



Self-Paced Courseware

Performing Network and Security Analysis with Ethereal™

Laura Chappell, Sr. Protocol/Security Analyst, Protocol Analysis Institute, LLC

Watch narrated and animated moving screen captures as Laura shows you step-by-step how to capture troubling network traffic, interpret those traces and build graphical reports to explain the problems found. Follow along with the analysis process by using the included trace files.

- ✍ Create and interpret throughput, roundtrip latency, and TCP sequence number graphs that provide a graphical answer to troubling network traffic.
- ✍ Use Ethereal's Expert to spot the cause of slow file transfers.
- ✍ Create Capture Filters to perform application analysis and baselines.
- ✍ Use the Flow graphs to separate and analyze one-to-many communications on the network.
- ✍ Work with the time value settings in Ethereal to identify the cause of "The Network is Slow" problem.
- ✍ Customize Ethereal to make the most of your analysis sessions.
- ✍ Set up protocol forcing to re-interpret suspicious communications.
- ✍ Work through several case studies and test your knowledge of interpretation and analysis of suspicious and performance-impairing traffic.

Course Outline

- Session 1: Basics of TCP/IP Communications
- Session 2: Install and Customize Ethereal
- Session 3: Place Ethereal on Your Network
- Session 4: Capture Filters – Isolate Traffic Off the Wire
- Session 5: Display Filters – Build Advanced Filters
- Session 6: Charts and Graphs – Throughput, Roundtrip, TCP Sequences
- Session 7: Use Ethereal's Expert System and TCP SEQ/ACK Analysis and Analyze TCP Window Issues
- Session 8: Advanced Protocol Settings
- Session 9: Build an Effective Analysis Report
- Session 10: Case Studies – Test Your Analysis Skills

Course Pricing and Details

Purchase online at www.podbooks.com.

Pricing: US \$249.00

Included Materials

This course contains ten (10) narrated, audio/video training sessions with related trace files for self-study (one DVD).

Duration

26 mins	Session 1: Basics of TCP/IP Communications
35 mins	Session 2: Install and Customize Ethereal
22 mins	Session 3: Place Ethereal on Your Network
30 mins	Session 4: Capture Filters – Isolate Traffic Off the Wire
27 mins	Session 5: Display Filters – Build Advanced Filters
21 mins	Session 6: Charts and Graphs – Throughput, Roundtrip, TCP Sequences
43 mins	Session 7: Use Ethereal's Expert System and TCP SEQ/ACK Analysis and Analyze TCP Window Issues
13 mins	Session 8: Advanced Protocol Settings
34 mins	Session 9: Build an Effective Analysis Report
31 mins	Session 10: Case Studies – Test Your Analysis Skills

Detailed Course Outline

Session 1: Basics of TCP/IP Communications

This first session covers “must know” prerequisite knowledge for any protocol analyst. How does the application define a port number to use for the communication? What are the three steps involved in the name resolution process? How does a host learn whether the target is local or remote based on addressing rules? What are the key processes in route resolution? How does a host locate the MAC address of a target? Given a sample network design and application, can you define each packet that should be seen on the wire? What if the default gateway is not the best way to go to get to the target? What if the DNS server is on a remote network? This first course is highly recommended for anyone working on TCP/IP networks.

Session 2: Install and Customize Ethereal

This session discusses the installation procedures for Ethereal (Windows and Linux) and dependencies on Winpcap in the Windows environment. Students learn to customize Ethereal’s user interface, layout, summary columns, fonts and colors, capture settings, name resolution processes and protocol settings. Some of the key configurations are used to count cumulative bytes transferred in a trace file and streamline Ethereal for high-traffic networks.

Session 3: Place Ethereal on Your Network

Since most networks today are switched, a protocol analyzer can only hear four types of traffic: broadcast, multicast, unknown destination MAC traffic and traffic to and from the analyzer system itself. This limits your ability to listen in on a host’s problematic communications. In this session you learn the tricks of hubbing out and port mirroring/spanning when necessary. Which is the most effective way of determining the cause of problems and how do you ‘trace back’ to pinpoint problem areas.

Session 4: Capture Filters – Isolate Traffic Off the Wire

Demonstrating tcpdump filters, this session shows how to filters to isolate the traffic captured off the wire based on host address, host name, gateway usage and MAC address. In addition, this session introduces negative and Boolean operands to the capture filter process. Finally, you’ll get a chance to test your filter making abilities with a test.

Session 5: Display Filters – Build Advanced Filters

Display filters enable you to apply granular rules to captured traffic to isolate or remove specific traffic from the trace file viewer. Using several short-cuts and graph views you can easily isolate a specific conversation in the trace file or hide it from view. This is important when drilling down through a trace file to find the unusual conversations. Boolean operands add greater capabilities to isolate specific traffic.

Session 6: Charts and Graphs – Throughput, Roundtrip, TCP Sequences

One of the exciting additions to Ethereal is the enhancement to the charting and graphing capabilities. In this session you examine input/output (IO) graphs and plot comparative IO rates in color-coded graphs. In addition, this session examines and contrasts conversation and endpoint charts and explains how to correlate information displayed in throughput graphs with roundtrip time graphs and TCP sequence graphs. You also learn how to use Ethereal's HTTP graphs (load distribution, packet counter and requests) to identify web browsing faults and security concerns. Finally you learn to build and interpret flow graphs to depict one-to-one and one-to-many communication patterns.

Session 7: Use Ethereal's Expert System and TCP SEQ/ACK Analysis

As Ethereal matures, its Expert System continues to evolve to point out problems or anomalies in network communication. In this session you examine Expert analysis information Ethereal's TCP SEQ/ACK analysis that helps spot lost packets and retransmissions on the wire. Learn to use the TCP SEQ/ACK analysis feature to learn whether a client, server or network path is at fault in problematic network communications. In addition, Laura added a section covering the TCP window size negotiation and fault isolation process.

Session 8: Advanced Protocol Settings

There are times when altering the way Ethereal handles specific protocols can make the process of trace file interpretation much easier. In this session you learn to change Ethereal's method of interpreting these communications and perform protocol forcing to completely change the decoded protocol to identify suspicious behavior on the network.

Session 9: Build an Effective Analysis Report

Show management or a customer what you found by building a clear, concise and graphical report of your findings. Learn the key components to include in your report and the add-on tools and exporting functions that can support your findings.

Session 10: Case Studies – Test Your Analysis Skills

Now test your own skills at isolating problems on the network and classifying traffic. In this session Laura presents a series of trace files with some general network information. Use your analysis skills to explain what is going on in the trace files and create the desired charts, graphs and filters to support your findings.