

точка банк

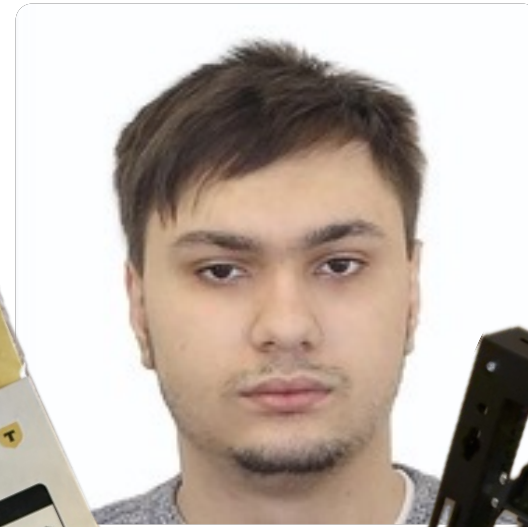
НЕФРОНТЕНДЕРСКИЕ ОПТИМИЗАЦИИ

Ускорение без единой строчки JS

РОМАН ФУРСОВ

Frontend-разработчик

- В сфере 5 лет
- Поддерживал легаси, писал Web3
- Играю в CTF
- Держу домашние сервера
- По вечерам строю завод в Factorio и город в Cities: Skylines



ПРЕДЫСТОРИЯ

КРЕАТИВНЫЙ ПОДХОД ВМЕСТО РУТИНЫ

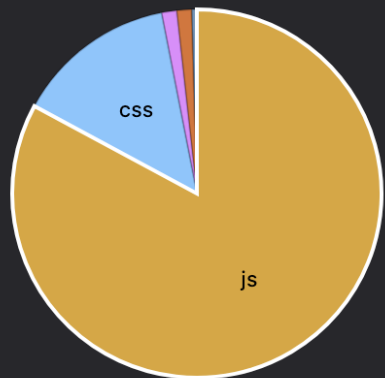
Мы в Точка Банке не боимся перемен — они случаются постоянно.

Вот и в нашей маленькой команде случились перестановки — появился техлид. Он-то и выявил проблему производительности: «Главная сервиса загружается долго».

Так и начинаются мои приключения в мире оптимизаций.

УЖАСНИТЕСЬ!

Primed cache ?



Type	Size	Transferred	Time	Non blocking time
25 js	1,344.40 kB	1,349.30 kB	0.58 s	0.60 s
2 css	227.94 kB	228.36 kB	0.03 s	0.03 s
3 images	21.37 kB	21.57 kB	0.02 s	0.02 s
4 xhr	20.96 kB	22.62 kB	1.79 s	1.79 s
1 html	7.55 kB	1.50 kB	0.05 s	0.05 s
1 ws	0 kB	0.28 kB	0.75 s	0.75 s

Cached responses: 0
Total requests: 36
Size: 1,622.22 kB
Transferred Size: 1,623.63 kB
Time: 3.22 seconds
Non blocking time: 3.24 seconds



Performance



Accessibility



Best Practices

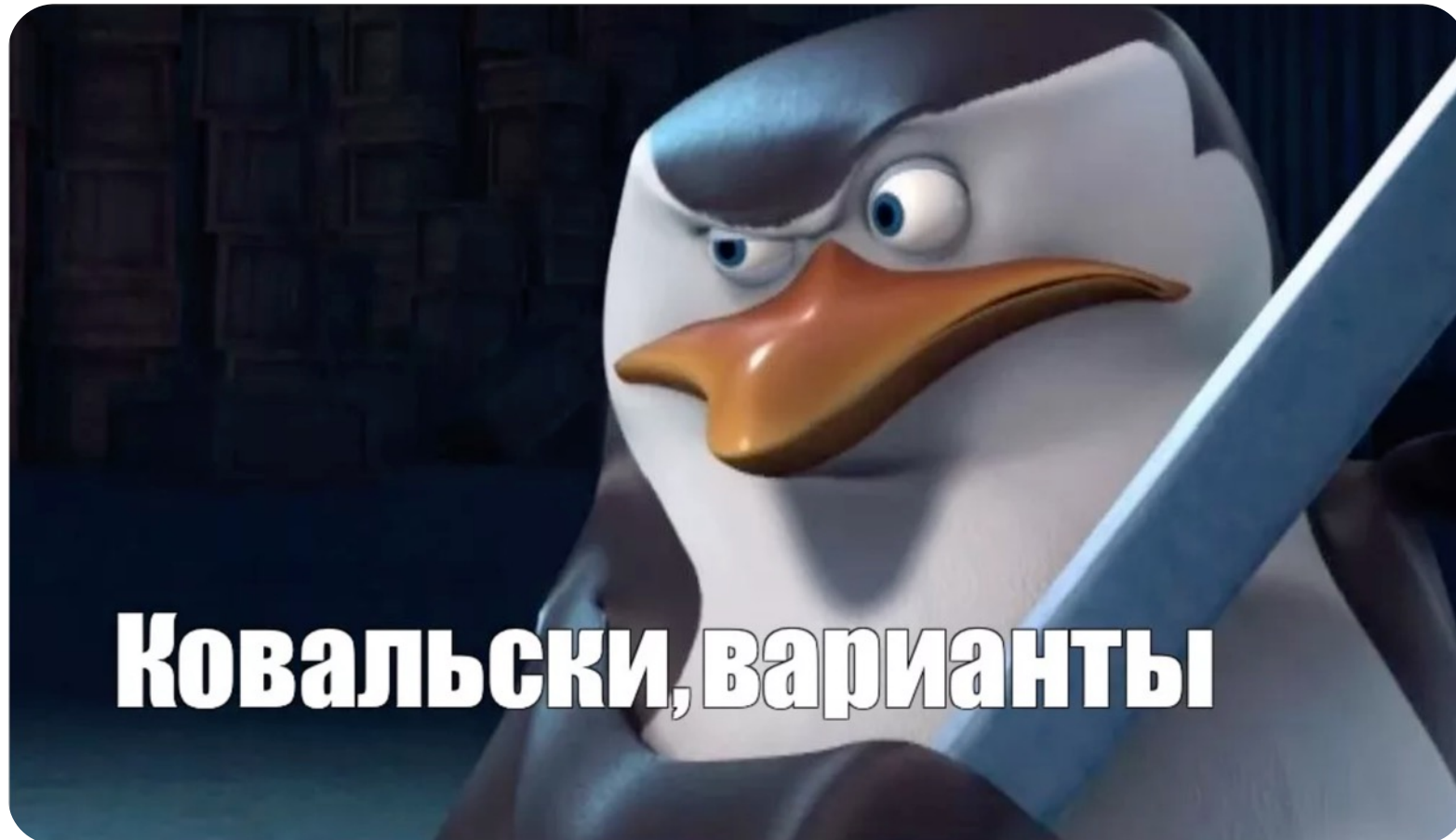


SEO

3,22 СЕКУНДЫ

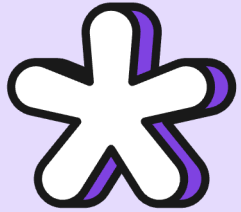
КАК БУДЕМ ОПТИМИЗИРОВАТЬ?

точка банк



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



TCP Fast Open



??? ?????? ??????



???? ??????

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

The image shows a Wireshark capture of a network session. The main pane displays a list of packets. A red circle highlights the first three packets, which constitute a TCP 3-way handshake:

- Packet 1: SYN, ECE, CWR. Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=702491050 TSecr=2503300801
- Packet 2: SYN, ACK, ECE. Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2503300801 TSecr=702491056
- Packet 3: ACK. Seq=1 Ack=1 Win=131776 Len=0 TSval=702491056 TSecr=2503300801

A handwritten note "3-way handshake" with a red arrow points to these three packets. Below the packet list, the details pane shows the structure of the first packet:

- Frame 1: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interf
- Ethernet II, Src: Apple_36:0c:c7 (80:a9:97:36:0c:c7), Dst: ChangwangTec_06:cc:f4 (a8:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.197, Dst: 192.168.1.246
- Transmission Control Protocol, Src Port: 54907, Dst Port: 8080, Seq: 0, Len: 0

The bottom status bar indicates "Packets: 20" and "Profile: Default".

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

точка банк

4



1

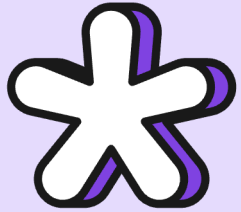
Пакета

Долго, но надёжно

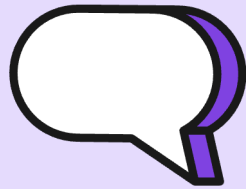
Пакет

Быстро, но с нюансами

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



TCP Fast Open

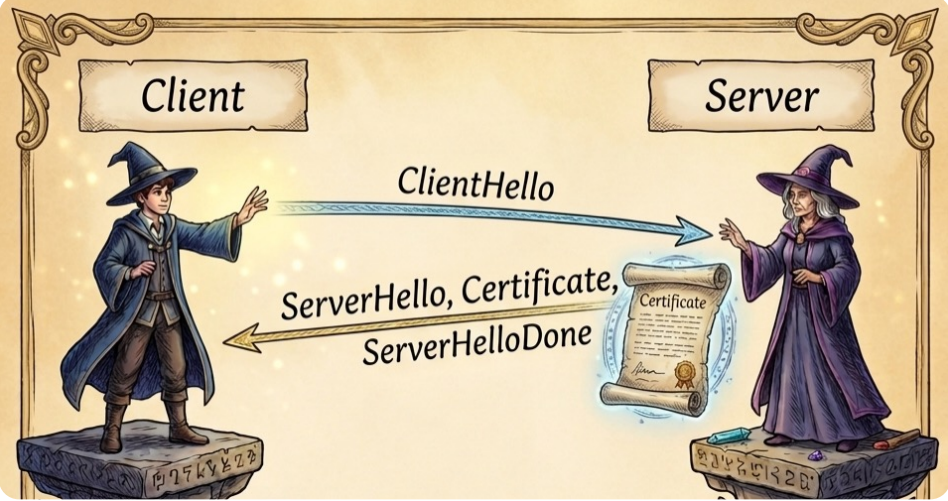


TLS Early Data
TLS False Start



???? ??????

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

Всё стандартно

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.197	192.168.1.110	TCP	78	55713 → 8412 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3979714821 TSecr=2974016831
2	0.003776	192.168.1.110	192.168.1.197	TCP	74	8412 → 55713 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2974016831 TSecr=2974016831
3	0.003993	192.168.1.197	192.168.1.110	TCP	66	55713 → 8412 [ACK] Seq=1 Ack=1 Win=131776 Len=0 TSval=3979714825 TSecr=2974016831
4	0.004824	192.168.1.197	192.168.1.110	TCP	1514	55713 → 8412 [ACK] Seq=1 Ack=1 Win=131776 Len=1418 TSval=3979714825 TSecr=2974016831 [RST] Seq=1996 Win=0 Len=0
5	0.004852	192.168.1.197	192.168.1.110	TCP	524	Client Hello (SNI=tst.playtime.home)
6	0.007735	192.168.1.110	192.168.1.197	TCP	76	8412 → 55713 [ACK] Seq=1 Ack=1903 Win=63488 Len=0 TSval=2974016835 TSecr=3979714825
7	0.014333	192.168.1.110	192.168.1.197	TLSv1.2	1485	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8	0.014413	192.168.1.197	192.168.1.110	TCP	66	55713 → 8412 [ACK] Seq=1996 Ack=1763 Win=130752 Len=0 TSval=3979714840 TSecr=2974016840
9	0.015897	192.168.1.197	192.168.1.110	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.019762	192.168.1.110	192.168.1.197	TLSv1.2	340	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.019763	192.168.1.110	192.168.1.197	TLSv1.2	135	Application Data
12	0.019867	192.168.1.197	192.168.1.110	TCP	66	55713 → 8412 [ACK] Seq=1996 Ack=1763 Win=130752 Len=0 TSval=3979714840 TSecr=2974016840
13	0.020388	192.168.1.197	192.168.1.110	TLSv1.2	165	Application Data
14	0.020419	192.168.1.197	192.168.1.110	TLSv1.2	445	Application Data
15	0.020576	192.168.1.197	192.168.1.110	TLSv1.2	104	Application Data
16	0.023743	192.168.1.110	192.168.1.197	TCP	66	8412 → 55713 [ACK] Seq=1763 Ack=2512 Win=63488 Len=0 TSval=2974016852 TSecr=3979714841
17	0.025734	192.168.1.110	192.168.1.197	TLSv1.2	191	Application Data
18	0.025818	192.168.1.197	192.168.1.110	TCP	66	55713 → 8412 [ACK] Seq=2512 Ack=1888 Win=131008 Len=0 TSval=3979714846 TSecr=2974016855
19	0.127495	192.168.1.197	192.168.1.110	TCP	54	[TCP Keep-Alive] 55713 → 8412 [ACK] Seq=2511 Ack=1888 Win=131072 Len=0
20	0.131876	192.168.1.110	192.168.1.197	TCP	66	[TCP Keep-Alive ACK] 8412 → 55713 [ACK] Seq=1888 Ack=2512 Win=63488 Len=0 TSval=2974016855 TSecr=3979714846

```
> Frame 7: Packet, 1485 bytes on wire (11880 bits), 1485 bytes captured (11880 bits) on 0
> Ethernet II, Src: ChangwangTec_06:cc:6c (a8:b8:e0:06:cc:6c), Dst: Apple_36:0c:c7 (08:00:0e:36:0c:c7)
> Internet Protocol Version 4, Src: 192.168.1.110, Dst: 192.168.1.197
  > Transmission Control Protocol, Src Port: 8412, Dst Port: 55713, Seq: 1, Ack: 1903,
    Source Port: 8412
    Destination Port: 55713
    [Stream index: 0]
    [Stream Packet Number: 7]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1419]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 2470524283
    [Next Sequence Number: 1420 (relative sequence number)]
    Acknowledgment Number: 1903 (relative ack number)
    Acknowledgment number (raw): 3596193137
    1000 ... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 62
    [Calculated window size: 63488]
    [Window size scaling factor: 1024]
    Checksum: 0x21c2 [unverified]
```

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

This document describes a technique that alleviates the latency burden imposed by TLS: the client-side TLS False Start. If certain conditions are met, the client can start to send application data when the full handshake is only partially complete, namely, when the client has sent its own ChangeCipherSpec and Finished messages (thus having updated its TLS Record Protocol write state as negotiated in the handshake) but has yet to receive the server's ChangeCipherSpec and Finished messages. (Per [Section 7.4.9 of \[RFC5246\]](#), after a full handshake, the client would have to delay sending application data until it has received and validated the server's Finished message.) Accordingly, the latency penalty for using TLS with HTTP can be kept at one round-trip time.

Note that in practice, the TCP three-way handshake [RFC0793] typically adds one round-trip time before the client can even send the ClientHello. See [RFC7413] for a latency improvement at that level.

When an earlier TLS session is resumed, TLS uses an abbreviated handshake with only three protocol flights. For application protocols in which the client sends data first, this abbreviated handshake adds just one round-trip time to begin with, so there is no need for a client-side False Start. However, if the server sends application data first, the abbreviated handshake adds two round-trip times, and this could be reduced to just one added round-trip time by doing a server-side False Start. There is little need for this in practice, so this document does not consider server-side False Starts further.

Note also that TLS versions 1.3 [TLS13] and beyond are out of scope for this document. False Start will not be needed with these newer versions since protocol flows minimizing the number of round trips have become a first-order design goal.

In a False Start, when the client sends application data before it has received and verified the server's Finished message, there are two possible outcomes:

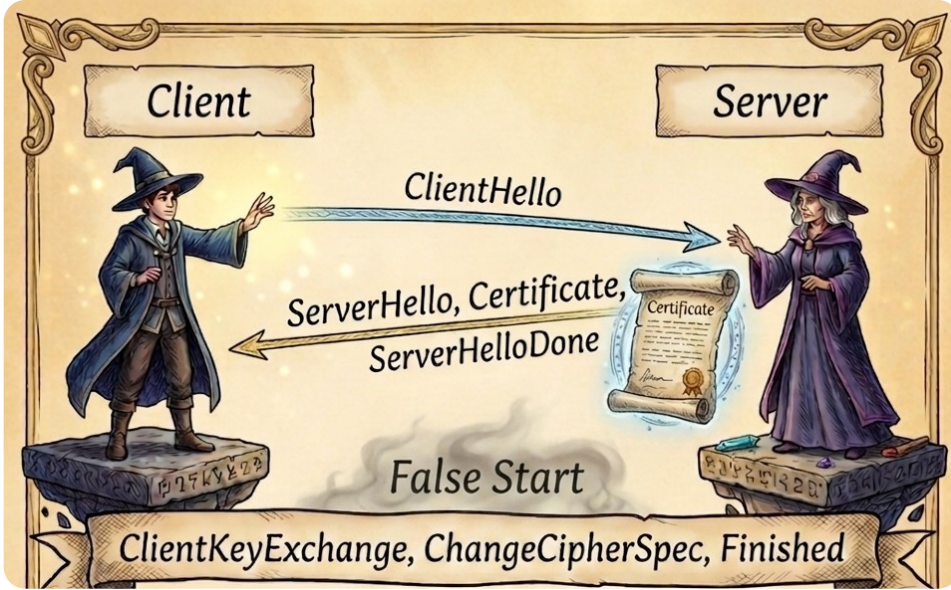
- o The handshake completes successfully: The handshake is retroactively validated when both Finished messages have been received and verified. This retroactively validates the handshake. In this case, the transcript of protocol data carried over the transport underlying TLS will look as usual, apart from the different timing.

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

Note that in practice, the TCP three-way handshake [[RFC0793](#)] typically adds one round-trip time before the client can even send the ClientHello. See [[RFC7413](#)] (TCP Fast Open) for a latency improvement at that level.

Note also that TLS versions 1.3 [[TLS13](#)] and beyond are out of scope for this document. False Start will not be needed with these newer versions since protocol flows minimizing the number of round trips have become a first-order design goal.

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

Всё по-прежнему

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.197	192.168.1.110	TCP	78	49248 → 8443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=731058377 TSecr=731058377
2	0.004055	192.168.1.110	192.168.1.197	TCP	74	8443 → 49248 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2948745163 TSecr=731058377
3	0.004237	192.168.1.197	192.168.1.110	TCP	66	49248 → 8443 [ACK] Seq=1 ACK=1 Win=131776 Len=0 TSval=731058381 TSecr=2948745163
4	0.005683	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [ACK] Seq=230 Ack=1454 Win=130368 Len=0 TSval=731058394 TSecr=2948745174
5	0.009999	192.168.1.110	192.168.1.197	TCP	1514	Server Hello, Certificate, Server Key Exchange
6	0.016131	192.168.1.110	192.168.1.197	TLSv1.2	71	Server Hello Done
7	0.016134	192.168.1.110	192.168.1.197	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
8	0.016300	192.168.1.197	192.168.1.110	TCP	117	Change Cipher Spec, Encrypted Handshake Message
9	0.017636	192.168.1.197	192.168.1.110	TLSv1.2	66	49248 → 8443 [ACK] Seq=438 Ack=2387 Win=130240 Len=0 TSval=731058403 TSecr=2948745186
10	0.022012	192.168.1.110	192.168.1.197	TCP	97	Encrypted Alert
11	0.022119	192.168.1.197	192.168.1.110	TCP	66	49248 → 8443 [ACK] Seq=469 Ack=2387 Win=131072 Len=0 TSval=731058404 TSecr=2948745186
12	0.022295	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [FIN, ACK] Seq=2387 Ack=469 Win=65536 Len=0 TSval=2948745190 TSecr=731058404
13	0.026005	192.168.1.110	192.168.1.197	TCP	66	[TCP Retransmission] 49248 → 8443 [FIN, ACK] Seq=469 Ack=2388 Win=131072 Len=0 TSval=731058404 TSecr=2948745191
14	0.026145	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404
15	0.026879	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404
16	0.027042	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404
17	0.029989	192.168.1.110	192.168.1.197	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404
18	0.030147	192.168.1.197	192.168.1.110	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404
19	0.032049	192.168.1.110	192.168.1.197	TCP	66	8443 → 49248 [ACK] Seq=2388 Ack=470 Win=65536 Len=0 TSval=2948745191 TSecr=731058404

```
Length: 229
Version: TLS 1.2 (0x0303)
> Random: c268d0321211252a2464e1a6f15c0b936a8acb6bcecb738b8f4091682ded98dc
Session ID Length: 0
Cipher Suites Length: 54
> Cipher Suites (27 suites)
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 125
> Extension: renegotiation_info (len=1)
> Extension: server_name (len=22) name=tst.playtime.home
> Extension: ec_point_formats (len=2)
> Extension: supported_groups (len=12)
> Extension: application_layer_protocol_negotiation (len=14)
> Extension: encrypt_then_mac (len=0)
> Extension: extended_master_secret (len=0)
> Extension: signature_algorithms (len=42)
[JA4: t12uz700nz_a24000018678_eed5f152405c]
[JA4_r [...]: t12d2708h2_002f,0033,0035,0039,003c,003d,0067,006b,009c,009d,00a0,00a1,00a2,00a3,00a4,00a5,00a6,00a7,00a8,00a9,00aa,00ab,00ac,00ad,00ae,00af,00b0,00b1,00b2,00b3,00b4,00b5,00b6,00b7,00b8,00b9,00ba,00bb,00bc,00bd,00be,00bf,00c0,00c1,00c2,00c3,00c4,00c5,00c6,00c7,00c8,00c9,00ca,00cb,00cc,00cd,00ce,00cf,00d0,00d1,00d2,00d3,00d4,00d5,00d6,00d7,00d8,00d9,00da,00db,00dc,00dd,00de,00df,00e0,00e1,00e2,00e3,00e4,00e5,00e6,00e7,00e8,00e9,00ea,00eb,00ec,00ed,00ee,00ef,00f0,00f1,00f2,00f3,00f4,00f5,00f6,00f7,00f8,00f9,00fa,00fb,00fc,00fd,00fe,00ff,0100,0101,0102,0103,0104,0105,0106,0107,0108,0109,010a,010b,010c,010d,010e,010f,0110,0111,0112,0113,0114,0115,0116,0117,0118,0119,011a,011b,011c,011d,011e,011f,0120,0121,0122,0123,0124,0125,0126,0127,0128,0129,012a,012b,012c,012d,012e,012f,0130,0131,0132,0133,0134,0135,0136,0137,0138,0139,013a,013b,013c,013d,013e,013f,0140,0141,0142,0143,0144,0145,0146,0147,0148,0149,014a,014b,014c,014d,014e,014f,0150,0151,0152,0153,0154,0155,0156,0157,0158,0159,015a,015b,015c,015d,015e,015f,0160,0161,0162,0163,0164,0165,0166,0167,0168,0169,016a,016b,016c,016d,016e,016f,0170,0171,0172,0173,0174,0175,0176,0177,0178,0179,017a,017b,017c,017d,017e,017f,0180,0181,0182,0183,0184,0185,0186,0187,0188,0189,018a,018b,018c,018d,018e,018f,0190,0191,0192,0193,0194,0195,0196,0197,0198,0199,019a,019b,019c,019d,019e,019f,01a0,01a1,01a2,01a3,01a4,01a5,01a6,01a7,01a8,01a9,01aa,01ab,01ac,01ad,01ae,01af,01b0,01b1,01b2,01b3,01b4,01b5,01b6,01b7,01b8,01b9,01ba,01bb,01bc,01bd,01be,01bf,01c0,01c1,01c2,01c3,01c4,01c5,01c6,01c7,01c8,01c9,01ca,01cb,01cc,01cd,01ce,01cf,01d0,01d1,01d2,01d3,01d4,01d5,01d6,01d7,01d8,01d9,01da,01db,01dc,01dd,01de,01df,01e0,01e1,01e2,01e3,01e4,01e5,01e6,01e7,01e8,01e9,01ea,01eb,01ec,01ed,01ee,01ef,01f0,01f1,01f2,01f3,01f4,01f5,01f6,01f7,01f8,01f9,01fa,01fb,01fc,01fd,01fe,01ff,0200,0201,0202,0203,0204,0205,0206,0207,0208,0209,020a,020b,020c,020d,020e,020f,0210,0211,0212,0213,0214,0215,0216,0217,0218,0219,021a,021b,021c,021d,021e,021f,0220,0221,0222,0223,0224,0225,0226,0227,0228,0229,022a,022b,022c,022d,022e,022f,0230,0231,0232,0233,0234,0235,0236,0237,0238,0239,023a,023b,023c,023d,023e,023f,0240,0241,0242,0243,0244,0245,0246,0247,0248,0249,024a,024b,024c,024d,024e,024f,0250,0251,0252,0253,0254,0255,0256,0257,0258,0259,025a,025b,025c,025d,025e,025f,0260,0261,0262,0263,0264,0265,0266,0267,0268,0269,026a,026b,026c,026d,026e,026f,0270,0271,0272,0273,0274,0275,0276,0277,0278,0279,027a,027b,027c,027d,027e,027f,0280,0281,0282,0283,0284,0285,0286,0287,0288,0289,028a,028b,028c,028d,028e,028f,0290,0291,0292,0293,0294,0295,0296,0297,0298,0299,029a,029b,029c,029d,029e,029f,02a0,02a1,02a2,02a3,02a4,02a5,02a6,02a7,02a8,02a9,02aa,02ab,02ac,02ad,02ae,02af,02b0,02b1,02b2,02b3,02b4,02b5,02b6,02b7,02b8,02b9,02ba,02bb,02bc,02bd,02be,02bf,02c0,02c1,02c2,02c3,02c4,02c5,02c6,02c7,02c8,02c9,02ca,02cb,02cc,02cd,02ce,02cf,02d0,02d1,02d2,02d3,02d4,02d5,02d6,02d7,02d8,02d9,02da,02db,02dc,02dd,02de,02df,02e0,02e1,02e2,02e3,02e4,02e5,02e6,02e7,02e8,02e9,02ea,02eb,02ec,02ed,02ee,02ef,02f0,02f1,02f2,02f3,02f4,02f5,02f6,02f7,02f8,02f9,02fa,02fb,02fc,02fd,02fe,02ff,0300,0301,0302,0303,0304,0305,0306,0307,0308,0309,030a,030b,030c,030d,030e,030f,0310,0311,0312,0313,0314,0315,0316,0317,0318,0319,031a,031b,031c,031d,031e,031f,0320,0321,0322,0323,0324,0325,0326,0327,0328,0329,032a,032b,032c,032d,032e,032f,0330,0331,0332,0333,0334,0335,0336,0337,0338,0339,033a,033b,033c,033d,033e,033f,0340,0341,0342,0343,0344,0345,0346,0347,0348,0349,034a,034b,034c,034d,034e,034f,0350,0351,0352,0353,0354,0355,0356,0357,0358,0359,035a,035b,035c,035d,035e,035f,0360,0361,0362,0363,0364,0365,0366,0367,0368,0369,036a,036b,036c,036d,036e,036f,0370,0371,0372,0373,0374,0375,0376,0377,0378,0379,037a,037b,037c,037d,037e,037f,0380,0381,0382,0383,0384,0385,0386,0387,0388,0389,038a,038b,038c,038d,038e,038f,0390,0391,0392,0393,0394,0395,0396,0397,0398,0399,039a,039b,039c,039d,039e,039f,03a0,03a1,03a2,03a3,03a4,03a5,03a6,03a7,03a8,03a9,03aa,03ab,03ac,03ad,03ae,03af,03b0,03b1,03b2,03b3,03b4,03b5,03b6,03b7,03b8,03b9,03ba,03bb,03bc,03bd,03be,03bf,03c0,03c1,03c2,03c3,03c4,03c5,03c6,03c7,03c8,03c9,03ca,03cb,03cc,03cd,03ce,03cf,03d0,03d1,03d2,03d3,03d4,03d5,03d6,03d7,03d8,03d9,03da,03db,03dc,03dd,03de,03df,03e0,03e1,03e2,03e3,03e4,03e5,03e6,03e7,03e8,03e9,03ea,03eb,03ec,03ed,03ee,03ef,03f0,03f1,03f2,03f3,03f4,03f5,03f6,03f7,03f8,03f9,03fa,03fb,03fc,03fd,03fe,03ff,0400,0401,0402,0403,0404,0405,0406,0407,0408,0409,040a,040b,040c,040d,040e,040f,0410,0411,0412,0413,0414,0415,0416,0417,0418,0419,041a,041b,041c,041d,041e,041f,0420,0421,0422,0423,0424,0425,0426,0427,0428,0429,042a,042b,042c,042d,042e,042f,0430,0431,0432,0433,0434,0435,0436,0437,0438,0439,043a,043b,043c,043d,043e,043f,0440,0441,0442,0443,0444,0445,0446,0447,0448,0449,044a,044b,044c,044d,044e,044f,0450,0451,0452,0453,0454,0455,0456,0457,0458,0459,045a,045b,045c,045d,045e,045f,0460,0461,0462,0463,0464,0465,0466,0467,0468,0469,046a,046b,046c,046d,046e,046f,0470,0471,0472,0473,0474,0475,0476,0477,0478,0479,047a,047b,047c,047d,047e,047f,0480,0481,0482,0483,0484,0485,0486,0487,0488,0489,048a,048b,048c,048d,048e,048f,0490,0491,0492,0493,0494,0495,0496,0497,0498,0499,049a,049b,049c,049d,049e,049f,04a0,04a1,04a2,04a3,04a4,04a5,04a6,04a7,04a8,04a9,04aa,04ab,04ac,04ad,04ae,04af,04b0,04b1,04b2,04b3,04b4,04b5,04b6,04b7,04b8,04b9,04ba,04bb,04bc,04bd,04be,04bf,04c0,04c1,04c2,04c3,04c4,04c5,04c6,04c7,04c8,04c9,04ca,04cb,04cc,04cd,04ce,04cf,04d0,04d1,04d2,04d3,04d4,04d5,04d6,04d7,04d8,04d9,04da,04db,04dc,04dd,04de,04df,04e0,04e1,04e2,04e3,04e4,04e5,04e6,04e7,04e8,04e9,04ea,04eb,04ec,04ed,04ee,04ef,04f0,04f1,04f2,04f3,04f4,04f5,04f6,04f7,04f8,04f9,04fa,04fb,04fc,04fd,04fe,04ff,0500,0501,0502,0503,0504,0505,0506,0507,0508,0509,050a,050b,050c,050d,050e,050f,0510,0511,0512,0513,0514,0515,0516,0517,0518,0519,051a,051b,051c,051d,051e,051f,0520,0521,0522,0523,0524,0525,0526,0527,0528,0529,052a,052b,052c,052d,052e,052f,0530,0531,0532,0533,0534,0535,0536,0537,0538,0539,053a,053b,053c,053d,053e,053f,0540,0541,0542,0543,0544,0545,0546,0547,0548,0549,054a,054b,054c,054d,054e,054f,0550,0551,0552,0553,0554,0555,0556,0557,0558,0559,055a,055b,055c,055d,055e,055f,0560,0561,0562,0563,0564,0565,0566,0567,0568,0569,056a,056b,056c,056d,056e,056f,0570,0571,0572,0573,0574,0575,0576,0577,0578,0579,057a,057b,057c,057d,057e,057f,0580,0581,0582,0583,0584,0585,0586,0587,0588,0589,058a,058b,058c,058d,058e,058f,0590,0591,0592,0593,0594,0595,0596,0597,0598,0599,059a,059b,059c,059d,059e,059f,05a0,05a1,05a2,05a3,05a4,05a5,05a6,05a7,05a8,05a9,05aa,05ab,05ac,05ad,05ae,05af,05b0,05b1,05b2,05b3,05b4,05b5,05b6,05b7,05b8,05b9,05ba,05bb,05bc,05bd,05be,05bf,05c0,05c1,05c2,05c3,05c4,05c5,05c6,05c7,05c8,05c9,05ca,05cb,05cc,05cd,05ce,05cf,05d0,05d1,05d2,05d3,05d4,05d5,05d6,05d7,05d8,05d9,05da,05db,05dc,05dd,05de,05df,05e0,05e1,05e2,05e3,05e4,05e5,05e6,05e7,05e8,05e9,05ea,05eb,05ec,05ed,05ee,05ef,05f0,05f1,05f2,05f3,05f4,05f5,05f6,05f7,05f8,05f9,05fa,05fb,05fc,05fd,05fe,05ff,0600,0601,0602,0603,0604,0605,0606,0607,0608,0609,060a,060b,060c,060d,060e,060f,0610,0611,0612,0613,0614,0615,0616,0617,0618,0619,061a,061b,061c,061d,061e,061f,0620,0621,0622,0623,0624,0625,0626,0627,0628,0629,062a,062b,062c,062d,062e,062f,0630,0631,0632,0633,0634,0635,0636,0637,0638,0639,063a,063b,063c,063d,063e,063f,0640,0641,0642,0643,0644,0645,0646,0647,0648,0649,064a,064b,064c,064d,064e,064f,0650,0651,0652,0653,0654,0655,0656,0657,0658,0659,065a,065b,065c,065d,065e,065f,0660,0661,0662,0663,0664,0665,0666,0667,0668,0669,066a,066b,066c,066d,066e,066f,0670,0671,0672,0673,0674,0675,0676,0677,0678,0679,067a,067b,067c,067d,067e,067f,0680,0681,0682,0683,0684,0685,0686,0687,0688,0689,068a,068b,068c,068d,068e,068f,0690,0691,0692,0693,0694,0695,0696,0697,0698,0699,069a,069b,069c,069d,069e,069f,06a0,06a1,06a2,06a3,06a4,06a5,06a6,06a7,06a8,06a9,06aa,06ab,06ac,06ad,06ae,06af,06b0,06b1,06b2,06b3,06b4,06b5,06b6,06b7,06b8,06b9,06ba,06bb,06bc,06bd,06be,06bf,06c0,06c1,06c2,06c3,06c4,06c5,06c6,06c7,06c8,06c9,06ca,06cb,06cc,06cd,06ce,06cf,06d0,06d1,06d2,06d3,06d4,06d5,06d6,06d7,06d8,06d9,06da,06db,06dc,06dd,06de,06df,06e0,06e1,06e2,06e3,06e4,06e5,06e6,06e7,06e8,06e9,06ea,06eb,06ec,06ed,06ee,06ef,06f0,06f1,06f2,06f3,06f4,06f5,06f6,06f7,06f8,06f9,06fa,06fb,06fc,06fd,06fe,06ff,0700,0701,0702,0703,0704,0705,0706,0707,0708,0709,070a,070b,070c,070d,070e,070f,0710,0711,0712,0713,0714,0715,0716,0717,0718,0719,071a,071b,071c,071d,071e,071f,0720,0721,0722,0723,0724,0725,0726,0727,0728,0729,072a,072b,072c,072d,072e,072f,0730,0731,0732,0733,0734,0735,0736,0737,0738,0739,073a,073b,073c,073d,073e,073f,0740,0741,0742,0743,0744,0745,0746,0747,0748,0749,074a,074b,074c,074d,074e,074f,0750,0751,0752,0753,0754,0755,0756,0757,0758,0759,075a,075b,075c,075d,075e,075f,0760,0761,0762,0763,0764,0765,0766,0767,0768,0769,076a,076b,076c,076d,076e,076f,0770,0771,0772,0773,0774,0775,0776,0777,0778,0779,077a,077b,077c,077d,077e,077f,0780,0781,0782,0783,0784,0785,0786,0787,0788,0789,078a,078b,078c,078d,078e,078f,0790,0791,0792,0793,0794,0795,0796,0797,0798,0799,079a,079b,079c,079d,079e,079f,07a0,07a1,07a2,07a3,07a4,07a5,07a6,07a7,07a8,07a9,07aa,07ab,07ac,07ad,07ae,07af,07b0,07b1,07b2,07b3,07b4,07b5,07b6,07b7,07b8,07b9,07ba,07bb,07bc,07bd,07be,07bf,07c0,07c1,07c2,07c3,07c4,07c5,07c6,07c7,07c8,07c9,07ca,07cb,07cc,07cd,07ce,07cf,07d0,07d1,07d2,07d3,07d4,07d5,07d6,07d7,07d8,07d9,07da,07db,07dc,07dd,07de,07df,07e0,07e1,07e2,07e3,07e4,07e5,07e6,07e7,07e8,07e9,07ea,07eb,07ec,07ed,07ee,07ef,07f0,07f1,07f2,07f3,07f4,07f5,07f6,07f7,07f8,07f9,07fa,07fb,07fc,07fd,07fe,07ff,0800,0801,0802,0803,0804,0805,0806,0807,0808,0809,080a,080b,080c,080d,080e,080f,0810,0811,0812,0813,0814,0815,0816,0817,0818,0819,081a,081b,081c,081d,081e,081f,0820,0821,0822,0823,0824,0825,0826,0827,0828,0829,082a,082
```

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

точка банк



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

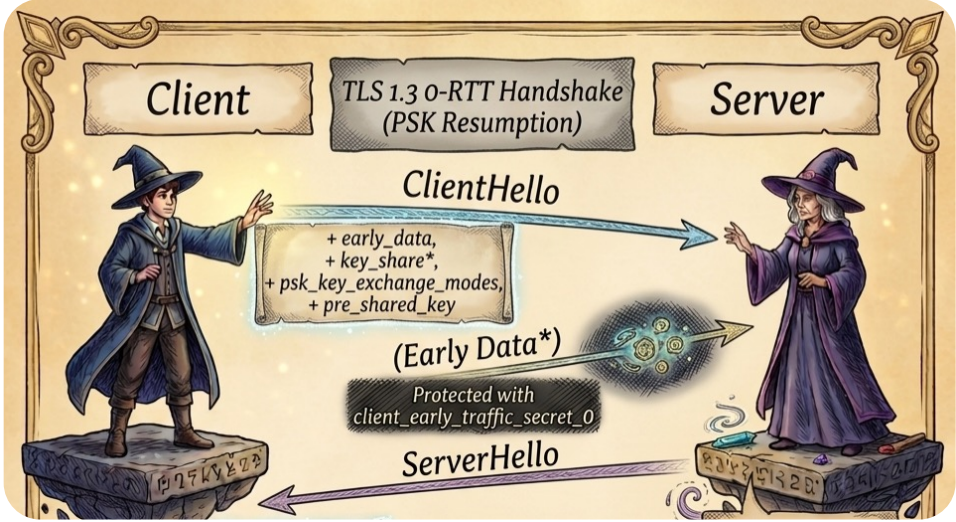
точка банк



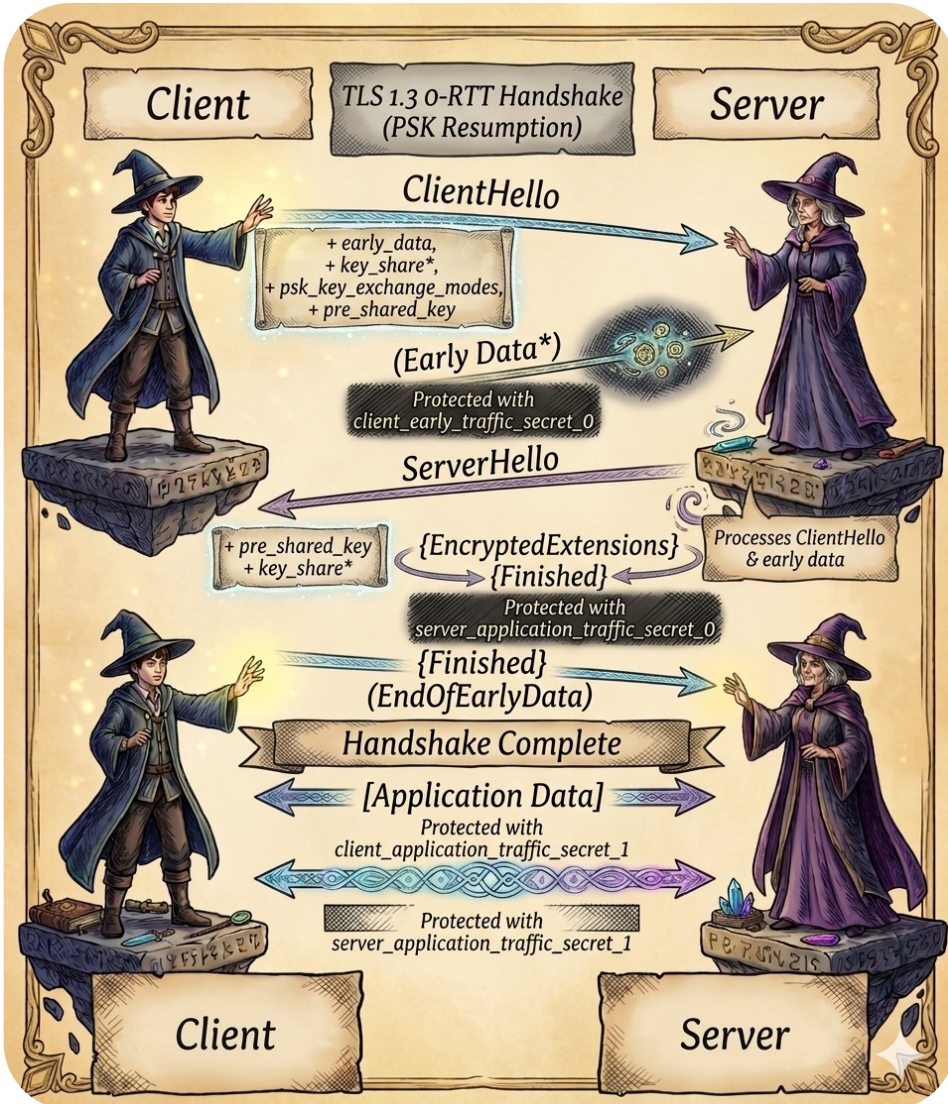
ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

The screenshot displays a network traffic capture in Wireshark. The main pane shows a list of packets, with packet 5 selected. A red box highlights packets 5 and 6, which are the Client Hello and Server Hello messages of a TLS handshake. A handwritten note in Russian, "Сработало!" (It worked!), with a red arrow points to the Client Hello packet. The packet details pane on the left shows the structure of the selected packet, including the TLSv1.3 Record Layer and the Application Data extension. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.197	192.168.1.110	TCP	78	52287 → 8413 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3275862662 TSecr=2014973017
2	0.008693	192.168.1.110	192.168.1.197	TCP	74	8413 → 52287 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=2014973017 TSecr=0
3	0.008886	192.168.1.197	192.168.1.110	TCP	66	52287 → 8413 [ACK] Seq=1 Ack=1 Win=131776 Len=0 TSval=3275862671 TSecr=2014973017
4	0.009839	192.168.1.197	192.168.1.110	TCP	1514	52287 → 8413 [ACK] Seq=1 Ack=1 Win=131776 Len=1440 TSval=3275862672 TSecr=2014973017
5	0.009846	192.168.1.197	192.168.1.110	TLSv1.3	166	Client Hello (SNI=tst.playtime.home), Change Cipher Spec, Application Data
6	0.013395	192.168.1.110	192.168.1.197	TLSv1.3	1514	8413 → 52287 [ACK] Seq=1 Ack=1552 Win=64512 Len=0 TSval=2014973023 TSecr=3275862672
7	0.018693	192.168.1.110	192.168.1.197	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
8	0.018695	192.168.1.110	192.168.1.197	TLSv1.3	1275	Application Data, Application Data, Application Data
9	0.018793	192.168.1.197	192.168.1.110	TCP	66	52287 → 8413 [ACK] Seq=1552 Ack=2658 Win=129152 Len=0 TSval=3275862681 TSecr=2014973023
10	0.019856	192.168.1.197	192.168.1.110	TLSv1.3	140	Application Data
11	0.024730	192.168.1.110	192.168.1.197	TLSv1.3	377	Application Data
12	0.024732	192.168.1.110	192.168.1.197	TLSv1.3	377	Application Data
13	0.024845	192.168.1.197	192.168.1.110	TCP	66	52287 → 8413 [ACK] Seq=1626 Ack=3280 Win=130496 Len=0 TSval=3275862687 TSecr=2014973030
14	0.323538	192.168.1.197	192.168.1.110	TCP	54	[TCP Keep-Alive] 52287 → 8413 [ACK] Seq=1625 Ack=3280 Win=131072 Len=0
15	0.331730	192.168.1.110	192.168.1.197	TCP	66	[TCP Keep-Alive ACK] 8413 → 52287 [ACK] Seq=3280 Ack=1626 Win=64512 Len=0 TSval=2014973030

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

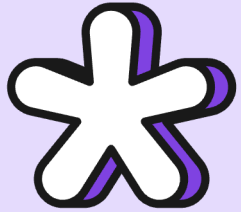
точка банк

Ура! 🎉

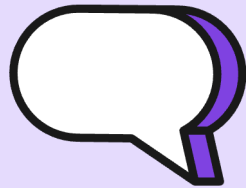
И клиент, и сервер отправили
данные раньше.



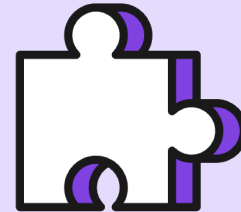
ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



TCP Fast Open



TLS Early Data
TLS False Start



QUIC 0-RTT

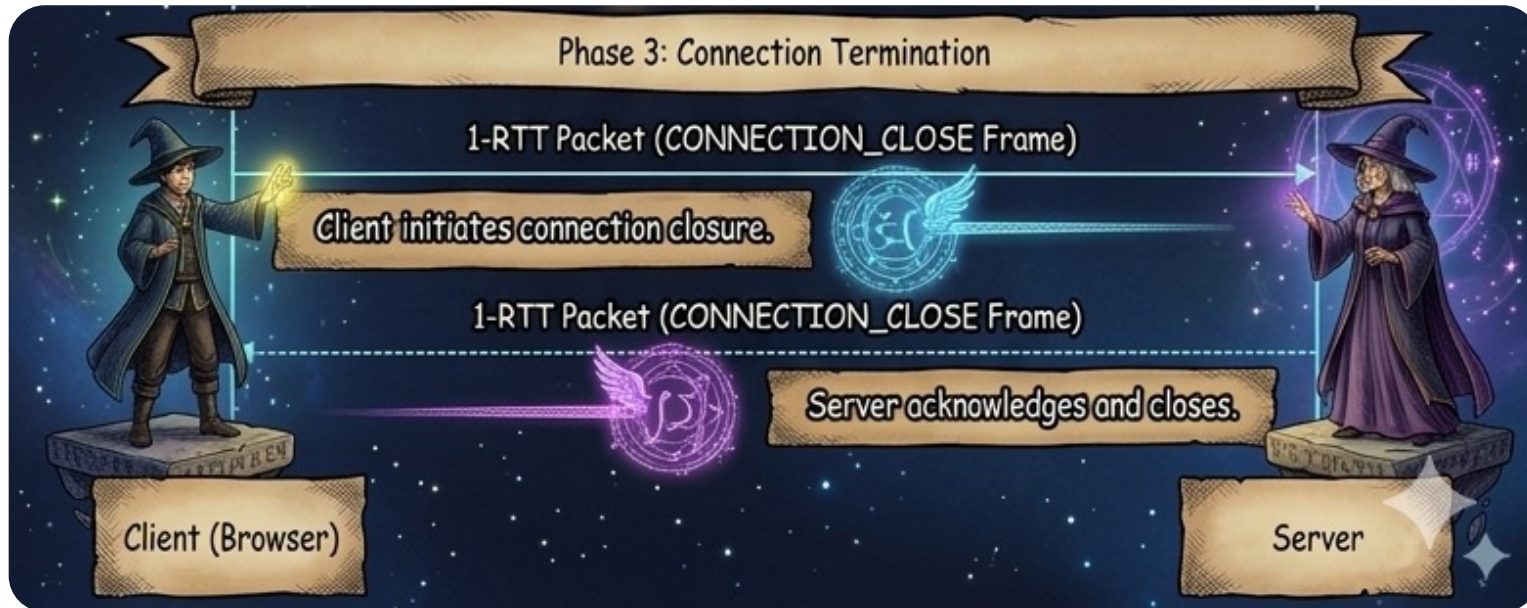
ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

The screenshot shows a network traffic capture in Wireshark. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Red boxes and arrows highlight specific fields:

- Packet 1: Initial, DCID=1cb3aaedf2921cb53399960c6a7c4fc3, SCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f
- Packet 2: Handshake, DCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f, SCID=0000000000000025e731248619e78fa64516d61
- Packet 3: Handshake, DCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f, SCID=0000000000000025e731248619e78fa64516d61
- Packet 4: Handshake, DCID=0000000000000025e731248619e78fa64516d61, SCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f
- Packet 5: SETTINGS
- Packet 6: HTTP3
- Packet 7: HTTP3
- Packet 8: HTTP3
- Packet 9: HTTP3
- Packet 10: Protected Payload (KP0), DCID=0000000000000025e731248619e78fa64516d61, PKN: 7, ACK
- Packet 11: Protected Payload (KP0), DCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f, PKN: 1, ACK
- Packet 12: HEADERS: 200 OK, DATA, STREAM(0)
- Packet 13: Protected Payload (KP0), DCID=0000000000000025e731248619e78fa64516d61, PKN: 8, ACK
- Packet 14: Protected Payload (KP0), DCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f, PKN: 3, MS
- Packet 15: Protected Payload (KP0), DCID=e863cf095b73f7a3c3b7d8a6d917212898e5dd6f, PKN: 4, PING

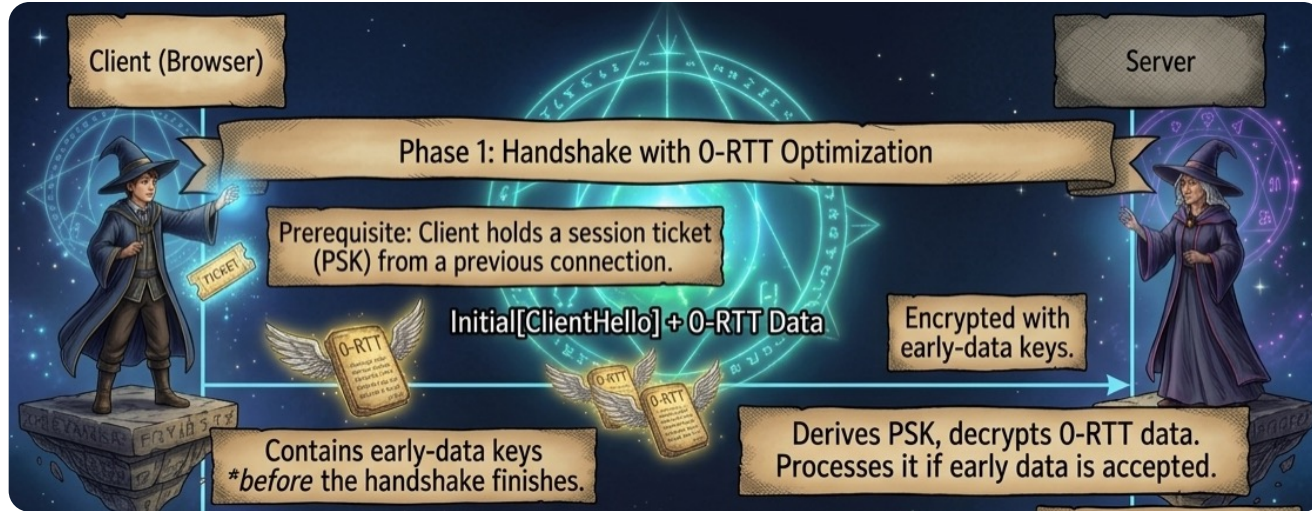
Red annotations include:

- Посылаем** (Send) pointing to the DCID field in packet 1.
- Досылаем** (Finish sending) pointing to the DCID field in packet 11.
- Фиксируем результат** (Fix the result) pointing to the HEADERS field in packet 12.

The bottom pane shows the details of the selected packet (packet 12), highlighting the 'supported_versions' extension in the TLSv1.3 Record Layer. The extension list includes TLS 1.3.

```
0000 06 00 40 ff 01 00 00 fb 03 03 a0 6c d2 f1 37 75 ..@.....l..7u
0010 ba 03 d2 4a 5d 5b 19 68 53 c6 c0 0b 85 91 d4 87 ...J][h S.....
0020 0a 67 b8 39 1c bd 56 cb ea b1 00 00 06 13 01 13 ...g·9·V·.....
0030 02 13 03 01 00 00 cc 00 00 00 16 00 14 00 00 11 ..:.....
0040 74 73 74 2e 70 6c 61 79 74 69 6d 65 2e 68 6f 6d tst.playtime.hom
0050 65 00 0a 00 08 00 06 00 1d 00 17 00 18 00 10 00 e.....
0060 05 00 03 02 68 33 00 0d 00 14 00 12 04 03 08 04 ...h3.....
0070 04 01 05 03 08 05 05 01 08 06 06 01 02 01 00 33 ..&·$.....6...i·
0080 00 26 00 24 00 1d 00 20 ee cb 36 9f d3 d9 69 0d ...R.:g·n·x·D·
0090 99 e3 52 94 3a 09 67 ed d9 1f 6e a7 f7 78 44 0a B·LC·\A·.....+
00a0 42 05 a7 6c 43 fe 5c 41 00 2d 00 02 01 01 00 2b .....9·J·.....
00b0 00 03 02 03 04 00 39 00 4a 01 04 80 01 d4 c0 03 ..:.....
00c0 04 80 00 ff f7 04 04 80 10 00 00 05 04 80 02 00 00 06 04 80 02 00 07 04 80 02 00 00 08 02 40 .....@
00d0 64 09 02 40 64 0a 01 03 0b 01 19 0c 00 0f 14 e8 d·@·d·.....
00e0 63 cf 09 5b 73 f7 a3 c3 b7 d8 a6 d9 17 21 28 98 c·[s·.....!(·
0100 e5 dd 6f ..o
```

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ



ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

The screenshot displays a Wireshark interface with a packet capture of a QUIC connection. The main pane shows a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A red circle highlights packet 1322, which is a '0-RTT, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e' packet. A handwritten note in Russian, 'Да есть же!', is written over this packet. Below the main pane, the 'Packet 1322' details pane is expanded to show the 'Decrypted QUIC' section, which includes the 'Reassembled TLS Handshake (1782 bytes)' details. The handshake details show 'Handshake Protocol: Client Hello (last fragment)' and 'Handshake Type: Client Hello (1)' with a length of 1778 bytes. The 'Version' is TLS 1.2 (0x0303). The 'Random' value is 1b4383ee7d5f92d448ec5d774b5ce890e1dad7bc1864e4df360b1c00d71de4a. The 'Session ID Length' is 0. The 'Cipher Suites Length' is 6. The 'Compression Methods Length' is 1. The 'Extensions Length' is 1731. The 'Extension: server_name (len=19) name=cloudflare.com' is present. The 'Extension: ec_point_formats (len=2)' is present. The 'Extension: session_ticket (len=0)' is present. The 'Extension: renegotiation_info (len=1)' is present. The 'Extension: extended_master_secret (len=0)' is present. The 'Extension: signed_certificate_timestamp (len=0)' is present. The 'Extension: early_data (len=0)' is present.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.153277	192.168.1.197	198.18.120.134	HTTP3	133	HEADERS: GET https://cloudflare.com/cdn-cgi/trace
12	0.285829	198.18.120.134	192.168.1.197	HTTP3	579	SETTINGS
13	0.285831	198.18.120.134	192.168.1.197	HTTP3	70	
14	0.286485	192.168.1.197	198.18.120.134	QUIC	86	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 3, A
15	0.287883	198.18.120.134	192.168.1.197	HTTP3	76	
16	0.287884	198.18.120.134	192.168.1.197	HTTP3	95	
17	0.288274	192.168.1.197	198.18.120.134	QUIC	86	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 4, A
18	0.288295	192.168.1.197	198.18.120.134	QUIC	88	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 5, S
19	0.291811	198.18.120.134	192.168.1.197	HTTP3	414	HEADERS: 200 OK, DATA
20	0.291814	198.18.120.134	192.168.1.197	HTTP3	72	DATA
21	0.292238	192.168.1.197	198.18.120.134	QUIC	86	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 6, A
22	0.292835	192.168.1.197	198.18.120.134	QUIC	84	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 7, C
23	0.303271	192.168.1.197	198.18.120.134	QUIC	1322	Initial, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e, PKN: 0, CRYPTO, C
24	0.303278	192.168.1.197	198.18.120.134	QUIC	1322	0-RTT, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e
25	0.303285	192.168.1.197	198.18.120.134	QUIC	152	0-RTT, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e
26	0.419726	198.18.120.134	192.168.1.197	QUIC	60	Protected Payload (KP0), DCID=08a32911, PKN: 12, ACK
27	0.420134	192.168.1.197	198.18.120.134	QUIC	84	Protected Payload (KP0), DCID=01da7a8f87a6475dc3d8f38f50a652ef0ceebcfa, PKN: 7, C
28	0.504611	192.168.1.197	198.18.120.134	QUIC	1322	Initial, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e, PKN: 2, CRYPTO, C
29	0.504687	192.168.1.197	198.18.120.134	QUIC	1322	Initial, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e, PKN: 3, PADDING, C
30	0.905716	192.168.1.197	198.18.120.134	QUIC	1322	Initial, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e, PKN: 4, CRYPTO, C
31	0.905796	192.168.1.197	198.18.120.134	QUIC	1322	Initial, DCID=0cfe7eba0c721786a9987072a1bd49f0, SCID=d1200f1e, PKN: 5, PADDING, C

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

Maximum Transmission Unit

Обычно 1 500 байт

ПРОТОКОЛЬНЫЕ ОПТИМИЗАЦИИ

Maximum Transmission Unit

Обычно 1 500 байт

Replay attack

Позволяет атакующему отправить тот же пакет

ШИФРОВАНИЕ

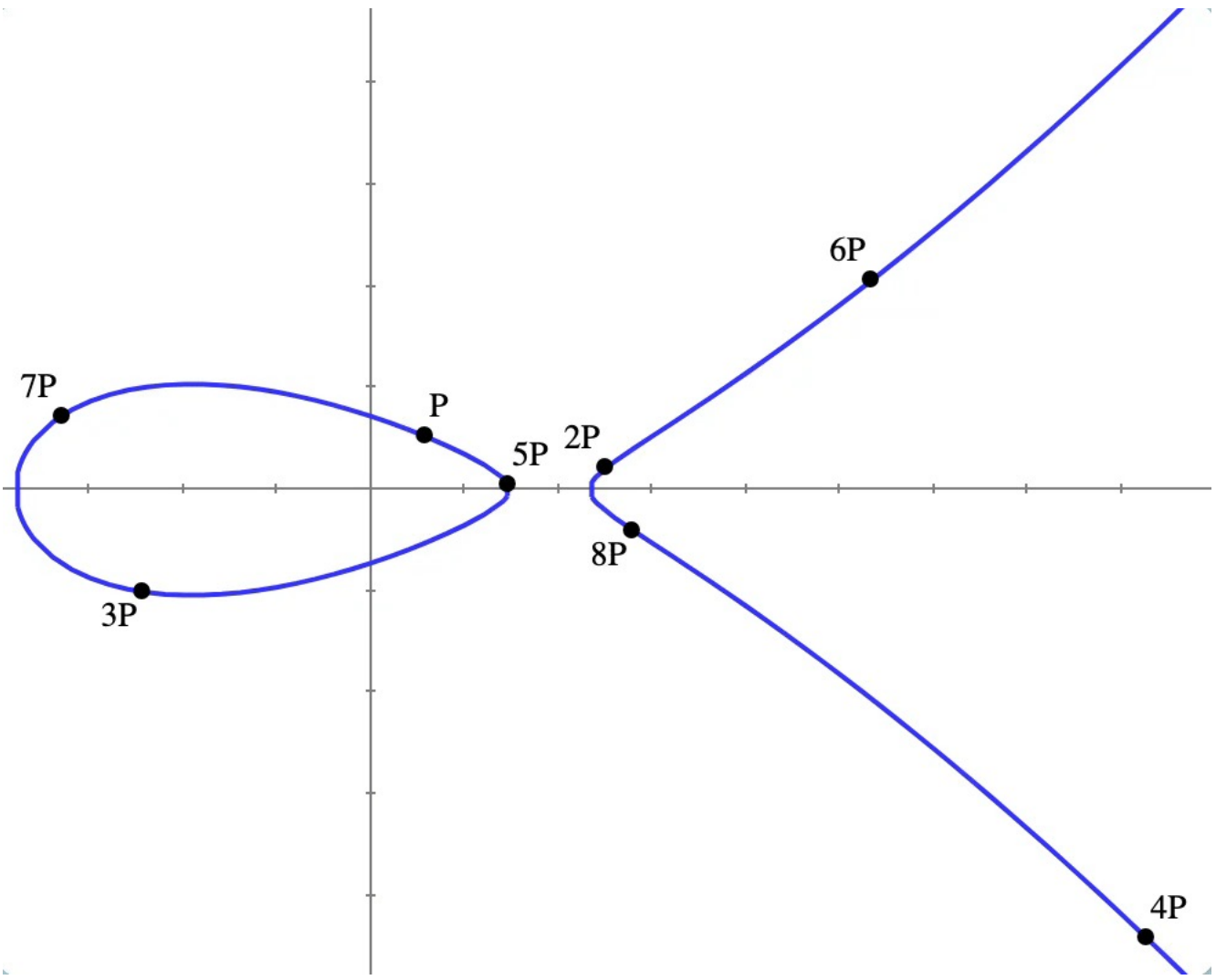
АЛГОРИТМЫ ШИФРОВАНИЯ



АЛГОРИТМЫ ШИФРОВАНИЯ



АЛГОРИТМЫ ШИФРОВАНИЯ



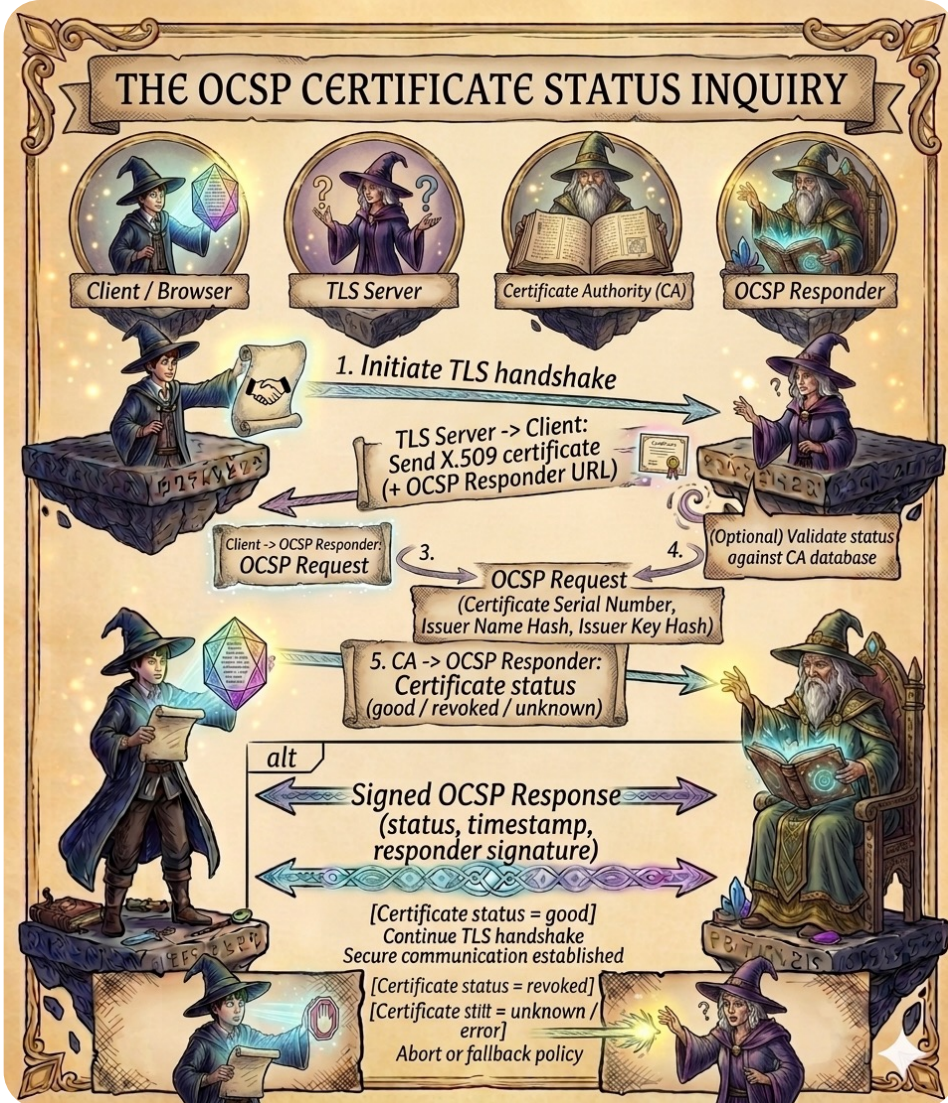
RSA

1. Требуется высокой энтропии
2. Требуется два больших простых числа
3. Кол-во бит ключа ≥ 2048

Curve25519

1. Не требователен к ГСЧ
2. Базовая точка лежит на кривой
3. Количество бит ключа всегда 256

OCSP STAPLING



OCSP STAPLING

```
└─$ openssl s_client -connect www.stackoverflow.com:443 -status -servername www.stackoverflow.com
Connecting to 198.252.206.1
CONNECTED(00000005)
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=E7
verify return:1
depth=0 CN=www.stackoverflow.com
verify return:1
OCSP responses: no responses sent
```

OCSP STAPLING



OCSP STAPLING

```
└─$ openssl s_client -connect www.cloudflare.com:443 -status -servername www.cloudflare.com
Connecting to 104.16.124.96
CONNECTED(00000006)
depth=2 C=US, O=Google Trust Services LLC, CN=GTS Root R4
verify return:1
depth=1 C=US, O=Google Trust Services, CN=WE1
verify return:1
depth=0 CN=www.cloudflare.com
verify return:1
OCSP responses: number of responses: 1
```

OCSP Response Data:

```
OCSP Response Status: successful (0x0)
Response Type: Basic OCSP Response
Version: 1 (0x0)
Responder Id: 9077923567C4FFA8CCA9E67BD980797BCC93F938
Produced At: Apr 18 20:28:36 2026 GMT
Responses:
Certificate ID:
  Hash Algorithm: sha1
  Issuer Name Hash: B9BED5F1A61E40B24196B0C29E7E1A9D8BFCB520
  Issuer Key Hash: 9077923567C4FFA8CCA9E67BD980797BCC93F938
  Serial Number: FC16480808FFC32B13ADE752E0C4B713
Cert Status: good
This Update: Apr 18 20:28:36 2026 GMT
Next Update: Apr 25 19:28:35 2026 GMT
```

Signature Algorithm: ecdsa-with-SHA256

Signature Value:

```
30:46:02:21:00:c1:ca:80:53:b4:fc:64:66:08:a4:f1:30:86:
3c:91:98:2c:7a:68:6d:35:50:35:23:f1:d9:0d:ea:7b:a1:ef:
b9:02:21:00:90:f4:94:36:12:6e:93:7b:52:86:97:e5:d2:64:
f5:4f:9f:bb:97:2d:2d:20:d5:ae:60:40:25:06:51:e4:e5:9a
```

ПРО ФАЙЛЫ

1

Проверка пути

Путь `../../././%20\ flag.png`
точно валидный?

1

Проверка пути

Путь `../../././%20\ flag.png`
точно валидный?

2

Метаданные

С какой ФС работаем?
Есть ли права на чтение?

1

Проверка пути

Путь `../../././%20\ flag.png`
точно валидный?

2

Метаданные

С какой ФС работаем?
Есть ли права на чтение?

3

Создание файлового дескриптора

Наконец-то начинаем читать.

1

Проверка пути

Путь `./.././../%20\ flag.png`
точно валидный?

2

Метаданные

С какой ФС работаем?
Есть ли права на чтение?

3

Создание файлового дескриптора

Наконец-то начинаем читать.

4

А откуда читать?

Попадаем в кеш, если ранее
уже читали, и напрямую с
диска, если нет.

1

Проверка пути

Путь `./.././../%20\ flag.png`
точно валидный?

2

Метаданные

С какой ФС работаем?
Есть ли права на чтение?

3

Создание файлового дескриптора

Наконец-то начинаем читать.

4

А откуда читать?

Попадаем в кеш, если ранее уже читали, и напрямую с диска, если нет.

5

Копирование

Происходит из пространства ядра в пользовательское.

1

Проверка пути

Путь `./.././../%20\ flag.png`
точно валидный?

2

Метаданные

С какой ФС работаем?
Есть ли права на чтение?

3

Создание файлового дескриптора

Наконец-то начинаем читать.

4

А откуда читать?

Попадаем в кеш, если ранее уже читали, и напрямую с диска, если нет.

5

Копирование

Происходит из пространства ядра в пользовательское.

6

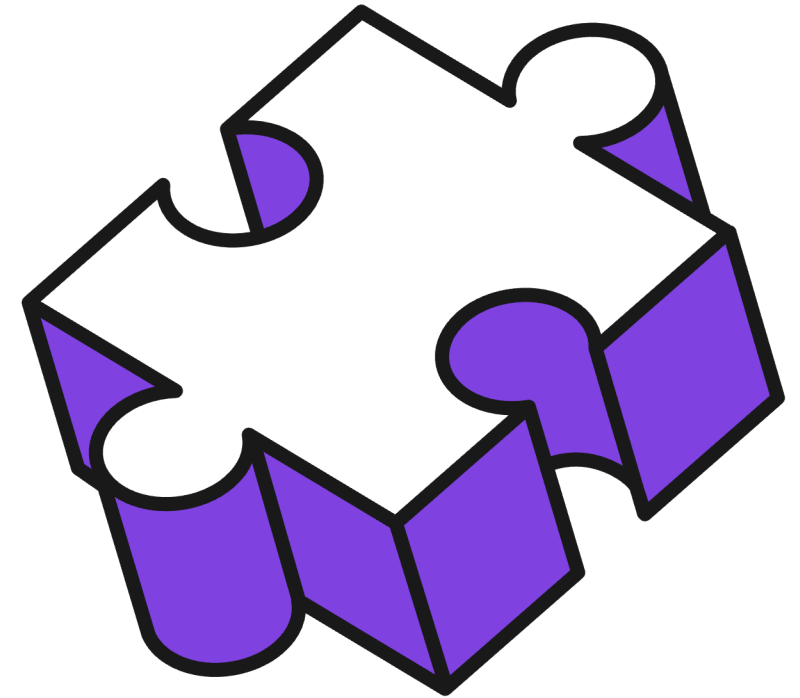
Финишная прямая

Данные получены, теперь их можно отправить пользователю.

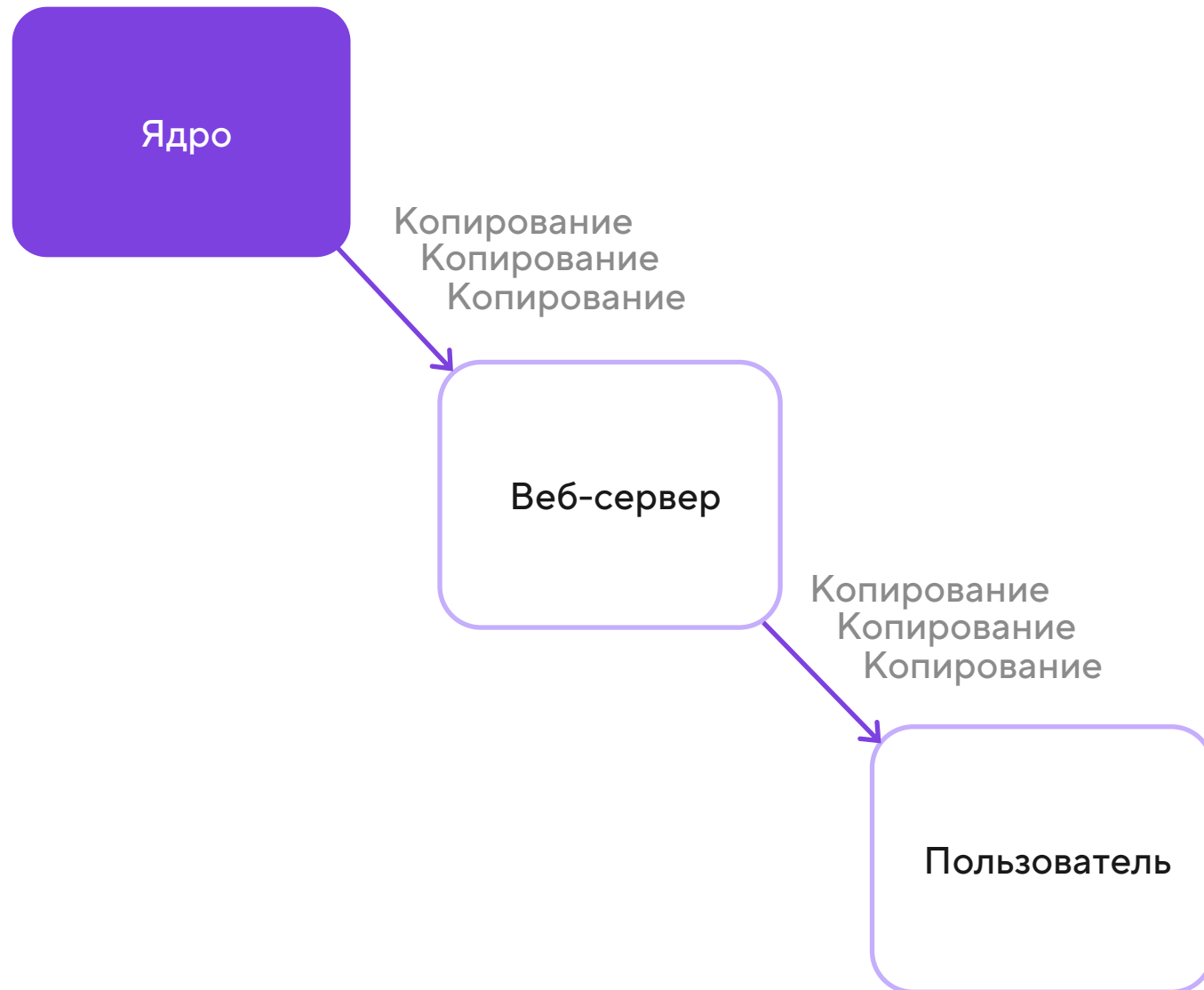
BLAZINGLY FAST

Незамеченные подводные камни

1. Копирование из ядра
в пользовательское пространство
2. Всё синхронно
3. Большие файлы не помещаются в кеш



ПРО ФАЙЛЫ



Огр не понимает



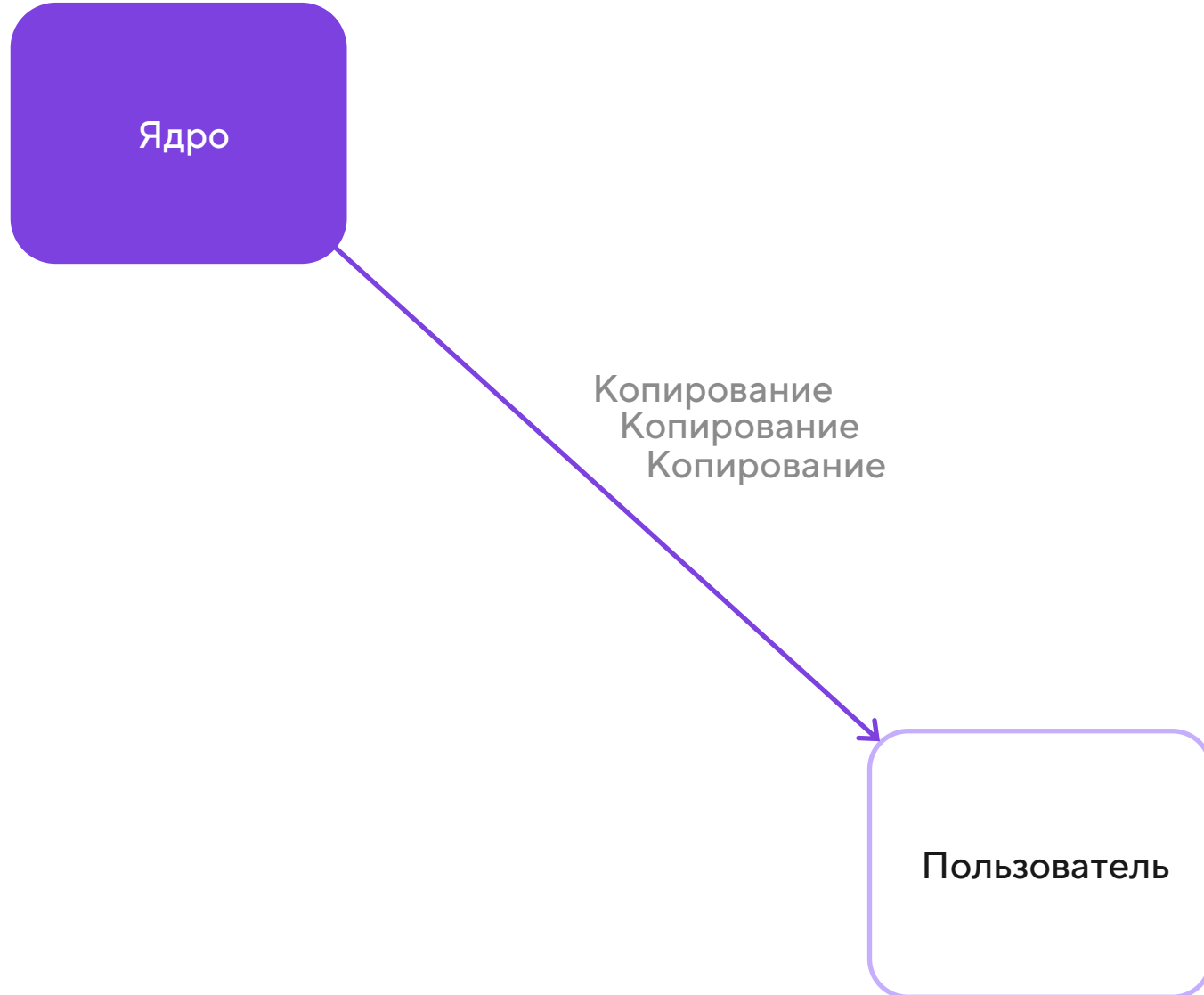
ПРО ФАЙЛЫ

```
const express = require('express');
const app = express();
const path = require('path');
const PORT = 3000;

app.get('/', function (req, res) {
  const options = {
    root: path.join(__dirname)
  };

  const fileName = 'Hello.txt';
  res.sendFile(fileName, options, function (err) {
    if (err) {
      console.error('Error sending file:', err);
    } else {
      console.log('Sent:', fileName);
    }
  });
});
```

ПРО ФАЙЛЫ



Огр одобряет

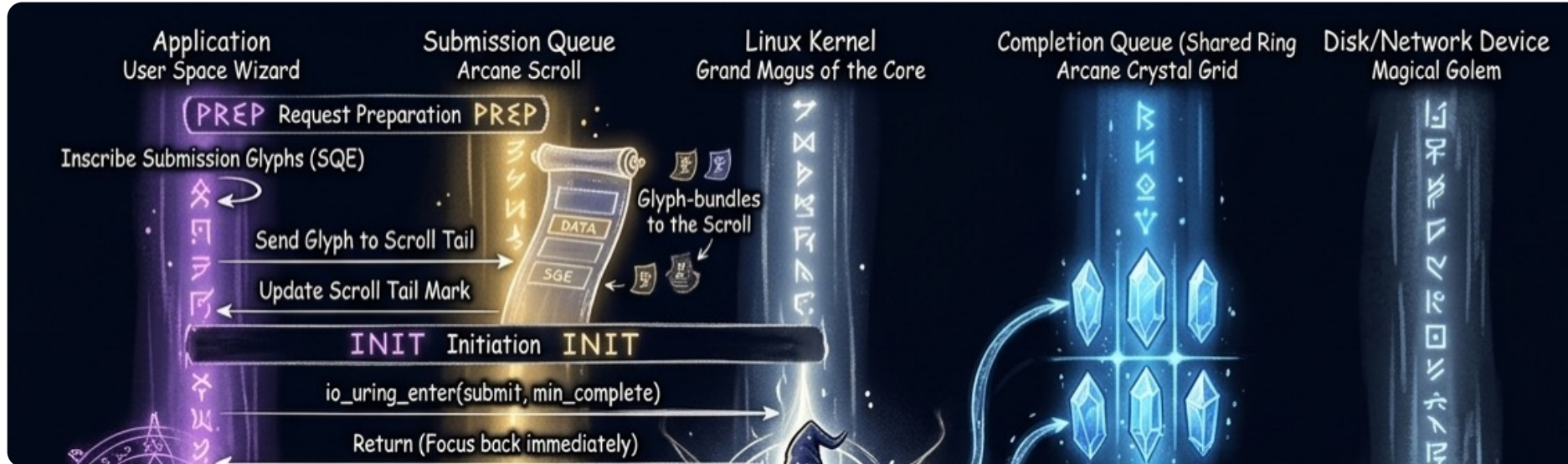


ПРО ФАЙЛЫ

```
const file = fs.readFileSync('index.html');  
response.write(file);
```



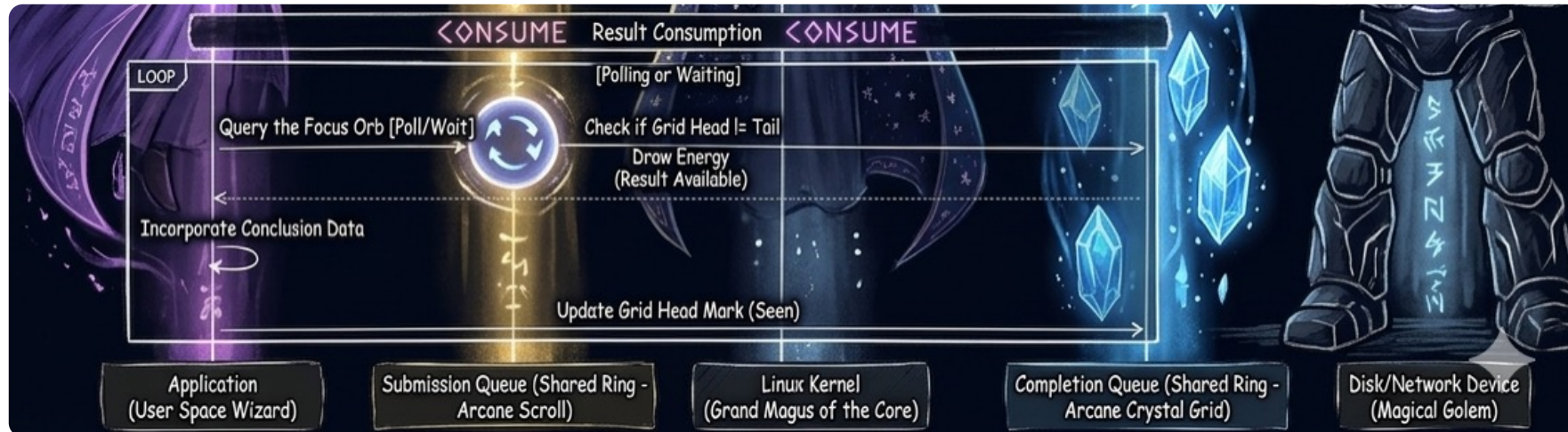
ПРО ФАЙЛЫ



ПРО ФАЙЛЫ



ПРО ФАЙЛЫ



ПРО ФАЙЛЫ



```
const file = await fs.readFile('index.html');  
response.write(file);
```

ПРО ФАЙЛЫ

точка банк



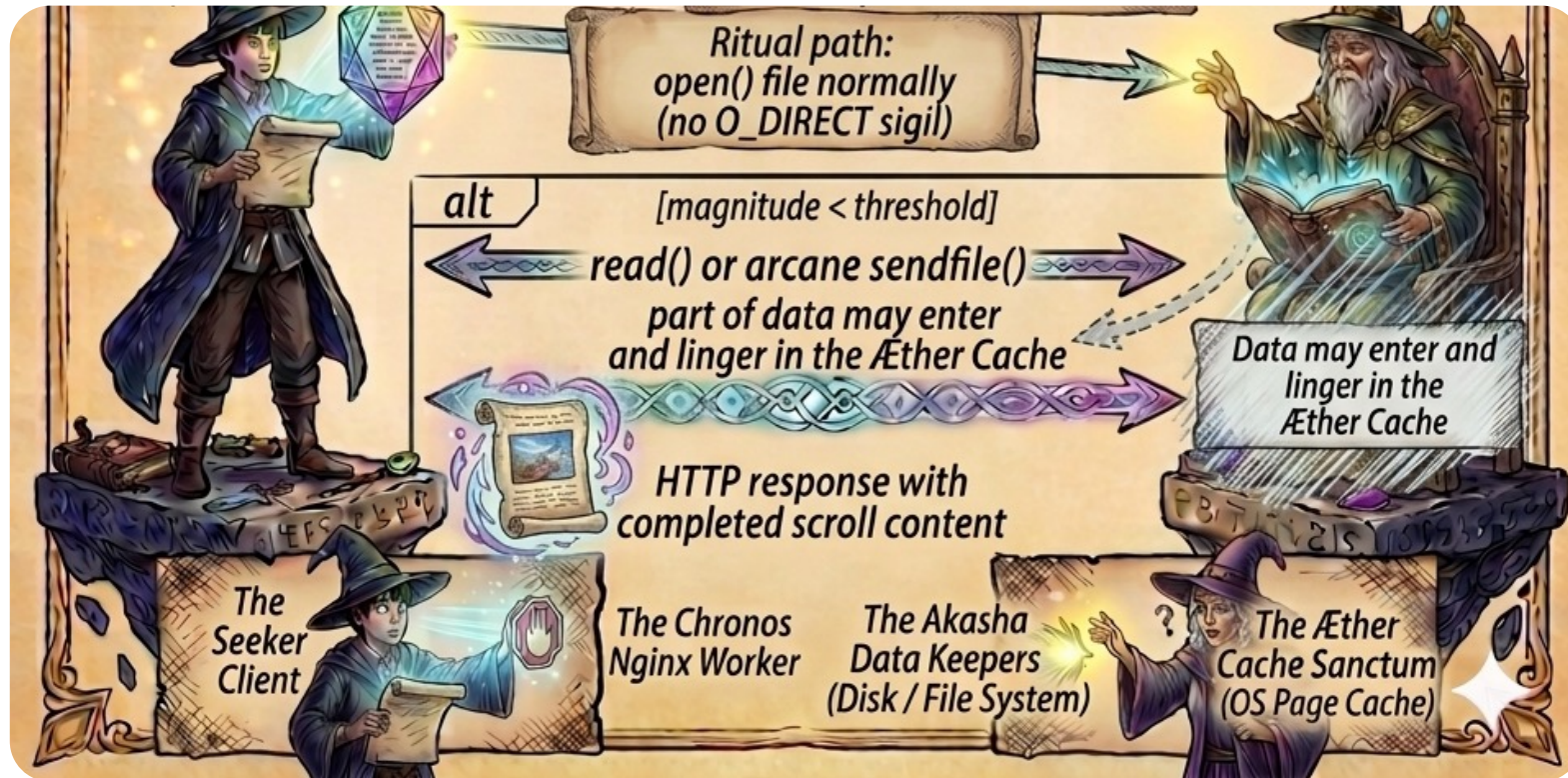
ПРО ФАЙЛЫ

точка банк





ПРО ФАЙЛЫ



ПРО ФАЙЛЫ

точка банк



КОМПРЕССИЯ

СЖАТИЕ – ЭТО БАЗА

► POST

Status	200 ?
Version	HTTP/2
Transferred	15.76 kB (714.09 kB size) ← x45
Referrer Policy	unsafe-url
DNS Resolution	System

▼ Response Headers (436 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin:
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: gzip ← GNU Zip

СЖАТИЕ – ЭТО БАЗА

► POST

Status	200 ?
Version	HTTP/2
Transferred	15.76 kB (714.09 kB size) ← x45
Referrer Policy	unsafe-url
DNS Resolution	System

▼ Response Headers (436 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin:
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: gzip ← GNU Zip

► POST

Status	200 ?
Version	HTTP/2
Transferred	8.92 kB (714.09 kB size) ← x80
Referrer Policy	unsafe-url
DNS Resolution	System

▼ Response Headers (436 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin:
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: zstd ← Zstandard

СЖАТИЕ – ЭТО БАЗА

► POST

Status	200 ?
Version	HTTP/2
Transferred	15.76 kB (714.09 kB size) ← x45
Referrer Policy	unsafe-url
DNS Resolution	System

▼ Response Headers (436 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin: GNU Zip
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: gzip ←

► POST

Status	200 ?
Version	HTTP/2
Transferred	4.83 kB (714.09 kB size) ← x147
Referrer Policy	strict-origin-when-cross-origin
DNS Resolution	System

▼ Response Headers (434 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin: brotli
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: br ←

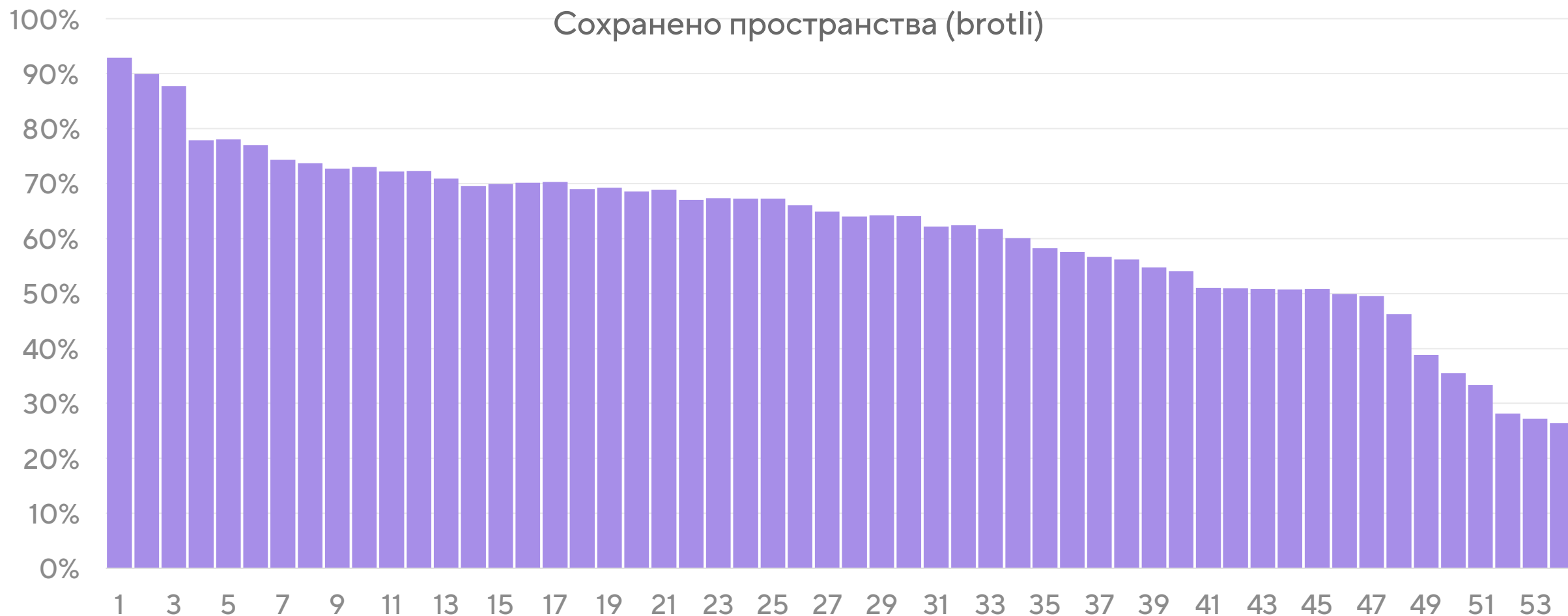
► POST

Status	200 ?
Version	HTTP/2
Transferred	8.92 kB (714.09 kB size) ← x80
Referrer Policy	unsafe-url
DNS Resolution	System

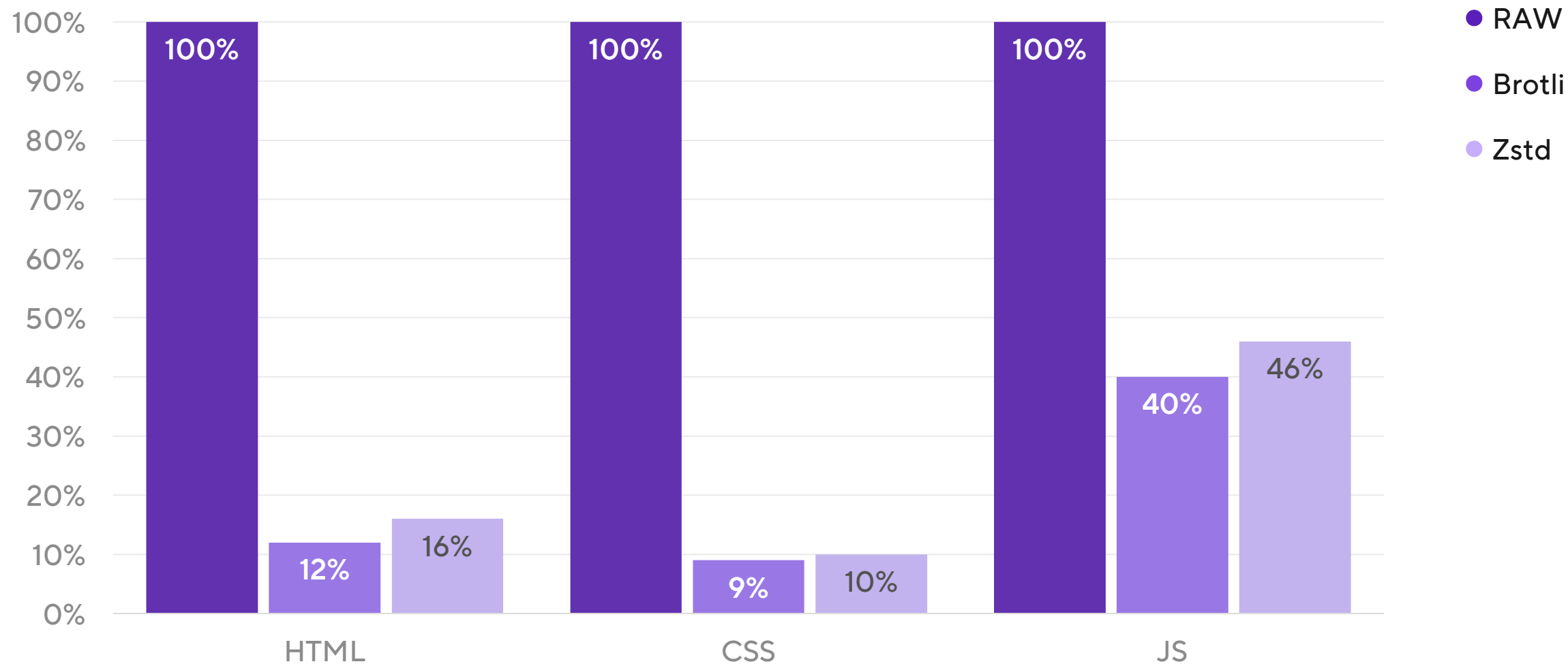
▼ Response Headers (436 B)

- ? access-control-allow-credentials: true
- ? access-control-allow-origin: Zstandard
- ? access-control-expose-headers: Content-Disposition
- ? content-encoding: zstd ←

СЖАТИЕ – ЭТО БАЗА



СЖАТИЕ – ЭТО БАЗА



DICTIONARY-BASED COMPRESSION

DVC – ЭТО НОВАЯ БАЗА



DVC – ЭТО НОВАЯ БАЗА



DVC – ЭТО НОВАЯ БАЗА

The image shows a browser's developer tools interface. On the left, the 'Network' panel displays a list of network requests. The top request is highlighted with a red box and has a red arrow pointing to the 'content-encoding: br' header in the 'Headers' panel on the right.

Transferred	Size	Priority
125.99 kB	459.60 kB	Highest
Blocked By uBlock Origin		
936 B	258 B	Low
2.93 kB	2.40 kB	Low
40.29 kB	39.46 kB	High
22.89 kB	22.06 kB	High
0 B	344 B	Lowest
0 B	60 B	Lowest
0 B	288 B	Lowest
0 B	660 B	Lowest
0 B	496 B	Lowest

Headers Cookies Request Response Timings

Filter Headers

GET https://www.google.com/search?q=test

Status 200 ?

Version HTTP/2

Transferred 125.99 kB (459.60 kB size)

Request Priority Highest

DNS Resolution System

Response Headers (1.593 kB)

accept-ch: Sec-CH-Prefers-Color-Scheme

alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

cache-control: private, max-age=0

content-encoding: br

DVC – ЭТО НОВАЯ БАЗА

The image shows a browser's developer tools interface. On the left, the 'Network' panel displays a list of network requests. The first request is highlighted in blue, with its 'Transferred' size (73.42 kB) and 'Size' (461.28 kB) columns circled in red. A red arrow points from the 'Size' column to the 'Headers' panel on the right. The 'Headers' panel shows the request details for 'GET https://www.google.com/search?q=test'. The status is 200. The 'Response Headers' section is expanded, showing several headers, with 'content-encoding: dcb' circled in red. Other headers include 'accept-ch', 'alt-svc', and 'cache-control'.

Transferred	Size	Priority
73.42 kB	461.28 kB	Highest
Blocked By uBlock Origin		Lowest
Blocked By uBlock Origin		Lowest
937 B	258 B	Low
2.93 kB	2.40 kB	Low
40.29 kB	39.46 kB	High
0 B	344 B	Lowest
0 B	60 B	Lowest
0 B	288 B	Lowest
0 B	660 B	Lowest
0 B	496 B	Lowest

Headers Cookies Request Response Timings

Filter Headers

GET https://www.google.com/search?q=test

Status 200 ?

Version HTTP/2

Transferred 73.42 kB (461.28 kB size)

Request Priority Highest

DNS Resolution System

Response Headers (1.431 kB)

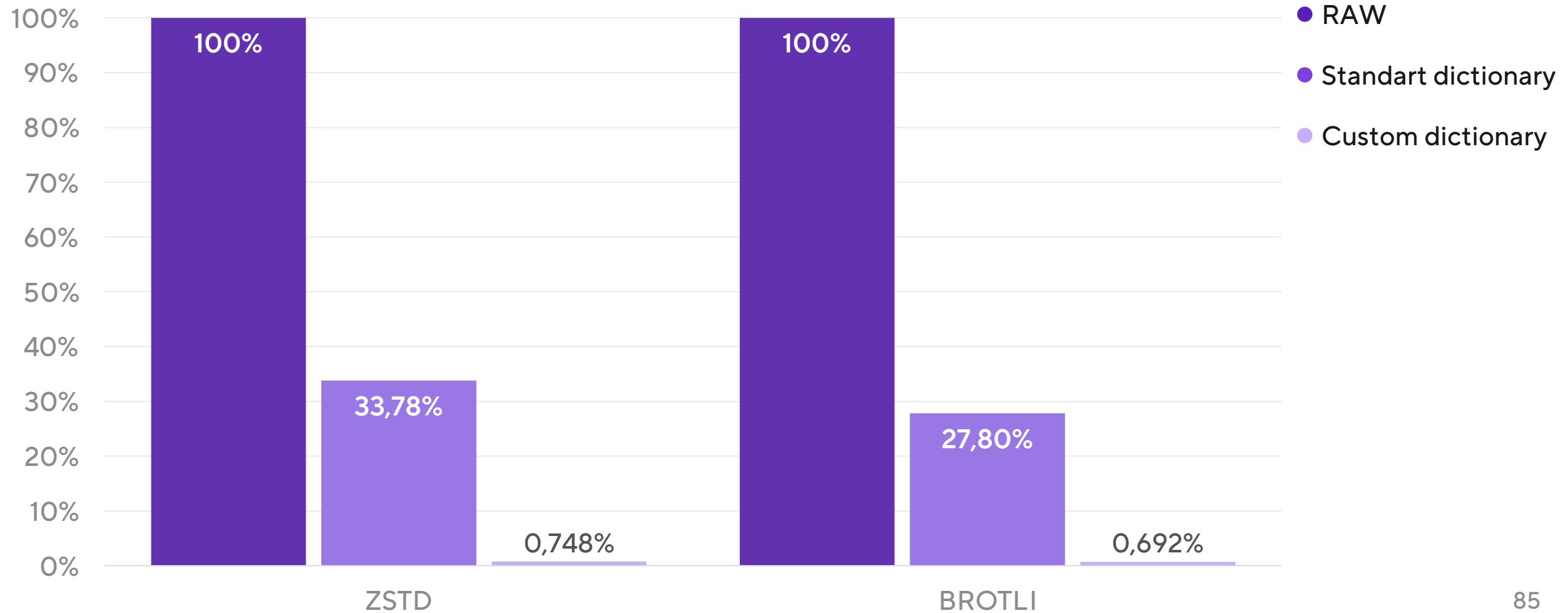
accept-ch: Sec-CH-Prefers-Color-Scheme

alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

cache-control: private, max-age=0

content-encoding: dcb

DVC – ЭТО НОВАЯ БАЗА



EARLY HINTS



Как мы в 4 раза
ускорили мобильную
версию ВКонтакте



Тарас
Иванов

ВКонтакте

EARLY HINTS

```
Link: <https://fonts.googleapis.com/>; rel=dns-prefetch
```

```
Link: <https://cdn.example.com>; rel=preconnect, <https://cdn.example.com>; rel=preconnect; crossorigin
```

```
Link: </style.css>; rel=preload; as=style; fetchpriority=high
```

```
Link: </vendors.js>; rel=modulepreload; as=script; fetchpriority=high
```

```
Link: </dictionary.dat>; rel="compression-dictionary"
```

EARLY HINTS

```
<link rel="dns-prefetch" href="https://fonts.googleapis.com/">  
<link rel="preconnect" href="https://cdn.example.com">  
<link rel="preconnect" href="https://cdn.example.com" crossorigin>  
<link rel="preload" href="/style.css" as="style" fetchpriority="high">  
<link rel="modulepreload" href="/vendors.js" as="script" fetchpriority="high">  
<link rel="compression-dictionary" href="/dictionary.dat">
```

СПЕКУЛЯТИВНЫЕ ПРАВИЛА

СПЕКУЛЯТИВНЫЕ ПРАВИЛА

точка банк



Ускорение веб-приложений за счет предзагрузки страниц: опыт Ozon



Юрий Амелин
Ozon Tech

СПЕКУЛЯТИВНЫЕ ПРАВИЛА

```
<script type="speculationrules">
  {
    "prerender": [
      {
        "where": {
          "href_matches": "/me"
        },
        // Политика загрузки: immediate – "настолько быстро, насколько возможно"
        "eagerness": "immediate"
      },
      {
        "where": {
          "selector_matches": ".product .with-banner"
        },
        // Политика загрузки: moderate – предзагрузка запускается через
        // Десктоп: 10 мс после наведения курсора
        // Мобилки: 50 мс после попадания кандидата во viewport
        "eagerness": "eager"
      },
      {
        "where": {
          "selector_matches": ".promoted-product"
        },
        // Политика загрузки: moderate – предзагрузка запускается через
        // Десктоп: 200 мс после наведения курсора
        // Мобилки: 500 мс после остановки скrolла и в пределах 30% viewport'a от предыдущего кандидата
        "eagerness": "moderate"
      }
    ]
  }
</script>
```

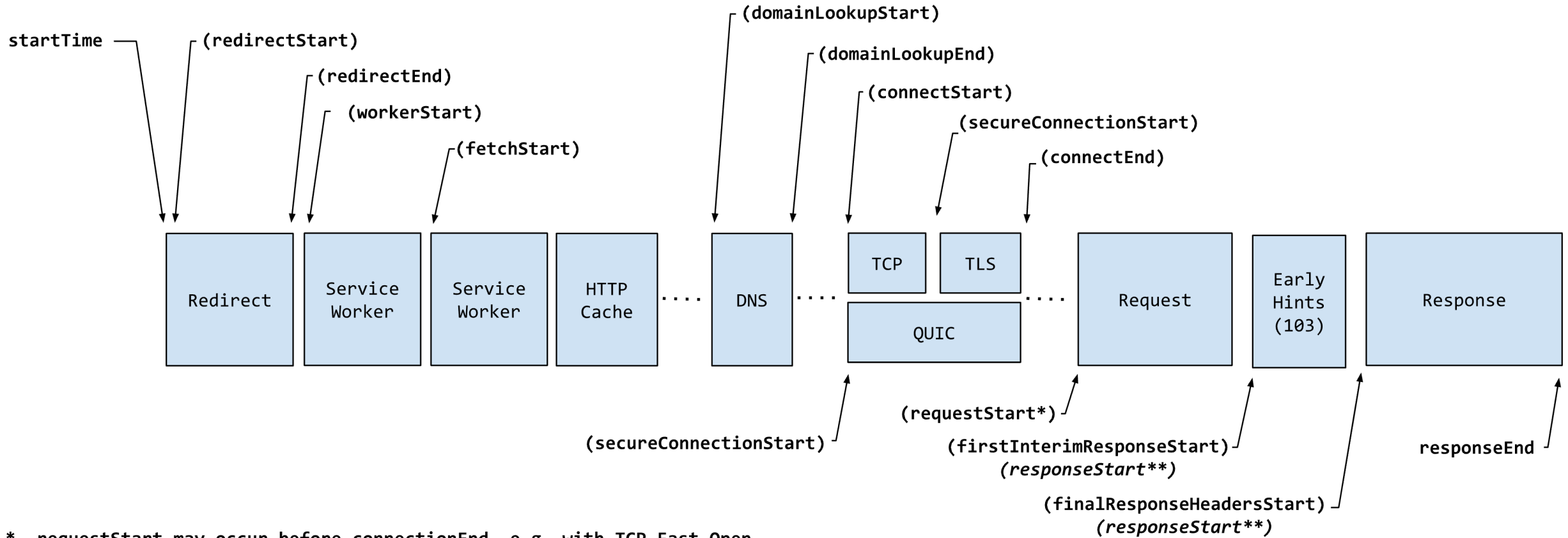
СЕРВИС-ВОРКЕР



Ускорение веб-приложений за счет предзагрузки страниц: опыт Ozon



Юрий Амелин
Ozon Tech



* requestStart may occur before connectionEnd, e.g. with TCP Fast Open

** responseStart is equal to firstInterimResponseStart if non-zero or finalResponseHeadersStart

.... Client-side delays can occur before the DNS, TCP/QUIC, and request phases, e.g. due to connection/in-flight request limit.

СОВРЕМЕННЫЕ ФОРМАТЫ МЕДИА

СОВРЕМЕННЫЕ ФОРМАТЫ МЕДИА

```
<picture>
  <source                                76kB
    srcset="/a-squoosh-screenshot-show-37b8d06c5a8c5_1920.avif"
    type="image/avif"
  />
  <source                                126kB
    srcset="/a-squoosh-screenshot-show-37b8d06c5a8c5_1920.webp"
    type="image/webp"
  />
  <source                                487kB
    srcset="/a-squoosh-screenshot-show-37b8d06c5a8c5_1920.jpg"
    type="image/jpeg"
  />
  
</picture>
```

МНШ ДНХ = ЛЧШ

МЕНЬШЕ ДАННЫХ = ЛУЧШЕ

точка банк

```
fursov@Fursovs-MBP /Volumes/ADATA SD810  
$ ll bank.html  
-rwx-----@ 1 fursov  staff  1.2M Feb 26 10:27 bank.html
```

МЕНЬШЕ ДАННЫХ = ЛУЧШЕ

```
fursov@Fursovs-MBP /Volumes/ADATA SD810  
$ ll bank.html  
-rwx-----@ 1 fursov  staff  1.2M Feb 26 10:27 bank.html
```

```
vim NORMAL / bank.html  
3992 matches on 34 lines
```

МЕНЬШЕ ДАННЫХ = ЛУЧШЕ

```
fursov@Fursovs-MBP /Volumes/ADATA SD810  
$ ll bank.html  
-rwx-----@ 1 fursov  staff   1.2M Feb 26 10:27 bank.html
```

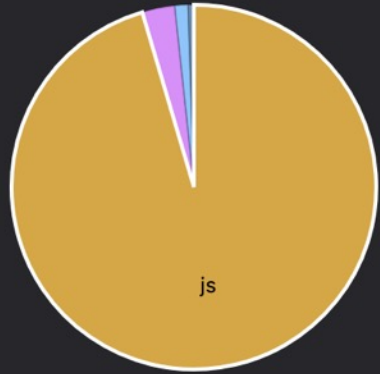
```
vim NORMAL / bank.html  
3992 matches on 34 lines
```

```
fursov@Fursovs-MBP /Volumes/ADATA SD810  
$ ll bank-cleared.html  
-rwx-----@ 1 fursov  staff   26K Feb 26 10:58 bank-cleared.html
```


В ЗАВЕРШЕНИЕ

В ЗАВЕРШЕНИЕ

Primed cache ?



Type	Size	Transferred	Time	Non blocking time
22 js	1,772.99 kB	483 kB	0 s	0 s
3 images	53.39 kB	20.47 kB	0 s	0 s
2 css	21.81 kB	0 kB	0 s	0 s
1 html	9.20 kB	1.53 kB	0.02 s	0.02 s
5 xhr	0.65 kB	2.62 kB	1.11 s	1.11 s
1 ws	0 kB	0.28 kB	0.53 s	0.53 s

Cached responses: 0
Total requests: 34
Size: 1,858.04 kB
Transferred Size: 507.89 kB
Time: 1.66 seconds
Non blocking time: 1.66 seconds



Performance



Accessibility



Best Practices



SEO

**СОФТЫ ТОЖЕ
ВАЖНЫ**

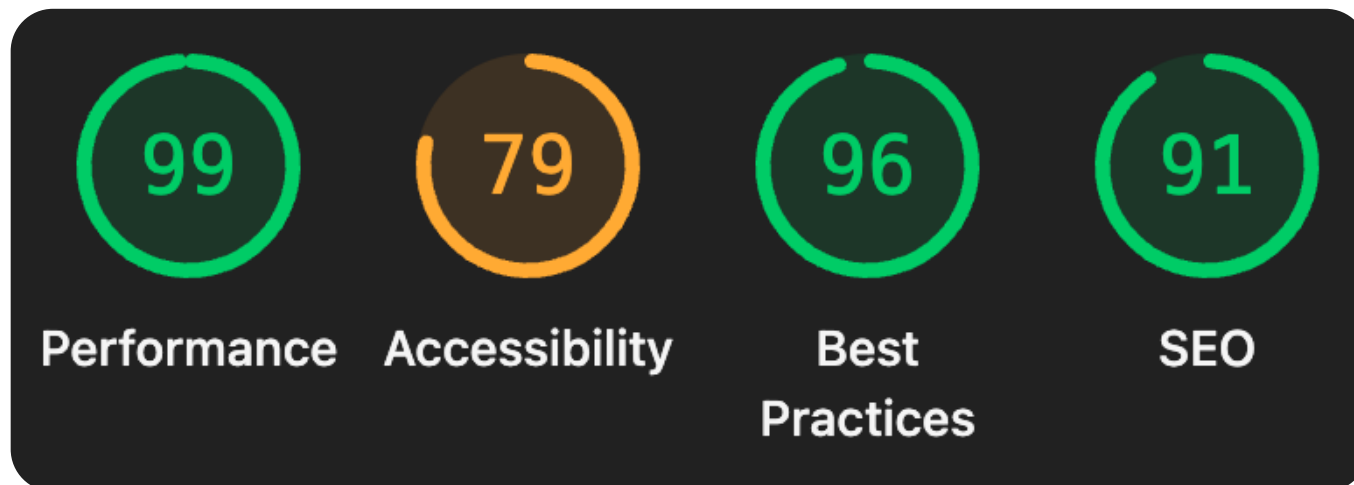
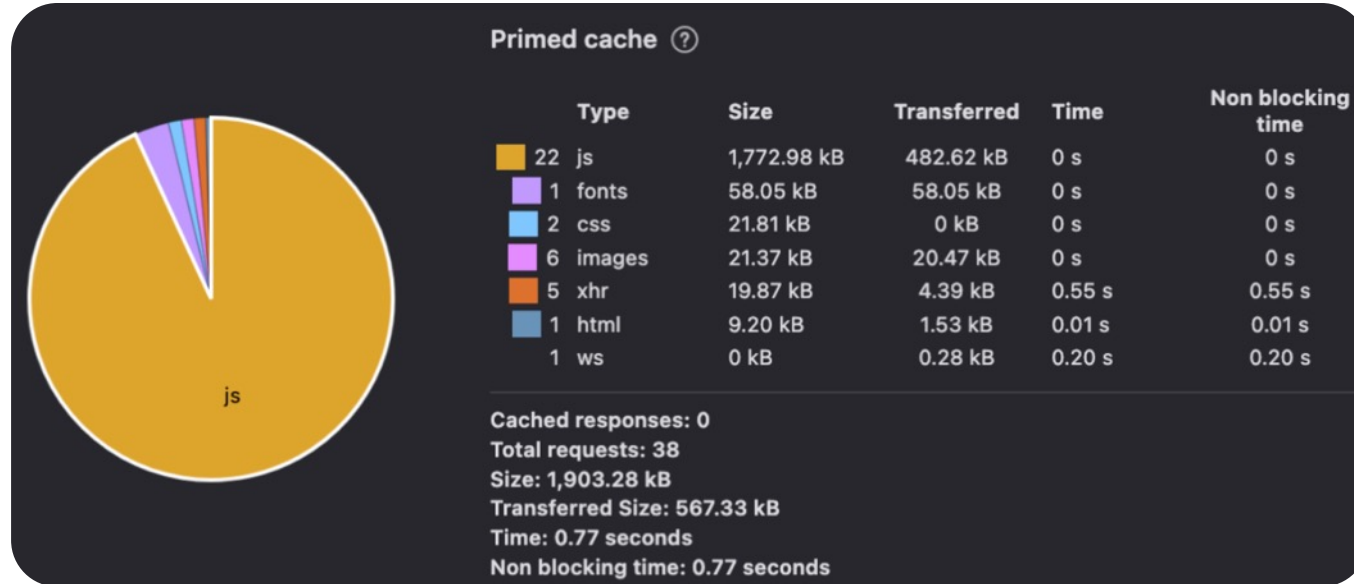
СОФТЫ ТОЖЕ ВАЖНЫ

точка банк

Достаточно просто
поговорить



~~В ЗАВЕРШЕНИЕ~~ (ИСПРАВЛЕНО)



точка банк



Здесь преза

Здесь я

**СПАСИБО
ЗА ВНИМАНИЕ!**

