CJ446
The Criminalistics of Computer Forensics [Onsite]

Course Description:

This course introduces the student to system forensics investigation and response including procedures for investigating computer and cybercrimes and concepts for collecting, analyzing, recovering and preserving forensic evidence.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: CJ243 The Criminalistics of Cybercrime

Credit hours: 4

Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

Syllabus: The Criminalistics of Computer Forensics

Instructor:	_____
Office hours:	_____
Class hours:	_____

Major Instructional Areas

1. The role of computer hardware and software in computer crime investigations
2. Classification of high-tech crimes and criminality
3. Tracking and tracing of high-tech criminals
4. Investigation of online sexual predators and pedophiles
5. Application of the Fourth Amendment in investigating high-tech crime
6. Protocols for seizing digital evidence
7. Analysis of digital evidence
8. Examination of digital evidence

Course Objectives

1. Recognize the specific hardware, software, and media components of computer systems and their importance to computer forensics.
2. Identify types of digital evidence and locations where they are found.
3. Explain common e-mail-based high-tech criminal offenses and specific investigative protocols for each type of offense.
4. Identify scams and other forms of high-tech frauds, the devices used to commit these frauds, and the techniques to investigate them.
5. Examine the high-tech methods that terrorists and drug traffickers use.
6. Describe the different types of hackers and how they operate.
7. Define Internet communications protocols, Internet data routing rules and patterns, and tools and techniques used to trace Internet communications back to their source.

8. Describe practices and techniques that predatory pedophiles use for enticing children online and producing and sharing child pornography.
9. Define investigative protocols used to locate, obtain, and preserve digital evidence of online child enticement or the manufacture or sharing of child pornography.
10. Describe federal laws and constitutional rights applicable to the investigation and prosecution of high-tech crime.
11. Define procedures and legal issues regarding the distribution of digital evidence and forensic software reports to the defense during pretrial discovery.
12. Identify types of search warrants and subpoenas utilized to obtain digital evidence, subscriber records, and other evidences from high-tech sources such as Internet Service Providers (ISPs).
13. Explain protocols to document, seize, transport, and store high-tech evidence.
14. Examine digital evidence using computer forensic software.
15. Analyze digital evidence using computer forensic software.

SCANS Objectives

SCANS is an acronym for Secretary's Commission on Achieving Necessary Skills. The committee, created by the National Secretary of Labor in the early 1990s, created a list of skills and competencies that the committee feels are necessary for employees to function in a high-tech job market.

1. Complete the assignments while maintaining academic integrity and honesty.
2. Demonstrate the ability to utilize traditional and electronic library sources.
3. Identify the need for data, evaluate information, and communicate the results to others in written, graphical, and pictorial formats.
4. Juxtapose two theories, and defend one of the two.
5. Communicate ideas to justify positions.
6. Interpret and respond to written and verbal messages and other cues.
7. Locate and interpret written information.
8. Develop critical-reading skills and thinking processes.
9. Apply technology to tasks.
10. Select a technology.
11. Use computers to process information.

Course Outline

Unit	Activities
1–Computer Hardware, Software, and Operating Systems	Content Covered: *Investigating High-Tech Crime:* ○ Chapter 1, "Computer Hardware, Software, and the Internet," pp. 1-27 ○ Chapter 2, " Introduction to Operating Systems," pp. 29-49 • Writing Assignment: 1 • Research Assignment: 1 and 2 • Lab: 1
2–High-Tech Criminal Offenses and E-mail-Based Crimes	Read from *Investigating High-Tech Crime:* ○ Chapter 3, "High-Tech Criminal Offenses and E-mail-Based Crimes," pp. 51-92 • Writing Assignment: 1 • Research Assignment: 1 • Course Project: Introduction • Lab: 1
3–High-Tech Frauds	• Read from *Investigating High-Tech Crime:* ○ Chapter 4, "High-Tech Frauds," pp. 97-116 • Writing Assignment: 1 and 2 • Research Assignment: 1 • Lab: 1
4–High-Tech Vice Crimes, Hackers, and Terrorists	• Read from *Investigating High-Tech Crime:* ○ Chapter 5, "High-Tech Vice Crimes, Hackers, and Terrorists," pp. 119-142 • Writing Assignment: 1

Unit	Activities
	• Research Assignment: 1 • Lab: 1
5–Tracking and Tracing Internet Crimes	• Read from *Investigating High-Tech Crime:* ○ Chapter 6, "Tracking and Tracing Internet Crimes," pp. 147–180 • Writing Assignment: 1 and 2 • Research Assignment: 1 • Lab: 1
6–Pedophiles, Online Child Enticement, and Child Pornography	• Read from *Investigating High-Tech Crime:* ○ Chapter 7, "Pedophiles, Online Child Enticement, and Child Pornography," pp. 183–207 • Writing Assignment: 1 • Research Assignment: 1 • Research Assignment: 2
7–Legal Issues	• Read from *Investigating High-Tech Crime:* ○ Chapter 9, "Legal Issues," pp. 237–273 • Writing Assignment: 1 • Research Assignment: 1 • Lab: 1
8–Handling of Digital Evidence	• Read from *Investigating High-Tech Crime:* ○ Chapter 10, "Handling Digital Evidence," pp. 277–302 • Writing Assignment: 1 • Research Assignment: 1 • Lab: 1
9–Examination of Digital Evidence: Part 1	• Read from *Investigating High-Tech Crime:* ○ Chapter 11, "Developing a Computer Forensics Unit," pp. 305–321 • Course Project: Submission • Lab: 1

Unit	Activities

10–Examination of Digital Evidence: Part 2	• Review the material from *Investigating High-Tech Crime:*
	  ○ Chapter 10, "Handling Digital Evidence," pp. 277-302
	  ○ Chapter 11, "Developing a Computer Forensics Unit," pp. 305-321
	• Lab: 1

11–Course Review and Final Exam	• Final Exam

Instructional Methods

This course will help you understand basic concepts related to computer forensics. You will examine theoretical as well as practical aspects of computer forensics with the help of the textbook, writing assignments, exams, and research and analysis. A detailed project during the course will help you apply your understanding and perspectives on the effectiveness of the procedures for investigating computer and cybercrimes. You will also apply your understanding of the concepts to collecting, analyzing, recovering, and preserving forensic evidence.

Instructional Materials and References

Student Textbook Package

- Knetzger, Michael, and Jeremy Muraski. *Investigating High-Tech Crime. Upper Saddle River, NJ: Prentice Hall, 2008.*

- AccessData Ultimate Toolkit, Demo Version. Contains:
  - Forensic Toolkit
  - Password Recovery Toolkit
  - Distributed Network Attack
  - Registry Viewer
  - FTK Imager

Recommended Resources

A Universal Serial Bus (USB) key—512 MB or larger—to store software utilities used in labs, assignments, and other digital evidence files placed by the instructor

References

ITT Tech Virtual Library

Log on to the ITT Tech Virtual Library at http://www.library.itt-tech.edu/ to access online books, journals, and other reference resources selected to support ITT Tech curricula.

Books
You may click "Books" or use the "Search" function on the home page to find the following books:

Books> Ebrary:

- Greenfield, Robert S. and Albert J. Marcella. eds., *Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes.*

Auerbach Publishers, Incorporated, 2002.

Periodicals
You may click "Periodicals" or use the "Search" function on the home page to find the following periodicals.

Periodicals> ProQuest> ProQuest Criminal Justice Periodicals:

- "Introduction to software forensics." Robert M Slade. *Computer Security Journal. San* Francisco: Winter 2005. Vol. 21, Iss. 1; p. 21

- "Computer forensics: the new, must-have skill." Gerry Blackwell. *Canadian Lawyer.* Aurora: Jul 2005. Vol. 29, Iss. 7; p. 10

- "Cross-examining the computer forensics expert." Craig Ball. *Trial. Washington: Jul* 2004. Vol. 40, Iss. 7; p. 78

- "New Computer Forensics Tools." Tim Dees. *Law & Order. Wilmette: Jun 2004. Vol.* 52, Iss. 6; p. 24 (2 pages)

- Computer Forensics: Characteristics and Preservation of Digital Evidence

  Loren D Mercer. *FBI Law Enforcement Bulletin. Washington: Mar 2004. Vol. 73, Iss. 3; p. 28 (5 pages)*

- "Digital evidence standards." Anonymous. *Law & Order. Wilmette: Sep* 2003. Vol. 51, Iss. 9; p. 6

- "Digital tools from NIST." Peter Piazza. *Security Management. Arlington: Feb 2003.* Vol. 47, Iss. 2; p. 30 (1 page)

- "Computer Forensics: Incident Response Essentials Maria Kiriakova." *Law Enforcement News. New York: Apr 30, 2002. Vol. 28, Iss. 576; p. S4*

- "Hurdles to cyberjustice." Peter Piazza. *Security Management. Arlington: Aug 2001.* Vol. 45, Iss. 8; p. 45 (1 page)

Other References

The following resources can be found **outside** of the ITT Tech Virtual Library, whether online or in hard copy.

Web sites:

- http://www.cybercrime.gov/ (accessed on July 9, 2007)

This Web site presents an insight into topics such as "intellectual property", "computer crimes" and "electronic evidence".

- http://www.gocsi.com/ (accessed on July 9, 2007)

This Web site belongs to Computer Security Institute (CSI), which serves the needs of Information Security Professionals through membership, educational events, security surveys and awareness tools.

- http://all.net/ (accessed on July 9, 2007)

This Web site provides highly informative content on the latest advancements on Information protection.

- http://crimetime.com/ (accessed on July 9, 2007)

This Web site provides important information for private investigators.

- http://cu-digest.org/ (accessed on July 9, 2007)

The website offers Journals, newsletters and digest of debates, news, research, discussions of legal, social and other issues related to computer culture.

- http://searchsecurity.techtarget.com/ (accessed on July 9, 2007)

This Web site presents current issues, tips, news on information security.

- http://law.udayton.edu/cybercrimes (accessed on July 9, 2007)

  This Web site focuses on the legal issues cybercrime raises

- http://www.computerforensicsworld.com/ (accessed on July 9, 2007)

The Web site focuses on unique information on cyber crime laws.

- http://www.rcfl.gov/ (accessed on July 9, 2007)

This Web site of Regional Computer Forensics laboratory offers access to the premier digital forensics laboratory network in the country

- http://artofhacking.com/files/phrack/index.htm (accessed on July 9, 2007)

  An online hacker magazine that presents latest related articles

All links to Web references outside of the ITT Tech Virtual Library are always subject to change without prior notice.

Course Evaluation and Grading

Evaluation Criteria

The final grades will be based on the following categories:

CATEGORY	WEIGHT
Writing Assignments	10%
Research Assignments	15%
Course Project	25%
Labs	25%
Final Exam	25%
Total	**100%**

Grade Conversion Table

The final grades will be calculated from the percentages earned in the course, as follows:

A	90-100%	4.0
B+	85-89%	3.5
B	80-84%	3.0
C+	75-79%	2.5
C	70-74%	2.0
D+	65-69%	1.5
D	60-64%	1.0
F	<60%	0.0

(End of Syllabus)

