Netzwerkanalyse mit Wireshark: Welche (Meta-)daten werden weitergegeben?

Luis Herzog

April 2023

Abbildung 1: Wireshark Logo

Inhaltsverzeichnis

Es gibt viele verschiedenen Arten von Daten. Somit ebenfalls verschiedene Definitionen.

Bevor man über die Wireshark Software sprechen kann, müssen die Basics geklärt werden:

- Was sind Protokolle?
- Welche Protokolle gibt es?
- Wie funktionieren die Protokolle?
- das OSI Modell (IP/TCP)
- welcche Protokolle (welche können ausgelesen werden?

1 Metadaten

Metadaten sind tolle Daten **TODOO**

1.1 Verwendungszwecke

2 Das Programm: Wireshark

2.1 Programm

Wireshark ist eine Netzwerkpaketanalyse Software. Diese kann den aufgenommenen Netzwerktraffic in hohem Detail darstellen, um die Analyse dessen zu erleichtern. Die Darstellung der Ergebnisse erfolgt zum einen in Textform und zum anderen in Form von Grafiken, wie Diagrammen. Das Programm ist Open Source[1] und auf vielen Plattformen installierbar. Dazu gehören Windows, MacOS, Linux, Unix und BSD-Derivative. Im unteren Screenshot wird der Netzwerktraffic in einer VPN, in diesem Fall Mullvad VPN[2] untersucht. Was direkt auffällt ist die Menge an Requests, die in nur wenigen Sekunden gesendet werden.

2.2 Funktionsumfang

Wireshark ist eine Software mit sehr vielen Funktionen. Sie bietet wirklich alles rund um das Thema Netzwerkanalyse. Die wichtigsten Funktionen sind:

- Die Verfügbarkeit aus sehr vielen Platformen
- Die Möglichkeit dumps von anderen Personen importieren zu können
- Das Filtern von Paketen nach sehr vielen Kriterien

[1] Der Code des Programms ist öffentlich

[2] www.mullvad.net

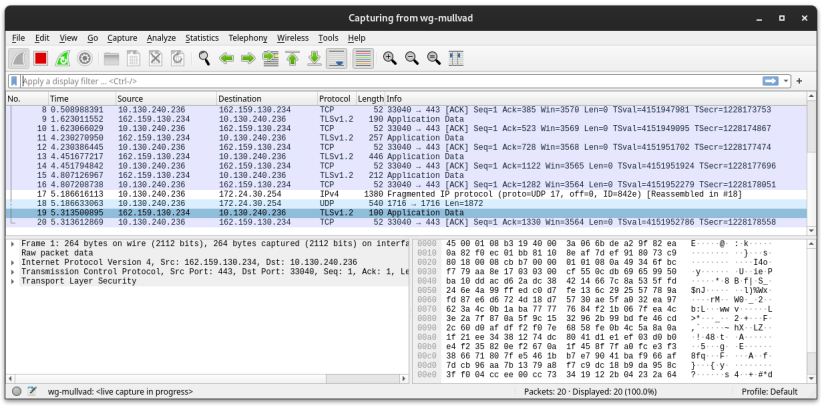

Abbildung 2: Beispielscreenshot aus der Wireshark Software

Besonders die letztere Funktion ist sehr wichtig, da man ohne diese schnell die Orientierung in der Software verlieren kann. [1]

2.3 Anwendungsbereiche

Wie im oberen Teil schon dargestellt, hat Wireshark sehr viele Funktionen. Allein deswegen wird es auch als Schweizer Taschenmesser der Netzwerktechnik bezeichnet. Somit kann Wireshark in sehr vielen Situationen Anwendung finden. Es kann beispielsweise von Netzwerk Administratoren benutzt werden, um Netzwerk Probleme zu Analysieren und zu lösen. Es kann außerdem von Netzwerk Sicherheits Analysten benuzt werden, um Sicherheitsprobleme in Netzwerken zu finden. Wiederum kann es auch von Anwendungsentwicklern benutzt werden, um Netzwerkprotokoll Implementationen zu debuggen. Zuletzt kann es auch benutzt werden um mehr über Netzwerktraffic zu lernen und diesen zu Analysieren. Es gibt natürlich auch viele weitere Möglichkeiten WIreshark zu benutzen. [2]

3 Netzwerk

3.1 Aufbau

3.2 Protokolle

3.3 OSI Modell

Das OSI-Modell wird benutzt, um den Aufbau eines Netzwerks zu vereinfachen, es ist ein tolles Werkzeug um das erstellen von sachen zu erleichtern

Abbildung 3: OSI-Modell

3.3.1 Bitübertragungsschicht

3.3.2 Sicherungsschicht

3.3.3 Netzwerkschicht

3.3.4 Transportschicht

3.3.5 Sitzungsschicht

3.3.6 Präsentationsschicht

3.3.7 Anwendungsschicht

4 Analyse

4.1 Beispiel

4.2 Browser

4.2.1 Mozilla Firefox

4.2.2 Microsoft Edge

4.2.3 Mullvad Browser

4.2.4 Opera Browser

5 Fazit

Abbildungsverzeichnis

Literatur

[1] The Wireshark Contributors. Wireshark - features. Zuletzt besucht: 15. Juni 2023, Quelle: www.wireshark.org.

[2] The Wireshark Contributors. Wireshark - intended purposes. Zuletzt besucht: 16. Mai 2023, Quelle: www.wireshark.org.

6 Anlagen