



COURSE DETAILS

INTENDED AUDIENCE

Current & Prospective CSIRT Managers and Members; other technical staff involved with incident handling or computer forensics activities, including law enforcement investigators.

LENGTH

Five Days; Days 1-4 (0900-1700), Day 5 (0900-1500)

COST

\$2749 including course notebook, courseware CD., and exercise materials. Lab Fee of \$250 includes student use of all PC and software required for the class. Refreshments and catered lunch provided.

PREREQUISITES

It is recommended that attendees have a moderate understanding of computers and networking.

This course may also be offered by arrangement at customer sites. Contact Outbreak Security for further information.

Outbreak Security

7 West Queens Way
Hampton, VA 23669 USA
1.757.265.0891

www.outbreaksecurity.com

INTRODUCTION TO NETWORK FORENSICS

Overview:

This five day course will present the InfoSecure CEA Forensic Methodology(tm) for a complete forensic investigation. Designed around real-life scenarios, this course will provide participants with practical techniques and hands-on experience in conducting and completing a forensics investigation.

Beginning with the necessary background in computer architecture and information storage and continuing with a complete implementation of the InfoSecure CEA Forensic Methodology for seizure, collection, examination and analysis of forensic data, this course gives attendees the knowledge required to become a skilled forensics examiner.

Topics Include:

- Overview of computer forensics
- Search and Seizure techniques
- Artifact analysis and tools
- Chain of custody
- All-Source data collection
- Forensic tool selection
- Creation of a forensic toolkit

This course includes significant hands-on exercise where attendees will be introduced to forensic software tools and techniques and asked to conduct a complete computer forensics investigation according to the InfoSecure CEA Forensic Methodology.

Objectives

At the conclusion of this course, participants should understand computer forensics, be familiar with the tools, techniques and best practices for conducting a computer forensic examination, know how to conduct a forensic examination using the InfoSecure CEA Forensic Methodology, and will have up to 15 hours of practical experience during the course to use conduct a complete forensic examination and analysis.

About Outbreak:

Outbreak Security was established in 2007 by four distinguished information security professionals whose operational and executive information security and incident handling experience in the government, military, and private sector dates back to 1988 and the birth of the incident response community. Outbreak's instructors are also Visiting Scientists at the Software Engineering Institute at Carnegie Mellon University and have taught numerous incident handling courses there for the CERT/CC.

Instructor biographies and corporate information may be found at www.outbreaksecurity.com.