

Wireshark Aufgabe

Aufgabe 1 & 2

➔ Einleitung

Aufgabe 3

1. Nennen Sie mindestens 5 Protokolle, die Wireshark erkannt hat.

1. HTTP
2. TCP
3. DNS
4. TLS
5. ARP

2. Wie lange hat es vom Senden des HTTP Requests (<http://gaia.cs.umass.edu/wireshark-labs/>

INTRO-wireshark-file1.html) bis zum Erhalt der HTTP Response gedauert?

64	3.365659	128.119.245.12	141.37.168.36	HTTP	540 HTTP/1.1 200 OK (text/html)
61	3.258669	141.37.168.36	128.119.245.12	HTTP	454 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

▼ Frame 64: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Interface id: 0 (\Device\NPF_{00634C18-0EE0-4C16-A3D9-1ADA734B3B15})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 25, 2022 15:59:24.595532000 W. Europe Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1666706364.595532000 seconds

[Time delta from previous captured frame: 0.000715000 seconds]

[Time delta from previous displayed frame: 0.106990000 seconds]

[Time since reference or first frame: 3.365659000 seconds]

Frame Number: 64

Frame Length: 540 bytes (4320 bits)

Capture Length: 540 bytes (4320 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

> Ethernet II, Src: Dell_ce:82:c2 (54:bf:64:ce:82:c2), Dst: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 141.37.168.36

> Transmission Control Protocol, Src Port: 80, Dst Port: 57019, Seq: 1, Ack: 401, Len: 486

> Hypertext Transfer Protocol

> Line-based text data: text/html (4 lines)

3. Was ist die Internet-Adresse ihres Rechners?

=> 141.37.168.36

Was ist die Ethernet-Adresse (MAC-Adresse, physikalische Adresse) ihres Rechners?

=> 90:1B:0E:F1:7B:62

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

⇒ 34:17:EB:46:9E:02

67	3.489145	128.119.245.12	141.37.168.36	HTTP	538 HTTP/1.1 404 Not Found (text/html)
65	3.381428	141.37.168.36	128.119.245.12	HTTP	411 GET /favicon.ico HTTP/1.1
64	3.365659	128.119.245.12	141.37.168.36	HTTP	540 HTTP/1.1 200 OK (text/html)
61	3.258669	141.37.168.36	128.119.245.12	HTTP	454 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

> Frame 61: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface 0

▼ Ethernet II, Src: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62), Dst: Dell_46:9e:02 (34:17:eb:46:9e:02)

> Destination: Dell_46:9e:02 (34:17:eb:46:9e:02)

> Source: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 141.37.168.36, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 57019, Dst Port: 80, Seq: 1, Ack: 1, Len: 400

> Hypertext Transfer Protocol

```
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix  . : htwg-konstanz.de  
Description . . . . . : Intel(R) Ethernet Connection (2) I219-LM  
Physical Address. . . . . : 90-1B-0E-F1-7B-62  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::dfa:de2e:9e27:4075%2(Preferred)  
IPv4 Address. . . . . : 141.37.168.36(Preferred)  
Subnet Mask . . . . . : 255.255.255.192  
Lease Obtained. . . . . : Friday, 21 October 2022 11:31:27  
Lease Expires . . . . . : Wednesday, 26 October 2022 15:45:46  
Default Gateway . . . . . : 141.37.168.1  
DHCP Server . . . . . : 141.37.10.96  
DHCPv6 IAID . . . . . : 42998542  
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-2A-EC-0C-90-1B-0E-F1-7B-62  
DNS Servers . . . . . : 141.37.0.1  
                        141.37.0.2  
NetBIOS over Tcpip. . . . . : Enabled
```

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

Welchem Netzknoten können Sie die Ziel-MAC-Adresse zuordnen?

No.	Time	Source	Destination	Protocol	Length	Info
59	3.258097	128.119.245.12	141.37.168.36	TCP	66	80 → 57019 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=128
58	3.178619	FujitsuT_f1:7b:62	Broadcast	ARP	42	Who has 141.37.168.32? Tell 141.37.168.36
57	3.152548	141.37.168.36	128.119.245.12	TCP	66	57019 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
56	3.148567	FujitsuT_f1:7b:62	Broadcast	ARP	60	Who has 141.37.168.32? Tell 141.37.168.40

> Frame 64: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

▼ Ethernet II, Src: Dell_ce:82:c2 (54:bf:64:ce:82:c2), Dst: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

> Destination: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

> Source: Dell_ce:82:c2 (54:bf:64:ce:82:c2)

Type: IPv4 (0x0800)

4581	13.610377	185.172.148.128	141.37.168.36	TLSv1.3	393	Application Data
4582	13.610418	141.37.168.36	185.172.148.128	TCP	54	57346 → 443 [ACK] Seq=5052 Ack=494148 Win=262144 Len=0
4583	13.615045	185.172.148.128	141.37.168.36	TCP	1434	443 → 57346 [ACK] Seq=494148 Ack=4884 Win=42496 Len=1380 [TCP segment of a reassembled PDU]
4584	13.615046	185.172.148.128	141.37.168.36	TLSv1.3	1206	Application Data
4585	13.615119	141.37.168.36	185.172.148.128	TCP	54	57346 → 443 [ACK] Seq=5052 Ack=496680 Win=262144 Len=0
4586	13.615692	185.172.148.128	141.37.168.36	TCP	1434	443 → 57346 [ACK] Seq=496680 Ack=4968 Win=42496 Len=1380 [TCP segment of a reassembled PDU]
4587	13.615694	185.172.148.128	141.37.168.36	TCP	1434	443 → 57346 [ACK] Seq=498060 Ack=4968 Win=42496 Len=1380 [TCP segment of a reassembled PDU]
4588	13.615695	185.172.148.128	141.37.168.36	TCP	1434	443 → 57346 [ACK] Seq=499440 Ack=4968 Win=42496 Len=1380 [TCP segment of a reassembled PDU]
4589	13.615695	185.172.148.128	141.37.168.36	TLSv1.3	702	Application Data

> Frame 4581: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0

▼ Ethernet II, Src: Dell_ce:82:c2 (54:bf:64:ce:82:c2), Dst: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

> Destination: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)

> Source: Dell_ce:82:c2 (54:bf:64:ce:82:c2)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 185.172.148.128, Dst: 141.37.168.36

> Transmission Control Protocol, Src Port: 443, Dst Port: 57346, Seq: 493809, Ack: 4800, Len: 339

> [3 Reassembled TCP Segments (3099 bytes): #4579(1380), #4580(1380), #4581(339)]

> Transport Layer Security

⇒ Netzknoten: Dell_ce (siehe Bilder)

4. Betrachten Sie ein HTTP Paket. Welche weiteren Protokolle werden genutzt, um ein http Paket zu übertragen? Welchen Schichten des TCP/IP-Schichtenmodells können Sie die Pakete zuordnen?

67	3.489145	128.119.245.12	141.37.168.36	HTTP	538 HTTP/1.1 404 Not Found (text/html)
65	3.381428	141.37.168.36	128.119.245.12	HTTP	411 GET /favicon.ico HTTP/1.1
64	3.365659	128.119.245.12	141.37.168.36	HTTP	540 HTTP/1.1 200 OK (text/html)
61	3.258669	141.37.168.36	128.119.245.12	HTTP	454 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

>	Frame 64: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
>	Ethernet II, Src: Dell_ce:82:c2 (54:bf:64:ce:82:c2), Dst: FujitsuT_f1:7b:62 (90:1b:0e:f1:7b:62)
>	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 141.37.168.36
>	Transmission Control Protocol, Src Port: 80, Dst Port: 57019, Seq: 1, Ack: 401, Len: 486
>	Hypertext Transfer Protocol
>	Line-based text data: text/html (4 lines)

⇒ TCP, IP, Ethernet

Aufgabe 4:

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

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

=> Ziel: 38-22-D6-67-19-00

=> Quelle: 00-21-CC-63-82-2C

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

=> Ziel: 5B C6 AE C0 [91.198.174.192]

=> Quelle: 8D 25 1D 5D [141.37.29.93]

4. Was sind die verwendeten TCP-Ports des dargestellten Pakets?

=> Ziel: 00 50 [Port 80]

=> Quelle: E2 26 [Port 57.894(E226) oder 226(E2) 38(26)??]

	Ziel	Quelle	
0000	38 22 d6 67 19 00	00 21 cc 63 82 2c	08 00 45 00
0010	02 9c 02 ed 40 00	80 06 40 66	8d 25 1d 5d 5b c6
0020	ae c0 e2 26	00 50	4f 4c 29 24 72 ce 3c d4 50 18
0030	40 b0 62 e7 00 00	47 45 54 20 2f 77 69 6b 69 2f	
0040	53 69 6d 70 6c 65 5f 53 65 72 76 69 63 65 5f 44		
0050	69 73 63 6f 76 65 72 79 5f 50 72 6f 74 6f 63 6f		
0060	6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74		
0070	3a 20 64 65 2e 77 69 6b 69 70 65 64 69 61 2e 6f		
0080	72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20		
0090	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e		
00a0	64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57		
00b0	36 34 3b 20 72 76 3a 33 32 2e 30 29 20 47 65 63		

8".g...!.c.,...E.
....@...@f.%.)[.
...&.POL)\$r.<.P.
@.b...GET /wiki/
Simple_Service_D
iscovery_ProtoCo
l HTTP/1.1..Host
: de.wikipedia.o
rg..User-Agent:
Mozilla/5.0 (Win
dows NT 6.1; WOW
64; rv:32.0) Gec

Aufgabe 5

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

=> **tcp.port == 80 && http**

2. Erhalten Sie das gleiche Ergebnis wie bei dem Filter HTTP? Erklären Sie ihre Erkenntnis

=> Ja da Port 80 den HTTP Port darstellt

3. Was bewirkt der Filter: `http && !(udp.port==1900)`

=> Es werden lediglich http Anfragen gefiltert die nicht über den UDP port 1900 laufen

=> „UDP port 1900 besorgt einen unzuverlässigen Dienst und Datagramme können ohne Meldung verdoppelt, unzulässig kommen oder verschwinden. UDP port 1900 denkt, dass die Fehlernachprüfung und -korrektion nicht erforderlich ist oder in dieser Anwendung nicht vollgezogen wird, um das Overhead dieser Bearbeitung auf dem Netzwerkschnittstellenniveau zu vermeiden“ [Quelle: <https://de.adminsub.net/tcp-udp-port-finder/1900>]

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

=> **ip.dst == 141.37.168.36** (bzw. `ip.dst == xxx.xxx.xxx.xxx` wobei x = eigene IP)