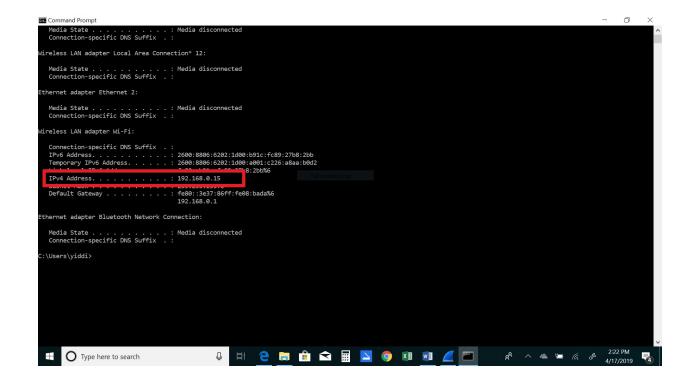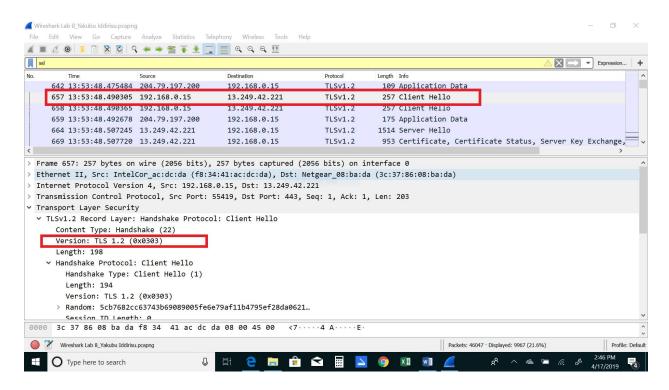# Lab 8 – SSL/TLS

Questions:
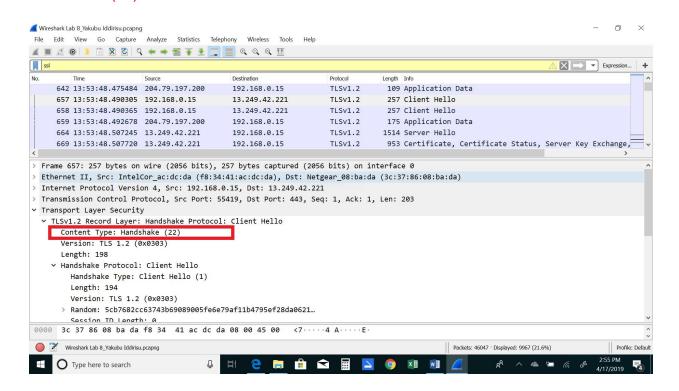Client Hello Record:
1. What is the SSL/TLS version of the of the Client Hello frame?
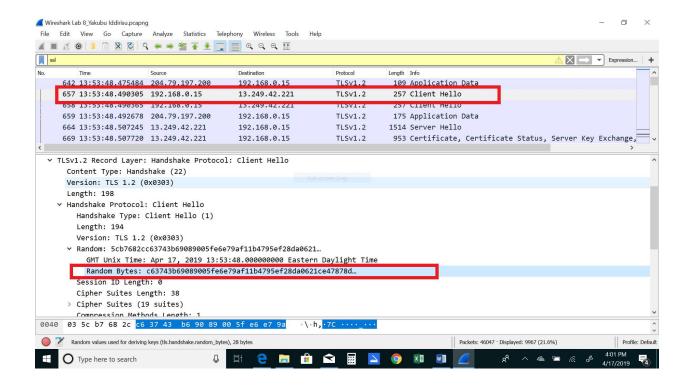   TLS 1.2

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?

Handshake (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?

c63743b69089005fe6e79af11b4795ef28da0621ce47878d…

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?

Yes, it does advertise cyber suites.
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA284 (0xc02c)

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?
YTLS_ECDHE_RSA_WITH_AES_128_GSM_SHA256 (0xc02f)

No.   Time   Source   Destination   Protocol Length Info
      8 13:53:41.961211 2600:8806:6202:1d00:b91c:fc89:27b8:2bb 2607:f8b0:4000:802::2003 HTTP   280   GET /GTSGIAG3.crl HTTP/1.1
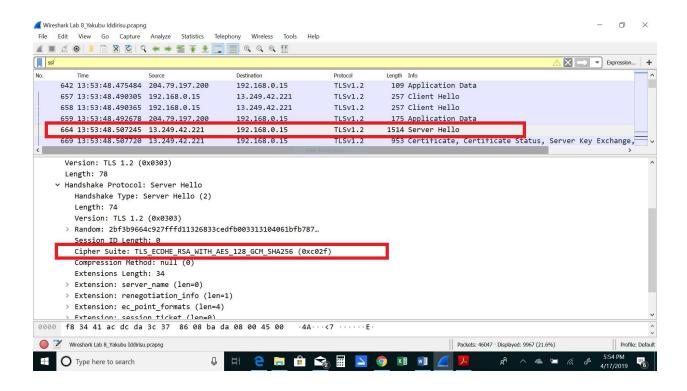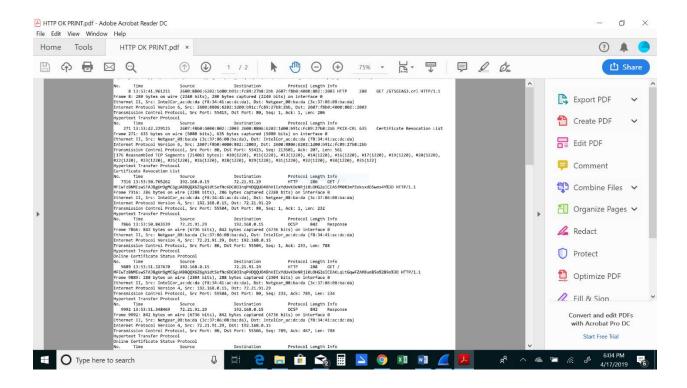Frame 8: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 6, Src: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb, Dst: 2607:f8b0:4000:802::2003
Transmission Control Protocol, Src Port: 55415, Dst Port: 80, Seq: 1, Ack: 1, Len: 206
Hypertext Transfer Protocol
No.   Time   Source   Destination   Protocol Length Info
    271 13:53:42.229125   2607:f8b0:4000:802::2003 2600:8806:6202:1d00:b91c:fc89:27b8:2bb PKIX-CRL 635   Certificate Revocation List
Frame 271: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 6, Src: 2607:f8b0:4000:802::2003, Dst: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb
Transmission Control Protocol, Src Port: 80, Dst Port: 55415, Seq: 213501, Ack: 207, Len: 561
[176 Reassembled TCP Segments (214061 bytes): #10(1220), #11(1220), #13(1220), #14(1220), #16(1220), #17(1220), #19(1220), #20(1220),
#22(1220), #23(1220), #25(1220), #26(1220), #28(1220), #29(1220), #31(1220), #32(1220), #34(1220), #35(122]
Hypertext Transfer Protocol
Certificate Revocation List
No.   Time   Source   Destination   Protocol Length Info
   7316 13:53:50.765262   192.168.0.15   72.21.91.29   HTTP   286   GET /
MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUO48hHIIxYdUvkOeNRji0LOHG2eICEA5fM0R3mPZeksxdD5wos4Y%3D HTTP/1.1
Frame 7316: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 1, Ack: 1, Len: 232
Hypertext Transfer Protocol
No.   Time   Source   Destination   Protocol Length Info
   7866 13:53:50.843539   72.21.91.29   192.168.0.15   OCSP   842   Response
Frame 7866: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 1, Ack: 233, Len: 788
Hypertext Transfer Protocol
Online Certificate Status Protocol
No.   Time   Source   Destination   Protocol Length Info
   9889 13:53:51.327670   192.168.0.15   72.21.91.29   HTTP   288   GET /
MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUO48hHIIxYdUvkOeNRji0LOHG2eICEAKLqLtGqwFZAM8umB5o%2B9o%3D HTTP/1.1
Frame 9889: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 233, Ack: 789, Len: 234
Hypertext Transfer Protocol
No.   Time   Source   Destination   Protocol Length Info
   9992 13:53:51.348469   72.21.91.29   192.168.0.15   OCSP   842   Response
Frame 9992: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 789, Ack: 467, Len: 788
Hypertext Transfer Protocol
Online Certificate Status Protocol
No.   TIme   Source   Destination   Protocol Length Info

```
No.     Time            Source                  Destination             Protocol Length Info
      8 13:53:41.961211 2600:8806:6202:1d00:b91c:fc89:27b8:2bb 2607:f8b0:4000:802::2003 HTTP    280     GET /GTSGIAG3.crl HTTP/1.1
Frame 8: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 6, Src: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb, Dst: 2607:f8b0:4000:802::2003
Transmission Control Protocol, Src Port: 55415, Dst Port: 80, Seq: 1, Ack: 1, Len: 206
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
    271 13:53:42.229125 2607:f8b0:4000:802::2003 2600:8806:6202:1d00:b91c:fc89:27b8:2bb PKIX-CRL 635     Certificate Revocation List
Frame 271: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 6, Src: 2607:f8b0:4000:802::2003, Dst: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb
Transmission Control Protocol, Src Port: 80, Dst Port: 55415, Seq: 213501, Ack: 207, Len: 561
[176 Reassembled TCP Segments (214061 bytes): #10(1220), #11(1220), #13(1220), #14(1220), #16(1220), #17(1220), #19(1220), #20(1220),
#22(1220), #23(1220), #25(1220), #26(1220), #28(1220), #29(1220), #31(1220), #32(1220), #34(1220), #35(122)]
Hypertext Transfer Protocol
Certificate Revocation List
No.     Time            Source                  Destination             Protocol Length Info
   7316 13:53:50.765262 192.168.0.15            72.21.91.29             HTTP     286     GET /
MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEASfM0R3mPZeksxdD5wos4Y%3D HTTP/1.1
Frame 7316: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 1, Ack: 1, Len: 232
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
   7866 13:53:50.843539 72.21.91.29             192.168.0.15            OCSP     842     Response
Frame 7866: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 1, Ack: 233, Len: 788
Hypertext Transfer Protocol
Online Certificate Status Protocol
No.     Time            Source                  Destination             Protocol Length Info
   9889 13:53:51.327670 192.168.0.15            72.21.91.29             HTTP     288     GET /
MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6gAidtSefNc6DC0OInqPHDQQUD4BhHIIxYdUvKOeNRji0LOHG2eICEAKLqLtGqwFZAM8umB5o%2B9o%3D HTTP/1.1
Frame 9889: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 233, Ack: 789, Len: 234
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
   9992 13:53:51.348469 72.21.91.29             192.168.0.15            OCSP     842     Response
Frame 9992: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 789, Ack: 467, Len: 788
Hypertext Transfer Protocol
Online Certificate Status Protocol
No.     Time            Source                  Destination             Protocol Length Info
  13266 13:53:54.573386 192.168.0.15            151.101.194.167         HTTP     357     GET / HTTP/1.1
Frame 13266: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 151.101.194.167
Transmission Control Protocol, Src Port: 55550, Dst Port: 80, Seq: 1, Ack: 1, Len: 303
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
  13268 13:53:54.587675 151.101.194.167         192.168.0.15            HTTP     333     HTTP/1.1 301 Moved Permanently
Frame 13268: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 4, Src: 151.101.194.167, Dst: 192.168.0.15
Transmission Control Protocol, Src Port: 80, Dst Port: 55550, Seq: 1, Ack: 304, Len: 279
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
  13298 13:53:54.685263 2600:8806:6202:1d00:b91c:fc89:27b8:2bb 2606:4700::6812:15e2 HTTP     315     GET /rootr1/
ME8wTTBLMEkwRzAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDkbwjNvPLFRm7zMB3V80 HTTP/1.1
Frame 13298: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
Internet Protocol Version 6, Src: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb, Dst: 2606:4700::6812:15e2
Transmission Control Protocol, Src Port: 55552, Dst Port: 80, Seq: 1, Ack: 1, Len: 241
Hypertext Transfer Protocol
No.     Time            Source                  Destination             Protocol Length Info
  13302 13:53:54.711825 2606:4700::6812:15e2 2600:8806:6202:1d00:b91c:fc89:27b8:2bb OCSP     851     Response
Frame 13302: 851 bytes on wire (6808 bits), 851 bytes captured (6808 bits) on interface 0
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
Internet Protocol Version 6, Src: 2606:4700::6812:15e2, Dst: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb
Transmission Control Protocol, Src Port: 80, Dst Port: 55552, Seq: 1361, Ack: 242, Len: 777
[2 Reassembled TCP Segments (2137 bytes): #13301(1360), #13302(777)]
Hypertext Transfer Protocol
Online Certificate Status Protocol
No.     Time            Source                  Destination             Protocol Length Info
  42184 13:56:05.531537 192.168.0.15            52.218.224.179          HTTP     133     GET /quantcast.html HTTP/1.1
```