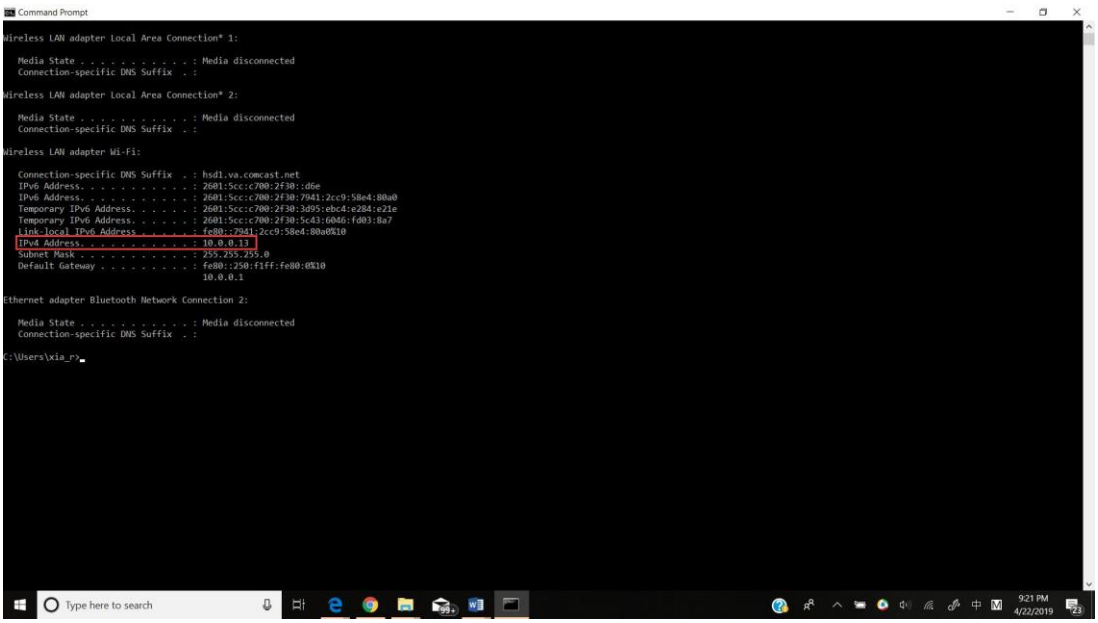
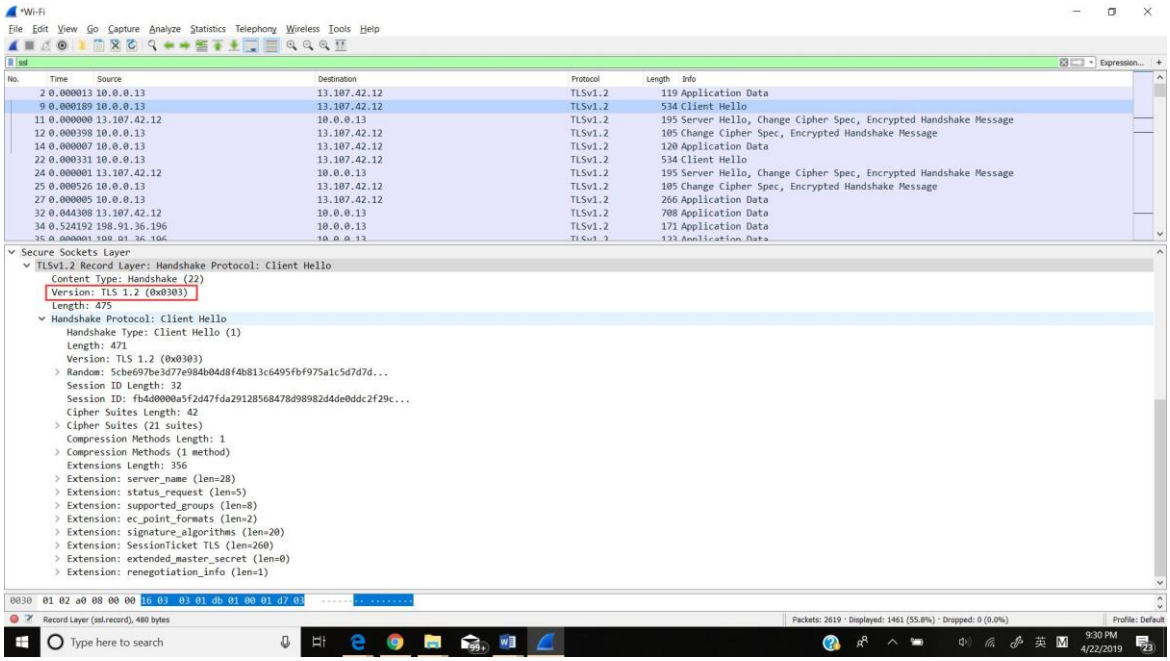


My IP is 10. 0. 0. 13

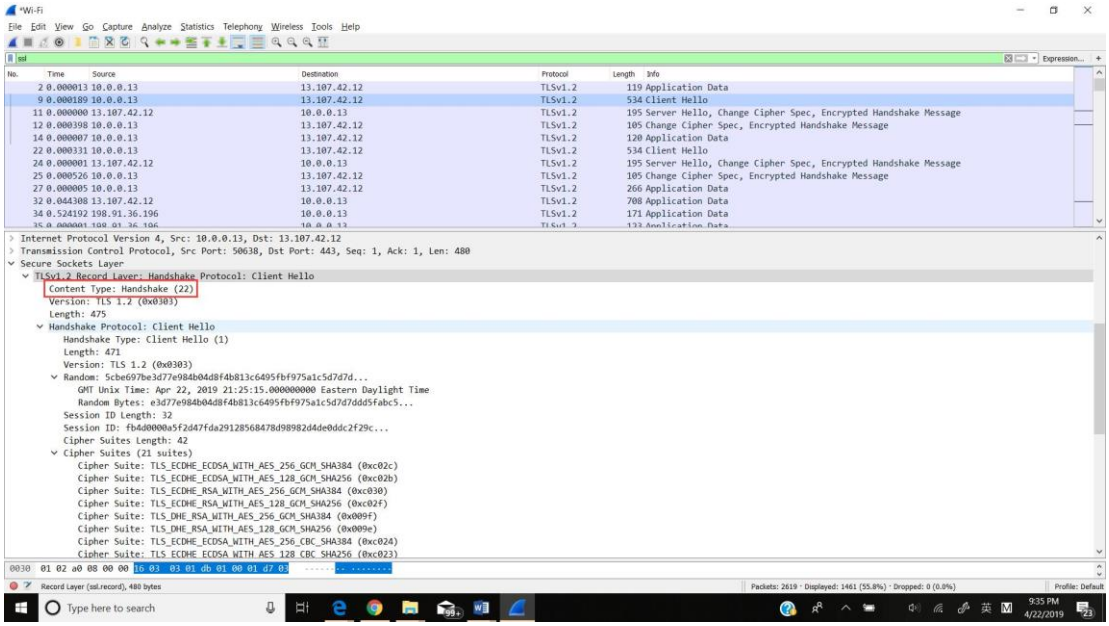
Client Hello Record:

1. What is the SSL/TLS version of the of the Client Hello frame?



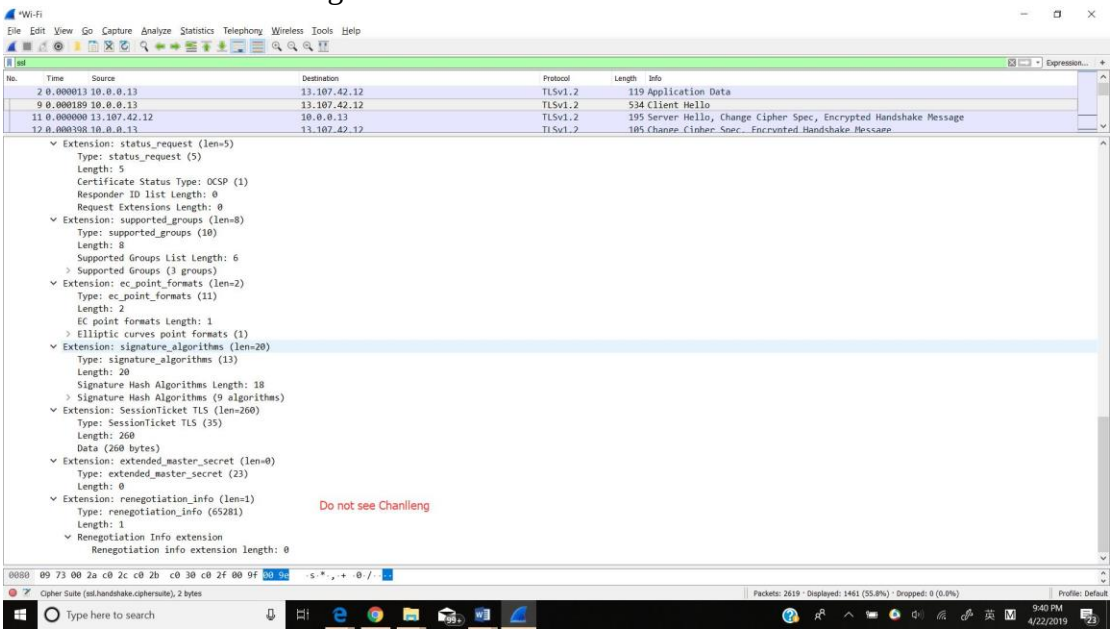
Version: TLS 1.2

2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?



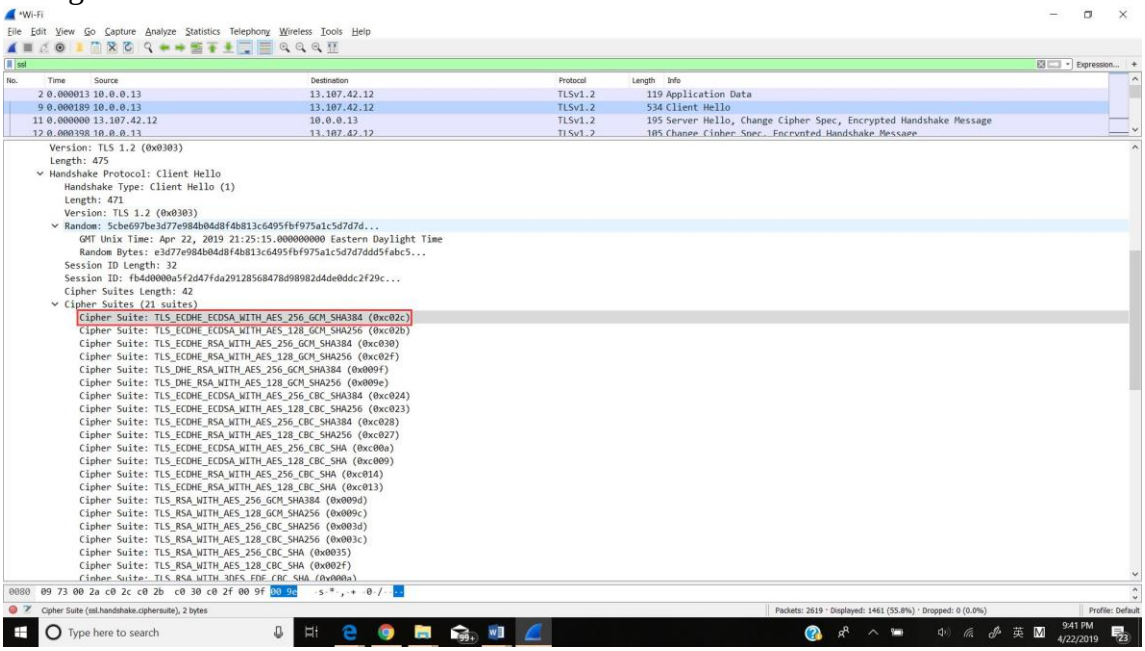
Content Type: 22

3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?



No Challenge found.

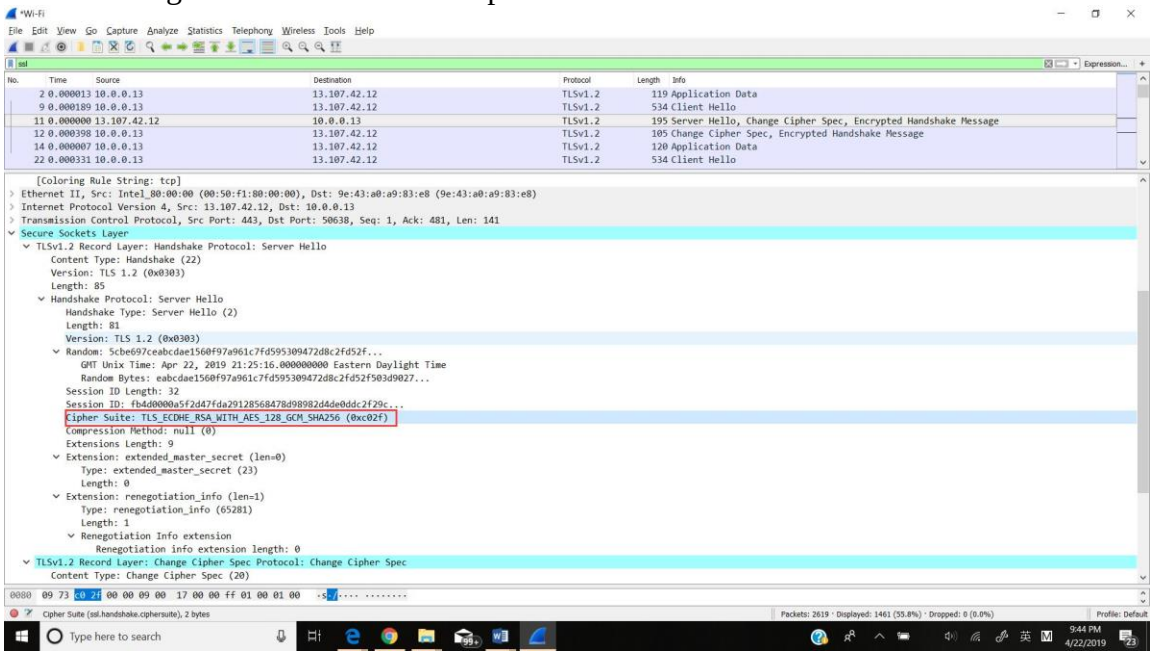
4. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?



Public-key algorithm: ECDHE (Elliptic-Curve Diffe-Hellman) and ECHSA (Elliptic Curve Digital Signature Algorithm)
Symmetric-key algorithm: AES-256 and GCM (Galois/ Counter Mode)
Hash algorithm: SHA-384 (Secure Hash Algorithm 384)

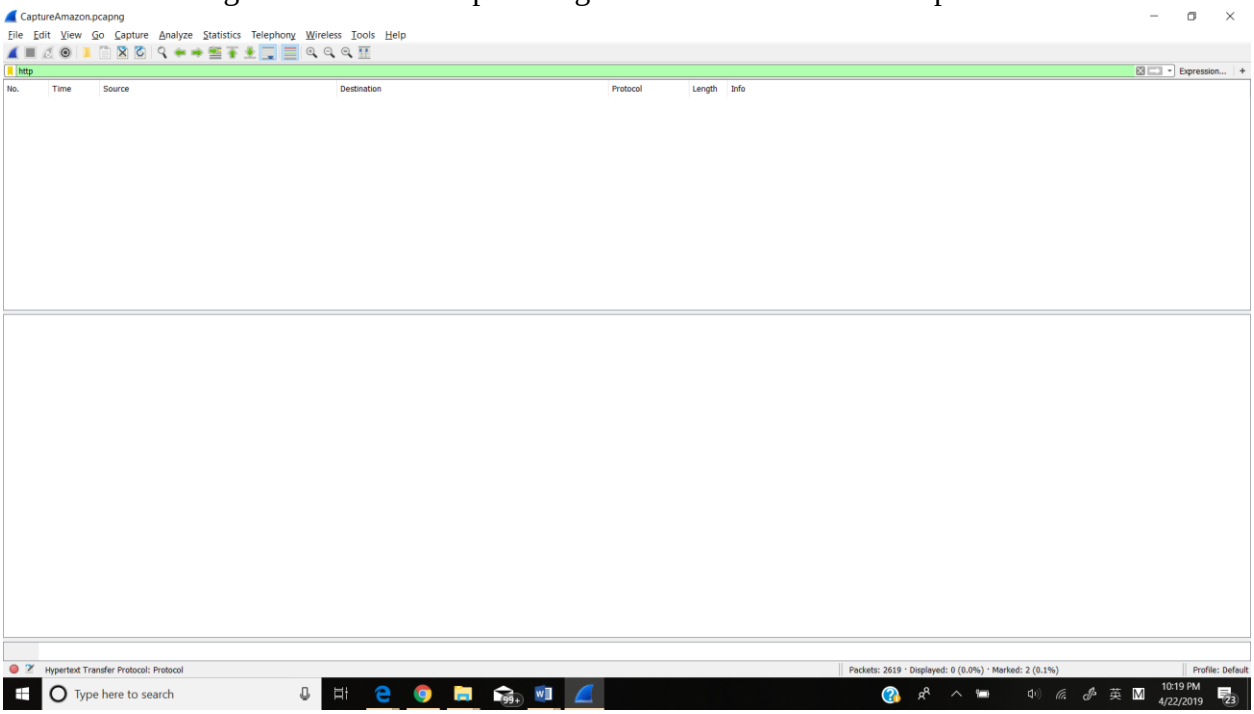
Server Hello Record:

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?



Public-key algorithm: ECDHE-RSA
Symmetric-key algorithm: AES-128 and GCM (Galois/ Counter Mode)
Hash algorithm: SHA-256 (Secure Hash Algorithm 256)

HTTP OK message: Can not find http message in Wireshark from this lap:



So I attached full print of SSL client hello and server hello records in the following pages.

```
No.     Time           Source                Destination           Protocol Length Info
      9 0.000189       10.0.0.13             13.107.42.12          TLSv1.2  534    Client Hello
Frame 9: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0
    Interface id: 0 (\Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374})
        Interface name: \Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374}
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 22, 2019 21:25:15.997461000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1555982715.997461000 seconds
    [Time delta from previous captured frame: 0.000189000 seconds]
    [Time delta from previous displayed frame: 0.072079000 seconds]
    [Time since reference or first frame: 0.072092000 seconds]
    Frame Number: 9
    Frame Length: 534 bytes (4272 bits)
    Capture Length: 534 bytes (4272 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8), Dst: Intel_80:00:00 (00:50:f1:80:00:00)
    Destination: Intel_80:00:00 (00:50:f1:80:00:00)
        Address: Intel_80:00:00 (00:50:f1:80:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        Address: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.13, Dst: 13.107.42.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 520
    Identification: 0x294e (10574)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x8e1e [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.13
    Destination: 13.107.42.12
Transmission Control Protocol, Src Port: 50638, Dst Port: 443, Seq: 1, Ack: 1, Len: 480
    Source Port: 50638
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 480]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 481    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····AP···]
    Window size value: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0xa008 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.019559000 seconds]
        [Bytes in flight: 480]
        [Bytes sent since last PSH flag: 480]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.019748000 seconds]
        [Time since previous frame in this TCP stream: 0.000189000 seconds]
    TCP payload (480 bytes)
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
```

```
    Version: TLS 1.2 (0x0303)
    Length: 475
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 471
        Version: TLS 1.2 (0x0303)
        Random: 5cbe697be3d77e984b04d8f4b813c6495fbf975a1c5d7d7d...
            GMT Unix Time: Apr 22, 2019 21:25:15.000000000 Eastern Daylight Time
            Random Bytes: e3d77e984b04d8f4b813c6495fbf975a1c5d7d7ddd5fabc5...
        Session ID Length: 32
        Session ID: fb4d0000a5f2d47fda29128568478d98982d4de0ddc2f29c...
        Cipher Suites Length: 42
        Cipher Suites (21 suites)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
            Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
            Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
            Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
            Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
            Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
            Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
            Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
            Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
            Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
        Compression Methods Length: 1
        Compression Methods (1 method)
            Compression Method: null (0)
        Extensions Length: 356
        Extension: server_name (len=28)
            Type: server_name (0)
            Length: 28
            Server Name Indication extension
                Server Name list length: 26
                Server Name Type: host_name (0)
                Server Name length: 23
                Server Name: sn3301.storage.live.com
        Extension: status_request (len=5)
            Type: status_request (5)
            Length: 5
            Certificate Status Type: OCSP (1)
            Responder ID list Length: 0
            Request Extensions Length: 0
        Extension: supported_groups (len=8)
            Type: supported_groups (10)
            Length: 8
            Supported Groups List Length: 6
            Supported Groups (3 groups)
                Supported Group: x25519 (0x001d)
                Supported Group: secp256r1 (0x0017)
                Supported Group: secp384r1 (0x0018)
        Extension: ec_point_formats (len=2)
            Type: ec_point_formats (11)
            Length: 2
            EC point formats Length: 1
            Elliptic curves point formats (1)
                EC point format: uncompressed (0)
        Extension: signature_algorithms (len=20)
            Type: signature_algorithms (13)
            Length: 20
            Signature Hash Algorithms Length: 18
            Signature Hash Algorithms (9 algorithms)
                Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
                    Signature Hash Algorithm Hash: SHA256 (4)
                    Signature Hash Algorithm Signature: RSA (1)
                Signature Algorithm: rsa_pkcs1_sha384 (0x0501)
                    Signature Hash Algorithm Hash: SHA384 (5)
                    Signature Hash Algorithm Signature: RSA (1)
                Signature Algorithm: rsa_pkcs1_sha1 (0x0201)
                    Signature Hash Algorithm Hash: SHA1 (2)
                    Signature Hash Algorithm Signature: RSA (1)
                Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
                    Signature Hash Algorithm Hash: SHA256 (4)
                    Signature Hash Algorithm Signature: ECDSA (3)
                Signature Algorithm: ecdsa_secp384r1_sha384 (0x0503)
                    Signature Hash Algorithm Hash: SHA384 (5)
                    Signature Hash Algorithm Signature: ECDSA (3)
                Signature Algorithm: ecdsa_sha1 (0x0203)
```

```
                Signature Hash Algorithm Hash: SHA1 (2)
                Signature Hash Algorithm Signature: ECDSA (3)
            Signature Algorithm: SHA1 DSA (0x0202)
                Signature Hash Algorithm Hash: SHA1 (2)
                Signature Hash Algorithm Signature: DSA (2)
            Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
                Signature Hash Algorithm Hash: SHA512 (6)
                Signature Hash Algorithm Signature: RSA (1)
            Signature Algorithm: ecdsa_secp521r1_sha512 (0x0603)
                Signature Hash Algorithm Hash: SHA512 (6)
                Signature Hash Algorithm Signature: ECDSA (3)
    Extension: SessionTicket TLS (len=260)
        Type: SessionTicket TLS (35)
        Length: 260
        Data (260 bytes)
    Extension: extended_master_secret (len=0)
        Type: extended_master_secret (23)
        Length: 0
    Extension: renegotiation_info (len=1)
        Type: renegotiation_info (65281)
        Length: 1
        Renegotiation Info extension
            Renegotiation info extension length: 0
```

```
No.     Time           Source                Destination           Protocol Length Info
     11 0.000000       13.107.42.12          10.0.0.13             TLSv1.2  195    Server Hello, Change Cipher Spec, Encrypted Handshake Message
Frame 11: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface 0
    Interface id: 0 (\Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374})
        Interface name: \Device\NPF_{87ECFDF9-CA2E-4423-8880-E5CB87989374}
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 22, 2019 21:25:16.028146000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1555982716.028146000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.030685000 seconds]
    [Time since reference or first frame: 0.102777000 seconds]
    Frame Number: 11
    Frame Length: 195 bytes (1560 bits)
    Capture Length: 195 bytes (1560 bits)
    [Frame is marked: True]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Intel_80:00:00 (00:50:f1:80:00:00), Dst: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
    Destination: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        Address: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Intel_80:00:00 (00:50:f1:80:00:00)
        Address: Intel_80:00:00 (00:50:f1:80:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 13.107.42.12, Dst: 10.0.0.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 181
    Identification: 0x7af8 (31480)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 119
    Protocol: TCP (6)
    Header checksum: 0x46c7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 13.107.42.12
    Destination: 10.0.0.13
Transmission Control Protocol, Src Port: 443, Dst Port: 50638, Seq: 1, Ack: 481, Len: 141
    Source Port: 443
    Destination Port: 50638
    [Stream index: 1]
    [TCP Segment Len: 141]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 142    (relative sequence number)]
    Acknowledgment number: 481    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······AP···]
    Window size value: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0xcb0c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.019559000 seconds]
        [Bytes in flight: 141]
        [Bytes sent since last PSH flag: 141]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.050433000 seconds]
        [Time since previous frame in this TCP stream: 0.000000000 seconds]
    TCP payload (141 bytes)
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
```

```
    Version: TLS 1.2 (0x0303)
    Length: 85
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.2 (0x0303)
        Random: 5cbe697ceabcdae1560f97a961c7fd595309472d8c2fd52f...
            GMT Unix Time: Apr 22, 2019 21:25:16.000000000 Eastern Daylight Time
            Random Bytes: eabcdae1560f97a961c7fd595309472d8c2fd52f503d9027...
        Session ID Length: 32
        Session ID: fb4d0000a5f2d47fda29128568478d98982d4de0ddc2f29c...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 9
        Extension: extended_master_secret (len=0)
            Type: extended_master_secret (23)
            Length: 0
        Extension: renegotiation_info (len=1)
            Type: renegotiation_info (65281)
            Length: 1
            Renegotiation Info extension
                Renegotiation info extension length: 0
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
        [Expert Info (Note/Sequence): This session reuses previously negotiated keys (Session resumption)]
            [This session reuses previously negotiated keys (Session resumption)]
            [Severity level: Note]
            [Group: Sequence]
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```