

IS411 Cyber Investigation (formerly IS406D) – Fall 2010 Syllabus

Dr. Peter Stephenson, CISSP, CISM, FICAF
Email: pstephen@norwich.edu
AIM: nuciso

Office Address: Dewey 205
Telephone Number: 485-2007

Text/Materials:

Digital Crime and Digital Terrorism second edition. Taylor, Fritsch, Liederbach and Holt, pub Pearson, ISBN 0-13-700877-5.

1. Numerous readings will be available in pdf form on NUoodle.
2. The instructor will provide (via NUoodle) course notes, supplementary readings, web links and the course PowerPoint presentations. Frequent student visits to NUoodle are expected.

Course Description

This course is an introduction to cyber investigation. It includes elements of cyber crime, cyber warfare and cyber terrorism. The course will examine investigative techniques for cyber investigators, case studies of representative cyber crimes and cyber warfare incidents, some cyber investigation tools and expert witnessing. The course builds up to a mock trial where students act as a cyber investigation task force on a case called "Black Market Travel Agents", an actual case of 38 defendants in a massive on-line fraud case. This is a course that incorporates very heavy reading.

Prerequisite

None

Class Hours

Wednesday Evenings – 1800-2030 Dewey 106 and the Cyber Weapons Range War Room

Grading

Exams (2)	20%
On-line discussions (2)	30%
Class/Lab Participation and Attendance	25%
Mock Trial	25%
TOTAL	100%

Class Policies

Class Participation: Part of your grade will be based on your participation in the classroom and lab. Your grade will be lowered for the following situations: non-attendance, disruption of the class/lab, non-participation in lab exercises, not being prepared for class/lab, and non-participation in on-line discussions on NUoodle.

Quizzes: In preparation for most classes I will assign readings that you must know for the next class meeting. A quiz will normally take place on-line and will be shown on the syllabus.

Assignments/Projects: You are required to keep a copy of every item that you submit to me for review or grading. If the assignment does not make it to me (i.e. lost in cyberspace), you need to have a backup. You are expected to read this syllabus and to adhere the assignment dates. Late assignments will be penalized.

Academic Dishonesty: Plagiarism and cheating are serious offenses and may be punished by failure on exam, paper or project, failure in course and/or expulsion from the University. For more information refer to the "Academic Dishonesty" policy in the University Undergraduate Catalog.

Lab Access (room and software): Students will be provided access to the Cyber Weapons Range lab facility and will have access to appropriate software.

COURSE CALENDAR (Subject to change based on Dr. Stephenson’s travel schedule – students will be notified – When Dr. Stephenson is off campus, assignments will be conducted via NUoodle.)

DATE **TOPIC**

To be completed before first class: Text: Section I – provided readings

Sep 1 Intro to cyber crime, Technical aspects of cyber crime (TCP/IP as an investigative tool, network intrusions)
Text Chapter 5, 7 and 8

8 Search and Seizure, human factors
Text: Chapters 9, 10, and 11, provided reading “Getting the Whole Picture”

15 Investigation issues, Evidence management
Readings: “Electronic Crime Scene Investigation - DoJ” (NUoodle) – start on page 1 skipping all of the front matter.

22 On-line discussion (NUoodle) and on-line open book/notes quiz.
Case study 1: US v Parson (NUoodle), Case study 2: US v Shan (NUoodle)
NO CLASS TODAY

29 Lab 1: Link analysis, Lab 2: log analysis

Oct 6 Expert witnessing
Readings on NUoodle

13 Intro to the mock trial case: Black Market Travel Agents
Text: Chapter 6

20 Investigating malware
Reading: “Writing Internet Worms for Fun and Profit”

27 On-line discussion (NUoodle) and on-line open book/notes quiz/analysis:
who is “Stealth”? from the 20th’s reading.
NO CLASS TODAY

Nov 3 Cyber terrorism and review of the “Stealth” exercise
Reading: Cyber warfare case study, Estonia, on NUoodle

10 Cyber warfare – Discussion of the Estonia case study

17 Mock Trial evidence review

===== 19 – 28 Nov – Thanksgiving Break =====

Dec	1	Mock Trial Preparation
	8	Mock Trial
	15	Reading Day
Dec	16 - 21	EXAMS