Tugas Praktikum SKJ ke-10

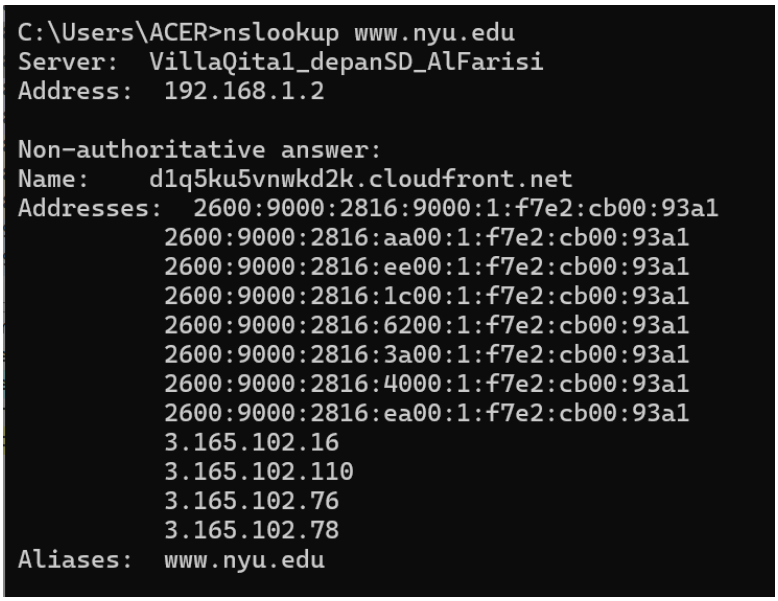
Nama : Bagus Cipta Pratama

NIM : 23/516539/PA/22097

Kelas : KOMC

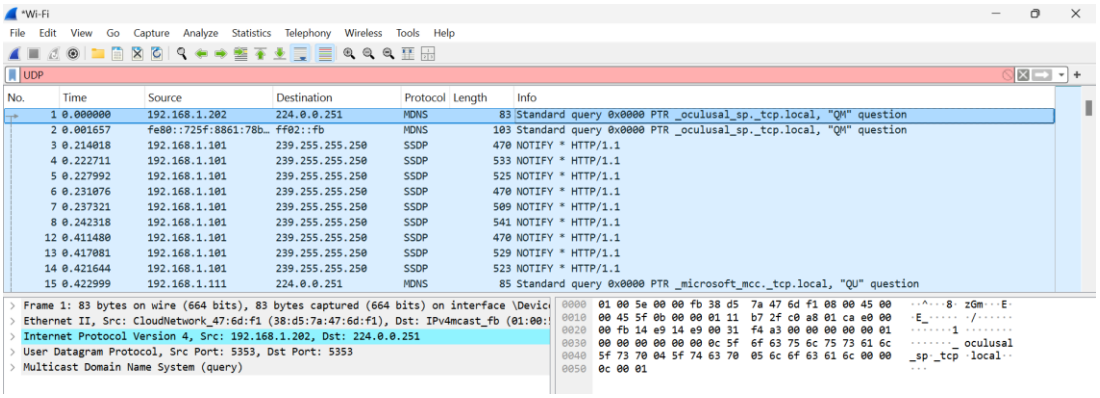
Aktivitas : Menangkap Paket UDP .

Perhatikan sebelum memulai menjawab keempat pertanyaan tadi , seperti yang tertera pada aktivitas , saya sudah mencoba menjalankan nslookup dengan Alamat www.nyu.edu , untuk setelahnya kita akan lebih mengeksplorasi apa yang ada pada paket UDP .



1. Pilih segmen UDP pertama di jejak Anda (segmen dengan nomor paket terendah). Perhatikan bahwa paket ini mungkin tidak selalu merupakan pesan DNS yang dikirim oleh nslookup. Apa nomor paket segmen ini di jejak Anda? Jenis pesan lapisan aplikasi atau pesan protokol apa yang dibawa dalam segmen UDP ini? Lihat rincian paket ini di Wireshark. Berapa banyak field yang ada di header UDP? (Jangan menjawab berdasarkan pengetahuan buku teks Anda! Jawab berdasarkan apa yang Anda amati langsung di jejak paket.) Apa nama nama field ini?

   Ketika saya melakukan filtering , dapat kita lihat pada screenshot dibawah ini bahwa protocol dengan nomor terkecil berjenis MDNS .




```
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
    Source Port: 5353
    Destination Port: 5353
    Length: 49
    Checksum: 0xf4a3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (41 bytes)
```

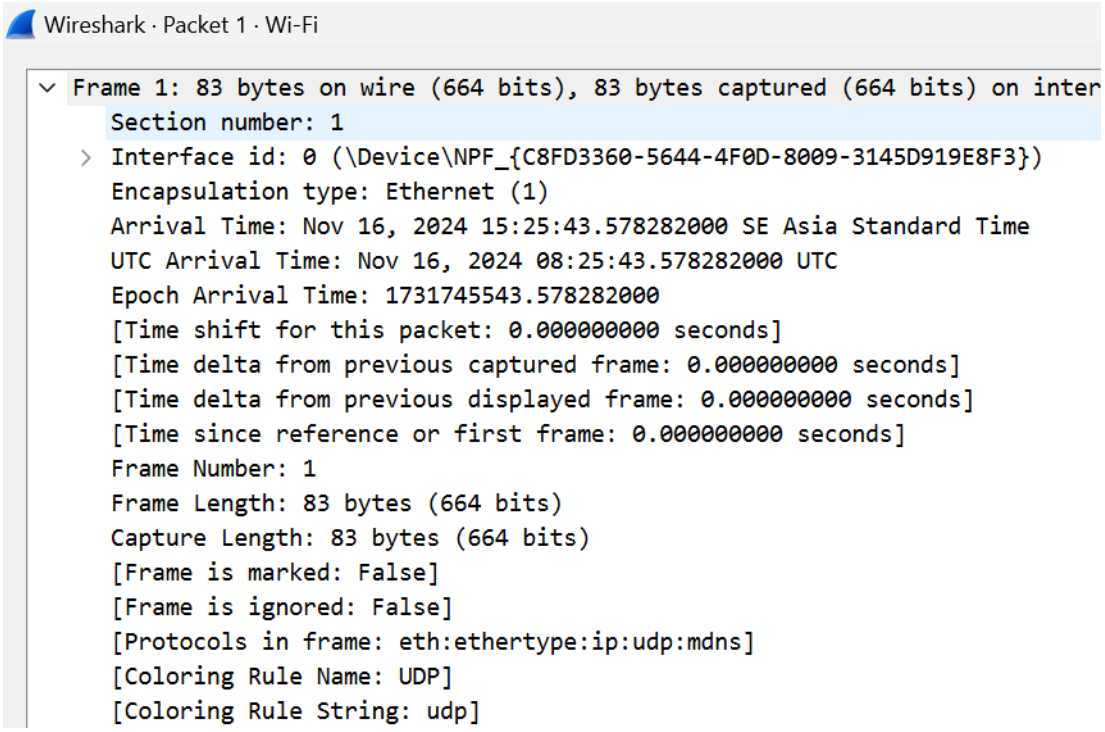
Paket UDP pertama yang terdeteksi dalam tangkapan data Wireshark adalah paket dengan nomor urut 1, yang menggunakan protokol aplikasi mDNS (Multicast Domain Name System). Protokol ini berjalan di atas UDP dan digunakan untuk melakukan query nama domain dalam jaringan lokal tanpa memerlukan server DNS terpusat. Paket ini memiliki Source Port 5353 dan Destination Port 5353, dengan panjang total paket sebesar 49 byte, yang mencakup header UDP dan payload. Nilai Checksum pada header UDP adalah 0xf4a3, meskipun statusnya tidak terverifikasi oleh Wireshark.

Paket ini membawa payload sebesar 41 byte, yang memuat informasi query untuk mDNS. Dari segi aktivitas, paket ini dikirim dari alamat IP 192.168.1.202 ke alamat multicast standar mDNS 224.0.0.251. Dengan demikian, paket nomor 1 dapat dikonfirmasi sebagai segmen UDP pertama yang berhasil ditangkap, meskipun jenis protokol aplikasinya adalah mDNS. Paket ini tetap termasuk kategori UDP karena menggunakan protokol tersebut di lapisan transport.

2. dengan melihat isi paket yang ditampilkan di bagian Isi Paket (ditampilkan dalam heksadesimal dan ASCII), berapa panjang masing-masing field header UDP ini (dalam byte)?

   Berdasarkan screenshot yang saya lakukan tadi, header UDP pada paket pertama memiliki total panjang 8 byte, terdiri dari empat field utama: Source Port (2 byte), Destination Port (2 byte), Length (2 byte, menunjukkan total panjang paket 49 byte), dan Checksum (2 byte, nilai 0xf4a3, tidak terverifikasi). Payload UDP memiliki panjang 41 byte, sesuai dengan nilai pada field Length yang mencakup total panjang header dan payload. Struktur ini mencerminkan standar format header UDP.

3. Apa yang ditunjukkan nilai di field Panjang tentang panjangnya? (Anda dapat menjawab pertanyaan ini berdasarkan pengetahuan buku teks Anda.) Verifikasi jawaban Anda berdasarkan paket UDP yang Anda tangkap.

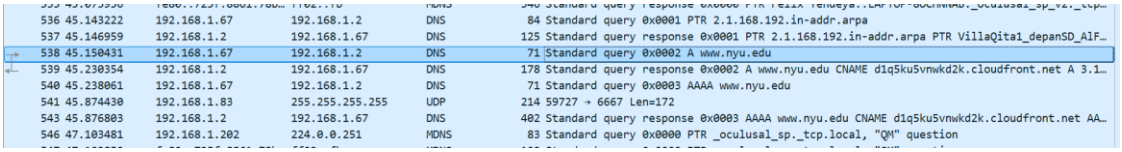


   Berdasarkan screenshot, panjang total paket UDP pertama adalah 83 byte, seperti yang terlihat pada field Frame Length. Nilai ini menunjukkan panjang keseluruhan paket, termasuk header Ethernet, header IP, header UDP, dan payload. Jika dibandingkan dengan field

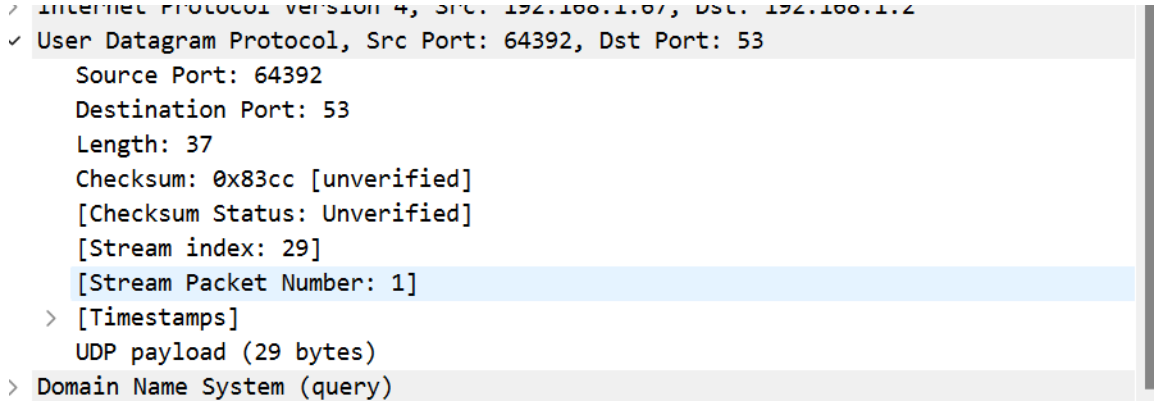
Length pada header UDP yang bernilai 49 byte, panjang ini hanya mencakup bagian UDP, yaitu header UDP (8 byte) dan payload UDP (41 byte). Sisa panjang paket berasal dari header protokol lapisan bawah, seperti header Ethernet (14 byte) dan header IP (20 byte). Dengan demikian, nilai Length pada header UDP sesuai dengan panjang data yang ditransport oleh UDP dalam paket ini. Analisis ini mengonfirmasi bahwa field Length pada header UDP menggambarkan panjang UDP secara spesifik, bukan panjang total frame.

4. Periksa sepasang paket UDP di jejak Anda, di mana host Anda mengirim paket UDP pertama dan paket UDP kedua adalah respons terhadap paket UDP pertama. (Petunjuk: Anda dapat menggunakan nslookup untuk menghasilkan sepasang paket ini.) Paket kedua dianggap sebagai respons terhadap paket pertama jika pengirim paket pertama adalah tujuan paket kedua. Temukan pasangan ini di jejak Anda. Apa nomor paket dari segmen pertama dari kedua segmen UDP ini? Apa nomor paket dari segmen kedua dari kedua segmen UDP ini? Jelaskan hubungan antara nomor port di kedua paket.

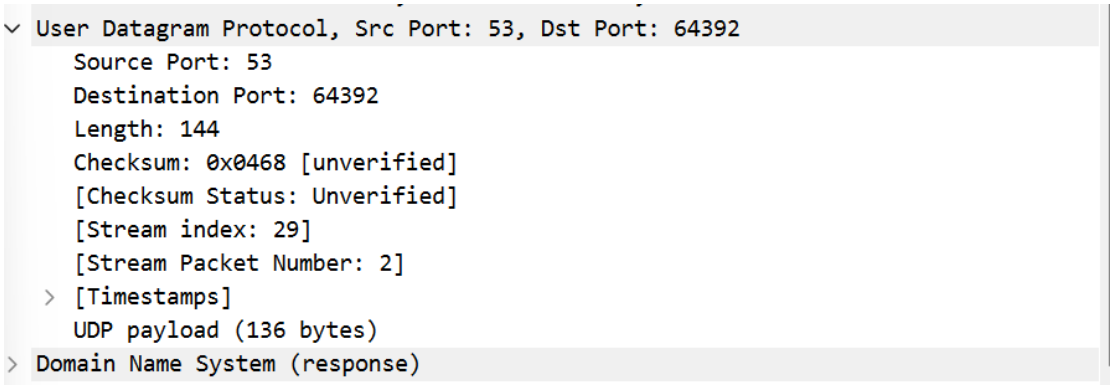
   Berikut adalah screenshot menggunakan nslookup www.nyu.edu yang sudah saya lakukan sebelumnya ,



   Ini adalah screenshot pada paket pertama query



Sedangkan ini adalah screenshot paket kedua yang merupakan response terhadap paket pertama ,



Dapat dilihat dan diperhatikan bahwa pada screenshot pertama , source port nya adalah 64392 dan destination portnya adalah 53 dan sebaliknya di bagian response kebalikannnya . Dari Hal tersebut , dapat diverifikasi bahwa kedua paket tersebut adalah komunikasi yang terjadi adalah komunikasi dua arah pada port yang sama .