**네트워크 보안**

패킷 스니핑 툴 조사

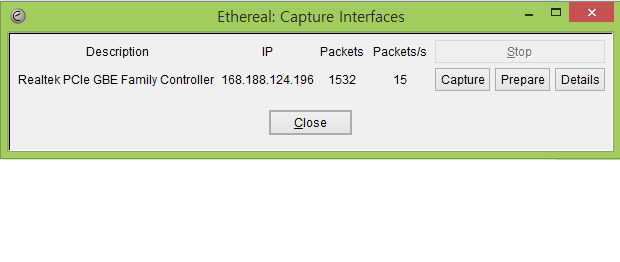
|  |  |
| --- | --- |
| 학번 | 이름 |
| 201002424 | 박지현 |
| 201102435 | 박민수 |
| 201102 | 이겨레 |

**1. Ethereal**

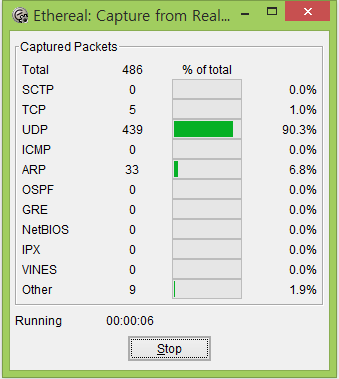
* 네트워크 모니터링 툴로, 자신이 보낸 패킷과 받은 패킷의 내용을 직접 볼 수 있다.
* 사용법

1) Ethereal 과 WinPcap을 설치한 후 Ethereal을 실행한다.

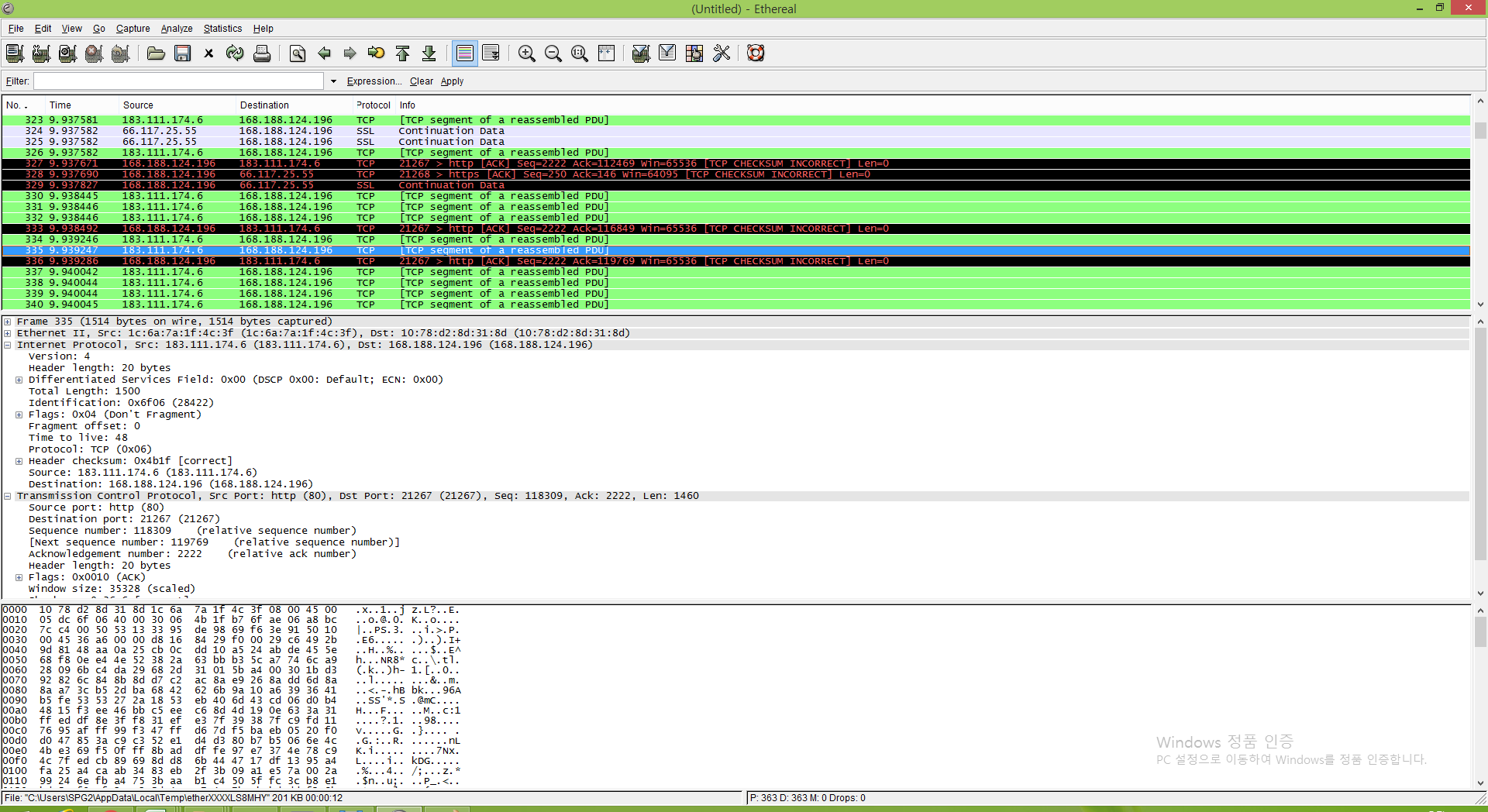
2) Capture에서 Interface를 누르면



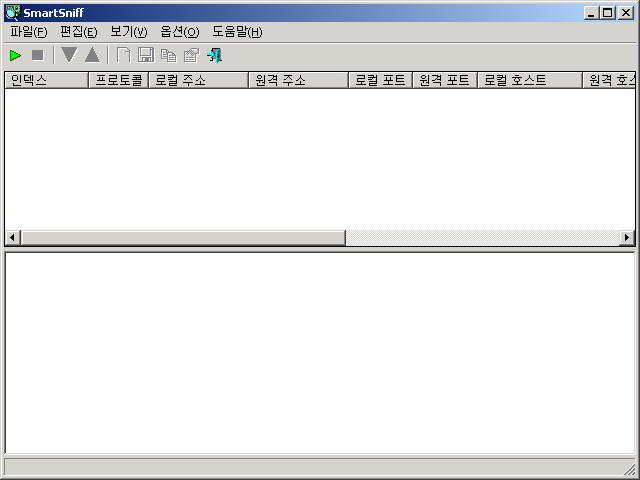
위와 같은 창이 나오는데, 여기서 자신의 IP에 해당하는 Capture를 선택하면 다음과 같은 창이 나온다.



3) 원하는 사이트에 들어가서 로그인 한 후 stop버튼을 누르면 아래와 같이 패킷이 캡처된 모습을 볼 수 있다.

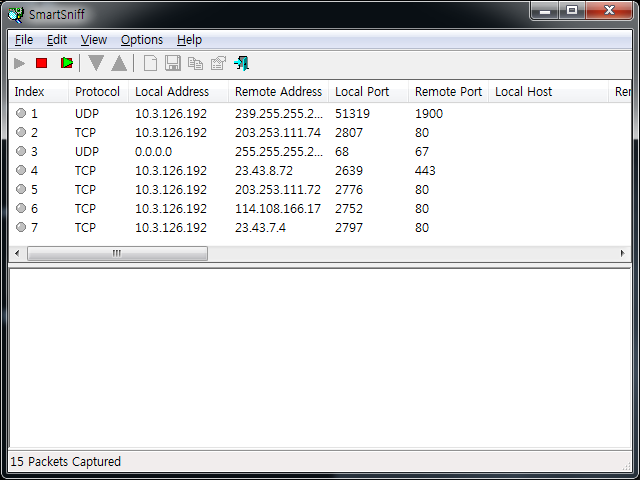


**2. Smart Sniff**



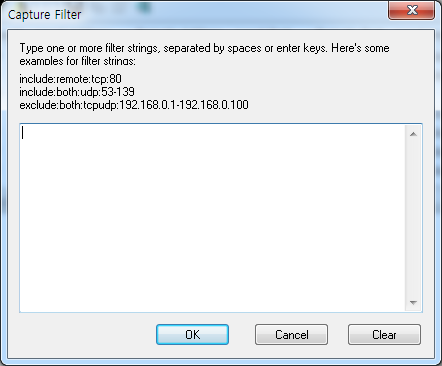
Download : http://www.nirsoft.net/utils/smsniff.html

패킷 캡쳐 기능

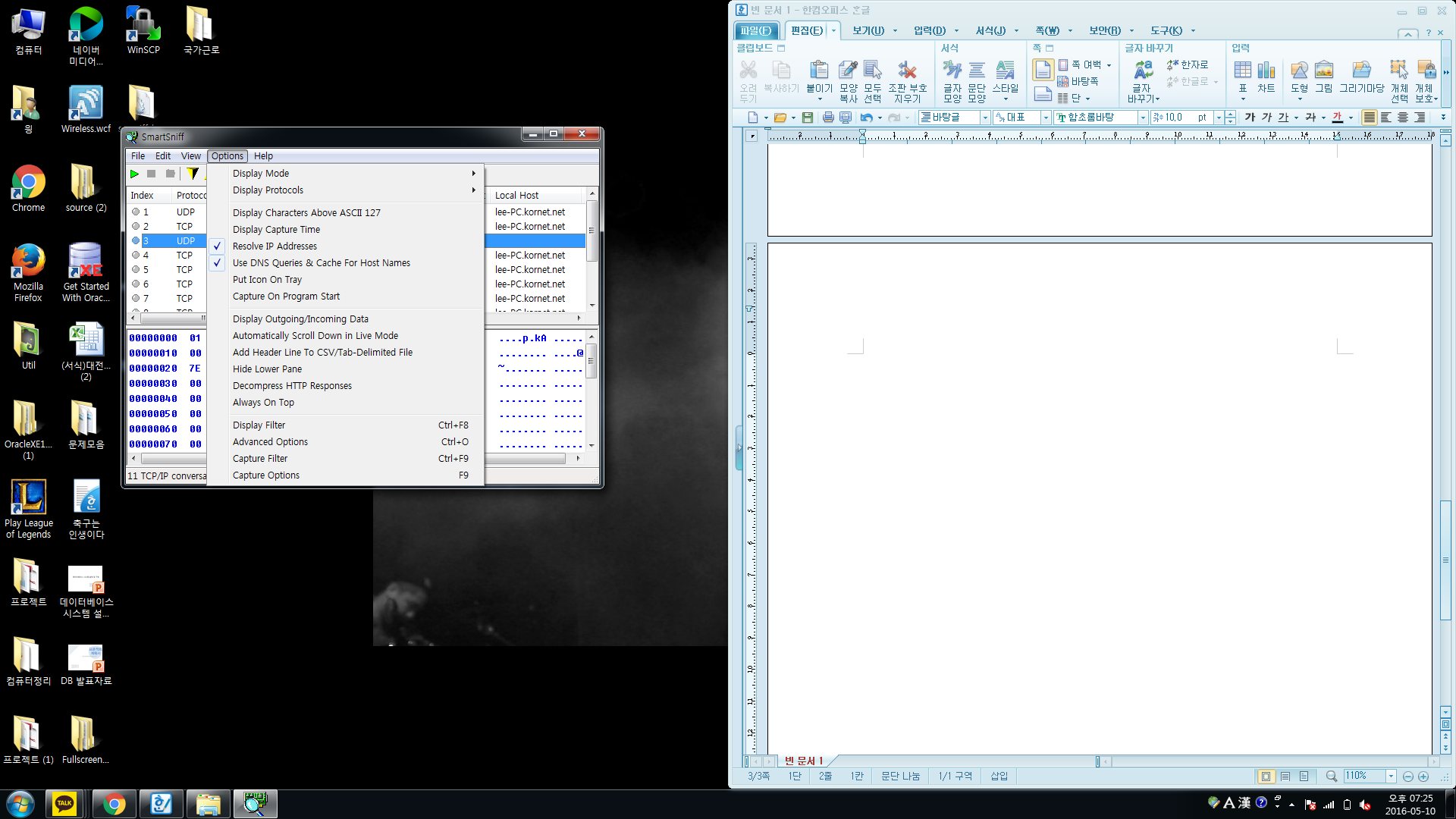


좌측 상단의 초록색 삼각형을 누르면 패킷을 캡쳐하기 시작한다.

캡쳐는 기본적으로 TCP UDP ICMP 세종류를 캡쳐하며 Option을 통해 필터링을 할 수 있다.



(필터화면)

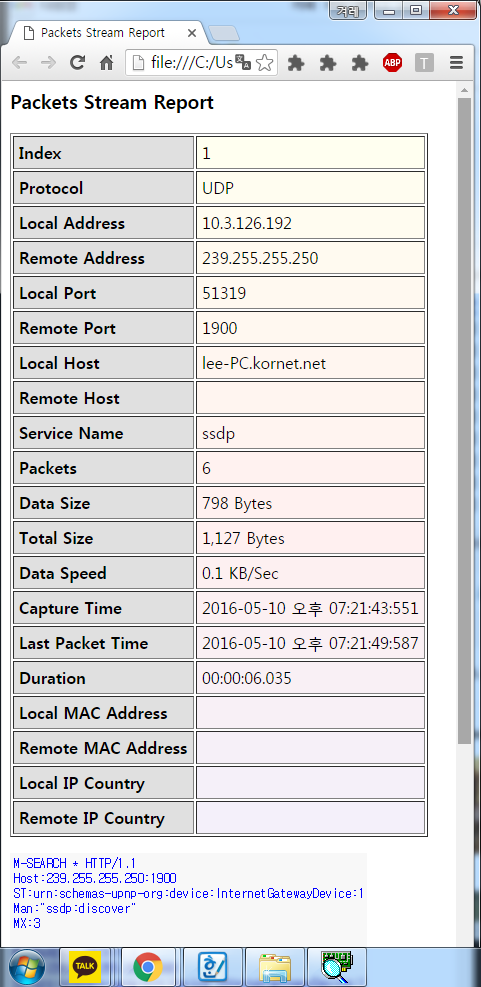


옵션창은 위와 같은데 주요 기능들은 다음과 같다.

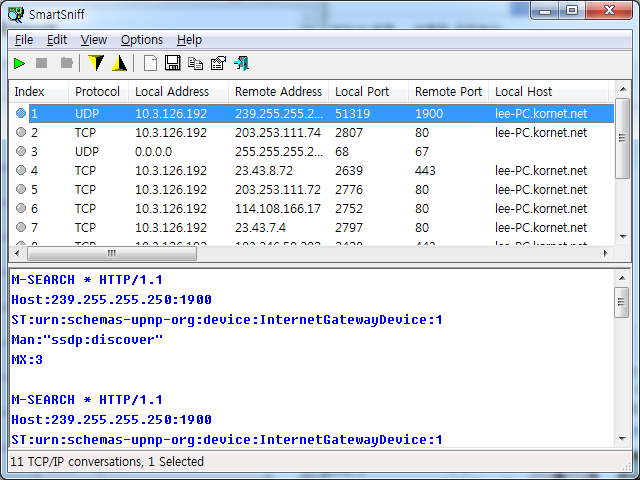
Display Protocols : TCP ICMP UDP 세가지중 보이고 싶은 protocol을 필터링한다.

Display Filter : Filterring 기능을 수행한다.

HTML reprot : 웹 페이지상에 패킷 흐름 정보를 출력한다.



캡쳐가 시작되면 다음과 같은화면이 출력되며 아래에 패킷의 정보가 보이게 된다.



패킷을 캡쳐하여 파일로 저장하고 분석하는데 도움을 주는 도구로써

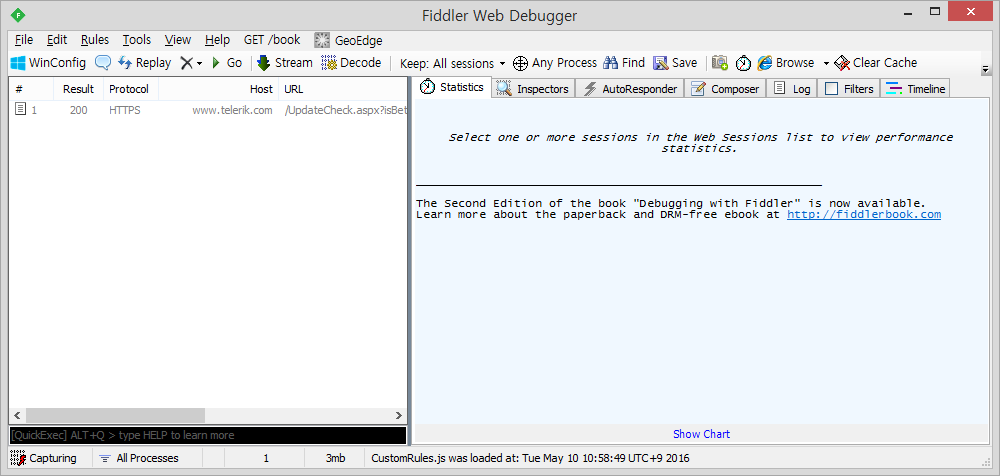
간편하게 사용 가능한 도구이며 작은 용량으로 간단한 패킷을 분석할 수 있는 도구이다.

**3. Fiddler**

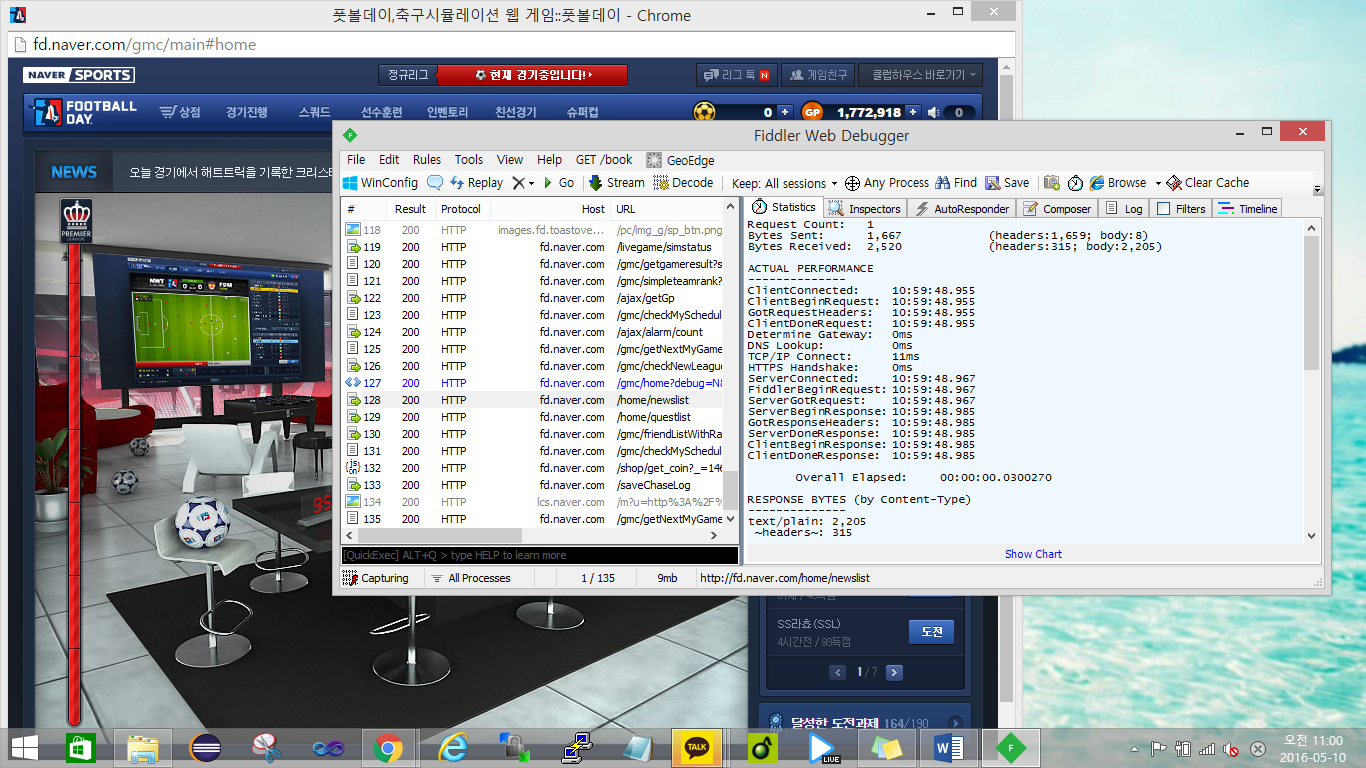
* 웹이나 모바일 등 네트워크를 통하는 모든 세션을 검사해 볼 수 있는 도구로서, 매우 간단하고 쉽게 패킷 스니핑이 가능하다.
* 사용법

1) Fiddler프로그램을 설치한다.

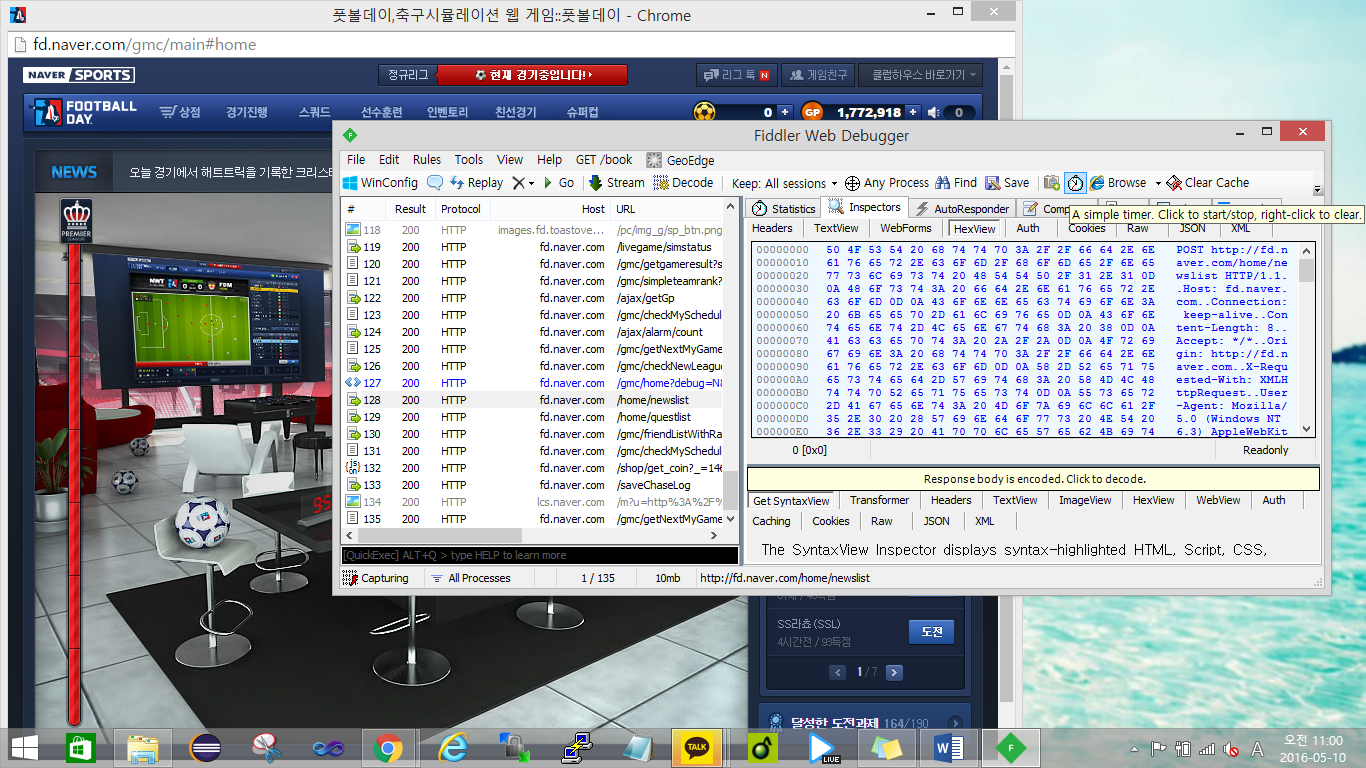
2) 설치 후 응용프로그램을 실행하면 다음과 같은 창이 뜬다.



2) 자신이 원하는 인터넷 사이트에 접속하면 좌측에 정보가 뜨는 것을 확인할 수 있다.

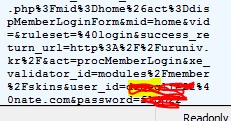


3) 자신이 보고싶은 세션을 선택한 후에 오른쪽에 Inspectors탭을 누르면 우측에서 각 내용을 확인할 수 있다.



**4. 취약점이 있는 사이트**

1) <http://uruniv.kr/> (Fiddler 툴 이용)



* 피들러를 이용하여 uruniv.kr 의 패킷을 캡처한 결과 id와 비밀번호가 나오는 것을 알 수 있음.