

<https://gleaming.notion.site/Chapter-02-95291429a29242c19a2dd71f4920c12c>

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

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

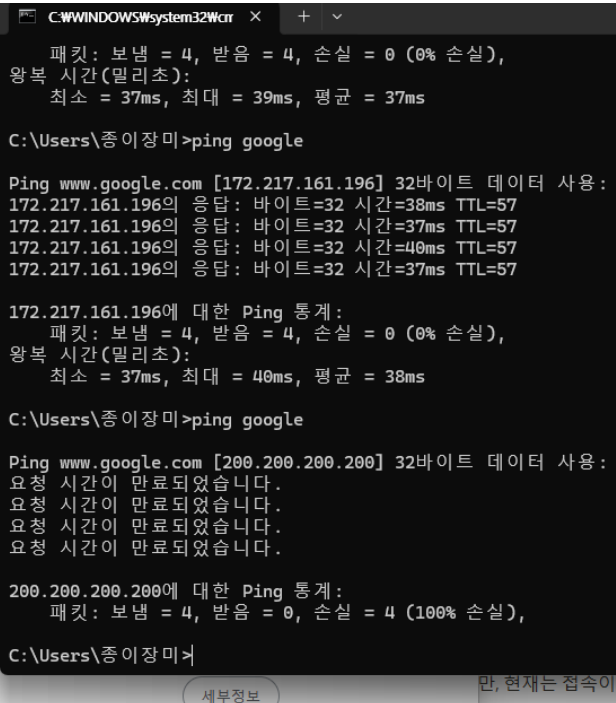
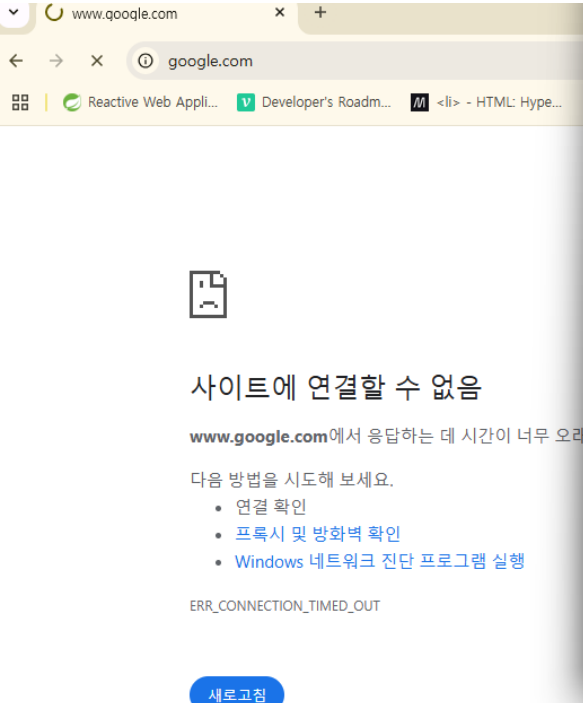
그래서 ping명령어가 google을 DNS에 묻지 않고 host파일에 지정한 IP로 바로 연결한 것임

3. 잘못된 주소를 등록하여 사이트 접속 차단

```
# For example:
#
# 102.54.94.97 rhino.acme.com # source 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
```

200.200.200.200 www.google.com google



```
C:\Users\종이장미>ping google

패킷 : 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
최소 = 37ms, 최대 = 39ms, 평균 = 37ms

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>ping google

Ping www.google.com [200.200.200.200] 32바이트 데이터 사용 :
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.
요청 시간이 만료되었습니다.

200.200.200.200에 대한 Ping 통계 :
패킷 : 보냄 = 4, 받음 = 0, 손실 = 4 (100% 손실),

C:\Users\종이장미>
```

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 때
문에 사이트가 막힌 것

google.com 을 강제로 매핑시킨것임

3. DNS 서버 검색 정보 수집

```
C:\> Administrator: C:\Windows\system32\cmd.exe - nslookup

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

> 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
          172.217.25.163
```

DNS 조회에 사용할 서버를 새로 지정함

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

```
> 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 = ns1.google.com
google.co.kr    nameserver = ns4.google.com
google.co.kr    nameserver = ns3.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 ns로 바꿈, ns 레코드를 조회하여 등록된 네임서버와 IP주소를 확인

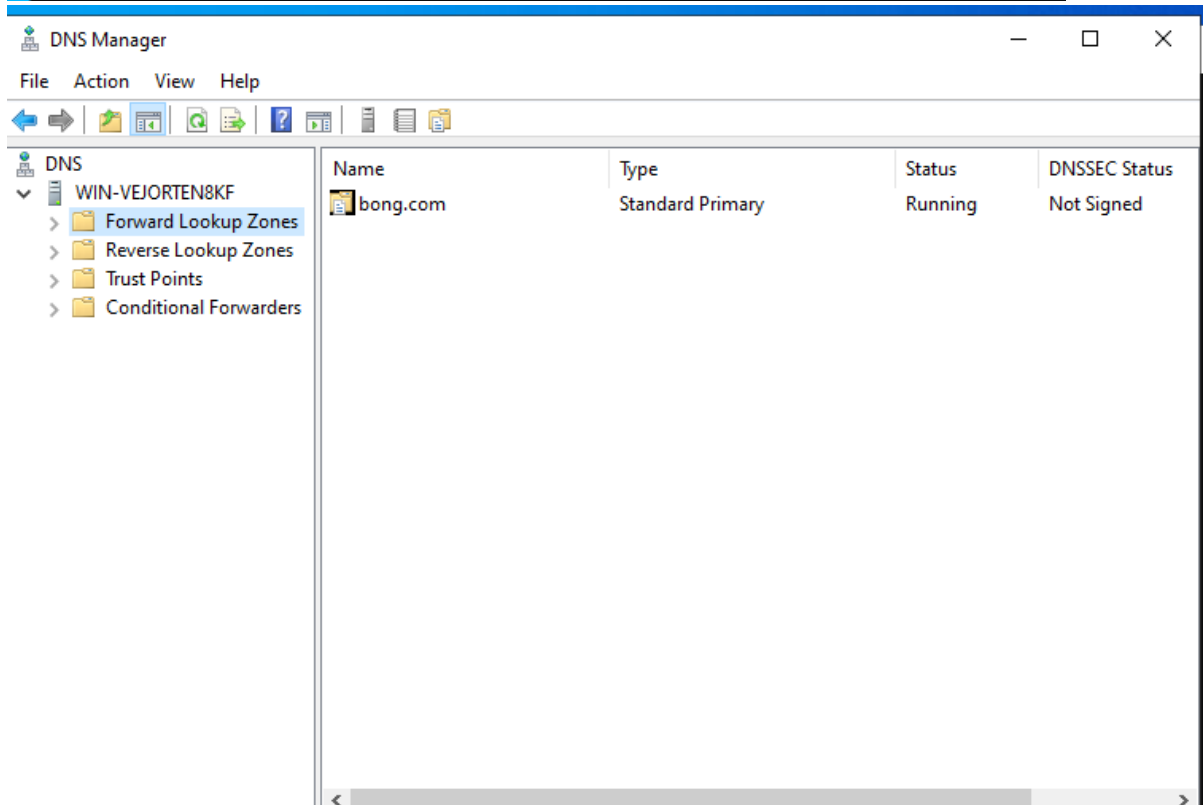
```

> 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.co.kr
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

```
PS C:\Users\종이장미> nslookup
기본 서버:  kns.kornet.net
Address:  168.126.63.1

> server 192.168.174.129
기본 서버:  [192.168.174.129]
Address:  192.168.174.129

> web.bong.com
서버:      [192.168.174.129]
Address:  192.168.174.129

이름:      web.bong.com
Address:  192.168.174.129

>
> db.bong.com
서버:      [192.168.174.129]
Address:  192.168.174.129

이름:      db.bong.com
Address:  192.168.174.130

>
> was.bong.com
서버:      [192.168.174.129]
Address:  192.168.174.129

이름:      was.bong.com
Address:  192.168.174.131
```

위에 사진대로 설정한 DNS로 매핑이 성공됨

```

> set type=all
> bong.com
서버 : [192.168.174.129]
Address: 192.168.174.129

bong.com          nameserver = win-vejorten8kf
bong.com
                primary name server = win-vejorten8kf
                responsible mail addr = hostmaster
                serial    = 4
                refresh  = 900 (15 mins)
                retry    = 600 (10 mins)
                expire   = 86400 (1 day)
                default TTL = 3600 (1 hour)
>

```

```

> ls bong.com
[[192.168.174.129]]
*** 도메인 bong.com을(를) 나열할 수 없습니다. Query refused
DNS 서버가 영역 bong.com을(를) 사용 중인 컴퓨터에 전송하는 것을 거부했습니다.
잘못된 경우에는 IP 주소 192.168.174.129의 DNS에서 bong.com의 영역 전송 보안 설정을
확인하십시오.

> ls bong.com
[[192.168.174.129]]
bong.com.      NS      server = win-vejorten8kf
db             A       192.168.174.130
was           A       192.168.174.131
web           A       192.168.174.129
>

```

처음에 레코드를 확인하려했는데 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 하려고 하면 필수적인 부분을 한 것임