



WIRESHARK felhasználói tanfolyam

Wireshark

1. What is Wireshark?

Protocol analysers, Wireshark features, Wireshark versions, troubleshooting techniques with Wireshark.

2. Installing Wireshark

Downloading Wireshark, UNIX issues, Microsoft issues, the role of winpcap, promiscuous mode, installing Wireshark. Wireshark documentation and help.

Hands on: Downloading and installing Wireshark.

3. Capturing traffic

Starting and stopping basic packet captures, the packet list pane, packet details pane, packet bytes pane, interfaces, using Wireshark in a switched architecture.

Hands on: Capturing packets with Wireshark.

4. Troubleshooting networks with Wireshark

Common packet flows.

Hands on: Analysing a variety of problems with Wireshark.

5. Capture filters

Capture filter expressions, capture filter examples (host, port, network, protocol, worm), primitives, combining primitives, payload matching.

Hands on: Configuring capture filters.

6. Working with captured packets

Live packet capture, saving to a file, capture file formats, reading capture files from other analysers, merging capture files, finding packets, going to a specific packet, display filters, display filter expressions.

Hands on: Saving captured data, configuring display filters.

7. Analysis and statistics with Wireshark

Enabling/disabling protocols, user specified decodes, following TCP streams, protocol statistics, conversation lists, endpoint lists, I/O graphs, protocol specific statistics.

Hands on: Using the analysis and statistics menus.

8. Command line tools

Tshark, tethereal, capinfos, editcap, mergecap, text2pcap, idl2eth.

Hands on: Using tshark.

9. Advanced issues

802.11 issues, management frames, monitor mode, packet reassembling, name resolution, customising Wireshark.

Hands on: Customising name resolution.

A tanítás nyelve: magyar nyelven de angol nyelvű tananyag alapján folyik.

Az általános részvételi feltételekről itt olvashat bővebben: <http://www.education.rrc.hu/index.html>