JARINGAN KOMPUTER – TUGAS PENDAHULUAN MODUL 10
IP (INTERNET PROTOCOL)

Nama : Muhammad Hamzah Haifan Ma'ruf

NIM : 2311102091

Kelas : S1IF-11-07

Kode Dosen : AIZ

JAWABAN MODUL

A. Teori

1. Hubungan antara OSI Model dan TCP/IP Model

   OSI Model terdiri dari tujuh lapisan: Physical, Data Link, Network, Transport, Session, Presentation, dan Application. Sementara itu, TCP/IP Model memiliki empat lapisan: Network Access, Internet, Transport, dan Application. Lapisan-lapisan ini memiliki fungsi yang serupa namun dengan pembagian yang berbeda. Lapisan Application pada TCP/IP mencakup tiga lapisan teratas OSI, yaitu Application, Presentation, dan Session. Lapisan Transport pada kedua model memiliki fungsi yang sama, yaitu mengatur komunikasi end-to-end dan kontrol error. Lapisan Internet pada TCP/IP setara dengan Network pada OSI, yang bertanggung jawab atas routing dan pengalamatan. Terakhir, lapisan Network Access pada TCP/IP mencakup Data Link dan Physical pada OSI, yang menangani transmisi data secara fisik melalui media jaringan. Protokol seperti HTTP dan DNS berada pada lapisan Application; TCP dan UDP berada pada lapisan Transport; sedangkan IP berada pada lapisan Network (OSI) atau Internet (TCP/IP).

2. Konsep Dasar dan Format Alamat IPv4

   Alamat IPv4 adalah alamat 32-bit yang digunakan untuk mengidentifikasi perangkat dalam jaringan. Alamat ini ditulis dalam format desimal bertitik, terdiri dari empat oktet yang dipisahkan oleh titik, misalnya 192.168.0.1. Setiap oktet merepresentasikan 8 bit, dengan nilai antara 0 hingga 255. Alamat IP dibagi menjadi bagian jaringan dan host, yang ditentukan oleh subnet mask. Alamat jaringan memiliki semua bit host diatur ke 0, alamat broadcast memiliki semua bit host diatur ke 1, dan alamat host berada di antara keduanya. Subnet mask digunakan untuk menentukan bagian mana dari alamat IP yang mewakili jaringan dan mana yang mewakili host. Contohnya, subnet mask 255.255.255.0 atau /24 dalam notasi CIDR menunjukkan bahwa 24 bit pertama adalah bagian jaringan.

3. Fragmentasi dalam IPv4

   Fragmentasi terjadi ketika paket IP lebih besar dari ukuran Maximum Transmission Unit (MTU) jaringan dan harus dibagi menjadi beberapa bagian agar dapat dikirim. Router akan memecah paket menjadi fragment berdasarkan MTU, dan setiap fragment membawa informasi seperti offset dan flag untuk menandai apakah masih ada potongan lain. Tujuan (host penerima) akan merakit ulang fragmentasi tersebut. Fragmentasi menambah overhead karena membutuhkan tambahan header untuk setiap fragment dan meningkatkan beban pemrosesan pada router dan host. Jika satu fragment hilang, seluruh paket harus dikirim ulang, yang dapat menyebabkan penurunan kinerja jaringan.

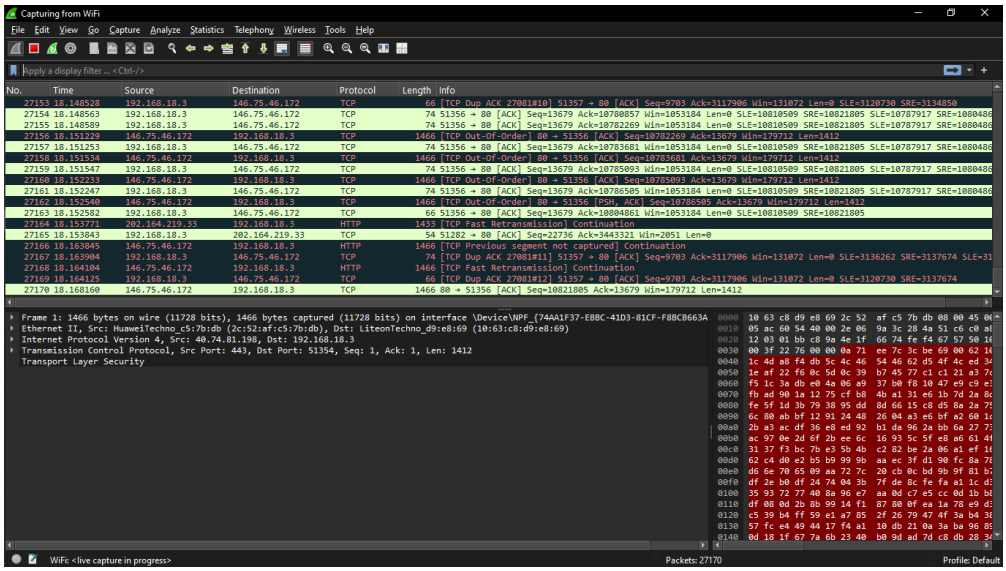
4. Perbedaan IPv6 dan IPv4

   IPv6 adalah versi terbaru dari protokol IP yang dirancang untuk menggantikan IPv4. Perbedaan utama antara keduanya terletak pada panjang alamat, struktur header, dan pendekatan fragmentasi. IPv4 menggunakan alamat 32-bit, sedangkan IPv6 menggunakan alamat 128-bit, memungkinkan lebih banyak alamat unik. Header IPv6 lebih sederhana dan efisien dibandingkan IPv4. Dalam hal fragmentasi, IPv6 tidak mendukung fragmentasi di router intermediate; fragmentasi hanya dilakukan oleh pengirim, dan penerima akan merakit kembali paket. Notasi singkat "::" dalam IPv6 digunakan untuk menyederhanakan penulisan alamat dengan menggantikan satu atau lebih blok nol berturut-turut, sehingga alamat menjadi lebih ringkas dan mudah dibaca.

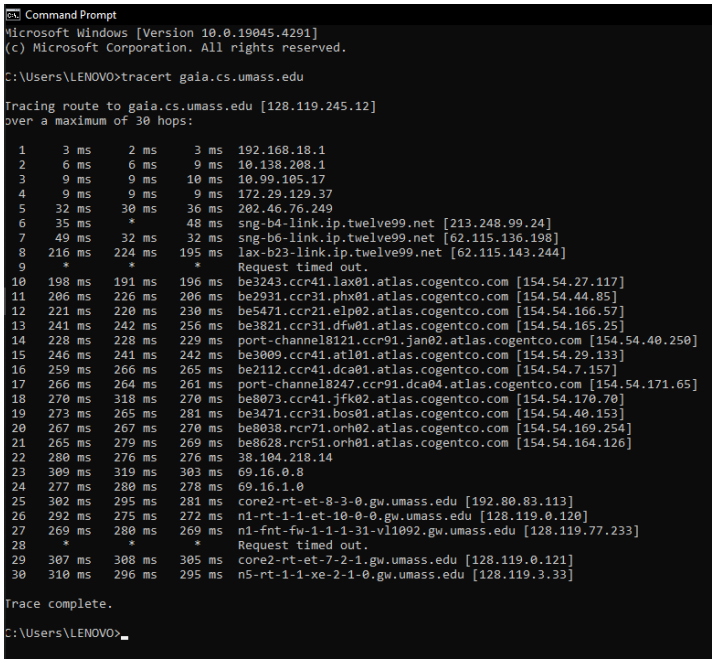
B. Traceroute

Lakukan setiap langkah berikut dan sertakan screenshot-nya:

1. Buka Wireshark dan mulai penangkapan paket



2. Eksekusi Traceroute sesuai OS yang anda gunakan:
   Untuk Pengguna Windows:
   - Ketik dua perintah tracert menggunakan dua situs web
   - (gaia.cs.umass.edu dan telkomuniversity.ac.id) sebagai tujuan.



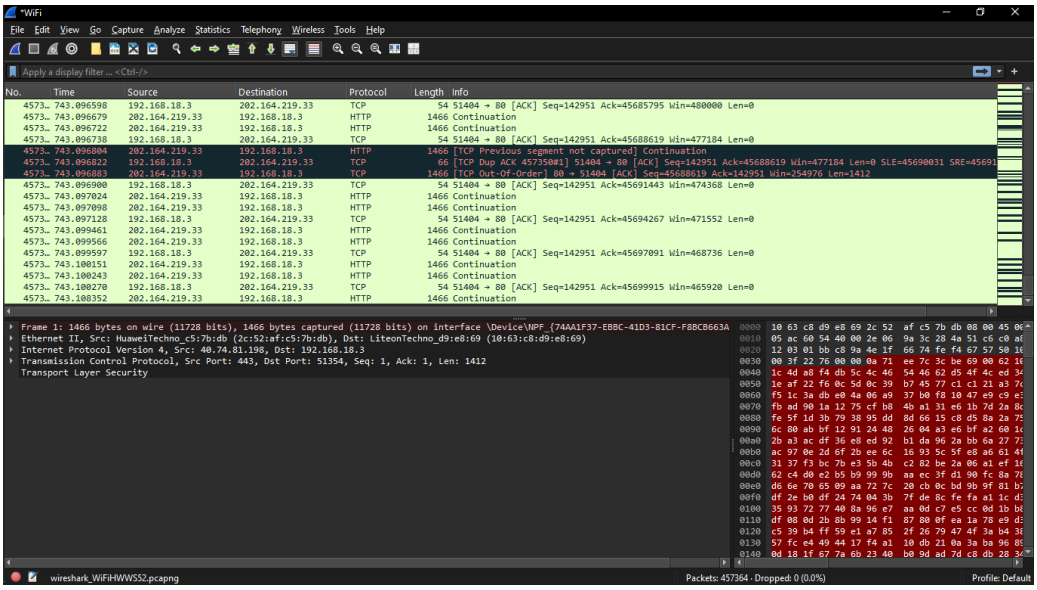
```
C:\Users\LENOVO>tracert telkomuniversity.ac.id

Tracing route to telkomuniversity.ac.id [172.67.74.57]
over a maximum of 30 hops:

  1     5 ms     2 ms     2 ms  192.168.18.1
  2    11 ms     8 ms    12 ms  10.138.208.1
  3    10 ms    16 ms    11 ms  10.99.105.17
  4     9 ms    12 ms    10 ms  172.29.129.37
  5    36 ms    32 ms    35 ms  202.46.76.249
  6    54 ms    35 ms    48 ms  cloudflare2.sgix.sg [103.16.102.229]
  7    59 ms    40 ms   119 ms  162.158.160.163
  8    31 ms    33 ms    40 ms  172.67.74.57

Trace complete.
```

3. Hentikan penangkapan paket.



C. Analisa Traceroute

1. Identifikasi Traceroute

- Versi Windows
  a. Saat menjalankan perintah tracert, jumlah hop (router) yang dilewati untuk masing-masing website bervariasi. Misalnya, ke gaia.cs.umass.edu bisa mencapai sekitar 18–25 hop, tergantung pada jalur jaringan internasional yang ditempuh, sedangkan ke telkomuniversity.ac.id biasanya lebih sedikit, sekitar 8–15 hop, karena masih dalam satu wilayah geografis. Jika ada lonjakan waktu latensi yang signifikan pada

salah satu hop, biasanya itu disebabkan oleh router yang memprioritaskan forwarding trafik daripada membalas paket ICMP, kemacetan di jalur jaringan, atau lokasi router yang jauh secara geografis (misalnya antar benua). Dalam beberapa kasus, lonjakan terjadi di jaringan internasional atau titik pertukaran antar-AS (Autonomous System).

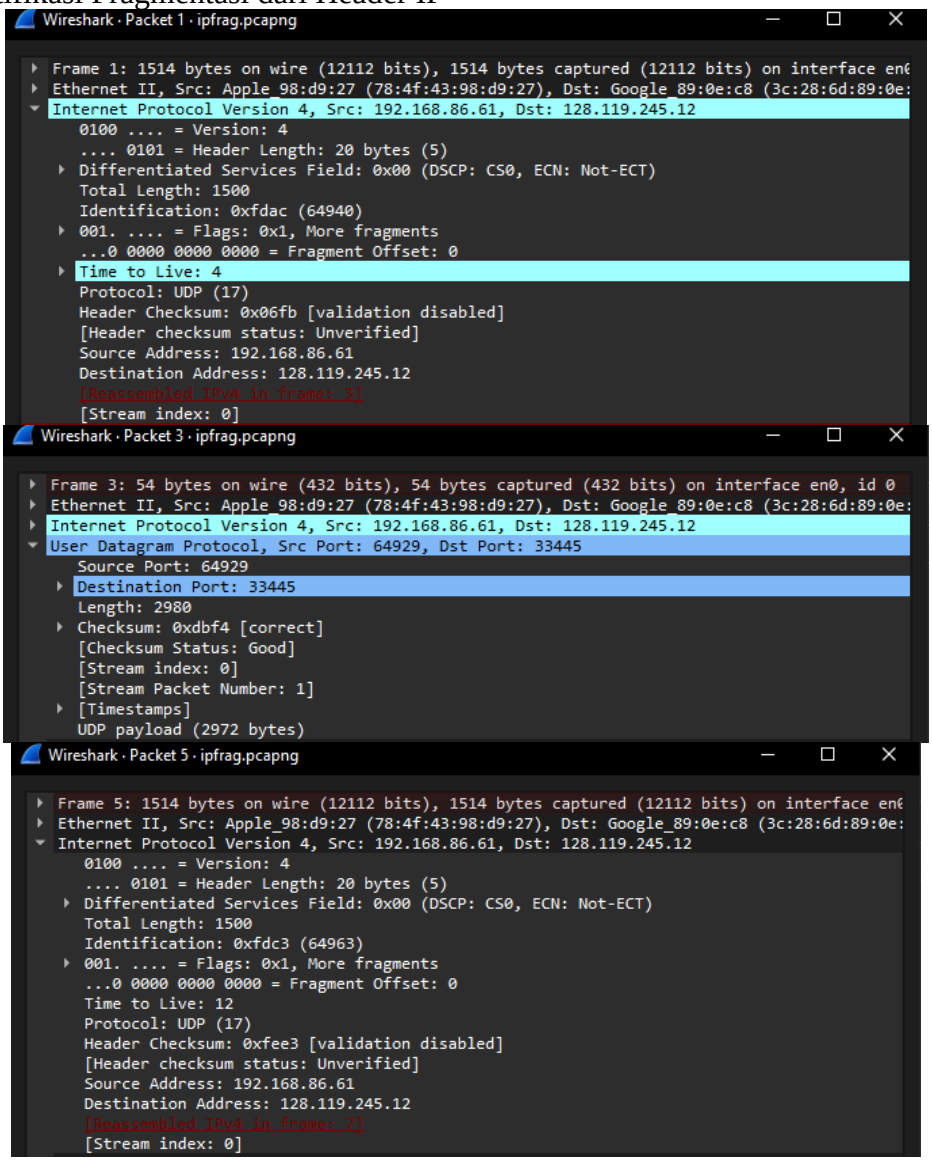
b. Tracert di Windows menggunakan protokol ICMP Echo Request yang ukurannya tetap dan tidak mengizinkan pengaturan ukuran payload dalam perintah tracert itu sendiri. Karena itu, tracert tidak dapat menghasilkan fragmentasi IP secara manual. Dampaknya terhadap analisis jalur jaringan adalah kita tidak bisa mendeteksi masalah yang terkait dengan batasan ukuran paket (seperti MTU bottleneck) atau perilaku jaringan terhadap paket-paket besar yang butuh difragmentasi. Dengan kata lain, analisa hanya fokus pada jumlah hop dan latensi, tanpa melihat bagaimana paket besar diproses.
c. Hasil tracert ke gaia.cs.umass.edu biasanya menunjukkan jumlah hop lebih banyak dan latensi yang lebih tinggi dibandingkan tracert ke telkomuniversity.ac.id. Ini karena gaia.cs.umass.edu berada di Amerika Serikat, sedangkan telkomuniversity.ac.id di Indonesia, sehingga membutuhkan jalur lebih panjang dan melintasi beberapa jaringan internasional. Selain itu, latensi ke Amerika cenderung lebih besar karena jarak fisik lebih jauh dan lebih banyak titik pertukaran jaringan yang dilewati.

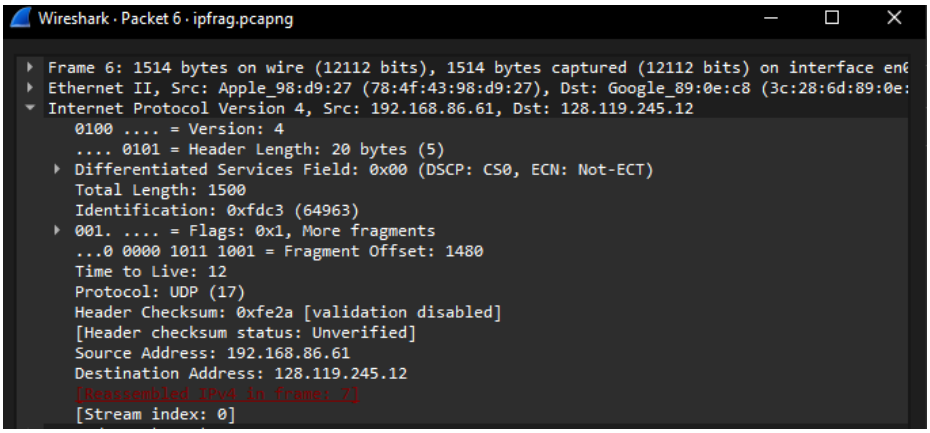
2. Interpretasi Traceroute

- Versi Windows
  a. Dari hasil tracert, hop-hop yang dilewati dapat diidentifikasi dengan melihat daftar router yang merespons di setiap langkah. Waktu latensi rata-rata untuk setiap hop bisa dihitung dengan mengambil rata-rata dari tiga waktu respon (ms) yang ditampilkan untuk setiap router. Jika ada lonjakan latensi di salah satu hop, biasanya karena router tersebut membatasi kecepatan respon ICMP untuk mengurangi beban kerja, adanya kemacetan jaringan lokal, atau perubahan jalur dinamis dalam backbone jaringan.
  b. Berdasarkan hasil `tracert` dan analisis Wireshark, dapat disimpulkan bahwa `tracert` di Windows memiliki keterbatasan dalam menganalisis fragmentasi IP karena tidak dapat mengubah ukuran paket. Ini membatasi pengamatan terhadap fenomena seperti MTU bottleneck atau fragmentasi IP. Dari pola jalur jaringan yang dilewati, terlihat bahwa paket menuju situs internasional (seperti gaia.cs.umass.edu) melewati backbone global dan exchange point yang berbeda dibandingkan paket menuju situs lokal (telkomuniversity.ac.id), yang lebih sederhana dan cepat karena lebih dekat secara geografis.

D. Wireshark Fragmentation

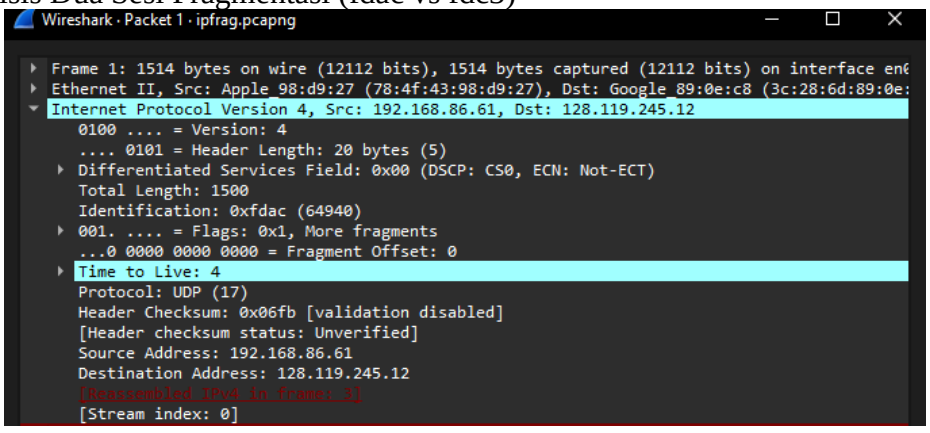
1. Identifikasi Fragmentasi dari Header IP

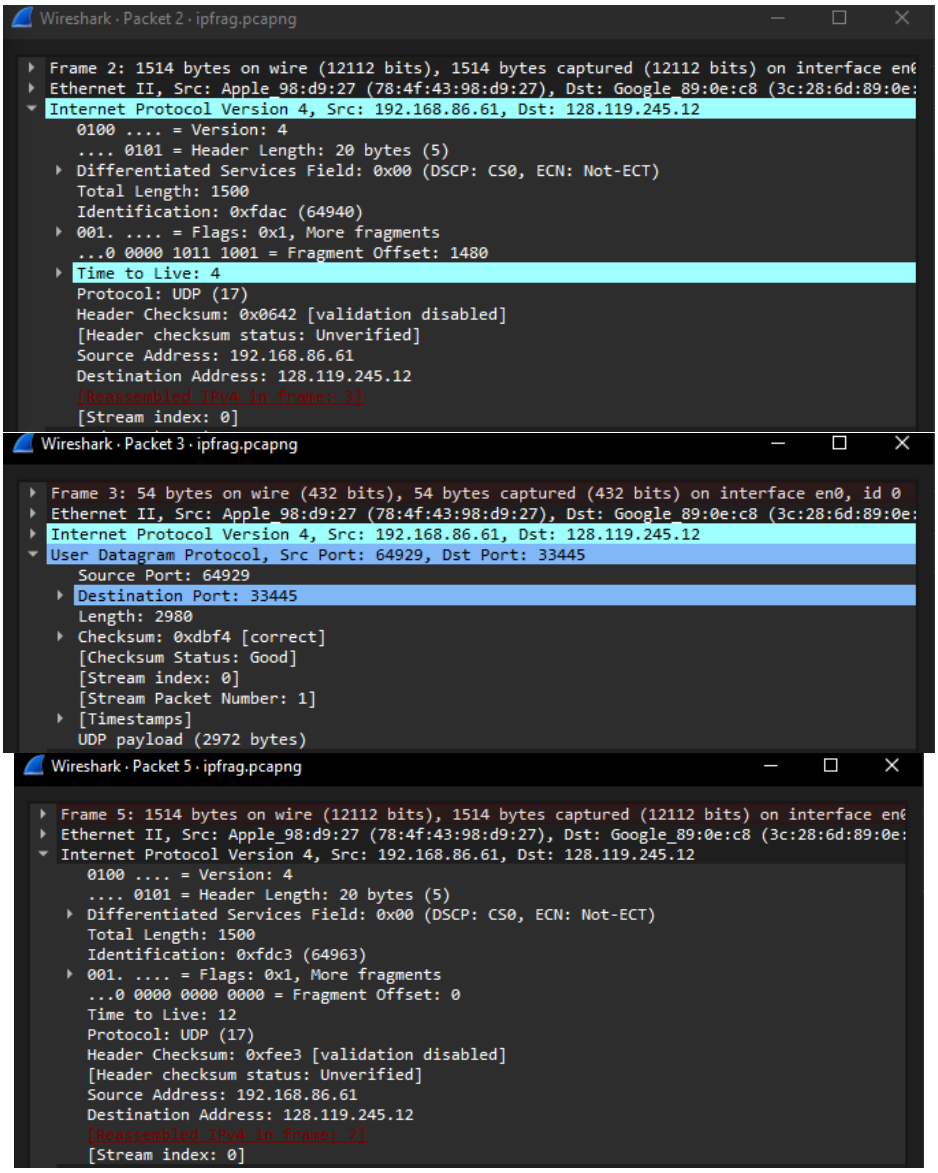


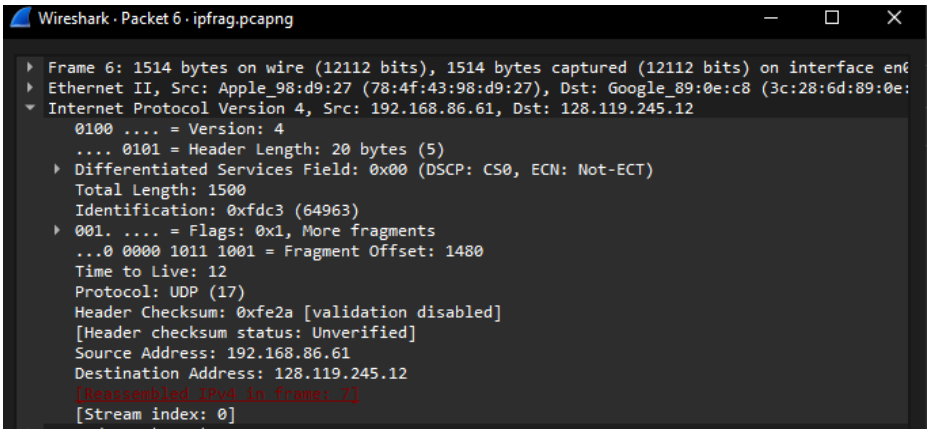


Fragmentasi pada paket IP dapat diidentifikasi dari informasi pada header IP, khususnya tiga parameter utama: Identification (ID), Fragment Offset, dan Flags. ID digunakan untuk mengelompokkan fragmen-fragmen yang berasal dari datagram IP yang sama. Fragment Offset menunjukkan posisi data fragmen tersebut dalam keseluruhan datagram asli. Flag penting dalam hal ini adalah bit "More Fragments (MF)", yang bernilai 1 jika masih ada fragmen berikutnya, dan 0 jika itu adalah fragmen terakhir. Dalam file Wireshark ipfrag.pcapng, paket No. 1 dan No. 2 memiliki ID yang sama dan offset yang berbeda, menandakan bahwa keduanya adalah bagian dari satu datagram besar yang telah dipecah. Begitu pula dengan paket No. 5 dan No. 6. Berdasarkan data di Wireshark, fragmentasi terjadi ketika panjang data melebihi batas tertentu. Misalnya, dari fragment offset dan total length, terlihat bahwa ukuran data yang melebihi sekitar 1480–1500 byte menyebabkan paket harus dipecah menjadi dua atau lebih bagian.

2. Analisis Dua Sesi Fragmentasi (fdac vs fdc3)

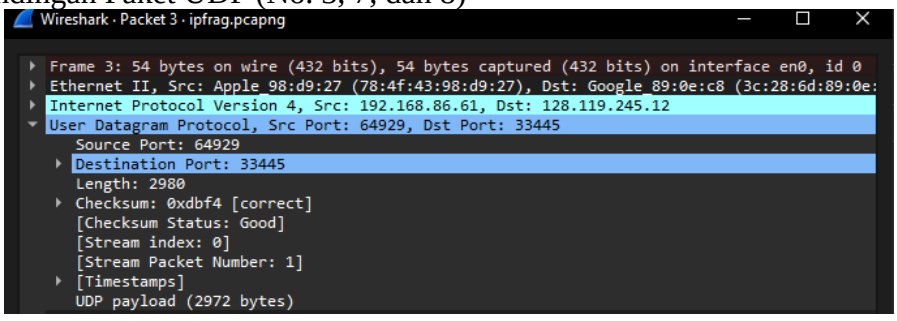


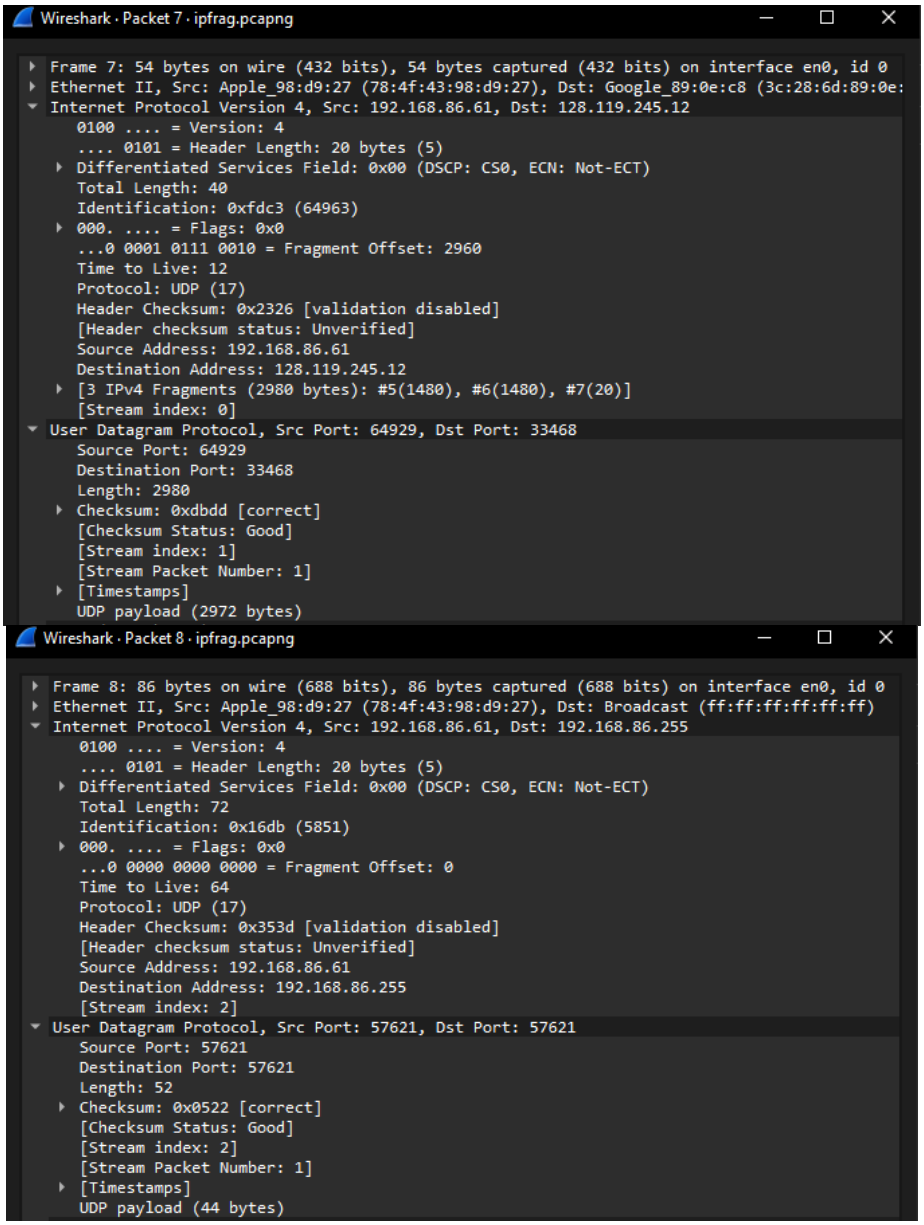

Wireshark · Packet 2 · ipfrag.pcapng
Frame 2: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:
Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xfdac (64940)
001. .... = Flags: 0x1, More fragments
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 4
Protocol: UDP (17)
Header Checksum: 0x0642 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.86.61
Destination Address: 128.119.245.12
[Reassembled IPv4 in frame: 3]
[Stream index: 0]
Wireshark · Packet 3 · ipfrag.pcapng
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:
Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
User Datagram Protocol, Src Port: 64929, Dst Port: 33445
Source Port: 64929
Destination Port: 33445
Length: 2980
Checksum: 0xdbf4 [correct]
[Checksum Status: Good]
[Stream index: 0]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (2972 bytes)
Wireshark · Packet 5 · ipfrag.pcapng
Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:
Internet Protocol Version 4, Src: 192.168.86.61, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xfdc3 (64963)
001. .... = Flags: 0x1, More fragments
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 12
Protocol: UDP (17)
Header Checksum: 0xfee3 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.86.61
Destination Address: 128.119.245.12
[Reassembled IPv4 in frame: 7]
[Stream index: 0]



Dalam file Wireshark, terdapat dua sesi fragmentasi IP yang berbeda: satu dengan ID fdac (paket No. 1 dan 2) dan satu lagi dengan ID fdc3 (paket No. 5 dan 6). Perbedaan utama antara keduanya terletak pada nilai offset dan tujuan akhir. Fragmen dengan ID fdac memiliki fragment offset awal 0 dan fragmen lanjutan dengan offset >0, yang dikirim ke alamat IP tertentu yang menjadi tujuan dari sesi pertama. Demikian pula ID fdc3 mewakili sesi fragmentasi kedua, dengan offset dan tujuan berbeda. Proses reassembly dilakukan oleh host tujuan dengan cara menyusun kembali fragmen-fragmen berdasarkan offset mereka. Wireshark membantu menunjukkan kapan semua fragmen sudah diterima dan berhasil dirakit kembali menjadi datagram lengkap, seperti yang terlihat pada paket No. 3 untuk ID fdac dan paket No. 7 untuk ID fdc3. Jika dibandingkan, tidak ada indikasi yang kuat bahwa salah satu sesi lebih kompleks, tetapi sesi dengan lebih banyak fragmen (jika ada) umumnya akan memerlukan waktu reassembly yang sedikit lebih lama.

3. Perbandingan Paket UDP (No. 3, 7, dan 8)



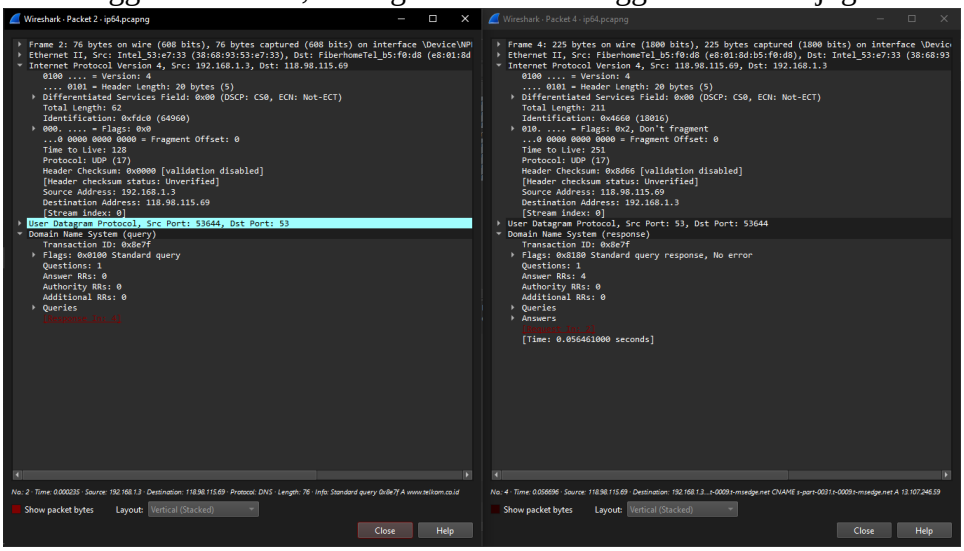


Paket No. 3 dan No. 7 adalah hasil reassembly dari proses fragmentasi dan masing-masing merupakan paket UDP utuh setelah beberapa fragmen disatukan. Keduanya ditujukan ke alamat spesifik, kemungkinan sebagai bagian dari komunikasi langsung antara dua perangkat. Panjang datanya cukup besar, sehingga sebelumnya perlu dipecah menjadi beberapa fragmen. Sebaliknya, paket No. 8 adalah paket UDP yang ditujukan ke alamat broadcast (192.168.86.255) dan memiliki ukuran data yang lebih kecil, sehingga tidak perlu mengalami fragmentasi. Dari sisi port tujuan dan sumber, biasanya port pada paket broadcast berbeda dan digunakan untuk layanan lokal seperti discovery atau announcement di jaringan lokal.

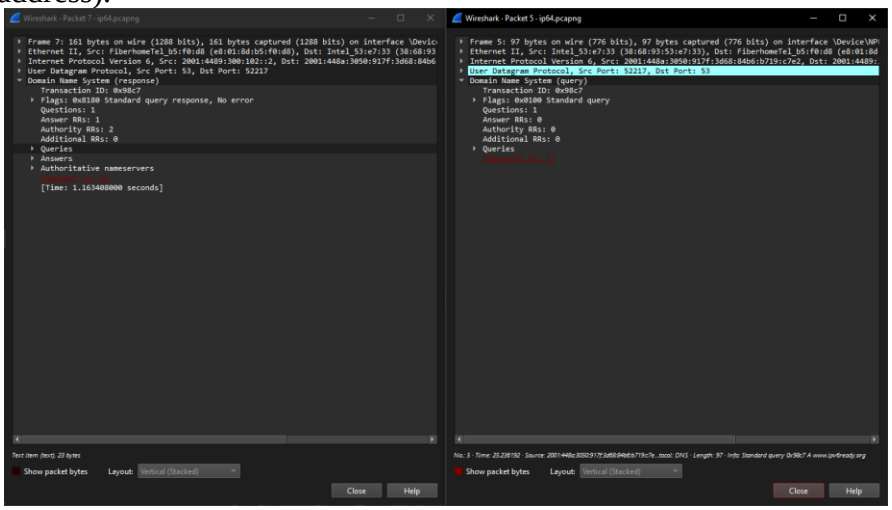
Kesimpulannya, paket No. 3 dan 7 digunakan untuk komunikasi data besar yang ditujukan secara langsung (unicast), sementara paket No. 8 digunakan untuk penyebaran informasi singkat ke seluruh perangkat di jaringan lokal. Tidak terjadinya fragmentasi pada paket No. 8 karena ukurannya memang di bawah batas MTU (sekitar 1500 byte), sehingga cukup dikirim dalam satu paket tunggal tanpa perlu dipecah.

E. Wireshark IPv4 dan UPv6

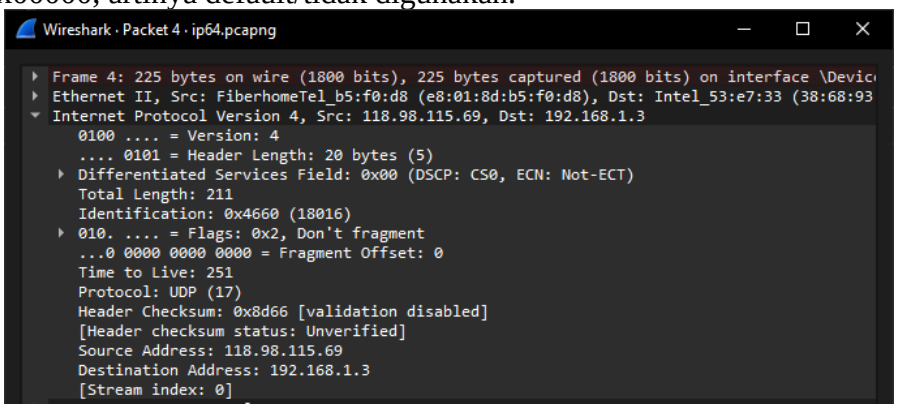
1. Baris 2 menggunakan IPv4, sedangkan Baris 4 menggunakan IPv4 juga.



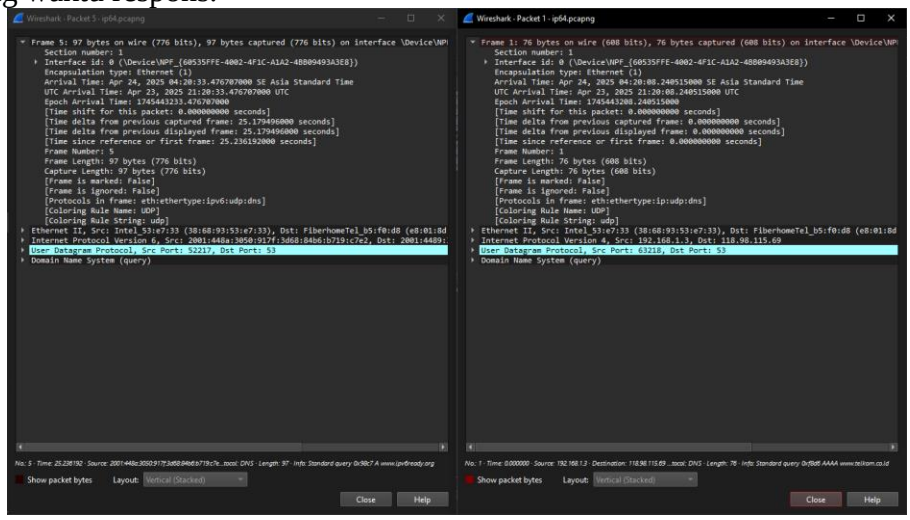
2. Baris 5: Hasil untuk DNS A (IPv6 address) dan baris 7: Hasil untuk DNS AAAA (IPv6 address).



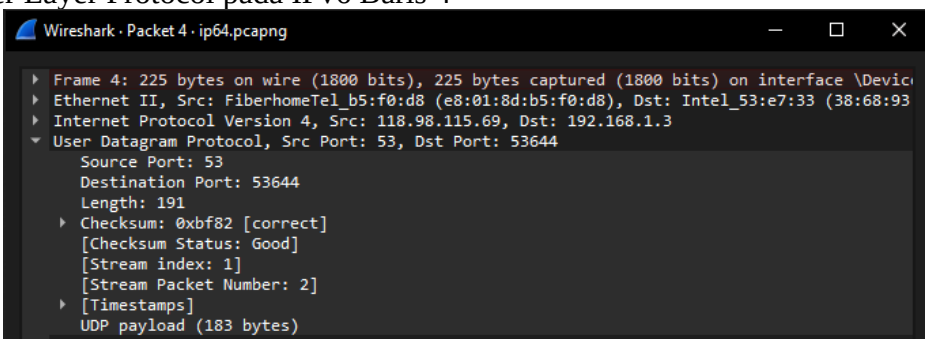
3. Jika 0x00000, artinya default/tidak digunakan.



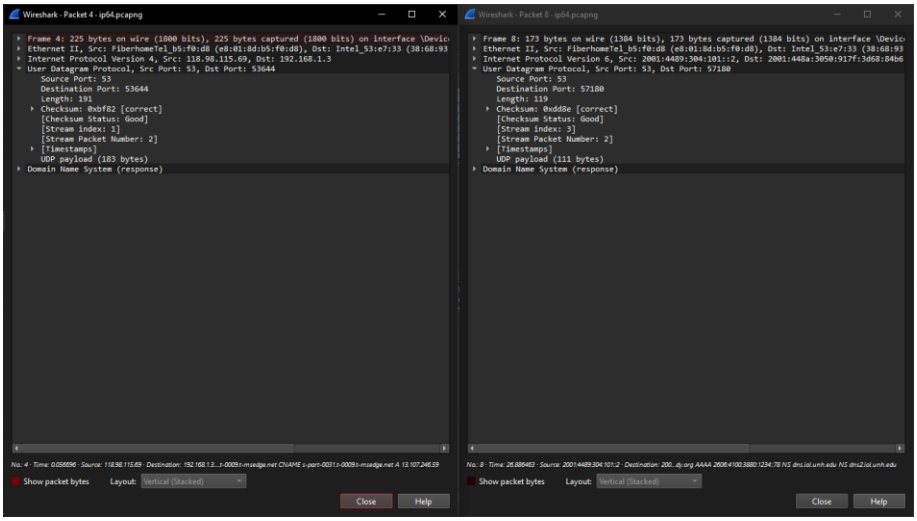
4. Hitung waktu respons.



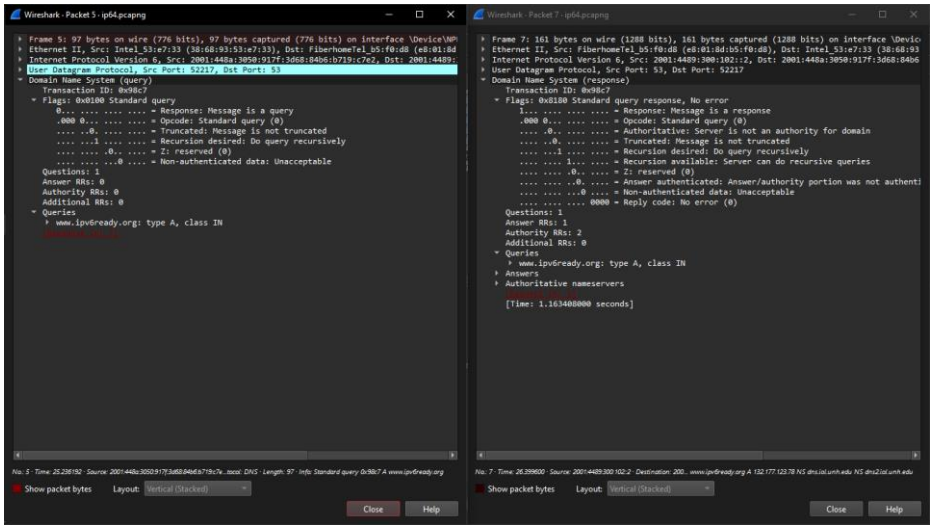
5. Upper Layer Protocol pada IPv6 Baris 4



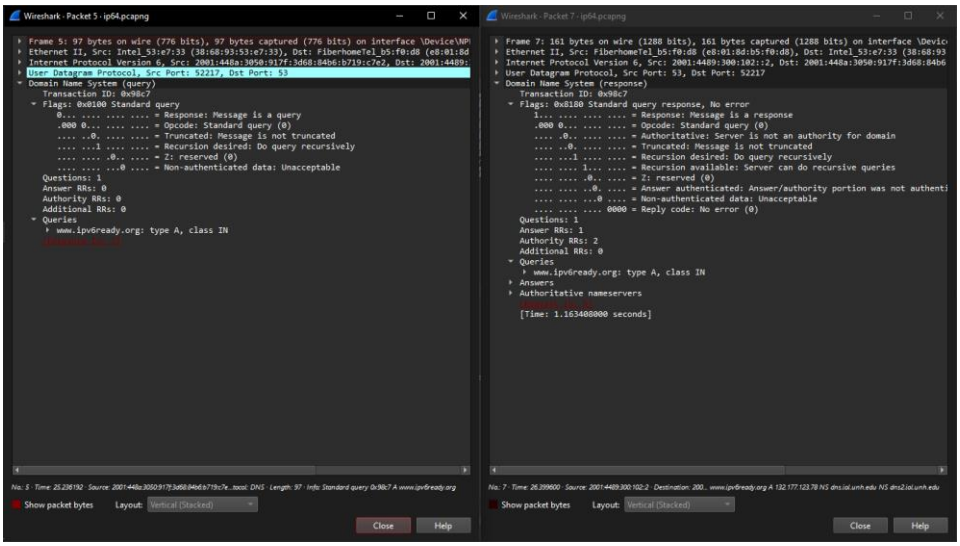
6. Efisiensi Ukuran Paket IPv4 vs IPv6



7. Konsistensi Nama Server



8. Dukungan Dual-Stack



9. Prioritas Query AAAA vs A

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.3	118.98.115.69	DNS	76	Standard query 0xf8d6 AAAA www.telkom.co.id
2	0.000235	192.168.1.3	118.98.115.69	DNS	76	Standard query 0x8e7f A www.telkom.co.id
3	0.010549	118.98.115.69	192.168.1.3	DNS	237	Standard query response 0xf8d6 AAAA www.telkom.co.id CNAME tci-aro-endpoint-e4hzfravdpbadqa7.a02.azurefd.net C
4	0.056696	118.98.115.69	192.168.1.3	DNS	225	Standard query response 0x8e7f A www.telkom.co.id CNAME tci-aro-endpoint-e4hzfravdpbadqa7.a02.azurefd.net CNAM
5	25.236192	2001:448a:3050:917f…	2001:4489:300:102::2	DNS	97	Standard query 0x98c7 A www.ipv6ready.org
6	25.783118	2001:448a:3050:917f…	2001:4489:304:101::2	DNS	97	Standard query 0xa7a9 AAAA www.ipv6ready.org
7	26.399600	2001:4489:300:102::2	2001:448a:3050:917f…	DNS	161	Standard query response 0x98c7 A www.ipv6ready.org A 132.177.123.78 NS dns.iol.unh.edu NS dns2.iol.unh.edu
8	26.886463	2001:4489:304:101::2	2001:448a:3050:917f…	DNS	173	Standard query response 0xa7a9 AAAA www.ipv6ready.org AAAA 2606:4100:3880:1234::78 NS dns.iol.unh.edu NS dns2.

10. Interoperabilitas IPv4 dan IPv6