

Лабораторная работа №4

Студент: Султанов Артур Радикович, группа: Р3313

Расшифровка HTTPS

Расшифровка HTTPS-трафика Firefox на Linux в Wireshark с помощью SSLKEYLOGFILE

```
$ SSLKEYLOGFILE="$HOME/firefox-keys.log" firefox &  
$ ls -lah ~/firefox-keys.log  
-rw-r--r-- 1 sultanowskii sultanowskii 9.1K May  2 11:52  
/home/sultanowskii/firefox-keys.log
```

Записанный расшифрованный HTTP-трафик не прикладывается к материалам ЛР из соображений безопасности.

Подготовка

Для сбора пакетов был выбран интерфейс `wlp0s20f3` - т.к. ноутбук подключен к Wi-Fi.

Целевым веб-сайтом был выбран <https://github.com/sultanowskii> - мой Github-профиль.

Анализ трафика утилиты ping

Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP

Запустим ping. Сделаем это на 100, 128, 256, 512, 1024, 2048, 4096, 10000 байтах.

```
ping -c 5 -s 100 github.com
```

И заглянем в получившийся записанный трафик (с фильтром `(ip.dst_host == 140.82.112.4) || (ip.src_host == 140.82.112.4)`):

(ip.dst == 140.82.121.4) (ip.src == 140.82.121.4)			
time	source	destination	protocol length info
12 1.558105863	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0016, seq=1/256, ttl=64 (reply in 13)
13 1.558105863	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0016, seq=1/256, ttl=64 (request in 12)
20 3.399138413	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0016, seq=2/512, ttl=64 (reply in 21)
21 3.399138413	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0016, seq=2/512, ttl=64 (request in 20)
24 3.700986397	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0016, seq=3/768, ttl=64 (reply in 25)
25 3.700986397	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0016, seq=3/768, ttl=64 (request in 24)
26 3.992260527	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0016, seq=4/1024, ttl=64 (reply in 27)
27 3.992260527	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0016, seq=4/1024, ttl=64 (request in 26)
32 5.363792194	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0016, seq=5/1280, ttl=64 (reply in 33)
33 5.363792194	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0016, seq=5/1280, ttl=64 (request in 32)
38 5.602849380	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0017, seq=1/256, ttl=64 (request in 39)
39 5.602849380	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0017, seq=1/256, ttl=64 (request in 38)
45 6.099583893	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0017, seq=2/512, ttl=64 (reply in 46)
46 6.099583893	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0017, seq=2/512, ttl=64 (request in 45)
58 7.600178928	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0017, seq=3/768, ttl=64 (reply in 59)
59 7.600178928	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0017, seq=3/768, ttl=64 (request in 58)
60 8.643890149	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0017, seq=4/1024, ttl=64 (request in 61)
61 8.643890149	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0017, seq=4/1024, ttl=64 (request in 60)
66 9.669228604	192.168.0.106	140.82.121.4	ICMP 142 Echo (ping) request id=0x0017, seq=5/1280, ttl=64 (reply in 67)
67 9.669228604	140.82.121.4	192.168.0.106	ICMP 142 Echo (ping) reply id=0x0017, seq=5/1280, ttl=64 (request in 66)
72 9.646563945	192.168.0.106	140.82.121.4	ICMP 298 Echo (ping) request id=0x0018, seq=1/256, ttl=64 (reply in 73)
73 9.646563945	140.82.121.4	192.168.0.106	ICMP 298 Echo (ping) reply id=0x0018, seq=1/256, ttl=64 (request in 72)
78 10.647593594	192.168.0.106	140.82.121.4	ICMP 298 Echo (ping) request id=0x0018, seq=2/512, ttl=64 (reply in 79)
79 10.647593594	140.82.121.4	192.168.0.106	ICMP 298 Echo (ping) reply id=0x0018, seq=2/512, ttl=64 (request in 78)
83 11.649058394	192.168.0.106	140.82.121.4	ICMP 298 Echo (ping) request id=0x0018, seq=3/768, ttl=64 (reply in 84)
84 11.649058394	140.82.121.4	192.168.0.106	ICMP 298 Echo (ping) reply id=0x0018, seq=3/768, ttl=64 (request in 83)
87 12.665128796	192.168.0.106	140.82.121.4	ICMP 298 Echo (ping) request id=0x0018, seq=4/1024, ttl=64 (reply in 88)
88 12.665128796	140.82.121.4	192.168.0.106	ICMP 298 Echo (ping) reply id=0x0018, seq=4/1024, ttl=64 (request in 87)
93 13.688063302	192.168.0.106	140.82.121.4	ICMP 298 Echo (ping) request id=0x0018, seq=5/1280, ttl=64 (reply in 94)
94 13.688063302	140.82.121.4	192.168.0.106	ICMP 298 Echo (ping) reply id=0x0018, seq=5/1280, ttl=64 (request in 93)
95 13.692098807	192.168.0.106	140.82.121.4	ICMP 554 Echo (ping) request id=0x0019, seq=1/256, ttl=64 (reply in 96)
96 13.692098807	140.82.121.4	192.168.0.106	ICMP 554 Echo (ping) reply id=0x0019, seq=1/256, ttl=64 (request in 95)
99 14.728663505	192.168.0.106	140.82.121.4	ICMP 554 Echo (ping) request id=0x0019, seq=2/512, ttl=64 (reply in 100)
100 14.728663505	140.82.121.4	192.168.0.106	ICMP 554 Echo (ping) reply id=0x0019, seq=2/512, ttl=64 (request in 99)
103 15.694881945	192.168.0.106	140.82.121.4	ICMP 554 Echo (ping) request id=0x0019, seq=3/768, ttl=64 (reply in 104)
104 15.694881945	140.82.121.4	192.168.0.106	ICMP 554 Echo (ping) reply id=0x0019, seq=3/768, ttl=64 (request in 103)
109 16.730257441	192.168.0.106	140.82.121.4	ICMP 554 Echo (ping) request id=0x0019, seq=4/1024, ttl=64 (reply in 110)
110 16.730257441	140.82.121.4	192.168.0.106	ICMP 554 Echo (ping) reply id=0x0019, seq=4/1024, ttl=64 (request in 109)
111 17.732999970	192.168.0.106	140.82.121.4	ICMP 554 Echo (ping) request id=0x0019, seq=5/1280, ttl=64 (reply in 112)
112 17.732999970	140.82.121.4	192.168.0.106	ICMP 554 Echo (ping) reply id=0x0019, seq=5/1280, ttl=64 (request in 111)
117 17.737011390	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=1/256, ttl=64 (reply in 118)
118 17.737011390	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=1/256, ttl=64 (request in 117)
121 18.737571197	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=2/512, ttl=64 (reply in 122)
122 18.737571197	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=2/512, ttl=64 (request in 121)
127 19.738635140	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=3/768, ttl=64 (reply in 128)
128 19.738635140	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=3/768, ttl=64 (request in 127)
131 20.739998442	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=4/1024, ttl=64 (reply in 132)
132 20.739998442	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=4/1024, ttl=64 (request in 131)
137 21.748998329	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=5/1280, ttl=64 (reply in 138)
138 21.748998329	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=5/1280, ttl=64 (request in 137)
143 21.780606181	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5323) [Reassembled in #144]
144 21.780606181	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) request id=0x001b, seq=1/256, ttl=64 (reply in 146)
145 21.815216846	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5374) [Reassembled in #146]
146 21.815216846	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) reply id=0x001b, seq=1/256, ttl=64 (request in 144)
149 22.781996306	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5387) [Reassembled in #150]
150 22.781996306	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) request id=0x001b, seq=2/512, ttl=64 (reply in 152)
151 22.817721904	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5477) [Reassembled in #154]
152 22.817721904	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) request id=0x001b, seq=2/512, ttl=64 (reply in 152)
153 23.783603791	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5477) [Reassembled in #154]

Действительно, видны ICMP-запросы и ответы.

Пакет без фрагментации (DON'T FRAGMENT):

137 21.740998329	192.168.0.106	140.82.121.4	ICMP 1066 Echo (ping) request id=0x001a, seq=5/1280, ttl=64 (reply in 138)
138 21.776396372	140.82.121.4	192.168.0.106	ICMP 1066 Echo (ping) reply id=0x001a, seq=5/1280, ttl=64 (request in 137)
143 21.780606181	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5323) [Reassembled in #144]
144 21.780606181	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) request id=0x001b, seq=1/256, ttl=64 (reply in 146)
145 21.815216846	140.82.121.4	192.168.0.106	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5374) [Reassembled in #146]
146 21.816066048	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) reply id=0x001b, seq=1/256, ttl=64 (request in 144)
149 22.781996306	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5387) [Reassembled in #150]
150 22.781996306	140.82.121.4	192.168.0.106	IPv4 610 Echo (ping) request id=0x001b, seq=2/512, ttl=64 (reply in 152)
151 22.817721904	140.82.121.4	192.168.0.106	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5477) [Reassembled in #154]
153 23.783603791	192.168.0.106	140.82.121.4	IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5477) [Reassembled in #154]

name 137: 1066 bytes on wire (8528 bits), 1066 bytes captured (8528 bits) on interface wlp0s20f3, id 0	Fr
Internet II, Src: Intel_8d:3e:d4 (dc:21:5c:8d:3e:d4), Dst: TplinkPte_50:c3:0f (98:25:4a:50:c3:0f)	Et
Ethernet Protocol Version 4, Src: 192.168.0.106, Dst: 140.82.121.4	En
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 1052	
Identification: 0x5320 (21280)	
010 = Flags: 0x2, Don't fragment	
0 = Reserved bit: Not set	
..1. = Don't fragment: Set	
..0. = More fragments: Not set	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 64	
Protocol: ICMP (1)	
Header Checksum: 0xd58 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.0.106	
Destination Address: 140.82.121.4	
[Stream index: 3]	

Пакет с фрагментацией (MORE FRAGMENTS):

143	21.780601819	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5323) [Reassembled in #144]
144	21.780606803	192.168.0.106	140.82.121.4	ICMP	610	Echo (ping) request id=0x001b, seq=1/256, ttl=64 (reply in 146)
145	21.815216846	140.82.121.4	192.168.0.106	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f374) [Reassembled in #146]
146	21.816066048	140.82.121.4	192.168.0.106	ICMP	610	Echo (ping) reply id=0x001b, seq=1/256, ttl=44 (request in 144)
149	22.781999095	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=538f) [Reassembled in #150]
150	22.781999095	192.168.0.106	140.82.121.4	ICMP	610	Echo (ping) request id=0x001b, seq=2/512, ttl=64 (reply in 152)
151	22.817721904	140.82.121.4	192.168.0.106	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f469) [Reassembled in #152]
152	22.818388507	140.82.121.4	192.168.0.106	ICMP	610	Echo (ping) reply id=0x001b, seq=2/512, ttl=44 (request in 150)
153	23.783603791	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=547f) [Reassembled in #154]

Frame 143: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: Intel_8d:3e:d4 (dc:21:5c:8d:3e:d4), Dst: TplinkPte_50:c3:0f (98:25:4a:50:c3:0f)
 Internet Protocol Version 4, Src: 192.168.0.106, Dst: 140.82.121.4
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 1500
 Identification: 0x5323 (21283)
 001. = Flags: 0x1, More fragments
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..1. = More fragments: Set
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: ICMP (1)
 Header Checksum: 0x3b95 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.0.106
 Destination Address: 140.82.121.4
 [Reassembled IPv4 in frame: 144]
 [Stream index: 3]

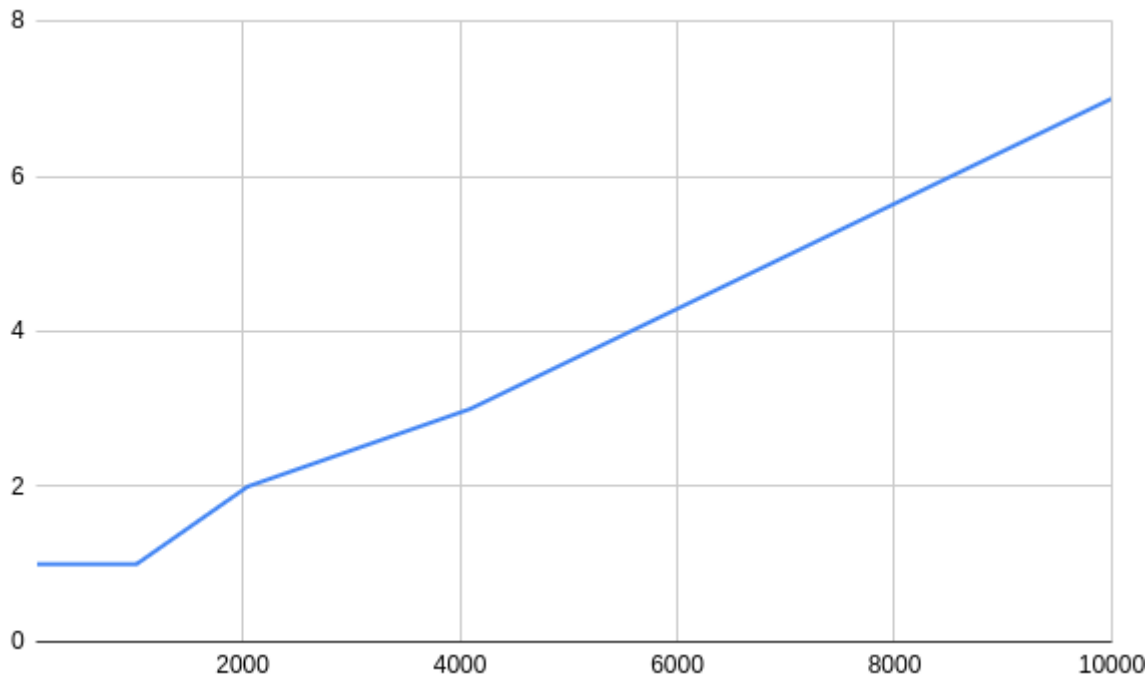
Пакет с фрагментацией, который означает конец потока (не установлены флаги):

143	21.780601819	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5323) [Reassembled in #144]
144	21.780606803	192.168.0.106	140.82.121.4	ICMP	610	Echo (ping) request id=0x001b, seq=1/256, ttl=64 (reply in 146)
145	21.815216846	140.82.121.4	192.168.0.106	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f374) [Reassembled in #146]
146	21.816066048	140.82.121.4	192.168.0.106	ICMP	610	Echo (ping) reply id=0x001b, seq=1/256, ttl=44 (request in 144)
149	22.781999095	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=538f) [Reassembled in #150]
150	22.781999095	192.168.0.106	140.82.121.4	ICMP	610	Echo (ping) request id=0x001b, seq=2/512, ttl=64 (reply in 152)
151	22.817721904	140.82.121.4	192.168.0.106	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=f469) [Reassembled in #152]
152	22.818388507	140.82.121.4	192.168.0.106	ICMP	610	Echo (ping) reply id=0x001b, seq=2/512, ttl=44 (request in 150)
153	23.783603791	192.168.0.106	140.82.121.4	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=547f) [Reassembled in #154]

Frame 144: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: Intel_8d:3e:d4 (dc:21:5c:8d:3e:d4), Dst: TplinkPte_50:c3:0f (98:25:4a:50:c3:0f)
 Internet Protocol Version 4, Src: 192.168.0.106, Dst: 140.82.121.4
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 596
 Identification: 0x5323 (21283)
 000. = Flags: 0x0
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 1011 1001 = Fragment Offset: 1480
 Time to Live: 64
 Protocol: ICMP (1)
 Header Checksum: 0x5e64 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.0.106
 Destination Address: 140.82.121.4
 [2 IPv4 Fragments (2056 bytes): #143(1480), #144(576)]
 [Stream index: 3]

Итого, макс. размер ICMP без разбиения (опытным путем) - 1472 байта.

Зависимость кол-ва фрагментов от размера сообщения:



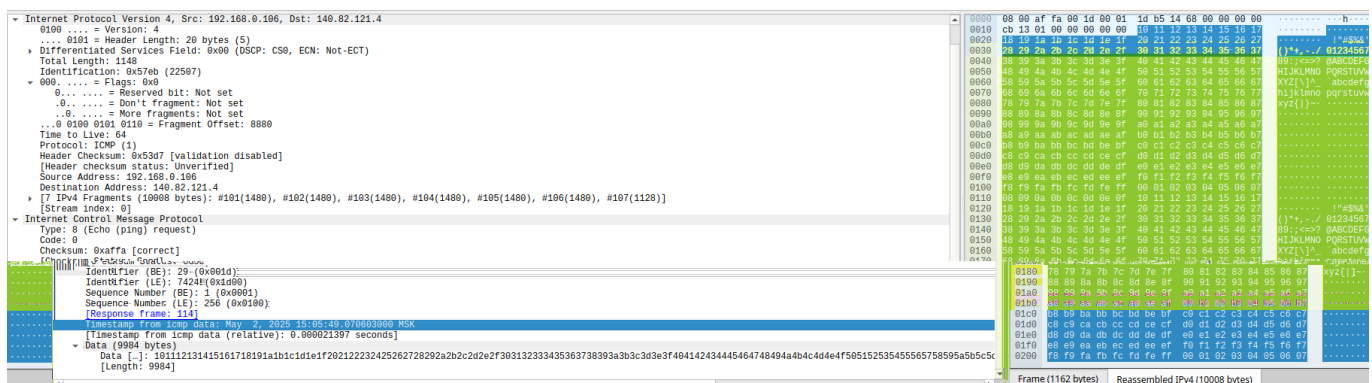
Изменить TTL можно параметром `-t`:

```
-t <tll> define time to live
```

Пример:

```
$ ping -c 1 -t 2 -s 1470 github.com
PING github.com (140.82.121.3) 1470(1498) bytes of data.
From 10.40.86.1 icmp_seq=1 Time to live exceeded
--- github.com ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

В данных может лежать что угодно (главное, чтобы в ответ пришло ровно то, что отправлялось), но есть и определенные реализации, которые задают формат.



Анализ трафика утилиты tracert (traceroute)

Traceroute — служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP.

Может использовать ICMP, TCP, UDP, GRE по своему усмотрению. Можно настроить.

Принцип работы traceroute - каждый раз, когда роутер пересылает сообщение дальше, он уменьшает TTL (в IP) на один. Соответственно, traceroute последовательно отправляет запросы со все растущим TTL. На первый запрос (TTL=1) вернет ответ 1 роутер с TTL **Exceeded**. Потом отправится второй пакет, с TTL=2, на который с TTL **Exceeded** ответит второй роутер и т.д. Делает он так по умолчанию 3 раза (3 попытки для каждого TTL) - потому и 3 колонки времени.

* * * в выводе означают, что на этом TTL он превысил время ожидания ответа - либо никто не ответил, либо роутер умеет распознавать такие "простуки".

Флаг **-n**:

-n Do not resolve IP addresses to their domain names

```
$ sudo traceroute -n github.com
traceroute to github.com (140.82.121.3), 30 hops max, 60 byte packets
 1  192.168.0.1    2.938 ms  2.912 ms  2.905 ms
 2  10.40.86.1     2.536 ms  2.529 ms  2.522 ms
 3  10.37.131.141  3.109 ms  3.102 ms  3.096 ms
 4  10.37.254.110  3.090 ms  3.084 ms  4.797 ms
 5  10.37.5.165    4.849 ms  4.843 ms  4.837 ms
 6  10.37.2.69     3.829 ms  3.144 ms  3.128 ms
 7  10.37.5.85     3.277 ms  2.921 ms  2.880 ms
 8  10.37.129.190  3.547 ms  3.470 ms  3.460 ms
 9  194.68.128.180 13.232 ms 13.210 ms 13.203 ms
10  94.103.180.71  34.187 ms 33.320 ms 33.444 ms
11  94.103.180.3   34.251 ms 34.244 ms 33.989 ms
12  94.103.180.2   33.981 ms 34.509 ms 34.500 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  94.103.180.24  33.284 ms 33.272 ms 33.758 ms
18  45.153.82.37   33.823 ms 33.833 ms 45.153.82.39 33.804 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

A hop that outputs * * * means that the router at that hop doesn't respond to the type of packet you were using for the traceroute.

No.	Time	Source	Destination	Protocol	Length	TTL	custom	Info
0	0.000000000	192.168.0.106	20.42.65.84	TCP	66	64	47448	Seq=1 Ack=1 Win=501 Len=0 TSval=1159102793 TSecr=624443162
2	0.231263875	20.42.65.84	192.168.0.106	TCP	66	104	TCP ACKed unseen segment	443 → 47448 [ACK] Seq=1 Ack=2 Win=16381 Len=0 TSval=6244480114 TSecr=1159056952
3	3.326068637	192.168.0.106	192.168.0.1	DNS	70			64 Standard query 0xb6a6 A github.com
4	3.330000000	192.168.0.1	192.168.0.1	DNS	70			64 Standard query response 0xb6a6 A github.com
5	3.330000000	192.168.0.1	192.168.0.1	DNS	96			64 Standard query response 0xb6a6 A github.com
6	3.330130442	192.168.0.1	192.168.0.106	DNS	164			57 Standard query response 0xb6a6 AAAA github.com SOA ns=1707.awsdns-21.co.uk
7	3.330547837	192.168.0.106	140.82.121.4	UDP	74	1	52676	→ 33434 Len=32
8	3.330586897	192.168.0.106	140.82.121.4	UDP	74	1	34499	→ 33435 Len=32
9	3.330602909	192.168.0.106	140.82.121.4	UDP	74	1	37966	→ 33436 Len=32
10	3.330614109	192.168.0.106	140.82.121.4	UDP	74	1	49706	→ 33437 Len=32
11	3.330627313	192.168.0.106	140.82.121.4	UDP	74	1	243572	→ 33438 Len=32
12	3.330638832	192.168.0.106	140.82.121.4	UDP	74	1	243852	→ 33439 Len=32
13	3.330652897	192.168.0.106	140.82.121.4	UDP	74	1	355221	→ 33440 Len=32
14	3.330663185	192.168.0.106	140.82.121.4	UDP	74	1	338968	→ 33441 Len=32
15	3.330674583	192.168.0.106	140.82.121.4	UDP	74	1	32806	→ 33442 Len=32
16	3.330680274	192.168.0.106	140.82.121.4	UDP	74	1	435571	→ 33443 Len=32
17	3.330690278	192.168.0.106	140.82.121.4	UDP	74	1	344186	→ 33444 Len=32
18	3.330711561	192.168.0.106	140.82.121.4	UDP	74	1	457735	→ 33445 Len=32
19	3.330720011	192.168.0.106	140.82.121.4	UDP	74	1	541010	→ 33446 Len=32
20	3.330733234	192.168.0.106	140.82.121.4	UDP	74	1	52639	→ 33447 Len=32
21	3.330746692	192.168.0.106	140.82.121.4	UDP	74	1	52377	→ 33448 Len=32
22	3.330750056	192.168.0.106	140.82.121.4	UDP	74	1	635808	→ 33449 Len=32
23	3.330746593	192.168.0.106	192.168.0.106	ICMP	70	254	1	Time-to-live exceeded (Time to live exceeded in transit)
24	3.332974129	192.168.0.106	192.168.0.106	ICMP	70	254	1	Time-to-live exceeded (Time to live exceeded in transit)
25	3.333052928	192.168.0.106	140.82.121.4	UDP	74	1	654464	→ 33450 Len=32
26	3.333062363	192.168.0.106	140.82.121.4	UDP	74	1	655118	→ 33451 Len=32
27	3.333101514	192.168.0.106	192.168.0.106	ICMP	70	254	1	Time-to-live exceeded (Time to live exceeded in transit)
28	3.333201242	192.168.0.106	140.82.121.4	UDP	74	1	750833	→ 33452 Len=32
29	3.333371522	192.168.0.1	192.168.0.106	ICMP	102	64	1	Time-to-live exceeded (Time to live exceeded in transit)
30	3.333377582	192.168.0.1	192.168.0.106	ICMP	102	64	1	Time-to-live exceeded (Time to live exceeded in transit)
31	3.333377611	192.168.0.1	192.168.0.106	ICMP	102	64	1	Time-to-live exceeded (Time to live exceeded in transit)
32	3.333482001	192.168.0.106	192.168.0.106	ICMP	70	250	1	Time-to-live exceeded (Time to live exceeded in transit)
33	3.334207991	192.168.0.106	192.168.0.1	DNS	83			64 Standard query 0x7387 PTR 1.86.40.10.in-addr.arpa
34	3.334303213	192.168.0.1	192.168.0.106	ICMP	102	64	1	Time-to-live exceeded (Time to live exceeded in transit)
35	3.334303213	192.168.0.106	192.168.0.106	ICMP	102	64	1	Time-to-live exceeded (Time to live exceeded in transit)
36	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
37	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
38	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
39	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
40	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
41	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
42	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
43	3.334509052	192.168.0.106	192.168.0.106	ICMP	70	253	1	Time-to-live exceeded (Time to live exceeded in transit)
44	3.336884275	192.168.0.1	192.168.0.106	DNS	118			57 Standard query response 0x7387 No such name PTR 1.86.40.10.in-addr.arpa SOA 10.in-addr.arpa
45	3.336944105	192.168.0.106	140.82.121.4	UDP	74	1	741937	→ 33453 Len=32
46	3.336954206	192.168.0.106	140.82.121.4	UDP	74	1	747919	→ 33454 Len=32
47	3.336963729	192.168.0.106	140.82.121.4	UDP	74	1	841148	→ 33455 Len=32
48	3.336969686	192.168.0.106	140.82.121.4	UDP	74	1	835179	→ 33456 Len=32
49	3.337112290	192.168.0.106	192.168.0.1	DNS	86			64 Standard query 0x8016 PTR 141.131.37.10.in-addr.arpa
50	3.339971760	192.168.0.106	192.168.0.106	ICMP	70	251	1	Time-to-live exceeded (Time to live exceeded in transit)
51	3.339971828	192.168.0.106	192.168.0.106	ICMP	70	251	1	Time-to-live exceeded (Time to live exceeded in transit)
52	3.339972000	192.168.0.106	192.168.0.106	ICMP	70	251	1	Time-to-live exceeded (Time to live exceeded in transit)
53	3.339955105	192.168.0.106	192.168.0.106	ICMP	70	249	1	Time-to-live exceeded (Time to live exceeded in transit)
54	3.339955334	192.168.0.106	192.168.0.106	ICMP	70	249	1	Time-to-live exceeded (Time to live exceeded in transit)
55	3.339969474	192.168.0.106	192.168.0.106	ICMP	70	248	1	Time-to-live exceeded (Time to live exceeded in transit)

Как видно, у последующих запросов растет TTL - для того, чтобы "достать" до все более дальнего и дальнего роутера.

Основное отличие traceroute и ping с точки зрения ICMP - что у traceroute при каждой итерации увеличивается TTL.

Если убрать **-n**, то дополнительно будет идти DNS-трафик.

Анализ HTTP-трафика

Записанный трафик:

No	Time	Source	Destination	Protocol	Length	TTL	custom	Info
21	1.46354339	192.168.0.106	172.64.41.4	HTTP2	164			64 Magic, SETTINGS[0], WINDOW_UPDATE[0]
22	1.468030802	172.64.41.4	192.168.0.106	HTTP2	137			53 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
30	1.468049379	192.168.0.106	172.64.41.4	HTTP2	248			64 HEADERS[3]: POST /dns-query
31	1.468049394	192.168.0.106	172.64.41.4	DNS	650			64 Standard query 0x0000 HTTPS github.com OPT, Standard query 0x0000 AAAA github.com OPT, Standard query 0x0000 A github.com OPT
32	1.472897668	172.64.41.4	192.168.0.106	HTTP2	191			53 WINDOW_UPDATE[3]
33	1.474269951	172.64.41.4	192.168.0.106	DNS	585			53 Standard query response 0x0000 HTTPS github.com SOA dns.p8l.nsone.net OPT
34	1.474269951	172.64.41.4	192.168.0.106	HTTP2	122			53 HEADERS[3]: 200 OK
35	1.474269951	172.64.41.4	192.168.0.106	DNS	585			53 Standard query response 0x0000 AAAA github.com SOA ns-1707.awsdns-21.co.uk OPT
36	1.474269951	172.64.41.4	192.168.0.106	HTTP2	122			53 HEADERS[7]: 200 OK
37	1.474269951	172.64.41.4	192.168.0.106	DNS	585			53 Standard query response 0x0000 A github.com A 140.82.121.4 OPT
40	1.475727289	192.168.0.106	172.64.41.4	HTTP2	122			64 HEADERS[3]: POST /dns-query
41	1.475727289	192.168.0.106	172.64.41.4	DNS	225			64 Standard query 0x0000 AAAA github.com OPT
44	1.476219981	192.168.0.106	172.64.41.4	DNS	280			64 Standard query 0x0000 A github.com OPT
45	1.480590931	172.64.41.4	192.168.0.106	HTTP2	122			53 HEADERS[3]: 200 OK
46	1.480590931	172.64.41.4	192.168.0.106	DNS	585			53 Standard query response 0x0000 AAAA github.com SOA ns-1707.awsdns-21.co.uk OPT
47	1.481258472	172.64.41.4	192.168.0.106	HTTP2	122			53 HEADERS[3]: 200 OK
50	1.481258472	172.64.41.4	192.168.0.106	DNS	585			53 Standard query response 0x0000 A github.com A 140.82.121.4 OPT
80	1.553049607	192.168.0.106	140.82.121.4	HTTP2	158			64 Magic, SETTINGS[0], WINDOW_UPDATE[0]
81	1.553049607	140.82.121.4	192.168.0.106	HTTP2	133			44 SETTINGS[0], SETTINGS[0]
92	1.585737960	192.168.0.106	140.82.121.4	HTTP2	97			64 SETTINGS[0]
94	1.585737960	140.82.121.4	192.168.0.106	HTTP2	576			44 HEADERS[3]: 200 OK[TLIS segment of a reassembled PDU]
104	1.585737960	140.82.121.4	192.168.0.106	TLISv1	3	2914		44 DATA[3]
113	1.585737960	140.82.121.4	192.168.0.106	TLISv1	3	2914		44 DATA[3]
132	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	2914		44 DATA[3]
133	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	2914		44 DATA[3]
142	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
151	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
152	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
153	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
154	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
155	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
156	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
157	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
158	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
159	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
160	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
161	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
162	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
163	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
164	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
165	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
166	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
167	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
168	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
169	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
170	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
171	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
172	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
173	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
174	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
175	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
176	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
177	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
178	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
179	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
180	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
181	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
182	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
183	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
184	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
185	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
186	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
187	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
188	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
189	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
190	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
191	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
192	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
193	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
194	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
195	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
196	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
197	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
198	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
199	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
200	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
201	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
202	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
203	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
204	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
205	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
206	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
207	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
208	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
209	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
210	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
211	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
212	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
213	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
214	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
215	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
216	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
217	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
218	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
219	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
220	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
221	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
222	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
223	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
224	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
225	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
226	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
227	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
228	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
229	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
230	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
231	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
232	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
233	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
234	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
235	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
236	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
237	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
238	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
239	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
240	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
241	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
242	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
243	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
244	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
245	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		44 DATA[3]
246	2.015686443	140.82.121.4	192.168.0.106	TLISv1	3	841		

87	1.551919523	192.168.0.106	140.82.121.4	HTTP2	1483	64	HEADERS[3]: GET /sultanowski1, WINDOW_UPDATE[3]
91	1.585667180	140.82.121.4	192.168.0.106	HTTP2	130	44	SETTINGS[0], SETTINGS[0]
92	1.585737960	192.168.0.106	140.82.121.4	HTTP2	97	64	SETTINGS[0]
94	1.946348605	140.82.121.4	192.168.0.106	HTTP2	5762	44	HEADERS[3]: 200 OK[TLS segment of a reassembled PDU]
104	1.980538376	140.82.121.4	192.168.0.106	TLSpv1.3	2914	44	DATA[3]
113	1.981786278	140.82.121.4	192.168.0.106	TLSpv1.3	2914	44	DATA[3]
132	2.015666443	140.82.121.4	192.168.0.106	TLSpv1.3	2914	44	DATA[3]
133	2.015666515	140.82.121.4	192.168.0.106	HTTP2	2914	44	DATA[3][TLS segment of a reassembled PDU]
142	2.016455477	140.82.121.4	192.168.0.106	TLSpv1.3	841	44	DATA[3], DATA[3] (text/html)

1280	0.380076197	192.168.0.106	140.82.121.4	HTTP2	1471	64	HEADERS[11]: GET /sultanowski/, WINDOW_UPDATE[11]
1282	0.933838779	140.82.121.4	192.168.0.106	HTTP2	7738	44	HEADERS[11]: 200 OK, DATA[11]
1288	0.933920269	140.82.121.4	192.168.0.106	TLSv1.3	4338	44	[TLS segment of a reassembled PDU]
1293	0.933945921	140.82.121.4	192.168.0.106	TLSv1.3	1260	44	DATA[11]
1301	0.934127961	140.82.121.4	192.168.0.106	TLSv1.3	3907	44	DATA[11]
1303	0.934128010	140.82.121.4	192.168.0.106	HTTP2	1490	44	DATA[11]
1310	0.934636207	140.82.121.4	192.168.0.106	TLSv1.3	4108	44	DATA[11], DATA[11] (text/html)

```

Frame 1282: 7738 bytes on wire (61904 bits), 7738 bytes captured (61904 bits) on interface wlp92s0f3, id 0
  Ethernet II, Src: TpLinkPcs:50:c3:0f, Dst: IntelBd:8e:3d4 (dc:21:5c:8d:3e:4)
  Internet Protocol Version 4, Src: 140.82.121.4, Dst: 192.168.0.106
    .... : Version: 4
    .... : Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 7724
    Identification: 6x2740 (10945)
    Flags: 0x02, Don't fragment
    0 .... : Reserved bit: Not set
    0 .... : Don't fragment: Not set
    0 .... : More fragments: Not set
    0x00 0000 0000 0000 = Fragment offset: 0
    0x00 0000 0000 0000 = Fragment offset: 0
    Protocol: TCP (6)
    Seq Number: 94322 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.82.121.4
    Destination Address: 192.168.0.106
    [Stream index: 4]
  Transmission Control Protocol, Src Port: 443, Dst Port: 44936, Seq: 143550, Ack: 7107, Len: 7672
    Source Port: 443
    Destination Port: 44936
    [Stream index: 6]
    [TCP Sequence Number: 142]
    [Conversation completeness: Incomplete, DATA (15)]
    TCP Sequence Len: 7672
    Sequence Number: 143550 (relative sequence number)
    Sequence Number (raw): 325851990
    Next Sequence Number: 151231 (relative sequence number)
    Acknowledgment Number: 7107 (relative ack number)

```

172.64.41.4 - Cloudflare, CDN. Прежде, чем "дать доступ" к Github, Cloudflare анализирует трафик и только потом "пропускает", давая IP-адрес и сетевой доступ.

[illegible]

- 1

Виды DNS-записей:

- **A:** IPv4-адрес
- **AAAA:** IPv6 адрес
- **CNAME:** форвардинг с поддомена/домена на поддомен (mail.yandex.ru)
- **MX:** направляет письмо на email-сервер
- **TXT:** произвольные текстовые заметки
- **SOA:** информация о поддомене
- **SRV:** указание порта для специфичных сервисов
- **NS:** указание NS-сервера, ответственного за определенное имя

Анализ ARP-трафика

```
$ sudo arp -d 192.168.0.1
$
```

Как видно, при попытке "сходить в интернет", отсылается (от компьютера [192.168.0.106](#)) ARP-запрос (2) на поиск роутера [192.168.0.1](#). После - роутер отвечает ([192.168.0.1](#)).

No.	Time	Source	Destination	Protocol	Length	TTL custom	Info
1	0.000000000	TpLinkPte_50:c3:0f	Broadcast	ARP	42		Who has 192.168.0.124? Tell 192.168.0.1
2	3.653372171	Intel_8d:3e:d4	Broadcast	ARP	42		Who has 192.168.0.1? Tell 192.168.0.106
3	3.656225468	TpLinkPte_50:c3:0f	Intel_8d:3e:d4	ARP	42		192.168.0.1 is at 98:25:4a:50:c3:0f
4	11.980697747	TpLinkPte_50:c3:0f	Broadcast	ARP	42		Who has 192.168.0.124? Tell 192.168.0.1
5	13.004739789	TpLinkPte_50:c3:0f	Broadcast	ARP	42		Who has 192.168.0.124? Tell 192.168.0.1
6	14.028565212	TpLinkPte_50:c3:0f	Broadcast	ARP	42		Who has 192.168.0.124? Tell 192.168.0.1

ARP-запрос:

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Intel_8d:3e:d4 (dc:21:5c:8d:3e:d4)
  Sender IP address: 192.168.0.106
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.1
```

Он содержит адрес отправителя, чтобы за меньшее число операций у других участников сети появилась информация об этом устройстве. К тому же, если бы не было этого поля, то коммутатор просто не смог бы обучаться.

Вывод

В данной лабораторной работе была произведена запись сетевого трафика с помощью утилиты Wireshark. Я записал трафик утилит ping, tracert, а также запросов в веб-браузере. Были на практике проанализированы протоколы ICMP, UDP, IP, DNS, HTTP, ARP.