

Тестовый запуск Wireshark

Wireshark interface showing a packet capture of a trace file (trace file.pcapng). The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter bar (Apply a display filter ... <Ctrl-/>).

The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
76	10.399257105	192.168.0.100	173.194.220.95	QUIC	75	Protected Payload (KP0), DCID=e1be8a102420a5da
77	10.426658112	192.168.0.100	173.194.222.95	QUIC	75	Protected Payload (KP0), DCID=d41067a828c64096
78	10.449832350	173.194.221.94	192.168.0.100	TCP	74	https(443) → 49188 [SYN, ACK] Seq=0 Ack=1 Win=6553
79	10.449929920	192.168.0.100	173.194.221.94	TCP	66	49188 → https(443) [ACK] Seq=1 Ack=1 Win=64256 Len
80	10.450500169	192.168.0.100	173.194.221.94	TLSv1...	583	Client Hello
81	10.450508439	64.233.164.100	192.168.0.100	QUIC	1292	Protected Payload (KP0)
82	10.450508719	64.233.164.100	192.168.0.100	QUIC	824	Protected Payload (KP0)
83	10.450508769	64.233.164.100	192.168.0.100	QUIC	216	Protected Payload (KP0)
84	10.451274806	192.168.0.100	64.233.164.100	QUIC	121	Handshake, DCID=c7a39594206a11bc
85	10.451360366	192.168.0.100	64.233.164.100	QUIC	75	Protected Payload (KP0), DCID=c7a39594206a11bc
86	10.451574606	192.168.0.100	64.233.164.100	QUIC	1288	Protected Payload (KP0), DCID=c7a39594206a11bc
87	10.451591916	192.168.0.100	64.233.164.100	QUIC	130	Protected Payload (KP0), DCID=c7a39594206a11bc
88	10.453432231	108.177.14.190	192.168.0.100	QUIC	1292	Protected Payload (KP0)
89	10.453432611	108.177.14.190	192.168.0.100	QUIC	829	Protected Payload (KP0)
90	10.453432641	108.177.14.190	192.168.0.100	QUIC	237	Protected Payload (KP0)
91	10.453740680	192.168.0.100	108.177.14.190	QUIC	120	Handshake, DCID=f45118ee3b3ce8c7
92	10.453823440	192.168.0.100	108.177.14.190	QUIC	75	Protected Payload (KP0), DCID=f45118ee3b3ce8c7
93	10.453983509	192.168.0.100	108.177.14.190	QUIC	925	Protected Payload (KP0), DCID=f45118ee3b3ce8c7
94	10.455057576	173.194.220.95	192.168.0.100	QUIC	66	Protected Payload (KP0)
95	10.456568932	128.119.245.12	192.168.0.100	TCP	74	http(80) → 42522 [SYN, ACK] Seq=0 Ack=1 Win=28960
96	10.456677102	192.168.0.100	128.119.245.12	TCP	66	42522 → http(80) [ACK] Seq=1 Ack=1 Win=64256 Len=0
97	10.456983341	192.168.0.100	128.119.245.12	HTTP	635	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
98	10.457560450	128.119.245.12	192.168.0.100	TCP	74	http(80) → 42536 [SYN, ACK] Seq=0 Ack=1 Win=28960
99	10.457573140	192.168.0.100	128.119.245.12	TCP	66	42536 → http(80) [ACK] Seq=1 Ack=1 Win=64256 Len=0
100	10.480290329	64.233.164.100	192.168.0.100	QUIC	66	Protected Payload (KP0)

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlp2s0, id 0

trace file.pcapng Packets: 165 · Displayed: 165 (100.0%) Profile: Default

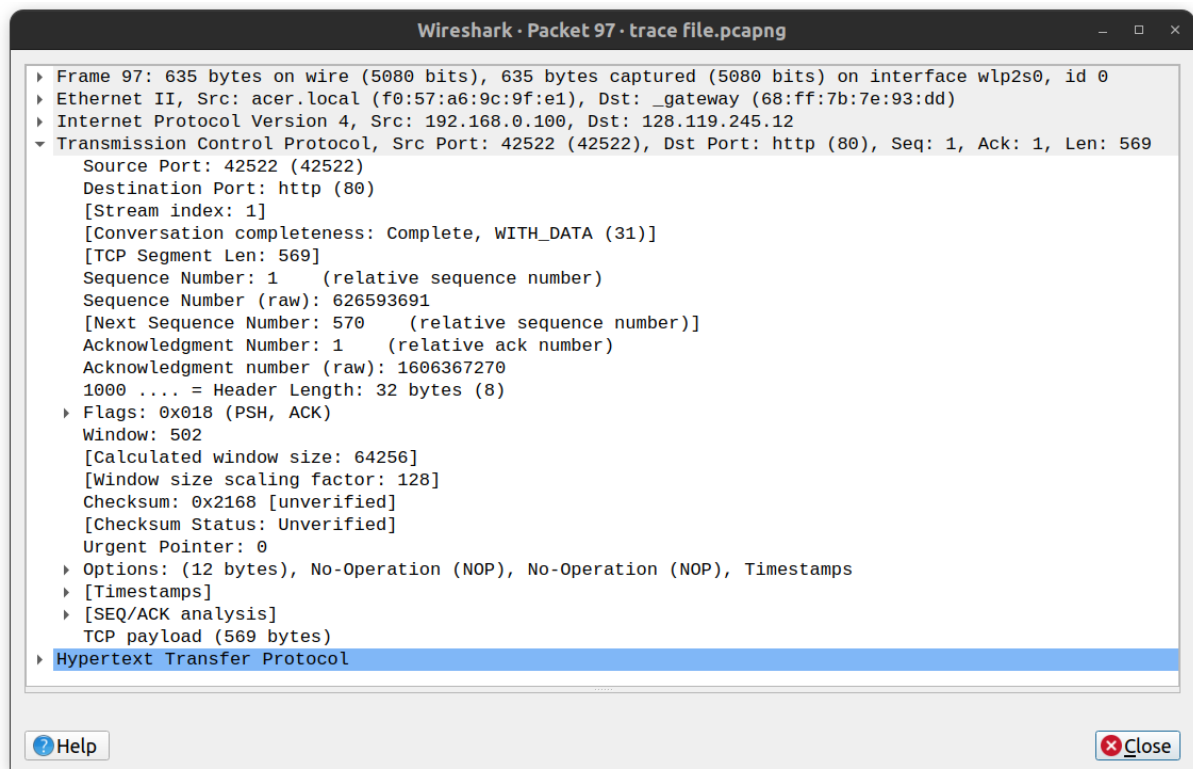
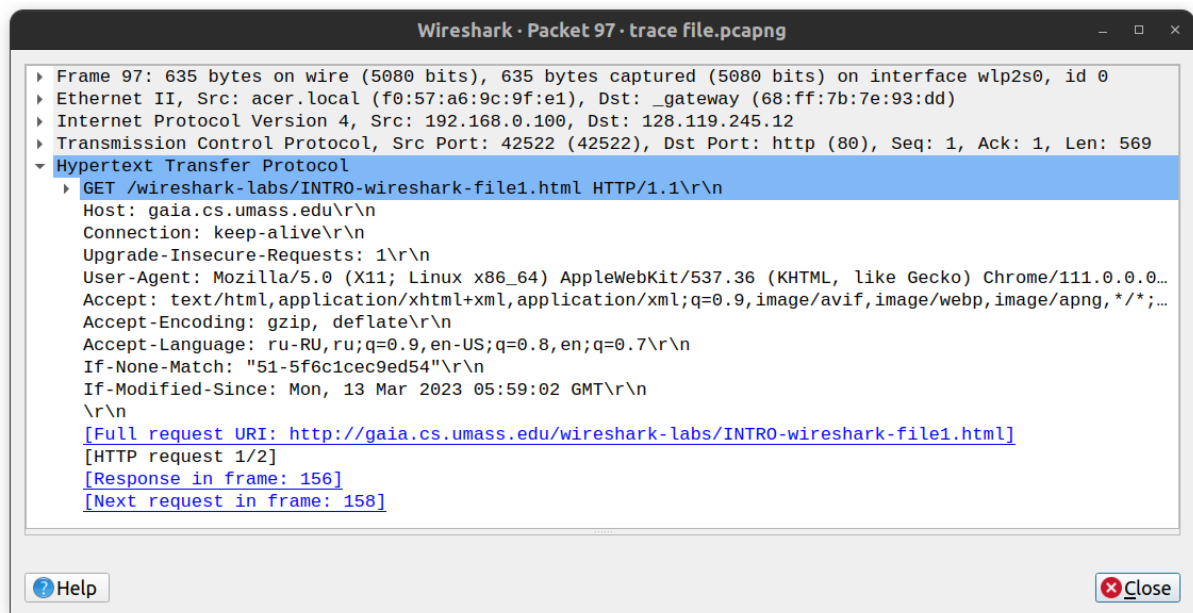
Wireshark interface showing a packet capture of a trace file (trace file.pcapng). The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter bar (Apply a display filter ... <Ctrl-/>).

The packet list pane shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
97	10.456983341	192.168.0.100	128.119.245.12	HTTP	635	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
156	10.676928046	128.119.245.12	192.168.0.100	HTTP	504	HTTP/1.1 200 OK (text/html)
158	10.810392432	192.168.0.100	128.119.245.12	HTTP	496	GET /favicon.ico HTTP/1.1
159	11.123141490	128.119.245.12	192.168.0.100	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlp2s0, id 0

trace file.pcapng Packets: 165 · Displayed: 4 (2.4%) Profile: Default



- Какие из следующих протоколов отображаются (т. е. перечислены в столбце «Протокол» Wireshark) в вашем файле трассировки: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?
 - Отображаются следующие протоколы: ARP, TCP, DNS, QUIC, TLSv1.2, HTTP
- Сколько времени прошло с момента отправки сообщения HTTP GET до получения ответа HTTP OK?
 - GET запрос отправлен в 10.456983341, ответ получен в 10.676928046, т.е. прошло 0.219944705 секунды

- Какой интернет-адрес у сайта `gaia.cs.umass.edu`? Каков интернет-адрес вашего компьютера?
 - `128.119.245.12` (`gaia.cs.umass.edu`)
 - `192.168.0.100`
- Какой тип веб-браузера выдал HTTP-запрос?
 - `User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36`
- Каков номер порта назначения, на который отправляется этот HTTP-запрос?
 - `80` порт