Protocol Analyzer: Wireshark 설치 가이드

2008년 10월

경북대학교 통신프로토콜연구실

김지인 (jiin16@gmail.com)

요 약

현재 다양한 Protocol Analyzer가 존재하고 있다. 이 문서는 그 중 하나인 Wireshark에 대한 일종의 매뉴얼로 Wireshark에 대한 정보와 그 설치법에 대해 정리한 것이다.

목 차

1. 서론

현재 시중에는 다양한 Packet Analyzer(sniffer라고 부르기도 함)가 나와있다. 몇 가지 예를 들면 dSniff, Ettercap, Microsoft Network Monitor, tcpdump 등을 들 수 있다. 하지만 그 중에서 가장 많이 쓰는 것은 바로 Wireshark이다.

Wireshark라 하면 생소한 사람들도 있을 것이다. 그럼 이 이름은 어떤가? Ethereal. Wireshark는 실제로 Ethereal이라는 이름으로 더 잘 알려져 있다. 하지만 2006년 Wireshark의 개발자 Gerald Combs가 이직을 하게 되면서 전 회사가 가진 Ethereal의 상표권으로 인해 현재는 Ethereal이라는 이름이 아닌 Wireshark라는 이름을 사용하고 있다. 쉽게 말하면 Ethereal의 이름이 Wireshark로 바뀐 것이다.

이 Wireshark를 활용하면 packet capture를 통해 다양한 일을 할 수 있다. 예를 들면, Wireshark로 capture한 패킷을 통해 책에서만 보던 프로토콜 구조에 대해서 직접 눈으로 확인도 가능하며, 직접 작성한 프로토콜을 테스트 할 때도 프로토콜이 정상 작동하는지 알아볼 수 있다. 반면에 악의적인 용도로 활용할 경우 패킷 캡쳐를 할 경우 packet 내 암호화하지 않은 정보는 모두 알 수 있다. 홈페이지를 로그인할 때 패킷을 캡쳐할 경우 아이디 뿐만 아니라 심한 경우 패스워드까지 알 수 있다(홈페이지 제작 시 반드시 주요 정보는 암호화 하도록 하자). 본 고에서는 2장에서 Wireshark에 대해서 알아보고 3장에서 설치 및 활용법에 대해서 소개하고 4장에서 결론을 정리한다.

2. Wireshark란?

Wireshark는 공개된 packet sniffer 프로그램이다. 네트워크에 문제가 발생하거나 분석용 소프트웨어, 프로토콜 개발, 교육용으로 사용된다. 2006년 6월 상표권 문제로 인해 Ethereal 프로젝트에서 Wireshark로 이름이 바뀌었다.

Wireshark는 tcpdump와 매우 유사한 기능을 제공한다. 그러나 추가로 GUI(Graphical User Interface)를 지원하고, filtering option과 정렬을 통해 더 많은 정보를 제공한다. 그리고 network interface를 promiscuous mode[1]로 설정함으로써 네트워크를 지나다니는 모든 packet을 사용자가 볼 수 있게 해 준다. 그리고 알려진 프로토콜 중에서 일부분에 대해서는 직접 parsing을 하여 내용을 보여주기도 한다.

다음은 Wireshark에 대한 장점은 wireshark 공식 홈페이지(http://www.wireshark.org)에서 발췌한 내용이다.[1]

- ✓ 몇 백 개의 프로토콜을 분석 할 수 있으면 계속 추가되고 있음
- ✓ Live capture와 offline 분석이 가능

[1] NIC(Network Interface Card)는 물리적 주소(MAC address)를 가진다. 일반적으로 NIC가 packet을 받으면 자신의 주소와 비교를 한 후 다르면 packet을 drop하는데 promiscuous mode의 경우 packet을 drop하지 않는다. 그래서 컴퓨터는 모든 packet을 읽을 수 있다.

- ✓ Multi-platform에서 사용 가능(Windows, Linux, Solaris, MAC OS X 등)
- ✓ GUI 환경 지원
- ✓ 여러 개의 파일 포맷을 읽기 / 쓰기 가능(tcpdump, Microsoft Network Monitor 등)
- ✓ capture하면서 gzip으로 압축 가능
- ✓ Ethernet / IEEE 802.11, PPP/HDLC 등을 읽어 들일 수 있음
  - IEEE 802.11(Wireless LAN)을 capture하기 위해서는 별도의 라이브러리인 AirPCAP을 구매해야 함
- ✓ Packet을 분석하면서 색상을 적용해 구별 가능
- ✓ 암호화된 packet을 분석 (IPsec, Kerneros, SSL/TLS 등)
- ✓ Capture 결과를 XML 등으로 export 가능

3. 설치 및 사용법

3.1 설치

위에서 소개한 것처럼, Wireshark는 multi-platform을 지원한다. 즉 다시 말해 여러 OS(Operating System)에서 사용이 가능하다. 여기에서는 일반적으로 사용하는 Windows와 linux(Ubuntu)에서의 설치법을 설명하였다.

3.1.1 Windows

모든 윈도우 응용 프로그램이 그렇듯 Wireshark 또한 설치가 간단하다. 프로그램은 Wireshark 공식 홈페이지에서 구할 수 있다.

http://www.wireshark.org/download.html

http://sourceforge.net/project/downloading.php?groupname=wireshark&filename=wireshark-setup-1.0.3.exe&use_mirror=nchc

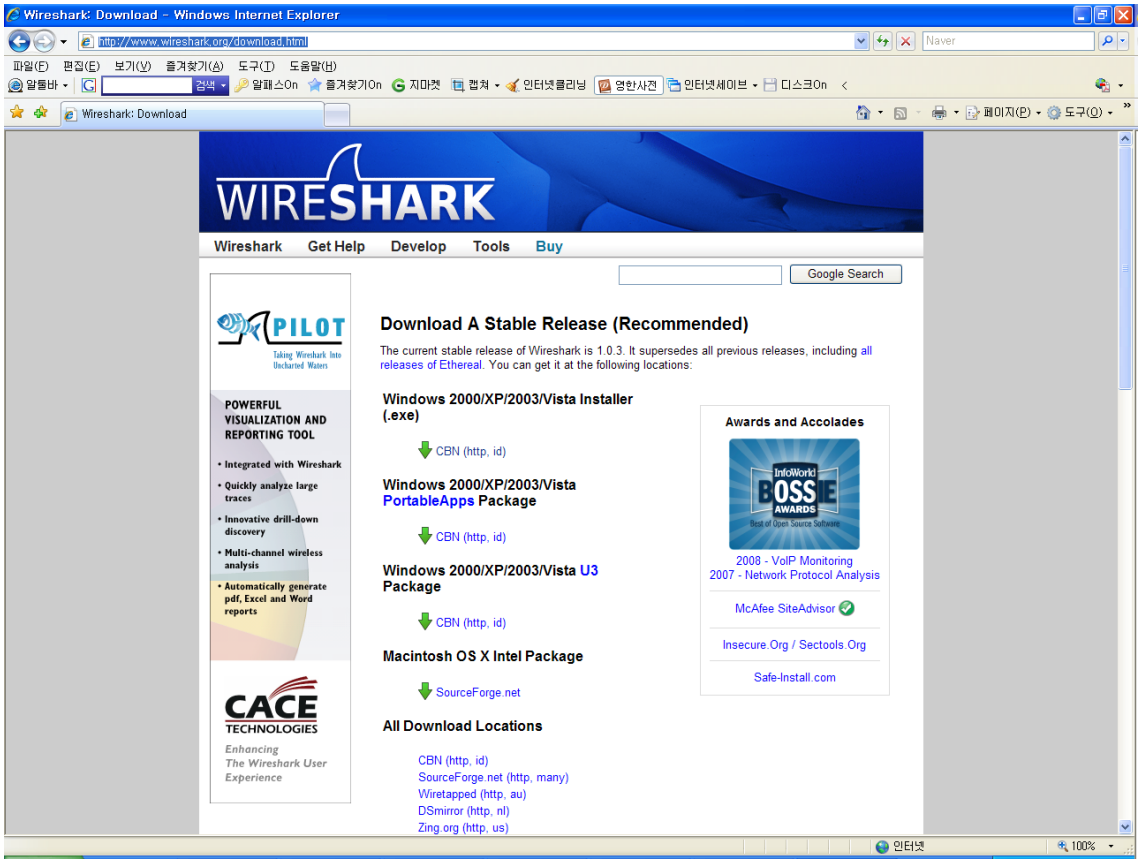

그림 1. Wireshark 다운로드 페이지

그림 1을 Wireshark를 다운 받을 수 있는 페이지이다. 설치 파일은 제일 위에 있는 Windows 2000/XP/2003/Vista Installer(.exe)이다. 다운 받은 후 Installer를 실행한다.

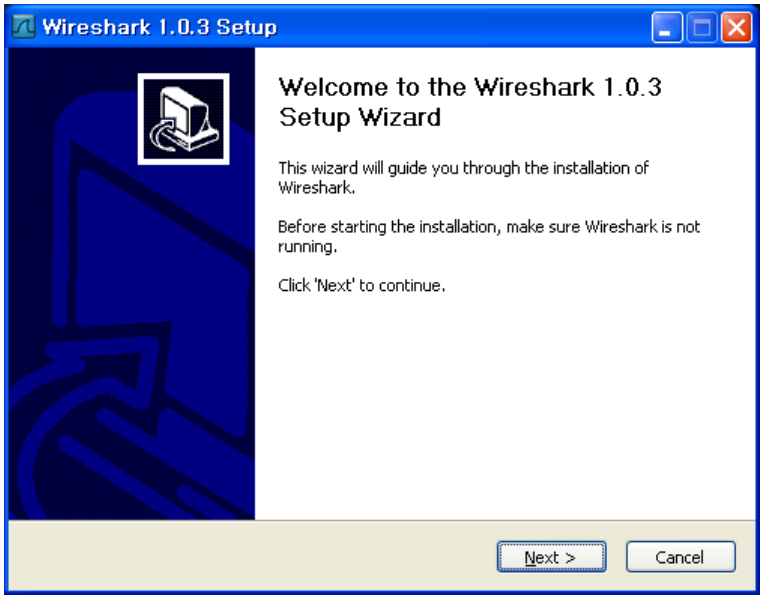

그림 2. Wireshark 설치화면

Next를 클릭해서 설치를 계속 진행한다. 아래는 Wireshark 저작권 동의에 대한 창이다. Wireshark는 기본적으로 GPL을 따른다.

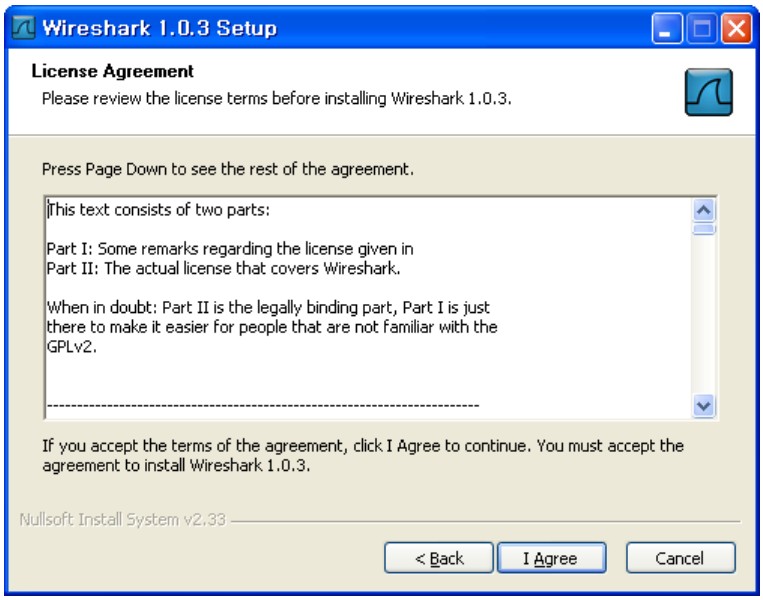

그림 3. Wireshark 설치화면

I Agree를 클릭해서 설치를 계속 진행한다. 아래는 컴포넌트를 선택하는 화면이다. 기본적인 컴포넌트를 설치하는데 약 90MB가 필요하다.

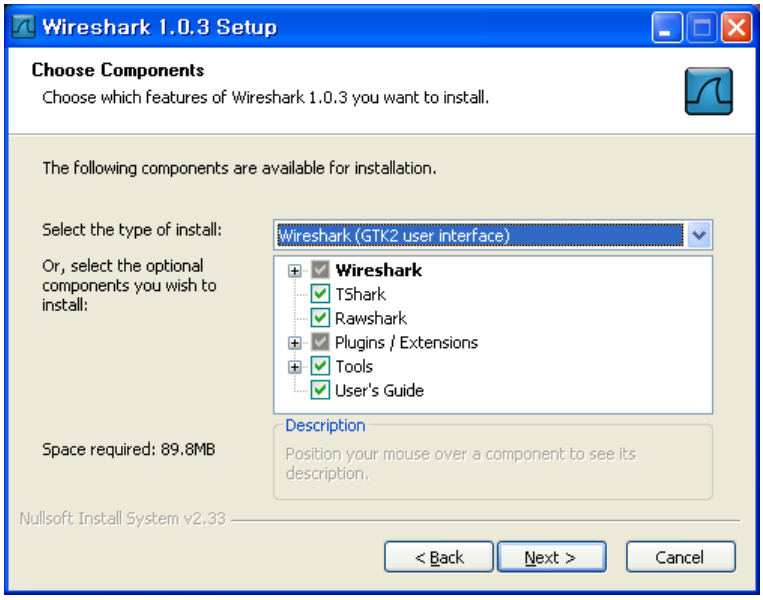

그림 4. Wireshark 설치화면

Next를 클릭하여 다음 단계로 넘어간다. 다음은 바로 가기, 빠른 실행 등을 추가할 것인지 파일 확장자를 추가할 것인지 선택하는 부분이다.

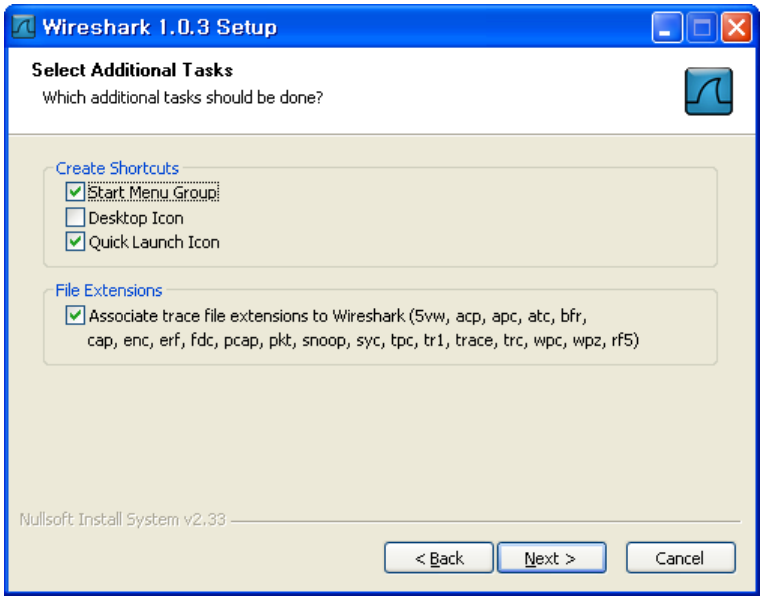

그림 5. Wireshark 설치화면

Next를 클릭하여 다음 단계로 넘어간다. 다음 단계에서는 Wireshark의 설치 경로를 설정하는 단계이다. 기본적으로 Wireshark는 C:₩Program Files₩Wireshark에 설치된다.

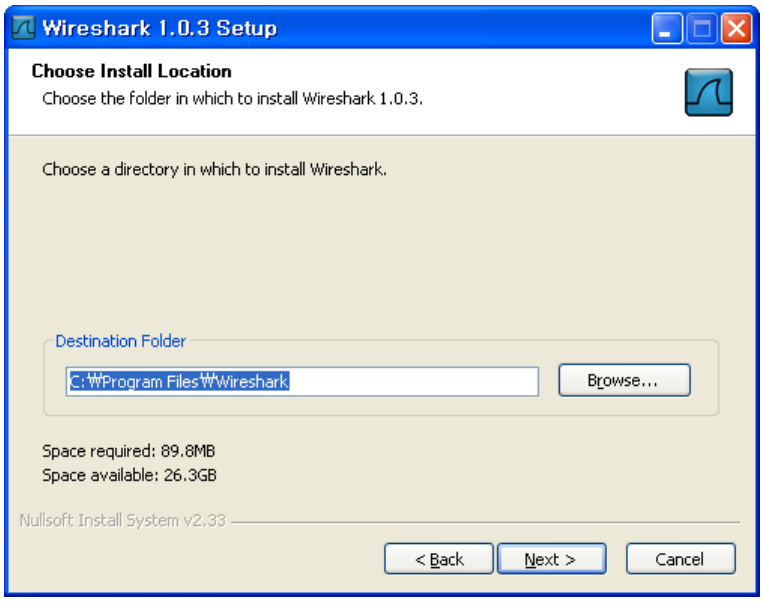

그림 6. Wireshark 설치화면

설치 경로를 지정하고 Next를 선택해 다음 단계로 넘어간다. 다음 단계는 WinPcap을 설치할 것인지 선택하는 단계이다. WinPcap을 설치해야 실시간으로 data packet을 capture 할 수 있다. 그리고 시작 시 NPF 서비스를 시작할 경우 사용자가 administrator가 아니라도 packet capture가 가능하다.

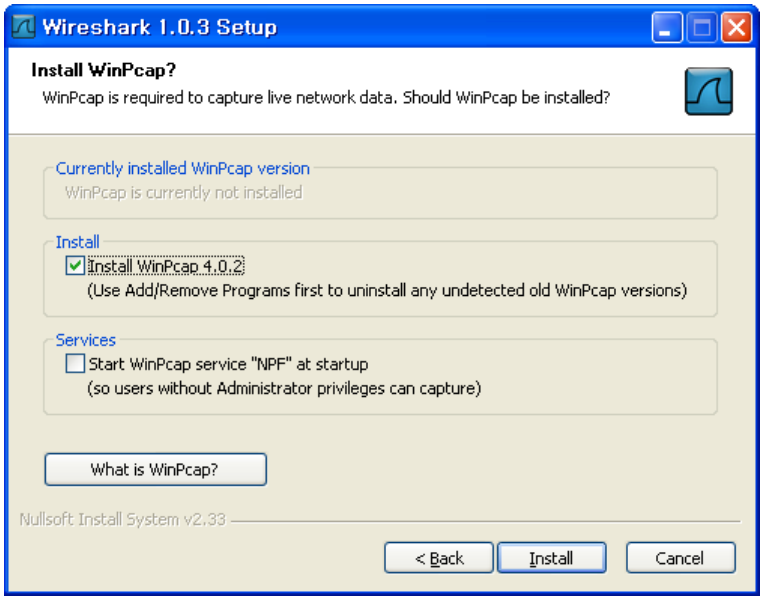

그림 7. Wireshark 설치화면

Install을 선택하여, 이제 설치를 시작한다. 아래 그림은 설치 화면이다.

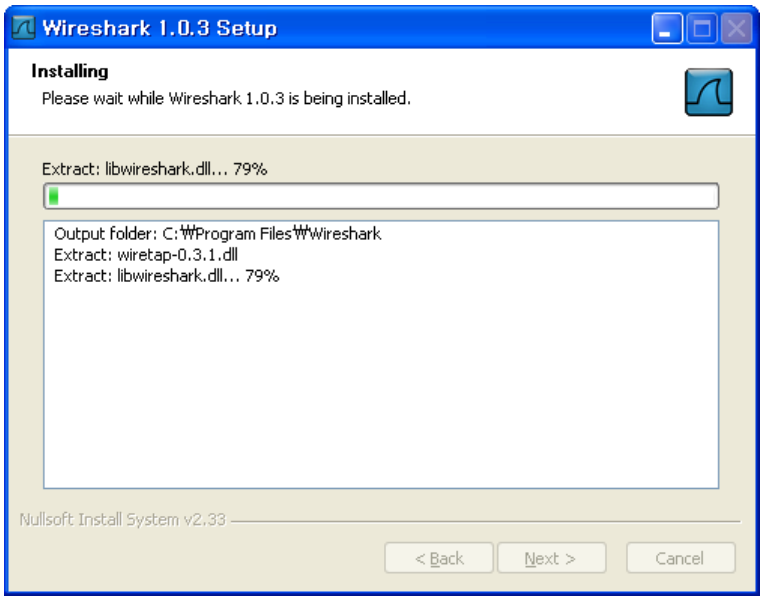

그림 8. Wireshark 설치화면

Wireshark를 설치하는 중 아래와 같은 WinPcap을 설치하는 화면이 나타난다.

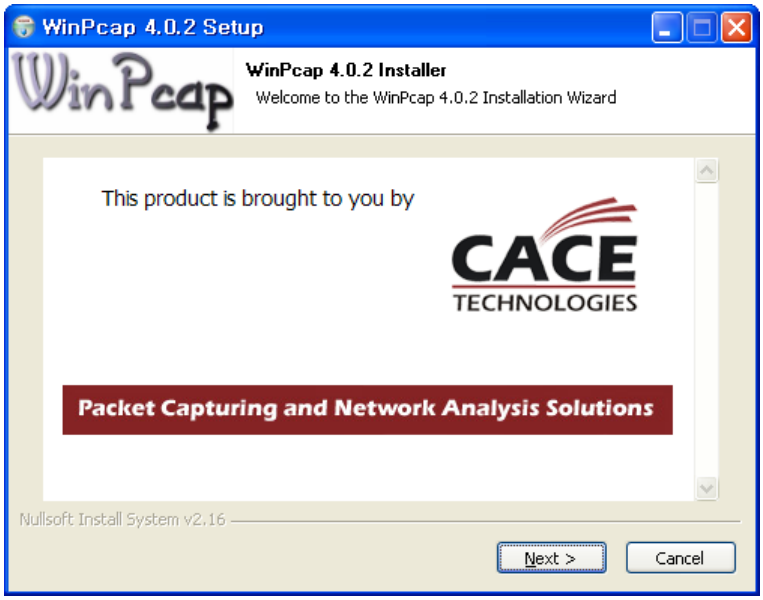

그림 9. WinPcap 설치화면

WinPcap을 설치한다. 설치법은 Wireshark와 마찬가지로 매우 간단하다.

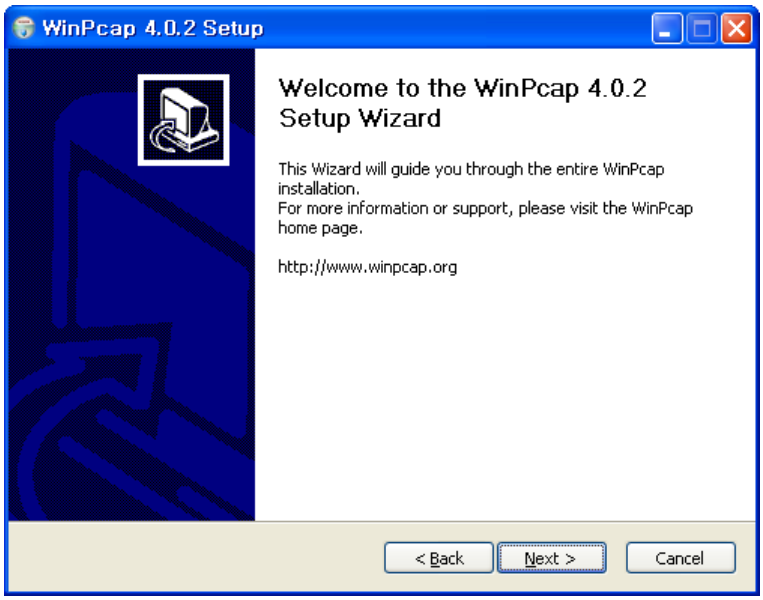

그림 10. WinPcap 설치화면

Next를 선택하여 계속 설치를 한다. 다음 단계는 저작권 동의를 구하는 단계이다.

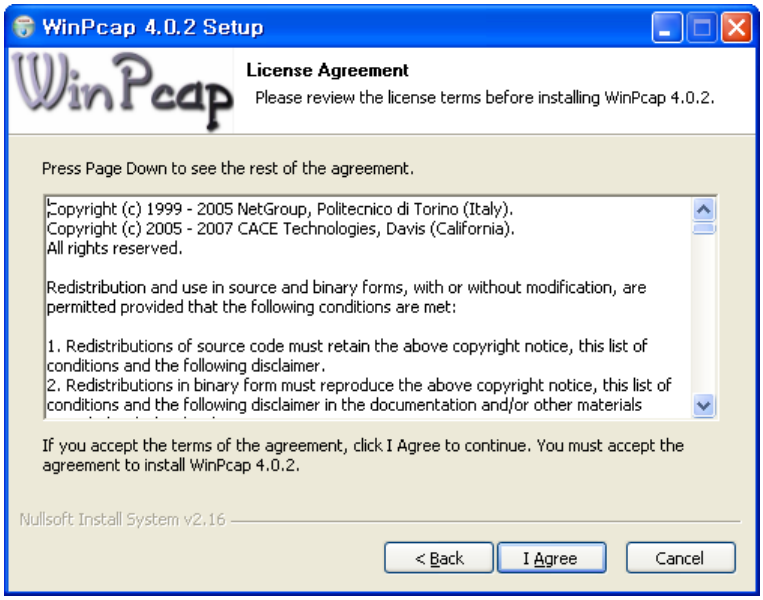

그림 11. WinPcap 설치화면

I Agree를 선택하여 동의하면 설치 화면으로 넘어간다.

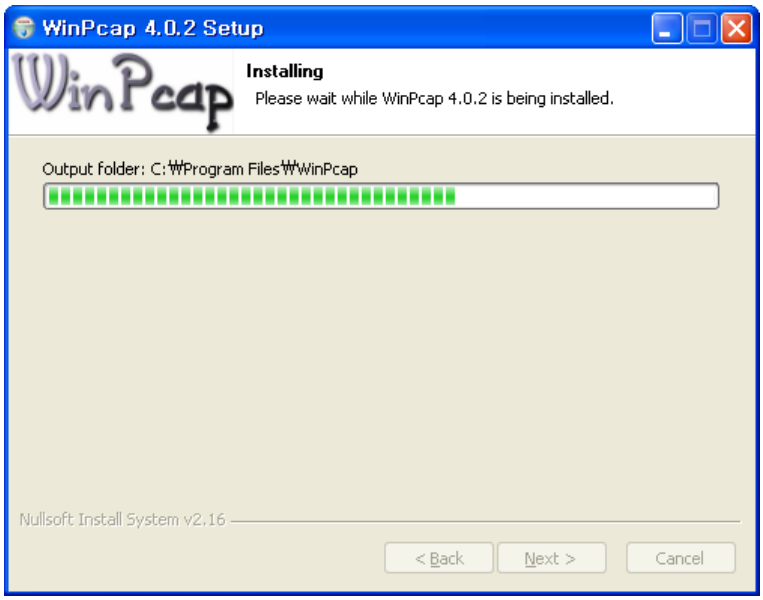

그림 12. WinPcap 설치화면

Finish를 선택한다. 이제 WinPcap 설치가 완료됐다.

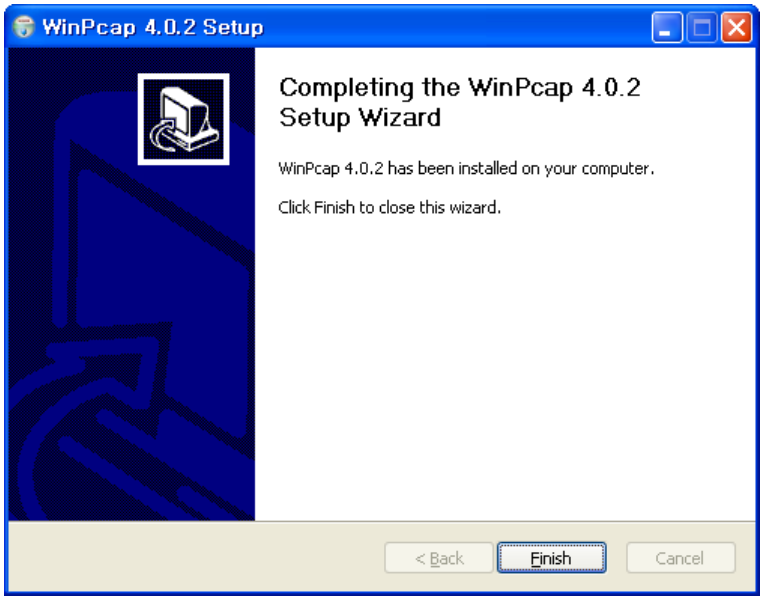

그림 13. WinPcap 설치화면

WinPcap이 설치가 완료되면 Wireshark도 남은 부분을 설치를 하게 된다. 아래는 설치 완료 화면이다.

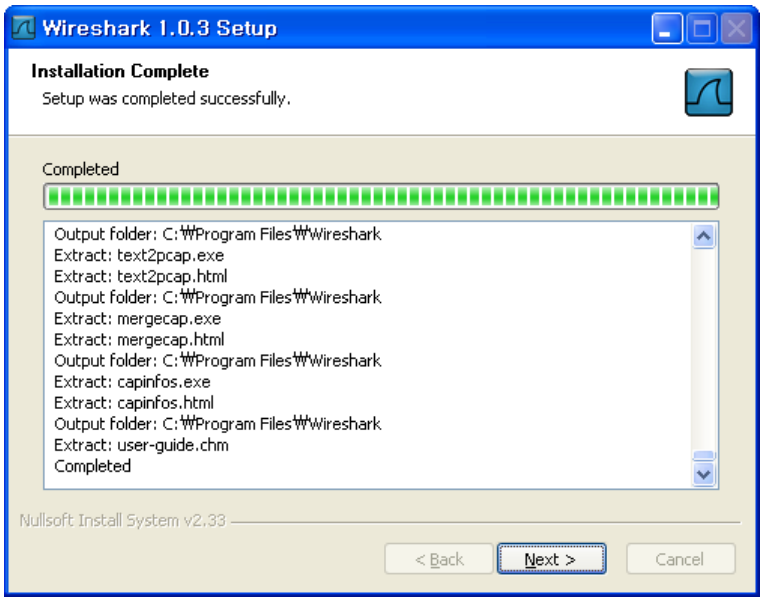

그림 14. Wireshark 설치화면

Next를 선택화면 Wireshark 설치가 완료되고 다음 화면이 나온다.

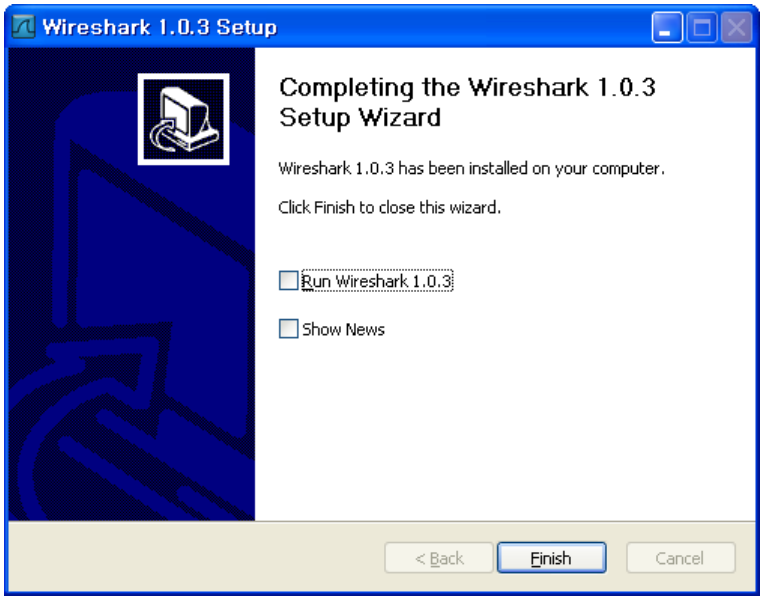

그림 15. Wireshark 설치화면

Finish를 선택하면 설치가 끝난다.

3.1.2 Linux

거의 대부분의 Linux의 경우 Wireshark는 기본 package로 포함이 되어 있다. 여기서는 Ubuntu에서의 설치법을 설명하도록 하겠다.

$sudo apt-get install wireshark

한 줄의 명령으로 설치가 가능하다.

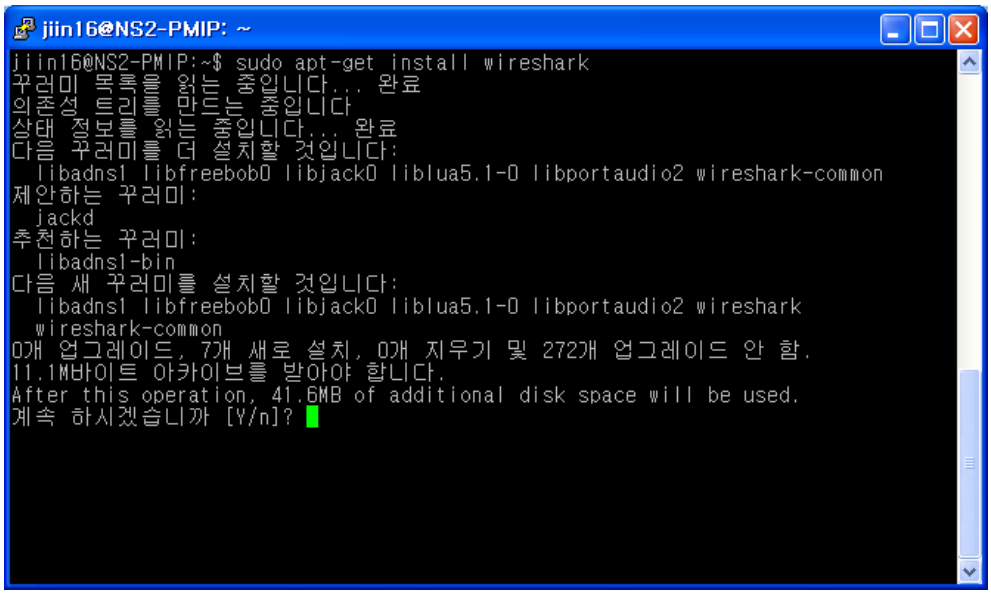

그림 16. Wireshark 설치화면

Wireshark를 설치하기 위해서 필요한 라이브러리가 존재하는데 libadns1, libfreebob0, libjack0,liblua5.1-0, libportaudio2이 이에 해당하며, 이들 라이브러리와 wireshark를 설치하기 위해서는 41.6MB의 여유 공간이 필요하다. Y를 입력하여 설치를 계속 진행한다.

아래는 설치화면이다.

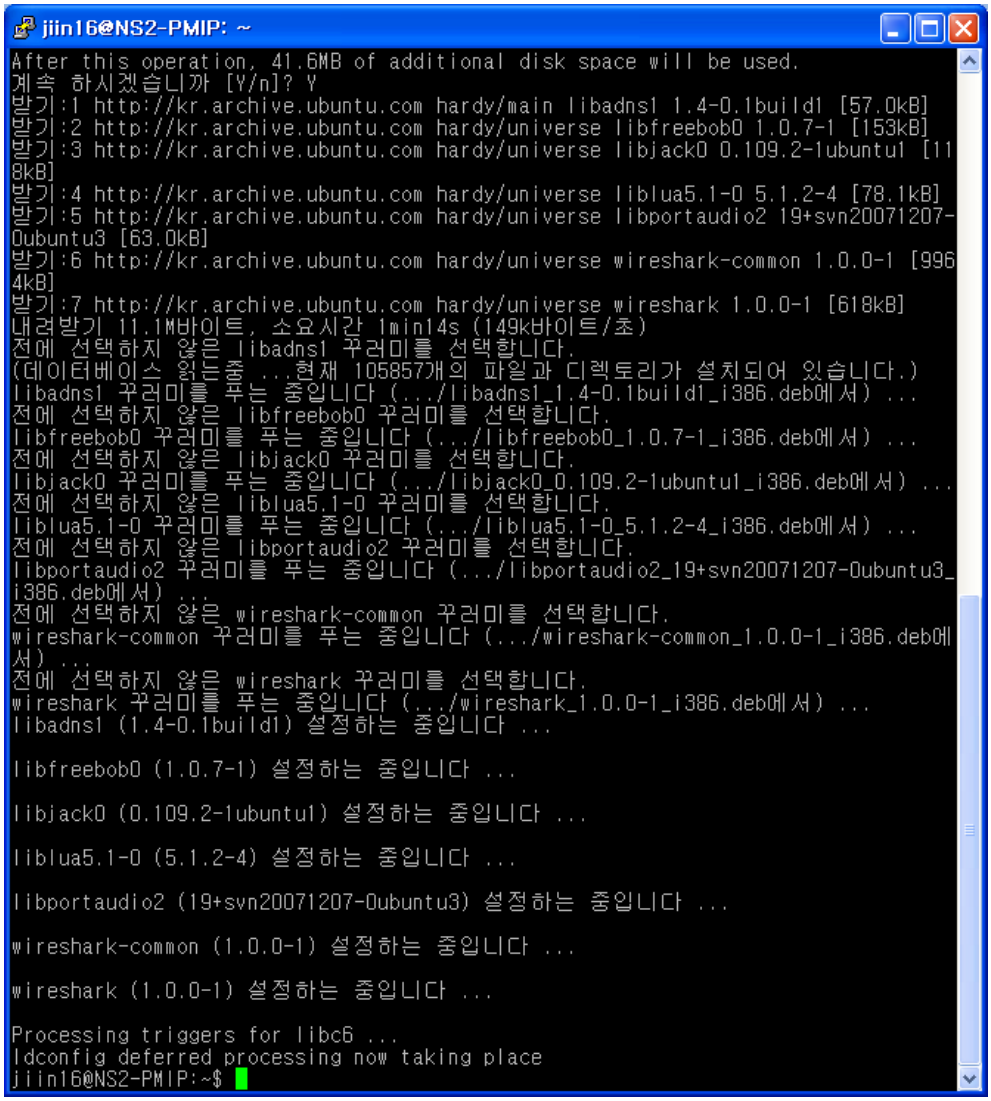

그림 17. Wireshark 설치화면

Ubuntu에서의 Wireshark 설치가 완료 되었다.

Redhat 계열의 Linux(Redhat, Fedora 등)의 경우는 rpm을 이용하여 손쉽게 설치 할 수 있다.

3.2 사용법

사용법은 Windows와 Linux 둘 다 동일하므로 Windows를 기준으로 설명하겠다. Wireshark를 실행하면 아래와 같은 화면이 나타난다.

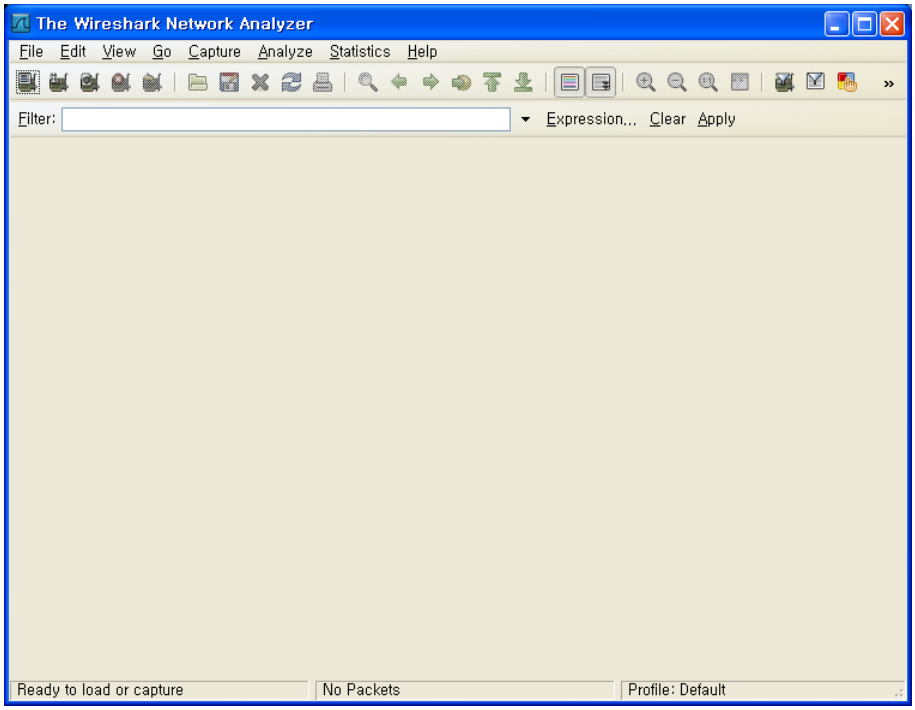

그림 18. Wireshark 기본화면

기본적으로 capture를 하는 방법과 capture한 packet을 보는 법에 대해서 설명하겠다. 먼저 capture를 하는 방법이다. Capture는 interface 별로 구분해서 capture가 가능하다.

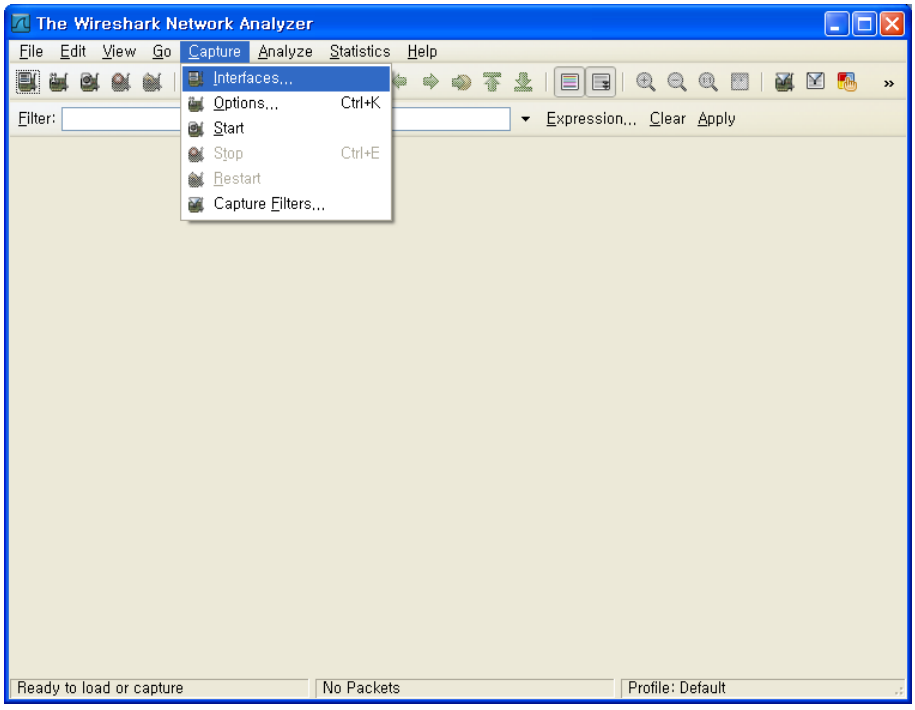

그림 19. Wireshark를 이용한 packet capture

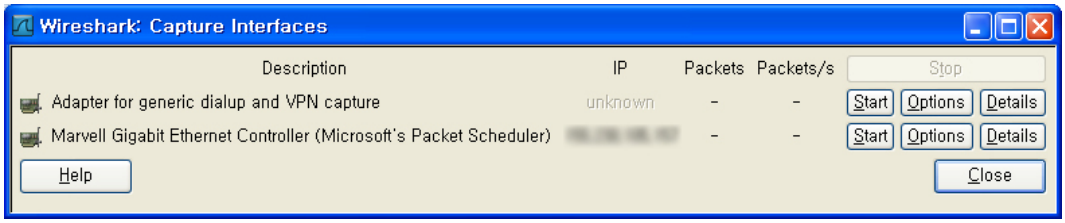

그림 20. Capute할 interface 선택

Start를 누르면 capture를 시작하고, Option을 통해 capture할 packet을 filtering 하거나 다양한 option을 줄 수 있다.

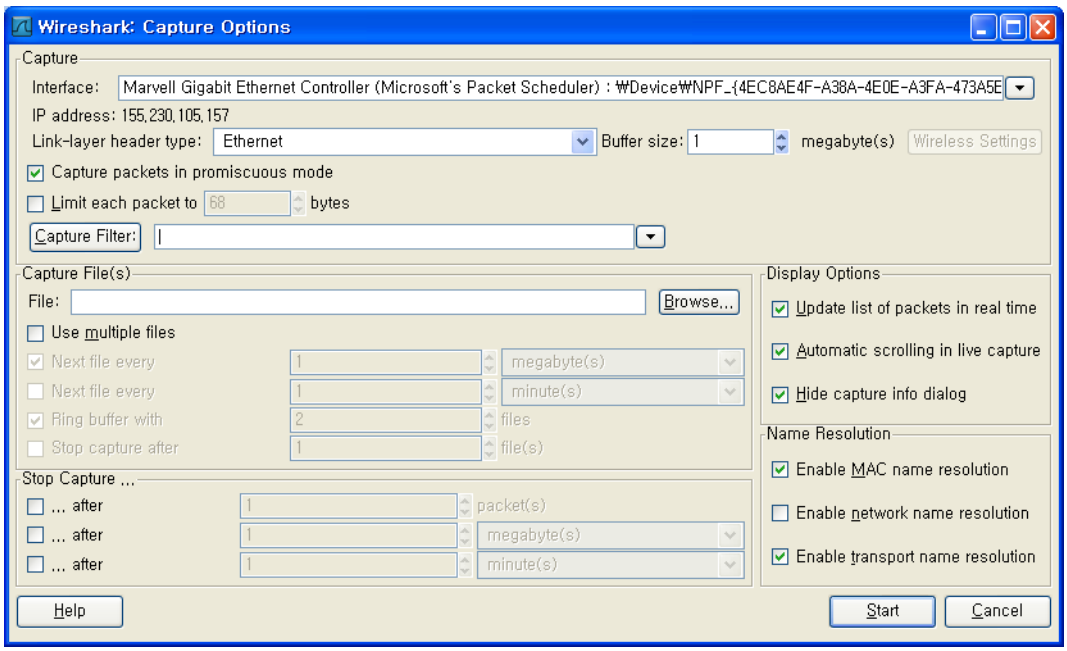

그림 21. Capture option 화면

Option을 설정한 뒤 Start를 하게 되면 아래와 같이 packet이 capture 되는 것을 확인할 수 있다.

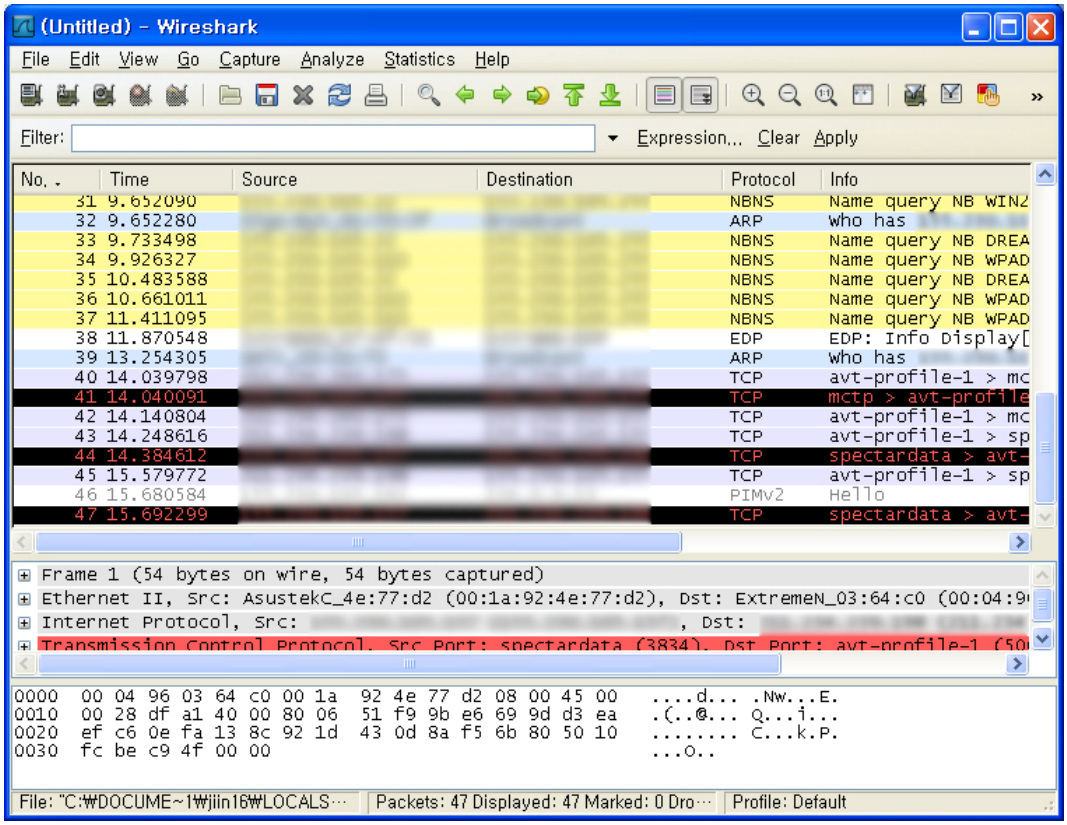

그림 22. Wireshark를 이용한 packet capture 화면

Privacy 관계로 IP 주소 부분은 블라인드 처리 하였다. 위의 화면처럼 capture한 packet을 분석할 수 있으며, 잘 알려진 protocol의 경우 직접 분석해서 보여준다. 이를 저장할 경우 언제든 저장한 파일을 읽어와 볼 수 있다.

4. 결론

지금까지 본 고에서는 Wireshark가 무엇이며, 설치 방법과 사용법에 대해서 살펴보았다. Wireshark는 packet analyzer로 실시간으로 packet을 capture하고 이를 분석하는 도구이다. 앞으로 네트워크를 공부하는 많은 사람들에게 유용한 툴로 사용될 것으로 전망된다.

참고 문헌

[1] Wireshark, http://www.wireshark.org

[2] Wireshark – Wikipedia, http://en.wikipedia.org/wiki/Wireshark