

COMPUTER NETWORK LAB

LAB 8

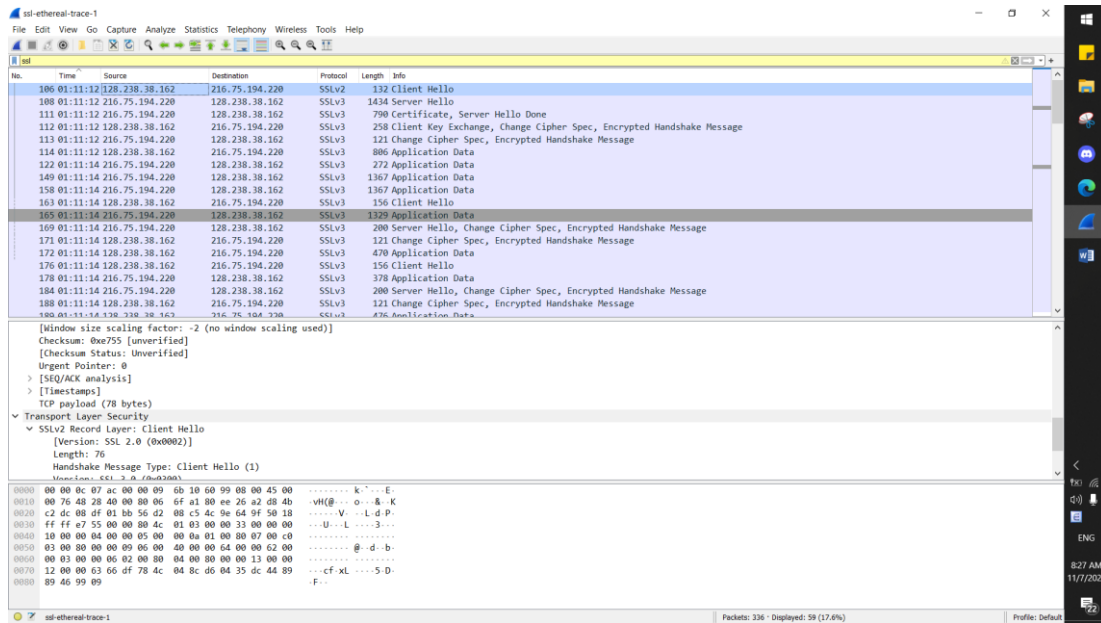
Name: Đinh Hoàng Anh

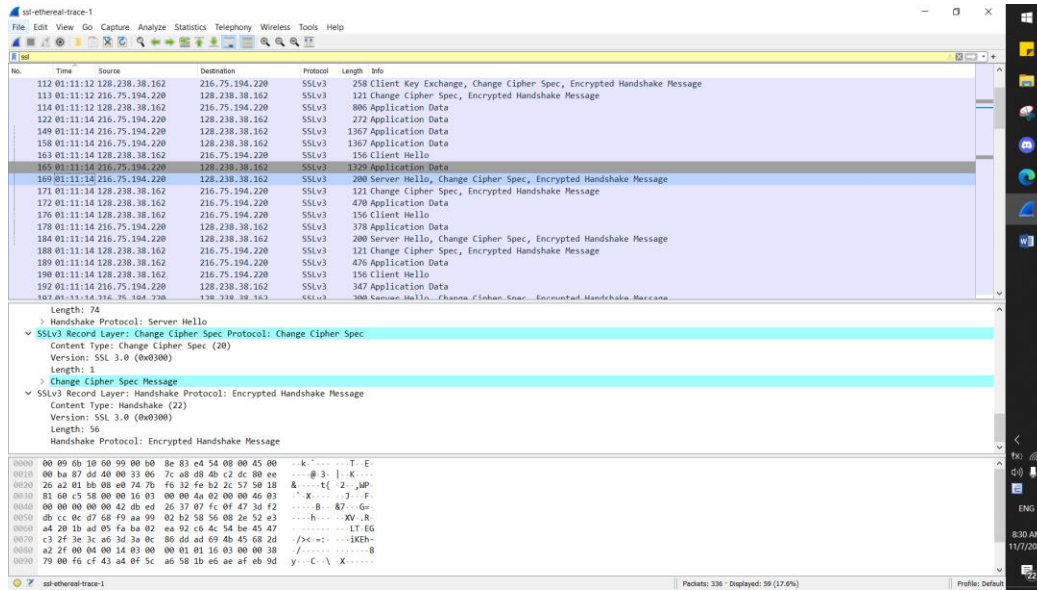
Student ID: 1952553

LAB 8

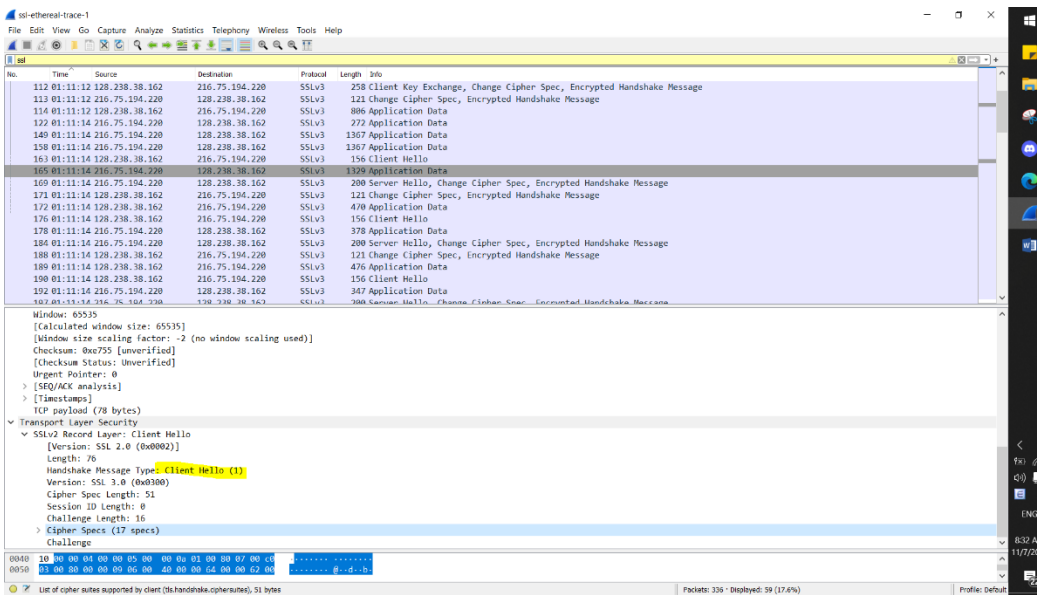
1.

Frame	Source	Destination	SSL Count	SSL Type
106	128.238.38.162	216.75.194.220	1	Client Hello
108	216.75.194.220	128.238.38.162	1	Server Hello
111	216.75.194.220	128.238.38.162	2	Server Hello Done
112	128.238.38.162	216.75.194.220	3	Client Key Exchange
113	216.75.194.220	128.238.38.162	2	Change Cipher Spec
114	128.238.38.162	216.75.194.220	1	Application Data
122	216.75.194.220	128.238.38.162	1	Application Data
149	216.75.194.220	128.238.38.162	1	Application Data





2. Content type : 1 byte Version: 2 bytes Length: 2 bytes



3. The content type is 22, for Handshake Message, with a handshake type of 01, Client Hello

4. 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5. Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

6. Public key algorithm: RSA

Symmetric-key algorithm: RC4

Hash algorithm: MD5

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

- Packet List Pane:** Shows a list of captured packets. The first packet is a Client Hello from 192.168.1.108 to 192.168.1.104. Subsequent packets include Server Hello, Certificate, Key Exchange, Change Cipher Spec, and Application Data.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. The 'Transport Layer Security' section is expanded, showing the 'SSLv3 Record Layer: Handshake Protocol: Server Hello' and 'Handshake Protocol: Server Hello' details. The 'Handshake Type: Server Hello (2)' is selected, showing the 'Session ID Length: 32' and 'Session ID: 1ba09f1aba026a926dc4548e54732f3e3ca63d3ab0c8d6da60456782da22f'.
- Packet Bytes Pane:** Displays the raw packet data in hexadecimal and ASCII format.

The status bar at the bottom indicates 'Packets: 336 / Displayed: 50 (17.6%)' and 'Profile: Default'.

There is no certificate in this record. The certificate is in the separate record. Yes, the certificate is included in the record.
The certificate is included in the record as a single Ethernet frame.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for common actions like opening files, saving, and filtering. The main window is divided into three panes: the packet list, packet details, and packet bytes.

The packet list pane shows a list of captured packets. The selected packet is packet 16, which is an SSL/TLS handshake message. The packet details pane shows the structure of the selected packet, including the Client Key Exchange, Change Cipher Spec, and Encrypted Handshake Message. The packet bytes pane at the bottom shows the raw data of the selected packet, including the SSL/TLS handshake message structure.

The packet details pane for packet 16 shows the following structure:

- SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: SSL 3.0 (0x0300)
 - Length: 132
 - Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 128
 - RSA Encrypted PreMaster Secret
 - Encrypted PreMaster: bc04040729aa2590477f0859056ae78956c77b12ef08047c609e51f104b0bf83e41c08d...
- SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: SSL 3.0 (0x0300)
 - Length: 1
 - Change Cipher Spec Message
- SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
 - Content Type: Handshake (22)
 - Version: SSL 3.0 (0x0300)
 - Length: 56
 - Handshake Protocol: Encrypted Handshake Message

The packet bytes pane shows the raw data of the selected packet, including the SSL/TLS handshake message structure. The data is displayed in hexadecimal and ASCII format.

This secret is used for creating master secret

The secret is encrypted by public key, the encrypted secret is 120 bytes

No.	Time	Source	Destination	Protocol	Length	Info
106	01:11:12.128	216.75.194.220	128.238.38.162	SSLv2	132	Client Hello
108	01:11:12.216	75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	01:11:12.216	75.194.220	128.238.38.162	SSLv3	790	Certificate, Server Hello Done
112	01:11:12.228	238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	01:11:12.216	75.194.220	128.238.38.162	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
114	01:11:12.228	238.38.162	216.75.194.220	SSLv3	886	Application Data
122	01:11:14.216	75.194.220	128.238.38.162	SSLv3	272	Application Data
149	01:11:14.216	75.194.220	128.238.38.162	SSLv3	1367	Application Data
158	01:11:14.216	75.194.220	128.238.38.162	SSLv3	1367	Application Data
163	01:11:14.228	238.38.162	216.75.194.220	SSLv3	156	Client Hello
165	01:11:14.216	75.194.220	128.238.38.162	SSLv3	1329	Application Data
169	01:11:14.216	75.194.220	128.238.38.162	SSLv3	200	Server Hello, Change Cipher Spec, Encrypted Handshake Message
171	01:11:14.228	238.38.162	216.75.194.220	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
172	01:11:14.228	238.38.162	216.75.194.220	SSLv3	470	Application Data
176	01:11:14.228	238.38.162	216.75.194.220	SSLv3	156	Client Hello
178	01:11:14.216	75.194.220	128.238.38.162	SSLv3	378	Application Data
184	01:11:14.216	75.194.220	128.238.38.162	SSLv3	200	Server Hello, Change Cipher Spec, Encrypted Handshake Message
188	01:11:14.228	238.38.162	216.75.194.220	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
189	01:11:14.228	238.38.162	216.75.194.220	SSLv3	470	Application Data

Window: 33120
[Calculated window size: 33120]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x79ac [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
TCP payload (67 bytes)
Transport Layer Security
SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: SSL 3.0 (0x0300)
Length: 1
Change Cipher Spec Message
SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 56
Handshake Protocol: Encrypted Handshake Message

0000 00 09 6b 10 60 99 00 b0 8e 83 e4 54 00 00 45 00 ...k...T.E.
0010 00 6b 87 c1 40 00 33 06 7d 13 d8 4b c2 dc 80 ee ...k: @ 3: }-K...

11. Purpose of the Change Cipher Spec record is: used to indicate the content of the next SSL records will be encrypted. It is 6 bytes.

12. All handshake messages and MAC addresses are concatenated and encrypted. They are sent to the server

13. Yes, the server also send a change cipher record and an encrypted handshake

15. No comment