A. Course Description

Credits: 4

Prerequisites: CFS 380 Digital Evidence Analysis AND ICS 382 Computer Security

Lab Hours/ Weeks: Corequisites: None

Lecture Hours/ Week :

MnTC Goals: None

This course is designed to provide students an opportunity to practice what they have learned from the computer forensics program through a group project. The topic of the project must be approved by either the instructor or the director of the program. Each project must have a written report and an oral presentation. This course is recommended to be taken in the last semester of the program study.

B. Course Effective Dates: 08/15/2017 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. Assist either prosecution or defense in a criminal case, or can assist plaintiff or defense in a civil case, to prepare and present digital evidence.
2. Draft a technical witness statement.
3. Play appropriate roles in a criminal trial or a civil litigation or an internal affair investigation under a real or mock situation, such as a digital evidence examiner, a defendant, an expert witness, a lawyer, or a judge.
4. Present a technical witness in a court of law.
5. Support human rights organizations for protecting privacy
6. Support the department of homeland security in fighting cyber terrorism.
7. Use the industry-recognized tools to perform digital data acquisition, preservation, identification, and analysis.
8. Work on a real-world case and collect, preserve, and analyze proper digital evidence in supporting the case.
9. Work with the law enforcement in a cyberspace investigation.

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information

Note: This course is offered to the students majoring in computer forensics only.