



# Network

## Fundamentals of TCP/IP Transport and Applications

# Wireshark TCP

The image shows a Wireshark packet capture of a TCP connection. The packet list at the top shows six packets. Packet 4 is selected, showing details for the TCP segment and the HTTP GET request. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a reassembled PDU]

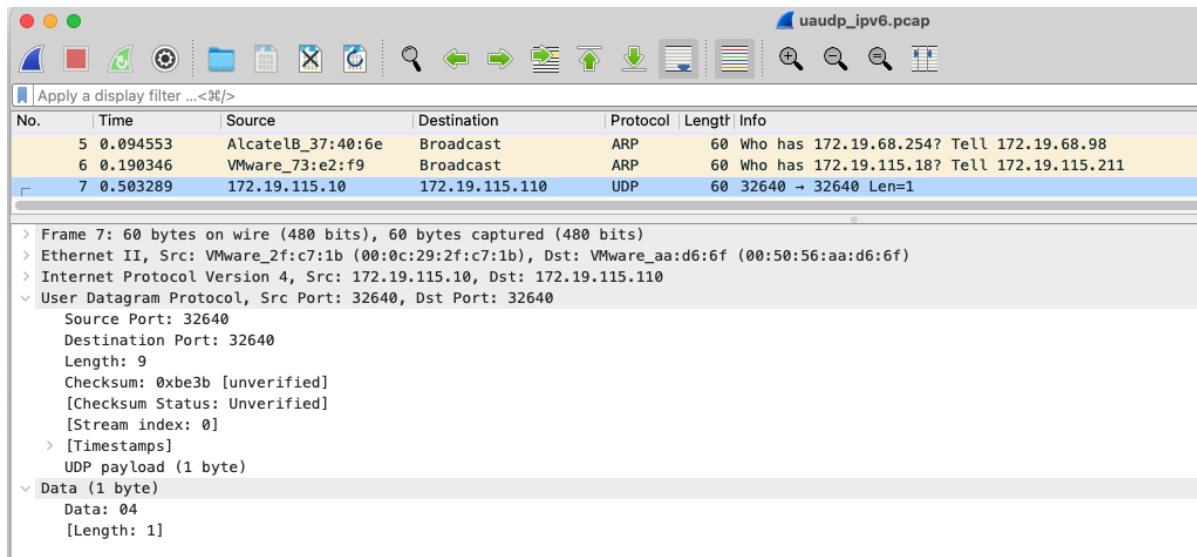
**Packet 4 Details:**

- Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
- Ethernet II, Src: Xerox\_00:00:00:00:00:00, Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
- Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
- Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
  - Source Port: 3372
  - Destination Port: 80
  - [Stream index: 0]
  - [TCP Segment Len: 479]
  - Sequence Number: 1 (relative sequence number)
  - Sequence Number (raw): 951057940
  - [Next Sequence Number: 480 (relative sequence number)]
  - Acknowledgment Number: 1 (relative ack number)
  - Acknowledgment number (raw): 290218380
  - 0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
  - Window: 9660
  - [calculated window size: 9660]
  - [Window size scaling factor: -2 (no window scaling used)]
  - Checksum: 0xa958 [unverified]
  - [Checksum Status: Unverified]
  - Urgent Pointer: 0
  - [SEQ/ACK analysis]
  - [Timestamps]
  - TCP payload (479 bytes)
- Hypertext Transfer Protocol

**Packet 4 Bytes:**

```
0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00  ...E.....E-
0010 02 07 0f 45 48 00 80 86 90 10 91 fe a0 ed 41 00  ...Eg.....A-
0020 e4 ff 0d 2c 00 50 38 af fe 14 11 4c 61 8c 50 18  .....PB...LaP
0030 25 bc a9 58 00 00 47 45 54 20 2f 64 6f 77 6e 6c  %-.X.GE T /downl
0040 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e  oad.html HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68  i..Host: www.eth
0060 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d  ereal.co m=User-
0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35  Agent: Mozilla/5
0080 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20  .0 (Windows; U;
0090 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20  Windows NT 5.1;
00a0 65 6e 2d 55 53 3b 20 76 3a 31 2e 36 20 20 47 6  en-US; rv:1.6) G
00b0 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41  ecko/200 40113; A
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c  ccept: text/xml,
00d0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c  applicat ion/xml,
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d  applicat ion/xml
00f0 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b  t+xml; te xt/html;
0100 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e  q=0.9, te xt/plain
```

# Wireshark UDP



uauudp\_ipv6.pcap

Apply a display filter ...<=>

No.	Time	Source	Destination	Protocol	Length	Info
5	0.094553	AlcatelB_37:40:6e	Broadcast	ARP	60	Who has 172.19.68.254? Tell 172.19.68.98
6	0.190346	VMware_73:e2:f9	Broadcast	ARP	60	Who has 172.19.115.18? Tell 172.19.115.211
7	0.503289	172.19.115.10	172.19.115.110	UDP	60	32640 → 32640 Len=1

> Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

> Ethernet II, Src: VMware\_2f:c7:1b (00:0c:29:2f:c7:1b), Dst: VMware\_aa:d6:6f (00:50:56:aa:d6:6f)

> Internet Protocol Version 4, Src: 172.19.115.10, Dst: 172.19.115.110

✓ User Datagram Protocol, Src Port: 32640, Dst Port: 32640

- Source Port: 32640
- Destination Port: 32640
- Length: 9
- Checksum: 0xbe3b [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]
- > [Timestamps]
- UDP payload (1 byte)

✓ Data (1 byte)

- Data: 04
- [Length: 1]

# TCP/UDP

---

## Concept of Ports

Reliability

Speed

TCP based applications

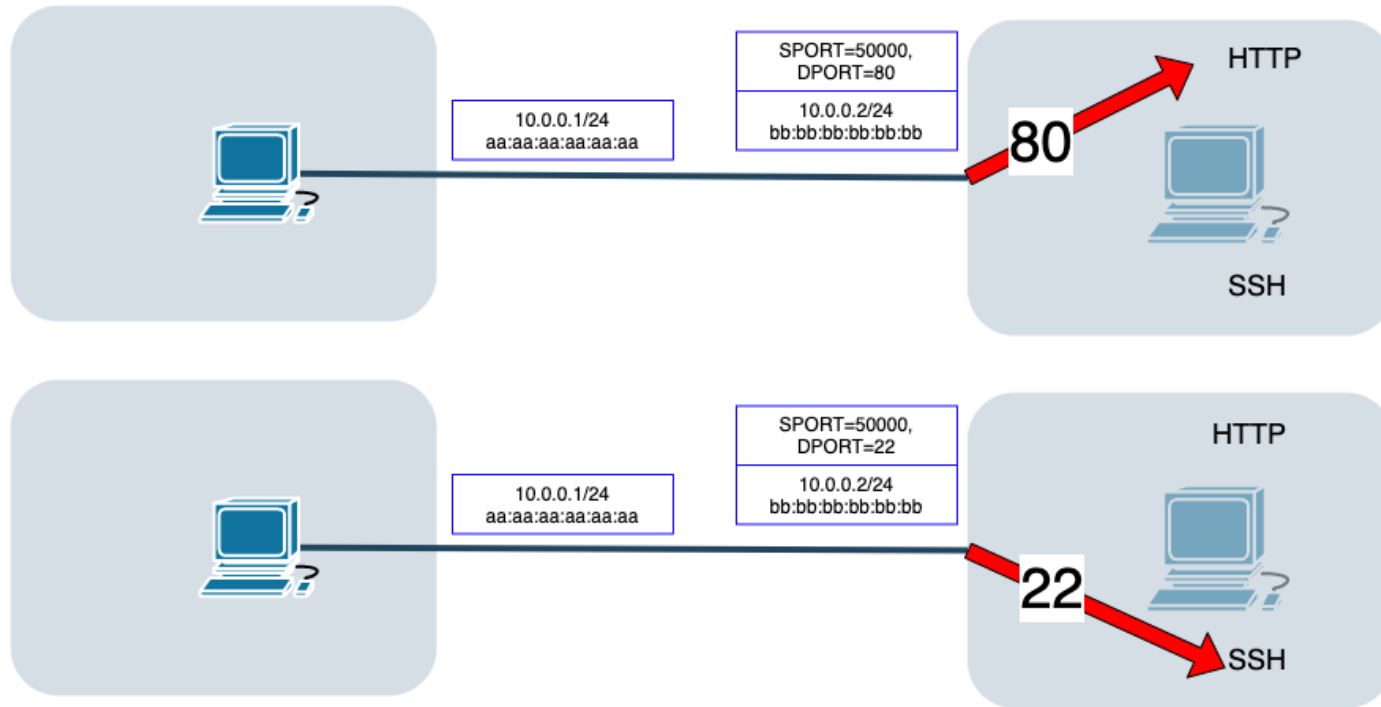
UDP based applications

Could be torrent over TCP?

Could be voip be over TCP?

Could be chrome(firefox) working http over UDP?

# TCP/UDP



# Ports

---

20/21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
67,68	UDP	DHCP
80	TCP	HTTP
110	TCP	POP3
445	TCP	HTTPS

# Endpoints see

---

Ethernet		IP		TCP
dmac:aa:aa:aa:aa:aa:aa	smac:bb:bb:bb:bb:bb	sip:10.1.0.100	dip:10.0.0.1	SPORT:2000, DPORT:80



# Endpoints see

---

TCP uses 3-way handshake  
UDP doesn't

3way handshake:

PC1 → SYN → PC2

PC1 ← SYN,ACK ← PC2

PC1 → ACK → PC2

TCP/UDP



# Endpoints see

---

TCP:

1)init: 3-way handshake

PC1  $\rightarrow$  SYN(n)  $\rightarrow$  PC2

PC1  $\leftarrow$  SYN(m),ACK(n+1)  $\leftarrow$  PC2

PC1  $\rightarrow$  ACK(m+1)  $\rightarrow$  PC2



2)send $\rightarrow$

$\leftarrow$ commit

send $\rightarrow$

$\leftarrow$ commit

Send $\rightarrow$

Send $\rightarrow$

Send $\rightarrow$

$\leftarrow$  commit

...etc

UDP:

1)Send $\rightarrow$

Send $\rightarrow$

Send $\rightarrow$

# How to get ports

```
[root@sun /]# ss -t
```

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
ESTAB	0	52	192.168.1.78:ssh	192.168.1.65:50252	

```
[root@sun /]#
```

```
[root@sun /]# ss -nt
```

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
ESTAB	0	52	192.168.1.78:22	192.168.1.65:50336	

```
[root@sun /]#
```

```
[root@sun /]# nmap ya.ru
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-13 15:41 MSK
Nmap scan report for ya.ru (87.250.250.242)
Host is up (0.0067s latency).
Other addresses for ya.ru (not scanned): 2a02:6b8::2:242
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
[root@sun /]#
```

**THANK YOU**