

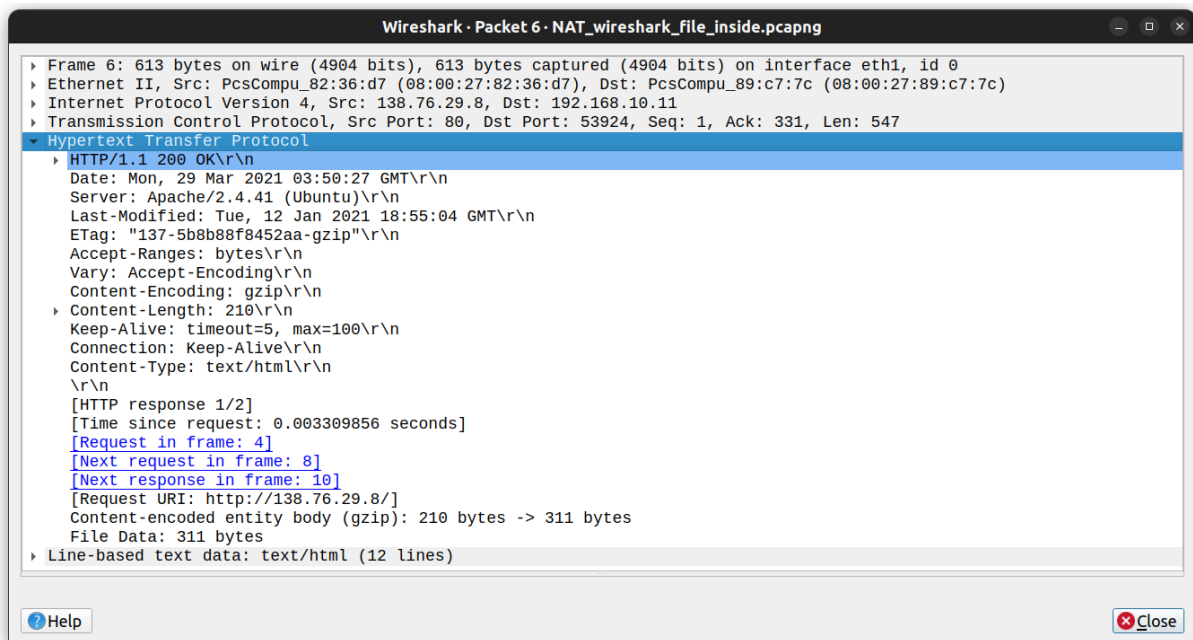
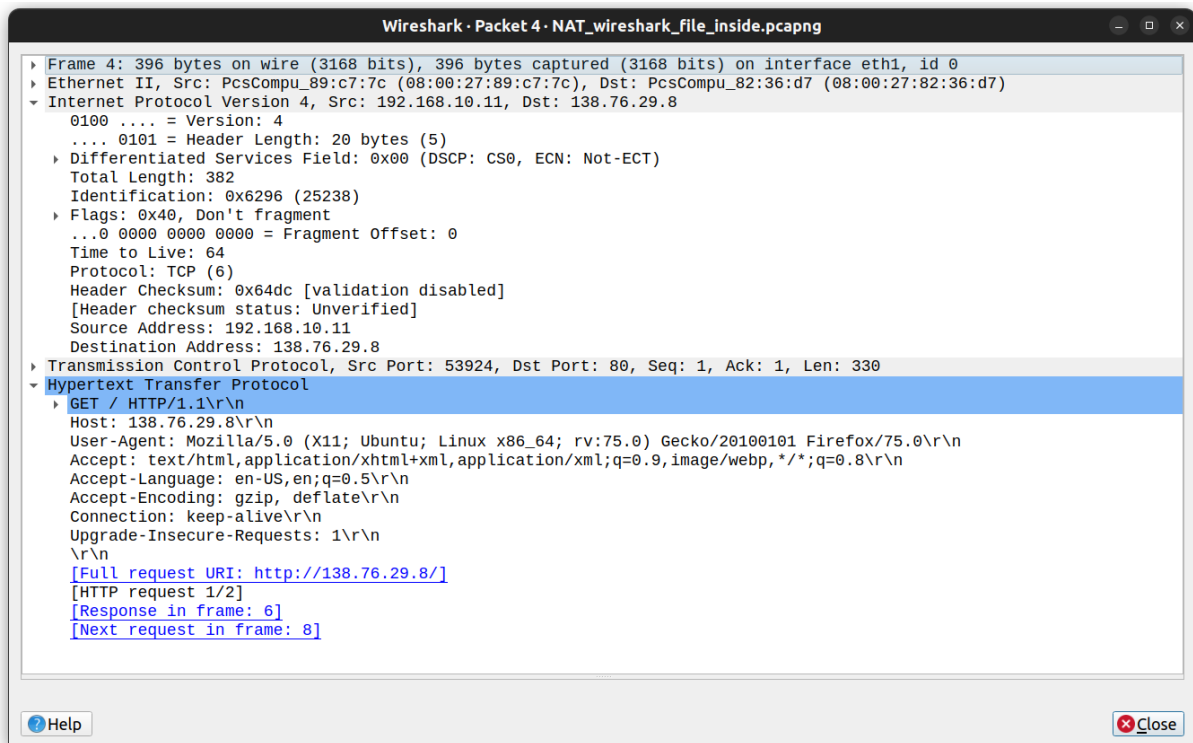
Сценарий измерения NAT

Будем захватывать пакеты, содержащие простое сообщение с запросом HTTP GET от клиента внутри домашней сети к удаленному серверу и соответствующий HTTP-ответ от этого сервера. В домашней сети маршрутизатор домашней сети предоставляет услугу NAT. Перехватываем пакеты в двух местах, и, таким образом, есть два файла трассировки: пакеты, полученные на стороне локальной сети (LAN) маршрутизатора NAT, и пакеты, пересылаемые маршрутизатором NAT на стороне, обращенной к Интернету. Сначала посмотрим, что происходит на стороне LAN маршрутизатора NAT.

The image shows a Wireshark packet capture window titled "NAT_wireshark_file_inside.pcapng". The packet list on the left shows a series of packets. Packet 6 is highlighted, showing an HTTP GET request from 138.76.29.8 to 192.168.10.11. The packet details pane on the right shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=322727249 TSecr=0 WS=128
2	0.002891700	138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=802266926 TSecr=5
3	0.002870917	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029390199	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031464845	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232896589	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233703166	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	0.189772327	PcsCompu_82:c7:...	PcsCompu_89:c7:7c	ARP	42	Who has 192.168.10.11? Tell 192.168.10.254
13	0.191799501	PcsCompu_89:c7:...	PcsCompu_82:c7:7c	ARP	60	192.168.10.11 is at 08:00:27:89:c7:7c
14	0.234545253	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
15	0.234709589	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
16	0.236143161	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
17	0.238485288	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484
18	0.241721585	PcsCompu_89:c7:...	PcsCompu_82:c7:7c	ARP	60	Who has 192.168.10.254? Tell 192.168.10.11
19	0.241747598	PcsCompu_82:c7:...	PcsCompu_89:c7:7c	ARP	42	192.168.10.254 is at 08:00:27:82:36:d7

Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_82:c7:7c (08:00:27:82:36:d7), Dst: PcsCompu_89:c7:7c (08:00:27:89:c7:7c)
Internet Protocol Version 4, Src: 138.76.29.8, Dst: 192.168.10.11
... .. = Version: 4
... .. 0101 = Header Length: 20 bytes (5)
... .. Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 599
Identification: 0x6c7c (27772)
Flags: 0x40, Don't fragment
... .. 0000 0000 0000 = Fragment Offset: 0
Time to Live: 62
Protocol: TCP (6)
Header Checksum: 0x5c1d [validation disabled]
[Header checksum status: Unverified]
Source Address: 138.76.29.8
Destination Address: 192.168.10.11
Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547
Frame (613 bytes) | Uncompressed entity body (311 bytes)
NAT_wireshark_file_inside.pcapng
Packets: 19 - Displayed: 19 (100.0%)
Profile: Default



1. Каков IP-адрес клиента, отправляющего HTTP-запрос GET? Каков номер исходного порта сегмента TCP в этой дейтаграмме, содержащей запрос HTTP GET? Каков IP-адрес назначения этого запроса HTTP GET? Каков номер порта назначения сегмента TCP в этой дейтаграмме, содержащей запрос HTTP GET?

- IP-адрес источника - 192.168.10.11
- Исходный TCP-порт - 53924
- IP-адрес получателя - 138.76.29.8
- TCP-порт назначения - 80

2. В какое время пересылается соответствующее сообщение HTTP 200 OK с веб-сервера маршрутизатором NAT клиенту на стороне маршрутизатора в локальной сети?

- Через 0.030672101s от начала трассировки пересылается сообщение HTTP OK

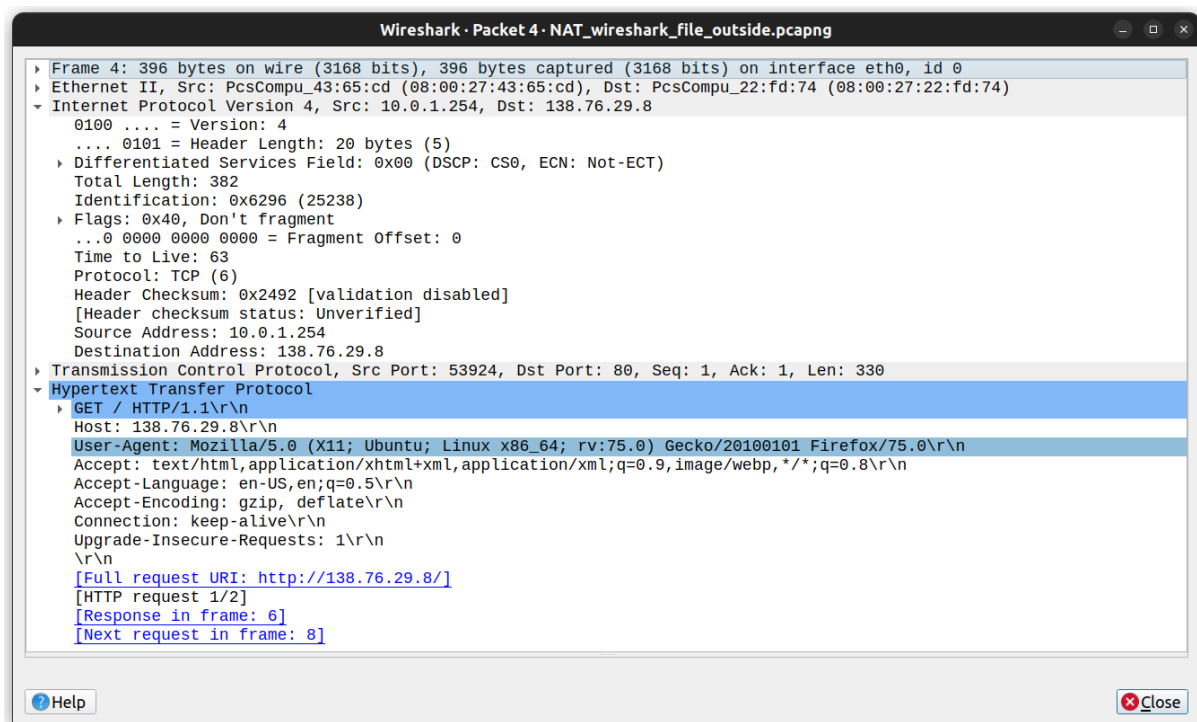
3. Каковы IP-адреса источника и получателя, а также TCP-порты источника и получателя в дейтаграмме IP, несущей это сообщение HTTP 200 OK?

- IP-адрес источника - 138.76.29.8
- Исходный TCP-порт - 80
- IP-адрес получателя - 192.168.10.11
- TCP-порт назначения - 53924

Далее мы сосредоточимся на этих двух сообщениях HTTP (GET и 200 OK). Наша цель ниже будет заключаться в том, чтобы найти эти два HTTP-сообщения в файле трассировки, захваченном на интернет-канале между маршрутизатором и провайдером.

Поскольку захваченные пакеты, направляющиеся к серверу, уже были перенаправлены через маршрутизатор NAT, некоторые IP-адреса и номера портов будут изменены в результате преобразования NAT.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000s	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=322727249 TSecr=0 WS=128
2	0.002058086s	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=802266926 TSecr=3
3	0.002853940s	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.002859221s	138.76.29.8	10.0.1.254	HTTP	396	GET /favicon.ico HTTP/1.1
5	0.029338911s	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030625966s	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670s	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231400190s	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863610s	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233043313s	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (text/html)
11	0.233687113s	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	5.189837924s	PcsCompu_43:65:...	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 10.0.1.254
13	5.191700729s	PcsCompu_43:65:...	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:22:fd:74
14	5.231662506s	PcsCompu_22:fd:...	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10.0.1.253
15	5.231707677s	PcsCompu_43:65:...	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:43:65:cd
16	5.234487950s	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
17	5.234707098s	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
18	5.236144603s	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ack=1030 Win=64128 Len=0 TSval=322732485 TSecr=802272150
19	5.238001105s	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1030 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484



4. В какое время это сообщение HTTP GET появляется в файле трассировки, захваченном на интернет-канале между маршрутизатором и провайдером?
- Через 0.027356291s от начала трассировки отправляется сообщение HTTP GET
5. Каковы IP-адреса источника и получателя, а также номера TCP-портов источника и получателя в дейтаграмме IP, несущей этот HTTP GET?
- IP-адрес источника - 10.0.1.254
 - Исходный TCP-порт - 53924
 - IP-адрес получателя - 138.76.29.8
 - TCP-порт назначения - 80
6. Какое из этих четырех полей отличается от вашего ответа на вопрос 1 выше?
- Отличается IP-адрес источника
7. Изменились ли какие-либо поля в сообщении HTTP GET?
- Поля в сообщении HTTP GET остались неизменны
8. Какие из следующих полей в IP-датаграмме, содержащей HTTP GET, изменены с дейтаграммы, полученной в локальной сети, на соответствующую дейтаграмму, пересылаемую на стороне Интернета маршрутизатора NAT: *Version*, *Header Length*, *Flags*, *Checksum*?
- Изменилось значение поля *Checksum*, т.к. изменился IP-адрес источника

Найдите ответ HTTP, содержащий сообщение «200 OK», которое было получено в ответ на запрос HTTP GET, который вы только что рассмотрели в вопросах 4–8 выше.

NAT_wireshark_file_outside.pcapng					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-F>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.1.254	138.76.29.8	TCP	74 53924 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=322727249 TSecr=0 WS=128
2	0.002058086	138.76.29.8	10.0.1.254	TCP	74 80 → 53924 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=802266926 TSecr=
3	0.002853949	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=322727252 TSecr=802266926
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396 GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=1 Ack=331 Win=64896 Len=0 TSval=802266954 TSecr=322727277
6	0.030425053	138.76.29.8	10.0.1.254	HTTP	613 HTTP/1.1 200 OK (text/html)
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=331 Ack=548 Win=64128 Len=0 TSval=322727281 TSecr=802266955
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317 GET /favicon.ico HTTP/1.1
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=548 Ack=582 Win=64768 Len=0 TSval=802267157 TSecr=322727481
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555 HTTP/1.1 404 Not Found (text/html)
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322727483 TSecr=802267158
12	5.189837924	PcsCompu_43:65:...	PcsCompu_22:fd:74	ARP	42 Who has 10.0.1.253? Tell 10.0.1.254
13	5.191709729	PcsCompu_22:fd:...	PcsCompu_43:65:cd	ARP	60 10.0.1.253 is at 08:00:27:22:fd:74
14	5.231662506	PcsCompu_22:fd:...	PcsCompu_43:65:cd	ARP	60 Who has 10.0.1.254? Tell 10.0.1.253
15	5.231707677	PcsCompu_43:65:...	PcsCompu_22:fd:74	ARP	42 10.0.1.254 is at 08:00:27:43:65:cd
16	5.234487950	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [FIN, ACK] Seq=1037 Ack=582 Win=64768 Len=0 TSval=802272158 TSecr=322727483
17	5.234707098	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [FIN, ACK] Seq=582 Ack=1037 Win=64128 Len=0 TSval=322732484 TSecr=802267158
18	5.236144683	10.0.1.254	138.76.29.8	TCP	66 53924 → 80 [ACK] Seq=583 Ack=1038 Win=64128 Len=0 TSval=322732485 TSecr=802272158
19	5.238001105	138.76.29.8	10.0.1.254	TCP	66 80 → 53924 [ACK] Seq=1038 Ack=583 Win=64768 Len=0 TSval=802272161 TSecr=322732484

Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0
 Frame (613 bytes) uncompressed entity body (311 bytes)

NAT_wireshark_file_outside.pcapng Packets: 19 · Displayed: 19 (100.0%) Profile: Default

Wireshark · Packet 6 · NAT_wireshark_file_outside.pcapng	
▶ Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0 ▶ Ethernet II, Src: PcsCompu_22:fd:74 (08:00:27:22:fd:74), Dst: PcsCompu_43:65:cd (08:00:27:43:65:cd) ▶ Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254	
0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 599 Identification: 0x6c7c (27772) ▶ Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 63 Protocol: TCP (6) Header Checksum: 0x19d3 [validation disabled] [Header checksum status: Unverified] Source Address: 138.76.29.8 Destination Address: 10.0.1.254	▶ Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547 ▶ Hypertext Transfer Protocol ▶ HTTP/1.1 200 OK\r\n Date: Mon, 29 Mar 2021 03:50:27 GMT\r\n Server: Apache/2.4.41 (Ubuntu)\r\n Last-Modified: Tue, 12 Jan 2021 18:55:04 GMT\r\n ETag: "137-5b8b88f8452aa-gzip"\r\n Accept-Ranges: bytes\r\n Vary: Accept-Encoding\r\n Content-Encoding: gzip\r\n ▶ Content-Length: 210\r\n Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n Content-Type: text/html\r\n \r\n [HTTP response 1/2] [Time since request: 0.003269675 seconds] [Request in frame: 4] [Next request in frame: 8] [Next response in frame: 10] [Request URI: http://138.76.29.8/] Content-encoded entity body (gzip): 210 bytes -> 311 bytes File Data: 311 bytes ▶ Line-based text data: text/html (12 lines)

Help Close

9. В какое время появляется это сообщение в файле трассировки?

- Через 0.030625966s от начала трассировки пересылается сообщение HTTP OK

10. Каковы IP-адреса источника и получателя и номера TCP-портов источника и получателя в дейтаграмме IP, несущей это сообщение HTTP-ответа («200 OK»)?

- IP-адрес источника - 138.76.29.8
- Исходный TCP-порт - 80
- IP-адрес получателя - 10.0.1.254
- TCP-порт назначения - 53924