# Alexandria Technical and Community College

# CVNP 2655: Cyber Forensics

## A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: 2

Lab Hours/Week: 2

OJT Hours/Week: *.*

Prerequisites: None

Corequisites: None

MnTC Goals: None

This course explores security incidents and intrusions, including identifying and categorizing incidents, responding to incidents, log analysis, network traffic analysis, various tools, and creating an incident response team.

## B. COURSE EFFECTIVE DATES: 10/21/2020 - Present

## C. OUTLINE OF MAJOR CONTENT AREAS

1. Use investigative strategies to find digital information.
2. Create a security assessment review.
3. Understand computer criminal methods.
4. Deploy forensics tools to examine evidence.
5. Collect and prepare evidence for examination in the legal system.
6. Understand techniques for hiding evidence.
7. Recover data from digital systems.
8. Deploy email forensics to investigate email cases.
9. Investigate malware using digital forensics.
10. Examine Windows, Linux and Macintosh computers using forensics methods.
11. Investigate mobile devices using digital forensics methods.
12. Perform network analysis to look for information.
13. Create an incident and intrusion response plan.

## D. LEARNING OUTCOMES (General)

1. Detect and characterize various types of computer and network incidents.
2. Demonstrate a practical understanding of the analysis of artifacts left on a compromised system.
3. Demonstrate an understanding of how to effectively respond to privileged and major event incidents.
4. Demonstrate an understanding of advisories, alerts, and management briefings.
5. Demonstrate the ability to communicate incident response findings to personnel to add users and hardware to the existing operating system.

## E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

## F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

## G. SPECIAL INFORMATION

None noted