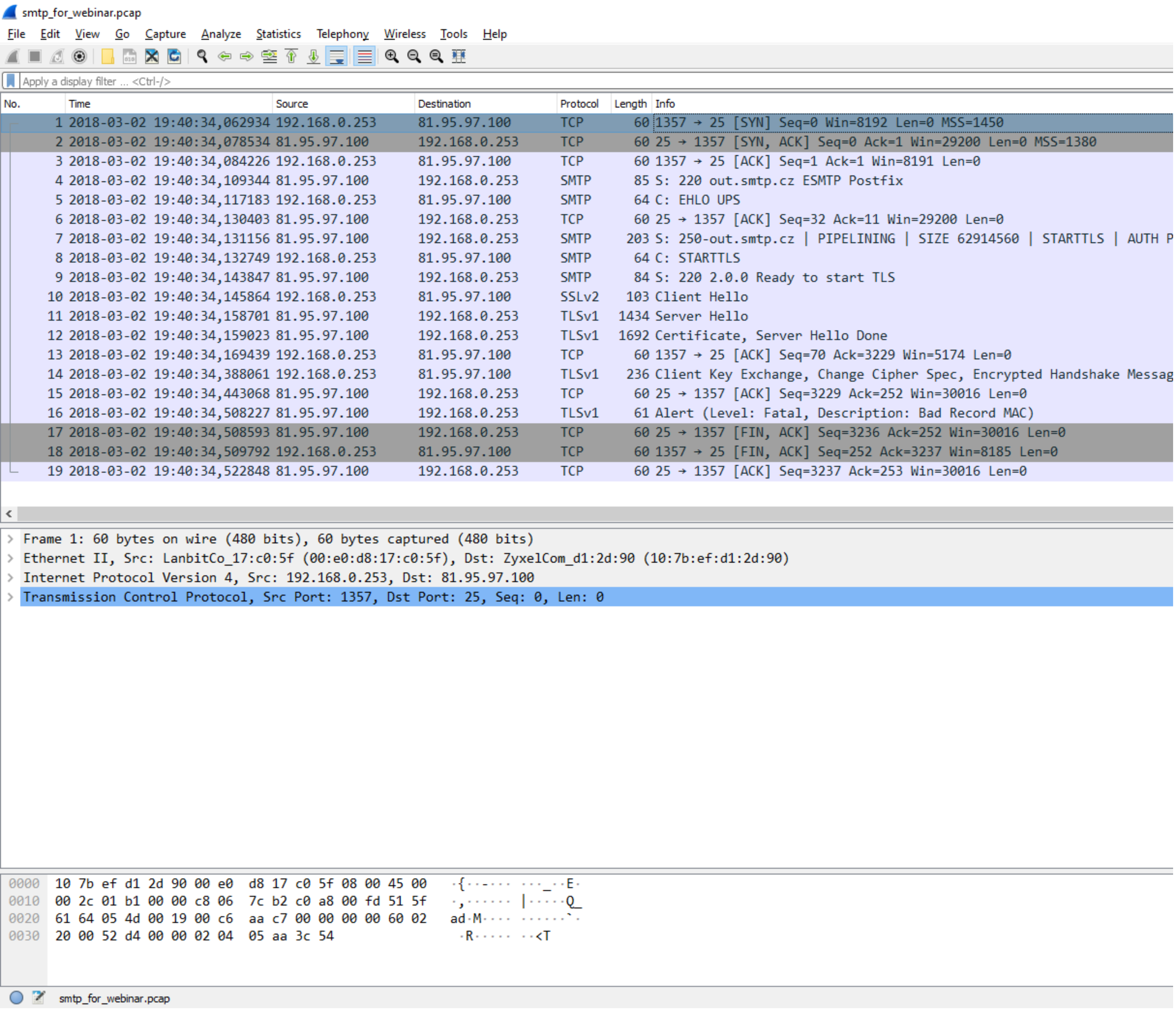
PCAP Analysis Task

Pavel Minařík, Chief Technology Officer

Flowmon
Driving Network Visibility


smtp_for_webinar.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                        Source          Destination     Protocol  Length  Info
   1 2018-03-02 19:40:34,062934 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
   2 2018-03-02 19:40:34,078534 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
   3 2018-03-02 19:40:34,084226 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
   4 2018-03-02 19:40:34,109344 81.95.97.100    192.168.0.253   SMTP         85 S: 220 out.smtp.cz ESMTP Postfix
   5 2018-03-02 19:40:34,117183 192.168.0.253   81.95.97.100    SMTP         64 C: EHLO UPS
   6 2018-03-02 19:40:34,130403 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
   7 2018-03-02 19:40:34,131156 81.95.97.100    192.168.0.253   SMTP        203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
   8 2018-03-02 19:40:34,132749 192.168.0.253   81.95.97.100    SMTP         64 C: STARTTLS
   9 2018-03-02 19:40:34,143847 81.95.97.100    192.168.0.253   SMTP         84 S: 220 2.0.0 Ready to start TLS
  10 2018-03-02 19:40:34,145864 192.168.0.253   81.95.97.100    SSLv2       103 Client Hello
  11 2018-03-02 19:40:34,158701 81.95.97.100    192.168.0.253   TLSv1      1434 Server Hello
  12 2018-03-02 19:40:34,159023 81.95.97.100    192.168.0.253   TLSv1      1692 Certificate, Server Hello Done
  13 2018-03-02 19:40:34,169439 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
  14 2018-03-02 19:40:34,388061 192.168.0.253   81.95.97.100    TLSv1       236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
  15 2018-03-02 19:40:34,443068 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
  16 2018-03-02 19:40:34,508227 81.95.97.100    192.168.0.253   TLSv1        61 Alert (Level: Fatal, Description: Bad Record MAC)
  17 2018-03-02 19:40:34,508593 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
  18 2018-03-02 19:40:34,509792 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
  19 2018-03-02 19:40:34,522848 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

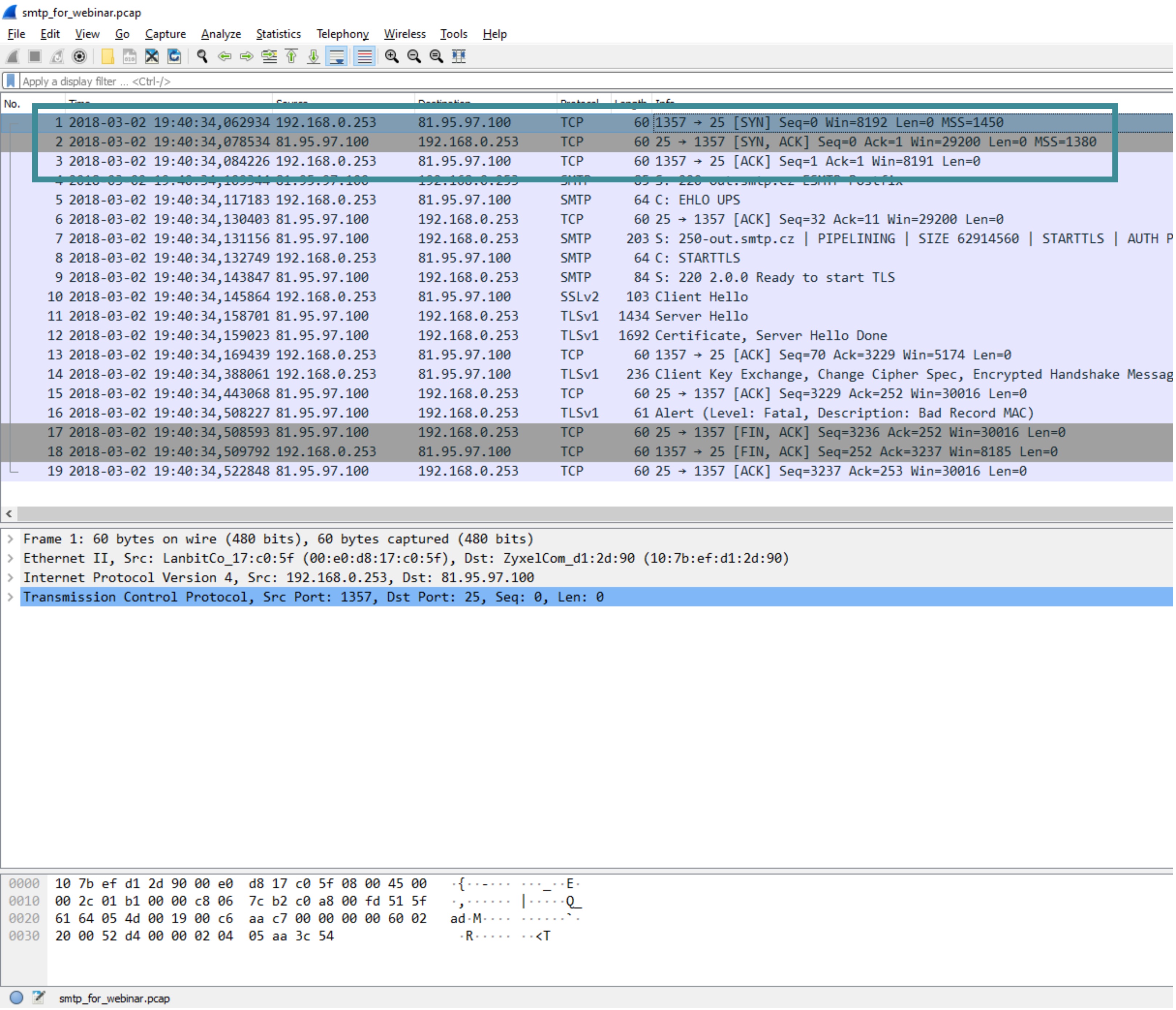
```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R······  ··<T
```

TASK:

Analyze full packet trace (PCAP) file and find out where the problem is.

Flowmon
Driving Network Visibility

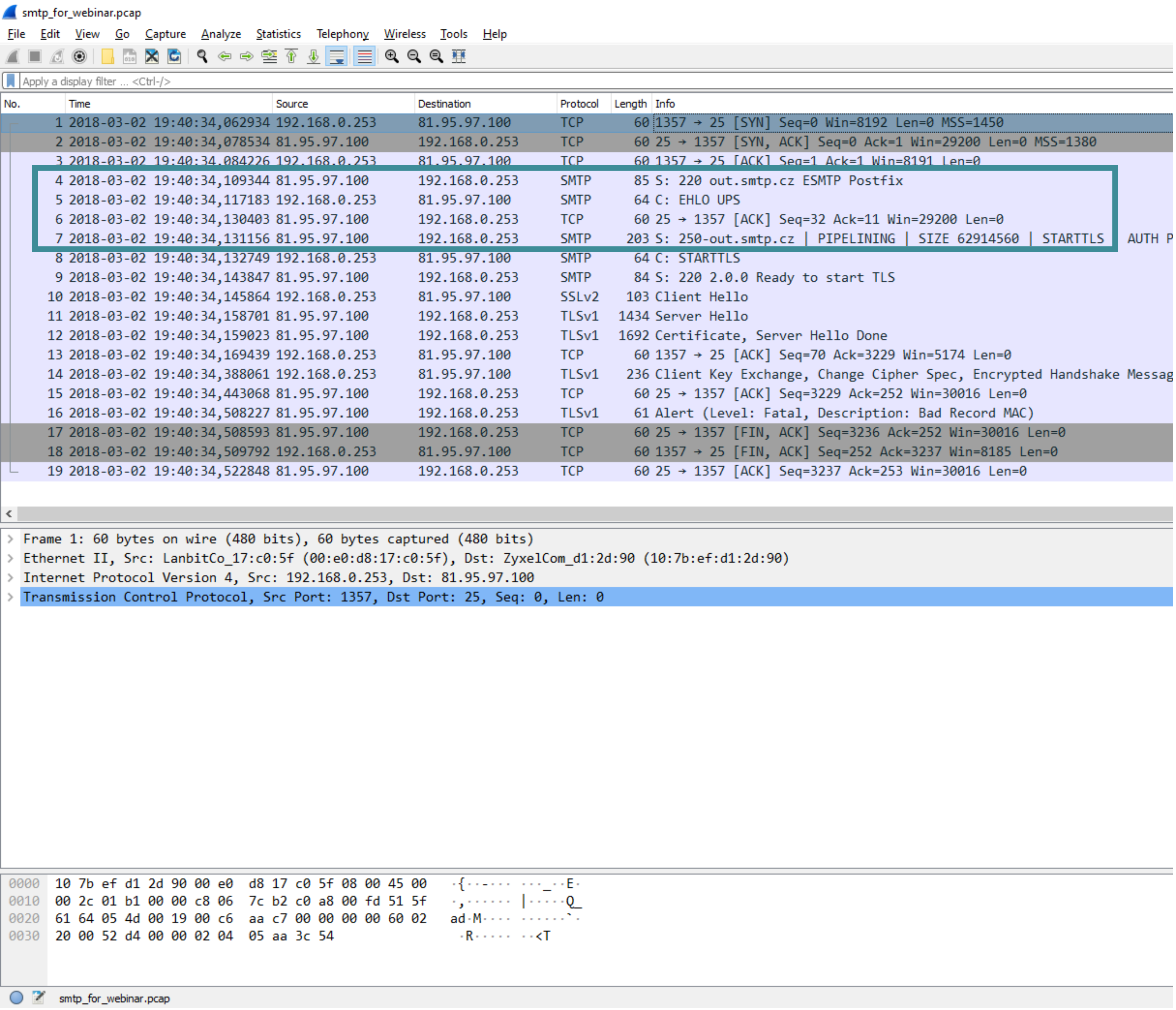

smtp_for_webinar.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time                       Source          Destination     Protocol Length Info
    1 2018-03-02 19:40:34,062934 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
    2 2018-03-02 19:40:34,078534 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
    3 2018-03-02 19:40:34,084226 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
    4 2018-03-02 19:40:34,109344 81.95.97.100    192.168.0.253   SMTP       85 S: 220 out.smtp.cz ESMTP Postfix
    5 2018-03-02 19:40:34,117183 192.168.0.253   81.95.97.100    SMTP       64 C: EHLO UPS
    6 2018-03-02 19:40:34,130403 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
    7 2018-03-02 19:40:34,131156 81.95.97.100    192.168.0.253   SMTP      203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
    8 2018-03-02 19:40:34,132749 192.168.0.253   81.95.97.100    SMTP       64 C: STARTTLS
    9 2018-03-02 19:40:34,143847 81.95.97.100    192.168.0.253   SMTP       84 S: 220 2.0.0 Ready to start TLS
   10 2018-03-02 19:40:34,145864 192.168.0.253   81.95.97.100    SSLv2     103 Client Hello
   11 2018-03-02 19:40:34,158701 81.95.97.100    192.168.0.253   TLSv1    1434 Server Hello
   12 2018-03-02 19:40:34,159023 81.95.97.100    192.168.0.253   TLSv1    1692 Certificate, Server Hello Done
   13 2018-03-02 19:40:34,169439 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
   14 2018-03-02 19:40:34,388061 192.168.0.253   81.95.97.100    TLSv1     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
   15 2018-03-02 19:40:34,443068 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
   16 2018-03-02 19:40:34,508227 81.95.97.100    192.168.0.253   TLSv1      61 Alert (Level: Fatal, Description: Bad Record MAC)
   17 2018-03-02 19:40:34,508593 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
   18 2018-03-02 19:40:34,509792 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
   19 2018-03-02 19:40:34,522848 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R······  ··<T
```

TCP handshake, session established properly

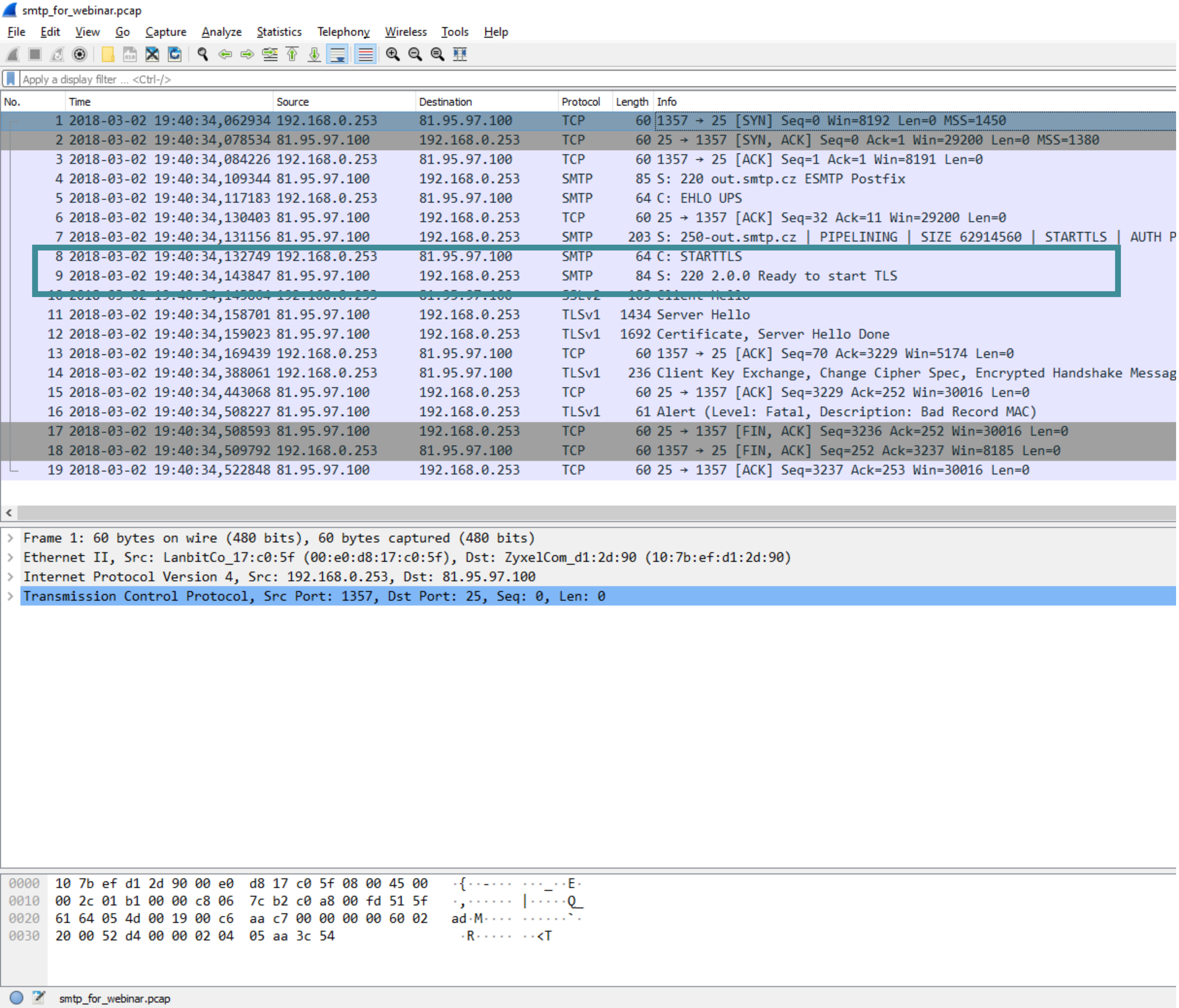

smtp_for_webinar.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No. Time                       Source         Destination    Protocol Length Info
  1 2018-03-02 19:40:34,062934 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
  2 2018-03-02 19:40:34,078534 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
  3 2018-03-02 19:40:34,084226 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
  4 2018-03-02 19:40:34,109344 81.95.97.100   192.168.0.253  SMTP       85 S: 220 out.smtp.cz ESMTP Postfix
  5 2018-03-02 19:40:34,117183 192.168.0.253  81.95.97.100   SMTP       64 C: EHLO UPS
  6 2018-03-02 19:40:34,130403 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
  7 2018-03-02 19:40:34,131156 81.95.97.100   192.168.0.253  SMTP      203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
  8 2018-03-02 19:40:34,132749 192.168.0.253  81.95.97.100   SMTP       64 C: STARTTLS
  9 2018-03-02 19:40:34,143847 81.95.97.100   192.168.0.253  SMTP       84 S: 220 2.0.0 Ready to start TLS
 10 2018-03-02 19:40:34,145864 192.168.0.253  81.95.97.100   SSLv2     103 Client Hello
 11 2018-03-02 19:40:34,158701 81.95.97.100   192.168.0.253  TLSv1    1434 Server Hello
 12 2018-03-02 19:40:34,159023 81.95.97.100   192.168.0.253  TLSv1    1692 Certificate, Server Hello Done
 13 2018-03-02 19:40:34,169439 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
 14 2018-03-02 19:40:34,388061 192.168.0.253  81.95.97.100   TLSv1     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
 15 2018-03-02 19:40:34,443068 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
 16 2018-03-02 19:40:34,508227 81.95.97.100   192.168.0.253  TLSv1      61 Alert (Level: Fatal, Description: Bad Record MAC)
 17 2018-03-02 19:40:34,508593 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
 18 2018-03-02 19:40:34,509792 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
 19 2018-03-02 19:40:34,522848 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R·····  ··<T
```

SMTP Hello, server capabilities provided to the client device



smtp_for_webinar.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

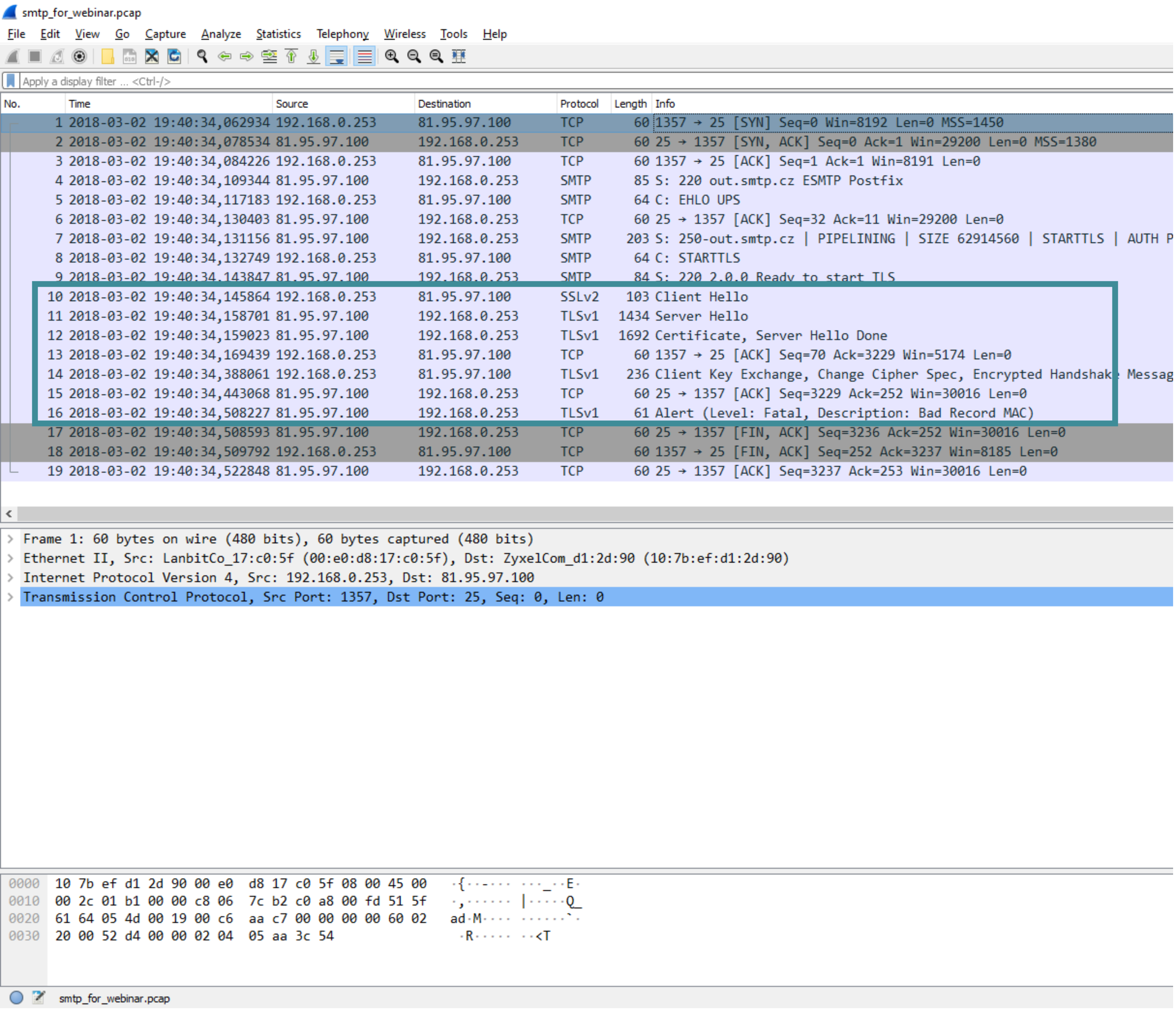
```
No.  Time                         Source          Destination     Protocol  Length Info
   1 2018-03-02 19:40:34,062934 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
   2 2018-03-02 19:40:34,078534 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
   3 2018-03-02 19:40:34,084226 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
   4 2018-03-02 19:40:34,109344 81.95.97.100    192.168.0.253   SMTP         85 S: 220 out.smtp.cz ESMTP Postfix
   5 2018-03-02 19:40:34,117183 192.168.0.253   81.95.97.100    SMTP         64 C: EHLO UPS
   6 2018-03-02 19:40:34,130403 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
   7 2018-03-02 19:40:34,131156 81.95.97.100    192.168.0.253   SMTP        203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
   8 2018-03-02 19:40:34,132749 192.168.0.253   81.95.97.100    SMTP         64 C: STARTTLS
   9 2018-03-02 19:40:34,143847 81.95.97.100    192.168.0.253   SMTP         84 S: 220 2.0.0 Ready to start TLS
  10 2018-03-02 19:40:34,145864 192.168.0.253   81.95.97.100    SSLv2       103 Client Hello
  11 2018-03-02 19:40:34,158701 81.95.97.100    192.168.0.253   TLSv1      1434 Server Hello
  12 2018-03-02 19:40:34,159023 81.95.97.100    192.168.0.253   TLSv1      1692 Certificate, Server Hello Done
  13 2018-03-02 19:40:34,169439 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
  14 2018-03-02 19:40:34,388061 192.168.0.253   81.95.97.100    TLSv1       236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
  15 2018-03-02 19:40:34,443068 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
  16 2018-03-02 19:40:34,508227 81.95.97.100    192.168.0.253   TLSv1        61 Alert (Level: Fatal, Description: Bad Record MAC)
  17 2018-03-02 19:40:34,508593 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
  18 2018-03-02 19:40:34,509792 192.168.0.253   81.95.97.100    TCP          60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
  19 2018-03-02 19:40:34,522848 81.95.97.100    192.168.0.253   TCP          60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R·····  ··<T
```

Requested to move from plain text to encrypted session

Flowmon
Driving Network Visibility



```
No.  Time                       Source         Destination    Protocol Length Info
   1 2018-03-02 19:40:34,062934 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
   2 2018-03-02 19:40:34,078534 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
   3 2018-03-02 19:40:34,084226 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
   4 2018-03-02 19:40:34,109344 81.95.97.100   192.168.0.253  SMTP       85 S: 220 out.smtp.cz ESMTP Postfix
   5 2018-03-02 19:40:34,117183 192.168.0.253  81.95.97.100   SMTP       64 C: EHLO UPS
   6 2018-03-02 19:40:34,130403 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
   7 2018-03-02 19:40:34,131156 81.95.97.100   192.168.0.253  SMTP      203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
   8 2018-03-02 19:40:34,132749 192.168.0.253  81.95.97.100   SMTP       64 C: STARTTLS
   9 2018-03-02 19:40:34,143847 81.95.97.100   192.168.0.253  SMTP       84 S: 220 2.0.0 Ready to start TLS
  10 2018-03-02 19:40:34,145864 192.168.0.253  81.95.97.100   SSLv2     103 Client Hello
  11 2018-03-02 19:40:34,158701 81.95.97.100   192.168.0.253  TLSv1    1434 Server Hello
  12 2018-03-02 19:40:34,159023 81.95.97.100   192.168.0.253  TLSv1    1692 Certificate, Server Hello Done
  13 2018-03-02 19:40:34,169439 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
  14 2018-03-02 19:40:34,388061 192.168.0.253  81.95.97.100   TLSv1     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
  15 2018-03-02 19:40:34,443068 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
  16 2018-03-02 19:40:34,508227 81.95.97.100   192.168.0.253  TLSv1      61 Alert (Level: Fatal, Description: Bad Record MAC)
  17 2018-03-02 19:40:34,508593 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
  18 2018-03-02 19:40:34,509792 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
  19 2018-03-02 19:40:34,522848 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

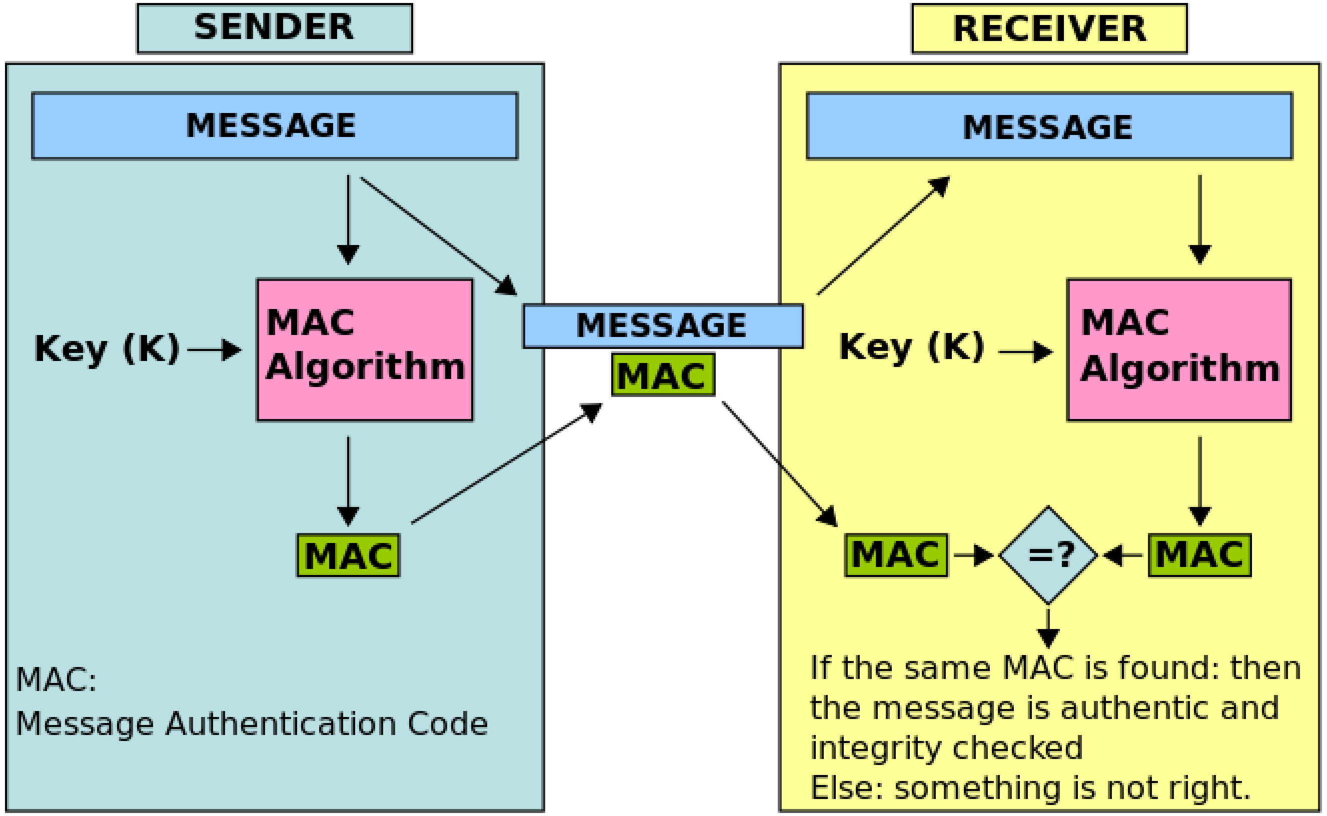
```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R······  ··<T
```

TLS handshake, error message “BAD RECORD MAC”, client is not able to negotiate encryption with server

Flowmon
Driving Network Visibility

BAD RECORD MAC

- Message Authentication Code



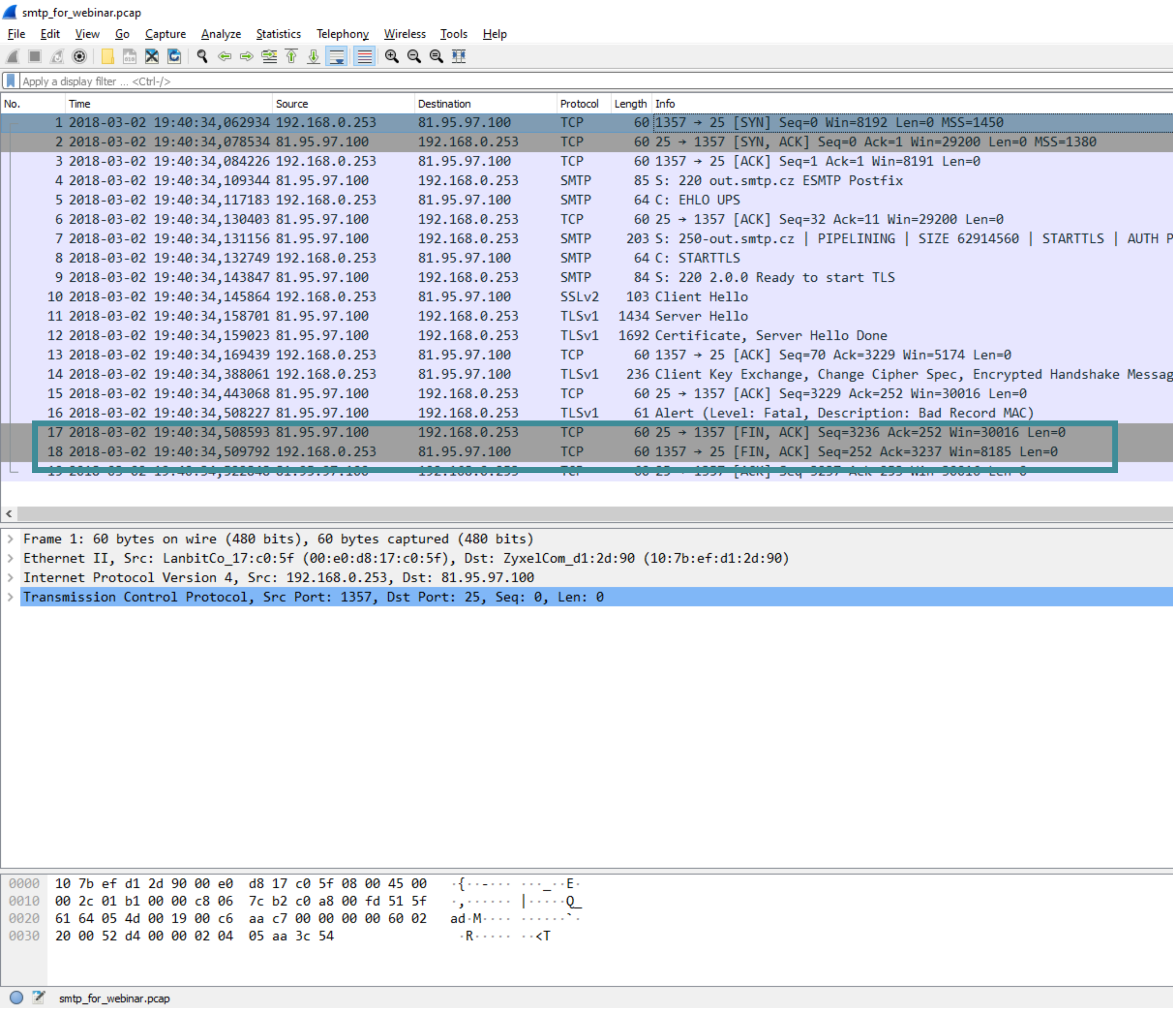
MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

source: Wikipedia

Conclusion

- Client is not able to negotiate secured (encrypted) session with the SMTP server, not a network problem
- There is an incompatibility in encryption (SSL/TLS version, cypher suites, etc.)
- Usually one of the communication partners is outdated or not configured properly (e.g. client speaks TLS 1.0 or 1.1 where server is configured to accept only TLS 1.2 or 1.3)


smtp_for_webinar.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

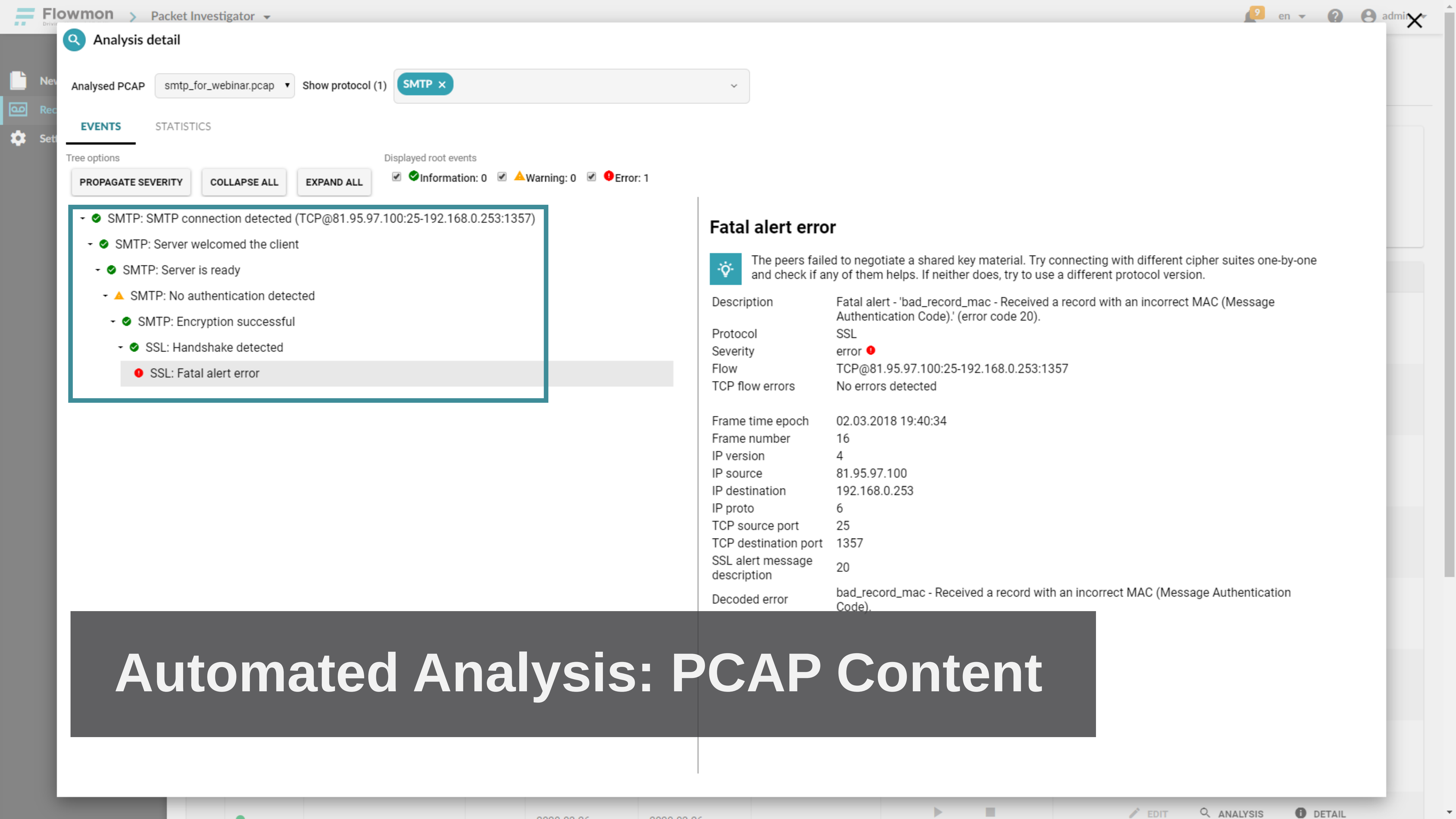
```
No.  Time                       Source          Destination     Protocol Length Info
   1 2018-03-02 19:40:34,062934 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
   2 2018-03-02 19:40:34,078534 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
   3 2018-03-02 19:40:34,084226 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
   4 2018-03-02 19:40:34,109344 81.95.97.100    192.168.0.253   SMTP       85 S: 220 out.smtp.cz ESMTP Postfix
   5 2018-03-02 19:40:34,117183 192.168.0.253   81.95.97.100    SMTP       64 C: EHLO UPS
   6 2018-03-02 19:40:34,130403 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
   7 2018-03-02 19:40:34,131156 81.95.97.100    192.168.0.253   SMTP      203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
   8 2018-03-02 19:40:34,132749 192.168.0.253   81.95.97.100    SMTP       64 C: STARTTLS
   9 2018-03-02 19:40:34,143847 81.95.97.100    192.168.0.253   SMTP       84 S: 220 2.0.0 Ready to start TLS
  10 2018-03-02 19:40:34,145864 192.168.0.253   81.95.97.100    SSLv2     103 Client Hello
  11 2018-03-02 19:40:34,158701 81.95.97.100    192.168.0.253   TLSv1    1434 Server Hello
  12 2018-03-02 19:40:34,159023 81.95.97.100    192.168.0.253   TLSv1    1692 Certificate, Server Hello Done
  13 2018-03-02 19:40:34,169439 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
  14 2018-03-02 19:40:34,388061 192.168.0.253   81.95.97.100    TLSv1     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
  15 2018-03-02 19:40:34,443068 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
  16 2018-03-02 19:40:34,508227 81.95.97.100    192.168.0.253   TLSv1      61 Alert (Level: Fatal, Description: Bad Record MAC)
  17 2018-03-02 19:40:34,508593 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
  18 2018-03-02 19:40:34,509792 192.168.0.253   81.95.97.100    TCP        60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
  19 2018-03-02 19:40:34,522848 81.95.97.100    192.168.0.253   TCP        60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LanbitCo_17:c0:5f (00:e0:d8:17:c0:5f), Dst: ZyxelCom_d1:2d:90 (10:7b:ef:d1:2d:90)
> Internet Protocol Version 4, Src: 192.168.0.253, Dst: 81.95.97.100
> Transmission Control Protocol, Src Port: 1357, Dst Port: 25, Seq: 0, Len: 0
```

```
0000  10 7b ef d1 2d 90 00 e0  d8 17 c0 5f 08 00 45 00   ·{··-···  ···_··E·
0010  00 2c 01 b1 00 00 c8 06  7c b2 c0 a8 00 fd 51 5f   ·,······  |·····Q_
0020  61 64 05 4d 00 19 00 c6  aa c7 00 00 00 00 60 02   ad·M····  ······`·
0030  20 00 52 d4 00 00 02 04  05 aa 3c 54                ·R······  ··<T
```

TCP session terminated between client and server

Flowmon
Driving Network Visibility



Analysis detail

Analysed PCAP: smtp_for_webinar.pcap
Show protocol (1): SMTP ×

EVENTS | STATISTICS

Tree options: PROPAGATE SEVERITY | COLLAPSE ALL | EXPAND ALL

Displayed root events: ☑ ✓Information: 0 ☑ ⚠Warning: 0 ☑ ●Error: 1

- ✓ SMTP: SMTP connection detected (TCP@81.95.97.100:25-192.168.0.253:1357)
  - ✓ SMTP: Server welcomed the client
    - ✓ SMTP: Server is ready
      - ⚠ SMTP: No authentication detected
        - ✓ SMTP: Encryption successful
          - ✓ SSL: Handshake detected
            - ● SSL: Fatal alert error

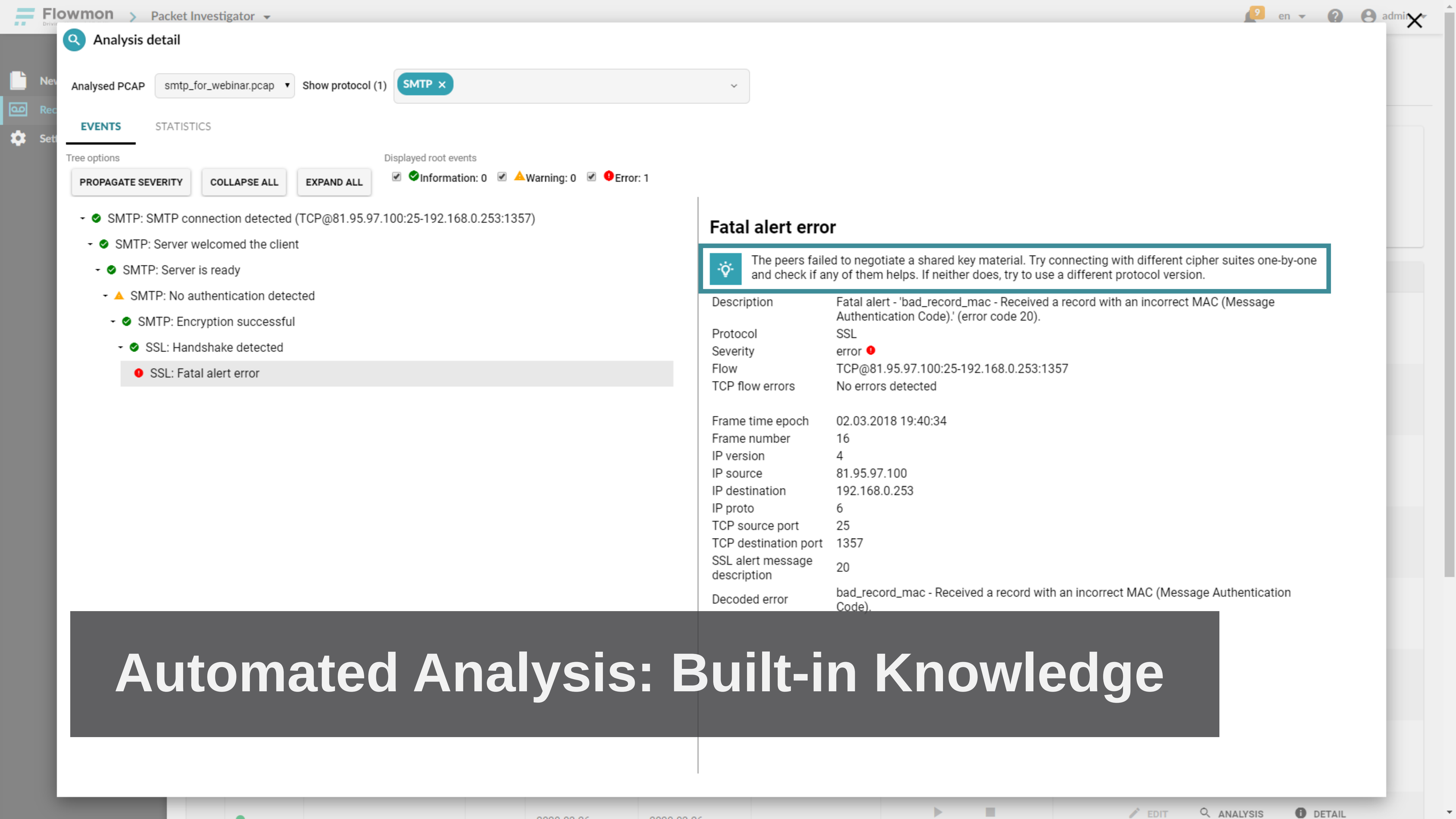
Fatal alert error

The peers failed to negotiate a shared key material. Try connecting with different cipher suites one-by-one and check if any of them helps. If neither does, try to use a different protocol version.

Description	Fatal alert - 'bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).' (error code 20).
Protocol	SSL
Severity	error ●
Flow	TCP@81.95.97.100:25-192.168.0.253:1357
TCP flow errors	No errors detected
Frame time epoch	02.03.2018 19:40:34
Frame number	16
IP version	4
IP source	81.95.97.100
IP destination	192.168.0.253
IP proto	6
TCP source port	25
TCP destination port	1357
SSL alert message description	20
Decoded error	bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).

Automated Analysis: PCAP Content

Automated Analysis: Built-in Knowledge



Analysis detail

Analysed PCAP smtp_for_webinar.pcap ▾ Show protocol (1) SMTP ×

EVENTS STATISTICS

Tree options

PROPAGATE SEVERITY | COLLAPSE ALL | EXPAND ALL

Displayed root events

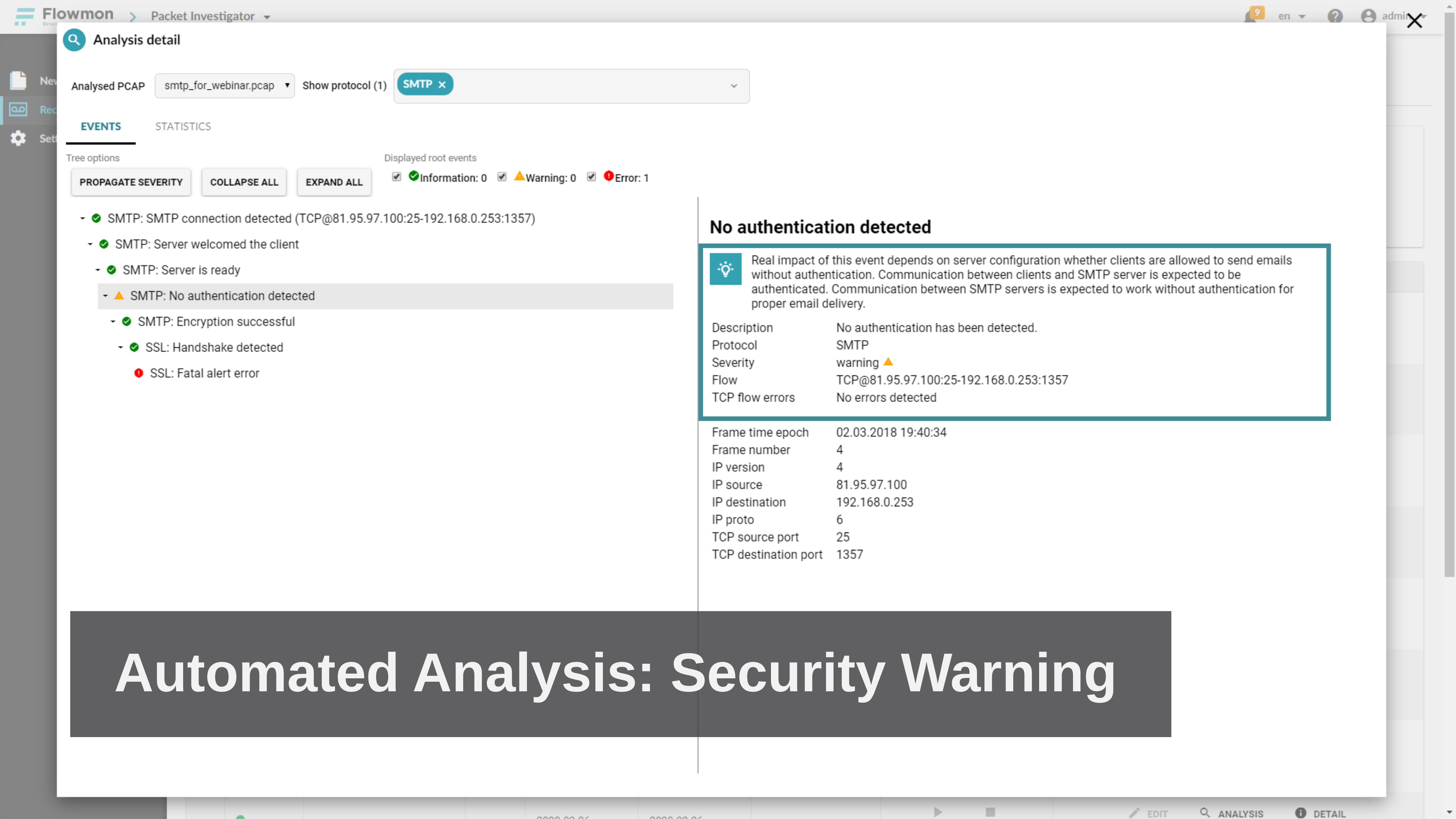
☑ ✓Information: 0 ☑ ⚠Warning: 0 ☑ ●Error: 1

- ✓ SMTP: SMTP connection detected (TCP@81.95.97.100:25-192.168.0.253:1357)
  - ✓ SMTP: Server welcomed the client
    - ✓ SMTP: Server is ready
      - ⚠ SMTP: No authentication detected
        - ✓ SMTP: Encryption successful
          - ✓ SSL: Handshake detected
            - ● SSL: Fatal alert error

Fatal alert error

The peers failed to negotiate a shared key material. Try connecting with different cipher suites one-by-one and check if any of them helps. If neither does, try to use a different protocol version.

Description	Fatal alert - 'bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).' (error code 20).
Protocol	SSL
Severity	error ●
Flow	TCP@81.95.97.100:25-192.168.0.253:1357
TCP flow errors	No errors detected
Frame time epoch	02.03.2018 19:40:34
Frame number	16
IP version	4
IP source	81.95.97.100
IP destination	192.168.0.253
IP proto	6
TCP source port	25
TCP destination port	1357
SSL alert message description	20
Decoded error	bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).



Analysis detail

Analysed PCAP: smtp_for_webinar.pcap ▾   Show protocol (1): SMTP ×

EVENTS   STATISTICS

Tree options: PROPAGATE SEVERITY | COLLAPSE ALL | EXPAND ALL

Displayed root events: ☑ ✓Information: 0 ☑ ⚠Warning: 0 ☑ ●Error: 1

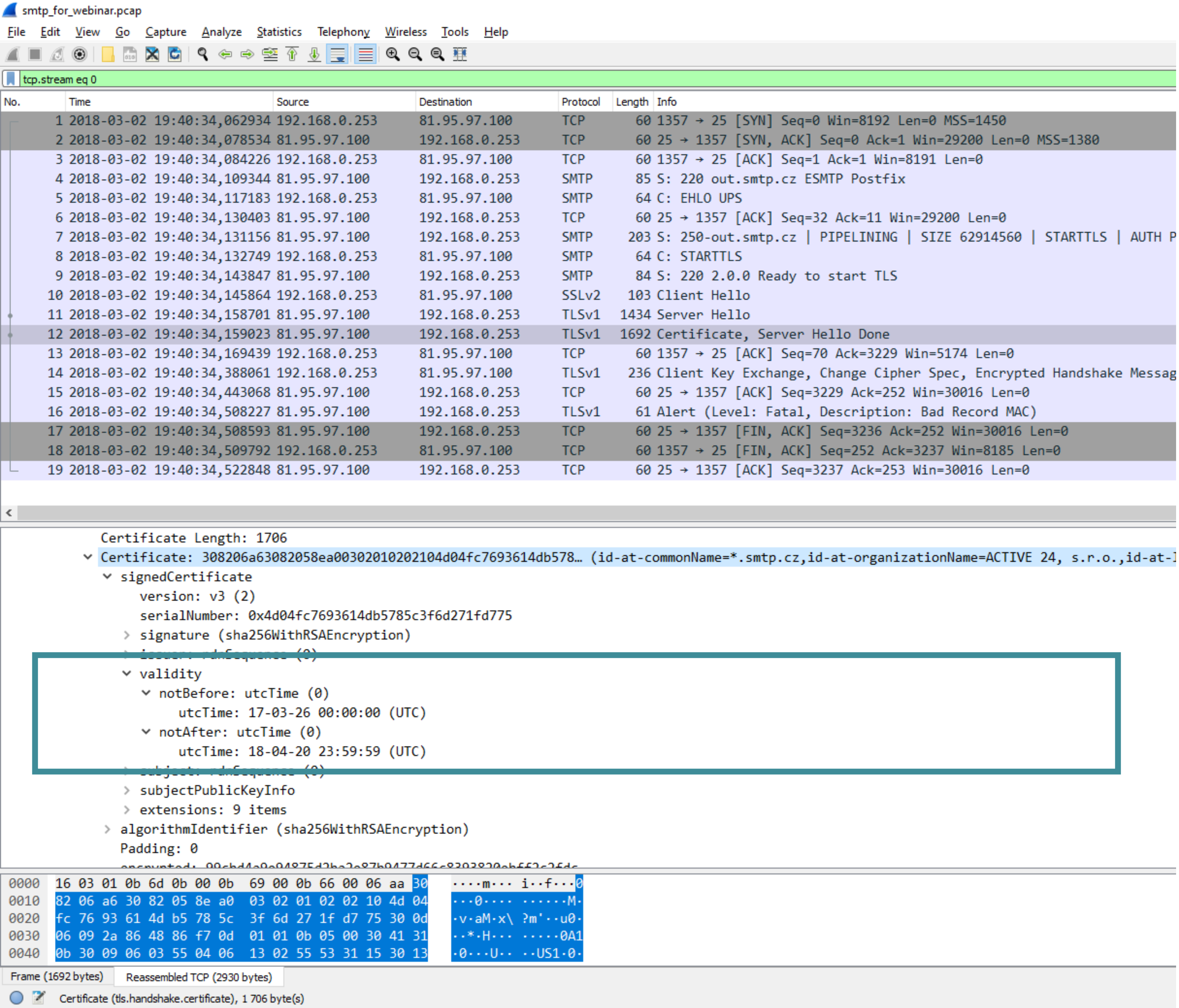
- ✓ SMTP: SMTP connection detected (TCP@81.95.97.100:25-192.168.0.253:1357)
  - ✓ SMTP: Server welcomed the client
    - ✓ SMTP: Server is ready
      - ⚠ SMTP: No authentication detected
        - ✓ SMTP: Encryption successful
          - ✓ SSL: Handshake detected
            - ● SSL: Fatal alert error

No authentication detected

Real impact of this event depends on server configuration whether clients are allowed to send emails without authentication. Communication between clients and SMTP server is expected to be authenticated. Communication between SMTP servers is expected to work without authentication for proper email delivery.

Description	No authentication has been detected.
Protocol	SMTP
Severity	warning ⚠
Flow	TCP@81.95.97.100:25-192.168.0.253:1357
TCP flow errors	No errors detected
Frame time epoch	02.03.2018 19:40:34
Frame number	4
IP version	4
IP source	81.95.97.100
IP destination	192.168.0.253
IP proto	6
TCP source port	25
TCP destination port	1357

Automated Analysis: Security Warning



tcp.stream eq 0

```
No.  Time                       Source         Destination    Protocol Length Info
   1 2018-03-02 19:40:34,062934 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1450
   2 2018-03-02 19:40:34,078534 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380
   3 2018-03-02 19:40:34,084226 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=1 Ack=1 Win=8191 Len=0
   4 2018-03-02 19:40:34,109344 81.95.97.100   192.168.0.253  SMTP       85 S: 220 out.smtp.cz ESMTP Postfix
   5 2018-03-02 19:40:34,117183 192.168.0.253  81.95.97.100   SMTP       64 C: EHLO UPS
   6 2018-03-02 19:40:34,130403 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=32 Ack=11 Win=29200 Len=0
   7 2018-03-02 19:40:34,131156 81.95.97.100   192.168.0.253  SMTP      203 S: 250-out.smtp.cz | PIPELINING | SIZE 62914560 | STARTTLS | AUTH P
   8 2018-03-02 19:40:34,132749 192.168.0.253  81.95.97.100   SMTP       64 C: STARTTLS
   9 2018-03-02 19:40:34,143847 81.95.97.100   192.168.0.253  SMTP       84 S: 220 2.0.0 Ready to start TLS
  10 2018-03-02 19:40:34,145864 192.168.0.253  81.95.97.100   SSLv2     103 Client Hello
  11 2018-03-02 19:40:34,158701 81.95.97.100   192.168.0.253  TLSv1    1434 Server Hello
  12 2018-03-02 19:40:34,159023 81.95.97.100   192.168.0.253  TLSv1    1692 Certificate, Server Hello Done
  13 2018-03-02 19:40:34,169439 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [ACK] Seq=70 Ack=3229 Win=5174 Len=0
  14 2018-03-02 19:40:34,388061 192.168.0.253  81.95.97.100   TLSv1     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messag
  15 2018-03-02 19:40:34,443068 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3229 Ack=252 Win=30016 Len=0
  16 2018-03-02 19:40:34,508227 81.95.97.100   192.168.0.253  TLSv1      61 Alert (Level: Fatal, Description: Bad Record MAC)
  17 2018-03-02 19:40:34,508593 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [FIN, ACK] Seq=3236 Ack=252 Win=30016 Len=0
  18 2018-03-02 19:40:34,509792 192.168.0.253  81.95.97.100   TCP        60 1357 → 25 [FIN, ACK] Seq=252 Ack=3237 Win=8185 Len=0
  19 2018-03-02 19:40:34,522848 81.95.97.100   192.168.0.253  TCP        60 25 → 1357 [ACK] Seq=3237 Ack=253 Win=30016 Len=0
```

```
        Certificate Length: 1706
      ⌄ Certificate: 308206a63082058ea00302010202104d04fc7693614db578… (id-at-commonName=*.smtp.cz,id-at-organizationName=ACTIVE 24, s.r.o.,id-at-I
        ⌄ signedCertificate
            version: v3 (2)
            serialNumber: 0x4d04fc7693614db5785c3f6d271fd775
          › signature (sha256WithRSAEncryption)
          › issuer: rdnSequence (0)
          ⌄ validity
            ⌄ notBefore: utcTime (0)
                utcTime: 17-03-26 00:00:00 (UTC)
            ⌄ notAfter: utcTime (0)
                utcTime: 18-04-20 23:59:59 (UTC)
          › subject: rdnSequence (0)
          › subjectPublicKeyInfo
          › extensions: 9 items
        › algorithmIdentifier (sha256WithRSAEncryption)
          Padding: 0
          encrypted: 00cbd4a9e04875d2ba2e87b0477d66c8393820ebff2c2fdc
```

```
0000  16 03 01 0b 6d 0b 00 0b  69 00 0b 66 00 06 aa 30   ····m··· i··f···0
0010  82 06 a6 30 82 05 8e a0  03 02 01 02 02 10 4d 04   ···0···· ······M·
0020  fc 76 93 61 4d b5 78 5c  3f 6d 27 1f d7 75 30 0d   ·v·aM·x\ ?m'··u0·
0030  06 09 2a 86 48 86 f7 0d  01 01 0b 05 00 30 41 31   ··*·H··· ·····0A1
0040  0b 30 09 06 03 55 04 06  13 02 55 53 31 15 30 13   ·0···U·· ··US1·0·
```

Certificate (tls.handshake.certificate), 1 706 byte(s)

Hidden trap: certificate is not valid any more but was valid in moment of traffic capture

Flowmon
Driving Network Visibility

Knowledge for the Task

- TCP/IP protocol stack
- SMTP
- SSL/TLS
- Wireshark

Thank you

Performance monitoring, visibility and security
with a single solution

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility