

Illinois IDEA HS Course Outline

College/Division: Illinois State University/Technology

Course Title: Computer Forensics and Computer Crime

Course Designator/Number: TEC 348.04

Credit Hours: 3

Instructor Name/Originator: Klaus Schmidt

Catalog Description:

This course provides a technical and conceptual framework to respond to a swiftly evolving area of computer crime using forensic methodologies to detect such crime by applying structured investigation techniques and the application of forensic software.

Pre-requisites: None

Restrictions/Suggestions: Students should have a basic understanding of computers and networks.

Rationale: This course is will be developed for students who *are* interested in learning about electronic evidence and the computer forensics methods to investigate it. Furthermore, it is intended to help students to become more aware and feel more secure in their own use of the Internet.

Intended Audience: This course is appropriate for students who are interested in a career in information security, criminal justice, accounting, law enforcement, and federal investigations.

Student Learning Outcomes:

Upon completion of this course, students will be able to

1. Apply tools used in computer crime investigation.
2. Manage various incident response tools.
3. Differentiate between forensic approaches in a variety of Operating Systems.
4. Integrate forensic tools with analytical forensic methodologies.
5. Analyze physical networks, wireless networks, and embedded systems.
6. Evaluate the investigative process, technology and law.
7. Apply forensic science to computers and networks.
8. Synthesize and evaluate Secure Log Repository (SLR) and Network Intrusion Detection (NID).

Text(s):

Required:

Linda Volonino, Reynaldo Anzaldúa, Jana Godwin: Computer Forensics: Principles and Practices. Pearson Prentice Hall: ISBN: 0-13-154727-5.

Recommended:

Eoghan Casey: Digital Evidence and Computer Crime - Forensic Science, computers and the Internet. Second Edition. Elsevier Academic Press.

Marjie T. Britz: Computer Forensics and Cyber Crime. An Introduction. Pearson Prentice Hall: ISBN: 0-13-090758-8.

Topical/subject matter outline/Course Content:

Admissibility of Electronic Evidence

Preparing for E-Evidence Collection and Preservation

Forensic Examination of Computers and Digital and Electronic Media

Detecting Intrusions, Malware, and Fraud

Digital Evidence and Computer Crime

Terminology and History of Computer Crime Investigation

Crime, Technology and Law

The Investigative Process and Reconstruction

Digital Evidence in the Courtroom

Forensic Science and Computers

Forensic Science and Networks

Tools of Computer Crime Investigation

Ethical Hacking

Course Activities

Four major online modules will be developed in order to achieve above objectives. Each module states what activities, reading assignments, and evaluation methods will be applied

Activities for Online Module I:

1. Read pages 1 - 71 of your textbook and answer the multiple choice questions on pages 71 - 72 to prepare for the online quiz which is worth 25 points! The quiz based on the textbook will be posted on WebCT as Quiz Module 1. However, questions may or may not be similar to the ones reviewed on pages 71-72.

2. Write a 3 page paper (25 points).

Use Times New Roman, font size 12, 1 inch margins!

Choose one of the following topics:

Searching and Seizing Computers

What Motivates Hackers

Global Software Piracy

The paper should contain the following:

A clear definition of the topic you chose

Three refereed citations

A discussion of pro's and con's
Your personal opinion and views on the topic

3. Brief Research Project (25 points):

- a. Search online (or in the library) for a good explanation of the term probable cause, which is referenced in the Fourth Amendment. According to the Fourth Amendment, there can be no unreasonable search and seizures and no warrants without probable cause.
- b. Describe in one page (times New Roman, font size 12, 1 inch margins) two or three different definitions of *probable cause*. Include your own, personal interpretation of probable cause with a good example.

4. Online Discussion Forum (25 points):

- a. Post two questions to the WebCT Discussion Forum under online module. The questions could be based off of the portion of the text that you read for this module, or questions that you came across while doing your paper or research ~etc.
- b. Respond to two of the questions that have been posted by your classmates or your teacher. If a question that you would like to respond to has already been answered, you may review that response and discuss why you agree or disagree with the way the question was being answered by your peer.

Evaluation/Assessment:

Assignments as outlined for each of the four modules:

	Points	Total
Reading	25	100
Paper	25	
Research	25	
Discussion	25	
Final (online quiz)	100	100
Total		500

Grading Scale: 92-100% =A
 84- 91.9% = B
 76-83.9% =C
 68-75.9% =D
 0-67.9%=F

Bibliography/References:

Understanding and Managing Cybercrime --by Sam C. McQuade
The Art of Intrusion: The Real Stories Behind the Exploits of Hackers. Intruders & Deceivers: by Kevin D. Mitnick, William L. Simon
Real Digital Forensics: Computer Security and Incident Response by Keith J. Jones
Digital Crime and Digital Terrorism: by Robert W. Taylor

Articles (available on-line):

Computer crime at CEFORMA: a case study. Dhillon, Gurpreet; Silva, Leiser;
Backhouse, James

Cyber cops restrained by lack of cash. Horvath, John

Computer crime in the European Union. Van Buuren, Jelle

Computer crime in a borderless world. Grabosky, Peter

Electronic evidence recovery. Pilant, Lois