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

Tugas 10

Activity 1

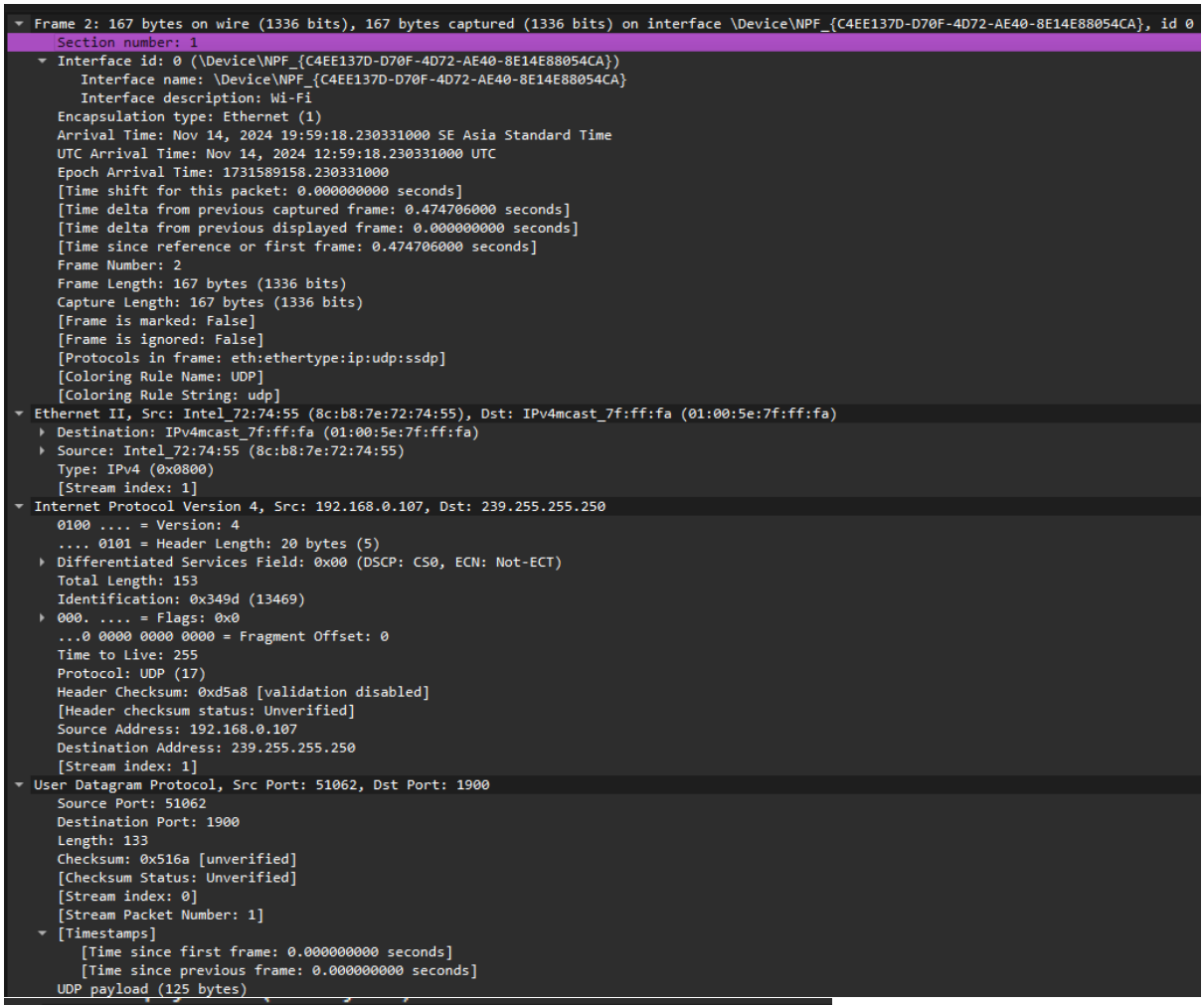
```
C:\Users\dhari>nslookup www.wikipedia.com
Server:  1.0.168.192.in-addr.arpa
Address:  192.168.0.1

Non-authoritative answer:
Name:    ncredir-lb.wikimedia.org
Addresses:  2001:df2:e500:ed1a::3
          103.102.166.226
Aliases:  www.wikipedia.com


C:\Users\dhari>_
```

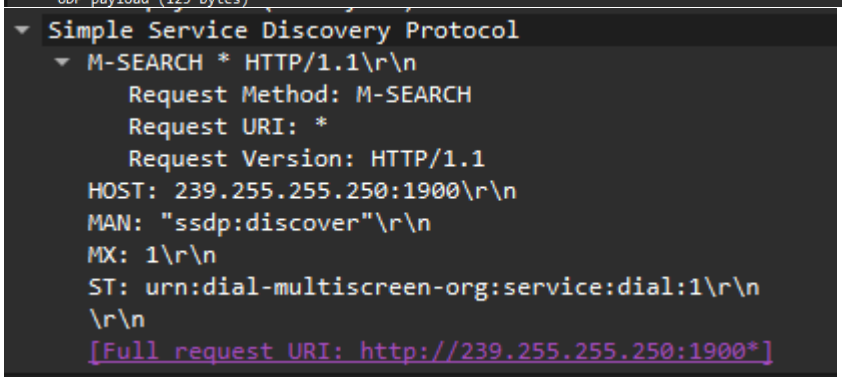
Mengunjungi situs Wikipedia.

udp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.474296	192.168.0.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.823819	192.168.0.102	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
4	0.826228	192.168.0.1	192.168.0.102	SSDP	455	HTTP/1.1 200 OK
23	1.499050	192.168.0.107	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
24	1.696920	192.168.0.102	224.77.77.77	UDP	148	12177 → 12177 Len=106
30	2.522742	192.168.0.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
31	3.144406	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
32	3.159389	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
33	3.163981	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
34	3.168895	192.168.0.1	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
35	3.173226	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
36	3.242438	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
37	3.247926	192.168.0.1	239.255.255.250	SSDP	521	NOTIFY * HTTP/1.1
38	3.262308	192.168.0.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
39	3.271413	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
40	3.276102	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
41	3.354010	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
42	3.443757	192.168.0.107	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
48	3.835657	192.168.0.102	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
49	3.867185	192.168.0.1	192.168.0.102	SSDP	455	HTTP/1.1 200 OK
50	4.705552	192.168.0.102	224.77.77.77	UDP	148	12177 → 12177 Len=106
51	5.491717	192.168.0.107	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
56	6.516366	192.168.0.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
57	6.567461	192.168.0.102	192.168.0.1	DNS	85	Standard query 0x5a1d A gew4-spclient.spotify.com
58	6.567618	192.168.0.102	192.168.0.1	DNS	85	Standard query 0xb854 HTTPS gew4-spclient.spotify.com
59	6.580899	192.168.0.1	192.168.0.102	DNS	150	Standard query response 0x5a1d A gew4-spclient.spotify.com CNAME edge-web-gew4.dual-gslb.spotify.com A 35.186.224.28
60	6.580899	192.168.0.1	192.168.0.102	DNS	213	Standard query response 0xb854 HTTPS gew4-spclient.spotify.com CNAME edge-web-gew4.dual-gslb.spotify.com SOA ns-cloud-d1.googledomains.com
61	6.581985	192.168.0.102	35.186.224.28	QUIC	1292	Initial, DCID=ca4f809d22c67c41, PKN: 1, CRYPTO
62	6.582028	192.168.0.102	35.186.224.28	QUIC	1292	Initial, DCID=ca4f809d22c67c41, PKN: 2, PADDING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO
63	6.618441	35.186.224.28	192.168.0.102	QUIC	82	Initial, SCID=ea4f809d22c67c41, PKN: 1, ACK
64	6.618500	35.186.224.28	192.168.0.102	QUIC	1292	Initial, SCID=ea4f809d22c67c41, PKN: 2, ACK, PADDING
65	6.628411	35.186.224.28	192.168.0.102	QUIC	1292	Protected Payload (KP0)
66	6.629491	192.168.0.102	35.186.224.28	QUIC	131	Handshake, DCID=ea4f809d22c67c41
67	6.629595	192.168.0.102	35.186.224.28	QUIC	110	Protected Payload (KP0), DCID=ea4f809d22c67c41
68	6.629841	192.168.0.102	35.186.224.28	QUIC	1288	Protected Payload (KP0), DCID=ea4f809d22c67c41
69	6.629875	192.168.0.102	35.186.224.28	QUIC	1108	Protected Payload (KP0), DCID=ea4f809d22c67c41
70	6.657385	35.186.224.28	192.168.0.102	QUIC	560	Protected Payload (KP0)
71	6.657385	35.186.224.28	192.168.0.102	QUIC	163	Protected Payload (KP0)
72	6.657385	35.186.224.28	192.168.0.102	QUIC	69	Protected Payload (KP0)
73	6.657781	192.168.0.102	35.186.224.28	QUIC	74	Protected Payload (KP0), DCID=ea4f809d22c67c41
74	6.683708	35.186.224.28	192.168.0.102	QUIC	66	Protected Payload (KP0)
75	6.684048	192.168.0.102	35.186.224.28	QUIC	73	Protected Payload (KP0), DCID=ea4f809d22c67c41
76	6.839137	192.168.0.102	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
77	6.926251	192.168.0.1	192.168.0.102	SSDP	455	HTTP/1.1 200 OK
78	7.051972	35.186.224.28	192.168.0.102	QUIC	216	Protected Payload (KP0)
79	7.051972	35.186.224.28	192.168.0.102	QUIC	277	Protected Payload (KP0)
80	7.052780	192.168.0.102	35.186.224.28	QUIC	77	Protected Payload (KP0), DCID=ea4f809d22c67c41
81	7.061060	35.186.224.28	192.168.0.102	QUIC	216	Protected Payload (KP0)
82	7.061586	192.168.0.102	35.186.224.28	QUIC	75	Protected Payload (KP0), DCID=ea4f809d22c67c41
83	7.140724	192.168.0.102	35.186.224.28	QUIC	72	Protected Payload (KP0), DCID=ea4f809d22c67c41
84	7.259757	35.186.224.28	192.168.0.102	QUIC	66	Protected Payload (KP0)

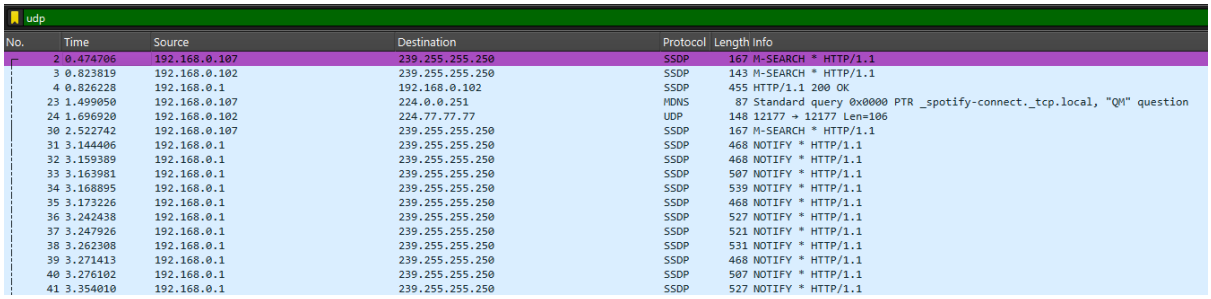
Tangkapan UDP





Isi Paket UDP pertama

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?
Jawab:



udp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.474706	192.168.0.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
3	0.823819	192.168.0.102	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
4	0.826228	192.168.0.1	192.168.0.102	SSDP	455	HTTP/1.1 200 OK
23	1.499050	192.168.0.107	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
24	1.696920	192.168.0.102	224.77.77.77	UDP	148	12177 → 12177 Len=106
30	2.522742	192.168.0.107	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
31	3.144406	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
32	3.159389	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
33	3.163981	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
34	3.168895	192.168.0.1	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
35	3.173226	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
36	3.242438	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1
37	3.247926	192.168.0.1	239.255.255.250	SSDP	521	NOTIFY * HTTP/1.1
38	3.262308	192.168.0.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
39	3.271413	192.168.0.1	239.255.255.250	SSDP	468	NOTIFY * HTTP/1.1
40	3.276102	192.168.0.1	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
41	3.354010	192.168.0.1	239.255.255.250	SSDP	527	NOTIFY * HTTP/1.1

- Nomor paket segmen UDP pada jejak yang diunggah adalah paket dengan nomor 2
- Jenis Pesan lapisan aplikasi yang dibawa dalam segmen UDP ini adalah SSDP (Simple Service Discovery Protocol), yang merupakan bagian dari protokol HTTP.
- Banyak field yang ada di header UDP ada 4 yakni:
    - Source Port (menunjukkan port asal paket)
    - Destination Port (menunjukkan port tujuan paket)
    - Length (menunjukkan panjang total dari header dan data UDP dalam byte)
    - Checksum (digunakan untuk verifikasi intergritas dalam paket UDP)

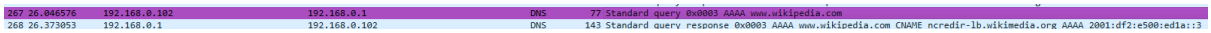
2. Dengan melihat isi paket yang ditampilkan di bagian Isi Paket (ditampilkan dalam heksadesimal dan ASCII), berapa panjang masing-masing field header UDP ini (dalam byte)?
Jawab:
Berdasarkan data, setiap field UDP berukuran 2 byte (16 bit) dalam representasi heksadesimal. Total panjang header UDP adalah 8 byte (4 field x 2 byte). Field- field header UDP tersebut menempati 4 karakter yakni:

- Source Port: 2 byte (16 bit atau 4 karakter heksadesimal)
- Destination Port: 2 byte (16 bit atau 4 karakter heksadesimal)
- Length: 2 byte (16 bit atau 4 karakter heksadesimal)
- Checksum: 2 byte (16 bit atau 4 karakter heksadesimal)

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.
Jawab:
Field Panjang (Length) pada header UDP menunjukkan total panjang datagram UDP dalam byte, yang mencakup panjang header UDP (8 byte) ditambah panjang data (payload) yang dikirim. Kita dapat memverifikasi ini dengan menghitung jumlah byte dari awal header UDP hingga akhir data.
Berdasarkan paket UDP yang ditangkap, kita dapat memverifikasi apakah nilai di field Panjang sesuai dengan ukuran total dari header dan data. Misalnya, jika field Panjang memiliki nilai 133 (dalam paket yang Anda lampirkan), berarti panjang total dari header UDP dan data adalah 133 byte.

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.
Jawab:

```
C:\Users\dhari>nslookup www.wikipedia.com
Server:  1.0.168.192.in-addr.arpa
Address:  192.168.0.1

Non-authoritative answer:
Name:    ncredir-lb.wikimedia.org
Addresses:  2001:df2:e500:ed1a::3
          103.102.166.226
Aliases:  www.wikipedia.com
```



- Nomor Paket segmen pertama adalah 267.

```
User Datagram Protocol, Src Port: 53478, Dst Port: 53
   Source Port: 53478
   Destination Port: 53
   Length: 43
   Checksum: 0xf5e8 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 15]
   [Stream Packet Number: 1]
 ▾ [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
   UDP payload (35 bytes)
```

  - Source IP dengan IP 192.168.0.102
  - Destination IP dengan IP 192.168.0.1
  - Source Port: 53478
  - Destination Port: 53

- Nomor Paket segmen kedua adalah 268.

```
User Datagram Protocol, Src Port: 53, Dst Port: 53478
   Source Port: 53
   Destination Port: 53478
   Length: 109
   Checksum: 0xe756 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 15]
   [Stream Packet Number: 2]
 ▾ [Timestamps]
      [Time since first frame: 0.326477000 seconds]
      [Time since previous frame: 0.326477000 seconds]
   UDP payload (101 bytes)
```

  - Source IP dengan IP 192.168.0.1
  - Destination IP dengan IP 192.168.0.102
  - Source Port: 53
  - Destination Port: 53478

- Hubungan antara nomor port pada kedua segmen adalah pada request (paket 265) source port adalah port dari host pengirim dan destination port biasanya 53 (port standar untuk DNS pada UDP), pada paket respons (paket 266) source port adalah port 53 (karena ini adalah server DNS yang mengirim respons), dan Destination Port sama dengan Source Port dari paket request (paket 23). Ini menunjukkan bahwa respons diarahkan kembali ke port asal dari pengirim request, untuk menjaga kesinambungan komunikasi.).