

# Wireshark를 이용한 DNS 패킷 분석

---

24.03.29

### 1. 실습 환경

- VMware workstation Pro - Ubuntu 20.04.0 환경에서 진행하였습니다.
- Machine address : 192.168.111.100
- Filter : udp.port == 53

### 2. 진행 과정

- (1) nslookup 명령어로 진입
- (2) www.cnu.ac.kr를 입력하여 IP 주소 알아내기(Standard Query)
- (3) (2)에서 알아낸 IP 주소를 입력하여 domain name 알아내기(Inverse Query)
- (4) 존재하지 않는 임의의 name을 입력하여 결과 확인하기

### 3. 결과

```
root@ub1-virtual-machine: ~/바탕화면
root@ub1-virtual-machine:~/바탕화면# nslookup 1
> www.cnu.ac.kr
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.cnu.ac.kr
Address: 168.188.253.130
> 168.188.253.130
130.253.188.168.in-addr.arpa    name = cnu.ac.kr.
130.253.188.168.in-addr.arpa    name = www.cnu.ac.kr.

Authoritative answers can be found from:
> not.available
Server:      127.0.0.53
Address:     127.0.0.53#53

** server can't find not.available: NXDOMAIN
>
```

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.111.100	192.168.111.2	DNS	84	Standard query 0x3442 A www.cnu.ac.kr OPT
2 0.011894	192.168.111.2	192.168.111.100	DNS	100	Standard query response 0x3442 A www.cnu.ac.kr A 168.188.253.130 OPT
3 0.012382	192.168.111.100	192.168.111.2	DNS	84	Standard query 0x5a03 AAAA www.cnu.ac.kr OPT
4 0.022234	192.168.111.2	192.168.111.100	DNS	134	Standard query response 0x5a03 AAAA www.cnu.ac.kr SOA baekma.cnu.ac.kr OPT
7 10.080175	192.168.111.100	192.168.111.2	DNS	99	Standard query 0x4655 PTR 130.253.188.168.in-addr.arpa OPT
8 10.095856	192.168.111.2	192.168.111.100	DNS	140	Standard query response 0x4655 PTR 130.253.188.168.in-addr.arpa PTR cnu.ac.kr PTR www.cnu.ac.kr OPT
11 27.801854	192.168.111.100	192.168.111.2	DNS	84	Standard query 0x97a4 A not.available OPT
12 27.811208	192.168.111.2	192.168.111.100	DNS	159	Standard query response 0x97a4 No such name A not.available SOA a.root-servers.net OPT
13 27.811406	192.168.111.100	192.168.111.2	DNS	73	Standard query 0x97a4 A not.available
14 29.817414	192.168.111.2	192.168.111.100	DNS	148	Standard query response 0x97a4 No such name A not.available SOA a.root-servers.net

● No. 1~4 : www.cnu.ac.kr 물어보기

```

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{B30F9CEC-0FAC-408D-8000-000000000000}
> Ethernet II, Src: VMware_b5:3a:45 (00:0c:29:b5:3a:45), Dst: VMware_ee:ac:87 (00:50:56:ee:ac:87)
> Internet Protocol Version 4, Src: 192.168.111.100 (192.168.111.100), Dst: 192.168.111.2 (192.168.111.2)
> User Datagram Protocol, Src Port: 47662, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x3442
  v 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: 1
  v Queries
    > www.cnu.ac.kr: type A, class IN
  Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_{B30F9CEC-0FAC-408D-8000-000000000000}
  Ethernet II, Src: VMware_ee:ac:87 (00:50:56:ee:ac:87), Dst: VMware_b5:3a:45 (00:0c:29:b5:3a:45)
  Internet Protocol Version 4, Src: 192.168.111.2 (192.168.111.2), Dst: 192.168.111.100 (192.168.111.100)
  User Datagram Protocol, Src Port: 53, Dst Port: 47662
  Domain Name System (response)
    Transaction ID: 0x3442
    v Flags: 0x8180 Standard query response, No error
      1... .. = Response: Message is a response
      .000 0... .. = Opcode: Standard query (0)
      .... 0... .. = Authoritative: Server is not an authority for domain
      .... 0... .. = Truncated: Message is not truncated
      .... 1... .. = Recursion desired: Do query recursively
      .... 1... .. = Recursion available: Server can do recursive queries
      .... 0... .. = Z: reserved (0)
      .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... 0... .. = Non-authenticated data: Unacceptable
      .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
    v Queries
      > www.cnu.ac.kr: type A, class IN
    v Answers
      > www.cnu.ac.kr: type A, class IN, addr 168.188.253.130

```

1번 프레임

- Standard Query, 해당 Domain name의 IP 주소를 물어본다.
- QR = 0 (Query), RD = 0 (Recursion desired), Type : A (IPv4), Class : IN (Internet)

2번 프레임

- Standard Query Response, 해당 Domain name의 IP 주소를 반환한다.
- QR = 1 (Response), RD = 0 (Do query recursively), rcode = 0 (No error)
- Answer 부분에 168.188.253.130을 반환했다.

3~4번 프레임: Recursive Query로 보낸 Frame 들이다. 내용은 Type이 AAAA (IPv6)인 것을 제외하면 같다.

## ● No. 7~8 : Inverse Query

Frame 7: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF\_{B30F9CEC-0F8A-Ethernet II, Src: VMware\_b5:3a:45 (00:0c:29:b5:3a:45), Dst: VMware\_ee:ac:87 (00:50:56:ee:ac:87)  
Internet Protocol Version 4, Src: 192.168.111.100 (192.168.111.100), Dst: 192.168.111.2 (192.168.111.2)  
User Datagram Protocol, Src Port: 57274, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x4655

▼ 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: 1

▼ Queries

> 130.253.188.168.in-addr.arpa: type PTR, class IN

Frame 8: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface \Device\NPF\_{B30F9CEC-0F8A-Ethernet II, Src: VMware\_ee:ac:87 (00:50:56:ee:ac:87), Dst: VMware\_b5:3a:45 (00:0c:29:b5:3a:45)

Internet Protocol Version 4, Src: 192.168.111.2 (192.168.111.2), Dst: 192.168.111.100 (192.168.111.100)

User Datagram Protocol, Src Port: 53, Dst Port: 57274

Domain Name System (response)

Transaction ID: 0x4655

▼ Flags: 0x8180 Standard query response, No error

1... .. = Response: Message is a response  
.000 0... .. = Opcode: Standard query (0)  
.... ..0... .. = Authoritative: Server is not an authority for domain  
.... ..0. .... = Truncated: Message is not truncated  
.... ..1 .... = Recursion desired: Do query recursively  
.... ..1... .. = Recursion available: Server can do recursive queries  
.... ..0... .. = Z: reserved (0)  
.... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server  
.... ..0 .... = Non-authenticated data: Unacceptable  
.... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 1

▼ Queries

> 130.253.188.168.in-addr.arpa: type PTR, class IN

▼ Answers

> 130.253.188.168.in-addr.arpa: type PTR, class IN, cnu.ac.kr

> 130.253.188.168.in-addr.arpa: type PTR, class IN, www.cnu.ac.kr

## 7번 프레임

- Question records 부분에서 130.253.188.168.in-addr.arpa를 통해 Domain name 질문
- QR = 0 (Query), Type : PTR (Pointer), Class : IN (Internet)

## 8번 프레임

- 7번 프레임에서 질의했던 IP 주소에 대한 Domain name을 반환한다.
- QR = 1 (Response), RD = 0 (Do query recursively), rcode = 0 (No error)
- Answer 부분에 www.cnu.ac.kr을 반환했다.



## ● No. 11~14 : Invalid Domain Name

Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF\_{B30F9CEC- Ethernet II, Src: VMware\_b5:3a:45 (00:0c:29:b5:3a:45), Dst: VMware\_ee:ac:87 (00:50:56:ee:ac:87)  
Internet Protocol Version 4, Src: 192.168.111.100 (192.168.111.100), Dst: 192.168.111.2 (192.168.111.2)  
User Datagram Protocol, Src Port: 51041, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x97a4

▼ 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: 1

▼ Queries

> not.available: type A, class IN

Frame 12: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface \Device\NPF\_{B30F9CEC- Ethernet II, Src: VMware\_ee:ac:87 (00:50:56:ee:ac:87), Dst: VMware\_b5:3a:45 (00:0c:29:b5:3a:45)

Internet Protocol Version 4, Src: 192.168.111.2 (192.168.111.2), Dst: 192.168.111.100 (192.168.111.100)

User Datagram Protocol, Src Port: 53, Dst Port: 51041

Domain Name System (response)

Transaction ID: 0x97a4

▼ Flags: 0x8183 Standard query response, No such name

1... .. = Response: Message is a response  
.000 0... .. = Opcode: Standard query (0)  
... ..0. .... = Authoritative: Server is not an authority for domain  
... ..0. .... = Truncated: Message is not truncated  
... ..1 .... = Recursion desired: Do query recursively  
... ..1 .... = Recursion available: Server can do recursive queries  
... ..0. .... = Z: reserved (0)  
... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server  
... ..0 .... = Non-authenticated data: Unacceptable  
... ..0011 = Reply code: No such name (3)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

▼ Queries

> not.available: type A, class IN

▼ Authoritative nameservers

> <Root>: type SOA, class IN, mname a.root-servers.net

▼ Additional records

> <Root>: type OPT

[\[Request In: 11\]](#)

[Time: 0.009354000 seconds]

### 11번 프레임

- Error를 받기 위해 존재하지 않는 Domain name을 Query한다.
- Query: not.available

### 12번 프레임

- Flag, Rcode에서 Error code를 반환한다.
- Rcode : 0011 (3) : No such name