htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Thema

Laborprotokoll TCP-UPD Header Verleich

Figure 1: memes klauen ist nicht ethisch

Unterrichtsgegenstand: NWT1|ZIVK
Jahrgang: 2BHIT
Name: Stefan Fürst, Marcel Raichle
Betreuer: ZIVK
Übungsdaten: 24.5.2024, 31.5.2024,7.6.2024
Abgabedatum: 7.6.2024

Contents

1 Aufgabenstellung

Zussamenfassung der Aufgabenstellung von Cat-gpt:

1. Work in groups of 2, each with their own PC and Virtual Box with Kali Linux. Make sure network settings are correct and virtual machines have IP addresses. Verify with a ping. Start Wireshark and record the ping. You'll need to capture other transmissions too. Document every step in a log.
2. Use netcat to start a TCP server on port 5000. Connect with your partner using netcat. Document with screenshots and Wireshark. Answer questions about TCP connections and flags. Find and document TCP header fields. Document what happens when the server is closed.
3. Use netcat to start a UDP server on port 5000. Connect with your partner, document with screenshots and Wireshark. Answer questions about UDP connections and headers. Document server closure process.
4. Research TCP and UDP headers. Show and describe the most important fields in a one-page document. Compare header sizes and differences between TCP and UDP headers.
5. Bonus: Document how TCP and UDP are recorded in Wireshark. Research how port addresses are displayed. Show which Wireshark filters to use.

2 Zusammenfassung

Netcad um einen TCP/UPD Server starten, mit Netcad verbinden und mit Wireshark die Verbindungen analysieren.

3 Übungsdurchführung

3.1 Aufsetzen der Server

Listing 1: Commands

```
# TCP
nc -l -p 5000
# UDP
nc -l -u -p 5000
```

3.1.1 Verbinden mit dem Sever (TCP)

nc 10.23.38.117 4201

3.1.2 TCP-Verbindungsaufbau

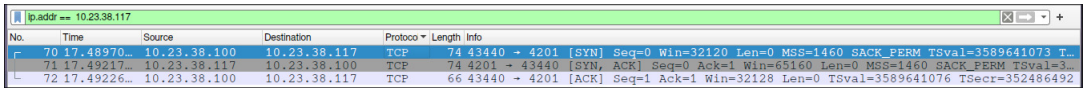

Figure 2: TCP 3 Way Handshake

3.1.3 Nachrichten verschicken und empfangen

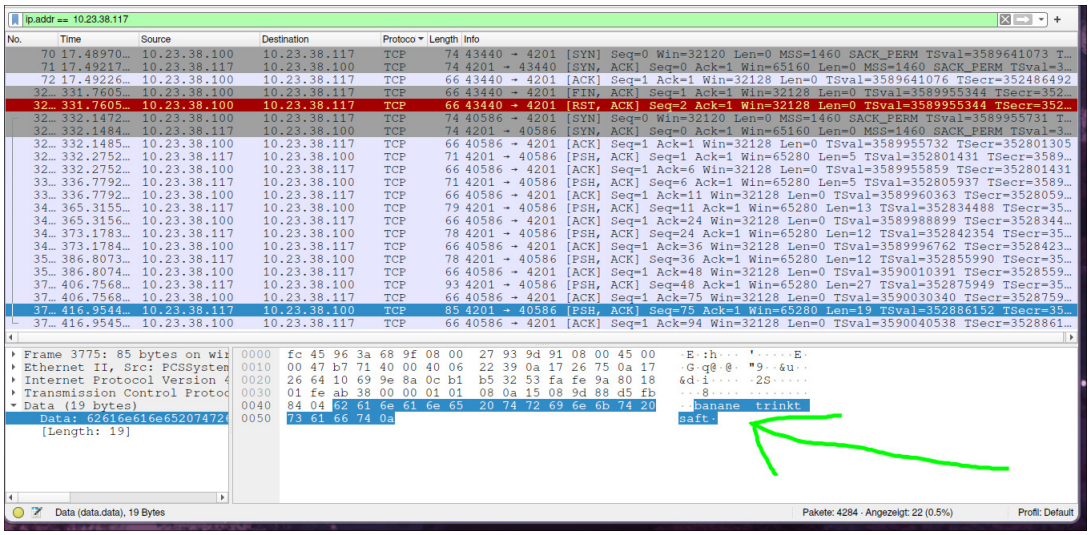

Figure 3: Nachricht

3.1.4 TCP-Flags

TCP-Flags dienen dazu um den Zustand, oder andere zusätzliche Informationen der Verbindung anzuzeigen. Diese diesen zum Troubleshooten. In der Übung ist die Push flag gesetzt, was bedeuted, dass die Nachricht sofort übertragen wird, ohne darauf zu warten, dass zusätliche Informationen auf der Senderseite gebuffert werden.[3]
Wird oft in Echtzeitapplikation benutzt.

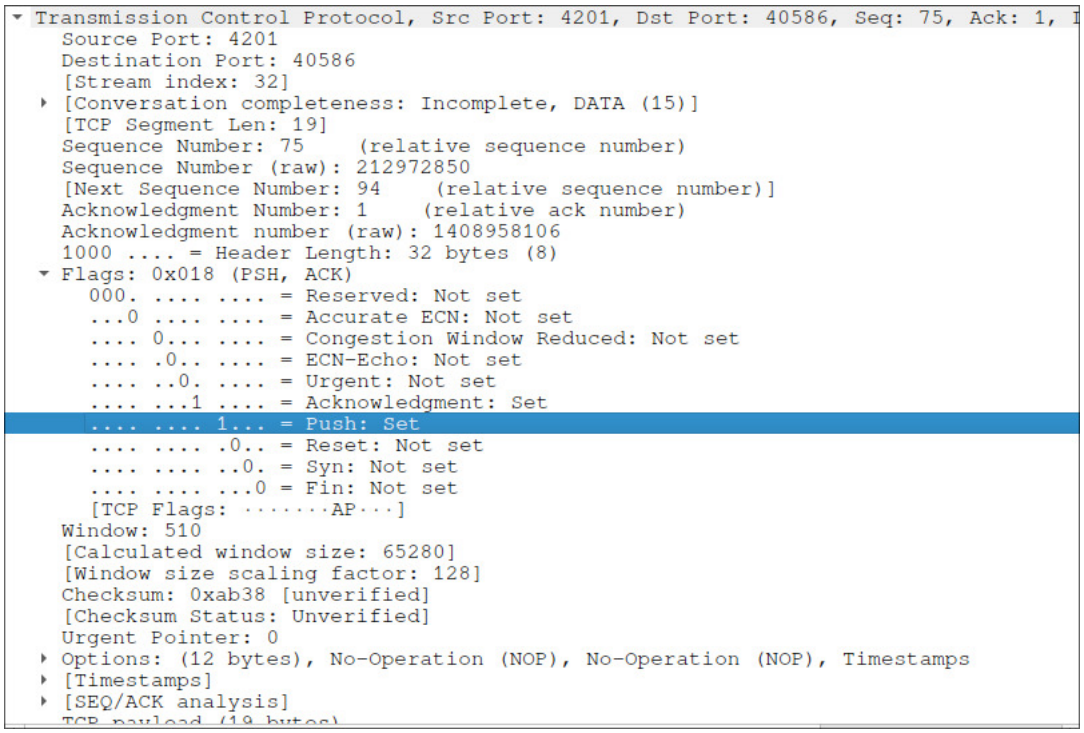

Figure 4: TCP-Flags

3.1.5 TCP-Header

Vorhandenen Felder

- Source Port
- Destination Port
- Sequence Number
  - Zeigt an wie viele Daten in der TCP Session übertragen werden.
- Acknowledgment Number
  - Vom Empfänger benutzt um das Nächste TCP Segment anzufordern

Nicht Vorhandene Felder

- Window
  - Gibt an wie viele bytes die der Empfänger empfangen will. Wird genutzt damit der Empfänger sagen kann, dass er mehr Daten empfagen will.
- RSV
  - 3 Reservierte Bits, die immer 0 sind.
- Urgent Pointer
  - Wenn die URG-Flag gesetzt ist, zeigt dieser Pointer an, wo die Urgent Daten enden.
- DO
  - Länge des Headers.
- Flags
  - Vorher bereits erklärt.
- Checksum
  - Benutzt für eine Prüfsumme um sicherzugehen, dass der TCP header korrekt is.

[4]

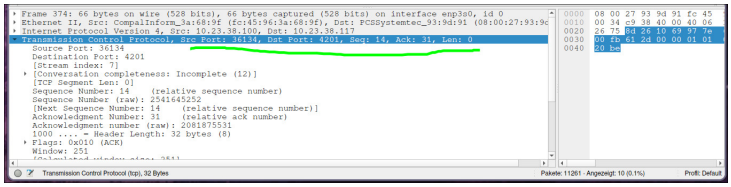

Figure 5: TCP-Header

3.1.6 Verbindungsabbruch

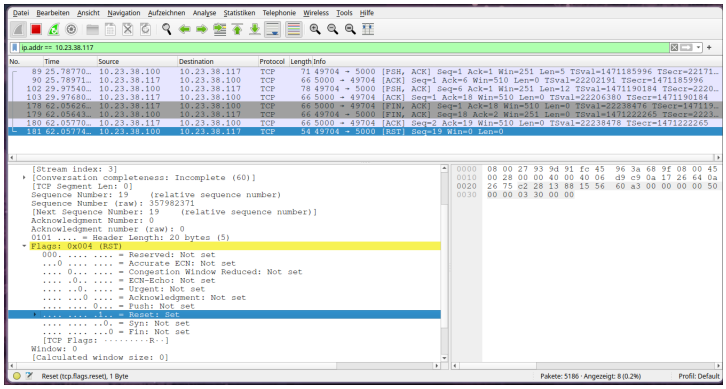

Figure 6: Verbindungsabbruch

Die TCP-Flag Reset wird im Packet gesetzt und dann ist die Verbindung mit diesem Packet beendet.

3.1.7 Verbinden mit dem Sever (UDP)

nc -u 10.23.38.117 4201

3.1.8 UDP-Verbindungsaufbau

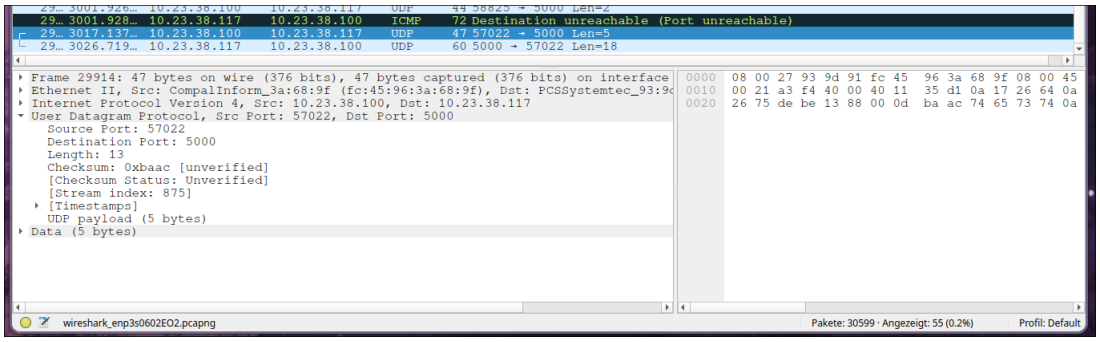

Figure 7: UDP-Verbindungsaufbau

Im gegensatz zu TCP gibt es hier keinen 3-Way-Handsake und die Verbindung beginnt direkt.

3.1.9 UDP-Nachrichten

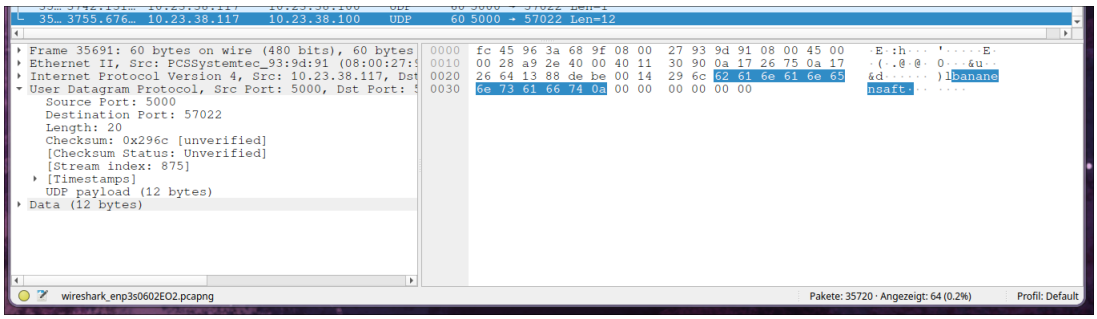

Figure 8: UDP-Nachricht

3.1.10 UDP-Header

- Source Port
- Destination Port
- Länge
- Checksum

Diese Felder haben die selben bedeutungen wie bei TCP. [2]

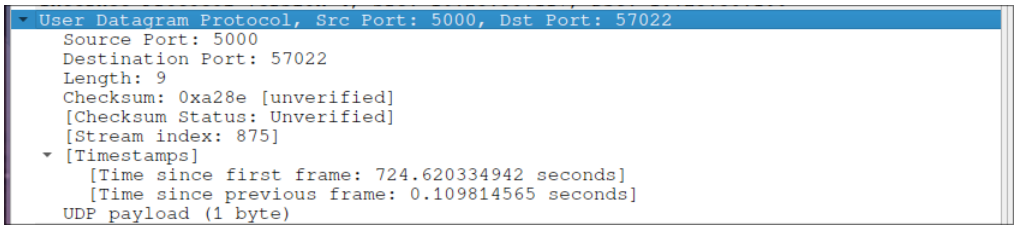

Figure 9: UDP-Header

3.1.11 UDP-Verbindungsabbruch

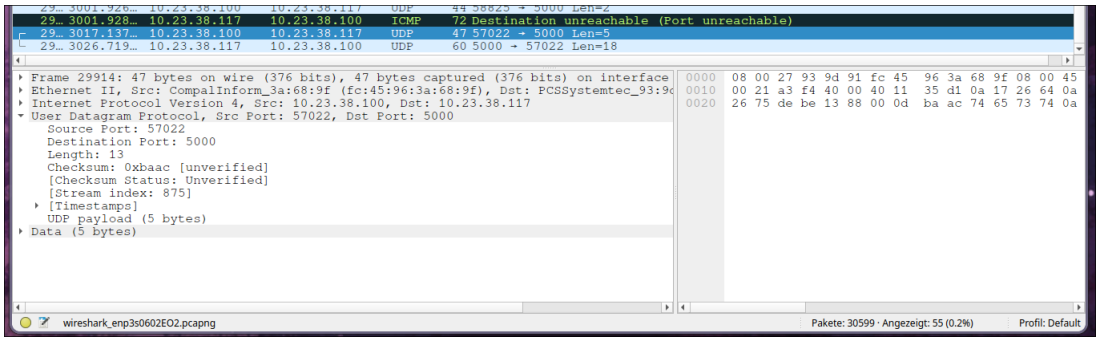

Figure 10: UDP-Verbindungsabbruch

Die Verbindung endet einfach und es wird kein Packet zum Beenden der Verbindung geschickt.

3.2 TCP und UDP Headervergleich

Im gegensatz zu TCP, UDP hat weniger Felder, da extra Felder wie Window, Sequnece und Achknowledgment Number einfach nicht benötigt, da der Sinn von UDP es ist, weniger overhead zu haben, damit eine schnellere Übertragung möglich ist.
Der TCP-Header hat eine Minimale größe ein 20 Bytes, während der UDP-Header immer 8 Bytes groß ist. [4][1]
UDP hat nur die nur die Esenziellsten Felder, die benögtigt werden um eine Kommunikation durchzuführen.
Wichtigste Felder:

- Src/Destination Port
  - Ohne diesem Feld kann kommunikation nicht funktionieren.
- Checksum
  - Wichtig um sicherzugehen, dass das Packet nicht Korrupt ist.

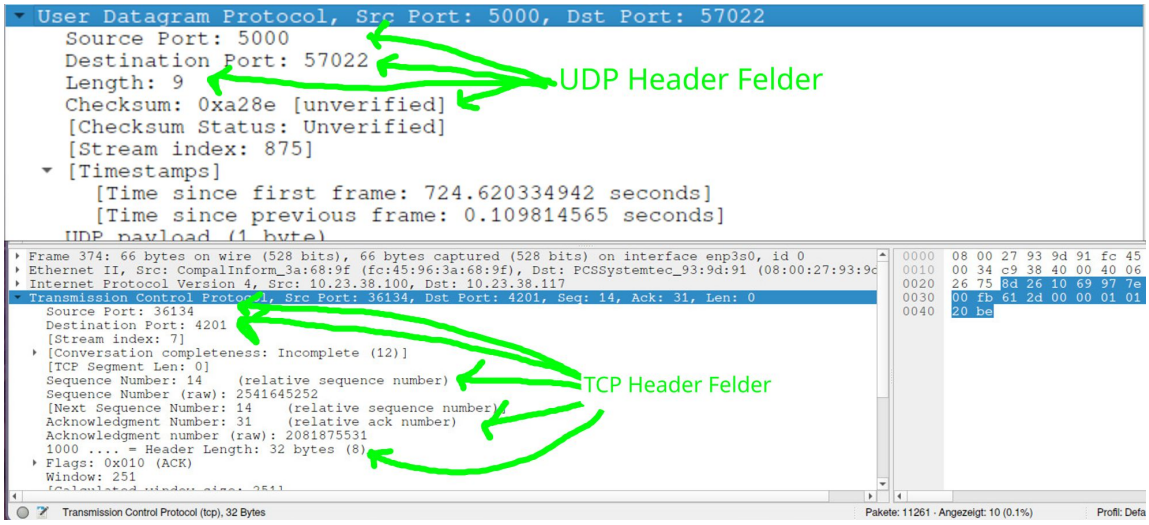

Figure 11: Header Vergleich

3.3 Nach Ports filtern

Nur Nach Port filtern:
Protokoll.port == port
Logische Operatoren können für komplexere Filter angewandt werden[5]

Listing 2: Commands

```
# tcp port 80 oder udp port 80
tcp.port == 80 || udp.port == 80

# auf port 80 nach verlorenen tcp segmenten filtern
tcp.port == 80 && tcp.analysis.lost_segment
```

4 Quellen

References

[1] User Datagram Protocol (UDP) in Computer Network, December 2021. [Online; accessed 7. Jun. 2024].

[2] Autoren der Wikimedia-Projekte. User Datagram Protocol – Wikipedia, January 2003. [Online; accessed 2. Jun. 2024].

[3] GeeksforGeeks. TCP flags. *GeeksforGeeks*, April 2023.

[4] Rene Molenaar. TCP Header. *NetworkLessons*, October 2019.

[5] Lee Stanton. How to Filter by Port with Wireshark. *Alphr*, June 2021.

5 Abbildungsverzeichnis

List of Figures