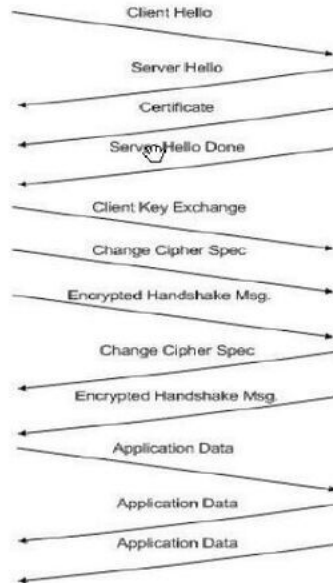


NOT: Uygulama için <http://www.clubboon.com> adresinden üyelik alınmış giriş yapılmış ve çıkış yapılmıştır.

- For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

Wireshark capture of an SSL/TLS handshake. The packet list shows frames 31 through 98. Frame 31 is a Client Hello, frame 33 is a Server Hello, frame 37 is a Certificate, frame 39 is a Client Key Exchange, frame 47 is a Server Key Exchange, frame 55 is a Client Application Data, frame 67 is a Server Application Data, and frame 69 is a Server Application Data. The packet details pane for frame 31 shows the TLSv1.2 Record Layer: Handshake Protocol: Client Hello. The packet bytes pane shows the raw data of the frame.

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



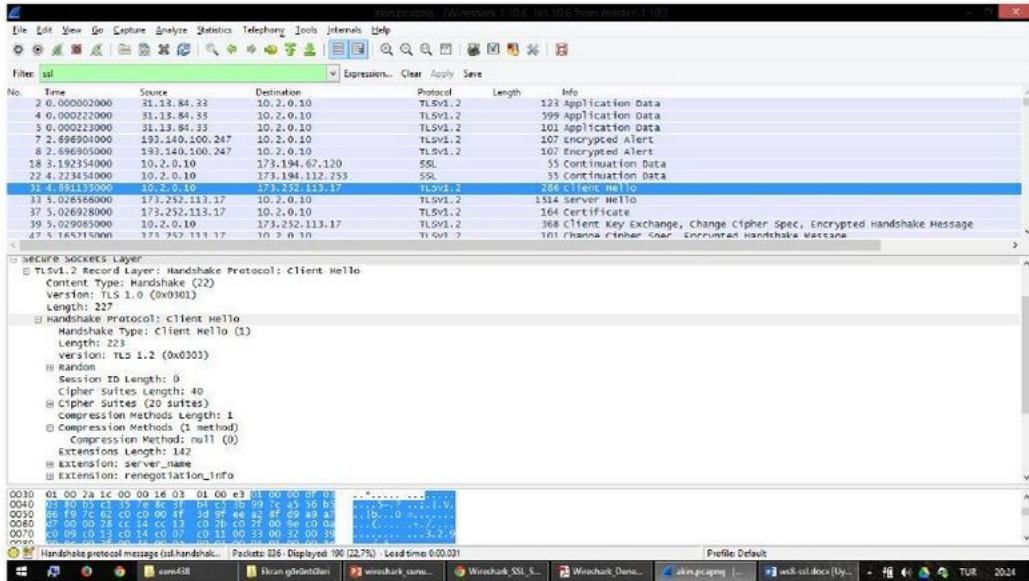
2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.

Content Type: 1 byte
Version: 2 bytes
Length: 2 bytes

Bunlar “Secure socket” leridir.

Wireshark packet capture showing an SSL/TLS handshake. The packet list shows packets 8 through 16. Packet 8 is a TLSv1.2 record layer handshake protocol client key exchange. Packet 9 is a TLSv1.2 record layer change cipher spec protocol change cipher spec. Packet 10 is a TLSv1.2 record layer handshake protocol encrypted handshake message. Packet 11 is a TLSv1.2 record layer handshake protocol client key exchange. Packet 12 is a TLSv1.2 record layer change cipher spec protocol change cipher spec. Packet 13 is a TLSv1.2 record layer handshake protocol encrypted handshake message. Packet 14 is a TLSv1.2 record layer handshake protocol client key exchange. Packet 15 is a TLSv1.2 record layer change cipher spec protocol change cipher spec. Packet 16 is a TLSv1.2 record layer handshake protocol encrypted handshake message. The packet details pane shows the structure of the TLSv1.2 record layer handshake protocol client key exchange, including the content type (handshake), version (TLS 1.2), and length (262). The packet bytes pane shows the raw data of the handshake message.

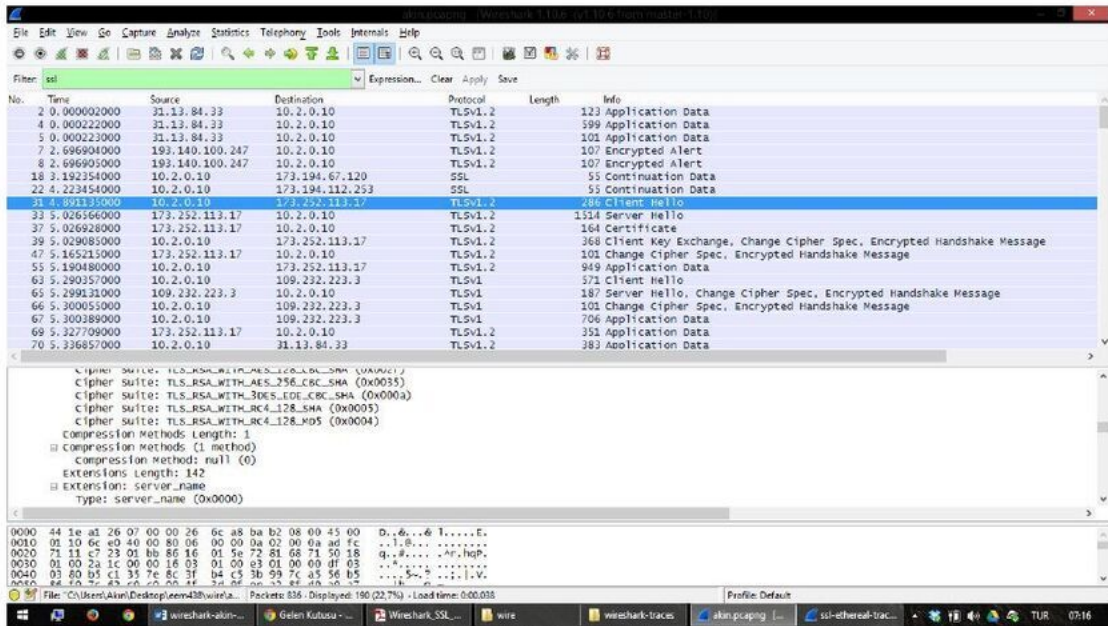
3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?



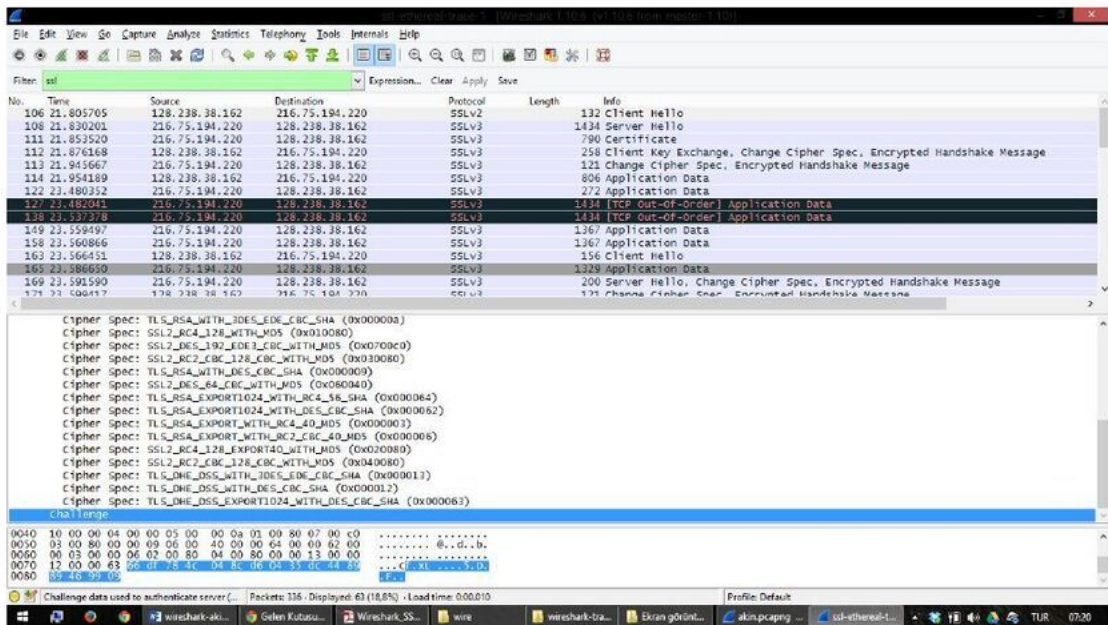
Handshake mesajları ekranda gözüktüğü üzere gösterilmektedir.

4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

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



Şekil 4-b

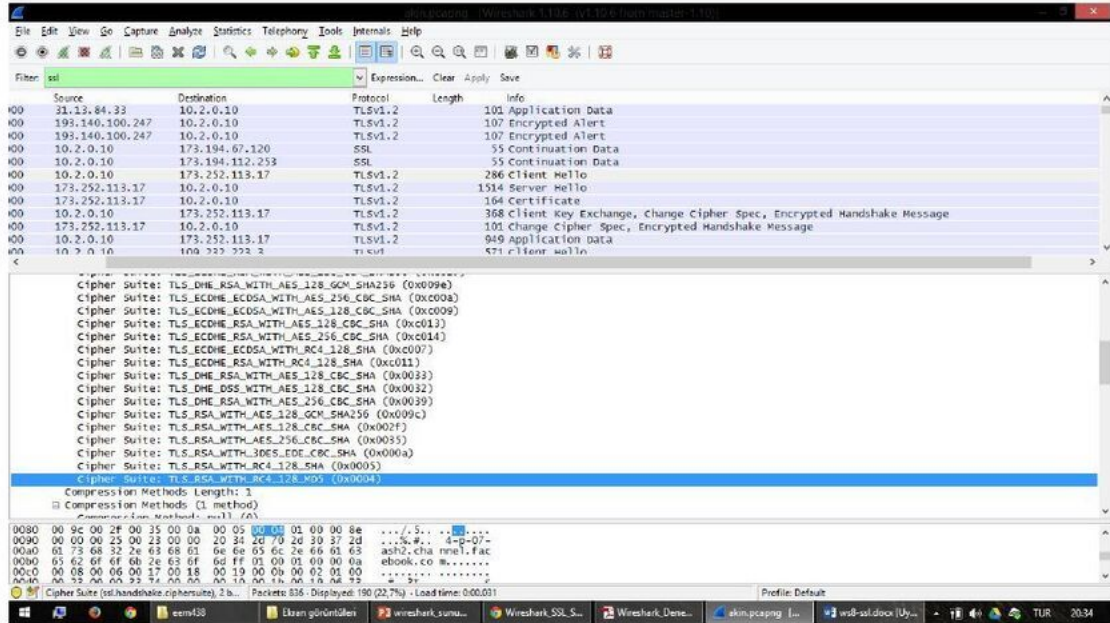
5. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

RSA, RC4, MD5 şifreleme metodları kullanılmış.

RSA = açık anahtarlama şifrelemesi,

RC4 = simetrik anahtar şifreleme,

MD5 = karma algoritma.



6. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Wireshark capture of an SSL handshake. The packet list shows a ServerHello record at packet 66. The packet details pane shows the TLS record structure, including the cipher suite: TLS_RSA_WITH_RC4_128_SHA (0x0005). The packet bytes pane shows the raw data of the ServerHello record.

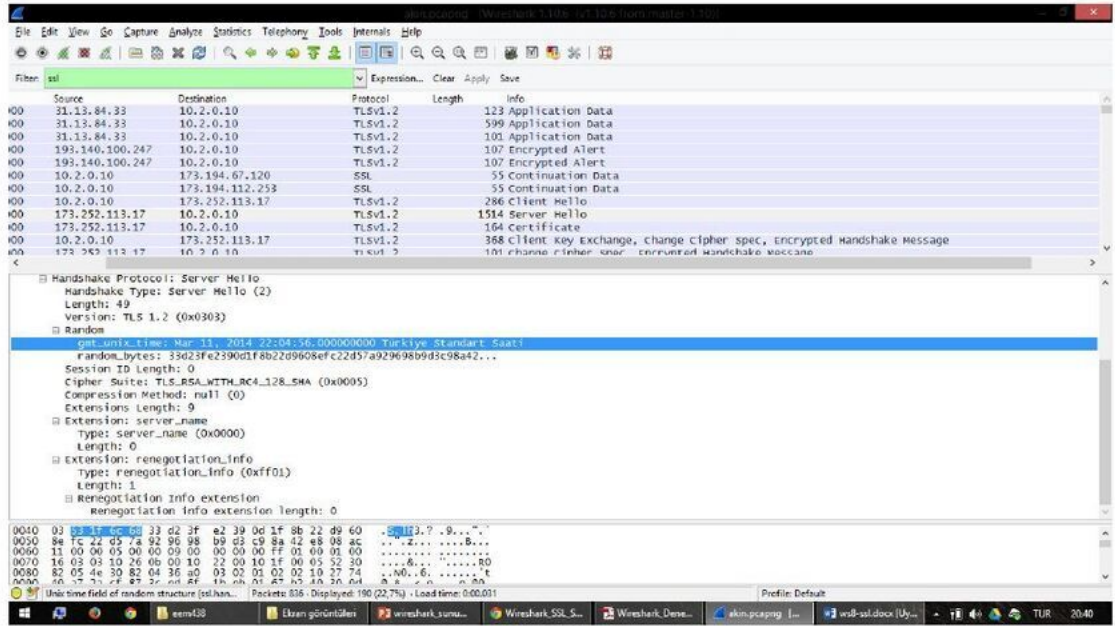
Tek satırda RSA, RC4 ve MD5 şifrelemeleri yapılıyor.

7. Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

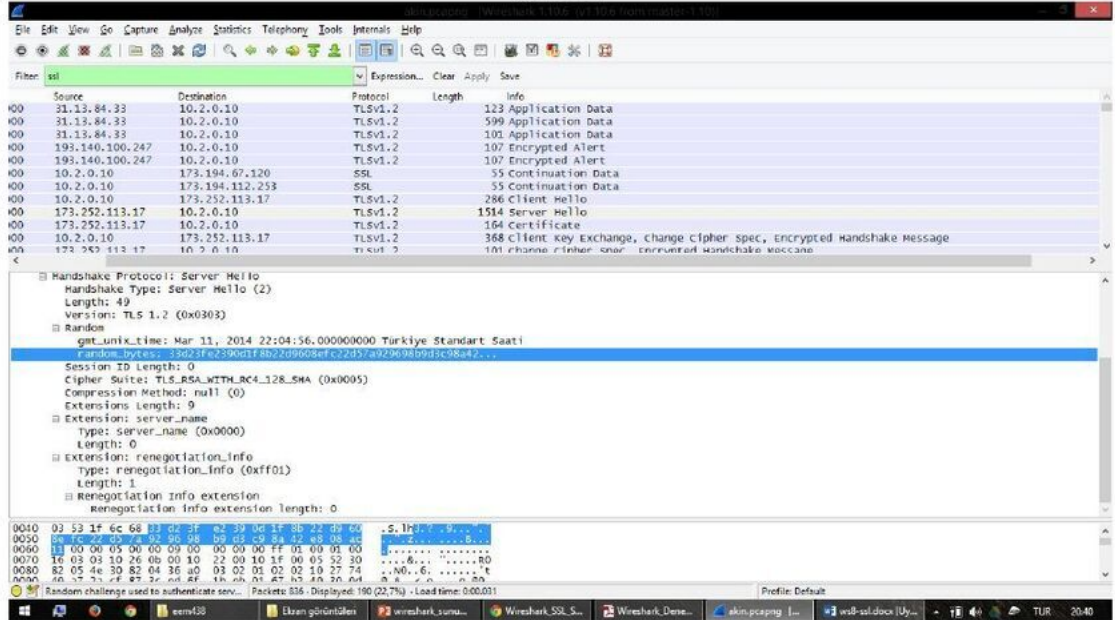
Wireshark capture of an SSL handshake. The packet list shows a ServerHello record at packet 66. The packet details pane shows the TLS record structure, including the cipher suite: TLS_RSA_WITH_RC4_128_SHA (0x0005). The packet bytes pane shows the raw data of the ServerHello record.

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)



Şekil 7-a



Şekil 7-b

8. Does this record include a session ID? What is the purpose of the session ID?

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

Wireshark capture showing a TLS handshake. The selected packet is a 'Handshake Protocol: Server Hello' (packet 11). The details pane shows the 'Session ID Length: 0' field, indicating no session ID is present. The 'Random' field shows a 32-byte value. The 'Cipher Suite' is TLS_RSA_WITH_RC4_128_SHA. The 'Extensions' field shows a renegotiation info extension.

9. Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

Wireshark capture showing a TLS handshake. The selected packet is a 'Handshake Protocol: Server Hello Done' (packet 12). The details pane shows the 'Certificate Length: 4127' field, indicating a certificate is present. The 'Certificate' field shows a 4127-byte value. The 'Certificate' field shows a 4127-byte value. The 'Certificate' field shows a 4127-byte value.

Aynı bir başlık altında certificate içermektedir.

10. Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

The image shows a Wireshark packet capture of a TLSv1.2 handshake. The packet list at the top shows several packets, with packet 39 (Time: 5.029085000) being the 'Client Key Exchange' record. The packet details pane for this record shows the 'RSA Encrypted PreMaster Secret' field. The 'Encrypted PreMaster' length is 256 bytes, and the 'Encrypted PreMaster' field contains the hex value: 990570bbf7e859b792e2cfa7cb5e401a76ffbb175a60f400... The packet bytes pane at the bottom shows the raw data of the packet, starting with 0030 00 00 2a 6e 00 00 16 03 03 01 06 10 00 01 02 01...

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

11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

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. In the encrypted handshake record, what is being encrypted? How?

The image shows a Wireshark capture of a TLSv1.2 handshake. The packet list shows a TLSv1.2 record of type 'encrypted handshake message' (length 36). The packet details pane shows the 'Handshake Protocol' section with 'encrypted handshake message' (length 36). The packet bytes pane shows the raw data of the encrypted handshake message.

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

13. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

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

14. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

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. Comment on and explain anything else that you found interesting in the trace.

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