

Nama: Daffa Harikhsan
NIM: 23/513044/PA/21918

Tugas 8

Activity 8.3

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?

Jawab:

```
C:\Users\dhari>nslookup www.iitb.ac.in
Server: UnKnown
Address: 10.13.10.13

Non-authoritative answer:
Name: www.iitb.ac.in
Address: 103.21.124.133
```

Alamat IP dari www.iitb.ac.in itu adalah 103.21.124.133

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

Jawab:

Alamat IP dari server DNS adalah 10.13.10.13

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

Jawab:

Non-authoritative

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?

Jawab:

```
C:\Users\dhari>nslookup -type=NS iitb.ac.in
Server: UnKnown
Address: 10.13.10.13

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

dns1.iitb.ac.in internet address = 103.21.125.129
dns2.iitb.ac.in internet address = 103.21.126.129
dns3.iitb.ac.in internet address = 103.21.127.129
```

Nama server otoritatif: dns3.iitb.ac.in

Alamat IP nya 103.21.127.129, ini didapat dari perintah nslookup sendiri, saat kita menginputkan perintah nslookup muncul internet address (IP address)

Activity 8.4.1

No.	Time	Source	Destination	Protocol	Length	Info
676	2.884506	10.6.166.129	10.13.10.13	DNS	83	Standard query 0xc20 A spclient.vg.spotify.com
677	2.88452	10.6.166.129	10.13.10.13	DNS	83	Standard query 0x9ca0 HTTPS spclient.vg.spotify.com
1583	4.858450	10.6.166.129	10.13.10.13	DNS	85	Standard query 0x377d A gew4-spclient.spotify.com
1584	4.858625	10.6.166.129	10.13.10.13	DNS	85	Standard query 0xa302 HTTPS gew4-spclient.spotify.com
2528	7.970423	10.6.166.129	10.13.10.13	DNS	85	Standard query 0xc68b A gew4-spclient.spotify.com
2529	7.970586	10.6.166.129	10.13.10.13	DNS	85	Standard query 0xc2c7d HTTPS gew4-spclient.spotify.com
2764	9.139098	10.6.166.129	10.13.10.13	TCP	66	50289 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2765	9.139222	10.6.166.129	10.13.10.13	TCP	66	50290 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2768	9.142906	10.6.166.129	10.13.10.13	TCP	54	50289 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2769	9.142925	10.6.166.129	10.13.10.13	TCP	54	50290 → 53 [ACK] Seq=1 Ack=1 Win=65535 Len=0
2770	9.143275	10.6.166.129	10.13.10.13	DNS	100	Standard query 0x7893 A android.clients.google.com
2771	9.143279	10.6.166.129	10.13.10.13	TCP	56	50290 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=2 [TCP PDU reassembled in 2772]
2772	9.143337	10.6.166.129	10.13.10.13	DNS	98	Standard query 0x54aa HTTPS android.clients.google.com
2778	9.146140	10.6.166.129	10.13.10.13	TCP	54	50290 → 53 [FIN, ACK] Seq=47 Ack=121 Win=65415 Len=0
2779	9.146405	10.6.166.129	10.13.10.13	TCP	54	50289 → 53 [FIN, ACK] Seq=47 Ack=575 Win=64768 Len=0
2786	9.150875	10.6.166.129	10.13.10.13	TCP	54	50289 → 53 [ACK] Seq=48 Ack=576 Win=64768 Len=0
2787	9.150883	10.6.166.129	10.13.10.13	TCP	54	50290 → 53 [ACK] Seq=48 Ack=122 Win=65415 Len=0
2811	9.234308	10.6.166.129	10.13.10.13	TCP	66	50291 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2812	9.234398	10.6.166.129	10.13.10.13	TCP	66	50292 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2815	9.248288	10.6.166.129	10.13.10.13	TCP	54	50291 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2816	9.248394	10.6.166.129	10.13.10.13	TCP	54	50292 → 53 [ACK] Seq=1 Ack=1 Win=65380 Len=0

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

Jawab:

Alamat dikirim ke destination IP 10.13.10.13 yang itu sesuai dengan IP address laptop windows saya berdasarkan Ipconfig

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : UGM-Hotspot_MIPA
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 34-6F-24-A5-55-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::32b3:ef03:cd8b:c9c5%19(Preferred)
IPv4 Address. . . . . : 10.6.166.129(Preferred)
Subnet Mask . . . . . : 255.255.224.0
Lease Obtained. . . . . : Monday, 04 November 2024 13:43:33
Lease Expires . . . . . : Monday, 04 November 2024 16:55:27
Default Gateway . . . . . : 10.6.160.1
DHCP Server . . . . . : 10.6.160.1
DHCPv6 IAID . . . . . : 154431268
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-B9-D2-1D-34-6F-24-A5-55-F3
DNS Servers . . . . . : 10.13.10.13
                        10.18.10.18
NetBIOS over Tcpip. . . . . : Enabled
```

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

Jawab:

```
▼ Domain Name System (query)
  Length: 38
  Transaction ID: 0x8304
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ writing.engr.psu.edu: type A, class IN
      [Response In: 24713]
```

Tipe dari permintaan DNS tersebut adalah type A, dan tidak mengandung jawaban

```
▼ Domain Name System (query)
  Length: 38
  Transaction ID: 0x561d
  ▶ Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ writing.engr.psu.edu: type HTTPS, class IN
    [Response In: 24871]
```

Tipe dari permintaan DNS tersebut adalah type HTTPS, dan tidak mengandung jawaban

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

Jawab:

```
▼ Domain Name System (response)
  Length: 276
  Transaction ID: 0x8304
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 4
  Additional RRs: 6
  ▼ Queries
    ▶ writing.engr.psu.edu: type A, class IN
  ▶ Answers
  ▶ Authoritative nameservers
  ▶ Additional records
  [Request In: 24536]
  [Time: 0.576799000 seconds]
```

Tipe dari permintaan DNS tersebut adalah type A. Pertanyaan yang muncul dalam pesan balasan ini mengandung 1 pertanyaan dan 2 jawaban

```
▼ Domain Name System (response)
  Length: 119
  Transaction ID: 0x561d
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 0
  ▼ Queries
    ▶ writing.engr.psu.edu: type HTTPS, class IN
  ▶ Answers
  ▶ Authoritative nameservers
  [Request In: 24537]
  [Time: 1.460848000 seconds]
```

Tipe dari permintaan DNS tersebut adalah type HTTPS. Pertanyaan yang muncul dalam pesan balasan ini mengandung 1 pertanyaan dan 1 jawaban

Activity 8.4.2

```
C:\Users\dhari>nslookup -type=NS umass.edu
Server:  UnKnown
Address:  10.13.10.13

Non-authoritative answer:
umass.edu      nameserver = ns1.umass.edu
umass.edu      nameserver = ns3.umass.edu
umass.edu      nameserver = ns2.umass.edu

ns3.umass.edu  internet address = 69.16.40.18
ns1.umass.edu  internet address = 128.119.10.27
ns2.umass.edu  internet address = 128.119.10.28
```

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

Jawab:

```
DHCP Server . . . . . : 10.6.160.1
DHCPv6 IAID . . . . . : 154431268
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-B9-D2-1D-34-6F-24-A5-55-F3
DNS Servers . . . . . : 10.13.10.13
                        10.18.10.18
NetBIOS over Tcpip. . . . . : Enabled
```

Alamat IP ini menggunakan destination IP 10.13.10.13 yang mana alamat IP tersebut sesuai dengan alamat IP address yang digunakan laptop windows saya

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

Jawab:

```
▼ Domain Name System (response)
  Transaction ID: 0x0002
  ▶ Flags: 0x8183 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  ▶ Queries
  ▶ Authoritative nameservers
  [Request In: 8787]
  [Time: 0.002526000 seconds]
```

Pesan permintaan DNS mengandung 1 pertanyaan, dan tidak mengandung jawaban

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?

Jawab:

```
▼ Domain Name System (response)
  Transaction ID: 0x0003
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 3
  ▶ Queries
  ▼ Answers
    ▶ umass.edu: type NS, class IN, ns ns3.umass.edu
    ▶ umass.edu: type NS, class IN, ns ns1.umass.edu
    ▶ umass.edu: type NS, class IN, ns ns2.umass.edu
  ▼ Additional records
    ▶ ns3.umass.edu: type A, class IN, addr 69.16.40.18
    ▶ ns1.umass.edu: type A, class IN, addr 128.119.10.27
    ▶ ns2.umass.edu: type A, class IN, addr 128.119.10.28
  [Request In: 8789]
  [Time: 0.001817000 seconds]
```

Jawaban yang dimiliki 3 jawaban, di jawaban tersebut berisi informasi 3 nameserver dan additional records sebanyak 3 juga