Wireshark Overview

IPC_123d | On-Demand | Transport | Express
Course Duration: 1 hour

Wireshark is an open-source protocol capture and analysis tool used by many wireless operators to help evaluate network performance and debug end-to-end operational failures. This self-paced eLearning course provides a high-level look at Wireshark and its key capabilities, taking a step-by-step approach to show the main elements of the user interface, the process of capturing and analyzing traces, and a brief overview of how Wireshark can be used to evaluate typical signaling flows in VoLTE networks. Frequent interactions are used to ensure student comprehension and engagement at every stage.

Intended Audience

This course is suitable for those looking for a high level introduction to Wireshark and how it may be used to evaluate and debug field issues.

Objectives

After completing this course, the student will be able to:

- Set up the elements of the user interface and Wireshark to their personal tastes
- Capture a network trace from their PC and save the packet capture file
- Search and select protocols and packets.
- Modify the time display and reference
- Analyze elements of IMS/VoIP protocols (i.e. SIP) and display a VoIP call graph

Course Prerequisites

No Prerequisites

Outline

1. User Interface
1.1 UI elements
1.2 Menu items

2. Capturing and Displaying Data
2.1 Capturing and saving traces
2.2 File management
2.3 Capture Filters

3. Wireshark Features
3.1 Filters and searching
3.2 Time display, reference, and shift
3.3 Using host files

4. Analyzing SIP Messages
4.1 SIP messages
4.2 VoIP call Flow
4.3 SIP filters