Wireshark Fundamentals

- 3 Days
- Lecture and Hands-on Labs

Course Overview

This Advanced Wireshark training course aims to equip participants with comprehensive skills in network analysis using Wireshark, Tshark, Termshark, and TCPdump. Throughout the course, students will learn the fundamentals of Wireshark, including installation, configuration, and basic packet capturing techniques. The course delves into advanced analysis techniques, such as protocol hierarchy analysis, time analysis, and the application of display filters for efficient data inspection. Participants will gain hands-on experience in troubleshooting common network issues, analyzing transport and application layer protocols, and performing specialized protocol analysis for UDP/TCP, VoIP, HTTP/HTTP2 and more. By the end of the course, students will be proficient in capturing, analyzing, and interpreting network traffic, enabling them to effectively troubleshoot and optimize modern networks. Review this course online at https://www.alta3.com/courses/wireshark

Who Should Attend

- 4G and 5G network professionals
- DevOps Engineers
- Software Developers
- Technical Managers and Leads
- System and Cloud Administrators
- Network Engineers and Developers

What You'll Learn

- Wireshark Fundamentals
- Advanced Analysis Techniques
- 4G and 5G Protocol Analysis
- Troubleshooting Network Issues
- Specialized Protocols and VoIP Analysis ## Outline

AI LLM Toolkit

- 💻 Lecture + Lab: Large Language Model toolkit for AI Solution Assistance

Introduction to Network Analysis

- 💬 Lecture: Overview of Network Analysis
- 💬 Lecture: Introduction to TCP IP Terms

Getting Started with Wireshark

- 💻 Lecture + Lab: Introduction to Using Wireshark

Capturing Packets

- 💬 Lecture: Starting and Stopping Captures with Wireshark
- 💻 Lecture + Lab: Using TCPdump to make pcap Files for Wireshark
- 💻 Lecture + Lab: Introduction to Termshark

Basic Analysis Techniques

- 💻 Lecture + Lab: Ethernet Analysis - ARP Broadcast
- 💻 Lecture + Lab: Ethernet Analysis - Unicast
- 💬 Lecture: Encoding
- 💻 Lecture + Lab: Using the Packet Bytes Window
- 💻 Lecture + Lab: Wireshark - tshark

Filtering Techniques

- 💬 Lecture: Display Filters in Wireshark
- 💻 Lecture + Lab: Working with Display Filters
- 💬 Lecture: Wireshark Colorization Rules
- 💻 Lecture + Lab: Find packet
- 💻 Lecture + Lab: Flow and IO Graphs
- 💻 Lecture + Lab: PCAPs to Text, CSV, JSON, XML, and PDF
- 💻 Lecture + Lab: Display Macros
- 💬 Lecture: Decoding SSL Traffic with Wireshark

5G Captures

- 💻 Lecture + Lab: 5G Registration Analysis with Wireshark
- 💻 Lecture + Lab: Analysis of NGAP and the N2 Interface with Wireshark
- 💻 Lecture + Lab: 5G NAS and Wireshark
- 💻 Lecture + Lab: GTP in 5G

Advanced Analysis Techniques

- 💻 Lecture + Lab: Resolve Network Addresses with Wireshark

Specialized Protocol Analysis and Wireshark for VoIP

Diameter

- 💬 Lecture: Diameter and SCTP
- 💻 Lecture + Lab: Diameter Analysis

SIP Stack

- 💻 Lecture + Lab: Introduction to Wireshark for VoIP
- 💻 Lecture + Lab: Successful REGISER by a User Agent
- 💻 Lecture + Lab: Packet Analysis with Wireshark
- 💻 Lecture + Lab: Troubleshooting a 404