

Nama: Ridwan ariana

Nim: 09031181520019

Kelas: SI4A

Dosen pembimbing: Deris stiawan,Ph.D

Tugas wireshark(analisis situs dengan wireshark)

1.Facebook.com

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : hotspot-id1.ilkom.unsri.ac.id
Link-local IPv6 Address . . . . . : fe80::91c7:6e24:f2f7:48ff%14
IPv4 Address. . . . . : 10.102.225.115
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 10.102.224.1

Tunnel adapter isatap.hotspot-id1.ilkom.unsri.ac.id:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : hotspot-id1.ilkom.unsri.ac.id
```

Gambar diatas merupakan sebuah ip.address dan mac address dari source(pc) yg sedang digunakan.

The screenshot displays the Wireshark interface with the following details:

- Filter:** ssl
- Packet List:** Shows a list of captured packets. Packet 593 is highlighted, showing a TLSv1.2 Client Hello from source 10.102.225.115 to destination 204.79.197.213.
- Packet Details:** Shows the structure of the selected packet:
 - Ethernet II, Src: Azurewav_97:12:fb (40:e2:30:97:12:fb), Dst: Dell_44:8a:74 (00:1e:c9:44:8a:74)
 - Internet Protocol Version 4, Src: 10.102.225.115, Dst: 204.79.197.213
 - Transmission Control Protocol, Src Port: 50630, Dst Port: 443, Seq: 201, Ack: 7642, Len: 214
 - Secure Sockets Layer
- Packet Bytes:** Shows the raw hex and ASCII data of the captured packet, including the TLS Client Hello structure.

Dari gambar diatas didapatkan sebuah pertukaran ip(handshake) dari situs facebook.com

Frame 593: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0	
Ethernet II, Src: Azurewav_97:12:fb (40:e2:30:97:12:fb), Dst: Dell_44:8a:74 (00:1e:c9:44:8a:74)	
Internet Protocol Version 4, Src: 10.102.225.115, Dst: 204.79.197.213	
Transmission Control Protocol, Src Port: 50630, Dst Port: 443, Seq: 201, Ack: 7642, Len: 214	
Secure Sockets Layer	
0000	00 1e c9 44 8a 74 40 e2 30 97 12 fb 08 00 45 00 ...D.t@. 0.....E.
0010	00 fe 34 f9 40 00 80 06 47 02 0a 66 e1 73 cc 4f ..4.@... G..f..s.O
0020	c5 d5 c5 c6 01 bb 0e e4 e2 74 10 ff 2f 37 50 18t../P.
0030	00 40 35 a5 00 00 16 03 03 00 66 10 00 00 62 61 .@5......f...ba
0040	04 c7 e6 9d dd 0a ad d5 7d 08 31 e7 da eb 68 fa}.1...h.
0050	b2 27 4e c0 0e 72 a3 a3 4e 2a c7 de 29 21 48 3b .'N..r.. N*..)!H;
0060	db c5 78 b3 f0 0d 0d ec 03 b2 d2 63 f9 da 52 84 ..x..... .C..R.
0070	38 a1 3a f5 55 f6 76 51 27 49 c0 11 a8 91 d5 b6 8.:.U.vQ 'I.....
0080	d4 c8 71 96 e9 ed 5f 3e 2d 62 e9 1d 5a 1e df 83 ..q...> -b..Z...
0090	70 a5 26 0e 2c d6 9e fc c2 43 0c aa 33 0a fa bf p.&..... .C..3...
00a0	e6 14 03 03 00 01 01 16 03 03 00 60 hc 52 ed a2C..R..

Jika dilihat dari gambar diatas terdapat beberapa ip beserta mac address dan port dari si source to si destination.

Berikut ip dan mac serta port yang didapat dari capture wireshark:

-ip

Source:10.102.225.15

Destination:204.79.197.213

-mac address

Source= 40:e2:30:97:12:fb

Destination= 00:1e:c9:44:8a:74

-port

Source:50630

Destination:443

```

Tracing route to facebook.com [157.240.13.35]
over a maximum of 30 hops:

  1      3 ms      4 ms      4 ms    192.168.43.1
  2      *          *          *       Request timed out.
  3      *          *          *       Request timed out.
  4      *          *          *       Request timed out.
  5    2521 ms    1984 ms    715 ms   118.98.84.113
  6     738 ms     723 ms    388 ms   188.240.193.158
  7     45 ms      44 ms     44 ms   188.240.193.157
  8     58 ms      44 ms     53 ms   188.240.204.65
  9    1720 ms    1790 ms    1674 ms  103.4.98.92
 10     *          *          1031 ms  157.240.41.36
 11    118 ms     61 ms     *       157.240.32.49
 12     62 ms     52 ms     50 ms   173.252.67.215
 13     49 ms     49 ms     48 ms   157.240.13.35

Trace complete.

```

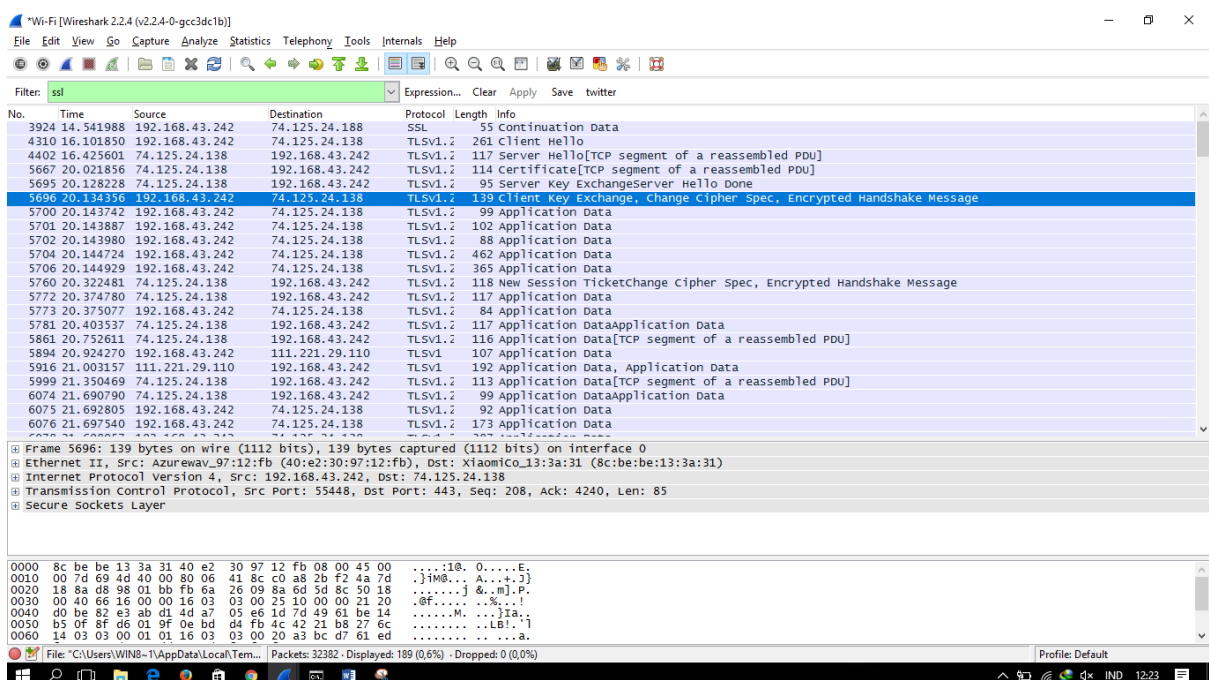
Dan saat di tracing (facebook.com) terdapat 13 loop dari source to destination.

note: tanda "" merupakan request timed out/jaringan tidak stabil

2.gmail.com

```
Wireless LAN adapter Wi-Fi:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::91c7:6e24:f2f7:48ff%14  
IPv4 Address. . . . . : 192.168.43.242  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.43.1
```

Gambar diatas merupakan ip dan mac address dari pc yg sedang dipakai.



Dari gambar diatas didapatkan sebuah pertukaran ip(handshake) dari situs gmail.com

```
Frame 5696: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0  
Ethernet II, Src: Azurewav_97:12:fb (40:e2:30:97:12:fb), Dst: xiaomiCo_13:3a:31 (8c:be:be:13:3a:31)  
Internet Protocol Version 4, Src: 192.168.43.242, Dst: 74.125.24.138  
Transmission Control Protocol, Src Port: 55448, Dst Port: 443, Seq: 208, Ack: 4240, Len: 85  
Secure Sockets Layer
```

```
0000 8c be be 13 3a 31 40 e2 30 97 12 fb 08 00 45 00 .....1@. 0.....E.  
0010 00 7d 69 4d 40 00 80 06 41 8c c0 a8 2b f2 4a 7d .}iM@... A...+J}  
0020 18 8a d8 98 01 bb fb 6a 26 09 8a 6d 5d 8c 50 18 .....j &..m].P.  
0030 00 40 66 16 00 00 16 03 03 00 25 10 00 00 21 20 .@f.....%...!  
0040 d0 be 82 e3 ab d1 4d a7 05 e6 1d 7d 49 61 be 14 .....M. ...}Ia..  
0050 b5 0f 8f d6 01 9f 0e bd d4 fb 4c 42 21 b8 27 6c ..... ..LB!..'  
0060 14 03 03 00 01 01 16 03 03 00 20 a3 bc d7 61 ed ..... ..a.
```

Jika dilihat dari gambar diatas terdapat beberapa ip beserta mac address dan port dari si source to si destination.

Berikut ip dan mac serta port yang didapat dari capture wireshark:

- ip
- Source:192.168.43.242
- Destination:74.125.24.138

-mac address
 Source= 40:e2:30:97:12:fb
 Destination= 8c:be:be:13:3a:31
 -port
 Source:55448
 Destination:443

```
Tracing route to gmail.com [74.125.200.19]
over a maximum of 30 hops:

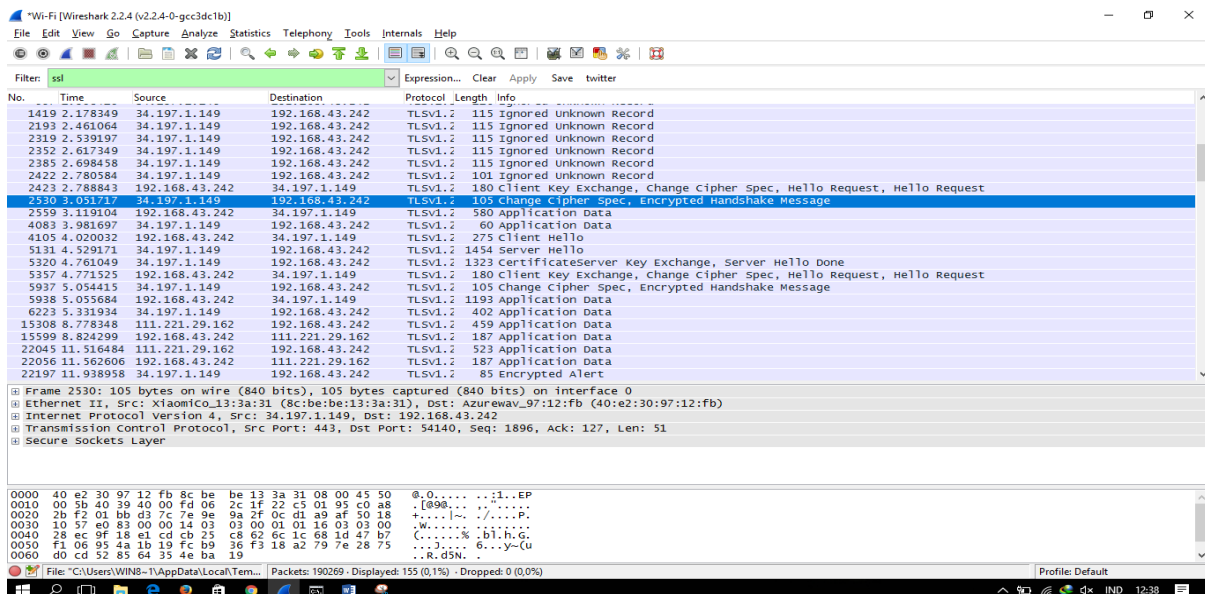
  0  3 ms    3 ms    3 ms    192.168.43.1
  1  *        *        *        Request timed out.
  2  *        *        *        Request timed out.
  3  *        *        *        Request timed out.
  4  *        *        *        Request timed out.
  5  44 ms   45 ms   41 ms   118.98.84.113
  6  55 ms   43 ms   51 ms   180.240.193.158
  7  58 ms   49 ms   48 ms   180.240.193.157
  8  49 ms   94 ms   45 ms   180.240.204.65
  9  48 ms   50 ms   44 ms   72.14.223.88
 10  87 ms   50 ms   59 ms   108.170.242.66
 11  49 ms   53 ms   64 ms   209.85.243.241
 12  75 ms   67 ms   166 ms  216.239.51.57
 13  *        *        *        Request timed out.
 14  *        *        *        Request timed out.
 15  *        *        *        Request timed out.
 16  *        *        *        Request timed out.
 17  *        *        *        Request timed out.
 18  *        *        *        Request timed out.
 19  *        *        *        Request timed out.
 20  *        *        *        Request timed out.
 21  43 ms   51 ms   67 ms   74.125.200.19

Trace complete.
```

Dan saat di tracing (gmail.com) terdapat 21 loop dari source to destination.

note: tanda "" merupakan request timed out/jaringan tidak stabil

3.stafabanddl.info



Gambar diatas merupakan pertukaran ip(handshake) dari situs stafabanddl.info

```

[+] Frame 2530: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
[+] Ethernet II, Src: XiaomiCo_13:3a:31 (8c:be:be:13:3a:31), Dst: Azurewav_97:12:fb (40:e2:30:97:12:fb)
[+] Internet Protocol Version 4, Src: 34.197.1.149, Dst: 192.168.43.242
[+] Transmission Control Protocol, Src Port: 443, Dst Port: 54140, Seq: 1896, Ack: 127, Len: 51
[+] Secure Sockets Layer

0000  40 e2 30 97 12 fb 8c be  be 13 3a 31 08 00 45 50  @.0..... :1..EP
0010  00 5b 40 39 40 00 fd 06  2c 1f 22 c5 01 95 c0 a8  .[@9@... ;".....
0020  2b f2 01 bb d3 7c 7e 9e  9a 2f 0c d1 a9 af 50 18  +...]|~. ./...P.
0030  10 57 e0 83 00 00 14 03  03 00 01 01 16 03 03 00  .w..... .....
0040  28 ec 9f 18 e1 cd cb 25  c8 62 6c 1c 68 1d 47 b7  (. ....% .bl.h.G.
0050  f1 06 95 4a 1b 19 fc b9  36 f3 18 a2 79 7e 28 75  ...J.... 6...y~(u
0060  d0 cd 52 85 64 35 4e ba  19                               ..R.d5N. .

```

Jika dilihat dari gambar diatas terdapat beberapa ip beserta mac address dan port dari si source to si destination.

Berikut ip dan mac serta port yang didapat dari capture wireshark:

- ip
- Source:34.197.1.149
- Destination:192.168.43.242
- mac address
- Source= 8c:be:be:13:3a:31
- Destination= 40:e2:30:97:12:fb
- port
- Source:55448
- Destination:443

```

Tracing route to 5.189.172.21 over a maximum of 30 hops

 1    5 ms     3 ms     3 ms    192.168.43.1
 2    *         *         *       Request timed out.
 3    *         *         *       Request timed out.
 4    *         *         *       Request timed out.
 5   40 ms    33 ms    31 ms    118.98.94.169
 6   47 ms    42 ms    43 ms    180.240.193.158
 7   38 ms    38 ms    36 ms    180.240.193.157
 8  252 ms   252 ms   280 ms    180.240.192.146
 9  222 ms   213 ms   211 ms    80.81.194.0
10  213 ms   213 ms   223 ms    5.189.172.21

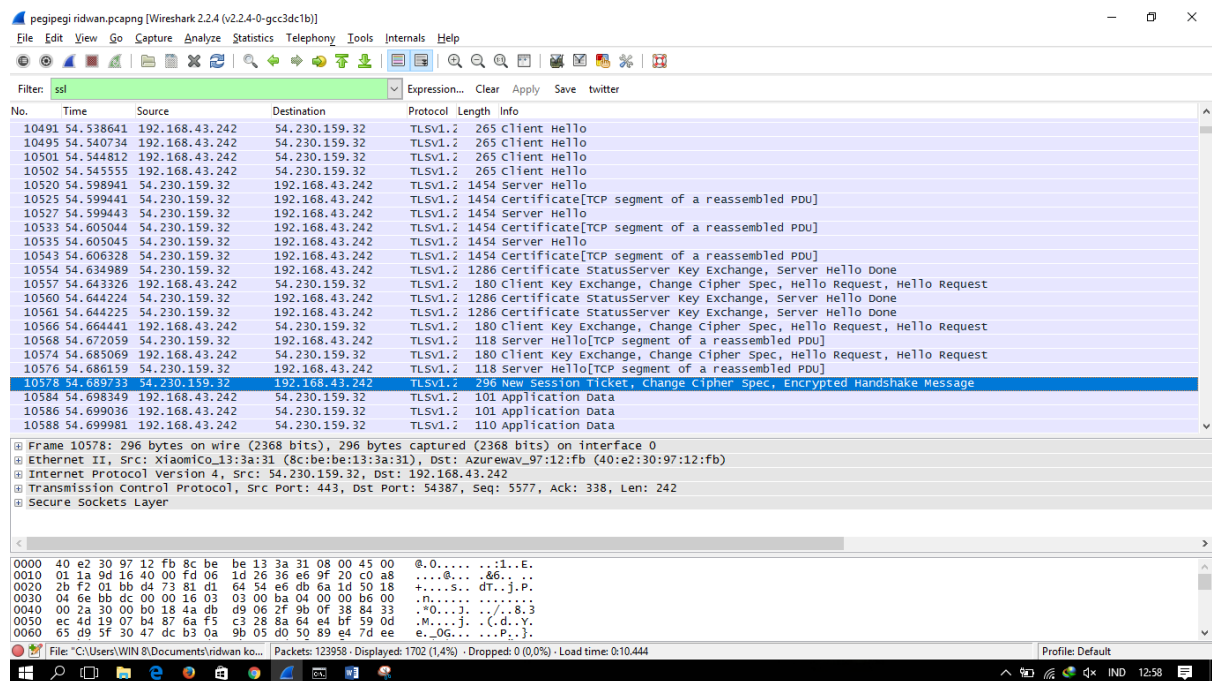
Trace complete.

```

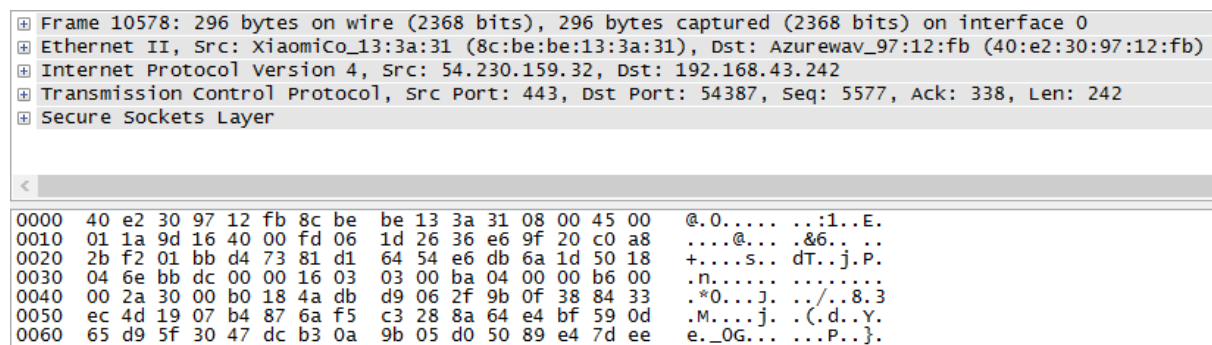
Dan saat di tracing (stafabanddl.info) terdapat 10 loop dari source to destination.

note: tanda "" merupakan request timed out/jaringan tidak stabil

4. pegipegi.com



Gambar diatas merupakan pertukaran ip(handshake) dari situs pegipegi.com



Jika dilihat dari gambar diatas terdapat beberapa ip beserta mac address dan port dari si source to si destination.

Berikut ip dan mac serta port yang didapat dari capture wireshark:

-ip

Source:54.230.159.32

Destination:192.168.43.242

-mac address

Source= 8c:be:be:13:3a:31

Destination= 40:e2:30:97:12:fb

-port

Source:443

Destination:54387

Kesimpulan:

Kesimpulan yang didapat dari menggunakan wireshark adalah bahwa kita dapat melacak http,tcp,ssl,dll. Kita juga dapat melakukan sniffing postingan dan user/password(jika bukan https).

Dan juga dapat melihat kegiatan pengiriman paket dari source ke destination serta pertukaran data ip/handshake antar ip.