

Wireshark – Network Packet Analyzer

S1 Teknik Telekomunikasi
Fakultas Teknik Elektro
Telkom University





Outline

- Overview
 - User Interface Wireshark
 - OSI Layer pada Wireshark
 - Mencari parameter QoS pada wireshark
- 



Overview





▶ Apa itu wireshark?

Wireshark adalah software penganalisa paket jaringan

Berlisensi Open Source yang dapat diunduh dan digunakan secara gratis

Wireshark dapat menyajikan paket data yang direkam di antarmuka jaringan sedetail mungkin





Apa Tujuan Menggunakan Wireshark ?

- Administrator jaringan → memecahkan masalah jaringan
 - Teknisi keamanan jaringan → memeriksa masalah keamanan
 - Teknisi QA → memverifikasi aplikasi jaringan
 - Pengembang Sistem / Aplikasi → men-debug implementasi protokol
 - Akademisi → mempelajari internal protokol jaringan
- 

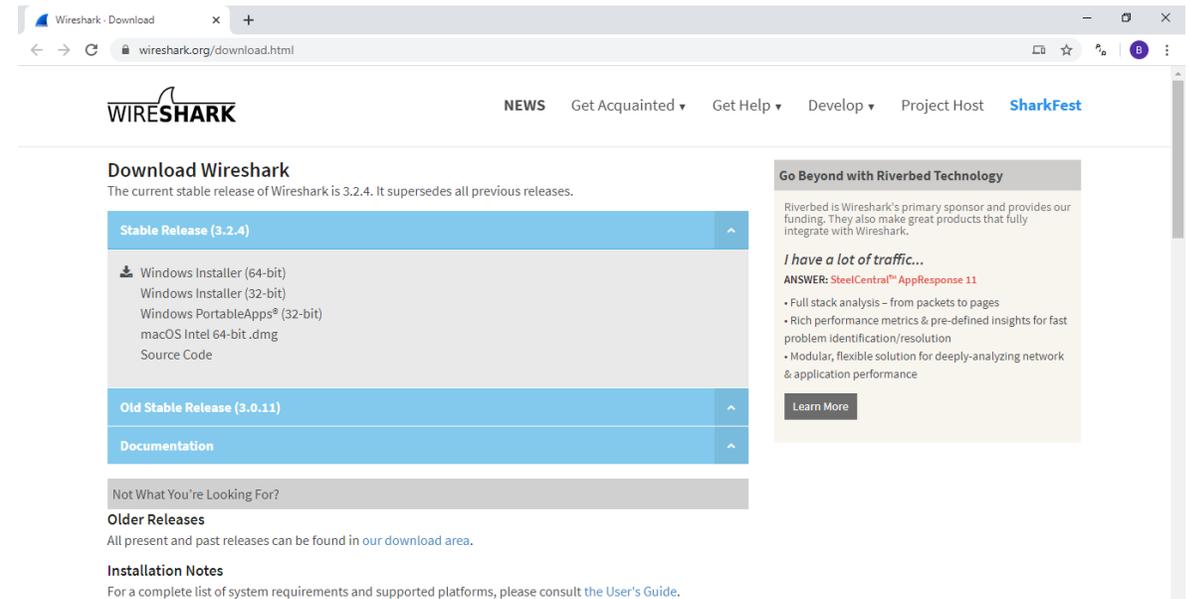


Fitur Wireshark

- Tersedia untuk sistem operasi UNIX dan Windows.
 - Menangkap data paket langsung dari antarmuka jaringan (LAN/WLAN)
 - Buka file yang berisi data paket yang diambil dengan tcpdump / WinDump, Wireshark, dan banyak lagi program penangkapan paket lainnya.
 - Tampilkan paket dengan informasi protokol yang sangat rinci.
 - Simpan data paket yang diambil ke dalam format csv
 - ... dan banyak lagi!
- 

Instalasi Wireshark

- ✓ Kunjungi website resminya di:
<https://www.wireshark.org/download.html>
- ✓ Unduh stable release sesuai sistem operasi yang dipakai
- ✓ Lakukan instalasi sesuai masing-masing sistem operasi yang digunakan



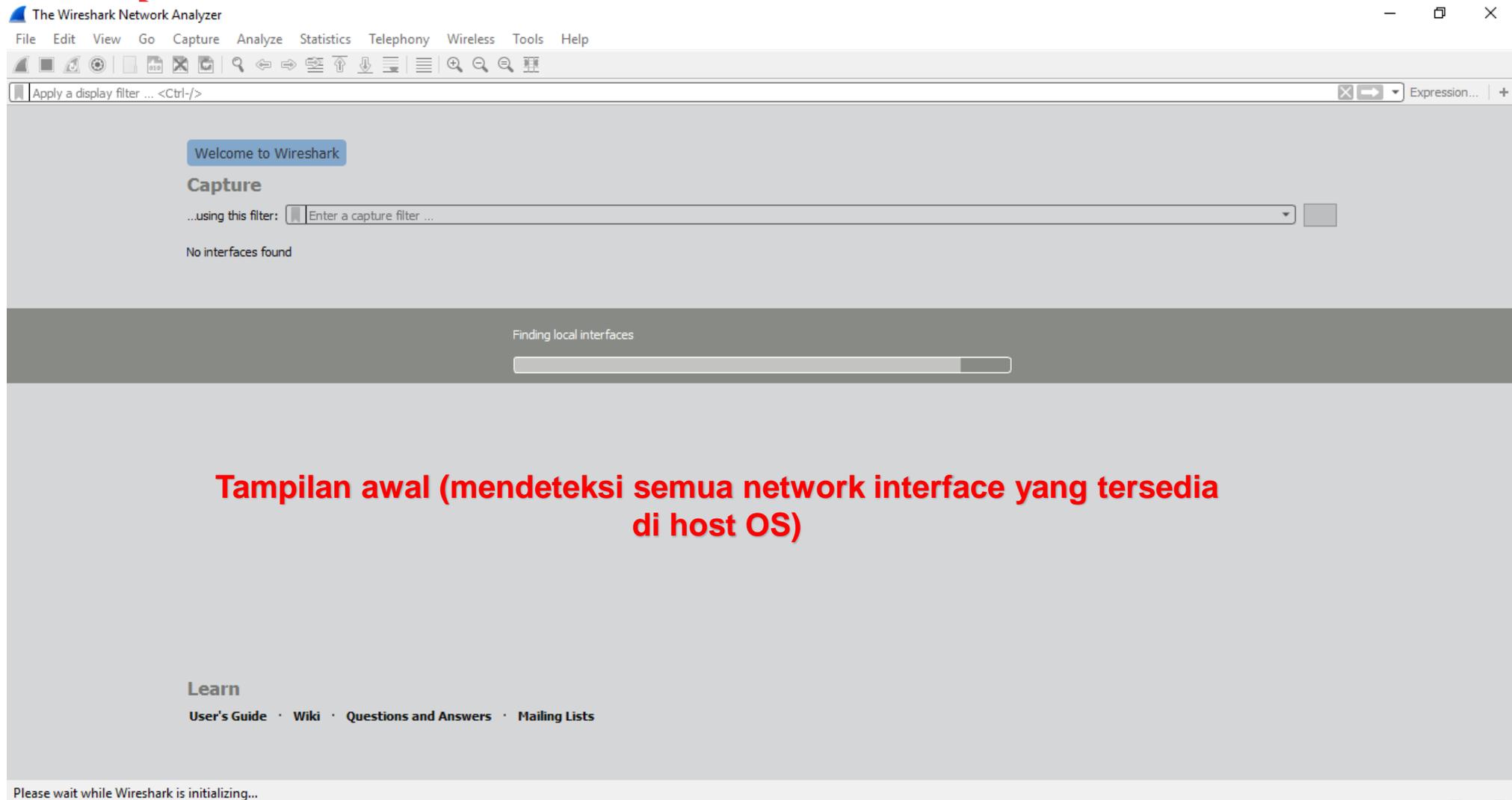
The screenshot shows the official Wireshark download page. The browser address bar displays 'wireshark.org/download.html'. The page features the Wireshark logo and navigation links such as 'NEWS', 'Get Acquainted', 'Get Help', 'Develop', 'Project Host', and 'SharkFest'. The main content area is titled 'Download Wireshark' and states that the current stable release is 3.2.4. Below this, there are expandable sections for 'Stable Release (3.2.4)', 'Old Stable Release (3.0.11)', and 'Documentation'. The 'Stable Release (3.2.4)' section lists download options: Windows Installer (64-bit), Windows Installer (32-bit), Windows PortableApps® (32-bit), macOS Intel 64-bit .dmg, and Source Code. A sidebar on the right contains a promotional message for Riverbed Technology with a 'Learn More' button. At the bottom, there are sections for 'Older Releases' and 'Installation Notes'.



User Interface Wireshark



User Interface Wireshark

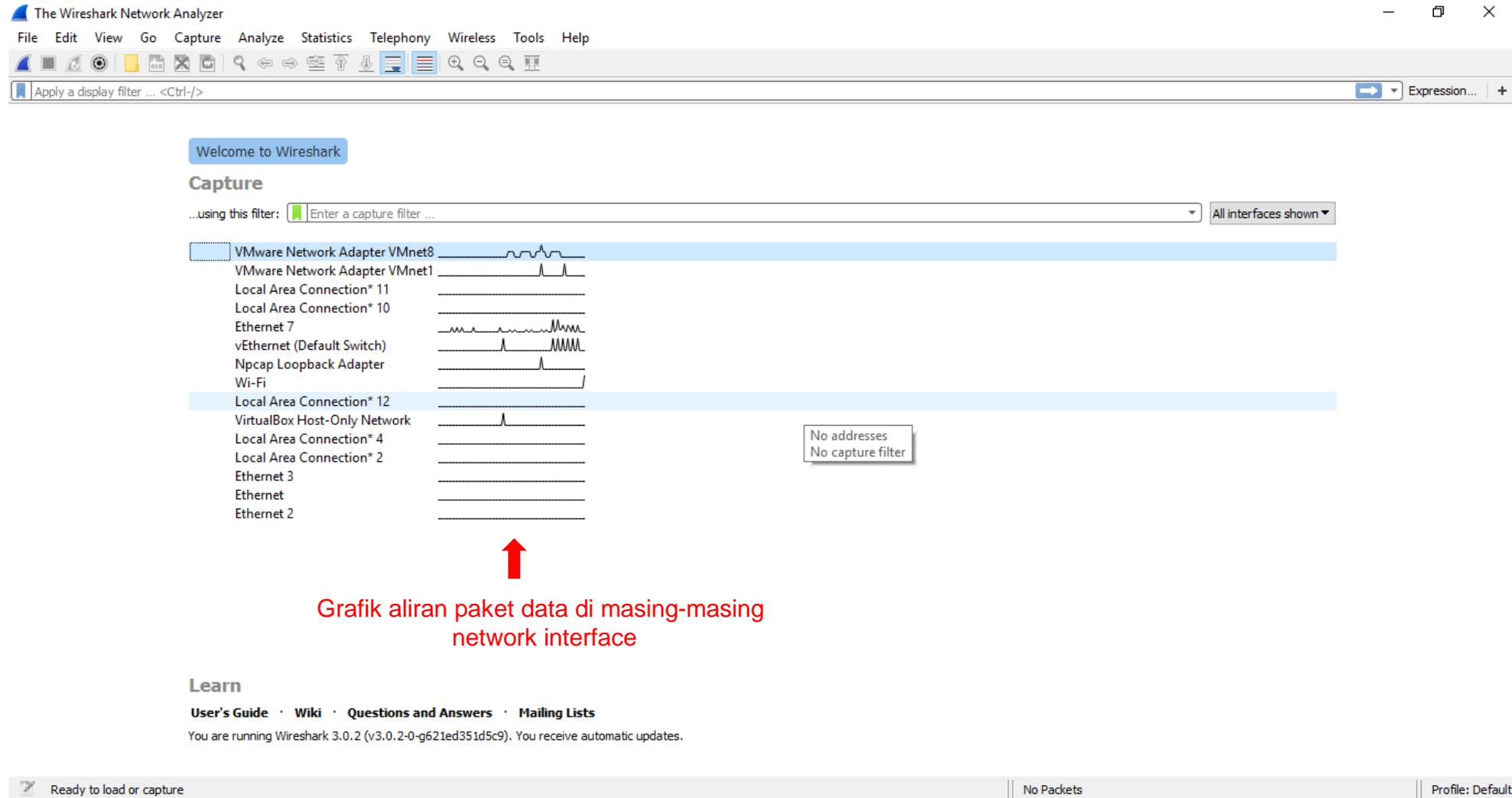


Tampilan awal (mendeteksi semua network interface yang tersedia di host OS)

User Interface Wireshark

Tampilan network interface yang tersedia di host OS →

Pilih salah satu network interface yang ingin dicapture →



The screenshot shows the Wireshark Network Analyzer interface. The title bar reads "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. Below the toolbar is a display filter field with the text "Apply a display filter ... <Ctrl-/>".

The main content area is titled "Welcome to Wireshark" and "Capture". It features a dropdown menu for "Enter a capture filter ..." and a button for "All interfaces shown". Below this is a list of network interfaces, each with a small traffic graph to its right. The interfaces listed are:

- VMware Network Adapter VMnet8
- VMware Network Adapter VMnet1
- Local Area Connection* 11
- Local Area Connection* 10
- Ethernet 7
- vEthernet (Default Switch)
- Npcap Loopback Adapter
- Wi-Fi
- Local Area Connection* 12
- VirtualBox Host-Only Network
- Local Area Connection* 4
- Local Area Connection* 2
- Ethernet 3
- Ethernet
- Ethernet 2

A red arrow points to the traffic graphs for the "Local Area Connection* 12" interface. A tooltip box next to the graph for "Local Area Connection* 2" contains the text "No addresses" and "No capture filter".

At the bottom of the interface, there is a "Learn" section with links for "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". Below these links, it states: "You are running Wireshark 3.0.2 (v3.0.2-0-g621ed351d5c9). You receive automatic updates."

The status bar at the bottom of the window shows "Ready to load or capture" on the left, "No Packets" in the center, and "Profile: Default" on the right.

Grafik aliran paket data di masing-masing network interface

User Interface Wireshark

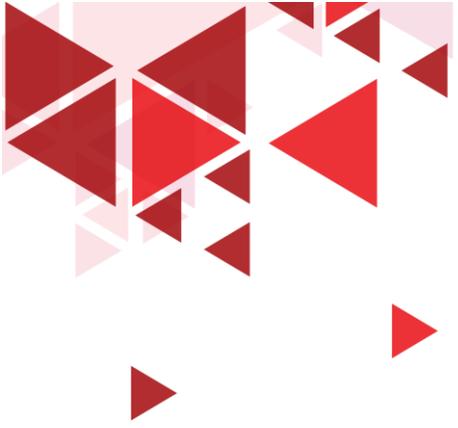
The screenshot shows the Wireshark interface with the following components labeled:

- Menu Utama:** The main menu bar at the top, including File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help.
- Toolbar Utama:** The main toolbar below the menu, containing icons for capture, analysis, and display.
- Toolbar Filter:** A filter toolbar located above the packet list, with a text input field and a search icon.
- Panel Packet List:** A table listing captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Panel Detail Packet:** A pane showing the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security.
- Panel Byte Packet:** A pane showing the raw bytes of the selected packet in hexadecimal and ASCII.
- Toolbar Status:** The bottom status bar, displaying the current capture status (Wi-Fi: <live capture in progress>), packet statistics (Packets: 79 · Displayed: 79 (100.0%)), and the active profile (Profile: Default).

No.	Time	Source	Destination	Protocol	Length	Info
66	8.224189	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=1 Ack=178 Win=555 Len=0
67	8.224931	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=1 Ack=217 Win=555 Len=0
68	8.225226	216.58.221.78	192.168.1.6	TLSv1.2	93	Application Data
69	8.232854	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=40 Ack=1249 Win=566 Len=0
70	8.267894	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=40 Win=258 Len=0
71	8.276617	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
72	8.282999	216.58.221.78	192.168.1.6	TLSv1.2	278	Application Data
73	8.283252	216.58.221.78	192.168.1.6	TLSv1.2	238	Application Data
74	8.283326	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=448 Win=257 Len=0
75	8.284216	216.58.221.78	192.168.1.6	TLSv1.2	250	Application Data
76	8.284218	216.58.221.78	192.168.1.6	TLSv1.2	93	Application Data
77	8.284364	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=683 Win=256 Len=0
78	8.287713	192.168.1.6	216.58.221.78	TLSv1.2	93	Application Data
79	8.308167	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=683 Ack=1288 Win=566 Len=0

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15}, id 0
> Ethernet II, Src: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d), Dst: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 69.171.250.60
> Transmission Control Protocol, Src Port: 14365, Dst Port: 443, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security
```

```
0000 24 d3 f2 cd 3a 2f d0 c5 d3 36 7e 8d 08 00 45 00  $...:/...6~...E.
0010 00 47 9d 90 40 00 40 06 9b 8a c0 a8 01 06 45 ab  .G..@.@.....E.
0020 fa 3c 38 1d 01 bb eb 87 20 50 66 85 73 6a 50 18  <8.....Pf.sjP.
0030 08 11 4d 45 00 00 17 03 03 00 1a b9 99 43 7d de  ..ME.....[C]
0040 3c de 5e 58 52 d1 35 92 3f 67 f4 bf fe 89 98 95  <^XR.S.?g.....
0050 4c a8 b0 b9 01  L....
```



Penjelasan User Interface Wireshark

- Menu Utama : digunakan untuk memulai tindakan.
 - Toolbar utama : menyediakan akses cepat ke item yang sering digunakan dari menu.
 - Toolbar filter : memungkinkan pengguna untuk mengatur filter tampilan untuk memfilter paket mana yang ditampilkan
 - Panel paket list : menampilkan ringkasan dari setiap paket yang diambil. (Dengan mengklik paket di panel ini Anda mengontrol apa yang ditampilkan di dua panel lainnya)
 - Panel detail packet : menampilkan paket yang dipilih di panel daftar paket secara lebih rinci.
 - Panel byte paket : menampilkan data dari paket yang dipilih di panel paket list, dan menyoroti bidang yang dipilih di panel detail paket.
 - Toolbar status : menunjukkan beberapa informasi terperinci tentang status program saat ini dan data yang diambil.
- 

Panel Packet List

No.	Time	Source	Destination	Protocol	Length	Info
66	8.224189	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=1 Ack=178 Win=555 Len=0
67	8.224931	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=1 Ack=217 Win=555 Len=0
68	8.225226	216.58.221.78	192.168.1.6	TLSv1.2	93	Application Data
69	8.232854	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=40 Ack=1249 Win=566 Len=0
70	8.267894	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=40 Win=258 Len=0
71	8.276617	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
72	8.282999	216.58.221.78	192.168.1.6	TLSv1.2	278	Application Data
73	8.283252	216.58.221.78	192.168.1.6	TLSv1.2	238	Application Data
74	8.283326	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=448 Win=257 Len=0
75	8.284216	216.58.221.78	192.168.1.6	TLSv1.2	250	Application Data
76	8.284218	216.58.221.78	192.168.1.6	TLSv1.2	93	Application Data
77	8.284364	192.168.1.6	216.58.221.78	TCP	54	14345 → 443 [ACK] Seq=1249 Ack=683 Win=256 Len=0
78	8.287713	192.168.1.6	216.58.221.78	TLSv1.2	93	Application Data
79	8.308167	216.58.221.78	192.168.1.6	TCP	56	443 → 14345 [ACK] Seq=683 Ack=1288 Win=566 Len=0

- No : urutan paket dalam file capture
- Time : waktu lewatnya paket pada saat di capture
- Source : Alamat dari mana paket ini berasal.
- Destination : Alamat tujuan paket ini.
- Protocol : Nama protokol
- Length : Panjang setiap paket.
- Info : Informasi tambahan tentang konten paket.

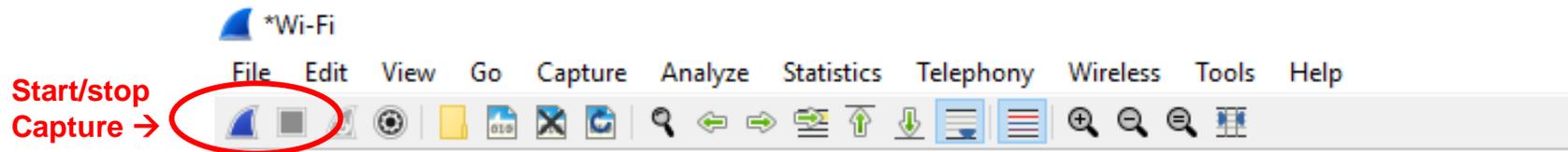


Capture Packet HTTP di Interface jaringan

Sesi Demo

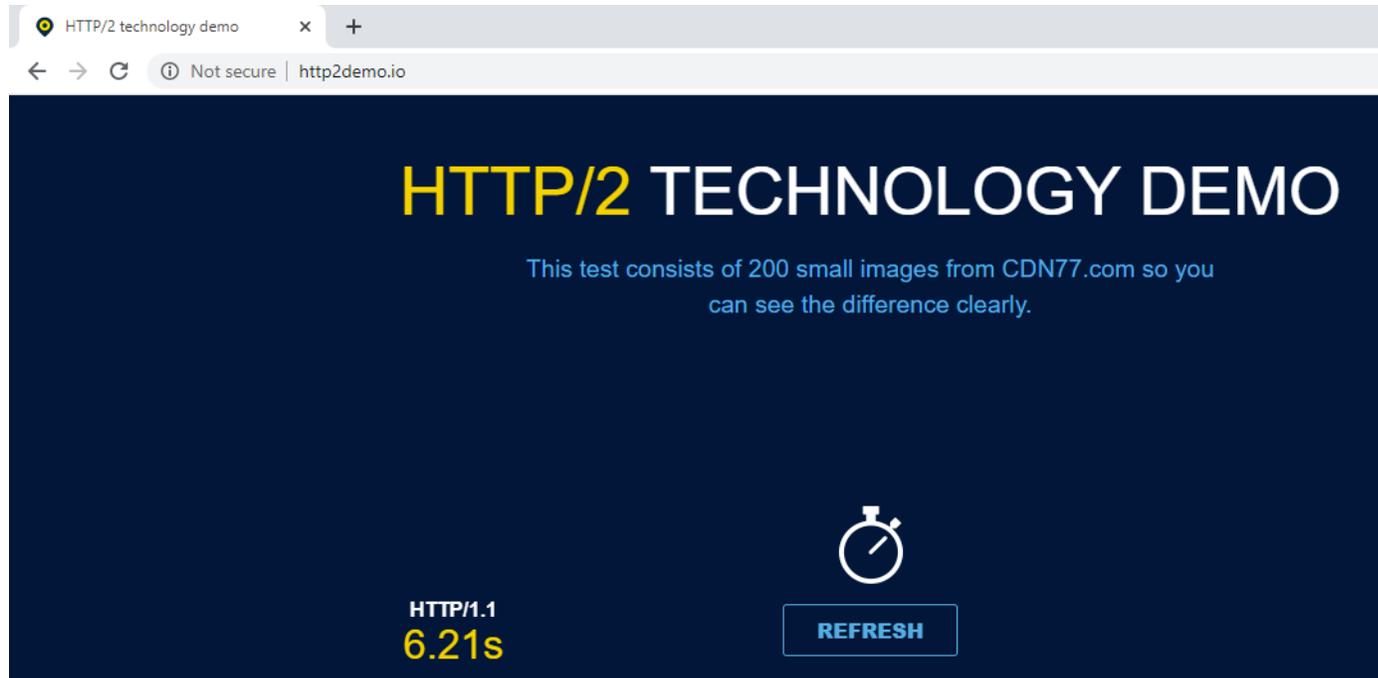


Start Capture Paket



Klik start capture di toolbar utama pada wireshark sesuai network interface yang telah dipilih sebelumnya (dalam contoh ini menggunakan Wifi Network Interface)

Open HTTP Website



Pada browser, kunjungi website yang masih menggunakan protocol HTTP ,
contoh : http2demo.io

▶ Stop Capture

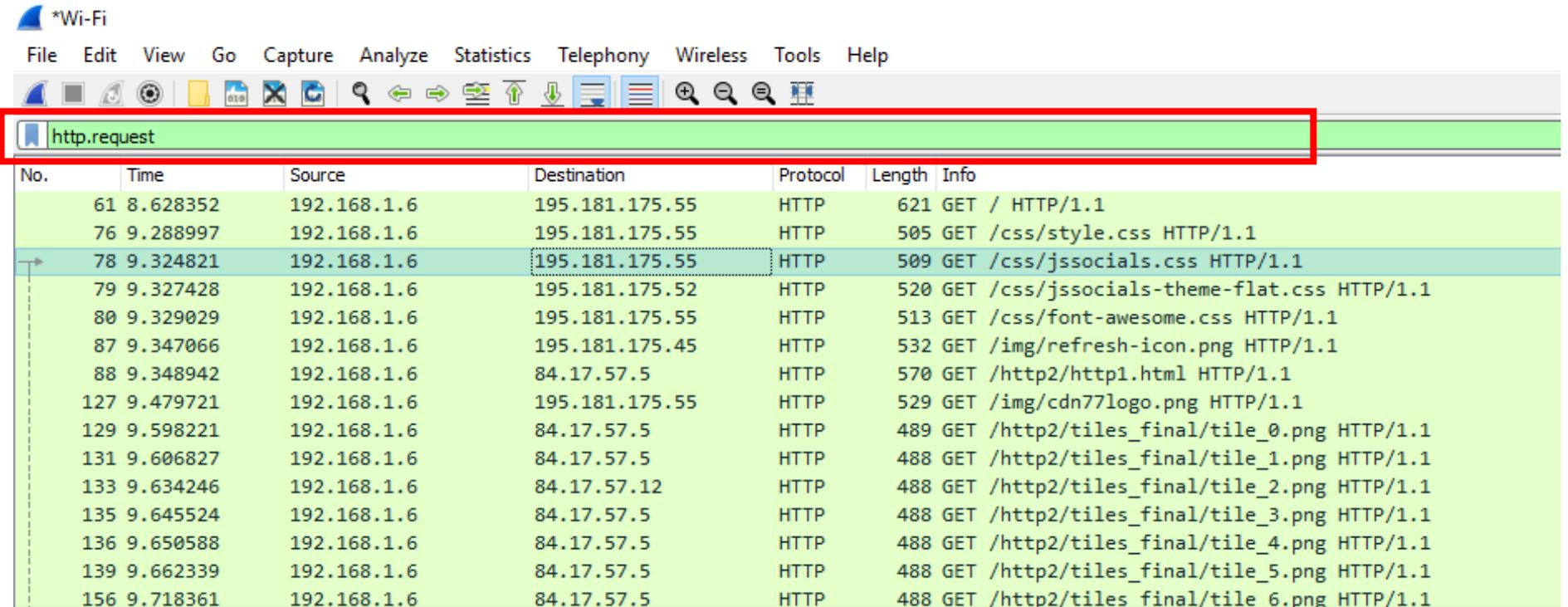


Klik stop capture di toolbar utama pada wireshark

Filter Paket HTTP Request

Filter →

- ✓ Ketikkan http.request pada filter toolbar, tekan enter
- ✓ Kemudian akan terlihat hasil filter pada panel packet list yaitu muncul hanya protocol http



The screenshot shows the Wireshark interface with the filter toolbar at the top. The filter text 'http.request' is entered in the filter field, which is highlighted with a red box. Below the toolbar, a table of network packets is displayed, showing only HTTP requests. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
61	8.628352	192.168.1.6	195.181.175.55	HTTP	621	GET / HTTP/1.1
76	9.288997	192.168.1.6	195.181.175.55	HTTP	505	GET /css/style.css HTTP/1.1
78	9.324821	192.168.1.6	195.181.175.55	HTTP	509	GET /css/jssocials.css HTTP/1.1
79	9.327428	192.168.1.6	195.181.175.52	HTTP	520	GET /css/jssocials-theme-flat.css HTTP/1.1
80	9.329029	192.168.1.6	195.181.175.55	HTTP	513	GET /css/font-awesome.css HTTP/1.1
87	9.347066	192.168.1.6	195.181.175.45	HTTP	532	GET /img/refresh-icon.png HTTP/1.1
88	9.348942	192.168.1.6	84.17.57.5	HTTP	570	GET /http2/http1.html HTTP/1.1
127	9.479721	192.168.1.6	195.181.175.55	HTTP	529	GET /img/cdn77logo.png HTTP/1.1
129	9.598221	192.168.1.6	84.17.57.5	HTTP	489	GET /http2/tiles_final/tile_0.png HTTP/1.1
131	9.606827	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles_final/tile_1.png HTTP/1.1
133	9.634246	192.168.1.6	84.17.57.12	HTTP	488	GET /http2/tiles_final/tile_2.png HTTP/1.1
135	9.645524	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles_final/tile_3.png HTTP/1.1
136	9.650588	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles_final/tile_4.png HTTP/1.1
139	9.662339	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles_final/tile_5.png HTTP/1.1
156	9.718361	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles_final/tile_6.png HTTP/1.1



Follow Protocol Stream

Fitur Follow protocol stream pada wireshark sangat membantu untuk melihat aliran protokol seperti yang dilihat oleh lapisan aplikasi.

Fitur ini juga biasa digunakan untuk mencari kata sandi dalam aliran paket Telnet, TCP maupun hanya untuk mencoba memahami aliran data.



Follow TCP Stream Paket HTTP Request

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets, with packet 88 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
61	8.628352	192.168.1.6	195.181.175.55	HTTP	621	GET / HTTP/1.1
76	9.288997	192.168.1.6	195.181.175.55	HTTP	505	GET /css/style.css HTTP/1.1
78	9.324821	192.168.1.6	195.181.175.55	HTTP	509	GET /css/jssocials.css HTTP/1.1
79	9.327428	192.168.1.6	195.181.175.52	HTTP	520	GET /css/jssocials-theme-flat.css HTTP/1.1
80	9.329029	192.168.1.6	195.181.175.55	HTTP	513	GET /css/font-awesome.css HTTP/1.1
87	9.347066	192.168.1.6	195.181.175.45	HTTP	532	GET /img/refresh-icon.png HTTP/1.1
88	9.348942	192.168.1.6	84.17.57.5	HTTP	570	GET /http2/http1.html HTTP/1.1
127	9.479721	192.168.1.6	195.181.175.55	HTTP	529	GET /img/cdn771c...
129	9.598221	192.168.1.6	84.17.57.5	HTTP	489	GET /http2/tiles...
131	9.606827	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles...
133	9.634246	192.168.1.6	84.17.57.12	HTTP	488	GET /http2/tiles...
135	9.645524	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles...
136	9.650588	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles...
139	9.662339	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles...
156	9.718361	192.168.1.6	84.17.57.5	HTTP	488	GET /http2/tiles...

The packet details pane for packet 88 shows the following structure:

- Frame 88: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface \Device\NPF...
- Ethernet II, Src: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d), Dst: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
- Internet Protocol Version 4, Src: 192.168.1.6, Dst: 84.17.57.5
- Transmission Control Protocol, Src Port: 14495, Dst Port: 80, Seq: 1, Ack: 1, Len: 516
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The context menu for packet 88 is open, with the 'Follow' option selected, which has opened a sub-menu with the following options:

- TCP Stream (Ctrl+Alt+Shift+T)
- UDP Stream (Ctrl+Alt+Shift+U)
- TLS Stream (Ctrl+Alt+Shift+S)
- HTTP Stream (Ctrl+Alt+Shift+H)
- HTTP/2 Stream
- QUIC Stream

```
GET /http2/http1.html HTTP/1.1
Host: 1153288396.rsc.cdn77.org
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.http2demo.io/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: W/"570b88dc-45c3"
```

```
HTTP/1.1 200 OK
Date: Mon, 15 Jun 2020 13:37:34 GMT
Content-Type: text/html
Transfer-Encoding: chunked
ETag: W/"570b88dc-45c3"
Cache-Control: no-cache
Access-Control-Allow-Origin: *
Server: CDN77-Turbo
X-Cache: HIT
X-Age: 30007064
Connection: Keep-Alive
Content-Encoding: gzip
```

```
a99
.....\iW.H...."C..`Z!....G..M.E.{<..hH.,.....,hw.3..+...
[.*..UP.u`.....C.....ca{^...;wxP.....m.d...GF...s.....;l.s..S.....@l.{Qb.s.J..x.$....=u....x<(...('....=0.z..?.
9X.....I.1.N.xKlGj|.w.....;d.iZ~...i....u..T..P.,.jx..S.....bm...M..Y..4..$.Y=.9fej.Q.U.....z.H.d.....y.s.z.l...
+..E.;.....g..Dt.....*..h.A.J Ze..
.
...../. /. .0..0..1..1.,.^..!..@.....@.....9..r0..`....,s...*0(.....AY..e...U`PV..}A...@...<..y...@..`... ..A
...0(.aP&..L.A...2..e...&0(..w_....
0..`.(. P.A...@...".E...a.9..e".D..I0(.`P&..L.A...2Ix..I.:6.A...@ ..2..e...0..a.(. P.Y.d...@.s0(.aP...L.A...2..e
.....@...
.....r..r.#r.....:$.N.Y.cr.....:(g.N.Y.H/...())@x..".dX).Fq...@qV.H+P....E n
..". ....E ~
..
```

Packet 88. 2 client pkts, 8 server pkts, 3 turns. Click to select.

Entire conversation (8639 bytes)

Show and save data as ASCII

Stream 15

Find:

Find Next

Filter Out This Stream

Print

Save as...

Back

Close

Help

Konten dari TCP Stream akan ditampilkan dalam urutan yang sama seperti yang muncul di jaringan.

Karakter yang tidak dapat dicetak diganti oleh titik-titik.

Lalu lintas dari klien ke server berwarna merah, sedangkan lalu lintas dari server ke klien berwarna biru.



OSI Layer pada Wireshark



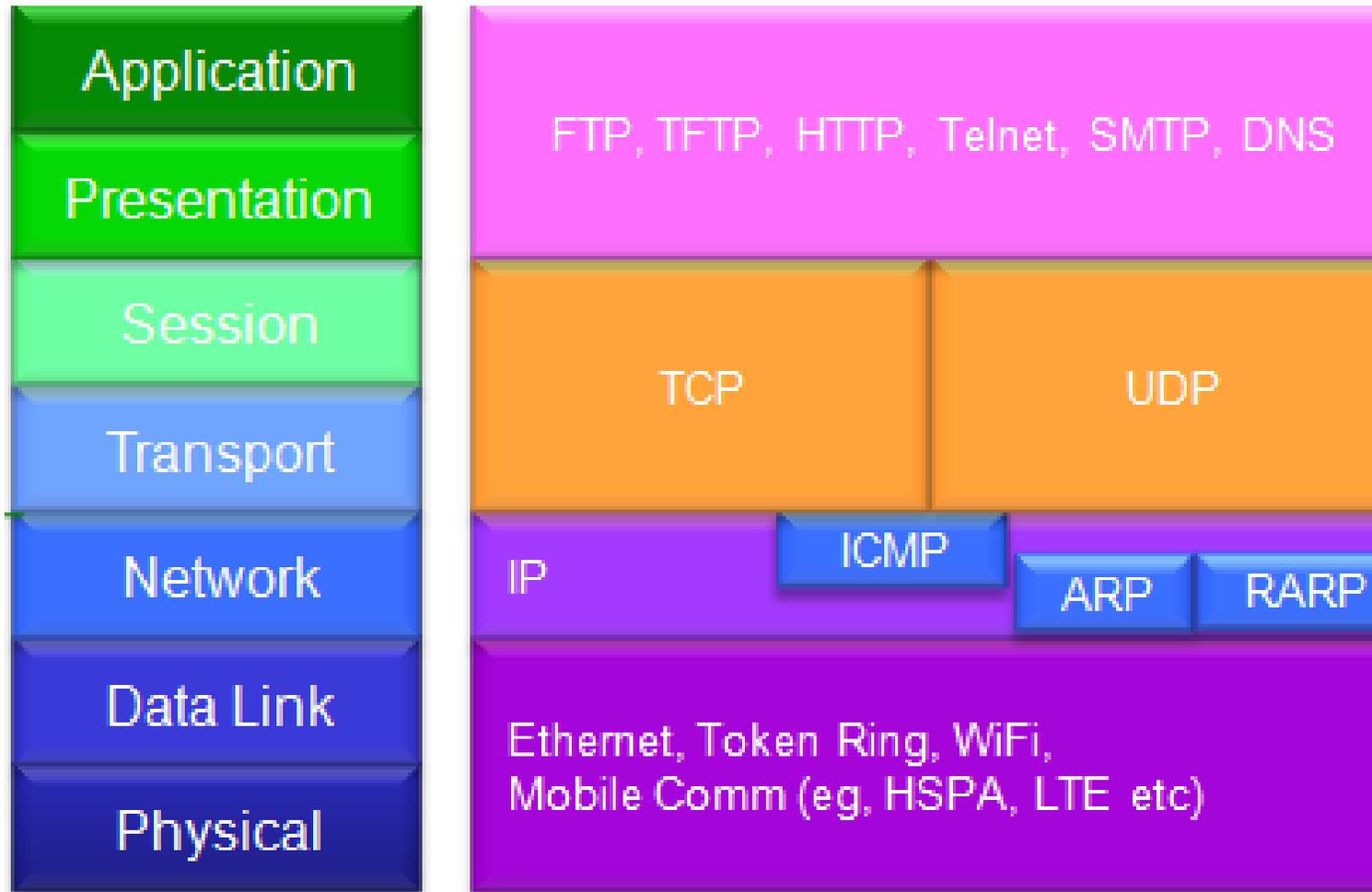


OSI layer pada wireshark

- Pada wireshark, kita dapat melihat detail protocol dari masing-masing paket di panel detail paket pada saat kita klik di paket yang kita pilih di Panel packet list



OSI Layer & Protocol



Mengetahui Detail Protocol per paket

*Wi-Fi

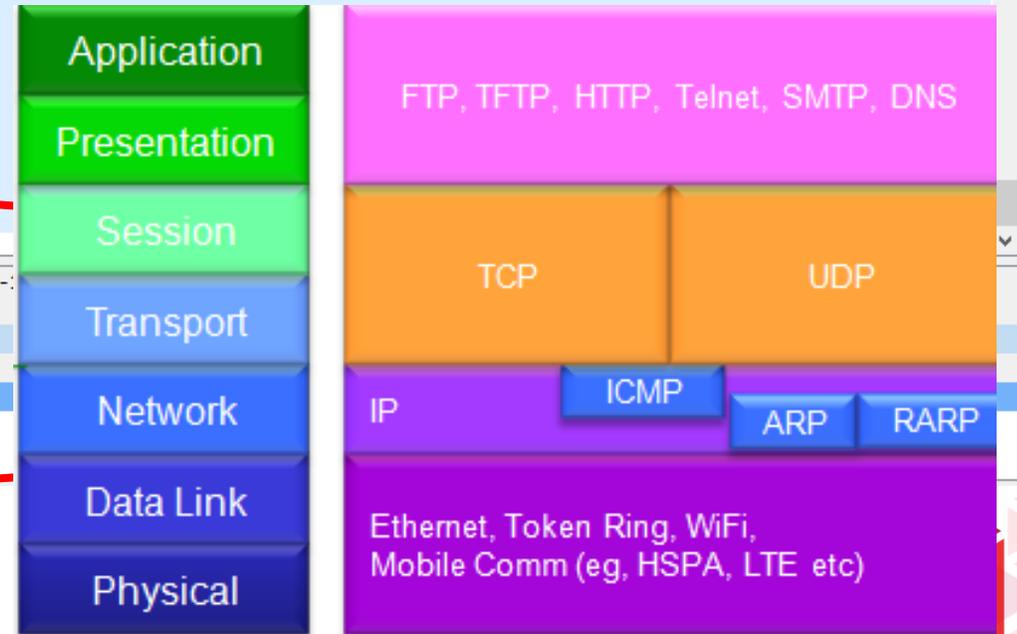
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Info
25625	558.494941	192.168.1.6	192.229.232.240	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?28763bbf77ccf54f HTTP/1.1
27426	599.363401	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
27513	602.370122	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
27928	605.377927	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
29178	608.500010	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
29723	611.501474	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
30283	614.507157	192.168.1.6	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
30470	626.839605	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
30487	627.849291	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
30500	628.854202	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
30504	629.859364	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
31224	746.815230	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
31228	747.818298	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
31238	748.825055	192.168.1.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Frame 76: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits) on interface \Device\NPF_{BB3EE3C1-...}

- Ethernet II, Src: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d), Dst: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
- Internet Protocol Version 4, Src: 192.168.1.6, Dst: 36.86.63.180
- Transmission Control Protocol, Src Port: 14613, Dst Port: 80, Seq: 1, Ack: 1, Len: 540
- Hypertext Transfer Protocol





Panel Packet Detail

OSI Layer pada Wireshark



Frame – Layer 1 OSI

```
▼ Frame 1: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface \Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15}, id 0
  ▼ Interface id: 0 (\Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15})
    Interface name: \Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15}
    Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 16, 2020 08:55:37.905035000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1592272537.905035000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 228 bytes (1824 bits)
    Capture Length: 228 bytes (1824 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
```

Ethernet – Layer 2 OSI

```
▼ Ethernet II, Src: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d), Dst: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
  ▼ Destination: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
    Address: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  ▼ Source: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d)
    Address: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Internet Protocol Version 4 – Layer 3 OSI

```
▼ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 74.125.24.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 214
  Identification: 0xa410 (42000)
  ▼ Flags: 0x4000, Don't fragment
    0... .... .... .... = Reserved bit: Not set
    .1.. .... .... .... = Don't fragment: Set
    ..0. .... .... .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (6)
  Header checksum: 0x7182 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.4
  Destination: 74.125.24.102
```

Transmission Control Protocol – Layer 4 & 5 OSI

Transmission Control Protocol, Src Port: 16851, Dst Port: 443, Seq: 1, Ack: 1, Len: 174

Source Port: 16851

Destination Port: 443

[Stream index: 0]

[TCP Segment Len: 174]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 625181290

[Next sequence number: 175 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 2331378382

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 254

[Calculated window size: 254]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x3867 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

▼ [SEQ/ACK analysis]

[Bytes in flight: 174]

[Bytes sent since last PSH flag: 174]

▼ [Timestamps]

[Time since first frame in this TCP stream: 0.000000000 seconds]

[Time since previous frame in this TCP stream: 0.000000000 seconds]

TCP payload (174 bytes)



Transport Layer Security – Layer 6 & 7 OSI

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 169

Encrypted Application Data: c0e7f729bdaef122845a5e81e8804965be71ec25499ef7e6...





Statistical Hierarchy Protocol

OSI Layer pada Wireshark





Statistical Hierarchy Protocol

- Ini adalah table dari semua protokol yang telah dicapture.
 - Di saat kita sedang melakukan capture paket dalam jumlah besar / jangka waktu yang cukup lama, terkadang kita ingin melihat distribusi dari protocol yang ada.
 - Berapa persen yang dicapture adalah protocol TCP, berapa persen IP, berapa persen DHCP, dan sebagainya.
 - Statistical Hierarchy Protocol dapat memudahkan kita untuk melakukan hal ini
- 

Statistical hierarchy protocol

The screenshot shows the Wireshark network protocol analyzer interface. The main window title is '*Wi-Fi'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The 'Statistics' menu is open, showing a list of statistical views. The 'Protocol Hierarchy' view is selected and expanded to show the following structure:

- Info
- GET /http2/http1.html HTTP/1.1
- 6 80 → 14495 [ACK] Seq=1 Ack=517 Win=28799 Len=0
- 5 80 → 14495 [PSH, ACK] Seq=1 Ack=517 Win=28799 Len=291 [TCP segment of a reassembled PDU]
- 9 80 → 14495 [ACK] Seq=292 Ack=517 Win=28799 Len=5 [TCP segment of a reassembled PDU]
- 6 80 → 14495 [ACK] Seq=297 Ack=517 Win=28799 Len=1452 [TCP segment of a reassembled PDU]
- 4 14495 → 80 [ACK] Seq=517 Ack=1749 Win=65340 Len=0
- 2 HTTP/1.1 200 OK (text/html)
- 4 14495 → 80 [ACK] Seq=517 Ack=3017 Win=64072 Len=0
- 9 GET /http2/tiles_final/tile_0.png HTTP/1.1
- 6 80 → 14495 [ACK] Seq=3017 Ack=952 Win=29234 Len=0
- 2 80 → 14495 [PSH, ACK] Seq=3017 Ack=952 Win=29234 Len=1448 [TCP segment of a reassembled PDU]
- 6 80 → 14495 [PSH, ACK] Seq=4465 Ack=952 Win=29234 Len=1452 [TCP segment of a reassembled PDU]
- 4 14495 → 80 [ACK] Seq=952 Ack=5917 Win=65340 Len=0
- 6 80 → 14495 [PSH, ACK] Seq=5917 Ack=952 Win=29234 Len=1452 [TCP segment of a reassembled PDU]
- 4 HTTP/1.1 200 OK (PNG)Continuation

The interface also shows a packet list on the left with columns for No., Time, and Source. The selected packet (No. 88) is expanded to show its protocol layers: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	10843	100.0	6957222	218 k	0	0	0
▼ Ethernet	100.0	10843	2.2	151802	4775	0	0	0
▼ Internet Protocol Version 6	1.1	115	0.1	4600	144	0	0	0
▼ User Datagram Protocol	0.7	78	0.0	624	19	0	0	0
Multicast Domain Name System	0.1	8	0.0	224	7	8	224	7
Link-local Multicast Name Resolution	0.0	4	0.0	88	2	4	88	2
Domain Name System	0.6	66	0.1	4923	154	66	4923	154
Internet Control Message Protocol v6	0.3	37	0.0	1445	45	37	1445	45
▼ Internet Protocol Version 4	98.8	10718	3.1	214360	6743	0	0	0
▼ User Datagram Protocol	0.4	44	0.0	352	11	0	0	0
Simple Service Discovery Protocol	0.2	20	0.0	3028	95	20	3028	95
NetBIOS Name Service	0.1	6	0.0	300	9	6	300	9
Multicast Domain Name System	0.1	8	0.0	224	7	8	224	7
Link-local Multicast Name Resolution	0.0	4	0.0	88	2	4	88	2
Domain Name System	0.1	6	0.0	802	25	6	802	25
▼ Transmission Control Protocol	98.4	10674	94.5	6572204	206 k	6059	3512800	110 k
VSS Monitoring Ethernet trailer	8.7	939	0.0	1878	59	939	1878	59
Transport Layer Security	34.2	3705	81.8	5693654	179 k	3658	5586093	175 k
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Hypertext Transfer Protocol	0.0	2	0.0	541	17	2	541	17
Data	0.1	15	0.3	21450	674	15	21450	674
Address Resolution Protocol	0.1	10	0.0	280	8	10	280	8

Semua protocol pada OSI layer 1 s.d 7 juga dapat ditemukan di hierarchy protocol ini, namun tidak sedetail pada panel packet detail



Kolom Pada Tabel Statistical Hierarchy Protokol

- Protokol : Nama protokol
 - Percent Paket : Persentase paket protokol (relatif terhadap semua paket dalam penangkapan)
 - Paket : Jumlah total paket protokol ini.
 - Percent Bytes: Persentase byte protokol (relatif terhadap total byte dalam tangkapan)
 - Bytes : Jumlah total byte dari protokol ini.
 - Bits / s : Bandwidth protokol (relatif terhadap waktu penangkapan)
- 



Contoh Kasus Benchmarking di jaringan

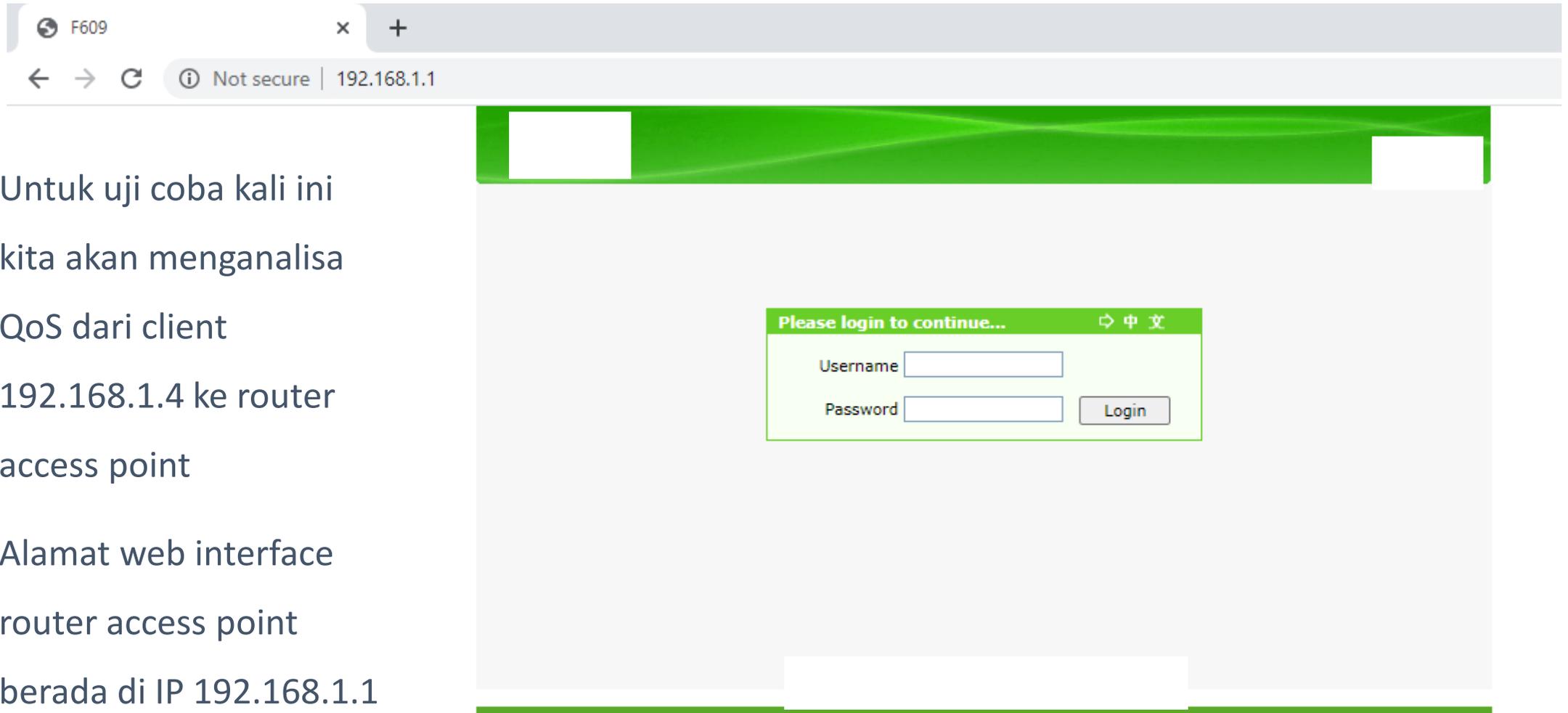
- Misal diketahui pada saat jaringan berjalan seperti biasa bahwa 10 persen trafik di jaringan biasanya adalah trafik ARP.
 - Namun suatu hari ditemukan trafik ARP sebesar 50 persen, maka ini ada sesuatu hal yang salah di jaringan (misal terdapat aktivitas ARP Flooding, dll) sehingga sebagai network administrator dapat segera melakukan tindakan.
 - Aktivitas ini bisa kita lakukan dengan menggunakan table statistical hierarchy protocol ini.
 - Dikarenakan jika menjumlah semua paket di masing-masing protocol secara manual akan menghabiskan waktu dan tenaga.
- 



Mencari parameter QoS pada wireshark



- Untuk uji coba kali ini kita akan menganalisa QoS dari client 192.168.1.4 ke router access point
- Alamat web interface router access point berada di IP 192.168.1.1





Tahapan Capture

- Seperti contoh sebelumnya, kita start capture di wifi interface pada wireshark
 - Selanjutnya, kunjungi URL target 192.168.1.1
 - Setelah halaman web router access point terbuka sempurna, kemudian stop capture pada wireshark
- 

Akan muncul banyak sekali paket yang tercapture di wireshark (bisa jadi ada paket ARP, TCP, UDP lainnya selain aktivitas browsing yang kita lakukan ke target 192.168.1.1)

The image shows a Wireshark network traffic capture window. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 1460 is highlighted, showing it is a TLSv1.3 packet of length 180 bytes. Below the packet list, the packet details pane shows the structure of the TLSv1.3 packet, including the Checksum, Urgent pointer, and SEQ/ACK analysis. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Time since previous frame in this TCP stream	Time since first frame in this TCP stream	Info
1445	30.915735	192.168.1.4	40.119.211.203	TCP	54	0.000163000	30.915735000	[TCP Keep-Alive ACK] 16644 → 443 [ACK]
1446	30.939210	40.119.211.203	192.168.1.4	TCP	56	0.023475000	30.939210000	[TCP Dup ACK 1#1] 443 → 16644 [ACK] Seq=16644
1447	34.200656	fe80::1	fe80::c4c5:9f4e:23b...	ICMPv6	86			Neighbor Solicitation for fe80::c4c5:9f4e:23b...
1448	34.200780	fe80::c4c5:9f4e:23b...	fe80::1	ICMPv6	86			Neighbor Advertisement fe80::c4c5:9f4e:23b...
1449	36.655043	172.217.194.84	192.168.1.4	TCP	56	30.356100000	31.011607000	[TCP Keep-Alive ACK] 443 → 17774 [ACK] Seq=17774
1450	36.655147	192.168.1.4	172.217.194.84	TCP	54	0.000104000	31.011711000	[TCP Keep-Alive ACK] 17774 → 443 [ACK] Seq=17774
1451	36.656427	172.217.194.84	192.168.1.4	TCP	56	0.001280000	31.012991000	[TCP Dup ACK 159#1] 443 → 17774 [ACK] Seq=17774
1452	37.475463	74.125.68.94	192.168.1.4	TCP	66	30.642436000	31.050515000	[TCP Keep-Alive ACK] 443 → 17778 [ACK] Seq=17778
1453	37.475465	74.125.68.94	192.168.1.4	TCP	56	0.000020000	31.050517000	[TCP Dup ACK 242#1] 443 → 17778 [ACK] Seq=17778
1454	37.475573	192.168.1.4	74.125.68.94	TCP	54	0.000108000	31.050625000	[TCP Dup ACK 232#1] 17778 → 443 [ACK] Seq=17778
1455	37.476263	74.125.200.95	192.168.1.4	TCP	56	30.644296000	31.020502000	[TCP Keep-Alive ACK] 443 → 17779 [ACK] Seq=17779
1456	37.476365	192.168.1.4	74.125.200.95	TCP	54	0.000102000	31.020604000	[TCP Keep-Alive ACK] 17779 → 443 [ACK] Seq=17779
1457	37.489213	74.125.200.95	192.168.1.4	TCP	56	0.012848000	31.033452000	[TCP Dup ACK 241#1] 443 → 17779 [ACK] Seq=17779
1458	39.168776	fe80::c4c5:9f4e:23b...	fe80::1	ICMPv6	86			Neighbor Solicitation for fe80::1 from fe80::c4c5:9f4e:23b...
1459	39.170318	fe80::1	fe80::c4c5:9f4e:23b...	ICMPv6	78			Neighbor Advertisement fe80::1 (rtr, s...
1460	40.081079	192.168.1.4	74.125.24.139	TLSv1.3	180	11.204152000	31.941948000	Application Data

Checksum: 0xd52d [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.025799000 seconds]
[Bytes in flight: 126]
[Bytes sent since last PSH flag: 126]
[Timestamps]
[Time since first frame in this TCP stream: 31.941948000 seconds]

0020 18 b5 45 75 01 bb a0 79 de 44 11 70 2d b2 50 18 ..Eu...y.D.p--P.
0030 00 ff d5 2d 00 00 17 03 03 00 79 ed d7 98 24 14y...\$.
0040 f4 c8 44 5d 4b 33 a6 bb 8d fb 86 82 15 4a 2f a4 ...D]K3...J/.
0050 c3 95 97 5c cd bf df 9e 95 ca 30 78 45 8f 4e 09 ... \...0xE.N.
0060 7e 67 08 49 0b 78 ce 33 c2 f8 76 38 99 0a 59 7e ~g:I:x:3 ~v8~Y~
0070 a3 4d da 31 fc 5b a3 8e a0 7c 97 95 89 9d f8 9d ~M:1[...]-.....
0080 c3 f1 86 f8 15 1c 8c 93 21 1d 3e 74 2c 71 18 58!>t,q~X

Time relative to first frame in this TCP stream (tcp.time_relative) | Packets: 1460 · Displayed: 1460 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

The image shows the Wireshark network protocol analyzer interface. The 'Statistics' menu is open, with 'Conversations' selected. The main display area shows a list of captured packets. Packet 33 is selected, and its details are shown in the lower pane, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol headers. The status bar at the bottom indicates that 198 packets are displayed out of 198 captured.

No.	Time	Source
183	0.799821	192.168.1.4
184	0.801299	192.168.1.1
185	1.160464	74.125.68.101
186	1.160548	192.168.1.4
187	1.180094	74.125.68.101
188	1.699661	172.217.194.1
189	1.699757	192.168.1.4
190	1.719136	172.217.194.1
191	1.896858	74.125.200.18
192	1.896947	192.168.1.4
193	1.921277	74.125.200.18
194	4.819558	fe80::c4c5:9f...
195	4.863877	fe80::1
196	7.728317	40.90.189.152
197	7.728419	192.168.1.4
198	7.728714	40.90.189.152

Maka, untuk mempermudah analisis kita, kita perlu memfilter IP tujuan kita terlebih dahulu. Untuk mempermudah pembuatan filter, kita bisa melakukan pengecekan langsung pada menu conversation

Wireshark · Conversations · Wi-Fi

Ethernet · 2 IPv4 · 3 IPv6 · 2 TCP · 11 UDP · 1

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
74.125.24.100	192.168.1.4	3	162	1	54	2	108	0.000000	0.1131	3820	
172.217.194.94	192.168.1.4	26	7848	13	5165	13	2683	0.219146	0.4698	87 k	
192.168.1.1	192.168.1.4	162	102 k	102	95 k	60	7255	0.000002	0.6217	1228 k	

- Apply as Filter ▶ Selected ▶ A → B
- Prepare a Filter ▶ Not Selected ▶ A → B
- Find ▶ ...and Selected ▶ B → A
- Colorize ▶ ...or Selected ▶ A → Any
- ▶ ...and not Selected ▶ A → Any
- ▶ ...or not Selected ▶ Any → A
- Any → B
- Any → B
- B → Any

Kemudian pilih tab IPv4, dan pilih yang bagian Address A 192.168.1.1 dan Address B 192.168.1.4

Klik kanan, pilih apply as filter, selected, pilih yang panah arah B ke A (source Address B, destination address A)

Hasil Apply Filter

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst==192.168.1.1 && ip.src==192.168.1.4

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000902	192.168.1.4	192.168.1.1	TCP	66	18309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.001384	192.168.1.4	192.168.1.1	TCP	66	18310 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.107477	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.109027	192.168.1.4	192.168.1.1	HTTP	546	GET / HTTP/1.1
8	0.110599	192.168.1.4	192.168.1.1	TCP	54	18310 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
16	0.159079	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=4787 Win=65536 Len=0
19	0.159541	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=7707 Win=65536 Len=0
22	0.160023	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=10627 Win=65536 Len=0
25	0.160320	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=13547 Win=65536 Len=0
34	0.163715	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=25227 Win=65536 Len=0
39	0.164262	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=31067 Win=65536 Len=0
42	0.165748	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=33987 Win=65536 Len=0
45	0.166155	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=36907 Win=65536 Len=0
48	0.167174	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=38822 Win=65536 Len=0
49	0.169005	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [FIN, ACK] Seq=493 Ack=38822 Win=65536 Len=0
59	0.276081	192.168.1.4	192.168.1.1	HTTP	469	GET /skin/priorgreen/css/login.css HTTP/1.1
60	0.277293	192.168.1.4	192.168.1.1	TCP	66	18312 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

0101 = Header Length: 20 bytes (5)

- > Flags: 0x018 (PSH, ACK)
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0x33b6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
- ▼ [SEQ/ACK analysis]
[iRTT: 0.106575000 seconds]
[Bytes in flight: 492]
[Bytes sent since last PSH flag: 492]
- ▼ [Timestamps]
[Time since first frame in this TCP stream: 0.108125000 seconds]

0020 01 01 47 85 00 50 7b e5 39 59 45 df 1b d7 50 18 ..G..P{. 9YE...P.
0030 01 00 33 b6 00 00 47 45 54 20 2f 20 48 54 54 50 ...3...GE T / HTTP

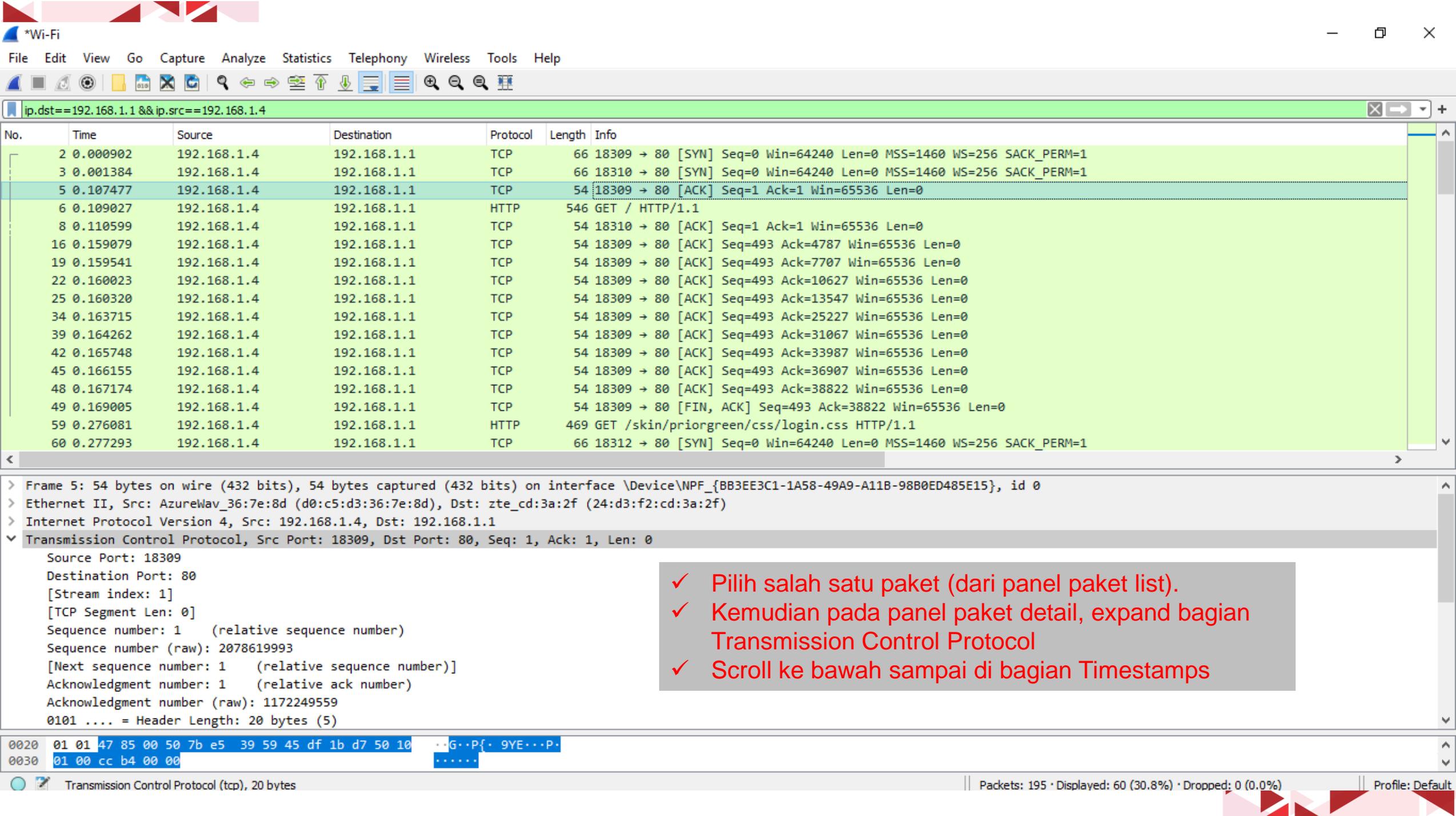
Time relative to first frame in this TCP stream (tcp.time_relative) | Packets: 195 · Displayed: 60 (30.8%) · Dropped: 0 (0.0%) | Profile: Default



Delay Paket TCP

Mencari Parameter QoS





ip.dst==192.168.1.1 && ip.src==192.168.1.4

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000902	192.168.1.4	192.168.1.1	TCP	66	18309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.001384	192.168.1.4	192.168.1.1	TCP	66	18310 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.107477	192.168.1.4	192.168.1.1	TCP	54	[18309 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.109027	192.168.1.4	192.168.1.1	HTTP	546	GET / HTTP/1.1
8	0.110599	192.168.1.4	192.168.1.1	TCP	54	18310 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
16	0.159079	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=4787 Win=65536 Len=0
19	0.159541	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=7707 Win=65536 Len=0
22	0.160023	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=10627 Win=65536 Len=0
25	0.160320	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=13547 Win=65536 Len=0
34	0.163715	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=25227 Win=65536 Len=0
39	0.164262	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=31067 Win=65536 Len=0
42	0.165748	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=33987 Win=65536 Len=0
45	0.166155	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=36907 Win=65536 Len=0
48	0.167174	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [ACK] Seq=493 Ack=38822 Win=65536 Len=0
49	0.169005	192.168.1.4	192.168.1.1	TCP	54	18309 → 80 [FIN, ACK] Seq=493 Ack=38822 Win=65536 Len=0
59	0.276081	192.168.1.4	192.168.1.1	HTTP	469	GET /skin/priorgreen/css/login.css HTTP/1.1
60	0.277293	192.168.1.4	192.168.1.1	TCP	66	18312 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15}, id 0
> Ethernet II, Src: AzureWav_36:7e:8d (d0:c5:d3:36:7e:8d), Dst: zte_cd:3a:2f (24:d3:f2:cd:3a:2f)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
v Transmission Control Protocol, Src Port: 18309, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 18309
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 2078619993
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1172249559
0101 = Header Length: 20 bytes (5)

- ✓ Pilih salah satu paket (dari panel paket list).
- ✓ Kemudian pada panel paket detail, expand bagian Transmission Control Protocol
- ✓ Scroll ke bawah sampai di bagian Timestamps

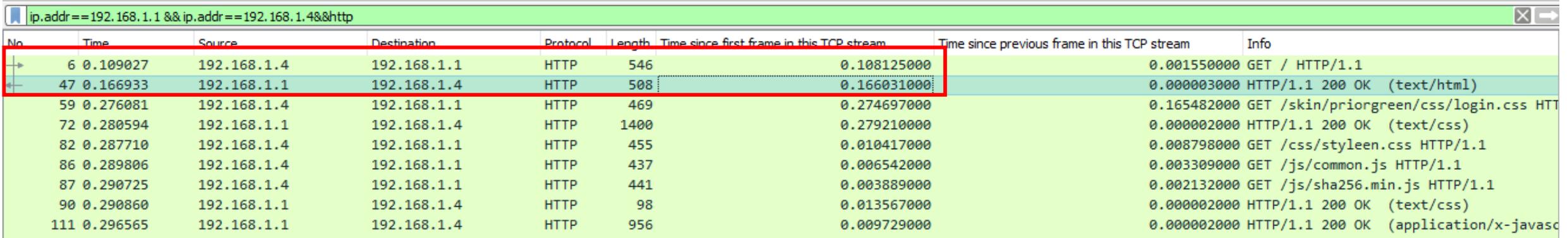
0020 01 01 47 85 00 50 7b e5 39 59 45 df 1b d7 50 10 ..G..P{.9YE...P.
0030 01 00 cc b4 00 00

No.	Time	Source	Destination	Protocol	Length	Time since first frame in this TCP stream	Time since previous frame in this TCP stream	Info
2	0.000902	192.168.1.4	192.168.1.1	TCP	66	0.000000000	0.000000000	18309 → 80 [SYN] Seq=0 Win=64240 Len=0
3	0.001384	192.168.1.4	192.168.1.1	TCP	66	0.000000000	0.000000000	18310 → 80 [SYN] Seq=0 Win=64240 Len=0
5	0.107477	192.168.1.4	192.168.1.1	TCP	54	0.106575000	0.000335000	18309 → 80 [ACK] Seq=1 Ack=1 Win=65536
6	0.109027	192.168.1.4	192.168.1.1	HTTP	546	0.108125000	0.001550000	GET / HTTP/1.1
8	0.110599	192.168.1.4	192.168.1.1	TCP	54	0.109215000	0.000229000	18310 → 80 [ACK] Seq=1 Ack=1 Win=65536
16	0.159079	192.168.1.4	192.168.1.1	TCP	54	0.158177000	0.000198000	18309 → 80 [ACK] Seq=493 Ack=4787 Win=
19	0.159541	192.168.1.4	192.168.1.1	TCP	54	0.158639000	0.000147000	18309 → 80 [ACK] Seq=493 Ack=7707 Win=
22	0.160023	192.168.1.4	192.168.1.1	TCP	54	0.159121000	0.000165000	18309 → 80 [ACK] Seq=493 Ack=10627 Win
25	0.160320	192.168.1.4	192.168.1.1	TCP	54	0.159418000	0.000117000	18309 → 80 [ACK] Seq=493 Ack=13547 Win
34	0.163715	192.168.1.4	192.168.1.1	TCP	54	0.162813000	0.000429000	18309 → 80 [ACK] Seq=493 Ack=25227 Win
39	0.164262	192.168.1.4	192.168.1.1	TCP	54	0.163360000	0.000234000	18309 → 80 [ACK] Seq=493 Ack=31067 Win
42	0.165748	192.168.1.4	192.168.1.1	TCP	54	0.164846000	0.000099000	18309 → 80 [ACK] Seq=493 Ack=33987 Win
45	0.166155	192.168.1.4	192.168.1.1	TCP	54	0.165253000	0.000140000	18309 → 80 [ACK] Seq=493 Ack=36907 Win
48	0.167174	192.168.1.4	192.168.1.1	TCP	54	0.166272000	0.000241000	18309 → 80 [ACK] Seq=493 Ack=38822 Win
49	0.169005	192.168.1.4	192.168.1.1	TCP	54	0.168103000	0.001831000	18309 → 80 [FIN, ACK] Seq=493 Ack=3882
59	0.276081	192.168.1.4	192.168.1.1	HTTP	469	0.274697000	0.165482000	GET /skin/priorgreen/css/login.css HTT
60	0.277293	192.168.1.4	192.168.1.1	TCP	66	0.000000000	0.000000000	18312 → 80 [SYN] Seq=0 Win=64240 Len=0

Maka bagian Packet List akan terlihat 2 kolom baru

1. Time since first frame in this TCP stream (selisih waktu antara paket tersebut dengan paket pertama di aliran TCP ini)
2. Time since previous frame in this TCP stream (selisih waktu antara paket tersebut dengan paket sebelumnya di aliran TCP ini)

Dari kedua kolom yang telah didapatkan, maka kita dapat melihat dengan jelas delay antar paket (selisih kedatangan paket kedua dengan paket pertama, dan seterusnya) maupun delay kedatangan dari paket ke N dengan paket pertama



No.	Time	Source	Destination	Protocol	Length	Time since first frame in this TCP stream	Time since previous frame in this TCP stream	Info
6	0.109027	192.168.1.4	192.168.1.1	HTTP	546	0.108125000	0.001550000	GET / HTTP/1.1
47	0.166933	192.168.1.1	192.168.1.4	HTTP	508	0.166031000	0.000003000	HTTP/1.1 200 OK (text/html)
59	0.276081	192.168.1.4	192.168.1.1	HTTP	469	0.274697000	0.165482000	GET /skin/priorgreen/css/login.css HTTP/1.1
72	0.280594	192.168.1.1	192.168.1.4	HTTP	1400	0.279210000	0.000002000	HTTP/1.1 200 OK (text/css)
82	0.287710	192.168.1.4	192.168.1.1	HTTP	455	0.010417000	0.008798000	GET /css/styleen.css HTTP/1.1
86	0.289806	192.168.1.4	192.168.1.1	HTTP	437	0.006542000	0.003309000	GET /js/common.js HTTP/1.1
87	0.290725	192.168.1.4	192.168.1.1	HTTP	441	0.003889000	0.002132000	GET /js/sha256.min.js HTTP/1.1
90	0.290860	192.168.1.1	192.168.1.4	HTTP	98	0.013567000	0.000002000	HTTP/1.1 200 OK (text/css)
111	0.296565	192.168.1.1	192.168.1.4	HTTP	956	0.009729000	0.000002000	HTTP/1.1 200 OK (application/x-javascript)

Sebagai contoh, ingin dilakukan perhitungan delay TCP pada protocol HTTP, sehingga pada gambar di atas ditambahkan filter `&&http`. Sehingga dapat digitung delay Round Trip menggunakan variable ***time since first frame in this TCP stream*** dimana Client 192.168.1.4 pada saat melakukan request GET HTTP ke 192.168.1.1 mendapatkan balasan HTTP OK (paket nomor 6 sampai dengan paket nomor 47) adalah $0.16603031000 \text{ ms} - 0.108125000 \text{ ms} = \mathbf{0.05790531 \text{ ms}}$



Troughput Paket TCP

Mencari Parameter QoS



Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.1 && ip.addr==192.168.1.1

No.	Time	Source
2	0.000902	192.168.1.4
3	0.001384	192.168.1.4
4	0.107142	192.168.1.1
5	0.107477	192.168.1.4
6	0.109027	192.168.1.4
7	0.110370	192.168.1.1
8	0.110599	192.168.1.4
11	0.114236	192.168.1.1
12	0.158277	192.168.1.1
13	0.158877	192.168.1.1
14	0.158879	192.168.1.1
15	0.158881	192.168.1.1
16	0.159079	192.168.1.4
17	0.159392	192.168.1.1
18	0.159394	192.168.1.1
19	0.159541	192.168.1.4
20	0.159856	192.168.1.1

- Capture File Properties
- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP
- HTTP2
- Sametime
- TCP Stream Graphs**
 - Time Sequence (Stevens)
 - Time Sequence (tcptrace)
 - Throughput**
 - Round Trip Time
 - Window Scaling
- UDP Multicast Streams
- F5
- IPv4 Statistics
- IPv6 Statistics

	Time since first frame in this TCP stream	Time since previous frame in this TCP stream	Info
6	0.000000000	0.000000000	18309 → 80 [SYN] Seq=0 Win=64240 Len=0
6	0.000000000	0.000000000	18310 → 80 [SYN] Seq=0 Win=64240 Len=0
6	0.106240000	0.106240000	80 → 18309 [SYN, ACK] Seq=0 Ack=1 Win=
4	0.106575000	0.000335000	18309 → 80 [ACK] Seq=1 Ack=1 Win=65536
6	0.108125000	0.001550000	GET / HTTP/1.1
6	0.108986000	0.108986000	80 → 18310 [SYN, ACK] Seq=0 Ack=1 Win=
4	0.109215000	0.000229000	18310 → 80 [ACK] Seq=1 Ack=1 Win=65536
4	0.113334000	0.005209000	80 → 18309 [ACK] Seq=1 Ack=493 Win=156
0	0.157375000	0.044041000	80 → 18309 [PSH, ACK] Seq=1 Ack=493 Wi
4	0.157975000	0.000600000	80 → 18309 [ACK] Seq=407 Ack=493 Win=1
4	0.157977000	0.000002000	80 → 18309 [ACK] Seq=1867 Ack=493 Win=
4	0.157979000	0.000002000	80 → 18309 [ACK] Seq=3327 Ack=493 Win=
4	0.158177000	0.000198000	18309 → 80 [ACK] Seq=493 Ack=4787 Win=
4	0.158490000	0.000313000	80 → 18309 [ACK] Seq=4787 Ack=493 Win=
4	0.158492000	0.000002000	80 → 18309 [ACK] Seq=6247 Ack=493 Win=
4	0.158639000	0.000147000	18309 → 80 [ACK] Seq=493 Ack=7707 Win=
4	0.158954000	0.000315000	80 → 18309 [ACK] Seq=7707 Ack=493 Win=

Interface \Device\NPF_{BB3EE3C1-1A58-49A9-A11B-98B0ED485E15}, id 0
(24:d3:f2:cd:3a:2f)

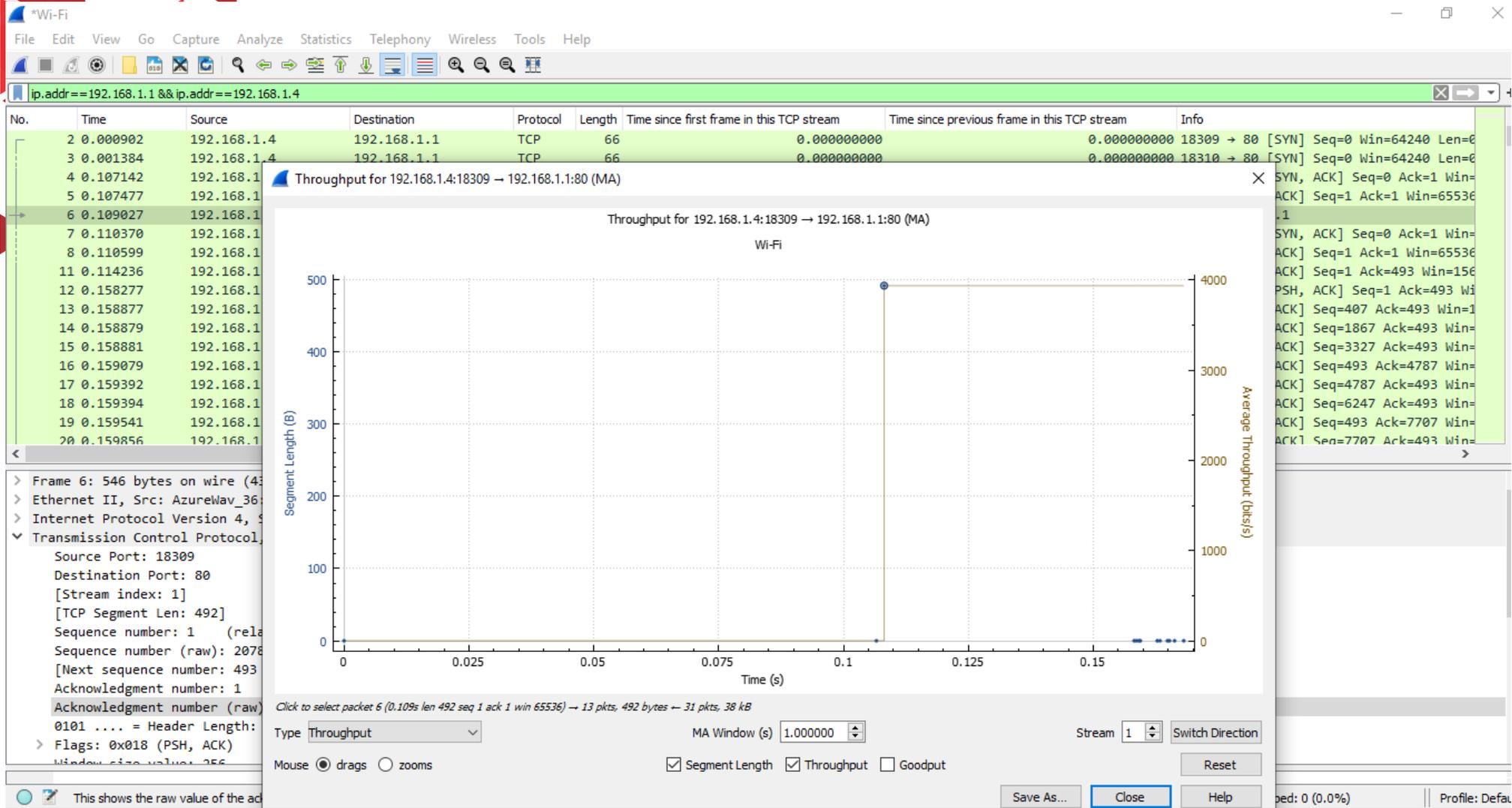
1, Len: 492

Source Port: 18309
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 492]
Sequence number: 1 (relative)
Sequence number (raw): 20786199
[Next sequence number: 493
Acknowledgment number: 1 (relative)
Acknowledgment number (raw): 11010101
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 256

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 bytes

Packets: 195 · Displayed: 162 (83.1%) · Dropped: 0 (0.0%)

Profile: Default



Throughput dari semua paket yang dikirim 192.168.1.4 ke 192.168.1.1 adalah **492 B** dan paket yang diterima 192.168.1.4 dari 192.168.1.1 adalah : **38kB**