**LAPORAN KONSEP JARINGAN**

**[Teori 07] Wireshark: DNS**



Disusun Oleh:

Aldow Fan Dzikri (NRP. 3121500022)

2 D3 ITA

Dosen Pengampu:

Iwan Syarif S.Kom., M.Kom., M.Sc., Ph.D.

**PROGRAM STUDI D3 TEKNIK INFORMATIKA**

**DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**2022**

1. **nslookup**

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Saya sengaja menggunakan dns server dari google terlihat server yang saya miliki tertulis dns.google dan dilengkapi address: 8.8.8.8, Lantas pertanyaannya apa ip address web server di asia yang saya tuju yaitu server dengan nama detik.com dengan dua address 103.49.221.211 dan 203.190.242.211

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Sama seperti soal nomor 1 server yang digunakan adalah dns server dari google, serta DNS servers untuk sebuah universitas di eropa memiliki IP address 36.86.63.182.

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Sebuah gambar berisi teks

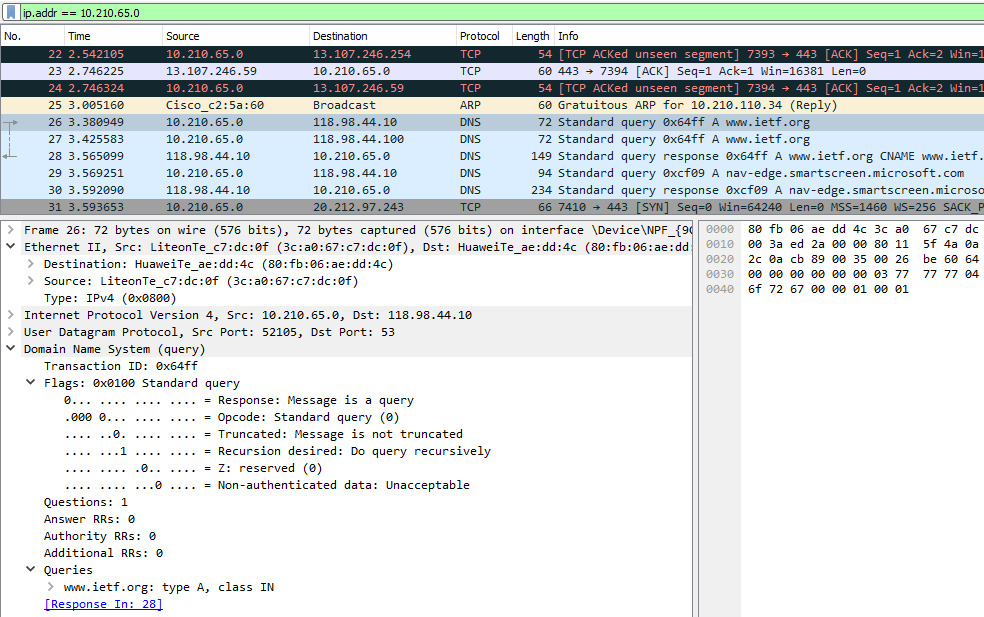
Deskripsi dibuat secara otomatis

**Analisis:**

IP address dari mail server adalah 18.0.72.3

1. **Tracing DNS with Wireshark**

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?



Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Dikirim melalui UDP

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

**Analisis:**

Dengan acuan gambar di soal nomor 2, dapat dipastikan bahwa Port destination DNS query message dan source port DNS Response message adalah 53.

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Itu dikirim ke 192.168.1.1, yang merupakan alamat IP dari salah satu server DNS lokal saya.

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Analisis:**

Type dari DNS Query adalah type A yang berarti tidak mengandung isi didalamnya.

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Keduanya memiliki kesamaan IP Address.

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Analis: Tidak.

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

* ***DNS Query Message***

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

Sebuah gambar berisi meja

Deskripsi dibuat secara otomatis

Sebuah gambar berisi meja

Deskripsi dibuat secara otomatis

* ***DNS Response Massage***

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Berdasarkan gambar diatas, dapat dipastikan bahwa Port destination DNS query message dan source port DNS Response message sama sama memiliki port 53.

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

**Analisis:**

Itu dikirim ke 10.210.65.0 yang bisa kita lihat dengan perintah ipconfig –all tangkapan layar, tangkapan layer tersebut adalah server DNS lokal default.

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Analisis:**

Type dari DNS Query adalah type A yang berarti tidak mengandung isi didalamnya.

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

15. Provide a screenshot.

Now repeat the previous experiment, but instead issue the command:

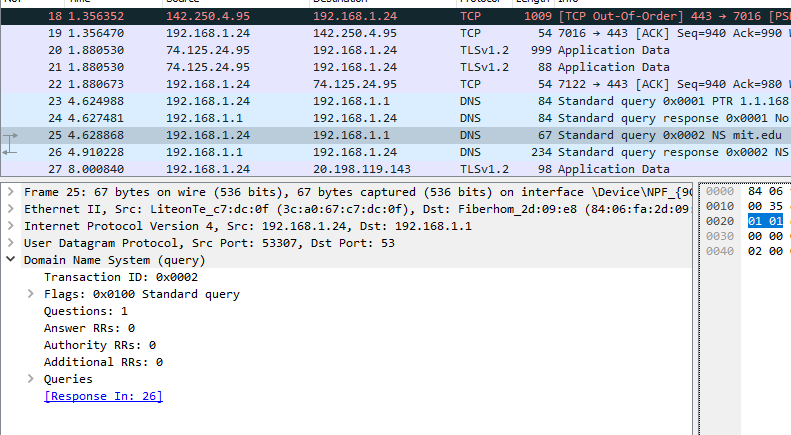
**nslookup –type=NS mit.edu**

Answer the following questions5 :

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis



**Analisis:**

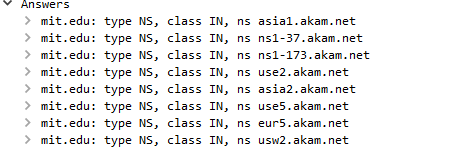
IP address DNS Query message dan default local address DNS Server memiliki IP address yang sama, yaitu 192.168.1.24, bisa dibuktikan dengan mengetikan perintah ipconfig /all diterminal perangkat yang digunakan.

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Analisis:**

Hasil DNS Query adalah NS yang berarti itu tidak ada jawaban.

18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?



19. Provide a screenshot

Now repeat the previous experiment, but instead issue the command:

nslookup

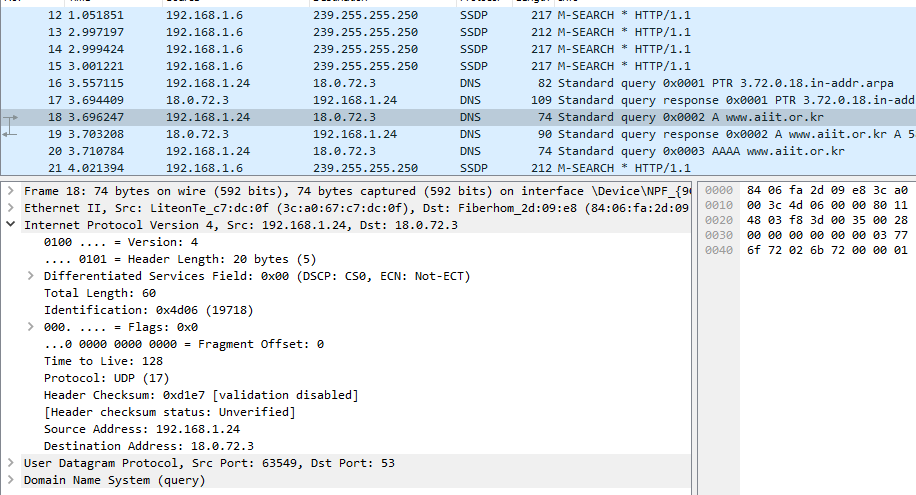
www.aiit.or.kr bitsy.mit.edu

Answer the following questions6:

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Sebuah gambar berisi teks

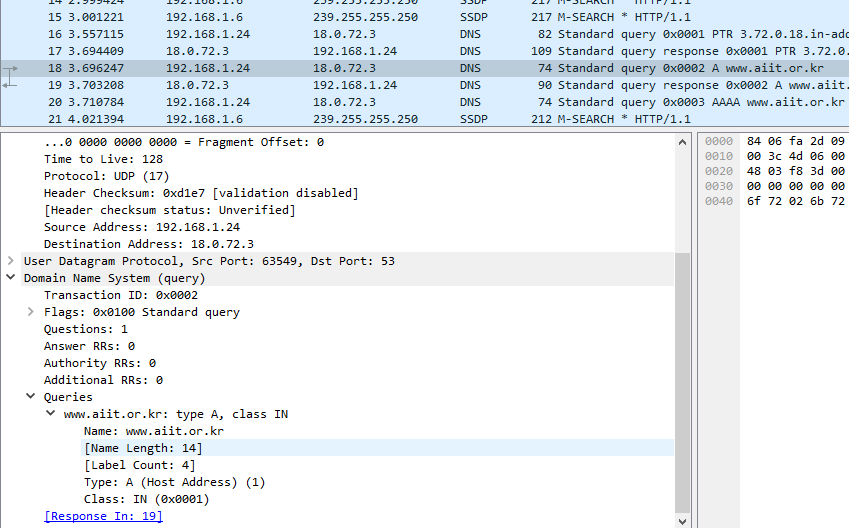
Deskripsi dibuat secara otomatis



**Analisis:**

IP address DNS Query message dan default local address DNS Server memiliki IP address yang sama, yaitu 192.168.1.24, bisa dibuktikan dengan mengetikan perintah ipconfig /all diterminal perangkat yang digunakan.

21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



**Analisis:**

Type A, hal ini sama seperti sebelumnya yaitu tidak ada jawaban yang dihasilkan.

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?



23. Provide a screenshot