네트워크 보안 과제2

Whois와 DNS조사, IP주소 추적

202246109
김기현
2025년 3월 27일

실습환경

사용 소프트웨어

- VMware workstation 17 Player (WIndows 11에서 실행)
- Cisco Packet Tracer(네트워크 시뮬레이터)

실습 환경

Client: Windows10 (VMware)

DNS Server: Window Server 2022 (VMware)

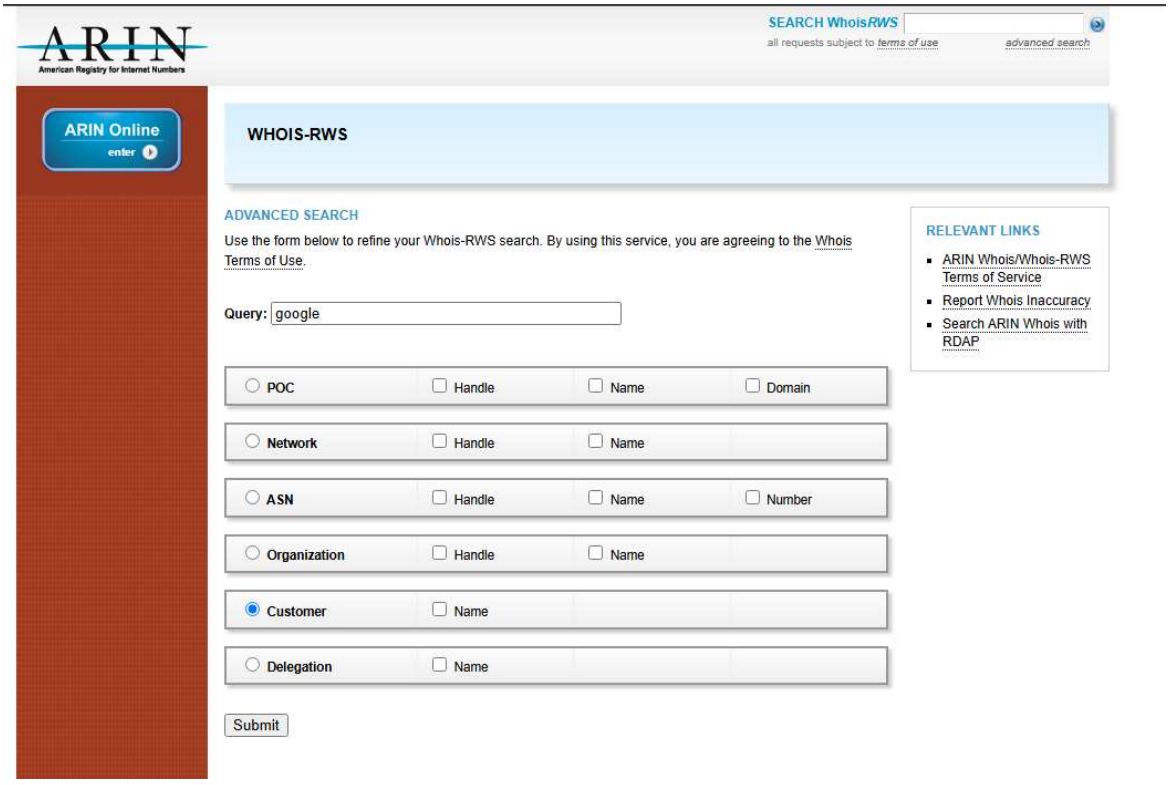
Whois는 도메인 이름, IP 주소 와 같은 인터넷 자원의 소유자 정보 및 범위를 조회하기 위한 통신 프로토콜입니다. 이 프로토콜을 통해 도메인이나 IP 주소와 관련된 정보를 저장하고 제공하는 서버를 whois 서버라고 합니다.

1. Whois 서버에 쿼리 입력하기

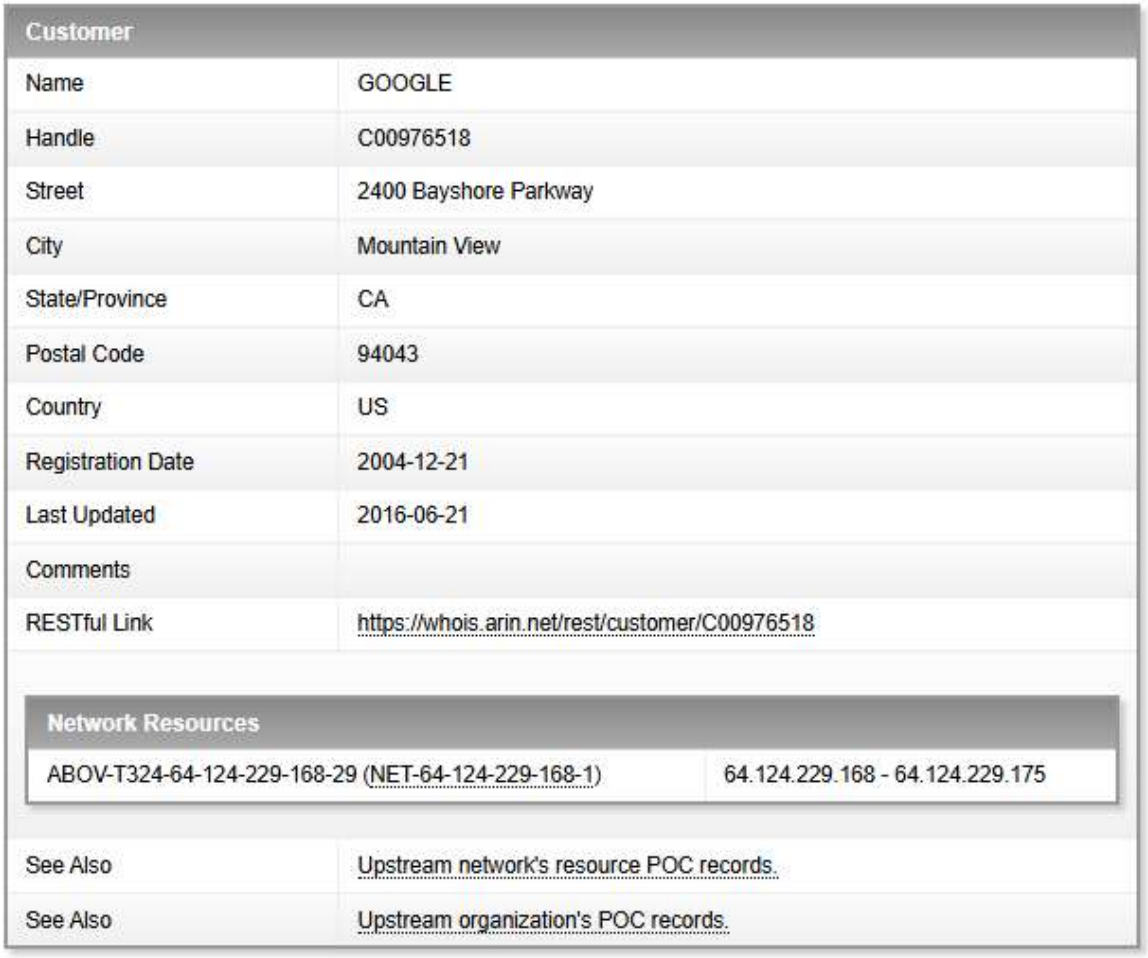
Whois 홈페이지에 접속하겠습니다.

- http://Whois.arin.net/ui/advanced.jsp

Query에 google을 입력하고, Customer를 체크한 뒤 Submit 해보겠습니다.



2. Whois 서버에서 검색한 결과 확인하기



Customer	
Name	GOOGLE
Handle	C00976518
Street	2400 Bayshore Parkway
City	Mountain View
State/Province	CA
Postal Code	94043
Country	US
Registration Date	2004-12-21
Last Updated	2016-06-21
Comments	
RESTful Link	https://whois.arin.net/rest/customer/C00976518

Network Resources	
ABOV-T324-64-124-229-168-29 (NET-64-124-229-168-1)	64.124.229.168 - 64.124.229.175

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

Whois 서버 조회 결과 도메인 소유자의 주소와 등록일자, 네트워크 범위 등의 정보를 구체적으로 확인 할 수 있습니다.

3. whois 서버로 원하는 내용 검사하기

이번엔 이름이 jesus인 사람이 등록한 사이트를 검색 해보겠습니다.

Points of Contact
Jesus (JESUS11-ARIN)
Jesus, Manuel (MJ342-ARIN)
Jesus, Michael (MJ602-ARIN)

이번 실습에서는 hosts파일을 변조사여 정상적인 도메인에 접속하더라도 접속이 되지 않도록 차단시켜 보겠습니다.

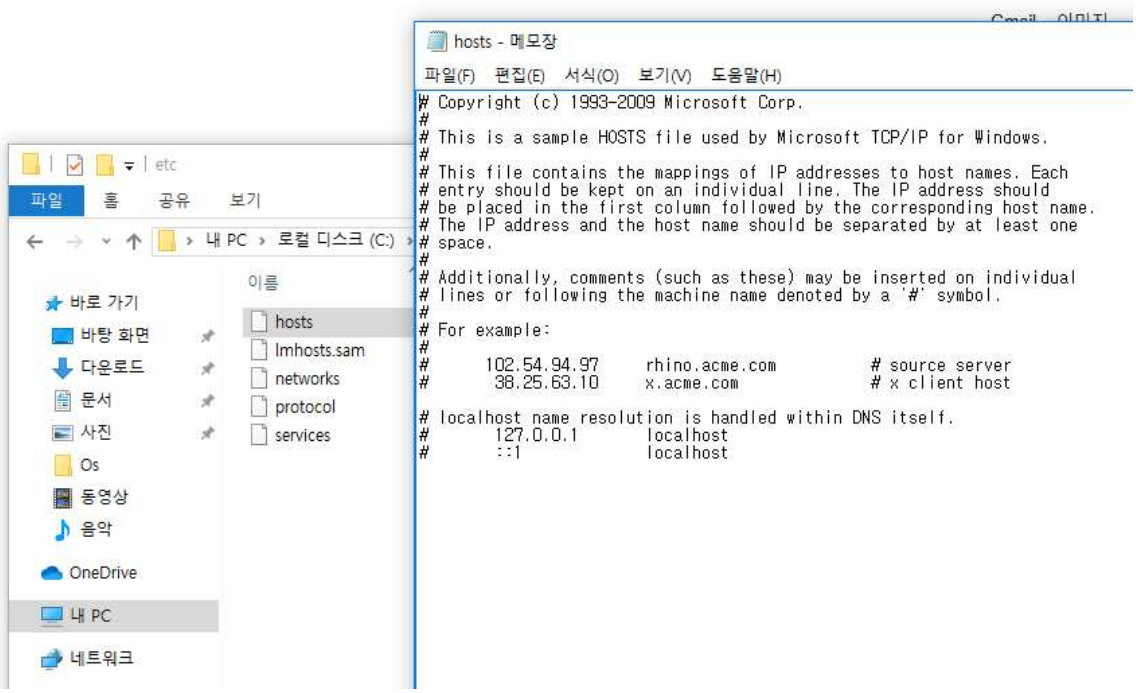
1. 도메인 등록하기

ping 명령어를 통해 도메인과 연결해보겠습니다.

```
C:₩Users₩PC>ping www.google.com

Ping www.google.com [142.250.207.100] 32바이트 데이터 사용:
142.250.207.100의 응답: 바이트=32 시간=35ms TTL=128
142.250.207.100의 응답: 바이트=32 시간=30ms TTL=128
142.250.207.100의 응답: 바이트=32 시간=34ms TTL=128
142.250.207.100의 응답: 바이트=32 시간=30ms TTL=128

142.250.207.100에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 30ms, 최대 = 35ms, 평균 = 32ms
```

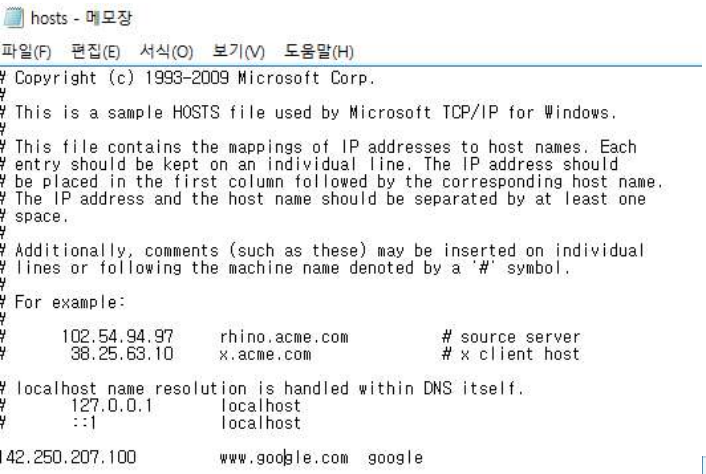
2. hosts 파일 동작 확인하기

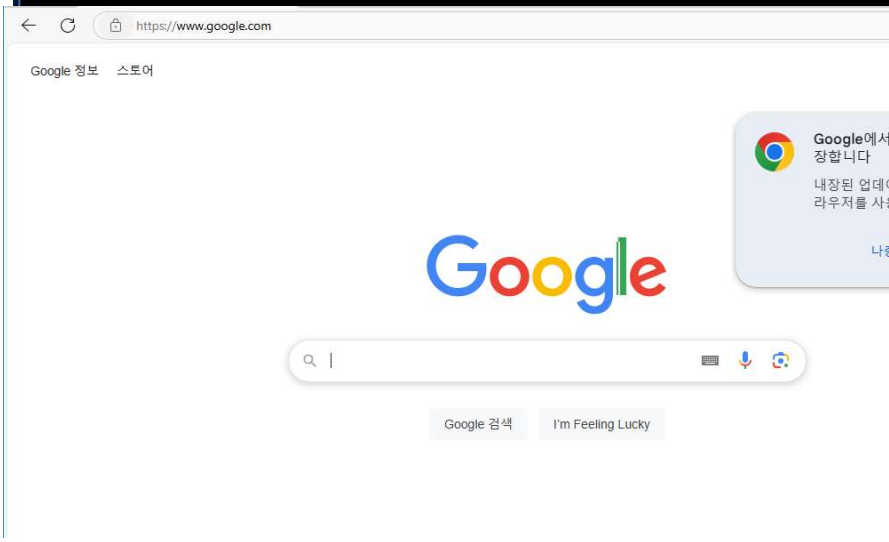
C:\Windows\System32\drivers\etc\hosts 을 확인했습니다.



142.250.207.100 www.google.com google

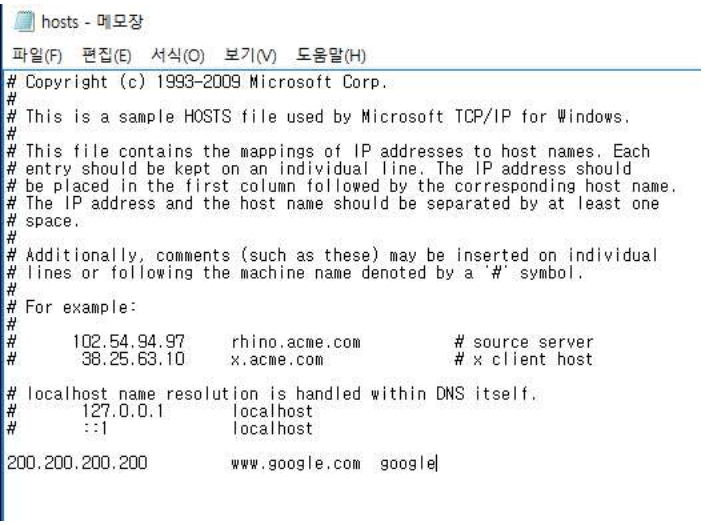
를 추가하고 hosts 파일이 잘 동작하는지 확인해보겠습니다.

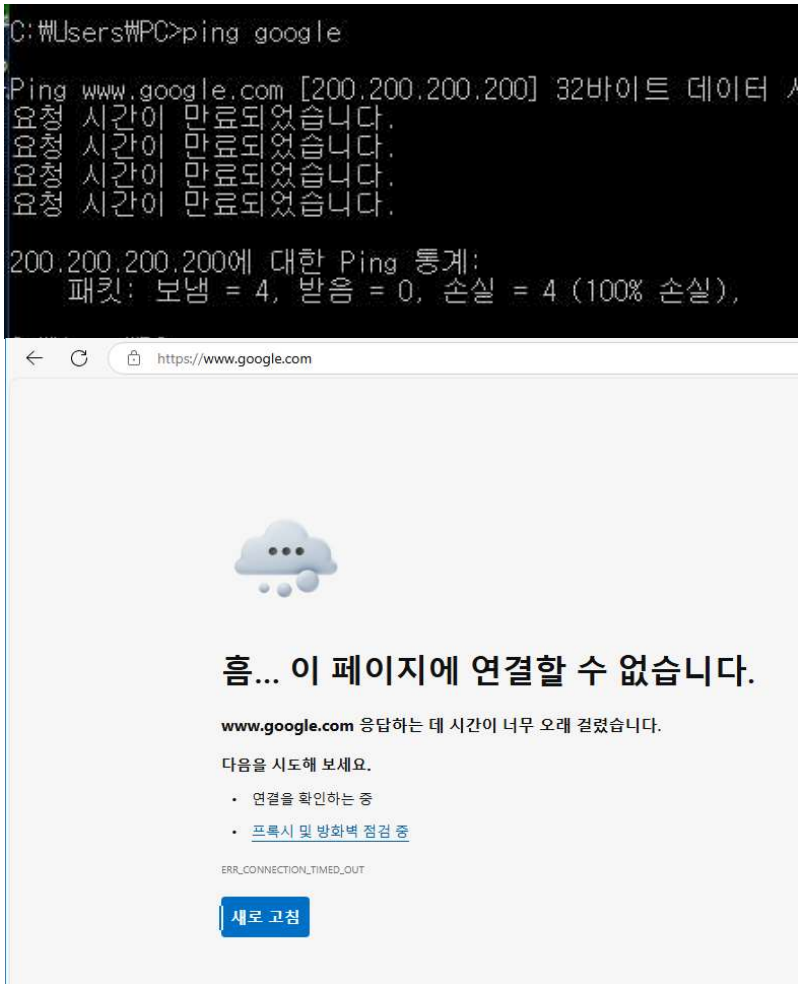




정상적으로 접속이 가능한걸 확인했습니다.

3. 잘못된 주소를 등록하여 사이트 접속 차단하기





142.250.207.100 를 200.200.200.200으로 수정한 결과 www.google.com에 접속이 불가능해졌습니다.

이러한 이유는 웹 브라우저가 도메인 접속 시 DNS서버 보다 먼저 hosts파일을 참조하기 때문인데 hosts 파일에 잘못된 IP주소가 설정되어 있어 존재하지 않는 서버로 접속을 시도하게 되어 접속이 불가능 한 것입니다.

1. nslookup 실행하고 DNS 설정하기

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server:  kns.kornet.net
Address:  168.126.63.1

> server 219.250.36.130
Default Server:  bns2.hananet.net
Address:  219.250.36.130
```

DNS서버를 bns2.hananet.net 으로 설정했습니다.

2. 도메인 정보 수집하기

```
> www.google.co.kr
Server:  bns2.hananet.net
Address:  219.250.36.130

Non-authoritative answer:
Name:    www.google.co.kr
Addresses:  2404:6800:400a:804::2003
          142.250.198.3

>
```

기본적인 도메인 질의를 통해 www.google.co.kr의 IP주소를 확인할 수 있습니다.

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

Non-authoritative answer:
google.co.kr    nameserver = ns2.google.com
google.co.kr    nameserver = ns3.google.com
google.co.kr    nameserver = ns4.google.com
google.co.kr    nameserver = ns1.google.com

ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
>
```

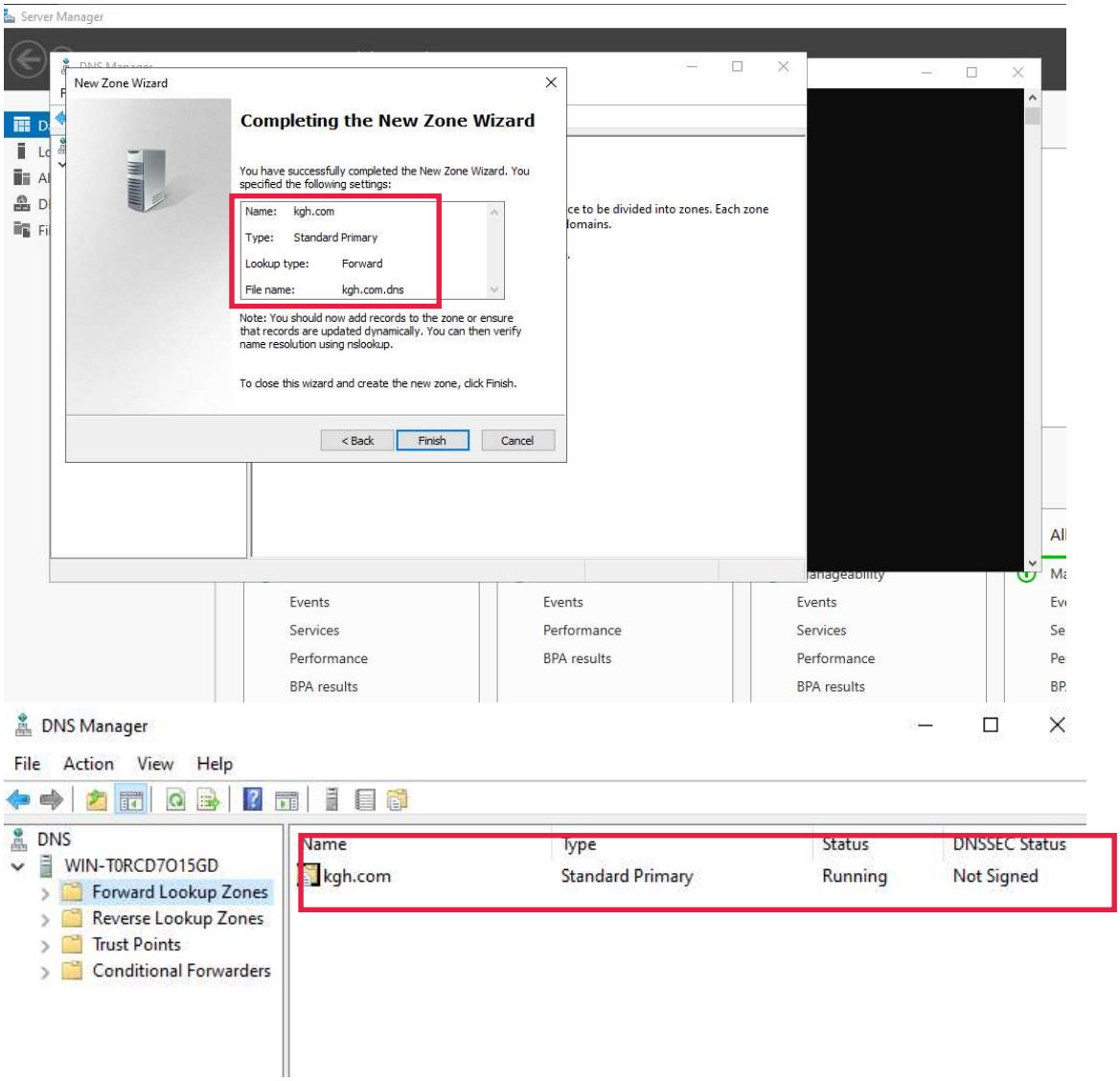
질의 유형을 NS(Name Server)로 설정한 후 google.co.kr에 대해 실행하면 해당 도메인을 관리하는 네임서버 정보를 확인할 수 있습니다.

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

Non-authoritative answer:
google.co.kr
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 740697311
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
google.co.kr    ??? unknown type 257 ???
google.co.kr    MX preference = 0, mail exchanger = smtp.google.com
google.co.kr    text =

        "v=spf1 -all"
google.co.kr    internet address = 216.58.220.99
google.co.kr    AAAA IPv6 address = 2404:6800:4004:812::2003
google.co.kr    nameserver = ns3.google.com
google.co.kr    nameserver = ns2.google.com
google.co.kr    nameserver = ns1.google.com
google.co.kr    nameserver = ns4.google.com
```

질의 유형을 all로 설정하면 google.co.kr에 대한 모든 DNS 레코드를 확인 할 수 있습니다.

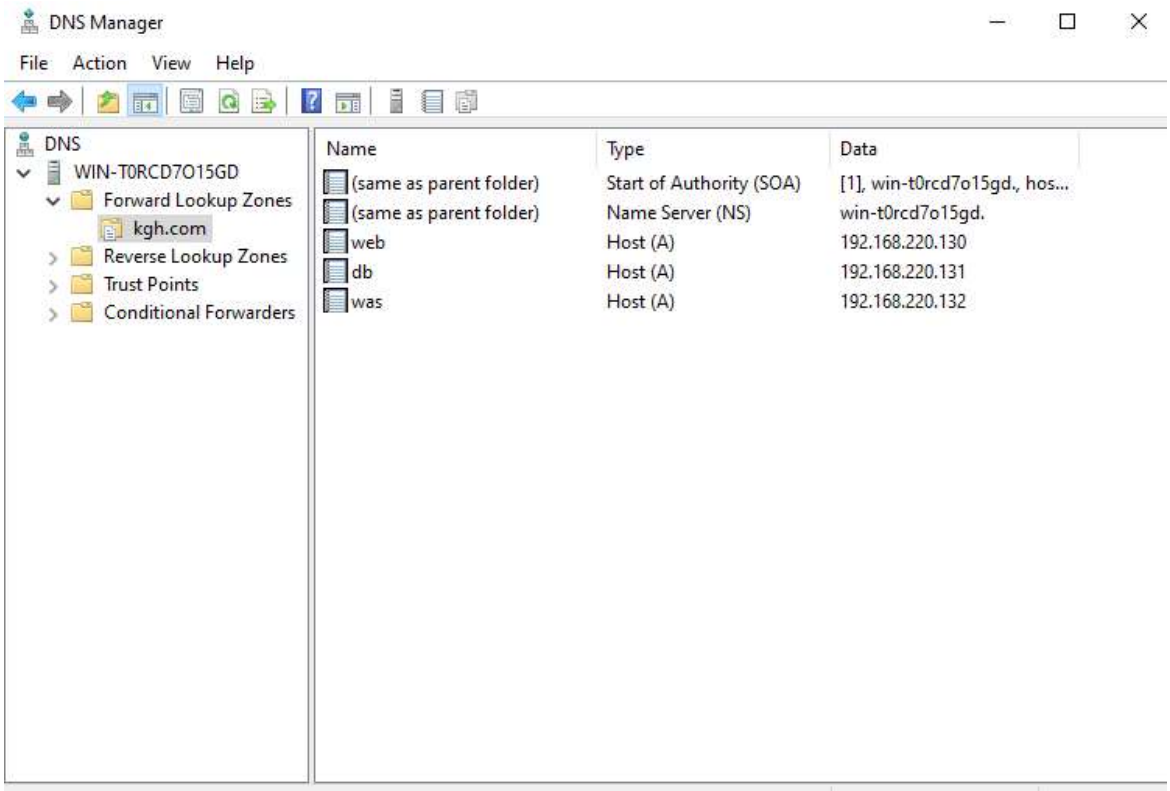
3. DNS 영역 전송하기

1) DNS zone 생성하기



DNS 서버 설치 및 기본 설정을 완료한 후 관리 도구를 통해 Forward Lookup Zone에 Primary Zone을 생성하였습니다. 실습 테스트 도메인으로 kgh.com을 생성하였습니다.

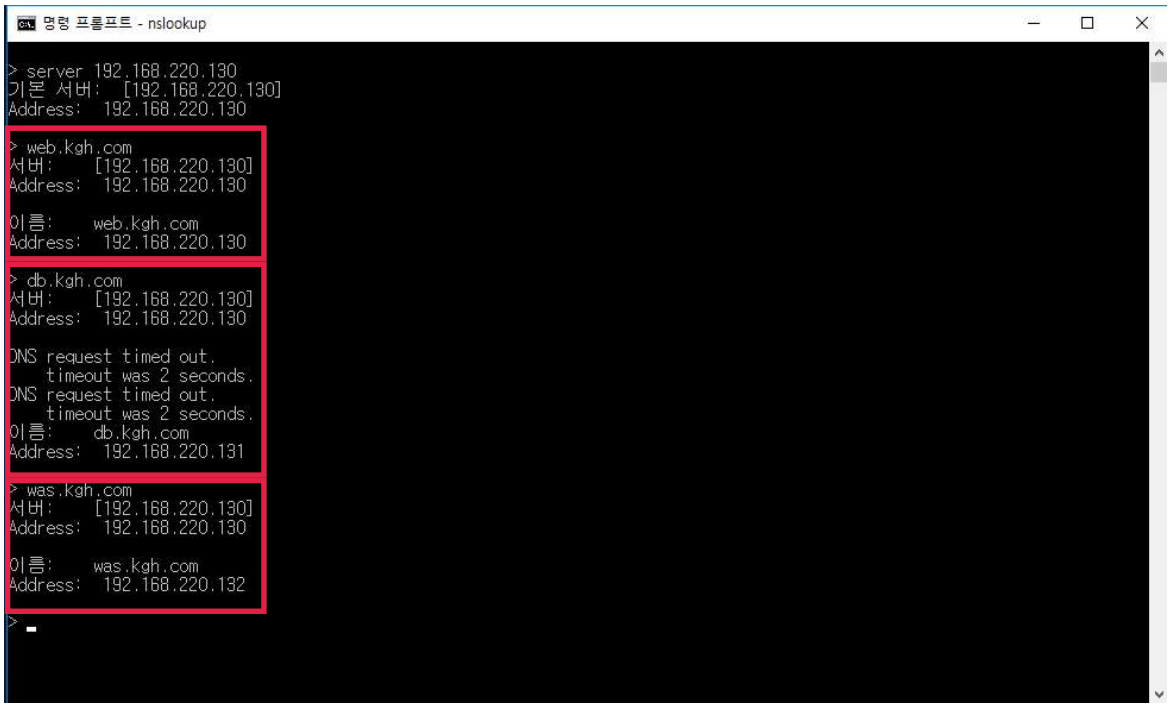
2) zone에 대한 서버 등록하기



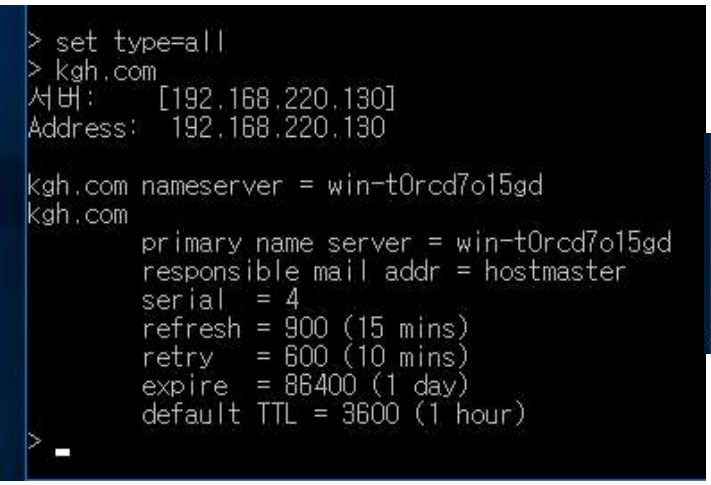
생성한 Zone(kgh.com)에 대해 web, db, was 세 개의 호스트 이름을 각각 등록했습니다.

host	domain	ip
web	web.kgh.com	192.168.220.130
db	db.kgh.com	192.168.220.131
was	was.kgh.com	192.168.220.132

4) DNS 영역 확인하기



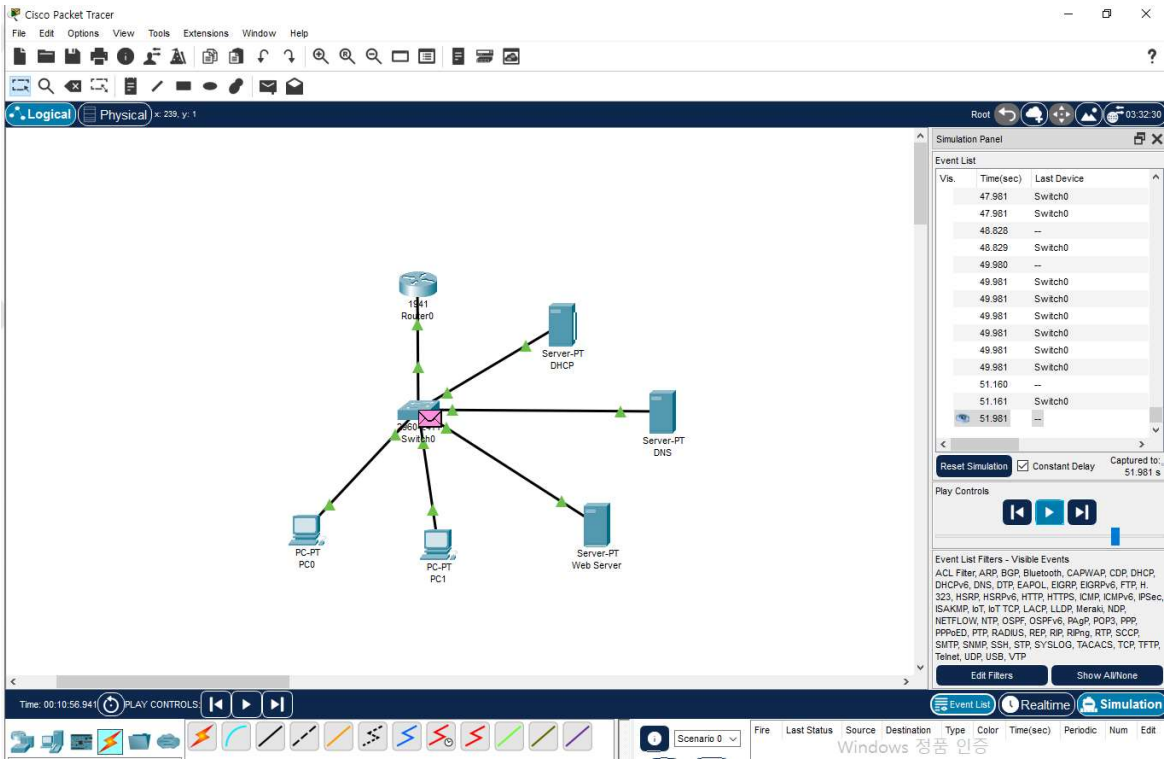
server 192.168.220.130 명령어를 통해 DNS서버를 지정하고 위에서 생성한 도메인 web.kgh.com, db.kgh.com, was.kgh.com에 대해 질의를 해봤습니다.



set type=all과 ls kgh.com 명령어를 실행한 결과 해당 Zone에 대한 다양한 DNS 정보가 출력되는 것을 확인하였습니다.

이를 통해 DNS 서버가 kgh.com 영역에 대해 올바르게 구성되었음을 확인했습니다.

1. 네트워크 장치 연결하기



교재의 실습 내용과 같이 라우터 1대, 스위치 1대, PC 2대, 서버 3대로 구성하였습니다.

장비	IP 주소
Router	192.168.16.1
DHCP Server	192.168.16.5
DNS Server	192.168.16.6
Web Server	192.168.16.7

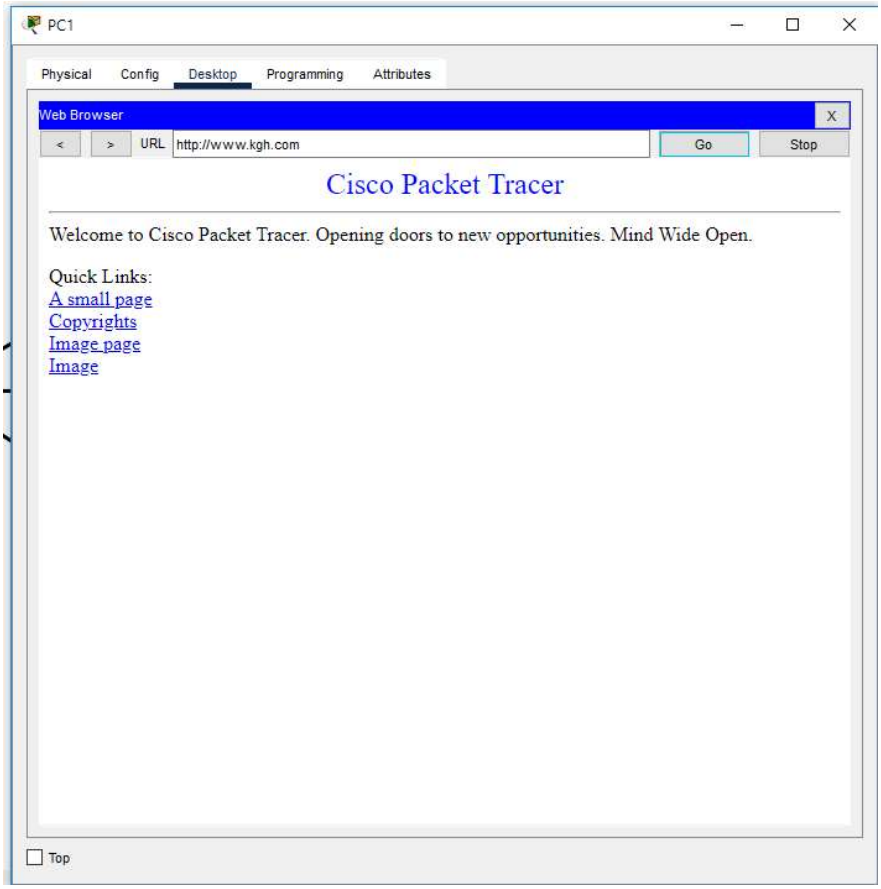
클라이언트 PC는 다음과 같이 설정했습니다.

PC	IP주소	기본 게이트웨이	DNS 서버 주소
PC0	192.168.16.100	192.168.16.1	192.168.16.6
PC1	192.168.16.101	192.168.16.1	192.168.16.6

마찬가지로 DNS 서버에 www.kgh.com 도메인을 등록했습니다.

설정이 정상이라면 클라이언트는 www.kgh.com 도메인네임을 통해 웹 서버에 접근 할 수 있습니다.

2. 서버 연결 확인하기



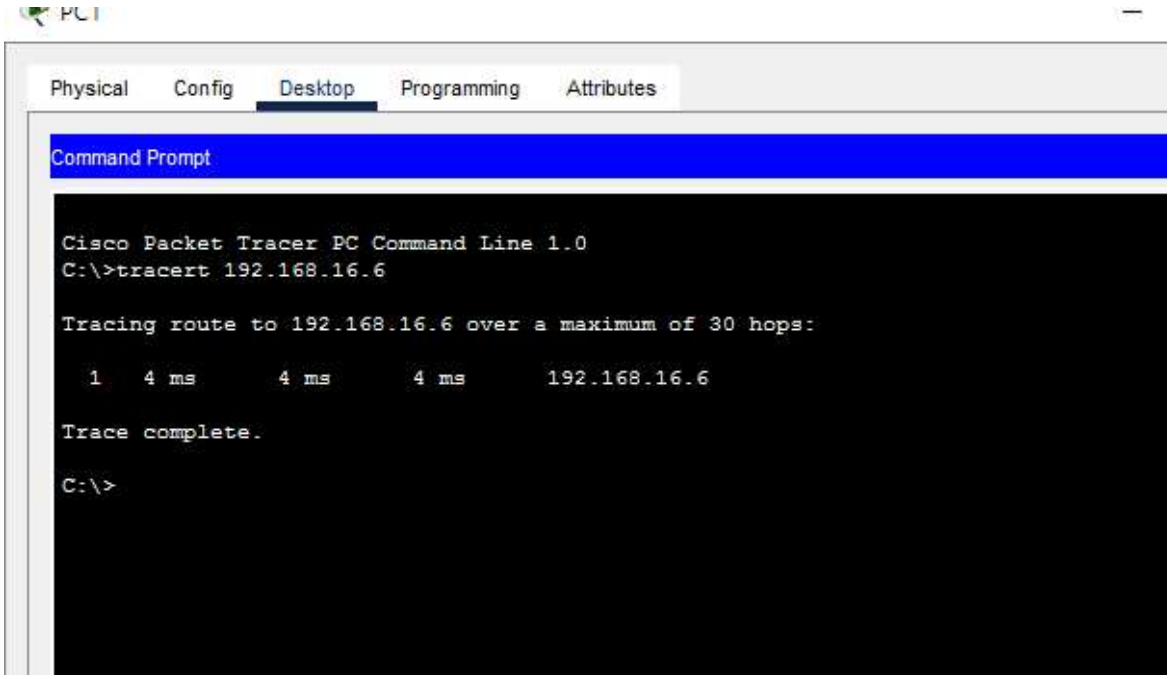
PC1의 웹브라우저에서 www.kgh.com으로 접속한 결과 웹 페이지가 정상적으로 로딩됐습니다. 어떻게 www.kgh.com에 접속했을 때 웹 페이지가 뜨는 것일까요?

웹 페이지가 정상적으로 뜨는 이유를 분석해보겠습니다.

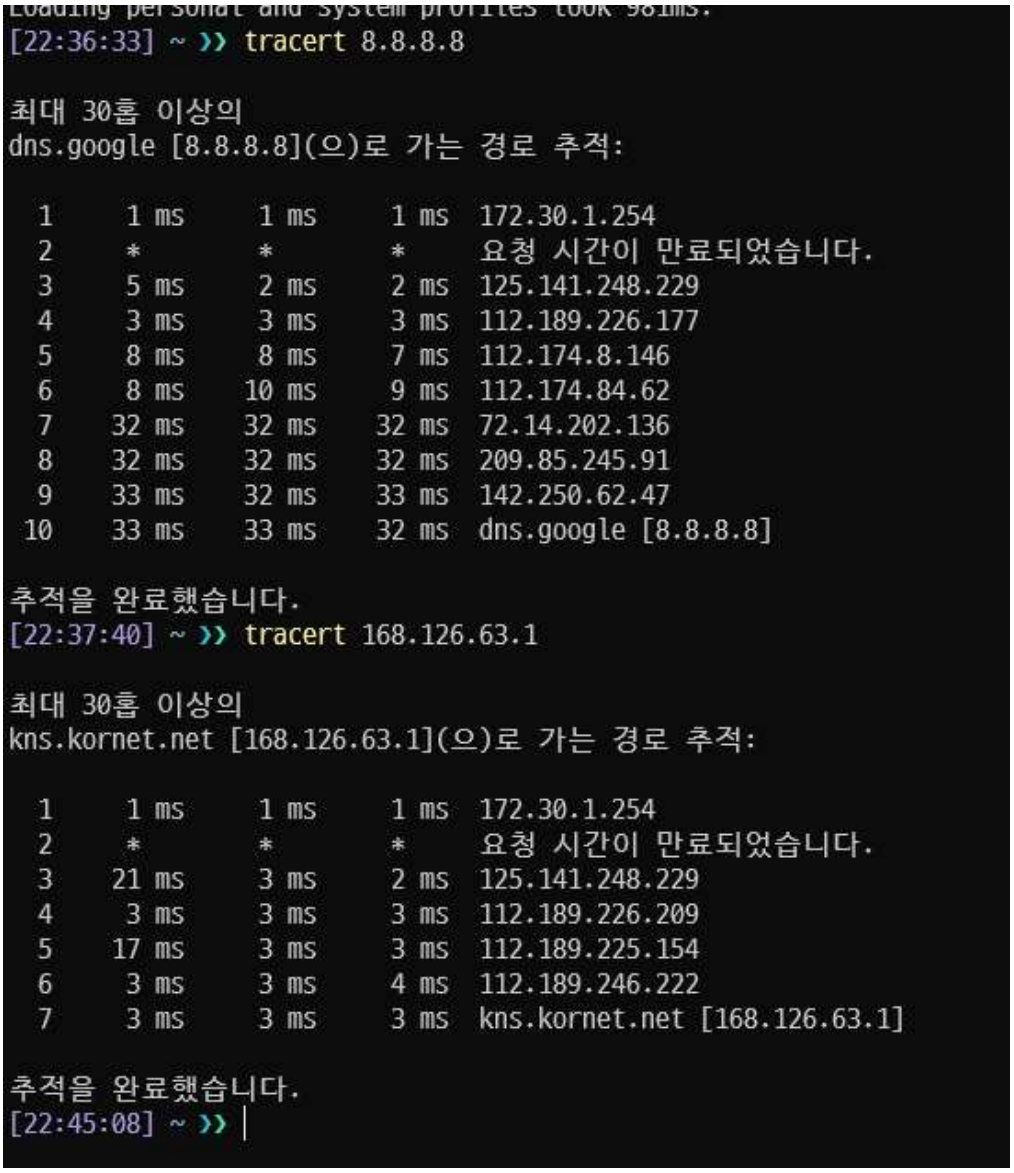
1. PC1의 DNS 설정은 192.168.16.6으로 되어있고 이는 DNS서버를 가리킵니다.
2. 클라이언트가 웹 브라우저에 www.kgh.com을 입력하면 PC1은 해당 도메인의 IP를 알기 위해 DNS서버에 물어봅니다.
3. DNS서버는 설정된 A 레코드에 따라 192.168.16.7을 응답합니다.
4. 이후 PC1은 해당 IP로 HTTP 요청을 보내고 Web Server는 이에 대한 웹 페이지를 응답함으로써 정상적인 접속이 이루어집니다.

3. 네트워크 경로 추적하기

tracert 명령어를 사용해 PC1에서 DNS로 가는 네트워크 경로를 추적해보겠습니다.



PC1에서 tracert 192.168.16.6 명령어를 실행한 결과 별다른 경유지 없이 바로 목적지에 도달한 것을 확인할 수 있습니다. 이는 PC1과 DNS서버가 같은 로컬 네트워크 내에 있어 라우터를 거치치 않고 직접 통신하기 때문입니다.



이번엔 제 개인 PC에서 실제 외부 DNS서버를 대상으로 tracert 명령어를 사용해 라우팅 경로를 확인해 보겠습니다.

8.8.8.8과 168.126.63.1으로 tracert명령어를 수행한 결과 8.8.8.8은 dns.google 168.126.63.1은 kns.kornet.net으로 정상적으로 해석되고 응답되었습니다.

tracert 명령어를 통해 실제 인터넷 환경에서 데이터가 어떤 경로를 거쳐 목적지까지 도달하는지를 시각적으로 확인할 수 있었습니다.