

Wireshark 이해

네트워크 프로그래밍

휴먼지능정보공학과
201810776 소재휘



#1 Wireshark capture

Network programming

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
27	0.408483	172.16.24.78	224.0.0.251	MDNS	151	Standard query 0x000f PTR _6EBE3B41._sub._googlecast._tcp.local, "QM" qu...
28	0.513793	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.25.3? Tell 172.16.24.1
29	0.513793	172.16.24.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x5722fb81
30	0.513794	172.16.25.34	172.16.31.255	NBNS	92	Name query NB WPAD<00>
31	0.513794	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.231? Tell 172.16.24.1
32	0.513795	172.16.25.120	224.0.0.251	MDNS	368	Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _compan...
33	0.513795	fe80::1cf2:ced6:6e0...	ff02::fb	MDNS	388	Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _compan...
34	0.513796	SamsungE_cf:25:08	Broadcast	ARP	60	Who has 172.16.24.1? Tell 172.16.25.134
35	0.513796	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.26.147? Tell 172.16.24.1

> Frame 34: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> Ethernet II, Src: SamsungE_cf:25:08 (50:77:05:cf:25:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

```
0000  ff ff ff ff ff 50 77 05 cf 25 08 08 06 00 01  ....Pw  ..%....
0010  08 00 06 04 00 01 50 77 05 cf 25 08 ac 10 19 86  ....Pw  ..%....
0020  00 00 00 00 00 00 ac 10 18 01 00 00 00 00 00  ....
0030  00 00 00 00 00 00 00 00 98 19 a4 0f  ....
```

Packet
List
Window

Packet
Detail
Window

Packet
Bytes
Window



#1 Wireshark capture

Network programming

캡처한 패킷들을 순서대로 보여주는 역할.

캡처된 순서(Number), 캡처된 시간(time), 출발지와 목적지의 주소(Source, Destination), 패킷에 포함되어 있는 주요 프로토콜(Protocol), 패킷의 byte단위 길이(Length), Packet이 내포하는 주요정보(Info)를 확인할 수 있다.

Packet
List
Window

선택된 패킷의 자세한 사항들을 확인할 수 있다.
대표적으로 일련번호를 확인할 수 있다.

Packet
Detail
Window

Packet Detail Window에서 선택한 부분에 해당하는 16진수 데이터를 보여준다.

Packet
Bytes
Window



#2 ARP Packet capture

Network programming

Wireshark packet capture interface showing ARP packets. The packet list shows several ARP requests from various sources to the broadcast address. The packet details pane shows the structure of a selected ARP packet (Frame 34). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
31	0.513794	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.231? Tell 172.16.24.1
34	0.513796	SamsungE_cf:25:08	Broadcast	ARP	60	Who has 172.16.24.1? Tell 172.16.25.134
35	0.513796	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.26.147? Tell 172.16.24.1
43	0.716580	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.153? Tell 172.16.24.1
54	1.126306	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.103? Tell 172.16.24.1
58	1.228646	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.241? Tell 172.16.24.1
63	1.331729	ExtremeN_98:d3:a3	Broadcast	ARP	60	Who has 172.16.24.19? Tell 172.16.24.2
64	1.331729	ExtremeN_98:d3:a3	Broadcast	ARP	60	Who has 172.16.24.18? Tell 172.16.24.2
65	1.433002	Fortinet_eb:64:b2	Broadcast	ARP	60	Who has 172.16.24.94? Tell 172.16.24.1

Frame 34: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Interface id: 0 (\\Device\\NPF_{DB1E3F10-3268-4110-A4D8-EDE55A6C84A5})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 20, 2019 12:55:58.913667000 대한민국 표준시
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1568951758.913667000 seconds
[Time delta from previous captured frame: 0.000001000 seconds]
[Time delta from previous displayed frame: 0.000002000 seconds]
[Time since reference or first frame: 0.513796000 seconds]
Frame Number: 34

0000 ff ff ff ff ff 50 77 05 cf 25 08 08 06 00 01Pw ..%....
0010 08 00 06 04 00 01 50 77 05 cf 25 08 ac 10 19 86Pw ..%....
0020 00 00 00 00 00 ac 10 18 01 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 98 19 a4 0f

다음은 캡처한 패킷 중
ARP 패킷 하나를
선택한 것이다.

ARP는 Network layer에
해당한다.



#2 ARP Packet capture

Network programming

Ethernet II, Src: SamsungE_cf:25:08 (50:77:05:cf:25:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: SamsungE_cf:25:08 (50:77:05:cf:25:08)

다음은 ARP packet의 Ethernet에서의 목적지 주소(DA)와 발신지 주소(SA)이다. ARP에서는 DA와 SA가 존재하지 않는다.

▼ Address Resolution Protocol (request) 25:08)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

ARP 는 3계층에 해당한다. 따라서 2계층의 정보가 담긴 헤더와 3계층의 정보가 담긴 데이터가 인캡슐레이션된다. Hardware type에서 명시한 Ethernet(1)은 2계층(데이터링크 계층)에 해당하는 프로토콜이고 Protocol type에서 명시한 IPv4(0x0800)은 3계층(네트워크 계층)에 해당하는 프로토콜이다.



#2 ARP Packet capture

Network programming

ff ff ff ff ff ff	50 77 05 cf 25 08	08 06	00 01
08 00 06 04 00 01	50 77 05 cf 25 08	ac 10 19 86	
00 00 00 00 00 00	ac 10 18 01	00 00 00 00 00 00	
00 00 00 00 00 00	00 00 98 19 a4 0f		

.....Pw ..%.
.....Pw ..%.
.....
.....

Encapsulation 구조

Wireshark에서는 관찰 불가능. 오류
검사(CRC)

DA	SA	Type (ARP)	ARP Packet	Padding	Trailer
6byte	6byte	2byte	28byte	18byte	4byte

Header

Hardware type(2byte)	Protocol type(2byte)	Hardware size(1byte)	Protocol size(1byte)	Opcode(2 byte)	Sender MAC address(6byte)	Sender IP address(4byte)	Target MAC address(6byte)	Target IP address(4byte)
-------------------------	-------------------------	-------------------------	-------------------------	-------------------	------------------------------	-----------------------------	------------------------------	-----------------------------



#3 DNS Packet capture

Network programming

▼ Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

> Interface id: 0 (\Device\NPF_{DB1E3F10-3268-4110-A4D8-EDE55A6C84A5})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 24, 2019 17:21:57.660481000 대한민국 표준시

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1569313317.660481000 seconds

[Time delta from previous captured frame: 0.212606000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 8.610141000 seconds]

Frame Number: 317

Frame Length: 83 bytes (664 bits)

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	·[·d· ·+····E·
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	·E8···· 1····
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e····5·1 6a3d···
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e	·····c tldl·win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te·com··
0050	01 00 01	···

다음은 캡처한 패킷
중 DNS 패킷 하나를
선택한 것이다.

DNS는 응용 계층에
해당한다.



#3 DNS Packet capture

Network programming

- ✓ Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
 - > Destination: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
 - > Source: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
 - Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- > User Datagram Protocol, Src Port: 53210, Dst Port: 53
- > Domain Name System (query)

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	·[·d· ·+···E·
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	·E8· · · 1· · · ·
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e· · · · 5· 1 6a3d· · ·
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e	· · · · · c tldl·win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te·com· ·
0050	01 00 01	· · ·

다음은 Header에 해당하는 2계층(데이터링크 계층)에 해당하는 Ethernet II 프로토콜과 3계층(네트워크 계층)에 해당하는 IPv4(0x0800) 프로토콜을 확인할 수 있다.

또한 DA에 해당하는 Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)와 SA에 해당하는 IntelCor_2b:bb:b4(a0:c5:89:2b:bb:b4)를 확인할 수 있다.

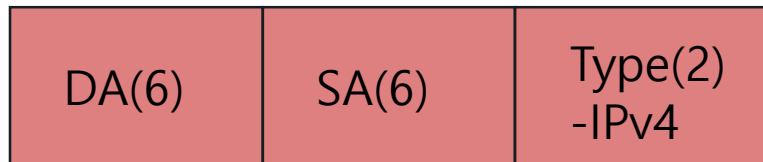


#3 DNS Packet capture

Network programming

- ✓ Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
 - > Destination: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
 - > Source: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
 - Type: IPv4 (0x0800)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- > User Datagram Protocol, Src Port: 53210, Dst Port: 53
- > Domain Name System (query)

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	·[··d··· ·+····E·
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	·E8····· 1·····
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e····5·1 6a3d····
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e	·······c tldl·win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te·com··
0050	01 00 01	···



다음은 2계층 Ethernet II header의 layer 구조이다.
괄호안 숫자는 byte를 의미한다.



#3 DNS Packet capture

Network programming

```
> Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
> Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
▼ Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 69
    Identification: 0x38e8 (14568)   Header checksum: 0x3116 [validation disabled]
    Flags: 0x0000                  [Header checksum status: Unverified]
    Time to live: 128               Source: 172.16.27.27
    Protocol: UDP (17)              Destination: 164.124.101.2

0000  08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00  .[.d...+...E.
0010  00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c  .E8....1.....
0020  65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01  e....5.1 6a3d...
0030  00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e  ....c tldlwin
0040  64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00  dowsupda te.com..
0050  01 00 01  ...
```

다음에서는 3계층(네트워크 계층)에 해당하는 IPv4 프로토콜과 4계층에 속하는 UDP 프로토콜을 확인할 수 있다. IPv4의 SA와 DA는 각각 172.16.27.27와 164.124.101.2이다.



#3 DNS Packet capture

Network programming

```
> Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
> Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
> Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 69
    Identification: 0x38e8 (14568)
    Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x3116 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.27.27
    Destination: 164.124.101.2
```

```
0000 08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00 .[.d... +....E.
0010 00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c .E8.....1.....|
0020 65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01 e.5.1 6a3d...
0030 00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e .....c tld1.win
0040 64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00 dowsupda te.com..
0050 01 00 01 ...
```

Version(1)	Differentiated Services Field(1)	Total length(2)	Identification(2)	Flags(2)	Time to live(1)
Protocol(1) -UDP	Header checksum(2)	Source(4)	Destination(4)	다음은 3계층 IPv4의 header의 layer 구조이다. 괄호안 숫자는 byte를 의미한다.	



#3 DNS Packet capture

Network programming

- > Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
- > Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- > User Datagram Protocol, Src Port: 53210, Dst Port: 53
 - Source Port: 53210
 - Destination Port: 53
 - Length: 49
 - Checksum: 0x3661 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 94]
 - > [Timestamps]

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	·[·d· ·+···E·
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	·E8· · · · 1· · · ·
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e· · · · 5· 1 6a3d· · ·
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e	· · · · · · · c tldl·win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te·com· ·
0050	01 00 01	· · ·

다음에서는 4계층(전송 계층)의 UDP 프로토콜을 확인할 수 있다.
출발지인 Src Port의 번호는 53210, 도착지인 Dst Port의 번호는 53이다.



#3 DNS Packet capture

Network programming

- > Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
- > Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- ▼ User Datagram Protocol, Src Port: 53210, Dst Port: 53
 - Source Port: 53210
 - Destination Port: 53
 - Length: 49
 - Checksum: 0x3661 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 94]
 - > [Timestamps]

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	[. . . d + E .
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	. E8 1
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e 5 . 1 6a3d
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e c tld1 . win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te . com . .
0050	01 00 01	. . .

Source port(2)	Destination port(2)	Length(2)	Checksum(2)
----------------	---------------------	-----------	-------------

다음은 4계층 UDP header의 layer 구조이다.
괄호안 숫자는 byte를 의미한다.



#3 DNS Packet capture

Network programming

- > Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
- > Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- > User Datagram Protocol, Src Port: 53210, Dst Port: 53
- ✓ Domain Name System (query)
 - Transaction ID: 0x3364
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	. [. . d + E .
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	. E8 1
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e 5 . 1 6 a 3 d
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e c t l d 1 . w i n
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	d o w s u p d a t e . c o m . .
0050	01 00 01	. . .

마지막으로 응용 계층에서의 DNS 프로토콜을 확인할 수 있다.



#3 DNS Packet capture

Network programming

- > Frame 317: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
- > Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
- > Internet Protocol Version 4, Src: 172.16.27.27, Dst: 164.124.101.2
- > User Datagram Protocol, Src Port: 53210, Dst Port: 53
- ✓ Domain Name System (query)
 - Transaction ID: 0x3364
 - > Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0

0000	08 5b 0e eb 64 b2 a0 c5 89 2b bb b4 08 00 45 00	·[··d··· ·+····E·
0010	00 45 38 e8 00 00 80 11 31 16 ac 10 1b 1b a4 7c	·E8····· 1·····
0020	65 02 cf da 00 35 00 31 36 61 33 64 01 00 00 01	e····5·1 6a3d····
0030	00 00 00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e	·······c tld1·win
0040	64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00	dowsupda te·com··
0050	01 00 01	···

다음은 5계층 DNS의 layer 구조이다.
괄호안 숫자는 byte를 의미한다.

Transaction ID(2)	Flags(2)	Question(2)	Answer RRs(2)	Authority RRs(2)	Additional RRs(2)	Queries(29)
-------------------	----------	-------------	---------------	------------------	-------------------	-------------



#3 DNS Packet capture

Network programming

DNS의 계층별 프로토콜을 정리해 보면 다음과 같다.

2계층(Data link layer) : Ethernet II

3계층(Network layer) : IPv4

4계층(Transport layer) : UDP

5계층(Application layer) : DNS



#3 DNS Packet capture

Network programming

08 5b 0e eb 64 b2	a0 c5 89 2b bb b4	08 00 45 00
00 45 38 e8 00 00	80 11 31 16 ac 10 1b 1b	a4 7c
65 02 cf da 00 35 00 31	36 61 33 64 01 00 00 01	
00 00 00 00 05 63 74 6c 64 6c 0d 77 69 6e		
64 6f 77 73 75 70 64 61 74 65 03 63 6f 6d 00 00		
01 00 01		

```
·[...d... ..+....E·  
·E8..... 1.....|  
e.....5·1 6a3d....  
.....c tld1·win  
dowsupda te·com··  
...
```

이를 바탕으로 DNS 패킷의 레이어 구조를 살펴보겠다. 다음은 DNS의 패킷의 데이터를 색으로 레이어를 구분하고 필드별로 나눈 것이다. 이 구조를 뒤 슬라이드에서 각 레이어 별 구조를 자세히 살펴보겠다.



#3 DNS Packet capture

Network programming

괄호안 숫자는 byte를 의미한다.

Datalink Ethernet II	Network IPv4	Transport UDP	Application DNS
-------------------------	-----------------	------------------	--------------------

DA(6)	SA(6)	Type(2) -IPv4	Version(1)	Differentiated Services Field(1)	Total length(2)
Identification(2)	Flags(2)	Time to live(1)	Protocol(1) -UDP	Header checksum(2)	Source(4)
Destination(4)	Source port(2)	Destination port(2)	Length(2)	Checksum(2)	Transaction ID(2)
Flags(2)	Question(2)	Answer RRs(2)	Authority RRs(2)	Additional RRs(2)	Queries(29)

다음은 각 계층 별 Field를 Encapsulation한 layer 구조이다. 이 DNS packet은 총 데이터링크 계층에서 14byte, 네트워크 계층에서 20byte, 전송 계층에서 8byte, 응용 계층에서 41byte가 인캡슐레이션 되어 있는 구조이다.