



## WSU02 [Self-Paced Course] TCP/IP Network Analysis



### Course Format

This course is available only in self-paced format (voice-over-video) taught by **Laura Chappell**. The course DVD includes videos, supplemental files (in PDF format) and reference/resource materials for the network analyst.

### Course Content

This course focuses on both the normal and abnormal communication patterns of the TCP/IP suite and most common applications including DHCP, DNS, FTP, Telnet, HTTP, POP and SMTP.

#### Course Overview - Introduction

##### Section 1: TCP/IP Functionality Overview

- a) Resources and References for Analysts
- b) Capture on Hubbed, Switched and Routed Networks
- c) The TCP/IP Resolution Process
- d) Packets Going the Wrong Way
- e) Faults in the Resolution Process
- f) Test Yourself: What If...

##### Section 2: Analyze DNS Traffic

- a) Understand DNS Packet Structure
- b) Filter on DNS Traffic
- c) Analyze Normal DNS Traffic
- d) Analyze Unusual DNS Traffic

##### Section 3: Analyze ARP Traffic

- a) Understand ARP Packet Structure
- b) Filter on ARP Traffic
- c) Analyze Normal ARP Traffic
- d) Analyze Unusual ARP Traffic

##### Section 4: Analyze IPv4 Traffic

- a) Understand IPv4 Packet Structure
- b) Filter on IPv4 Traffic
- c) Analyze Normal IPv4 Traffic
- d) Analyze Unusual IPv4 Traffic



- Section 5: Analyze ICMP Traffic
- a) Understand ICMP Packet Structure
  - b) Filter on ICMP Traffic
  - c) Analyze Normal ICMP Traffic
  - d) Analyze Unusual ICMP Traffic
- Section 6: Analyze UDP Traffic
- a) Understand UDP Packet Structure
  - b) Filter on UDP Traffic
  - c) Analyze Normal UDP Traffic
  - d) Analyze Unusual UDP Traffic
- Section 7: Analyze TCP Traffic
- a) Understand TCP Packet Structure
  - b) Filter on TCP Traffic
  - c) Analyze Normal TCP Traffic
  - d) Analyze Unusual TCP Traffic
- Section 8: Analyze DHCP Traffic
- a) Understand DHCP Packet Structure
  - b) Filter on DHCP Traffic
  - c) Analyze Normal DHCP Traffic
  - d) Analyze Unusual DHCP Traffic
- Section 9: Analyze HTTP Traffic
- a) Understand HTTP Packet Structure
  - b) Filter on HTTP Traffic
  - c) Analyze Normal HTTP Traffic
  - d) Analyze Unusual HTTP Traffic
- Section 10: Analyze Telnet Traffic
- a) Understand Telnet Packet Structure
  - b) Filter on Telnet Traffic
  - c) Analyze Normal Telnet Traffic
  - d) Analyze Unusual Telnet Traffic
- Section 11: Analyze FTP Traffic
- a) Understand FTP Packet Structure
  - b) Filter on FTP Traffic
  - c) Analyze Normal FTP Traffic
  - d) Analyze Unusual FTP Traffic



- Section 12: Analyze POP Traffic
- a) Understand POP Packet Structure
  - b) Filter on POP Traffic
  - c) Analyze Normal POP Traffic
  - d) Analyze Unusual POP Traffic

- Section 13: Analyze SMTP Traffic
- a) Understand SMTP Packet Structure
  - b) Filter on SMTP Traffic
  - c) Analyze Normal SMTP Traffic
  - d) Analyze Unusual SMTP Traffic

### Recommended Course Prerequisites

This course focuses on both the normal and abnormal communication patterns of the TCP/IP suite and most common applications including DHCP, DNS, FTP, Telnet, HTTP, POP and SMTP.

#### Recommended prerequisite knowledge:

- Basic network components (hubs, switches, routers)
- IP network address structure
- Wireshark functionality and features (see Wireshark University Course WSU01)
  - Navigation
  - Packet detail tree expansion
  - Capture traffic
  - Display filtering on protocol or field
  - Create basic Wireshark graphs
  - Save packets based on filters, markers or range value



**Note:**

If you cannot check off at 70% of the items listed in the prerequisite checklist, we recommend you take the WSU01: Wireshark Functionality and Fundamentals course.

**Note:** This course is a recommended prerequisite course for Wireshark University Courses WSU03 (Troubleshooting Network Performance) and WSU04 (Network Forensics and Security)