Protokoll zur Wireshark Aufgabe

Arbeitsstellung:

Eine unverschlüsselte Webadresse, bei dieser Aufgabe mail.webfischer.at, aufrufen und über Wireshark den Datenverkehr mitlesen.

Filter in Wireshark

Nach der Netzwerkauswahl in Wireshark müssen Filter für das vereinfachte Suchen verwendet werden. Um nur die Pakete zur und von der gewünschten Seite zu sehen muss die IP-Adresse angegeben werden

Um die IP-Adresse von der gesuchten Webseite zu finden kann diese über das CMD-Fenster gepingt werden.

C:\Users\jakob>ping mail.webfischer.at

Pinging mail.webfischer.at [91.114.39.20] with 32 bytes of data:

Reply from 91.114.39.20: bytes=32 time=33ms TTL=47

Reply from 91.114.39.20: bytes=32 time=49ms TTL=47

Reply from 91.114.39.20: bytes=32 time=45ms TTL=47

Ping statistics for 91.114.39.20:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 33ms, Maximum = 49ms, Average = 42ms

Nach dem Ping kann die gefundene IP-Adresse in einen Wireshark Filter in der Obersten Zeile geschrieben werden.

ip.addr == 91.114.39.20 && tcp

Um noch nach allen TCP Paketen zu Filtern kann nach einem doppeltem und-Zeichen der gewünschte Filter eingegeben werden.

Bei den ersten drei Paketen kann man den „3 Way Handshake“ erkennen, wo eine Verbindung vom Host zum Server aufgebaut wird.

Beim vierten Paket ist die erste „HTTP GET Request“ zu sehen, wo der erste Teil des Webseitencodes mitgesendet wird.