other source documents available to you. You must list your references in APA or CM writing style. References are not a part of the word minimum. A source document for your postings on the discussion is not Wikipedia.

Since this is a graduate course, you are expected to think critically of the weekly subject matter and be able to develop the rationale for your opinions as to what is working or not working and be able to provide some evidence for your conclusion(s).

Uploading Assignments

A video that describes how to upload assignments in Blackboard can be viewed by clicking this link:
Uploading Blackboard Assignments - video
A printable version of these instructions can be viewed by clicking this link:
Uploading Blackboard Assignments - PDF

Warning
Any PLAGIARISM will not be tolerated and can result in the failure of a course and dismissal from the University.

Rubrics

Discussion forums and writing assignments will be graded using a standardized rubric. It is recommended that you be familiar with these grading criteria and keep them in mind as you complete the writing assignments. There are two rubrics. Click the link to download the PDF document:
Discussion Rubric

Date and Time of Final Exam

There is no final exam in this course. The Final Project is in place for this reason.

Course Organization

Module 1:

Lesson 1 Computer Basics for Digital Investigators (cpt 15)
A basic understanding of how computers operate and how data is stored is a fundamental skil for forensic examiners. This includes understanding and controlling the boot process, recovering data, and analyzing data. Most digital investigators use automated forensic tools; however, it is absolutely crucial that they understand what these tools are doing. The best way to gain that understanding is by experimentation. That would include creating a file and viewing the results, deleting the file and viewing those results, using a low level hex editor, and carving data associated with the file into a new one.

Lesson2 Network Basics for Digital Investigators (cpt 21)
All digital investigators require some understanding of networks since most computers we encounter are connected to one. In fact, computers have become network-centered and it is no longer sufficient to only think of digital evidence on storage media. To comprehend traces of Internet activities left on personal computers and to establish continuity of offense, digital investigators require knowledge of evidence that exists on surrounding networks. These sources include server logs, network devices, and traffic on both wired and wireless networks.

Module 2:

Lesson 3 Language of Computer Crime Investigation (cpt 2)
Since the late 1980s there have been significant advances in investigating crime involving computers. In addition to advances in tool development, there have been refinements in the law, computer crime categories, and digital investigative methods

and theory. However, because it is still an emerging field, digital forensics requires additional development and refinement. Even the term digital forensics has only recently replaced computer forensics, forensic computing, and other terms that describe the field as a whole.

Lesson 4 Cybercrime Law: A United States Perspective (cpt 4)
The ultimate aim of this lesson is to have students compare the policies and laws in the US and EU, and highlight the similarities and differences between them. Technology provides criminals with new opportunities, and many existing laws do not adequately address the use of computers. Prosecution of crimes such as child exploitation, theft of intellectual property, Internet fraud, and cyberstalking has yet to be resolved, for a number of reasons. One issue is jurisdiction. If an Internet fraud is conducted in one state, via an offshore ISP, against a victim in another state – who has jurisdiction? Where did the crime take place? A related issue is extradition of criminals from other countries.

Module 3:

Lesson 5 Foundations of Digital Forensics (cpt 1).
Digital evidence has come to play some part in virtually every crime. It would, in fact, be difficult to describe a crime scene that does *not* have a digital element. Criminals have always found ways to use technology to their own ends, and digital technology is no different. There is an upside to this – the more digital technology is used, the more likely that there will be resulting digital evidence.
Digital forensics has undergone a number of changes from little more than looking at the hexadecimal values on floppy media to automated forensic tools that process terabytes of data in search of digital evidence.

Lesson 6 Digital Evidence in the Courtroom (cpt 3)
The foundation of a case involving digital evidence is proper evidence handling from proper practices of seizing, storing, and accessing evidence, and verification that evidence was properly handled.
It is important to emphasize that digital investigators will be presenting their findings to a non- technical audience. Therefore, is imperative that digital investigators are able to convey complex concepts in easier to understand terms

Module 4:

Lesson 7 Conducting Digital Investigations (cpt 6)
Following the twelve steps described in this lesson increase the likelihood that an investigation will lead to the truth and will serve justice. More specifically, the ultimate aim of the model covered in this lesson is to help investigators ascend a sequence of steps that are generally accepted, reliable, and repeatable, and lead to logical, well-documented conclusions of high integrity. To fully appreciate the flexibility and power of this model, it is necessary to explore how it applies to different types of investigations.

Lesson 8 Modus Operandi, Motive, and Technology (cpt 9)
Investigatory reconstruction provides a methodology for gaining a better understanding of a crime and focusing an investigation. Objectively reviewing available evidence provides a greater understanding of the case. This lesson also discusses threshold assessment and investigative reconstruction.

Module 5:

Lesson 9 Violent Crime and Digital Evidence (cpt 10)
To date, there are huge amounts of information about people’s personal and professional lives stored on computers, mobile devices, corporate computers, and the Internet. This vast store of information can show where victims of violent offenders were, and what they were doing, when the attack occurred. Digital evidence may reveal investigative leads, likely suspects, previously unknown crimes, and personal information that put the victim at risk.

Lesson 10 Digital Evidence as Alibi (cpt 11)
With people spending an increasing amount of time using mobile devices, computers, and networks, there are bound to be more alibis that depend on digital evidence. Digital evidence will rarely show that someone was at a specific location at a specific time; however, it can show that the device was at that location. Through the use of other supporting evidence, such as a phone call in progress or an e-mail sent, the device can be associated with an individual.

Module 6:

Lesson 11 Computer Intrusions (cpt 13)
Just as a company’s most valuable assets may be the data on its computers, failure to protect those assets may result in financial loss, regulatory sanctions, and reputational harm. More than one company has been forced into bankruptcy when the computer containing their company information crashed. A common truth is that criminals tend to steal things of value. Therefore, a company’s information may be a target.

Lesson 12 Applying Forensic Science to Computers (cpt 16)
Computer technology continues to evolve rapidly but the fundamental components have changed little. Because processes at the top level have not changed rapidly, it is both possible and reasonable to develop SOPs to be used in the field.

Module 7:

Lesson 13 Applying Forensic Science to Networks (cpt 22)
As discussed in earlier lessons, when handling digital evidence it is necessary to establish chain of custody, document the state of items in situ, and take other steps to preserve the evidence so that it can be authenticated at a later date. This lesson presents a methodology for processing digital evidence and describes key concepts and their

importance, including copying all data from a disk and calculating the cryptographic hash of a disk. Students will benefit from hands-on exercises dealing with preservation of digital evidence at this stage. The guidelines in the next lesson provide a basis for a Standard Operating Procedure (SOP) for preserving and documenting digital evidence on computers.

Lesson 14 Digital Evidence on the Internet (cpt 23)
The Internet is both an attractive venue for criminal activities and a powerful investigative tool. This lesson discusses both aspects to give investigators intelligence about how criminals operate online, and to help investigators use digital evidence on the Internet to apprehend offenders. The main Internet services are covered, including the Web, e-mail, newsgroups, Internet chat, and P2P. New services are emerging that extend the capabilities of the Internet, providing criminals with new opportunities, and making digital investigations more challenging. Therefore, in addition to becoming familiar with existing Internet services, students need to learn how to explore new technologies from an evidentiary and investigative viewpoint, as well as from a criminal viewpoint.

Module 8:

Lesson 15 Digital Evidence on Physical and Data-Link Layers (cpt 24)
This lesson expands on the overview provided in lesson 3, describing network technologies in more detail, focusing on Ethernet. Tools and techniques for preserving, examining, and analyzing network traffic are presented.

Lesson 16 Digital Evidence at the Network and Transport Layers (cpt 25)
This lesson expands on the overview provided in lesson 3, describing TCP/IP in more detail and demonstrating the usefulness of IP addresses in investigations. Because TCP/IP forms such an integral part of the Internet, information related to these layers are too numerous to describe individually. The glue that holds a network together gets stuck in many places for digital investigators to recover. Case examples are provided to improve students' familiarity with the many types of evidence that contain data relating to the transport and network layers.

Course Policies

Participation

In this class ***everyone***, brings something to the table. Your ideas and thoughts do count, not only to me, but the entire class. Feel free to ask questions either via e-mail or the discussion board. **Check the discussion board regularly.** Many student questions are applicable to the class as a whole, as are the responses. You may be surprised how many of your classmates have the same questions and concerns as you. I may simply post your particular question on the discussion board and allow your classmates to provide the answer through their own posts.

To some, this may be their first online class and naturally, it could seem somewhat intimidating. As a class, we are together to help each other with this learning process and share our collective knowledge on how best to communicate; how to resolve technical issues that may arise (if we have the expertise), and to assist each other to find answers to our questions.
We will learn and work as a team.

Courtesy and Respect

Courtesy and Respect are essential ingredients to this course. We respect each other's opinions and respect their point of view at all times while in our class sessions. The use of profanity & harassment of any form is strictly prohibited (Zero Tolerance), as are those remarks concerning one's ethnicity, life style, race (ethnicity), religion, etc., violations of these rules will result in immediate dismissal from the course.

Attendance

This is an online course and attendance is not taken. However, failure to participate in the discussion board, to communicate or respond to e-mails from the professor, is an indication something is wrong. Therefore, we have made both a significant component of the course grade as an enticement to keep you engaged in the learning process. Failure to participate or communicate on the part of a student will result in an appropriate reduction of your grade and possibly in your failure of this course.

Late Work

Late work will result in a deduction of 10 points per day. No late work will be accepted after the third day an assignment or discussion is late.

Incompletes

The University policy on grades of "Incomplete" is that the deficiency in performance must be addressed satisfactorily by the end of the next long (16 week) semester or the grade automatically becomes a "F". Grades of "Incomplete" will only be awarded to students who have demonstrated sufficient progress to earn the opportunity to complete the course outside of the normal course duration. The award of an "Incomplete" will only be made in rare circumstances, with the concurrence of the student and the professor on what specific tasks remain and when they are due for the grade to be changed to a higher grade. The determination of the need to award an "Incomplete" is entirely up to the professor's personal judgment.

Important Dates

Students may add this course up to the last Friday of the first week of class.

Students may drop this course up to the 6th day of the class or the last drop date as specified by the University Administration.

Office Hours and/or Hours of Outside-of Class Contact

This is an online course, thus there are no set office hours. Refer to the Instructor Information section in the Blackboard course for details regarding the instructor's contact information.

University Policies

Academic Integrity

Angelo State University expects its students to maintain complete honesty and integrity in their academic pursuits. Students are responsible for understanding and complying with the university Academic Honor Code and the ASU Student Handbook.

Accommodations for Disability

The Student Life Office is the designated campus department charged with the responsibility of reviewing and authorizing requests for reasonable accommodations based on a disability, and it is the student’s responsibility to initiate such a request by contacting the Student Life Office at (325) 942-2191 or (325) 942-2126 (TDD/FAX) or by e-mail at Student.Life@angelo.edu to begin the process. The Student Life Office will establish the particular documentation requirements necessary for the various types of disabilities.

Student absence for religious holidays

A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.