```
    112 0.022648       128.238.38.162        216.75.194.220        SSLv3    258    Client Key Exchange, Change Cipher Spec, Encrypted
Handshake Message
Frame 112: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 18, 2005 11:11:12.694171000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1121710272.694171000 seconds
    [Time delta from previous captured frame: 0.022648000 seconds]
    [Time delta from previous displayed frame: 0.022648000 seconds]
    [Time since reference or first frame: 21.876168000 seconds]
    Frame Number: 112
    Frame Length: 258 bytes (2064 bits)
    Capture Length: 258 bytes (2064 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssl]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
    Destination: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        Address: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Ibm_10:60:99 (00:09:6b:10:60:99)
        Address: Ibm_10:60:99 (00:09:6b:10:60:99)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.238.38.162, Dst: 216.75.194.220
    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: 244
    Identification: 0x482c (18476)
    Flags: 0x02 (Don't Fragment)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x6f1f [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.238.38.162
    Destination: 216.75.194.220
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 2271, Dst Port: 443, Seq: 79, Ack: 2785, Len: 204
    Source Port: 2271
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 204]
    Sequence number: 79    (relative sequence number)
    [Next sequence number: 283    (relative sequence number)]
    Acknowledgment number: 2785    (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: 64799
    [Calculated window size: 64799]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xc2d9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 111]
        [The RTT to ACK the segment was: 0.022648000 seconds]
        [iRTT: 0.022082000 seconds]
```

```
        [Bytes in flight: 204]
        [Bytes sent since last PSH flag: 204]
    TCP payload (204 bytes)
Secure Sockets Layer
    SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 132
        Handshake Protocol: Client Key Exchange
            Handshake Type: Client Key Exchange (16)
            Length: 128
            RSA Encrypted PreMaster Secret
                Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c...
    SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: SSL 3.0 (0x0300)
        Length: 1
        Change Cipher Spec Message
    SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
        Content Type: Handshake (22)
        Version: SSL 3.0 (0x0300)
        Length: 56
        Handshake Protocol: Encrypted Handshake Message
```