

Tugas Pertemuan 8

Praktikum Sistem Komputer dan Jaringan

Kosmas Rio Legowo

23/512012/PA/21863

Departemen Ilmu Komputer dan Elektronika

Universitas Gadjah Mada

kosmasriolegowo@mail.ugm.ac.id

Chapter 8 Sistem Nama Domain (DNS)

Aktivitas 1 - nslookup

Hasil Aktivitas 1:

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 : IP dari server web untuk IITB (www.iitb.ac.in) adalah 103.21.124.133.

```
root@LAPTOP-VLGF85TL: ~  
root@LAPTOP-VLGF85TL:~# nslookup www.iitb.ac.in  
;; Got recursion not available from 192.168.128.1  
Server:          192.168.128.1  
Address:         192.168.128.1#53  
  
Non-authoritative answer:  
Name:   www.iitb.ac.in  
Address: 103.21.124.133  
Name:   dns1.iitb.ac.in  
Address: 103.21.125.129  
Name:   dns2.iitb.ac.in  
Address: 103.21.126.129  
Name:   dns3.iitb.ac.in  
Address: 103.21.127.129
```

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

Jawab :

Server : 192.168.128.1

Address : 192.168.128.1#53

DNS Server (alamat IPv4 komputer) : 10.13.10.13

```
Server:          192.168.128.1  
Address:         192.168.128.1#53  
  
DNS Servers . . . . . : 10.13.10.13  
                      10.18.10.18
```

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

Jawab : Berasal dari server non-otoritatif, dapat dilihat pada gambar di bawah ini:

```
Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.133
Name:   dns1.iitb.ac.in
Address: 103.21.125.129
Name:   dns2.iitb.ac.in
Address: 103.21.126.129
Name:   dns3.iitb.ac.in
Address: 103.21.127.129
```

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 : Nama server otoritatif pertama adalah dns1.iitb.ac.in. Untuk mengambil alamat IP dari server nama otoritatif kita dapat langsung melihat IP nya setelah nama server otoritatif itu sendiri, sebagai contoh untuk server otoritatif pertama:

```
Name: dns1.iitb.ac.in
Address: 103.21.125.129
```

Maka IP address dari dns1.iitb.ac.in adalah 103.21.125.129.

```
root@LAPTOP-VLGF85TL:~# nslookup -type=NS iitb.ac.in
;; Got recursion not available from 192.168.128.1
Server:           192.168.128.1
Address:          192.168.128.1#53

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.
Name:   dns1.iitb.ac.in
Address: 103.21.125.129
Name:   dns2.iitb.ac.in
Address: 103.21.126.129
Name:   dns3.iitb.ac.in
Address: 103.21.127.129
```

Aktivitas 2: Melacak DNS dari aktivitas web-surfing dengan Wireshark

Hasil Aktivitas 2:

The screenshot shows a web browser window displaying a website titled "Writing as an Engineer or Scientist". The website content includes a header, a main text area, and a section with video thumbnails labeled "Collection of Short Films", "Tutorial: Reports", and "Tutorial". To the right of the browser window, the Wireshark network traffic analysis tool is open. The top pane shows a list of captured packets, with the selected packet being a DNS query from 10.6.177.194 to 10.13.10.13. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Domain Name System (query) section.

Pertanyaan-pertanyaan:

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

Jawab : Permintaan dikirim ke alamat IP 10.13.10.13 yang merupakan IP dari server DNS lokal saya. Yang dapat dilihat pada ipconfig /all.

The screenshot shows the Wireshark network traffic analysis tool. The top pane shows a list of captured packets, with the selected packet being a DNS query from 10.6.177.194 to 10.13.10.13. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Domain Name System (query) section. The details section shows the query for "writing.engr.psu.edu" and the response from "10.13.10.13".

```
DNS Servers . . . . . : 10.13.10.13
                        10.18.10.18
```

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

Jawab : 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.

No.	Time	Source	Destination	Protocol	Length	Info
670	3.293128	10.6.177.194	10.13.10.13	DNS	80	Standard query 0x3d35 A writing.engr.psu.edu
671	3.293340	10.6.177.194	10.13.10.13	DNS	80	Standard query 0xa91e HTTPS writing.engr.psu.edu
672	3.297758	10.6.177.194	10.13.10.13	DNS	81	Standard query 0xdd77 A wpad.UGM-Hotspot_MIPA
673	3.303107	10.13.10.13	10.6.177.194	DNS	156	Standard query response 0xdd77 No such name A wpad.UGM-Hotspot_MIPA SOA a.root-servers.net
676	3.311378	10.6.177.194	10.13.10.13	DNS	80	Standard query 0x9adb A writing.engr.psu.edu
714	3.591186	10.13.10.13	10.6.177.194	DNS	318	Standard query response 0x3d35 A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 146.186.145.12 NS ns6.psu.edu NS ns5.psu.edu
715	3.591186	10.13.10.13	10.6.177.194	DNS	318	Standard query response 0x9adb A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 146.186.145.12 NS ns6.psu.edu NS ns3.psu.edu
716	3.591186	10.13.10.13	10.6.177.194	DNS	161	Standard query response 0xa91e HTTPS writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu SOA ns5.psu.edu

> Frame 670: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0
> Ethernet II, Src: Routerboard_36:e0:68 (d4:01:c3:36:e0:68), Dst: Routerboard_36:e0:68 (d4:01:c3:36:e0:68)
> Internet Protocol Version 4, Src: 10.6.177.194, Dst: 10.13.10.13
> User Datagram Protocol, Src Port: 60798, Dst Port: 53
> Domain Name System (query)
Transaction ID: 0x3d35
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 714]

0000 d4 01 c3 36 e0 68 4c 44 5b 35 11
0010 00 42 69 b4 00 00 80 11 00 00 0e
0020 0a 0d ed 7e 00 35 00 2e d0 21 3f
0030 00 00 00 00 00 07 77 72 69 7a
0040 0e 67 72 03 70 73 75 03 65 64 7

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

Jawab : Jumlah pertanyaan adalah 1, ditunjukkan di bagian Questions: 1. Jumlah jawaban adalah 2, ditunjukkan di bagian Answer RRs: 2.

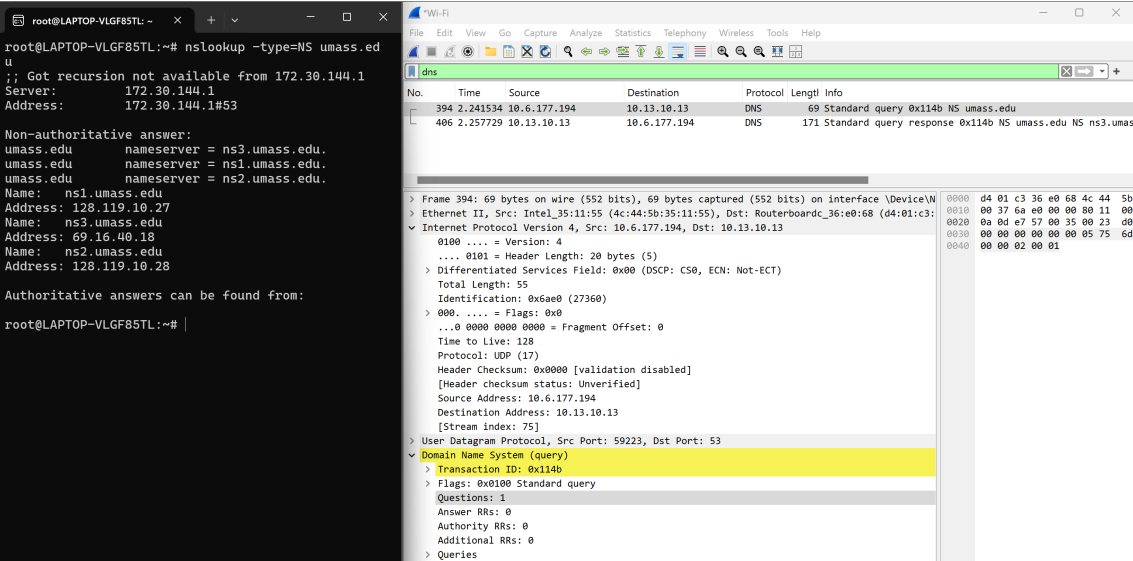
No.	Time	Source	Destination	Protocol	Length	Info
670	3.293128	10.6.177.194	10.13.10.13	DNS	80	Standard query 0x3d35 A writing.engr.psu.edu
671	3.293340	10.6.177.194	10.13.10.13	DNS	80	Standard query 0xa91e HTTPS writing.engr.psu.edu
672	3.297758	10.6.177.194	10.13.10.13	DNS	81	Standard query 0xdd77 A wpad.UGM-Hotspot_MIPA
673	3.303107	10.13.10.13	10.6.177.194	DNS	156	Standard query response 0xdd77 No such name A wpad.UGM-Hotspot_MIPA SOA a.root-servers.net
676	3.311378	10.6.177.194	10.13.10.13	DNS	80	Standard query 0x9adb A writing.engr.psu.edu
714	3.591186	10.13.10.13	10.6.177.194	DNS	318	Standard query response 0x3d35 A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 146.186.145.12 NS ns6.psu.edu NS ns5.psu.edu
715	3.591186	10.13.10.13	10.6.177.194	DNS	318	Standard query response 0x9adb A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 146.186.145.12 NS ns6.psu.edu NS ns3.psu.edu
716	3.591186	10.13.10.13	10.6.177.194	DNS	161	Standard query response 0xa91e HTTPS writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu SOA ns5.psu.edu

> Frame 714: 318 bytes on wire (2544 bits), 318 bytes captured (2544 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0
> Ethernet II, Src: Routerboard_36:e0:68 (d4:01:c3:36:e0:68), Dst: Intel_35:11:55 (4c:44:5b:35:11:55)
> Internet Protocol Version 4, Src: 10.13.10.13, Dst: 10.6.177.194
> User Datagram Protocol, Src Port: 53, Dst Port: 60798
> Domain Name System (response)
Transaction ID: 0x3d35
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 4
Additional RRs: 6
Queries
writing.engr.psu.edu: type CNAME, class IN, cname coe-a10-01.ncts.psu.edu
coe-a10-01.ncts.psu.edu: type A, class IN, addr 146.186.145.12
Authoritative nameservers
psu.edu: type NS, class IN, ns ns6.psu.edu
psu.edu: type NS, class IN, ns ns5.psu.edu
psu.edu: type NS, class IN, ns ns3.psu.edu
psu.edu: type NS, class IN, ns ns4.psu.edu
Additional records
ns4.psu.edu: type A, class IN, addr 128.118.25.5
ns4.psu.edu: type AAAA, class IN, addr 2610:8:7800::14
ns5.psu.edu: type A, class IN, addr 128.118.25.4
ns5.psu.edu: type AAAA, class IN, addr 2610:8:7800::5
ns3.psu.edu: type A, class IN, addr 52.224.90.37
ns6.psu.edu: type A, class IN, addr 128.118.70.4
[Request In: 670]
[Time: 0.298858000 seconds]

0000 4c 44 5b 35 11 55 d4 01 c3 36 e0 68 00 00 45 f
0010 01 30 b6 36 00 00 3c 11 ef a4 0a 0d 0a 0d 0a
0020 b1 c2 00 35 ed 7e 01 1c db eb 3d 35 81 80 0
0030 00 02 00 04 00 06 07 77 72 69 74 69 6e 67 04
0040 6e 67 72 03 70 73 75 03 65 64 75 00 00 01 00
0050 c0 0c 00 05 00 01 00 00 03 cb 00 12 0a 63 6f
0060 2d 61 31 30 2d 30 31 04 6e 63 74 73 c0 19 c0
0070 00 01 00 01 00 00 02 58 00 04 92 ba 91 0c c0
0080 00 02 00 01 00 01 4c 77 00 06 03 6e 73 36 c0
0090 c0 19 00 02 00 01 00 01 4c 77 00 06 03 6e 73
00a0 c0 19 c0 19 00 02 00 01 00 01 4c 77 00 06 03
00b0 73 33 c0 19 c0 19 00 02 00 01 00 01 4c 77 00
00c0 03 6e 73 34 c0 19 c0 96 00 01 00 01 00 01 4c
00d0 00 04 00 76 19 05 c0 96 00 1c 00 01 00 01 4c
00e0 00 10 25 10 00 00 78 00 00 00 00 00 00 00
00f0 00 04 c0 72 00 01 00 01 00 01 4c 77 00 04 80
0100 19 04 c0 72 00 1c 00 01 00 01 4c 77 00 10 26
0110 00 06 78 00 00 00 00 00 00 00 00 00 05 c0
0120 00 01 00 01 00 01 4c 77 00 04 34 e0 5a 25 c0
0130 00 01 00 01 00 01 4c 77 00 04 80 76 46 04

Aktivitas 3: Melacak DNS dari nslookup dengan Wireshark

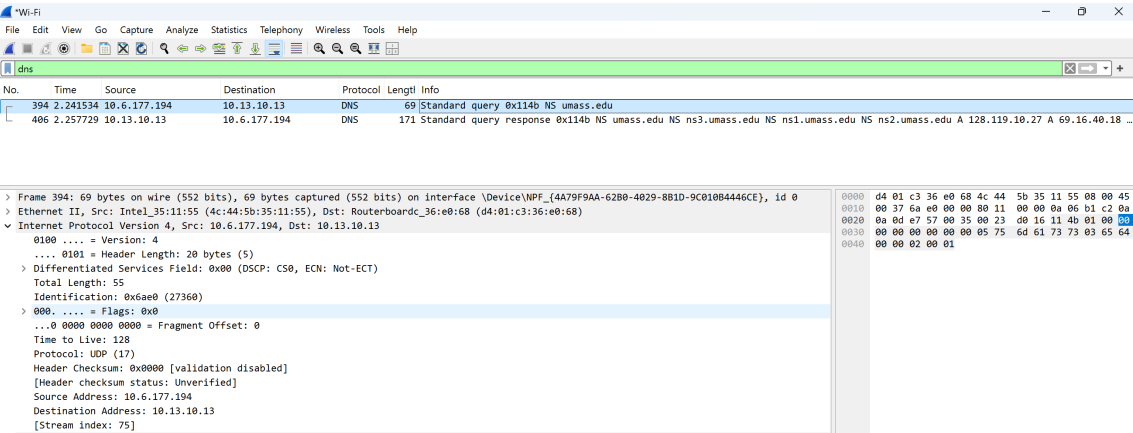
Hasil Aktivitas 3:



Pertanyaan-pertanyaan:

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

Jawab : Permintaan dikirim ke alamat IP 10.13.10.13 yang merupakan IP dari server DNS lokal saya. Yang dapat dilihat pada ipconfig /all.



DNS Servers : 10.13.10.13
10.18.10.18

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

Jawab : 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.

No.	Time	Source	Destination	Protocol	Length	Info
394	2.241534	10.6.177.194	10.13.10.13	DNS	69	Standard query 0x114b NS umass.edu
406	2.257729	10.13.10.13	10.6.177.194	DNS	171	Standard query response 0x114b NS umass.edu NS ns3.umass.edu NS ns1.umass.edu NS ns2.umass.edu A 128.119.10.27 A 69.16.40.18 ...

> Frame 394: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0	0000	d4 01 c3 36 e0 68 4c 44 5b 35 11 55 08 00 45 f
> Ethernet II, Src: Intel_35:11:55 (4c:44:5b:35:11:55), Dst: Routerboard_36:e0:68 (d4:01:c3:36:e0:68)	0010	00 37 6a e0 00 00 80 11 00 00 0a 06 b1 c3 0a f
> Internet Protocol Version 4, Src: 10.6.177.194, Dst: 10.13.10.13	0020	0a 00 e7 57 00 35 00 23 d0 16 11 4b 01 00 00 f
> User Datagram Protocol, Src Port: 59223, Dst Port: 53	0030	00 00 00 00 00 00 05 75 6d 61 73 73 03 65 64 f
> Domain Name System (query)	0040	00 00 02 00 01
> Transaction ID: 0x114b		
> Flags: 0x0100 Standard query		
> Questions: 1		
> Answer RRs: 0		
> Authority RRs: 0		
> Additional RRs: 0		
> Queries		

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 : Jumlah pertanyaan adalah 1, ditunjukkan di bagian Questions: 1. Jumlah jawaban adalah 3, ditunjukkan di bagian Answer RRs: 3. Daftar jawaban adalah sebagai berikut:

- (a) umass.edu: type NS, class IN, ns ns3.umass.edu
- (b) umass.edu: type NS, class IN, ns ns1.umass.edu
- (c) umass.edu: type NS, class IN, ns ns2.umass.edu

Respons DNS mengembalikan 3 catatan sumber tambahan (Additional Records) yang terlihat pada nilai dari Additional RRs adalah 3, informasi tambahan yang disertakan yaitu:

- (a) ns1.umass.edu: type A, class IN, addr 128.119.10.27
- (b) ns3.umass.edu: type A, class IN, addr 69.16.40.18
- (c) ns2.umass.edu: type A, class IN, addr 128.119.10.28

No.	Time	Source	Destination	Protocol	Length	Info
394	2.241534	10.6.177.194	10.13.10.13	DNS	69	Standard query 0x114b NS umass.edu
406	2.257729	10.13.10.13	10.6.177.194	DNS	171	Standard query response 0x114b NS umass.edu NS ns3.umass.edu NS ns1.umass.edu NS ns2.umass.edu A 128.119.10.27 A 69.16.40.18 ...

> Frame 406: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface \Device\NPF_{4A79F9AA-62B0-4029-8B1D-9C01084446CE}, id 0	0000	4c 44 5b 35 11 55 d4 01 c3 36 e0 68 08 00 45 f
> Ethernet II, Src: Routerboard_36:e0:68 (d4:01:c3:36:e0:68), Dst: Intel_35:11:55 (4c:44:5b:35:11:55)	0010	00 9d bd 43 00 00 3c 11 f1 2a 0a 0d 0a 0d 0a f
> Internet Protocol Version 4, Src: 10.13.10.13, Dst: 10.6.177.194	0020	b1 c2 00 35 e7 57 00 89 a4 d9 11 4b 81 80 00 f
> User Datagram Protocol, Src Port: 53, Dst Port: 59223	0030	00 01 00 00 00 03 05 75 6d 61 73 73 03 65 64 f
> Domain Name System (response)	0040	00 00 02 00 01 c0 0c 00 02 00 01 00 09 26 f
> Transaction ID: 0x114b	0050	06 03 6e 73 33 c0 0c c0 0c 00 02 00 01 00 00 f
> Flags: 0x0100 Standard query response, No error	0060	26 00 06 03 6e 73 31 c0 0c c0 0c 00 02 00 01 f
> Questions: 1	0070	00 00 26 00 06 03 6e 73 32 c0 0c c0 39 00 01 f
> Answer RRs: 3	0080	01 00 02 9d fc 00 04 80 77 0a 1b c0 27 00 01 f
> Authority RRs: 0	0090	01 00 02 9d fc 00 04 45 10 28 12 c0 20 4b 00 01 f
> Additional RRs: 3	00a0	01 00 02 9d fc 00 04 80 77 0a 1c
> 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		
> ns1.umass.edu: type A, class IN, addr 128.119.10.27		
> ns3.umass.edu: type A, class IN, addr 69.16.40.18		
> ns2.umass.edu: type A, class IN, addr 128.119.10.28		
[Request In: 394]		
[Time: 0.016195000 seconds]		