ITT Technical Institute

IT362

Networking Security III

Onsite Course

SYLLABUS

Credit hours: 4

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

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

Prerequisite: IT361 Networking Security II

Course Description:

This introduces system forensics investigation and response. Topics include processes and procedures for investigating computer and cyber crime and techniques in collecting, analyzing, recovering and preserving forensic evidence.

Major Instructional Areas

1. Solving business challenges with forensic investigations
2. Performing digital forensic investigations
3. Using forensic environments and tools
4. Collecting and handling evidence
5. Making forensic reports

Course Objectives

1. Identify the role of computer forensics in responding to crimes and solving business challenges.
2. Examine system forensics issues, laws, and skills.
3. Examine the purpose and structure of a digital forensics lab.
4. Examine the evidence life cycle.
5. Procure evidence in physical and virtualized environments.
6. Examine the impact of sequestration on the evidence-gathering process.
7. Collect evidence in network and e-mail environments.
8. Examine automated digital forensic analysis.
9. Report investigative findings of potential evidentiary value.
10. Examine the constraints on digital forensic investigations.

SCANS Objectives

SCANS is an acronym for Secretary's Commission on Achieving Necessary Skills. The committee, appointed by the National Secretary of Labor in 1990, created a list of skills and competencies that continue to be a valuable resource for individuals developing their careers in a high-tech job market. For more information on the SCANS objectives, visit The U.S. Department of Labor Employment and Training Administration: www.doleta.gov.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Vacca, John R., and K. Rudolph. *System Forensics, Investigation, and Response*. 1st ed. Sudbury, MA: Jones & Bartlett, 2010.	■		
Printed Student Lab Manual accompanying the textbook	■		
Additional VMs, Apps, Tools needed for the Student VM workstation to perform the labs for this course. (For both onsite and online)	■		

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

Books

Periodicals

EbscoHost

Books24X7

Hal Berghel

"Hiding data, forensics, and anti-forensics", *Communications of the ACM*, Apr2007, Vol. 50 Issue 4, (Page 15)

Richard A. Clark, et al

"CYBER WAR: The Next Threat to National Security and What to Do About It", *New York Times Book Review*, Aug2010, (Page 16)

Warren G. Kruse, et al

"Computer forensics; incident response essentials", Dec2001, Vol. 25 Issue 4

John R. Vacca
Computer and Information Security Handbook

John R. Vacca
"The essential guide to area networks", Mar2002, Vol. 26 Issue 1

Professional Associations

- American Academy of Forensic Sciences
  This Web site provides an understanding of advance science and its application to the legal system.

  http://www.aafs.org (accessed September 3, 2010)

- ADFSL-Association of Digital Forensics, Security and Law
  This Web site focuses on the academics and research of digital forensics, security, and law.

  http://www.adfsl.org/ (accessed September 3, 2010)

- DoD Cyber Crime Center
  This Web site provides an understanding about cyber investigation training courses for Department of Defense (DoD) organizations, Defense Criminal Investigative Organizations, military counterintelligence agencies, and law enforcement organizations.

  http://www.dc3.mil/dcita/dcitaAbout.php (accessed September 3, 2010)

- HTCIA: High Tech Crime Investigation Association
  This Web site explains the effect of the voluntary exchange of data, information, experience, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its members.

  http://www.htcia.org/ (accessed September 3, 2010)

Other References

- e-evidence info: The Electronic Evidence Information Center
  http://www.e-evidence.info (accessed September 3, 2010)

- FBI Laboratory: Computer Analysis and Response Team
  http://www.fbi.gov/hq/lab/org/cart.htm (accessed September 3, 2010)

- National Center for Forensic Science
  http://www.ncfs.ucf.edu (accessed September 3, 2010)

- SANS
  http://www.sans.org (accessed September 3, 2010)

- Computer Crime & Intellectual Property Section: United States Department of Justice
  http://www.justice.gov/criminal/cybercrime/ (accessed September 3, 2010)

- U.S. Immigration and Customs Enforcement
  http://www.ice.gov/partners/investigations/services/cyberbranch.htm (accessed September 3, 2010)

NOTE: All links are subject to change without prior notice.

Keywords:

- Computer forensics
- Cybercrime
- Data exposure
- Digital forensics
- Forensic investigation
- Forensics
- Sensitive data
- System forensics
- Admissibility
- Chain of custody
- Evidence
- Expert witness
- Forensic investigator competence
- Forensic investigator traits

- Hearsay
- Innocent until proven guilty
- Presumption of innocence
- Privacy laws
- Testimony

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Introduction to System Forensics	*System Forensics, Investigation, and Response:* ▪ Chapter 1 ▪ Chapter 2 ▪ Chapter 14 (Pages 270–277)	Discussion	1.1	Common Data Threats and Cybercrimes	1
			Lab	1.2	Perform a Byte-Level Computer Audit	2
			Assignment	1.3	Report Cybercrimes	2
2	System Forensics Issues	*System Forensics, Investigation, and Response:* ▪ Chapter 2 ▪ Chapter 3 Federal Rules of Evidence, http://www.law.cornell.edu/rules/fre/ (accessed September 13, 2010)	Discussion	2.1	Investigator or Expert Witness Skills and Qualifications	1
			Lab	2.2	Apply the Daubert Standard on the Workstation Domain	2
			Assignment	2.3	Examine Computer Forensics and Privacy	2
3	Forensics Labs and Software	*System Forensics, Investigation, and Response:* ▪ Chapter 3 ▪ Chapter 4 ▪ Chapter 5	Assignment	3.1	Potential Sources of Data Modification	1
			Lab	3.2	Create a Mock Forensic System Image for Analyzing Forensic Evidence	2
			Assignment	3.3	Create a Digital Forensic Software or Equipment Proposal	2
4	Evidence Life Cycle	*System Forensics, Investigation, and Response:* ▪ Chapter 7 National Institute of Justice: Forensic	Assignment	4.1	Identify Chain of Custody Roles and Requirements	1
			Lab	4.2	Uncover New Digital Evidence Using Bootable Utilities	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
		13, 2010)	Assignment	4.3	Write a Digital Evidence Procedure	2
5	Evidence Collection Basics	*System Forensics, Investigation, and Response:* ▪ Chapter 5 ▪ Chapter 6 ▪ Chapter 9	Discussion	5.1	Proper Methods for Capturing Data	1
			Lab	5.2	Automate Evidence Discovery Using Paraben's P2 Commander	2
			Assignment	5.3	Create a Data Recovery Plan	2
6	Hidden Data and Live Monitoring	*System Forensics, Investigation, and Response:* ▪ Chapter 8 ▪ Chapter 9 ▪ Chapter 12	Discussion	6.1	Steganography and Its Implications for Security	1
			Lab	6.2	Apply Steganography to Uncover Modifications to an Image File	2
			Assignment	6.3	Document a Password Recovery Procedure	2
7	Network Evidence Collection	*System Forensics, Investigation, and Response:* ▪ Chapter 10 ▪ Chapter 11 ▪ Chapter 13	Discussion	7.1	Incident Response Team Roles	1
			Lab	7.2	Monitor & Define a Baseline Definition for Network Traffic	2
			Assignment	7.3	Overcome Difficulties of Network Monitoring	2
8	Automated Analysis and Tools	*System Forensics, Investigation, and Response:* ▪ Chapter 5 ▪ Chapter 11 ▪ Chapter 12	Assignment	8.1	Identify Appropriate Analysis Tools	1
			Lab	8.2	Automate Image Evaluations and Identify Suspicious or Modified Files	2
			Assignment	8.3	Create an Analysis Tool Acquisition Proposal	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
9	Evidence Protection and Reporting	*System Forensics, Investigation, and Response:* ▪ Chapter 7 National Institute of Justice: Forensic Examination of Digital Evidence: A Guide for Law Enforcement http://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Pages 19–38) (accessed September 13, 2010)	Assignment	9.1	Provide a Testimony as an Expert Witness	1
			Lab	9.2	Craft an Evidentiary Report for a Digital Forensics Case	2
			Assignment	9.3	Document a Clear Chain of Custody	2
10	Investigation Constraints	*System Forensics, Investigation, and Response:* ▪ Chapter 3 (Page 45) ▪ Chapter 14 ▪ Chapter 15	Discussion	10.1	Implications of Anonymous and Shared Logons	1
			Lab	10.2	Perform an Incident Response Investigation for a Suspicious Login	2
			Assignment	10.3	Write an Acceptable Use Policy	2
11	Course Review and Final Examination	N/A	Project	11.1	Investigate Evidence and Create a Report of the Findings	25
			Exam	11.2	Final Exam	25

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Assignment	24%
Lab	20%
Project	25%
Discussion	6%
Exam	25%
TOTAL	**100%**

Grade Conversion

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

Grade	Percentage	Credit
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

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)