JARINGAN KOMPUTER – TUGAS PENDAHULUAN MODUL 13
ETHERNET & ARP (ADDRESS RESOLUTION PROTOCOL)

Nama : Muhammad Hamzah Haifan Ma'ruf

NIM : 2311102091

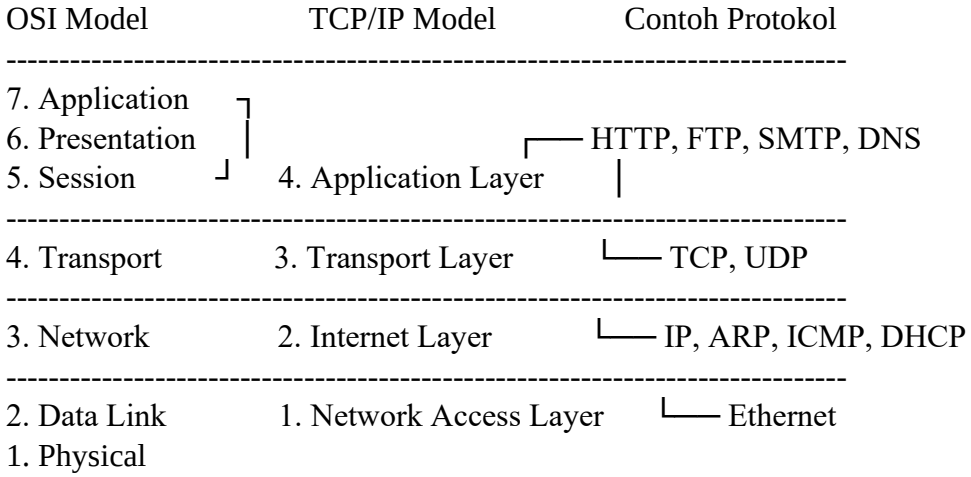
Kelas : S1IF-11-07

Kode Dosen : AIZ

JAWABAN MODUL

A. Teori

1. Hubungan OSI Model dan TCP/IP Model + Letak Protokol



Model OSI dan model TCP/IP merupakan dua arsitektur referensi jaringan yang menjelaskan cara kerja komunikasi data antar perangkat. Model OSI terdiri dari tujuh lapisan: Physical, Data Link, Network, Transport, Session, Presentation, dan Application. Sementara itu, model TCP/IP hanya memiliki empat lapisan utama, yaitu Network Access, Internet, Transport, dan Application. Secara visual, tiga lapisan teratas pada model OSI (Application, Presentation, dan Session) disederhanakan menjadi satu lapisan Application pada model TCP/IP. Lapisan Transport pada OSI langsung setara dengan Transport pada TCP/IP, sedangkan

lapisan Network pada OSI setara dengan Internet pada TCP/IP. Dua lapisan terbawah OSI (Data Link dan Physical) digabungkan menjadi Network Access dalam model TCP/IP. Beberapa protokol umum dapat dikelompokkan ke dalam masing-masing lapisan tersebut. Protokol HTTP, FTP, SMTP, dan DNS berada di lapisan Application baik pada OSI maupun TCP/IP. TCP dan UDP berada di lapisan Transport. IP, ARP, dan DHCP termasuk dalam lapisan Network (OSI) atau Internet (TCP/IP). Sementara itu, Ethernet beroperasi di lapisan Data Link (OSI) atau Network Access (TCP/IP).

2. Perbedaan antara ARP Request dan ARP Reply

   ARP Request dan ARP Reply adalah dua jenis pesan dalam protokol Address Resolution Protocol (ARP) yang berfungsi untuk menerjemahkan alamat IP menjadi alamat MAC dalam jaringan lokal (LAN). Perbedaan utama antara keduanya terletak pada field opcode dan cara pengiriman pesan. ARP Request memiliki opcode bernilai 1 yang menandakan permintaan pencarian MAC address, sedangkan ARP Reply memiliki opcode bernilai 2 yang menunjukkan balasan dengan informasi MAC address. Dalam ARP Request, alamat MAC tujuan (destination MAC address) diatur ke nilai broadcast (FF:FF:FF:FF:FF:FF) sehingga pesan dikirim ke semua perangkat di jaringan. Sebaliknya, ARP Reply dikirim secara unicast langsung ke alamat MAC pengirim ARP Request. Dengan demikian, ARP Request digunakan untuk mencari pemilik alamat IP tertentu, sedangkan ARP Reply memberikan jawaban berupa alamat MAC yang diminta.

3. Alur Komunikasi dari HTTP Request sampai Response Berdasarkan Sequence Diagram

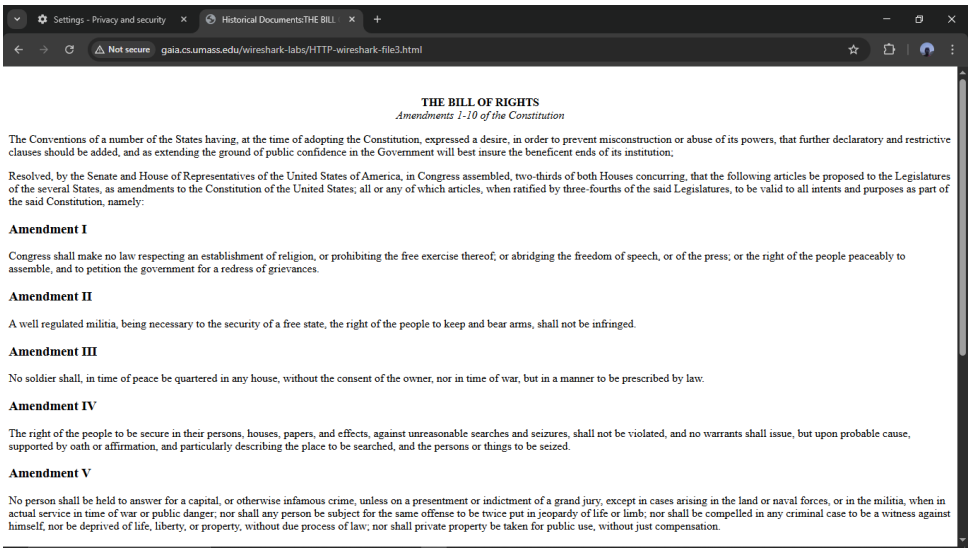
   Berdasarkan diagram interaksi antara Host dan Server melalui protokol ARP dan Ethernet, alur komunikasi dimulai ketika Host ingin mengirim permintaan HTTP GET ke Server. Sebelum data dikirim, Host akan memeriksa ARP Cache untuk melihat apakah MAC address dari IP tujuan sudah tersedia. Jika sudah ada, Host langsung membungkus data HTTP GET ke dalam frame Ethernet dan mengirimnya ke Server. Jika tidak ditemukan, Host akan mengirim ARP Request berupa siaran (broadcast) ke seluruh perangkat dalam jaringan LAN untuk menanyakan siapa yang memiliki IP tertentu. Perangkat yang memiliki IP tersebut, seperti Server, akan membalas dengan ARP Reply yang berisi MAC address-nya. Setelah itu, Host akan memperbarui ARP Cache dengan informasi IP-to-MAC tersebut. Kemudian, Host membungkus HTTP GET request ke dalam frame Ethernet yang berisi MAC address tujuan dan mengirimkannya ke Server. Server lalu membalas dengan HTTP

Response yang juga dikemas dalam frame Ethernet. Dalam proses ini, Ethernet berperan sebagai protokol di lapisan data-link yang membungkus data aplikasi menjadi frame dan memastikan pengiriman dari MAC source ke MAC destination. ARP berperan penting dalam menerjemahkan alamat IP ke MAC sebelum data dapat dikirim, dan keberadaan ARP Cache sangat membantu dalam mempercepat proses karena menghindari kebutuhan untuk melakukan ARP Request berulang-ulang. Frame Ethernet yang digunakan mencakup header dengan field penting seperti destination MAC, source MAC, dan EtherType untuk menandai tipe protokol di atasnya (misalnya IPv4).

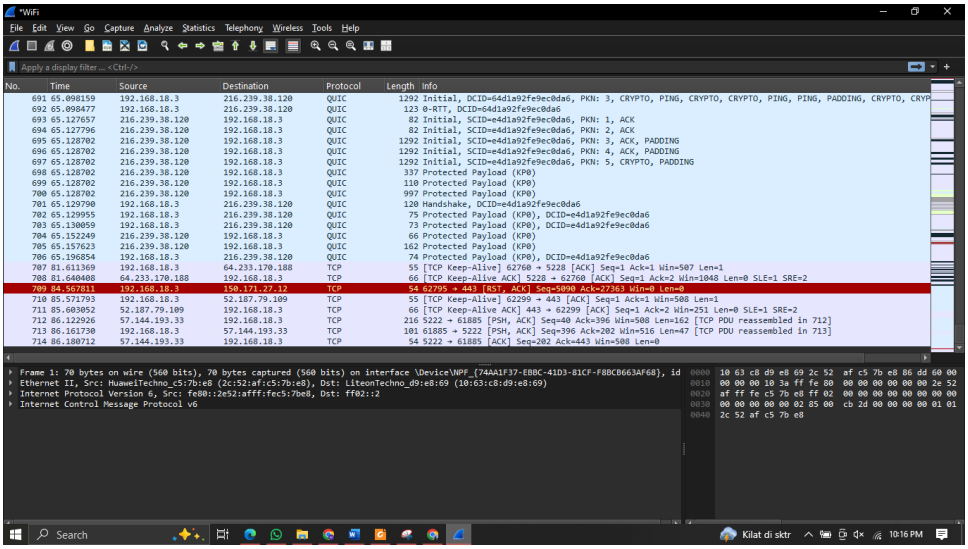
4. Alamat MAC dan Letak Karakter ASCII "G" dalam Frame Ethernet HTTP GET

   Dalam sebuah frame Ethernet yang membawa permintaan HTTP GET, alamat MAC source berisi alamat MAC dari Host (pengirim), dan alamat MAC destination adalah alamat MAC dari Server (penerima) yang diperoleh dari proses ARP. Informasi ini sangat penting karena Ethernet bekerja berdasarkan pengalamatan MAC, bukan IP. Sebelum pengiriman dilakukan, ARP digunakan untuk memastikan bahwa MAC tujuan diketahui dan valid. Jika tidak diketahui, Host harus melakukan ARP Request terlebih dahulu. Setelah MAC address tersedia, data HTTP GET dikemas ke dalam frame Ethernet. Struktur frame ini terdiri dari header Ethernet (14 byte), diikuti oleh header IP (20 byte), header TCP (20 byte), dan baru kemudian payload data HTTP. Karakter pertama dari perintah "GET" yaitu huruf "G" merupakan bagian dari payload aplikasi yang muncul setelah header-header tersebut. Dengan menghitung offset dari awal frame, karakter "G" umumnya muncul di byte ke-55, setelah header Ethernet (14 byte), IP (20 byte), dan TCP (20 byte). Ini menunjukkan bagaimana Ethernet hanya mengangkut data tanpa memahami isi aplikasi, dan bahwa setiap lapisan jaringan berperan dalam proses enkapsulasi data dari lapisan aplikasi hingga dikirim secara fisik di jaringan.

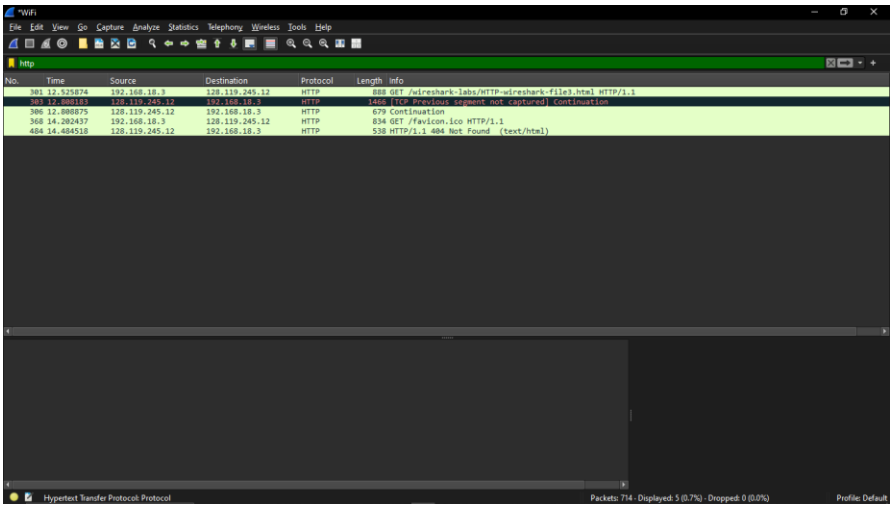
B. Capturing Ethernet Frames
   1. Pastikan cache browser kosong
   2. Buka dan Jalankan Wireshark untuk men-capture paket dan ketik URL berikut ke browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark file3.html. Browser akan menampilkan US Bill of Rights yang agak panjang.



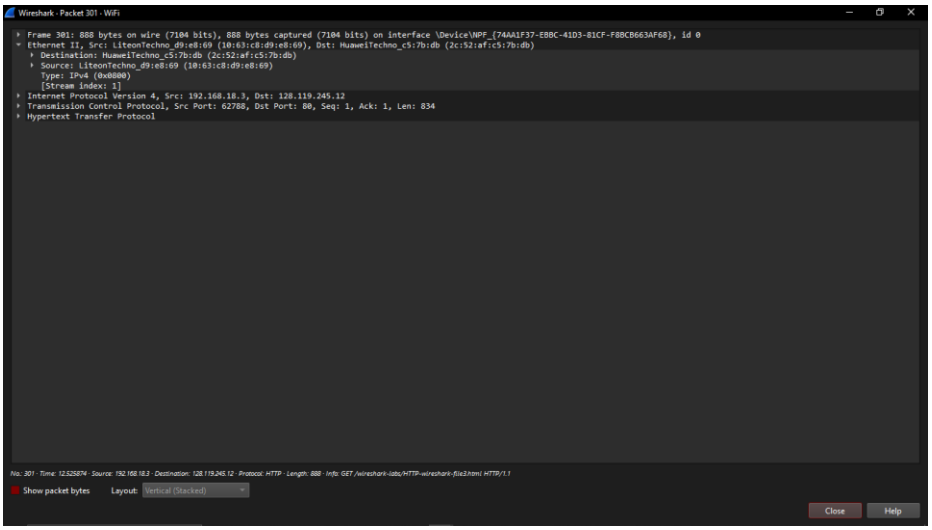
3. Hetikan capture paket di Wireshark dan tutup browser



4. Tunjukkan hasil capturenya

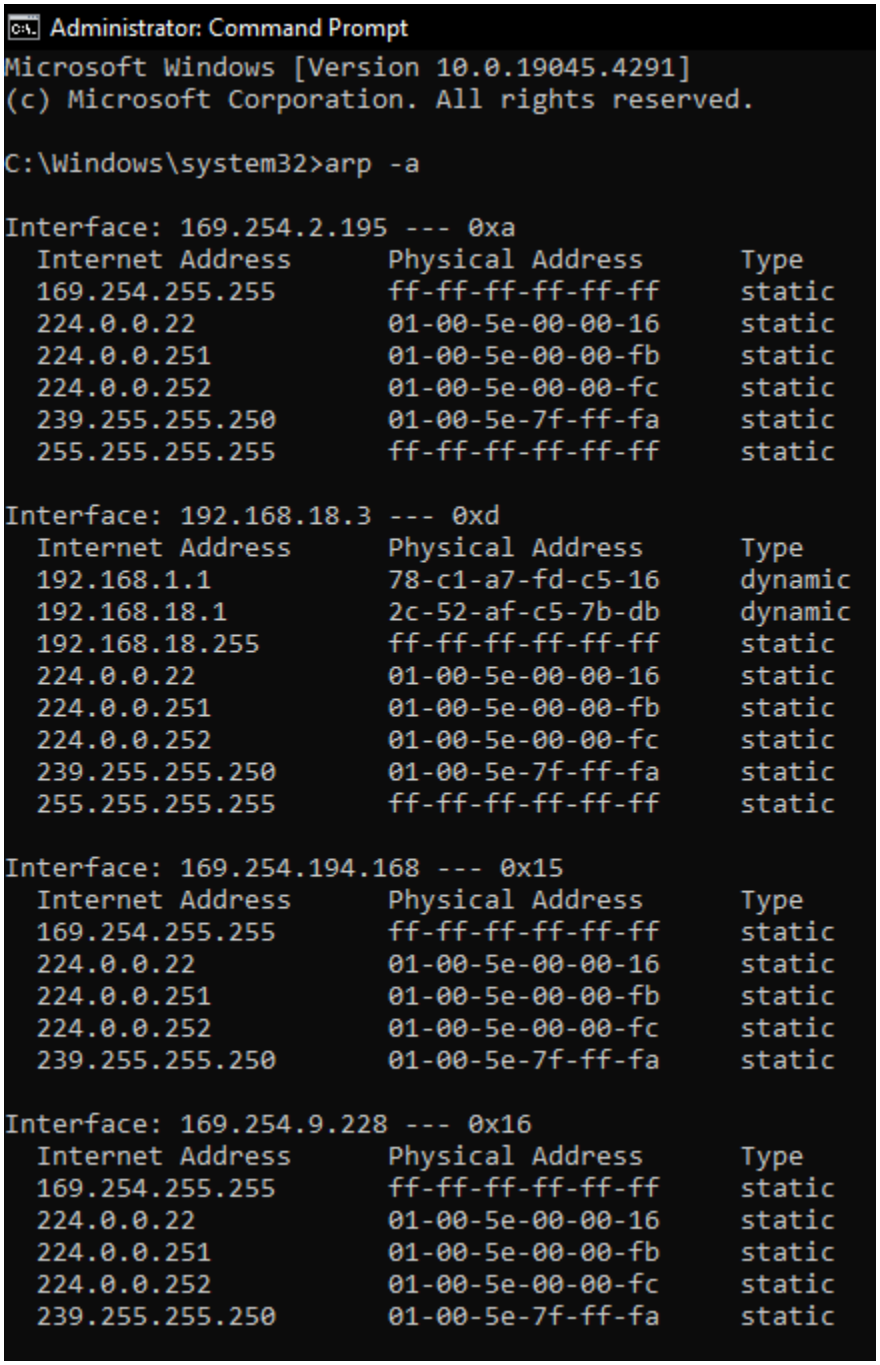


5. Tunjukkan Ethernet source dan destinationnya dari URL yang sudah diakses! query filter apa yang harus digunakan?



C. Caching ARP

1. Tunjukkan isi cache ARP di computer/laptop Anda dengan menggunakan command “arp -a”!



Jumlah total entry:
Terdapat total 27 baris entri, namun jika difokuskan pada interface 192.168.18.3, terdapat 10 entri, di antaranya 2 bertipe dynamic, dan sisanya static.

Isi setiap entry ARP:

- Internet Address → Alamat IP perangkat lain di jaringan.
- Physical Address → Alamat MAC dari perangkat tersebut.
- Type → Jenis entri, apakah dynamic (dibuat otomatis oleh ARP) atau static (ditambahkan secara manual atau sistem tetap).

Perbedaan static vs dynamic:

- Dynamic: Entri yang dibuat otomatis saat host mengirim ARP request dan mendapat balasan.
- Static: Ditambahkan secara manual dan bersifat permanen (tidak hilang setelah restart atau timeout).

2. Lakukan penghapusan salah satu entry statis dalam cache ARP berdasarkan alamat IP yang telah ditampilkan oleh perintah arp -a!

```
C:\Windows\system32>arp -d 224.0.0.252

C:\Windows\system32>arp -a

Interface: 169.254.2.195 --- 0xa
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.18.3 --- 0xd
  Internet Address      Physical Address      Type
  192.168.1.1           78-c1-a7-fd-c5-16     dynamic
  192.168.18.1          2c-52-af-c5-7b-db     dynamic
  192.168.18.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 169.254.194.168 --- 0x15
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 169.254.9.228 --- 0x16
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Internet Address: 224.0.0.252
Physical Address: 01-00-5e-00-00-fc
Type: static

Perintah untuk menghapus entry:
arp -d 224.0.0.252

Mengapa entry ini bersifat statis?

Karena 224.0.0.252 adalah alamat multicast yang biasanya digunakan oleh protokol tertentu (misalnya LLMNR). Oleh karena itu, sistem menetapkannya sebagai static agar selalu tersedia dalam komunikasi jaringan multicast.

3. Tambahkan kembali entry ARP statis yang telah Anda hapus pada aktivitas sebelumnya menggunakan perintah arp -s!

```
C:\Windows\system32>arp -s 224.0.0.252 01-00-5e-00-00-fc

C:\Windows\system32>arp -a

Interface: 169.254.2.195 --- 0xa
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.18.3 --- 0xd
  Internet Address      Physical Address      Type
  192.168.1.1           78-c1-a7-fd-c5-16     dynamic
  192.168.18.1          2c-52-af-c5-7b-db     dynamic
  192.168.18.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 169.254.194.168 --- 0x15
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 169.254.9.228 --- 0x16
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Alamat IP: 224.0.0.252

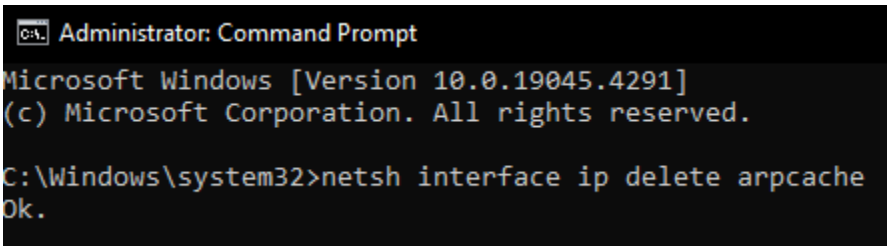
MAC Address: 01-00-5e-00-00-fc

Perintah penambahan entry static:
arp -s 224.0.0.252 01-00-5e-00-00-fc

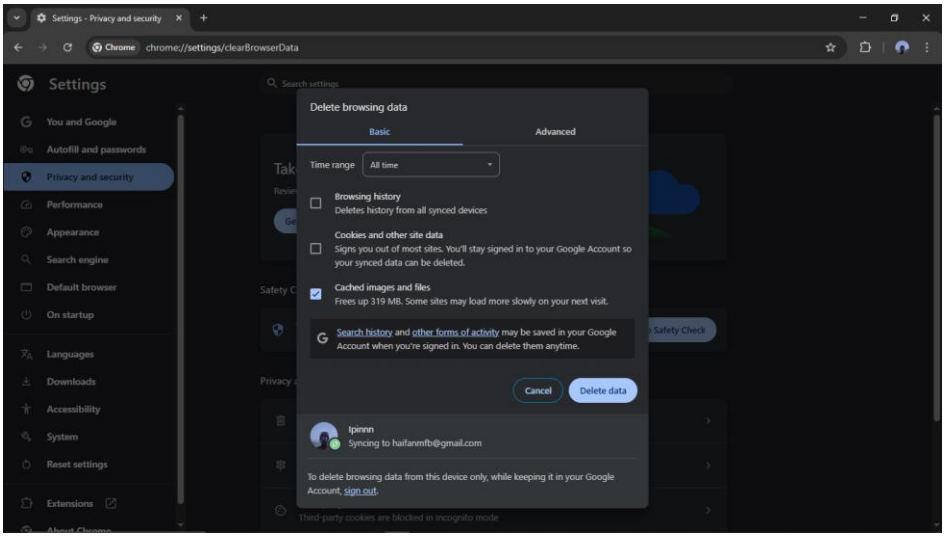
Cara verifikasi bahwa entry telah ditambahkan:
Jalankan kembali:
arp -a
Pastikan IP 224.0.0.252 muncul kembali dengan MAC yang sesuai dan tipe static.

D. Capturing ARP

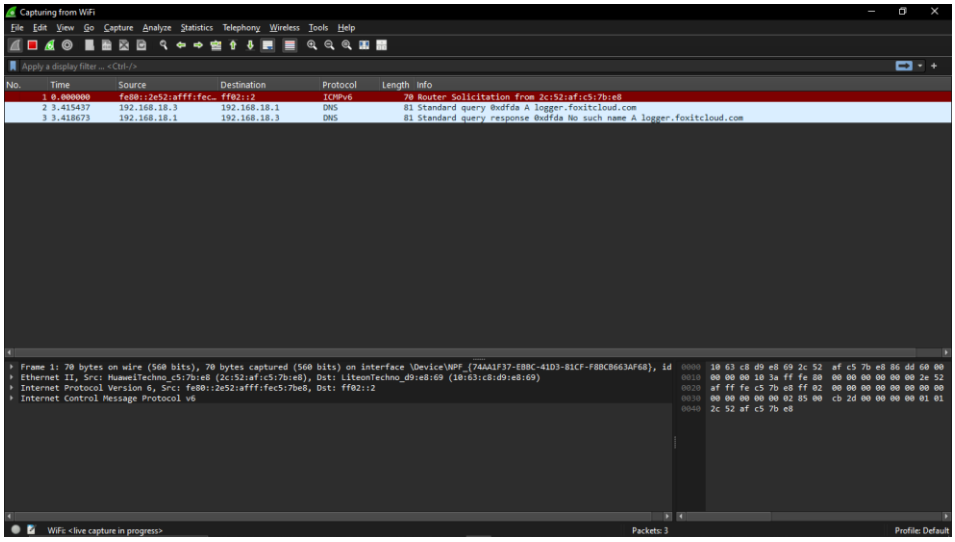
1. Kosongkan cache ARP Anda, command apa yang harus digunakan?



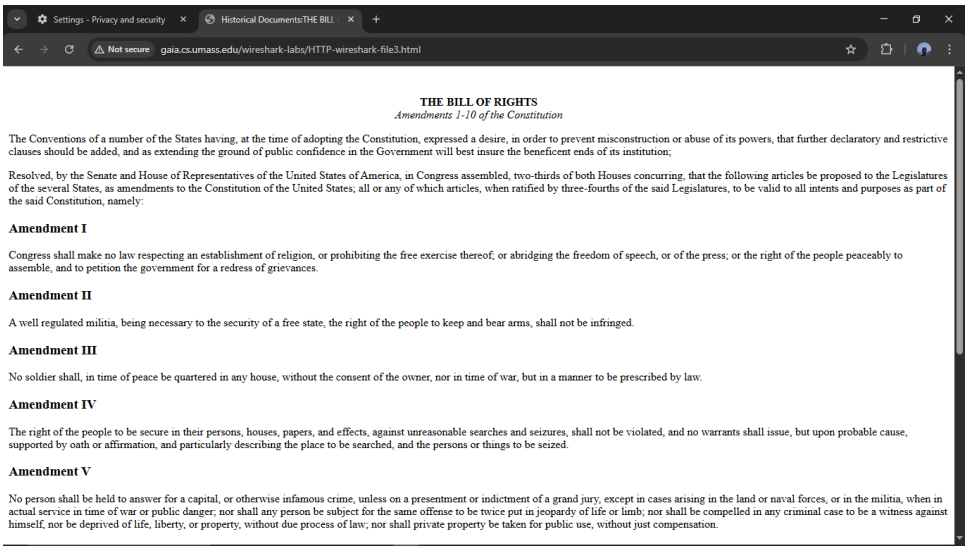
2. Pastikan cache browser sudah dibersihkan dari dokumen/file yang di unduh sebelumnya!



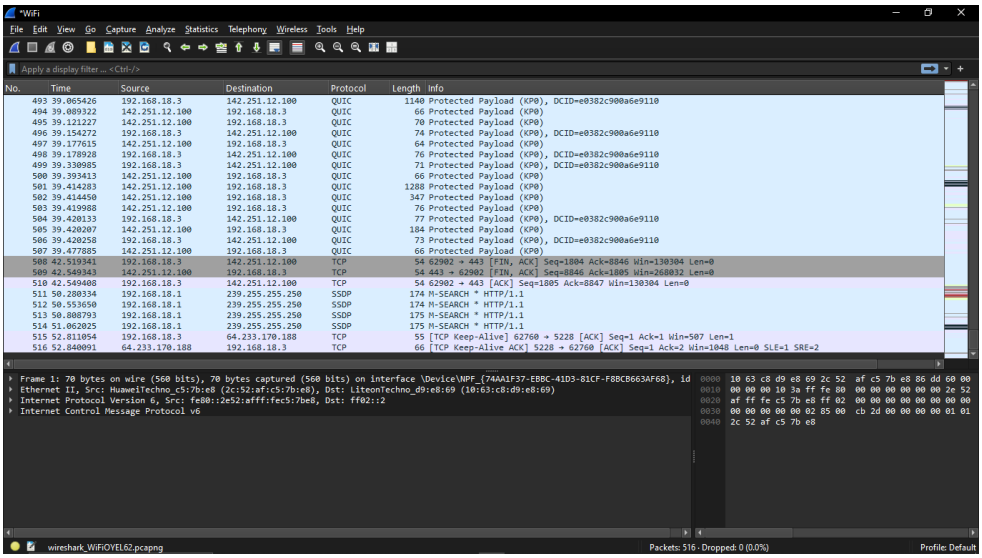
3. Buka dan Jalankan Wireshark untuk men-capture paket



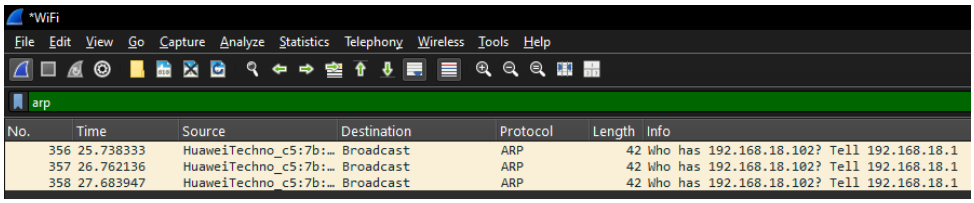
4. Ketik URL berikut ke browser: http://gaia.cs.umass.edu/wireshark labs/HTTP-wireshark file3.html. Browser akan menampilkan US Bill of Rights yang agak panjang.



5. Hetikan capture paket di Wireshark dan tutup browser



6. Tunjunkkah hasil capturenya!
7. Tunjukkan ARP Request dan ARP Reply/Response dari URL yang sudah diakses! query filter apa yang harus digunakan?



E. ARP RFC

Dalam dokumen RFC 826, struktur pesan Address Resolution Protocol (ARP) dijelaskan secara rinci sebagai format protokol yang digunakan untuk memetakan alamat IP (logis) ke alamat MAC (fisik) dalam jaringan lokal (LAN). Protokol ini bekerja pada lapisan jaringan (Network Layer) namun beroperasi secara langsung dengan alamat fisik di lapisan data-link.

Struktur pesan ARP terdiri dari beberapa elemen penting, masing-masing memiliki peran dalam proses resolusi alamat:

- Hardware Type (HTYPE): Menunjukkan jenis jaringan fisik yang digunakan. Untuk Ethernet, nilainya adalah 1.

- Protocol Type (PTYPE): Menentukan jenis protokol logis yang digunakan, misalnya IPv4 diwakili dengan 0x0800.

- Hardware Address Length (HLEN) dan Protocol Address Length (PLEN): Menentukan panjang alamat fisik (MAC, biasanya 6 byte) dan alamat protokol (IP, biasanya 4 byte).

- Operation (OPER): Menyatakan jenis pesan, 1 untuk ARP Request, 2 untuk ARP Reply.

- Sender Hardware Address (SHA) dan Sender Protocol Address (SPA): Alamat MAC dan IP dari pengirim ARP.

- Target Hardware Address (THA) dan Target Protocol Address (TPA): Alamat MAC dan IP dari penerima ARP. Dalam ARP Request, THA dikosongkan karena belum diketahui.

Dalam proses pembentukan entri ARP, saat sebuah host ingin mengirimkan data ke IP tertentu namun tidak mengetahui MAC address-nya, host akan membuat ARP Request yang mengisi semua field di atas, kecuali THA. Setelah perangkat tujuan menjawab dengan ARP Reply, maka field THA akan terisi dengan MAC address yang sesuai. Informasi dari ARP Reply inilah yang akan disimpan dalam tabel ARP (ARP cache) sebagai entri IP-to-MAC.

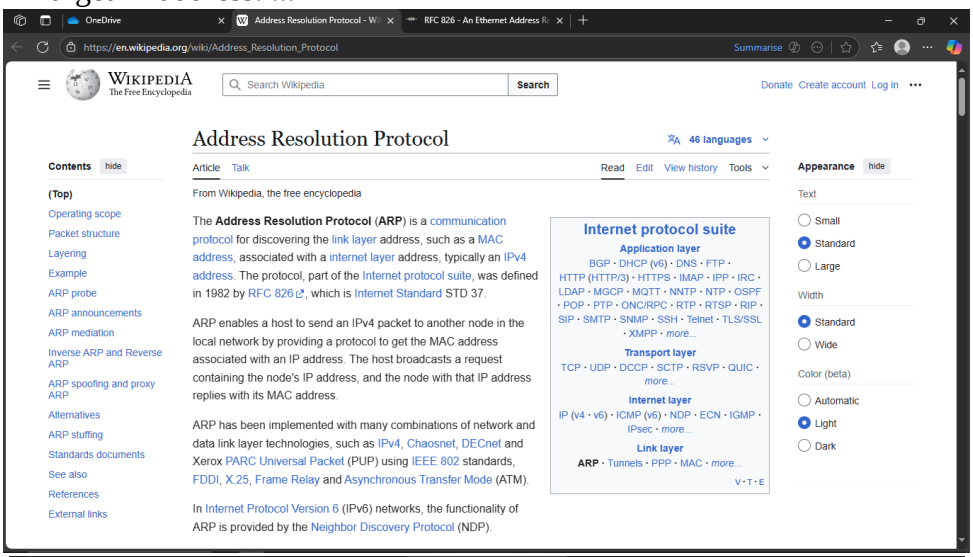
Contoh kutipan dari RFC 826 (halaman awal):

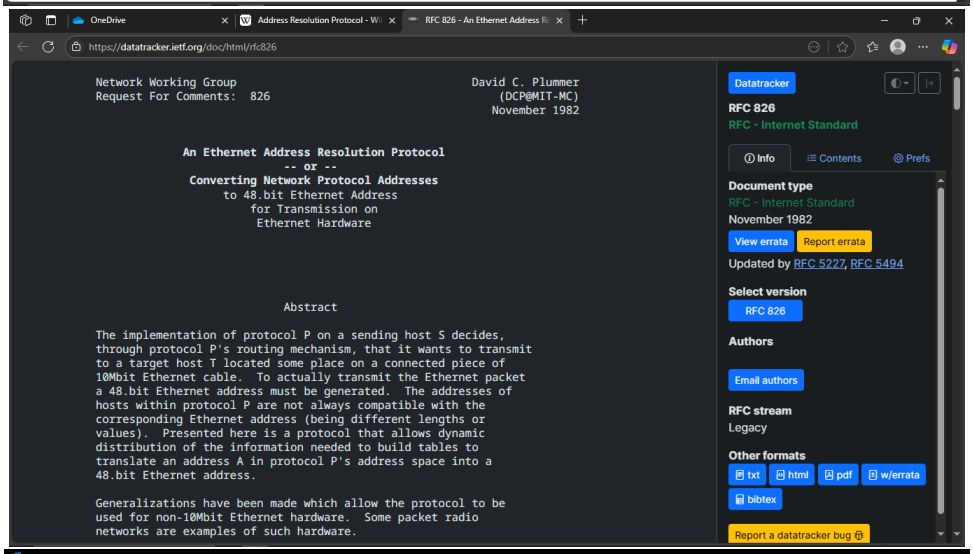
"This is a request to resolve the hardware address which corresponds to the given protocol address."
(RFC 826, Section: Packet format)

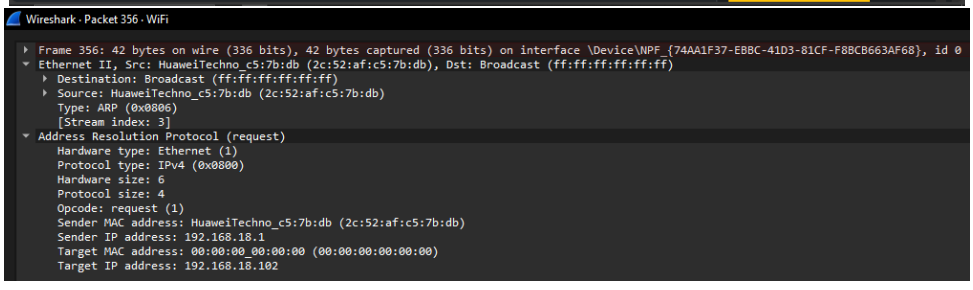
Bukti struktur pesan juga ditampilkan dalam Wireshark saat paket ARP ditangkap. Pada tampilan detail Wireshark, kita dapat melihat field seperti:

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Opcode: request (1) / reply (2)
- Sender MAC address: ...
- Sender IP address: ...
- Target MAC address: ...

- Target IP address: ...

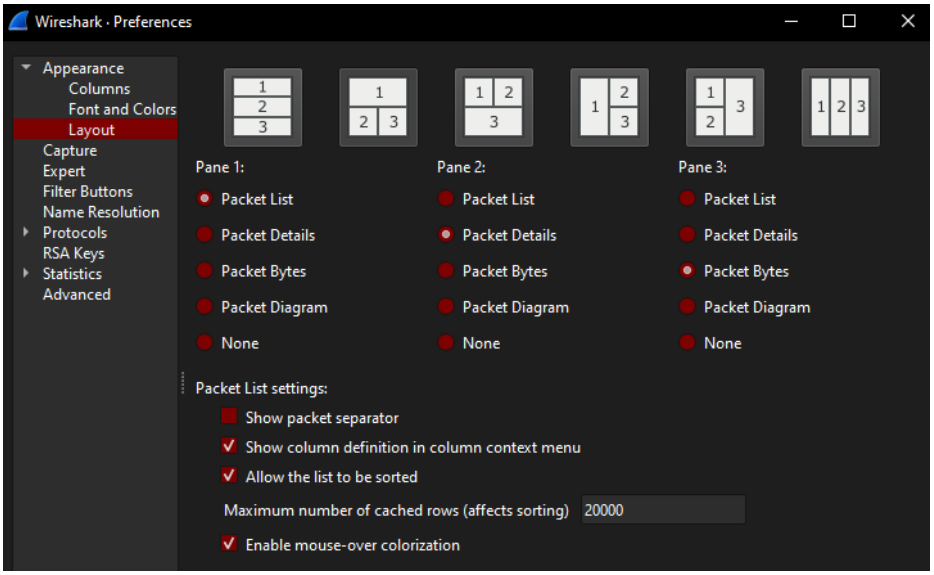




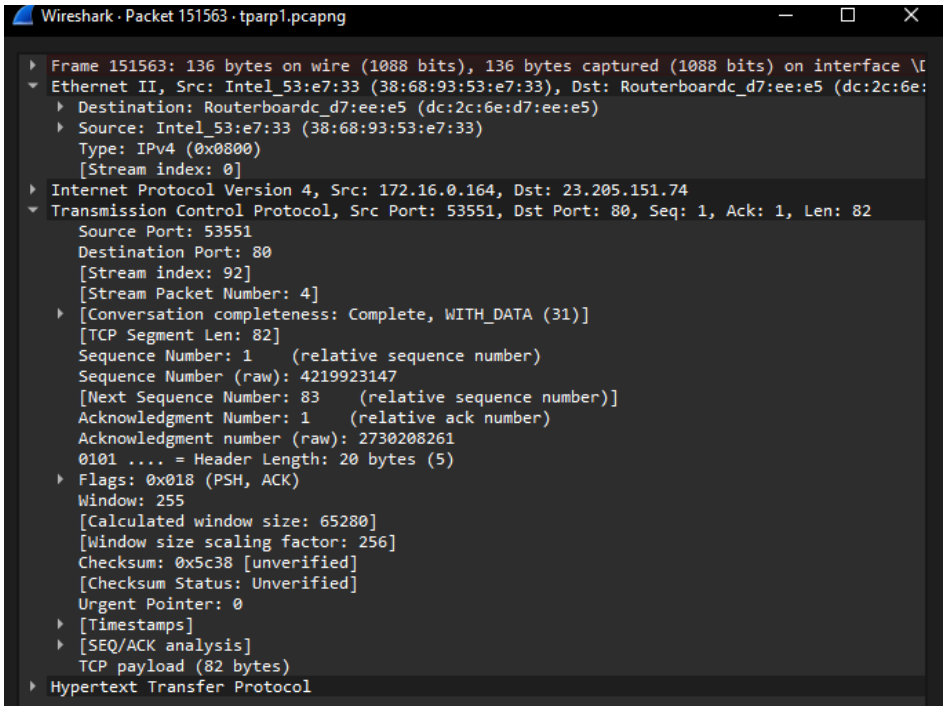


F. Wireshark ARP

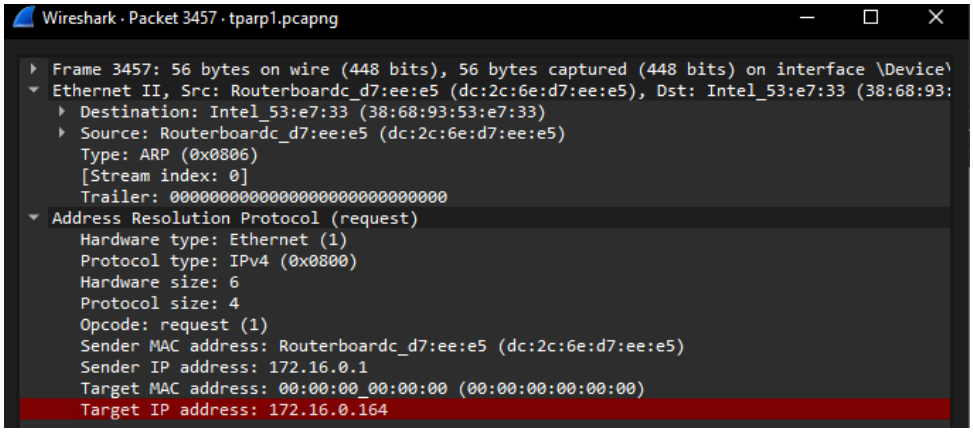
1. Pengaturan Cache Size Wireshark agar semua paket terbaca



2. Analisis Protokol HTTP, TCP, ARP dalam Ethernet Frame (tparp1.pcapng)

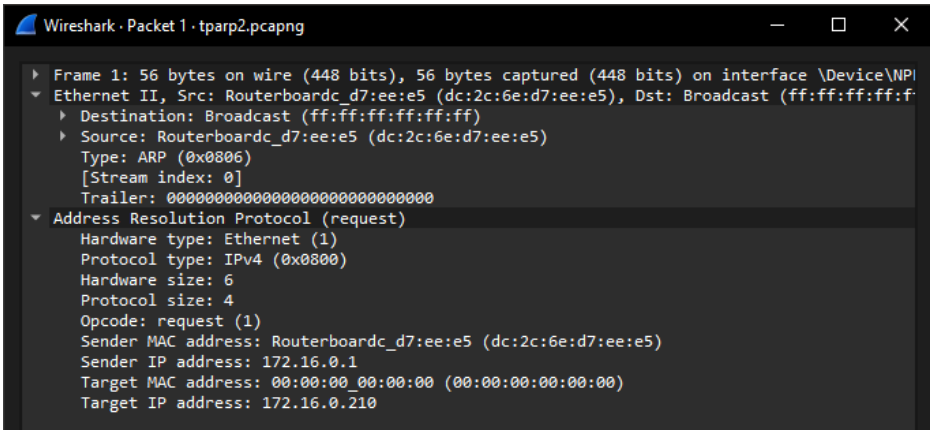


Ethernet II, Src: Intel_53:e7:33 (38:68:93:53:e7:33), Dst: Routerboardc_d7:ee:e5 (dc:2c:6e:d7:ee:e5)
Internet Protocol Version 4, Src: 172.16.0.164, Dst: 23.205.151.74
Transmission Control Protocol, Src Port: 53551, Dst Port: 80, Seq: 1, Ack: 1, Len: 82



Ethernet II, Src: Routerboardc_d7:ee:e5 (dc:2c:6e:d7:ee:e5), Dst: Intel_53:e7:33 (38:68:93:53:e7:33)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Sender IP address: 172.16.0.1
Target IP address: 172.16.0.164

3. Analisis ARP Multisumber dalam tparp2.pcapng



Sumber MAC Address yang muncul:

- Routerboardc_d7:ee:e5: biasanya perangkat gateway/router.
- Mengirim ARP Request seperti: “Who has 172.16.0.208?”
- XiaomiCommun_02:dd:7c: bisa jadi perangkat IoT/ponsel.
- 92:3a:4b:6d:ef:7c: PC atau server.
- Intel_53:e7:33: biasanya laptop/PC berbasis Intel NIC.

Jenis pesan ARP:

- Semua mengirimkan ARP Request (Opcode = 1).
- Tujuannya: mencari pemilik IP tertentu agar MAC address-nya diketahui.

Semua dikirim ke Broadcast (ff:ff:ff:ff:ff:ff):

- Karena pengirim tidak tahu MAC tujuan, maka siaran ke seluruh LAN.
- Hanya pemilik IP yang sesuai akan membalas.

Peran masing-masing sumber:

- Sumber berbeda menunjukkan siapa yang aktif melakukan query.
- Router mungkin menyebar informasi ke semua node.
- Laptop atau HP melakukan ARP saat memulai koneksi baru.

4.Mengapa ARP Request Selalu ke Broadcast (tparp2.pcapng)

ARP Request dikirim ke broadcast (ff:ff:ff:ff:ff:ff) karena:

- Fungsi ARP adalah menerjemahkan IP ke MAC.
- Saat IP tujuan diketahui tapi MAC tidak, broadcast dilakukan ke seluruh jaringan lokal
- Semua host menerima pesan, hanya host dengan IP yang ditanyakan yang akan membalas.

Contoh (dari file capture):

- “Who has 172.16.0.208? Tell 172.16.0.1”
- Ethernet Header Destination = ff:ff:ff:ff:ff:ff
- Ini membuat host 172.16.0.208 merespons dengan ARP Reply

Ini mendukung efisiensi jaringan lokal karena hanya host yang relevan merespons dan ARP cache akan menyimpan hasilnya untuk komunikasi selanjutnya.

5. Analisis Format Pesan ARP: Request, Reply, dan Gratuitous ARP

Contoh pesan berbeda dalam tparp2.pcapng:

Who has 172.16.0.208? Tell 172.16.0.1

- Tipe: ARP Request (Opcode: 1)
- Tujuan: broadcast
- Fungsi: mencari MAC dari IP 172.16.0.208

Gratuitous ARP for 172.16.2.119 (Reply)

- Tipe: ARP Reply tanpa ada Request sebelumnya
- Tujuan: broadcast
- Fungsi: memperbarui cache semua host, atau memberitahu “saya adalah pemilik IP ini”

Gratuitous ARP for 172.16.0.210 (Request)

- Tipe: ARP Request, namun dikirim oleh pemilik IP ke semua
- Fungsi: deteksi konflik IP atau pengumuman IP/MAC secara proaktif

Peran Opcode:

- 1: ARP Request
- 2: ARP Reply

Header Ethernet:

- Source MAC = pengirim ARP
- Destination MAC = broadcast (ff:ff:ff:ff:ff:ff) untuk Request/Gratuitous