

## Aufgabe 1 – Netzwerkkonfiguration IPv4 (7 Punkte)

1a. (1 Punkt) VMs deb1220 und server: jeweils Screenshots von Aufrufen `ip addr show` und `cat /etc/resolv.conf`.

### Deb1220:

```
toor@deb1220:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fe:f6:25 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.0.2.10/24 brd 192.0.2.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefe:f625/64 scope link
        valid_lft forever preferred_lft forever
toor@deb1220:~$
```

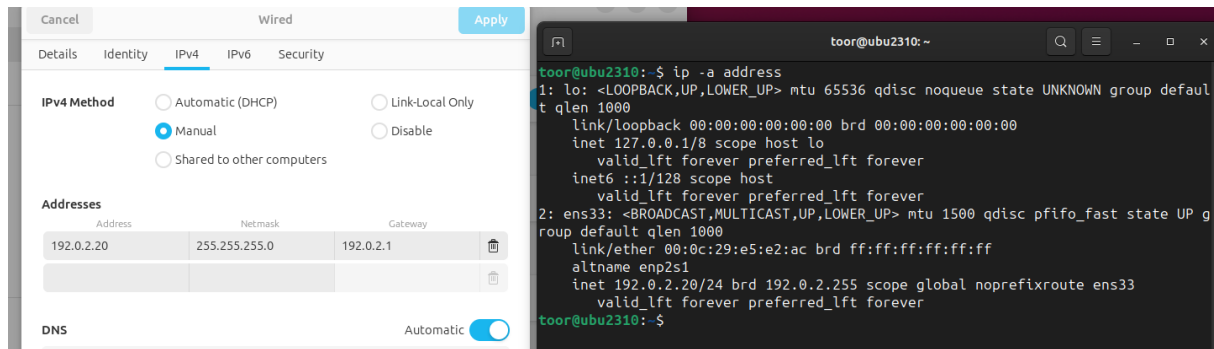
```
toor@deb1220:~$ cat /etc/resolv.conf
nameserver 203.0.113.10
toor@deb1220:~$
```

### Server

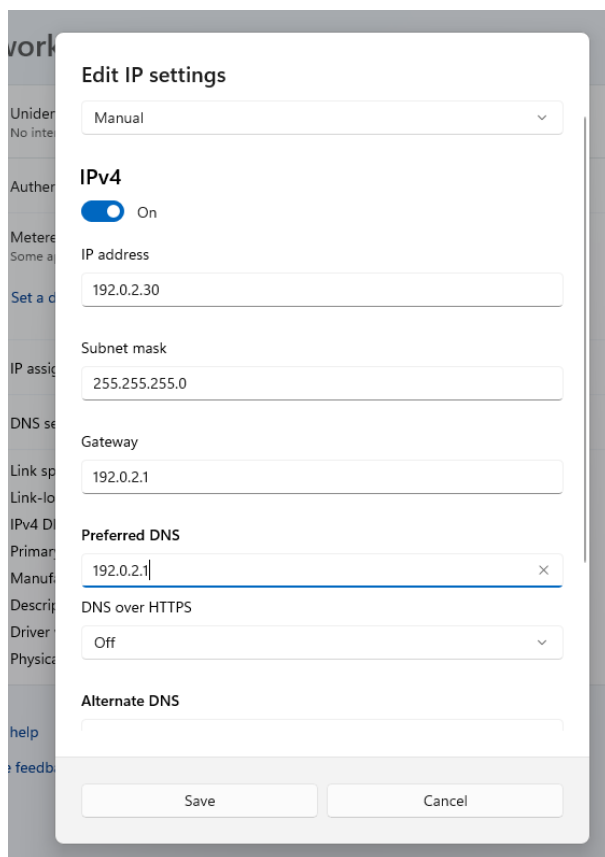
```
toor@server:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b7:ad:67 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 203.0.113.10/24 brd 203.0.113.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb7:ad67/64 scope link
        valid_lft forever preferred_lft forever
toor@server:~$ _
```

```
toor@server:~$ cat /etc/resolv.conf
nameserver 203.0.113.10
toor@server:~$ _
```

1b. (1 Punkt) VM ubu2310: Screenshots des IPv4-Tabs in den "Wired Settings" und des Aufrufs `ip addr show`.



1c. (1 Punkt) VM win11: Screenshots des IPv4-Dialogs und des Aufrufs von `ipconfig /all`.



```

PS C:\Users\toor> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-LG8J0NV
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain


Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-34-AC-98
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b326:f75e:37ca:bc73%7(Preferred)
IPv4 Address. . . . . : 192.0.2.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.0.2.1
DHCPv6 IAID . . . . . : 117443625
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-EC-B5-C8-00-0C-29-34-AC-98
DNS Servers . . . . . : 192.0.2.1
Primary WINS Server . . . . . : 192.168.138.2
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Users\toor>
  
```

Zum Testen der Konfiguration sollen von den VMs win11, ubu2310 und deb1220 jeweils vier Pings zur VM server gesendet werden.

1d. (1 Punkt) Auf all diesen VMs ist der Erfolg der Pings mittels eines Screenshots zu dokumentieren.

#### Deb1220:

```
toor@deb1220:~$ ping -c4 203.0.113.10
PING 203.0.113.10 (203.0.113.10) 56(84) bytes of data.
64 bytes from 203.0.113.10: icmp_seq=1 ttl=62 time=1.34 ms
64 bytes from 203.0.113.10: icmp_seq=2 ttl=62 time=3.81 ms
64 bytes from 203.0.113.10: icmp_seq=3 ttl=62 time=3.80 ms
64 bytes from 203.0.113.10: icmp_seq=4 ttl=62 time=3.70 ms

--- 203.0.113.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.343/3.162/3.807/1.050 ms
toor@deb1220:~$
```

#### Ubu2310:

```
toor@ubu2310:~$ ping -c4 203.0.113.10
PING 203.0.113.10 (203.0.113.10) 56(84) bytes of data.
64 bytes from 203.0.113.10: icmp_seq=1 ttl=62 time=0.962 ms
64 bytes from 203.0.113.10: icmp_seq=2 ttl=62 time=0.858 ms
64 bytes from 203.0.113.10: icmp_seq=3 ttl=62 time=4.08 ms
64 bytes from 203.0.113.10: icmp_seq=4 ttl=62 time=3.79 ms

--- 203.0.113.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.858/2.421/4.079/1.515 ms
```

#### Win11:

```
PS C:\Users\toor> ping 203.0.113.10

Pinging 203.0.113.10 with 32 bytes of data:
Reply from 203.0.113.10: bytes=32 time=1ms TTL=62
Reply from 203.0.113.10: bytes=32 time=1ms TTL=62
Reply from 203.0.113.10: bytes=32 time=3ms TTL=62
Reply from 203.0.113.10: bytes=32 time=4ms TTL=62

Ping statistics for 203.0.113.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
PS C:\Users\toor>
```

1e. (2 Punkt) Auf der VM ubu2310 sollen diese Pings (und die dazugehörigen Antworten) mittels Wireshark aufgezeichnet und in einer PCAP-Datei gespeichert werden. Diese PCAP-Datei soll exakt nur diese Pings und Antworten enthalten

**Siehe pings\_ipv4\_1e.pcap**

*Zum Testen der Konfiguration soll weiters ein Traceroute (mittels ICMP Nachrichten) von der VM ubu2310 zur VM server durchgeführt werden.*

*1f. (1 Punkt) Dieser traceroute-Aufruf soll mittels eines Screenshots dokumentiert werden.*

```
toor@ubu2310:~$ sudo !!
sudo traceroute -I 203.0.113.10
traceroute to 203.0.113.10 (203.0.113.10), 30 hops max, 60 byte packets
 1  _gateway (192.0.2.1)  0.627 ms  0.372 ms  *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * 203.0.113.10 (203.0.113.10)  4.374 ms  4.044 ms
```

**Aufgabe 2 – Netzwerkkonfiguration IPv6 (7 Punkte)**

*2a. (1 Punkt) VMs deb1220 und server: Screenshots von Aufrufen ip addr show und cat /etc/resolv.conf.*

**Deb1220:**

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fe:f6:25 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.0.2.10/24 brd 192.0.2.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 2001:db8:1::10/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefe:f625/64 scope link
        valid_lft forever preferred_lft forever
toor@deb1220:~$ _
```

```
toor@deb1220:~$ cat /etc/resolv.conf
nameserver 203.0.113.10
nameserver 2001:db8:3::10
toor@deb1220:~$
```

**Server:**

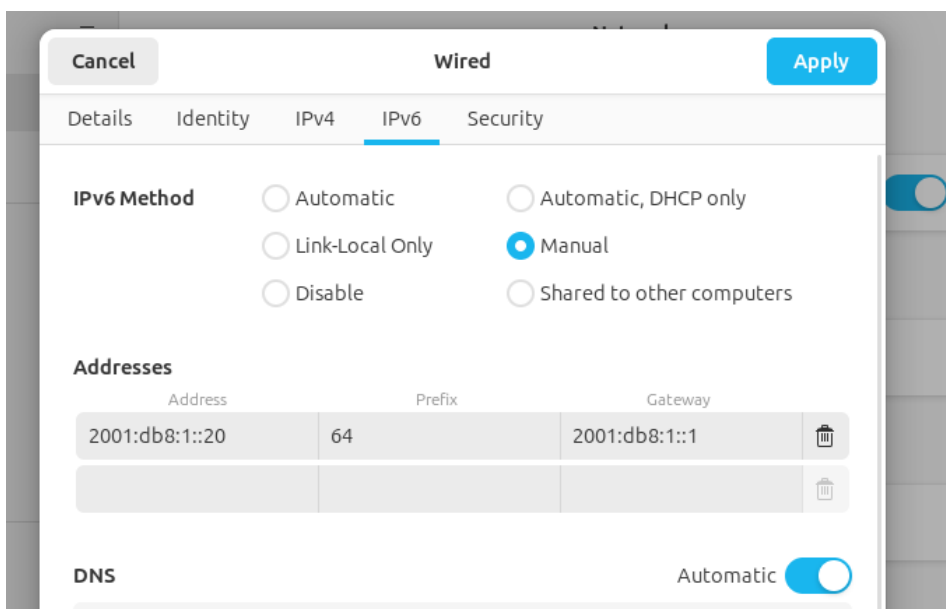
```
toor@server:~$ cat /etc/resolv.conf
nameserver 203.0.113.10
nameserver 2001:db8:3::10
toor@server:~$ _
```

```

Last login: Thu Nov 23 19:03:06 CET 2023 on tty1
toor@server:~$ ip -a addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b7:ad:67 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 203.0.113.10/24 brd 203.0.113.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 2001:db8:3::10/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb7:ad67/64 scope link
        valid_lft forever preferred_lft forever
toor@server:~$

```

2b. (1 Punkt) VM ubu2310: Screenshots des IPv6-Tabs in den "Wired Settings" und des Aufrufs `ip addr show`.



```

2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:e5:e2:ac brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.0.2.20/24 brd 192.0.2.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 2001:db8:1::20/64 scope global noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee5:e2ac/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

2c. (1 Punkt) VM win11: Screenshots des IPv6-Dialogs und des Aufrufs von `ipconfig /all`.

## IPv6

☒ On

IP address

2001:db8:1::30

Subnet prefix length

64

Gateway

2001:db8:1::1

Preferred DNS

2001:db8:1::1

DNS Servers

```
PS C:\Users\toor> ipconfig /all
```

### Windows IP Configuration

```
Host Name . . . . . : DESKTOP-LG8J0NV
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

### Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-34-AC-98
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:1::30(Preferred)
Link-local IPv6 Address . . . . . : fe80::b326:f75e:37ca:bc73%12(Preferred)
IPv4 Address. . . . . : 192.0.2.30(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 2001:db8:1::1
                             192.0.2.1
DNS Servers . . . . . : 2001:db8:1::1
                             192.0.2.1
NetBIOS over Tcpip. . . . . : Enabled
```

```
PS C:\Users\toor> |
```

*Zum Testen der Konfiguration sollen von den VMs win11, ubu2310 und deb1220 jeweils vier Pings über IPv6 zur VM server gesendet werden.,*

*2d. (1 Punkt) Auf all diesen VMs ist der Erfolg der Pings mittels eines Screenshots zu dokumentieren.*

#### Deb1220:

```
toor@deb1220:~$ ping -c4 2001:db8:3::10
PING 2001:db8:3::10(2001:db8:3::10) 56 data bytes
64 bytes from 2001:db8:3::10: icmp_seq=1 ttl=62 time=3.67 ms
64 bytes from 2001:db8:3::10: icmp_seq=2 ttl=62 time=3.74 ms
64 bytes from 2001:db8:3::10: icmp_seq=3 ttl=62 time=3.79 ms
64 bytes from 2001:db8:3::10: icmp_seq=4 ttl=62 time=4.21 ms

--- 2001:db8:3::10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 3.673/3.850/4.207/0.209 ms
toor@deb1220:~$
```

#### Ubu2310:

```
toor@ubu2310:~$ ping -c4 2001:db8:3::10
PING 2001:db8:3::10(2001:db8:3::10) 56 data bytes
64 bytes from 2001:db8:3::10: icmp_seq=1 ttl=62 time=1.99 ms
64 bytes from 2001:db8:3::10: icmp_seq=2 ttl=62 time=4.46 ms
64 bytes from 2001:db8:3::10: icmp_seq=3 ttl=62 time=4.36 ms
64 bytes from 2001:db8:3::10: icmp_seq=4 ttl=62 time=4.11 ms

--- 2001:db8:3::10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.988/3.729/4.460/1.013 ms
```

#### Win11:

```
PS C:\Users\toor> ping 2001:db8:3::10

Pinging 2001:db8:3::10 with 32 bytes of data:
Reply from 2001:db8:3::10: time=1ms
Reply from 2001:db8:3::10: time=4ms
Reply from 2001:db8:3::10: time=8ms
Reply from 2001:db8:3::10: time=2ms

Ping statistics for 2001:db8:3::10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 3ms
PS C:\Users\toor>
```

2e. (2 Punkte) Auf der VM ubu2310 sollen diese Pings (und die dazugehörigen Antworten) mittels Wireshark aufgezeichnet und in einer PCAP-Datei gespeichert werden. Diese PCAP-Datei soll exakt nur diese Pings und Antworten enthalten.

Siehe pings\_ipv6\_2e.pcap

Zum Testen der Konfiguration soll weiters ein Traceroute über IPv6 (mittels ICMP Nachrichten) von der VM ubu2310 zur VM server durchgeführt werden.

2f. (1 Punkt) Dieser traceroute-Aufruf soll mittels eines Screenshots dokumentiert werden.

```
toor@ubu2310:~$ sudo traceroute -I -6 2001:db8:3::10
traceroute to 2001:db8:3::10 (2001:db8:3::10), 30 hops max, 80 byte packets
 1  _gateway (2001:db8:1::1)  0.520 ms  0.437 ms  *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * 2001:db8:3::10 (2001:db8:3::10)  6.294 ms  10.013 ms
```

### Aufgabe 3- PCAP Analyse (6 Punkt)

3a. (1 Punkt) Welche IP-Adresse(n) hat das System, auf dem die Aufzeichnung – höchstwahrscheinlich – erstellt wurde?

IP-Adressen: **172.16.72.130**, 127.0.0.1 😊

Wie z.B. in Zeile 9 zu sehen, bei einem HTTP get-request ist 172.16.72.130 die Source => daher ist anzunehmen, dass dies die IP vom System ist

9	1.141631590	172.16.72.130	35.222.85.5	HTTP	143 GET / HTTP/1.1
---	-------------	---------------	-------------	------	--------------------

3b. (1 Punkt) Wie viele TCP Verbindungen sind in dieser Aufzeichnung enthalten?

Anzahl TCP-Verbindungen: **81** (Statistics -> Conversations -> Tcp)

The screenshot shows the Wireshark 'Conversations' window with the 'TCP' tab selected. It lists several connections between 10.0.0.10 and 172.16.72.130 on various ports.

Ethernet	IPv4 · 32	IPv6	TCP · 81	UDP
Address A	Port A	Address B	Port B	
10.0.0.10	52318	10.0.0.20		
172.16.72.130	48490	13.227.156.17	4	
172.16.72.130	53558	13.227.156.62	4	
172.16.72.130	53560	13.227.156.62	4	
172.16.72.130	48688	13.227.156.109	4	
172.16.72.130	45058	34.107.221.82		



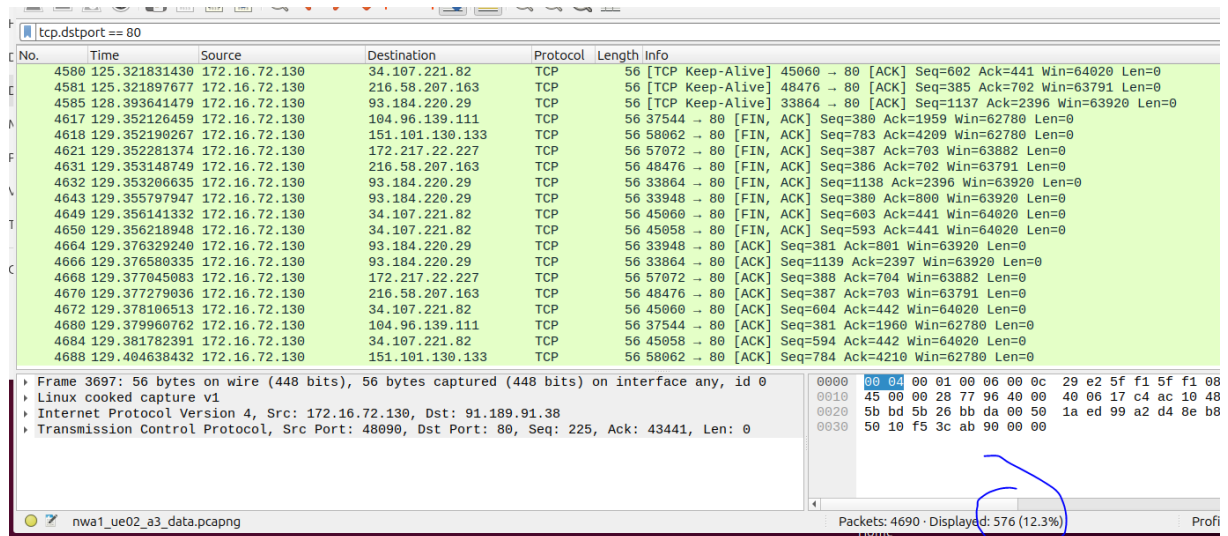
3c. (1 Punkt) Was ist die umfangreichste TCP Verbindung in Bezug auf gesamt übertragene Datenmenge in beide Richtungen (angegeben durch Client-IP-Adresse, Server-IP-Adresse, Client-Port, Server-Port und Transportprotokoll)?

Umfangreichste TCP Verbindung: **627kB** (Statistics -> Conversations -> Tcp -> Sortieren nach Bytes)

Client-IP-Adresse: **172.16.72.130**, Server-IP-Adresse: **91.189.91.38**, Client-Port: **48090**, Server-Port: **80** und Transportprotokoll: **TCP**

3d. (1 Punkt) Wie viele Dateneinheiten mit Zielport 80 sind in der Aufzeichnung enthalten?

Dateneinheiten mit Zielport 80: **576**



No.	Time	Source	Destination	Protocol	Length	Info
4580	125.321831430	172.16.72.130	34.187.221.82	TCP	56	[TCP Keep-Alive] 45060 → 80 [ACK] Seq=602 Ack=441 Win=64020 Len=0
4581	125.321897677	172.16.72.130	216.58.207.163	TCP	56	[TCP Keep-Alive] 48476 → 80 [ACK] Seq=385 Ack=702 Win=63791 Len=0
4585	128.393641479	172.16.72.130	93.184.220.29	TCP	56	[TCP Keep-Alive] 33864 → 80 [ACK] Seq=1137 Ack=2396 Win=63920 Len=0
4617	129.352126459	172.16.72.130	104.96.139.111	TCP	56	37544 → 80 [FIN, ACK] Seq=380 Ack=1959 Win=62780 Len=0
4618	129.352190267	172.16.72.130	151.101.130.133	TCP	56	58062 → 80 [FIN, ACK] Seq=783 Ack=4209 Win=62780 Len=0
4621	129.352261374	172.16.72.130	172.217.22.227	TCP	56	57072 → 80 [FIN, ACK] Seq=387 Ack=703 Win=63882 Len=0
4631	129.353148749	172.16.72.130	216.58.207.163	TCP	56	48476 → 80 [FIN, ACK] Seq=386 Ack=702 Win=63791 Len=0
4632	129.353206635	172.16.72.130	93.184.220.29	TCP	56	33864 → 80 [FIN, ACK] Seq=1138 Ack=2396 Win=63920 Len=0
4643	129.355797947	172.16.72.130	93.184.220.29	TCP	56	33948 → 80 [FIN, ACK] Seq=380 Ack=800 Win=63920 Len=0
4649	129.356141332	172.16.72.130	34.107.221.82	TCP	56	45060 → 80 [FIN, ACK] Seq=603 Ack=441 Win=64020 Len=0
4650	129.356218948	172.16.72.130	34.107.221.82	TCP	56	45058 → 80 [FIN, ACK] Seq=593 Ack=441 Win=64020 Len=0
4664	129.376329240	172.16.72.130	93.184.220.29	TCP	56	33948 → 80 [ACK] Seq=381 Ack=801 Win=63920 Len=0
4666	129.376580335	172.16.72.130	93.184.220.29	TCP	56	33864 → 80 [ACK] Seq=1139 Ack=2397 Win=63920 Len=0
4668	129.377045083	172.16.72.130	172.217.22.227	TCP	56	57072 → 80 [ACK] Seq=388 Ack=704 Win=63882 Len=0
4670	129.377279636	172.16.72.130	216.58.207.163	TCP	56	48476 → 80 [ACK] Seq=387 Ack=703 Win=63791 Len=0
4672	129.378106513	172.16.72.130	34.107.221.82	TCP	56	45060 → 80 [ACK] Seq=604 Ack=442 Win=64020 Len=0
4680	129.379960762	172.16.72.130	104.96.139.111	TCP	56	37544 → 80 [ACK] Seq=381 Ack=1960 Win=62780 Len=0
4684	129.381782391	172.16.72.130	34.107.221.82	TCP	56	45058 → 80 [ACK] Seq=594 Ack=442 Win=64020 Len=0
4688	129.404638432	172.16.72.130	151.101.130.133	TCP	56	58062 → 80 [ACK] Seq=784 Ack=4210 Win=62780 Len=0

Frame 3697: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0  
 Linux cooked capture v1  
 Internet Protocol Version 4, Src: 172.16.72.130, Dst: 91.189.91.38  
 Transmission Control Protocol, Src Port: 48090, Dst Port: 80, Seq: 225, Ack: 43441, Len: 0

Packets: 4690 · Displayed: 576 (12.3%)

3e. (2 Punkte) In der Aufzeichnung hat sich die Übertragung von Zugangsdaten (Benutzername und Passwort) im Klartext "versteckt". Finde diese und speichere die dazugehörige TCP Verbindung (und ausschließlich diese) in einer eigenen PCAP-Datei ab

telnet -> follow -> tcp stream

Siehe telnet\_3e.pcap