Revised 6/2023

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 276 COMPUTER FORENSICS I (3 CR.)

Current information on NOVA's Cybersecurity Program is located at www.nvcc.edu/cybersecurity. Note that this statement must be copied onto all syllabi for this course.

Course Description

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. Lecture 3 hours per week.

General Course Purpose

This class is designed to train computer technicians in the elements of computer forensics investigation and provide skills for network support personnel in security incident response.

Course Prerequisites/Corequisites

Prerequisites: ITN 106 and ITN 107, or ITE 221.

Corequisite: ITN 260

Course Objectives

Upon completing the course, the student will be able to:

a) Discuss computer forensics as a field and career.
b) Collect digital evidence on a variety of computer systems using accepted forensic processes.
c) Correctly use court accepted imaging and analysis tools.
d) Identify the legal challenges to collecting and analyzing digital evidence.

Major Topics to be Included.

- Understanding Computer Forensics (CCR)
    - History of computer forensics
    - Computer forensics as a career
    - Professional certification and organizations

- Legal Issues in Computer Forensics (CCR, DFS, PLE)
    - Law enforcement investigations
    - corporate investigations
    - Professional ethics and conduct

- Preparing for an Investigation (DFS, PLE)
    - Forensic resources
    - Preparing a forensic toolkit

- Securing a System for Investigation (DFS, PLE)
    - Evidence Preparation.

- Employing media wiping tools.
- Employing checksums/hashing as validation
- Bit-by-bit copies

- Analyzing and Understanding File Systems (DVF, MEF)
  - FAT 32
  - exFAT
  - NTFS
  - HFS/APFS
  - EXT

- Data Acquisition at a Physical Layer (MEF, NWF)
  - Imaging a system using forensic tools
  - Using write-blockers.
  - Using court accepted tools to duplicate drives
  - Understanding drive geometry
  - Understanding file systems and disk partitioning
  - Hashing the drive

- Analyzing Data (MEF, DFS, DVF)
  - Recovering data at physical layer using court accepted forensic tool.
  - Examining DOS and Windows disk structures
  - Understanding the boot sequence
  - Examining NTFS and FAT file systems
  - NTFS Data Streams

- Examining Other Media Structures (DVF)
  - CDs
  - Thumb/flash drives

Recovering Deleted and Encrypted Data from a File System (DVF, MEF, DFS)

- Manually recovering a deleted file, directory and partition in the FAT file system
- Manually recovering data remnants from slack space in the FAT file system
- Manually recovering data remnants from unallocated space in the FAT file system
- Manually recovering file names from the directory entry table in the FAT file system
- Examining the NTFS file system
- Manually recovering deleted files in the NTF file system
- NTFS Encrypted File Systems (EFS)
- EFS Recovery Agent

Recovering Hidden Data at a Physical Layer (DFS)

- Hidden partitions
- Bit-shifting

- Data Carving (DFS, HOF)
    - Slack space
    - Free space

- Cataloging and Storing Digital Evidence (DFS)
    - Chain of custody
    - Evidence transport
    - Evidence storage
    - Evidence Locker Room

CAE2Y Knowledge Unit Domain Index

KU Category	Course Content KU Mapping	CAE2Y KU Name	Description
Core Non-Technical CDE Knowledge	PLE	Policy, Legal, Ethics, and Compliance	Provide students with and understanding of information assurance in context and the rules and guidelines that control them.
Optional Knowledge Units	CCR	Cyber Crime	Provide students with an understanding of Cyber Crimes and other abuses arising in a cyber environment.
	DFS	Digital Forensics	Provide students with the skills to apply forensics techniques throughout an investigation life cycle with a focus on complying with legal requirements.
	DVF	Device Forensics	Provide students with the ability to apply forensics techniques to investigate and analyze a device.
	HOF	Host Forensics	Provide students with the ability to apply forensics techniques to investigate and analyze a host in a network.
	MEF	Media Forensics	Provide students with the ability to apply forensics techniques to investigate and analyze a host in a

			network.

NOTE: the course content KU mapping represents the KU Domain topic as shown in the Center of Academic Excellence (CAE) KU mapping matrix (Excel file).

Required Time Allocation per Topic

To standardize the core topics of ITN 276, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best if they reflect up to date versions of the instructional tools used in this course. There are normally 45 student contact-hours per semester for a three-credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 3 = 45 hours. Sections of the course that are given in alternative formats to the standard 16-week section still meet for the same number of contact hours.) The final exam time is not included in the timetable. The changes in computer forensics are happening so fast that some of the content easily could be less significant soon. So it is really important to include the changes in the syllabus. Also, additional topic/ Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	Hours	Percentage
Understanding Computer Forensics	3	6.7%
Legal Issues in Computer Forensics	3	6.7%
Preparing for an Investigation	3	6.7%
Securing a System for Investigation	1	2.1%
Evidence Preparation	2	4.4%
Analyzing and Understanding File Systems	9	20%
Data Acquisition at the Physical Layer	3	6.7%
	3	6.7%
Analyzing Data	3	6.7%
Examining Other Media Sources	3	6.7%
Recovering Deleted and Encrypted Data from a File System	3	6.7%
Recovering Hidden Data at a Physical Layer	2	4.4%
Data Carving	2	4.4%
Cataloging and Storing Digital Evidence	2	4.4%

Testing to include quizzes, tests, and exams (not including final exam)	3	6.7%
Total	45	100%