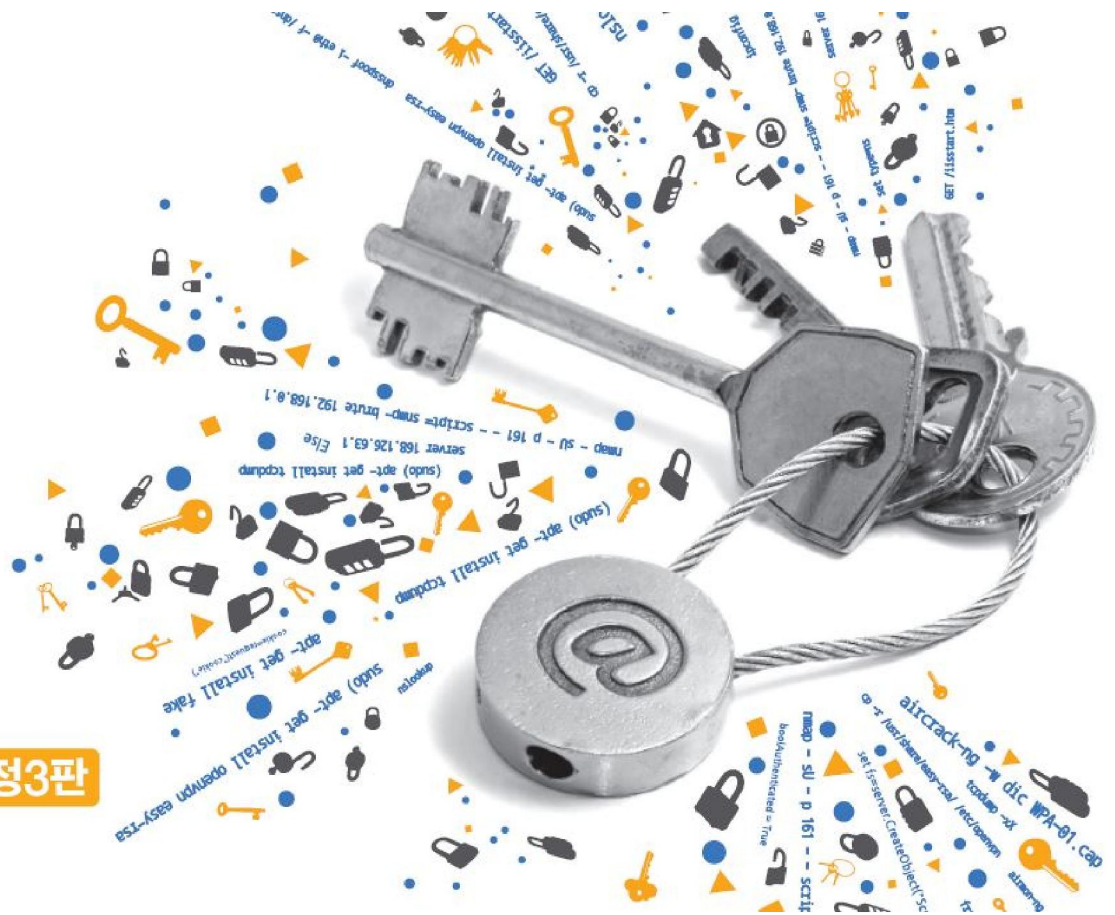




# 네트워크 해킹과 보안

정보 보안 개론과 실습

개정3판



## Chapter 04 IP 주소 추적

# 목차

**01** IP 주소 추적에 대한 이해

**02** IP 주소 추적하기

# 학습목표

- IP 주소를 추적하는 다양한 방법을 알아본다.
- 공격 대상의 IP 주소를 직접 추적해본다.

# 1. IP 주소 추적에 대한 이해

## 1.1 IP 주소 추적의 기본

### ■ IP 주소 추적의 기본

- IP 주소 추적의 기본은 출발지 IP 주소 확인하기

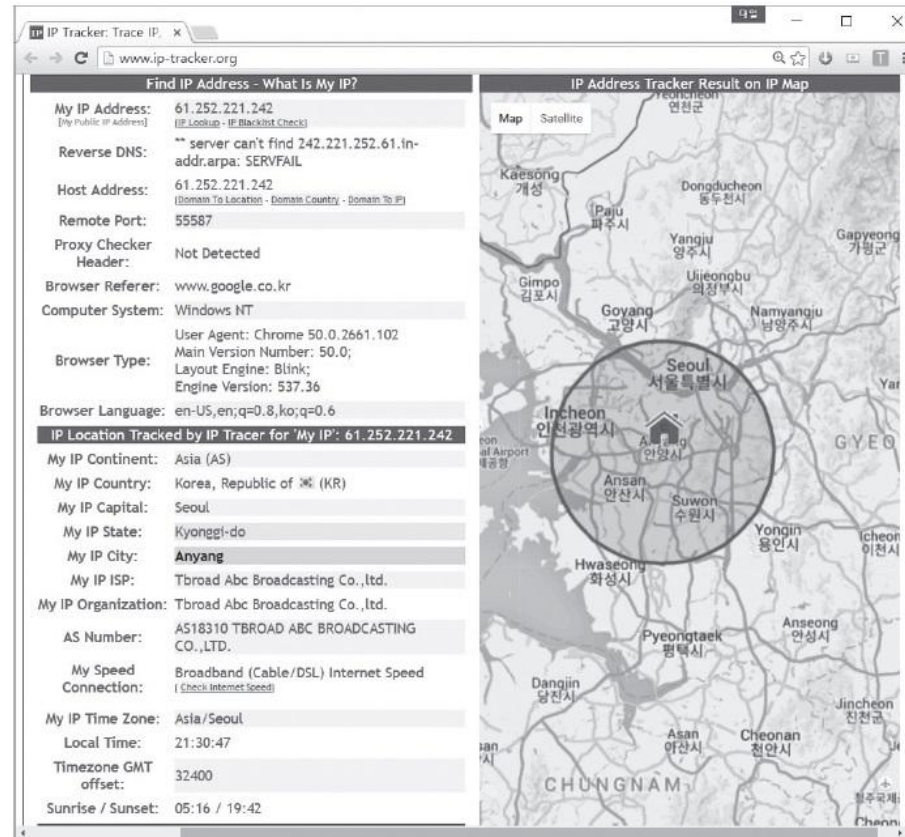


그림 4-1 IP 정보를 확인할 수 있는 사이트(www.ip-tracker.org)

## 2. IP 주소 추적하기

### 2.1 메일 이용하기

#### ■ 수신된 메일의 구조

- 작성된 메일은 여러 메일 서버를 거쳐 최종 목적지까지 전달

n차 메일 서버 정보
~
3차 메일 서버 정보
2차 메일 서버 정보
1차 메일 서버 정보
작성된 메일

## 2. IP 주소 추적하기

### 2.1 메일 이용하기

#### ① 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 ESMTTP 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>
```

## 2. IP 주소 추적하기

### 2.1 메일 이용하기

#### ② 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
```



## 2. IP 주소 추적하기

### 2.1 메일 이용하기

#### ② 2차 메일 서버 정보

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

표 4-1 SPF 결과 값

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.



## 2. IP 주소 추적하기

### 2.1 메일 이용하기

---

#### ③ 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>
```

#### ④ 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)
```

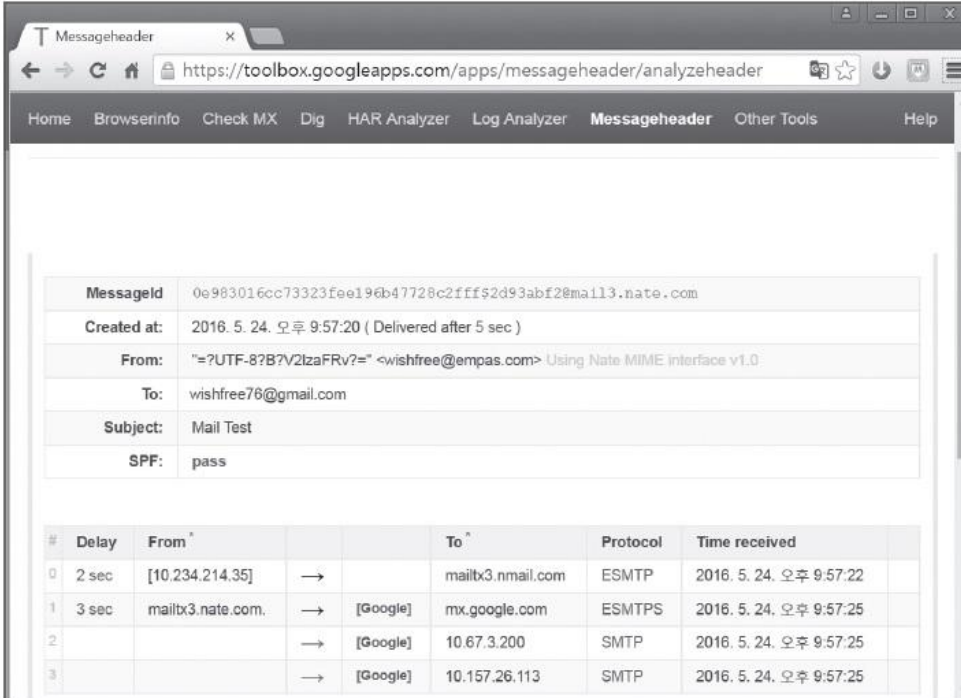
## 2. IP 주소 추적하기

### 2.1 메일 이용하기

#### ■ 메일 헤더 분석

- 전송된 메일 서버의 IP 주소 및 메일 전송자의 위치까지 확인 가능할 수 있어 매우 유용

<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>



The screenshot shows the Messageheader tool interface. The top navigation bar includes links for Home, Browserinfo, Check MX, Dig, HAR Analyzer, Log Analyzer, Messageheader, Other Tools, and Help. The main content area displays the following email header information:

Messageid	0e983016cc73323fee196b47728c2fff52d93abf2@mail3.nate.com
Created at	2016. 5. 24. 오후 9:57:20 ( Delivered after 5 sec )
From	"=?UTF-8?B?V2lzaFRv?=" <wishfree@empas.com> Using Nate MIME interface v1.0
To	wishfree76@gmail.com
Subject	Mail Test
SPF	pass

Below the header information is a routing table with the following data:

#	Delay	From *		To *	Protocol	Time received
0	2 sec	[10.234.214.35]	→	mailtx3.nmail.com	ESMTP	2016. 5. 24. 오후 9:57:22
1	3 sec	mailtx3.nate.com.	→	[Google] mx.google.com	ESMTPS	2016. 5. 24. 오후 9:57:25
2			→	[Google] 10.67.3.200	SMTP	2016. 5. 24. 오후 9:57:25
3			→	[Google] 10.157.26.113	SMTP	2016. 5. 24. 오후 9:57:25

그림 4-5 메일 헤더 분석 결과

## 2. IP 주소 추적하기

### 2.2 P2P 서비스 이용하기

---

#### ■ P2P 서비스

- 대표적인 예는 카카오톡, 스카이프, 네이트온 등의 메신저 또는 보이스톡과 같은 개인 간 통신 서비스, 토렌트와 같은 파일 공유 프로그램 등
- 'Peer to Peer', 즉 당사자 간의 통신이라는 특성 때문에 서비스를 이용하는 사용자의 IP 정보가 노출될 수 있음.

## 2. IP 주소 추적하기

### 2.2 P2P 서비스 이용하기

#### ■ P2P 서비스의 메시지 전송

- 일반적으로 텍스트를 교환하는 형태의 정보 교환에서는 사용자의 IP가 노출되지 않음.

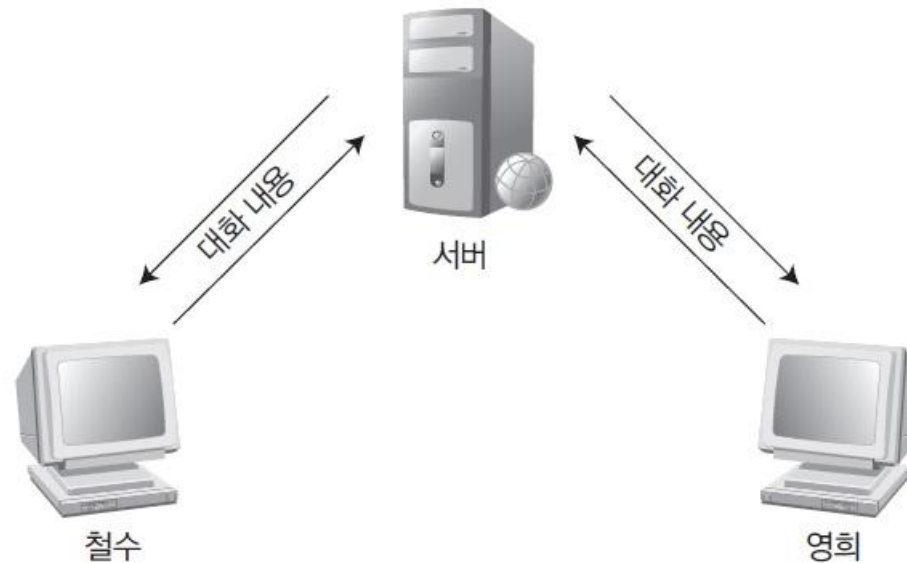


그림 4-6 P2P 서비스의 메시지 전송

## 2. IP 주소 추적하기

### 2.2 P2P 서비스 이용하기

#### ■ P2P 서비스의 파일 전송

- 많은 양의 데이터 전송이 필요하거나 인터넷 전화 서비스를 이용하는 경우 사용자 간의 직접 통신이 이루어져 상대방의 IP를 쉽게 확인할 수 있음.
- 최근에는 IP 노출을 제한하는 P2P 서비스가 점점 많아지고 있음.

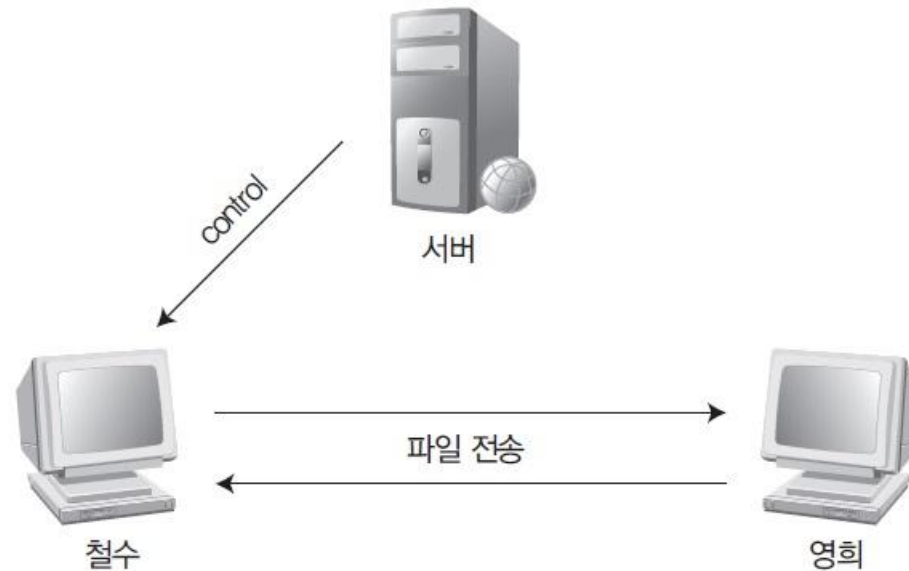


그림 4-7 P2P 서비스의 파일 전송

## 2. IP 주소 추적하기

### 2.3 웹 게시판 이용하기

---

#### ■ 웹 해킹 공격

- 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.

## 2. IP 주소 추적하기

### 실습 4-1 웹 접속자의 IP 주소 확인하기

- 실습환경**
- IIS 웹 서버가 설치된 서버(윈도우 서버 2012)
  - 서버와 같은 랜에 연결된 클라이언트 시스템(윈도우 7)

#### ① 웹 서버 설치 후 접속하기

- 윈도우 2012에 IIS를 설치한 뒤, 해당 웹 서버의 기본 페이지로 접속

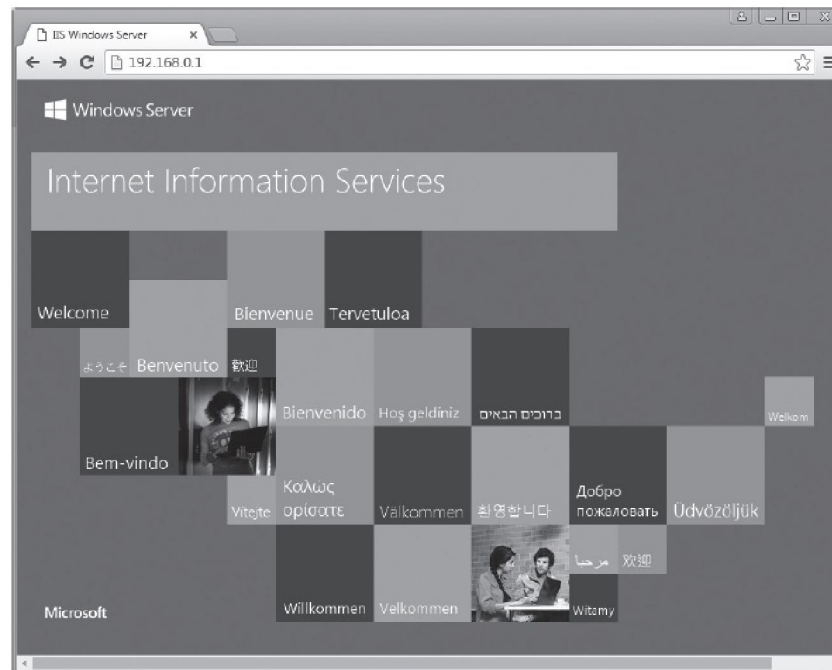


그림 4-8 IIS의 기본 페이지로 접근하기



## 2. IP 주소 추적하기

### 실습 4-1 웹 접속자의 IP 주소 확인하기

#### ② 웹 서버 로그 설정 확인하기

- [제어판]-[관리도구]-[IIS 매니저]에서 로그 생성에 관한 옵션 확인

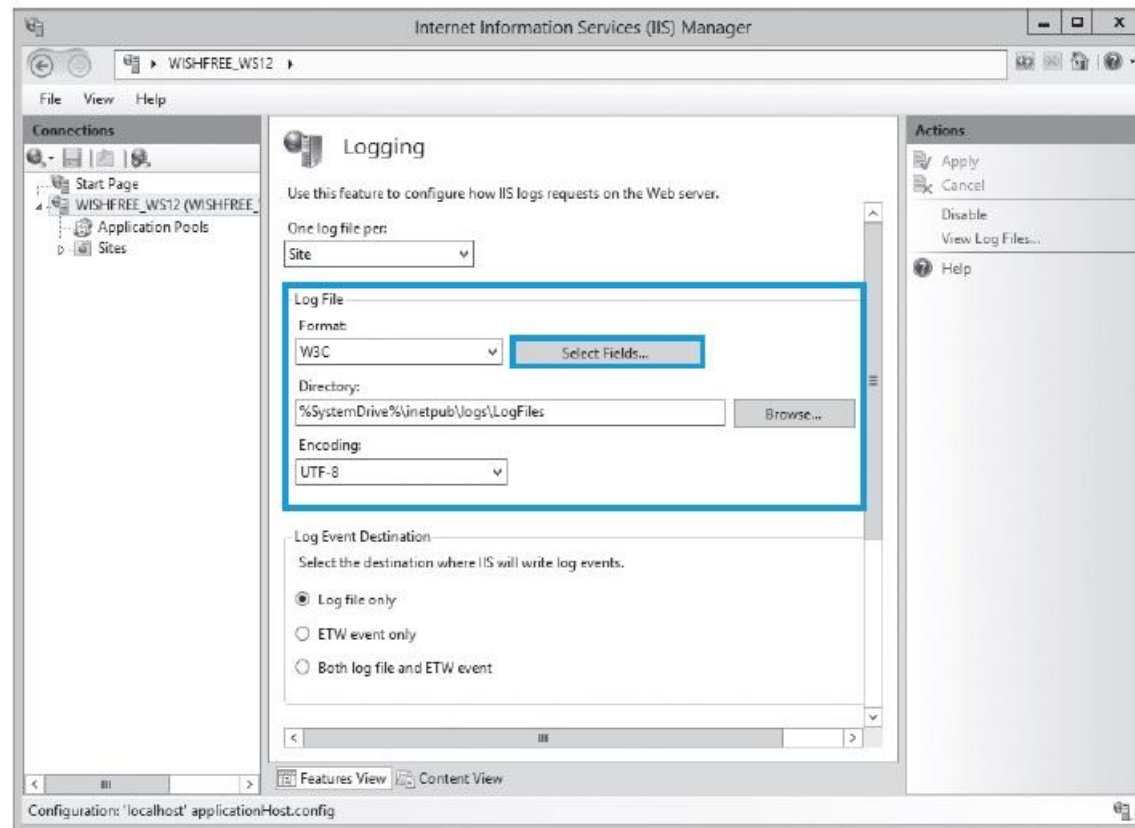


그림 4-9 IIS 로그 설정 페이지

## 2. IP 주소 추적하기

### 실습 4-1 웹 접속자의 IP 주소 확인하기

#### ② 웹 서버 로그 설정 확인하기

- <Select Fields>를 누르면 현재 설정된 로그 필드를 확인할 수 있음.

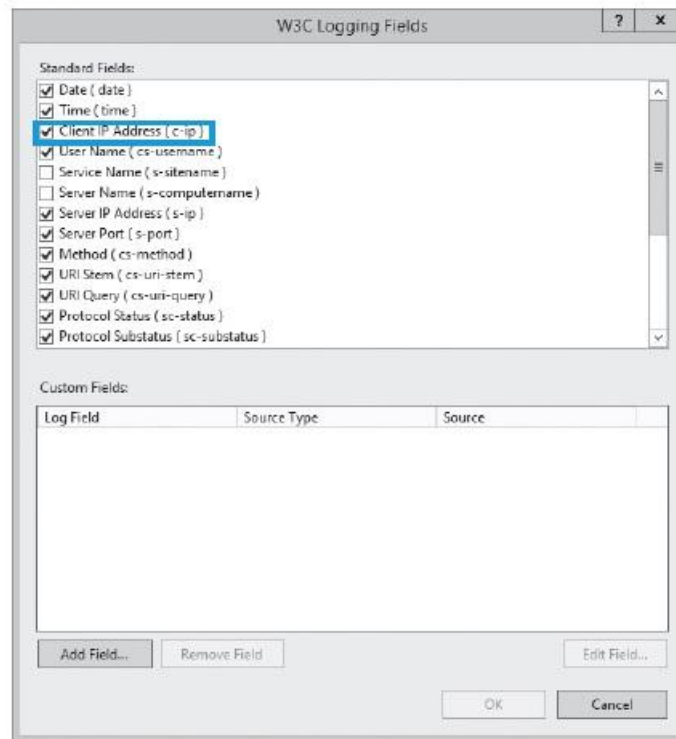


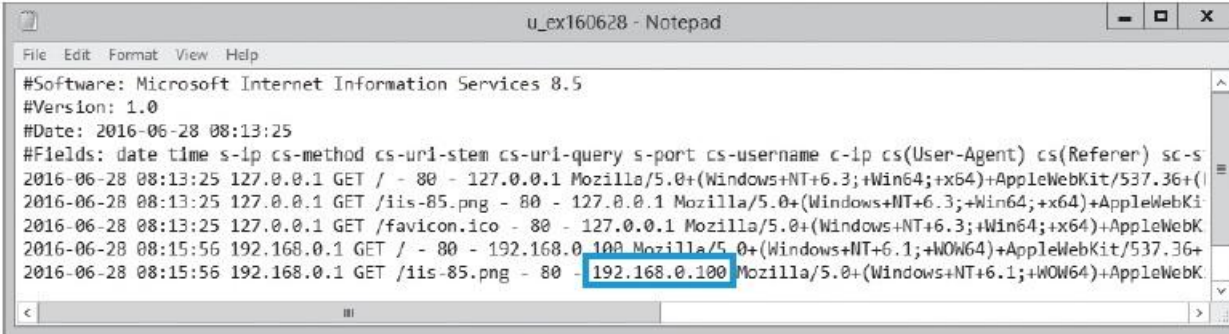
그림 4-10 IIS 로그 설정의 상세 항목

## 2. IP 주소 추적하기

### 실습 4-1 웹 접속자의 IP 주소 확인하기

#### ③ 웹 서버 로그 확인하기

- 보통 'C:\inetpub\logs\logfiles\W'에서 로그 파일 확인 가능
- 로그에서 접근한 클라이언트의 IP 관련 정보를 확인할 수 있음.



```
u_ex160628 - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 8.5
#Version: 1.0
#Date: 2016-06-28 08:13:25
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-s
2016-06-28 08:13:25 127.0.0.1 GET / - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKit/537.36+(l
2016-06-28 08:13:25 127.0.0.1 GET /iis-85.png - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebKi
2016-06-28 08:13:25 127.0.0.1 GET /favicon.ico - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+6.3;+Win64;+x64)+AppleWebK
2016-06-28 08:15:56 192.168.0.1 GET / - 80 - 192.168.0.100 Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+
2016-06-28 08:15:56 192.168.0.1 GET /iis-85.png - 80 - 192.168.0.100 Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebK
```

그림 4-11 웹 서버에 접속한 로그

## 2. IP 주소 추적하기

### 2.4 Traceroute 이용하기

---

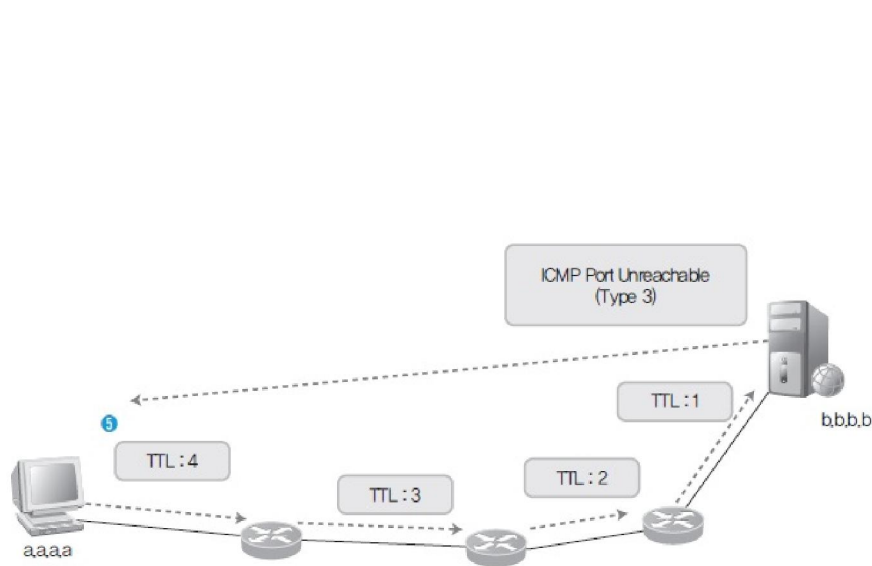
#### ■ traceroute(트레이스라우트)

- 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.

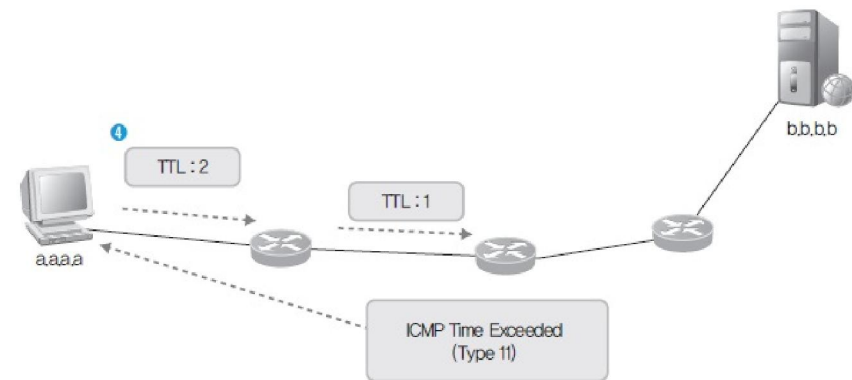
## 2. IP 주소 추적하기

### 2.4 Traceroute 이용하기

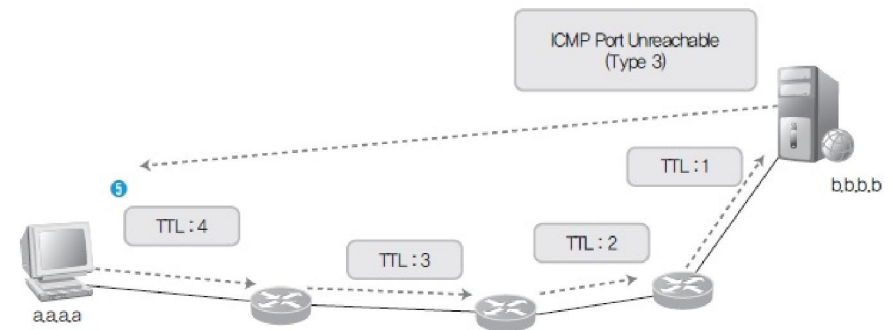
#### ■ traceroute(트레이스라우트)



(c) traceroute의 목적지 도달 시 패킷 흐름  
그림 4-12 traceroute의 패킷 흐름



(b) traceroute의 두 번째 패킷 흐름



(c) traceroute의 목적지 도달 시 패킷 흐름  
그림 4-12 traceroute의 패킷 흐름

## 2. IP 주소 추적하기

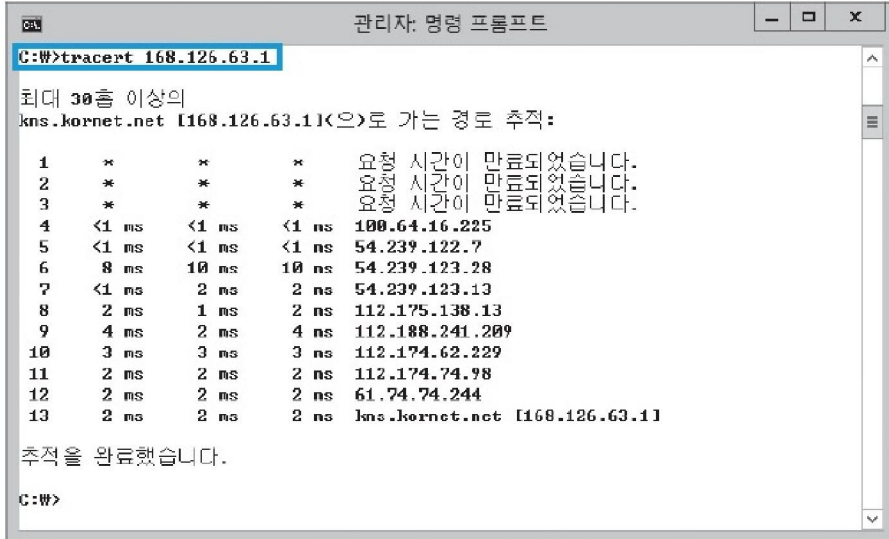
### 실습 4-2 traceroute를 이용해 라우팅 경로 확인하기

- 실습환경**
- 인터넷이 연결된 클라이언트 시스템(윈도우 서버 2012)
  - 필요 프로그램 : traceroute, Open Visual Trace Route, Sam Spade

#### ① 패킷 내용 확인하기

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

tracert 168.126.63.1



```
관리자: 명령 프롬프트
C:\W>tracert 168.126.63.1

최대 30홉 이상의
kns.kornet.net [168.126.63.1](<)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 ms 54.239.123.28
 7  <1 ms 2 ms 2 ms 54.239.123.13
 8  2 ms  1 ms 2 ms 112.175.138.13
 9  4 ms  2 ms 4 ms 112.188.241.209
10  3 ms  3 ms 3 ms 112.174.62.229
11  2 ms  2 ms 2 ms 112.174.74.98
12  2 ms  2 ms 2 ms 61.74.74.244
13  2 ms  2 ms 2 ms kns.kornet.net [168.126.63.1]

추적을 완료했습니다.

C:\W>
```

그림 4-13 tracert 명령 실행하기

## 2. IP 주소 추적하기

### 실습 4-2 traceroute를 이용해 라우팅 경로 확인하기

#### ① 패킷 내용 확인하기

- Open Visual TraceRoute는 지구본상에 패킷의 흐름을 그려주어 패킷의 지리적인 위치를 확인할 수 있음.

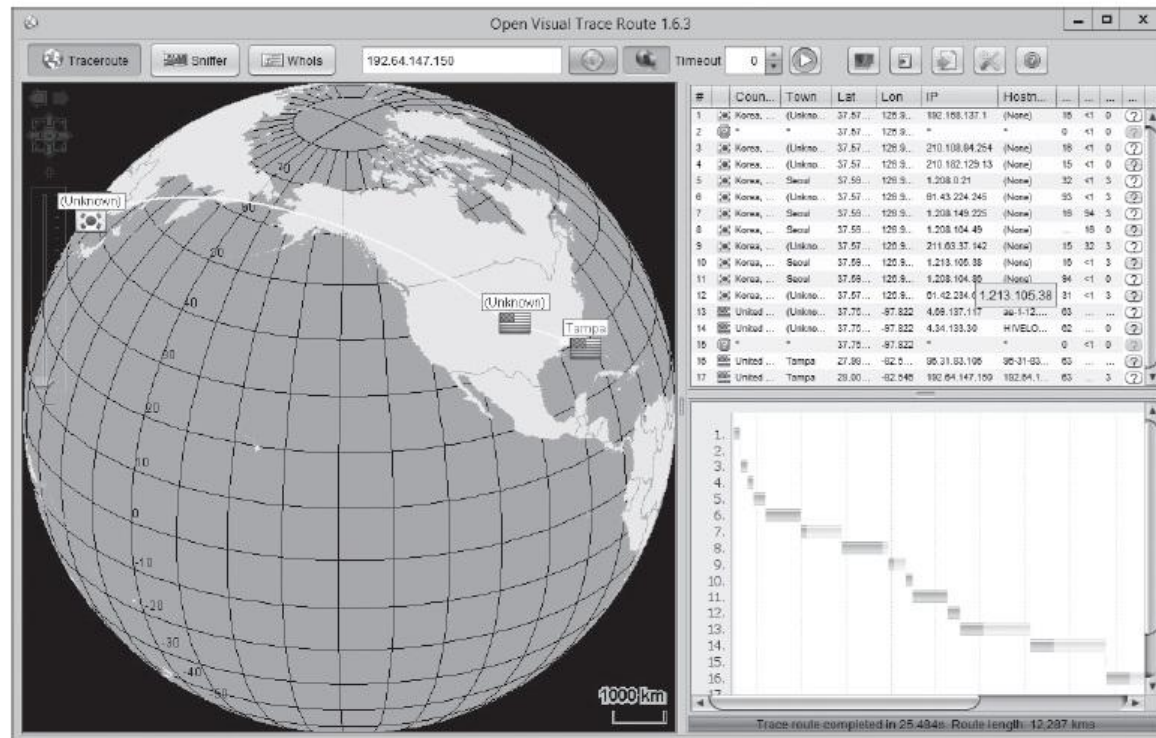


그림 4-14 Open Visual Trace Route를 이용한 traceroute



## 2. IP 주소 추적하기

### 실습 4-2 traceroute를 이용해 라우팅 경로 확인하기

#### ① 패킷 내용 확인하기

- 전통적인 툴인 Sam Spade(샘 스페이드)

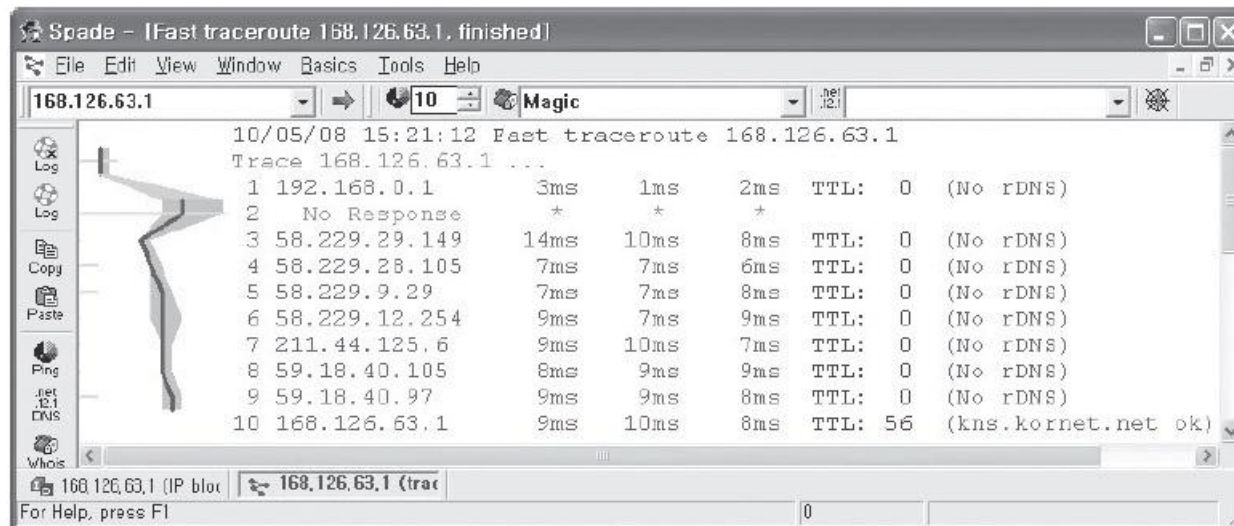
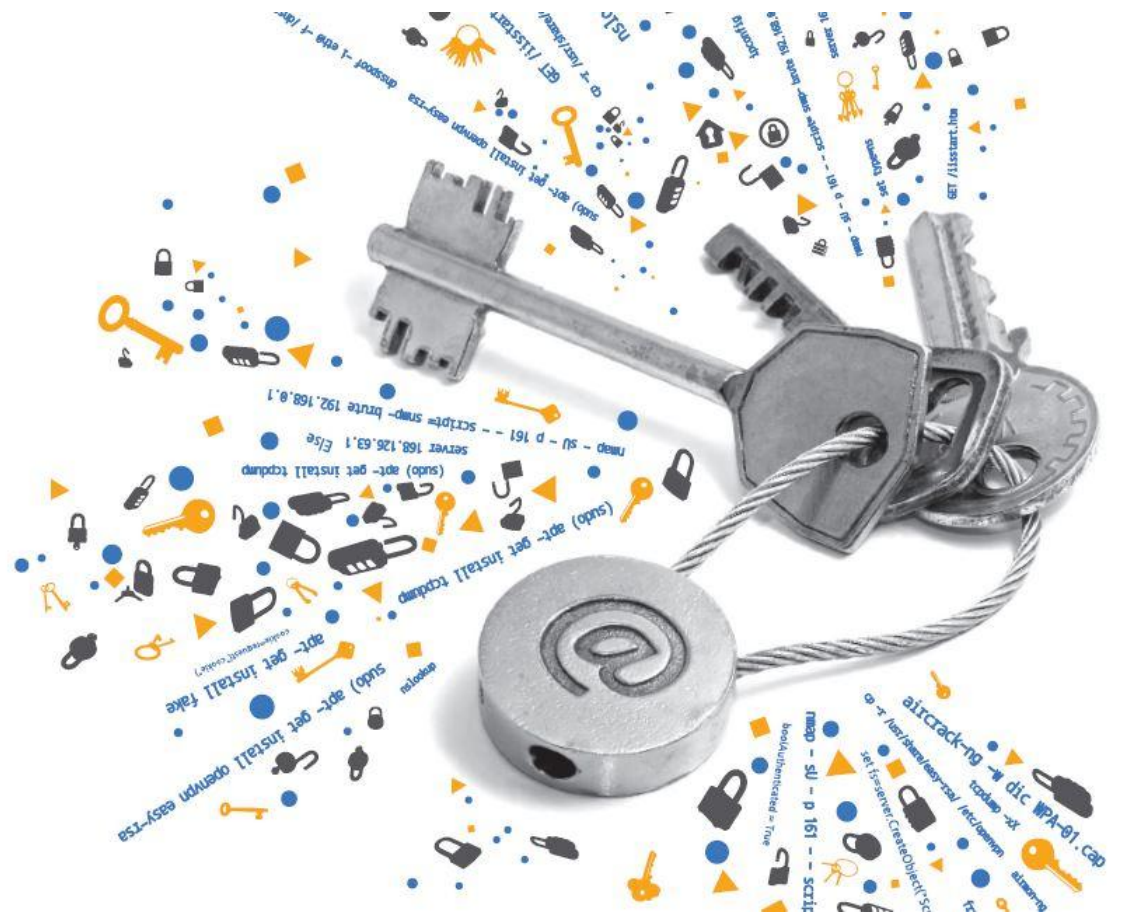


그림 4-15 Sam Spade를 이용한 traceroute



# 감사합니다.

## 네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습

---