

RESPONDERS TRACK

RT-220, DE-Introduction to Cyber Investigations (DE-ICI)

Who Should Attend

DCIO federal and military investigators that are new to cyber crime, federal and military computer forensic examiners, or support personnel that directly support cyber investigations

Prerequisites

None

Duration

40 Hours / 5 Weeks

Course Description

Presents the processes, techniques, specialized documentation, legal guidelines and requirements for conducting a basic cyber crime investigation through the use of lecture, practical exercises, scenarios and case studies.

Please note: This course does not provide the depth needed to conduct an advanced cyber crime investigation (i.e., Intrusions).

Objectives

- Define cyber crime
- Explain the scope and nature of cyber crime
- Explain the technical fundamentals of cyber investigations
- Explain the legal fundamentals of cyber investigations
- Collect evidence in cyber investigations
- Explain the role of computer forensic laboratories in a cyber investigation
- Describe the guidelines and requirements that must be met to fulfill the role of case agent during basic cyber crime investigations

Topics Covered

Introduction to Cyber Investigations

Technical Fundamentals

- IP Addresses
- Uniform Resource Locators
- Metadata and Logs
- E-Mail and Newsgroups
- Browser Evidence

Legal Fundamentals

- Authority to Search, Gather Records and Intercept Communications
- Prosecution of Cyber Crime

Special Aspects of Cyber Case Management

- On-Scene and Online Evidence Collection
- Cyber Forensic Laboratory Support
- Cyber Interviews
- Covert Online Investigations

Subjects of Cyber Investigations

- Motivations for Cyber Crime
- Military, Corporate and International Subjects

RESPONDERS TRACK

Preparation

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

- Review the Introduction to Networks and Computer Hardware (INCH) and Computer Incident Responders Course (CIRC) course books
- CCIPS Web site (<http://www.usdoj.gov/criminal/cybercrime/>)

INCH/CIRC topics can also be found on the dcita.edu portal (<https://www.dcita.edu>). 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.

DE-ICI Grading Policy

The minimum passing score on all Knowledge and Performance Tests is 70%. If a student fails the final Knowledge or Performance Exam, a re-test will not be given and the student fails the course.

In the DE-ICI course, the student's progress will be monitored through instructor observation of student participation in assignments, practical exercises and Knowledge Tests.