

# Basic Computer Networking and Internet Topics for First Responders

**DATE and TIME:** Tuesday, August 24, 2010—8:00 a.m. until 4:00 p.m.

**LOCATION:** Western Illinois Police Training Unit, 1801 Windish Drive, Galesburg

**INSTRUCTOR:** John Briscoe, Sergeant,

## **Purpose of Course:**

This course is designed to introduce officers to the investigative value associated with networks and the Internet. Officers will obtain the basic knowledge and skills to recognize networking and Internet topics for law enforcement personnel. Areas addressed in this course include the networking hardware, software, ethics, and network examination standards. Special emphasis will be given to computer network investigations as it pertains to cyber crime, terrorists and the Internet. The course will also address legal principles regarding computer crimes, digital investigative units. Future computer investigations and cyber terrorism are addressed in this course including: “Cloud Computing”, “Data Centers”, “NGI-New Generation Internet”, “Intranet & VOIP”, “Convergence Technology”, and “Private Security Objectives & Law Enforcement”. This eight-hour program has been designed by Sergeant John Briscoe.

## **Course Overview:**

The primary focus of the course will be to provide law enforcement officers with the specialized skills, knowledge and abilities needed to collect and submit electronic evidence for analysis. Officers will be instructed on the identification and preservation of electronic crime scene evidence.

## **Course Goals:**

1) Describe the different cyber crime situations where computer forensic investigation would be appropriate in a network environment. Describe basic network configuration.

**CONTINUED ON PAGE 2**

## **Basic Computer Networking and Internet Topics for First Responders**

### **Page 2**

- 2) Describe types of evidence investigator may encounter with computer networks and the Internet. Describe network data, discuss how large amounts of data are usually broken down into small packets and transferred over a network environment. (I.P. tracking, firewalls, virus protection, etc.)
- 3) Describe software (Neo Trace, Net Tumbler, etc.) and forensic ethical standards, as well as legal and privacy issues.
- 4) Describe and demonstrate how to identify, investigate, capture, analyze, preserve, and process computer network evidence.
- 5) Demonstrate the use of proven investigative and examination strategies. Follow guidelines from the National Institute of Justice, RCFL and Secret Service.
- 6) Describe the need to only use specialists and networking professionals in the collection of network related evidence.
- 7) Describe and demonstrate acquisition, collection, seizure, and safekeeping of storage media and how it relates to chain of custody requirements. On site enforcement activities with "E-Kit Field Collection Materials".
- 8) Describe law enforcement assistance available to first responders with networking or cyber criminals: Secret Service Electronics Crimes Task Forces; Metropolitan Federal Identity Theft Task Force; High Tech Criminal Investigators Association; F.B.I. Cart Response Unit and National Security Administration.
- 9) Utilize common forensic tools in the electronic discovery process with subpoenas, search warrant, and consent to search. Describe the "chain of custody" as it relates to the proper collection and documentation of networking evidence.
- 10) A special emphasis will be placed on the legal and civil liability associated with private business. Officers should always seek legal assistance from their States Attorney's Office with Law Enforcement activities. This is also true for Federal Agents who should seek out assistance from the U.S. Attorneys Office.

### **Registration:**

Contact Western Illinois Police Training Unit at 309-344-3366; fax 309-344-5215; e-mail [wiptu@gallatinriver.net](mailto:wiptu@gallatinriver.net) or online [www.wiptu.org](http://www.wiptu.org).