Class Overview

SOF685: Digital Forensics

School of Computer Information Systems

Course Overview

Course Section:	5NAX
Class Schedule:	TUE , 6:00 PM - 10:30 PM
Quarter:	Q4, 2016
Number of Credits:	4.500 total credits
Prerequisite(s):	
Cancellation #:	

Instructor

Yohannes Abate

yabate@stratford.edu *Email*

Office Hours

Office Location

Office Phone

Phone

Course

Description

This course focuses on review of the specific manifestations of cybercrime, including hacking, viruses, and other forms of malicious software. Methods to investigate cybercrime, focuses on requirements for collection and reporting of evidence for possible use in criminal cases. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present evidence and conclusions in a court of law.

Student Learning Objectives

Upon completion of this course, the student will be able to:

• Compare various types of computer crimes and how computer forensic methodologies vary dependent upon the nature of the crime
• Analyze the role that digital evidence currently plays in criminal investigations
• Differentiate common terms associated with computer forensic examinations
• Assess the computer forensics process
• Discuss basic legal issues associated with computer forensic examinations
• Explain the role of digital crime scene technicians, digital evidence examiners, and digital investigators
• Utilize network basics of relevance to conduct computer forensic examinations
• Identify unique forensic concerns related to computer intrusion (hacker) investigations
• Differentiate the basic hardware and components of relevance to computer forensic examinations
• Develop investigative and data collection plans
• Develop a basic computer forensic reports

Textbooks and Resources

There is no required textbook for this course. All textbooks and other resources are embedded in the Moodle course.

Instructional Methods and Assignments

Delivery Mode:

Courses are delivered either hybrid or online. Hybrid courses require that students complete at least part of their learning online through the Moodle course. This may be up to 49% of the course but at a minimum 9 hours of online discussion in a term. Online courses are mainly asynchronous but some may include a required synchronous session.

Stratford University is a project centric school. As such all courses are designed to engage students in active learning through authentic projects. Projects may include case study analysis, community involvement, debates, solving significant problems, and innovative new project ideas. As a student you will be actively engaged in teams similar to real work environments. See catalog for more information.

Assignments:

Discussion - This is where you discuss and share information and opinions. This is where you learn from one another, challenge each other, and critically think about the topics and current event in the field.

Task - The task includes all the out of class activities and assignments. Tasks include curated content, resources, and a graded assignment.

Lesson - The lesson includes hands on learning experiences, instructional technology integration, and self discovery. Students work in teams on authentic, significant projects.

Details of assignments are located in Moodle.

Credits & Grading

Grading Scale

The following grading scale is used to determine a letter grade for the course associated with a point value:

Score Range	Grade	Quality Points	Description
93.0 - 100	A	4.00	Excellent

Score Range	Grade	Quality Points	Description
90.0 - 92.9	A-	3.67	
87.0 - 89.9	B+	3.33	
83.0 - 86.9	B	3.00	Average
80.0 - 82.9	B-	2.67	
77.0 - 79.9	C+	2.33	
73.0 - 76.9	C	2.00	Poor
70.0 - 72.9	C-	1.67	
67.0 - 69.9	D+	1.33	
60.0 - 66.9	D	1.00	Very Poor
Below 60.0	F	0.00	Failing
Incomplete	I	0.00	Incomplete
Withdrawal	W	0.00	Withdrawal

Course Outline

Course Outline / Lesson Plan

This is a sample pre-text

Outline

- 1

  Module 1

Topics

Task 1:

Design an investigation plan that outlines the most effective, safe, and efficient way to conduct this computer forensic investigation.Include suggested software tools that might be needed and what hardware and software you will need access to for the investigation.

In order to complete this module, you will need to complete 4 parts: 1) Resource Activities; 2) Virtual Labs; 3) Assignment; 4) Discussion Forum.

1. Complete the Resource Activities (click on each activity to access). It is important to complete these activities in order to develop the competency to complete the virtual labs and assignment.:

- Work Through Section 2, Preparing for a Forensic Investigation in LYNDA Computer Forensics
- Read Phases of a Computer Forensics Investigation Work through Learning Computer Forensics Tutorial | Forensic Workstation
- Work through Learning Computer Forensics Tutorial File Systems
- Read Computer Forensics and Investigation Methodology 8 Steps
- Watch Evidence Acquisition
- Watch Common Forms of Cybersecurity Attack

2. Virtual Lab: Perform Computer Hacking Forensics Investigator Version 8 (CHFI V8) iLabs:

Homework

Complete These Virtual Labs: Directions for accessing virtual labs is attached in the Introduction section of Moodle:

- Computer Forensics Investigative Process
- Computer Forensics lab
- Understanding Hard Disks and File Systems
- Windows Forensics

Live Session Adobe Connedt

Discussion:

Read: 6 Juicy Criminal Cases that Used Computer Forensics - http://tips4pc.com/computer_tips_and_tricks/6-juicy-criminal-cases-that-used-computer-forensics.htm

Conduct a search to find out more about the 6 Criminal cases. You will have to dig deep into the resources on the Internet and even attempt to do phone interviews with people whowere involved or affected.

- 2

Module 2

Topics

Task 2:

The company has designed and obtained patents for some important parts used by the government in a new Air Force drone. The company suspects that someone on the inside is smuggling plans for this device on USB drives and selling them to competitors. Using USBDeview and Helix, investigate the suspected computer for evidence that the computer was used for this purpose and that information was transferred to a USB drive. Determine whether the person who owns the computer was involved.

1.Complete the learning resources activities:

Examples of Steps in a Forensic Investigation based on a Case

Complete: Introduction to Computer Forensics and Investigations

-Work through Section 1:Watch Activity 2 Video

-Complete Exercise 1

-Complete the Bit of Practical Fun activity -This will necessitate downloading and using USBDeview (download at http://download.cnet.com/USBDeview/3000-2094_4-10614190.html?tag=mncol;1)and Helix (download at http://www.e-fense.com/h3-enterprise.php)These are both free but you may have to register on the site.

Work through tutorial Computer Forensics- 3 Preserving Data

Homework

Perform Computer Hacking Forensics Investigator Version 8 (CHFI V8) iLabs:

Data Acquistion and Duplication

Recovering Deleted Files and Deleted Partitions

Forensics investigation using AccessData FTK

Forensics Investigtion Usuing EnCase

Live Session

Discussion

1. Read: What are some cases solved by Computer Forensics - http://elwoodforensics.wikispaces.com/What+are+some+cases+solved+by+Computer+Forensics%3F
2. Conduct a search to find out more about the McGuire. You will have to dig deep into the resources on the Internet and even attempt to do phone interviews with people who were involved or affected.

- 3

Week 3

Topics

Task 3: The director of information technology at the company, who has just suddenly resigned and moved to an island in the West Indies, is suspected of intercepting the email of the CEO and several other key employees, and using information obtained to manipulate important research data, affecting product development. Investigate the computers to determine whether the IT director intercepted email from the computer of the CEO and CIO, and recover data he may have obtained without destroying evidence.

1. Complete the Resource Activities:

    - Watch Email tracing: Trace any email to know actual sender
    - Watch The Buildabizonline Email Tracker
    - Watch Forensic Data Recovery and File Carving

Homework

Virtual Lab: Perform Computer Hacking Forensics Investigator Version 8 (CHFI V8) iLabs:

- Steganography and Image File Forensics
- Application Password Crackers
- Log Capturing and Event Correlation
- Network Forensics, Investigating logs and investigating network traffic

Live Session

Discussion

1. Read: Computer Evidence Helps Crack Criminal Cases- http://www.usnews.com/news/world/articles/2008/02/27/calli
2. Conduct a search to find out more about the Columbian CyberCops. You will have to dig deep into the resources on the Internet and even attempt to do phone interviews with people who were involved or affected.

- 4

Week 4

Topics

Task 4:

Several researchers in R & D have noticed strange bits of code in their computers and occasional blinks on their machines when they attempt to access certain cites. They suspect that someone has hacked into the system. Carry out an investigation on the computer to determine whether it has been hacked and whether any Malware exists on the machine. Attempt to trace who initiated the breach and their footsteps.

In order to complete this module, you will need to complete 4 parts: 1) Resource Activities; 2) Virtual Labs; 3) Task; 4) Discussion Forum.

1. To complete this task work through the resources:

- Continue to work through Computer Forensics 5 Analyzing Datahttp://www.lynda.com/Developer-tutorials/Computer-Forensics-Essential-Training/170337-2.html
- Work through: Learning Computer Forensics Tutorial Dynamic Malware Analysis http://youtu.be/4RP2CHLgAeQ
- Watch LYNDA video Malware http://www.lynda.com/Help-Desk-tutorials/Malware/184174/188942-4.html
- Read Malware Analysis: https://hard2bit.wordpress.com/2013/09/16/introduction-to-malware-analysis-case-study-with-real-virus/
- Complete the tutorial http://www.lynda.com/N-Stalker-tutorials/Hackers-kill-chain/164982/187647-4.html
- Complete the tutorial http://www.lynda.com/N-Stalker-tutorials/Stuxnet-kill-chain/164982/187648-4.html

Homework

Virtual Labs: Perform Computer Hacking Forensics Investigator Version 8 (CHFI V8) iLabs:

- Investigating wireless attacks - https://eccouncil.learnondemand.net/Lab/12782
- Tracking emails and investigating email crimes - https://eccouncil.learnondemand.net/Lab/12784
- Investigative reports - https://eccouncil.learnondemand.net/Lab/12786

Live Session

Discussion

1. Read: Hall v. Great-West Case - http://www.infosecusa.com/hall-computer-forensics-employment-litigation-georgia
2. Conduct a search to find out more about Hall vs Great-West. You will have to dig deep into the resources on the Internet and even attempt to do phone interviews with people who were involved or affected.

- 5

Week 5

Topics

Task 5:

An employee who was fired two months ago is now one of the prime suspects for leaking information. The investigation so far has led back to her and her computer. Unfortunately, the computer was erased after she left and is not in the dead computer room. As the investigator you need to find out if files still exist on the computer that provide evidence of stealing of plans. This employee was a front office clerk and did not have a secret clearance for any research information.

When you have completed this investigation, put together your report on all four major components of the computer forensic investigation with a summary for the company on what you found, along with what you were able to repair.

Homework

To complete this task work through these resources:

- Watch: How to recover erased files from computer http://youtu.be/QeqJtJj8kUg
- Download Data Recovery Pro http://www.datarecoverydownload.com/
- Watch How to recover permanently deleted files without software in WINDOWS (Subtitles in English/Hindi) http://youtu.be/8zPHoAtcrRk

This is a sample post-text

Learning Resource Center (LRC)

To access electronic resources, along with information about LRC holdings, please visit http://www.stratford.edu/library

Policies & Procedures

Inclement Weather Policy

In the event of inclement weather, consult the Stratford University website at www.stratford.edu for information on University closings and delays.

Campus Security

Any person in immediate danger due to crime or emergency while on University property should contact local police immediately by dialing 911. When the emergency has subsided, the victim should also report the incident as soon as possible to the Campus Director.

University Wide Policies and Procedures

Please access the University catalog and supplemental addendum.http://www.stratford.edu/catalog for detailed information regarding all University-wide policies and procedures, including:

- Disability-related accommodations;
- Attendance policy;
- Drops and withdrawals;
- Appeals;
- Honor code;
- Academic and non-academic misconduct;
- Grade appeals process.