Whois와 DNS 조사

IT융합공학부 윤세영

유투브 주소: https://youtu.be/wbUiOyZu4-w

Whois 서버에 대한 이해

Whois 서버란?

- 도메인과 관련된 사람과 인터넷 자원을 찾아보기 위한 프로토콜로 만들어졌다.
- Whois는 도메인 정보 확인을 위해 유용하게 쓰인다.

Whois 서버에서 얻을 수 있는 정보들

- 도메인 등록 및 관리 기관 정보
- 도메인 이름과 관련된 인터넷 자원 정보
- 목표 사이트의 네트워크 주소와 IP 주소
- 등록자, 관리자, 기술 관리자의 이름, 연락처, 이메일 계정
- 레코드의 생성 시기와 갱신 시기
- 주 DNS 서버와 보조 DNS 서버
- IP 주소의 할당 지역 위치

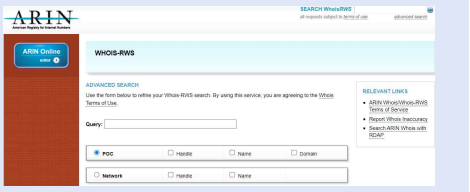
담당 지역	Whois 서버
전체	whois.internic.net
유럽	www.ripe.net
아시아 태평양 지역	www.apnic.net
	www.arin.net
호주	whois.aunic.net
프랑스	whois.nic.fr
일본	whois.nic.ad.jp
영국	whois.nic.uk
한국	whois.krnic.net
해커들을 위한 Whois	whois.greektoos.com

Whois 서버에 대한 이해

Whois 서버를 이용해 정보 획득하기 - Whois 서버 접속

- **Whois 서버를 이용하면 특정 URL의 소유자와 관리자 등의 정보를 얻을 수 있다.**
- **(실습환경) 인터넷이 연결된 클라이언트 시스템**

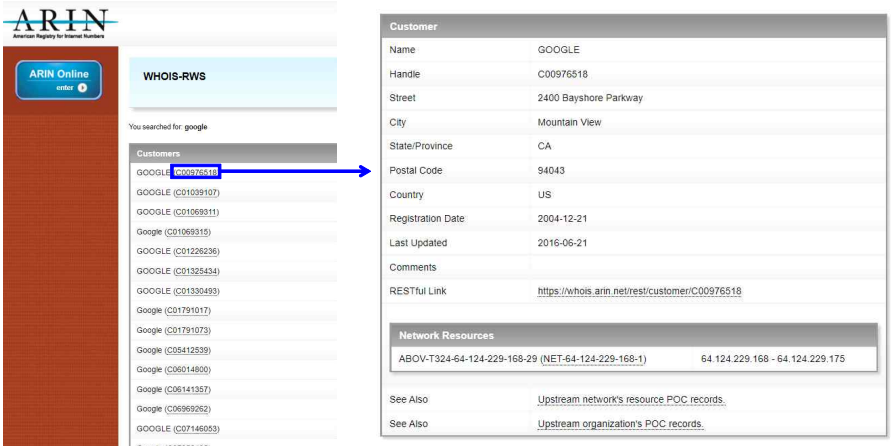
http://Whois.arin.net/ui/advanced.jsp



<whois.arin.net 서버의 Whois 쿼리 입력 화면>

Whois 서버에 대한 이해

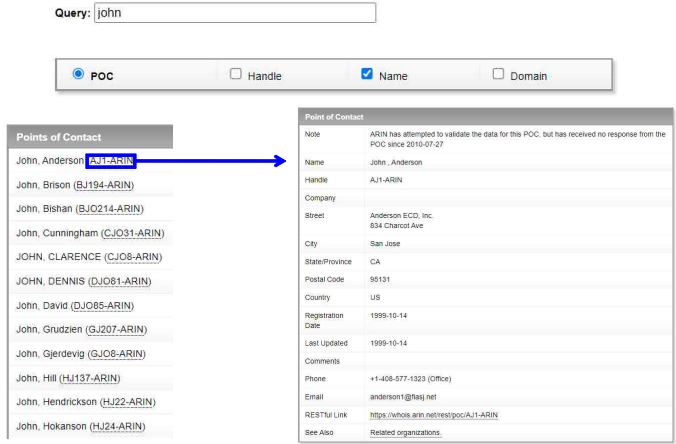
Whois 서버를 이용해 정보 획득하기 - 정보 획득 대상 확인



<whois.arin.net 서버에서 구글의 Whois 서버를 검색한 결과>

Whois 서버에 대한 이해

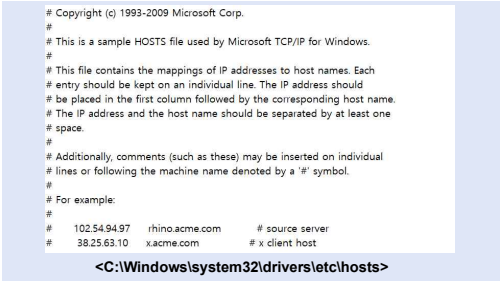
Whois 서버를 이용해 정보 획득하기 - 원하는 내용 검사



<john이라는 이름과 관련된 Whois 서버 정보>

hosts 파일에 대한 이해

hosts 파일이란?



```
# 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
```

<C:\Windows\system32\drivers\etc\hosts>

hosts 파일의 기본 구조

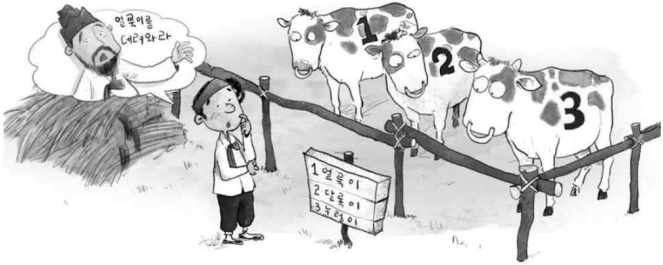
IP 주소	도메인 이름 또는 임의의 명칭

- **IP주소와 도메인을 매핑해주는 파일이다.**
- **도메인 이름이 될 수도 있지만, 아니어도 상관없다.**
- **'도메인 이름 또는 임의의 명칭'이 반드시 하나일 필요는 없다.**
- **'C:₩Windows₩System32₩drivers₩etc'에 위치한다.**
- **hosts 파일은 따로 확장자가 없으며, 메모장이나 코드 에디터를 통해 열 수 있다.**

DNS에 대한 이해

DNS란?

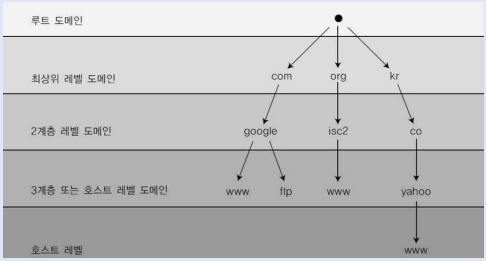
- **IP 주소를 도메인 이름으로 상호 매칭시켜주는 시스템이다.**
- **인터넷을 사용하는 동안 항상 사용하는 서비스로, 계층 구조를 이용한다.**



DNS에 대한 이해

DNS 계층 구조 및 두 번째 개체에 대한 내용

DNS의 계층 구조



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

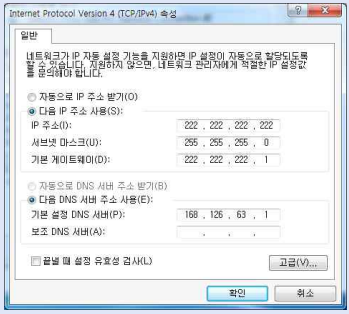
DNS의 동작 원리

DNS 서버 등록 및 현재 이용 중인 DNS 서버 확인

현재 이용 중인 DNS 서버는 'ipconfig /all' 명령으로 확인

```
C:₩Users₩     >ipconfig /all

Windows IP 구성

   호스트 이름 . . . . . . . . . . . . : DESKTOP-
   주 DNS 접미사 . . . . . . . . . . . :
   노드 유형 . . . . . . . . . . . . . : 혼성
   IP 라우팅 사용 . . . . . . . . . . . : 아니요
   WINS 프록시 사용 . . . . . . . . . . : 아니요

이더넷 어댑터 VirtualBox Host-Only Network:

   연결별 DNS 접미사 . . . . :
   설명 . . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   물리적 주소 . . . . . . . . . . . . : 0A-00-27-00-
   DHCP 사용 . . . . . . . . . . . . . : 아니요
   자동 구성 사용 . . . . . . . . . . . : 예
   링크-로컬 IPv6 주소 . . . . . : fe80::1aff:          (기본 설정)
   IPv4 주소 . . . . . . . . . . . . . : 192.          (기본 설정)
```

<'ipconfig /all' 명령으로 설정된 DNS 서버 확인하기>

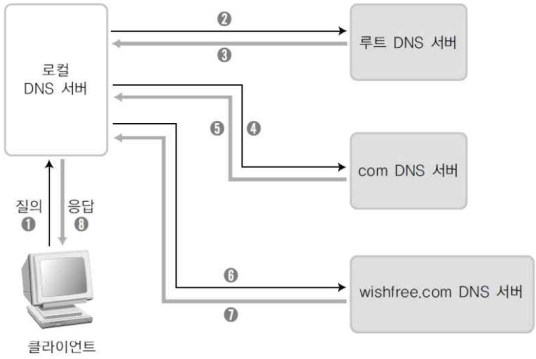


<인터넷 프로토콜(TCP/IP) 등록 정보>

출처: https://www.snoopybox.co.kr/1630

DNS의 동작 원리

DNS 서버의 이름 해석 순서

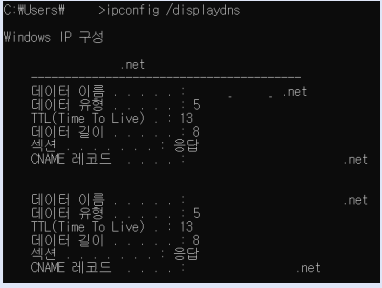


<DNS 서버로부터 해당 도메인 이름에 대한 IP 주소를 얻는 순서>

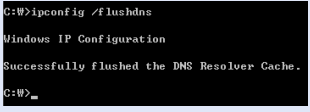
DNS의 동작 원리

(윈도우에서) 캐시된 DNS 정보 확인과 삭제

‘ipconfig /displaydns’로 캐시된 DNS 정보 확인



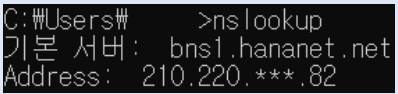
‘ipconfig /flushdns’로 캐시된 DNS 정보 삭제



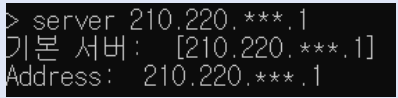
DNS를 이용한 정보 습득

nslookup 실행하고 DNS 설정하기

'nslookup' 명령 실행



조회 대상 DNS 서버 번경 (server *.***.***.***)**



DNS를 이용한 정보 습득

도메인 정보 수집하기

www.google.co.kr에 대한 nslookup

```
> www.google.co.kr
서버:    bns1.hananet.net
Address:  210.220.    .82

권한 없는 응답:
이름:    www.google.co.kr
Addresses:  2404:6800:400a:80e::2003
          172.217.161.227
```

www.google.co.kr의 DNS 서버 목록

```
> set type=ns
> google.co.kr
서버:    bns1.hananet.net
Address:  210.220.    .82

권한 없는 응답:
google.co.kr    nameserver = ns2.google.com
google.co.kr    nameserver = ns3.google.com
google.co.kr    nameserver = ns1.google.com
google.co.kr    nameserver = ns4.google.com
```

DNS를 이용한 정보 습득

DNS 레코드의 종류

DNS 레코드 종류		내용
A	Address	호스트 이름 하나에 IP 주소가 여러 개 있을 수 있으며, IP 주소 하나에 호스트 이름이 여러 개 있을 수 있다. 이때 이를 정의하는 레코드 유형이다. 다음과 같이 정의된다. 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	각 도메인에 적어도 한 개 이상 있어야 하며, DNS 서버를 가리킨다.
MX	Mail Exchanger	도메인 이름으로 보낸 메일을 받는 호스트 목록을 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.

google.co.kr에 등록된 모든 DNS 레코드

```
> set type=all
> google.co.kr
서버:   bns1.hananet.net
Address:  210.220.   .82

권한 없는 응답:
google.co.kr
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 500367442
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
google.co.kr    MX preference = 0, mail exchanger = smtp.google.com
google.co.kr    ??? unknown type 257 ???
google.co.kr    text =

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

Q & A