# 컴퓨터 보안_02

실습 10주차

동국대학교 CSDC Lab.
실습조교 김선규
2023.05.10 (Wed.)

# Index

1. 실습 10주차 소개

- 스노트(Snort) 윈도우 시스템 구축하기
- 무선 네트워크 분석을 위한 WiFi 탐색툴 Vistumbler 사용하기

2. Q & A

# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

dongguk UNIVERSITY

## ➢ 스노트(Snort) 윈도우 시스템 구축하기

- 본 과제에서는 스노트(Snort) 시스템을 윈도우 기반의 PC에 구축하는 것이다. 스노트(Snort)는 오픈 소스인데 네트워크 침입 차단 시스템(NIPS: Network Intrusion Prevention System)이자, 동시에 네트워크 침입 탐지 시스템(NIDS: Network Intrusion Detection System)으로서, 마틴 로시가 1998년에 개발하였다. 스노트는 현재 로시가 창립자이자 개발자로 있는 Sourcefire라는 회사에 의해 개발되고 있으며, 이 회사는 2013년 이후로 시스코 시스템즈가 소유중이다.

- 스노트의 네트워크 기반 침입 탐지 시스템(NIDS)은 실시간 트래픽 분석과 IP에서의 패킷 로깅을 수행하는 능력을 갖는다. 스노트는 프로토콜 분석, 내용 검색 그리고 매칭을 수행한다. 이 프로그램은 또한 조사나 공격을 탐지하는데 사용될 수 있다. 이러한 조사나 공격으로는 공용 TCP/IP 스택 핑거프린팅, 공용 게이트웨이 인터페이스, 버퍼 오버플로, 서버 메시지 블록 조사 그리고 스텔스 포트 스캔 등이 있다.

- 스노트는 3가지의 주요 모드로 설정될 수 있다. 스니퍼, 패킷 로거 그리고 네트워크 침입 탐지 모드가 있다. 스니퍼 모드에서 프로그램은 네트워크 패킷을 읽고 콘솔에 보여준다. 패킷 로거 모드에서 프로그램은 패킷을 디스크에 기록한다. 침입 탐지 모드에서 프로그램은 네트워크 트래픽을 모니터하고 사용자에 의해 정의된 규칙에 반하는지를 분석한다. 프로그램은 그 후 특정한 동작을 수행한다.

# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

dongguk UNIVERSITY

➢ **[실습 내용]**

- 이번 실습은 스노트를 윈도우 PC에 설치하고 설정하는 프로세스에 대한 가이드를 제공한다. 필요한 도구는 윈도우 7, 8, 10 혹은 11이 설치된 컴퓨터와 스노트 소프트웨어이다.

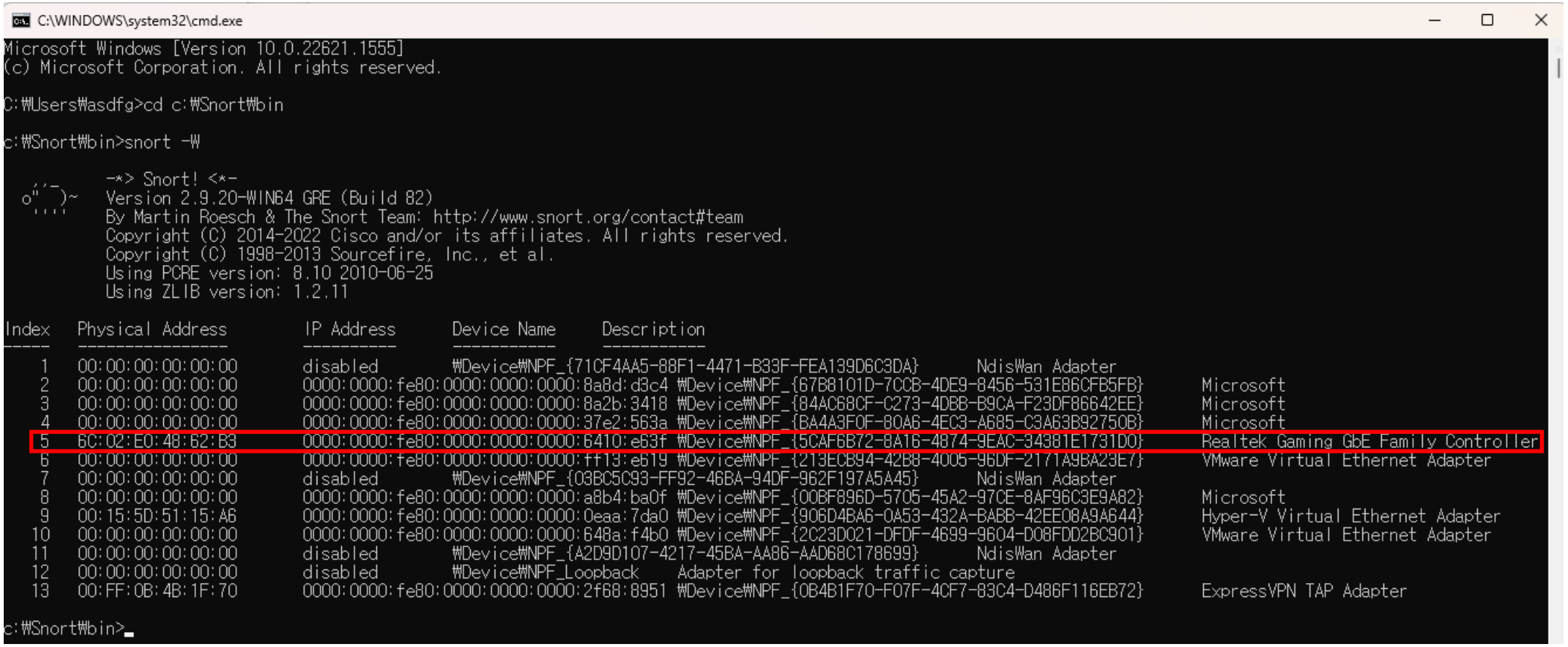
1. https://www.winpcap.org/install/default.htm에서 Version 4.1.3 Installer for Windows (Winpcap.exe)를 다운로드 한다. 이 파일은 하위 레벨 패킷 드라이버인데 스노트가 작동하기 위해 필요하다. Next를 통해 계속 설치하면 된다.
2. https://npcap.updatestar.com/ko에서 Npcap의 최신 버전을 설치한다.
3. https://www.snort.org/downloads에서 스노트 최신 버전(Snort_2_9_20_Installer.x64.exe)을 다운로드 하고 설치를 시작한다.
4. Next를 통해 계속 설치하면 된다. 설치 완료 후 C:\Snort\etc 폴더로 이동한다.
5. snort.conf을 메모장(notepad)로 오픈한다. 컨트롤 + F 를 통해서 “HOME_NET”를 검색한다.
6. 변수구문 ipvar HOME_NET Any를 검색하고 해당 네트워크에 맞게 세팅한다 (예, ipvar HOME_NET localhost/24)
7. 문구 include classification.conf를 검색하고 다음과 같이 변경한다 (include c:\snort\etc\classification.config).
8. 문구 include reference.config를 검색하고 다음과 같이 변경한다 (include c:\snort\etc\reference.config).

# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

9. 저장하고 파일을 닫는다. 스노트가 제대로 설정되었는지 확인하기 위해 2개의 명령 프롬프트를 연다.

10. 첫번째 프롬프트에서는 c:\Snort\bin 폴더로 이동하여 snort -W를 입력한다.

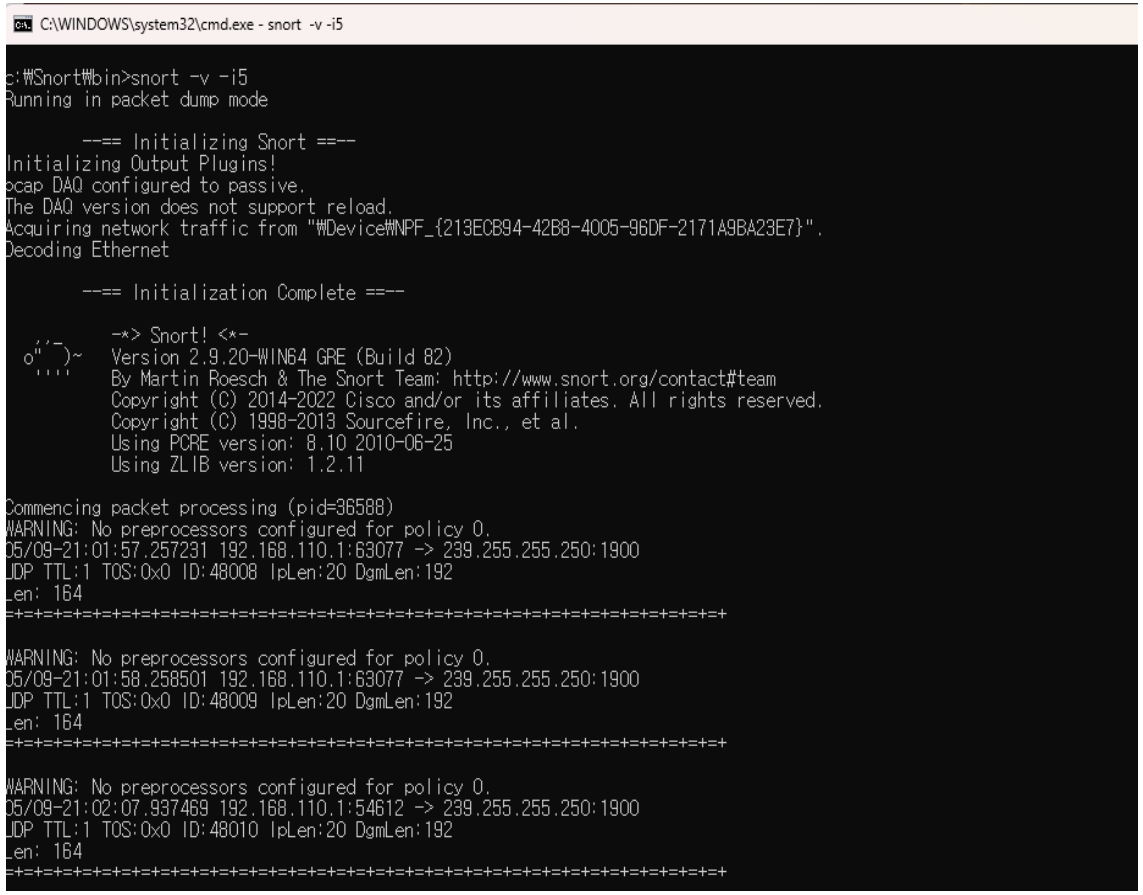
    센서에 설치할 수 있는 어댑터 목록을 확인할 수 있을 것이다. (wifi가 아닌 경우 보통 Controller가 붙어있는 어댑터를 대상으로 한다.)

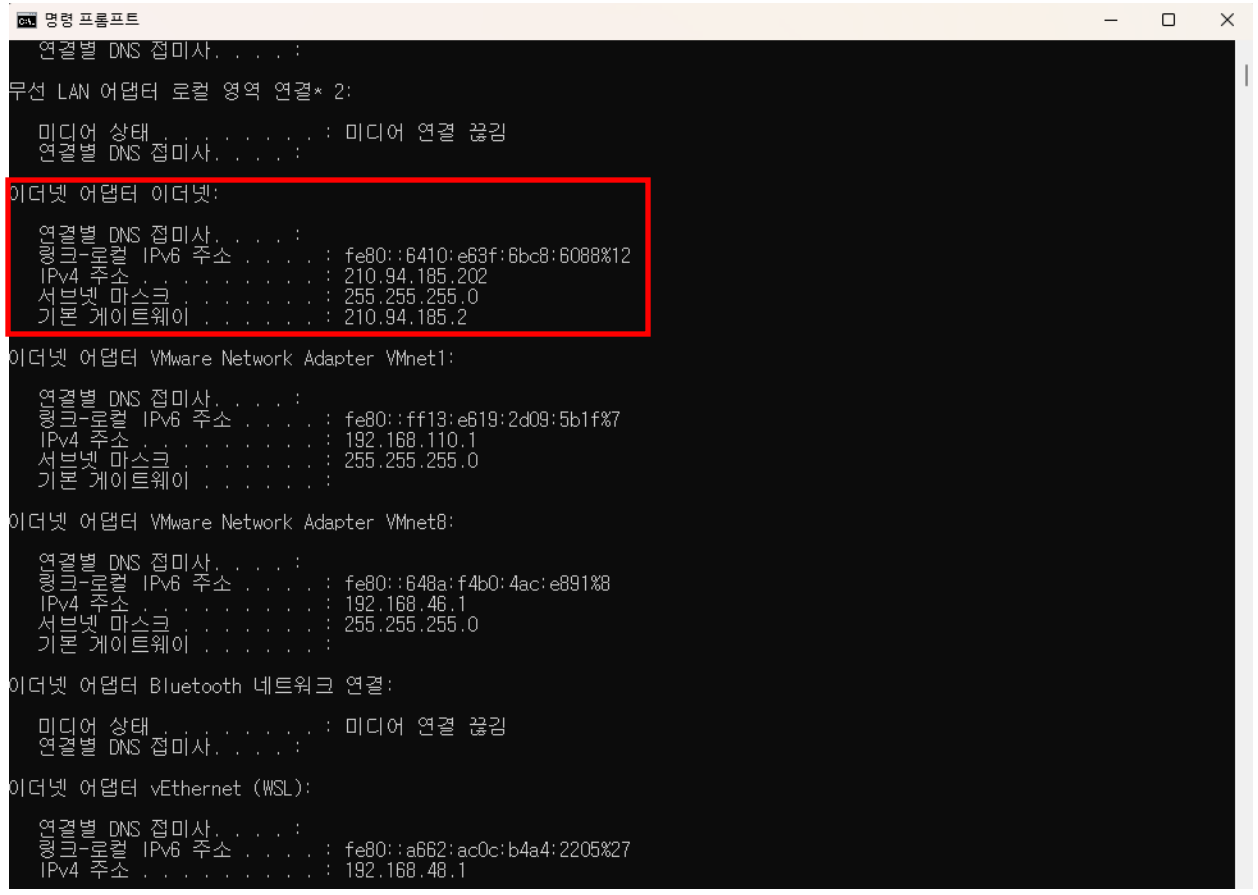


# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

11. c:\Snort\bin> 프롬프트에서 snort -v -ix를 입력하는데, 이때 x는 스노트 센서가 위치할 NIC카드의 번호이다.

12. 두번째 명령 프롬프트에서 ipconfig를 통해 **이더넷 어댑터 이더넷**의 기본 게이트웨이 아이피 주소를 알아낸다. (혹은 무선 LAN 어댑터 Wi-Fi)

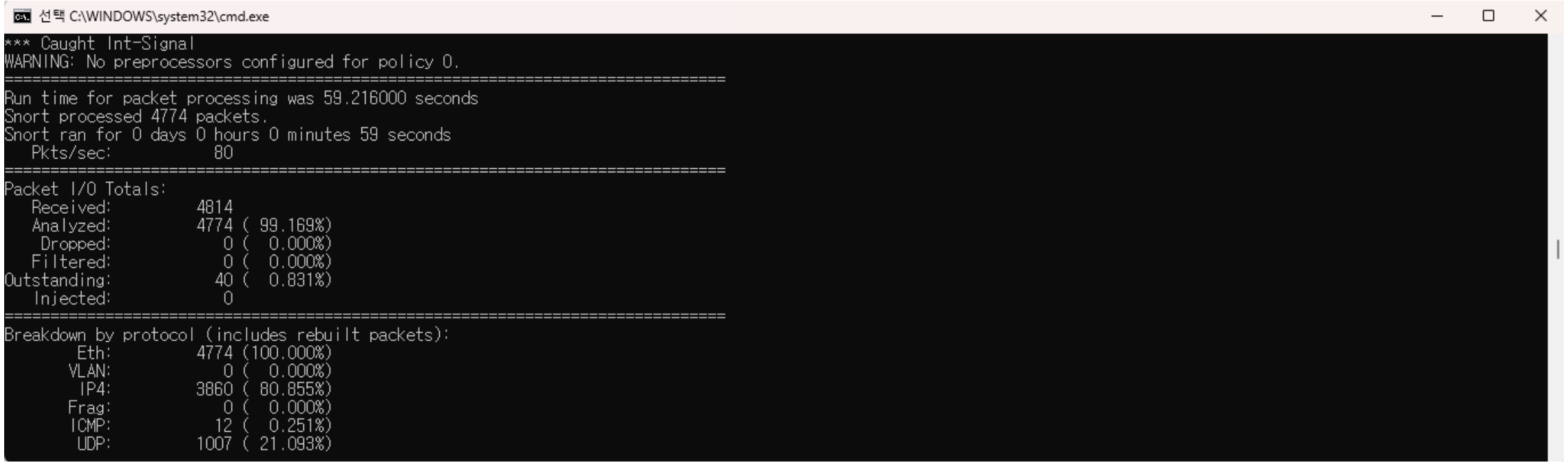


# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

13. 두번째 명령 프롬프트에서 기본 게이트웨이로 핑을 보낸다 (ping 기본 게이트웨이 아이피)

14. 핑이 완료되면 스노트가 실행되고 있는 첫번째 명령 프롬프트에서 Ctrl+C로 스노트를 멈춘다.




이때 스노트의 기본적인 기능을 보여줄 수 있는 메시지가 보이지만, 모든 사람이 다 콘솔을 지속적으로 모니터링할 수 있는 시간적인 여유나 능력을 갖고 있지는 않다. 따라서 나중에 분석을 하기 위해 활동을 로깅할 수 있는 방법이 필요하다. 이는 다음과 같은 방법으로 할 수 있다. 아래의 로깅 방법을 따라해보고 관련 내용을 순서대로 캡처하고 설명하여라.

# 실습10-1: 스노트(Snort) 윈도우 시스템 구축하기

dongguk UNIVERSITY

1) 스노트를 설치했던 디렉토리로 이동하여 명령 프롬프트에서 snort -ix -dev -l \snort\log를 입력한다.

   이 명령은 스노트를 시작하면서 \snort\log 폴더에 헤더를 기록하도록 지시한다.

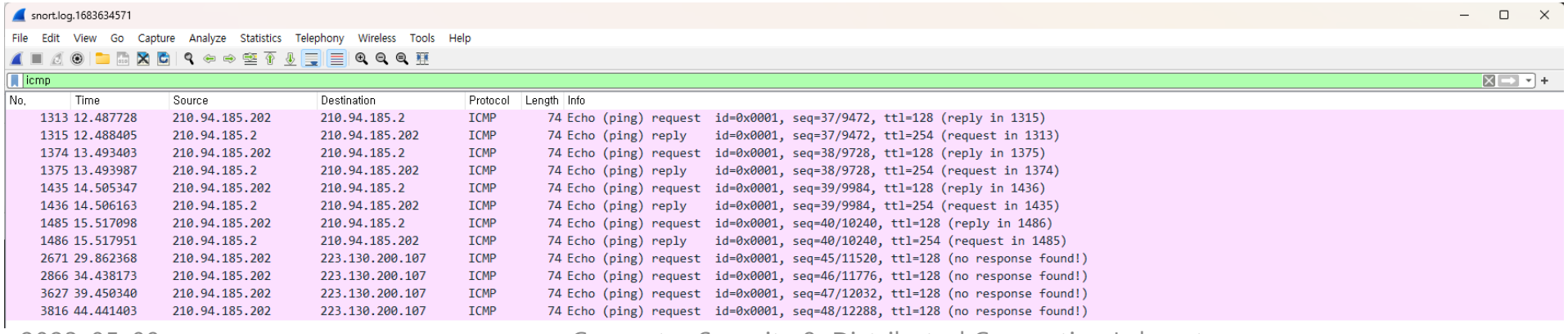
2) 게이트웨이 같은 디바이스를 핑(ping)한다. 네트워크에 또 다른 컴퓨터가 있다면 그 컴퓨터를 핑해도 되고, 아니면 Nmap으로도 스캔할 수 있다.

   목적은 snort\log 폴더에 로깅될 트래픽을 생성하는 것이다.

3) 핑 트래픽을 생성했다면 로컬 머신 대상으로 스캔을 하고 Ctrl+C를 눌러 패킷 캡처를 멈춘다.

4) 윈도우 익스플로러를 이용하여 c:\snort\log 폴더로 이동해보면 몇몇 파일을 발견할 수 있다.

5) 와이어샤크를 이용하여 캡처된 패킷의 콘텐츠를 살펴본다.



# 실습10-2: WiFi 탐색툴 Vistumbler

dongguk UNIVERSITY

## ➢ 무선 네트워크 분석을 위한 WiFi 탐색툴 Vistumbler 사용하기

- 무선랜(WLAN)은 실제로 스니핑 프로그램을 통해 암호가 걸려있지 않은 백화점 결제 시스템의 AP에 접속하여 결재정보를 살펴보거나 접속 ID를 도용하여 정상적으로 접속한 후 이를 악의적으로 이용하는 경우도 종종 발생하고 있다. 그러나 이러한 사실보다 더 심각한 것은 해커들의 정보 습득 사례가 빈번하더라고 특징적인 증상이 나타나지 않기 때문에 사용자 스스로가 피해 사실을 인지하지 못한다는데 있다.

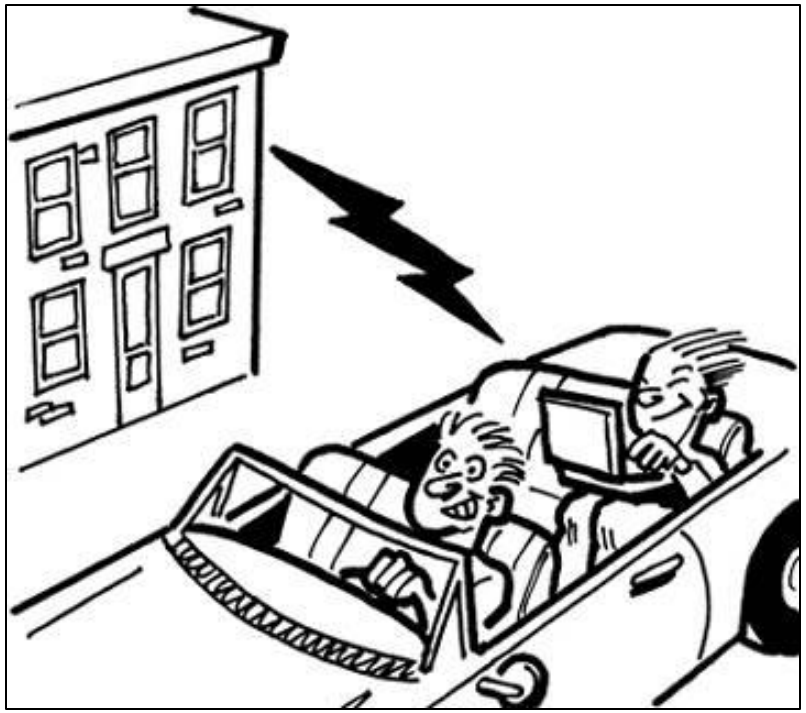
- 이와 같이 무선랜이 가진 보안 취약점으로 인해 네트워크 관리 비용은 훨씬 증가되고 있다. 따라서 무선랜의 현상을 분석하고 관리하는 문제는 매우 중요하다. 현재 관리의 목적이 아니더라도 무선랜을 긍정적으로 이용하기 위해 이를 탐색하기 위한 다양한 툴이 존재한다. 본 과제에서는 공개된 WiFi 탐색 Tool을 이용하여 여러 가지 테스트 시도를 해볼 수 있다.

# 실습10-2: WiFi 탐색툴 Vistumbler

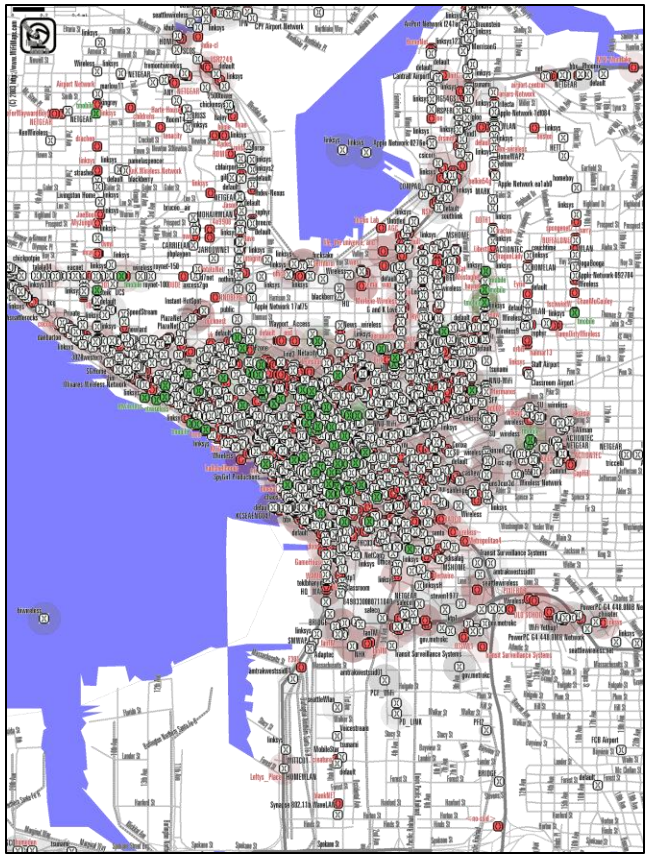
dongguk UNIVERSITY

➢ 무선 네트워크 분석을 위한 WiFi 탐색툴 Vistumbler 사용하기

- 워드라이빙(War-driving)은 차량으로 이동하면서 타인의 무선랜망에 무단으로 접속하는 행위를 뜻한다. 광범위한 무선랜에서 인터넷을 통해 자료와 자원에 접근하는 경우나 자가 위성 위치 확인 시스템 (GPS)을 장착한 차량으로 지역별 무선 액세스 상태를 파악하여 시스템 지도를 만드는 경우에 이용한다.



[War-driving]

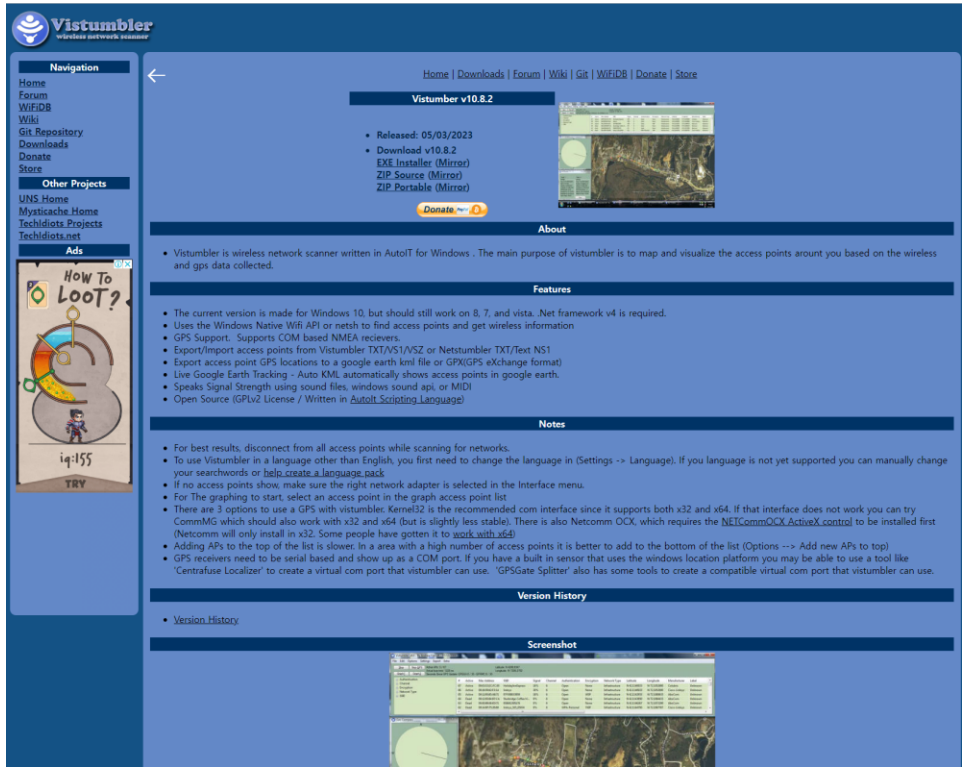


[A map of Wi-Fi nodes]

# 실습10-2: WiFi 탐색툴 Vistumbler

➢ 무선 네트워크 분석을 위한 WiFi 탐색툴 Vistumbler 사용하기

- 이번 실습은 비즈텀블러(Vistumbler)를 이용하여 활성화된 AP를 스캔하여 본다. 실습을 위해 랩톱과 무선 카드가 필요하다.




1. https://www.vistumbler.net/에서 비즈텀블러 프로그램을 다운로드한다.
2. 윈도우 PC에 설치한 후 적절한 무선 카드를 로딩했는지 확인한다.
3. 비즈텀블러를 실행한다. 프로그램이 실행되면 'Scan Aps'를 클릭하여 스캔 프로세스를 시작한다.
4. 아무런 AP가 포착되지 않는다면 돌아다녀 보거나 랩톱을 외부에 설치하는 것을 고려해보자.
5. 대부분의 도심에서는 몇 개의 돌아다니는 신호를 찾아내는데 큰 어려움이 없을 것이다.

# 실습10-2: WiFi 탐색툴 Vistumbler

dongguk UNIVERSITY

➢ **[과제 내용]**

- 아래의 각 문제에 대한 수행 결과를 캡처하여 분석하고 설명하는 내용을 개인적인 견해와 함께 레포트에 모두 반영하여야 한다.
- 설치한 해당 WiFi 탐색툴의 사용법을 익히고 아래에 제시하는 과제를 수행한다.

1. 해당 WiFi 탐색툴이 자신의 노트북에서 제대로 동작하도록 설치파일을 다운로드하여 올바르게 설치한다.
2. 설치한 WiFi 탐색툴을 실행하여 현재 내 주변에 탐지되는 무선랜 SSID는 몇가지나 있으며 접속하여 사용하기에 가장 신호상태가 양호한 무선랜은 어떤것인가 ?
3. 주로 어떤 암호화 기법이 사용되는가? 또 그 기법은 어떠한 기법인가?
4. 해당 WiFi 탐색툴이 제공하는 데이터와 기능은 무엇이며 각각 무엇을 의미하는가?
    - Authentication, Channel, Encryption, Network Type, SSID, RSSI 등
5. 탐지된 무선랜 SSID 중 가장 취약하다고 판단되는 SSID는 무엇이며 그 이유는 무엇인가?

# Q & A