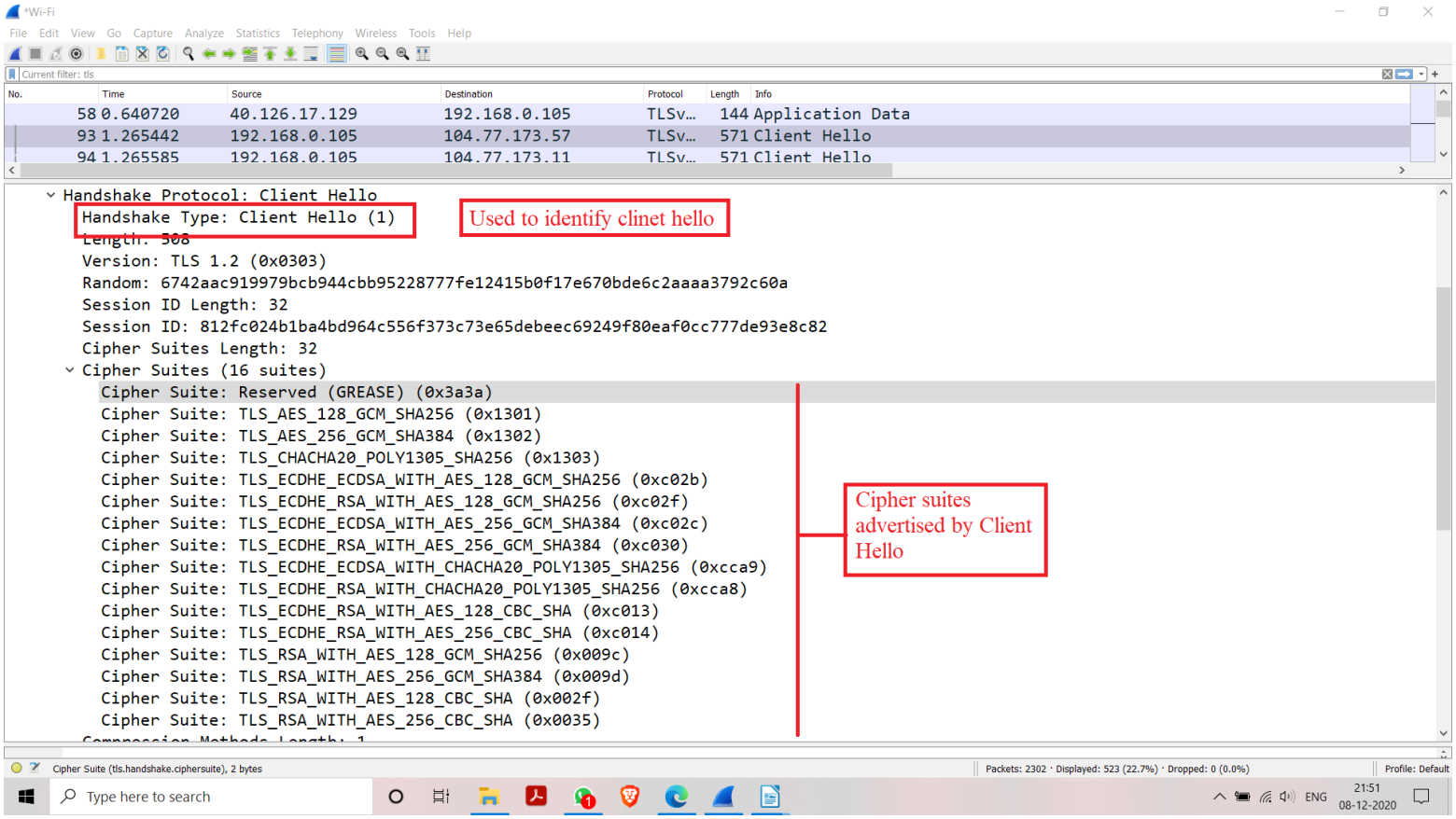
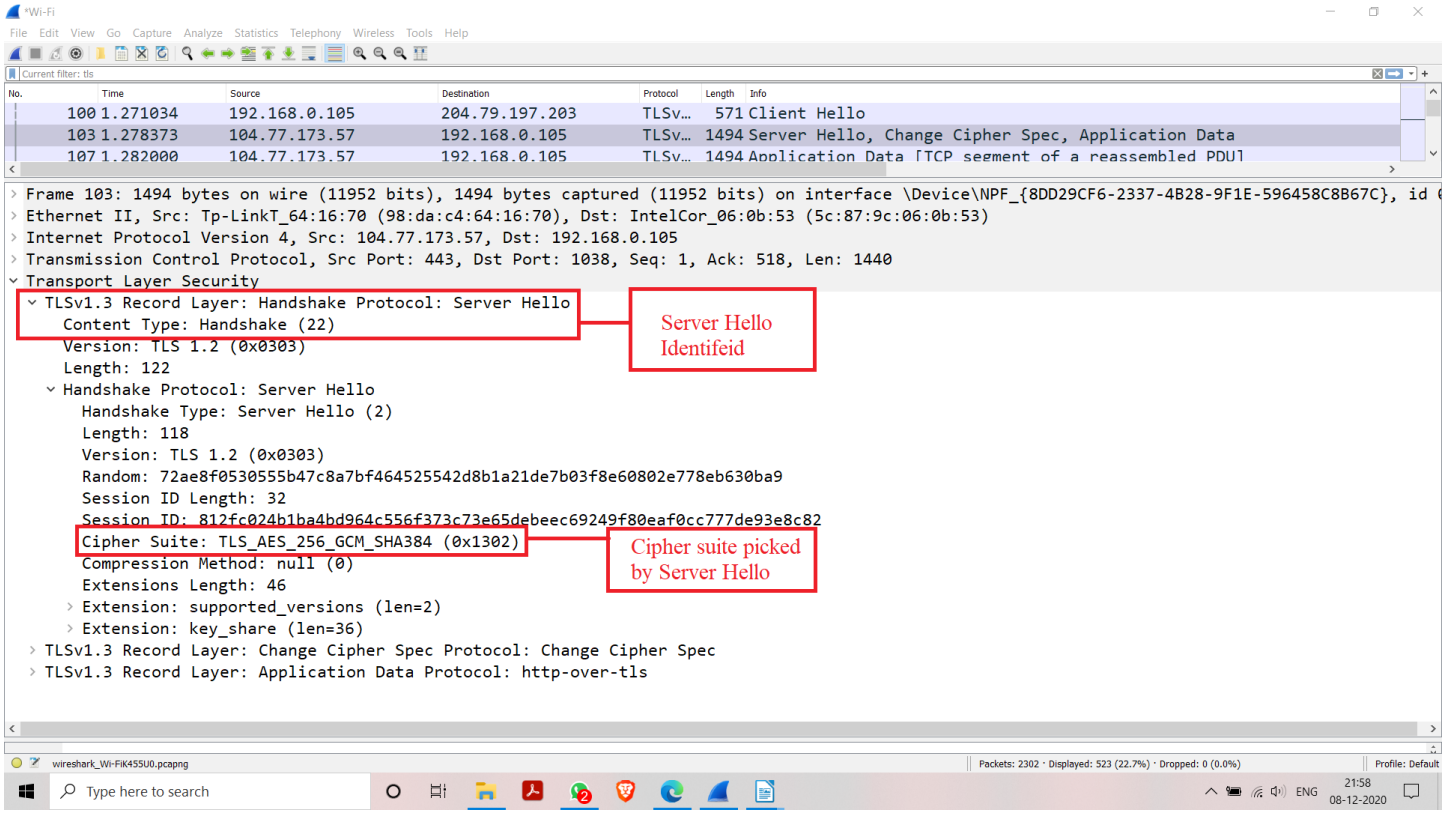
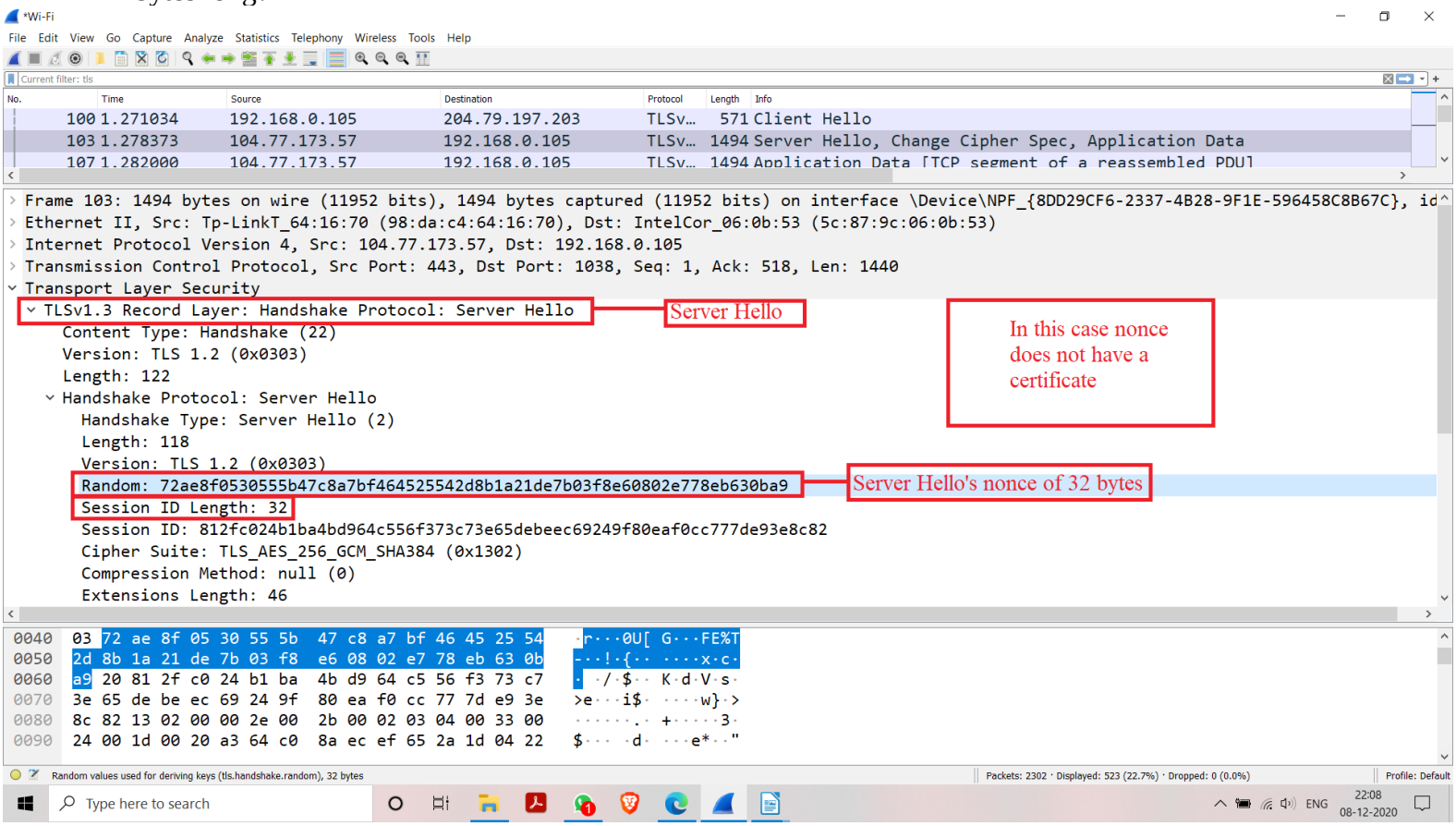
1. What are the cipher suites advertised by client hello record? How do you identify the client hello record?



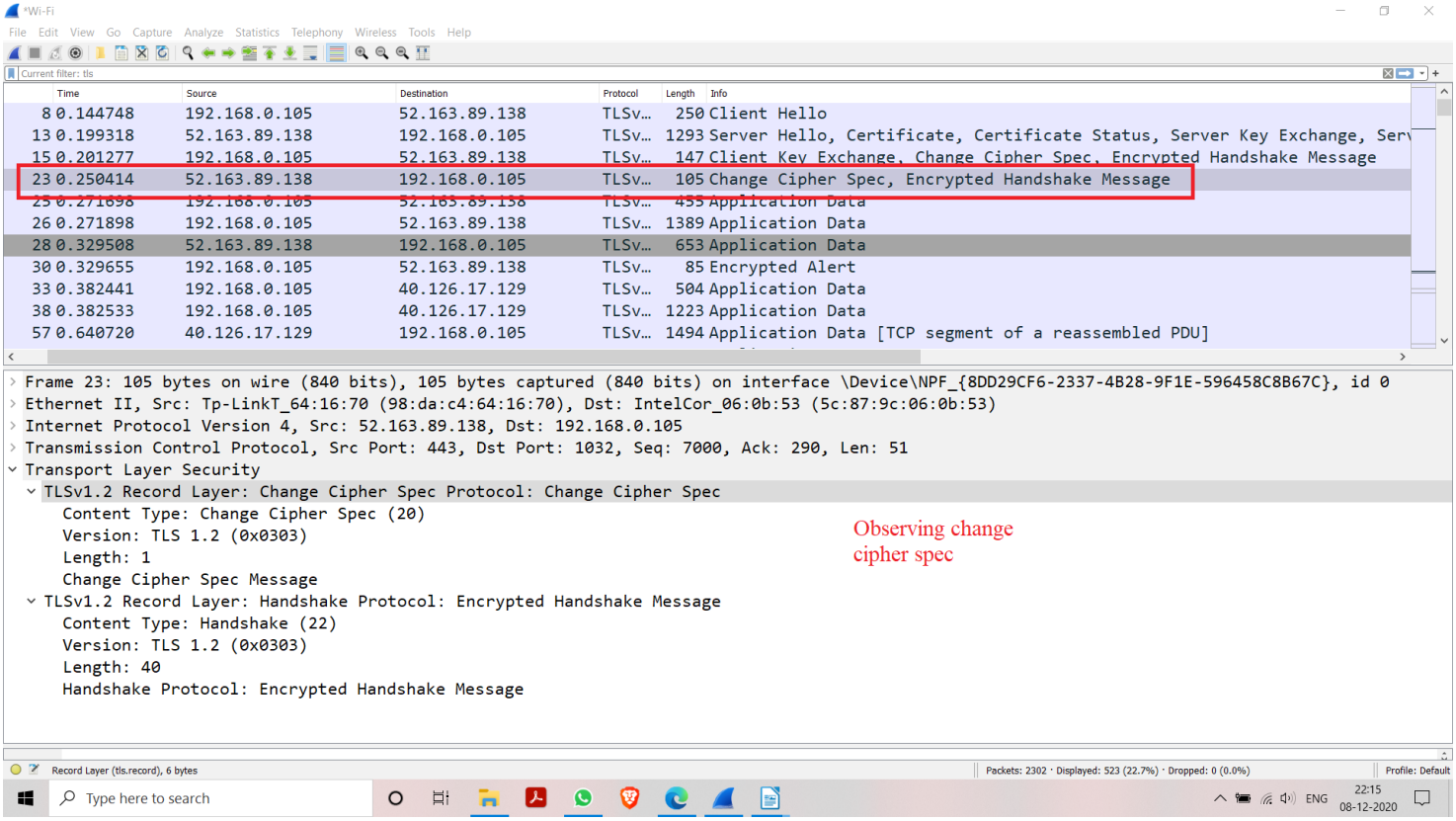
2. What cipher suite is picked by the server hello? How do you identify the server Hello record?

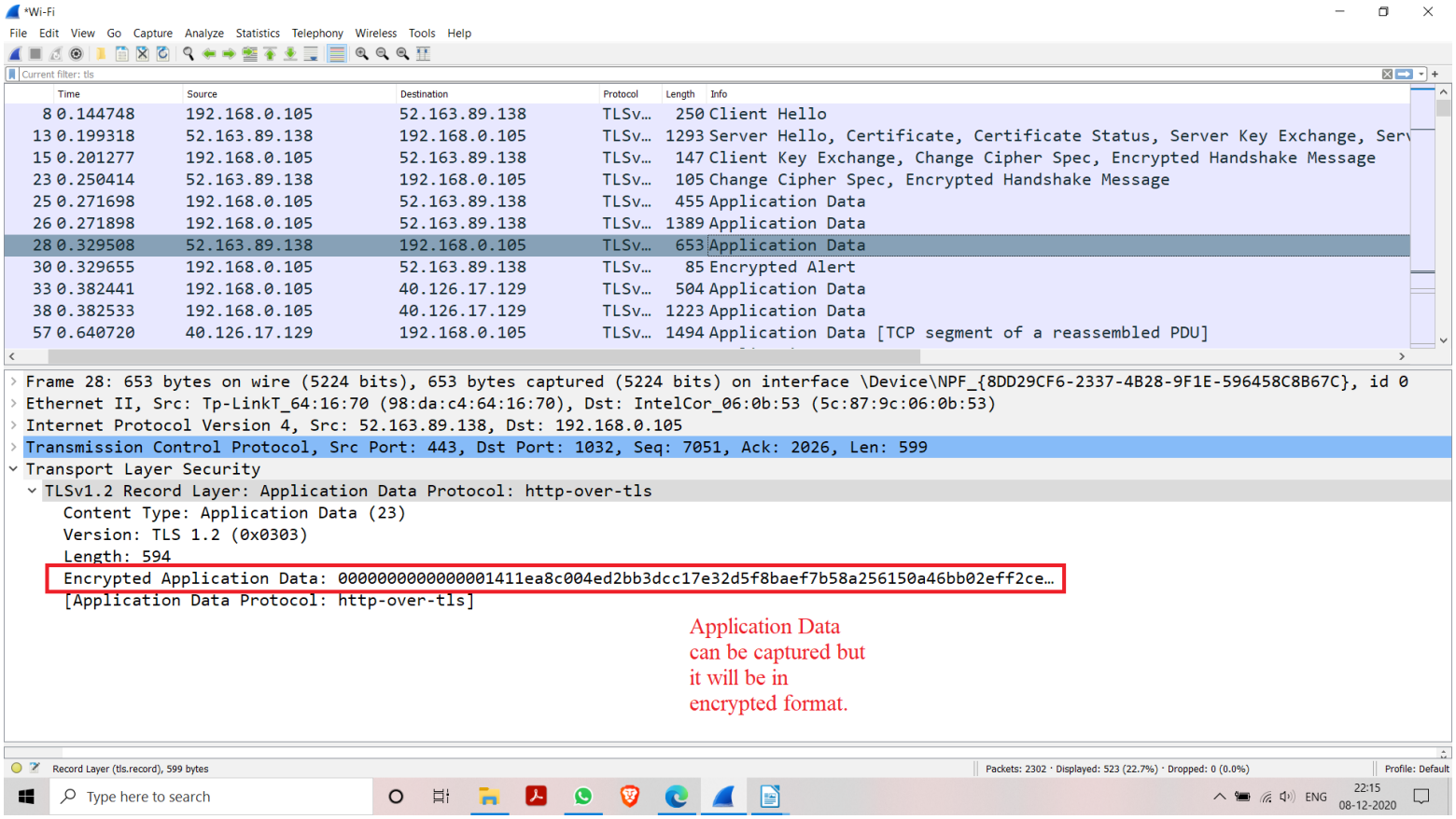


3. Does the server hello contain a nonce? What is its value? Does it have a certificate? How many bytes long?



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




*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, Serv
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
Type here to search
ENG
22:15
08-12-2020