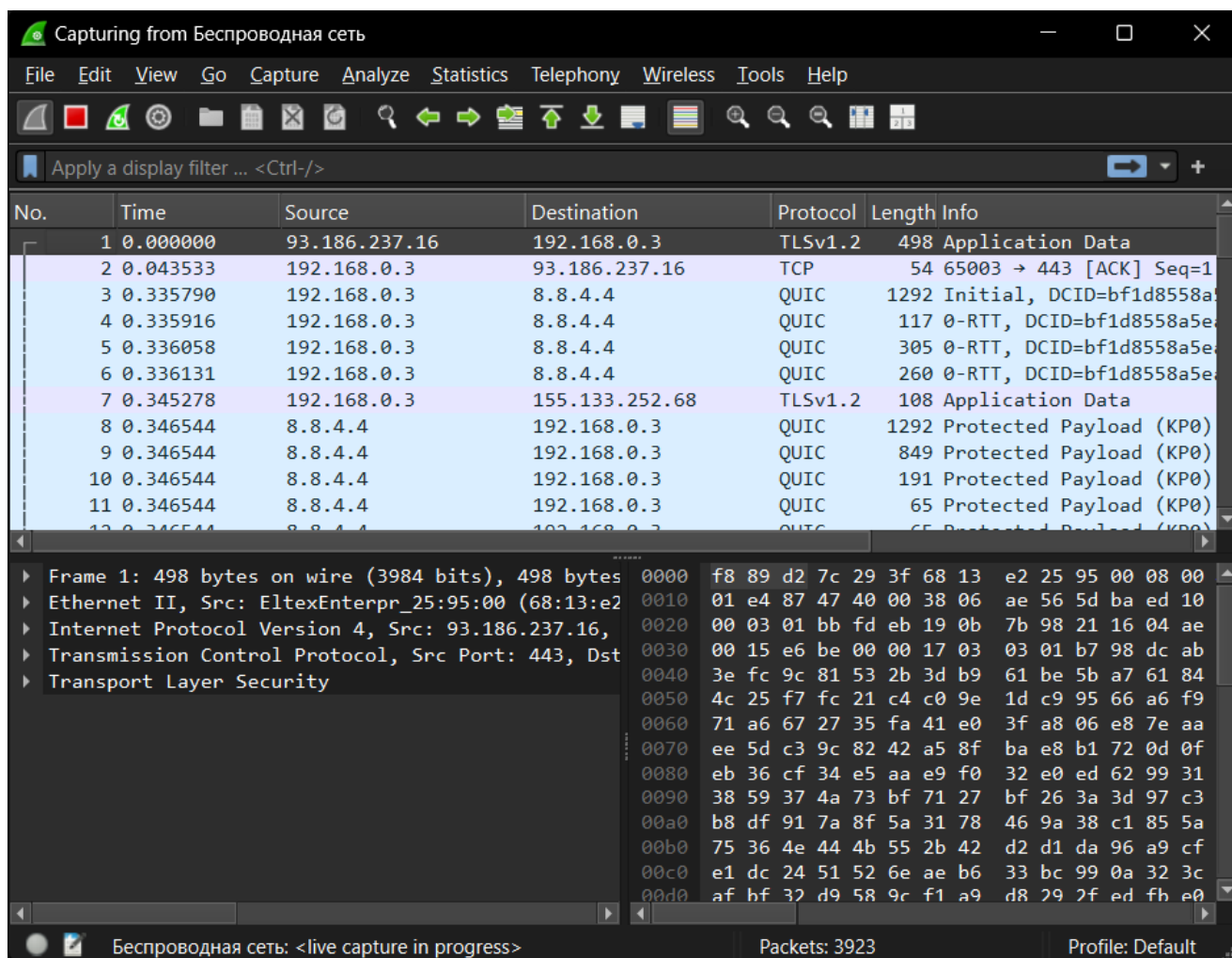


1. Запуск просмотра Беспроводной сети



2. Список хостов IPv4 с IP-адресами (хостов), с которыми компьютер обменивался данными. Для каждого IP указано количество отправленных и полученных пакетов.

Wireshark · Endpoints · Беспроводная сеть

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

Protocol

Bluetooth

BPv7

DCCP

✓ Ethernet

FC

FDDI

IEEE 802.11

IEEE 802.15.4

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country
40.126.53.24	3	175 bytes	2	120 bytes	1	55 bytes	
45.136.22.36	7	416 bytes	4	252 bytes	3	164 bytes	
52.104.127.39	20	17 kB	10	13 kB	10	3 kB	
52.168.112.66	3	162 bytes	1	54 bytes	2	108 bytes	
62.217.160.2	16	968 bytes	8	528 bytes	8	440 bytes	
62.217.160.3	6	363 bytes	3	198 bytes	3	165 bytes	
62.217.160.4	6	363 bytes	3	198 bytes	3	165 bytes	
62.217.160.6	6	363 bytes	3	198 bytes	3	165 bytes	
64.233.165.188	6	363 bytes	3	198 bytes	3	165 bytes	
77.88.21.90	10	605 bytes	5	330 bytes	5	275 bytes	
77.88.21.119	6	363 bytes	3	198 bytes	3	165 bytes	
77.88.55.88	26	2 kB	13	858 bytes	13	715 bytes	
87.240.129.132	25	6 kB	13	2 kB	12	4 kB	
87.240.132.67	86	60 kB	45	46 kB	41	14 kB	
87.240.132.78	8	508 bytes	5	345 bytes	3	163 bytes	
87.240.190.90	59	26 kB	28	12 kB	31	14 kB	
87.250.251.20	10	605 bytes	5	330 bytes	5	275 bytes	
87.250.251.92	6	363 bytes	3	198 bytes	3	165 bytes	

Close Help

3. Все протоколы, участвующие в передаче данных. Для каждого протокола указано процентное соотношение относительно общего трафика.

Wireshark · Protocol Hierarchy Statistics · Беспроводная сеть

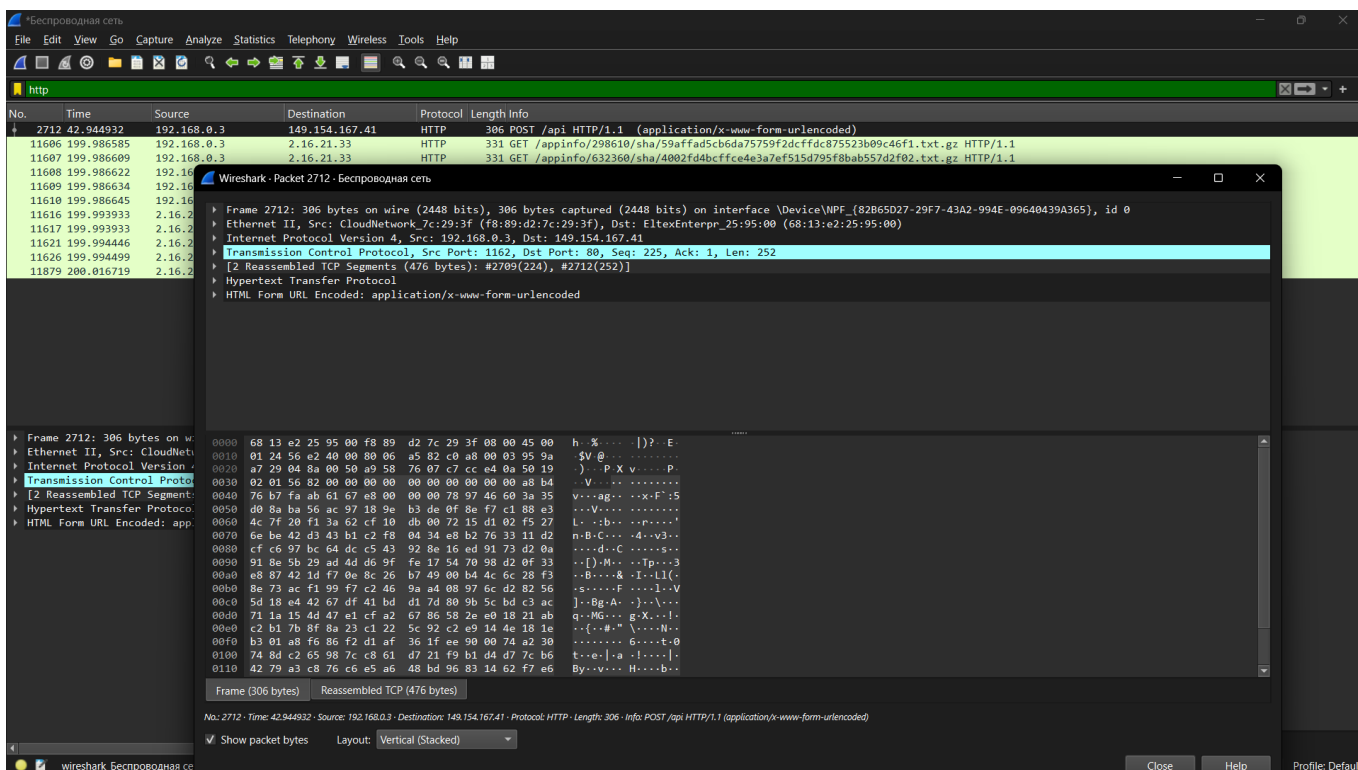
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	10104	100.0	8511676	449 k	0	0	0	10104
Ethernet	100.0	10104	1.7	141456	7478	0	0	0	10104
Internet Protocol Version 6	0.1	6	0.0	240	12	0	0	0	6
User Datagram Protocol	0.1	6	0.0	48	2	0	0	0	6
Multicast Domain Name System	0.1	6	0.0	692	36	6	692	36	6
Internet Protocol Version 4	99.8	10088	2.4	201776	10 k	0	0	0	10088
User Datagram Protocol	4.3	436	0.0	3488	184	0	0	0	436
Simple Service Discovery Protocol	0.7	68	0.2	21176	1119	68	21176	1119	68
QUIC IETF	3.3	338	1.3	110912	5863	338	106071	5607	351
Multicast Domain Name System	0.1	9	0.0	1020	53	9	1020	53	9
Domain Name System	0.2	16	0.0	1805	95	16	1805	95	16
Data	0.0	5	0.0	185	9	5	185	9	5
Transmission Control Protocol	95.5	9648	2.3	195732	10 k	8674	176252	9317	9648
Transport Layer Security	9.4	949	92.3	7855696	415 k	949	7517250	397 k	975
Hypertext Transfer Protocol	0.0	1	0.0	224	11	0	0	0	1
HTML Form URL Encoded	0.0	1	0.0	252	13	1	252	13	1
Data	0.2	20	0.0	1349	71	20	1349	71	20
Apache JServ Protocol v1.3	0.0	4	0.0	3088	163	4	3088	163	4
Internet Group Management Protocol	0.0	4	0.0	32	1	4	32	1	4
Address Resolution Protocol	0.1	10	0.0	280	14	10	280	14	10

No display filter.

Close Copy Protocols Help

4. POST-запрос используется для отправки данных на сервер. Источник: 192.168.0.3, назначение: 149.154.167.41. В секции HTML Form URL Encoded видно, что данные передаются в теле запроса. Параметры или значения (внизу в

hex-данных) включают ключи и их значения. Данные не зашифрованы. Любой, кто прослушивает сеть, может увидеть передаваемые значения.



5. GET-запрос используется для запроса данных с сервера. Источник: 192.168.0.3, назначение: 2.16.21.33. Параметры запроса передаются в URL. Параметры передаются в открытом виде в URL-запросе. Это значит, что любой перехватчик сможет увидеть, какие данные запрашиваются.

Wireshark - Беспроводная сеть

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2712	42.944932	192.168.0.3	149.154.167.41	HTTP	306	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
11606	199.986585	192.168.0.3	2.16.21.33	HTTP	331	GET /appinfo/298610/sha/59affad5cb6da75759f2dcffdc875523b09c46f1.txt.gz HTTP/1.1

Wireshark - Packet 11606 - Беспроводная сеть

Frame 11606: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits) on interface [Device\NPF_{82B65027-29F7-43A2-994E-09640439A365}], id 0

Ethernet II, Src: CloudNetwork 7c:29:3f (f8:89:d2:7c:29:3f), Dst: EltexEnterpr_25:95:00 (68:13:e2:25:95:00)

Internet Protocol Version 4, Src: 192.168.0.3, Dst: 2.16.21.33

Transmission Control Protocol, Src Port: 1174, Dst Port: 80, Seq: 1, Ack: 1, Len: 277

Hypertext Transfer Protocol

0000 68 13 e2 25 95 00 f8 89 d2 7c 29 3f 08 00 45 00 h: %... }?: E-
0010 01 3d 35 6e 40 00 00 06 ec 70 c0 a8 00 03 02 10 :5p@...p...
0020 15 21 04 96 00 50 05 45 a1 b1 40 ce aa 8b 50 18 : P E...P
0030 02 04 ee 99 00 00 47 45 54 20 2f 61 70 70 69 6e :...GE T /appin
0040 66 6f 2f 32 39 38 36 31 30 2f 73 68 61 2f 35 39 fo/29861 0/sha/59
0050 61 66 66 61 64 35 63 62 36 64 61 37 35 37 35 39 affad5cb 6da75759
0060 66 32 64 63 66 66 64 63 38 37 35 35 32 33 62 30 f2dcffdc 875523b0
0070 39 63 34 36 66 31 2e 74 78 74 2e 67 7a 20 48 54 9c46f1t xt.gz HT
0080 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 6c TP/1.1. Host: cl
0090 69 65 6e 74 63 6f 6e 66 69 67 2e 61 6b 61 6d 61 ientconf ig.akama
00a0 69 2e 73 74 65 61 6d 73 74 61 74 69 63 2e 63 6f i.steams tatic.co
00b0 6d 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f m: Accep t: text/
00c0 68 74 6d 6c 2c 2a 2f 2a 3b 71 3d 30 2e 39 0d 0a html,/f ;q=0.9
00d0 61 63 63 65 70 74 2d 65 6e 63 6f 64 69 6e 67 3a accept-e ncoding:
00e0 20 67 7a 69 70 2c 69 64 65 6e 74 69 74 79 2c 2a gzip,id entity,*
00f0 3b 71 3d 30 0d 0a 61 63 63 65 70 74 2d 63 68 61 ;q=0 'ac cept-cha
0100 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 rset: IS O-8859-1
0110 2c 75 74 66 2d 38 2c 2a 3b 71 3d 30 2e 37 0d 0a ,utf-8,* ;q=0.7
0120 75 73 65 72 2d 61 67 65 6e 74 3a 20 56 61 6c 76 user-ago nt: Valv
0130 65 2f 53 74 65 61 6d 20 48 54 54 50 20 43 6c 69 e/Steam HTTP Cli

No: 11606 Time: 199.986585 Source: 192.168.0.3 Destination: 2.16.21.33 Protocol: HTTP Length: 331 Info: GET /appinfo/298610/sha/59affad5cb6da75759f2dcffdc875523b09c46f1.txt.gz HTTP/1.1

Show packet bytes Layout: Vertical (Stacked)

Close Help Profile: Default