WireShark 프로그램의 기능 분석_ver1.1

추가 사항
1. 메인 윈도우 설명 삽입
2. 다이얼로그 박스 식별

1 메인 윈도우

- 와이어샤크의 '메인 윈도우'는 아래와 같다.

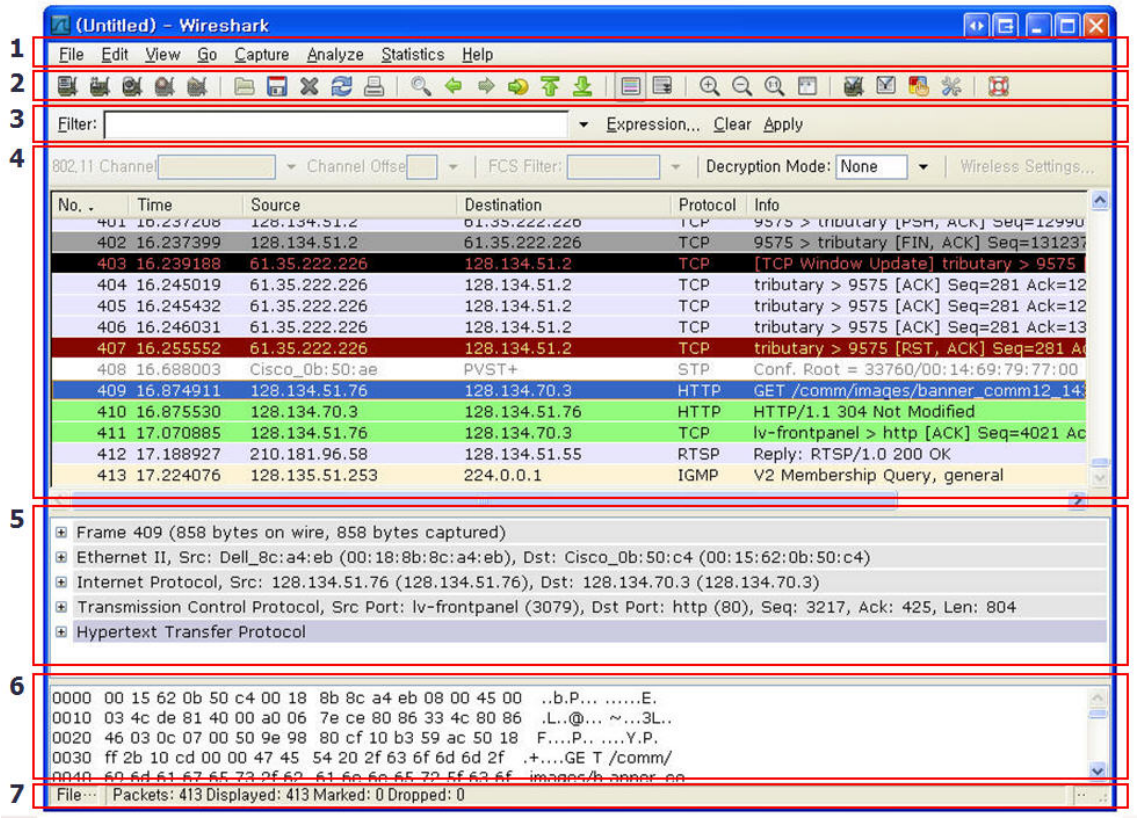

그림 1 메인 윈도우

- 1 : 메뉴바는 다양한 드롭&다운 메뉴 아이템들로 구성되어 있다.
- 2 : 툴바는 메뉴에서 제공하는 아이템들을 아이콘으로 제공함으로써, 신속한 접근을 제공한다. 또한 툴바 아이콘들은 사용자의 마우스 포인터 접근 시에 사용 툴 팁을 제공한다.
- 3 : 필터 툴바는 사용자가 패킷의 필터링된 화면을볼 수 있도록, 캡쳐할 패킷 혹은 현재 캡쳐된 패킷에 제약조건을 주는 방법을 제공한다.
- 4 : 패킷 목록 패인은 캡쳐된 패킷의 요약을 표시한다. 패킷의 클릭을 통해서, 자세한 패킷 정보를 볼수 있다.
- 5 : 패킷 상세 패인은 패킷 목록 패인에서 선택된 패킷의 상세한 정보를 표시한다.
- 6 : 패킷 비트 패인은 패킷 목록 패인에서 선택된 패킷의 데이터를 헥사값으로 표시한다.
- 7 : 상태바는 현재 프로그램 상태와 캡쳐된 데이터의 일부 상세화된 정보를 보여준다.

2 메뉴

- 와이어샤크에서 아래 그림과 같은 메뉴바를 제공하고 있으며, 본 1장에서는 메뉴의 각 기능과 사용법을 분석한다.

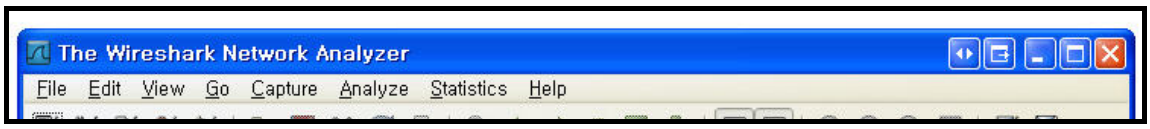

그림 2. 메뉴바

File	캡쳐 파일들을 열고(open), 합치고(merge), 전체나 일부를 저장(save)/프린트(print)/익스포트(export)하는 아이템들, Ethereal를 종료하는 아이템들을 제공한다.
Edit	패킷을 발견(find packet), 타임 레퍼런스(time reference), 한 개나 그 이상의 패킷에 대한 마크 레퍼런스(mark reference), 당신의 선택을 셋팅(set preference)하는 아이템들을 제공한다.
View	윈도우에서 보여주는 패킷들의 표시방법을 제어할 수 있도록, 폰트의 색깔과 크기 조절, 개별 윈도우에서의 패킷 표시, 패킷 상세정보상에서 트리조절 등의 아이템들을 제공한다.
Go	특정 패킷으로 이동하는 아이템들을 제공한다.
Capture	패킷 캡쳐의 시작과 종료, 캡쳐 필터들의 수정을 제공한다.
Analyze	표시 필터들을 다루고, 프로토콜들의 정밀한 분석 옵션을 제공한다.
Statistics	다양한 통계 윈도우들을 표시하기 위한 메뉴 아이템들을 제공한다.
Help	지원되는 프로토콜들의 목록, 메뉴얼 페이지, 일부 웹페이지에 대한 온라인 접근 등, 유저의 사용을 돕는 아이템들을 포함한다.

2.1 File

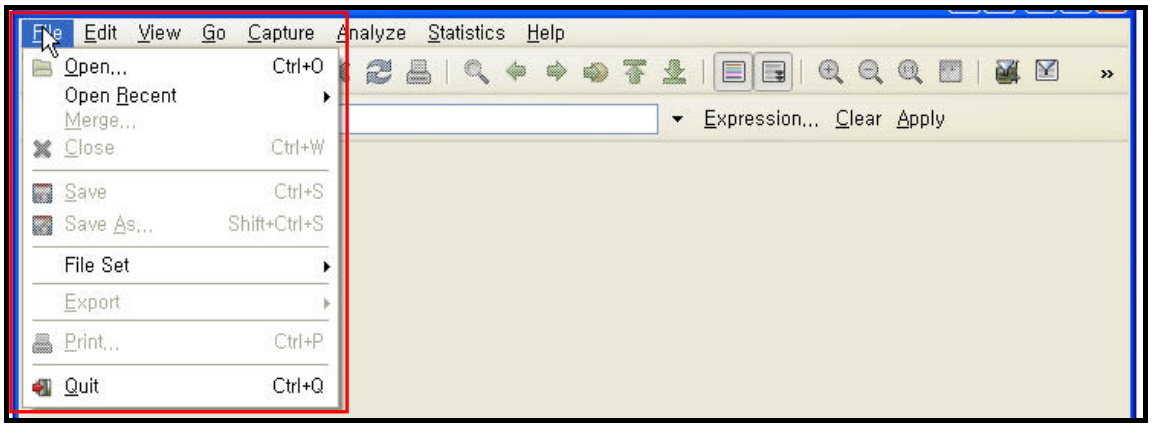

그림 3. File

▪ Open(Ctrl+O) : 캡쳐 파일을 로드한다.

-> File open dialog 박스 실행.

▪ Open Recent : 최근에 오픈되었던 캡퍼 파일들을 포함하는 서브 메뉴를 보여준다.

▪ Merge : 현재의 캡쳐 파일을 최근에 로드된 파일에 합치는 것을 허락하는 서브 메뉴를 보여준다.

-> Merge file dialg box 실행.

▪ Close(Ctrl+W) : 현재 캡쳐를 종료한다.

▪ Save(Ctrl+S) : 현재 캡쳐를 저장한다.

-> Save Capture As dialog box 실행.

▪ Save As(Shift+Ctrl+S) : 현재 캡쳐 파일을 다른 이름과 포맷으로 저장한다.

-> Save Capture As dialog box 실행.

▪ File Set > List Files : File set의 파일 리스트들을 보여준다.

-> Wireshark List File Set dialog box 실행.

▪ File Set > Next File : 현재 로드된 파일이 File set의 한 부분이라면, set의 다음 파일로 점프한다. 그렇지 않다면, 이 아이템은 비활성화 되어 있다.

▪ File Set > Previous File : 현재 로드된 파일이 File set의 한 부분이라면, set의 이전 파일로 점프한다. 그렇지 않다면, 이 아이템은 비활성화 되어 있다.

▪ Export > as "Plain Text" file : 파일상의 패킷들의 전부나 일부를 평이한 ASCII 텍스프 파일로 익스포트하는 것을 허락한다.

-> Wireshark Export dialog box 실행.

▪ Export > as "PostScript" file... : 캡쳐 파일상의 (일부) 패킷들을 PostScript 파일에 익스포트하는 것을 허락한다.

-> Wireshark Export dialog box 실행.

▪ Export > as "PSML" file... : 캡쳐 파일상의 (일부) 패킷들을 PSML(pac ket summary markup language) XML 파일에 익스포트한다.

-> Wireshark Export dialog box 실행.

▪ Export > as "PDML" file... : 캡쳐 파일상의 (일부) 패킷들을 PSML(packet details markup language) XML 파일에 익스포트한다.

-> Wireshark Export dialog box 실행.

▪ Export > Selected Packet Bytes...(Ctrl+H) : 패킷 바이트들 페인(pane)상의 현재 선택된 바이트들을 패킷들을 바이너리 파일에 익스포트한다.

-> Wireshark Export dialog box 실행.

▪ Print...(Ctrl+P) : 캡쳐 파일상의 전체(또는 일부) 패킷들을 프린트한다.

-> Wireshark Print dialog box 실행.

▪ Quit(Ctrl+Q) : 와이어셔크를 종료한다.

2.2 Edit

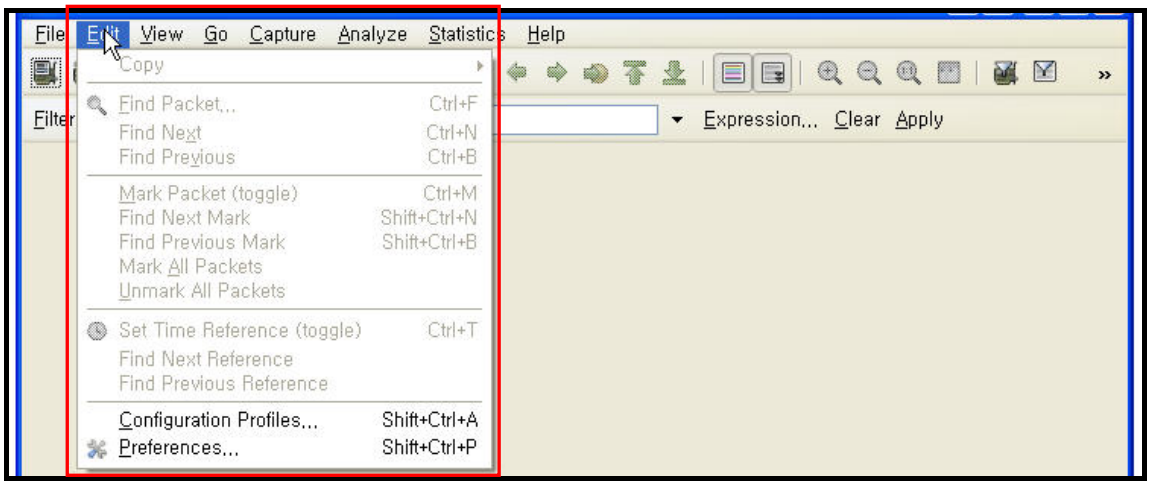

그림 4. Edit

▪ Copy > As Filter(Shift+ Ctrl+ C) : 디스플레이 필터를 만들기 위해 사용된다. 그후 디스플레이 필터는 클립보드에 복사된다.

▪ Find Packet...(Ctrl+ F) : 디스플레이 필터(display filter)나 기타 여러 기준에 의해서 패킷을 찾는다.

-> Find Packet dialog box 실행.

▪ Find Next(Ctrl+ N) : "Find Packet..."의 셋팅들에 대하여 일치하는 패킷을 찾으다.

▪ Find Previous(Ctrl+ B) : "Find Packet..."의 셋팅들에 대하여 이전에 일치하는 패킷을 찾는다.

▪ Mark Packet(Ctrl+ M) : 현재 선택된 패킷을 마크한다.

▪ Find Next Mark (Shift+ Ctrl+ N) : 이후에 마크된 패킷을 찾는다.

▪ Find Previous Mark (Shift+ Ctrl+ B) : 이전에 마크된 패킷을 찾는다.

▪ Mark All Packets : 모든 패킷들을 마크한다.

▪ UnMark All Packets : 마크된 모든 패킷을 해제한다.

▪ Set Time Reference(Ctrl+ T) : 현재 선택된 캡쳐에 대하여 time reference를 셋팅한다.

▪ Find Next Reference: 다음에 참조된(time referenced) 패킷을 찾는다.

▪ Find Previous Reference: 이전에 참조된(time referenced) 패킷다.

▪ Configuration Profiles(Shift+ Ctrl+ A)

-> Configuration profile들을 컨트롤 하기위한 dialog box 실행.

▪ Preferences...(Shift+ Ctrl+ P) : 와이어샤크를 제어하는 많은 파라미터들을 통하여 선호들(preferences)을 셋팅한다.

-> Preferences dialog box 실행.

2.3 View

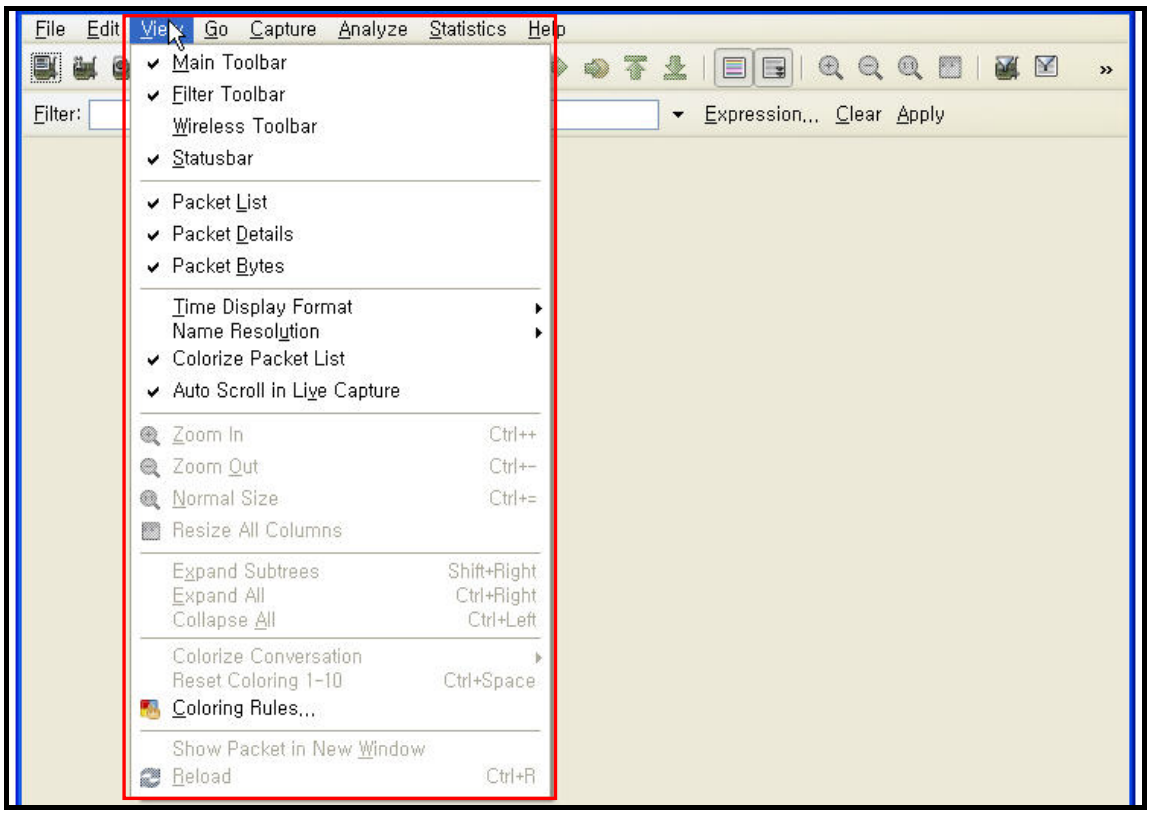

그림 5. View

- Main Toolbar : 메인 툴바를 숨기거나 보여준다.
- Filter Toolbar : 필터 툴바를 숨기거나 보여준다.
- Wireless Toolbar : 와이어리스 툴바를 숨기거나 보여준다.
- Statusbar : 상태바를 숨기거나 보여준다.
- Packet List : 패킷 리스트 페인(pane)을 숨기거나 보여준다.
- Packet Details : 패킷 상세내용 페인(pane)을 숨기거나 보여준다.
- Packet Bytes : 패킷 바이츠 페인(pane)을 숨기거나 보여준다.
- Time Display Format > Time of Day : 와이어샤크의 데이터 포맷의 시간에 있어서 타임 스탬프들을 표시한다.
- Time Display Format > Date and Time of Day : 와이어샤크의 데이터 포맷의 날짜와 시간에 있어서 타임 스탬프들을 표시한다.
- Time Display Format > Seconds Since Beginning of Capture : 와이어샤크의 캡쳐 포맷의 시작 이후의 초(Second)들에 타임 스탬프들을 표시한다.
- Time Display Format > Seconds Since Previous Packet : 와이어샤크가 이번 패킷 포맷 이후의 초(Second)들에 타임 스탬프들을 표시한다.

▪ Name Resolution > Resolve Name : 현재 패킷에 대한 네임 리졸브를 시작한다.
▪ Name Resolution > Enable for MAC Layer : 와이어샤크의 MAC 주소들을 네임들로 변환할 것인지 제어한다.
▪ Name Resolution > Enable for Network Layer : 와이어샤크의 네트워크 주소들을 네임들로 변환할 것인지 제어한다.
▪ Name Resolution > Enable for Transport Layer : 와이어샤크의 트랜스포트 주소들을 네임들로 변환할 것인지 제어한다.
▪ Auto Scroll in Live Capture : 와이어샤크가 패킷 목록 페인(pane)을 스크롤해야 하는 것을 명세화하는 것을 허락한다.
▪ Zoom In(Ctrl++) : 패킷 데이터의 폰트사이즈를 증가시킨다.
▪ Zoom Out(Ctrl+-) : 패킷 데이터의 폰트사이즈를 축소시킨다.
▪ Normal Size : 패킷 데이터의 폰트사이즈를 표준으로 바꾼다.

2.4 Go

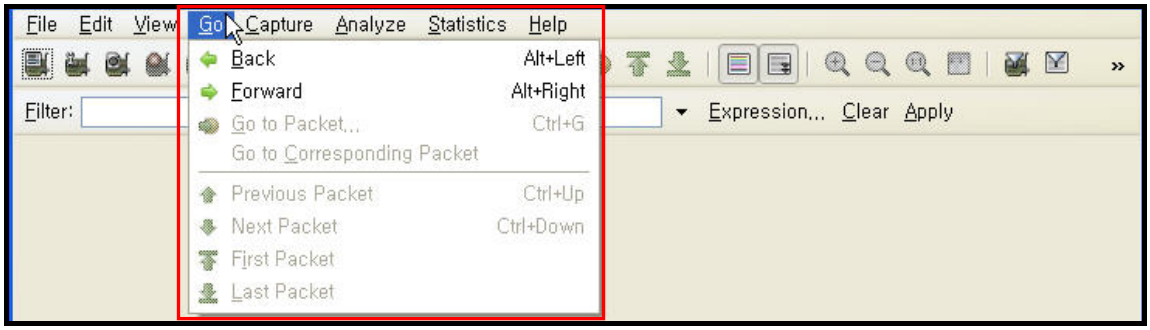

그림 6. Go

▪ Back : 패킷 히스토리에 저장되어 있는 가장 최근의 패킷으로 이동한다.
▪ Forward : 패킷 히스토리에 저장되어 있는 다음 패킷으로 이동한다.
▪ Go to Packet...(Ctrl-G) : 패킷 번호를 명세화하는 것을 허락하는 다이얼로그 박스를 호출하고, 그 패킷으로 이동한다.
▪ Go to Corresponding Packet : 현재 선택된 프로토콜 필드에 상응하는 패킷으로 이동한다.
▪ Previous Packet : 이전 패킷으로 이동한다.
▪ Next Packet : 다음 패킷으로 이동한다.
▪ First Packet : 캡쳐 파일의 처음 패킷으로 이동한다.
▪ Last Packet : 캡쳐 파일의 마지막 패킷으로 이동한다.

2.5 Capture

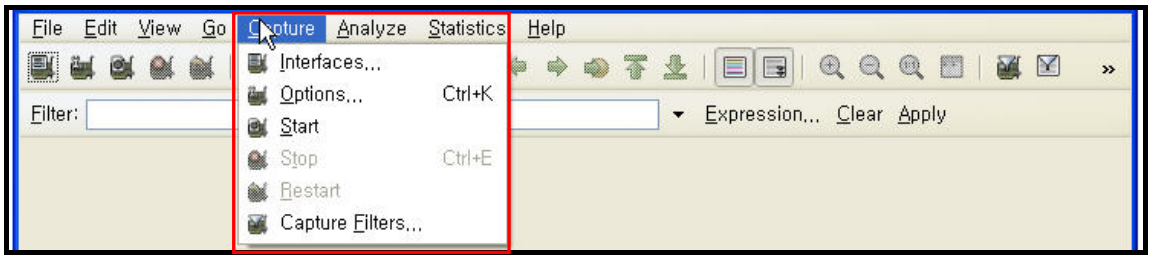

그림 7. Capture

▪ Interface : 선택할 수 있는 네트워크 인터페이스를 보여준다.

-> Capture Interface dialog box 실행.

▪ Option (Ctrl+K) : 캡쳐 옵션의 다이얼로그 박스를 호출한다.

-> Capture Option dialog box 실행.

▪ Start... : 당신이 패킷들을 캡쳐하는 것을 시작한다.

▪ Stop...(Ctrl+E) : 현재 작동중인 캡쳐를 정지한다.

▪ Capture Filters... : 캡쳐 필터들을 생성하고 수정하는 것을 허락하는 다이얼로그 박스를 호출한다.

-> Capture Filter dialog box 실행.

2.6 Analyze

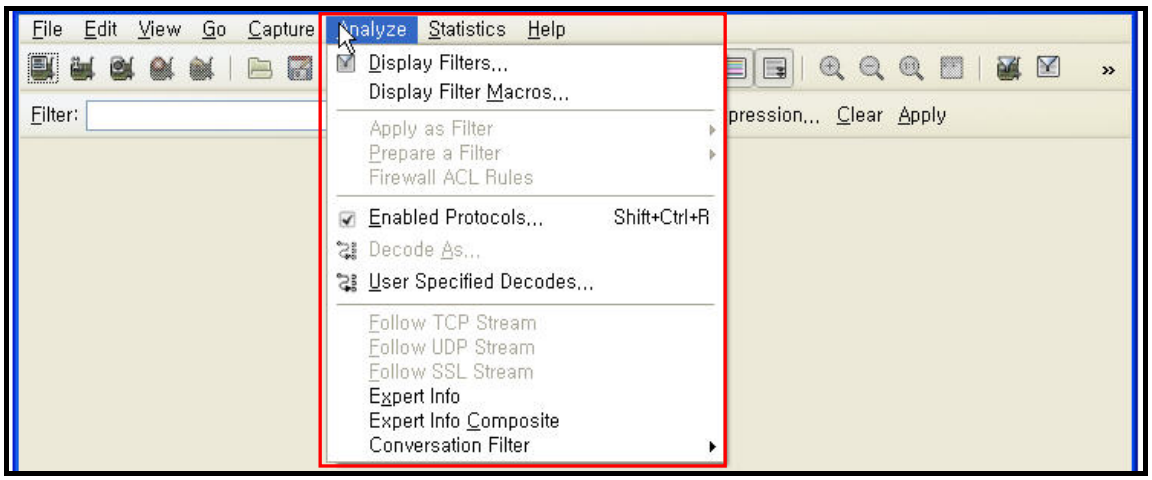

그림 8. Analyze

▪ Display Filters... : 디스플레이 필터들을 생성하고 수정하는 것을 허락하는 다이얼로그 박스를 호출한다.

-> Display Filter dialog box 실행.

▪ Display Filter Macros

-> Display Filter Macros dialog box 실행.

▪ Apply as Filter > ... : 현재 디스플레이 필터를 변경하고 즉시 변경된 필터를 적용한다.

▪ Prepare a Filter > ... : 현재 디스플레이 필터를 변경하지만, 바로 적용하지 않는다. 선택된 메뉴 아이템에 따라서, 현재 디스플레이 필터 스트링은 패킷 상세 페인상의 선택된 프로토콜 필드곁에 대치되거나 추가된다.

▪ Enabled Protocols...(Shift+ Ctrl+ R) : 프로토콜 해부기구들을 사용 가능하게 하거나 사용 불가능하게 한다.

▪ Decode As... : 와이어샤크가 어떤 패킷들을 특정 프로토콜로 강제적으로 디코드한다.

▪ User Specified Decodes... : 와이어샤크가 어떤 패킷들을 특정 프로토콜로 강제적으로 디코드한다.

▪ Follow TCP Stream : 분리된 윈도우를 호출하고 선택된 패킷으로써 같은 TCP 커넥션상에 존재하는 모든 캡쳐된 TCP 세그먼트들을 표시한다.

▪ Follow UDP Stream : 분리된 윈도우를 호출하고 선택된 패킷으로써 같은 UDP 커넥션상에 존재하는 모든 캡쳐된 UDP 세그먼트들을 표시한다.

▪ Follow SSL Stream : 분리된 윈도우를 호출하고 선택된 패킷으로써 같은 SSL 커넥션상에 존재하는 모든 캡쳐된 SSL 세그먼트들을 표시한다.

2.7 Statistics

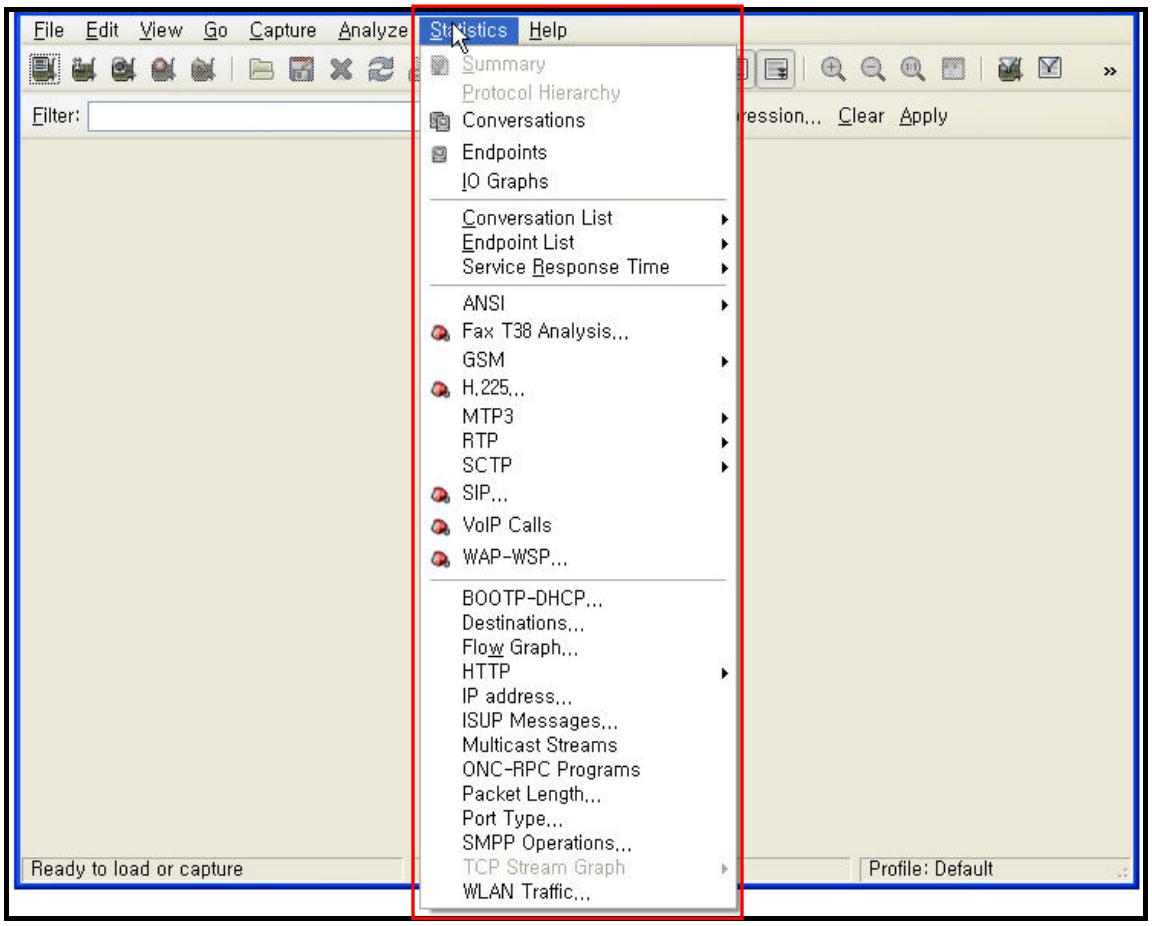

그림 9. Statistics

- **Summary** : 캡쳐된 데이터에 대한 정보를 보여준다.

-> Summary dialog box 실행.

- **Protocol Hierarchy** : 프로토콜 통계의 계층구조를 표시한다.

-> Protocol Hierarchy Statistics dialog box 실행.

- **Conversations** : 대화들의 목록을 표시한다.

-> Conversations dialog box 실행.

- **Endpoints** : 종점들의 목록을 표시한다.

-> Endpoints dialog box 실행.

- **IO Graphs** : 명세화된 그래프들을 표시한다.

-> IO Graphs dialog box 실행.

- **Conversation List** : Conversations 창에서 사용하지 않는 대화 목록들을 표시한다.
- **Endpoint List** : Endpints 창에서 사용하지 않는 종점들의 목록을 표시한다.

▪ Service Response Time : 요청과 그에 상응하는 응답 사이의 시간을 표시한다.

2.8 Help

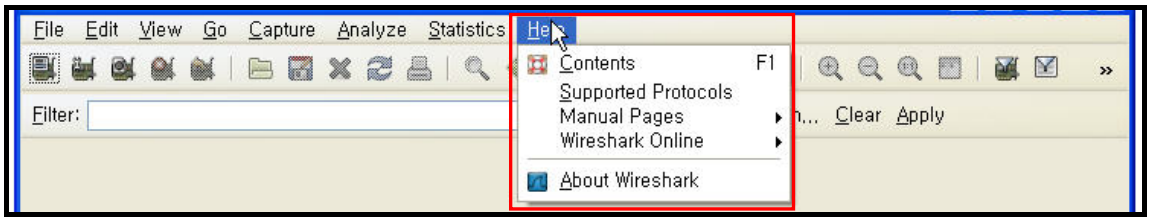

그림 10. Help

▪ Contents(F1) : 기본 헬프 시스템을 호출한다.

-> User's Guide dialog box 실행.

▪ Supported Protocols : 지원되는 프로토콜들과 프로토콜 필드들을 보여주는 다이얼로그 박스를 호출한다.

-> Supported Protocols dialog box 실행.

▪ Manual Pages > ... : 로컬에 설치된 html 매뉴얼 페이지들 중 한개를 보여주는 웹 브라우저를 실행한다.

▪ Wireshark Online > ... : http://www.wireshark.org 웹 브라우져를 실행한다.

▪ About WireShark : 플러그인들과 사용된 폴더들과 같은 Ethereal에 대한 일부 정보를 공급하는 정보 창을 호출한다.

-> About WireShark dialog box 실행.