

EEM-413 Bilgisayar Ağları Lab5 (SSL)

NOT: Uygulama için <http://www.clubboon.com> adresinden üyelik alınmış giriş yapılmış ve çıkış yapılmıştır.

1.

The image shows a Wireshark capture of an SSL/TLS session. The packet list on the left shows frames 31 through 69. The packet details pane on the right shows the structure of the selected frame (Frame 31: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

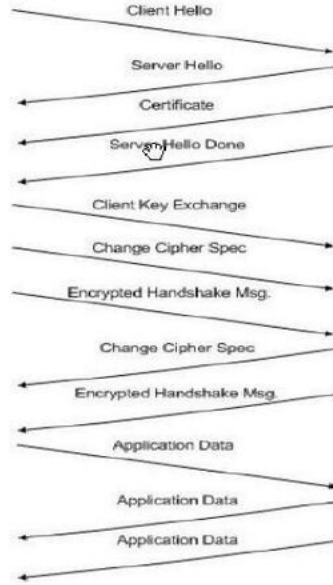
No.	Time	Source	Destination	Protocol	Length	Info
31	4.891135000	10.2.0.10	173.252.113.17	TLsv1.2	286	Client Hello
33	5.026566000	173.252.113.17	10.2.0.10	TLsv1.2	1514	Server Hello
37	5.026566000	173.252.113.17	10.2.0.10	TLsv1.2	164	Certificate
39	5.026566000	10.2.0.10	173.252.113.17	TLsv1.2	368	Client Key Exchange, change cipher spec, encrypted handshake message
47	5.165215000	173.252.113.17	10.2.0.10	TLsv1.2	101	change cipher spec, encrypted handshake message
55	5.190480000	10.2.0.10	173.252.113.17	TLsv1.2	949	Application data
63	5.290357000	10.2.0.10	109.232.223.3	TLsv1	571	client hello
65	5.290357000	109.232.223.3	10.2.0.10	TLsv1	187	Server Hello, change cipher spec, encrypted handshake message
66	5.300055000	10.2.0.10	109.232.223.3	TLsv1	101	change cipher spec, encrypted handshake message
67	5.300389000	10.2.0.10	109.232.223.3	TLsv1	706	Application data
69	5.327709000	173.252.113.17	10.2.0.10	TLsv1.2	351	Application data
70	5.336857000	10.2.0.10	31.13.84.33	TLsv1.2	383	Application data
81	5.412546000	109.232.223.3	10.2.0.10	TLsv1	1514	(retransmission) Application data, Application data, Application data
83	5.451648000	10.2.0.10	195.39.12.66	TLsv1	720	Application data, Application data
86	5.510378000	31.13.84.33	10.2.0.10	TLsv1.2	1378	Application data
87	5.512238000	195.39.12.66	10.2.0.10	TLsv1	363	Application data
92	5.878945000	10.2.0.10	2.21.111.203	TLsv1.2	1033	Application data
96	5.979716000	10.2.0.10	173.194.112.233	TLsv1.2	187	Application data
97	5.979892000	10.2.0.10	173.194.112.233	TLsv1.2	437	Application data, Application data
98	5.999884000	2.21.111.203	10.2.0.10	TLsv1.2	923	Application data

Frame 31: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0
 Ethernet II, Src: Inventec_AS:ba:b2 (00:26:8c:a8:b2), Dst: Hewlett-26:07:00 (44:1e:a1:26:07:00)
 Internet Protocol Version 4, Src: 10.2.0.10 (10.2.0.10), Dst: 173.252.113.17 (173.252.113.17)
 Transmission Control Protocol, Src Port: 50979 (50979), Dst Port: https (443), Seq: 1, Ack: 1, Len: 232
 Secure Sockets Layer
 TLsv1.2 Record Layer: Handshake Protocol: Client Hello

0000 44 1e a1 26 07 00 00 26 6c a8 ba b2 08 00 45 00 D...&...1....E.
 0010 02 10 6c e0 40 00 80 06 00 00 0a 02 00 0a ad fc ..l.....
 0020 71 11 c7 23 01 00 86 16 01 5e 72 81 68 71 50 18 q... ..Ap.hgP.
 0030 01 00 2a 1c 00 00 16 03 01 00 e3 01 00 00 df 03
 0040 03 80 b5 c1 35 7e 8c 3f b4 c5 3b 99 7c a5 56 b5 ...S~? ...l.V.
 0050 4e f0 7c 87 20 c1 00 34 24 0f 00 15 81 0a 10 17 h.....

Frame	Source	SSL Count	SSL Type
31	Client	1	Client Hello
33	Server	1	Server Hello
37	Server	2	Certificate Server Hello Done
39	Client	3	Client Key Exchange Change Cipher Spec Encrypted Handshake Message
47	Server	2	Change Cipher Spec Encrypted Handshake Message
55	Client	1	Application Data
67	Server	1	Application Data
69	Server	1	Application Data

EEM-413 Bilgisayar Ağları Lab5 (SSL)



2.

Content Type: 1 byte

Version: 2 bytes

Length: 2 bytes

Bunlar "Secure socket" leridir.

The image shows a Wireshark packet capture of an SSL/TLS handshake and data transfer. The filter is set to 'ssl'. The packet list shows the following packets:

- 8. 2.696905000 193.140.100.247 10.2.0.10 TLSv1.2 107 Encrypted Alert
- 18. 3.192354000 10.2.0.10 173.194.67.120 SSL 55 Continuation Data
- 22. 4.223454000 10.2.0.10 173.194.112.253 SSL 55 Continuation Data
- 31. 4.891135000 10.2.0.10 173.252.113.17 TLSv1.2 286 Client Hello
- 33. 5.026566000 173.252.113.17 10.2.0.10 TLSv1.2 1514 Server Hello
- 37. 5.026928000 173.252.113.17 10.2.0.10 TLSv1.2 164 Certificate
- 39. 5.029085000 10.2.0.10 173.252.113.17 TLSv1.2 368 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- 47. 5.165215000 173.252.113.17 10.2.0.10 TLSv1.2 101 Change Cipher Spec, Encrypted Handshake Message
- 55. 5.190480000 10.2.0.10 173.252.113.17 TLSv1.2 949 Application Data
- 63. 5.290357000 10.2.0.10 109.232.223.3 TLSv1 571 Client Hello
- 65. 5.290357000 109.232.223.3 10.2.0.10 TLSv1 187 Server Hello, Change Cipher Spec, Encrypted Handshake Message
- 66. 5.300055000 10.2.0.10 109.232.223.3 TLSv1 101 Change Cipher Spec, Encrypted Handshake Message

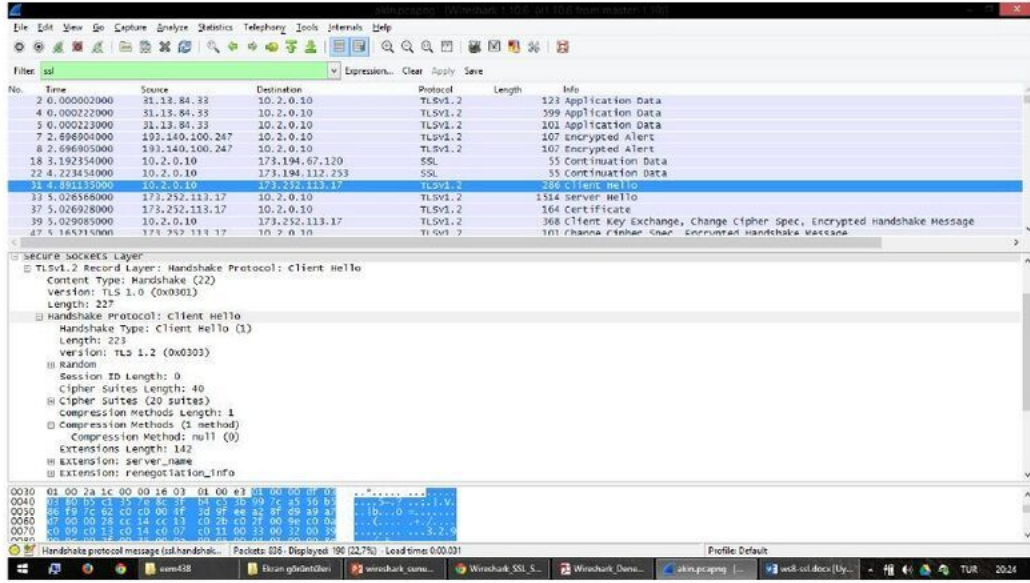
The packet details pane shows the selected packet (66) and its structure:

- Internet Protocol Version 4, Src: 10.2.0.10, Dst: 109.232.113.17
- Transmission Control Protocol, Src Port: 50979, Dst Port: https (443), Seq: 233, Ack: 4207, Len: 314
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 262
 - Handshake Protocol: Client Key Exchange
 - 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: 96
 - Handshake Protocol: Encrypted Handshake Message

The packet bytes pane shows the raw data of the selected packet.

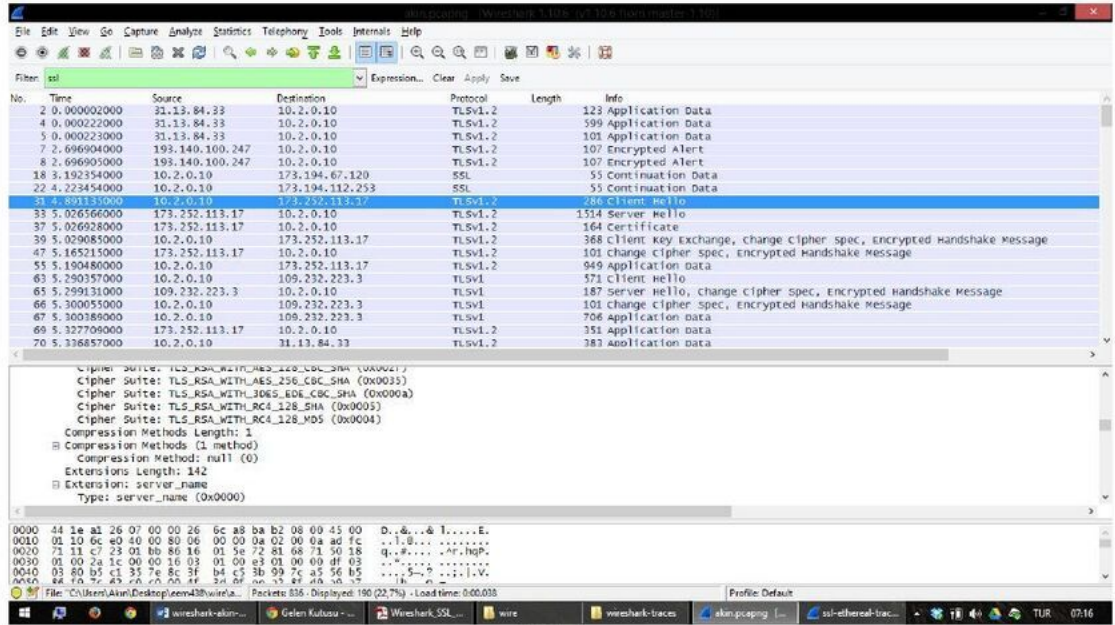
EEM-413 Bilgisayar Ağları Lab5 (SSL)

3.



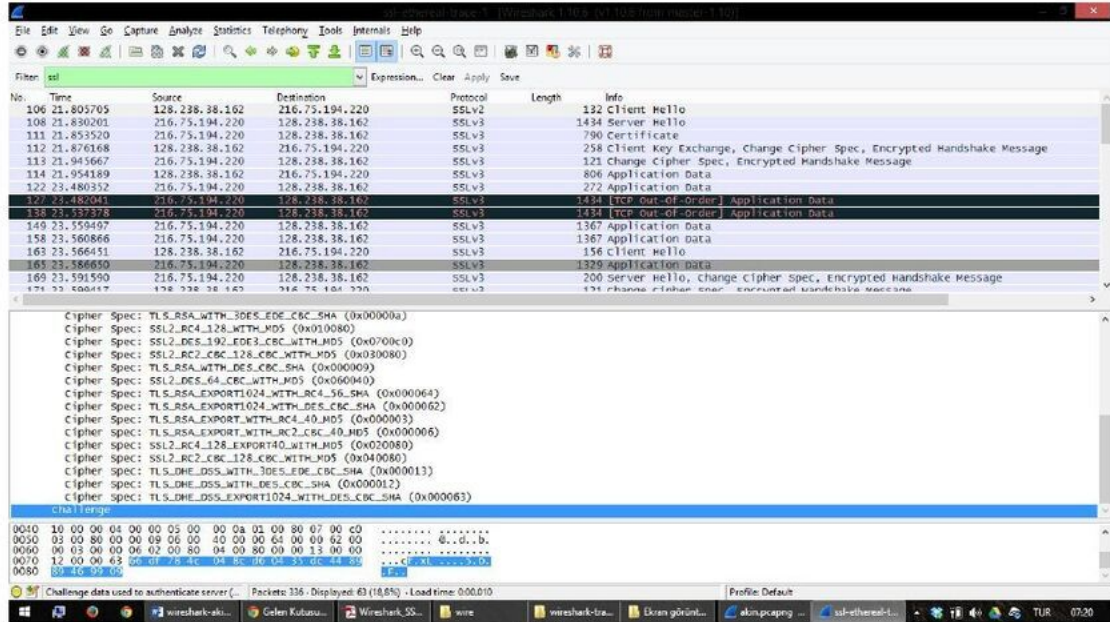
Handshake mesajları ekranda gözüktüğü üzere gösterilmektedir.

4. Sonda yer alması gereken challenge, güncelliği garanti etmektedir. Fakat aldığım çıktılarda (şekil 4-a) yer almamaktadır. Bu yüzden olması gereken resmi (şekil 4-b) verilen örnek trace üzerinden koymuş bulunmaktayım.



Şekil 4-a

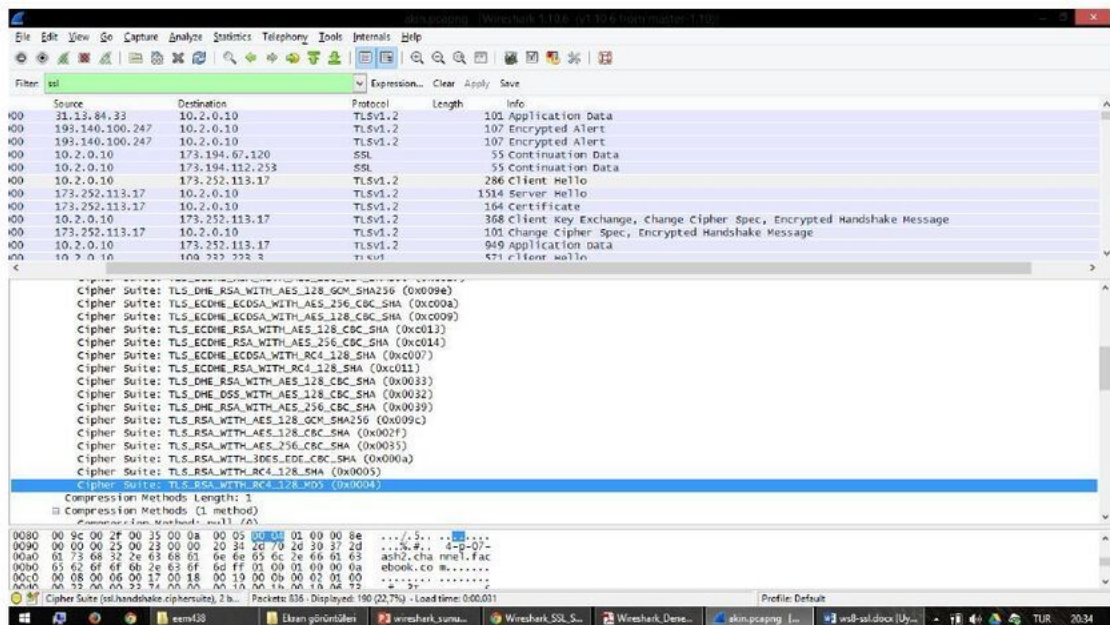
EEM-413 Bilgisayar Ağları Lab5 (SSL)



Şekil 4-b

5.

RSA, RC4, MD5 şifreleme metodları kullanılmış.
 RSA = açık anahtarlama şifrelemesi,
 RC4 = simetrik anahtar şifreleme,
 MD5 = karma algoritma.



EEM-413 Bilgisayar Ağları Lab5 (SSL)

6.

Wireshark capture of an SSL handshake. The packet list shows a sequence of messages including Application Data, Encrypted Alert, Encrypted Handshake Message, Change Cipher Spec, and Server Hello. The packet details pane for the selected packet (No. 33) shows the TLS 1.2 structure with fields like Random, Session ID, Cipher Suite, Compression Method, and Extensions. The packet bytes pane shows the raw hex and ASCII data.

Tek satırda RSA, RC4 ve MD5 şifrelemeleri yapılıyor.

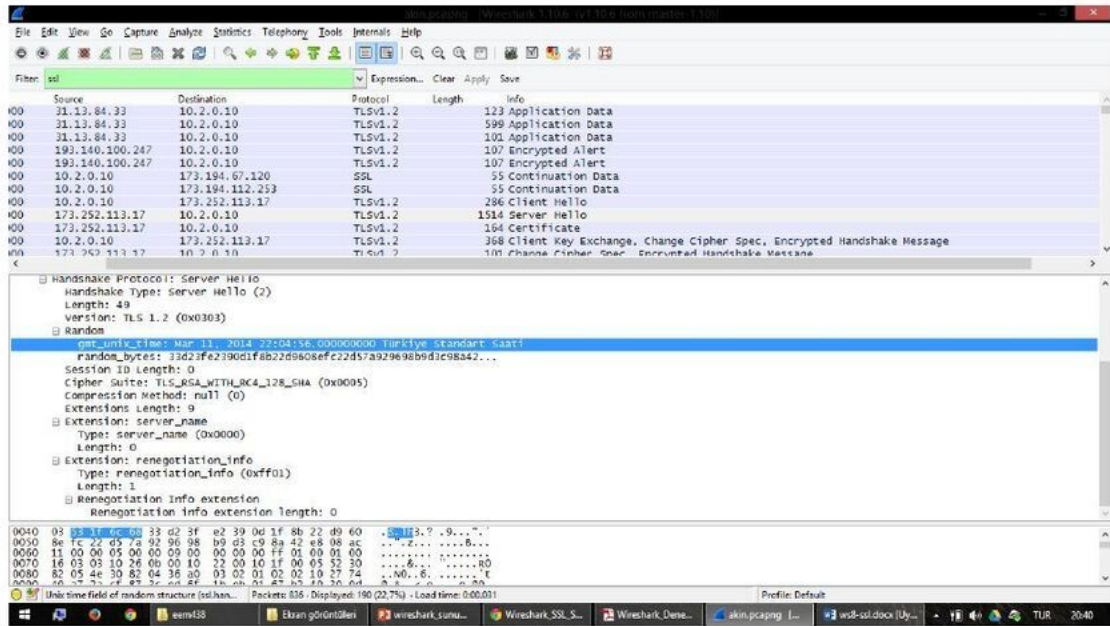
7.

Wireshark capture of an SSL handshake. The packet list shows a sequence of messages including Application Data, Encrypted Alert, Encrypted Handshake Message, Change Cipher Spec, and Server Hello. The packet details pane for the selected packet (No. 33) shows the TLS 1.2 structure with fields like Random, Session ID, Cipher Suite, Compression Method, and Extensions. The packet bytes pane shows the raw hex and ASCII data.

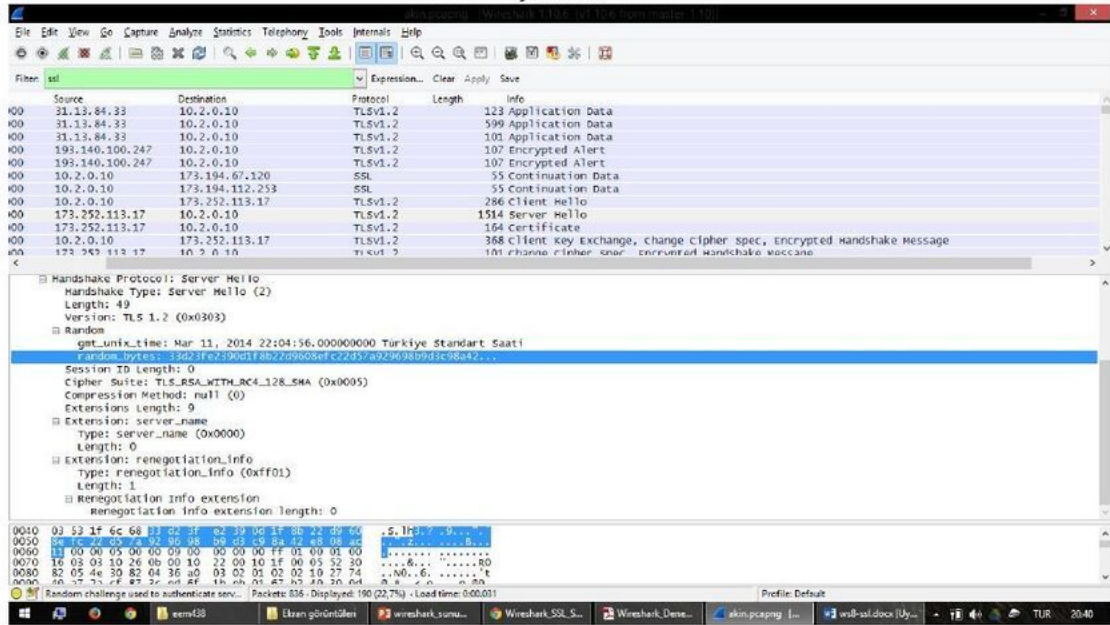
Evet bu random içindeki iki satır yer almaktadır. Aşağıda byte cinsinden değerleri verilmiştir.

- > 1. Satır 4 byte (şekil 7-a)
- > 2. Satır 28 byte (şekil 7-b)

EEM-413 Bilgisayar Ağları Lab5 (SSL)



Şekil 7-a



Şekil 7-b

EEM-413 Bilgisayar Ağları Lab5 (SSL)

8.

Evet içeriyor bu “Beni hatırla” durumunu gerçekleştirmeye yarıyor. Çıkış yapıldığında şifre ve kullanıcı adını hatırlar.

Wireshark capture of an SSL handshake. The packet list shows the Server Hello (1514 bytes) and Certificate (164 bytes) packets. The packet details pane shows the Server Hello structure, including the cipher suite (TLS_RSA_WITH_RC4_128_SHA) and extensions. The packet bytes pane shows the raw data of the Server Hello packet.

9.

Wireshark capture of an SSL handshake. The packet list shows the Server Hello (1514 bytes) and Certificate (164 bytes) packets. The packet details pane shows the Certificate structure, including the certificate (1362 bytes) and the Secure Sockets Layer (SSL) record layer. The packet bytes pane shows the raw data of the Certificate packet.

Aynı bir başlık altında certificate içermektedir.

10.

The screenshot shows a Wireshark capture of an SSL/TLS handshake. The packet list at the top shows several packets, including a Client Key Exchange (No. 39) and a Change Cipher Spec (No. 47). The packet details pane for packet 39 shows the following structure:

- Length: 262
- Handshake Protocol: Client Key Exchange
- Handshake Type: Client Key Exchange (16)
- Length: 258
- SSL Encrypted PreMaster Secret
 - Encrypted PreMaster length: 256
 - Encrypted PreMaster: 590570bbf7e859b792e2cfa7cb5e401a76ffbb175a60f400...
- TLV1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: TLS 1.2 (0x0303)

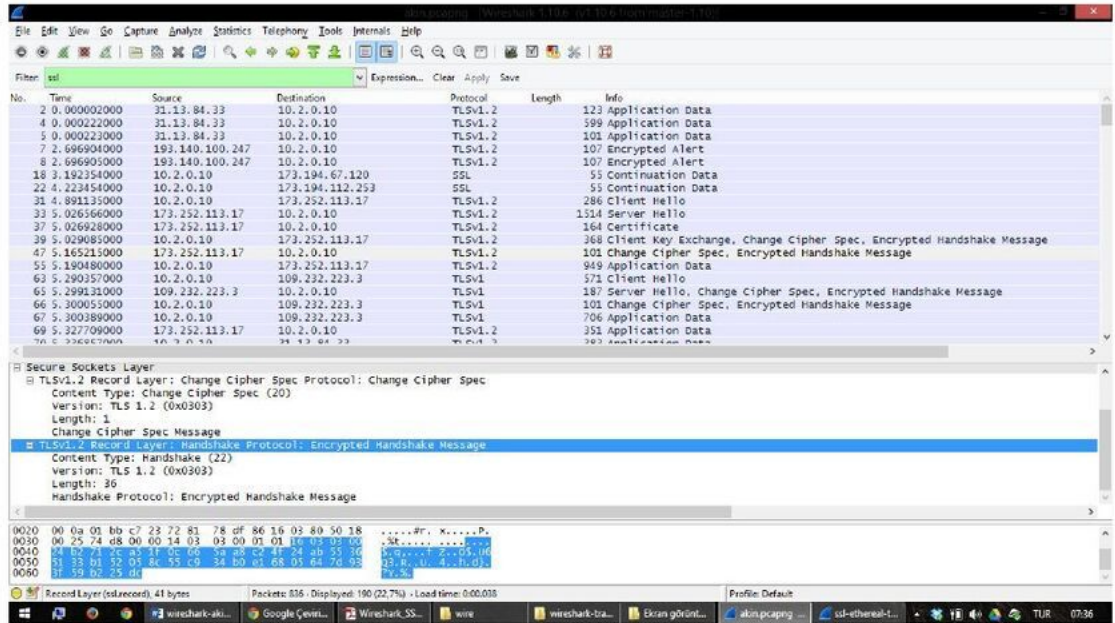
The packet bytes pane at the bottom shows the raw data of the Client Key Exchange packet, starting with 0030 01 00 2a 6e 00 00 16 03 03 01 06 10 00 01 02 00...

Evet, premaster secret içermektedir. Bu mac adreslerini şifreleme için kullanılmaktadır. 256 byte uzunluğundadır.

11.

Sıralı gelen paket mac id ile hep birlikte gönderiyor bir sonraki id de yer alıyor böylece kayıp olmuyor. Sonra gelen paket şifresinde 6 byte yer alıyor. (6 byte = 1 byte mesaj 5 byte header)

12.



Encrypted Handshake Message -> kendinden önceki hadshake mesajlarını şifreleyerek gönderiyor, bunun amacı garantilemedir.

13. Biri client biri server tarafından Change Cipher Spec record tek mac, encrypted handshake record bütün mac adreslerine göre şifreleyerek gönderiyor.

14. Application data RC4 şifrelemesi kullanılarak başlanmış sonrasında pre-master key ve en sonunda ise challenge işlemi yapılarak şifreleme hem server hemde kullanıcı arasında gerçekleşmiştir.

15. Data gönderiminde SSL mesaj alışverişi için TLSv1.2 kullanılmaktadır ve bazı ClientHello mesajında TLSv1 kullanırken bazılarında TLSv1.2 kullanılmıştır.