Freie Universität Berlin

Telematics

Tutorial

Basic tutorial on the Wireshark packet analyzer.

Dipl. Ing. (FH) Stephan Adler

Computer Systems and Telematics (CST)

Institute of Computer Science

Freie Universität Berlin

http://cst.mi.fu-berlin.de

Contents

- What's wireshark?
- Getting started
- Live Demonstration
  - Sniffing traffic
  - Analyze Traffic
    - Packet layers
    - TCP/IP
      - 3 way handshake
      - SMTP, HTTP
    - UDP
      - DNS

What's wireshark?

- Network sniffing tool
  - Able to 'tap' devices
    - Ethernet: promiscuous mode
    - WiFi: monitor mode
  - Please respect privacy when playing with wireshark!
- Packet analyzer
  - Started 1996 with TCP/IP
  - Today:
    - PPPoE
    - USB
    - DVB-T
    - VoIP (with voice extraction)
    - …. hundreds of protocols

Getting started

- Install from website (www.wireshark.org)
  - Alternatively: apt-get install wireshark
  - For sniffing: needs privileged user

- Resources
  - Sample Dumps (Interesting!): http://wiki.wireshark.org/SampleCaptures
  - User Guide: https://www.wireshark.org/docs/wsug_html_chunked/
  - http://packetlife.net/
    - Cheats sheets
    - Blog
    - Wiki