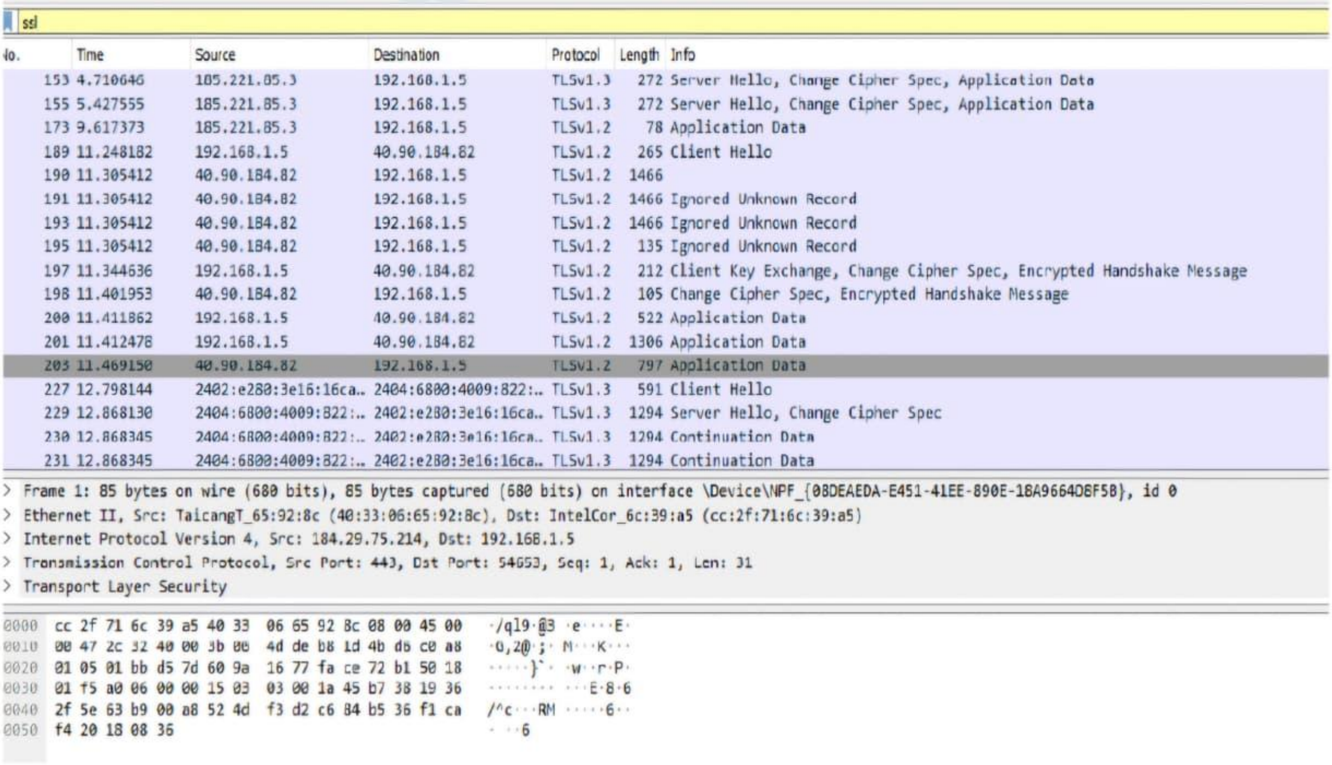
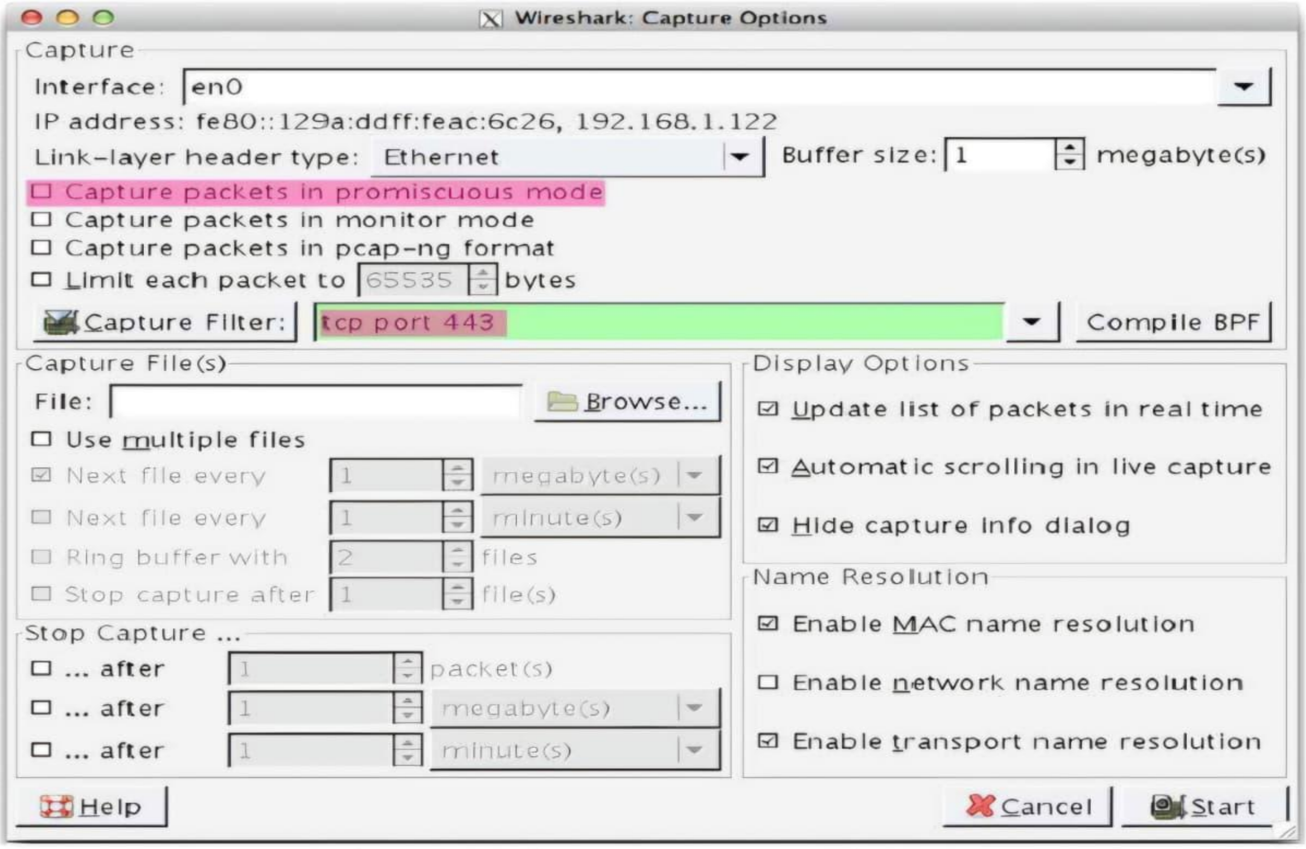
To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e- commerce etc.)



```
ssl
No.    Time       Source                Destination           Protocol Length Info
   153 4.710646   185.221.85.3          192.168.1.5           TLSv1.3   272 Server Hello, Change Cipher Spec, Application Data
   155 5.427555   185.221.85.3          192.168.1.5           TLSv1.3   272 Server Hello, Change Cipher Spec, Application Data
   173 9.617373   185.221.85.3          192.168.1.5           TLSv1.2    78 Application Data
   189 11.248182  192.168.1.5           40.90.184.82          TLSv1.2   265 Client Hello
   190 11.305412  40.90.184.82          192.168.1.5           TLSv1.2  1466
   191 11.305412  40.90.184.82          192.168.1.5           TLSv1.2  1466 Ignored Unknown Record
   193 11.305412  40.90.184.82          192.168.1.5           TLSv1.2  1466 Ignored Unknown Record
   195 11.305412  40.90.184.82          192.168.1.5           TLSv1.2   135 Ignored Unknown Record
   197 11.344636  192.168.1.5           40.90.184.82          TLSv1.2   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   198 11.401953  40.90.184.82          192.168.1.5           TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
   200 11.411862  192.168.1.5           40.90.184.82          TLSv1.2   522 Application Data
   201 11.412478  192.168.1.5           40.90.184.82          TLSv1.2  1306 Application Data
   203 11.469150  40.90.184.82          192.168.1.5           TLSv1.2   797 Application Data
   227 12.798144  2402:e280:3e16:16ca.. 2404:6800:4009:822:.. TLSv1.3   591 Client Hello
   229 12.868130  2404:6800:4009:822:.. 2402:e280:3e16:16ca.. TLSv1.3  1294 Server Hello, Change Cipher Spec
   230 12.868345  2404:6800:4009:822:.. 2402:e280:3e16:16ca.. TLSv1.3  1294 Continuation Data
   231 12.868345  2404:6800:4009:822:.. 2402:e280:3e16:16ca.. TLSv1.3  1294 Continuation Data

> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{0BDEAEDA-E451-41EE-890E-18A9664D8F5B}, id 0
> Ethernet II, Src: TaicangT_65:92:8c (40:33:06:65:92:8c), Dst: IntelCor_6c:39:a5 (cc:2f:71:6c:39:a5)
> Internet Protocol Version 4, Src: 184.29.75.214, Dst: 192.168.1.5
> Transmission Control Protocol, Src Port: 443, Dst Port: 54653, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security

0000  cc 2f 71 6c 39 a5 40 33  06 65 92 8c 08 00 45 00   ·/ql9·@3 ·e····E·
0010  00 47 2c 32 40 00 3b 06  4d de b8 1d 4b d6 c0 a8   ·G,2@·;· M···K···
0020  01 05 01 bb d5 7d 60 9a  16 77 fa ce 72 b1 50 18   ·····}`· ·w··r·P·
0030  01 f5 a0 06 00 00 15 03  03 00 1a 45 b7 38 19 36   ········ ···E·8·6
0040  2f 5e 63 b9 00 a8 52 4d  f3 d2 c6 84 b5 36 f1 ca   /^c···RM ·····6··
0050  f4 20 18 08 36                                     · ··6
```



Capture

Interface: en0

IP address: fe80::129a:ddff:feac:6c26, 192.168.1.122

Link-layer header type: Ethernet

Buffer size: 1 megabyte(s)

☐ Capture packets in promiscuous mode

☐ Capture packets in monitor mode

☐ Capture packets in pcap-ng format

☐ Limit each packet to 65535 bytes

Capture Filter: tcp port 443

Capture File(s)

File:

☐ Use multiple files

☑ Next file every 1 megabyte(s)

☐ Next file every 1 minute(s)

☐ Ring buffer with 2 files

☐ Stop capture after 1 file(s)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

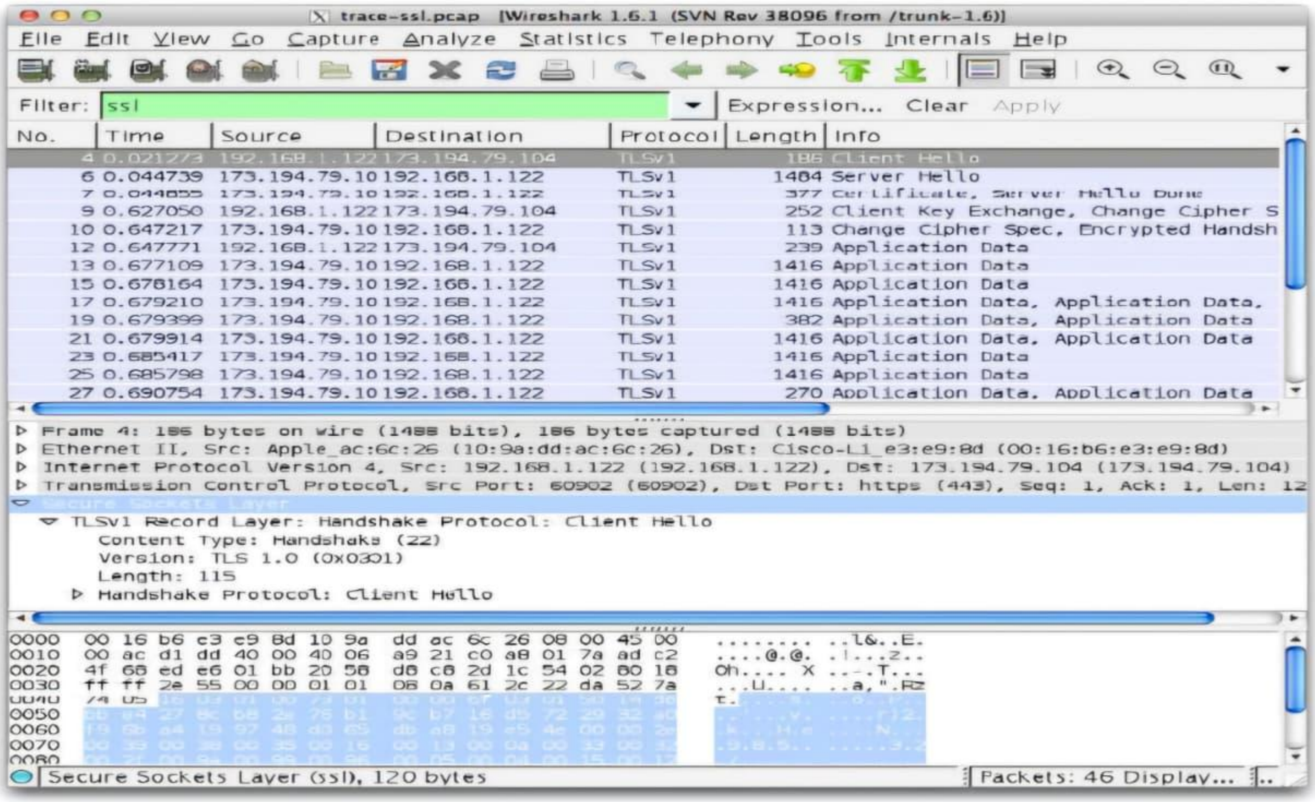
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Figure 1: Setting up the capture options



trace-ssl.pcap [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

Filter: ssl

```
No.   Time       Source          Destination     Protocol  Length Info
    4 0.021273   192.168.1.122   173.194.79.104  TLSv1      186 Client Hello
    6 0.044739   173.194.79.10   192.168.1.122   TLSv1     1484 Server Hello
    7 0.044855   173.194.79.10   192.168.1.122   TLSv1      377 Certificate, Server Hello Done
    9 0.627050   192.168.1.122   173.194.79.104  TLSv1      252 Client Key Exchange, Change Cipher S
   10 0.647217   173.194.79.10   192.168.1.122   TLSv1      113 Change Cipher Spec, Encrypted Handsh
   12 0.647771   192.168.1.122   173.194.79.104  TLSv1      239 Application Data
   13 0.677109   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data
   15 0.678164   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data
   17 0.679210   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data, Application Data,
   19 0.679399   173.194.79.10   192.168.1.122   TLSv1      382 Application Data, Application Data
   21 0.679914   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data, Application Data
   23 0.685417   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data
   25 0.685798   173.194.79.10   192.168.1.122   TLSv1     1416 Application Data
   27 0.690754   173.194.79.10   192.168.1.122   TLSv1      270 Application Data, Application Data
```

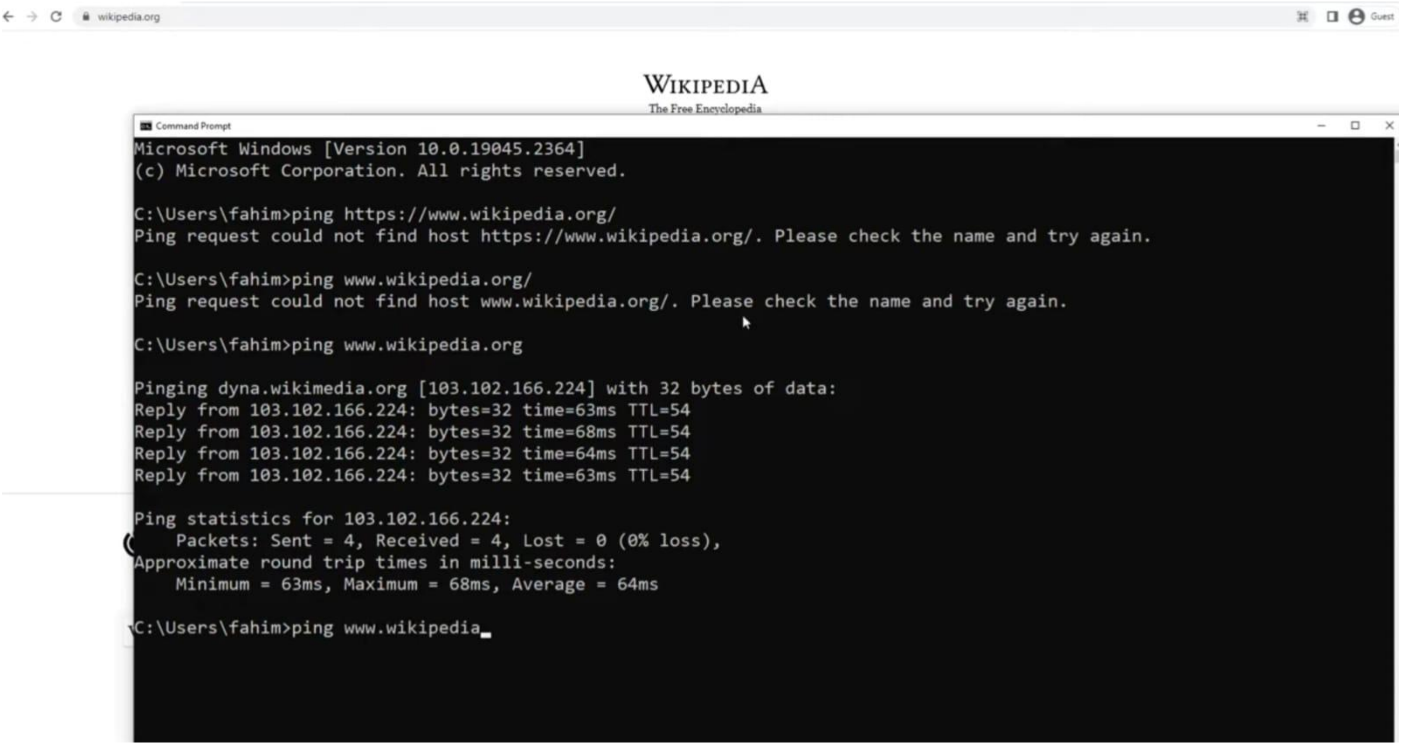
```
▷ Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)
▷ Ethernet II, Src: Apple_ac:6c:26 (10:9a:dd:ac:6c:26), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
▷ Internet Protocol Version 4, Src: 192.168.1.122 (192.168.1.122), Dst: 173.194.79.104 (173.194.79.104)
▷ Transmission Control Protocol, Src Port: 60902 (60902), Dst Port: https (443), Seq: 1, Ack: 1, Len: 12
▽ Secure Sockets Layer
  ▽ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshaks (22)
      Version: TLS 1.0 (0x0301)
      Length: 115
    ▷ Handshake Protocol: Client Hello
```

```
0000  00 16 b6 e3 e9 8d 10 9a  dd ac 6c 26 08 00 45 00   ........ ..l&..E.
0010  00 ac d1 dd 40 00 40 06  a9 21 c0 a8 01 7a ad c2   ....@.@. .!...z..
0020  4f 68 ed e6 01 bb 20 58  d8 c8 2d 1c 54 02 80 18   Oh.... X ..-.T...
0030  ff ff 2e 55 00 00 01 01  08 0a 61 2c 22 da 52 7a   ...U.... ..a,".Rz
0040  74 05 16 03 01 00 73 01  00 00 6f 03 01 50 14 8e   t.....s. ..o..P..
0050  cb e4 27 8c b8 2a 76 b1  9c b7 16 d5 72 29 32 a0   ..'..*v. ....r)2.
0060  19 6b a4 19 97 48 d3 65  db a8 19 e5 4e 00 00 2e   .k...H.e ....N...
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   .9.8.5.. .....3.2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ./
```

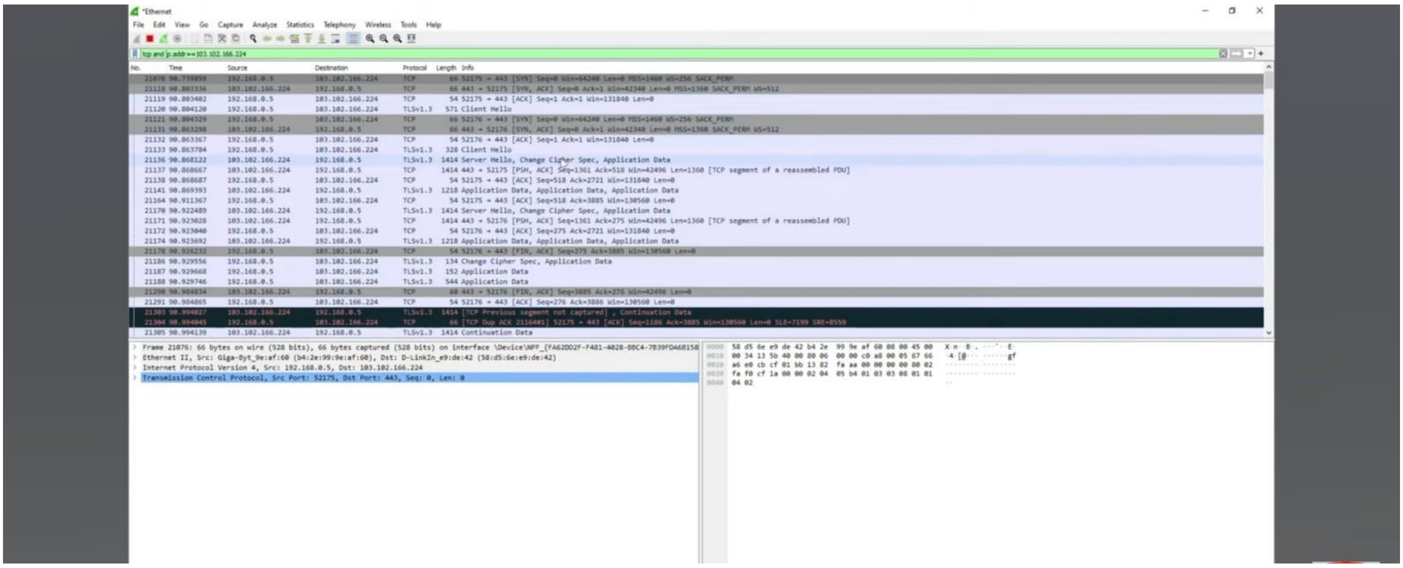
Secure Sockets Layer (ssl), 120 bytes

Packets: 46 Display...

Capture packets using Wireshark, write the exact packet capture filter expressions to accomplish the operations given and save the output in file

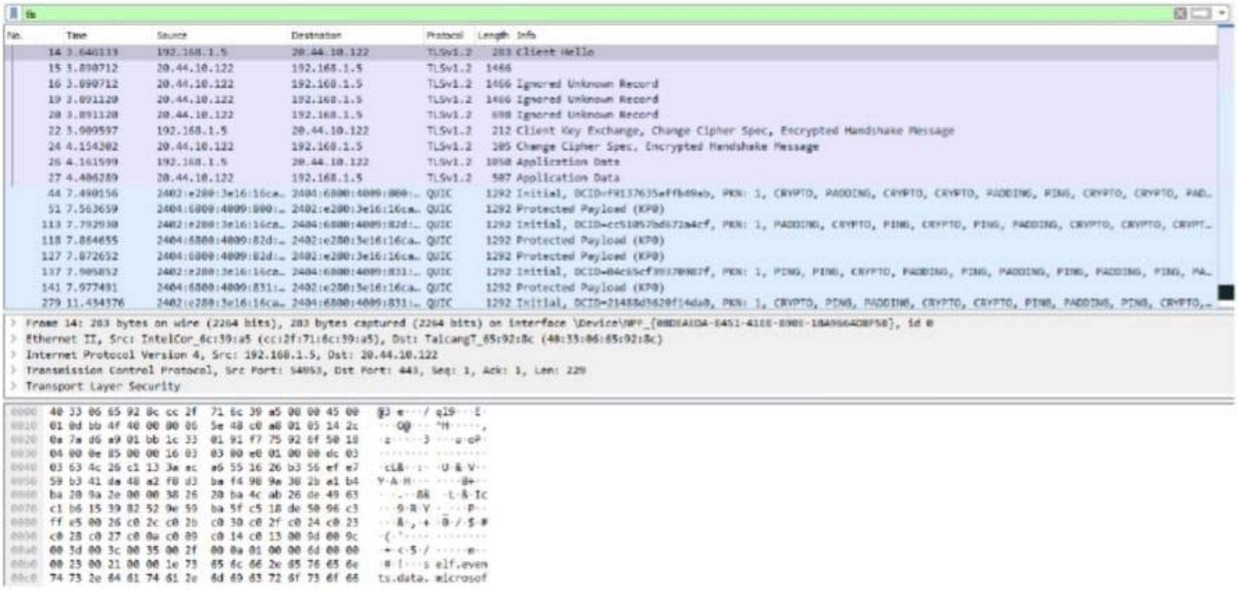


```
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\fahim>ping https://www.wikipedia.org/
Ping request could not find host https://www.wikipedia.org/. Please check the name and try again.

C:\Users\fahim>ping www.wikipedia.org/
Ping request could not find host www.wikipedia.org/. Please check the name and try again.

C:\Users\fahim>ping www.wikipedia.org

Pinging dyna.wikimedia.org [103.102.166.224] with 32 bytes of data:
Reply from 103.102.166.224: bytes=32 time=63ms TTL=54
Reply from 103.102.166.224: bytes=32 time=68ms TTL=54
Reply from 103.102.166.224: bytes=32 time=64ms TTL=54
Reply from 103.102.166.224: bytes=32 time=63ms TTL=54

Ping statistics for 103.102.166.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 63ms, Maximum = 68ms, Average = 64ms

C:\Users\fahim>ping www.wikipedia
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp and ip.addr==103.102.166.224

No.   Time      Source           Destination      Protocol Length Info
21076 90.739859 192.168.0.5      103.102.166.224  TCP        66 52175 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21118 90.803336 103.102.166.224  192.168.0.5      TCP        66 443 → 52175 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1360 SACK_PERM WS=512
21119 90.803402 192.168.0.5      103.102.166.224  TCP        54 52175 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
21120 90.804120 192.168.0.5      103.102.166.224  TLSv1.3   571 Client Hello
21121 90.804329 192.168.0.5      103.102.166.224  TCP        66 52176 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
21131 90.863298 103.102.166.224  192.168.0.5      TCP        66 443 → 52176 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1360 SACK_PERM WS=512
21132 90.863367 192.168.0.5      103.102.166.224  TCP        54 52176 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
21133 90.863784 192.168.0.5      103.102.166.224  TLSv1.3   328 Client Hello
21136 90.868122 103.102.166.224  192.168.0.5      TLSv1.3  1414 Server Hello, Change Cipher Spec, Application Data
21137 90.868667 103.102.166.224  192.168.0.5      TCP      1414 443 → 52175 [PSH, ACK] Seq=1361 Ack=518 Win=42496 Len=1360 [TCP segment of a reassembled PDU]
21138 90.868687 192.168.0.5      103.102.166.224  TCP        54 52175 → 443 [ACK] Seq=518 Ack=2721 Win=131840 Len=0
21141 90.869393 103.102.166.224  192.168.0.5      TLSv1.3  1218 Application Data, Application Data, Application Data
21164 90.911367 192.168.0.5      103.102.166.224  TCP        54 52175 → 443 [ACK] Seq=518 Ack=3885 Win=130560 Len=0
21170 90.922489 103.102.166.224  192.168.0.5      TLSv1.3  1414 Server Hello, Change Cipher Spec, Application Data
21171 90.923028 103.102.166.224  192.168.0.5      TCP      1414 443 → 52176 [PSH, ACK] Seq=1361 Ack=275 Win=42496 Len=1360 [TCP segment of a reassembled PDU]
21172 90.923040 192.168.0.5      103.102.166.224  TCP        54 52176 → 443 [ACK] Seq=275 Ack=2721 Win=131840 Len=0
21174 90.923692 103.102.166.224  192.168.0.5      TLSv1.3  1218 Application Data, Application Data, Application Data
21178 90.926232 192.168.0.5      103.102.166.224  TCP        54 52176 → 443 [FIN, ACK] Seq=275 Ack=3885 Win=130560 Len=0
21186 90.929556 192.168.0.5      103.102.166.224  TLSv1.3   134 Change Cipher Spec, Application Data
21187 90.929668 192.168.0.5      103.102.166.224  TLSv1.3   152 Application Data
21188 90.929746 192.168.0.5      103.102.166.224  TLSv1.3   544 Application Data
21290 90.984834 103.102.166.224  192.168.0.5      TCP        60 443 → 52176 [FIN, ACK] Seq=3885 Ack=276 Win=42496 Len=0
21291 90.984865 192.168.0.5      103.102.166.224  TCP        54 52176 → 443 [ACK] Seq=276 Ack=3886 Win=130560 Len=0
21303 90.994027 103.102.166.224  192.168.0.5      TLSv1.3  1414 [TCP Previous segment not captured] , Continuation Data
21304 90.994045 192.168.0.5      103.102.166.224  TCP        66 [TCP Dup ACK 21164#1] 52175 → 443 [ACK] Seq=1186 Ack=3885 Win=130560 Len=0 SLE=7199 SRE=8559
21305 90.994139 103.102.166.224  192.168.0.5      TLSv1.3  1414 Continuation Data

> Frame 21076: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{FA62DD2F-F481-4028-BBC4-7B39FDA6B158
> Ethernet II, Src: Giga-Byt_9e:af:60 (b4:2e:99:9e:af:60), Dst: D-LinkIn_e9:de:42 (58:d5:6e:e9:de:42)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 103.102.166.224
> Transmission Control Protocol, Src Port: 52175, Dst Port: 443, Seq: 0, Len: 0

0000  58 d5 6e e9 de 42 b4 2e  99 9e af 60 08 00 45 00   X·n··B·.···`··E·
0010  00 34 13 5b 40 00 80 06  00 00 c0 a8 00 05 67 66   ·4·[@·········gf
0020  a6 e0 cb cf 01 bb 13 82  fa aa 00 00 00 00 80 02   ················
0030  fa f0 cf 1a 00 00 02 04  05 b4 01 03 03 08 01 01   ················
0040  04 02                                              ··
```

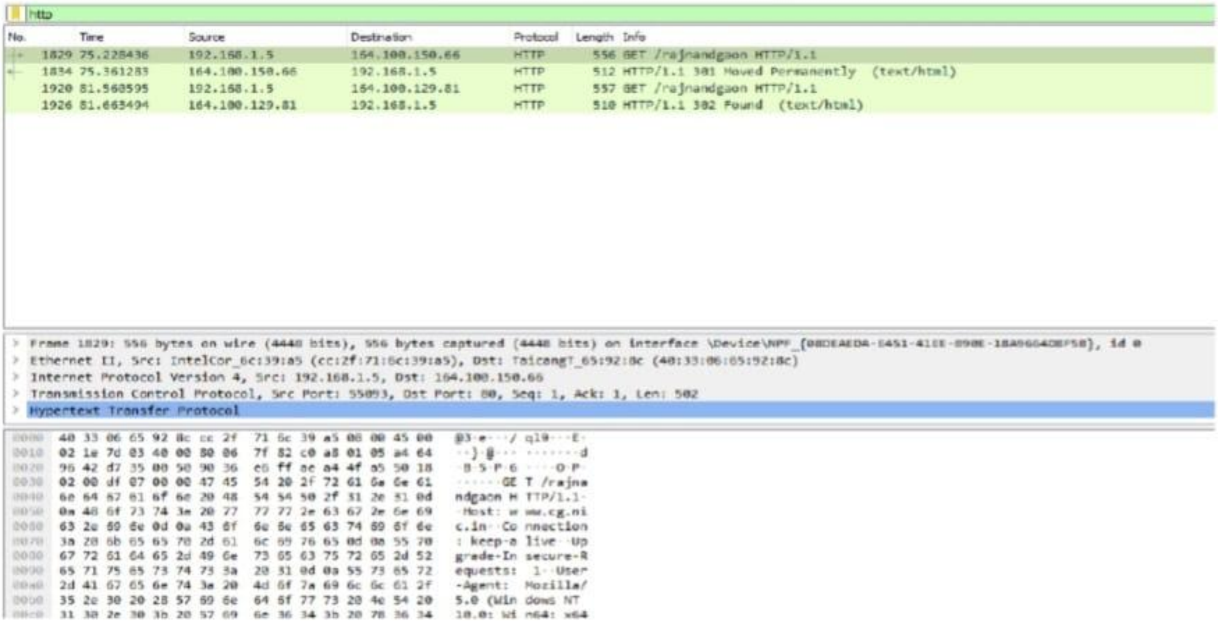
Study and Analyze the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool



```
No.     Time        Source                    Destination               Protocol  Length Info
     14 3.646133    192.168.1.5               20.44.10.122              TLSv1.2    283 Client Hello
     15 3.890712    20.44.10.122              192.168.1.5               TLSv1.2   1466
     16 3.890712    20.44.10.122              192.168.1.5               TLSv1.2   1466 Ignored Unknown Record
     19 3.891120    20.44.10.122              192.168.1.5               TLSv1.2   1466 Ignored Unknown Record
     20 3.891120    20.44.10.122              192.168.1.5               TLSv1.2    698 Ignored Unknown Record
     22 3.909597    192.168.1.5               20.44.10.122              TLSv1.2    212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
     24 4.154302    20.44.10.122              192.168.1.5               TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
     26 4.161599    192.168.1.5               20.44.10.122              TLSv1.2   1050 Application Data
     27 4.406289    20.44.10.122              192.168.1.5               TLSv1.2    587 Application Data
     44 7.490156    2402:e280:3e16:16ca…      2404:6800:4009:800:…      QUIC      1292 Initial, DCID=f9137635affb49ab, PKN: 1, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, PAD…
     51 7.563659    2404:6800:4009:800:…      2402:e280:3e16:16ca…      QUIC      1292 Protected Payload (KP0)
    113 7.792930    2402:e280:3e16:16ca…      2404:6800:4009:82d:…      QUIC      1292 Initial, DCID=cc51057bd672a4cf, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, CRYPT…
    118 7.864655    2404:6800:4009:82d:…      2402:e280:3e16:16ca…      QUIC      1292 Protected Payload (KP0)
    127 7.872652    2404:6800:4009:82d:…      2402:e280:3e16:16ca…      QUIC      1292 Protected Payload (KP0)
    137 7.905852    2402:e280:3e16:16ca…      2404:6800:4009:831:…      QUIC      1292 Initial, DCID=04c65cf393709e7f, PKN: 1, PING, PING, CRYPTO, PADDING, PING, PADDING, PING, PADDING, PING, PA…
    141 7.977491    2404:6800:4009:831:…      2402:e280:3e16:16ca…      QUIC      1292 Protected Payload (KP0)
    279 11.434376   2402:e280:3e16:16ca…      2404:6800:4009:831:…      QUIC      1292 Initial, DCID=21488d3620f14da0, PKN: 1, CRYPTO, PING, PADDING, CRYPTO, CRYPTO, PING, PADDING, PING, CRYPTO,…
```

```
> Frame 14: 283 bytes on wire (2264 bits), 283 bytes captured (2264 bits) on interface \Device\NPF_{08DEAEDA-E451-41EE-890E-18A9664D8F58}, id 0
> Ethernet II, Src: IntelCor_6c:39:a5 (cc:2f:71:6c:39:a5), Dst: TaicangT_65:92:8c (40:33:06:65:92:8c)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 20.44.10.122
> Transmission Control Protocol, Src Port: 54053, Dst Port: 443, Seq: 1, Ack: 1, Len: 229
> Transport Layer Security
```

```
0000  40 33 06 65 92 8c cc 2f  71 6c 39 a5 08 00 45 00   @3·e···/ q l9··E·
0010  01 0d bb 4f 40 00 80 06  5e 48 c0 a8 01 05 14 2c   ···O@··· ^H·····,
0020  0a 7a d6 a9 01 bb 1c 33  01 91 f7 75 92 6f 50 18   ·z·····3 ···u·oP·
0030  04 00 0e 85 00 00 16 03  03 00 e0 01 00 00 dc 03   ········ ········
0040  03 63 4c 26 c1 13 3a ec  a6 55 16 26 b3 56 ef e7   ·cL&··:· ·U·&·V··
0050  59 b3 41 da 48 a2 f8 d3  ba f4 98 9a 38 2b a1 b4   Y·A·H··· ····8+··
0060  ba 20 9a 2e 00 00 38 26  20 ba 4c ab 26 de 49 63   · ·.··8&  ·L·&·Ic
0070  c1 b6 15 39 82 52 9e 59  ba 5f c5 18 de 50 96 c3   ···9·R·Y ·_···P··
0080  ff e5 00 26 c0 2c c0 2b  c0 30 c0 2f c0 24 c0 23   ···&·,·+ ·0·/·$·#
0090  c0 28 c0 27 c0 0a c0 09  c0 14 c0 13 00 9d 00 9c   ·(·'···· ········
00a0  00 3d 00 3c 00 35 00 2f  00 0a 01 00 00 6d 00 00   ·=·<·5·/ ·····m··
00b0  00 23 00 21 00 00 1e 73  65 6c 66 2e 65 76 65 6e   ·#·!···s elf.even
00c0  74 73 2e 64 61 74 61 2e  6d 69 63 72 6f 73 6f 66   ts.data. microsof
```



```
No.     Time        Source            Destination       Protocol  Length Info
   1829 75.228436   192.168.1.5       164.100.150.66    HTTP       556 GET /rajnandgaon HTTP/1.1
   1834 75.361283   164.100.150.66    192.168.1.5       HTTP       512 HTTP/1.1 301 Moved Permanently  (text/html)
   1920 81.560595   192.168.1.5       164.100.129.81    HTTP       557 GET /rajnandgaon HTTP/1.1
   1926 81.663494   164.100.129.81    192.168.1.5       HTTP       510 HTTP/1.1 302 Found  (text/html)
```

```
> Frame 1829: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface \Device\NPF_{08DEAEDA-E451-41EE-890E-18A9664D8F58}, id 0
> Ethernet II, Src: IntelCor_6c:39:a5 (cc:2f:71:6c:39:a5), Dst: TaicangT_65:92:8c (40:33:06:65:92:8c)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 164.100.150.66
> Transmission Control Protocol, Src Port: 55093, Dst Port: 80, Seq: 1, Ack: 1, Len: 502
> Hypertext Transfer Protocol
```

```
0000  40 33 06 65 92 8c cc 2f  71 6c 39 a5 08 00 45 00   @3·e···/ ql9···E·
0010  02 1e 7d 03 40 00 80 06  7f 82 c0 a8 01 05 a4 64   ··}·@··· ·······d
0020  96 42 d7 35 00 50 90 36  e6 ff ae a4 4f a5 50 18   ·B·5·P·6 ····O·P·
0030  02 00 df 07 00 00 47 45  54 20 2f 72 61 6a 6e 61   ······GE T /rajna
0040  6e 64 67 61 6f 6e 20 48  54 54 50 2f 31 2e 31 0d   ndgaon H TTP/1.1·
0050  0a 48 6f 73 74 3a 20 77  77 77 2e 63 67 2e 6e 69   ·Host: w ww.cg.ni
0060  63 2e 69 6e 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   c.in··Co nnection
0070  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 55 70   : keep-a live··Up
0080  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52   grade-In secure-R
0090  65 71 75 65 73 74 73 3a  20 31 0d 0a 55 73 65 72   equests:  1··User
00a0  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00b0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
00c0  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34   10.0; Wi n64; x64
```

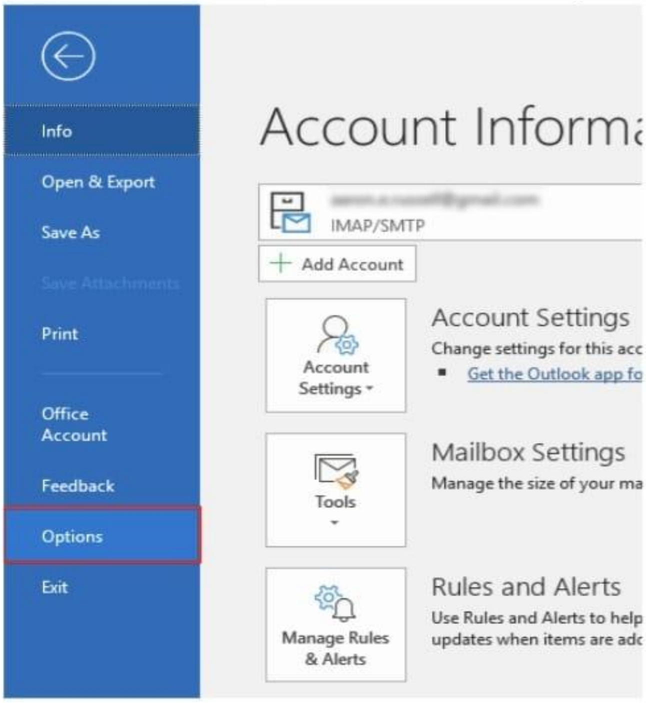
Conclusion:

Hence we have studied and analyzed the performance of HTTP, HTTPS and FTP protocol using Packet tracer tool.

Illustrate the steps for implementation of S/MIME email security through Microsoft® Office Outlook

2. **Open Outlook Options.**

In Outlook, select **File** from the main menu, then click **Options**.



Account Settings

Change settings for this acc

- Get the Outlook app fo

Mailbox Settings

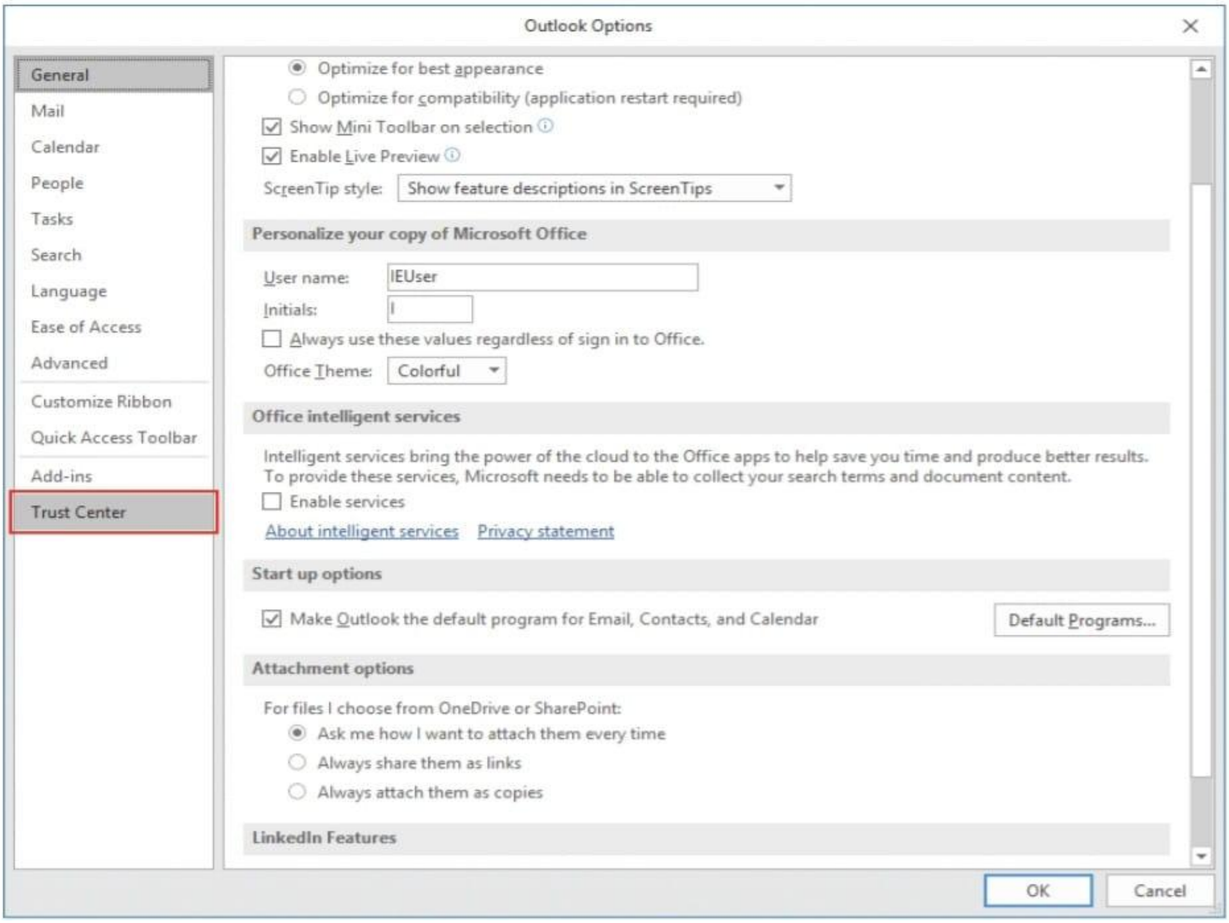
Manage the size of your ma

Rules and Alerts

Use Rules and Alerts to help updates when items are adc

3. **Open Trust Center.**

Select **Trust Center** at the bottom of the menu on the left side of the **Outlook Options** window.



● Optimize for best appearance

○ Optimize for compatibility (application restart required)

☑ Show Mini Toolbar on selection

☑ Enable Live Preview

ScreenTip style: Show feature descriptions in ScreenTips

Personalize your copy of Microsoft Office

User name: IEUser

Initials: I

□ Always use these values regardless of sign in to Office.

Office Theme: Colorful

Office intelligent services

Intelligent services bring the power of the cloud to the Office apps to help save you time and produce better results. To provide these services, Microsoft needs to be able to collect your search terms and document content.

□ Enable services

About intelligent services Privacy statement

Start up options

☑ Make Outlook the default program for Email, Contacts, and Calendar

Attachment options

For files I choose from OneDrive or SharePoint:

● Ask me how I want to attach them every time

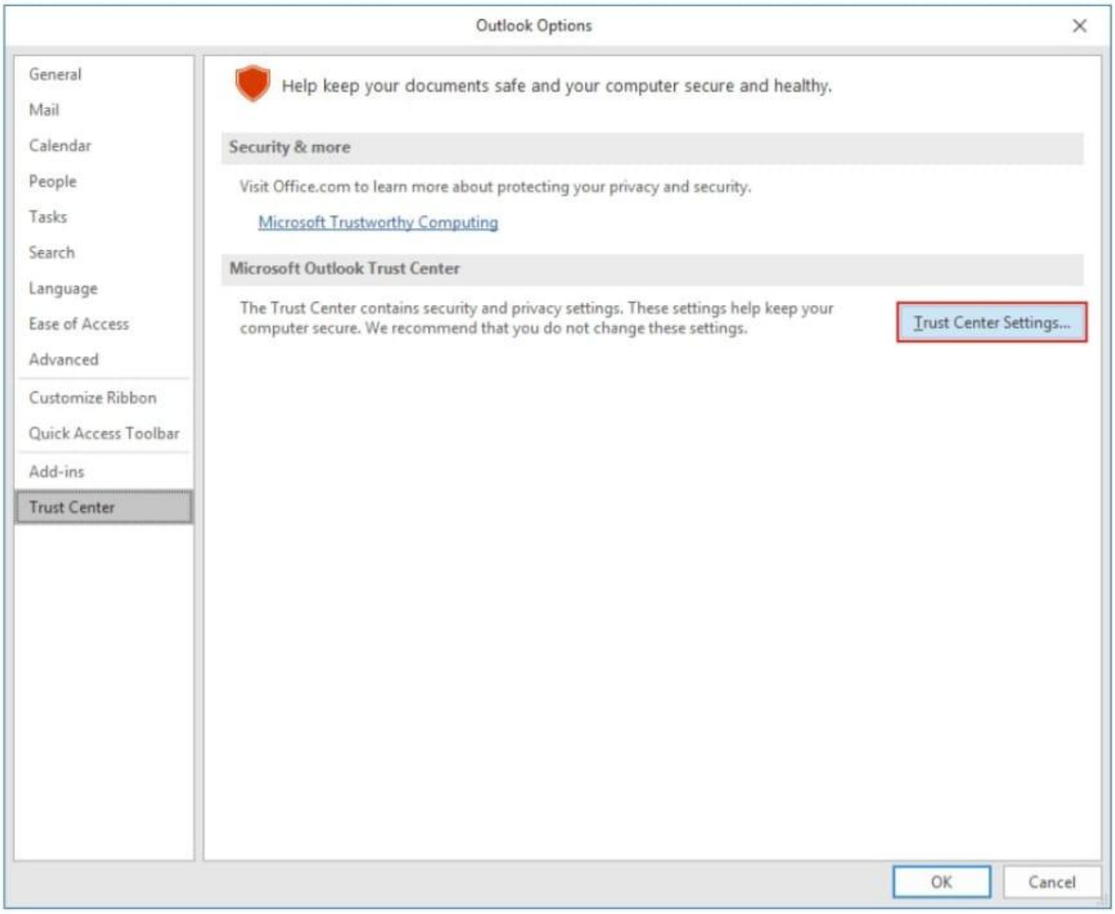
○ Always share them as links

○ Always attach them as copies

LinkedIn Features

4. **Open Trust Center Settings.**

   Click the **Trust Center Settings** button.



Help keep your documents safe and your computer secure and healthy.

Security & more

Visit Office.com to learn more about protecting your privacy and security.

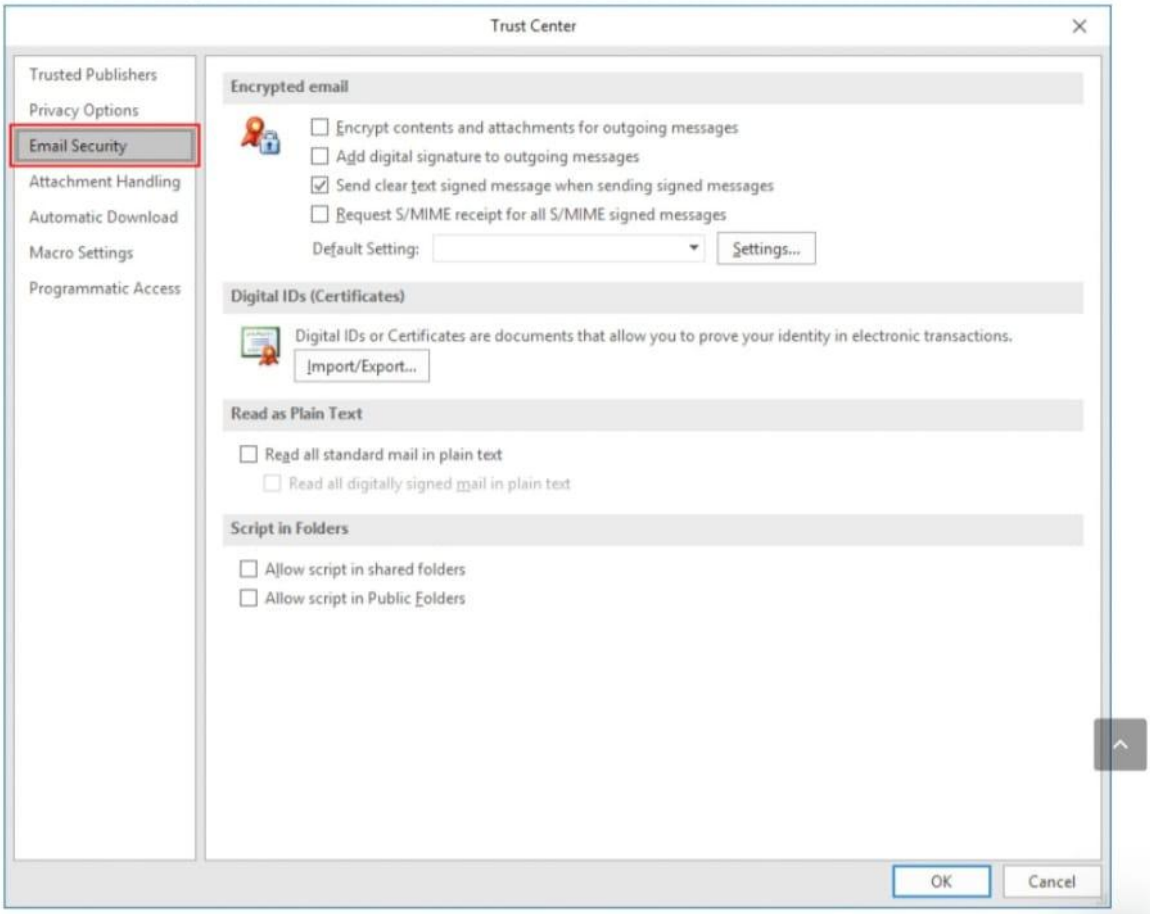
Microsoft Trustworthy Computing

Microsoft Outlook Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

5. **Select Email Security.**

   Select **Email Security** from the left-hand menu of the **Trust Center** window.



Encrypted email

☐ Encrypt contents and attachments for outgoing messages
☐ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

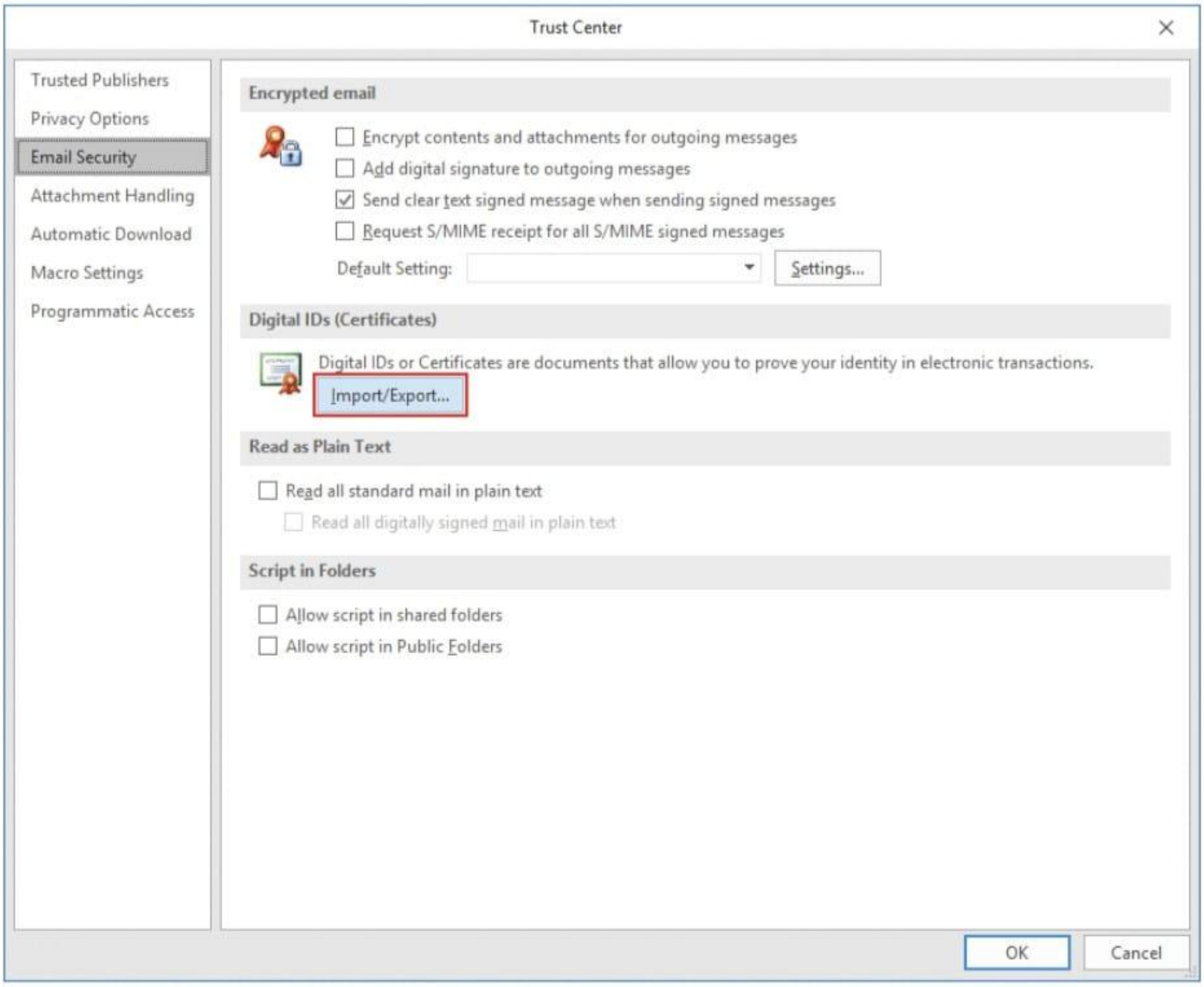
☐ Read all standard mail in plain text
☐ Read all digitally signed mail in plain text

Script in Folders

☐ Allow script in shared folders
☐ Allow script in Public Folders

6. **Click Import/Export.**

Click the **Import/Export** button, under **Digital IDs (Certificates)**.



Trust Center

Trusted Publishers
Privacy Options
Email Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access

Encrypted email

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: [ ] Settings...

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Import/Export...

Read as Plain Text

□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

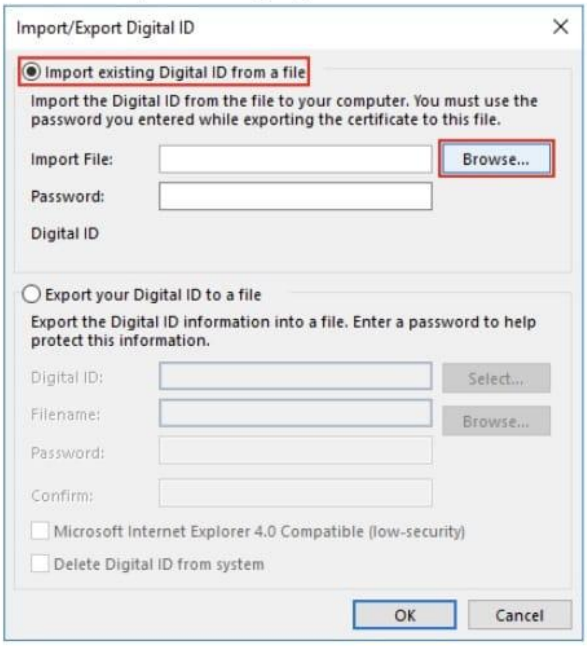
Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

OK Cancel

7. **Browse for file.**

Make sure **Import existing Digital ID from a file** is checked, then click **Browse...**



Import/Export Digital ID

● Import existing Digital ID from a file

Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file.

Import File: [ ] Browse...
Password: [ ]
Digital ID

○ Export your Digital ID to a file

Export the Digital ID information into a file. Enter a password to help protect this information.

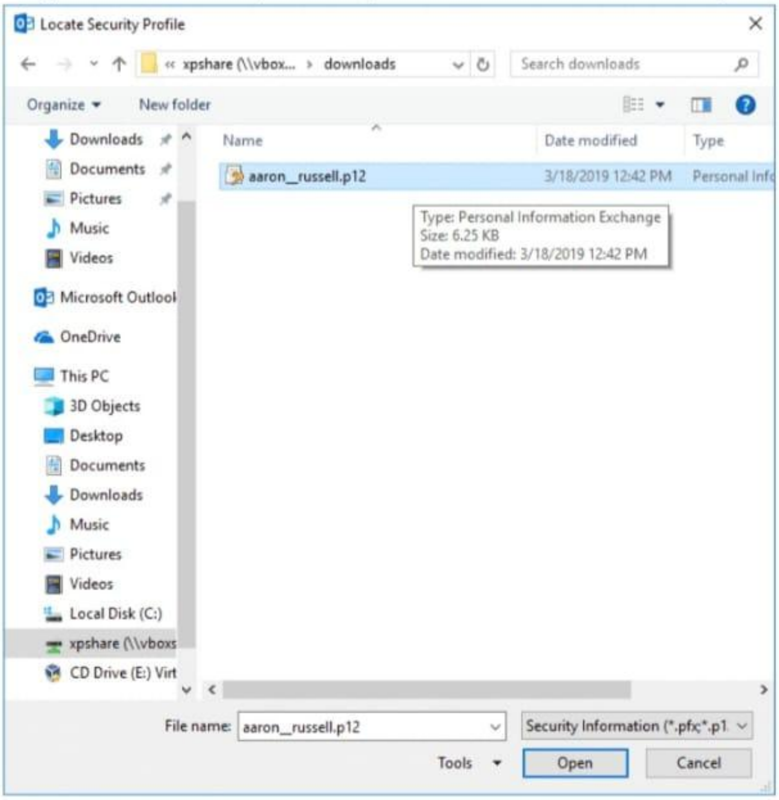
Digital ID: [ ] Select...
Filename: [ ] Browse...
Password: [ ]
Confirm: [ ]

□ Microsoft Internet Explorer 4.0 Compatible (low-security)
□ Delete Digital ID from system

OK Cancel

8. **Open file.**

   Navigate to the PKCS#12 file, then click **Open**. The filename extension should be `.p12`.



aaron__russell.p12 3/18/2019 12:42 PM Personal Info

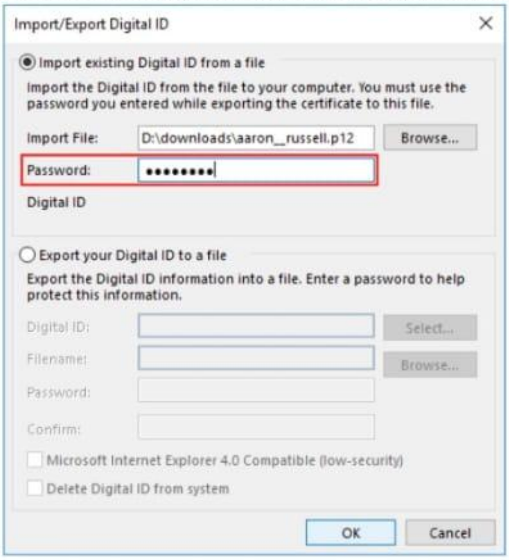
Type: Personal Information Exchange
Size: 6.25 KB
Date modified: 3/18/2019 12:42 PM

File name: aaron__russell.p12

Security Information (*.pfx;*.p1

9. **Enter PKCS#12 password.**

   Enter the password you used when downloading the PKCS#12 file, then click **OK**.



● Import existing Digital ID from a file

Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file.

Import File: D:\downloads\aaron__russell.p12

Password: ••••••••

○ Export your Digital ID to a file

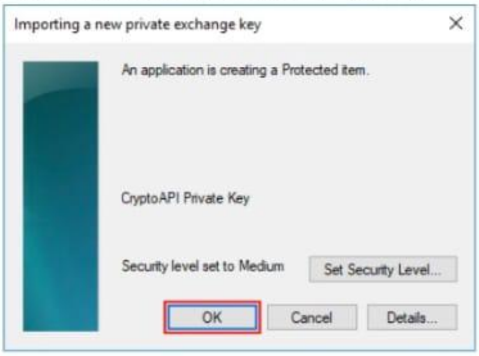
Export the Digital ID information into a file. Enter a password to help protect this information.

□ Microsoft Internet Explorer 4.0 Compatible (low-security)

□ Delete Digital ID from system

10. **Click OK.**

    Click **OK** on the security dialog box that pops up.



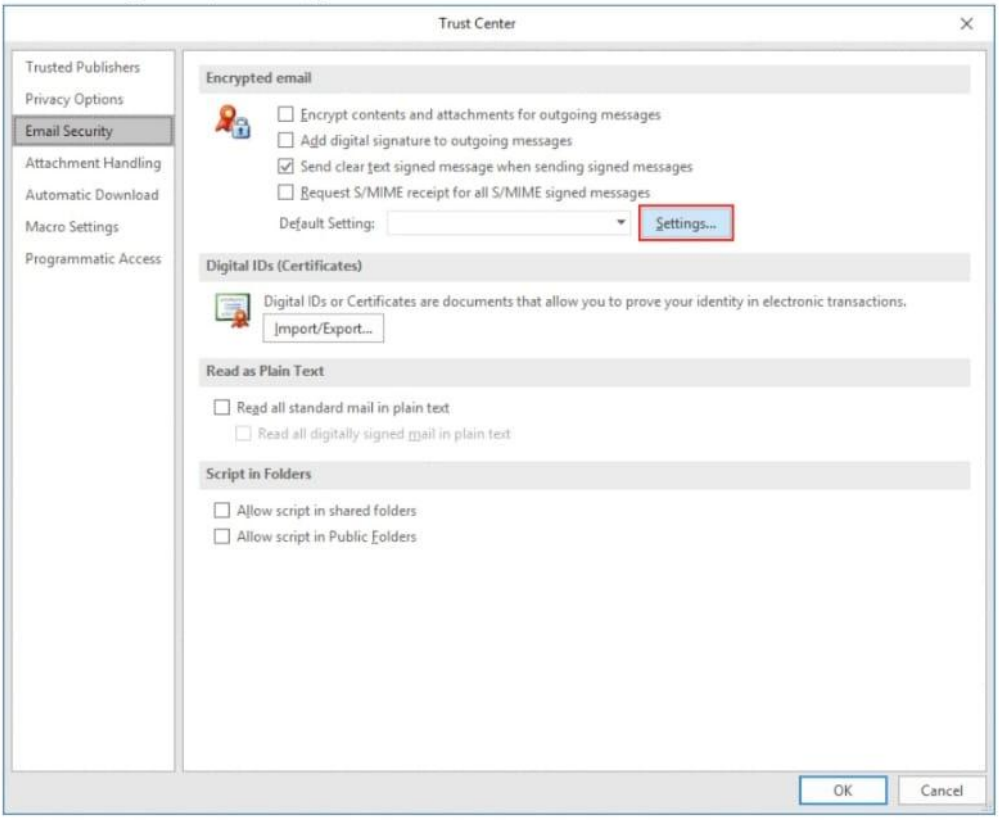
An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

11. **Open encrypted email settings.**

Click the **Settings** button, under **Encrypted email**.



Encrypted email

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

□ Read all standard mail in plain text

□ Read all digitally signed mail in plain text

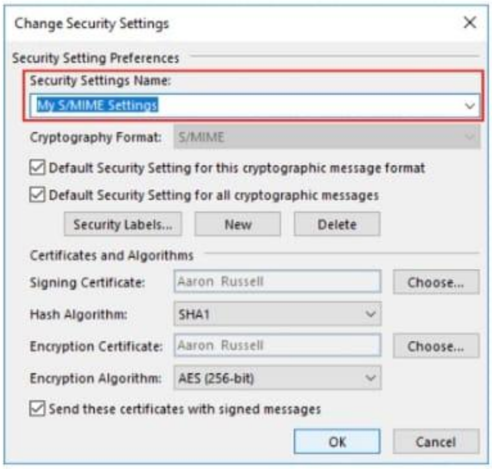
Script in Folders

□ Allow script in shared folders

□ Allow script in Public Folders

12. **Name security settings.**

Enter a name for your security settings.



Security Setting Preferences

Security Settings Name: My S/MIME Settings

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Aaron Russell

Hash Algorithm: SHA1

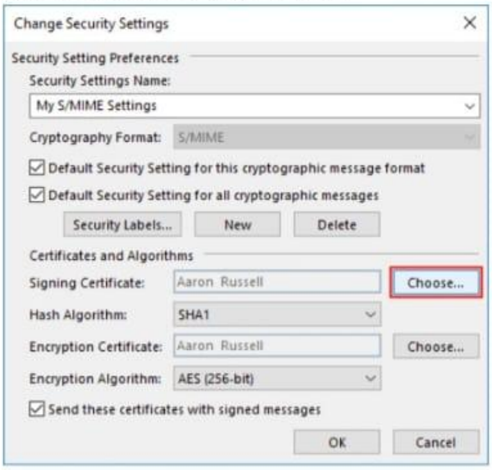
Encryption Certificate: Aaron Russell

Encryption Algorithm: AES (256-bit)

☑ Send these certificates with signed messages

13. **Choose signing certificate.**

Click **Choose**, next to **Signing Certificate**.



Security Setting Preferences

Security Settings Name: My S/MIME Settings

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Aaron Russell

Hash Algorithm: SHA1

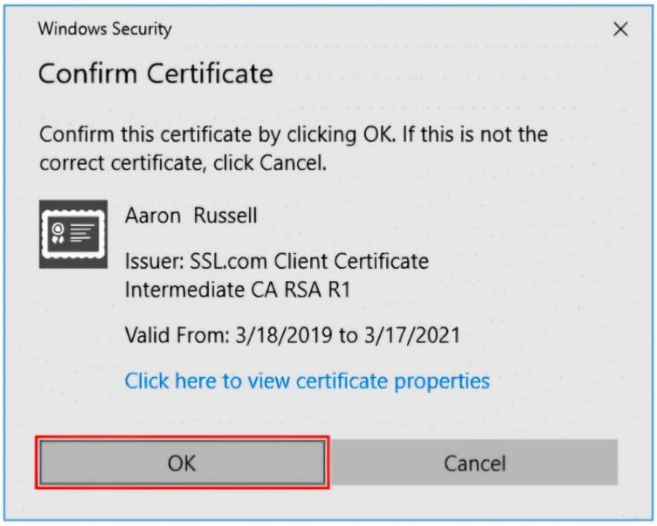
Encryption Certificate: Aaron Russell

Encryption Algorithm: AES (256-bit)

☑ Send these certificates with signed messages

14. **Confirm or select certificate.**

If you have only installed one certificate (as shown here), you can click **OK** on the **Confirm Certificate** dialog box that pops up. Otherwise, you will have to choose one from a list of installed certificates.



Windows Security

Confirm Certificate

Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

Aaron Russell

Issuer: SSL.com Client Certificate Intermediate CA RSA R1

Valid From: 3/18/2019 to 3/17/2021

Click here to view certificate properties