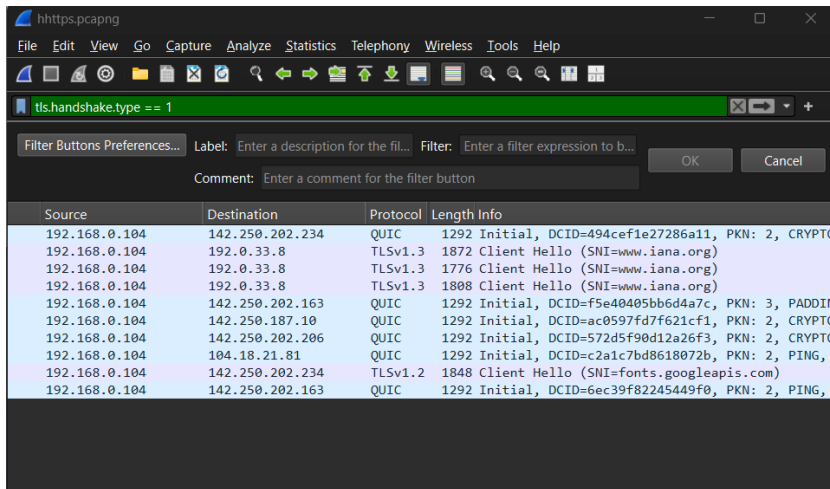


## Task 5: HTTPS Traffic Analysis

### Q1. Identify the website to which the client is connecting.

The client is connecting to the website: **www.iana.org**

This was identified from the TLS Client Hello message (SNI extension).



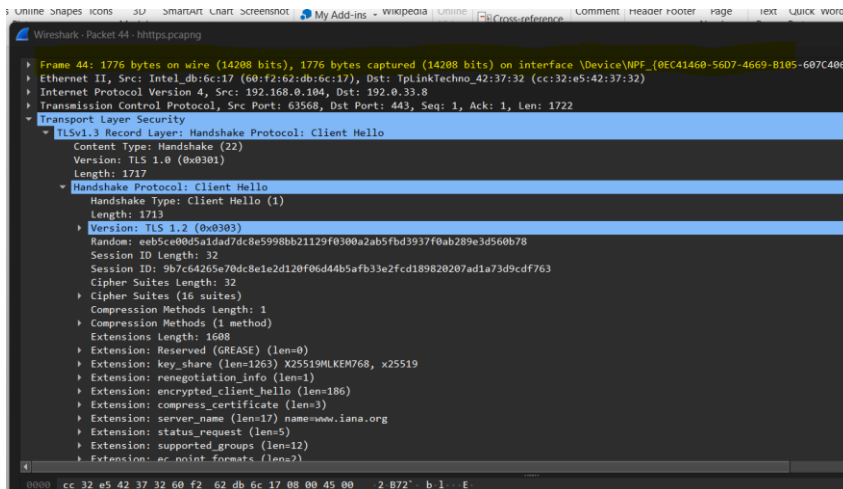
The image shows a Wireshark packet capture window titled 'hhttps.pcapng'. The filter bar at the top is set to 'tls.handshake.type == 1'. Below the filter bar, there is a table of captured packets. The table has columns for Source, Destination, Protocol, and Length Info. The packets are as follows:

Source	Destination	Protocol	Length Info
192.168.0.104	142.250.202.234	QUIC	1292 Initial, DCID=494cef1e27286a11, PKN: 2, CRYPTO
192.168.0.104	192.0.33.8	TLSv1.3	1872 Client Hello (SNI=www.iana.org)
192.168.0.104	192.0.33.8	TLSv1.3	1776 Client Hello (SNI=www.iana.org)
192.168.0.104	192.0.33.8	TLSv1.3	1808 Client Hello (SNI=www.iana.org)
192.168.0.104	142.250.202.163	QUIC	1292 Initial, DCID=f5e40405bb6d4a7c, PKN: 3, PADDI
192.168.0.104	142.250.187.10	QUIC	1292 Initial, DCID=ac0597fd7f621cf1, PKN: 2, CRYPTO
192.168.0.104	142.250.202.206	QUIC	1292 Initial, DCID=572d5f90d12a26f3, PKN: 2, CRYPTO
192.168.0.104	104.18.21.81	QUIC	1292 Initial, DCID=c2a1c7bd8618072b, PKN: 2, PING,
192.168.0.104	142.250.202.234	TLSv1.2	1848 Client Hello (SNI=fonts.googleapis.com)
192.168.0.104	142.250.202.163	QUIC	1292 Initial, DCID=6ec39f82245449f0, PKN: 2, PING,

### Q2. Find the Client Hello message in the capture. Which frame contains it?

The Client Hello message is found in Frame 44.

This marks the beginning of the TLS handshake initiated by the client.



The image shows the packet details pane for Frame 44 in Wireshark. The frame is selected, and the details are expanded to show the TLSv1.3 Record Layer: Handshake Protocol: Client Hello. The details are as follows:

- Frame 44: 1776 bytes on wire (14208 bits), 1776 bytes captured (14208 bits) on interface \Device\NPF\_{0EC41460-56D7-4669-B105-607C4069}
- Ethernet II, Src: Intel\_db:6c:17 (60:f2:62:db:6c:17), Dst: TpLinkTechno\_42:37:32 (cc:32:e5:42:37:32)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.0.33.8
- Transmission Control Protocol, Src Port: 63568, Dst Port: 443, Seq: 1, Ack: 1, Len: 1722
- Transport Layer Security
  - TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.0 (0x0301)
    - Length: 1717
    - Handshake Protocol: Client Hello
      - Handshake Type: Client Hello (1)
      - Length: 1713
      - Version: TLS 1.2 (0x0303)
      - Random: eeb5ce00d5aldad7dc8e5998bb21129f0300a2ab5fbd3937f0ab289e3d560b78
      - Session ID Length: 32
      - Session ID: 9b7c64265e70dc8e1e2d120f06d44b5afb33e2fcd189820207ad1a73d9cdf763
      - Cipher Suites Length: 32
      - Cipher Suites (16 suites)
      - Compression Methods Length: 1
      - Compression Methods (1 method)
      - Extensions Length: 1608
      - Extension: Reserved (GREASE) (len=0)
      - Extension: key\_share (len=1263) X25519MLKEM768, x25519
      - Extension: renegotiation\_info (len=1)
      - Extension: encrypted\_client\_hello (len=186)
      - Extension: compress\_certificate (len=3)
      - Extension: server\_name (len=17) name=www.iana.org
      - Extension: status\_request (len=5)
      - Extension: supported\_groups (len=12)
      - Extension: ec\_point\_formats (len=2)

### Q3. List the extensions present in the Client Hello message.

The Client Hello message (Frame 44) includes several extensions, such as:

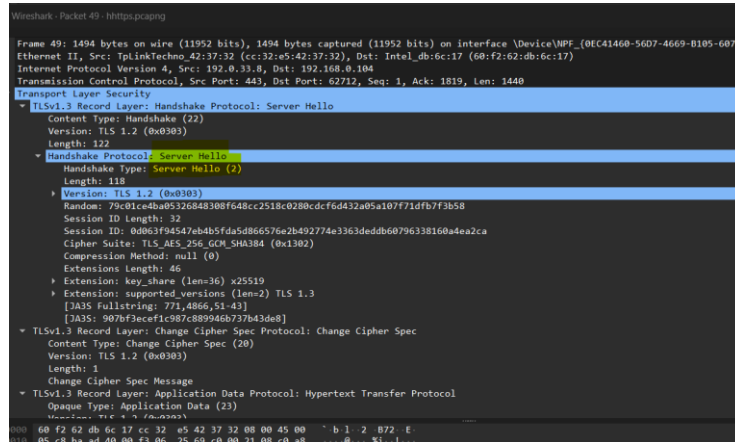
- Reserved (GREASE)
- key\_share (X25519MLKEM768, x25519)
- renegotiation\_info
- encrypted\_client\_hello
- compress\_certificate
- server\_name (www.iana.org)
- status\_request
- supported\_groups
- ec\_point\_formats
- Unknown type 17613
- session\_ticket
- psk\_key\_exchange\_modes
- signed\_certificate\_timestamp
- extended\_master\_secret
- application\_layer\_protocol\_negotiation
- supported\_versions (TLS 1.3, TLS 1.2)
- signature\_algorithms
- Reserved (GREASE)

```
Session ID: 907c64265e76d0c8e1e2d120f66d4b5a7035e27cd1898202078b1873d9cd763
Cipher Suites Length: 32
> Cipher Suites (16 suites)
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 1608
> Extension: Reserved (GREASE) (len=0)
> Extension: key_share (len=1263) X25519MLKEM768, x25519
> Extension: renegotiation_info (len=1)
> Extension: encrypted_client_hello (len=186)
> Extension: compress_certificate (len=3)
> Extension: server_name (len=17) name=www.iana.org
> Extension: status_request (len=5)
> Extension: supported_groups (len=12)
> Extension: ec_point_formats (len=2)
> Extension: Unknown type 17613 (len=5)
> Extension: session_ticket (len=0)
> Extension: psk_key_exchange_modes (len=2)
> Extension: signed_certificate_timestamp (len=0)
> Extension: extended_master_secret (len=0)
> Extension: application_layer_protocol_negotiation (len=14)
> Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
> Extension: signature_algorithms (len=18)
> Extension: Reserved (GREASE) (len=1)
[JA4: t13d1516h2_8daaf6152771_d8a2da3f94cd]
[JA4_r: t13d1516h2_002f,0035,009c,009d,1301,1302,1303,c013,c014,c02b,c02c,c02f,c030,cca8,cca9,0005,000a,000b,000c,000d,000e,000f,0010,0011,0012,0013,0014,0015,0016,0017,0018,0019,001a,001b,001c,001d,001e,001f,0020,0021,0022,0023,0024,0025,0026,0027,0028,0029,002a,002b,002c,002d,002e,002f,0030,0031,0032,0033,0034,0035,0036,0037,0038,0039,003a,003b,003c,003d,003e,003f,0040,0041,0042,0043,0044,0045,0046,0047,0048,0049,004a,004b,004c,004d,004e,004f,0050,0051,0052,0053,0054,0055,0056,0057,0058,0059,005a,005b,005c,005d,005e,005f,0060,0061,0062,0063,0064,0065,0066,0067,0068,0069,006a,006b,006c,006d,006e,006f,0070,0071,0072,0073,0074,0075,0076,0077,0078,0079,007a,007b,007c,007d,007e,007f,0080,0081,0082,0083,0084,0085,0086,0087,0088,0089,008a,008b,008c,008d,008e,008f,0090,0091,0092,0093,0094,0095,0096,0097,0098,0099,009a,009b,009c,009d,009e,009f,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,082b,082c,082d,082e,082f,0830,0831,0832,0833,0834,0835,0836,0837,0838,0839,083a,083b,083c,083d,083e,083f,0840,0841,0842,0843,0844,0845,0846,0847,0848,0849,084a,084b,084c,084d,084e,084f,0850,0851,0852,0853,0854,0855,0856,0857,0858,0859,085a,085b,085c,085d,085e,085f,0860,0861,0862,0863,0864,0865,0866,0867,0868,0869,086a,086b,086c,086d,086e,086f,0870,0871,0872,0873,0874,0875,0876,0877,0878,0879,087a,087b,087c,087d,087e,087f,0880,0881,0882,0883,0884,0885,0886,0887,0888,0889,088a,088b,088c,088d,088e,088f,0890,0891,0892,0893,0894,0895,0896,0897,0898,0899,089a,089b,089c,089d,089e,089f,08a0,08a1,08a2,08a3,08a4,08a5,08a6,08a7,08a8,08a9,08aa,08ab,08ac,08ad,08ae,08af,08b0,08b1,08b2,08b3,08b4,08b5,08b6,08b7,08b8,08b9,08ba,08bb,08bc,08bd,08be,08bf,08c0,08c1,08c2,08c3,08c4,08c5,08c6,08c7,08c8,08c9,08ca,08cb,08cc,08cd,08ce,08cf,08d0,08d1,08d2,08d3,08d4,08d5,08d6,08d7,08d8,08d9,08da,08db,08dc,08dd,08de,08df,08e0,08e1,08e2,08e3,08e4,08e5,08e6,08e7,08e8,08e9,08ea,08eb,08ec,08ed,08ee,08ef,08f0,08f1,08f2,08f3,08f4,08f5,08f6,08f7,08f8,08f9,08fa,08fb,08fc,08fd,08fe,08ff,0900,0901,0902,0903,0904,0905,0906,0907,0908,0909,090a,090b,090c,090d,090e,090f,0910,0911,0912,0913,0914,0915,0916,0917,0918,0919,091a,091b,091c,091d,091e,091f,0920,0921,0922,0923,0924,0925,0926,0927,0928,0929,092a,092b,092c,092d,092e,092f,0930,0931,0932,0933,0934,0935,0936,0937,0938,0939,093a,093b,093c,093d,093e,093f,0940,0941,0942,0943,0944,0945,0946,0947,0948,0949,094a,
```

#### Q4. Find the Server Hello message in the capture. Which frame contains it, and which cipher suite is selected?

The Server Hello message is found in Frame 49.

The selected cipher suite is: TLS\_AES\_256\_GCM\_SHA384.



#### Q5. Examine the Certificate message. Provide details of the certificate.

In TLS 1.3, the Certificate message is encrypted after the ServerHello, so Wireshark does not display it in the capture.

Therefore, we retrieved the certificate directly from the server using OpenSSL.

Details of the certificate for [www.iana.org](http://www.iana.org):

- Subject: C = US, ST = California, O = Internet Corporation For Assigned Names and Numbers, CN = \*.iana.org
- Issuer: C = GB, ST = Greater Manchester, L = Salford, O = Sectigo Limited, CN = Sectigo RSA Organization Validation Secure Server CA
- Validity:
  - Not Before: Dec 6, 2024
  - Not After: Jan 5, 2026
- Public Key Algorithm: RSA 4096-bit
- Signature Algorithm: RSA-SHA256

#### Q6. Find the first packet containing encrypted application data. Which frame is it, and why can't you see the HTTP headers?

The first encrypted Application Data is found in Frame 49.

The HTTP headers are not visible because in HTTPS, all HTTP payloads are encrypted inside TLS Application Data records. Without the decryption keys, Wireshark cannot reveal the actual HTTP headers.