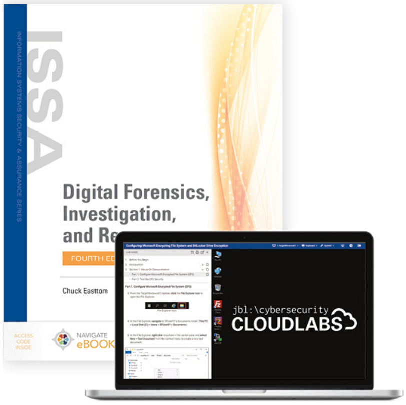
TRANSITION GUIDE


ISSA
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
Digital Forensics, Investigation, and Re
FOURTH ED
Chuck Easttom
NAVIGATE eBOOK
jbl:\cybersecurity
CLOUDLABS

Chuck Easttom

ISBN: 978-1284-22606-5
Paperback • 403 pages • © 2022

This transition guide serves to outline the updates and new content found in ***Digital Forensics, Investigation, and Response, Fourth Edition***.

GLOBAL UPDATES

- Near-total replacement of virtual labs from the second and third edition.
- Automated Lab Report functionality allows students to create Deliverables directly from the Lab Guide and download their Lab Reports as PDFs.
- Primary operating system updated to Windows Server 2019.
- Increased number of screenshots.
- Improved alignment with textbook chapters.
- Eliminated deliverable files, replacing with screenshots where applicable.
- Eliminated Assessment Worksheets and reduced Assessment Quizzes to 10 questions to simplify assessment options.

SPECIFIC LAB UPDATES

Lab 1: Applying the Daubert Standard to Forensic Evidence

- Updated evidence files.
- Reduced the number of forensic tools used in Section 1 from three to two.
- Eliminated use of Encase, added Autopsy.
- Updated Section 2 content for improved differentiation from Section 1.

Lab 2: Recognizing the Use of Steganography in Forensic Evidence

- Near total re-write of lab exercises.
- Added new steganography tools and evidence.

Lab 3: Recovering Deleted and Damaged Files

- New lab introducing tools and techniques for recovering deleted data.

Lab 4: Conducting an Incident Response Investigation

- Full re-write of original incident response lab.

Lab 5: Conducting Forensic Investigations on Windows Systems

- New lab introducing tools and techniques for performing forensic investigations in Windows.

Lab 6: Conducting Forensic Investigations on Linux Systems

- New lab introducing tools and techniques for performing forensic investigations in Linux.

Lab 7: Conducting Forensic Investigations on Email and Chat Logs

- Full re-write of original email forensics lab.

Lab 8: Conducting Forensic Investigations on Mobile Devices

- New lab introducing tools and techniques for performing forensic investigations on mobile device evidence.

Lab 9: Conducting Forensic Investigations on Network Infrastructure

- Full re-write of original packet analysis lab.
- Added a full multi-router network topology and live router / firewall forensic exercises.

Lab 10: Conducting Forensic Investigations on System Memory

- New lab introducing tools and techniques for creating and examining memory dumps.

STAY CONNECTED

Facebook:
https://www.facebook.com/jonesbartlettlearning/

Twitter:
@JBLearning

Blog:
https://blogs.jblearning.com/

Website:
jblearning.com

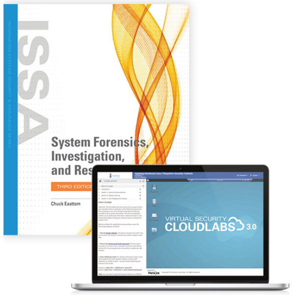
SourceCode: EAST4LABTG

JONES & BARTLETT
LEARNING
An Ascend Learning Company

Jones & Bartlett Learning | 25 Mall Road | Burlington, MA | 01803
phone: 1-800-832-0034 | fax: 978-443-8000 | **www.jblearning.com**

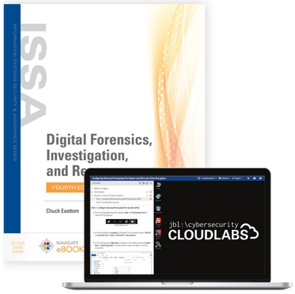
CHAPTER OUTLINE

This chapter outline has been created to help you easily transition to the fourth edition. Note that chapter content from the third edition may now be found in a different chapter in the fourth edition. Also note that chapter numbers and titles may have been updated.


ISSA
System Forensics, Investigation, and Res
THIRD EDITION
Chuck Easttom
VIRTUAL SECURITY CLOUDLABS 3.0

System Forensics, Investigation, and Response, Third Edition

By Chuck Easttom


ISSA
Digital Forensics, Investigation, and Re
FOURTH E
Chuck Easttom
NAVIGATE eBOOK
jbl:\cybersecurity CLOUDLABS

Digital Forensics, Investigation, and Response, Fourth Edition

By Chuck Easttom

Third Edition	Fourth Edition
Lab 1: Applying the Daubert Standard to Forensic Evidence	Lab 1: Applying the Daubert Standard to Forensic Evidence
Lab 2: Documenting a Workstation Configuration using Common Forensic Tools	Lab 2: Recognizing the Use of Steganography in Forensic Evidence
Lab 3: Uncovering New Digital Evidence Using Bootable Forensic Utilities	Lab 3: Recovering Deleted and Damaged Files
Lab 4: Creating a Forensic System Case File for Analyzing Forensic Evidence	Lab 4: Conducting an Incident Response Investigation
Lab 5: Analyzing Images to Identify Suspicious or Modified Files	Lab 5: Conducting Forensic Investigations on Windows Systems
Lab 6: Recognizing the Use of Steganography in Image Files	Lab 6: Conducting Forensic Investigations on Linux Systems
Lab 7: Automating E-mail Evidence Discovery Using P2 Commander	Lab 7: Conducting Forensic Investigations on Email and Chat Logs
Lab 8: Decoding an FTP Protocol Session for Forensic Evidence	Lab 8: Conducting Forensic Investigations on Mobile Devices
Lab 9: Identifying and Documenting Evidence from a Forensic Investigation	Lab 9: Conducting Forensic Investigations on Network Infrastructure
Lab 10: Conducting an Incident Response Investigation for a Suspicious Login	Lab 10: Conducting Forensic Investigations on System Memory