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.

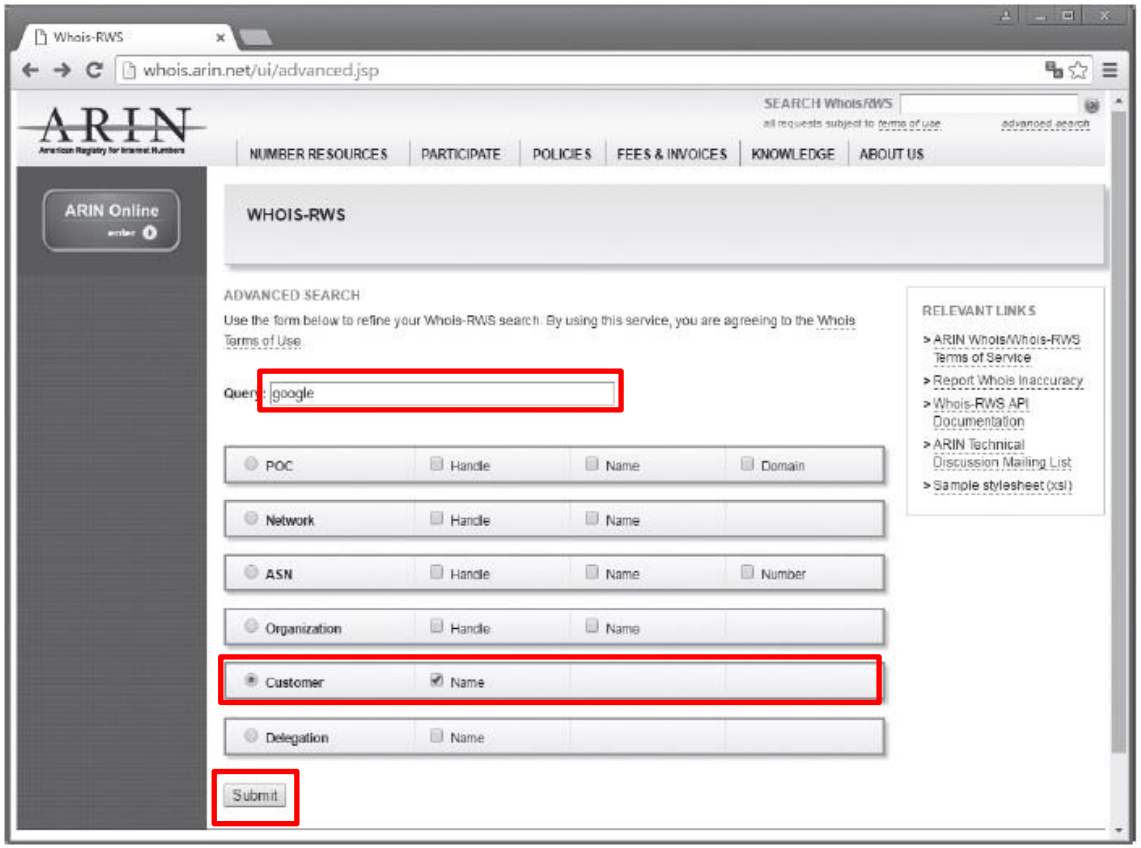
담당 지역	Whois 서버
전체	whois.internic.net
유럽	www.ripe.net
아시아 태평양 지역	www.apnic.net
	www.arin.net
호주	whois.aunic.net
프랑스	whois.nic.fr
일본	whois.nic.ad.jp
영국	whois.nic.uk
한국	whois.krnic.net
해커들을 위한 Whois	whois.greektoos.com

01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우 7)

① Whois 서버 접속하기

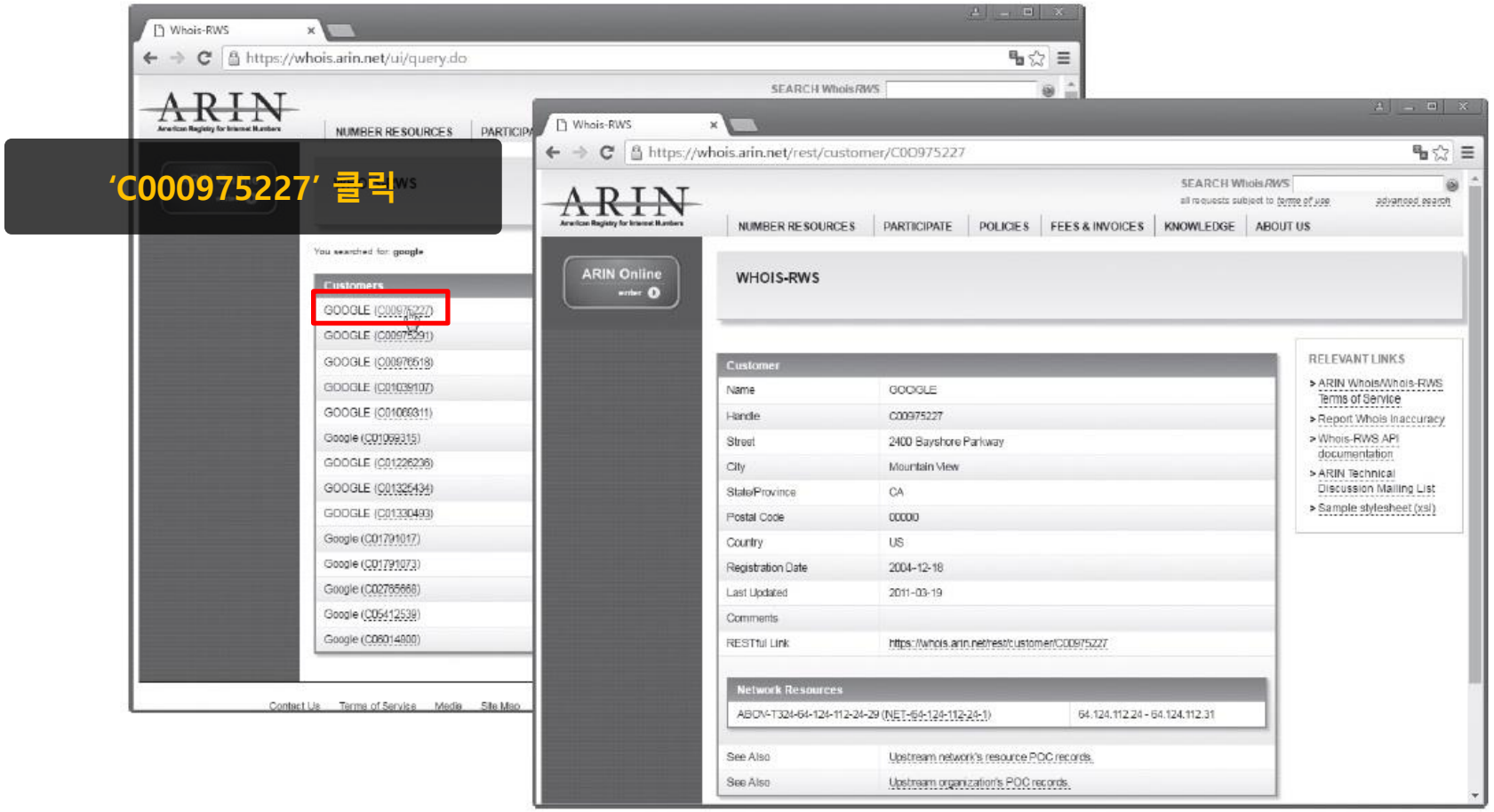
– http://Whois.arin.net/ui/advanced.jsp에서 Whois 서버 검색 가능



01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

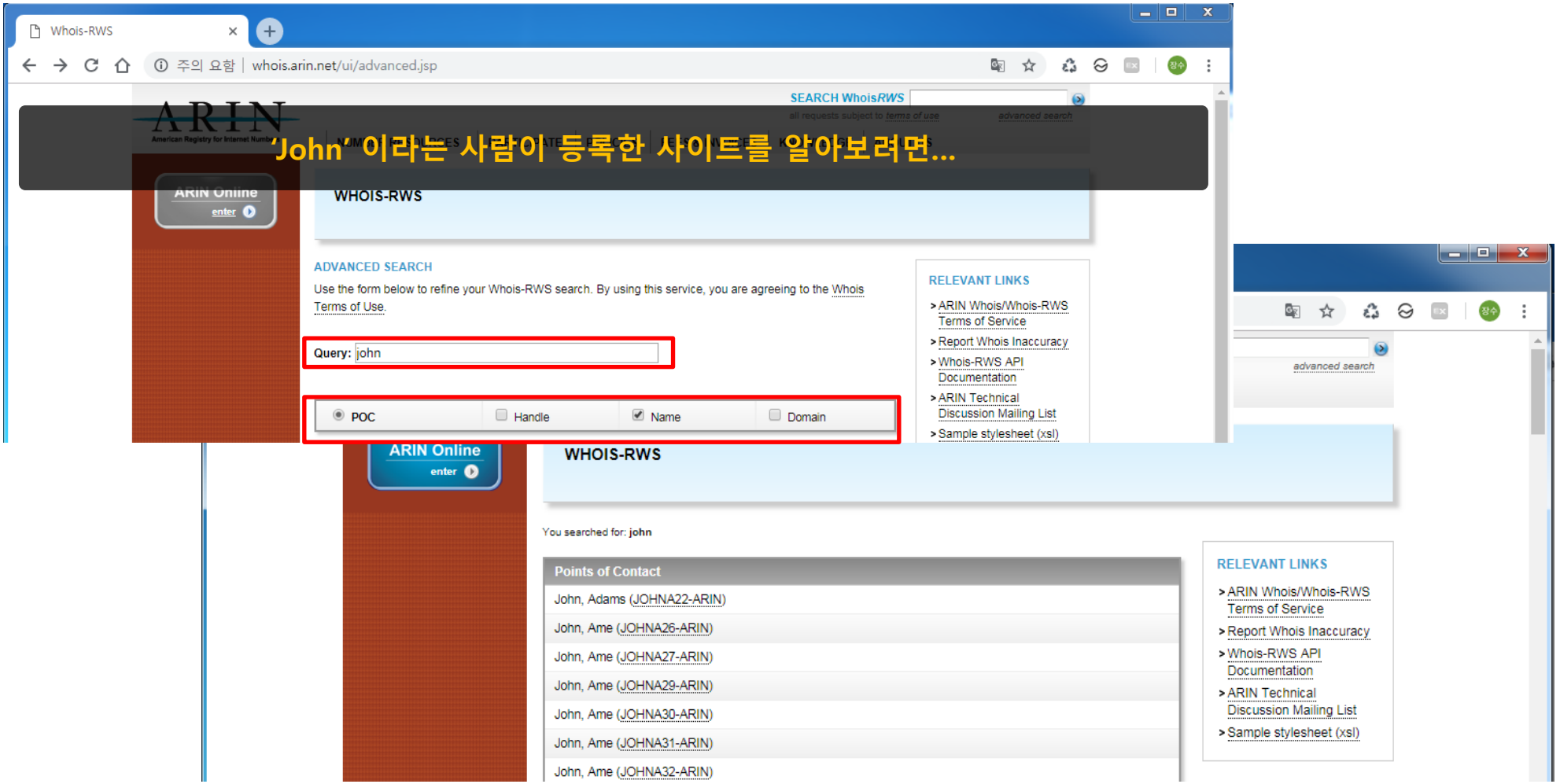
② 정보 획득 대상 확인하기

- 여러 네트워크와 서버 확인 가능



01_Whois 서버와 hosts 파일- Whois 서버를 이용해 정보 획득하기

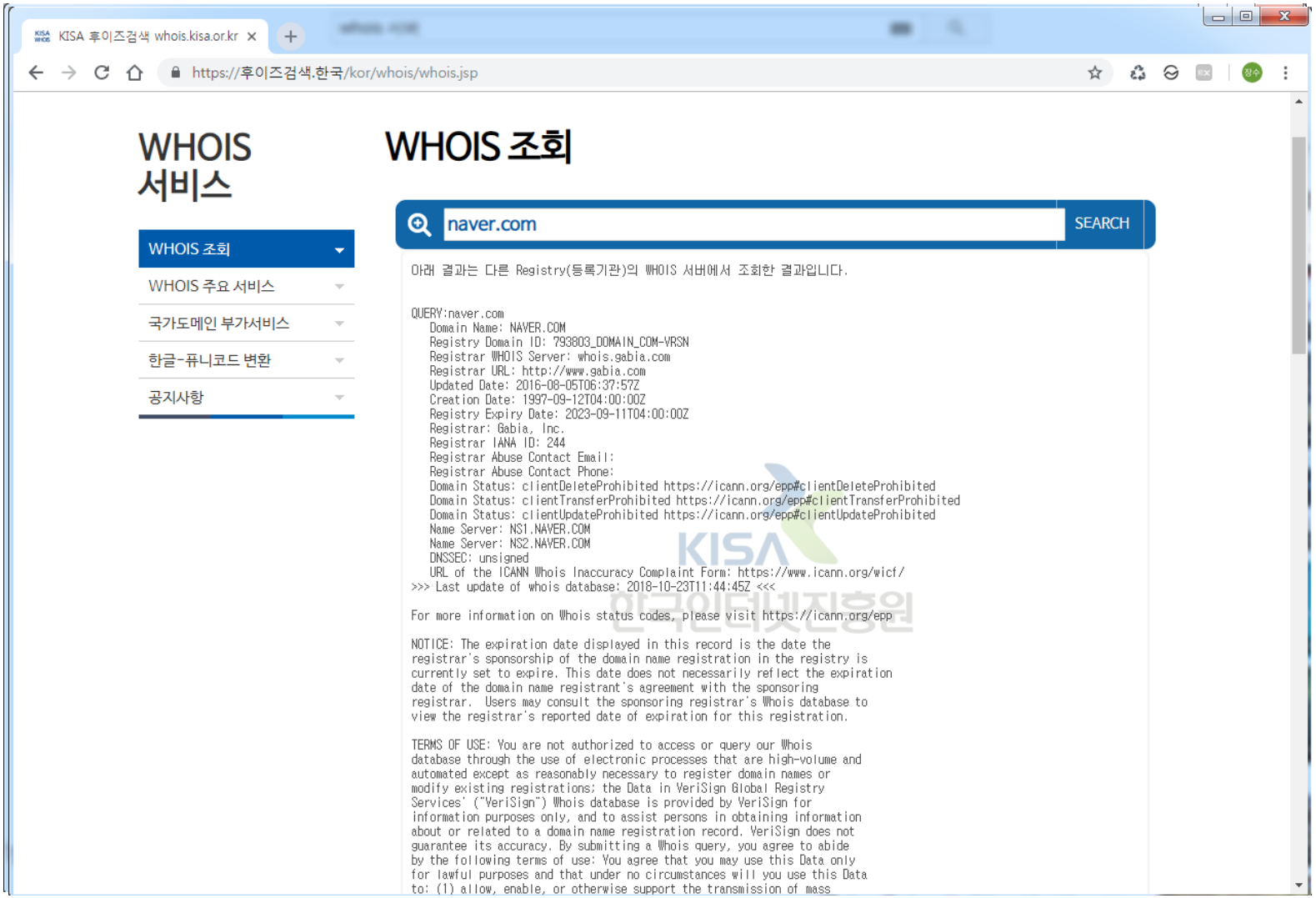
② Whois 서버로 원하는 내용 검사하기



01_Whois 서버와 hosts 파일- whois 도메인 정보 조회

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

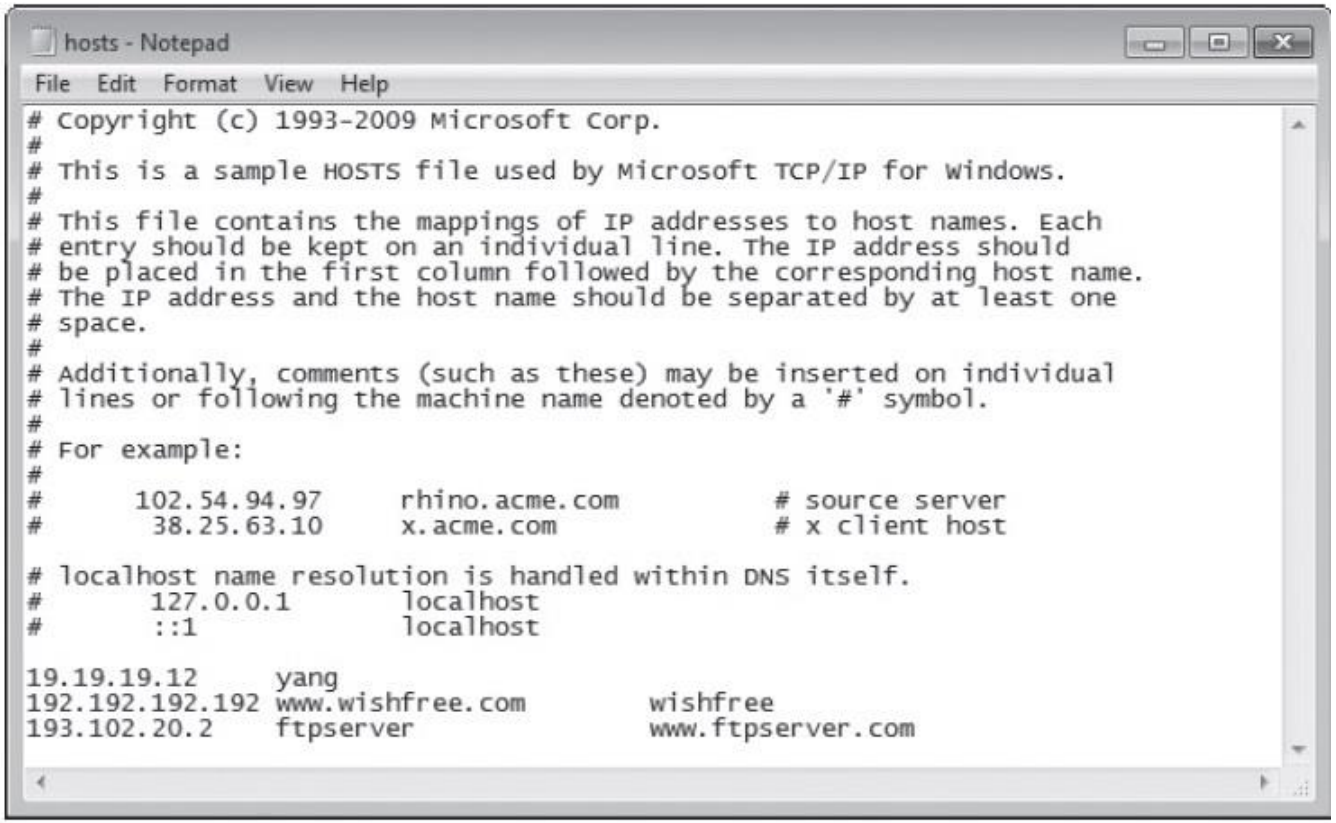
01_Whois 서버와 hosts 파일- whois 도메인 정보 조회



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



01_Whois 서버와 hosts 파일- hosts 파일에 대한 이해

❖ Hosts 파일

- 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.

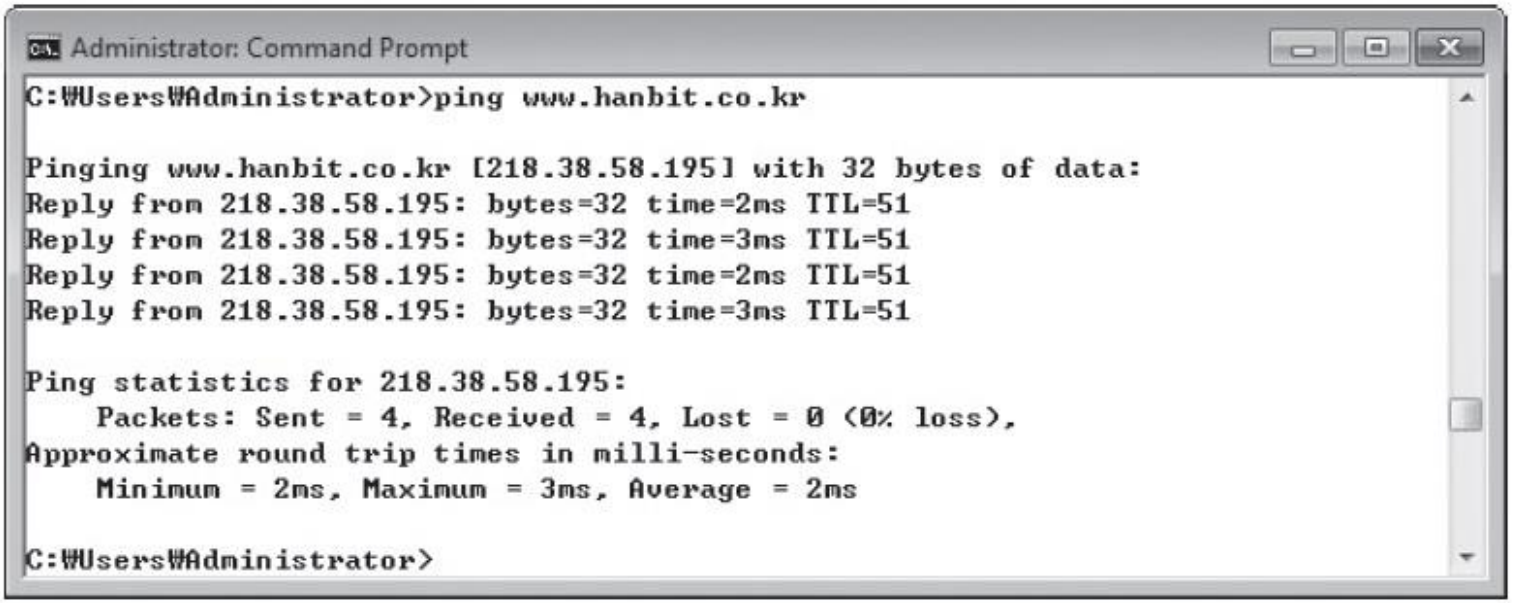
- **Hosts 파일의 각 행 앞에 #으로 표시된 것은 주석**
- **'IP주소'와 '도메인 이름 또는 임의의 명칭'은 Tab 또는 뛰어 쓰기로 구분**

01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우 7)

① 도메인 등록하기

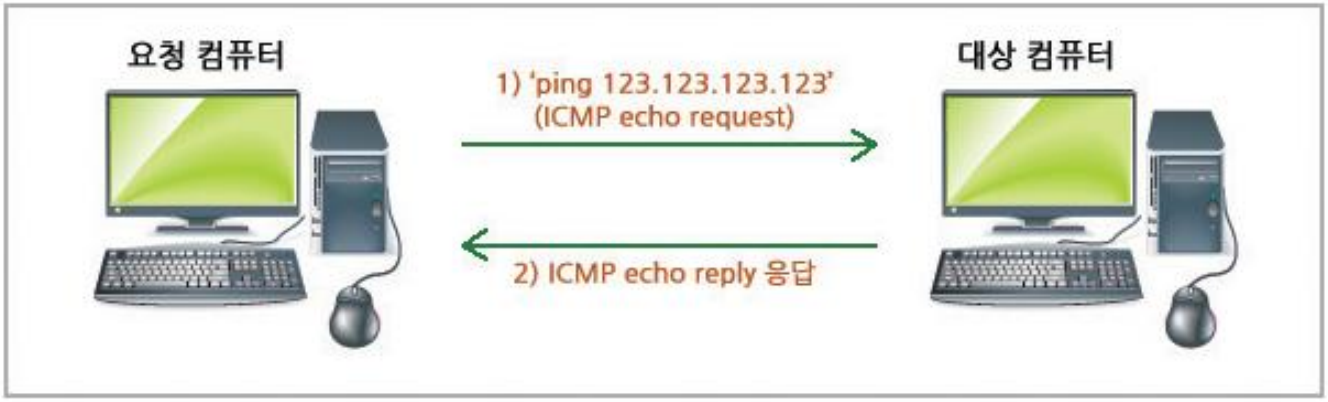
ping www.hanbit.co.kr



#_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.

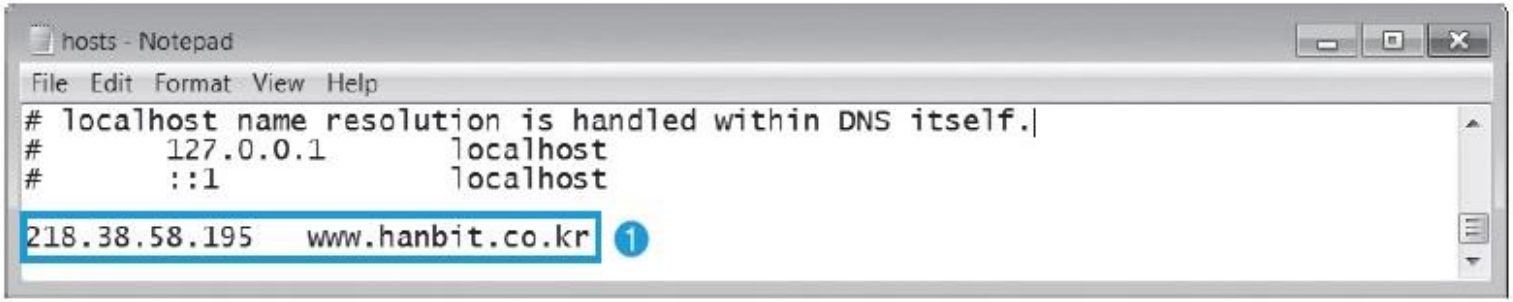
구 분	내 용
-t	Ctrl + C 로 중단시키기 전까지 계속 ping 패킷을 보낸다.
-a	도메인네임의 IP 주소를 보여준다.
-n *count*	Ping 패킷을 몇 번 보낼지 패킷 수를 지정한다. (기본 4회)
-l *size*	Ping 패킷 크기를 지정한다. (기본 32비트)
-f	요구 패킷이 라우터 등을 통과할 경우, 나누어지지 않게 한다.
-i *TTL*	사용할 TTL 값을 설정한다. (TTL은 라우터 하나를 거칠 때마다 1씩 값이 감소한다.(초기값 255)
-v *TOS*	패킷의 TOS를 지정하는 값으로 설정한다. (TOS는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

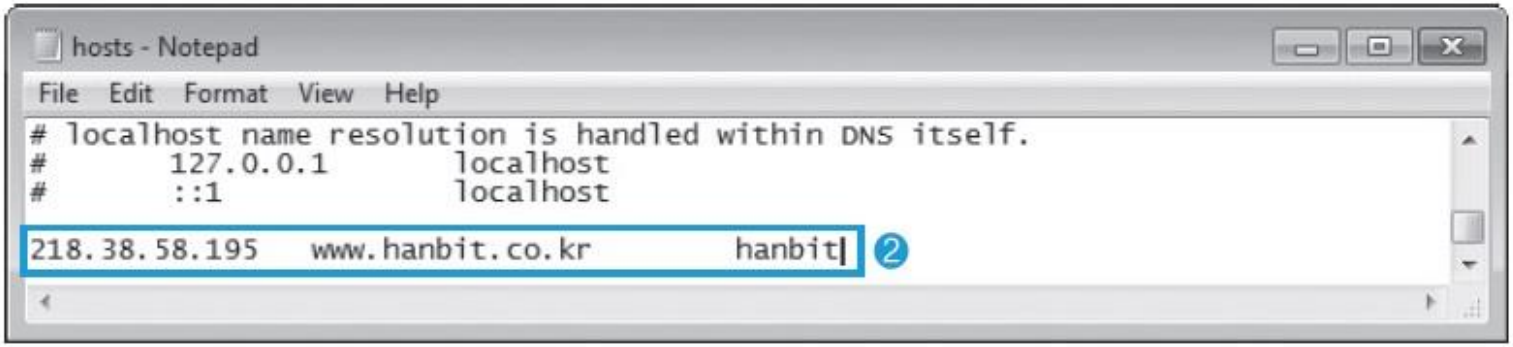
01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

① 도메인 등록하기

– C: \ Windows \ system32 \ drivers \ etc \ hosts 파일을 열어 해당 도메인 등록

218.38.58.195 www.hanbit.co.kr hanbit

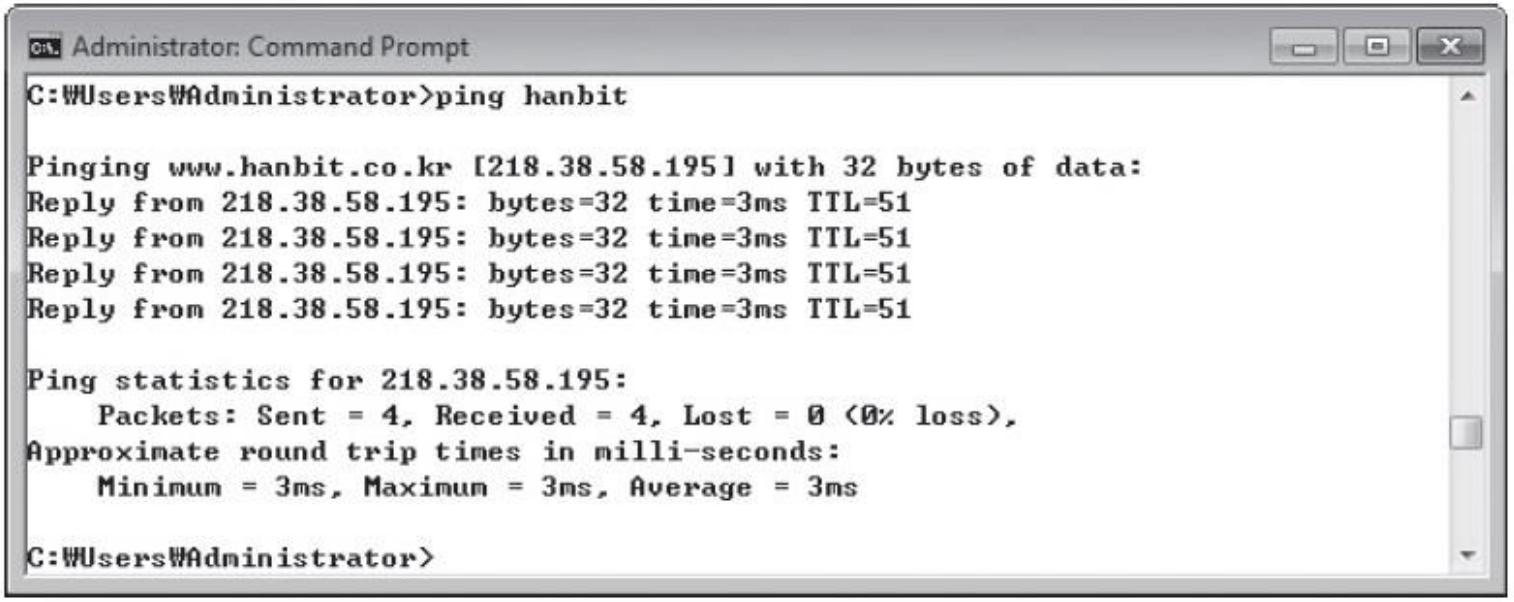




01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

② Hosts 파일 동작 확인하기

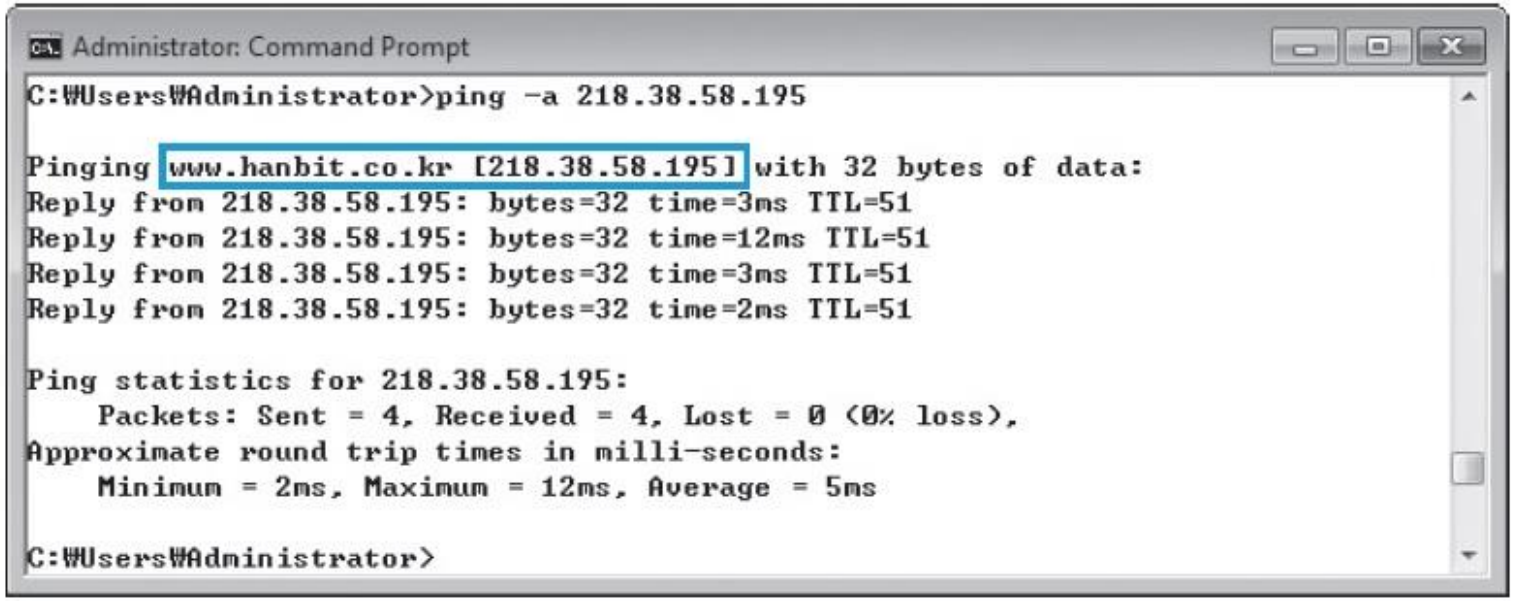
ping hanbit



01_Whois 서버와 hosts 파일- hosts 파일을 이용해 이름 해석하기

② Hosts 파일 동작 확인하기

ping –a 218.38.58.195



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 / 푯말: DNS서버 / 소: 웹 사이트

02_DNS- DNS에 대한 이해

❖ DNS의 계층 구조

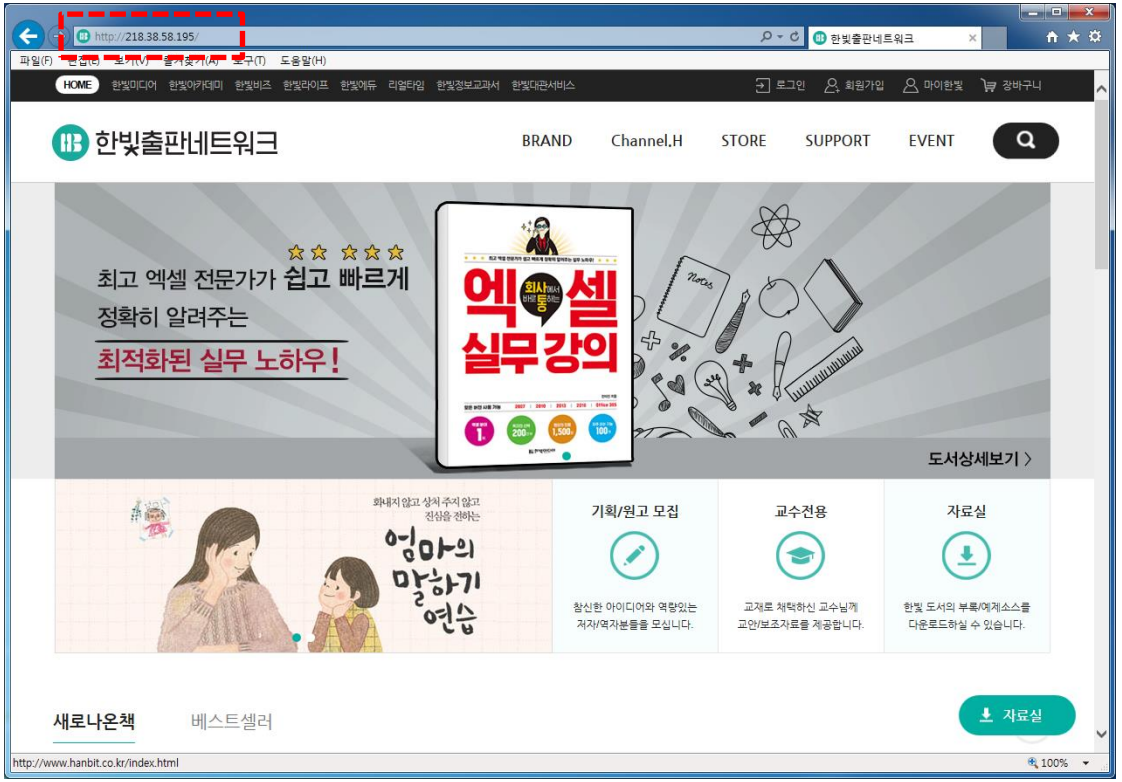
- 가장 상위 개체는 '.' (Root)
- 두 번째 개체는 국가와 조직체의 특성
- 보통 맨 앞은 자신의 DNS 서버에서 지정해놓은 www, ftp와 같은 특정 서버의 이름이 옴.
- FQDN(Fully Qualified Domain Name) : 완성된 주소(예 : www.wishfree.co.kr)

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

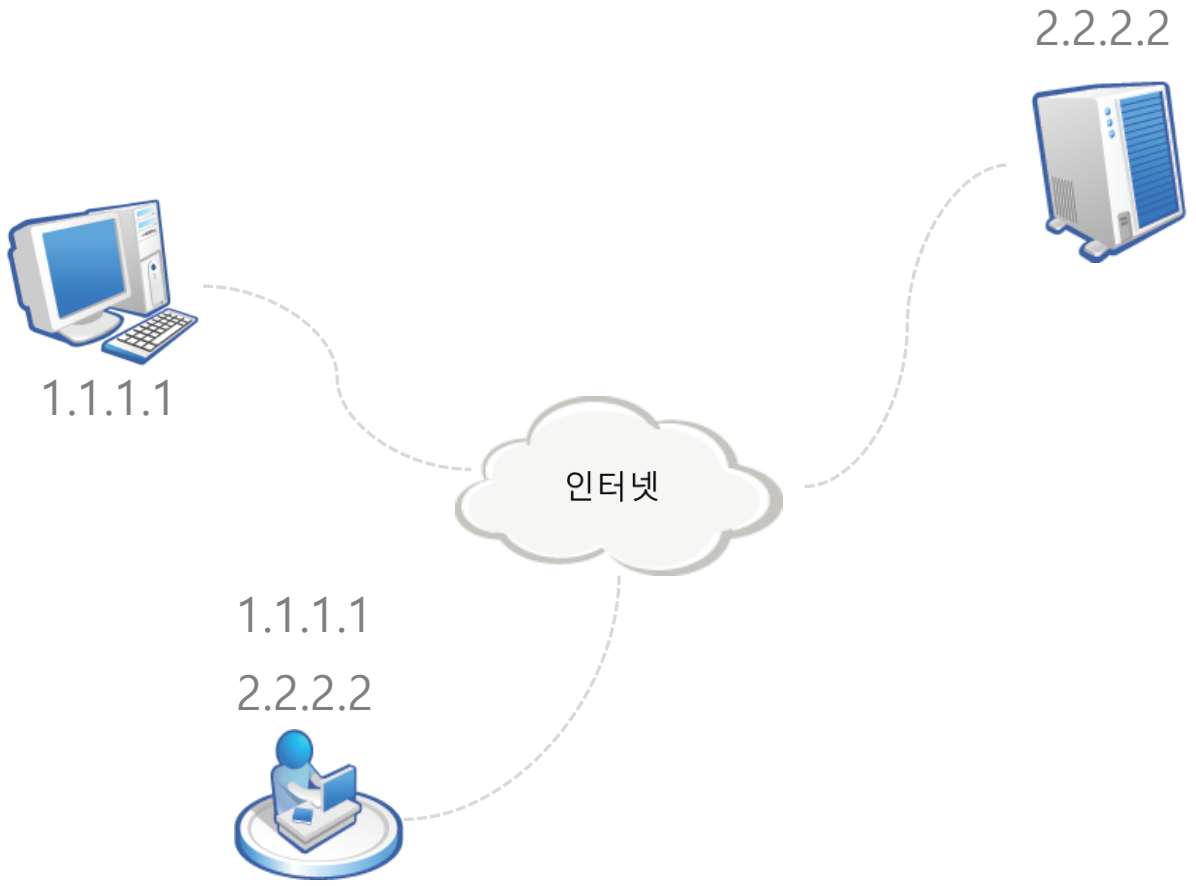
❖ DNS 서버의 개념

- 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



DNS 서버의 개념

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

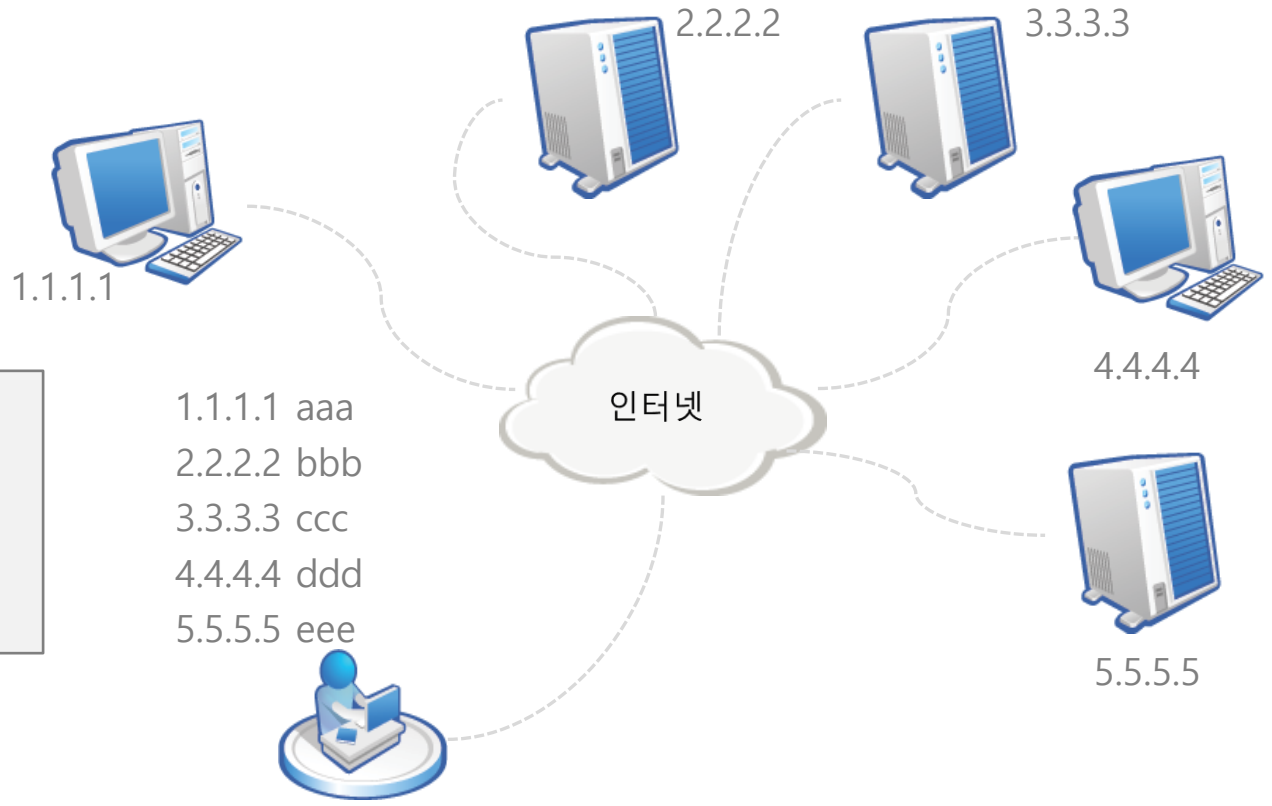


02_DNS- DNS에 대한 이해

❖ 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

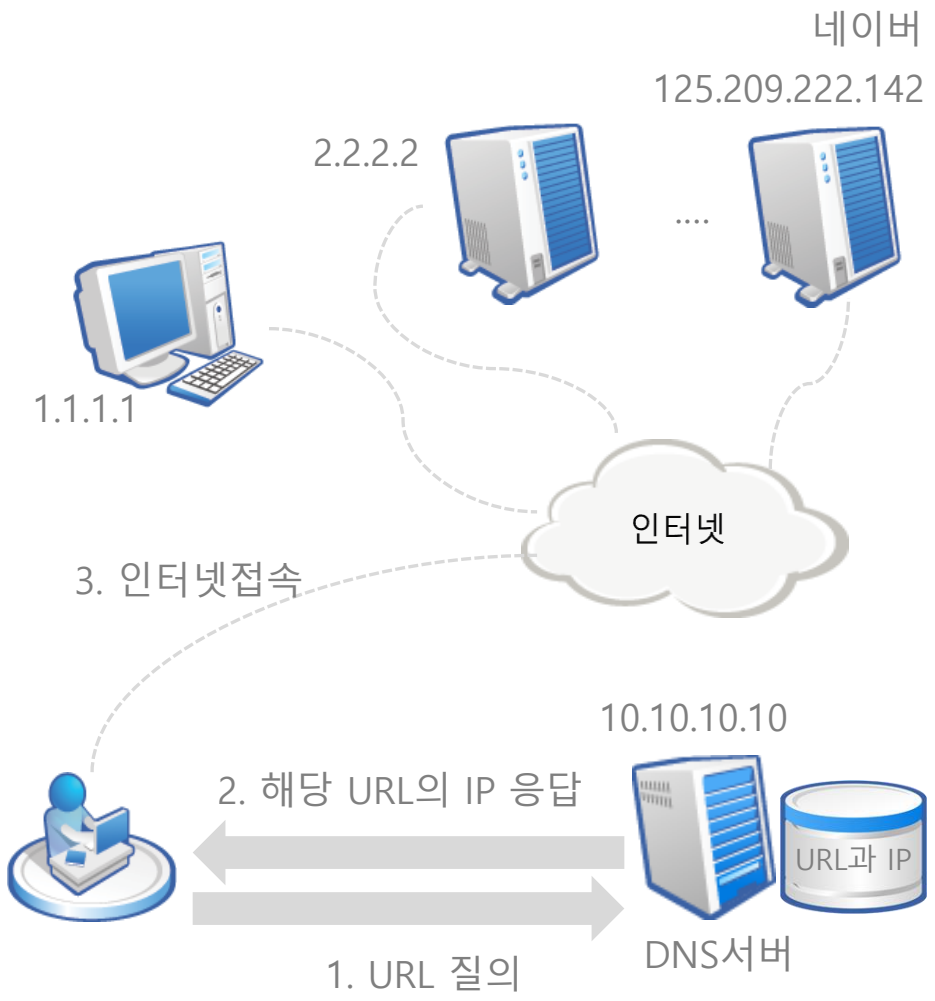
102.54.94.97	**rhino.acme.com**
38.25.63.10	**x.acme.com**
222.122.195.5	**www.naver.com**
127.0.0.1	**localhost**



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



❖ 운영체제별 DNS 서버 등록

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

❖ 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

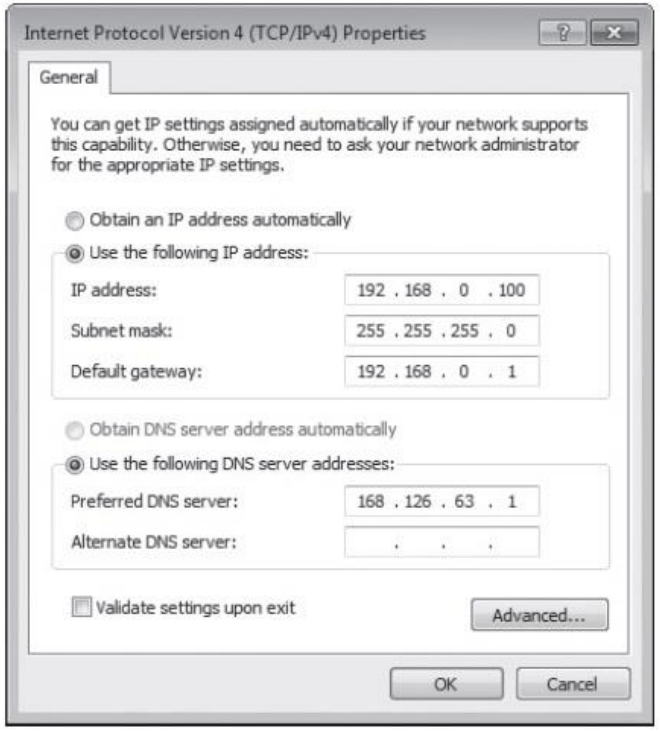


그림 3-14 인터넷 프로토콜(TCP/IP) 등록 정보

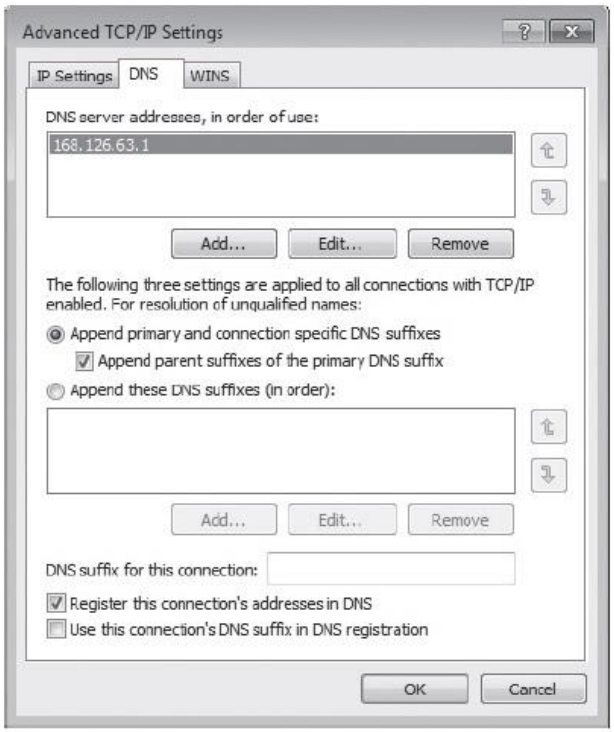


그림 3-15 TCP/IP 고급 설정

❖ 현재 운영 중인 DNS 서버 확인

- 명령 창에서 'ipconfig /all' 명령을 입력

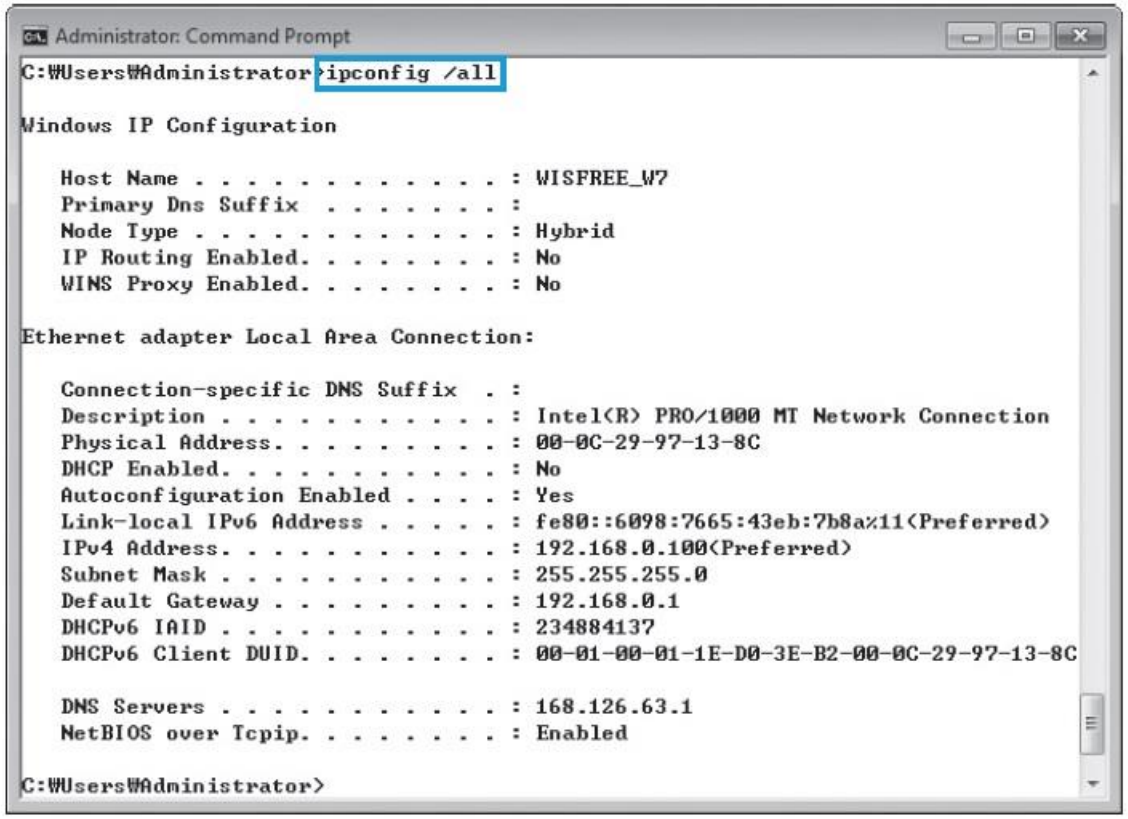
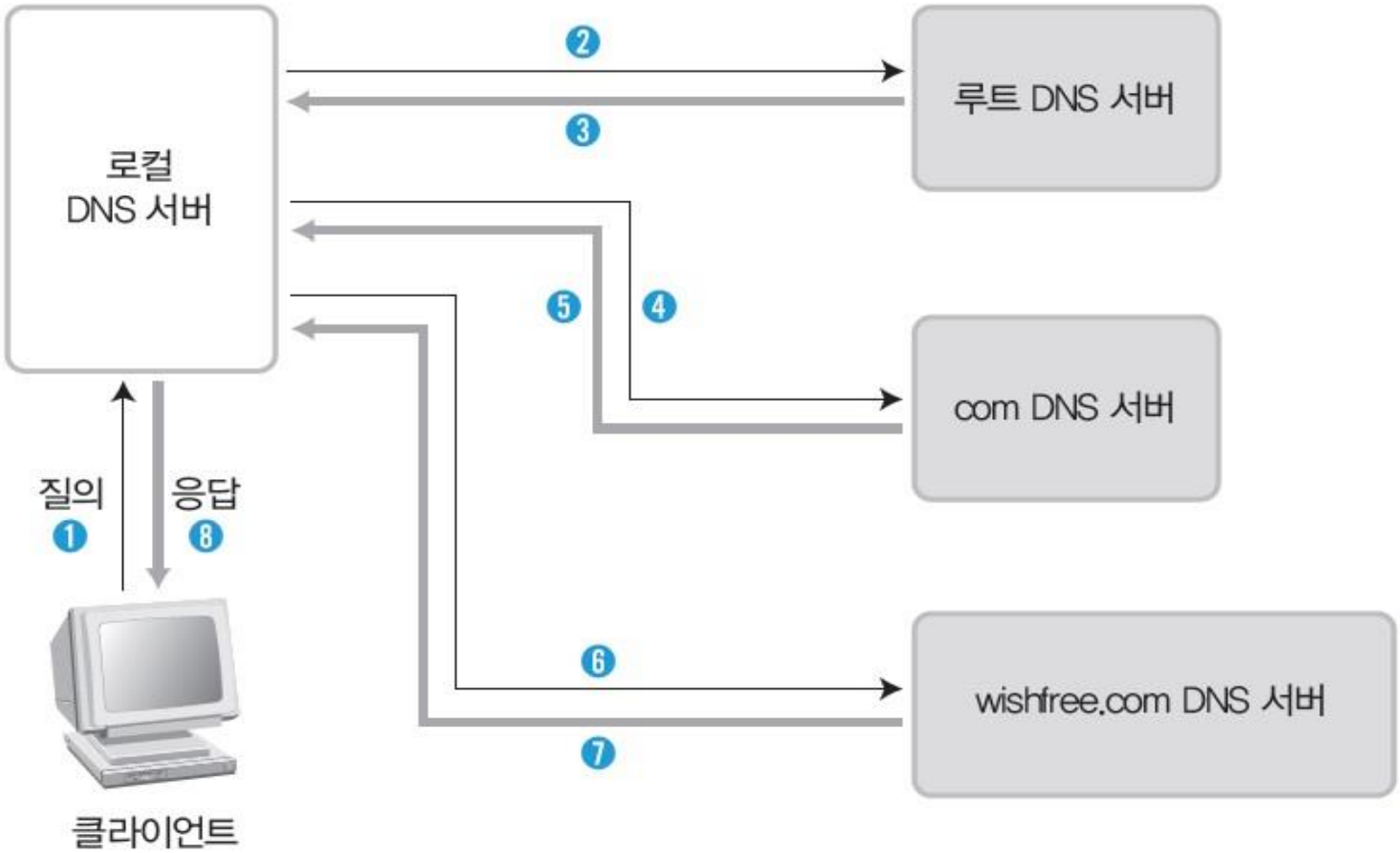


그림 3-16 'ipconfig /all' 명령으로 설정된 DNS 서버 확인하기

02_DNS- DNS의 동작 원리

❖ DNS 서버의 이름 해석 순서



❖ 시스템에 캐시된 DNS 정보 확인

ipconfig /displaydns

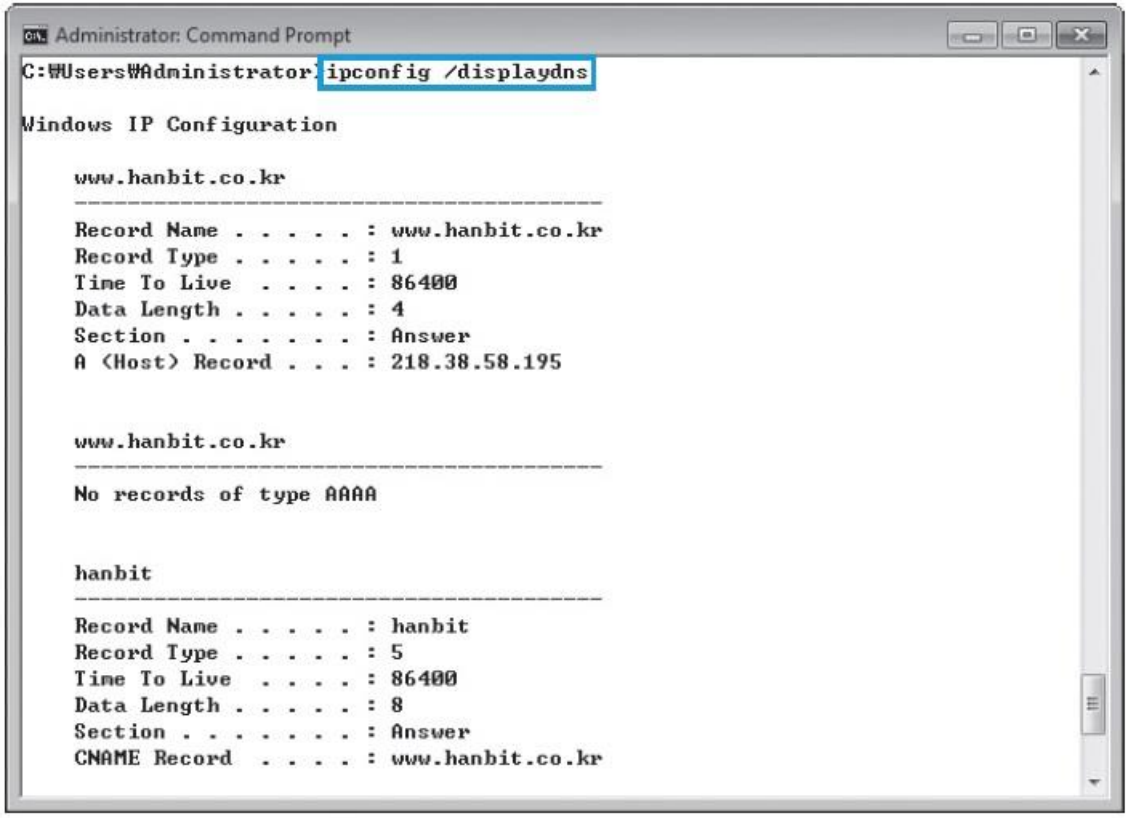


그림 3-18 윈도우에서 캐시된 DNS 정보 확인

❖ 시스템에 캐시된 DNS 정보 삭제

ipconfig /flushdns

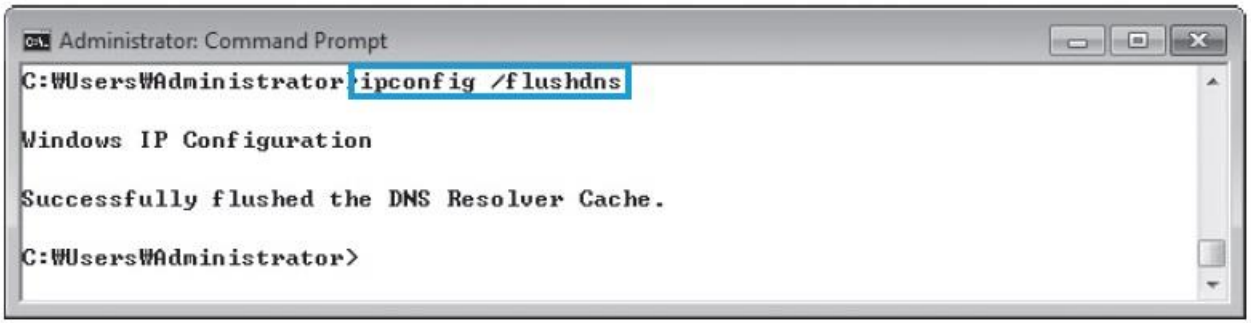


그림 3-19 윈도우에서 캐시된 DNS 정보 삭제

❖ 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

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

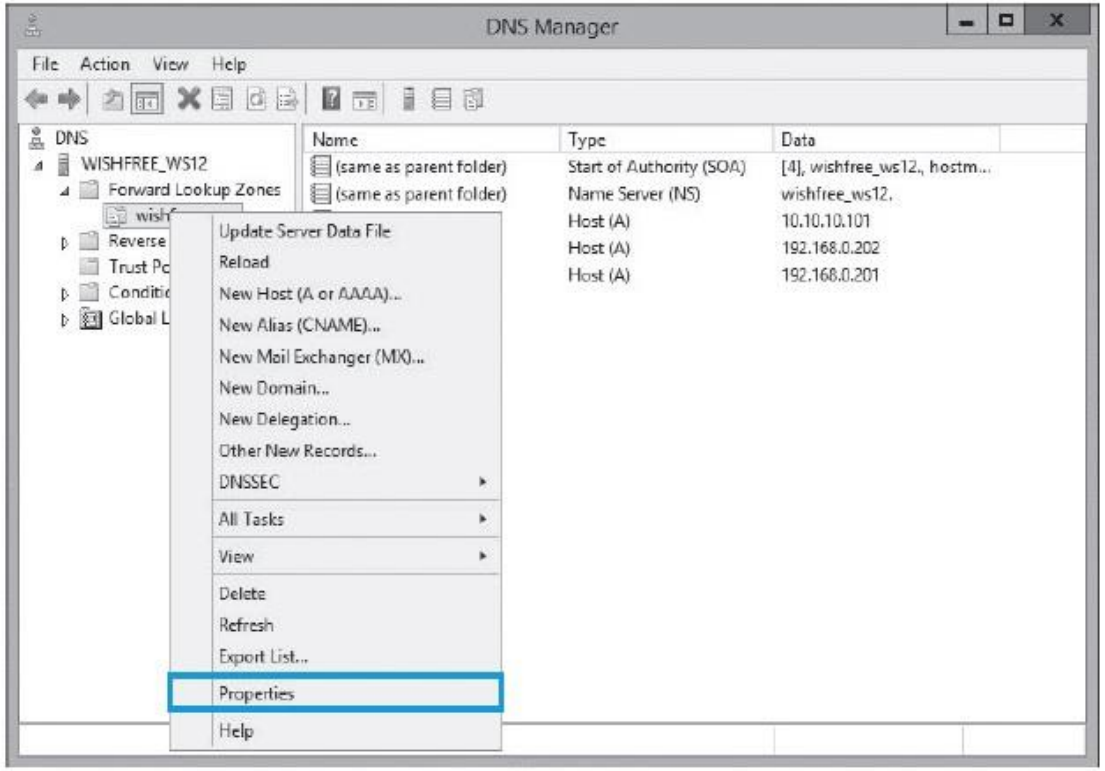
```
zone "wishfree.com" {
type master;
file "db.wishfree.com"
allow-transfer (10.10.10.1)
};
```

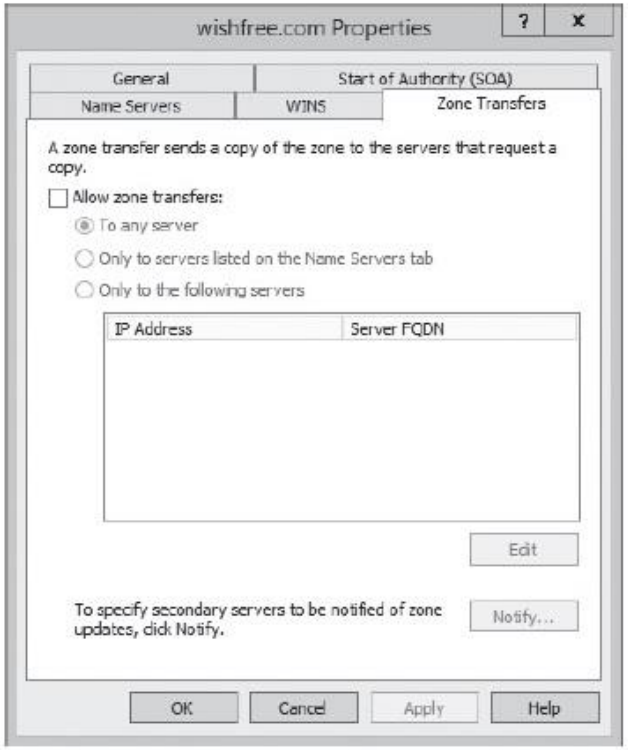
도메인 이름 입력

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

❖ 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

② 도메인 정보 수집하기

www.google.co.kr

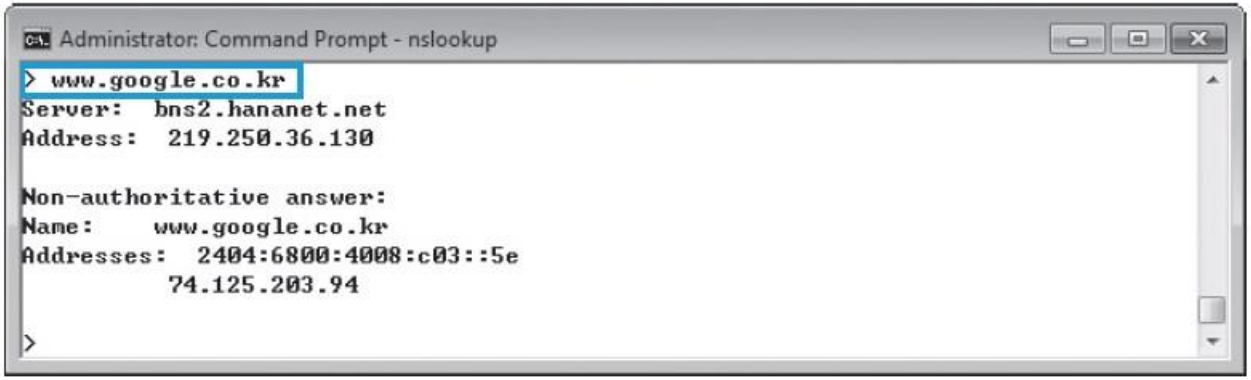


그림 3-23 www.google.co.kr에 대한 nslookup

② 도메인 정보 수집하기

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

set type=ns

google.co.kr

그림 3-24 www.google.co.kr의 DNS 서버 목록

② 도메인 정보 수집하기

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.

② 도메인 정보 수집하기

- 관련된 모든 서버 목록은 set type=all 명령으로 확인

set type=all

google.co.kr

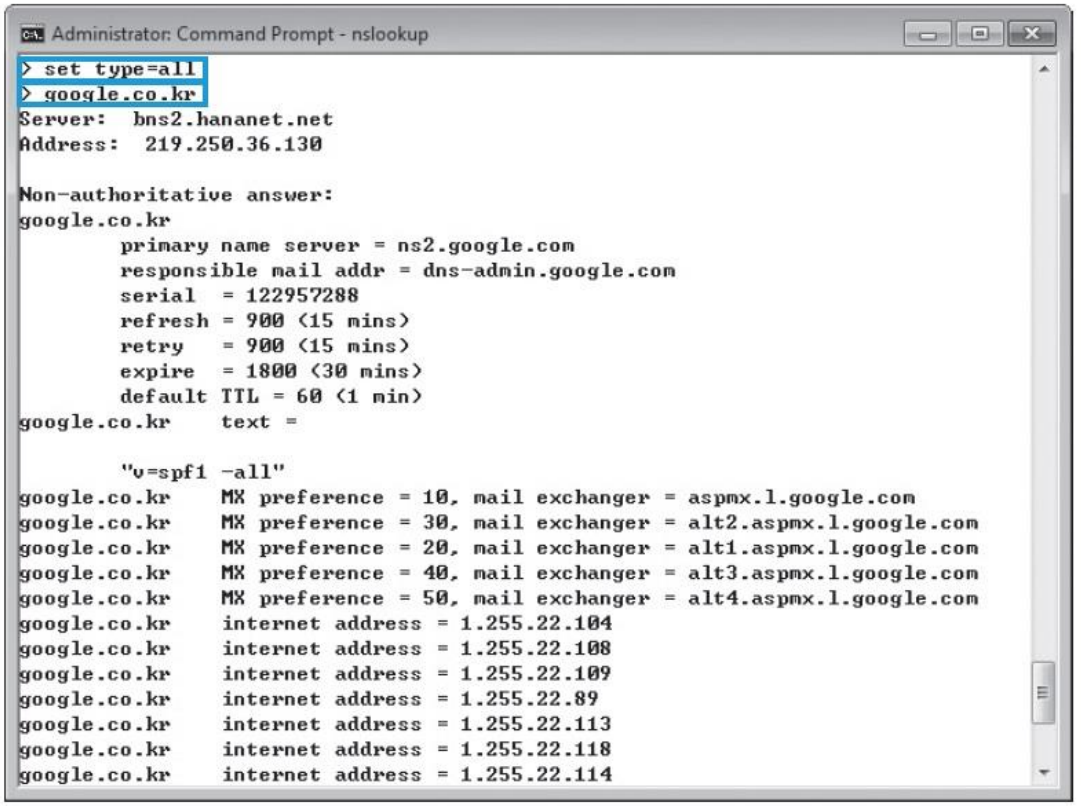


그림 3-25 google.co.kr에 등록된 모든 DNS 레코드

③ DNS 영역 전송하기

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

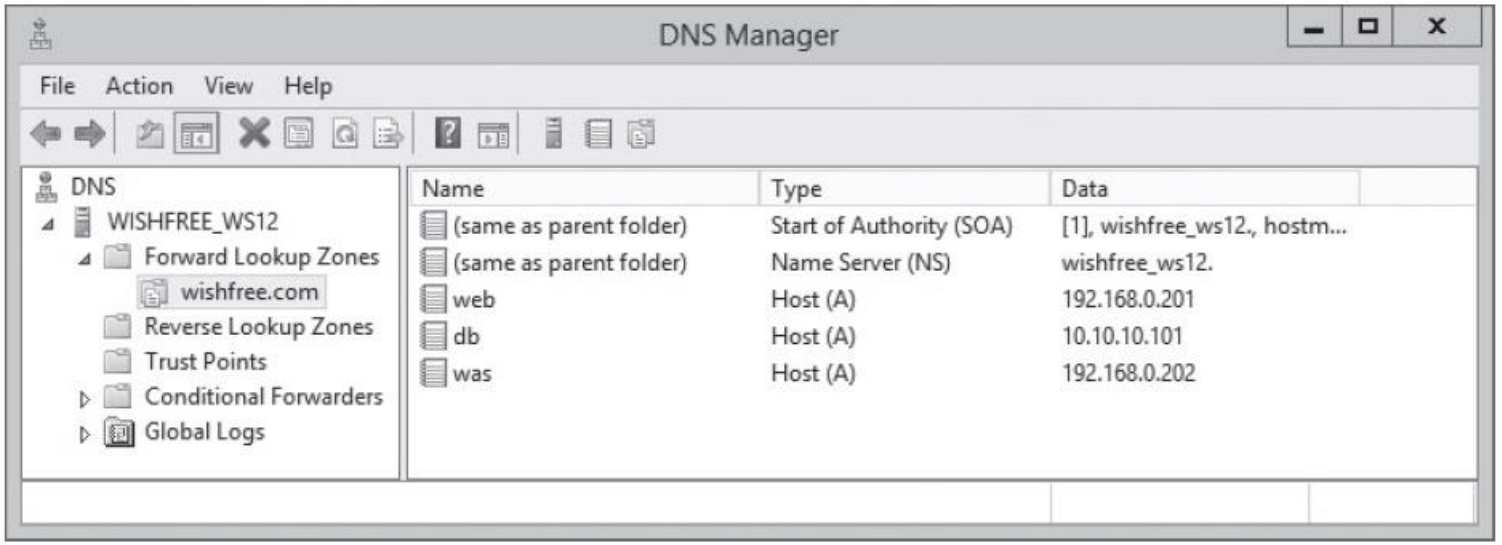


그림 3-26 wishfree.com 영역에 등록된 DNS 정보

③ DNS 영역 전송하기

- nslookup을 실행시킨 뒤, 서버를 설정한 DNS 서버로 바꿈.

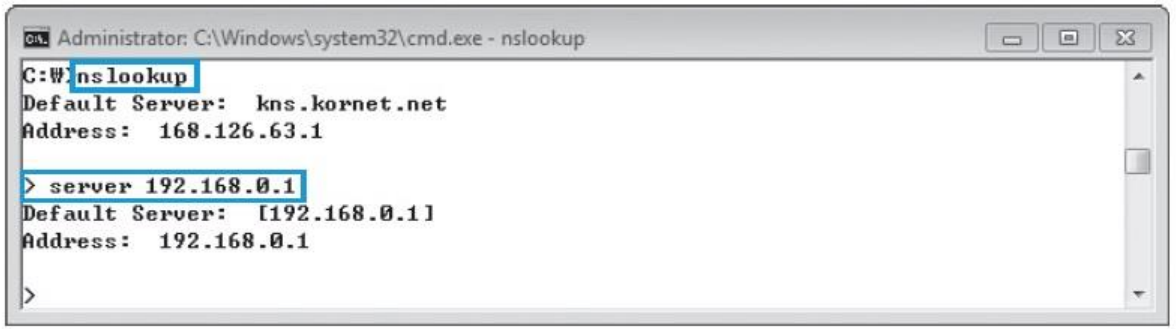


그림 3-27 DNS 변경

- web.wishfree.com과 같이 입력하여 해당 IP를 확인

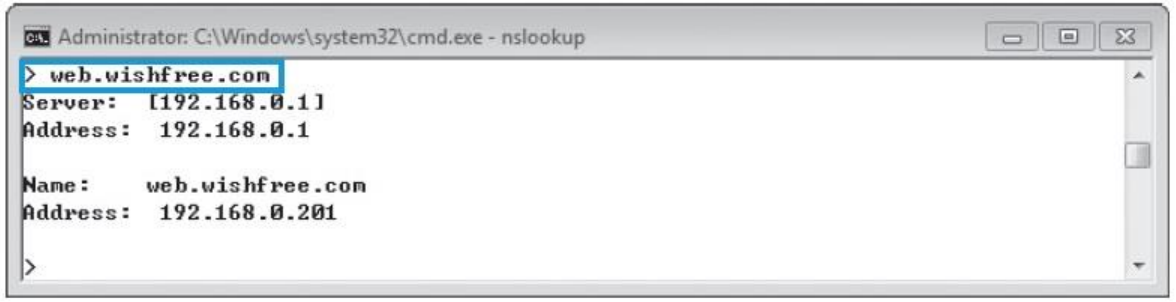


그림 3-28 web.wishfree.com에 대한 nslookup

③ DNS 영역 전송하기

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

set type=all

wishfree.com

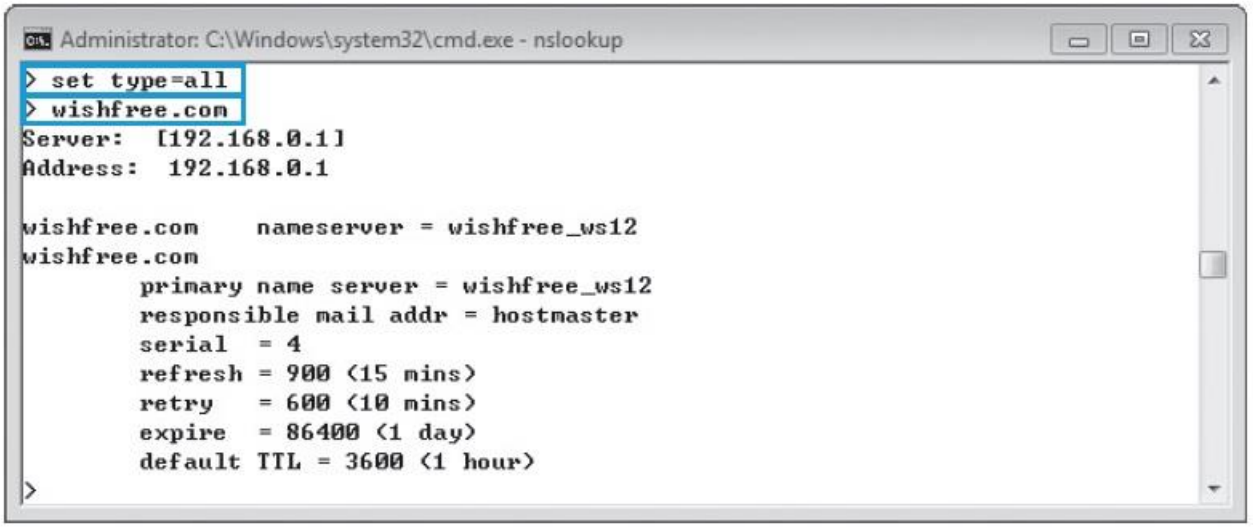


그림 3-29 wishfree.com에 대해 등록된 DNS 레코드 확인

③ DNS 영역 전송하기

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

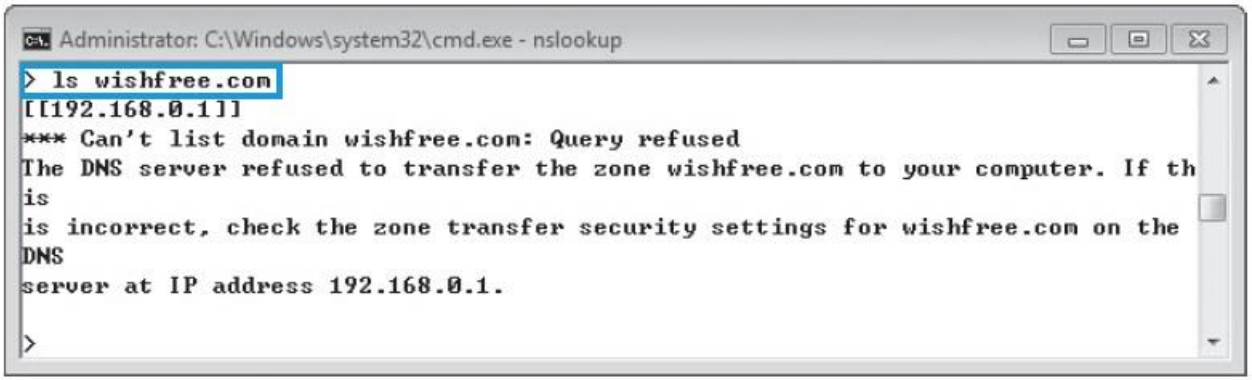


그림 3-30 wishfree.com에 대한 영역 전송 시도 – 실패

③ DNS 영역 전송하기

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

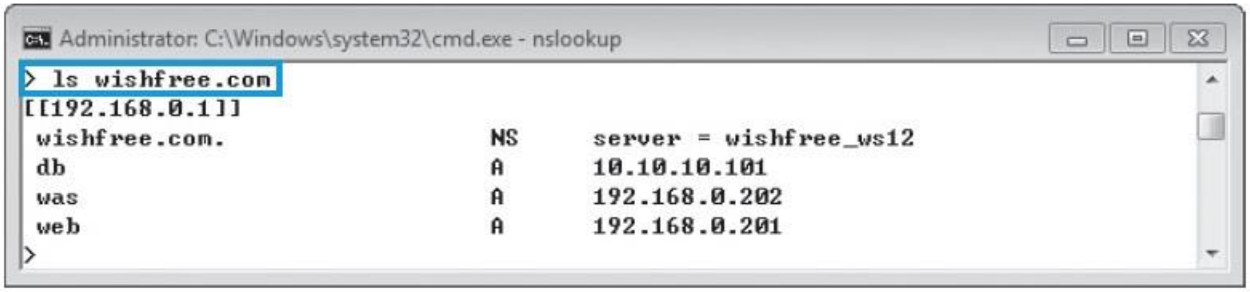
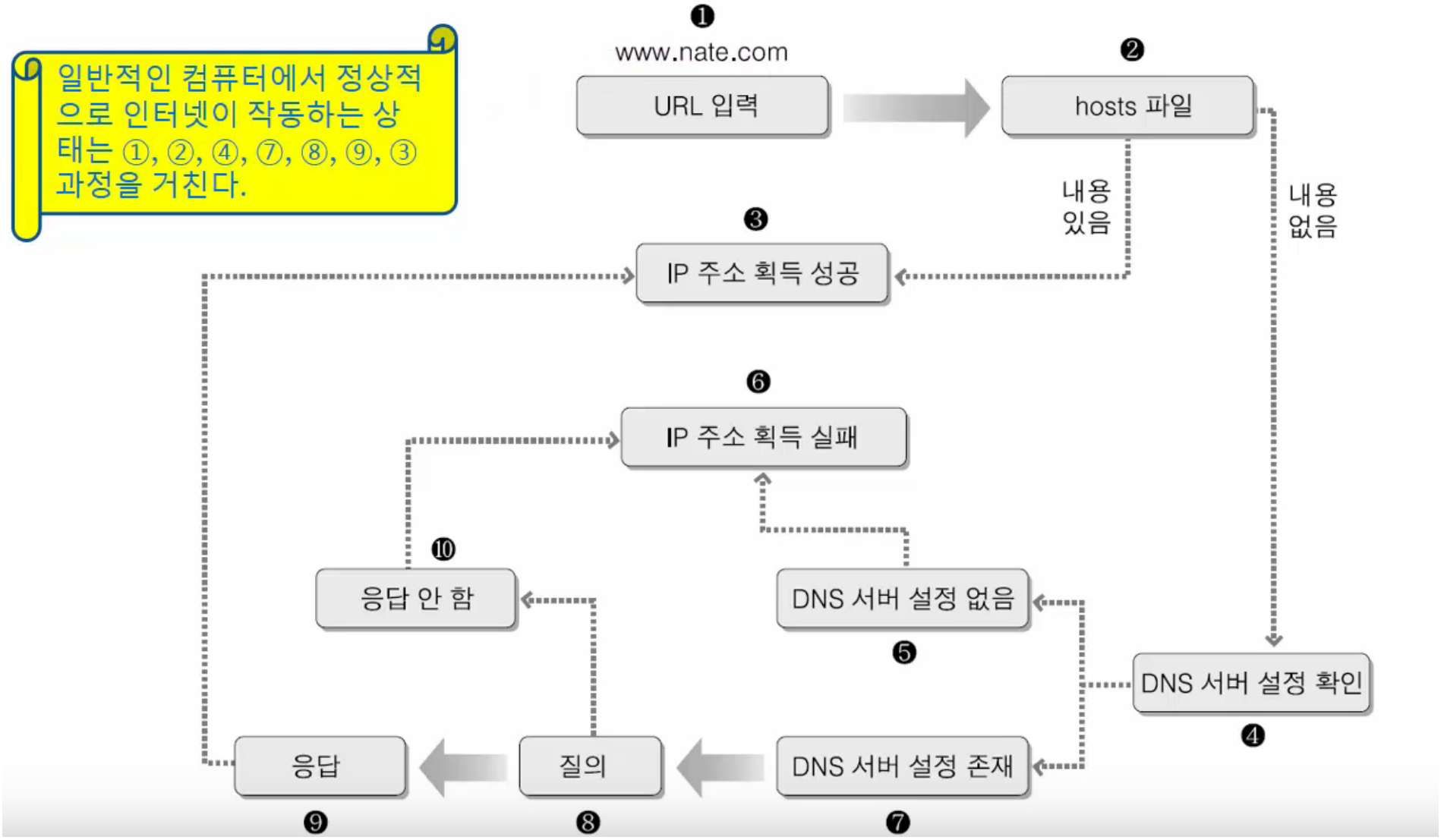


그림 3-31 wishfree.com에 대한 영역 전송 시도 – 성공

02_DNS- IP주소를 얻기 위한 내부 흐름

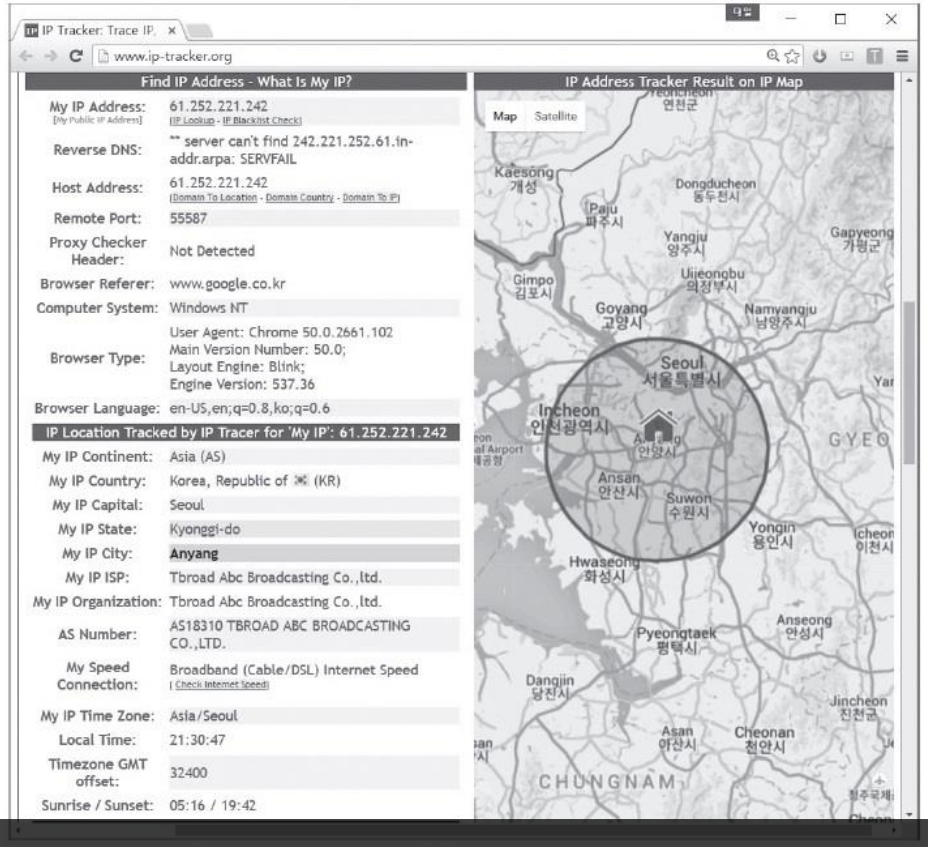
일반적인 컴퓨터에서 정상적으로 인터넷이 작동하는 상태는 ①, ②, ④, ⑦, ⑧, ⑨, ③ 과정을 거친다.



03_IP 주소 추적- IP 주소 추적의 기본

❖ IP 주소 추적의 기본

- IP 주소 추적의 기본은 출발지 IP 주소 확인하기



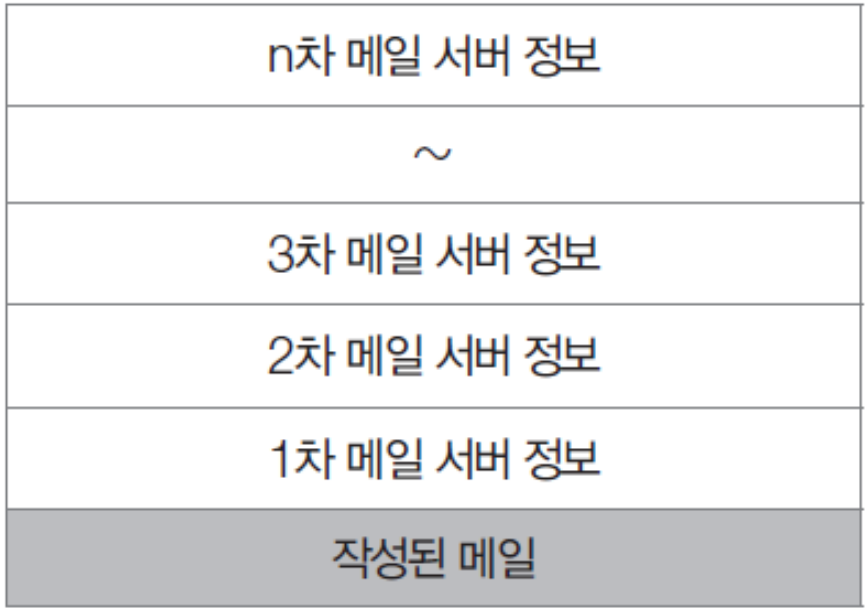
https://www.ip-tracker.org/

그림 4-1 IP 정보를 제공해 주는 사이트(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] → mx3.goolgle.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>
```

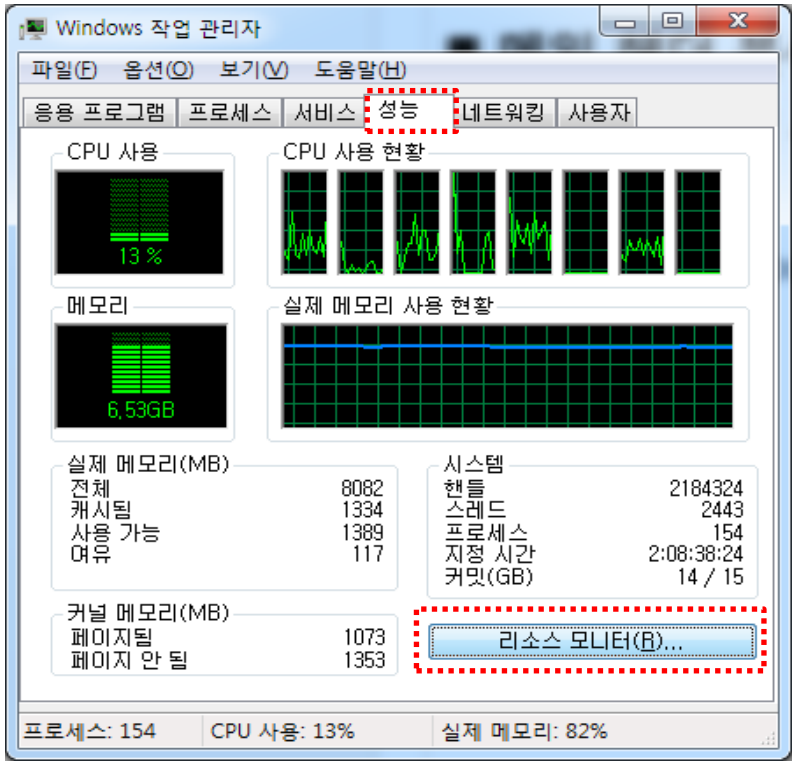
10.67.3.200 서버에 의해 메일이 수신

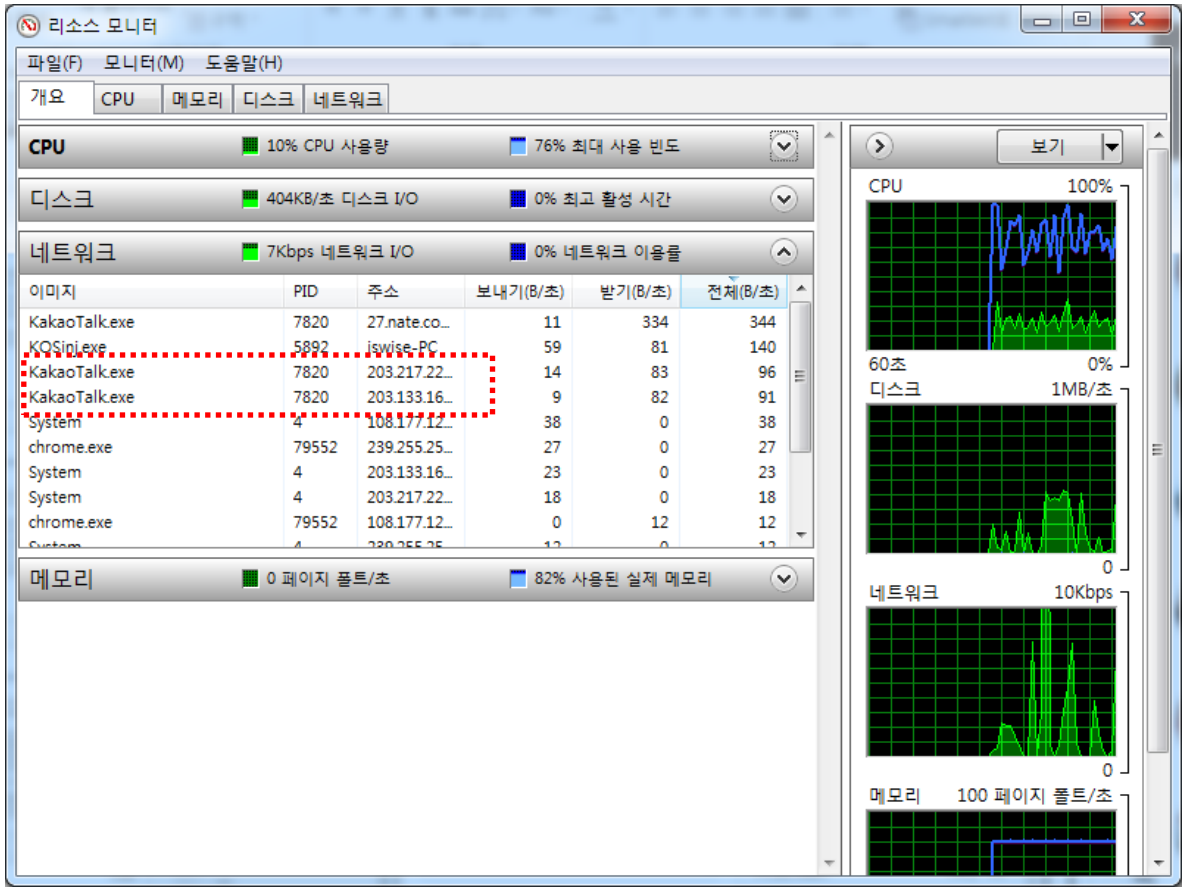
❖ 4차 메일 서버 정보

```
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)

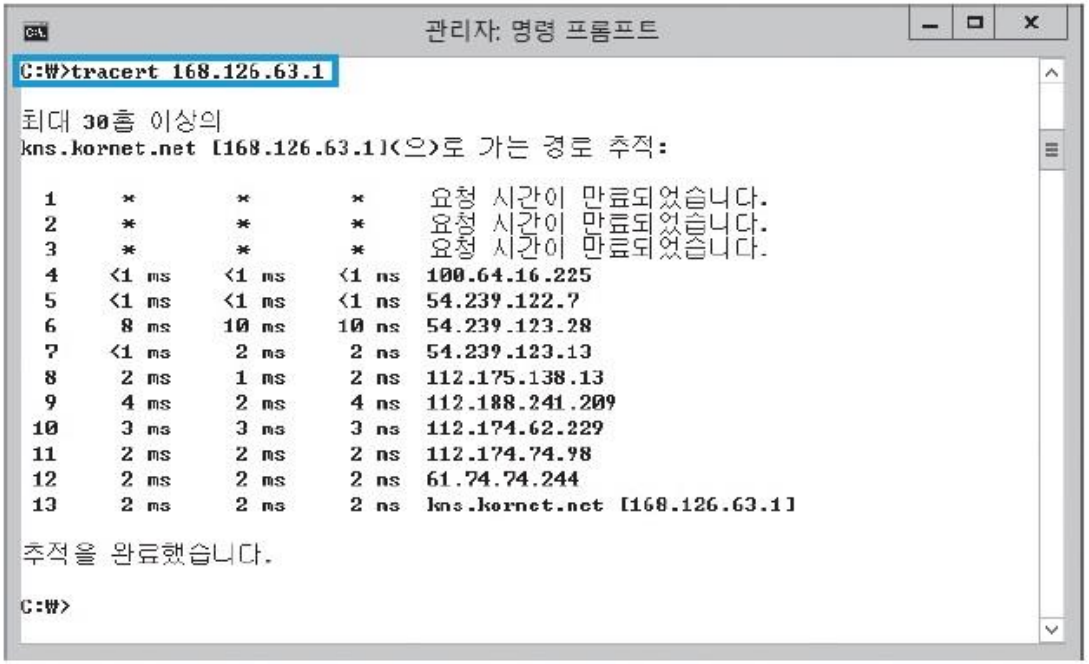
- 패킷이 목적지까지 도달하는 동안 거쳐가는 라우터의 IP를 확인하는 툴
- UDP와 ICMP, IP의 TTL 값을 이용
- 상대방의 IP 주소를 알고 있는 상태에서, 상대방이 속한 인터넷 구성 등을 짐작할 수 있음.
- traceroute를 수행할 때 경로가 매번 다르게 형성되다가 하나로 고정된다면 역추적을 당하고 있는 것일 수 있음.

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



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 달성될때까지 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 말하며 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