

RESPONDERS TRACK

RT120, Computer Incident Responders Course (CIRC)

Who Should Attend

DCIO Federal and CI investigators and prospective lab examiners.

Prerequisites

TT110 (INCH) or Test Out

Duration

10 Days

Course Description

In this First Response course, students learn how to seize and preserve digital evidence. They get extensive practice imaging hard disks, USB drives, and other media using a variety of methods and tools, including EnCase, FTK Imager, dc3dd, and hardware write-blocking devices. Using several operating systems, students learn to find and extract volatile information of evidentiary value, such as log files, user information, and access rights. They also learn what user information may reside only on network servers, such as user profile and e-mail content, and how to acquire it. Networking sections emphasize network topology so that students understand which log files contain potential evidence and where to find them. In addition, students get extensive practice collecting images in a network environment.

Objectives

- Demonstrate first responder basics of Microsoft Windows, Linux, and Sun Solaris network environments
- Explain incident response preparation
- Practice evidence collection for first responders to a network incident

Topics Covered

Evidence Handling

- Learn basic first response evidence collection and preservation techniques for different network operating systems
- Learn the necessary preparatory actions for responding to a home computer environment or a network incident
- Learn tools and system commands for first response evidence collection in Sun Solaris, Fedora Linux, and Windows operating systems
- Volatile information
- Imaging

Network Protocols

- Know what function different network protocols provide
- Identify the OSI Model, its seven layers and how they relate to network evidence
- Know the TCP/IP protocol stack and the functions of its protocols

Routers and Firewalls

- Know the main functions of a router and firewall and identify what type of information can be gathered on-site
- Understand what routers and firewalls are and how they work
- Identify what information can be secured from a router or firewall to help in a network investigation

Network Sniffers and IDS

- Know the main functions of a sniffer or intrusion detection system and identify what type of information can be gathered on-site
- Understand what sniffers and intrusion detection systems are and how they work
- Identify how sniffers are used by both hackers and investigators
- Learn how investigators use intrusion detection systems

RESPONDERS TRACK

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) course book, paying special attention to:
 - Hard Disk Drives
 - Operating Systems
 - Windows XP Command Line
 - Basic networks, Network Connectivity, Configuration (including ports), Protocols and Devices
 - IP Addresses, Subnets, Network Security
 - Linux – Definition and Commands
 - Working from a command prompt

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; Sort by Name Ascending.

CIRC Grading Policy

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