TCP/IP Network Troubleshooting Essentials with Wireshark

Duration: 3 Days **Course Code: GK9879**

Overview:

This course is designed as a “bring your own laptop” course – students must bring their own laptops with the latest version of Wireshark pre-installed. Students learn to master key Wireshark features and functions for troubleshooting networks more efficiently. In addition, students will customize Wireshark to quickly identify delays, application errors, and TCP problems.

Target Audience:

This course is intended for network support professionals who want to add Wireshark to their troubleshooting toolbox and/or improve their Wireshark and communications analysis skills. This course is recommended for those looking to achieve the WCNA Certification designation (formerly called the “Wireshark Certified Network Analyst” Certification).

Objectives:

- Create a custom Wireshark profile for troubleshooting
- Add, edit, and export custom column values
- Change key Wireshark preference settings
- Compare capture methods and options
- Perform an unattended capture
- Apply capture filters to focus on traffic of interest
- Apply display filters based on addresses, protocols, and field values
- Create buttons to speed up problem detection
- Build exclusion filters to remove packets from view
- Build and use regular expression filters
- Determine the most active hosts and conversations
- Identify applications used on the network
- Map IP addresses globally
- Reassemble traffic and objects
- Export reassembled objects
- Annotate a trace file
- Create a report from trace file annotations and comments
- Split and merge trace files
- Perform command-line capture
- Capture using filters and an autostop condition
- Use Tshark to extract field values from a trace file

Prerequisites:

Basic knowledge of network addressing

Basic knowledge of infrastructure devices (switches, routers)

Testing and Certification

Recommended as preparation for the following exam(s):

WCNA Certification (formerly referred to as the Wireshark Certified Network Analyst Certification)

Content:

Module 1: Introduction to Wireshark Resources and Analysis

- Tour of Wireshark Capabilities and Functions Tour
- Wireshark Capture Elements
- Frames vs. Packets vs. Segments
- Follow a Packet Through a Network
- Analyze a Trace File Using the Packet List Pane

Module 2: Customize Wireshark Views and Settings

- Create Custom Profiles
- Add, Edit, Export Columns
- Force Dissectors on Traffic that Uses Non-Standard Ports
- Set Key Wireshark Preferences (IMPORTANT)
- Locate Key Configuration Files
- Share and Import Profiles
- Configure Time Column to Spot Path and Server Latency Problems

Module 3: Determine the Best Capture Method and Apply Capture Filters

- Identify the Best Capture Location
- Capture on an Ethernet Network
- Capture on a Wireless Network
- Deal with Tons of Traffic (File Sets)
- Use Special Capture Techniques to Spot Sporadic Problems (Ring Buffer)
- Reduce the Amount of Traffic with Which You Have to Work
- Capture Traffic Based on Addresses (MAC/IP)
- Capture Traffic for a Specific Application
- Capture Specific ICMP Traffic

Module 4: Apply Display Filters to Focus on Specific Traffic

- Display Filter Methods and Syntax
- Edit and Use the Default Display Filters
- Filter Properly on HTTP Traffic
- Apply Display Filters Based on an IP Address, Range of Addresses or a Subnet
- Quickly Filter on a Field in a Packet
- Build Display Filter Buttons
- Filter to Detect Application Errors
- Filter on One or More Conversations (Streams)
- Expand Display Filters with Include and Exclude Conditions
- Use Parentheses to Change Filter Meaning
- Determine Why Your Display Filter Area is Yellow
- Use a Basic Regular Expression Filter to Locate a Set of Key Words in a Trace File
- Use Filters to Spot Communication Delays
- Import Display Filters into a Profile

Module 5: Color and Export Interesting Packets

- Identify and Edit Applied Coloring Rules
- Build a Coloring Rule to Highlight Delays
- Master the Intelligent Scrollbar
- Export Packets of Interest
- Export Packet Details (Excel Analysis)

Module 6: Build and Interpret Tables and Graphs

- Locate the Top Talkers
- Set Up GeoIP to Map Targets Globally
- List Applications Seen on the Network
- Detect Suspicious Protocols and Applications
- Graph Application and Host Bandwidth Usage
- Identify TCP Errors on the Network
- Understand What those Expert Errors Mean
- Identify an Overloaded Client

Module 7: Reassemble Traffic for Faster Analysis

- Reassemble Web Browsing Sessions
- Reassemble a File Transferred via FTP
- Extract a File from an FTP File Transfer
- Export HTTP Objects Transferred in a Web Browsing Session

Module 8: Add Comments to Your Trace Files and Packets

- Add Your Comments to Trace Files
- Add Your Comments to Individual Packets
- Export Packet Comments for a Report

Module 9: Use Command-Line Tools to Capture, Split, and Merge Traffic

- Split a Large Trace File into a File Set
- Merge Multiple Trace Files
- Capture Traffic at Command Line with Filters and an Autostop Condition

Use Tshark to Extract HTTP GET Requests

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK