

Tugas Praktikum SKJ ke-8

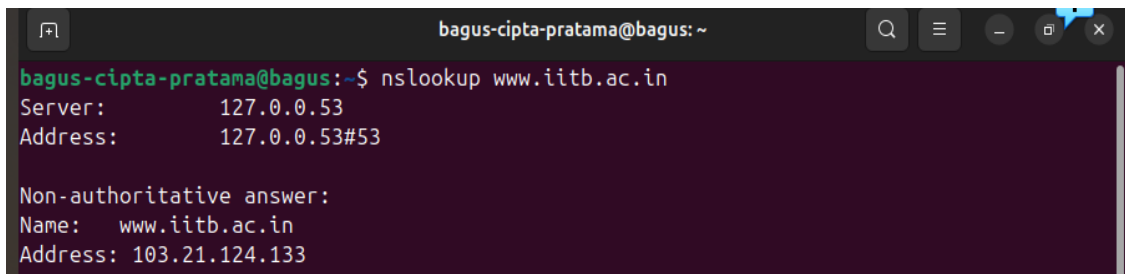
Nama : Bagus Cipta Pratama

NIM : 23/516539/PA/22097

Kelas : KOMC

Aktivitas pertama -nslookup :

1. Jalankan nslookup untuk memperoleh alamat IP dari server web untuk Indian Institute of Technology di Bombay, India: www.iitb.ac.in. Apa alamat IP dari www.iitb.ac.in?



```
bagus-cipta-pratama@bagus: ~  
bagus-cipta-pratama@bagus:~$ nslookup www.iitb.ac.in  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   www.iitb.ac.in  
Address: 103.21.124.133
```

Berdasarkan output tersebut didapatkan ip dari server web untuk iitb adalah 103.21.124.133

2. Apa alamat IP dari server DNS yang memberikan jawaban untuk perintah nslookup Anda di pertanyaan 1 di atas?

Dari output yang saya berikan diatas dapat dilihat bahwa

Server : 127.0.0.53

Address : 127.0.0.53#53

Sedangkan untuk DNS server yang saya dapatkan dalam cmd saya adalah sebagai berikut :

```
DNS Servers . . . . . : 10.13.10.13
```

3. Apakah jawaban dari perintah nslookup Anda di pertanyaan 1 di atas berasal dari server otoritatif atau non-otoritatif?

Jawaban berasal dari server non-otoritatif seperti yang ada pada output diatas . hal ini menunjukkan bahwa hasilnya kemungkinan berasal dari cache server dns local atau dari server perantara , yang merupakan jawaban non otoritatif

4. Gunakan perintah nslookup untuk menentukan nama server nama otoritatif untuk domain www.iitb.ac.in. Apa nama itu? (Jika ada lebih dari satu server otoritatif, apa nama dari server otoritatif pertama yang dikembalikan oleh nslookup)? Jika Anda harus menemukan alamat IP dari server nama otoritatif itu, bagaimana Anda akan melakukannya?

```
bagus-cipta-pratama@bagus:~$ nslookup -type=NS iitb.ac.in
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
iitb.ac.in      nameserver = dns3.iitb.ac.in.
iitb.ac.in      nameserver = dns1.iitb.ac.in.
iitb.ac.in      nameserver = dns2.iitb.ac.in.

Authoritative answers can be found from:
dns3.iitb.ac.in internet address = 103.21.127.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns1.iitb.ac.in internet address = 103.21.125.129
```

Berdasarkan output tersebut server otoritatif pertama adalah dns3.iitb.ac.in dan dapat dilihat bahwa Alamat ip untuk dns3.iitb.ac.in adalah 103.21.127.129 .

Aktivitas kedua -melacak dns dari aktivitas web surfing dengan wireshark

1. Ke alamat IP mana pesan permintaan DNS dikirim? Apakah ini alamat IP dari server DNS lokal default Anda?

permintaan dikirim ke Alamat IP 10.18.10.18 yang merupakan IP dari server DNS lokal saya . dapat dilihat dalam gambar berikut :

809	21.390757	10.6.172.250	10.18.10.18	DNS	92 Standard query 0xfa20 HTTPS writing.engr.psu.edu
811	21.390947	10.6.172.250	10.18.10.18	DNS	92 Standard query 0x45af A writing.engr.psu.edu
813	21.391116	10.6.172.250	10.18.10.18	DNS	107 Standard query 0x5b08 A optimizationguide-pa.googleapis.com
821	21.396452	10.6.172.250	10.18.10.18	DNS	92 Standard query 0x3ebc HTTPS writing.engr.psu.edu
823	21.396617	10.6.172.250	10.18.10.18	DNS	92 Standard query 0xe456 A writing.engr.psu.edu
837	21.430429	10.18.10.18	10.6.172.250	DNS	332 Standard query response 0x45af A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 14
838	21.430429	10.18.10.18	10.6.172.250	DNS	166 Standard query response 0xcd3d HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.
839	21.430429	10.18.10.18	10.6.172.250	DNS	175 Standard query response 0xfa20 HTTPS writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu :

2. Periksa pesan permintaan DNS. Apa "Tipe" dari permintaan DNS tersebut? Apakah pesan permintaan tersebut mengandung "jawaban"?

Jenis atau "Tipe" dari permintaan DNS pada pesan permintaan adalah standard query tipe A (Address). Ini terlihat dari bagian informasi pada kolom info yang mencantumkan "standard query A" diikuti oleh ID transaksi. Permintaan DNS tersebut mengandung 1 pertanyaan dan tidak mengandung jawaban. Pada bagian detail paket, terlihat bahwa Question bernilai 1 dan Answer RRs bernilai 0.

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

.... ..0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively

....0.. = Z: reserved (0)

....0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

3. Periksa pesan balasan DNS terhadap pesan permintaan. Berapa banyak "pertanyaan" yang terkandung dalam pesan balasan DNS ini? Berapa banyak "jawaban"?

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Dari screenshot yang ada diatas dapat dilihat bahwa ada 1 questions dan ada 2 jawaban yang berasal dari answer rrs .

Aktivitas ketiga - Melacak DNS dari nslookup dengan Wireshark

1. Ke alamat IP mana pesan permintaan DNS dikirim? Apakah ini alamat IP dari server DNS lokal default Anda?

perlu diperhatikan disini saya tidak langsung melakukan aktivitas 2 dan aktivitas 3 secara bersamaan sehingga ada perbedaan di aktivitas 2 dan 3 .

```
C:\Users\ACER>nslookup -type=NS umass.edu
Server:  VillaQita1_depanSD_AlFarisi
Address:  192.168.1.2
```

- Destination Address: 192.168.1.2
- [Stream index: 0]
- ✓ User Datagram Protocol, Src Port: 52390, Dst Port: 53
 - Source Port: 52390
 - Destination Port: 53
 - Length: 35
 - Checksum: 0x83ca [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 31]
 - [Stream Packet Number: 1]
 - ✓ [Timestamps]
 - [Time since first frame: 0.000000000 seconds]
 - [Time since previous frame: 0.000000000 seconds]
 - UDP payload (27 bytes)
 - ✓ Domain Name System (query)
 - Transaction ID: 0x0002
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - ✓ Queries
 - > umass.edu: type NS. class IN

Dapat dilihat bahwa Permintaan dikirim ke alamat IP 192.168.1.2 yang merupakan IP dari server DNS lokal saya.

2. Periksa pesan permintaan DNS. Berapa banyak pertanyaan yang dimiliki permintaan tersebut? Apakah pesan permintaan tersebut mengandung "jawaban"?

Jenis atau "Tipe" dari permintaan DNS pada pesan permintaan adalah standard query bertipe NS (Name Server). Ini terlihat dari bagian informasi pada kolom info yang mencantumkan "Standard query NS" diikuti oleh ID transaksi. Permintaan DNS tersebut mengandung 1 pertanyaan dan tidak mengandung jawaban. Pada bagian detail paket, terlihat bahwa Question bernilai 1 dan Answer RRs bernilai 0 .

```
✓ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ✓ Queries
    > umass.edu: type NS, class IN
    \[Response In: 505\]
```

3. Periksa pesan balasan DNS. Berapa banyak jawaban yang dimiliki balasan tersebut? Informasi apa yang terkandung dalam jawaban tersebut? Berapa banyak catatan sumber tambahan yang dikembalikan? Informasi tambahan apa yang disertakan dalam catatan sumber tambahan ini?

```
✓ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 3
  Additional RRs: 6
  > Queries
  ✓ Answers
    > umass.edu: type NS, class IN, ns ns3.umass.edu
    > umass.edu: type NS, class IN, ns ns2.umass.edu
    > umass.edu: type NS, class IN, ns ns1.umass.edu
  > Authoritative nameservers
  ✓ Additional records
    > ns3.umass.edu: type A, class IN, addr 69.16.40.18
    > ns2.umass.edu: type A, class IN, addr 128.119.10.28
    > ns1.umass.edu: type A, class IN, addr 128.119.10.27
    > ns2.umass.edu: type A, class IN, addr 128.119.10.28
    > ns1.umass.edu: type A, class IN, addr 128.119.10.27
    > ns3.umass.edu: type A, class IN, addr 69.16.40.18
    [Request In: 122]
    [Time: 0.009458000 seconds]
```

Perhatikan Balasan DNS ini memiliki **tiga jawaban** yang menunjukkan bahwa `umass.edu` menggunakan `ns3.umass.edu`, `ns2.umass.edu`, dan `ns1.umass.edu` sebagai nameserver. Selain itu, terdapat enam catatan sumber tambahan yang memberikan alamat IP untuk tiap nameserver tersebut: `ns3.umass.edu` dengan IP `69.16.40.18`, `ns2.umass.edu` dengan IP `128.119.10.28`, dan `ns1.umass.edu` dengan IP `128.119.10.27`. Namun, karena beberapa catatan ini bersifat duplikat, sejatinya hanya ada **tiga catatan tambahan unik** yang diperlukan. Meskipun ada duplikat, informasi ini tetap mempermudah client untuk menghubungi server terkait dalam proses resolusi nama `umass.edu`.