

1. What are the cipher suites advertised by client hello record? How do you identify the client hello record?

The image shows a Wireshark capture of a TLS Client Hello record. The packet list at the top shows three packets: a TLSv1.2 Application Data packet (No. 58), a TLSv1.2 Client Hello packet (No. 93), and another TLSv1.2 Client Hello packet (No. 94). The packet details pane for packet 93 is expanded, showing the 'Handshake Protocol: Client Hello' section. A red box highlights 'Handshake Type: Client Hello (1)' with a red arrow pointing to a red box labeled 'Used to identify client hello'. Another red box highlights the 'Cipher Suites (16 suites)' section, with a red arrow pointing to a red box labeled 'Cipher suites advertised by Client Hello'. The list of cipher suites includes: Reserved (GREASE), TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_CBC_SHA, and TLS_RSA_WITH_AES_256_CBC_SHA.

2. What cipher suite is picked by the server hello? How do you identify the server Hello record?

The image shows a Wireshark capture of a TLS Server Hello record. The packet list at the top shows three packets: a TLSv1.2 Client Hello packet (No. 100), a TLSv1.2 Server Hello packet (No. 103), and a TLSv1.2 Application Data packet (No. 107). The packet details pane for packet 103 is expanded, showing the 'Transport Layer Security' section. A red box highlights 'TLSv1.3 Record Layer: Handshake Protocol: Server Hello' with a red arrow pointing to a red box labeled 'Server Hello Identified'. Another red box highlights the 'Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)' with a red arrow pointing to a red box labeled 'Cipher suite picked by Server Hello'. The list of extensions includes 'supported_versions (len=2)' and 'key_share (len=36)'. The packet details pane also shows the 'Change Cipher Spec Protocol: Change Cipher Spec' and 'Application Data Protocol: http-over-tls' sections.

3. Does the server hello contain a nonce? What is its value? Does it have a certificate? How many bytes long?

The image shows a Wireshark capture of a TLS handshake. The packet list shows three packets: 100 (Client Hello), 103 (Server Hello), and 107 (Application Data). The packet details for packet 103 are expanded, showing the TLSv1.3 Record Layer: Handshake Protocol: Server Hello. The content type is Handshake (22), version is TLS 1.2 (0x0303), and length is 122. The handshake protocol details show the server hello message with a random value of 72ae8f0530555b47c8a7bf464525542d8b1a21de7b03f8e60802e778eb630ba9 and a session ID length of 32. The random value is highlighted with a red box and labeled "Server Hello's nonce of 32 bytes". A red box also highlights the "Server Hello" label in the packet details. A red box on the right contains the text "In this case nonce does not have a certificate". The packet bytes are shown at the bottom, with the random value highlighted in blue.

Wireshark capture showing the Server Hello message (Frame 103). The message contains a random value (nonce) of 32 bytes, highlighted in blue. The nonce is: 72ae8f0530555b47c8a7bf464525542d8b1a21de7b03f8e60802e778eb630ba9. The message also includes the Session ID Length (32) and the Session ID (812fc024b1ba4bd964c556f373c73e65debeec69249f80eaf0cc777de93e8c82).

Random values used for deriving keys (tls.handshake.random), 32 bytes

4. Observe what is done by the change cipher spec and authentication algorithms. Is it possible to capture the application data? Why?

The image shows a Wireshark capture of a TLS handshake. The packet list shows several packets, including 23 (Change Cipher Spec) and 25 (Encrypted Handshake Message). The packet details for packet 23 are expanded, showing the TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec. The content type is Change Cipher Spec (20), version is TLS 1.2 (0x0303), and length is 1. The packet details for packet 25 are also expanded, showing the TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message. The content type is Handshake (22), version is TLS 1.2 (0x0303), and length is 40. The handshake protocol details show the encrypted handshake message. The packet bytes are shown at the bottom, with the change cipher spec and encrypted handshake message highlighted in blue.

Wireshark capture showing the Change Cipher Spec message (Frame 23) and the Encrypted Handshake Message (Frame 25). The Change Cipher Spec message is highlighted in red. The Encrypted Handshake Message is highlighted in blue. The message contains the encrypted handshake data.

Record Layer (tls.record), 6 bytes

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: tls

Time	Source	Destination	Protocol	Length	Info
8 0.144748	192.168.0.105	52.163.89.138	TLSv...	250	Client Hello
13 0.199318	52.163.89.138	192.168.0.105	TLSv...	1293	Server Hello, Certificate, Certificate Status, Server Key Exchange, Ser...
15 0.201277	192.168.0.105	52.163.89.138	TLSv...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23 0.250414	52.163.89.138	192.168.0.105	TLSv...	105	Change Cipher Spec, Encrypted Handshake Message
25 0.271698	192.168.0.105	52.163.89.138	TLSv...	455	Application Data
26 0.271898	192.168.0.105	52.163.89.138	TLSv...	1389	Application Data
28 0.329508	52.163.89.138	192.168.0.105	TLSv...	653	Application Data
30 0.329655	192.168.0.105	52.163.89.138	TLSv...	85	Encrypted Alert
33 0.382441	192.168.0.105	40.126.17.129	TLSv...	504	Application Data
38 0.382533	192.168.0.105	40.126.17.129	TLSv...	1223	Application Data
57 0.640720	40.126.17.129	192.168.0.105	TLSv...	1494	Application Data [TCP segment of a reassembled PDU]

> Frame 28: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device\NPF_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0

> Ethernet II, Src: Tp-LinkT_64:16:70 (98:da:c4:64:16:70), Dst: IntelCor_06:0b:53 (5c:87:9c:06:0b:53)

> Internet Protocol Version 4, Src: 52.163.89.138, Dst: 192.168.0.105

> Transmission Control Protocol, Src Port: 443, Dst Port: 1032, Seq: 7051, Ack: 2026, Len: 599

> Transport Layer Security

- > TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 594
 - Encrypted Application Data: 00000000000000001411ea8c004ed2bb3dcc17e32d5f8baef7b58a256150a46bb02eff2ce...
 - [Application Data Protocol: http-over-tls]

Application Data
can be captured but
it will be in
encrypted format.

Record Layer (tls.record), 599 bytes

Packets: 2302 · Displayed: 523 (22.7%) · Dropped: 0 (0.0%)

Profile: Default

22:15
08-12-2020