

Nama: Villia Putriany
NIM: 09031381419103
Kelas: Sibil 4A

Analisis Packets dengan aplikasi Wireshark

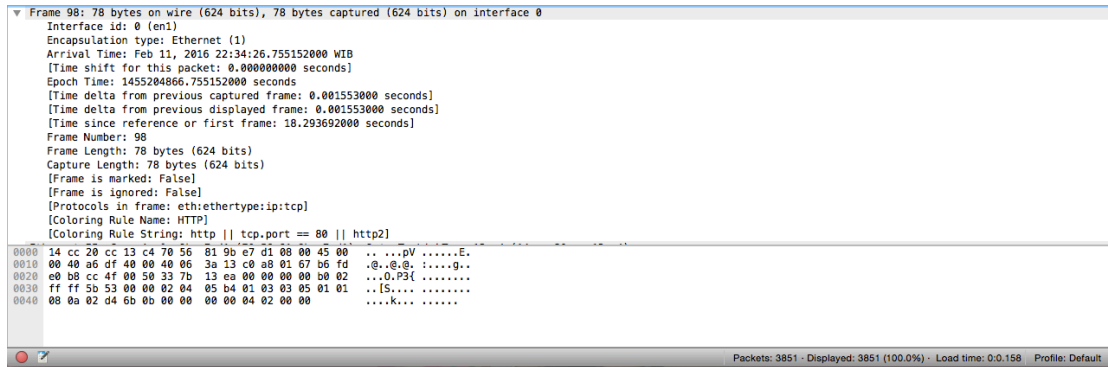
WIRESHARK adalah satu dari sekian banyak tool Network Analyzer yang dipakai oleh orang – orang yang bekerja di bidang jaringan yang ingin melihat atau menganalisa paket jaringan, pengembangan protokol jaringan serta edukasi bagi yang ingin memperdalam ilmu nya dalam jaringan komputer.

Aplikasi ini juga dapat menangkap paket-paket data/informasi yang ada dalam jaringan yang kita ingin lihat. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Kali ini saya akan menganalisa packet protocol yang ter-capture saat membuka situs website Tokopedia (tokopedia.com).

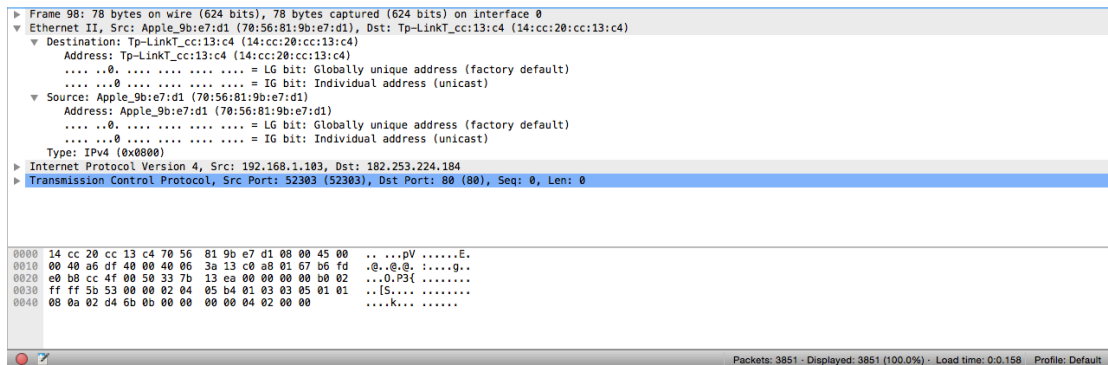
The screenshot shows the Wireshark interface with a list of captured packets. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a status bar at the bottom indicating 'Packets: 3851 - Displayed: 3851 (100.0%) - Load time: 0:0.158 - Profile: Default'. The packet list pane shows various protocols including TCP, UDP, TLSv1.2, IGMPv2, and RTPv2. Packet 98 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP). The packet bytes pane shows the raw hex and ASCII data for the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
83	18.	192.30.252.131	192.168.1.103	TCP	66	443 → 52299 [ACK] Seq=8833 Ack=375 Win=...
84	11.	151.20.215.165	192.168.1.103	UDP	145	47447 → 54781 Len=103
85	11.	192.30.252.131	192.168.1.103	TLSv1.2	1454	Application Data
86	11.	192.168.1.103	151.20.215.165	UDP	329	54781 → 47447 Len=287
87	12.	192.168.1.254	224.0.0.1	IGMPv2	68	Membership Query, general
88	12.	192.168.1.254	224.0.0.12	IGMPv2	68	Membership Report group 224.0.0.12
89	12.	192.30.252.131	192.168.1.103	TCP	1454	[TCP Retransmission] 443 → 52299 [ACK] ...
90	13.	99.157.105.135	192.168.1.103	UDP	143	6881 → 54781 Len=101
91	13.	192.168.1.103	99.157.105.135	UDP	327	54781 → 6881 Len=285
92	14.	192.168.1.254	192.168.1.255	RTPv2	80	Response
93	15.	182.208.163.102	192.168.1.103	UDP	145	34512 → 54781 Len=103
94	15.	192.168.1.103	182.208.163.102	UDP	329	54781 → 34512 Len=287
95	15.	192.30.252.131	192.168.1.103	TCP	1454	[TCP Retransmission] 443 → 52299 [ACK] ...
96	18.	192.168.1.103	65.111.161.119	DNS	73	Standard query 0x1348 A tokopedia.com
97	18.	65.111.161.119	192.168.1.103	DNS	186	Standard query response 0x1348 A tokope...
98	18.	192.168.1.103	182.253.224.184	TCP	78	52303 → 80 [SYN] Seq=0 Win=65535 Len=0 ...
99	18.	182.253.224.184	192.168.1.103	TCP	74	80 → 52303 [SYN, ACK] Seq=0 Ack=1 Win=1...
100	18.	192.168.1.103	182.253.224.184	TCP	66	52303 → 80 [ACK] Seq=1 Ack=1 Win=131840...
101	18.	192.168.1.103	182.253.224.184	HTTP	438	GET / HTTP/1.1
102	18.	182.253.224.184	192.168.1.103	TCP	66	80 → 52303 [ACK] Seq=1 Ack=373 Win=1587...
103	18.	182.253.224.184	192.168.1.103	HTTP	525	HTTP/1.1 301 Moved Permanently (text/h...
104	18.	192.168.1.103	182.253.224.184	TCP	66	52303 → 80 [ACK] Seq=373 Ack=460 Win=13...
105	18.	192.168.1.103	65.111.161.119	DNS	77	Standard query 0xfdcf A www.tokopedia.c...
106	18.	65.111.161.119	192.168.1.103	DNS	109	Standard query response 0xfdcf A www.to...
107	18.	192.168.1.103	182.253.224.184	TCP	78	52304 → 443 [SYN] Seq=0 Win=65535 Len=0...
108	18.	182.253.224.184	192.168.1.103	TCP	74	443 → 52304 [SYN, ACK] Seq=0 Ack=1 Win=...

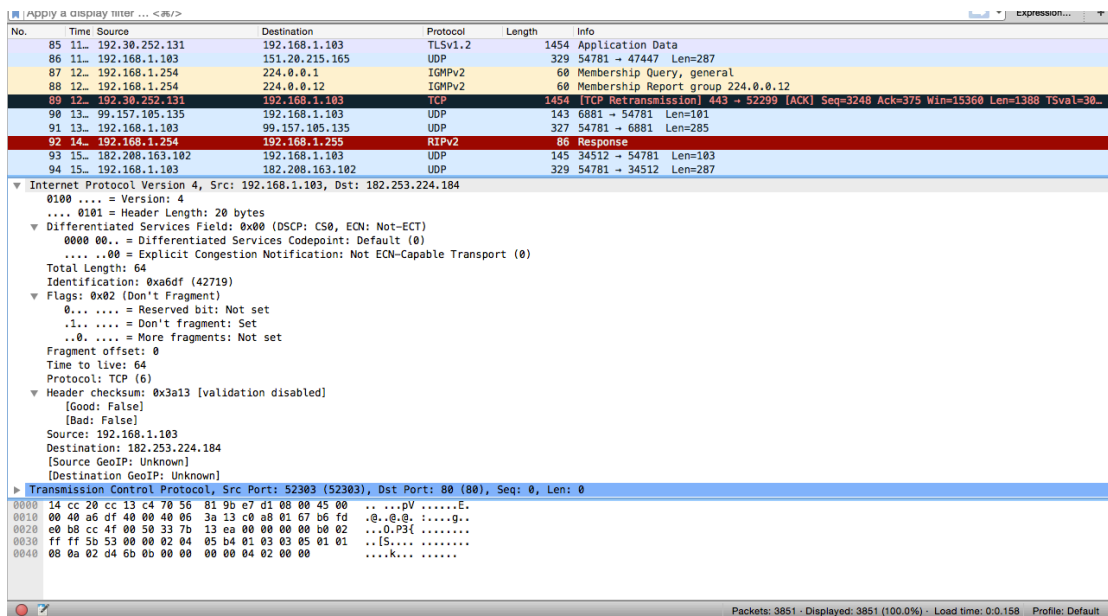
Berikut adalah hasil analisa jaringan yang ter-capture saat membuka dua tab website yaitu gmail.com dan tokopedia.com. Pertama saya akan menjelaskan per-layer (lapisan) pada analisis capture lalu saya akan menjelaskan jenis protocol yang tertangkap pada saat membuka website (HTTP, TCP, DNS, UDP)



Pada baris kedua terdapat beberapa layer, pada layer pertama, Frame layer, menjelaskan ringkasan dari frame.



Layer kedua, Ethernet Layer, terdapat alamat destinasi dan alamat sumber. Data link layer biasanya cukup sederhana hanya terpaku dalam mendapatkan frame ke simpul yang berdekatan berikutnya pada medium fisik.



Jika Ethernet layer terpaku pada simpul ke simpul, IP layer terpaku pada pergerakan antar jaringan (internetwork) dari gambar diatas dapat dilihat alamat IP sumber (192.168.1.103) dan IP tujuan (182.253.224.184) serta IP header length (20 bytes pada gambar). Dapat diperhatikan gambar dibawah adalah pengecekan IP komputer dengan ipconfig dan IP tokopedia dengantraceroute.

```

Villias-MacBook-Pro:~ villiaputriany$ ipconfig getifaddr en1
192.168.1.183
Villias-MacBook-Pro:~ villiaputriany$ ipconfig getpacket en1
op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 3563004786
secs = 0
ciaddr = 0.0.0.0
yiaddr = 192.168.1.103
siaddr = 192.168.1.254
giaddr = 0.0.0.0
chaddr = 78:56:81:9b:e7:d1
sname = TP-LINK
file =
options:
Options count is 10
dhcp_message_type (uint8): ACK 0x5
subnet_mask (ip): 255.255.255.0
router (ip_mult): {192.168.1.254}
domain_name_server (ip_mult): {192.168.1.254}
domain_name (string):
renewal_t1_time_value (uint32): 0x1f40
rebinding_t2_time_value (uint32): 0x375f0
lease_time (uint32): 0x3f480
server_identifier (ip): 192.168.1.254
end (none):
Villias-MacBook-Pro:~ villiaputriany$

Villias-MacBook-Pro:~ villiaputriany$ traceroute tokopedia.com
traceroute to tokopedia.com (182.253.224.184), 64 hops max, 52 byte packets
 1 192.168.1.254 (192.168.1.254) 589.218 ms 4.986 ms 0.818 ms
 2 36.69.48.1 (36.69.48.1) 132.417 ms 127.108 ms 25.540 ms
 3 125.160.0.29 (125.160.0.29) 24.566 ms 25.132 ms 50.450 ms
 4 61.94.115.205 (61.94.115.205) 24.831 ms 25.776 ms 25.594 ms
 5 118.98.63.249 (118.98.63.249) 53.687 ms 55.628 ms 51.719 ms
 6 157.subnet118-98-62.astinet.telkom.net.id (118.98.62.157) 60.575 ms 59.330 ms 60.049 ms
 7 61.94.0.249 (61.94.0.249) 143.944 ms 71.723 ms 59.478 ms
 8 122.subnet125-160-9.speedy.telkom.net.id (125.160.9.122) 48.606 ms 50.280 ms 55.023 ms
 9 * * biznet.openixp.net (218.100.36.91) 65.951 ms
10 203.142.67.50 (203.142.67.50) 48.788 ms 51.110 ms 53.381 ms
11 182.253.224.184 (182.253.224.184) 52.631 ms 50.298 ms 50.742 ms
Villias-MacBook-Pro:~ villiaputriany$

```

Kita juga bisa melihat Layanan Differentiated (DiffServ) daerah. Ini akan menjadi tempat informasi tambahan yang berkaitan dengan jenis paket layanan yang pergi. Bagi kebanyakan paket pada LAN ini diatur ke nol, yang berarti usaha terbaik. Ada beberapa tingkatan lain, seperti Expedited Forwarding, yang umumnya memiliki kehilangan rendah, delay rendah, dan jitter rendah. tingkat Diff Serv dapat digunakan ketika ingin menerapkan Quality of Service pada jaringan IP.

TCP

```

▶ Frame 98: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Ethernet II, Src: Apple_9b:e7:d1 (78:56:81:9b:e7:d1), Dst: TP-LINK_cc:13:c4 (14:cc:20:cc:13:c4)
▶ Internet Protocol Version 4, Src: 192.168.1.183, Dst: 182.253.224.184
▼ Transmission Control Protocol, Src Port: 52303 (52303), Dst Port: 80 (80), Seq: 0, Len: 0
  Source Port: 52303
  Destination Port: 80
  [Stream index: 4]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 44 bytes
  ▶ Flags: 0x002 (SYN)
  Window size value: 65535
  [Calculated window size: 65535]
  Checksum: 0x5b53 [validation disabled]
  [Good Checksum: False]
  [Bad Checksum: False]
  Urgent pointer: 0
  Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), Timestamps, SACK permitted, End of Option List (EOL)
    ▶ Maximum segment size: 1460 bytes
    ▶ No-Operation (NOP)
    ▶ Window scale: 5 (multiply by 32)
    ▶ No-Operation (NOP)
    ▶ No-Operation (NOP)
    ▶ Timestamps: Tsv1 47475467, TSecr 0
    ▶ TCP SACK Permitted Option: True
    ▶ End of Option List (EOL)

0000 14 cc 20 cc 13 c4 70 56 81 9b e7 d1 00 00 45 00 .. .pV .....E.
0010 00 40 a6 0f 40 00 40 06 3a 13 c0 a8 01 67 b6 fd .@.e.@. :.....g.
0020 e9 08 cc 4f 00 50 33 7b 13 ca 00 00 00 00 02 ..o.P[ .....
0030 ff ff 5b 53 00 00 02 04 05 b4 01 03 03 05 01 01 ..[S.....
0040 08 0a 02 d4 6b 0b 00 00 00 00 04 02 00 00 ....k.....

```

Transport layer menjelaskan di mana aplikasi berkomunikasi melalui port yang digunakan. Melihat capture ditunjukkan pada gambar diatas, kita dapat melihat bahwa port sumber adalah 52303, sedangkan port tujuan adalah 80. Hal menarik yang lain adalah panjang header (44 byte) dan nomor urut. Nomor urut umumnya akan berubah untuk setiap paket.

HTTP

No.	Time	Source	Destination	Protocol	Length	Info
101	18.	192.168.1.103	182.253.224.184	HTTP	438	GET / HTTP/1.1
103	18.	182.253.224.184	192.168.1.103	HTTP	525	HTTP/1.1 301 Moved Permanently (text/html)
2167	28.	192.168.1.103	23.15.155.27	OCSIP	492	Request
2170	28.	192.168.1.103	216.58.196.174	OCSIP	509	Request
2224	28.	23.15.155.27	192.168.1.103	OCSIP	428	Response
2227	28.	216.58.196.174	192.168.1.103	OCSIP	812	Response
2552	30.	192.168.1.103	104.25.129.31	HTTP	553	GET /img/px.png?ts=1455204878657-3326i=300&s=b&pid=620076sa=A20646tv=14551266931136...
2586	30.	192.168.1.103	117.18.237.29	OCSIP	511	Request

▼ Hypertext Transfer Protocol

- GET / HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n
 - [GET / HTTP/1.1\r\n
 - [Severity level: Chat
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /
 - Request Version: HTTP/1.1
 - Host: tokopedia.com\r\n
 - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:44.0) Gecko/20100101 Firefox/44.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 - Accept-Language: en-US,en;q=0.5\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Cookie: __auc=5ca36ace1520706b2bedffb06; _ga=GA1.2.638121234.1451816848\r\n
 - Cookie pair: __auc=5ca36ace1520706b2bedffb06
 - Cookie pair: _ga=GA1.2.638121234.1451816848
 - Connection: keep-alive\r\n
 - \r\n
 - [Full request URI: http://tokopedia.com/

[HTTP request 1/1]

```
0000 14 cc 20 cc 13 c4 70 56 81 9b e7 d1 08 00 45 00 ..pV.....E.
0010 01 a8 70 2a 40 00 40 06 6f 60 c0 a8 01 67 b6 fd ..p@e@.o'...g..
0020 e0 08 cc 4f 00 33 7b 13 eb c6 a7 45 4b 08 10 ...0.P34....EK..
0030 10 18 04 7d 00 00 01 01 08 0a 02 d4 6b 34 d5 4a ...}....K4.J
0040 9e ad 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 80 0a 48 6f 73 74 3a 20 74 6f 6b 6f 70 65 64 69 ..Host: tokopedi
0060 61 2e 63 6f 6d 04 05 73 65 72 2d 41 67 65 6e a.com..U ser-Agen
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
```

Dari data yang dicapture diatas kita dapat menganalisis beberapa informasi sebagai berikut.

1. Kemungkinan Web browser yang digunakan adalah Mozilla 5.0/Crome 25.0.1364/Safari 537.22 dengan operating sistem Macintosh; Intel Mac OS X 10.10
2. Web browser dan server Tokopedia sama-sama running HTML versi 1.1
3. Bahasa yang digunakan Web browser yang dapat diterima server adalah bahasa English US.
4. Akses ke tokopedia.com browser ini dah pernah dilakukan hingga terdapat cookie tersimpan di browser user.

No.	Time	Source	Destination	Protocol	Length	Info
96	18.	192.168.1.103	65.111.161.119	DNS	73	Standard query 0x1348 A tokopedia.com
97	18.	65.111.161.119	192.168.1.103	DNS	186	Standard query response 0x1348 A tokopedia.com A 182.253.224.184 NS ns2.p21.dynect
98	18.	192.168.1.103	182.253.224.184	TCP	78	52303 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=47475467 TSecr=0 SACK_
99	18.	182.253.224.184	192.168.1.103	TCP	74	80 → 52303 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1400 SACK_PERM=1 TSval=35784
100	18.	192.168.1.103	182.253.224.184	TCP	66	52303 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=47475508 TSecr=3578437293
101	18.	192.168.1.103	182.253.224.184	HTTP	438	GET / HTTP/1.1
102	18.	182.253.224.184	192.168.1.103	TCP	66	80 → 52303 [ACK] Seq=1 Ack=373 Win=15072 Len=0 TSval=3578437348 TSecr=47475508
103	18.	182.253.224.184	192.168.1.103	HTTP	525	HTTP/1.1 301 Moved Permanently (text/html)

▼ Hypertext Transfer Protocol

- HTTP/1.1 301 Moved Permanently\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n
 - [HTTP/1.1 301 Moved Permanently\r\n
 - [Severity level: Chat
 - [Group: Sequence]
 - Request Version: HTTP/1.1
 - Status Code: 301
 - Response Phrase: Moved Permanently
 - Server: nginx\r\n
 - Date: Thu, 11 Feb 2016 15:34:26 GMT\r\n
 - Content-Type: text/html\r\n
 - Content-Length: 178\r\n
 - [Content length: 178]
 - Connection: keep-alive\r\n
 - Location: https://www.tokopedia.com/\r\n
 - Set-Cookie: uid=tv3guFa8qKA4gInCfLLAg==; expires=Fri, 12-Feb-16 15:34:26 GMT; path=/\r\n
 - \r\n
 - [HTTP response 1/1]
 - [Time since request: 0.056631000 seconds]
 - [Request in frame: 101]

Line-based text data: text/html

```
0000 70 56 81 9b e7 d1 14 cc 20 cc 13 c4 08 00 45 00 pV.....E.
0010 01 ff db 9e 40 00 3a 06 09 95 b6 fd e0 b8 c0 a8 ...@.i.....
0020 01 67 00 50 cc 4f c6 a7 45 4b 33 7b 15 5f 08 10 .g.P.O..EK3f...
0030 00 1f 5c 12 00 00 01 01 08 0a 05 d4 9e 04 e2 d4 ..}....}J...
0040 6b 34 48 54 54 50 2f 31 2e 31 20 33 30 31 20 4d kHTTP/1.1 301 M
0050 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 oved Per manently
0060 0a 53 72 76 63 72 3a 20 6e 67 69 6e 78 0d ..Server : nginx.
0070 0a 44 61 74 65 3a 20 54 68 75 2c 20 31 21 20 46 .Date: T hu, 11 F
```

1. Server Sony menggunakan nginx
2. Status Code dari server ke browser kita adalah 301 yang artinya Moved Permanently
3. Website diakses pada Hari Kamis 11 Februari 2016 15:34:26 GMT
4. Content yang ditransfer pada sesi ini bertipe teks
5. Panjang Content-nya adalah 178 bytes

DNS

Dapat diketahui bahwa server DNS kita adalah 8.8.4.4 yang mempunyai IP address 192.168.203.1. Hal tersebut berdasar pada IP source dan destination pada penangkapan paket oleh wireshark. Untuk membuktikannya kita juga dapat mengecek melalui Terminal.

```
villiaputriany -- bash -- 87x24
You have new mail.
villias-MacBook-Pro:~ villiaputriany$ nslookup tokopedia.com
;; Got recursion not available from 65.111.161.119, trying next server
;; Got recursion not available from 8.8.8.8, trying next server
Server:      8.8.4.4
Address:     8.8.4.4#53

Non-authoritative answer:
Name:   tokopedia.com
Address: 182.253.224.184

villias-MacBook-Pro:~ villiaputriany$
```

Capture dengan wireshark:

The screenshot displays the Wireshark interface with a packet capture of a DNS response. The packet list pane shows a DNS Standard query response from 192.168.1.103 to 192.168.1.103. The packet details pane shows the Domain Name System (response) section with the source IP 192.168.1.103 and destination IP 192.168.1.103. The packet bytes pane shows the raw data of the DNS response.

No.	Time	Source	Destination	Protocol	Length	Info
92	14.152	192.168.1.254	192.168.1.255	RTSP	86	Response
93	15.182	208.163.102	192.168.1.103	UDP	145	34512 → 54781 Len=103
94	15.192	168.1.103	182.208.163.102	UDP	329	54781 → 34512 Len=287
95	15.192	30.252.131	192.168.1.103	TCP	1454	[TCP Retransmission] 443 → 52299 [ACK] Seq=3248 Ack=375 Win=15360 Len=1388 TSval=3
96	18.192	168.1.103	65.111.161.119	DNS	73	Standard query 0x1348 A tokopedia.com
97	18.65	111.161.119	192.168.1.103	DNS	186	Standard query response 0x1348 A tokopedia.com A 182.253.224.184 NS ns2.p21.dynect
98	18.192	168.1.103	182.253.224.184	TCP	78	52303 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=47475467 TSecr=0 SACK_
99	18.182	253.224.184	192.168.1.103	TCP	74	80 → 52303 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1400 SACK_PERM=1 TSval=35784
100	18.192	168.1.103	182.253.224.184	TCP	66	52303 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=47475508 TSecr=3578437293
101	18.192	168.1.103	182.253.224.184	HTTP	438	GET / HTTP/1.1
102	18.182	253.224.184	192.168.1.103	TCP	66	80 → 52303 [ACK] Seq=1 Ack=373 Win=15872 Len=0 TSval=3578437348 TSecr=47475508
103	18.182	253.224.184	192.168.1.103	HTTP	525	HTTP/1.1 301 Moved Permanently (text/html)
104	18.192	168.1.103	182.253.224.184	TCP	66	52303 → 80 [ACK] Seq=373 Ack=460 Win=131392 Len=0 TSval=47475564 TSecr=3578437348
105	18.192	168.1.103	65.111.161.119	DNS	77	Standard query 0xfdcf A www.tokopedia.com
106	18.65	111.161.119	192.168.1.103	DNS	189	Standard query response 0xfdcf A www.tokopedia.com A 182.253.224.184 A 182.253.224
107	18.192	168.1.103	182.253.224.184	TCP	78	52304 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=47475584 TSecr=0 SACK
108	18.182	253.224.184	192.168.1.103	TCP	74	443 → 52304 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1400 SACK_PERM=1 TSval=3578

▶ Frame 97: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
▶ Ethernet II, Src: Tp-LinkT_cc:13:c4 (14:cc:20:cc:13:c4), Dst: Apple_9b:e7:d1 (70:56:01:9b:e7:d1)
▶ Internet Protocol Version 4, Src: 65.111.161.119, Dst: 192.168.1.103
▼ User Datagram Protocol, Src Port: 53 (53), Dst Port: 55824 (55824)
Source Port: 53
Destination Port: 55824
Length: 152
▼ Checksum: 0xf626 [validation disabled]
[Good Checksum: False]
[Bad Checksum: False]
[Stream index: 11]
▶ Domain Name System (response)

```
0000 70 56 81 9b e7 d1 14 cc 20 cc 13 c4 08 00 45 00  pV.....E.
0010 00 ac 9a e2 40 00 fc 11 3e 68 41 6f a1 77 c0 a8  ...@...>hAo.w..
0020 01 67 00 35 d3 10 00 98 f6 26 13 48 81 80 00 01  .g5....&H...
0030 00 01 00 04 00 01 09 74 6f 6b 6f 70 65 64 69 61  .....t okopedia
0040 03 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00  .com.....
0050 01 51 00 00 04 b6 fd e0 b8 c0 0c 00 02 00 01 00  .0.....
0060 01 51 00 00 14 03 6e 73 32 03 70 32 31 00 64 79  .0.....ns 2.p21.dy
0070 6e 65 63 74 03 6e 65 74 00 c0 0c 00 02 00 01 00  nect.net .....
```

```

Domain Name System (response)
[Request In: 96]
[Time: 0.060570000 seconds]
Transaction ID: 0x1348
Flags: 0x0100 Standard query response, No error
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
.... 0... .. = Authoritative: Server is not an authority for domain
.... 0... .. = Truncated: Message is not truncated
.... 1... .. = Recursion desired: Do query recursively
.... 1... .. = Recursion available: Server can do recursive queries
.... 0... .. = Z: reserved (0)
.... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 0... .. = Non-authenticated data: Unacceptable
.... 0... .. = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 4
Additional RRs: 1
Queries
  tokopedia.com: type A, class IN
Answers
  tokopedia.com: type A, class IN, addr 182.253.224.184
Authoritative nameservers
  tokopedia.com: type NS, class IN, ns ns2.p21.dynect.net
  tokopedia.com: type NS, class IN, ns ns1.p21.dynect.net
  tokopedia.com: type NS, class IN, ns ns3.p21.dynect.net
  tokopedia.com: type NS, class IN, ns ns4.p21.dynect.net
Additional records
  <Root>: type OPT
0000 70 56 01 9b e7 d1 14 cc 20 cc 13 c4 00 00 45 00 pV.....E.
0010 00 ac 9a e2 40 00 fc 11 3e 68 41 6f a1 77 c0 a8 ...@...>hAo.w..
0020 01 67 00 35 da 10 00 90 f6 26 13 48 81 80 00 01 .g.S....>.h.H...
0030 00 01 00 04 00 01 89 74 6f 6b 6f 70 65 64 69 61 .....t okopedia
0040 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 .com.....
0050 01 51 80 00 04 b6 fd e0 b8 c0 0c 00 02 00 01 00 .Q.....
0060 01 51 80 00 14 03 6e 73 32 03 70 32 31 06 64 79 .0....ns 2.p21.dy
0070 6e 65 63 74 03 6e 65 74 00 c0 0c 00 02 00 01 00 nect.net .....
Packets: 3851 · Displayed: 3851 (100.0%) · Load time: 0:0.158 · Profile: De

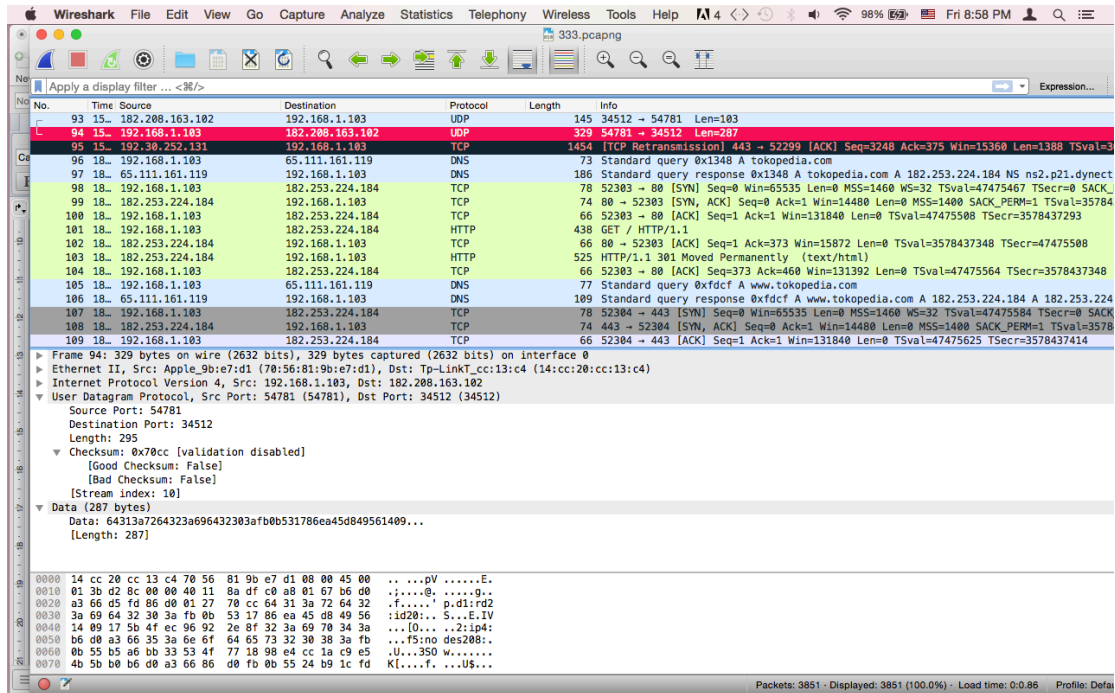
```

Pada dasarnya DNS (Domain Name System) adalah penerjemahan alamat IP ke hostname dan sebaliknya. Host meminta alamat yang akan dituju (tokopedia.com) kepada DNS server. Dapat dilihat untuk melakukan proses ini diperlukan 0.060570000 second.

Server DNS menjawab kepada host bahwa tokopedia.com dengan IP address 182.253.224.184. Ternyata data ini sama persis dengan informasi yang diperoleh pada nslookup Terminal. Kita dapat mengetahui bahwa queries alamat Tokopedia ini type A (host Address) dan Class IN (0x0001).

UDP

UDP adalah TCP yang connectionless. Hal ini berarti bahwa suatu paket yang dikirim melalui jaringan dan mencapai komputer lain tanpa membuat suatu koneksi. Sehingga dalam perjalanan ke tujuan paket dapat hilang karena tidak ada koneksi langsung antara kedua host, jadi UDP sifatnya tidak realibel. UDP tidak pernah digunakan untuk mengirim data penting seperti halaman web, informasi database, dan sebagainya. Tetapi UDP biasanya digunakan untuk streaming audio dan video, karena UDP mempunyai kelebihan yaitu pada kecepatan transfer. UDP lebih cepat dari TCP karena pada protokol UDP tidak ada bentuk kontrol aliran dan koreksi kesalahan.



Dari gambar diatas dapat dilihat protokol UDP yang tercapture wireshark diaman IP source 192.168.1.103 menggunakan port 54781 dimana pada sesi ini dia adalah pengirim data atau informasi dan IP destination 182.208.163.102 port 34512 adalah yang akan menerima informasi dari source. Pada UDP tidak ada proses koreksi kesalahan/flow control.