

## NETWORK INVESTIGATIONS TRACK

### IT290, Online Undercover Techniques (OUT)

#### **Who Should Attend**

DCIO and CI investigators and prospective lab examiners.

#### **Prerequisites**

NONE

#### **Duration**

5 Days

#### **Basic Knowledge Needed**

- Computer hardware and networking
- Undercover investigations training and experience
- Advanced internet skills highly recommended
- Prior undercover investigations training preferred

#### **Course Description**

Focuses on techniques used to conduct the online component of undercover investigations. Topics include how to prepare a workstation for undercover activity; how to use FTP, IRC, and peer-to-peer servers and other internet technology to identify and monitor the target; and how to collect and preserve evidence. {Mobile}

#### **Objectives**

- Explain online communication methods and their roles in investigations.
- Explain online information and evidence and how to preserve it
- Identify key legal concepts of conducting on-line undercover investigations
- Gather detailed information about a subject using internet based public records
- Gather and preserve web related artifacts
- Conduct internet based investigations employing methods of anonymity
- Describe online social communities
- Explain protocols used to transfer information across the internet.

#### **Topics Covered**

##### *Legal Guidelines*

- Legal Authorities
- Electronic Communications Privacy Act (ECPA), the Privacy Protection Act (PPA) and the Foreign Intelligence Surveillance Act (FISA)
- Define the terms Entrapment and the Lack of Predisposition

##### *Preparation for Investigation*

- Backstopping
- Internet Fundamentals, Internet Service Providers, IP Addresses and the Domain Name System

## NETWORK INVESTIGATIONS TRACK

- Preparing Your Workstation, including the preparation process, system Protection and Live CDs
- Anonymous Internet Connectivity through Public Access Points, Anonymous Internet Service Providers and Web Proxies
- Tool Analysis and Sanitizing the Test Environment
- Filtering Network Traffic and Performing Analysis

### *Investigating Internet Clients and Services*

- Investigating Web Pages, Email, Usenet and Internet Messaging (IM), Internet Chat, Web Forums, and Online Communities
- Voice over Internet Protocol (VoIP) Considerations

### *Investigating Internet File Sharing*

- File Transfer Protocol (FTP), Secure FTP and FTP Variations
- Peer-to-Peer File Sharing and Architecture, Multi-Protocol Clients, Darknets and Commonly Used Ports

### *Investigative Analysis*

- Artifact Analysis – Graphic Images, Audio and Multimedia Files, and Steganography
- Subject Identification – General Searches and Public Records

### **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:
  - Operating Systems, specifically MS Windows Operating Systems Basics
  - Windows XP Command Line
  - Windows 7, Internet Explorer 8
- Advanced Internet Skills are highly recommended for this course.

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.

### **OUT Grading Policy**

Student 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%.