

## Protocol Analyzers: Sniffer, EtherPeek, Ethereal

This course describes the key functions that make these analyzers some of the hottest products around. It also takes students through triggered sessions, alarms/alerts, basic and advanced filters. Participants will be up and running in no time using many of the techniques that Laura uses during her onsite analysis sessions.

### Recommended Pre-Requisites

- Introduction to Network Analysis

### Included Course Materials

- High-quality audio and visual training modules
- Presentation slides and handouts

### Duration

- Self-paced study
- Seven modules totaling 4 hrs, 30 min

### Participants Learn About

- Ethereal: The Ultimate Free Protocol Analyzer (Part 1 & 2)
- EtherPeek: Advanced Filtering (Patterns and Boolean Operands)
- Sniffer/EtherPeek: Triggers, Alarms and Notifications
- Sniffer: Address Filters
- Sniffer Network Analyzer: Advanced Filters
- Importing and Exporting Sniffer Filters

### Other Suggested Training

- Advanced Network Analysis

### Complete Master Library Information:

Web site: [www.packet-level.com/library/](http://www.packet-level.com/library/)

E-mail: [library@packet-level.com](mailto:library@packet-level.com)



## Detailed Course Outline

### **Ethereal: The Ultimate Free Protocol Analyzer (Part 1)**

This course starts with the installation and placement details of Ethereal, a free protocol analyzer that is distributed under the GNU public license. With over 100 contributors, this tool is maturing into a fantastic analyzer solution for folks on a budget. Laura then covers the packet capture process, how unique Ethereal's packet display window is, and how students can build and apply temporary filters to focus in on network problems.

This module is a 'must attend' for anyone who wants to deploy Ethereal as a no-cost solution to local or remote packet capturing.

### **Ethereal: The Ultimate Free Protocol Analyzer (Part 2)**

Part 2 of this module allows students to spend time working with Ethereal's capture and display filtering system – working with the TCPDUMP expression set and a variety of Boolean operands used in advanced filters. Participants learn how to perform TCP stream analysis and review TCP throughput and roundtrip time (RTT) values.

This unit is a 'must attend' for anyone who wants to deploy Ethereal as a no-cost solution to local or remote packet capturing.

### **EtherPeek: Advanced Filtering (Patterns and Boolean Operands)**

Advanced filters enable analysts to capture or display packets, based on specific values at specific offsets. Laura provides numerous examples of advanced filters built on hex decimal and ASCII strings. In addition, she covers the use of the key Boolean operands OR, AND and NOT.

### **Sniffer/EtherPeek: Triggers, Alarms and Notifications**

Capturing traffic in the middle of the night doesn't require an analyst's presence any more. Using triggers, they can set up their analyzers to begin capturing when a specific event occurs or at a specific time. Analysts can also configure many types of stop triggers (event based, time based, packet count based). The alarms and notifications let them know what's happened when they're off doing other tasks on the network. Laura teaches how to set up these captures. (This is a repeat of the Unattended Captures: Triggered Starts/Stops course)

### **Sniffer: Address Filters**

From MAC address filters to IP address filters to variable length subnet filters - this unit covers the gamut of options available for filtering on specific addresses. Laura makes recommendations for when to use MAC filters rather than protocol filters and she demonstrates how and the reasons to use the 'Exclude' option when gathering traces on the network.

### **Sniffer Network Analyzer: Advanced Filters**

Get to the nitty gritty of pattern based filtering. Capture traffic based on specific values located at specific offsets within the packets. Laura provides numerous examples of advanced filters built on hex, and ASCII strings. In addition, she covers the use of the key Boolean operands OR, AND and NOT.

### **Importing and Exporting Sniffer Filters**

There are numerous filters available online in the [www.packet-level.com](http://www.packet-level.com) library section.

How did Laura export these filters? How can analysts import them into Sniffer? This course provides students with step-by-step instructions on how to import a single or entire set of filters into Sniffer.