Advanced Network Understanding with Wireshark

This intermediate Wireshark training is designed for network engineers and SOC analysts who want to sharpen their packet analysis skills. You'll dive into key protocols like TCP, UDP, and DNS, build advanced Wireshark filter techniques, and learn how to identify performance bottlenecks or signs of malicious activity. By the end, you'll have the hands-on experience and practical skills to confidently analyze real-world network traffic and support faster, more secure network operations.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Introduction to Wireshark

Introduction to Wireshark

Uses of Wireshark

Being Promiscuous

Saving our Work for Later

Exporting Things From Wireshark

Filtering Results

Concepts of TCP/IP

Overview

Concepts of TCP/IP

Part of the Bigger Picture

Different parts of TCP/IP

Were do we Get These Packets From?

Replay the Traffic

Learning Binary and Hex

IP4

Overview

IPv4

Identifying IPv4

IPv4 Communication

IPv4 Addressing

Where is IPv4 in our Packet?

Packet Examples

WEEK 2

IP6

IPv6

Identifying IPv6

IPv6 Communication

IPv6 Addressing

Where is IPv6 in our Packet?

Packet Examples

TCP

Overview

TCP

Identifying TCP

TCP Communication

TCP Addressing

Where is TCP in our Packet?

Packet Examples

UDP

Overview

UDP

Identifying UDP

UDP Communication

UDP Addressing

Where is UDP in our Packet?

Packet Examples

WEEK 3

ICMP

Overview

ICMP

Identifying ICMP

ICMP Communication

ICMP Addressing

Where is ICMP in our Packet?

Packet Examples

DNS

Overview

DNS

Identifying DNS

DNS Communication

DNS Addressing

Where is DNS in our packet?

Packet Examples

Layer 4 and Beyond

Overview

Layer 4 and Beyond

Pen to Paper

DNS

Microsoft Protocols

HTTP

WEEK 4

Wireshark Display Filters

Overview

Wireshark Display Filters

To the Boolean-Mobile!

Knowing the Basic Filters

Expanding on Basic Filters

Syntax is Everything

Apply Filtering to Live Capture

Microsoft Protocols

Overview

Microsoft Protocols

NETBIOS

LDAP

RDP

Kerberos

SMB

RPC

Advanced Wireshark

Overview

Advanced Wireshark

Magic Numbers

Regular Expressions

BPF Filtering

Supplemental Material

WEEK 5

Last updated 6.27.2025