

NETWORK INVESTIGATIONS TRACK

IT220, Counterintelligence in Cyber Space Phase 1 (CICS1)

Who Should Attend

DoD Counterintelligence personnel.

Prerequisites

TT110 (INCH) and RT120 (CIRC) or Test Outs
JCITA CI Fundamentals Course (or respective agency CI Training equivalent)

Duration

10 Days

Course Description

Provides Department of Defense Counterintelligence (CI) personnel with the fundamentals for conducting basic cyber CI investigations. CICS builds upon the curriculum of CIRC and provides students with a working knowledge of online investigations, mobile and cell-phone acquisition and electronic media triage.

Objective

- Conduct a rapid evaluation of electronic devices likely to contain data of interest to the investigator
- Preserve, image, and analyze data stored on portable electronic devices
- Use the internet as an investigative tool while maintaining anonymity
- Define counterintelligence indicators on IT systems
- Explain the Cyber counter intelligence methodology
- Conduct a basic forensic examination limited in time and scope
- Design technical, IT-based questions for interviews.
- Identify new and emerging technologies likely to impact the CI mission.

Topics Covered

Cyber CI Environment

- Introduction to and Methodology of Cyber Counter Intelligence Investigations

Online Environment

- Investigative Preparation, Fundamentals and Anonymous Internet Connectivity

Internet Clients and Services

- Investigating Web Pages, E-mail, Usenet, Internet Messaging, Internet Chat, Web Forums and Online Communities
- VoIP Considerations

Investigating Internet File Sharing Clients and Services

- FTP and Peer-to-Peer

Online Investigative Analysis

- Artifact Analysis
- Subject Identification

Cyber CI Triage

- Triage of Electronic Information
- Pod Slurping
- Introduction to FTK Imager

NETWORK INVESTIGATIONS TRACK

EnCase Fundamentals

- Introduction to EnCase and its Graphical User Interface
- Beginning a Case in EnCase
- Bookmarking

Rudimental Forensic Analysis

- File Identification
- Using Hash Sets
- Keyword Searching and Data Extraction
- E-mail and Newsgroups
- Web Related Evidence

Alternative Devices and Technology Concerns

- Cellular Phones, PDAs, iPhone
- GPS Navigation Devices
- Digital Media Players and Cameras
- Steganography
- Encryption and Encrypted Volumes
- Wireless Hardware and Discovering Wireless Access Points
- Key Loggers
- Fundamentals of Log Analysis

Cyber Interview Techniques

- IT Interviews, Ad hoc Interviews and Questions

Preparation

To prepare for this course, we recommend the following review, reading, or research:

- Review the *Introduction to Networks and Computer Hardware* (INCH) course book, paying special attention to:
 - Hardware
 - Windows 2003 Server
 - Basic Linux functions such as mounting and logical file structure
 - Working from a command prompt
- Review the *Computer Incident Responders Course* (CIRC) book, paying special attention to:
 - Network topology
 - Command line use
 - Intrusion methodology
 - Microsoft Windows and Linux operating system basics

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (<https://www.dcita.edu>), the internet, at Books 24/7, in your organization's technical library or at the public library. Instructions for D-Prep on the dcita.edu portal: log in. Under Online Courses, select DPrep Training; Course Name (INCH/CIRC); Sort by Name Ascending.

CICS Grading Policy

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as final Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.