von
S & F

WireShark

15th October

1 - 2 Einleitung

Packet Sniffing: Wireshark acts as a packet sniffer, capturing packets exchanged between your computer and other devices over a network. It's a passive tool that doesn't send packets, but instead observes the ones being transmitted.

Packet Capture: The first step is selecting the appropriate network interface through which your computer is connected to the Internet to capture traffic.

Packet Analyzer: Wireshark not only captures packets but also analyzes and displays their details. It can dissect the content of each protocol layer (Ethernet, IP, TCP, HTTP) to show what's happening in the communication.

Interpreting Results: After capturing the traffic, you can analyze details such as the time taken for requests and responses, the protocols involved, and the structure of individual packets (HTTP GET and OK messages).

3 Fragen

Nennen Sie mindestens 5 Protokolle, die WireShark erkannt hat.

TLSv1.2, TLSv1.3, QUIC, TCP, UDP, ICMPv6, SSDP, HomePlug AV, 0x8912, EAPOL, MDNS

Wie lange hat es vom Senden des HTTP Requests bis zum Erhalt der HTTP Response gedauert?

- HTTP-Request (Paket 3070):
  - Zeit: 87, Info: `GET / HTTP/1.1`
- HTTP-Response (Paket 3079):
  - Zeit: 88, Info: `HTTP/1.1 204 No Content`
- Zeit des HTTP-Requests: 87.008928803 Sekunden
- Zeit der HTTP-Response: 88.00713720 Sekunden

Dauer = 88.00713720 - 87.008928803 = 0.998 Sekunden

Was ist die Internet-Adresse ihres Rechners?

192.168.178.73

Was ist die Ethernet-Adresse ihres Rechners?

34:7d:e4:4f:fc:eb

Welches ist die Ziel-MAC-Adresse, zu der ihr Rechner Pakete sendet?

AVMAudio_49:b2:b0 (f0:b0:14:49:b2:b0)

Vergleichen Sie die Ziel-MAC-Adresse für verschiedene Ziel-IP-Adressen.

Wenn man sich verschiedene Destinations anschaut, sieht man, dass AVMAudio_49:b2:b0 (f0:b0:14:49:b2:b0) die MAC-Adresse 34:7d:e4:4f:fc:eb zur Kommunikation verwendet. Bei anderen Paketen ist es andersrum (eingehende Pakete?).

Welchem Netzknoten könnten Sie die Ziel-MAC-Adresse wohl zuordnen?

Router?

Welche weiteren Protokolle werden genutzt, um ein http Paket zu übertragen?

siehe erste Frage

Welchen Schichten des ISO/OSI Schichtenmodells können Sie die Pakete zuordnen?

1. Application Layer: LSv1.2, TLSv1.3, SSDP, QUIC, mDNS
2. Transport Layer: TCP, UDP
3. Network Layer: ICMPv6
4. Link Layer: HomePlug AV (Ethernet)

4 Analyse eines Pakets

mithilfe von dieser Seite und WireShark

Markieren Sie im obigen Paket Ethernet, IP und TCP Header.

Ethernet Header are the first 14 bytes:
`38 22 d6 17 19 00 cc 63 82 2c 08 00`
IP sind die nächsten 20:
`45 00 02 9c 02 ed 40 00 80 06 40 66 8d 25 1d 5d 5b c6 ae c0`
TCP sind die nächsten 20:
`e2 26 00 50 4f 4c 29 24 72 ce 3c d4 50 18 40 b0 62 e7 00 00`

Was sind die Quell- und Ziel-MAC-Adressen Adressen des dargestellten Pakets?

Dst (0-5): `38 22 d6 67 19 00`
Src (6-11): `00 21 cc 63 82 2c`

Was sind die Quell- und Ziel-IP-Adressen des dargestellten Pakets?

Dst (30-33): `ae c0 e2 26`
Src (26-29): `1d 5d 5b c6`

Was sind die verwendeten TCP-Ports des dargestellten Pakets?

Dst (36-37): `4f 4c`
Src (34-35): `00 50`

5 Filter

Wie lautet der Filter, mit dem Sie über den TCP Port https Verkehr filtern können?

tcp.port = 443

Vergleiche Sie die Ergebnisse, wenn Sie http Verkehr direkt filtern oder http Verkehr über den TCP Port filtern. Können Sie sich die Unterschiede erklären?

HTTP gehört zur Anwendungsschicht und TCP zur Transportschicht, also werden über den Filter tcp.port == 80 mehr Pakete angezeigt, die normalweise keine HTTP-Daten enthalten.

Es gibt einen Filter http aber keinen Filter https. Haben Sie eine Idee warum?

Hypertext Transfer Protocol Secure ist durch TLS verschlüsselt.

Welcher Filter bewirkt, dass nur Pakete angezeigt, werden, die ihre eigene IP-Adresse als Ziel-Adresse haben?

ip.dst == your.ip.addr

6 Analyse einer Website

Wie viele Pakete wurden insgesamt übertragen? Unterscheiden Sie Upstream- und Downstream Pakete. Upstream- oder Uplink-Pakete sind Pakete, die von ihrem Rechner ins Internet gesendet werden und Downstream- oder Downlink-Pakete sind Pakete, die aus dem Internet zu ihrem Rechner übertragen werden.

Insgesamt	Upstream	Downstream
293759	18277	18838

Wie viele Bytes an Daten wurden insgesamt auf dem Uplink und Downlink übertragen?

Uplink | Downlink
2082538 | 11810426 von insgesamt 352433071

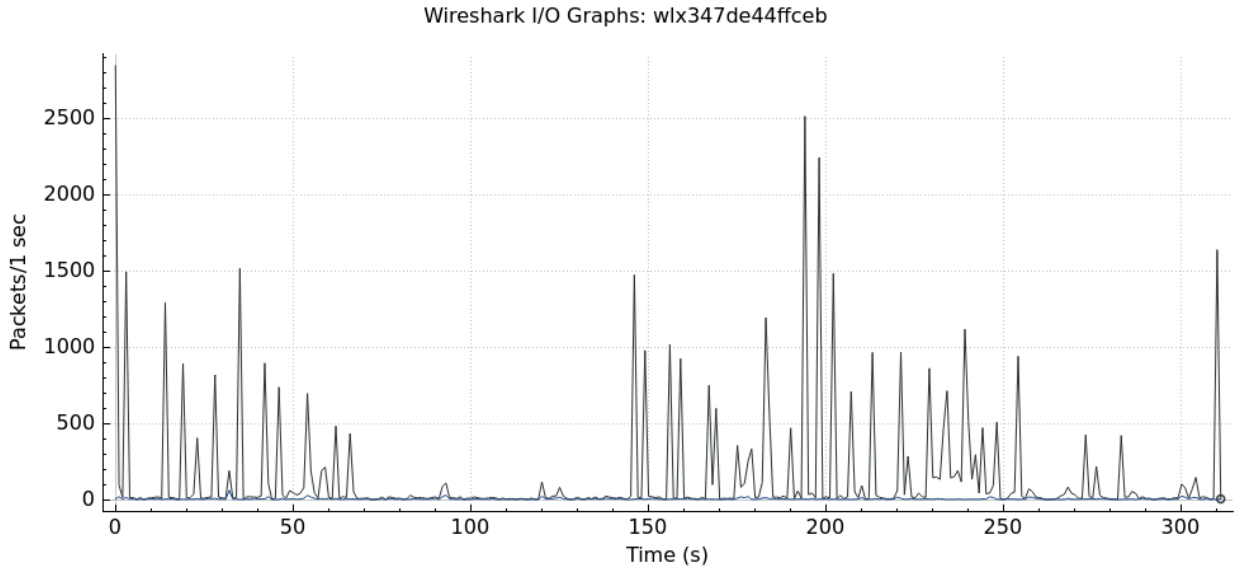
Von wie vielen IP Adressen hat ihr Rechner Daten empfangen?

IPv4 = 75, IPv6 = 148

Über wie viele TCP Sockets hat ihr Rechner die Daten empfangen? Ein Socket wird über Quell-IP-Adresse, Quell-Port sowie Ziel-IP-Adresse und Ziel-Port identifiziert.

4412

7 Aufzeichnen eines Audio-Streams



Upstream: 1996, 194674 bytes
Downstream: 1748, 330266 bytes

Peaks = Video puffern um ununterbrochen wiedergeben zu können