

NIM : 09031181520029

Nama : Dwi Zulia Lestari

Kelas : SIREG 4A

## Jaringan Komputer dan Komunikasi Data

Untuk melakukan analisis ini saya menggunakan 2 website internasional, yaitu [www.twitter.com](http://www.twitter.com) dan [www.instagram.com](http://www.instagram.com) kemudian 2 website nasional, yaitu [www.rcti.tv](http://www.rcti.tv) dan [www.globaltv.co.id](http://www.globaltv.co.id)

### 1. www.twitter.com

#### Analisis IP address

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . . . :
Link-local IPv6 Address . . . . . : fe80::f8b0:1b6f:c67f:bae5%6
IPv4 Address. . . . . : 192.168.43.81
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1
```

1287	28.637857	192.168.43.81	74.125.130.94	QUIC	305 Payload (Encrypted), PKN: 194, CID: 17145640863031176040
1288	28.660857	192.168.43.1	192.168.43.81	DNS	103 Standard query response 0x3509 A twitter.com A 104.244.42.193 A 104.244.42.65
1289	28.662470	192.168.43.81	104.244.42.65	TCP	66 59291 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1290	28.662832	192.168.43.81	104.244.42.65	TCP	66 59292 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1291	28.759141	104.244.42.65	192.168.43.81	TCP	66 443 → 59291 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=256
1292	28.759251	192.168.43.81	104.244.42.65	TCP	54 59291 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
1293	28.759522	192.168.43.81	104.244.42.65	TLSV1.2	257 Client Hello
1294	28.826893	74.125.130.94	192.168.43.81	QUIC	511 Payload (Encrypted), PKN: 338
1295	28.826894	74.125.130.94	192.168.43.81	QUIC	71 Payload (Encrypted), PKN: 339
1296	28.826894	104.244.42.65	192.168.43.81	TCP	66 443 → 59292 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=256

```
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differenziated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x3143 (12611)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x4a52 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.43.81
Destination: 104.244.42.65
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 59291, Dst Port: 443, Seq: 0, Len: 0
```

Pada gambar diatas tertera bahwa IP address source ialah **192.168.43.81** dan IP address destinationnya ialah **104.244.42.65** yang menunjukkan bahwa destinationnya sudah ke [www.twitter.com](http://www.twitter.com). Kemudian untuk port dari source ialah 59291 dan port dari destinationnya ialah 443.

## Analisis handshake www.twitter.com

The image shows a Wireshark packet capture for a TLS handshake to www.twitter.com. The source IP is 117.18.237.70 and the destination IP is 192.168.43.81. The destination port is 443. The handshake includes a ClientHello (seq=296) and a ServerHello (seq=296). The ClientHello contains a TLS version of 1.2, a random value, and a session ID. The ServerHello contains a TLS version of 1.2, a random value, a session ID, and a cipher suite of TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256. The handshake concludes with a ChangeCipherSpec (seq=296) and an EncryptedHandshakeMessage (seq=296).

No.	Time	Source	Destination	Protocol	Length	Info
28308	473.043541	104.244.42.1	192.168.43.81	TCP	66	[TCP Dup ACK 28028#2] 443 → 59593 [ACK] Seq=2912 Ack=204 Win=30464 Len=0 SLE=1 SRE=1
28309	473.043542	117.18.237.70	192.168.43.81	TCP	54	443 → 59599 [ACK] Seq=5501 Ack=644 Win=147456 Len=0
28310	473.043543	117.18.237.70	192.168.43.81	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
28311	473.043626	192.168.43.81	104.244.46.199	TCP	66	[TCP Dup ACK 28002#1] 59604 → 443 [ACK] Seq=206 Ack=1 Win=65792 Len=0 SLE=0 SRE=1
28312	473.055941	117.18.237.70	192.168.43.81	TCP	1454	[TCP segment of a reassembled PDU]
28313	473.061574	117.18.237.70	192.168.43.81	TCP	1454	[TCP segment of a reassembled PDU]
28314	473.064651	117.18.237.70	192.168.43.81	TLSv1.2	131	Application Data
28315	473.064740	192.168.43.81	117.18.237.70	TCP	54	59596 → 443 [ACK] Seq=1092 Ack=24264 Win=65792 Len=0
28316	473.065046	117.18.237.70	192.168.43.81	TCP	1454	[TCP segment of a reassembled PDU]

Internet Protocol Version 4, Src: 117.18.237.70, Dst: 192.168.43.81

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 282
- Identification: 0x9998 (39320)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 58
- Protocol: TCP (6)
- Header checksum: 0x57f3 [validation disabled]
- [Header checksum status: unverified]
- Source: 117.18.237.70
- Destination: 192.168.43.81
- [Source GeoIP: unknown]
- [Destination GeoIP: unknown]

Pada gambar diatas tertera bahwa IP Source nya ialah **117.18.237.70** dan Port sourcenya 443, kemudian IP Destination nya **192.168.43.81** dan Port Destinationnya 59616

## 2. [www.instagram.com](http://www.instagram.com)

### Analisis IP Address [www.instagram.com](http://www.instagram.com)

```
Wireless LAN adapter Wi-Fi:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::f8b0:1b6f:c67f:bae5%6  
IPv4 Address. . . . . : 192.168.43.81  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.43.1
```

The image shows a Wireshark packet capture for a TLS handshake to www.instagram.com. The source IP is 117.18.237.70 and the destination IP is 192.168.43.81. The destination port is 443. The handshake includes a ClientHello (seq=296) and a ServerHello (seq=296). The ClientHello contains a TLS version of 1.2, a random value, and a session ID. The ServerHello contains a TLS version of 1.2, a random value, a session ID, and a cipher suite of TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256. The handshake concludes with a ChangeCipherSpec (seq=296) and an EncryptedHandshakeMessage (seq=296).

No.	Time	Source	Destination	Protocol	Length	Info
2113	39.929881	112.215.101.165	192.168.43.81	QUIC	86	Payload (Encrypted), PKN: 18, CID: 11284053984511839461
2114	39.930122	112.215.184.46	192.168.43.81	QUIC	77	Payload (Encrypted), PKN: 26, CID: 14782572892700242045
2115	39.930123	112.215.101.165	192.168.43.81	TCP	349	[TCP Spurious Retransmission] 443 → 59677 [PSH, ACK] Seq=3449 Ack=208 Win=30336 Len=295[Reassembly]
2116	39.930256	192.168.43.81	112.215.101.165	TCP	66	[TCP Dup ACK 2091#1] 59677 → 443 [ACK] Seq=617 Ack=3744 Win=65792 Len=0 SLE=3449 SRE=3744
2117	39.933270	192.168.43.1	192.168.43.81	DNS	155	Standard query response 0xf0e2 A www.instagram.com CNAME black.ish.instagram.com CNAME instagram.c
2118	39.933275	192.168.43.81	157.240.2.52	TCP	66	[TCP Dup ACK 2091#1] 59677 → 443 [ACK] Seq=617 Ack=3744 Win=65792 Len=0 MSS=1460 WS=256 SACK_PERM=1
2119	39.975014	112.215.101.165	192.168.43.81	TCP	54	443 → 59677 [ACK] Seq=3744 Ack=519 Win=31360 Len=0
2120	39.975017	112.215.101.165	192.168.43.81	TCP	54	443 → 59677 [ACK] Seq=3744 Ack=617 Win=31360 Len=0
2121	39.987803	192.168.43.81	157.240.7.52	TCP	66	59680 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2122	39.989802	112.215.101.165	192.168.43.81	TLSv1.2	348	New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
2123	39.990003	112.215.101.165	192.168.43.81	TLSv1.2	152	Application Data, Application Data
2124	39.990078	192.168.43.81	112.215.101.165	TCP	54	59677 → 443 [ACK] Seq=617 Ack=4136 Win=65280 Len=0
2125	39.990785	192.168.43.81	112.215.101.165	TLSv1.2	92	Application Data
2126	39.997705	112.215.101.165	192.168.43.81	TLSv1.2	92	Application Data

0100 .... = Version: 4

- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52
- Identification: 0x4275 (17013)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x2731 [validation disabled]
- [Header checksum status: unverified]
- Source: 192.168.43.81
- Destination: 157.240.7.52
- [Source GeoIP: unknown]
- [Destination GeoIP: unknown]

Transmission Control Protocol, Src Port: 59679, Dst Port: 443, Seq: 0, Len: 0

Pada gambar diatas tertera bahwa IP address source ialah **192.168.43.81** dan IP address destinationnya ialah **157.240.2.52** yang menunjukkan bahwa destinationnya sudah ke [www.instagram.com](http://www.instagram.com). Kemudian untuk port dari source ialah 59679 dan port dari destinationnya ialah 443.

## Analisis Handshake www.instagram.com

instagram.pcapng [Wireshark 2.2.4 (v2.2.4-0-gcc3dc1b)]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
15805	324.180724	112.215.158.32	192.168.43.81	TLV1.2	1454	Ignored unknown Record
15806	324.180814	192.168.43.81	112.215.158.32	TCP	54	59759 → 443 [ACK] Seq=22869 Ack=4572700 win=187392 Len=0
15807	324.202702	112.215.158.32	192.168.43.81	TLV1.2	1454	Ignored unknown Record
15808	324.252736	192.168.43.81	112.215.158.32	TCP	54	59759 → 443 [ACK] Seq=22869 Ack=4574100 win=186112 Len=0
15809	324.266720	157.240.12.52	192.168.43.81	TLV1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
15810	324.266954	157.240.12.52	192.168.43.81	TLV1.2	135	Application Data
15811	324.267038	192.168.43.81	157.240.12.52	TCP	54	59793 → 443 [ACK] Seq=808 Ack=4166 win=64256 Len=0
15812	324.267686	192.168.43.81	157.240.12.52	TLV1.2	92	Application Data
15813	324.289767	112.215.158.32	192.168.43.81	TLV1.2	1454	Ignored unknown Record
15814	324.310440	112.215.158.32	192.168.43.81	TLV1.2	1454	Ignored unknown Record
15815	324.310529	192.168.43.81	112.215.158.32	TCP	54	59759 → 443 [ACK] Seq=22869 Ack=4576900 win=183296 Len=0
15816	324.330967	112.215.158.32	192.168.43.81	TLV1.2	1454	Ignored unknown Record
15817	324.349951	112.215.158.32	192.168.43.81	TCP	1454	[TCP segment of a reassembled PDU]
15818	324.350054	192.168.43.81	112.215.158.32	TCP	54	59759 → 443 [ACK] Seq=22869 Ack=4579700 win=180480 Len=0

Internet Protocol Version 4, Src: 157.240.12.52, Dst: 192.168.43.81

0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 314  
 Identification: 0x4e05 (19973)  
 Flags: 0x02 (Don't Fragment)  
 Fragment offset: 0  
 Time to live: 82  
 Protocol: TCP (6)  
 Header checksum: 0x439b [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 157.240.12.52  
 Destination: 192.168.43.81  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]

0000 80 a5 89 45 af f8 20 5e f7 02 4f 28 08 00 45 00 ...E..A..O(C..E  
 0010 01 3a 4e 05 40 00 52 06 43 9b 9d f0 0c 34 c0 a8 ...N.B.R. C...4.  
 0020 0b 31 01 0b e9 01 09 06 71 78 7d 1d 62 c1 90 18 ...Q.....92...P.  
 0030 00 73 a1 b7 00 00 16 03 03 00 da 04 00 00 de 00 ...S.....  
 0040 02 a3 00 00 00 04 de b7 71 e7 e8 14 b8 6b 64 aa .....N..q...kd.  
 0050 14 1b 7f 14 15 1b 7f 14 15 1b 7f 14 15 1b 7f ...

Frame (frame), 328 bytes | Packets: 17611 | Displayed: 17611 (100.0%) | Load time: 0:01:503 | Profile: Default

Pada gambar diatas tertera bahwa IP Source nya ialah **157.240.12.52** dan Port sourcenya 443, kemudian IP Destination nya **192.168.43.81** dan Port Destinationnya 59793

### 3. [www.rcti.tv](http://www.rcti.tv)

#### Analisis IP Address

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::f8b0:1b6f:c67f:bae5%6
IPv4 Address. . . . . : 192.168.43.81
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1
    
```

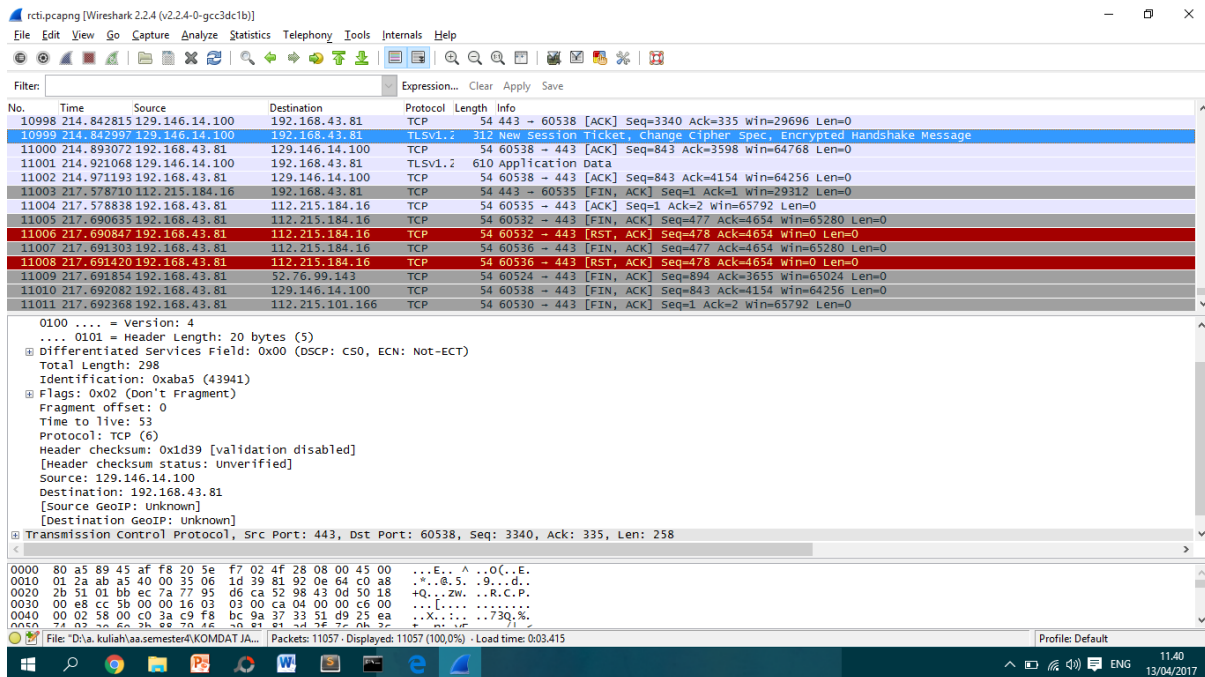
No.	Time	Source	Destination	Protocol	Length	Info
167	9.055868	192.168.43.81	74.125.200.94	QUIC	77	Payload (Encrypted), PKN: 45, CID: 14971001942602516043
168	9.305544	112.215.88.38	192.168.43.81	QUIC	78	Payload (Encrypted), PKN: 16, CID: 2350174736658424803
169	9.305778	192.168.43.81	112.215.88.38	QUIC	80	Payload (Encrypted), PKN: 11, CID: 2350174736658424803
170	9.310482	192.168.43.81	202.80.220.250	TCP	66	60377 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
171	9.311043	192.168.43.81	202.80.220.250	TCP	66	60378 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
172	9.311366	192.168.43.81	202.80.220.250	TCP	66	60379 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
173	9.312061	192.168.43.81	202.80.220.250	TCP	66	60380 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
174	9.313099	192.168.43.81	202.80.220.250	TCP	66	60381 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
175	9.313598	192.168.43.81	202.80.220.250	TCP	66	60382 → 80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
176	9.322180	192.168.43.81	112.215.101.165	QUIC	1392	Client Hello, PKN: 1, CID: 2982208697370484689
177	9.405706	202.80.220.250	192.168.43.81	TCP	66	80 → 60377 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1400 WS=128 SACK_PERM=1
178	9.405808	192.168.43.81	202.80.220.250	TCP	54	60377 → 80 [ACK] Seq=1 Ack=1 win=65792 Len=0
179	9.421374	202.80.220.250	192.168.43.81	TCP	66	80 → 60378 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1400 WS=128 SACK_PERM=1
180	9.421481	192.168.43.81	202.80.220.250	TCP	54	60378 → 80 [ACK] Seq=1 Ack=1 win=65792 Len=0

0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 52  
 Identification: 0x00f5 (245)  
 Flags: 0x02 (Don't Fragment)  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)  
 Header checksum: 0x668a [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.43.81  
 Destination: 202.80.220.250  
 [Source GeoIP: Unknown]  
 [Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 60377, Dst Port: 80, Seq: 0, Len: 0

Pada gambar diatas tertera bahwa IP address source ialah **192.168.43.81** dan IP address destinationnya ialah **202.80.220.250** yang menunjukkan bahwa destinationnya sudah ke **www.rcti.tv** . Kemudian untuk port dari source ialah 60377 dan port dari destinationnya ialah 80

#### Analisis Handshake [www.rcti.tv](http://www.rcti.tv)



Pada gambar diatas tertera bahwa IP Source nya ialah **129.146.43.81** dan Port sourcenya 443, kemudian IP Destination nya **192.168.43.81** dan Port Destinationnya 60538

#### 4. [www.globaltv.co.id](http://www.globaltv.co.id)

#### Analisis IP Address [www.globaltv.co.id](http://www.globaltv.co.id)

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : hotspot-id1.ilkom.unsri.ac.id
Link-local IPv6 Address . . . . . : fe80::f8b0:1b6f:c67f:bae5%6
IPv4 Address. . . . . : 10.100.226.162
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 10.100.224.1
    
```

No.	Time	Source	Destination	Protocol	Length	Info
4	0.022847	fe80::f98b:d99d:e1:ff02::c	ff02::c	UDP	686	50437 → 3702 Len=624
5	0.022850	10.102.226.3	10.102.239.255	BROWSEF	216	Get Backup List Request
6	0.022851	10.102.226.3	10.102.239.255	NBNS	92	Name query NB WORKGROUP<1b>
7	0.022852	10.102.226.3	10.102.239.255	NBNS	92	Name query NB WORKGROUP<1c>
8	0.023610	fe80::f98b:d99d:e1:ff02::c	ff02::c	UDP	686	50437 → 3702 Len=624
9	0.024541	10.102.226.3	239.255.255.250	UDP	666	50436 → 3702 Len=624
10	0.049470	202.80.220.28	10.102.224.182	TCP	1514	[TCP segment of a reassembled PDU]
11	0.049565	10.102.224.182	202.80.220.28	TCP	66	61818 → 80 [ACK] Seq=1 Ack=1461 win=256 Len=0 SLE=2921 SRE=11681
12	0.109890	202.80.220.28	10.102.224.182	TCP	1514	80 → 61798 [ACK] Seq=1 Ack=1 win=126 Len=1460
13	0.109994	10.102.224.182	202.80.220.28	TCP	74	61798 → 80 [ACK] Seq=1 Ack=1461 win=256 Len=0 SLE=10221 SRE=13141 SLE=5841 SRE=7301
14	0.120485	Guangdon_6d:db:d8	Broadcast	ARP	42	who has 10.100.224.1? Tell 10.100.225.115
15	0.165560	202.80.220.28	10.102.224.182	TCP	1514	80 → 61798 [ACK] Seq=1461 Ack=1 win=126 Len=1460
16	0.165668	10.102.224.182	202.80.220.28	TCP	74	61798 → 80 [ACK] Seq=1 Ack=2921 win=256 Len=0 SLE=10221 SRE=13141 SLE=5841 SRE=7301
17	0.220120	202.80.220.28	10.102.224.182	TCP	1514	80 → 61798 [ACK] Seq=2921 Ack=1 win=126 Len=1460

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
[ ] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x294e (10574)
[ ] Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x3fec [validation disabled]
[Header checksum status: unverified]
Source: 10.102.224.182
Destination: 202.80.220.28
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[ ] Transmission Control Protocol, Src Port: 61818, Dst Port: 80, Seq: 1, Ack: 1461, Len: 0

```

Pada gambar diatas tertera bahwa IP address source ialah **10.102.224.182** dan IP address destinationnya ialah **202.80.220.28** yang menunjukkan bahwa destinationnya sudah ke [www.globaltv.co.id](http://www.globaltv.co.id) . Kemudian untuk port dari source ialah 61818 dan port dari destinationnya ialah 80.

#### Handshake [www.globaltv.co.id](http://www.globaltv.co.id)

No.	Time	Source	Destination	Protocol	Length	Info
13769	172.365679	fe80::c1aa:948:8fe2:ff02::fb	ff02::fb	MDNS	74	Standard query response 0x0000
13770	172.367353	XiaomiCo_52:26:a6	Broadcast	ARP	60	who has 10.102.225.238? Tell 10.102.225.103
13771	172.367357	fe80::1db4:cee9:ed3:ff02::1:3	ff02::1:3	LLMNR	90	Standard query 0xe02a A ANGINA-PC
13772	172.367358	10.102.226.16	224.0.0.252	LLMNR	70	Standard query 0xe02a A ANGINA-PC
13773	172.435150	104.244.42.72	10.102.224.182	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
13774	172.440467	10.102.224.182	74.125.24.155	QUIC	1392	Client Hello, PKN: 1, CID: 16608210003507106074
13775	172.442466	10.102.224.182	74.125.24.155	QUIC	437	Payload (Encrypted), PKN: 2, CID: 16608210003507106074
13776	172.445606	10.102.224.182	216.58.196.110	TLSv1.2	505	Application Data
13777	172.463464	XiaomiCo_52:26:a6	Broadcast	ARP	60	who has 10.102.225.204? Tell 10.102.225.103
13778	172.463466	XiaomiCo_52:26:a6	Broadcast	ARP	60	who has 10.102.225.203? Tell 10.102.225.103
13779	172.464670	XiaomiCo_52:26:a6	Broadcast	ARP	60	who has 10.102.225.202? Tell 10.102.225.103
13780	172.464671	XiaomiCo_52:26:a6	Broadcast	ARP	60	who has 10.102.225.135? Tell 10.102.225.103
13781	172.464677	10.102.224.50	224.0.0.251	MDNS	54	Standard query response 0x0000
13782	172.465796	fe80::2976:65f8:f5b:ff02::fb	ff02::fb	MDNS	74	Standard query response 0x0000

```

.... 0101 = Header Length: 20 bytes (5)
[ ] Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 282
Identification: 0xbc72 (48242)
[ ] Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 48
Protocol: TCP (6)
Header checksum: 0x0f13 [validation disabled]
[Header checksum status: Unverified]
Source: 104.244.42.72
Destination: 10.102.224.182
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[ ] Transmission Control Protocol, Src Port: 443, Dst Port: 61911, Seq: 3142, Ack: 342, Len: 242
[ ] Secure Sockets Layer

```

Pada gambar diatas tertera bahwa IP Source nya ialah **104.244.42.72** dan Port sourcenya 443, kemudian IP Destination nya **10.102.224.182** dan Port Destinationnya 61911.