Wireshark Demo

Jens Lechtenbörger

Summer Term 2023

1 Background

I suppose that you know basics about the Internet, for example, as covered in my OER presentation Introduction to the Internet, to which I refer subsequently.

2 Wireshark Demo

- Wireshark is free/libre and open source software
  - `https://www.wireshark.org/`
- Analyze network traffic in real-time
  - Trouble-shooting
  - Understanding applications and protocols
    - What data is sent where?
    - How does encapsulation really look like?
  - Disable promiscuous mode to monitor only traffic addressed to you

Wireshark is free software to analyze network traffic in real-time. I use it to trouble-shoot network problems and to understand what applications send their data where on devices that I believe to control. I like Mr. Weasley's advice (in J.K. Rowling's *Harry Potter and the Chamber of Secrets*): "Never trust anything that can think for itself if you can't see where it keeps its brain."

Networked applications allow some insights into their brains and masters by looking at their network behavior, for which Wireshark provides all details. Other tools such as Chaosreader may be better suited for a quick overview.

Actually, since more and more application data is encrypted in response to the Snowden revelations in 2013, man-in-the-middle attacks against oneself are required to see such data. That, however, (a) requires additional tools, (b) fails for properly secured applications, and (c) is beyond the scope of this demo.

Still, Wireshark allows us to inspect headers on layers below the application layer, which is what we are going to do next.

2.1 Wireshark Filters

- **Capture** filter
  - Specify among Capture → Options, restrict what is being captured
    - Three qualifiers: **type** (`host`, `net`, `port`), **dir** (`src`, `dst`), **proto** (`ip`, `tcp`, `udp`, `arp`, ...)
      - `port 53`: Source or destination port is 53
      - `host www.uni-muenster.de`: Source or destination host has given name; also IP address instead of name possible
    - Boolean combinations with `and`, `or`, `not`, ...
      - `dst host 128.176.0.12 and udp dst port 53`
- **Display** filter
  - Restrict what is being displayed in filter bar below icons
    - E.g., `dns`, `arp`, `ip.addr==<some IP address>`
    - Alternatively, use decoded piece of protocol information
      - E.g., TCP layer, Flags, right click → "Apply as Filter"

2.2 Warning

- Inspecting other people's network traffic is **illegal**
  - Invasion of privacy, maybe worse
- Network cards can work in so-called **promiscuous mode**
  - Then, they accept **all** frames, regardless of destination address
  - Thus, turn promiscuous mode off
    - Unless you acquired consent of all affected parties

3 Live Demo

The demo illustrates the concept of message encapsulation in an Internet protocol stack with the help of Wireshark.

License Information