Whois와 DNS 조사

202213007 조서윤

Whois

도메인에 대한 정보를 조회하기 위한 프로토콜

인터넷이 ARPANET에서 분리될 당시 DARPA가 도메인 관리를 하던 유일한 기관,
도메인은 1984에 만들어진 RFC 920에 따라 등록되었다.
비슷한 시기에 도메인을 확인하고, 도메인과 관련된 사람과 인터넷 자원을
찾아보기 위한 프로토콜로 Whois가 만들어졌다.

Whois

도메인에 대한 정보를 조회하기 위한 프로토콜

초기 Whois에서는 와일드카드 문자열로 관련 도메인 검색 가능했다.
(사용자 이름 및 관련 정보만으로 도메인 검색 가능)
스팸 메일 증가로 기능은 사라졌다.

1993년 도메인 등록 및 관리의 책임이 DARPA에서 InterNIC로 이전되고,
1999년에는 다시 ICANN으로 이전되었으나 아직도 쓰인다.

01 도메인 등록 및 관리 기관 정보

02 도메인 이름과 관련된 인터넷 자원 정보

03 목표 사이트의 네트워크 주소와 IP 주소

04 등록자, 관리자, 기술 관리자 이름, 연락처, 이메일 계정

05 레코드의 생성 시기와 갱신 시기

06 주 DNS 서버와 보조 DNS 서버

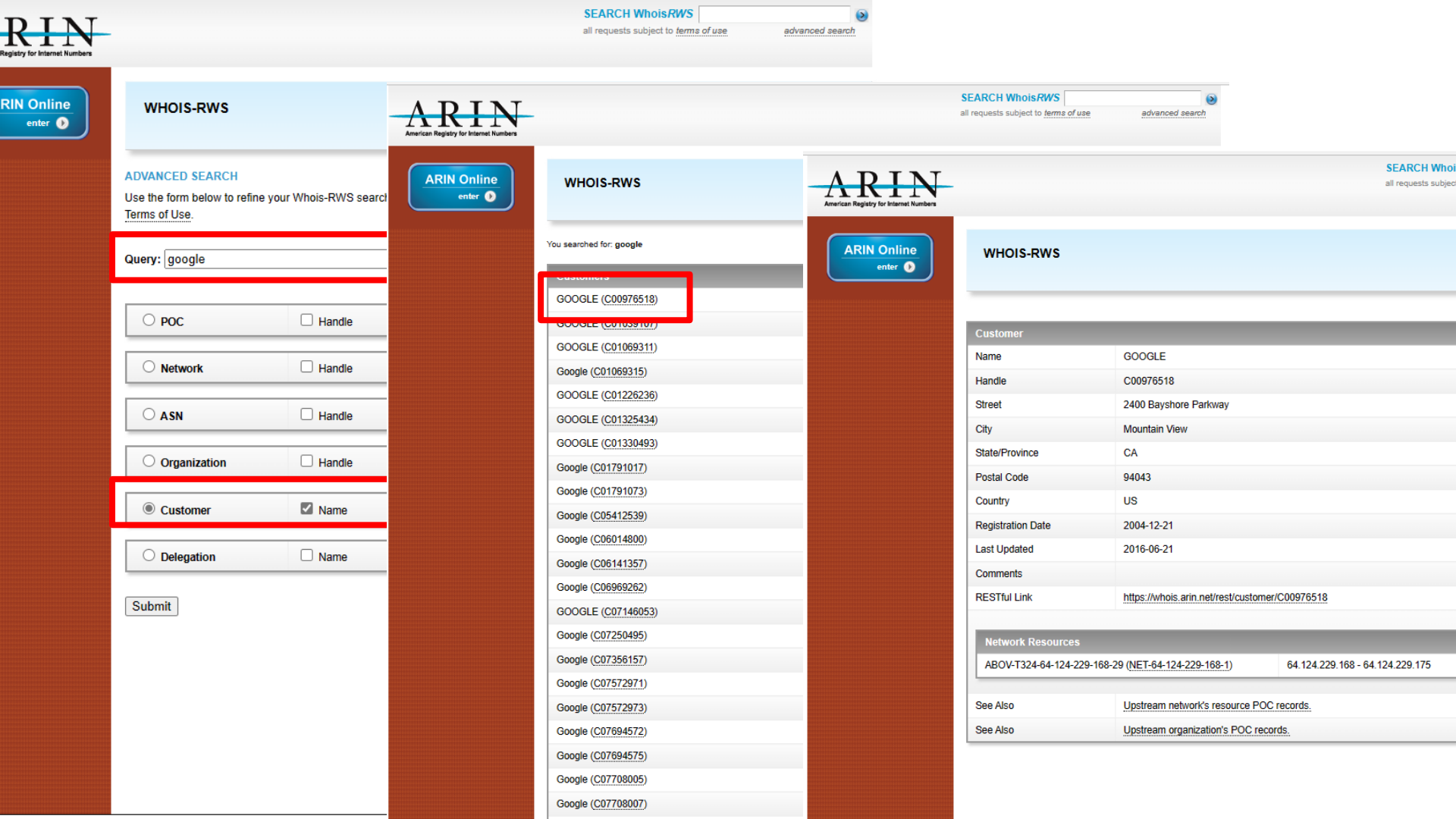
07 IP 주소의 할당 지역 위치

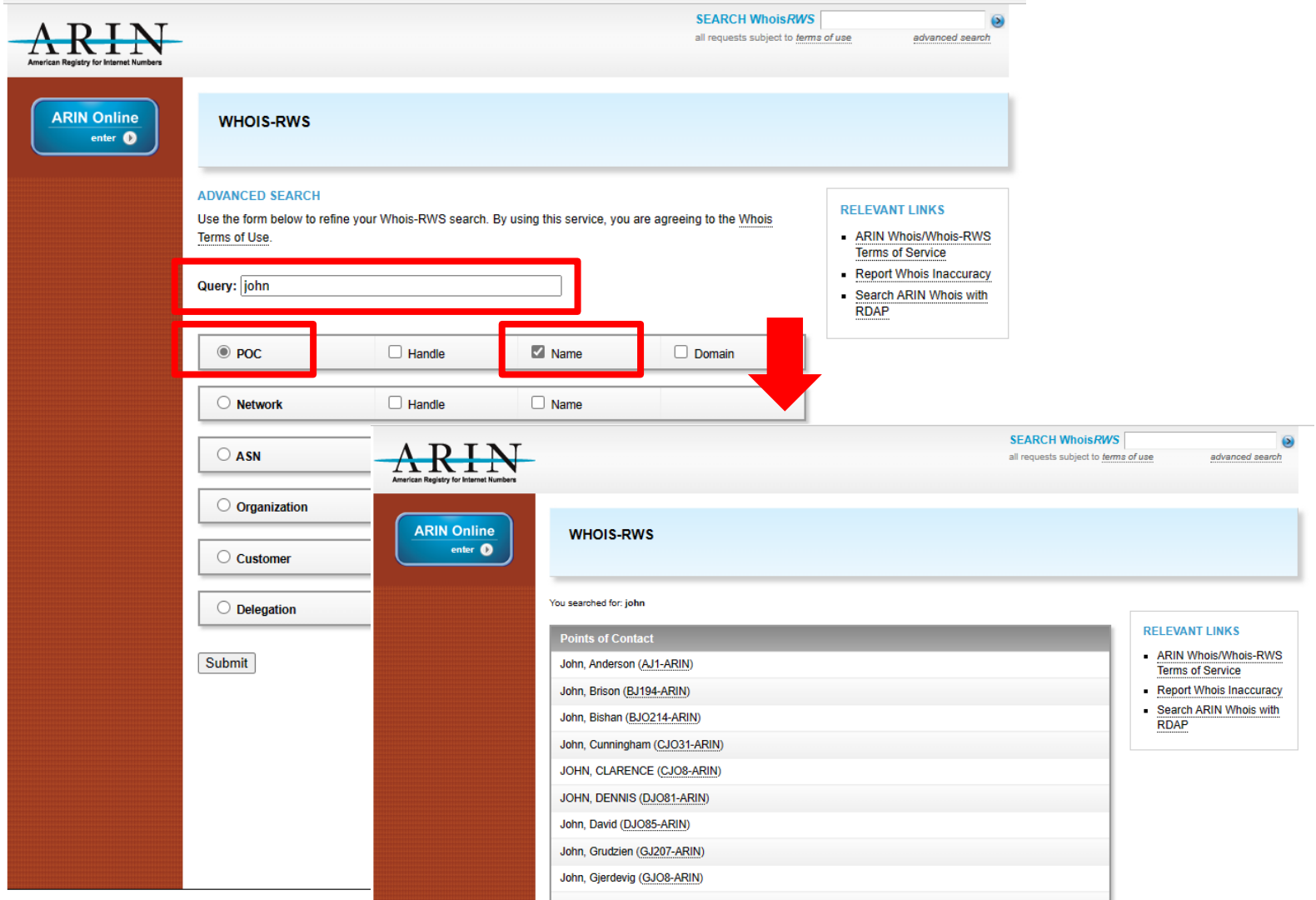
Whois

도메인을 등록하면 각 지역별 Whois 서버에 등록된다.

표 3-1 지역별 Whois 서버 목록

담당 지역	Whois 서버
전체	whois.internic.net
유럽	www.ripe.net
아시아 태평양 지역	www.apnic.net
	www.arin.net
호주	whois.aunic.net
프랑스	whois.nic.fr
일본	whois.nic.ad.jp
영국	whois.nic.uk
한국	whois.krnic.net
해커들을 위한 Whois	whois.greektoos.com


SEARCH WhoisRWS
all requests subject to terms of use
advanced search
ARIN Online
enter
WHOIS-RWS
ADVANCED SEARCH
Use the form below to refine your Whois-RWS search
Terms of Use.
Query: google
POC
Handle
Network
Handle
ASN
Handle
Organization
Handle
Customer
Name
Delegation
Name
Submit
You searched for: google
GOOGLE (C00976518)
GOOGLE (C01069311)
Google (C01069315)
GOOGLE (C01226236)
GOOGLE (C01325434)
GOOGLE (C01330493)
Google (C01791017)
Google (C01791073)
Google (C05412539)
Google (C06014800)
Google (C06141357)
Google (C06969262)
GOOGLE (C07146053)
Google (C07250495)
Google (C07356157)
Google (C07572971)
Google (C07572973)
Google (C07694572)
Google (C07694575)
Google (C07708005)
Google (C07708007)
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.

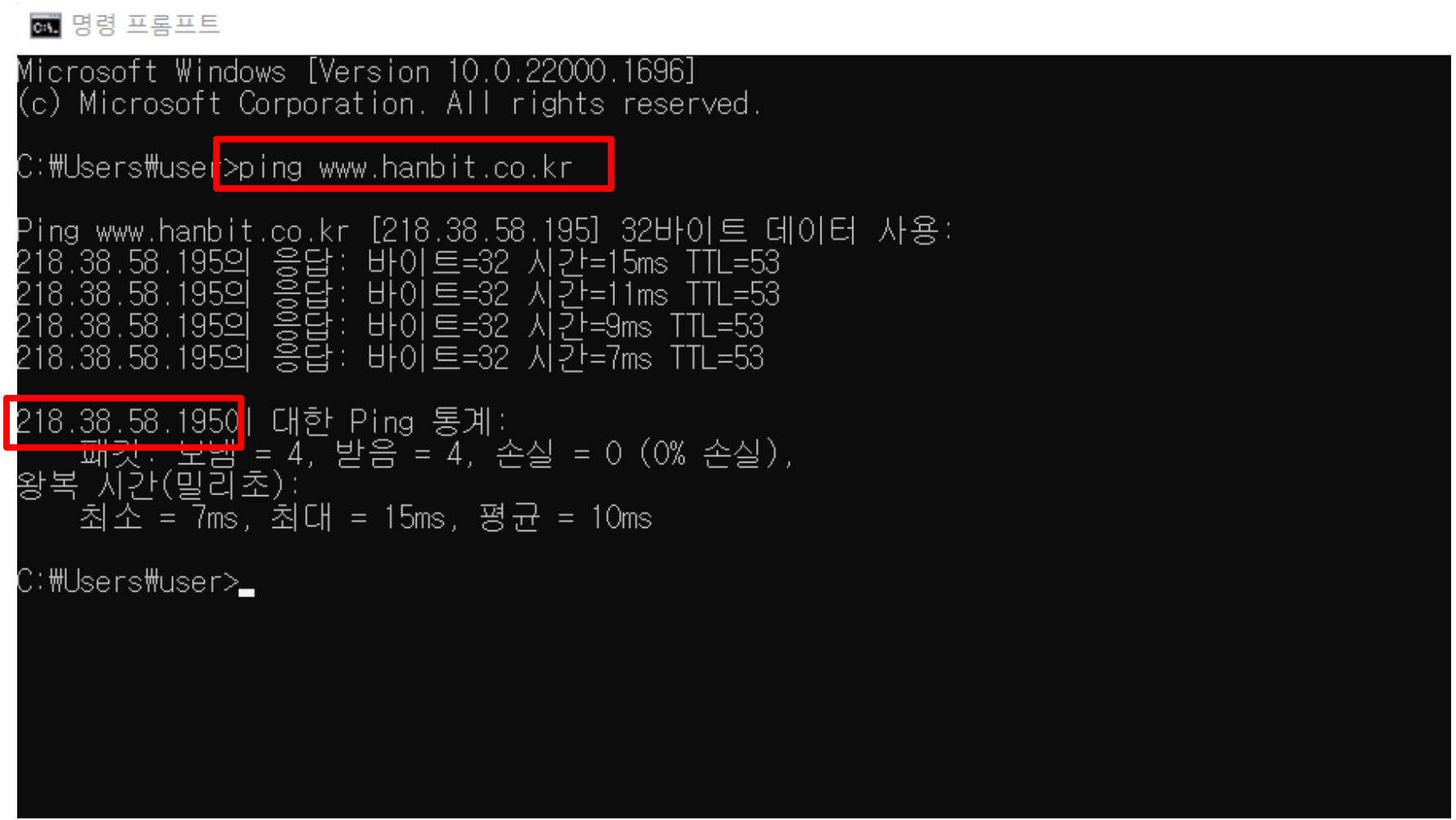

ARIN
American Registry for Internet Numbers
SEARCH WhoisRWS
all requests subject to terms of use
advanced search
ARIN Online
enter
WHOIS-RWS
ADVANCED SEARCH
Use the form below to refine your Whois-RWS search. By using this service, you are agreeing to the Whois Terms of Use.
Query: john
POC
Handle
Name
Domain
Network
Handle
Name
ASN
Organization
Customer
Delegation
Submit
RELEVANT LINKS
ARIN Whois/Whois-RWS Terms of Service
Report Whois Inaccuracy
Search ARIN Whois with RDAP
ARIN
American Registry for Internet Numbers
SEARCH WhoisRWS
all requests subject to terms of use
advanced search
ARIN Online
enter
WHOIS-RWS
You searched for: john
Points of Contact
John, Anderson (AJ1-ARIN)
John, Brison (BJ194-ARIN)
John, Bishan (BJO214-ARIN)
John, Cunningham (CJO31-ARIN)
JOHN, CLARENCE (CJO8-ARIN)
JOHN, DENNIS (DJO81-ARIN)
John, David (DJO85-ARIN)
John, Grudzien (GJ207-ARIN)
John, Gjerdevig (GJO8-ARIN)
RELEVANT LINKS
ARIN Whois/Whois-RWS Terms of Service
Report Whois Inaccuracy
Search ARIN Whois with RDAP

Hosts

초기의 인터넷은 IP 주소만 사용해 인터넷을 이용했다.
1983년 DNS가 만들어지기 전에는 PC의 hosts 파일에 도메인 대신 별명같은 원하는 명칭을 IP 주소와 매칭시켜 인터넷을 사용했다.

Hosts

DNS 서버가 작동하지 않을 때, 별도의 네트워크를 구성하여 임의로 사용하고자 할 때, 다른 IP 주소를 가진 여러 대의 서버가 같은 도메인으로 클러스터링되어 운용되는 상태에서 특정 서버에 접속하고자 할 때 유용하다.
잘못된 hosts 파일은 서버 접속 자체를 막을 수 있다.

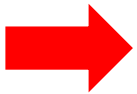

명령 프롬프트
Microsoft Windows [Version 10.0.22000.1696]
(c) Microsoft Corporation. All rights reserved.
C:₩Users₩user>ping www.hanbit.co.kr
Ping www.hanbit.co.kr [218.38.58.195] 32바이트 데이터 사용:
218.38.58.195의 응답: 바이트=32 시간=15ms TTL=53
218.38.58.195의 응답: 바이트=32 시간=11ms TTL=53
218.38.58.195의 응답: 바이트=32 시간=9ms TTL=53
218.38.58.195의 응답: 바이트=32 시간=7ms TTL=53
218.38.58.1950 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
최소 = 7ms, 최대 = 15ms, 평균 = 10ms
C:₩Users₩user>

*hosts - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# 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
```



```
#       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
218.38.58.195   www.hanbit.co.kr    hanbit
```

명령 프롬프트

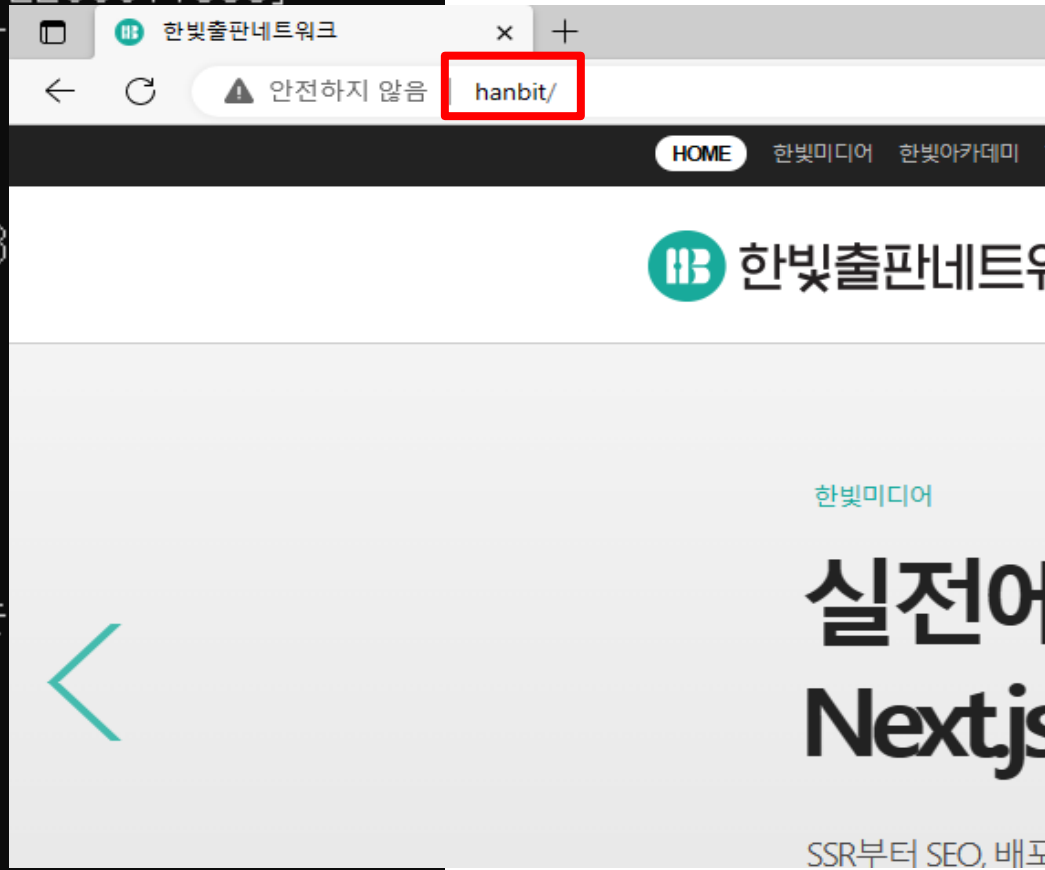
```
Microsoft Windows [Version 10.0.22000.1696]
(c) Microsoft Corporation. All r

C:₩Users₩user>ping hanbit

Ping www.hanbit.co.kr [218.38.58
218.38.58.195의 응답: 바이트=32
218.38.58.195의 응답: 바이트=32
218.38.58.195의 응답: 바이트=32
218.38.58.195의 응답: 바이트=32

218.38.58.195에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손
왕복 시간(밀리초):
    최소 = 11ms, 최대 = 48ms, 평

C:₩Users₩user>
```



```
C:₩WINDOWS₩system32>ping -a 218.38.58.195

Ping www.hanbit.co.kr [218.38.58.195] 32바이트 데이터 사용:
218.38.58.195의 응답: 바이트=32 시간=4ms TTL=52
218.38.58.195의 응답: 바이트=32 시간=4ms TTL=52
218.38.58.195의 응답: 바이트=32 시간=4ms TTL=52
218.38.58.195의 응답: 바이트=32 시간=4ms TTL=52

218.38.58.195에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 4ms, 최대 = 4ms, 평균 = 4ms

C:₩WINDOWS₩system32>
```


*hosts - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H
Copyright (c) 1993-2009 Microso
#
This is a sample HOSTS file used
#
This file contains the mappings o
entry should be kept on an indivi
be placed in the first column foll
The IP address and the host nam
space.
#
Additionally, comments (such as
lines or following the machine na
#
For example:
#
102.54.94.97 rhino.acme.com
38.25.63.10 x.acme.com
localhost name resolution is handled with
127. 0. 0. 1 localhost
::1 localhost
218.38.58.195 www. .kr hanbi
www.bing.com
https://www.bing.com/search?q=www.hanbit.co.kr&cvid=017c0e328f884466a90b202e6c7eab17&aqs=edge.2.69i60j69i59l2j69i57j69i60l4.4351j0j4&FORM=ANAB0
흠... 이 페이지에 연결할 수 없습니다.
www.bing.com's DNS 주소 을(를) 찾을 수 없습니다... 지금 문제를 진단 중입니다.
Windows 네트워크 진단을 실행해보세요..
DNS_PROBE_STARTED
새로 고침
localhost name resolution is handled within DNS i
127.0.0.1 localhost
::1 localhost
200.200.200.200 www.hanbit.co.kr hanbit

DNS

인터넷을 사용하는 동안 항상 사용하는 서비스로, 계층 구조를 이용

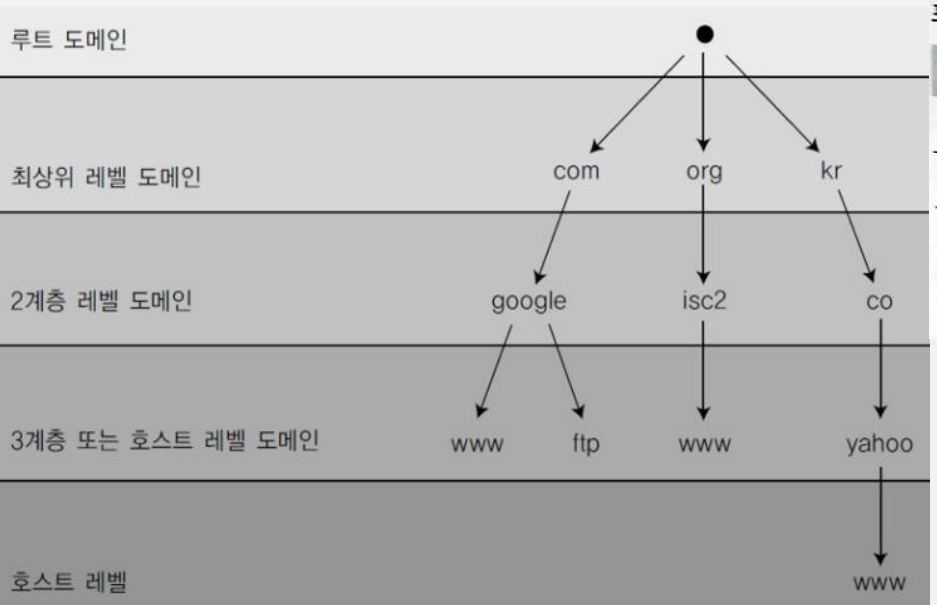
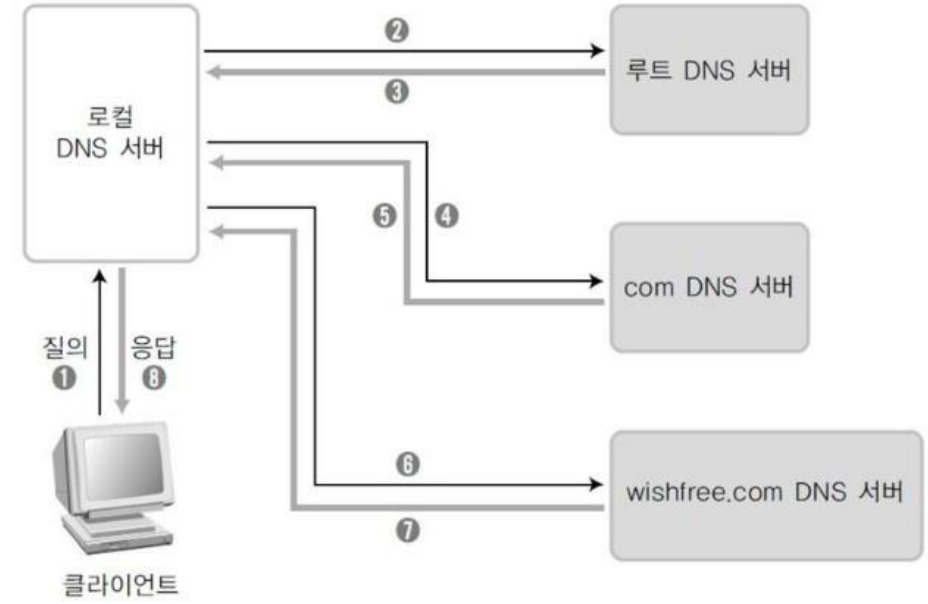


표 3-2 DNS의 두 번째 개체에 대한 내용

항목	내용	항목	내용
com	영리 기관	mil	군사 기관
net	네트워크 기관	edu	교육 기관
org	비영리 기관	int	국제 기관
gov	정부 기관	kr(Korea), jp(Japan)	국가 이름

DNS 서버로부터 도메인 이름에 대한 IP 주소를 얻는 순서



1. hosts 파일에 정보가 없으면 시스템에 설정된 DNS 서버인 로컬 DNS 서버에 질의한다.
2. 로컬 DNS 서버에도 해당 정보가 없으면 루트 DNS 서버에 질의를 보낸다.
3. 루트 DNS 서버에 www.wishfree.com에 대한 정보가 없으면 com을 관리하는 DNS 서버에 대한 정보를 보내준다.
4. 로컬 DNS 서버는 com www.wishfree.com에 대해 다시 질의한다.
5. 해당 정보가 없을 경우, com DNS 서버는 다시 wishfree.com에 대해 질의하도록 로컬 DNS 서버에 보낸다.
6. 로컬 DNS 서버는 마지막으로 wishfree.com의 DNS 서버에 질의한다.
7. wishfree.com의 DNS 서버로부터 www.wishfree.com에 대한 IP 주소를 얻는다.
8. 해당 IP 주소를 클라이언트에게 전달한다.

DNS

주 DNS 서버에서 관리하는 도메인 영역을 존이라 한다.
부 DNS 서버는 주 DNS 서버로부터 영역에 대한 정보를 전송받아 도메인에 대한 정보를 유지한다. 영역이 전송되는 대상을 부 DNS 서버로 제한하지 않으면 영역 정보를 해커가 획득하여 문제가 될 수 있다.

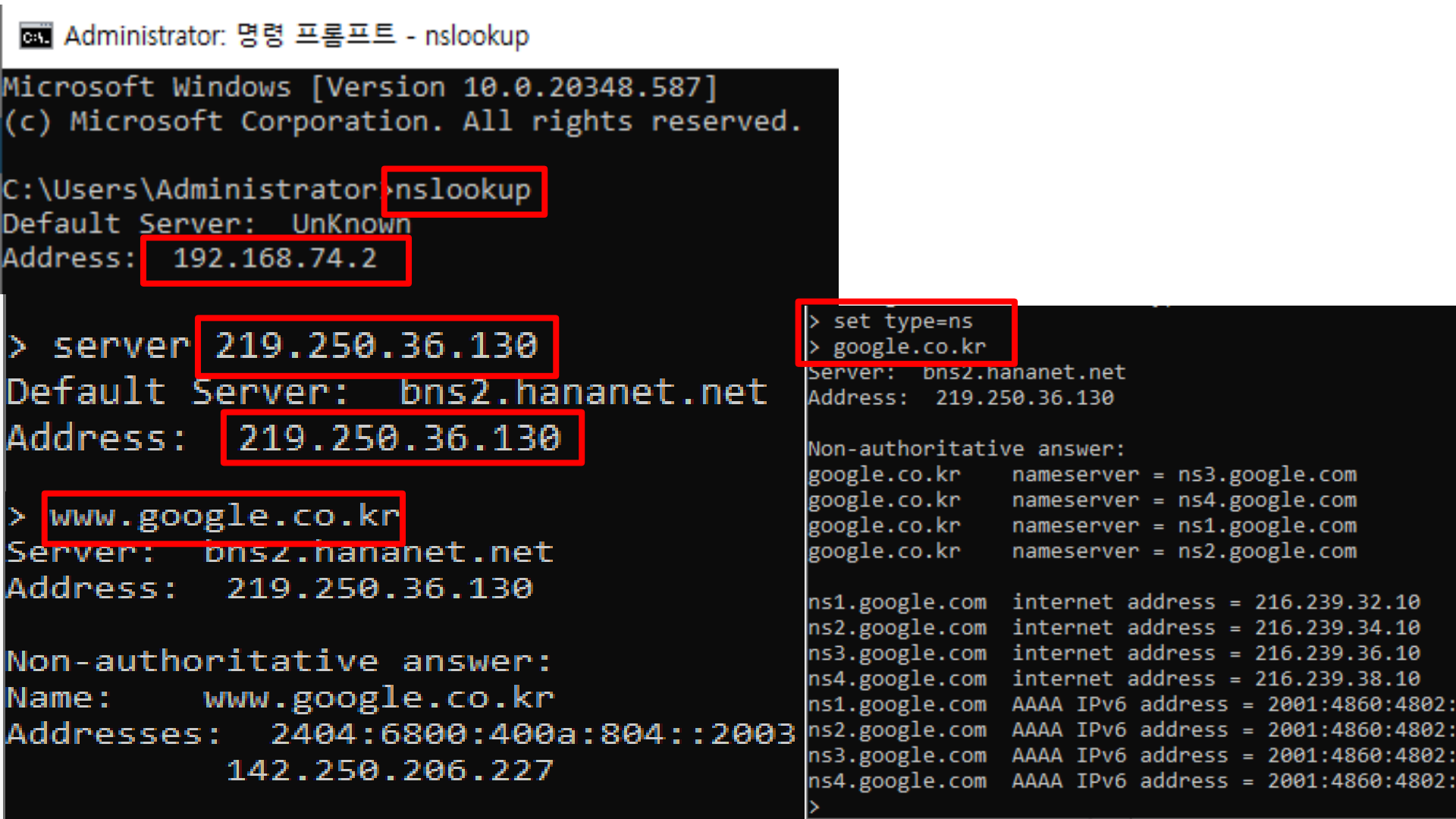

Administrator: 명령 프롬프트 - nslookup
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.74.2
> server 219.250.36.130
Default Server: bns2.hananet.net
Address: 219.250.36.130
> www.google.co.kr
Server: bns2.hananet.net
Address: 219.250.36.130
Non-authoritative answer:
Name: www.google.co.kr
Addresses: 2404:6800:400a:804::2003
142.250.206.227
> set type=ns
> google.co.kr
Server: bns2.hananet.net
Address: 219.250.36.130
Non-authoritative answer:
google.co.kr nameserver = ns3.google.com
google.co.kr nameserver = ns4.google.com
google.co.kr nameserver = ns1.google.com
google.co.kr nameserver = ns2.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:
ns2.google.com AAAA IPv6 address = 2001:4860:4802:
ns3.google.com AAAA IPv6 address = 2001:4860:4802:
ns4.google.com AAAA IPv6 address = 2001:4860:4802:
>

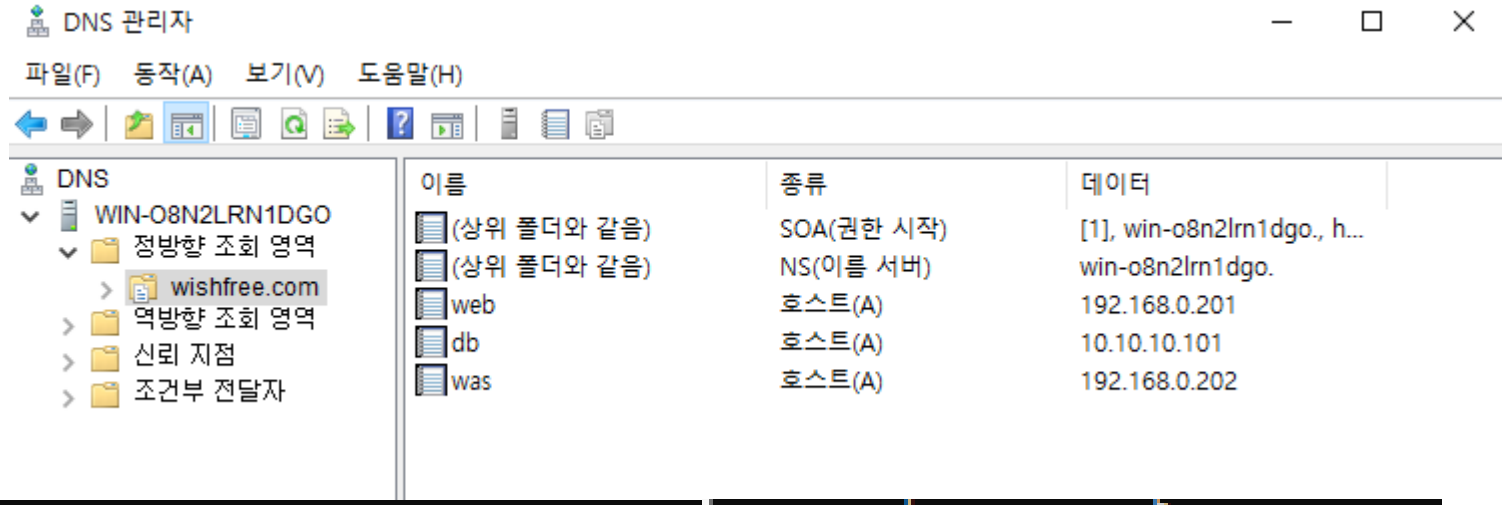
표 3-3 DNS 레코드의 종류

종류	내용
A(Address)	호스트 이름 하나에 IP 주소가 여러 개 있을 수 있고 IP 주소 하나에 호스트 이름이 여러 개 있을 수도 있다. 이를 정의하는 레코드 유형이 A이며, 다음과 같이 정의한다. – www A 200.200.200.20 – ftp A 200.200.200.20
PTR(Pointer)	A 레코드와 상반된 개념이다. A 레코드는 도메인에 대해 IP 주소를 부여하지만 PTR 레코드는 IP 주소에 대해 도메인명을 맵핑하는 역할을 한다.
NS(Name Server)	DNS 서버를 가리키며, 각 도메인에 적어도 한 개 이상 있어야 한다.
MX(Mail Exchanger)	도메인 이름으로 보낸 메일을 받는 호스트 목록으로 지정한다.
CNAME(Canonical Name)	호스트의 다른 이름을 정의하는 데 사용한다.
SOA(Start of Authority)	도메인에 대한 권한이 있는 서버를 표시한다.
HINFO(Hardware Info)	해당 호스트의 하드웨어 사양을 표시한다.
ANY(ALL)	DNS 레코드를 모두 표시한다.

```
> set type=all
> google.co.kr
Server:  dns2.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  = 521713658
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
google.co.kr    text =

        "v=spf1 -all"
google.co.kr    ??? unknown type 257 ???
google.co.kr    internet address = 142.250.206.227
google.co.kr    MX preference = 0, mail exchanger = smtp.google.com
google.co.kr    AAAA IPv6 address = 2404:6800:400a:804::2003
google.co.kr    nameserver = ns4.google.com
google.co.kr    nameserver = ns1.google.com
google.co.kr    nameserver = ns2.google.com
google.co.kr    nameserver = ns3.google.com
>
```



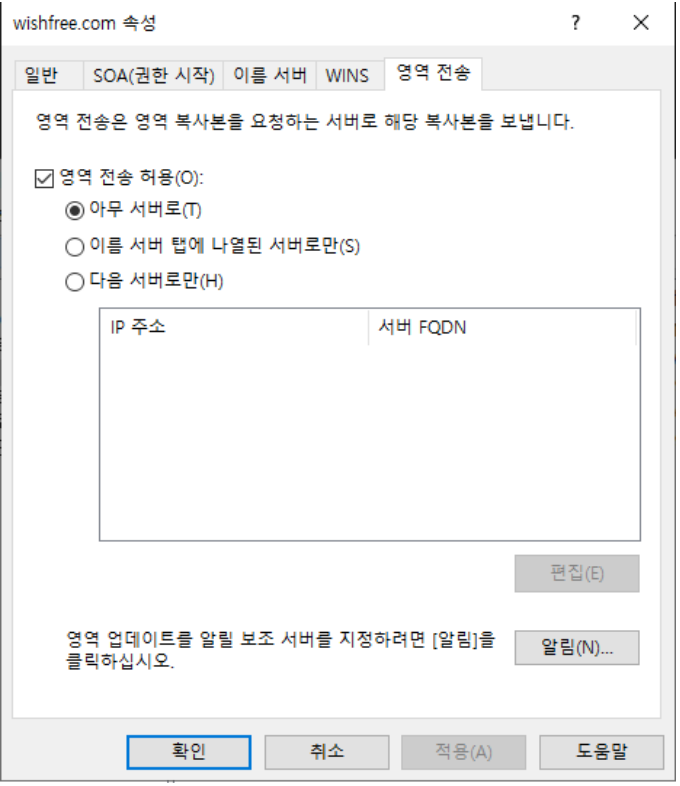

```
C:₩Users₩user>nslookup
기본 서버:  kns.kornet.net
Address:  168.126.63.1

>
> web.wishfree.com
Server:  [192.168.0.1]
Address:  192.168.0.1
```

```
> set type=all
> wishfree.com
Server:  [192.168.0.1]
Address:  192.168.0.1
```

DNS 서버나 메일 서버와 같이 외부에 공개되어 있어야만 하는 서버 이외에는 자세한 서버 목록을 확인할 수 없다.

```
> ls wishfree.com
*** Can't list domain wishfree.com: No response from server
The DNS server refused to transfer the zone wishfree.com to your computer. If this
is incorrect, check the zone transfer security settings for wishfree.com on the DNS
server at IP address 192.168.0.1.
```




```
> ls wishfree.com
[[192.168.0.1]]
 wishfree.com.          NS      server = wishfree_ws12
 db                     A       10.100.101
 was                    A       192.168.0.202
 web                    A       192.168.0.201
```