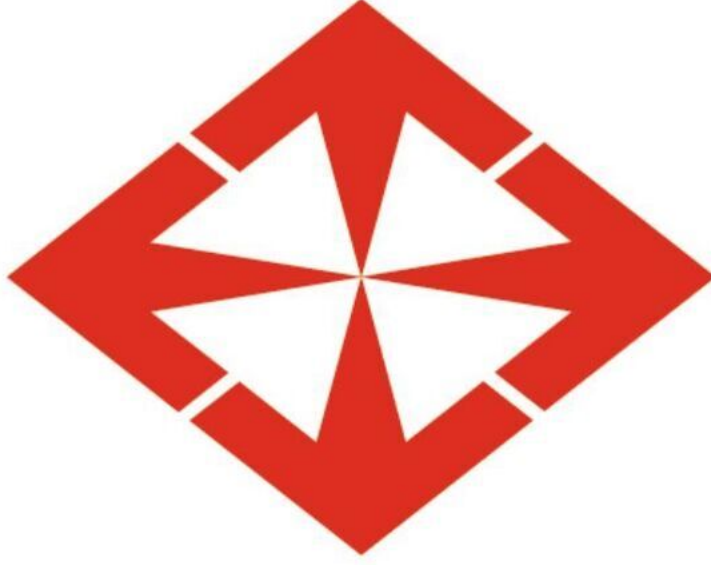




BAŞKENT ÜNİVERSİTESİ

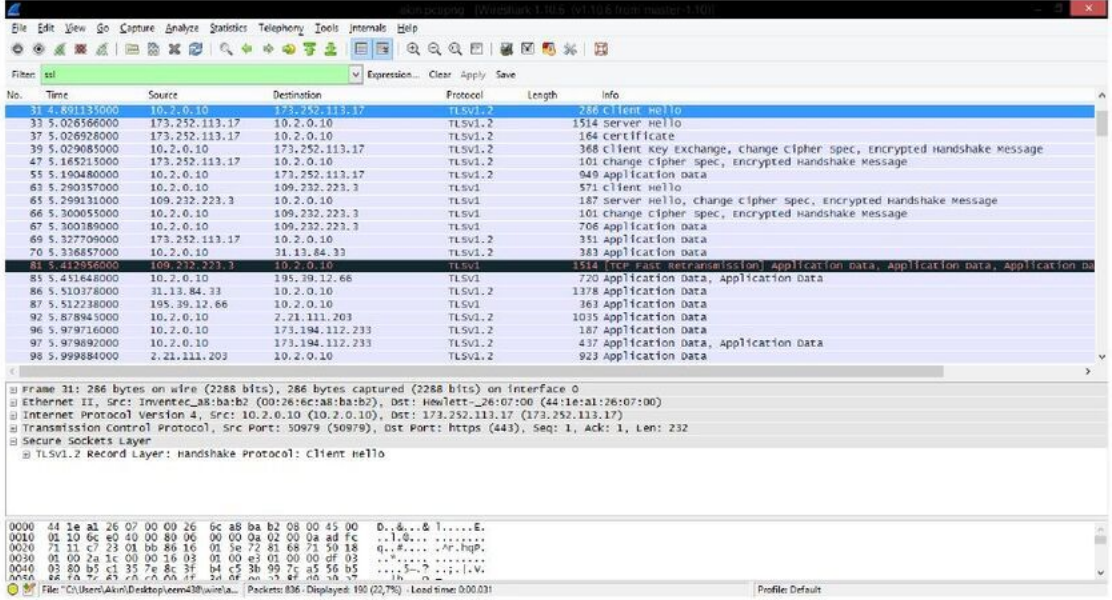
EEM 413

BİLGİSAYAR AĞLARI

DENEY-5 SSL

Uygulama Trace'lerden faydalanılarak gerçekleştirilmiştir.

1.)



2.)

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

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

Secure Socket'ler görülmektedir.

4.) 'Challenge' sonda yer almalıdır ve güncelliği garanti etmektedir. Şekil 4-B de trace üzerinden alınan çıktılarda challenge görülmektedir. (4-A program üzerinden alınan çıktılarda challenge yer almıyor.)

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 31 is selected, which is a TLSv1.2 packet of length 288 bytes, containing a Client Hello message.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the TLSv1.2 packet structure, including the Handshake Message (Type: server_hello).
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates the current file is "C:\Users\Akim\Desktop\packet31.pcap" and the profile is set to "Default".

The image shows a Wireshark packet capture of an SSL/TLS handshake. The top pane displays the packet list, with packet 122 selected. The middle pane shows the details of the selected packet, including the SSL/TLS handshake steps. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132	Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	21.835920	216.75.194.220	128.238.38.162	SSLv3	790	Certificate
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806	Application Data
122	22.480352	216.75.194.220	128.238.38.162	SSLv3	272	Application Data
123	22.480352	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello, Change Cipher Spec, Encrypted Handshake Message
135	23.337345	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello, Change Cipher Spec, Encrypted Handshake Message
149	23.559497	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
158	23.560866	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
163	23.566451	128.238.38.162	216.75.194.220	SSLv3	156	Client Hello
165	23.566850	216.75.194.220	128.238.38.162	SSLv3	1320	Application Data
169	23.591590	216.75.194.220	128.238.38.162	SSLv3	200	Server Hello, Change Cipher Spec, Encrypted Handshake Message
171	23.600417	128.238.38.162	216.75.194.220	SSLv3	131	Change Cipher Spec, Encrypted Handshake Message

The details pane for packet 122 shows the following information:

- Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000000a)
- Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x0000008)
- Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x00700c0)
- Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x0300800)
- Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x0000009)
- Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x0060040)
- Cipher Spec: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0000064)
- Cipher Spec: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0000062)
- Cipher Spec: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0000093)
- Cipher Spec: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0000006)
- Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x0200800)
- Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x0400800)
- Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0000013)
- Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0000012)
- Cipher Spec: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0000063)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The bottom pane shows the packet hex and ASCII.

5.)
RSA, RC4, MD5 şifreleme metodları kullanılmış.
RSA = açık anahtarlama şifrelemesi,
RC4 = simetrik anahtar şifreleme.

MD5 = karma algoritma.

The image shows a Wireshark packet capture of a TLS handshake. The top pane displays a list of packets, with packet 100 selected. The middle pane shows the details of the selected packet, specifically the 'Cipher Suite' field, which lists several cipher suites. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
100	31.13.84.33	10.2.0.10	10.2.0.10	TLSv1.2	101	Application Data
101	193.140.100.247	10.2.0.10	10.2.0.10	TLSv1.2	107	Encrypted Alert
102	193.140.100.247	10.2.0.10	10.2.0.10	TLSv1.2	107	Encrypted Alert
103	10.2.0.10	173.194.67.120	173.194.112.253	SSL	55	Continuation Data
104	10.2.0.10	173.194.112.253	173.252.113.17	SSL	55	Continuation Data
105	10.2.0.10	173.252.113.17	10.2.0.10	TLSv1.2	286	Client Hello
106	173.252.113.17	10.2.0.10	10.2.0.10	TLSv1.2	1514	Server Hello
107	173.252.113.17	10.2.0.10	10.2.0.10	TLSv1.2	164	Certificate
108	10.2.0.10	173.252.113.17	10.2.0.10	TLSv1.2	368	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
109	173.252.113.17	10.2.0.10	10.2.0.10	TLSv1.2	101	Change Cipher Spec, Encrypted Handshake Message
110	10.2.0.10	173.252.113.17	10.2.0.10	TLSv1.2	949	Application Data
111	10.2.0.10	100.233.233.2	10.2.0.10	TLSv1.2	571	Client Hello

Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc008)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Compression Methods: Length: 1
Compression Methods (1 method)

0090 00 9c 00 2f 00 35 00 0a 00 05 00 01 00 00 8e ... / 5 ...
00a0 01 73 68 32 2e 03 68 01 6e 6e 63 6c 2e 66 63 63 ... % # . 4-p-07-
00a0 63 62 6f 6f 6b 2e 63 6f 6d 6f 01 00 01 00 0a ... ebook.co m.....
00c0 00 08 00 06 00 17 00 18 00 19 00 0b 00 02 01 00
00d0 0a 52 0a 0a 35 1a 0a 0a 0a 1a 0a 1a 0a 1a 0a 1a ... # 3e

Cipher Suite (ssl.handshake.ciphersuite). 2 b... Packets: 836 - Displayed: 190 (22.7%) - Load time: 0.00.031

6.)

Wireshark capture showing TLS 1.2 handshake details. The packet list shows a Client Hello (packet 33) and a Server Hello (packet 63). The details pane for packet 33 shows the TLS 1.2 (0x0303) version, random bytes, session ID length 0, cipher suite TLS_RSA_WITH_RC4_128_SHA (0x0005), compression method null (0), and extensions length 9. The extensions list includes server_name (0x0000). The packet bytes pane shows the raw data of the Client Hello, with the first 32 bytes highlighted in blue.

Tek satırda RSA, RC4 ve MD5 şifrelemeleri yapılıyor.

7.)

Wireshark capture showing TLS 1.2 handshake details. The packet list shows a Client Hello (packet 33) and a Server Hello (packet 63). The details pane for packet 63 shows the TLS 1.2 (0x0303) version, random bytes, session ID length 0, cipher suite TLS_RSA_WITH_RC4_128_SHA (0x0005), compression method null (0), and extensions length 9. The extensions list includes server_name (0x0000). The packet bytes pane shows the raw data of the Server Hello, with the first 32 bytes highlighted in blue.

Kayıt içerisinde yer almaktadır. Byte cinsinden uzunlukları;

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



8.)

Kayıt session ID içermektedir. "Remember Me" durumunu gerçekleştirmeye yarıyor. Çıkış yapıldığında şifre ve kullanıcı adını hatırlar.

Wireshark packet capture showing an SSL/TLS handshake. The packet list shows a sequence of messages including Application Data, Encrypted Alert, Continuation Data, Server Hello, Client Hello, Certificate, and Key Exchange. The packet details pane for the Client Hello (packet 11) is expanded, showing fields like Version (TLS 1.2), Cipher Suite (TLS_RSA_WITH_RC4_128_SHA), and Extensions. The session ID field is highlighted in blue.

Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 49
Version: TLS 1.2 (0x0303)
Random
gmt_unix_time: Mar 11, 2014 22:04:56.000000000 Türkiye Standart Saati
random_bytes: 33d3fe2390d1f6b22d9608efc22d57a929698b9d3c9ba42...
Session ID Length: 0
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Compression Method: null (0)
Extensions Length: 9
Extensions: server_name
type: server_name (0x0000)
Length: 0
Extension: renegotiation_info
type: renegotiation_info (0xff01)
Length: 1
Renegotiation info extension
Renegotiation info extension length: 0

Length of session ID field (sslhandshake.ses...): Packets: 836 - Displayed: 190 (22.7%) - Load time: 0:00:031