

네트워크 정보 수집

01_Whois 서버와 hosts 파일- Whois 서버에 대한 이해

❖ Whois(후이즈)

- 1984년에 만들어진 도메인 확인, 도메인과 관련된 사람 및 인터넷 자원을 찾아 보기 위한 프로토콜
- 초기에는 와일드카드(*) 문자열로 관련 도메인 검색이 가능했으나, 인터넷이 상업화되고 스팸 메일이 증가함에 따라 기능 삭제

❖ Whois 서버로 얻을 수 있는 정보 (도메인 정보 확인을 위해 유용하게 사용)

- 도메인 등록 및 관련 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

01_Whois 서버와 hosts 파일 - Whois 서버에 대한 이해

❖ Whois 서버 목록

- 도메인을 등록하면 각 지역별 Whois 서버에 등록됨.

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

01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우 7)

① Whois 서버 접속하기

- <http://Whois.arin.net/ui/advanced.jsp>에서 Whois 서버 검색 가능

The screenshot shows the ARIN WHOIS-RWS Advanced Search interface. The search query 'google' is entered in the 'Query' field. The 'Customer' radio button is selected, and the 'Name' checkbox is checked. Other search options like POC, Network, ASN, Organization, Delegation, Handle, and Number are available but not selected. A 'Submit' button is at the bottom. The right sidebar contains links to ARIN WHOIS terms of service, reporting inaccuracies, API documentation, technical discussion mailing lists, and sample stylesheets.

01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

② 정보 획득 대상 확인하기

- 여러 네트워크와 서버 확인 가능

'C00975227' 클릭

Customer

Name	Handle	Street	City	State/Province	Postal Code	Country	Registration Date	Last Updated	Comments	RESTful Link
GOOGLE	C00975227	2400 Bayshore Parkway	Mountain View	CA	00000	US	2004-12-18	2011-03-19		https://whois.arin.net/rest/customer/C00975227

Network Resources

ABOVE-T324-64-124-112-24-29 (NET-64-124-112-24-1)	64.124.112.24 - 64.124.112.31
See Also	Upstream network's resource POC records.
See Also	Upstream organization's POC records.

01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

② Whois 서버로 원하는 내용 검사하기

The screenshot shows a web browser window with the ARIN Whois-RWS search interface. The URL is whois.arin.net/ui/advanced.jsp. The search query 'john' is entered in the 'Query:' field, which is highlighted with a red box. Below the query, there is a search refinement section with radio buttons for 'POC', 'Handle', 'Name', and 'Domain'. The 'Name' radio button is selected and highlighted with a red box. The search results for 'john' are displayed under the heading 'Points of Contact', listing several entries such as 'John, Adams (JOHNA22-ARIN)', 'John, Ame (JOHNA26-ARIN)', etc. On the right side of the page, there is a sidebar with 'RELEVANT LINKS' containing links to ARIN Whois/RWS Terms of Service, Report Whois Inaccuracy, Whois-RWS API Documentation, ARIN Technical Discussion Mailing List, and Sample stylesheet (xsl). The background of the main search area has a yellow banner with the text 'John 이라는 사람이 등록한 사이트를 알아보려면...'.

01_Whois 서버와 hosts 파일- whois 도메인 정보 조회

<https://xn--c79as89aj0e29b77z.xn--3e0b707e/kor/main.jsp>

The screenshot shows the KISA WHOIS search results for the domain 'naver.com'. The search bar at the top contains 'kisa.or.kr'. Below it, there are two sections: '도메' (Domain) showing 'naver.com' with sub-domains 'kis' and 'naver', and 'IP주소' (IP Address) showing '202.30.50.51 | 2001:02B8::/32 | AS9700'. To the right, there's a sidebar titled '공지사항' (Announcements) listing various system check and migration notices with their dates. Below that is a section for 'WHOIS 주요 서비스' (WHOIS Main Services) featuring links to WHOIS services, WHOIS OpenAPI, WHOIS 접근거부 조회 (WHOIS Blocklist Inquiry), and IP주소 추적에 관한 오해 (Misunderstanding about IP address tracking). At the bottom, there are links for '개인정보 처리방침' (Privacy Policy), '이메일 무단 수집 거부' (Email spam prevention), 'RSS', '해킹·스팸 개인정보침해 신고는 118' (Report hacking/spam personal information abuse to 118), 'KISA SNS 바로가기' (KISA SNS Direct Link) with icons for Twitter, Facebook, and YouTube, and contact information for various offices.

https://후이즈검색.한국/kor/main.jsp

ENGLISH | 대국민서비스 바로가기

KISA 한국인터넷진흥원

WHOIS

국가 인터넷주소관리기관인 한국인터넷진흥원은
안정적인 인터넷주소관리로 세계 최고의 인터넷 환경을 만들어 갑니다.

SEARCH

도메 naver.com

- kis
- naver

IP주소 202.30.50.51 | 2001:02B8::/32 | AS9700

WHOIS 서비스란?
WHOIS OpenAPI
WHOIS 접근거부 조회
IP주소 추적에 관한 오해

국가도메인 부가서비스

개인정보 처리방침 이메일 무단 수집 거부 RSS 해킹·스팸 개인정보침해 신고는 118 KISA SNS 바로가기

[나주청사] (58324) 전라남도 나주시 진출길 9 한국인터넷진흥원
[서울청사] (05717) 서울시 송파구 중대로 135 (가락동) IT벤처타워
[분원(서초사무소)] (06619) 서울시 서초구 서초로 398 (서초2동) 플래티넘타워
Copyright(C) 2016 KISA. All rights reserved.

TEL : 1544-5118
TEL : 02)405-5118
TEL : 02)405-5118

01_Whois 서버와 hosts 파일- whois 도메인 정보 조회

The screenshot shows a web browser window displaying the KISA WHOIS search results for the domain 'naver.com'. The URL in the address bar is <https://후이즈검색.한국/kor/whois/whois.jsp>. The page has a header 'WHOIS 조회' and a sidebar 'WHOIS 서비스' with options like 'WHOIS 주요 서비스', '국가도메인 부가서비스', '한글-퓨니코드 번역', and '공지사항'. The main content area shows the WHOIS record for 'naver.com' with details such as Domain Name: NAVER.COM, Registry Domain ID: 793803_DOMAIN_COM-VRSN, Registrar WHOIS Server: whois.gabia.com, Registrar URL: http://www.gabia.com, Updated Date: 2016-08-05T06:37:57Z, Creation Date: 1997-09-12T04:00:00Z, Registry Expiry Date: 2023-09-11T04:00:00Z, Registrant: Gabia, Inc., Registrar IANA ID: 244, Registrar Abuse Contact Email: gabia@naver.com, Registrar Abuse Contact Phone: +82-2-515-0000, Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited, Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited, Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited, Name Server: NS1.NAVER.COM, Name Server: NS2.NAVER.COM, DNSSEC: unsigned, URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/. The page also includes a notice about expiration dates and terms of use.

KISA
한국인터넷진흥원

WHOIS 조회

WHOIS 서비스

naver.com

SEARCH

아래 결과는 다른 Registry(등록기관)의 WHOIS 서버에서 조회한 결과입니다.

QUERY:naver.com

Domain Name: NAVER.COM
Registry Domain ID: 793803_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gabia.com
Registrar URL: http://www.gabia.com
Updated Date: 2016-08-05T06:37:57Z
Creation Date: 1997-09-12T04:00:00Z
Registry Expiry Date: 2023-09-11T04:00:00Z
Registrant: Gabia, Inc.
Registrar IANA ID: 244
Registrar Abuse Contact Email: gabia@naver.com
Registrar Abuse Contact Phone: +82-2-515-0000
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.NAVER.COM
Name Server: NS2.NAVER.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-10-23T11:44:45Z <<

For more information on Whois status codes, please visit <https://icann.org/epp>.

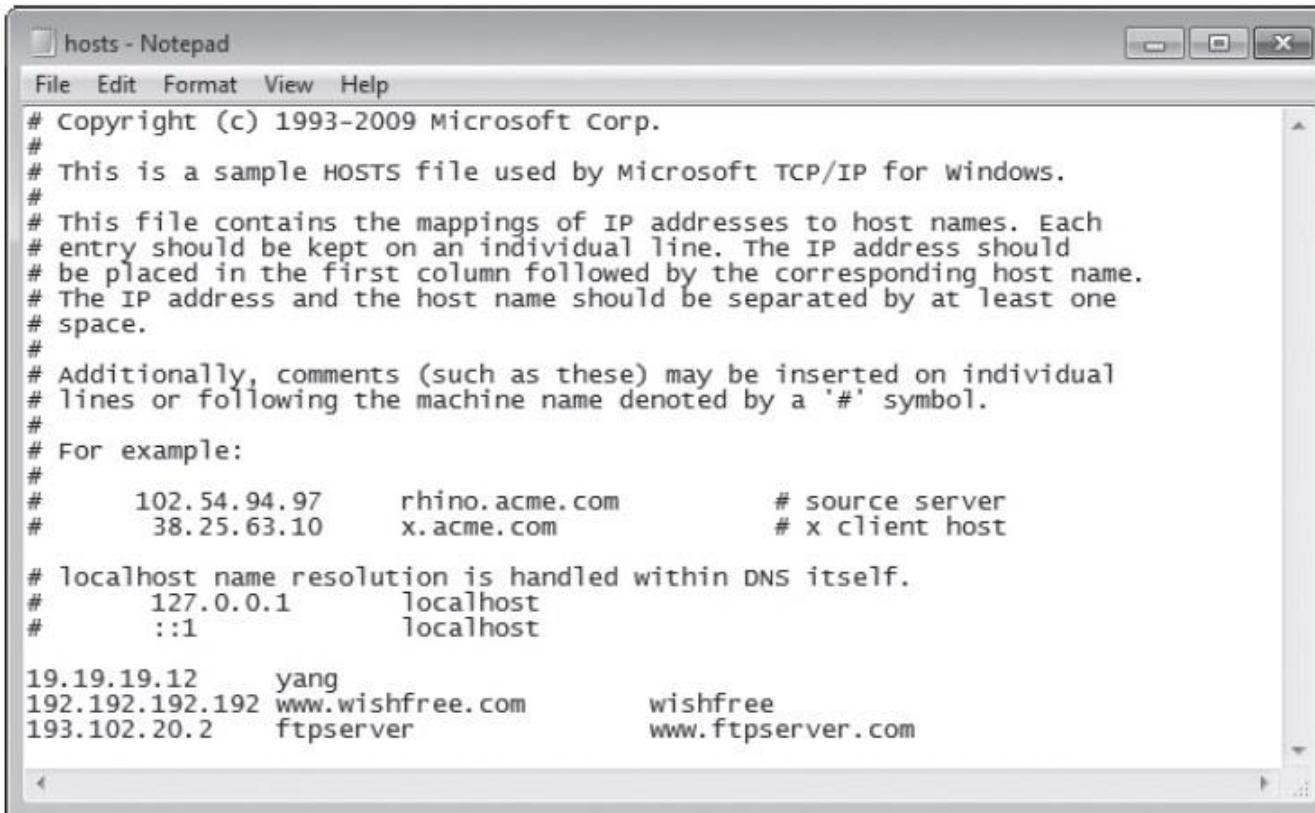
NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass

01_Whois 서버와 hosts 파일 - hosts 파일에 대한 이해

❖ Hosts 파일

- DNS가 존재하기 전에 사용했고, 지금도 목적에 따라 많이 사용하고 있음.
- 윈도우 계열 시스템은 (윈도우 운영체제 설치 디렉토리) \ system32 \ drivers \ etc \ hosts, 리눅스는 /etc/hosts가 이에 해당



The screenshot shows a Windows Notepad window titled "hosts - Notepad". The file contains the following text:

```
# 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  
  
19.19.19.12      yang  
192.192.192.192 www.wishfree.com      wishfree  
193.102.20.2     ftpserver           www.ftpserver.com
```

01_Whois 서버와 hosts 파일- hosts 파일에 대한 이해

❖ Hosts 파일

IP 주소

도메인 이름 또는 임의의 명칭

- 보통 hosts 파일은 비어 있음.
- DNS 서버가 작동하지 않을 때, 별도의 네트워크를 구성하여 임의로 사용할 때, 다른 IP 주소를 가진 여러 대의 서버가 같은 도메인으로 클러스터링(Clustering)되어 운영되는 상태에서 특정 서버에 접속하고자 할 때 유용
- 잘못된 hosts 파일은 서버 접속 자체를 막을 수도 있다.

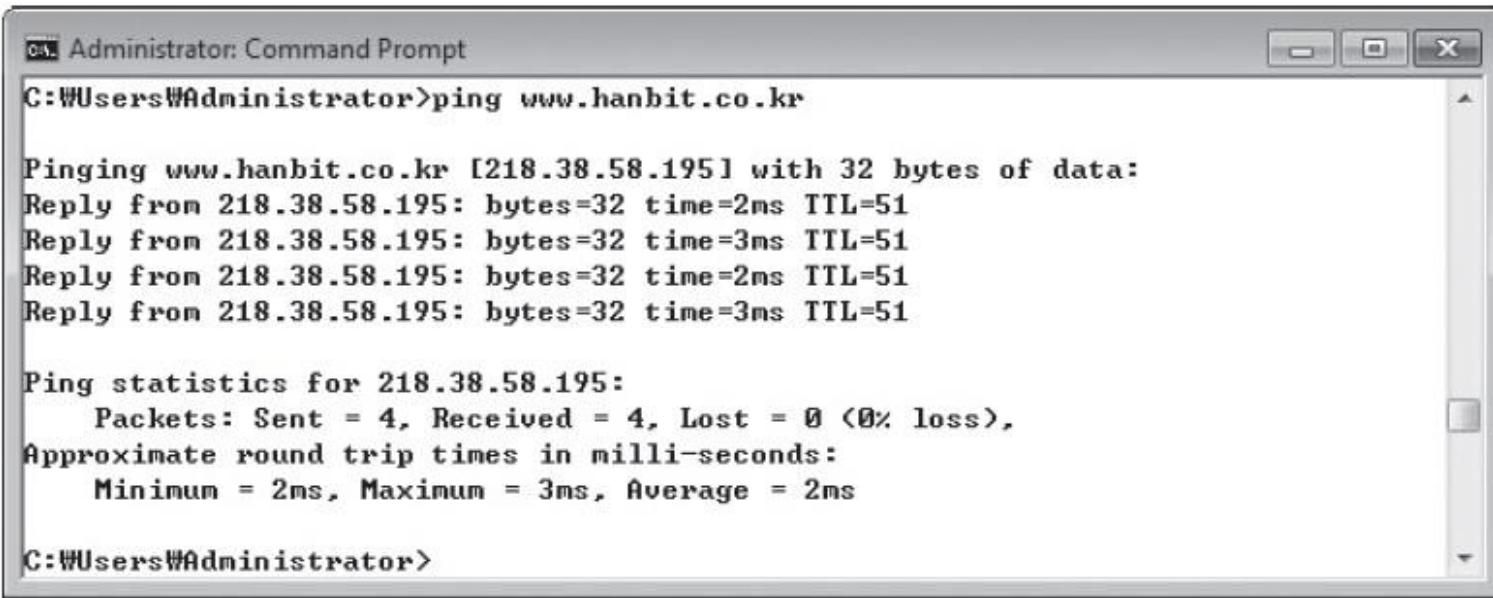
- Hosts 파일의 각 행 앞에 #으로 표시된 것은 주석
- 'IP주소'와 '도메인 이름 또는 임의의 명칭'은 Tab 또는 뛰어 쓰기로 구분

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우 7)

① 도메인 등록하기

ping www.hanbit.co.kr



```
Administrator: Command Prompt
C:\Users\Administrator>ping www.hanbit.co.kr

Pinging www.hanbit.co.kr [218.38.58.195] with 32 bytes of data:
Reply from 218.38.58.195: bytes=32 time=2ms TTL=51
Reply from 218.38.58.195: bytes=32 time=3ms TTL=51
Reply from 218.38.58.195: bytes=32 time=2ms TTL=51
Reply from 218.38.58.195: bytes=32 time=3ms TTL=51

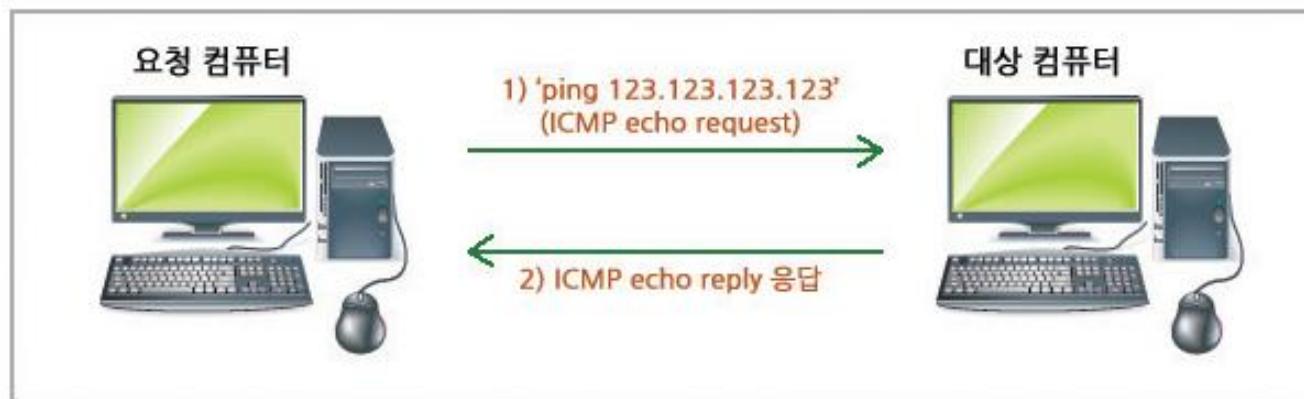
Ping statistics for 218.38.58.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Administrator>
```

#_ping 명령어

ping(Packet Internet Groper), 네트워크 상태를 점검하는 가장 간단한 명령어

ping 명령어의 기본적인 작동 원리는 그다지 복잡하지 않다. 네트워크 상태를 확인하려는 대상(target) 컴퓨터(또는 네트워크 기기)를 향해 일정 크기의 패킷(packet, 네트워크의 최소 전송단위)을 보낸 후(ICMP echo request), 대상 컴퓨터가 이에 대해 응답하는 메시지(ICMP echo reply)를 보내면 이를 수신, 분석하여 대상 컴퓨터가 작동하는지, 또는 대상 컴퓨터까지 도달하는 네트워크 상태가 어떠한지 파악할 수 있다.



#_ping 명령어

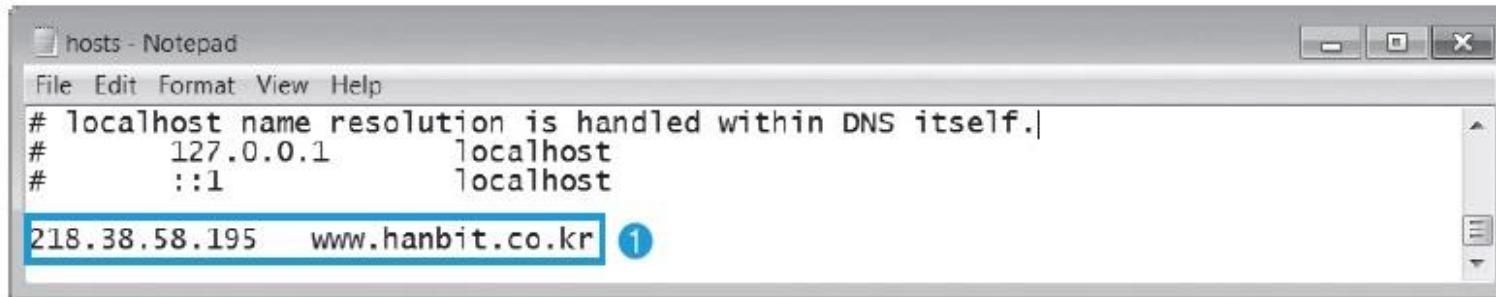
ping 명령어는 MS 윈도우 계열 운영체제에서는 '명령 프롬프트(보조프로그램 내)'를 통해, 리눅스/유닉스 계열 운영체제에서는 터미널 모드를 통해 실행할 수 있다. ping 명령어 바로 뒤에(공백 필요) 대상 컴퓨터의 IP 주소나 웹 사이트 등의 도메인 이름을 입력하면 된다.

구 분	내 용
-t	Ctrl + C 로 중단시키기 전까지 계속 ping 패킷을 보낸다.
-a	도메인네임의 IP 주소를 보여준다.
-n <i>count</i>	Ping 패킷을 몇 번 보낼지 패킷 수를 지정한다. (기본 4회)
-l <i>size</i>	Ping 패킷 크기를 지정한다. (기본 32비트)
-f	요구 패킷이 라우터 등을 통과할 경우, 나누어지지 않게 한다.
-i <i>TTL</i>	사용할 TTL 값을 설정한다. (TTL은 라우터 하나를 거칠 때마다 1씩 값이 감소한다.(초기값 255))
-v <i>TOS</i>	패킷의 TOS를 지정하는 값으로 설정한다. (TOS는 IP 패킷 헤더에 포함되는 필드의 하나로 QoS를 제어하기 위해 라우터의 패킷 우선순위를 지정하는 것이다.)
-r <i>count</i>	Count에 지정한 값만큼 라우터의 경로를 보여준다. (최대 9개)
-s <i>count</i>	Count에 지정한 값만큼 라우터의 주소와 시간을 기록한다. (최대 4개)
-j <i>host-list</i>	리스트의 컴퓨터를 통해서 패킷의 경로를 정할 수 있다. (최대 9개)
-k <i>host-list</i>	J와 같은 역할을 하지만 연속적인 컴퓨터의 경우, 중간 게이트를 구분할 수 없다.
-w <i>timeout</i>	대상 호스트의 응답을 기다리는 시간을 지정한다. (시간 단위는 밀리세컨드로 한다. (기본 4초))

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

① 도메인 등록하기

- C:\Windows\system32\drivers\etc\hosts 파일을 열어 해당 도메인 등록
218.38.58.195 www.hanbit.co.kr hanbit



```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1      localhost
#       ::1            localhost
218.38.58.195    www.hanbit.co.kr ①
```

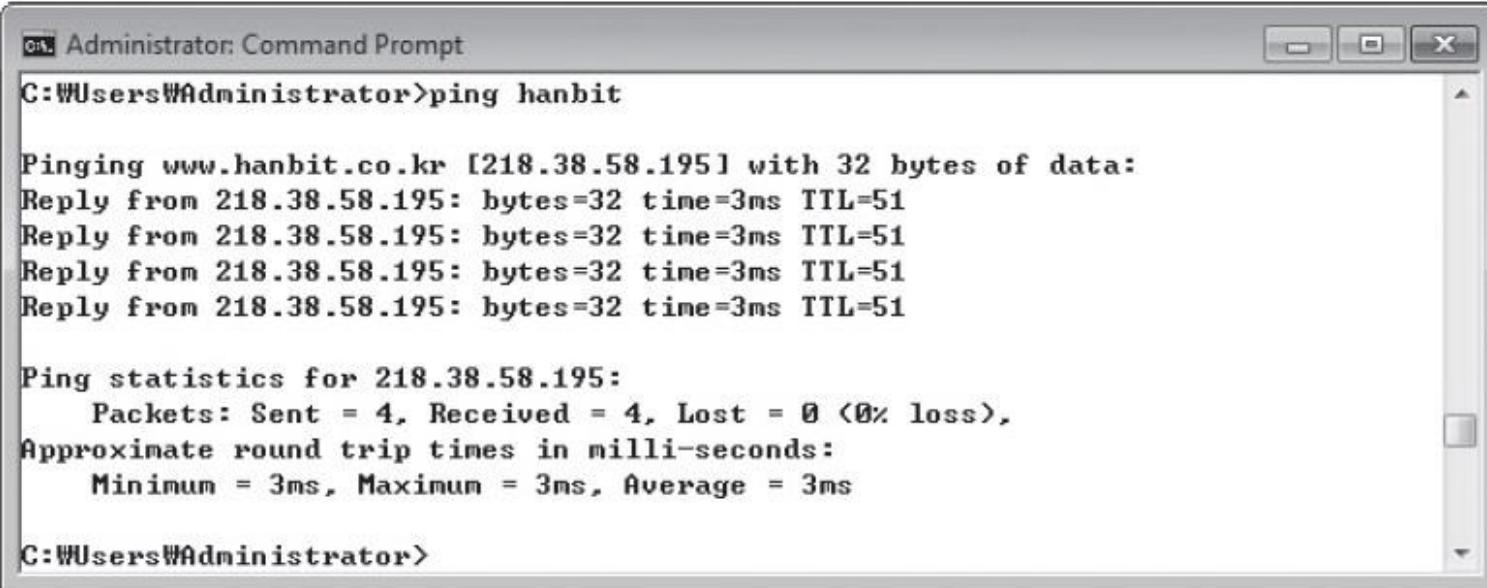


```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1      localhost
#       ::1            localhost
218.38.58.195    www.hanbit.co.kr    hanbit②
```

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

② Hosts 파일 동작 확인하기

ping hanbit



```
C:\Administrator>ping hanbit

Pinging www.hanbit.co.kr [218.38.58.195] with 32 bytes of data:
Reply from 218.38.58.195: bytes=32 time=3ms TTL=51

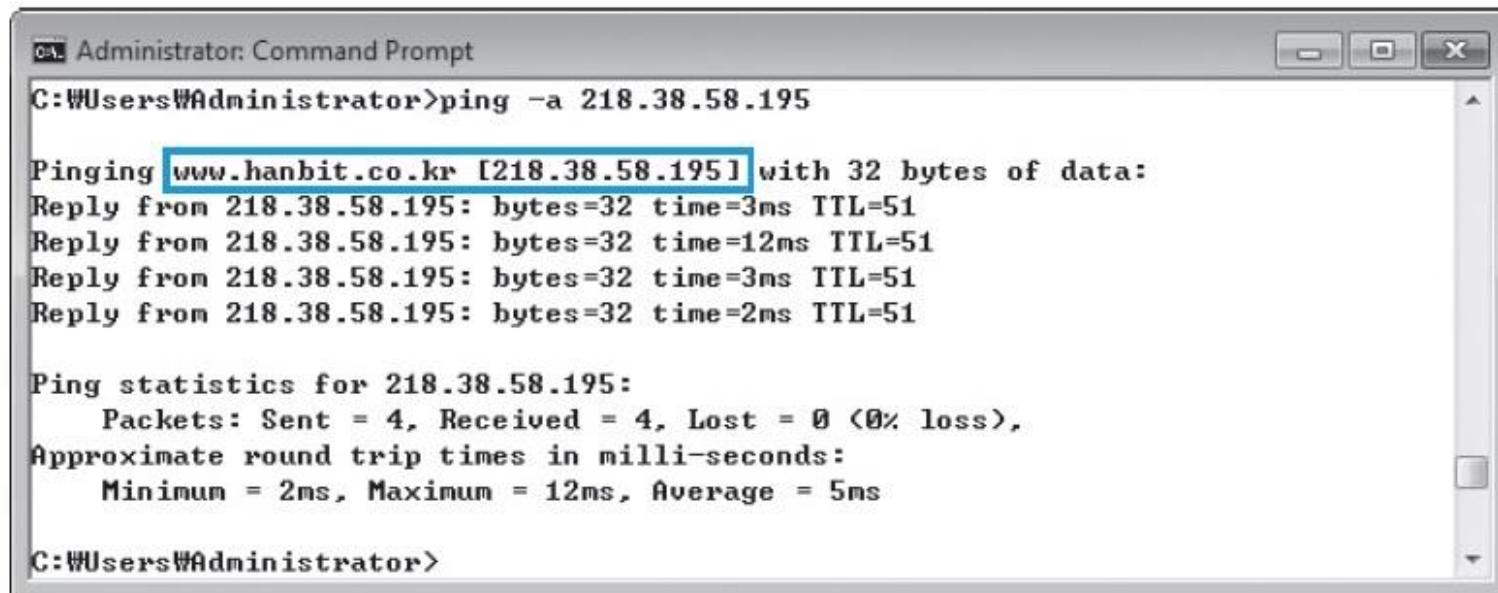
Ping statistics for 218.38.58.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Administrator>
```

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

② Hosts 파일 동작 확인하기

ping -a 218.38.58.195



```
Administrator: Command Prompt
C:\Users\Administrator>ping -a 218.38.58.195

Pinging www.hanbit.co.kr [218.38.58.195] with 32 bytes of data:
Reply from 218.38.58.195: bytes=32 time=3ms TTL=51
Reply from 218.38.58.195: bytes=32 time=12ms TTL=51
Reply from 218.38.58.195: bytes=32 time=3ms TTL=51
Reply from 218.38.58.195: bytes=32 time=2ms TTL=51

Ping statistics for 218.38.58.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 5ms

C:\Users\Administrator>
```

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

③ 잘못된 주소를 등록하여 사이트 접속 차단하기

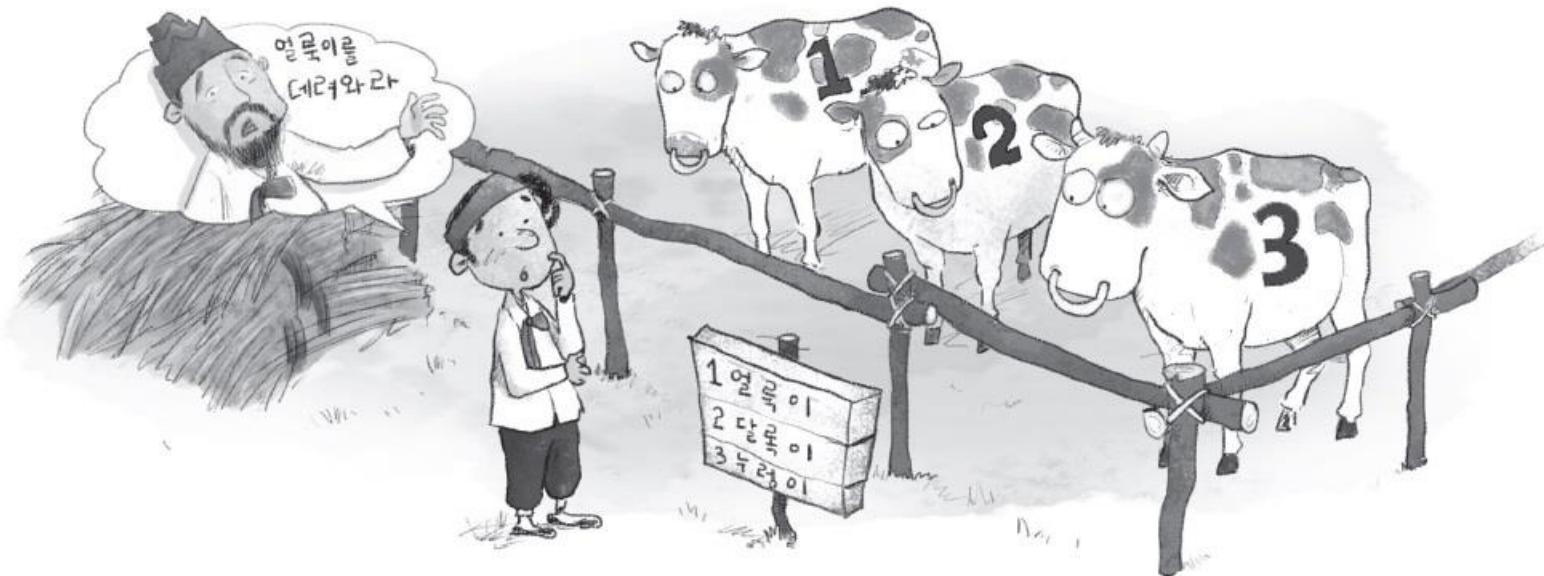
200.200.200.200 www.hanbit.co.kr



02_DNS- DNS에 대한 이해

❖ DNS(Domain Name System)

- 숫자로 구성된 네트워크 주소인 IP 주소를 사람이 이해하기 쉬운 명칭인 도메인 이름으로 상호 매칭시켜주는 시스템



주인: 인터넷 사용자 / 하인: 웹 브라우저 / 풋말: DNS서버 / 소: 웹 사이트

02_DNS - DNS에 대한 이해

❖ DNS의 계층 구조

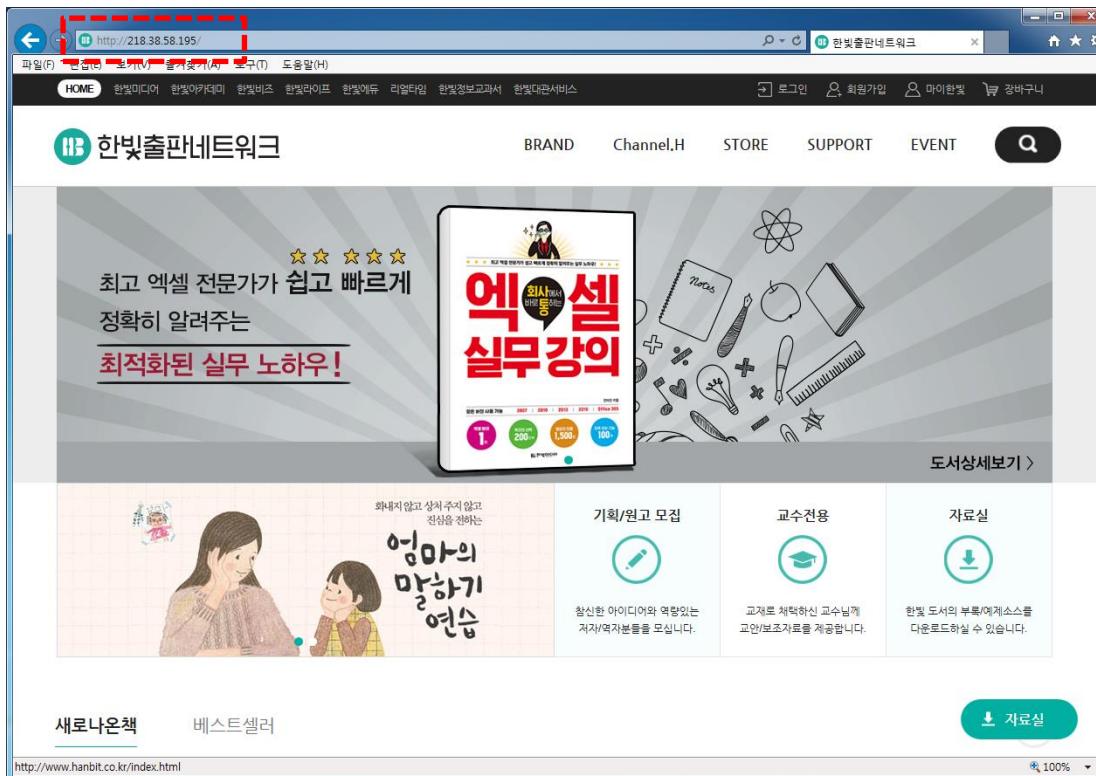
- 가장 상위 개체는 '.' (Root)
- 두 번째 개체는 국가와 조직체의 특성
- 보통 맨 앞은 자신의 DNS 서버에서 지정해놓은 www, ftp와 같은 특정 서버의 이름이 옴.
- FQDN(Fully Qualified Domain Name) : 완성된 주소(예 : www.wishfree.co.kr)

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

02_DNS - DNS에 대한 이해

❖ DNS 서버의 개념

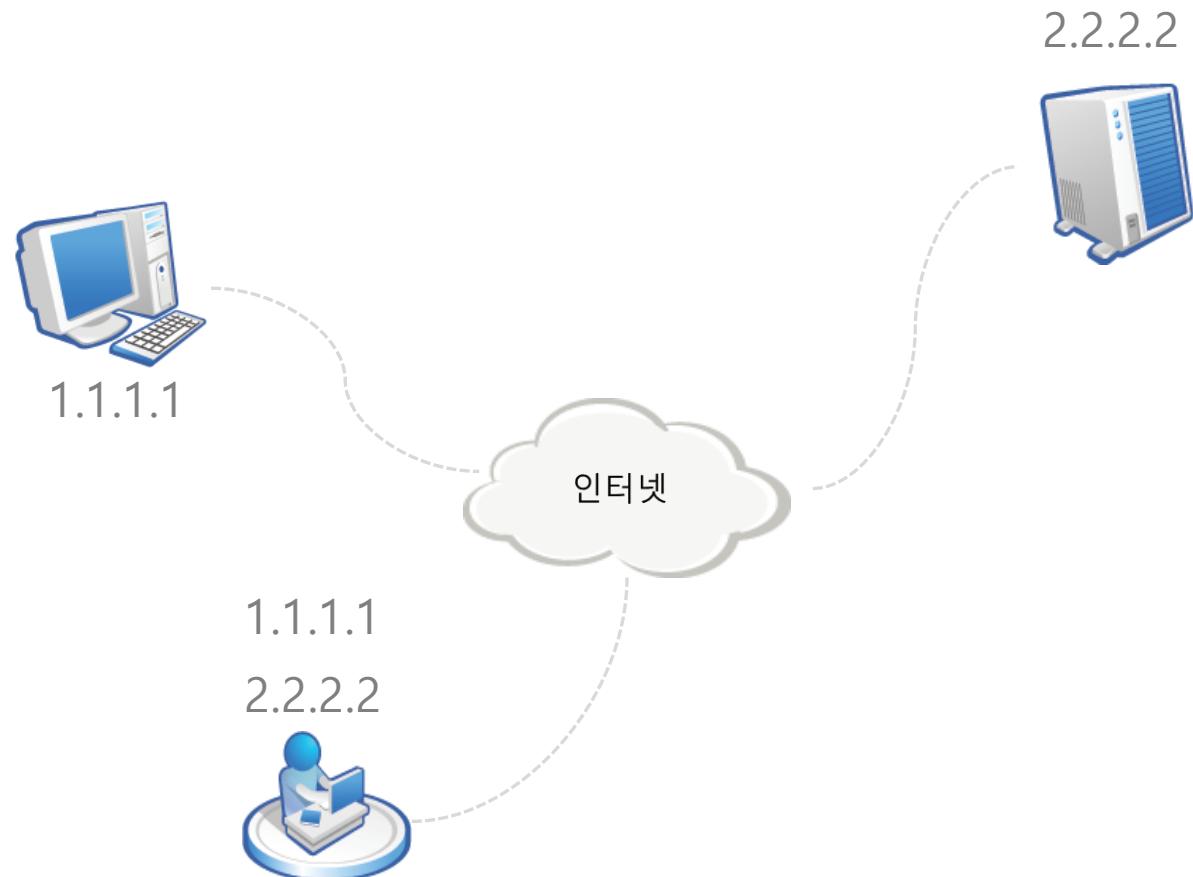
- DNS(Domain Name System) = 네임(Name) 서버
- 도메인 이름을 IP 주소로 변환시켜 주는 역할 = 이름 해석 (name resolution)
- 예) www.hanbit.co.kr → 218.38.58.195



02_DNS - DNS에 대한 이해

❖ DNS 서버의 개념

- 가장 초기의 네트워크 접속 방법
 - 컴퓨터가 몇 대 안됨
 - 사용자가 모두 외워서 직접 IP주소로 접근함

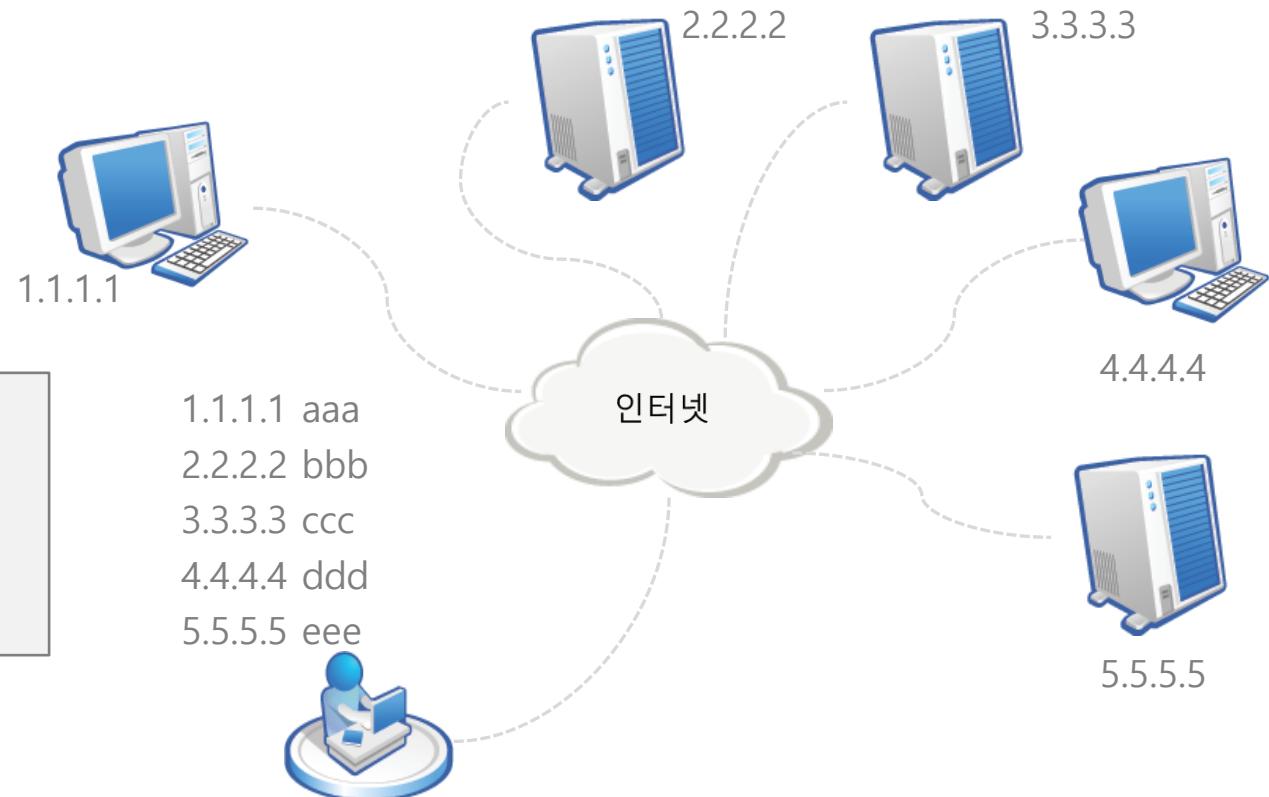


02_DNS - DNS에 대한 이해

❖ DNS 서버의 개념

- Hosts 파일을 이용하여 네트워크 접속
 - 인터넷에 연결된 컴퓨터가 수십 ~ 수백대로 늘어남
 - C:\Windows\system32\drivers\etc\hosts 파일에 URL과 IP주소를 기록해 놓는 방식 사용

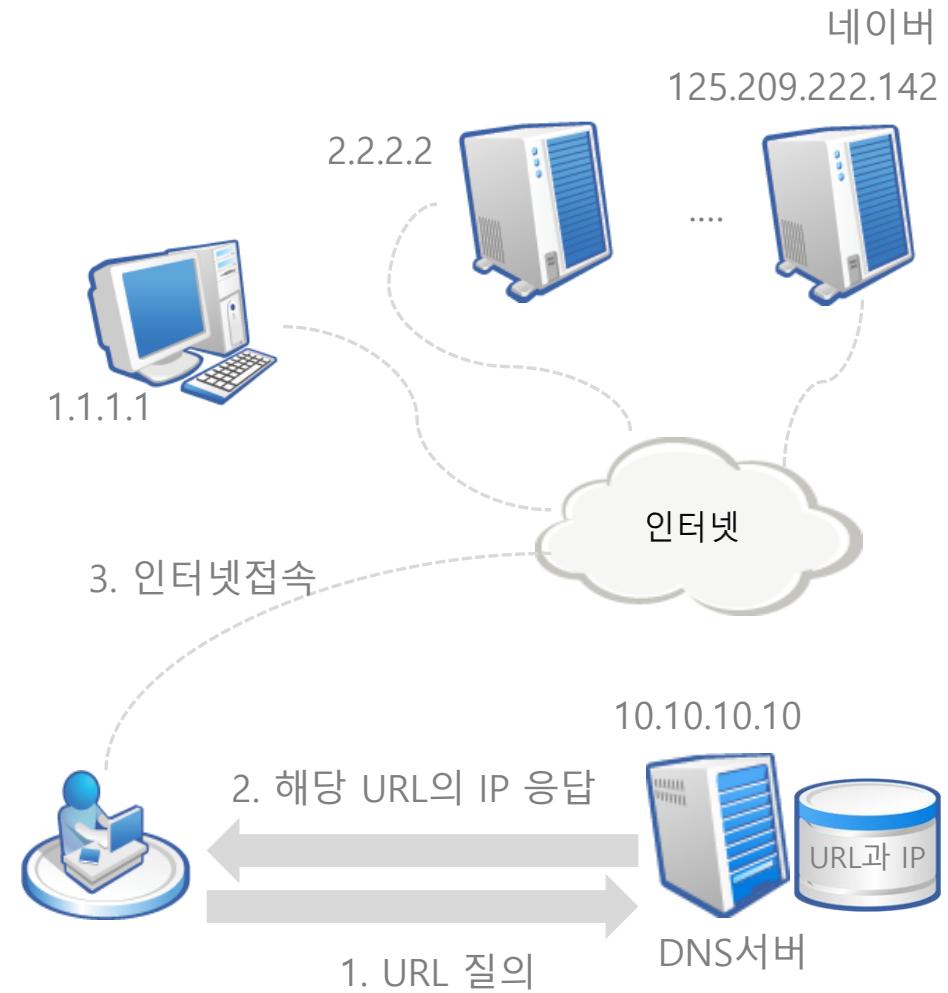
102.54.94.97	rhino.acme.com
38.25.63.10	x.acme.com
222.122.195.5	www.naver.com
127.0.0.1	localhost



02_DNS - DNS에 대한 이해

❖ DNS 서버의 개념

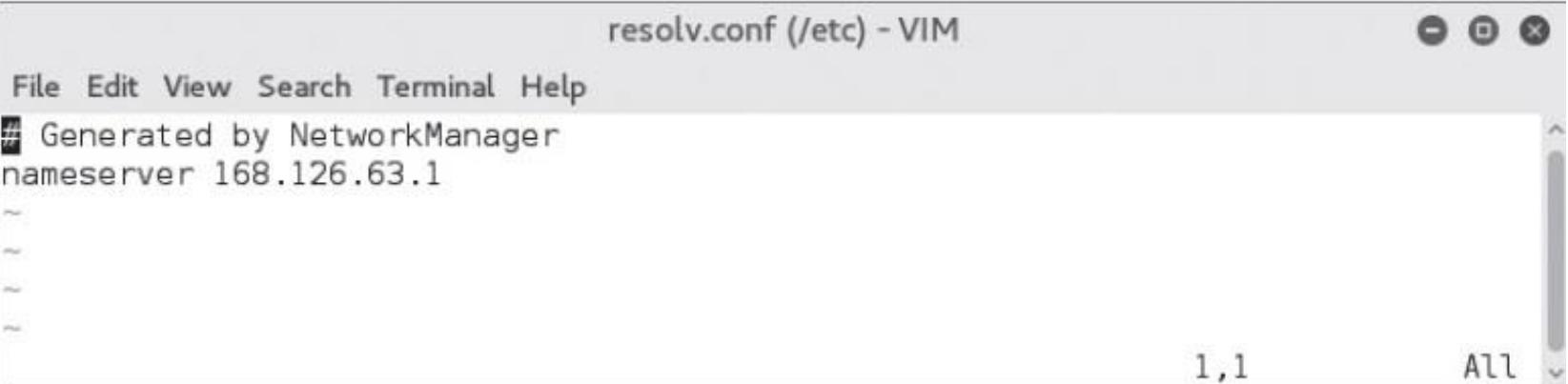
- DNS 서버를 이용하여 네트워크 접속
 - 기하급수적으로 늘어나는 네트워크 상의 컴퓨터에 대한 모든 IP정보를 파일 하나에 기록하는 것은 무리
 - 이를 해석(name resolution)을 전문적으로 해주는 서버 컴퓨터가 필요(=DNS 서버)
 - 전화 안내 서비스인 114와 같은 역할
 - DNS서버는 인터넷에 변화하는 모든 컴퓨터의 URL과 IP정보를 거의 실시간으로 제공하므로, 사용자는 더 이상 URL에 해당하는 IP주소를 신경 쓸 필요가 없어짐
 - URL만 알고 있으면 어디서든지 해당하는 컴퓨터 접속



02_DNS - DNS의 동작 원리

❖ 운영체제별 DNS 서버 등록

- 리눅스 : /etc/resolv.conf 파일에 DNS 서버를 입력



The screenshot shows a terminal window titled "resolv.conf (/etc) - VIM". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. Below the title bar is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main content area displays the contents of the /etc/resolv.conf file:

```
# Generated by NetworkManager
nameserver 168.126.63.1
```

At the bottom right of the editor window, there are status indicators showing "1,1" and "All".

02_DNS- DNS의 동작 원리

❖ 운영체제별 DNS 서버 등록

- 윈도우 : 인터넷 프로토콜(TCP/IP) 등록 정보에서 DNS 서버 두 개까지 입력
- <고급(Advanced)> 버튼을 누르면 좀 더 다양한 설정도 가능

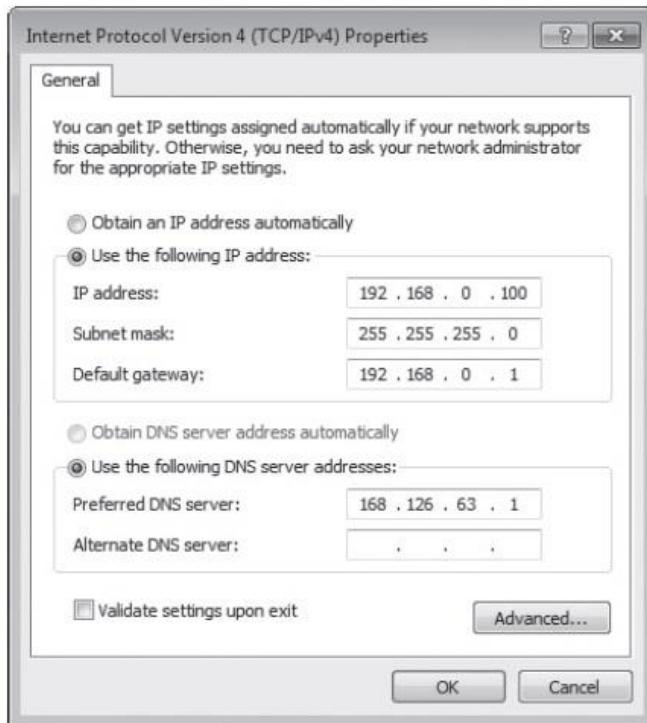


그림 3-14 인터넷 프로토콜(TCP/IP) 등록 정보

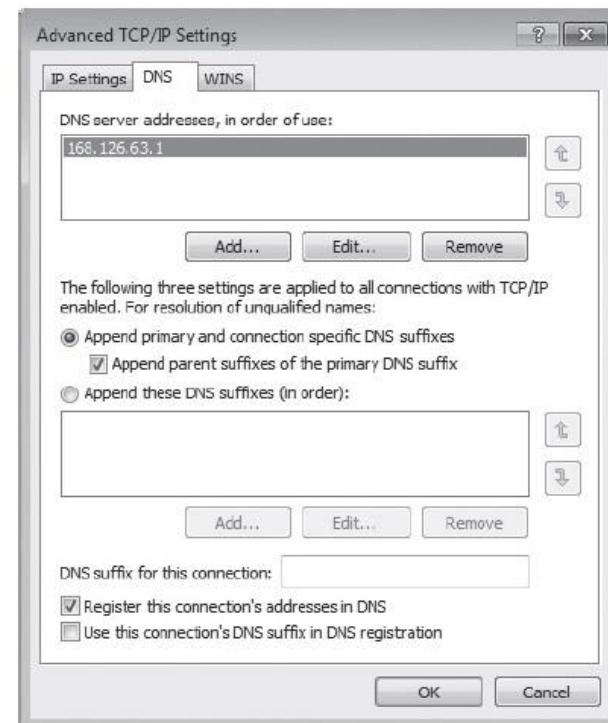
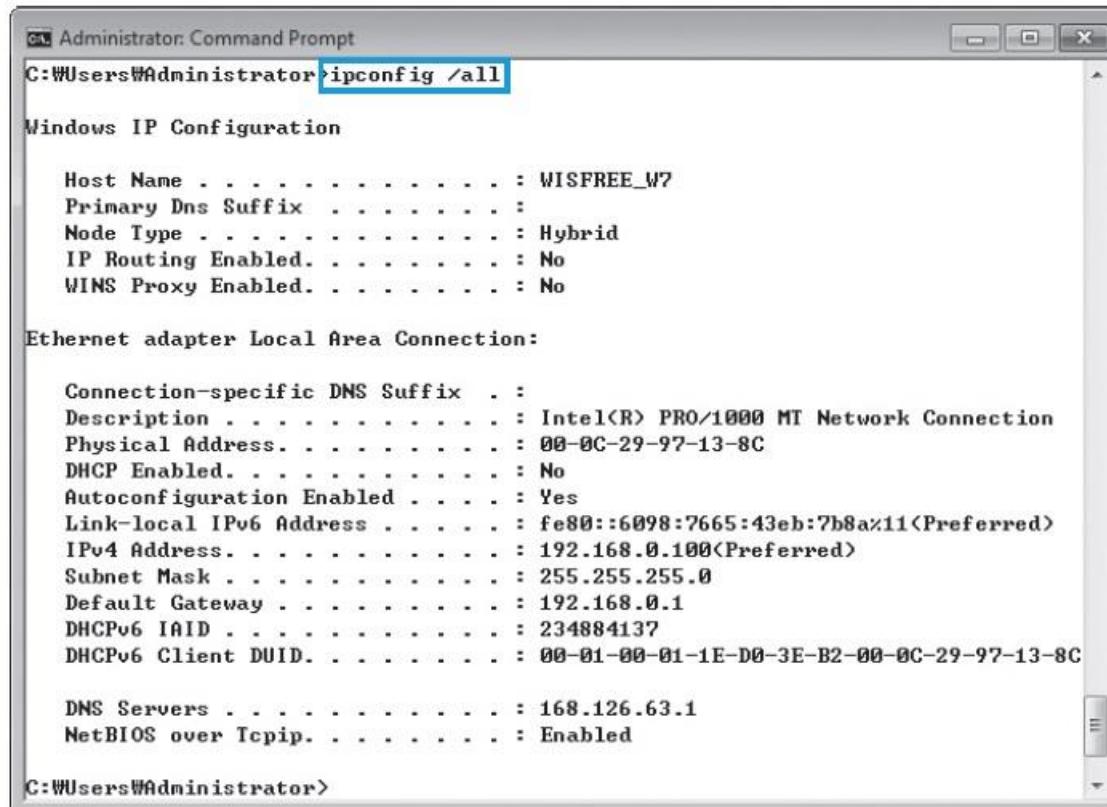


그림 3-15 TCP/IP 고급 설정

02_DNS- DNS의 동작 원리

❖ 현재 운영 중인 DNS 서버 확인

- 명령 창에서 'ipconfig /all' 명령을 입력



```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WISFREE_W7
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-97-13-8C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6098:7665:43eb:7b8a%11<Preferred>
IPv4 Address. . . . . : 192.168.0.100<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-D0-3E-B2-00-0C-29-97-13-8C

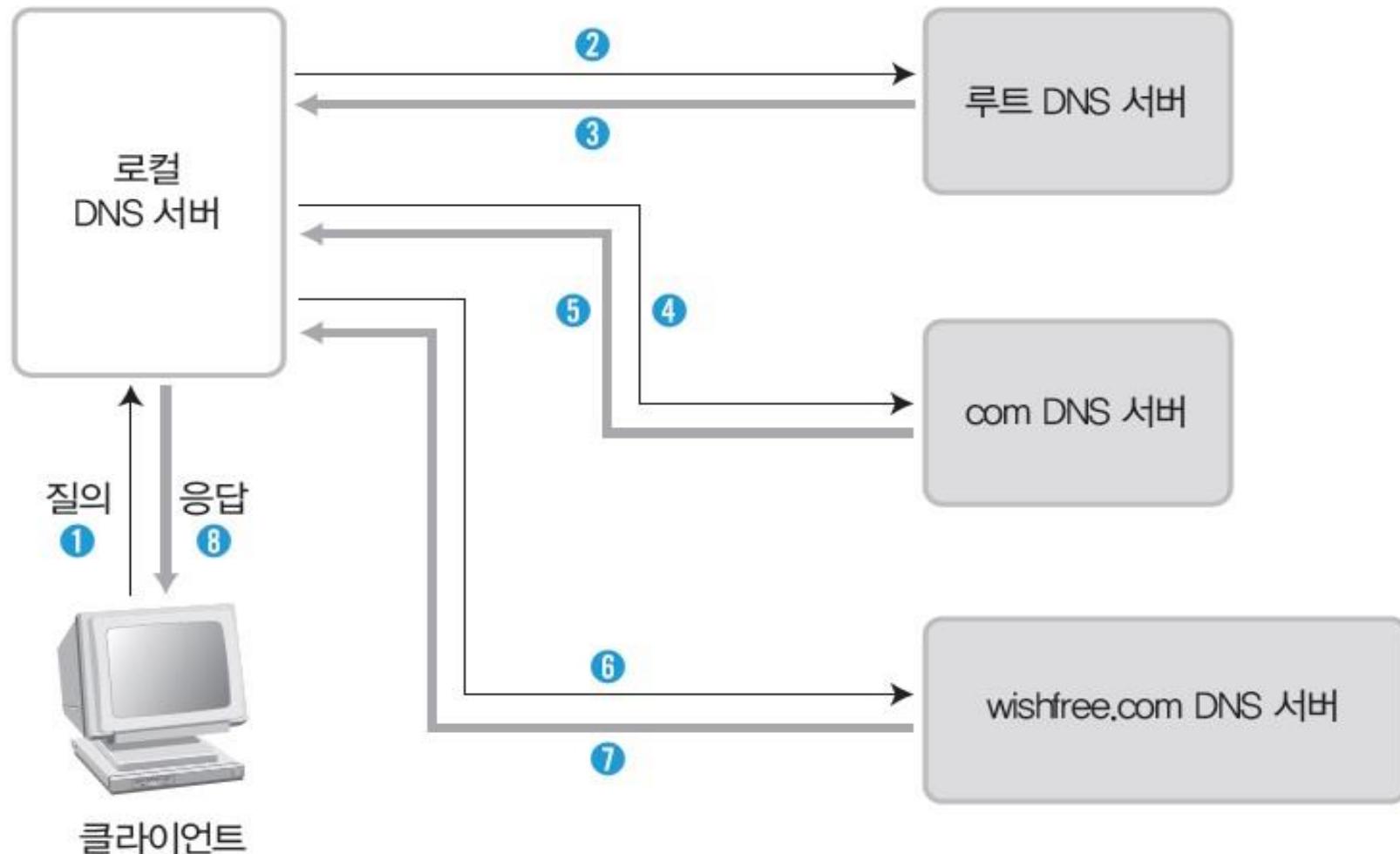
DNS Servers . . . . . : 168.126.63.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

그림 3-16 'ipconfig /all' 명령으로 설정된 DNS 서버 확인하기

02_DNS - DNS의 동작 원리

❖ DNS 서버의 이름 해석 순서



02_DNS- DNS의 동작 원리

❖ 시스템에 캐시된 DNS 정보 확인

ipconfig /displaydns

```
C:\> Administrator: Command Prompt
C:\Users\Administrator> ipconfig /displaydns

Windows IP Configuration

www.hanbit.co.kr
-----
Record Name . . . . . : www.hanbit.co.kr
Record Type . . . . . : 1
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . . . : Answer
A <Host> Record . . . . : 218.38.58.195

www.hanbit.co.kr
-----
No records of type AAAA

hanbit
-----
Record Name . . . . . : hanbit
Record Type . . . . . : 5
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . . . : Answer
CNAME Record . . . . . : www.hanbit.co.kr
```

그림 3-18 윈도우에서 캐시된 DNS 정보 확인

02_DNS - DNS의 동작 원리

❖ 시스템에 캐시된 DNS 정보 삭제

ipconfig /flushdns

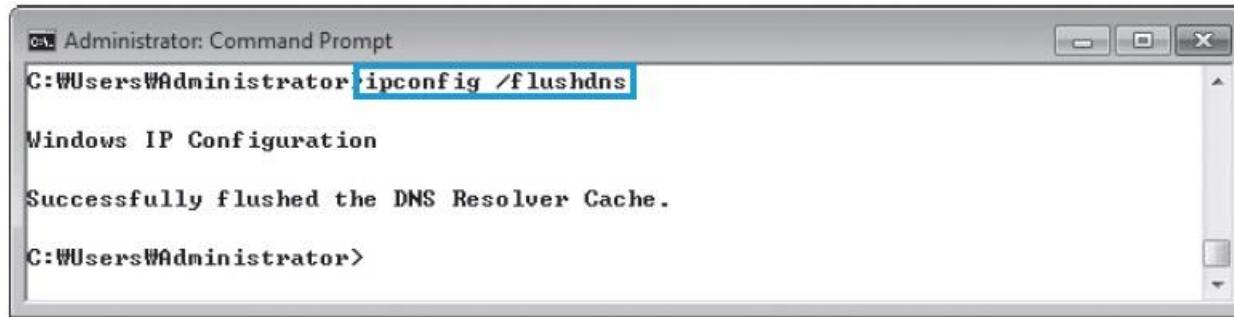


그림 3-19 윈도우에서 캐시된 DNS 정보 삭제

❖ DNS 서버의 구분

- 주 DNS 서버 : 도메인의 중심 DNS 서버
- 부 DNS 서버 : 주 DNS 서버의 백업 서버
- 캐시 DNS 서버 : 주 DNS 서버와 부 DNS 서버에 대한 접속이 불가능할 때를 대비한 임시 DNS 서버

02_DNS- DNS를 이용한 정보 습득

❖ DNS를 이용한 정보 습득

- DNS 서버의 기본적인 보안 문제는 영역이 전송되는 대상을 부 DNS 서버로 제한하지 않은 데서 발생

❖ 리눅스에서 DNS 영역에 대한 전송 설정

- /etc/named.conf(또는 /etc/bind/named.conf.local)에서 다음과 같은 형태로 설정

```
zone "wishfree.com" {  
    type master;  
    file "db.wishfree.com";  
    allow-transfer (10.10.10.1);  
};
```

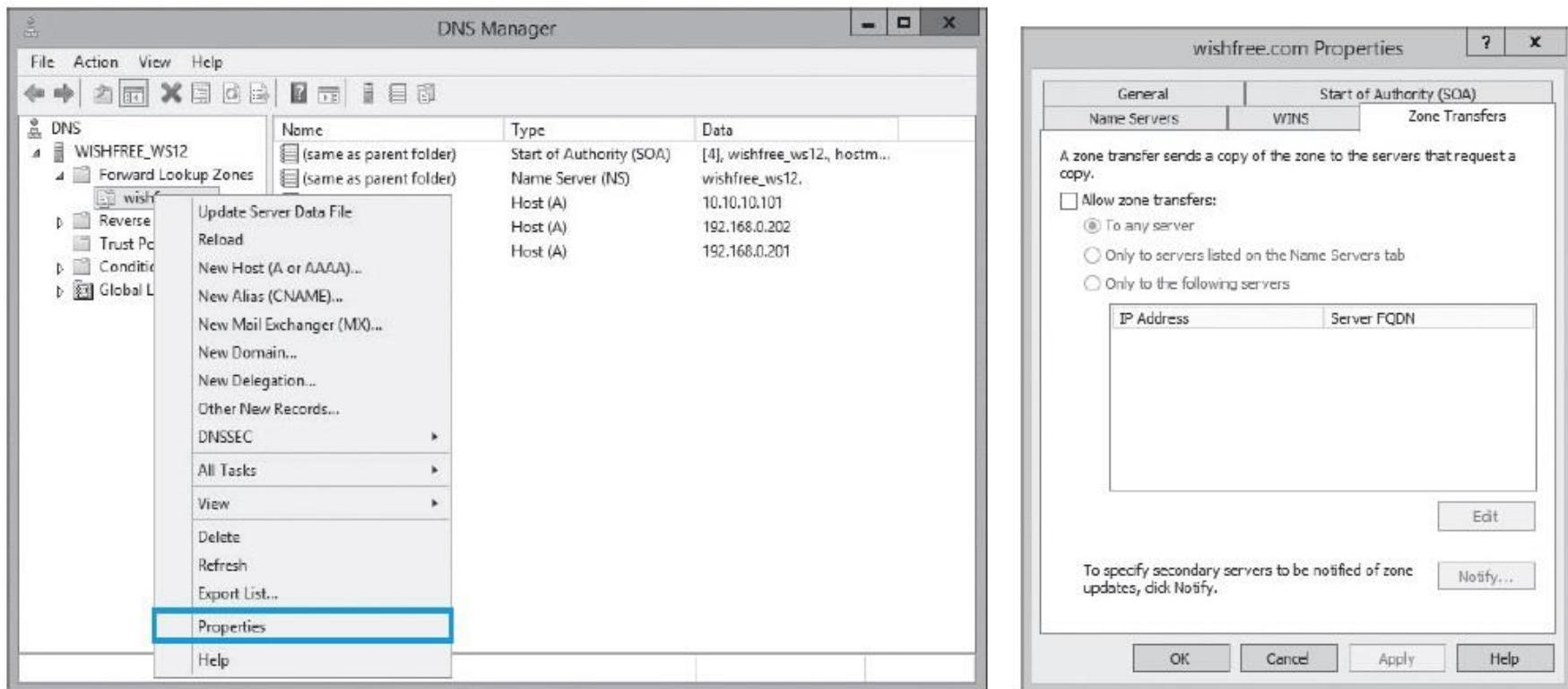
도메인 이름 입력

1차 네임서버(master)에 대한 설정은 db.wishfree.com 파일에 포함

02_DNS - DNS를 이용한 정보 습득

❖ 윈도우에서 DNS 영역에 대한 전송 설정

- 임의의 DNS 영역을 생성한 뒤, 'Property'를 확인 후 [Zone Transfers] 탭에서 DNS 영역에 대한 전송 여부 설정



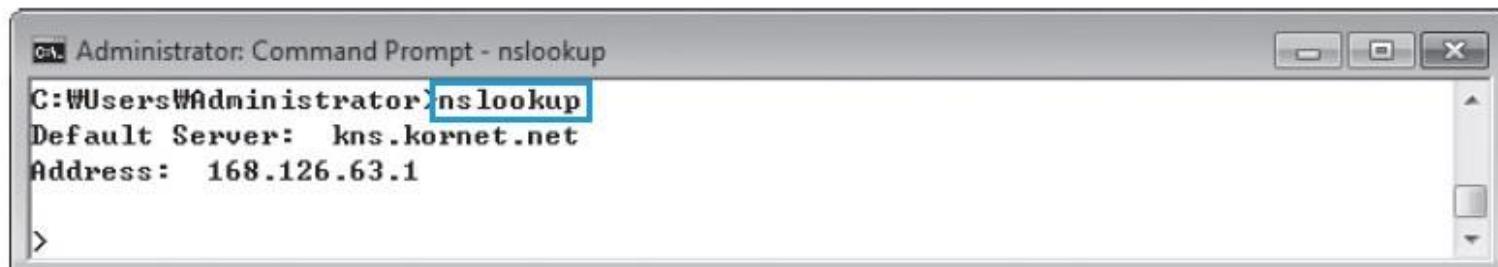
02_DNS - DNS 서버 검색으로 정보 습득하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우 7)

• 영역(Zone)과 해당 영역에 host가 등록된 DNS 서버(윈도우 2012)

① nslookup 실행하고 DNS 설정하기

nslookup



02_DNS- DNS 서버 검색으로 정보 습득하기

① nslookup 실행하고 DNS 설정하기

- 조사하려는 DNS 서버를 바꾸고 싶다면 'server ***.***.***.***' 형식으로 입력
server 168.126.63.1

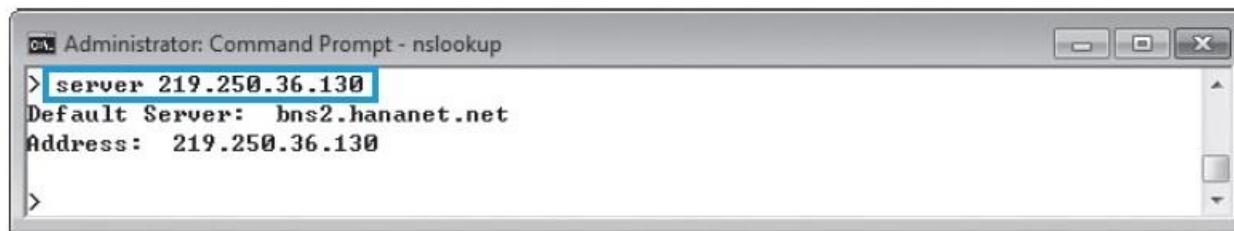
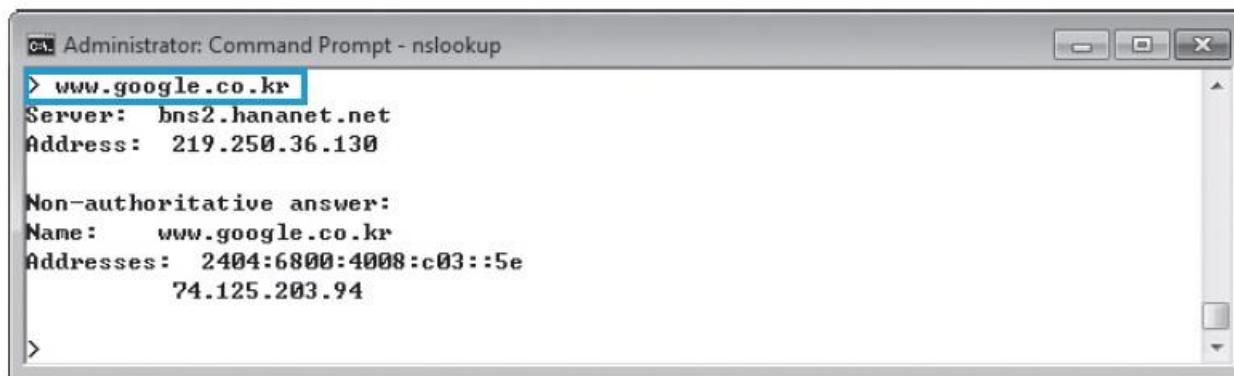


그림 3-22 조회 대상 DNS 서버 변경

02_DNS- DNS 서버 검색으로 정보 습득하기

② 도메인 정보 수집하기

www.google.co.kr



```
Administrator: Command Prompt - nslookup
> www.google.co.kr
Server: bns2.hananet.net
Address: 219.250.36.130

Non-authoritative answer:
Name: www.google.co.kr
Addresses: 2404:6800:4008:c03::5e
           74.125.203.94

>
```

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt - nslookup". The command entered is "> www.google.co.kr". The output shows the server used is "bns2.hananet.net" with address "219.250.36.130". It then provides a "Non-authoritative answer" for the name "www.google.co.kr", listing two addresses: "2404:6800:4008:c03::5e" and "74.125.203.94". The prompt ">" is visible at the bottom.

그림 3-23 www.google.co.kr에 대한 nslookup

02_DNS- DNS 서버 검색으로 정보 습득하기

② 도메인 정보 수집하기

- 이 DNS에 어떤 서버의 종류가 있는지 검색할 때에는 'set type' 명령을 이용

set type=ns

google.co.kr



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - nslookup". The user has entered the following commands:

```
> set type=ns
> google.co.kr
```

The output shows the server information and the non-authoritative answer for the nameservers:

```
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 = ns3.google.com
google.co.kr      nameserver = ns4.google.com
>
```

그림 3-24 www.google.co.kr의 DNS 서버 목록

02_DNS - DNS 서버 검색으로 정보 습득하기

② 도메인 정보 수집하기

종류	내용		
A(Address)	<p>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.</p> <p>- www A 200.200.200.20 - ftp A 200.200.200.20</p>		
PTR(Pointer)	<p>A 레코드와 상반된 개념이다. A 레코드는 도메인에 대해 IP 주소를 부여하지만 PTR 레코드는 IP 주소에 대해 도메인명을 맵핑하는 역할을 한다.</p>		
NS(Name Server)	<p>DNS 서버를 가리키며, 각 도메인에 적어도 한 개 이상 있어야 한다.</p>		
MX(Mail Exchanger)	<p>도메인 이름으로 보낸 메일을 받는 호스트 목록으로 지정한다.</p>		
CNAME(Canonical Name)	<p>호스트의 다른 이름을 정의하는 데 사용한다.</p>		
SOA(Start of Authority)	<p>도메인에 대한 권한이 있는 서버를 표시한다.</p>		
HINFO(Hardware Info)	<p>해당 호스트의 하드웨어 사양을 표시한다.</p>		
ANY(ALL)	<p>DNS 레코드를 모두 표시한다.</p>		

02_DNS- DNS 서버 검색으로 정보 습득하기

② 도메인 정보 수집하기

- 관련된 모든 서버 목록은 set type=all 명령으로 확인

set type=all

google.co.kr

```
c:\ Administrator: Command Prompt - nslookup
> set type=all
> google.co.kr
Server: bns2.hananet.net
Address: 219.250.36.130

Non-authoritative answer:
google.co.kr
    primary name server = ns2.google.com
    responsible mail addr = dns-admin.google.com
    serial = 122957288
    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    MX preference = 10, mail exchanger = aspmx.l.google.com
google.co.kr    MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.co.kr    MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.co.kr    MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.co.kr    MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.co.kr    internet address = 1.255.22.104
google.co.kr    internet address = 1.255.22.108
google.co.kr    internet address = 1.255.22.109
google.co.kr    internet address = 1.255.22.89
google.co.kr    internet address = 1.255.22.113
google.co.kr    internet address = 1.255.22.118
google.co.kr    internet address = 1.255.22.114
```

그림 3-25 google.co.kr에 등록된 모든 DNS 레코드

02_DNS- DNS 서버 검색으로 정보 습득하기

③ DNS 영역 전송하기

- 윈도우 2012 서버에 다음과 같이 wishfree.com이라는 영역(Zone)을 생성하고, web, db, was 서버를 등록

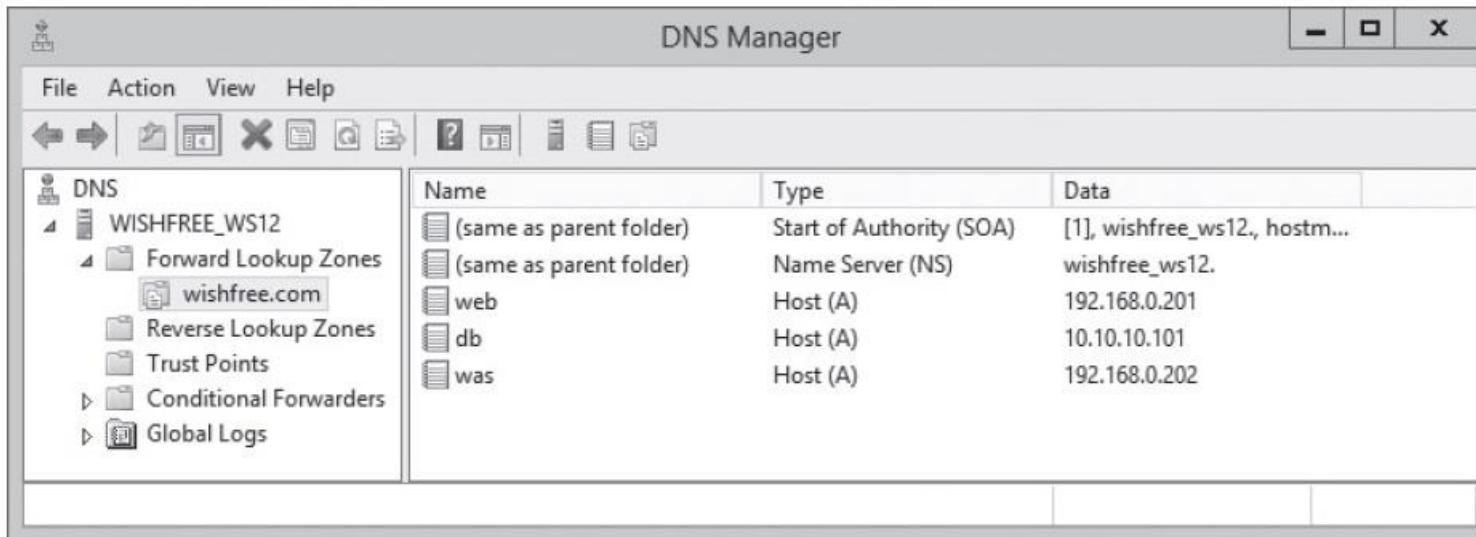
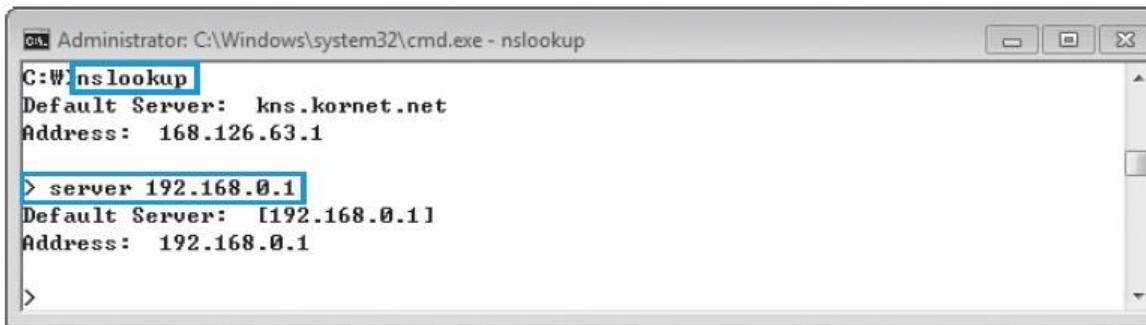


그림 3-26 wishfree.com 영역에 등록된 DNS 정보

02_DNS- DNS 서버 검색으로 정보 습득하기

③ DNS 영역 전송하기

- nslookup을 실행시킨 뒤, 서버를 설정한 DNS 서버로 바꿈.



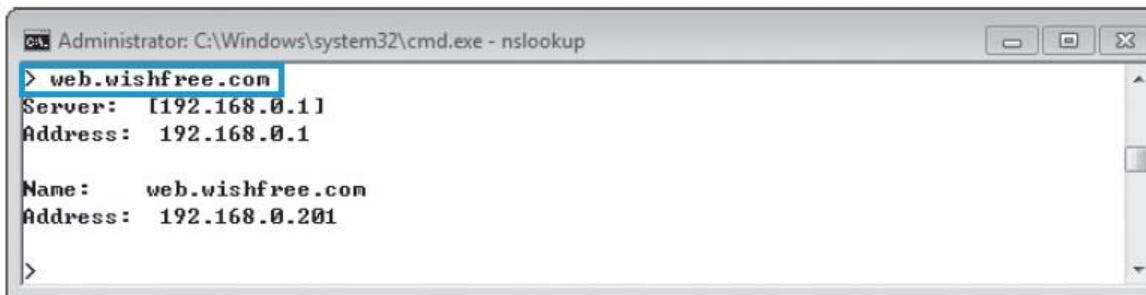
```
C:\> nslookup
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\> nslookup
Default Server: kns.kornet.net
Address: 168.126.63.1

> server 192.168.0.1
Default Server: [192.168.0.1]
Address: 192.168.0.1

>
```

그림 3-27 DNS 변경

- web.wishfree.com과 같이 입력하여 해당 IP를 확인



```
C:\> nslookup
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\> nslookup
Server: [192.168.0.1]
Address: 192.168.0.1

Name:   web.wishfree.com
Address: 192.168.0.201

>
```

그림 3-28 web.wishfree.com에 대한 nslookup

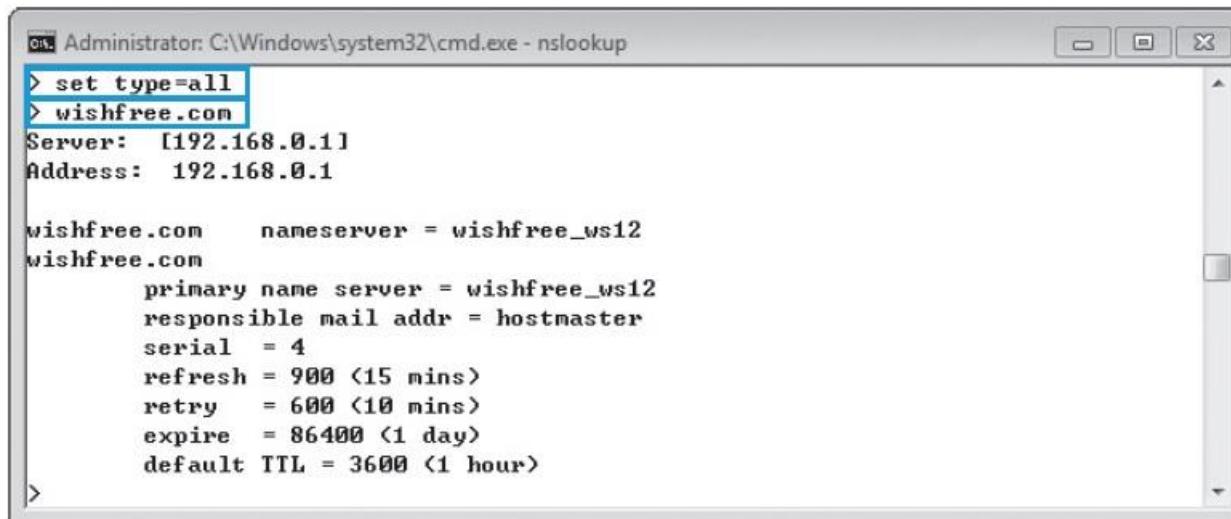
02_DNS- DNS 서버 검색으로 정보 습득하기

③ DNS 영역 전송하기

- 외부에 공개되어야 하는 서버 외에는 자세한 서버 목록을 확인할 수 없음.

set type=all

wishfree.com



```
Administrator: C:\Windows\system32\cmd.exe - nslookup
> set type=all
> wishfree.com
Server: [192.168.0.1]
Address: 192.168.0.1

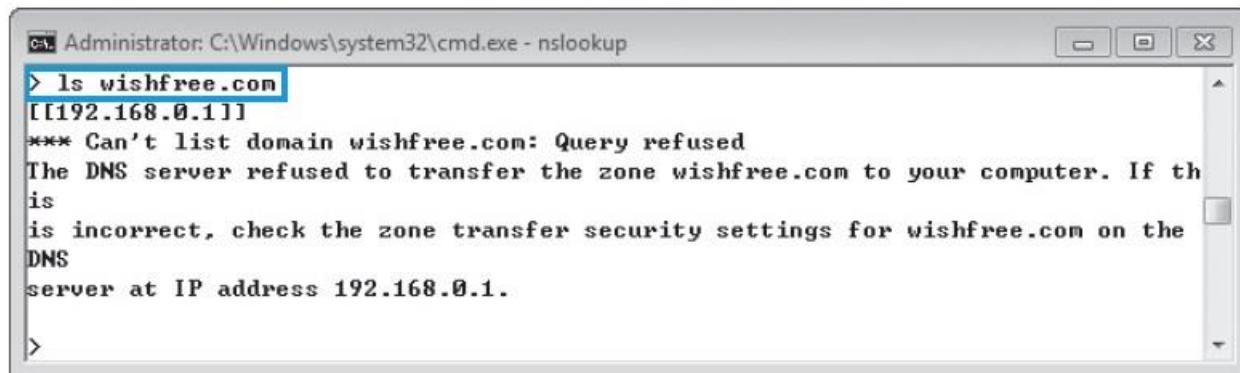
wishfree.com      nameserver = wishfree_ws12
wishfree.com
    primary name server = wishfree_ws12
    responsible mail addr = hostmaster
    serial = 4
    refresh = 900 <15 mins>
    retry = 600 <10 mins>
    expire = 86400 <1 day>
    default TTL = 3600 <1 hour>
>
```

그림 3-29 wishfree.com에 대해 등록된 DNS 레코드 확인

02_DNS- DNS 서버 검색으로 정보 습득하기

③ DNS 영역 전송하기

- 윈도우 2012의 DNS 서버는 기본적으로 영역 전송을 허용하지 않기 때문에 아무런 결과값을 얻을 수 없음.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe - nslookup". The command entered is "ls wishfree.com". The output shows an error message: "Can't list domain wishfree.com: Query refused". It explains that the DNS server refused to transfer the zone wishfree.com to the computer. It suggests checking the zone transfer security settings for the domain on the DNS server at IP address 192.168.0.1.

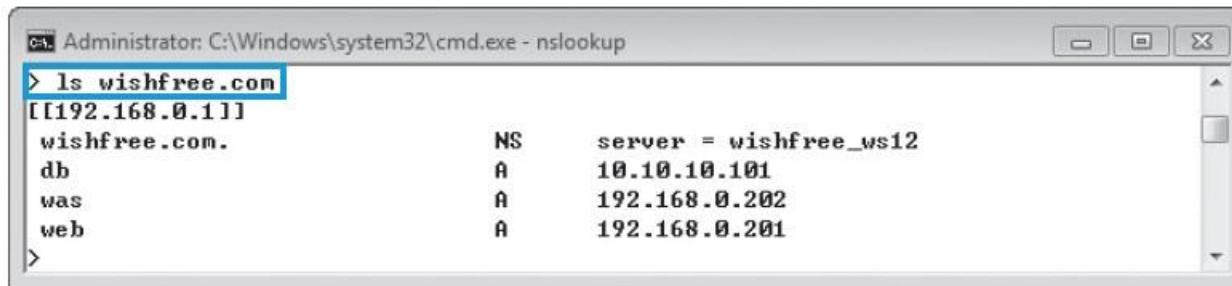
```
Administrator: C:\Windows\system32\cmd.exe - nslookup
> ls wishfree.com
[192.168.0.1]
*** Can't list domain wishfree.com: Query refused
The DNS server refused to transfer the zone wishfree.com to your computer. If this
is
incorrect, check the zone transfer security settings for wishfree.com on the
DNS
server at IP address 192.168.0.1.
```

그림 3-30 wishfree.com에 대한 영역 전송 시도 – 실패

02_DNS - DNS 서버 검색으로 정보 습득하기

③ DNS 영역 전송하기

- 영역 전송을 허용한 뒤, 실행하면 DNS 서버에 등록된 전체 서버 목록 확인 가능

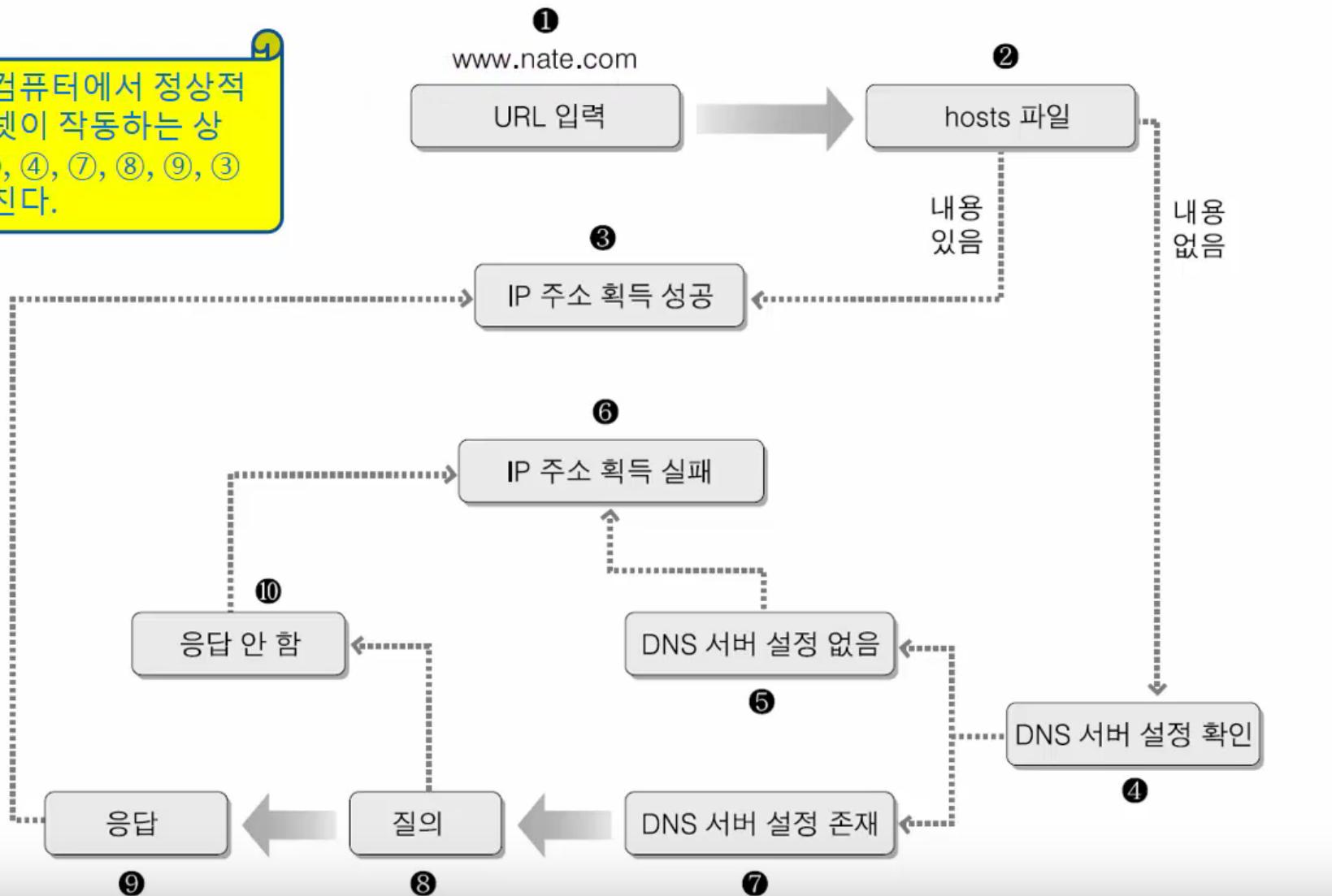


```
Administrator: C:\Windows\system32\cmd.exe - nslookup
> ls wishfree.com
[[192.168.0.1]]
wishfree.com.          NS      server = wishfree_ws12
db                      A       10.10.10.101
was                     A       192.168.0.202
web                     A       192.168.0.201
>
```

그림 3-31 wishfree.com에 대한 영역 전송 시도 – 성공

02_DNS- IP주소를 얻기 위한 내부 흐름

일반적인 컴퓨터에서 정상적으로 인터넷이 작동하는 상태는 ①, ②, ④, ⑦, ⑧, ⑨, ⑩ 과정을 거친다.



03_IP 주소 추적- IP 주소 추적의 기본

❖ IP 주소 추적의 기본

- IP 주소 추적의 기본은 출발지 IP 주소 확인하기

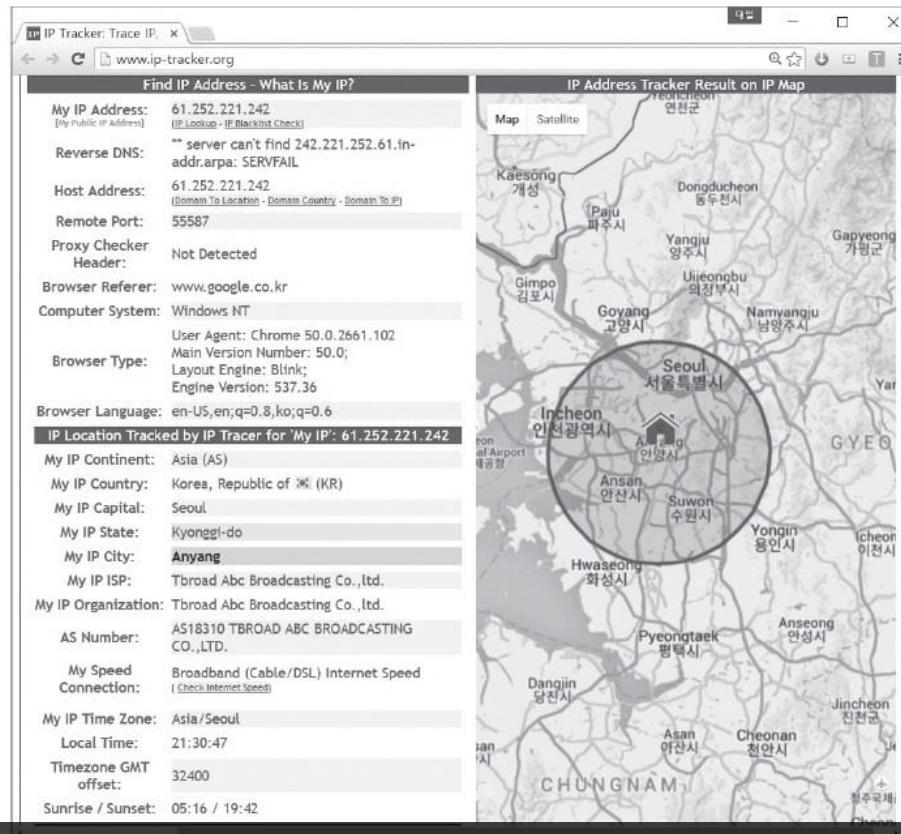
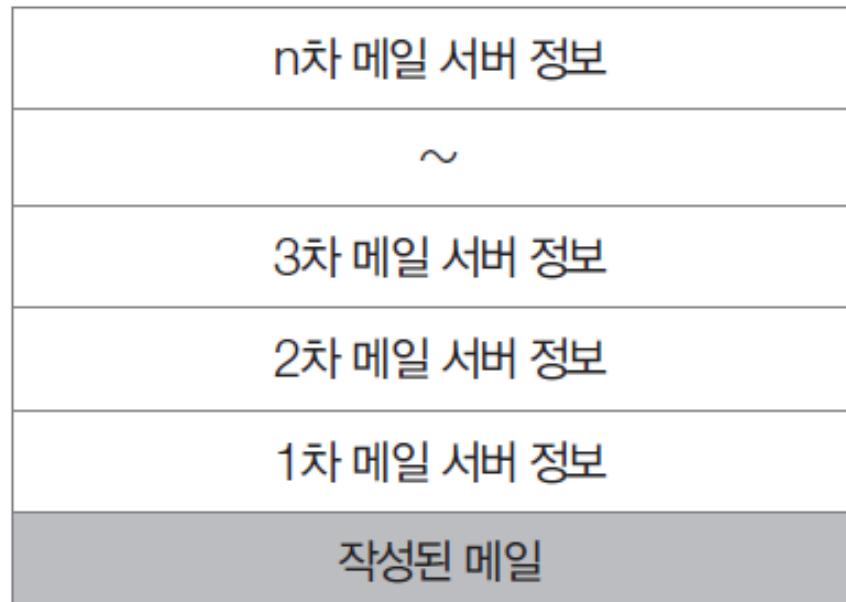


그림 4-1 IP 정보를 찾는 웹사이트(www.ip-tracker.org)

03_IP 주소 추적- 메일 이용하기

❖ 수신된 메일의 구조

- 작성된 메일은 여러 메일 서버를 거쳐 최종 목적지까지 전달



03_IP 주소 추적- 메일 이용하기

❖ 1차 메일 서버 정보

- 목적지로 전송하기 위해 서버에 메일을 저장하는 단계에 대한 정보
- 메일을 이용한 IP 추적에서 가장 중요한 정보

```
Received: from [10.234.214.35] ([10.234.214.35])
          by mailtx3.nmail.com ([10.234.214.16])
          with ESMTP id 1464094642.327675.2999692144.mailtx3
          for <wishfree76@gmail.com>;
Tue, 24 May 2016 21:57:22 +0900 (KST)
Message-ID: <0e983016cc73323fee196b47728c2fff$2d93abf2@mail3.nate.com>
```

mail의 고유한 식별을 위해 Message-ID를 부여

[10.234.214.35] 시스템 → mailtx3.nmail.com([10.234.214.16])

03_IP 주소 추적- 메일 이용하기

❖ 2차 메일 서버 정보

```
Received: from mailtx3.nmail.com (mailtx3.nate.com. [117.53.114.133])  
        by mx.google.com with ESMTPS id tn9si4707799pac.31.2016.05.24.05.57.24  
        for <wishfree76@gmail.com>  
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);  
        Tue, 24 May 2016 05:57:25 -0700 (PDT)  
  
Received-SPF: pass (google.com: domain of wishfree@empas.com designates  
117.53.114.133 as permitted sender) client-ip=117.53.114.133;  
Authentication-Results: mx.google.com;  
        spf=pass (google.com: domain of wishfree@empas.com designates 117.53.114.133  
as permitted sender) smtp.mailfrom=wishfree@empas.com
```

[117.53.114.133] → mx.google.com서버의 메일서버

03_IP 주소 추적- 메일 이용하기

❖ 2차 메일 서버 정보

- Received-SPF : 주요 메일 서버와 IP를 등록해두고, 메일이 전송된 서버의 IP와 메일 주소를 확인하여 스팸 메일 여부를 검사한 결과를 표시

값	내용
None	발신 도메인이 SPF 레코드를 설치하지 않았거나 제공된 발신자 정보에서 해당 도메인 정보를 구할 수 없어 메일의 위조 여부를 판정할 수 없음을 나타낸다.
Neutral	메일 발신 도메인이 자신의 도메인에서 발송되었다고 하는 메일에 대한 위조 여부를 판단하기를 원치 않음을 나타낸다. 'Neutral'은 'None' 판정 메일과 동일하게 취급된다.
Pass	메일 헤더가 위·변조 되지 않았으며(제공된 identity가 발신자와 일치함) 발신자가 메일에 대한 책임을 가진 도메인임을 나타낸다.
Fail	메일 헤더가 위·변조 되었음을 나타내며, 메일을 송신한 메일 서버의 IP와 도메인이 일치하지 않음을 나타낸다.
Softfail	'Fail'과 'Neutral'의 중간 정도 값을 나타내며, 이는 메일 헤더가 위·변조 되었으나 자신의 도메인이 메일 포워딩 등의 서비스를 통해 적법하게 위조될 수 있음을 나타낸다.
TempError	메일 수신 서버에서 SPF 결과 값을 확인할 때 문제가 발생하였음을 나타낸다.
PermError	메일 발송 도메인에 출판된 SPF 레코드 값이 발송 메일에 있는 'Mail From' 발신자 정보를 확인하는데 사용될 수 없음을 나타낸다.

03_IP 주소 추적- 메일 이용하기

❖ 3차 메일 서버 정보

X-Received: by 10.67.3.200 with SMTP id by8mr6585621pad.13.1464094645342;

Tue, 24 May 2016 05:57:25 -0700 (PDT)

Return-Path: <wishfree@empas.com>

10.67.3.200 서버에 의해 메일이 수신

❖ 4차 메일 서버 정보

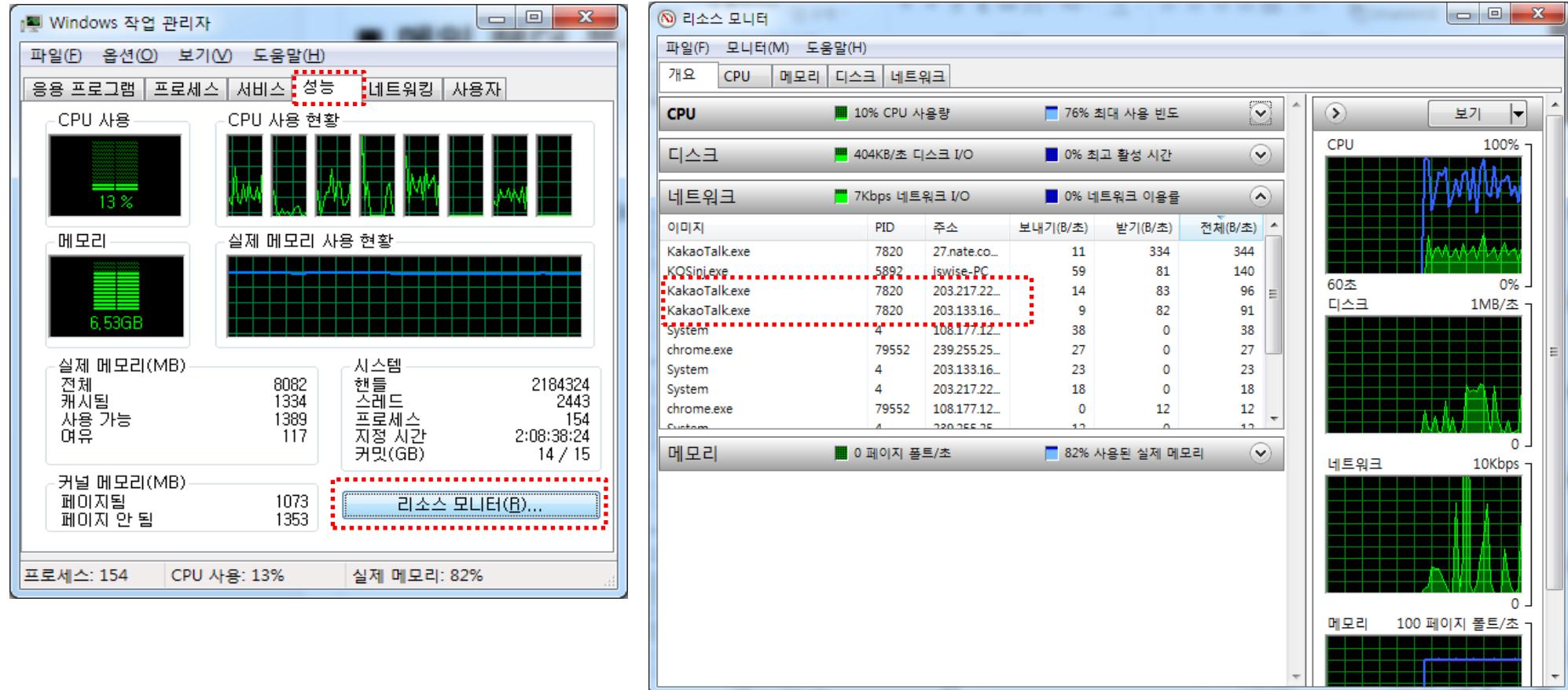
Delivered-To: wishfree76@gmail.com

Received: by 10.157.26.113 with SMTP id u46csp652881otu;

Tue, 24 May 2016 05:57:25 -0700 (PDT)

10.157.26.113 서버에 의해 메일이 수신, wishfree76@gamil.com 으로 전송이 완료

03_IP 주소 추적- 작업관리자를 이용하기



03_IP 주소 추적- Traceroute 이용하기

❖ traceroute(트레이스라우트)

- 패킷이 목적지까지 도달하는 동안 거쳐가는 라우터의 IP를 확인하는 툴
- UDP와 ICMP, IP의 TTL 값을 이용
- 상대방의 IP 주소를 알고 있는 상태에서, 상대방이 속한 인터넷 구성 등을 짐작 할 수 있음.
- traceroute를 수행할 때 경로가 매번 다르게 형성되다가 하나로 고정된다면 역 추적을 당하고 있는 것일 수 있음.

03_IP 주소 추적- Traceroute 이용하기

❖ 패킷 내용 확인하기

- traceroute 툴로 UDP 패킷을 이용하면 상대방에게 전송되는 경로를 확인할 수 있음(윈도우에서는 tracert 명령으로 수행)

tracert 168.126.63.1

The screenshot shows a Windows Command Prompt window titled "관리자: 명령 프롬프트". The command entered is "C:\>tracert 168.126.63.1". The output displays the traceroute path to the destination IP address 168.126.63.1. The path consists of 13 hops, with the last hop being the destination itself. Hops 1 through 3 are marked as "요청 시간이 만료되었습니다." (Request timed out). Hops 4 through 12 show varying round-trip times (RTTs) in milliseconds. The final hop (hop 13) shows the destination as "kns.kornet.net [168.126.63.1]". The message "추적을 완료했습니다." (Tracing completed) is displayed at the bottom.

```
C:\>tracert 168.126.63.1
최대 30홉 이상의
kns.kornet.net [168.126.63.1](으)로 가는 경로 추적:

 1 * * * 요청 시간이 만료되었습니다.
 2 * * * 요청 시간이 만료되었습니다.
 3 * * * 요청 시간이 만료되었습니다.
 4 <1 ms <1 ms <1 ms 100.64.16.225
 5 <1 ms <1 ms <1 ms 54.239.122.7
 6 8 ms 10 ms 10 ns 54.239.123.28
 7 <1 ms 2 ms 2 ns 54.239.123.13
 8 2 ms 1 ms 2 ns 112.175.138.13
 9 4 ms 2 ms 4 ns 112.188.241.209
10 3 ms 3 ms 3 ns 112.174.62.229
11 2 ms 2 ms 2 ns 112.174.74.98
12 2 ms 2 ms 2 ns 61.74.74.244
13 2 ms 2 ms 2 ns kns.kornet.net [168.126.63.1]

추적을 완료했습니다.

C:\>
```

03_IP 주소 추적- 웹 게시판 이용하기

❖ 웹 게시판 이용하기

- 요즘에는 웹 해킹 공격이 많이 발생
- 특히 최근에 이슈가 되고 있는 APT(Advanced Persistent Threat) 공격은 웹 페이지의 취약점을 이용하는 경우가 많음.
- 해커는 웹 사이트의 구조를 파악하고 공격하기 위해 웹 게시판에 접근하므로 서비스의 로그를 분석하면 해커의 IP를 확인할 수 있음.

APT (Advanced Persistent Threat)



APT(Advanced Persistence Threat)정의

특정 목적을 위해 특별한 형태와 방법으로 내부 시스템에 침투하여 자신을 은닉하고 목적이 달성될 때까지 지속적인 활동이 가능한 실제적인 위협

APT 공격절차 – Cyber Kill Chain

- ① 정찰(Reconnaissance)
- ② 무기 제작(Weaponization)
- ③ 배달(Delivery)
- ④ 취약점 공격(Exploitation)
- ⑤ 설치(Installation)
- ⑥ 명령 및 제어(Command and Control)
- ⑦ 표적 대상 행동(Actions on objectives)

실제 악성코드가 동작되는 Delivery(APT Life Cycle) 단계 부터 탐지 및 대응이 이루어져야 함



04_풋프린팅- 풋프린팅에 대한 이해

❖ 풋프린팅(Footprinting)

- 발자국을 살펴보는 일
- 공격 대상의 정보를 모으는 방법 중 하나



04_풋프린팅- 풋프린팅에 대한 이해

❖ 사회 공학 기법(Social Engineering)

- 실제로 패스워드가 노출되는 사건의 대부분이 사회 공학에 의한 것
- 친구끼리 사용자 계정이나 패스워드 정보를 주고 받거나, 패스워드를 잊지 않으려고 수첩이나 컴퓨터 옆에 적어 놓은 것들을 이용하는 해킹

04_풋프린팅- 풋프린팅에 대한 이해

❖ 해킹에 필요한 정보

- 침투하고자 하는 시스템의 사용자 계정
- 패스워드를 찾기 위한 계정을 사용하는 사람의 정보
- 게시판 이용
- 협력사나 계열사의 보안 조치 확인
- 주의사항 : 공격 대상 사이트를 직접 접속하는 것보다 유틸리티로 웹 사이트를 다운로드한 뒤 검색하는 것이 좋음.



04_스캔- 스캔에 대한 이해

❖ 스캔(Scan)

- 서비스를 제공하는 서버의 작동 여부와 서버가 제공하는 서비스를 확인하기, 위한 작업
- 전화를 걸었을 때 한 쪽에서 '여보세요'라고 말하면 다른 쪽도 '여보세요'라고 말 하며 서로를 확인하는 것과 같음.



04_스캔- ping

❖ Ping(핑)

- 네트워크와 시스템이 정상적으로 작동하는지 확인하기 위한 간단한 유틸리티
- ICMP(Internet Control Message Protocol)를 사용하며, 기본적으로 TCP/IP 네트워크에서 사용

04_스캔- ICMP 스캔

❖ ICMP를 이용해 공격 대상 시스템의 활성화 여부를 알아보는 방법

- ① Echo Request(Type 8)와 Echo Reply(Type 0) 이용하기
 - ② Timestamp Request(Type 13)와 Timestamp Reply(Type 14) 이용하기
 - ③ Information Request(Type 15)와 Information Reply(Type 16) 이용하기
 - ④ ICMP Address Mask Request(Type 17)와 ICMP Address Mask Reply(Type 18) 이용하기
- 가장 일반적인 방법은 Echo Request(Type 8)와 Echo Reply(Type 0)를 이용하는 것

04_스캔- ICMP 스캔

❖ 윈도우 실행 결과

- ① ICMP 패킷의 길이를 나타냄(윈도우는 32바이트, 유닉스나 리눅스는 56바이트)
- ② 공격 대상에서 보내온 ICMP Echo Reply 패킷의 크기
- ③ Echo Request 패킷을 보낸 후 Reply 패킷을 받기까지의 시간
- ④ TTL(Time To Live) 값
- ⑤ Request 패킷의 개수, Reply 패킷의 개수, 손실된 패킷의 개수
- ⑥ Request 패킷을 보낸 후 Reply 패킷이 오기까지의 시간 정보

```
C:\>Administrator: C:\Windows\system32\cmd.exe
C:\>ping 192.168.0.1
1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
2 3 4
Ping statistics for 192.168.0.1:
5 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
6 Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```