# WireShark 설치 & 사용법

2011년 3월 9일 수요일
오후 4:44

## 1. Site 접속

http://www.wireshark.org/ 에 들어가서 빨간 상자 안에 아이콘 클릭하세요.


## 2. Download

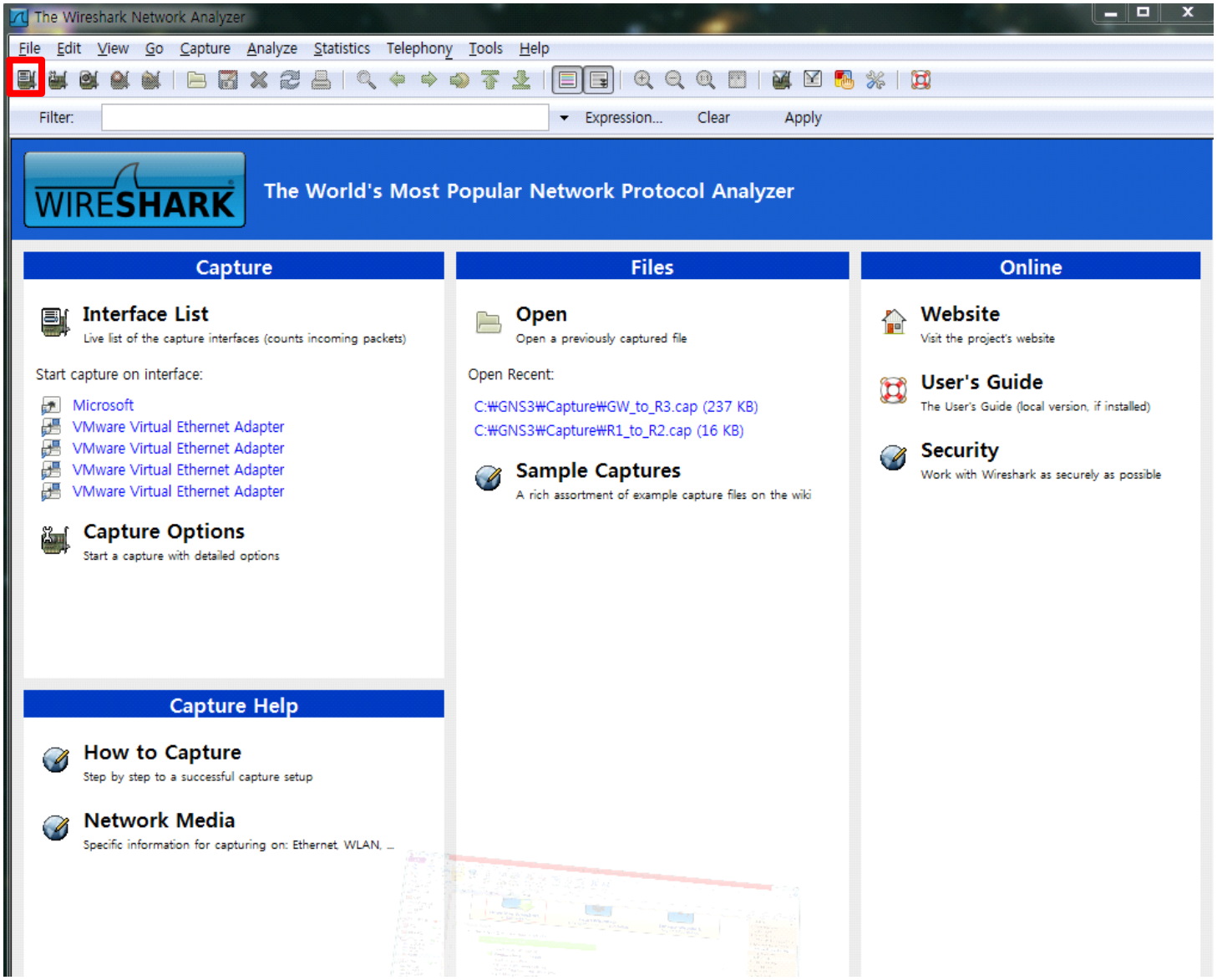
컴퓨터 OS버전에 맞춰서 download하세요.


## 3. 저장 후 설치

다음다음다음으로 설치 하다 보면 또 다른 프로그램을 설치하라고 나오는데 다음다음다음으로 그냥 설치하시면 되요.

## 4. 실행

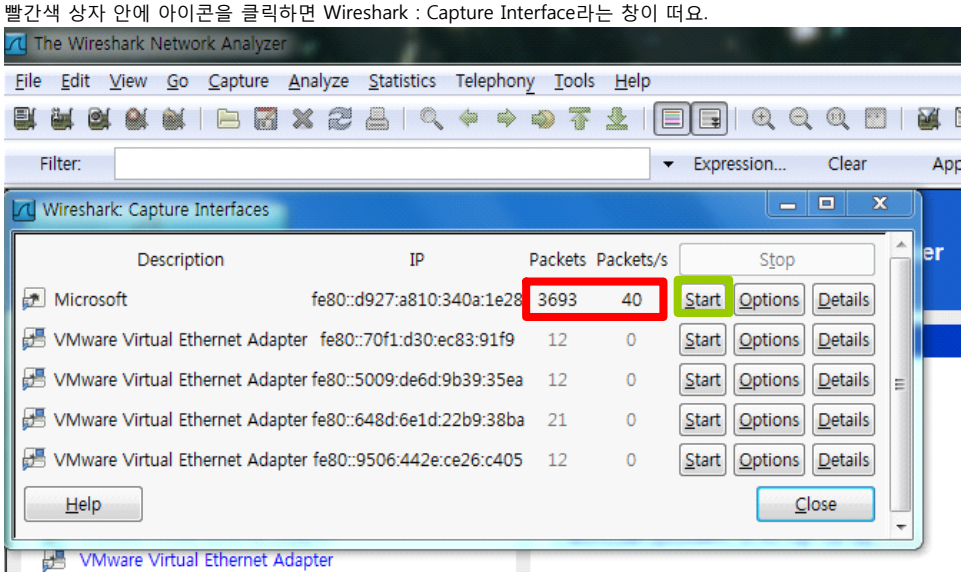
모든 설치가 끝났으면 실행 아이콘을 클릭해 주세요.



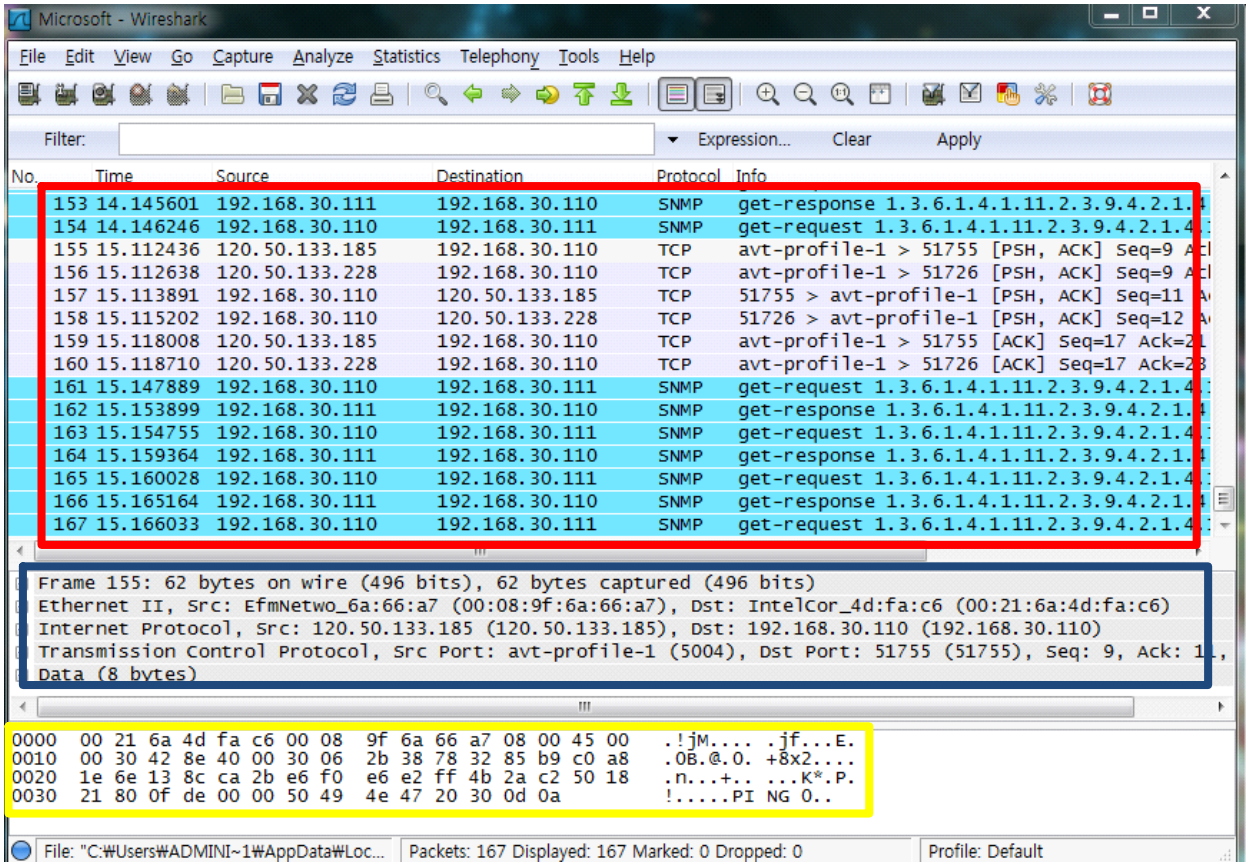

Wireshark 프로그램이 실행 됩니다.

## 5. 사용법

빨간색 상자 안에 아이콘을 클릭하면 Wireshark : Capture Interface라는 창이 떠요.




창 안에 숫자가 계속 올라가는 라인이 데이터가 전송되고 있는 LAN카드에요.
연두색 상자안에 Start 버튼을 클릭하면 해당하는 LAN카드를 통해서 나가고 들어오는 데이터를 볼 수 있는거죠.
이렇게 흘러가는 패킷을 잡아서 보는 걸 Capture한다고 해요.




### 1) 빨간색 네모

부분은 해당하는 LAN를 드나드는 데이터들의 목록이에요.

### 2) 파란색 네모

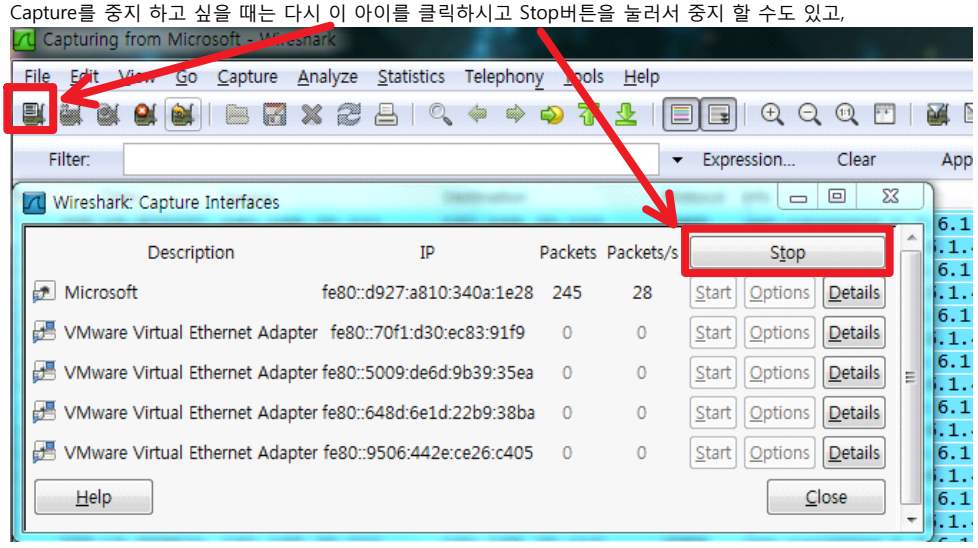
빨간색 네모 중 한 줄을 클릭하면 그 데이터의 헤더 상세 정보가 바로 아래에 나타나죠.

### 3) 노란색 네모

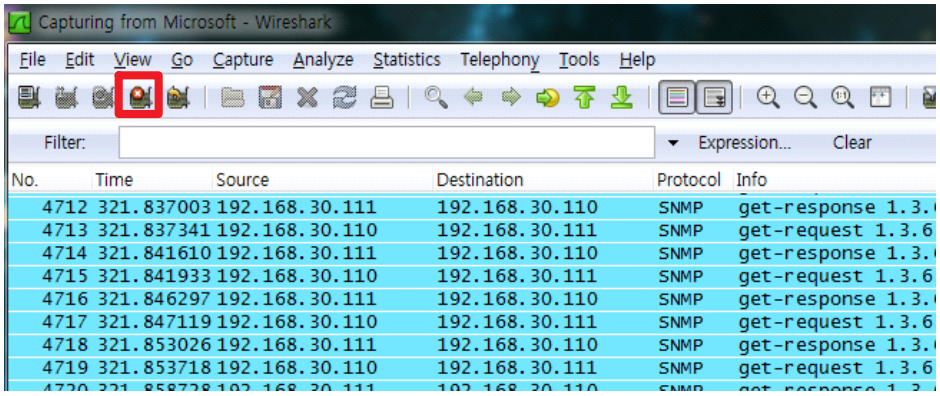
파란색 네모 안에는 데이터 안의 값을 사용자가 보기 쉽게 만들어 놓은 거에요.

노란색 네모 안에는 원래 컴퓨터가 이해할 수 있는 데이터의 값들이 들어 있어요.

Capture를 중지 하고 싶을 때는 다시 이 아이를 클릭하시고 Stop버튼을 눌러서 중지 할 수도 있고,




그냥 이 아이 하나 눌러서 중지 할 수도 있어요.




여기까지가 WireShark 설치와 기본적인 사용법입니다.
나머지 기능들은 직접 클릭해가면서 알아보세요.
아~~주 다양하고 신기한 기능들이 많아요~:D