ITN 277
Computer Forensics II

INSTRUCTOR:

OFFICE PHONE:

E-M AIL:

LAST DAY FOR NEW REGISTRATION:

LAST DAY TO WITHDRAW WITH FULL TUITION REFUND:

LAST DAY TO WITHDRAW WITHOUT MITIGATING CIRCUMSTANCES:

TEXTBOOK: Guide to Computer Forensics and Investigations 5th Edition – ISBN: 978-1285060033

COURSE OBJECTIVES:

- At the completion of this course the student will be able to understand the processes of conducting a digital and computer forensics case from initial evidence gathering to completion
- At the completion of this course the student will be able to understand the importance of proper report writing for court accepted cases
- At the completion of this course the student will be able to understand the basics of digital investigations of cloud/SaaS based applications
- At the completion of this course the student will be able to understand the Legal, Privacy and Ethical Issues associated with computer forensic investigations
- At the completion of this course the student will be able to understand basic understanding of circumventing encrypted files within forensic cases
- At the completion of this course the student will be able to understand how to completely process a computer forensic case using AccessData's Forensic ToolKit from gathering the initial forensic image to the completion and report writing

STUDENT PARTICIPATION: Participation in the class discussions is expected by all students.

CLASS ATTENDANCE: Attendance at all class sessions is required.

EVALUATION: Factors involved in evaluation will be tests and an examination. There will be approximately four (4) tests including an examination during the course. Tests and examination will be weighted equally in calculating and average.

GRADING SCALE:

90-100	A
80-89	B
70-79	C
60-69	D
59 or below	F

MAKEUP TESTS: Makeup tests are not given. If a test is missed, the lowest test or examination grade will be used as the grade for the missed test. If more than one test is missed, the lowest test grade is zero. There is no option for dropping lowest test grade in this course.

Special Needs Students:
"Any student with special needs or circumstances should feel free to meet with me during office hours. Please contact Ms. Cindi Fisher at 797-8441 if you need to pick up your classroom accommodation forms or register with Disability Services."

"Any student who feels that he or she may need an accommodation because of a disability (learning disability, attention deficit disorder, psychological, physical, etc.) please make an appointment to see me during office hours. Please contact Ms. Cindi Fisher at 797-8441 if you need to pick up your classroom accommodation forms or register with Disability

Services."

"If you need adaptations or accommodations because of a disability (learning disability, attention deficit disorder, psychological, physical, etc.), if you have emergency medical information to share with me, or if you need special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible. My office location and hours are .... Please contact Ms. Cindi Fisher at 797-8441 if you need to pick up your classroom accommodation forms or register with Disability Services."

Honor Code: By accepting admission to Danville Community College, each student makes a commitment to understand, support, and abide by the College Academic Honesty Policy without compromise or exception. Violations of academic integrity will not be tolerated. Consequences are at the discretion of this professor. This class will be conducted in strict observance of the Academic Honesty Policy as listed in the Student Handbook.

Plagiarism and Academic Dishonesty: Students will be expected to maintain complete honesty and integrity in their academic work in this class. Acts of academic dishonesty, such as cheating, plagiarism, or inappropriately using the work of others to satisfy course requirements, will not be tolerated and may result in failure of the affected assignments and/or failure of this class.

COMPUTER USAGE POLICY

1. Computer labs are to be used only by students currently enrolled in the networking curriculum.
2. Use is limited to software licensed to Danville Community College and currently installed on each computer.
3. No food, drink, or smoking is allowed in computer labs.
4. No excessive or loud behavior is permitted.
5. Under no circumstances should PC wallpaper, screensaver, or Internet Explorer Homepage, be changed.
6. Upon arriving in class all students must sign to the networking curriculum attendance web site. Failure to do so will constitute an absence for that day.
7. Prior to leaving the classroom, each PC should be properly logged off and the chair pushed under the desk. Also remember to remove all scrap paper and personal property before leaving.
8. Students utilizing Internet resources that are not directly related to the class topic for that day will not be tolerated.

SYLLABUS

DIVISION: Arts and Sciences **REVISED:** February 2014

CURRICULA IN WHICH COURSE IS TAUGHT: Cybercrime Investigation certificate

COURSE NUMBER AND TITLE: **ITN 277 – Computer Forensics II**

CREDIT HOURS: 3-4 **HOURS/WK Lecture:** 3-4 **HOURS/WK Lab:** 0 **LEC/LAB COMB:** 3-4

I. CATALOG DESCRIPTION: ITN 277 - Develops skills in the forensic extraction of computer evidence at a logical level using a variety of operating systems and applications (i.e., e-mail) and learn techniques for recovering data from virtual memory, temporary Internet files, and intentionally hidden files. Prerequisite: ITN 276, Computer Forensics I. Credit will be given to ITN 275 or ITN 276 and ITN 277, but not all three courses.

II. RELATIONSHIP OF THE COURSE TO CURRICULA OBJECTIVES:
This course helps students understand how to collect, analyze and evaluate evidence data from various sources using a variety of software.

III. REQUIRED BACKGROUND: ENF 2 as a corequisite

IV. COURSE CONTENT:

A. Digital Forensics Analysis and Validation
   a. Determining What Data to Collect
   b. Validating Forensic Data
   c. Addressing Data-Hiding Techniques
B. Virtual Machine Forensics, Live Acquisitions, and Network Forensics
   a. VM Forensic Overview
   b. Performing Live Acquisitions
   c. Network Forensic Overview
C. E-mail and Social Media Investigations
   a. Investigating E-mail crimes and violations
   b. Understanding E-mail Servers
   c. Specialized E-mail Forensics Tools
   d. Digital Forensics in Social Media
D. Mobile Device Forensics
   a. Understanding Mobile Forensics
   b. Acquisitions Procedures for Mobile Devices
E. Cloud Forensics
   a. Overview of Cloud Computing
   b. Legal Challenges in Cloud Forensics
   c. Technical Challenges in Cloud Forensics
   d. Cloud Acquisitions and Investigation
F. Report Writing for High-Tech Investigations
   a. Understanding the Importance of Reports
   b. Guidelines for Writing Reports
   c. Generating Report Findings with Forensics Software Tools
G. Expert Testimony
   a. Preparing for Testimony
   b. Testifying in Court
   c. Preparing for a Deposition
   d. Preparing Forensics Evidence for Court
H. Ethics for the Expert Witness
   a. Applying Ethics and Codes to Expert Witnesses
   b. Organizations with codes of Ethics
I. Ethical Difficulties in Expert Testimony Cyber Investigations
   a. Basic Data Analysis
   b. Cyber Threats
   c. Information Assurance Fundamentals
J. IT Systems Components
   a. Networking Concepts

b. Policy, Legal, Ethics and Compliance

K. Security Incident, Analysis, and Response
   a. Basic Data Analysis
   b. Cyber Threats
   c. Fundamentals Security Design Principals
   d. Information Assurance Fundamentals
   e. IT System Components
   f. Networking Concepts
   g. Policy and Legal Ethics and Compliance

L. Digital Forensics
   a. Basic Scripting
   b. Information Assurance Fundamentals
   c. Intro to Cryptography
   d. IT System Components
   e. Networking Concepts
   f. Policy, Legal Ethics, and Compliance
   g. Systems Administration

M. Secure mobile technologies
   a. Cyber Defense
   b. Cyber Threats
   c. Fundamental Security Design Principles
   d. Information Assurance Fundamentals
   e. IT System Components
   f. Networking Concepts
   g. Policy Legal ethics and compliance

V. THE FOLLOWING GENERAL EDUCATION OBJECTIVES WILL BE ADDRESSED IN THIS COURSE:

- Communication
- Critical Thinking
- Cultural and Social Understanding
- Information Literacy

VI. LEARNER OUTCOMES

Upon completion of the course the students will be able to:

A. Analyze a variety of operating systems and applications for computer evidence.
B. Understand and correctly use forensic software and tools.
C. Understand the basics of network forensics and incident response.
D. Collect digital evidence on a variety of computer systems using accepted Digital Forensic processes.
E. Understand and correctly use court accepted imaging and analysis tools for security incident response.
F. Understand the Policies, Legal Ethics, and Compliance challenges to collecting and analyzing digital evidence during Cyber Investigations.
G. Understand and correctly use IT System Components, Networking Concepts, and Information Assurance Fundamentals.
H. Understand Scripting and Cryptography fundamentals in relation to Cyber Threats
I. Understand Security Design Principles
J. Understand Systems Administration
K. Understand the fundamentals of secure mobile

VII. EVALUATION

Module 1:
Students will start with a lab on verifying their digital images from the previous semester. They will use Forensic ToolKit (FTK) to verify their case has not changed since they left it in the previous semester. Students will also continue to work with cryptography as they use hashing algorithms to verify various types of data.
Students will conduct lab exercises on the discovery and analysis of email within the investigation. They will organize, view and sort various emails that are found to be of “value” within the case. During this process, students will also discover messages via Instant Messenger.
Students will also use the index and live search features of FTK in order to search for items using wordlists and keywords.

Module 2:
Students will conduct lab exercises based on social media forensics. Students will use the Afentis Forensics software to see how digital forensics can be used in the world of social media.
Students will create and use filters and rules during further investigation on their case within FTK.
Students will start working on an introductory lab to mobile forensics.

technologies and the tools utilized in mobile digital forensics.	Module 3: Students will start working with Cloud forensics by completing basics labs and examining how the following popular cloud services work: Dropbox Google Drive Microsoft OneNote iTunes Students will then learn the importance of report writing in forensic investigations and will create a full report based on their work from the FTK case. Students will also create reports throughout both ITN 276 and ITN 277 on an as needed basis for different stages of the investigative process. Module 4: This module will consist of primarily lecture based discussions surrounding the forensic investigators ethics and commitment to unbiased opinions. We will also discuss how to become an expert witness as well as furthering education in computer and digital forensics. Students will be given written and/or multiple choice examinations where lab exercises cannot be conducted in order to validate their understanding of the issue involved in digital forensics (legal, ethical, etc).