

1-> CLIENT HELLO

1. Select filter box and filter results for “ssl contains amazon”.
2. Select the packet for “client hello”.
3. Expand “transport layer security”.
4. Expand “TLSv1.2 Record Layer: handshake protocol: Client Hello”.
5. Expand “Handshake Protocol: Client Hello”.
6. Take Screenshot

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane at the top shows a filter 'ssl contains amazon' and a list of captured packets. Packet 651 is selected, showing a TLSv1.2 Client Hello from 192.168.219.175 to 104.89.112.89. The packet details pane on the right shows the expanded structure of the selected packet, including the TLSv1.2 Record Layer, Handshake Protocol, and Client Hello. The Client Hello details include the TLS version (1.0), session ID, cipher suites, compression methods, and various extensions. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Activities Wireshark Dec 6 10:25

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl contains amazon

No.	Time	Source	Destination	Protocol	Length	Info
651	5.994897050	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
652	5.995512901	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
665	6.135273189	104.89.112.89	192.168.219.175	TLSv1.2	1516	Server Hello
668	6.135304493	104.89.112.89	192.168.219.175	TLSv1.2	2964	Server Hello
675	6.153829421	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
676	6.153831331	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
855	7.396336615	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
856	7.396927221	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
862	7.420096780	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1019	8.321052703	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1020	8.321336146	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1035	8.372842681	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1036	8.372950763	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1122	8.659162238	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1787	12.576093166	34.196.41.213	192.168.219.175	TLSv1.2	1516	Server Hello
1788	12.580637083	34.202.141.223	192.168.219.175	TLSv1.2	1516	Server Hello

Frame 651: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.219.175, Dst: 104.89.112.89

Transmission Control Protocol, Src Port: 48746, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Transport Layer Security

- TLv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: 58285408f5d4442a3f2ad133f8b535954fff97279f21c8...
 - Session ID Length: 32
 - Session ID: 9e265b139a9e6aba0f06023ba6911845b8694ec3bf8c1831...
 - Cipher Suites Length: 32
 - Cipher Suites (16 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 403
 - Extension: Reserved (GREASE) (len=0)
 - Extension: server_name (len=18)
 - Extension: extended_master_secret (len=0)
 - Extension: renegotiation_info (len=1)
 - Extension: supported_groups (len=10)
 - Extension: ec_point_formats (len=2)
 - Extension: session_ticket (len=0)
 - Extension: application_layer_protocol_negotiation (len=14)
 - Extension: status_request (len=5)
 - Extension: signature_algorithms (len=18)
 - Extension: signed_certificate_timestamp (len=0)
 - Extension: key_share (len=43)
 - Extension: psk_key_exchange_modes (len=2)
 - Extension: supported_versions (len=11)
 - Extension: compress_certificate (len=3)
 - Extension: Unknown type 17513 (len=5)
 - Extension: Reserved (GREASE) (len=1)
 - Extension: padding (len=198)

0020 68 59 70 59 be 6a 01 bb 37 f7 61 6a cd 8b 3f 0d htpv 1... 7.....?

0030 90 18 01 76 77 36 09 09 01 01 08 0a 7b 41 cc 09 w6...[A..

0040 00 37 08 81 16 03 01 02 00 01 00 01 7c 03 03 58 7c... ..X

Transmission Control Protocol (tcp), 32 bytes

Packets: 13940 · Displayed: 89 (0.6%) · Dropped: 0 (0.0%)

SERVER HELLO

1. Select filter box and filter results for “ssl contains amazon”.
2. Select the packet for “Server hello.”
3. Expand “transport layer security”.
4. Expand “TLSv1.2 Record Layer: handshake protocol: Server Hello”.
5. Expand “Handshake Protocol: Server Hello”.
6. Take Screenshot

The image shows a Wireshark network traffic capture. The top bar indicates the date and time as Dec 6 10:26. The filter bar at the top shows the filter "ssl contains amazon". The packet list on the left shows a list of captured packets, with packet 665 selected. The packet details pane on the right shows the structure of the selected packet, which is a TLSv1.2 Record Layer: handshake protocol: Server Hello. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
651	5.994897050	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
652	5.995512901	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
665	6.15578189	104.89.112.89	192.168.219.175	TLSv1.2	1516	Server Hello
668	6.155304403	104.89.112.89	192.168.219.175	TLSv1.2	2064	Server Hello
675	6.153029421	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
676	6.153031331	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
855	7.396336615	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
856	7.396927221	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
862	7.420906780	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1019	8.321052703	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1020	8.321336146	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1035	8.372842681	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1036	8.372950763	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1122	8.659162238	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1787	12.576093166	34.196.41.213	192.168.219.175	TLSv1.2	1516	Server Hello
1788	12.580637083	34.202.141.223	192.168.219.175	TLSv1.2	1516	Server Hello

Frame 665: 1516 bytes on wire (12128 bits), 1516 bytes captured (12128 bits) on interface any, id 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 104.89.112.89, Dst: 192.168.219.175
- Transmission Control Protocol, Src Port: 443, Dst Port: 48746, Seq: 1, Ack: 518, Len: 1448
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 78
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 74
 - Version: TLS 1.2 (0x0303)
 - Random: 405d6fc8a6d3a492beaea479a7e17b074632ccf6b6e648c9...
 - Session ID Length: 0
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Compression Method: null (0)
 - Extensions Length: 34
 - Extension: renegotiation_info (len=1)
 - Extension: server_name (len=0)
 - Extension: ec_point_formats (len=4)
 - Extension: session_ticket (len=0)
 - Extension: status_request (len=0)
 - Extension: application_layer_protocol_negotiation (len=5)

SSL CERTIFICATE

1. Select filter box and filter results for “ssl contains amazon”.
2. Select the packet for “Certificate Status, Server key exchange”.
3. Expand “transport layer security”.
4. Expand “TLSv1.2 Record Layer: handshake protocol: Certificate”.
5. Expand “Handshake Protocol: Certificate”.
6. Take Screenshot.

Activities Wireshark Dec 6 10:26 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl contains amazon

No.	Time	Source	Destination	Protocol	Length	Info
651	5.994897850	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
652	5.995512901	192.168.219.175	104.89.112.89	TLSv1.2	585	Client Hello
665	6.135273189	104.89.112.89	192.168.219.175	TLSv1.2	1516	Server Hello
668	6.135304403	104.89.112.89	192.168.219.175	TLSv1.2	2964	Server Hello
675	6.153029421	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
676	6.153031331	104.89.112.89	192.168.219.175	TLSv1.2	2339	Certificate, Certificate Status, Server Key Exchange, Server ...
855	7.336336615	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
856	7.396927221	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
862	7.420096780	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1019	8.321052703	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1020	8.321336146	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1035	8.372842601	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1039	8.372950783	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1122	8.659162238	192.168.219.175	199.232.253.16	TLSv1.3	585	Client Hello
1787	12.576093166	34.196.41.213	192.168.219.175	TLSv1.2	1516	Server Hello
1789	12.580637083	34.202.141.223	192.168.219.175	TLSv1.2	1516	Server Hello

Frame 676: 2339 bytes on wire (18712 bits), 2339 bytes captured (18712 bits) on interface any, id 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 104.89.112.89, Dst: 192.168.219.175
- Transmission Control Protocol, Src Port: 443, Dst Port: 48748, Seq: 2897, Ack: 518, Len: 2271
- [2 Reassembled TCP Segments (4253 bytes): #668(2813), #676(1440)]
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 4248
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 4244
 - Certificates Length: 4241
 - Certificates (4241 bytes)
 - Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate Status
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 479
 - Handshake Protocol: Certificate Status
 - Handshake Type: Certificate Status (22)
 - Length: 475
 - Certificate Status Type: OCSP (1)
 - OCSP Response Length: 471
 - OCSP Response
 - TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 333
 - Handshake Protocol: Server Key Exchange
 - Handshake Type: Server Key Exchange (12)
 - Length: 329
 - EC Diffie-Hellman Server Params
 - TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 4
 - Handshake Protocol: Server Hello Done
 - Handshake Type: Server Hello Done (14)
 - Length: 0

0020 c0 a8 db af 01 bb be 6c 94 85 d9 dd e8 cd b9 46 ... 01

Frame (2339 bytes) Reassembled TCP (4253 bytes)

Transmission Control Protocol (tcp), 32 bytes

Packets: 13940 · Displayed: 89 (0.6%) · Dropped: 0 (0.0%)