https://gleaming.notion.site/Chapter-03-Whois-DNS-840da852e70b404e8ecd2e03ce61fdef

실습환경

가상화 도구 : VMware Workstation 16 Player

운영체제 : Windows Server 2022 ISO

네트워크 시뮬레이터 : Cisco Packet Tracer

이번 실습은 네트워크 통신에서 핵심적인 역할을 수행하는 도메인 이름 해석(DNS) 관련된 여러 기술들을 직접 실습해보고,
이를 통해 도메인이 어떻게 작동하고, 네트워크 흐름이 어떻게 구성되는지를 이해하는 것이 목표임

실습에서는 먼저 Whois 서버를 활용해 특정 도메인의 등록자, 등록기관 등의 정보를 조회해보고,host 파일을 직접 수정하여 도메인 이름 해석을 수동으로 처리하는 방식도 실습하였음
또한, 의도적으로 잘못된 주소를 등록하여 사이트 접속을 차단하는 방법도 테스트해보며,이름 해석이 어떻게 동작하고, 어떤 보안적 활용이 가능한지도 함께 다룸

이후에는 Windows Server 2022 기반의 DNS 서버 구성, 그리고 Packet Tracer 를 이용한 가상 네트워크 구성 실습을 통해 웹서버, DHCP 서버, DNS 서버가 각각 어떤 역할을 하며 어떻게 동작하는지를 확인하며 이해함

마지막으로, tracert 명령어를 이용한 네트워크 경로 추적 실습을 통해
데이터가 인터넷상에서 어떤 라우터들을 거쳐 최종 목적지에 도달하는지를 시각적으로 확인함으로써,
실제 네트워크 동작 과정을 깊이 있게 파악할 수 있었음

1.Who is 서버를 이용해 정보 획득

Who is란? 도메인 이름의 등록자 정보를 조회할 수 있는 웹사이트

- 특정 도메인의 등록자, 등록일,만료일, 네임서버 등의 정보 조회 가능
- 도메인이 어떤 등록기관을 통해 등록되었는지 확인

You searched for: **json**

Point of Contact	
Name	Json
Handle	JSON-ARIN
Company	First State InTeL
Street	4860 Sandtown Road.
City	Felton
State/Province	DE
Postal Code	19943
Country	US
Registration Date	2023-09-30
Last Updated	2023-09-30
Comments	
Phone	+1-302-345-2203 (Office) +1-302-345-2203 (Mobile)
Email	Firststateintelcorp@gmail.com
RESTful Link	https://whois.arin.net/rest/poc/JSON-ARIN
See Also	Related organizations.

이름이 json인 사람이 등록한 사이트를 검색한 결과

Customer	
Name	Amazon
Handle	C05179991
Street	410 Terry Ave N.
City	Seattle
State/Province	WA
Postal Code	98109
Country	US
Registration Date	2014-07-22
Last Updated	2014-07-22
Comments	
RESTful Link	https://whois.arin.net/rest/customer/C05179991

Network Resources	
CYRUSONE-AMAZON-WAN-BLK (NET-216-117-72-176-1)	216.117.72.176 - 216.117.72.191

See Also	Upstream network's resource POC records.
See Also	Upstream organization's POC records.

아마존을 검색한 결과

216.117.72.176~216.117.72.191이 Amazon 소유라는 걸 보여줌

2. host 파일을 이용해 이름 해석하기

```
C:\Users\종이장미>ping www.google.com

Ping www.google.com [172.217.161.196] 32바이트 데이터 사용:
172.217.161.196의 응답: 바이트=32 시간=39ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=37ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=37ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=37ms TTL=57

172.217.161.196에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 37ms, 최대 = 39ms, 평균 = 37ms
```

한빛 사이트가 접속이 되지않아 구글로 대체

```
파일    편집    보기
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1       localhost
#      ::1             localhost

172.217.161.196          www.google.com        google
```

```
C:\Users\종이장미>ping google

Ping www.google.com [172.217.161.196] 32바이트 데이터 사용:
172.217.161.196의 응답: 바이트=32 시간=38ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=37ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=40ms TTL=57
172.217.161.196의 응답: 바이트=32 시간=37ms TTL=57

172.217.161.196에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 37ms, 최대 = 40ms, 평균 = 38ms

C:\Users\종이장미>
```

hosts파일을 수정하여 특정 도메인을 지정한 IP주소 연결시킴

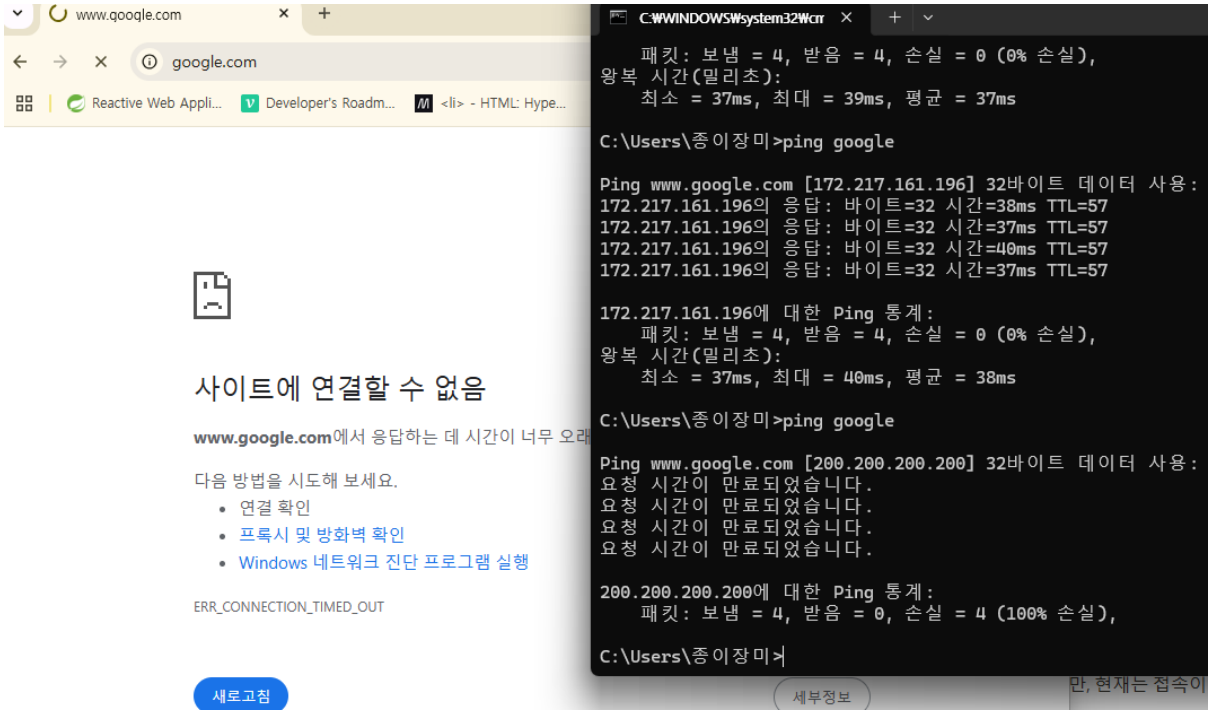
DNS를 서버에 묻기전에 매핑을 먼저시킴

google을 요청하면 172.217.161.196 으로 연결하라는 의미임

그래서 ping명령어가 google을 DNS에 묻지 않고 host파일에 지정한 IP로 바로 연결한 것임

3. 잘못된 주소를 등록하여 사이트 접속 차단

```
# For example:
#
#      102.54.94.97     rhino.acme.com          # source ser
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1       localhost
#      ::1             localhost

200.200.200.200         www.google.com          google
```



요청이 만료되었다라 뜨고 구글이 접속되어지지 않음

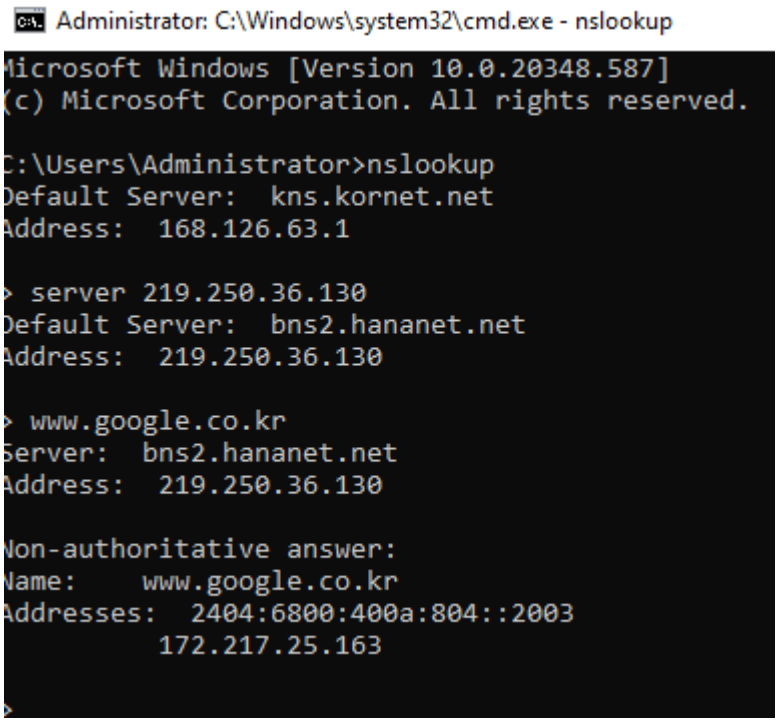
이제 접속이 되어지지 않음

hosts 파일은 IP주소에 대응되는 도메인 이름을 저장 해놓은 파일

도메인을 입력하면 hosts파일에 있는지 확인해보고 없으면 DNS서버에 묻는 식으로 작동하기 때문에 사이트가 막힌 것

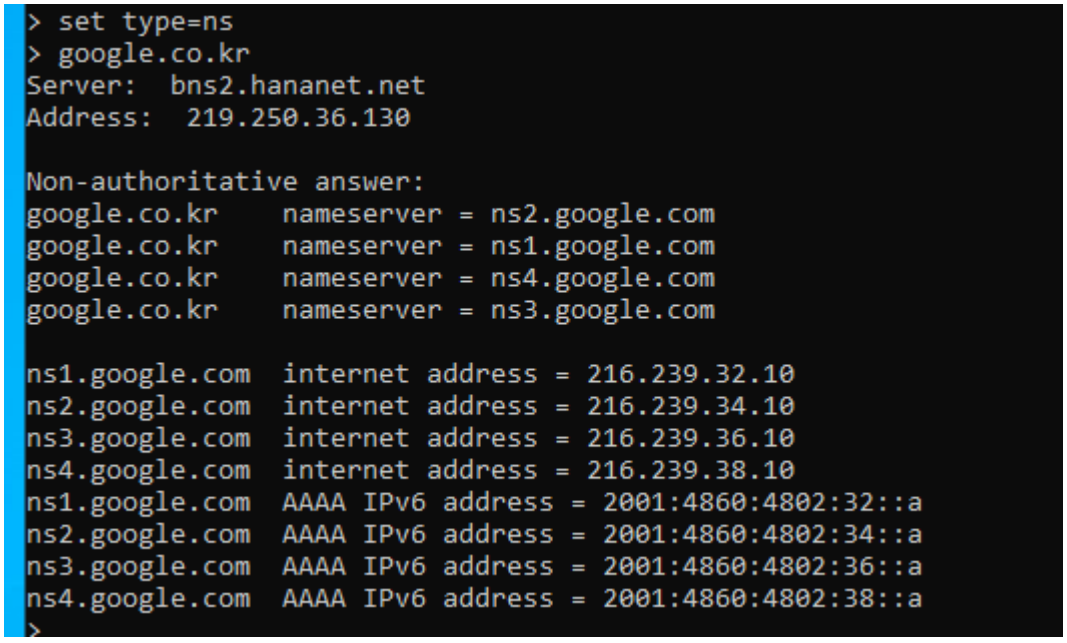
google.com 을 강제로 매핑시킨것임

4. DNS 서버 검색 정보 수집



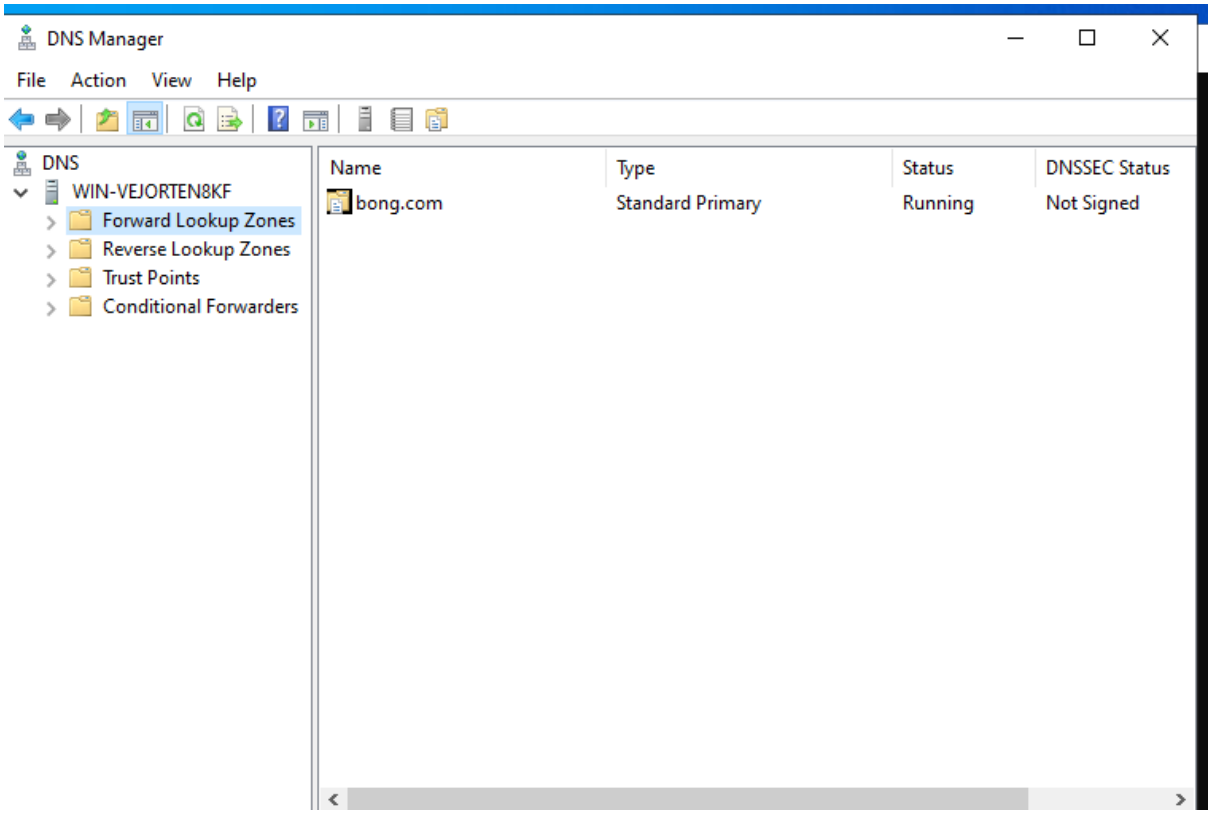
DNS 조회에 사용할 서버를 새로 지정함

기존의 DNS가 아닌 219.25..36.130 서버에서 직접 질의 한다는 말임

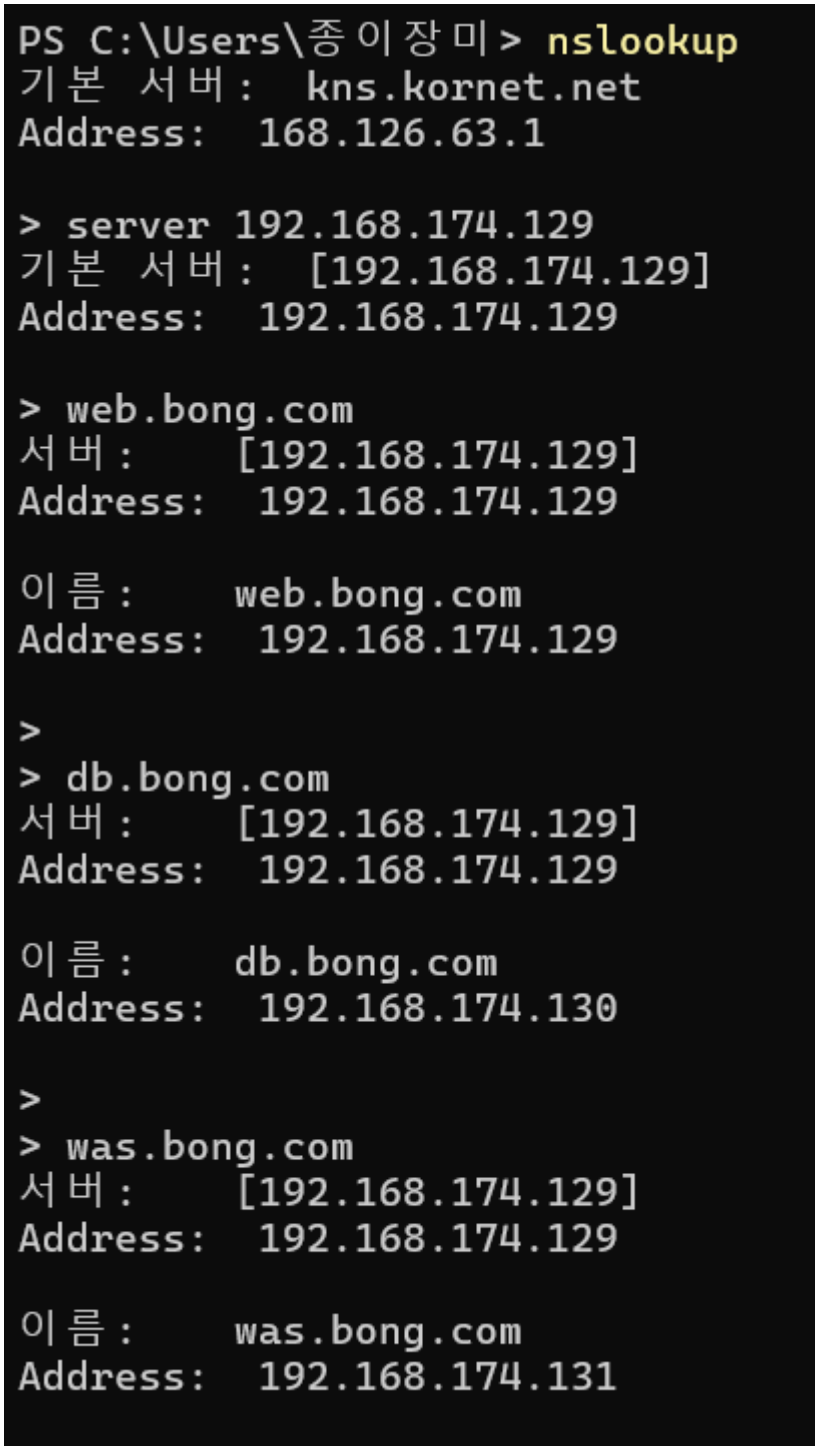


질의 유형을 ns로 바꿈, ns 레코드를 조회하여 등록된 네임서버와 IP주소를 확인

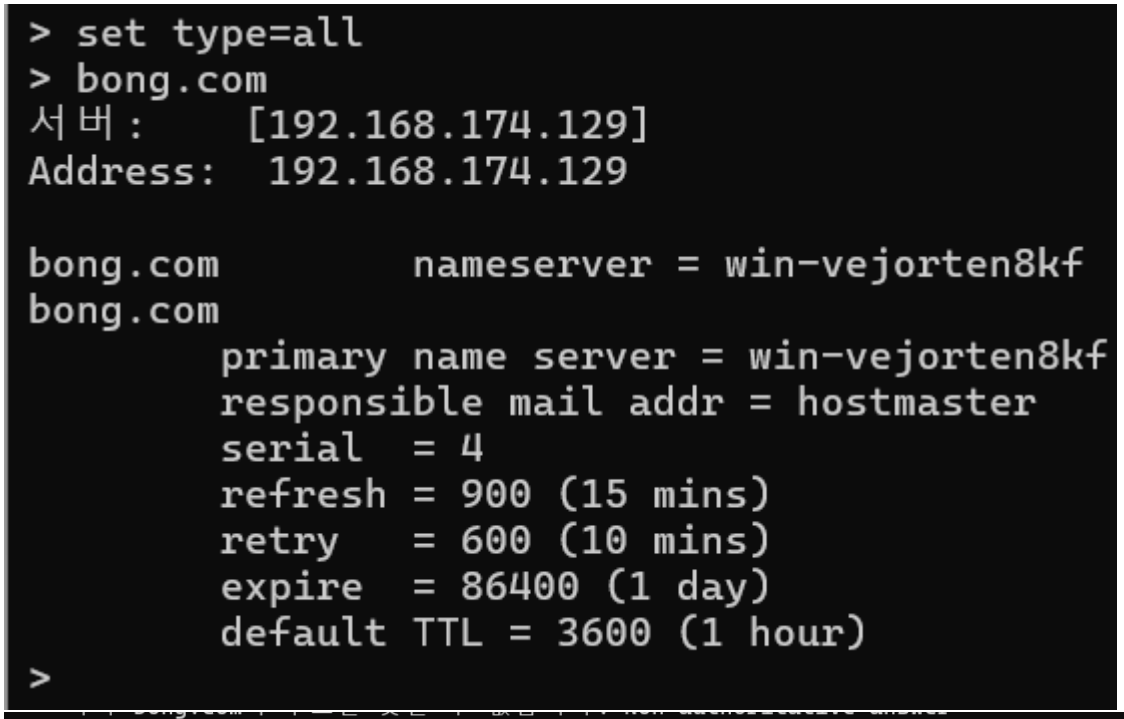
```
> set type=all
> google.co.kr
Server:  bns2.hananet.net
Address:  219.250.36.130

Non-authoritative answer:
google.co.kr    MX preference = 0, mail exchanger = smtp.google.c
google.co.kr    text =

        "v=spf1 -all"
google.co.kr
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 740276574
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
google.co.kr    AAAA IPv6 address = 2404:6800:4004:801::2003
google.co.kr    internet address = 172.217.26.227
google.co.kr    nameserver = ns4.google.com
google.co.kr    nameserver = ns2.google.com
google.co.kr    nameserver = ns1.google.com
google.co.kr    nameserver = ns3.google.com
google.co.kr    ??? unknown type 257 ???
>
```

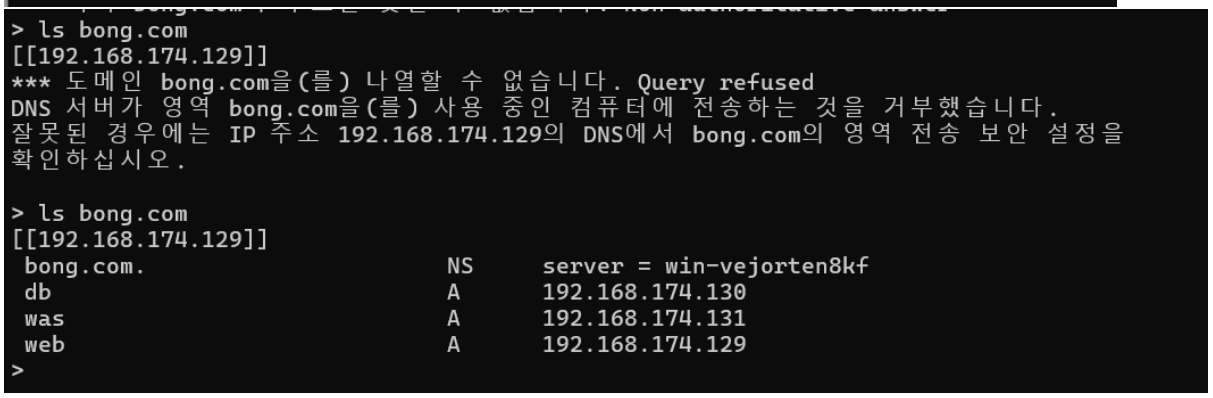


로컬 DNS 설정 도메인 이름과 IP주소를 매핑하는 DNS존을 관리하는것임



위에 사진대로 설정한 DNS로 매핑이 성공됨



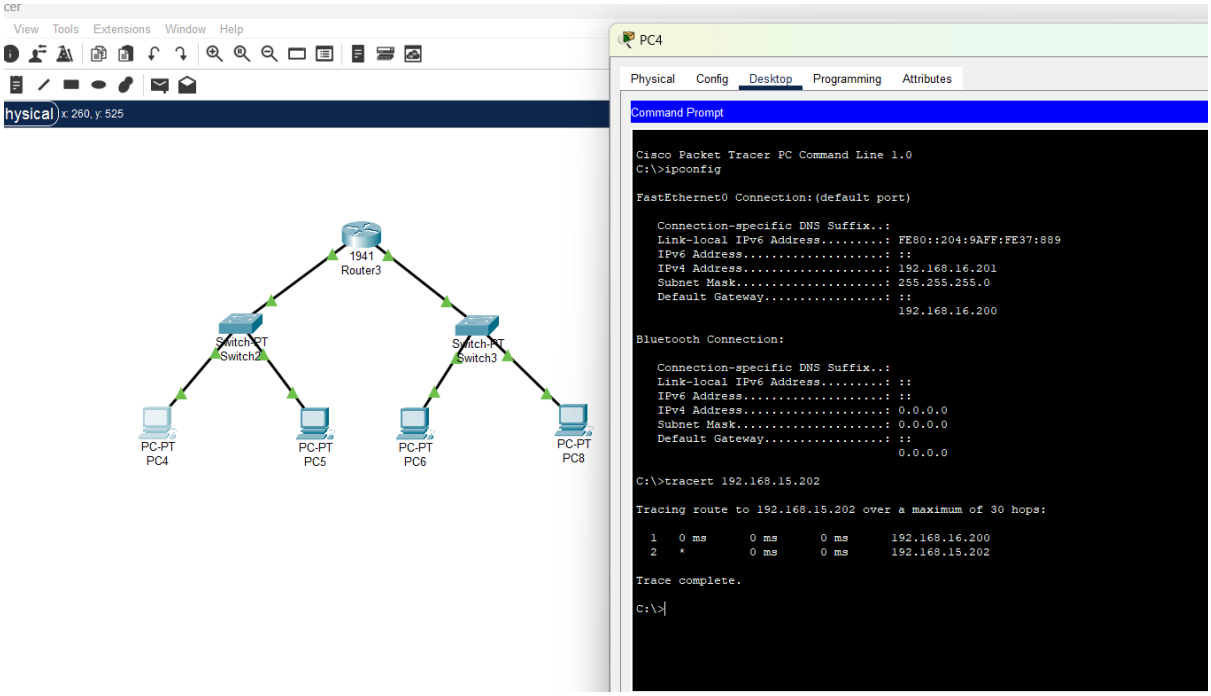


처음에 레코드를 확인 할려했는데 보안 문제로 거부가 난 상황

이유는 zone transfer 이 허용이 되지 않았기 때문 수정을 완료 후 다시 레코드를 검색해보니

모든 레코드를 볼 수 있음 DNS 레코드를 외부에서 조회를 할려고 하면 필수적인 부분을 한 것임

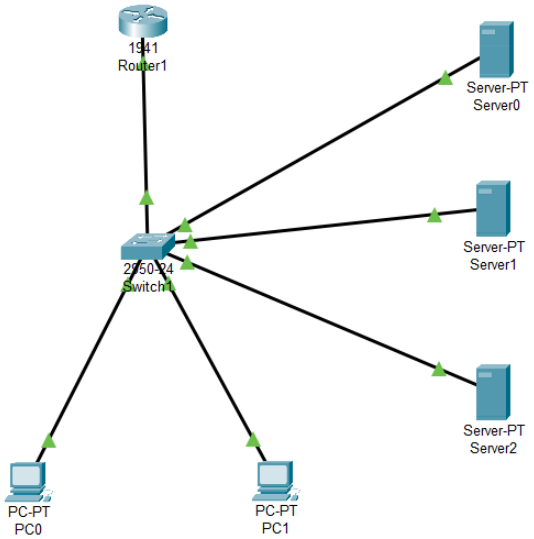
5. 패킷 트레이서를 이용해 네트워크 설정



라우터가 양쪽 서브넷을 제대로 라우팅을 하고 있음

IP,게이트웨이,서브넷,라우팅 전부 정상이 연결이 되었음

6.웹 DHCP, DNS서버 동작 원리 이해

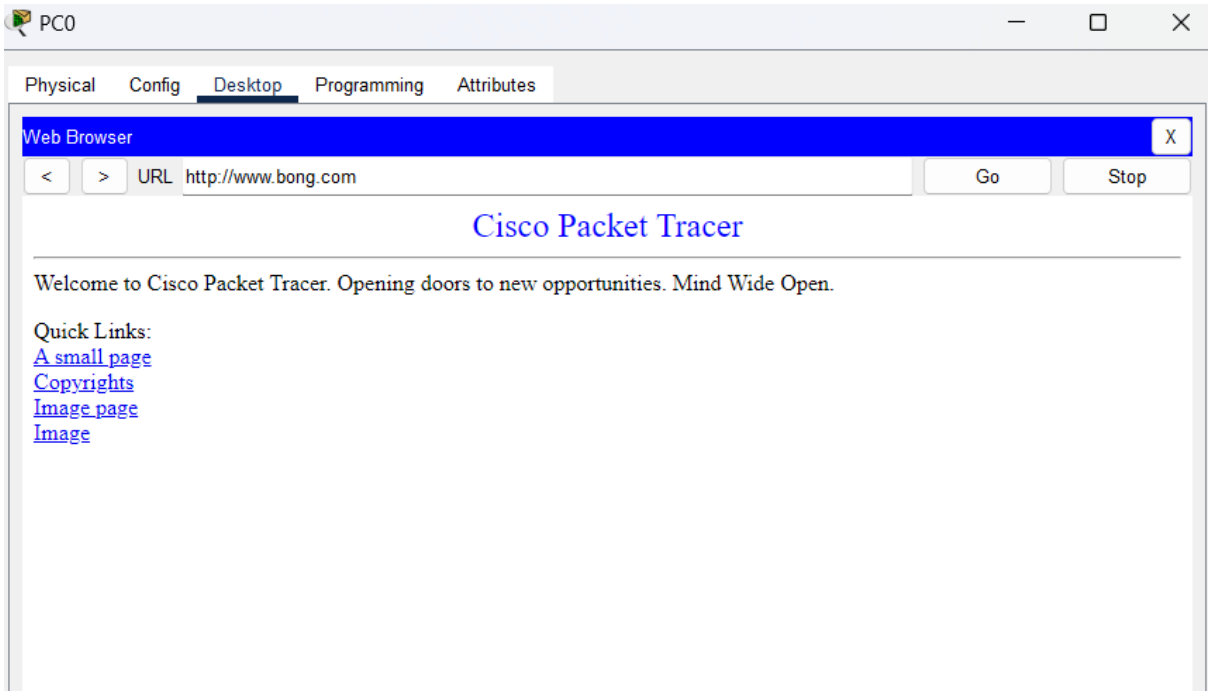


서버0 : DHCP로 설정, 클라가 네트워크에 접속할 때 IP주소를 자동으로 할당해주는 역할
IP범위, 서브넷 마스크, 게이트웨이, DNS서버 주소를 같이 설정하였음
DHCP 서버가 IP, 서브넷 마스크, 게이트웨이,DNS정보를 자동으로 할당하여 PC는 아무설정 없이 바로 네트워크 사용 가능함

서버1 : DNS서버 설정 레코드를 등록하여 특정 도메인 이름이 어떤 IP주소인지 기록함
www.bong.com = 192.168.16.7

서버2 : Web Server로 설정, 웹 페이지 파일을 저장하고 있다 브라우저가 요청하면 그 파일들은 HTTP프로토콜을 통해 전송해주는 역할임

흐름 : PC -> DHCP 요청 -> IP할당 받음
PC – DNS(www.bong.com) -> IP응답
PC -> 웹 서버 접속 (192.168.16.7) ->화면을 띄움



웹 페이지의 주인? : 서버 2 의 웹페이지임 index.html 이 저장된 서버

pc 는 DHCP 한테 IP 주소를 요청하고 DNS 서버 주소를 자동으로 할당받음

DNS 서버에 설정된 레코드(도메인 이름)을 받고 웹서버의 IP 를 알아냄

브라우저가 IP 주소로 변환된 곳으로 접속을 시도 웹서버가 index.html 로 응답하여 페이지를 보여줌

7. 네트워크 경로 추적

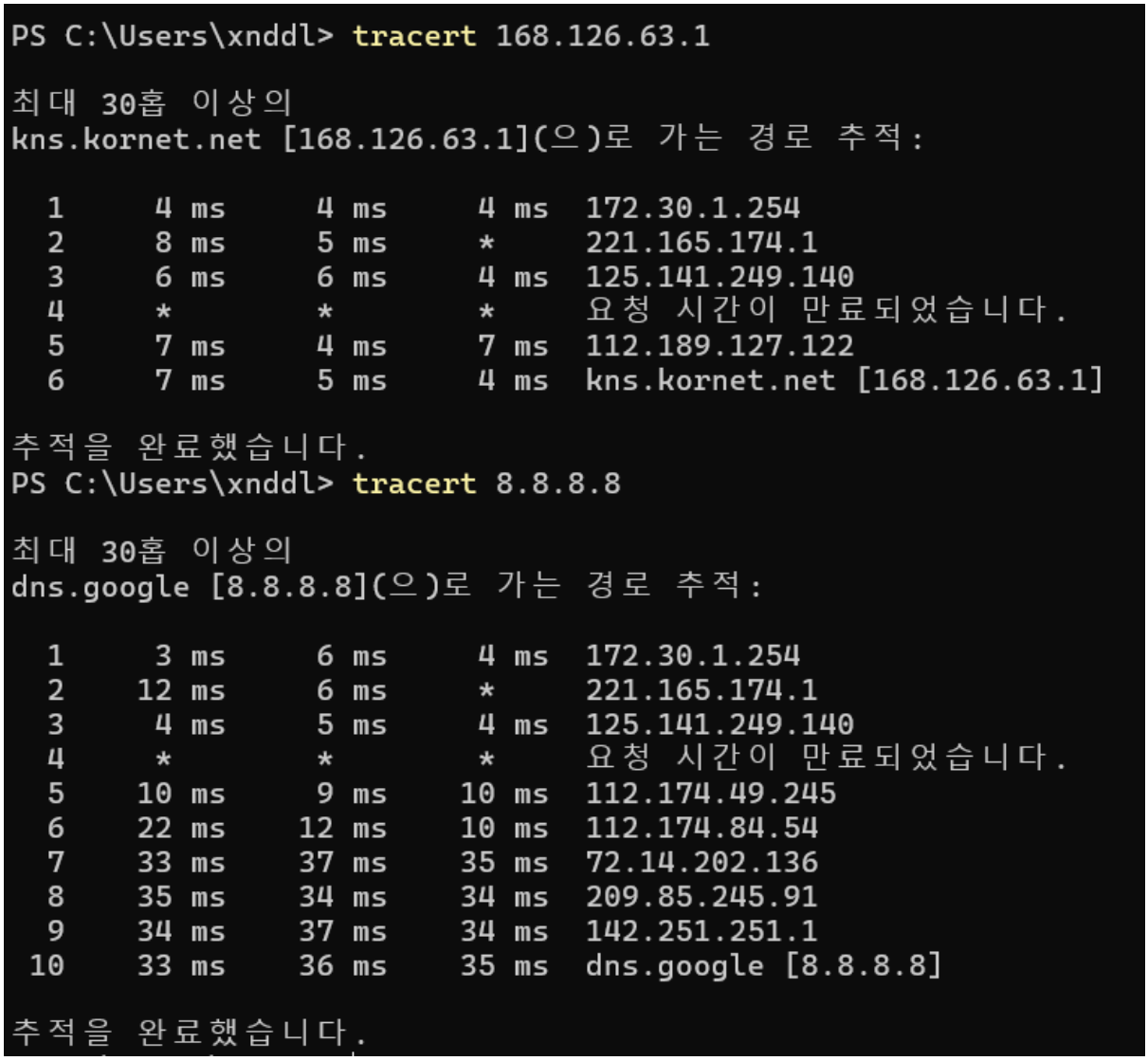
```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.16.6

Tracing route to 192.168.16.6 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.16.6

Trace complete.
```

PC0 에서 192.168.16.6(DNS 서버)까지 패킷이 어떤 경로를 통해 가는지 확인을 한 것임

첫번째 줄 : 목적지 IP 192.168.16.6 까지 바로 도착했다는 말임

두번째 줄 : 0~1ms 지연시간을 나타냄 네트워크가 가깝고 빠르다는 의미임. 같은 LAN 을 씀

Trace complete : 경로 추적이 성공적으로 끝났다는 의미



패킷이 목적지 IP 까지 도달하는 경로를 추적함

인터넷 진흥원

내부 네트워크에서 -> ISP -> KISA 로 가는 백본망 중 하나 -> 최종 목적지 IP