

**JOLIET JUNIOR COLLEGE
DEPARTMENT OF COMPUTER INFORMATION
AND OFFICE SYSTEMS**

COURSE SYLLABUS

Course Prefix and Number	CIS 296
Course Title	Computer Forensics
Curriculum	Computer Information & Office Systems
Lecture	4
Lab	0
Credit Hours	4
Prerequisites	CIS 275, and CIS 292, or consent of department.

Catalog Description

In this course students in develop the skills required to effectively use the tools and procedures utilized in computer forensics. This includes analyzing Windows computer systems and computer networks to retrieving lost, deleted, or hidden information.

Course Objectives: See attached.

Prepared by:

Reviewed by:

Dave Buckley
Dept. of CIOS
2/06

Revised 10/10
Revised 12/09

Ram Raghuraman
Department Chairperson Date

STUDENT MATERIALS

A. Textbook:

Title: Window Forensics Analysis DVD Toolkit, 2nd Ed.

Publisher: Carvey

Author: Syngress/Elsevier

First Responders Guide to Computer Forensics – PDF file available for free download at <http://www.cert.org/forensics/> or from instructors ICampus or FTP sites

B. Other Required Materials

Flash or external hard drive strongly recommended.

Student Evaluation (Type of Grading)

A. PROJECTS

During the semester, 4 group projects will be assigned. These will be extended lab/research projects that will require you to do research in books or on the Internet to obtain information about forensic tools and techniques related to the topics we are currently covering. Each project will be worth 50 points.

B. LAB ASSIGNMENTS

During the semester, a variety of labs will be performed to demonstrate the concepts, tasks, and strategies discussed in the current chapter. Five of these lab assignments will be collected for grading. Each Lab assignment will be worth 20 points and must be turned in the day the lab is assigned.

C. EXAMS AND WHAT TYPE:

Four – 50 question Exams with Multiple Choice, True/False, and short answer questions. Tests will be presented online on ICampus and taken in class.
Each Test = 100 points

15

Final Exam/Final Projects

Steganography_0707.pdf

How Online Criminals Make Themselves Tough to Find.pdf

FORM C, PART II

OBJECTIVES

Upon Completion of the course students will:

1. Have a good understanding of the theory, requirements and laws related to computer forensic analysis and network incident response.
2. Understand the procedures required to perform computer forensic examinations.
3. Develop the skills and knowledge used to analyze Windows computers and networks for forensic evidence.
4. Understand the tools and techniques used for forensic examination of volatile and persistent information on windows systems.