# ITN 276
# Computer Forensics I

---

**INSTRUCTOR:**

**OFFICE HONE:**

**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 basics of computer forensics, evidence collection, and processing and analysis of digital cases
- At the completion of this course the student will be able to understand the requirements for creating a forensic lab and safely processing and storing digital evidence
- At the completion of this course the student will be able to understand the different type of digital and computer forensic investigations
- 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 data analysis, scripting, cryptography and steganography in relation to the processing of digital evidence
- At the completion of this course the student will be able to understand basic digital forensic tool usage to include AccessData Forensic ToolKit and ProDiscover Basic

**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:** August 2016

**CURRICULA IN WHICH COURSE IS TAUGHT:** Cybercrime Investigation certificate

**COURSE NUMBER AND TITLE:** **ITN 276 – Computer Forensics I**

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

---

**I.** **CATALOG DESCRIPTION:** ITN 276 - Teaches computer forensic investigation techniques for collecting computer-related evidence at the physical layer from a variety of digital media (hard drives, compact flash and PDAs) and performing analysis at the file system layer.

**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

## I. IV. Course Content:

A. Understanding the Digital Forensics Profession and Investigations
   a. Digital Forensics Overview
   b. Preparing for Investigations
   c. Understanding Data Recovery
   d. Conducting an Investigation

B. The Investigator's Office and Lab
   a. Understanding Lab Accreditation
   b. Determining Requirements for Digital Forensics Lab
   c. Basic Forensics Workstation

C. Cyber Investigations
   a. Basic Data Analysis
   b. Cyber Threats
   c. Information Assurance Fundamentals
   d. IT Systems Components
   e. Networking Concepts
   f. Policy, Legal, Ethics and Compliance

D. 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

E. 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

F. Data Acquisition
   a. Understanding Storage Formats
   b. Acquisition Tools
   c. Performing Data Acquisitions

G. Processing Crime and Incident Scenes
   a. Identify and Collect Evidence
   b. Searching for Evidence
   c. Reviewing the Case

H. Working with Windows and CLI Systems
    a. Understanding File Systems
    b. Microsoft Structures
    c. Examining NTFS
    d. Understanding Whole Disk Encryption
    e. Understanding the Windows Registry
I. Current Digital Forensics Tools
    a. Evaluating Tool Needs
    b. Software Tools
    c. Hardware Tools
    d. Validating Software
J. Linux and Mac File Systems
    a. Examining Linux File Structures
    b. Understanding Mac File Structures
K. Recovering Graphics Files
    a. Recognizing a Graphics File
    b. Understanding Data Compression
    c. Locating and Recovering Graphics Files
    d. Identifying Unknown File Formats

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

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

| **VI. LEARNER OUTCOMES** | **VII. EVALUATION** |
|---|---|
| **Upon completion of the course the students will be able to:**<br>A. Collect digital evidence on a variety of computer systems using accepted Digital Forensic processes.<br>B. Understand and correctly use court accepted imaging and analysis tools for security incident response.<br>C. Understand the Policies, Legal Ethics, and Compliance challenges to collecting and analyzing digital evidence during Cyber Investigations.<br>D. Understand and correctly use IT System Components, Networking Concepts, and Information Assurance Fundamentals.<br>E. Understand Scripting and Cryptography fundamentals in relation to Cyber Threats<br>F. Understand Security Design Principles<br>G. Understand Systems Administration | Module 1:<br>Students will use ProDiscover Basic to view and collect evidence against forensically sound digital images. Using ProDiscover Basic, students will be able to learn the basic investigation procedures with an industry standard forensics tool. The student will conduct multiple labs based on “test cases”. These “test cases” will enable the student to perform basic forensic data analysis in a real life forensic scenario.<br><br>Module 2:<br>Students will use FTK Imager to create a forensically sound forensic image. Once completed, the student shall be able to display the knowledge on how to acquire, validate and preview digital evidence. Using FTK Imager, students will create, view, triage, convert and verify digital evidence. Students will also be able to export files, folders and hashes as well as detect encryption.<br><br>Module 3:<br>Students will use Registry Viewer or Registry Decoder in order to view the registry files within the Windows operating system. This will allow the student the opportunity to learn how the Windows registry hive structure functions as well as where to locate high value items. Students will create reports that contains items such as the SAM, SYSTEM and NTUSER.dat files.<br>In this module, students will also start to work with |

| | |
|---|---|
| | Forensic ToolKit (FTK). Students will use a forensically sound digital image to create a new forensic case. Students will use and learn all of the options available in FTK including the Tabs, Quickpicks, File Content Options and the Bookmark Tab. Students will also add newly discovered evidence to the forensic case that was created.<br><br>Module 4:<br>Students will continue to use FTK for labs in this module. Students will create and add bookmarks for “important” evidence items that will be used in their case. Students will examine metadata to further investigate items within the case. In this module, the students will begin to investigate images, graphics, videos and audio files that are found within the case. Students will learn how to discover hidden or deleted files. Cryptography will start to be covered in this module as students dive further into the labs. Encrypted files are present within the case and will need to be decrypted by the student. The students will also conduct labs on automatic and manual data carving.<br><br>Students will be given written and/or multiple choice examinations in order to test their skills and understanding of legal and ethical issues and dilemmas during a computer forensic investigation. |