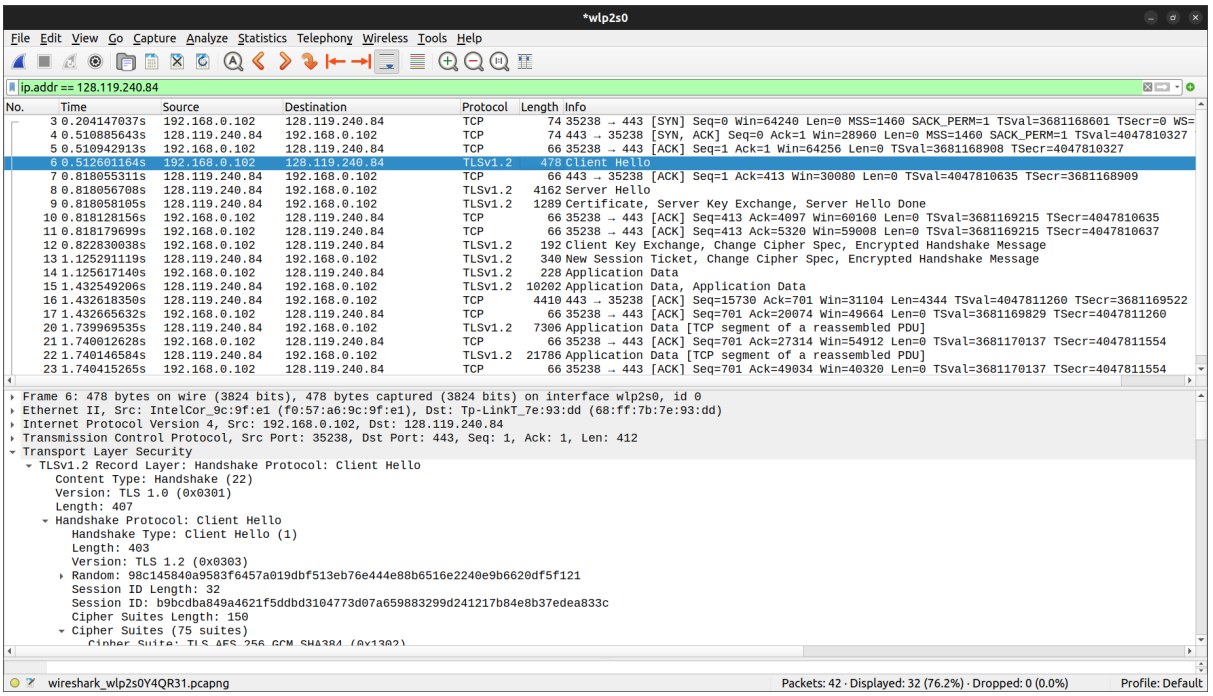
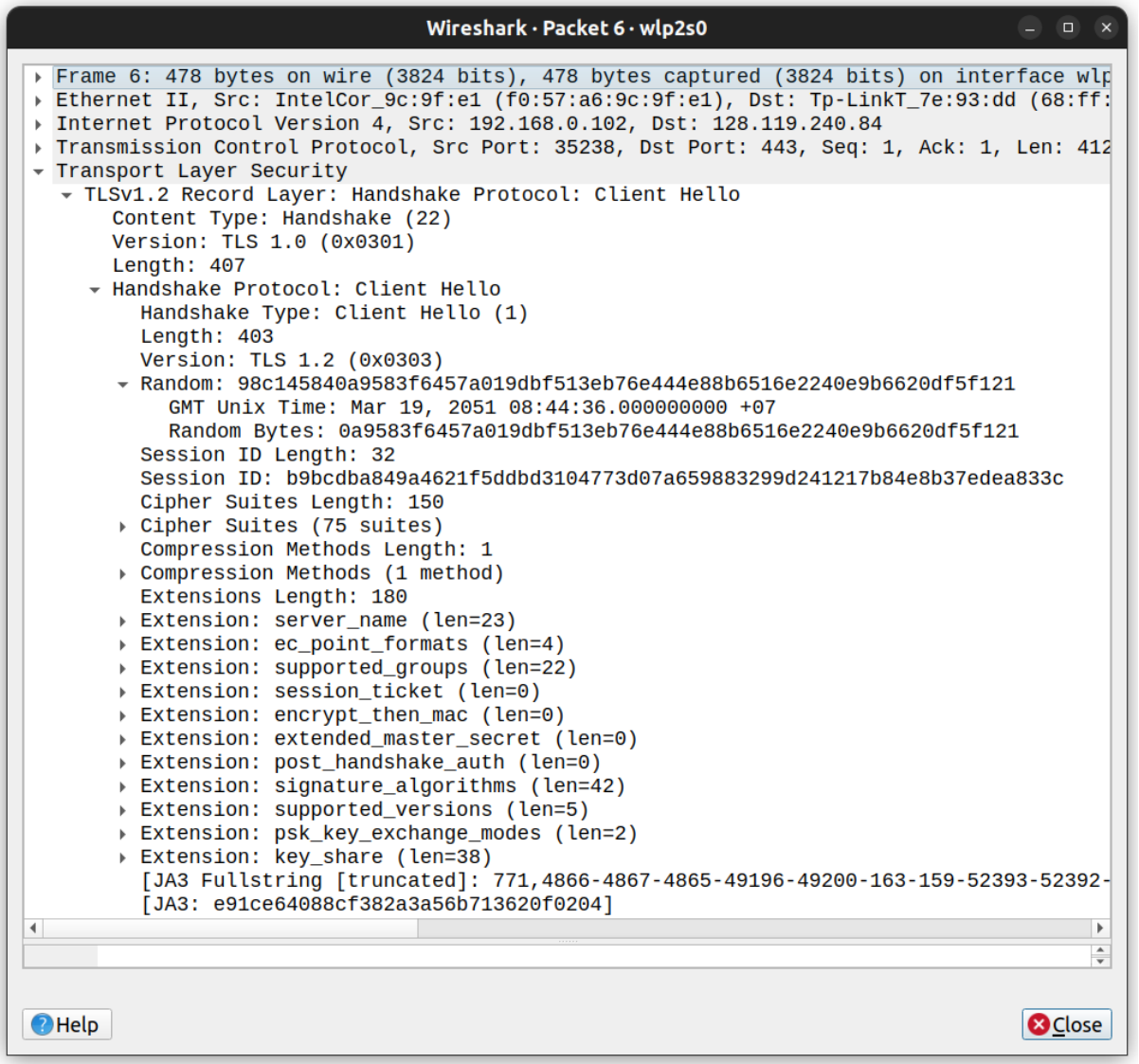
Первый взгляд на захваченные пакеты в сеансе TLS



1. Какой номер пакета в вашей трассировке, который содержит начальное сообщение TCP SYN?
    - Пакет 3 содержит TCP-сегмент SYN

2. Установлено ли соединение TCP до или после отправки первого сообщения TLS от клиента к серверу?
    - Соединение TCP установлено до отправки первого сообщение TLS

Рукопожатие TLS: Client Hello сообщение



3. Какой номер пакета в вашей трассировке, который содержит TLS сообщение Client Hello?
   - Номер пакета 6

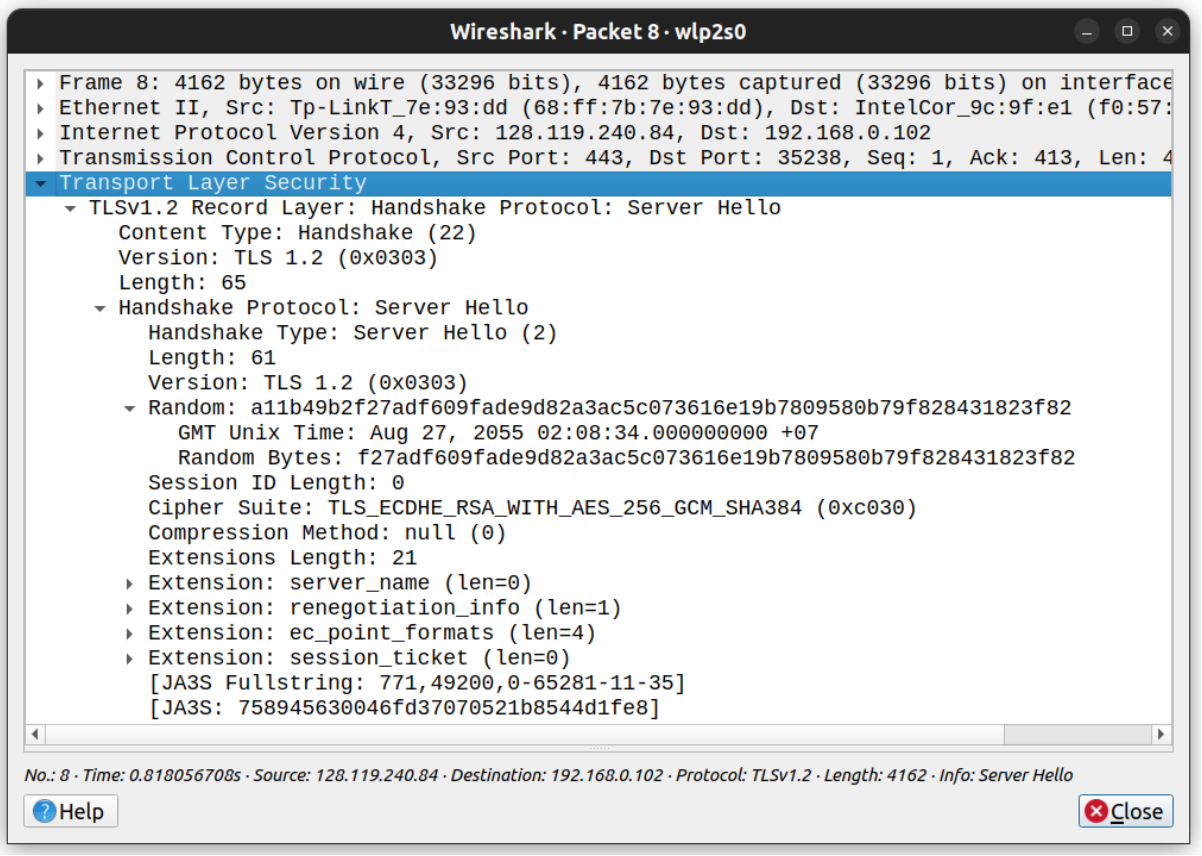
4. Какая версия TLS работает на вашем клиенте?
   - Version - TLS 1.2

5. Сколько комплектов шифров поддерживает ваш клиент?
   - Cipher Suite Length - 150 байтов, т.е. 75 комплектов шифров

6. Каковы первые две шестнадцатеричные цифры в поле *Random Bytes*?
   - Первые две шестнадцатеричные цифры - 0x0a

7. Каково назначение поля «случайные байты»?
   - Поле *Random Bytes* используется для генерации случайного начального вектора и ключей шифрования и аутентификации.

Рукопожатие TLS: Server Hello сообщение

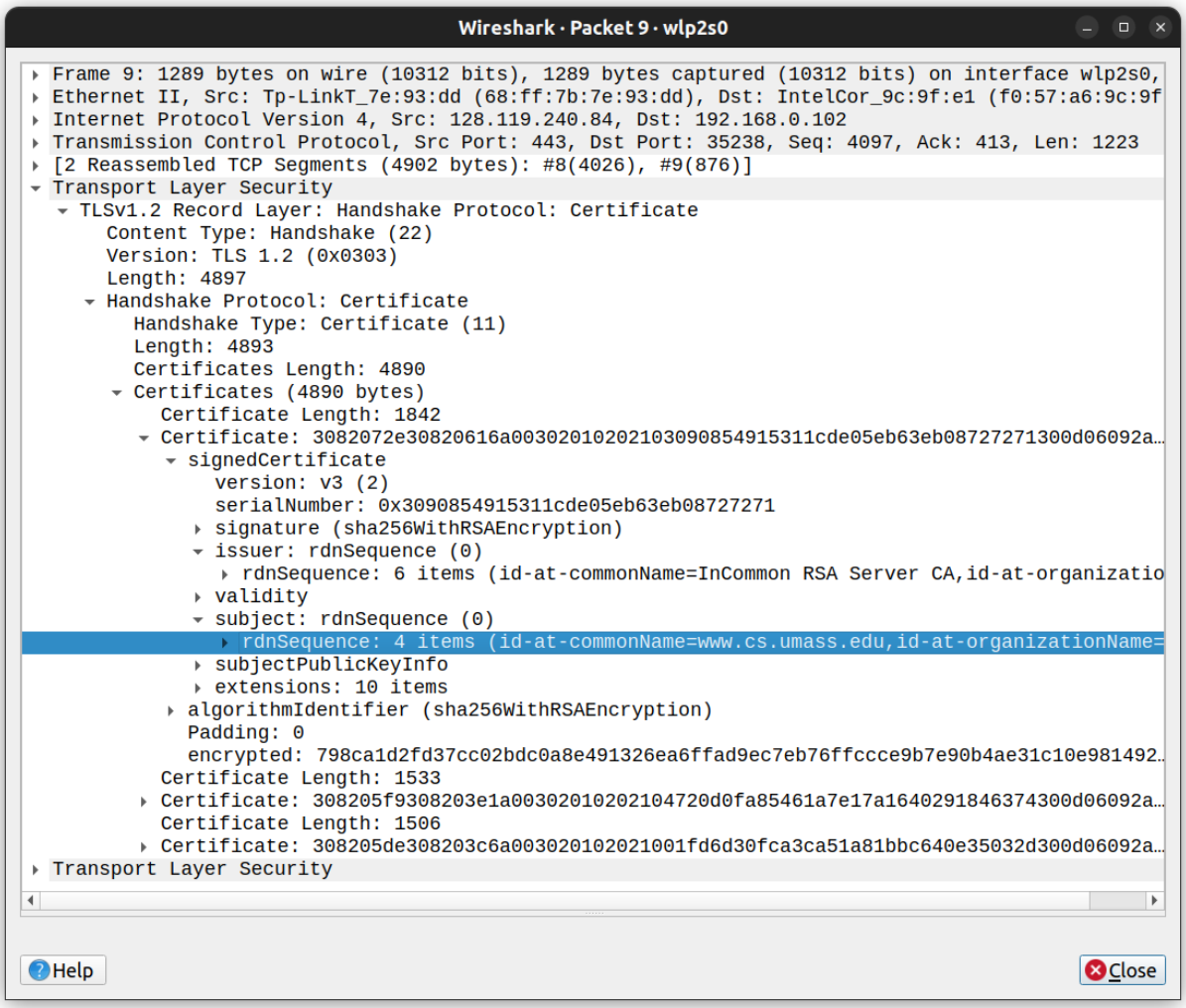


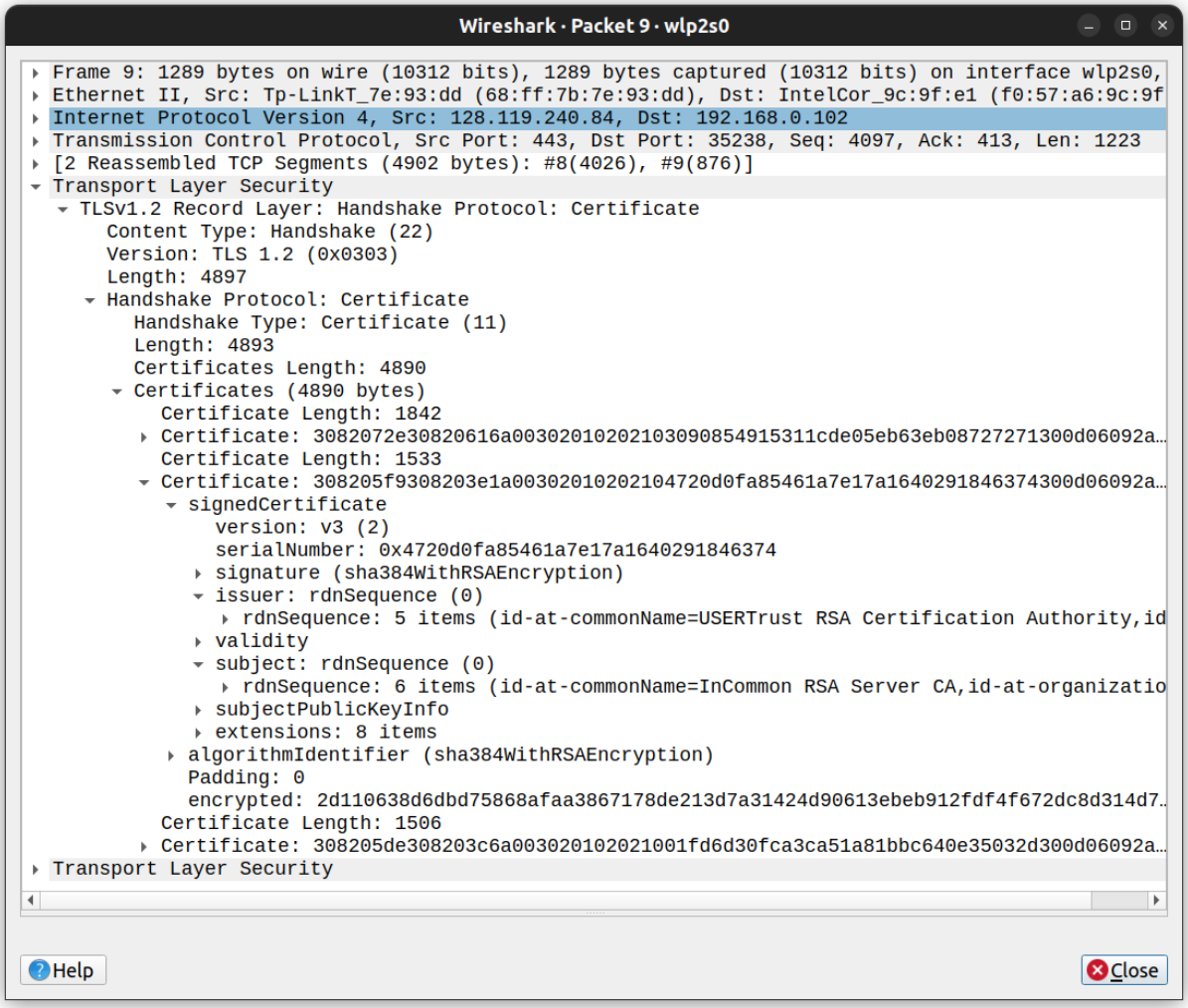
8. Какой номер пакета в вашей трассировке, который содержит TLS сообщение Server Hello?
   - Номер пакета 8

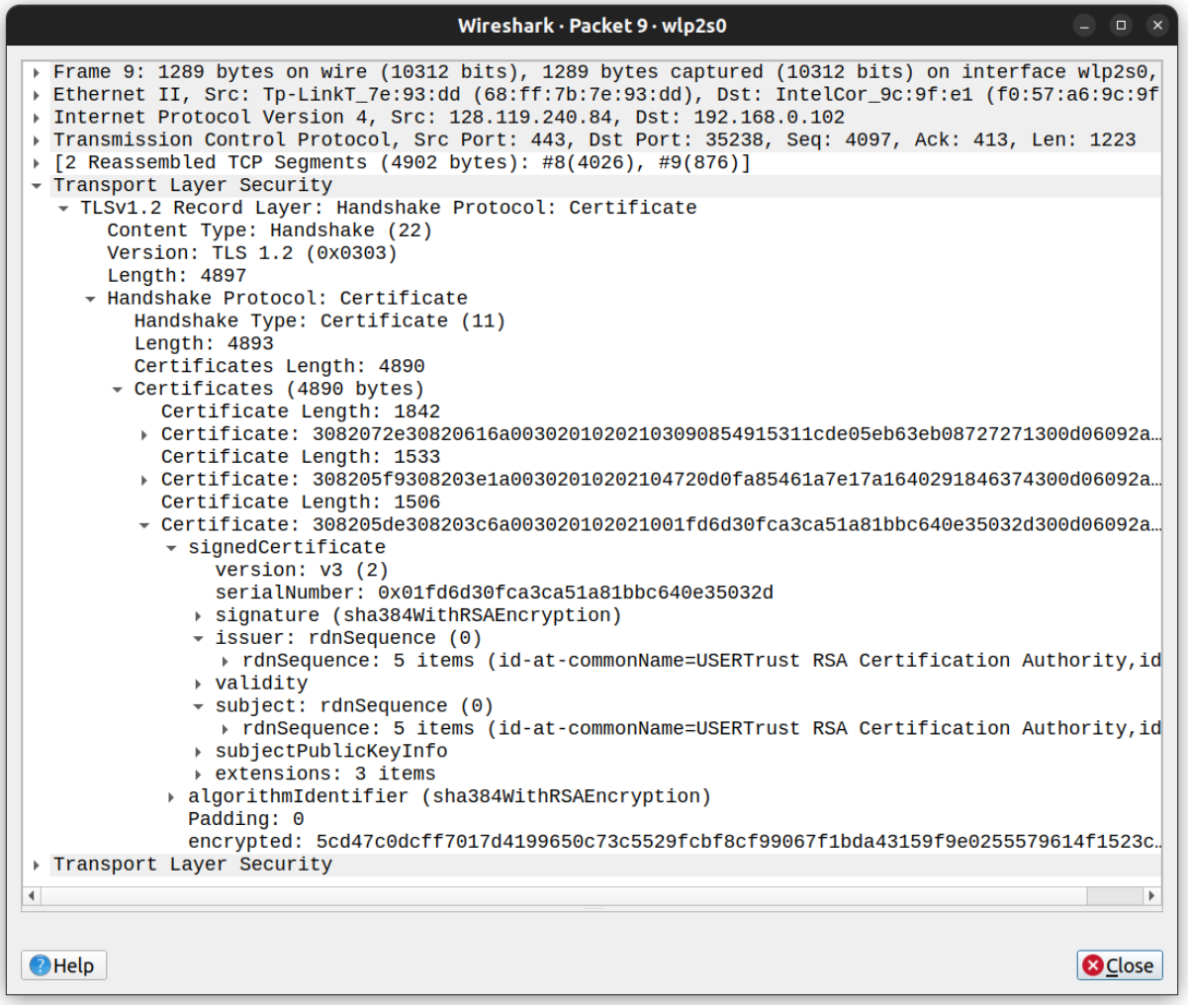
9. Какой набор шифров был выбран сервером из предложенных ранее в Client Hello сообщении?
   - Cipher Suite - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

10. Есть ли в Server Hello сообщении поле *Random Bytes*? И если да, то какова их цель?
   - Есть поле *Random Bytes*
   - Поле *Random Bytes* используется для генерации случайного начального вектора и ключей шифрования и аутентификации

Давайте углубимся в сертификат открытого ключа.


Wireshark · Packet 9 · wlp2s0
Frame 9: 1289 bytes on wire (10312 bits), 1289 bytes captured (10312 bits) on interface wlp2s0,
Ethernet II, Src: Tp-LinkT_7e:93:dd (68:ff:7b:7e:93:dd), Dst: IntelCor_9c:9f:e1 (f0:57:a6:9c:9f
Internet Protocol Version 4, Src: 128.119.240.84, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 443, Dst Port: 35238, Seq: 4097, Ack: 413, Len: 1223
[2 Reassembled TCP Segments (4902 bytes): #8(4026), #9(876)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4897
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4893
Certificates Length: 4890
Certificates (4890 bytes)
Certificate Length: 1842
Certificate: 3082072e30820616a003020102021030908549153 11cde05eb63eb08727271300d06092a…
signedCertificate
version: v3 (2)
serialNumber: 0x3090854915311cde05eb63eb08727271
signature (sha256WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 6 items (id-at-commonName=InCommon RSA Server CA,id-at-organizatio
validity
subject: rdnSequence (0)
rdnSequence: 4 items (id-at-commonName=www.cs.umass.edu,id-at-organizationName=
subjectPublicKeyInfo
extensions: 10 items
algorithmIdentifier (sha256WithRSAEncryption)
Padding: 0
encrypted: 798ca1d2fd37cc02bdc0a8e491326ea6ffad9ec7eb76ffccce9b7e90b4ae31c10e981492…
Certificate Length: 1533
Certificate: 308205f9308203e1a00302010202104720d0fa85461a7e17a1640291846374300d06092a…
Certificate Length: 1506
Certificate: 308205de308203c6a003020102021001fd6d30fca3ca51a81bbc640e35032d300d06092a…
Transport Layer Security
Help
Close


Wireshark · Packet 9 · wlp2s0
Frame 9: 1289 bytes on wire (10312 bits), 1289 bytes captured (10312 bits) on interface wlp2s0,
Ethernet II, Src: Tp-LinkT_7e:93:dd (68:ff:7b:7e:93:dd), Dst: IntelCor_9c:9f:e1 (f0:57:a6:9c:9f
Internet Protocol Version 4, Src: 128.119.240.84, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 443, Dst Port: 35238, Seq: 4097, Ack: 413, Len: 1223
[2 Reassembled TCP Segments (4902 bytes): #8(4026), #9(876)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4897
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4893
Certificates Length: 4890
Certificates (4890 bytes)
Certificate Length: 1842
Certificate: 3082072e30820616a003020102021030908549153 11cde05eb63eb08727271300d06092a…
Certificate Length: 1533
Certificate: 308205f9308203e1a00302010202104720d0fa85461a7e17a1640291846374300d06092a…
signedCertificate
version: v3 (2)
serialNumber: 0x4720d0fa85461a7e17a1640291846374
signature (sha384WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 5 items (id-at-commonName=USERTrust RSA Certification Authority,id
validity
subject: rdnSequence (0)
rdnSequence: 6 items (id-at-commonName=InCommon RSA Server CA,id-at-organizatio
subjectPublicKeyInfo
extensions: 8 items
algorithmIdentifier (sha384WithRSAEncryption)
Padding: 0
encrypted: 2d110638d6dbd75868afaa3867178de213d7a31424d90613ebeb912fdf4f672dc8d314d7…
Certificate Length: 1506
Certificate: 308205de308203c6a003020102021001fd6d30fca3ca51a81bbc640e35032d300d06092a…
Transport Layer Security
Help
Close



11. Каков номер пакета в вашей трассировке для части сообщения TLS, которая содержит сертификат открытого ключа для www.cics.umass.edu сервер?

- Номер пакеты 9

12. Сервер может возвращать более одного сертификата. Если возвращается более одного сертификата, все ли эти сертификаты предназначены для www.cs.umass.edu? Если не все, тогда для кого предназначены эти другие сертификаты?

- Вернулось 3 сертификаты
- 1 сертификат предназначен для www.cs.umass.edu
- Остальные 2 сертификата предназначены для InCommon RSA Server CA и USERTrust RSA Certification Authority

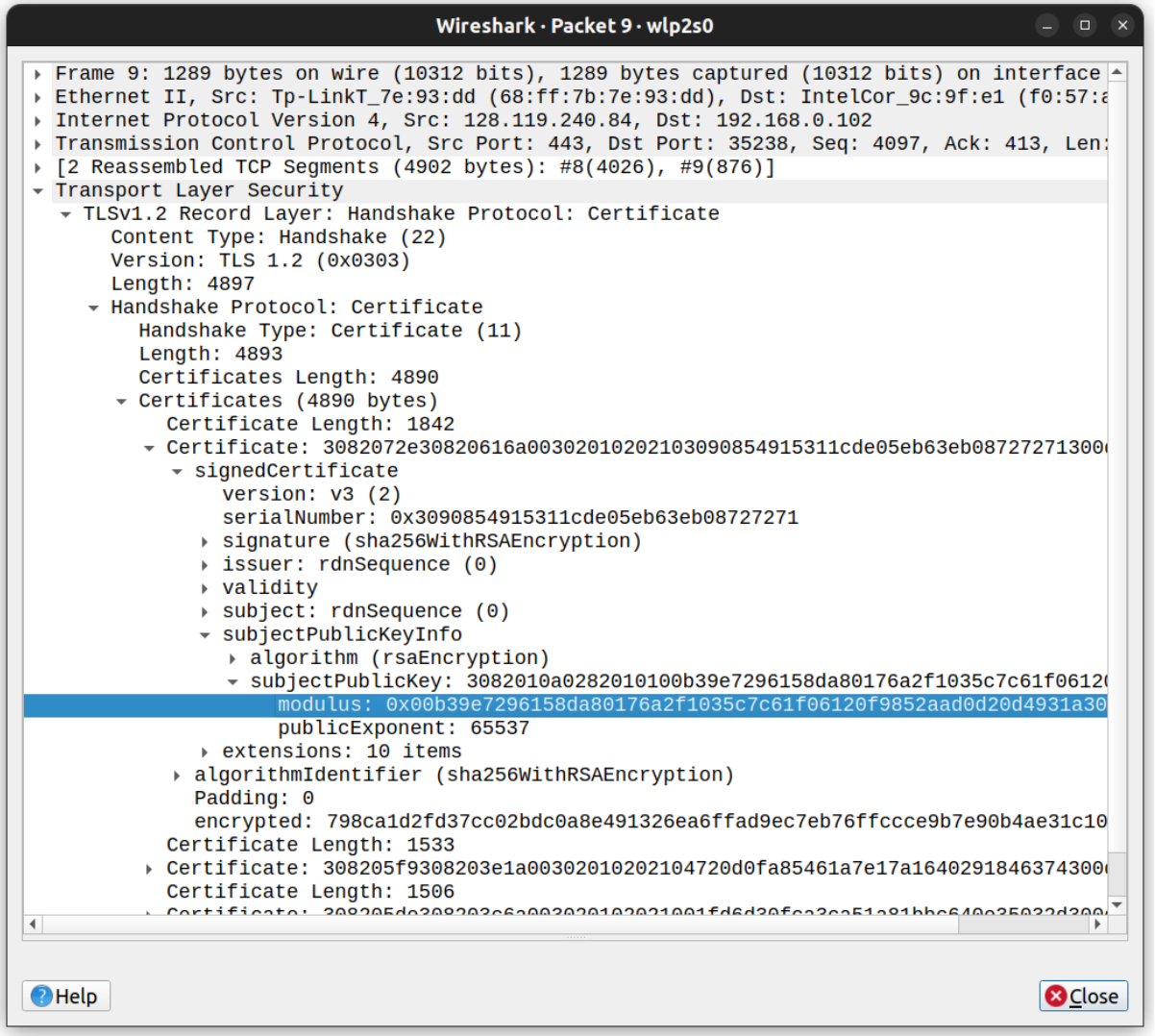
13. Как называется центр сертификации, выдавший сертификат для www.cs.umass.edu?

- Центр сертификации, выдавший сертификат для www.cs.umass.edu - InCommon RSA Server CA

14. Какой алгоритм цифровой подписи используется центром сертификации для подписания этого сертификата?

- Алгоритм цифровой подписи - sha256WithRSAEncryption

Давайте посмотрим, как выглядит настоящий открытый ключ.



15. Каковы первые четыре шестнадцатеричных цифры модуля открытого ключа, используемого www.cics.umass.edu?

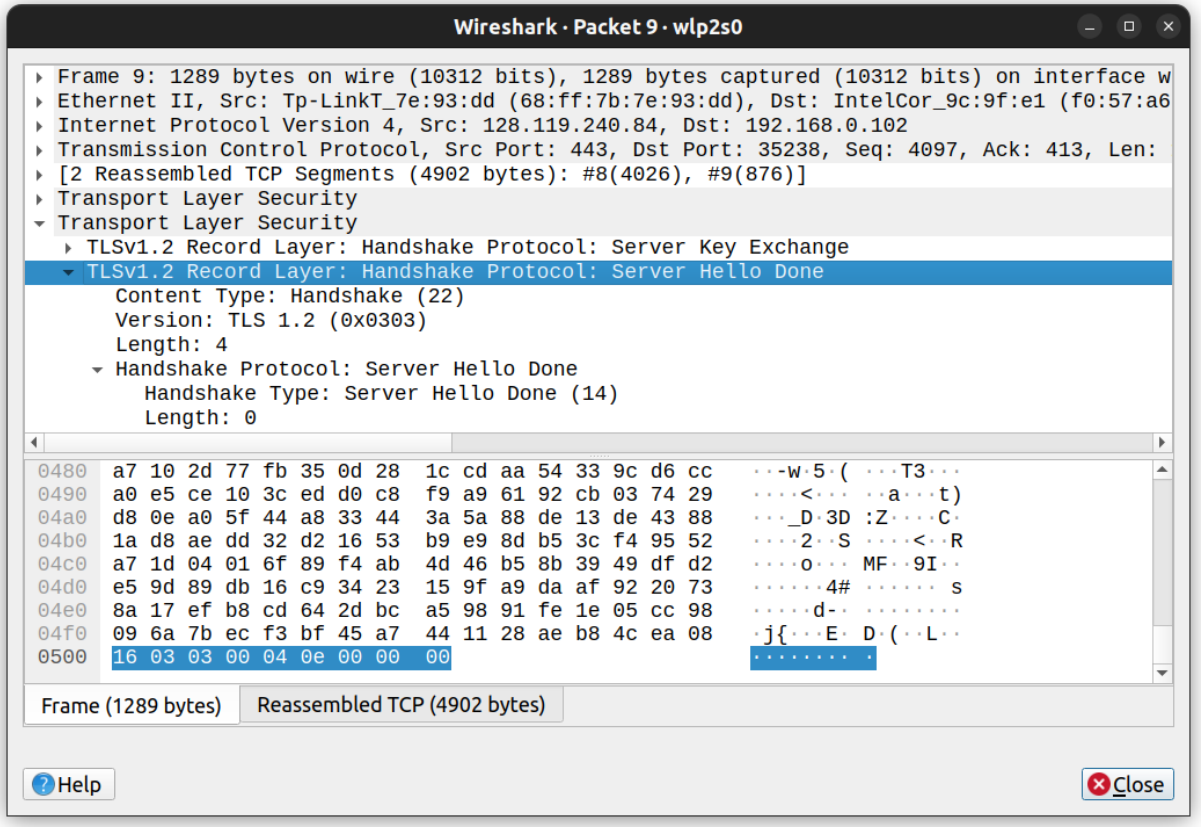
- 0x00b3

Загляните в свою трассировку. Найдите сообщения между клиентом и центром сертификации для получения информации об открытом ключе центра сертификации, чтобы клиент мог убедиться, что сертификат, подписанный центром сертификации и отправленный сервером, действительно действителен и не был подделан или изменен.

16. Вы видите такое сообщение в своей трассировке? Если да, то какой номер в трассировке первого пакета, отправленного вашим клиентом в ЦС? Если нет, объясните, почему клиент не обратился в ЦС.

- Таких сообщений нет. Если сертификат сервера был выдан доверенным центром сертификации, которым клиент уже доверяет, то запрос на проверку сертификата не отправляется

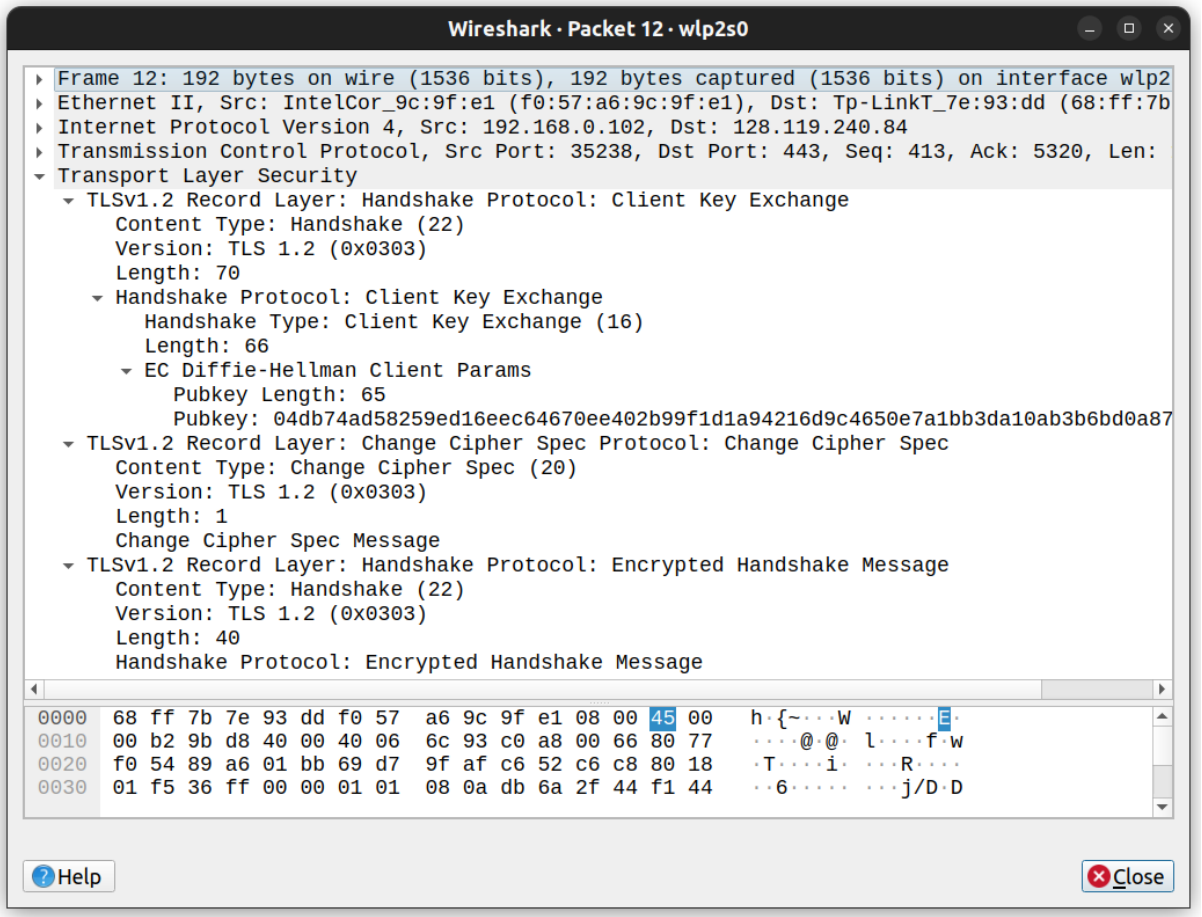
Server Hello сообщение всегда завершается явной записью Server Hello Done.



17. Каков номер пакета в вашей трассировке для части сообщения TLS, содержащей запись Server Hello Done?

- Номер пакета 9

Рукопожатие TLS: завершение рукопожатия



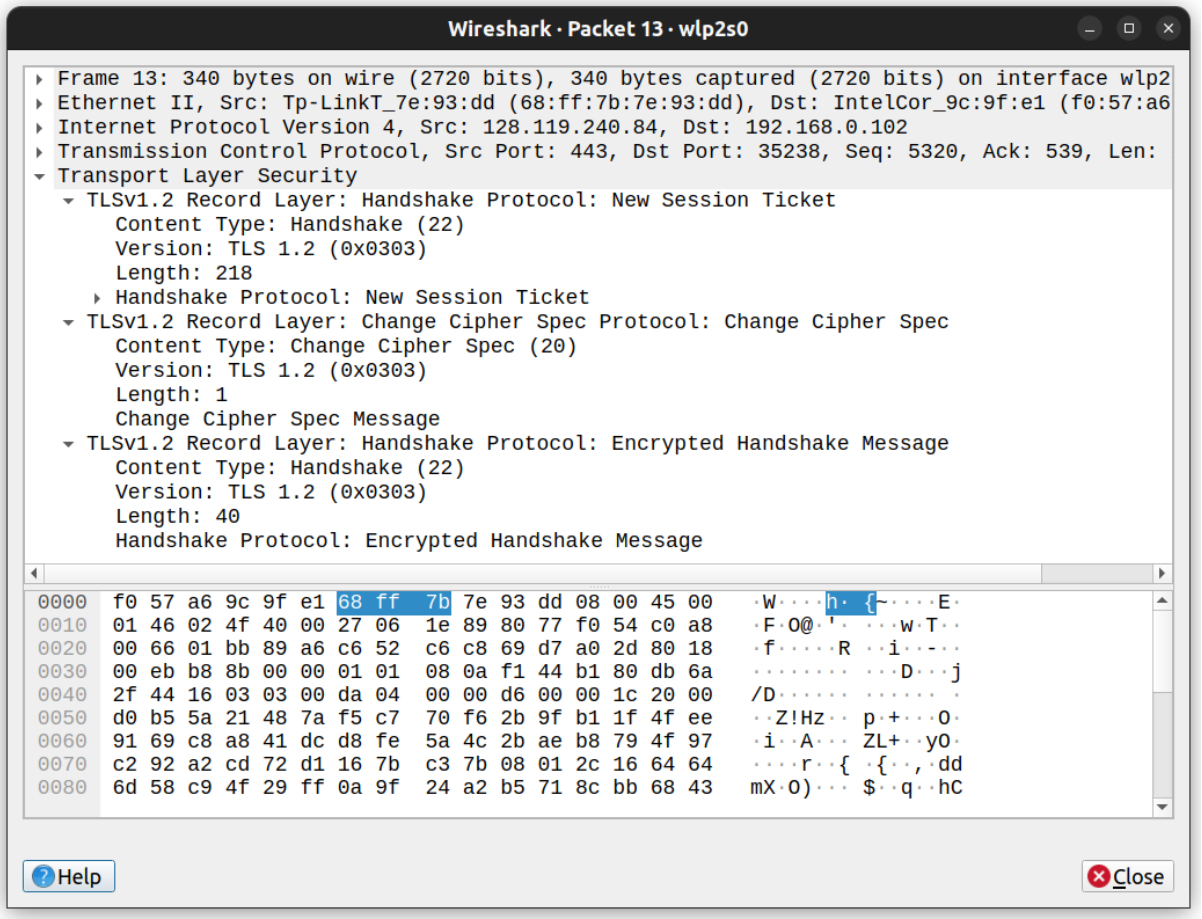
18. Каков номер пакета в вашей трассировке для сообщения TLS, содержащего информацию об открытом ключе, сообщение с записями Change Cipher Spec и Encrypted Handshake, отправляемое от клиента к серверу?

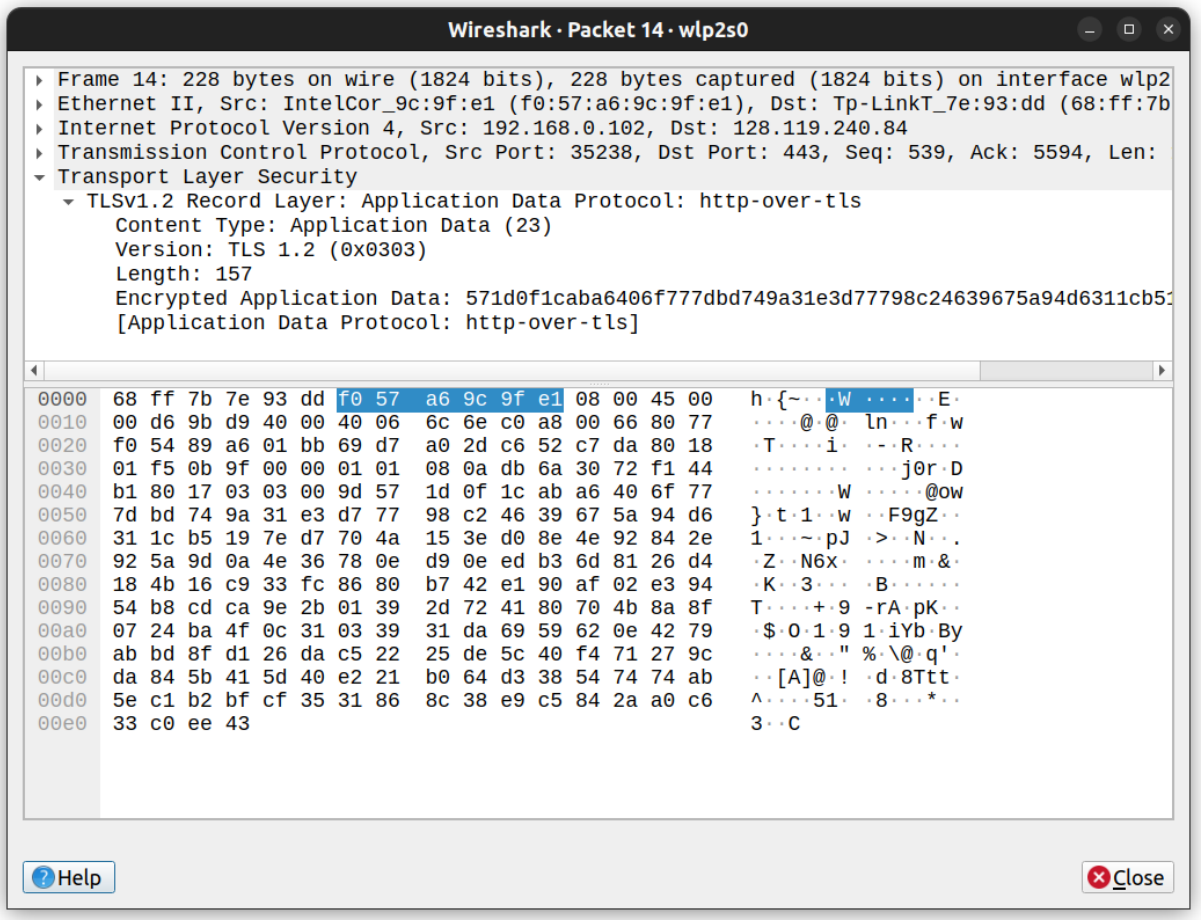
- Номер пакета 12

19. Предоставляет ли клиент свой собственный сертификат открытого ключа, подписанный Центром сертификации, обратно серверу? Если да, то каков номер пакета в вашей трассировке, содержащего сертификат вашего клиента?

- Клиент не предоставляет свой сертификат

Данные приложения





20. Какой алгоритм шифрования с симметричным ключом используется клиентом и сервером для шифрования данных приложения (в данном случае HTTP-сообщений)?

- Cipher Suite из Server Hello сообщения - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

21. В каком из сообщений TLS окончательно определен и объявлен этот алгоритм шифрования с симметричным ключом?

- Окончательно определен и объявлен этот алгоритм шифрования с симметричным ключом в ответном сообщении от сервера с записью Change Cipher Spec (номер пакета 13)

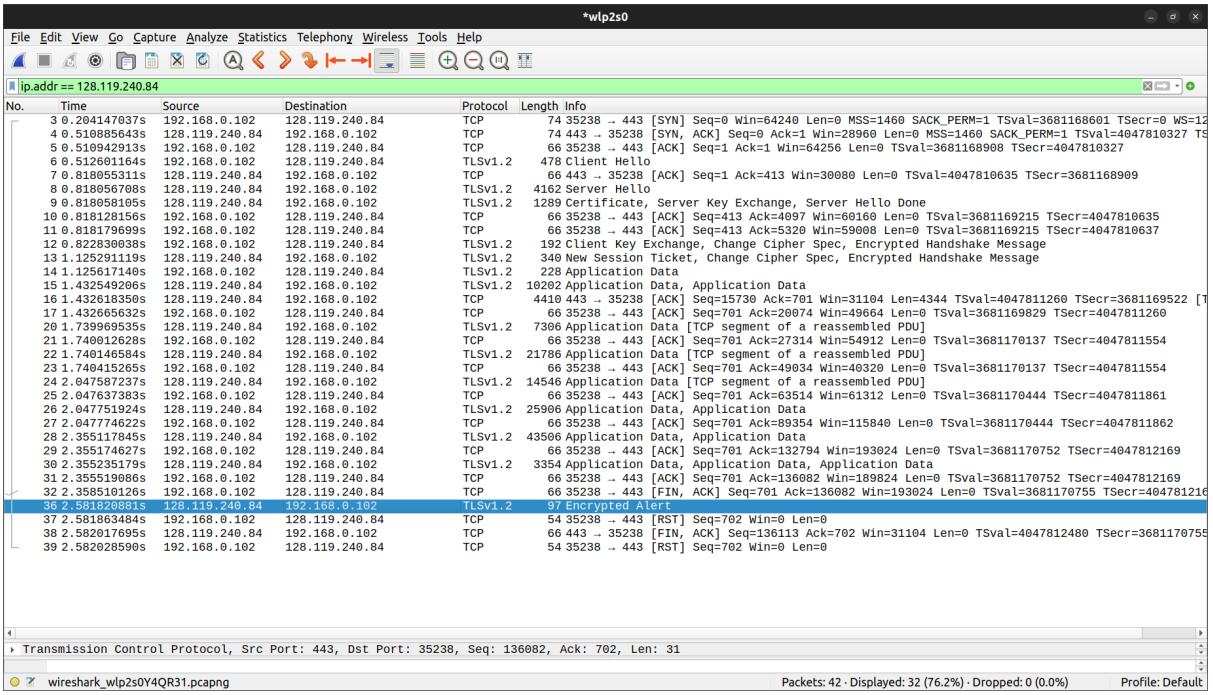
22. Каков номер пакета в вашей трассировке для первого зашифрованного сообщения, передающего данные приложения от клиента к серверу?

- Номер пакета 14

23. Как вы думаете, каково содержимое этих зашифрованных данных приложения, учитывая, что эта трассировка была сгенерирована путем получения домашней страницы www.cics.umass.edu?

- Содержимое зашифрованных данных - GET-запрос от клиета серверу и HTTP OK ответ сервера клиенту с содержимым html-страницы index.html

Давайте посмотрим, как клиент закрывает соединение TLS.



24. Какой номер пакета содержит сообщение TLS от клиента к серверу, которое закрывает соединение TLS?

- Сообщение с записью Encrypted Alert может свидетельствовать о закрытии TLS-соединения. Перед ним был отправлен TCP-сегмент FIN+ACK, который подтверждает намерение закрыть TCP-соединение. А после отправляются TCP-сегменты RST, которые принудительно закрывают TCP-соедение.