

## NETWORK INVESTIGATIONS TRACK

### NIT280, Cyber Analyst Course (CAC)

#### **Who Should Attend**

Traditional Analysts that will function as Cyber Analysts.

#### **Prerequisites**

TT110 (INCH) or Test Out

#### **Duration**

10 Days

#### **Course Description**

Provides the Cyber Analyst with the necessary skills to understand technical reports and their relevance, conduct research in order to create a comprehensive report and link analysis. Students will learn how to identify network intrusion and electronic artifacts. Course also provides instruction on how to analyze cyber information in order to create a comprehensive report and link analysis of related cyber cases.

#### **Objective**

- Explain the differences between traditional vs. cyber analyst roles
- Explain how network intrusions occur
- Explain how various logs are created
- Define electronic evidence
- Explain how electronic artifacts are forensically gathered
- Use the Internet as an information gathering tool while maintaining anonymity
- Analyze data contained in text logs
- Analyze data contained in reports to produce a comprehensive report and link analysis

#### **Topics Covered**

##### *Introduction to Cyber Analysis*

- Introduction to Cyber Analysis (includes case studies)
- Electronic Artifacts Primer

##### *Introduction to Cyber Analysis*

- Traditional Analyst versus Cyber Analyst
- Priority of Information in Cyber Analysis
- Resources for the Cyber Analyst
- Working with Other Agencies

##### *Applying Analysis Tools to Cyber*

- Types of Analysis Reports
- Introduction to i2 Analyst's Notebook 8

##### *Network Architecture and Information Assurance*

- Network Architecture Basics
- Introduction to Wireshark
- Network Protocol Analysis
- Application Protocol Analysis

# NETWORK INVESTIGATIONS TRACK

## *Identifying an Intrusion*

- Computer Intrusions
- Reconnaissance
- Attacks
- Entrenchment
- Abuse

## *System Analysis*

- The Windows Operating System
- Fundamentals of Windows Artifact Analysis
- Analyzing First Responder Data
- System Log Analysis

## *Network Device Analysis*

- Fundamentals of Network Artifact Analysis
- Network Device Artifact Analysis
- Network Traffic Capture Analysis

## **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
  - Have a fundamental understanding of network topologies

## **CAC 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%.