

Aufgabe1:

- 1) Welche ICMP-Pakettypen werden von *traceroute* verwendet ?

ICMP Destination unreachable (Type 3) und ICMP Time exceeded (Type 11)

The screenshot displays a network traffic capture in Wireshark. The left pane shows a list of packets, with the 'icmp' filter applied. The right pane shows the details of a selected ICMP packet, which is an 'ICMP Time exceeded' (Type 11) packet. The packet details show the source and destination IP addresses, the ICMP type and code, and the TTL value.

No.	Time	Source	Destination	Protocol	Length	Info
168	3.338458989	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
169	3.338529477	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
170	3.338592274	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
171	3.35722120	62.155.248.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
172	3.35722280	62.155.248.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
173	3.356308864	62.155.248.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
174	3.357934859	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
175	3.358078014	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
176	3.358096768	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
177	3.358379128	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
178	3.358809124	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
179	3.361410073	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
180	3.361528990	80.157.201.242	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
181	3.362458984	80.157.201.242	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
182	3.362509260	80.157.201.242	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
183	3.367442059	157.240.51.113	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
184	3.368342327	157.240.51.113	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
185	3.368712371	157.240.51.121	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
186	3.369210265	173.252.67.175	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
187	3.382588629	173.252.67.9	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
188	3.384762813	173.252.67.55	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
189	3.384762943	185.60.217.35	192.168.2.102	ICMP	102	Destination unreachable ...
190	3.387915333	185.60.217.35	192.168.2.102	ICMP	102	Destination unreachable ...
191	3.389204591	185.60.217.35	192.168.2.102	ICMP	102	Destination unreachable ...
192	3.3928597820	185.60.217.35	192.168.2.102	ICMP	102	Destination unreachable ...
193	3.394314013	185.60.217.35	192.168.2.102	ICMP	102	Destination unreachable ...

- 2) Welche Rolle spielt das TTL-Feld im IPv4-Paket für die Funktionsweise von *traceroute* ?

Mit TTL gibt der Sender die Lebensdauer des Pakets in Sekunden an. Jede Station, die ein IP-Paket weiterleiten muss, zieht von diesem Wert mindestens 1 ab. Hat der TTL-Wert 0 erreicht, wird das IP-Paket verworfen. Dieser Mechanismus verhindert, dass Pakete ewig Leben, wenn sie nicht zustellbar sind. TTL-Werte zwischen 30 und 64 sind typisch.

- 3) Wie lautet der Filterausdruck für Wireshark, um ausschließlich die Netzwerkpakete des Traceroute-Laufs (UDP bzw. ICMP-Anfragen und ICMP-Antworten) anzuzeigen?

icmp || udp

The screenshot shows the Wireshark interface with the filter 'icmp || udp' applied. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
163	3.336392610	192.168.2.102	185.60.217.35	UDP	74	37341 → 33448 Len=32
164	3.336402879	192.168.2.102	185.60.217.35	UDP	74	55875 → 33449 Len=32
165	3.336455939	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
166	3.336529477	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
167	3.336563480	192.168.2.102	192.168.2.1	DNS	84	Standard query 0x7dce PT...
168	3.336592274	192.168.2.1	192.168.2.102	ICMP	102	Time-to-live exceeded (T...
169	3.339951113	192.168.2.1	192.168.2.102	DNS	110	Standard query response ...
170	3.340505864	192.168.2.102	185.60.217.35	UDP	74	60766 → 33450 Len=32
171	3.340590683	192.168.2.102	185.60.217.35	UDP	74	58457 → 33451 Len=32
172	3.340616621	192.168.2.102	185.60.217.35	UDP	74	46055 → 33452 Len=32
173	3.355722120	62.155.240.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
174	3.355722250	62.155.240.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
175	3.355881979	192.168.2.102	192.168.2.1	DNS	87	Standard query 0xb7e9 PT...
176	3.356571062	192.168.2.1	192.168.2.102	DNS	130	Standard query response ...
177	3.356630864	62.155.240.146	192.168.2.102	ICMP	70	Time-to-live exceeded (T...
178	3.356680928	192.168.2.102	185.60.217.35	UDP	74	47194 → 33453 Len=32
179	3.356706796	192.168.2.102	185.60.217.35	UDP	74	35313 → 33454 Len=32
180	3.356770526	192.168.2.102	185.60.217.35	UDP	74	37283 → 33455 Len=32
181	3.357934859	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
182	3.358060495	192.168.2.102	192.168.2.1	DNS	85	Standard query 0xc14a PT...
183	3.358875814	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
184	3.359096768	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
185	3.359379128	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
186	3.359426236	192.168.2.1	192.168.2.102	DNS	158	Standard query response ...
187	3.359809124	217.5.101.58	192.168.2.102	ICMP	110	Time-to-live exceeded (T...
188	3.359936012	192.168.2.102	185.60.217.35	UDP	74	33657 → 33456 Len=32

Packet 177 details:

- Frame 177: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
- Ethernet II, Src: HuaweiTe_51:87:f7 (58:d7:59:51:87:f7), Dst: Giga-Byt_6a:14:35 (e0:d5:5e:6a:14:35)
- Internet Protocol Version 4, Src: 62.155.240.146, Dst: 192.168.2.102
- Internet Control Message Protocol

Packet 177 hex dump:

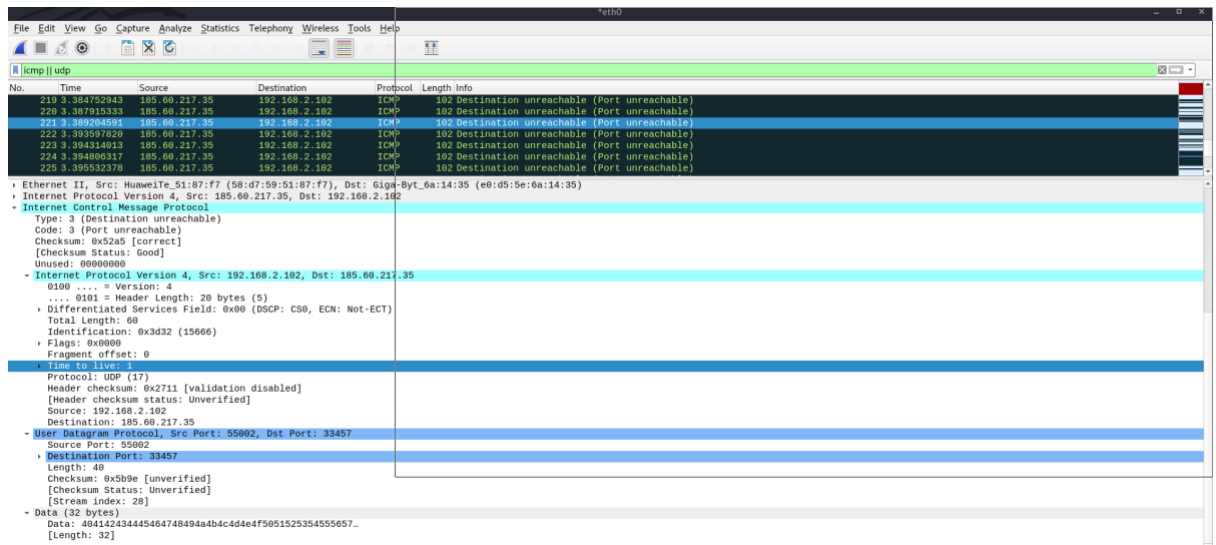
```

0000  e0 d5 5e 6a 14 35 00 00 00 00 00 00 00 00 00 00  ...J...L...
0010  00 38 00 00 00 00 fe 01 ca 88 3e 9b f0 92 c0 a8  .8.....>....
0020  02 66 0b 00 00 3f ad 00 00 00 00 45 00 00 3c 3d 20  .f..?....E..<=
0030  00 00 01 11 27 23 c0 a8 02 66 b9 3c d9 23 8c 85  ....'#...f.<.#..
0040  82 9f 00 28 a6 05  ...(.

```

Wireshark status bar: User Datagram Protocol: Protocol | Packets: 289 · Displayed: 96 (33.2%) · Dropped: 0 (0.0%) | Profile: Default

- 4) Wie entstehen die verschiedenen Zahlen (erste Spalte, IP-Adressen, Zeitmessungen) in der Bildschirmausgabe von "traceroute"? Welche sind direkt im Wireshark nachzulesen?



Wir können Source/Destination(IP-Adressen) und das TTL(ipv4) einfach lesen.

Aufgabe2:

Führen sie "traceroute" für 3 Webseiten ihrer Wahl durch. Ermitteln sie die **verschiedenen geographischen Standorte der Router**, die ihr Anfragepaket weiterleiten.



www.soundcloud.com

- 1-[192.168.2.1] (Berlin,DE)
- 2-[62.155.240.146](Hamburg,DE)
- 3-[217.5.101.30](Berlin,DE)
- 4-[217.5.101.30](Berlin,DE)
- 5-[80.156.161.178](Hessen,Frankfurt Am Main,DE)
- 6-[52.93.39.102](Washington,Seattle,US)
- 7-[52.93.49.123] (Washington,Seattle,US)
- 8-***
- 9-***
- 10-***
- 11-***
- 12-***
- 13-[99.84.147.46](Berlin,DE)

www.g2a.com

- 1-[192.168.2.1] (Berlin,DE)
- 2-[62.155.240.146](Hamburg,DE)
- 3-[217.239.40.46](Hessen,Frankfurt Am Main, DE)
- 4-[217.239.40.46](Hessen,Frankfurt Am Main, DE)
- 5-[4.68.73.5](California,San Jose,US)
- 6-[4.69.159.86](Greater London,Ealing,UK)
- 7-[213.242.69.166](Stockholms Lan,Stockholm,SE)
- 8-[104.27.188.140](California,San Jose,US)

www.splice.com

- 1-[192.168.2.1] (Berlin,DE)
- 2-[62.155.240.146](Hamburg,DE)
- 3-[217.239.40.46](Hessen,Frankfurt Am Main, DE)
- 4-[217.239.40.46](Hessen,Frankfurt Am Main, DE)
- 5-[4.68.73.5](California,San Jose,US)
- 6-[4.69.159.5](Hessen,Frankfurt Am Main,DE)
- 7-[212.162.40.34](Hessen,Frankfurt Am Manin,DE)
- 8-[104.17.165.41](New South Wales,Sydney,AU)

