Revised 08/2023

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 277 – COMPUTER FORENSICS II (3 CR.)

Current information on NOVA's Cybersecurity Program is located at

www.nvcc.edu/cybersecurity **Course Description**

Develops skills in the forensic extraction of computer evidence at a logical level using a variety of operating systems and applications (i.e. email) and learn techniques for recovering data from virtual memory, temporary Internet files, and intentionally hidden files. Lecture 3 hours per week.

General Course Purpose

This class is designed to train computer technicians in more advanced elements of computer forensics investigation and incident response.

Course Prerequisites/Corequisites

Prerequisite: ITN 276

Course Objectives

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

- Describe and/or demonstrate how to obtain evidence from a variety of operating systems and applications, including Linux and Windows
- List common forensics resources and tools
- Identify and correctly use tools to recover hidden images
- Demonstrate the ability to correctly use forensic software and tools in lab exercises
- Describe the basics of email forensics and identify commonly used email forensic tools
- Identify techniques associated with network forensics and commonly used network forensics tools
- Describe the basics of incident response procedures and tools

Major Topics to be Included

- Forensic resources and tools
- Data Acquisition and Analysis
- Recovering Image Files
- E-mail Investigations
- Network Forensics
- Web Forensics
- Create a written report of findings

Student Learning Outcomes

- Forensic resources and tools o Hardware.
  o Software imaging tools
  o Write blockers
  o Validation tools

- Data Acquisition and Analysis
  o Use software tools to image and validate digital evidence o Perform an analysis on Windows and DOS systems
    - Examine Windows registry data
    - Examine Windows temporary files
    - Examine Windows pagefile (virtual memory)
    - Explain the considerations for performing “live” inspections on a Windows system

- Use commonly used Windows utilities to explore the Internet

History o Perform an analysis on UNIX and Linux O/Ss

- Analyze UNIX and Linux boot processes
- Analyze the Linux Loader
- Analyze UNIX and Linux drives and partition scheme
- Analyze Unix and Linux file structure and commands

o Use court-accepted forensic tools to acquire and analyze data
o Explore encryption techniques
o Use password crackers to recover encrypted or data protected by passwords
o Find data hidden in applications

- Recovering Image Files
  - o Image File Types
  - o Use Forensic tools for viewing images
  - o Find data hidden in graphic files using steganography

- E-mail Investigations
  - o Understand email and Internet fundamentals
  - o Discover crimes involving email
  - o View and validate email headers
  - o Use Email forensic tools

- Network Forensics
  - o Describe Internet basics
  - o Describe Corporate legal considerations
    - Identify Corporate computer crimes and investigations
    - Locate Policy violations
    - Store content inspection versus network monitoring

  - o Retrieve evidence over the network
    - o Retrieve volatile data
    - o Use of network logs as evidence
      - Describe Log correlation
    - o Incorporate digital forensics into the Incident Response Plan (IRP)
    - o Track the source of an incident
      - Locate IP traceback
      - Locate ICMP traceback
      - Describe the Source Path Isolation Engine (SPIE)
    - o Identify Honeypots and Honeynets

- Analyze Web Forensics

- Create a written report of findings that includes
  - o Report summary
  - o Report outline
  - o Evidence presentation o Report dissemination
  - o Automated report generation

Optional Topics to be Included

- Examining layered images
- Imaging and investigating smart phones and other digital devices
- Conducting a Mock Trial as part evidence presentation
- Investigating social media
- Investigating video/audio

- Investigating backup and virtualized systems
- Analyzing systems for malicious software
- Analyzing and investigating Apple systems
- Cloud forensics
- Internet of Things (IoT) forensics

Required Time Allocation per Topic

In order to standardize the core topics of ITN 277 so that a course taught at one campus is equivalent to the same course taught at another campus, 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 as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 42 student-contact-hours per semester for a three credit course. (This includes 14 weeks of instruction and does not include the final exam week so 14* 3 = 42 hours. Sections of the course that are given in alternative formats from the standard 15 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	Time in Hours	Percentages
Preparing to examine a digital forensic evidence system	2	5%
Forensic resources and tools	3	7%
Data Acquisition and Analysis	6	14%
Recovering Image Files	3	7%
E-mail Investigations	6	14%
Network Forensics	9	22%
Web Forensics	2	5%
Advanced or Optional topics	3	7%
Creating a written report of findings	3	7%
Exams and Quizzes	5	12%
Total	42	100%