

Лабораториска вежба 10 – HTTPS, TLS, QUIC	Име и презиме	Индекс	Професор
--	---------------	--------	----------

Одговорите давајте ги со црвена боја.

Дел 1: TLS

Прашање 1: Краток опис на начинот за разрешување на www.cics.umass.edu. Поставете слика од одговорот.

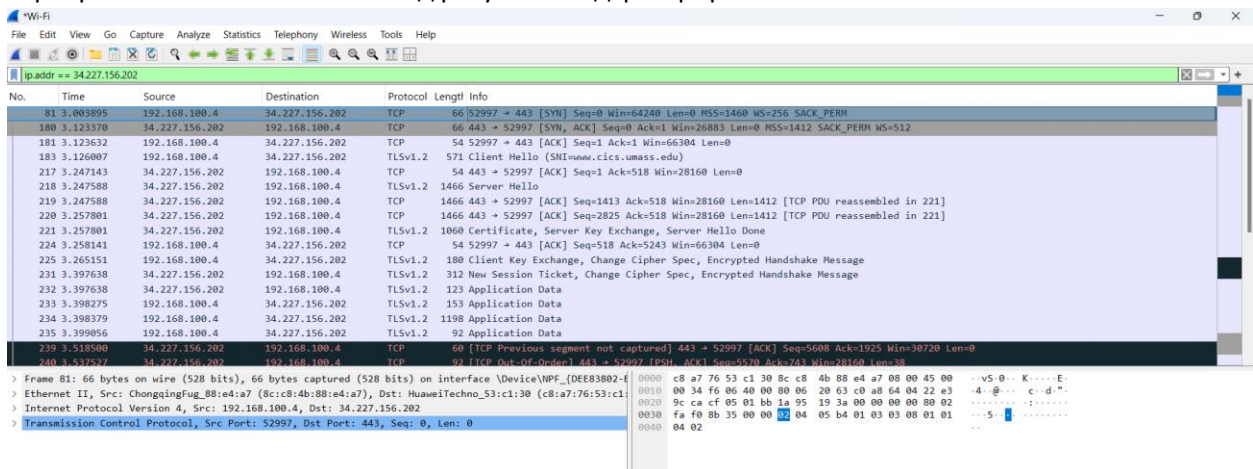
```
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Filip>nslookup www.cics.umass.edu
Server:      UnKnown
Address:     192.168.100.1

Non-authoritative answer:
Name:       ecosystem101live.enterprise-g1.acquia-sites.com
Address:    34.227.156.202
Aliases:    www.cics.umass.edu
            cics.ecosystem1.acsitefactory.com

C:\Users\Filip>
```

Прашање 2: Wireshark филтерот за филтрирање на сообраќајот само од/кон www.cics.umass.edu серверот. Поставете screenshot од резултатот од филтрирањето.



Прашање 3: Кој е бројот на пакет кој го содржи првичниот TCP SYN? Поставете слика од Wireshark прозорецот.

Бројот е 81

No.	Time	Source	Destination	Protocol	Length	Info
81	3.003895	192.168.100.4	34.227.156.202	TCP	66	52997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
180	3.123370	34.227.156.202	192.168.100.4	TCP	66	443 → 52997 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=512
181	3.123632	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
183	3.126007	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SNI=www.cics.umass.edu)

Прашање 4: Дали TCP конекцијата е воспоставена пред или по праќањето на првата TLS порака од клиентот до серверот?

Пред

No.	Time	Source	Destination	Protocol	Length	Info
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello
219	3.247588	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=1413 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
220	3.257801	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=2825 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
221	3.257801	34.227.156.202	192.168.100.4	TLSv1.2	1060	Certificate, Server Key Exchange, Server Hello Done
224	3.258141	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=518 Ack=5243 Win=66304 Len=0
225	3.265151	192.168.100.4	34.227.156.202	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
231	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
232	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	123	Application Data
233	3.398275	192.168.100.4	34.227.156.202	TLSv1.2	153	Application Data
234	3.398379	192.168.100.4	34.227.156.202	TLSv1.2	1198	Application Data
235	3.399056	192.168.100.4	34.227.156.202	TLSv1.2	92	Application Data
239	3.518500	34.227.156.202	192.168.100.4	TCP	60	[TCP Previous segment not captured] 443 → 52997 [ACK] Seq=5608 Ack=1925 Win=30720 Len=0
240	3.532527	34.227.156.202	192.168.100.4	TCP	92	[TCP Out-of-Order] 443 → 52997 [PSH, ACK] Seq=5520 Ack=741 Win=28160 Len=38

> Frame 81: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{DEE83802-...}

> Ethernet II, Src: ChongqingFug_88:e4:a7 (8c:c8:4b:88:e4:a7), Dst: HuaweiTechno_53:c1:30 (c8:a7:76:53:c1:30)

> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 34.227.156.202

> Transmission Control Protocol, Src Port: 52997, Dst Port: 443, Seq: 0, Len: 0

Прашање 5: Кој број на пакет ја содржи TLS Client Hello пораката?

Број 183

No.	Time	Source	Destination	Protocol	Length	Info
183	3.126007	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SNI=www.cics.umass.edu)
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello

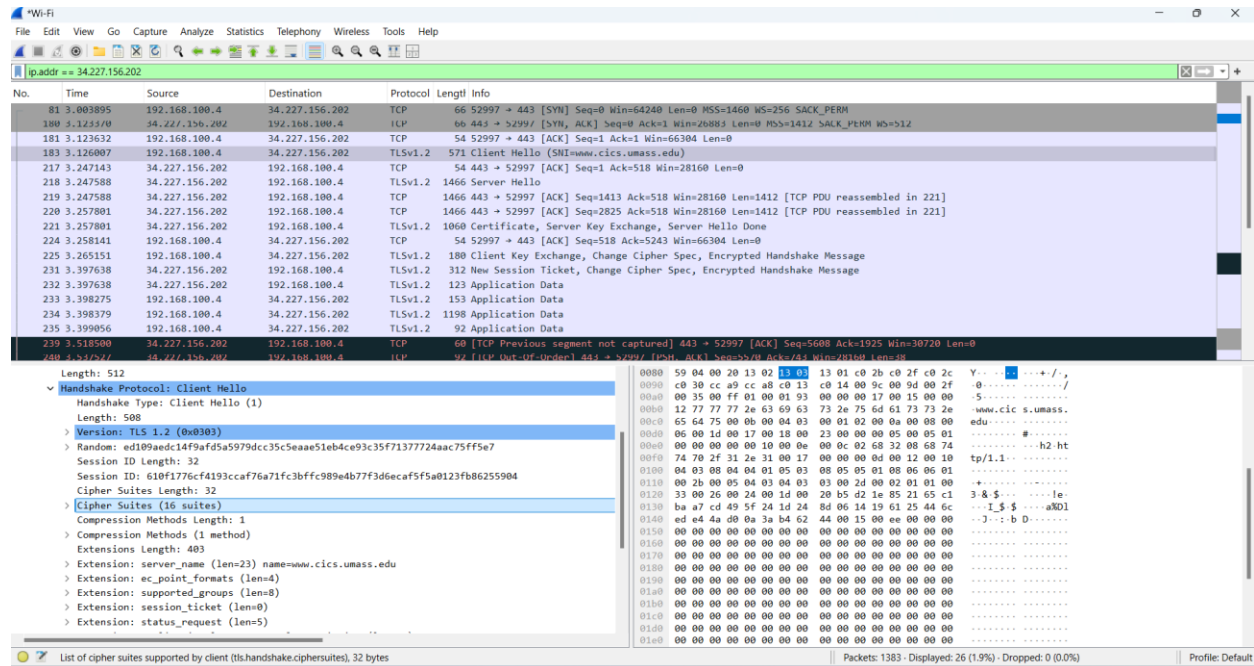
Прашање 6: Која е верзијата на TLS што се користи од страна на клиентот

Верзијата е TLSv1.2

- Frame 183: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{DEE83802-...}
- Ethernet II, Src: ChongqingFug_88:e4:a7 (8c:c8:4b:88:e4:a7), Dst: HuaweiTechno_53:c1:30 (c8:a7:76:53:c1:30)
- Internet Protocol Version 4, Src: 192.168.100.4, Dst: 34.227.156.202
- Transmission Control Protocol, Src Port: 52997, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Прашање 7: Колку методи за шифрирање поддржува клиентот? Поставете слика од одговорот.

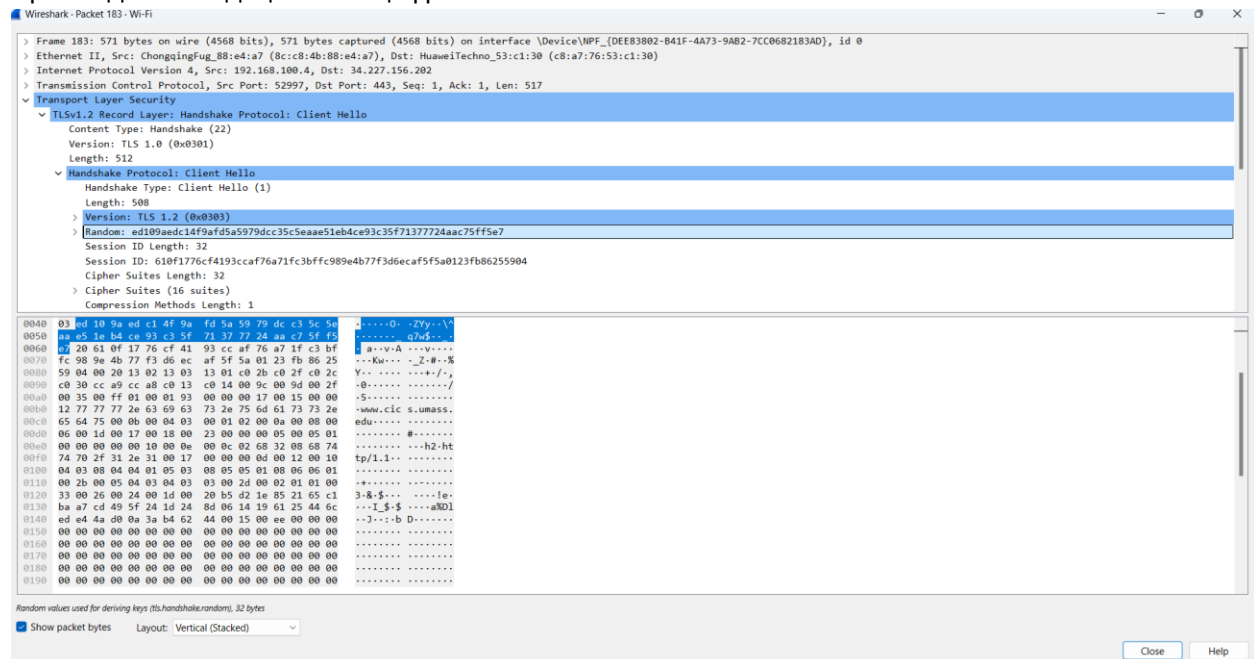
Клиентот подржува 16 методи на шифрирање



Wireshark capture of a TLS handshake. The packet list shows a Client Hello (packet 183) and a Server Hello (packet 218). The packet details for the Client Hello show the supported cipher suites: TLS 1.2 (0x0303). The packet bytes show the random bytes field (0000 59 04 00 20 13 02 13 03 13 01 c0 2b c0 2f c0 2c).

Прашање 8: Кои се првите две хексадецимални цифри во random bytes полето од Client Hello пораката?

Првите две хексадецимални цифри се **ed**



Wireshark packet details for the Client Hello (packet 183). The details show the random bytes field (0000 59 04 00 20 13 02 13 03 13 01 c0 2b c0 2f c0 2c). The packet bytes show the random bytes field (0000 59 04 00 20 13 02 13 03 13 01 c0 2b c0 2f c0 2c).

Прашање 9: Која е функцијата на random bytes полето во Client Hello пораката?

Полето Random Bytes се користи за да се обезбеди уникатност при TLS ракувањето. Се комбинира со Random Bytes од серверот за да се генерира сесискиот клуч, кој гарантира безбедна и независна комуникација за секоја сесија.

Прашање 10: Кој е бројот на пакет кој ја содржи TLS Server Hello пораката?

Бројот на пакетот е 218

The screenshot shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packet 218 (Time: 3.247588) as a TLSv1.2 1466 Server Hello. The packet details pane on the left shows the structure of the Server Hello message, including the random field. The packet bytes pane on the right shows the raw data of the message.

No.	Time	Source	Destination	Protocol	Length	Info
81	3.003895	192.168.100.4	34.227.156.202	TCP	66	52997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
180	3.123370	34.227.156.202	192.168.100.4	TCP	66	443 → 52997 [SYN, ACK] Seq=0 Ack=1 Win=66304 Len=0 MSS=1412 SACK_PERM WS=512
181	3.123632	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
183	3.126907	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SHA256, TLSv1.2)
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello

Packet 218 details:

- Length: 74
- Handshake Protocol: Server Hello
- Handshake Type: Server Hello (2)
- Length: 70
- Version: TLS 1.2 (0x0303)
- Random: 65a4c9e74b23f1a080e86e483190444d313071bc7c114c6cd006cf9db4b1db
- Session ID Length: 0
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Compression Method: null (0)
- Extensions Length: 30
- Extension: server_name (len=0)
- Extension: renegotiation_info (len=1)
- Extension: ec_point_formats (len=4)
- Extension: session_ticket (len=0)
- Extension: application_layer_protocol_negotiation (len=5)
- [JA3S Fullstring: 771,49199,0-65281-11-35-16]
- [JA3S: b898351eb5e26aeaf3723d466935494]
- TLS segment data (1333 bytes)

Прашање 11: Кој метод на шифрирање го има одбрано серверот од оние кои беа понудени од клиентот? Серверот го има одбрано методот за шифрирање:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

The screenshot shows the same Wireshark packet capture as before, but with the packet details pane expanded to show the Cipher Suite field. The packet bytes pane on the right shows the raw data of the message.

No.	Time	Source	Destination	Protocol	Length	Info
81	3.003895	192.168.100.4	34.227.156.202	TCP	66	52997 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
180	3.123370	34.227.156.202	192.168.100.4	TCP	66	443 → 52997 [SYN, ACK] Seq=0 Ack=1 Win=66304 Len=0 MSS=1412 SACK_PERM WS=512
181	3.123632	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
183	3.126907	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SHA256, TLSv1.2)
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello

Packet 218 details:

- Length: 74
- Handshake Protocol: Server Hello
- Handshake Type: Server Hello (2)
- Length: 70
- Version: TLS 1.2 (0x0303)
- Random: 65a4c9e74b23f1a080e86e483190444d313071bc7c114c6cd006cf9db4b1db
- Session ID Length: 0
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Compression Method: null (0)
- Extensions Length: 30
- Extension: server_name (len=0)
- Extension: renegotiation_info (len=1)
- Extension: ec_point_formats (len=4)
- Extension: session_ticket (len=0)
- Extension: application_layer_protocol_negotiation (len=5)
- [JA3S Fullstring: 771,49199,0-65281-11-35-16]
- [JA3S: b898351eb5e26aeaf3723d466935494]
- TLS segment data (1333 bytes)

Прашање 12: Дали Server Hello пораката исто така содржи random bytes, како што тоа беше случај за Client Hello пораката? Ако содржи, која е нивната намена? Поставете слика од одговорот.

Да Server Hello пораката содржи random bytes

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packet 221, which is a TLSv1.2 Server Hello. The packet details pane on the right shows the 'Random' field, which is a 32-byte random value used for key derivation. The packet bytes pane on the right shows the raw data of the random bytes.

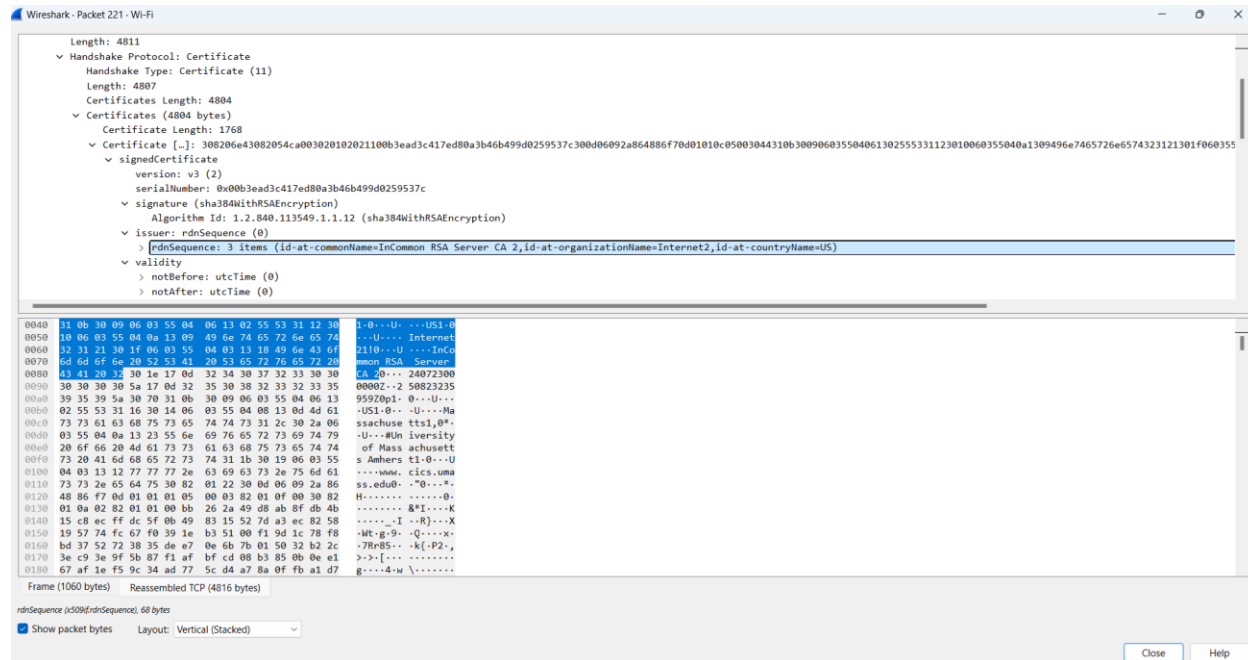
Прашање 13: Кој е бројот на пакет што го содржи јавниот клуч за сертификатот на www.cics.umass.edu серверот?

Бројот е 221

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packet 221, which is a TLSv1.2 Server Hello. The packet details pane on the right shows the 'Certificates' field, which contains the public key for the certificate. The packet bytes pane on the right shows the raw data of the certificates.

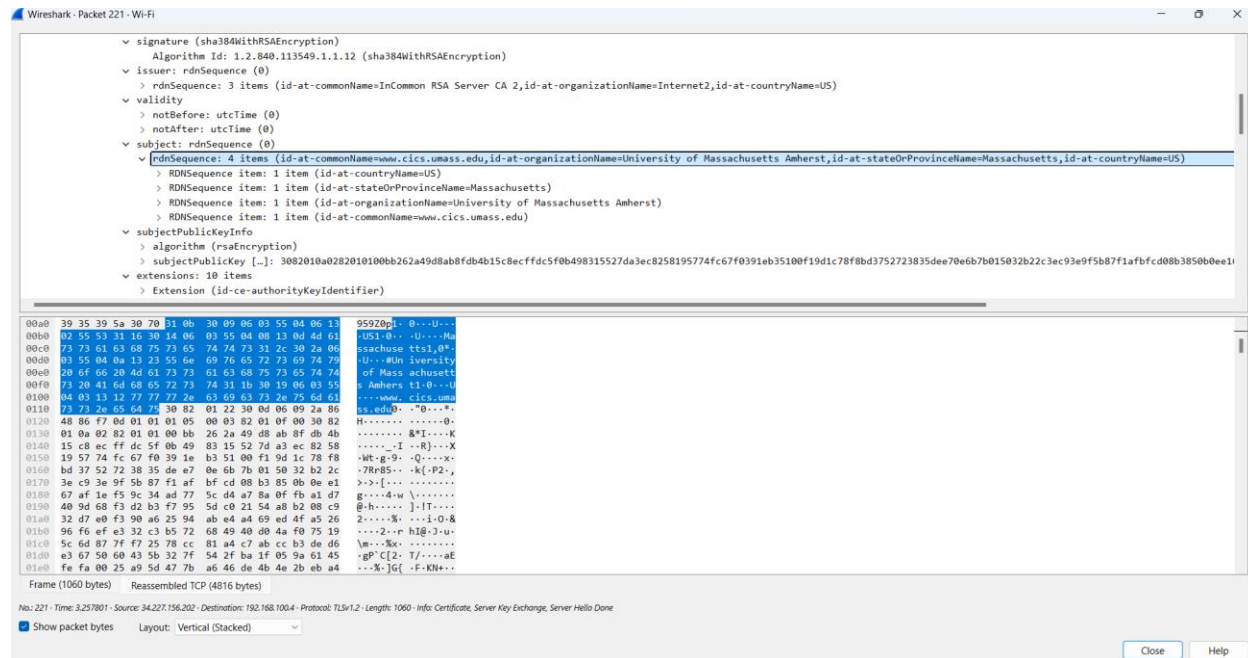
Прашање 14: Дали сите сертификати се за www.cs.umass.edu? Ако не се однесуваат сите сертификати на www.cs.umass.edu, тогаш на кого се однесуваат?

Не. Се однесуваат за Certificate Authority (CA)



Прашање 15: Кое е името на certificate authority-то кој го издал сертификатот со `id-at-commonName=www.cs.umass.edu`?

`id-at-commonName=InCommon RSA Server CA 2`



Прашање 16: Кој алгоритам за потпишување се користи од CA за потпишување на сертификатот?

Алгоритмот за потпишување што го користи СА за потпишување на сертификатот е **sha384WithRSAEncryption**

Wireshark packet capture showing a TLS handshake. The selected packet is packet 221, a TLSv1.2 1060 Certificate, Server Key Exchange, Server Hello Done. The packet details show the Handshake Type: Certificate (11), Length: 4807, Certificates Length: 4804, and the Certificate structure including version, serialNumber, signature, issuer, validity, subject, subjectPublicKeyInfo, extensions, and algorithmIdentifier.

Прашање 17: Извлечете ги првите 4 хексадецимални цифри за јавниот клуч од `subjectPublicKeyInfo` потполето од `SignedCertificate` полето за www.cs.umass.edu сертификатот.

00 bb

Wireshark - Packet 221 - Wi-Fi

> RDNSSequence item: 1 item (id-at-countryName=US)
 > RDNSSequence item: 1 item (id-at-stateOrProvinceName=Massachusetts)
 > RDNSSequence item: 1 item (id-at-organizationName=University of Massachusetts Amherst)
 > RDNSSequence item: 1 item (id-at-commonName=www.cics.umass.edu)

v subjectPublicKeyInfo
 > algorithm (rsaEncryption)
 Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
 v subjectPublicKey [...]: 3082010a0282010100b262a49d8ab8fdb4b15c8c8ffdc5f0b498315527da3ec8258195774fc6f70391eb35100f19d1c78f8db375272383dee70e6b7b015032b22c3ec9e9f5b7f1afbfcd08b3850b0ee11
 modulus: 0x00b262a49d8ab8fdb4b15c8c8ffdc5f0b498315527da3ec8258195774fc6f70391eb3511
 publicKeyExponent: 65537

v extensions: 10 items
 > Extension (id-ce-authorityKeyIdentifier)
 > Extension (id-ce-subjectKeyIdentifier)
 > Extension (id-ce-keyUsage)
 > Extension (id-ce-basicConstraints)
 > Extension (id-ce-extendedKeyUsage)
 > Extension (id-ce-certificatePolicies)
 > Extension (id-ce-cRLDistributionPoints)

0130 01 0a 02 82 01 01 00 bb 26 2a 49 d8 ab 8f db 4b&*I...X
 0140 15 c8 ec ff dc 5f 0b 49 83 15 52 7d a3 ec 82 58I...R...X
 0150 19 57 74 c6 70 39 1e b3 51 00 f1 9d 1c 78 f8 ...ht.g.9..Q...X
 0160 1d 37 52 78 30 35 de c7 0e db 7b 01 50 32 b2 24 ...70R55...Q...P2...X
 0170 1e 49 3e 9f 5b 87 f1 af bf cd 08 b3 85 0b 0e 01 ...2P2...I...X
 0180 67 af 1e f5 9c 34 ad 77 5c da a7 8a 0f bf a1 d7 ...g...4.w...V...X
 0190 40 9d 68 f3 d2 b3 f7 95 5d c0 21 54 a8 b2 08 c9 ...B.h...0...J...I...X
 01a0 32 d7 e0 f3 90 ae 25 94 ab e4 a4 69 ed 4f a5 26 ...2...X...i...O...X
 01b0 26 16 ef e3 22 b5 72 c8 49 40 d8 4a f0 75 15 ...2...e.hg...Q...X
 01c0 5c 6d 87 7f 7f 25 78 cc 81 a4 c7 ab c3 9d 0e ...X...K...X
 01d0 e3 67 50 60 43 5b 32 7f 54 2f ba f1 05 9a 61 a5 ...gP[2..T...at...X
 01e0 fe fa 00 25 a9 5d 47 7b a6 4e db 4e 2b eb a4 ...X...G[...F.KN...X
 01f0 25 87 43 3b 2c 13 97 62 82 79 10 c2 a4 cd cb 62 ...0...i...b...y...C...X
 0200 c2 e7 db 41 47 a3 f2 4b 8e 3b c9 51 ca 73 ab ...X...M...K...Q...X
 0210 b1 c7 45 09 bf 92 22 c6 f8 d1 c3 7d bb 37 d8 3a ...X...M...7...X
 0220 c2 49 de ab 50 74 5c bb 4b 61 c1 e3 9b eb aa a4 ...T...P...K...X
 0230 1b 30 35 1c eb 14 02 03 01 00 01 a3 82 03 23 ...02...X
 0240 30 82 03 1f 30 1f 06 03 55 1d 23 04 18 30 16 80 ...0...0...U...0...X
 0250 14 ef 4c 00 92 ae af 76 2e 5e 95 e2 c9 5f 87 1b ...L...U...X
 0260 19 45 4d e2 d9 30 1d 06 03 55 1d 0e 04 16 04 14 ...M...0...U...X
 0270 00 26 a2 8d 6b 45 aa 59 c0 b3 7f 2c 16 a2 f8 41 ...0...KE...Y...X

Frame (1060 bytes) Reassembled TCP (4816 bytes)

No. 221 - Time: 3.257801 - Source: 34.227.156.202 - Destination: 192.168.100.4 - Protocol: TLSv1.2 - Length: 1060 - Info: Certificate, Server Key Exchange, Server Hello Done

☒ Show packet bytes Layout: Vertical (Stacked)

Прашање 18: Кој е бројот на пакет со кој експлицитно се терминира Server Hello пораката?

Поставете слика од одговорот.

Бројот е 221

Version: TLS 1.2 (0x0303)
Length: 4811
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4807
Certificates Length: 4804
Certificates (4804 bytes)
Certificate Length: 1768
Certificate [..]: 308206e43082054ca00302010201100b3ead3c417ed80a3b46b499d0259537c300d06092
version: v3 (2)
serialNumber: 0x00b3ead3c417ed80a3b46b499d0259537c
signature (sha384WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.12 (sha384WithRSAEncryption)
issuer: rdnSequence (8)
rdnSequence: 3 items (id-at-commonName=InCommon RSA Server CA 2,id-at-organization
rdnSequence item: 1 item (id-at-countryName=US)
rdnSequence item: 1 item (id-at-organizationName=Internet2)

Reassembled TCP (4816 bytes)

Прашање 19: Кој е бројот на пакет што ги содржи јавниот клуч, Change Cipher Spec и Encrypted Handshake пораката испратени од клиентот кон серверот?

Бројот е 225

Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 70
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
EC Diffie-Hellman Client Params
Content Type: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 48
Handshake Protocol: Encrypted Handshake Message

Reassembled TCP (4816 bytes)

Прашање 20: Дали јавниот клуч кој го испраќа клиентот кон серверот е потпишан од страна на CA? Ако тоа е така, кој е бројот на пакетот во кој се наоѓа клиентскиот сертификат?

Не е потпишан од СА

Прашање 21: Кој алгоритам за симетрична енкрипција се користи за шифрирање на пораките помеѓу клиентот и серверот?

AES128

Прашање 22: Во кои TLS пораки е овој алгоритам за симетрична енкрипција договорен? Поставете слика од одговорот.

Во Server Hello пораката

The image shows a Wireshark network capture of a TLS handshake. The packet list on the left shows a series of TCP and TLSv1.2 packets. The packet details pane on the right is expanded to show the 'Handshake Protocol: Server Hello' section. Within this section, the 'Cipher Suite' is highlighted as 'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)'. The packet bytes pane on the far right shows the raw hexadecimal data of the packet.

Прашање 23: Кој е бројот на пакет кој ги содржи првите шифрирани податоци од апликациско ниво?

Бројот е 232

Wireshark packet capture showing TLSv1.2 handshake and application data. The packet list on the left shows packets 181 to 242. The packet details pane on the right shows the structure of the TLSv1.2 record, including the Application Data field.

No.	Time	Source	Destination	Protocol	Length	Info
181	3.123632	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
183	3.126007	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SHA=www.cics.umass.edu)
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello
219	3.247588	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=1413 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
220	3.257801	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=2825 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
221	3.257801	34.227.156.202	192.168.100.4	TLSv1.2	1060	Certificate, Server Key Exchange, Server Hello Done
224	3.258141	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=518 Ack=5243 Win=66304 Len=0
225	3.265151	192.168.100.4	34.227.156.202	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
231	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
232	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	123	Application Data
233	3.398275	192.168.100.4	34.227.156.202	TLSv1.2	153	Application Data
234	3.398379	192.168.100.4	34.227.156.202	TLSv1.2	1198	Application Data
235	3.399056	192.168.100.4	34.227.156.202	TLSv1.2	92	Application Data
239	3.518500	34.227.156.202	192.168.100.4	TCP	60	[TCP Previous segment not captured] 443 → 52997 [ACK] Seq=5008 Ack=1925 Win=30720 Len=0
240	3.537527	34.227.156.202	192.168.100.4	TCP	92	[TCP Out-Of-Order] 443 → 52997 [PSH, ACK] Seq=5570 Ack=743 Win=28160 Len=38
241	3.537527	34.227.156.202	192.168.100.4	TLSv1.2	553	Application Data
242	3.537897	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1925 Ack=6107 Win=65280 Len=0

Frame 232: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_{DEE83B8} Ethernet II, Src: HuaweiTechno_53:c1:30 (c8:a7:76:53:c1:30), Dst: ChongqingFug_88:e4:a7 (8c:c8:4b:88:e4: Internet Protocol Version 4, Src: 34.227.156.202, Dst: 192.168.100.4 Transmission Control Protocol, Src Port: 443, Dst Port: 52997, Seq: 5501, Ack: 644, Len: 69

Transport Layer Security

- TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 64
 - Encrypted Application Data: 0cd3e1fb8f3de96da34db34743a218d70af1d7e45b49373fec997999bb9962e798d638 [Application Data Protocol: HyperText Transfer Protocol 2]

Дел 2: QUIC

Прашање 24: Кои сè транспортни протоколи се употребуваат за комуникација со YouTube во отворената сатура датотека? Наведете по еден број на пакет за секој транспортен протокол кој ќе го идентификувате.

Пакет 232 за TCP, 233 за UDP

Wireshark packet capture showing TLSv1.2 handshake and application data. The packet list on the left shows packets 181 to 242. The packet details pane on the right shows the structure of the TLSv1.2 record, including the Application Data field.

No.	Time	Source	Destination	Protocol	Length	Info
181	3.123632	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
183	3.126007	192.168.100.4	34.227.156.202	TLSv1.2	571	Client Hello (SHA=www.cics.umass.edu)
217	3.247143	34.227.156.202	192.168.100.4	TCP	54	443 → 52997 [ACK] Seq=1 Ack=518 Win=28160 Len=0
218	3.247588	34.227.156.202	192.168.100.4	TLSv1.2	1466	Server Hello
219	3.247588	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=1413 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
220	3.257801	34.227.156.202	192.168.100.4	TCP	1466	443 → 52997 [ACK] Seq=2825 Ack=518 Win=28160 Len=1412 [TCP PDU reassembled in 221]
221	3.257801	34.227.156.202	192.168.100.4	TLSv1.2	1060	Certificate, Server Key Exchange, Server Hello Done
224	3.258141	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=518 Ack=5243 Win=66304 Len=0
225	3.265151	192.168.100.4	34.227.156.202	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
231	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
232	3.397638	34.227.156.202	192.168.100.4	TLSv1.2	123	Application Data
233	3.398275	192.168.100.4	34.227.156.202	TLSv1.2	153	Application Data
234	3.398379	192.168.100.4	34.227.156.202	TLSv1.2	1198	Application Data
235	3.399056	192.168.100.4	34.227.156.202	TLSv1.2	92	Application Data
239	3.518500	34.227.156.202	192.168.100.4	TCP	60	[TCP Previous segment not captured] 443 → 52997 [ACK] Seq=5008 Ack=1925 Win=30720 Len=0
240	3.537527	34.227.156.202	192.168.100.4	TCP	92	[TCP Out-Of-Order] 443 → 52997 [PSH, ACK] Seq=5570 Ack=743 Win=28160 Len=38
241	3.537527	34.227.156.202	192.168.100.4	TLSv1.2	553	Application Data
242	3.537897	192.168.100.4	34.227.156.202	TCP	54	52997 → 443 [ACK] Seq=1925 Ack=6107 Win=65280 Len=0

Frame 232: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface \Device\NPF_{DEE83B8} Ethernet II, Src: HuaweiTechno_53:c1:30 (c8:a7:76:53:c1:30), Dst: ChongqingFug_88:e4:a7 (8c:c8:4b:88:e4: Internet Protocol Version 4, Src: 34.227.156.202, Dst: 192.168.100.4 Transmission Control Protocol, Src Port: 443, Dst Port: 52997, Seq: 5501, Ack: 644, Len: 69

Transport Layer Security

- TLSv1.2 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 64
 - Encrypted Application Data: 0cd3e1fb8f3de96da34db34743a218d70af1d7e45b49373fec997999bb9962e798d638 [Application Data Protocol: HyperText Transfer Protocol 2]

Прашање 25: Во кој пакет се случува првата размена на порака преку QUIC протоколот? Дали тоа е во првиот пакет во датотеката или не? Ако не е во првиот пакет, зошто е тоа така?

Во пакет 233, но не е првиот пакет во датотеката затоа што започнува со HTTP/2 па серверот нуди опција за надградба во HTTP/3 со QUIC

Прашање 26: Која промена ја забележувате по избор на Master Secret датотеката? Образложете.

Шифрираните пакети беа дешифрирани и станаа достапни за преглед

Прашање 27: Во кој проток (stream) се наоѓа првото GET барање испратено за „/“? Внесете ја бројката на протокот во шаблонот со одговори.

Проток 15, Пакет 22

Прашање 28: Кој е status кодот на добиениот одговор? Поставете слика од одговорот.

Статус 302

Прашање 29: Разгледајте ги заглавјата на одговорот и обидете се да го најдете „alt-svc“ заглавјето. Прочитајте повеќе за ова заглавје и опишете со ваши зборови која е неговата намена.

Серверот му предлага на клиентот да се надогради во HTTP/3 со QUIC

Прашање 30: Кој е максималниот број на поддржани унидирекционални протоци (streams_uni)? Поставете слика од одговорот.

103