Wireshark

Jin Seek Choi
jinseek@hanyang.ac.kr
Ref: Hiral Chhaya, Anvita Priyam
By Fei Xu

About Wireshark

- **It is a packet sniffer Computer application**
- **Functionality is very similar to tcpdump**
- **Has a GUI front-end and many more information sorting and filtering options**

About Wireshark

- **Wireshark is a network packet/protocol analyzer.**
  - **A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.**
- **Wireshark is perhaps one of the best open source packet analyzers available today for UNIX and Windows.**
- **It has two libraries:**
  - **WinPcap for Windows OS**
  - **LibPcap for Linux OS**

Some intended purposes

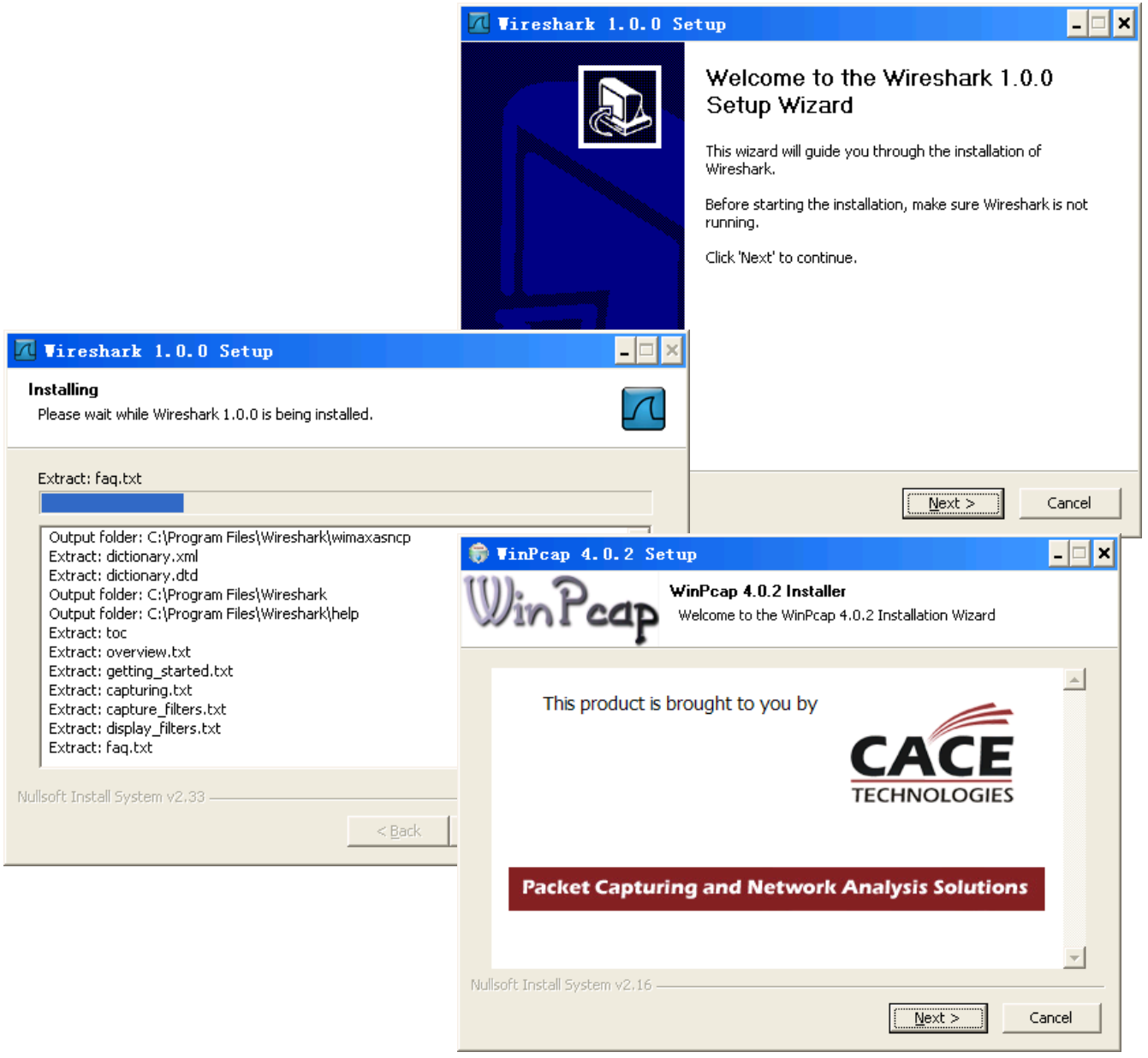
- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals
- Wireshark isn't an intrusion detection system
- Wireshark will not manipulate things on the network, it will only "measure" things from it

Install Wireshark

- **Visit this site**
  - **http://www.wireshark.org**
  - **http://wiki.wireshark.org**
- **Windows**
  - **Download**
    - wireshark-win32(or win64)-(version).exe
- **Debian/Ubuntu Linux**
  - **sudo apt-get install wireshark**
  - **sudo wireshark**

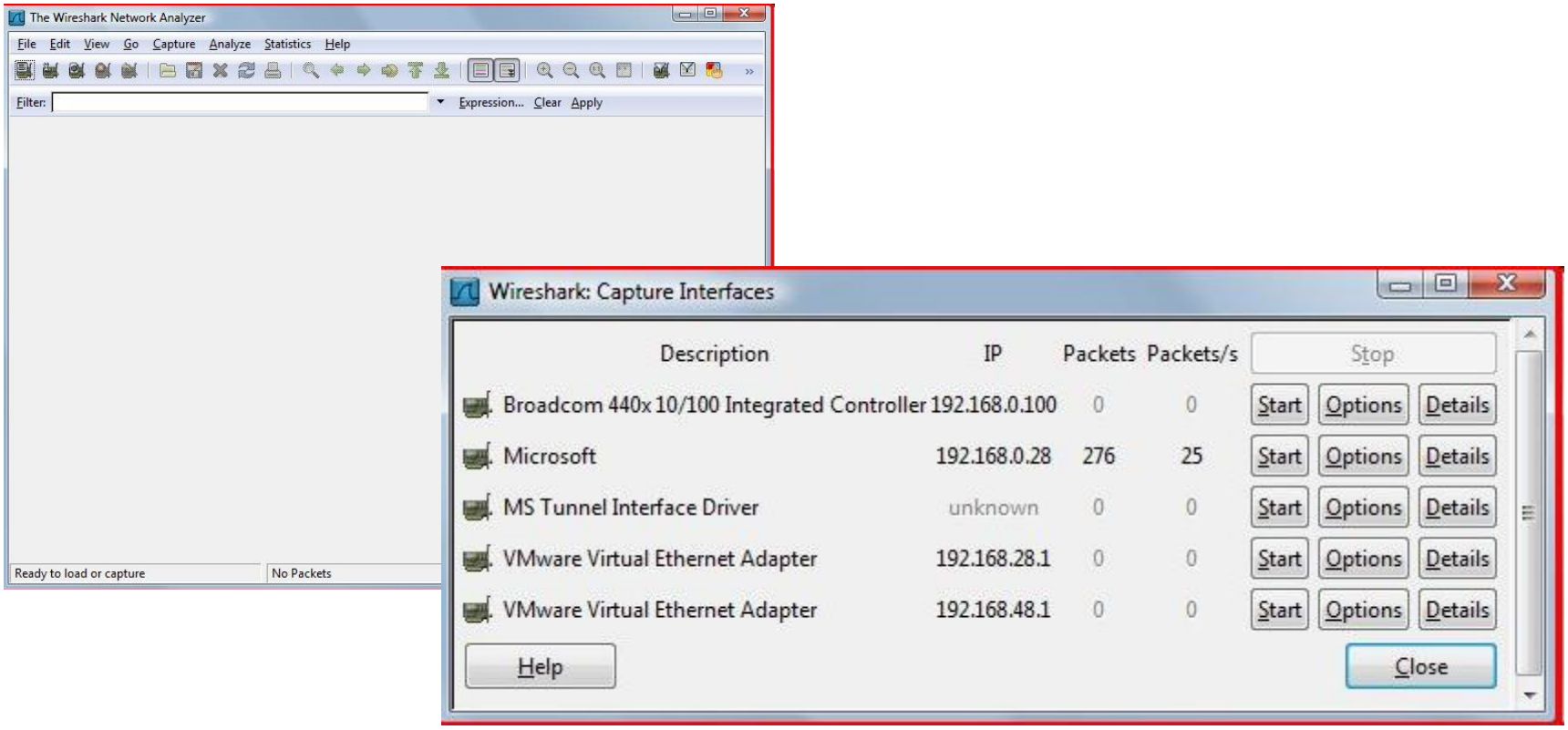
Install under Windows

- **Download**
- **Install**



Install under Debian/Ubuntu

- ***# apt-get install wireshark***

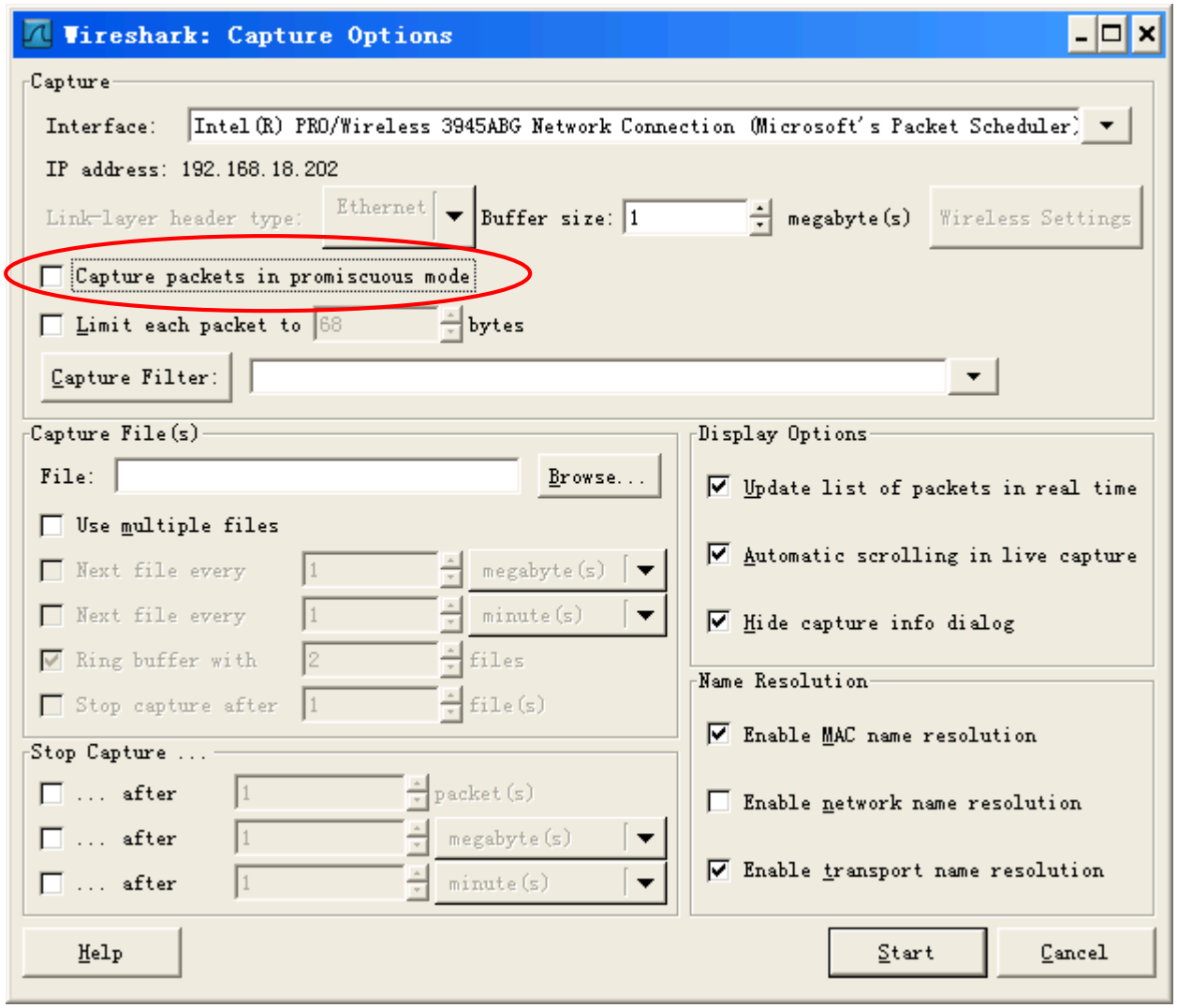


Configuration

- **Turn the PROMISCUOUS MODE off!**
- **If you are at work, your Network Administrator may see you running in PROMISCUOUS MODE: a feature normally used for packet sniffing**
- **You maybe considered as a sniffer and somebody may decide to fire you for that**

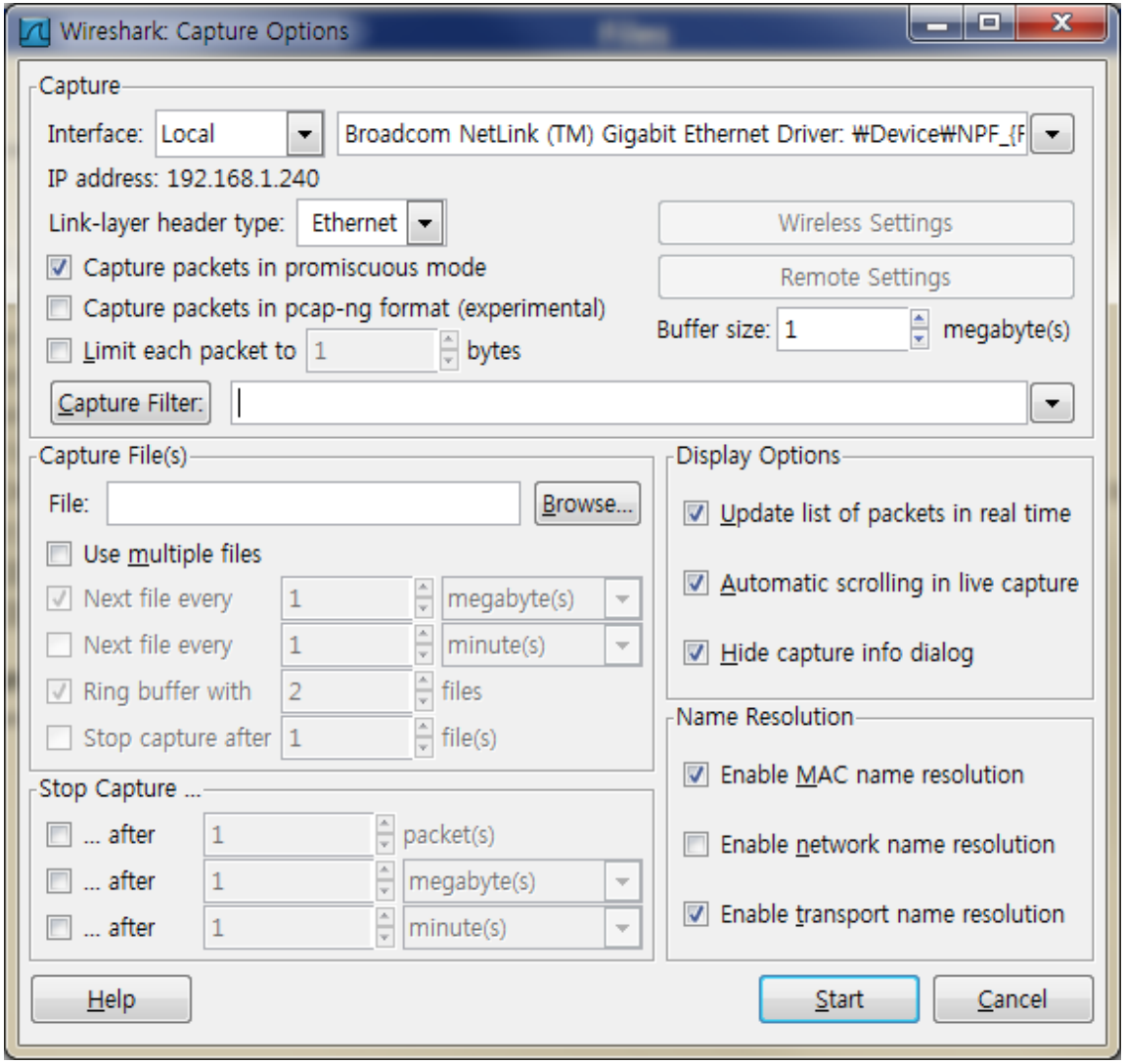
Configuration

This checkbox allows you to specify that Wireshark should put the interface in **promiscuous** mode when capturing. If you do not specify this, Wireshark will only capture the packets going to or from your computer (not all packets on your LAN segment)

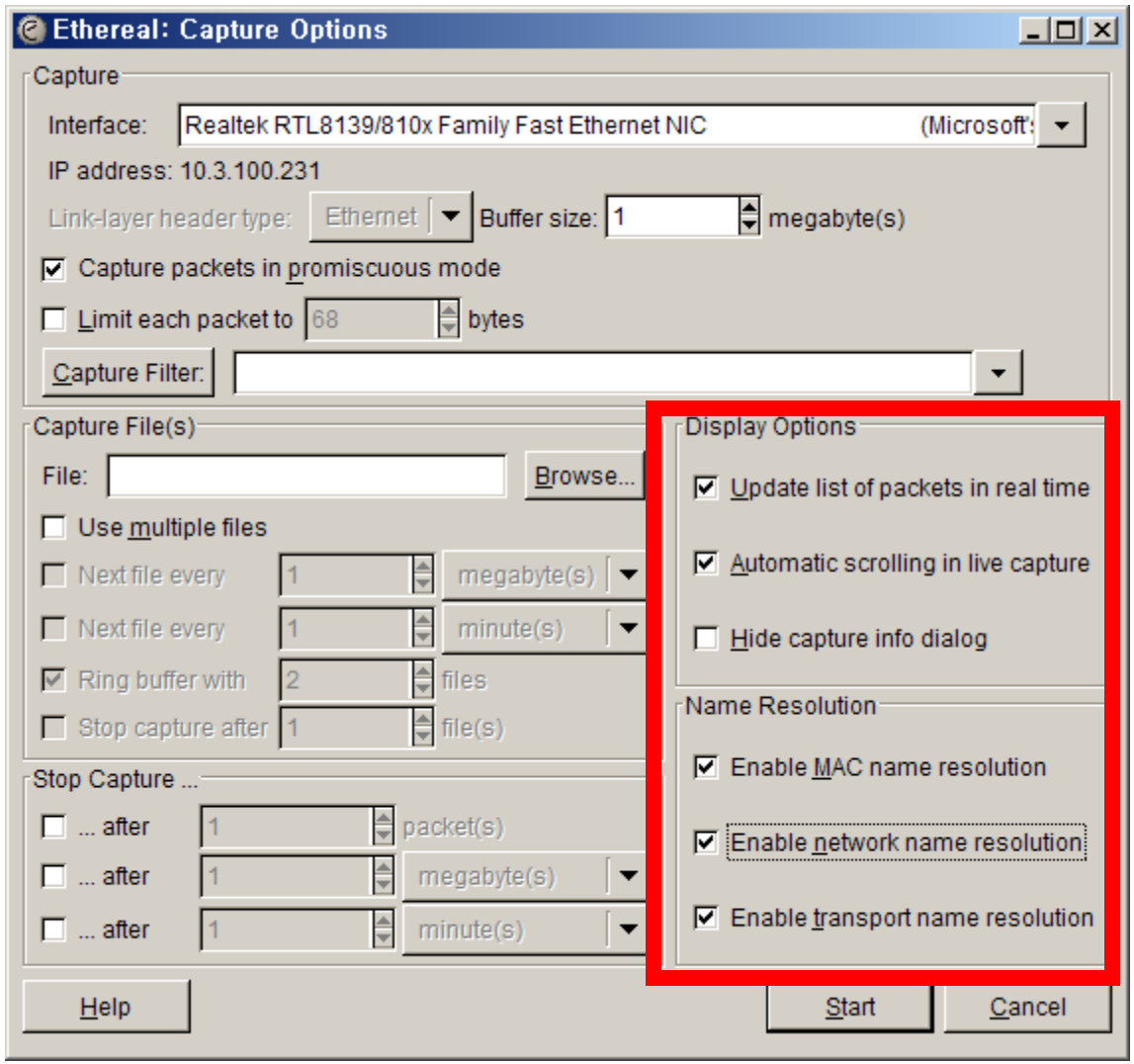


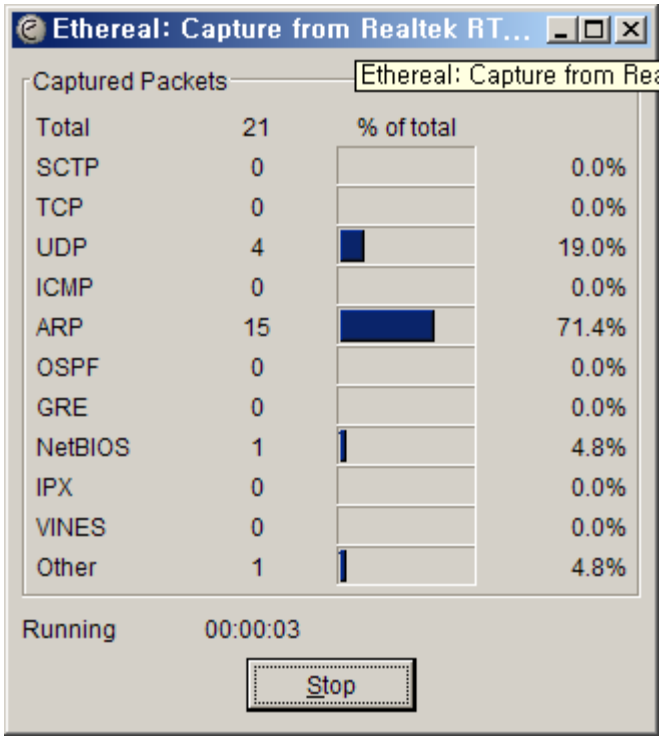
Configuration

- **Promiscuous mode**
  - promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just frames addressed to it



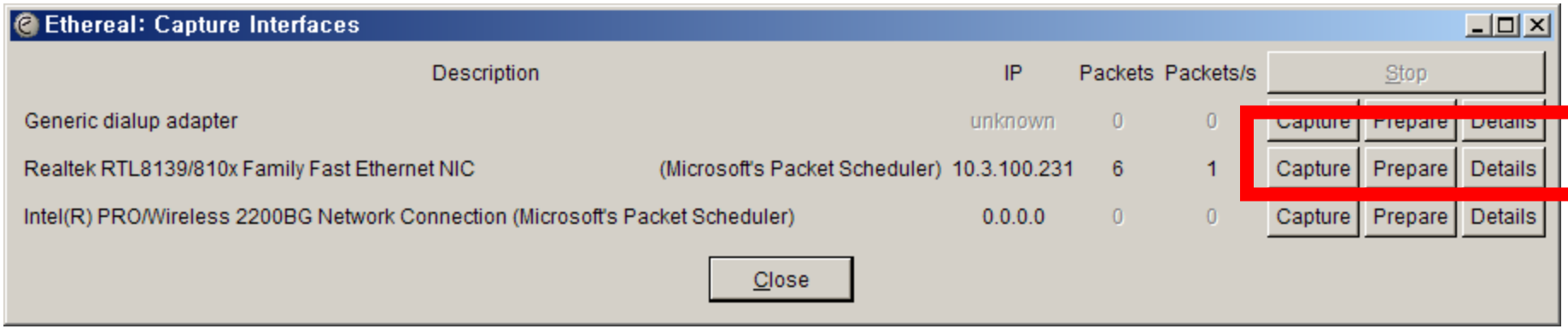
Configuration: Capture Options





Capturing Live Network Data

- **Start Capturing**
- **"Capture Interfaces" dialog box**
- **"Capture Options" dialog box**



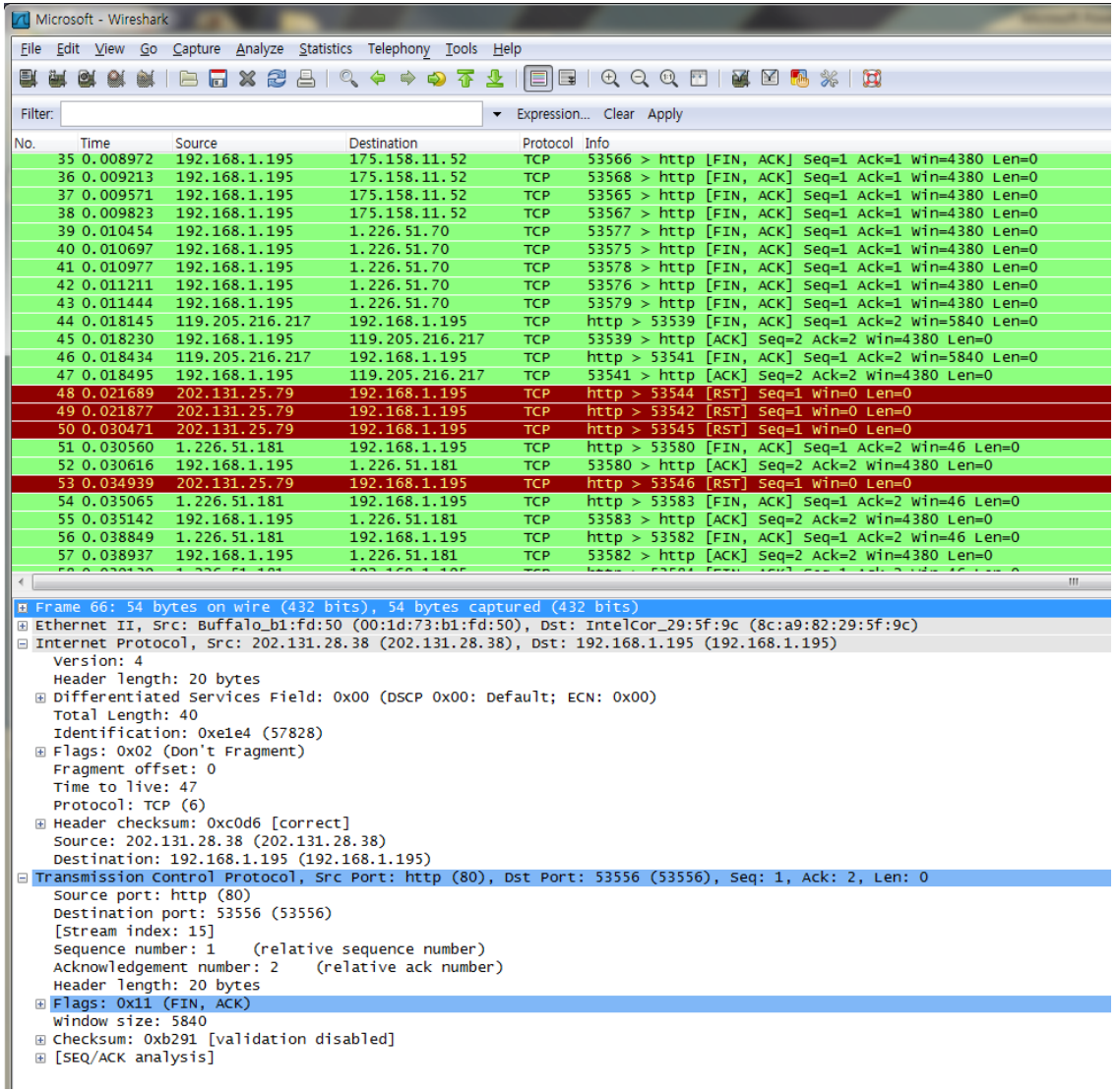
Demo

- ✓ **HTTP**
- **TCP**
- **DNS**
- **ARP**

Photo credit: Jeff Kubina

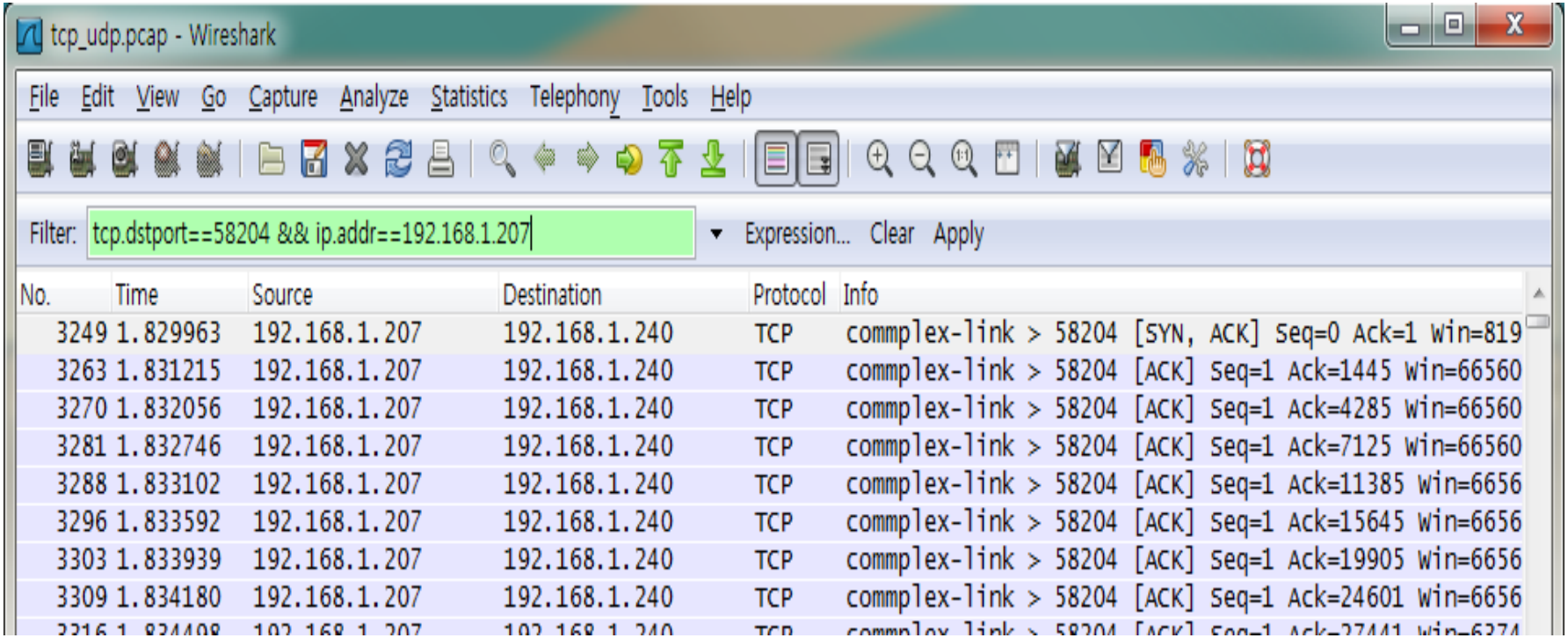
Demo: HTTP Packet Capture

- **When you browse Internet, you can capture HTTP (TCP) packets**



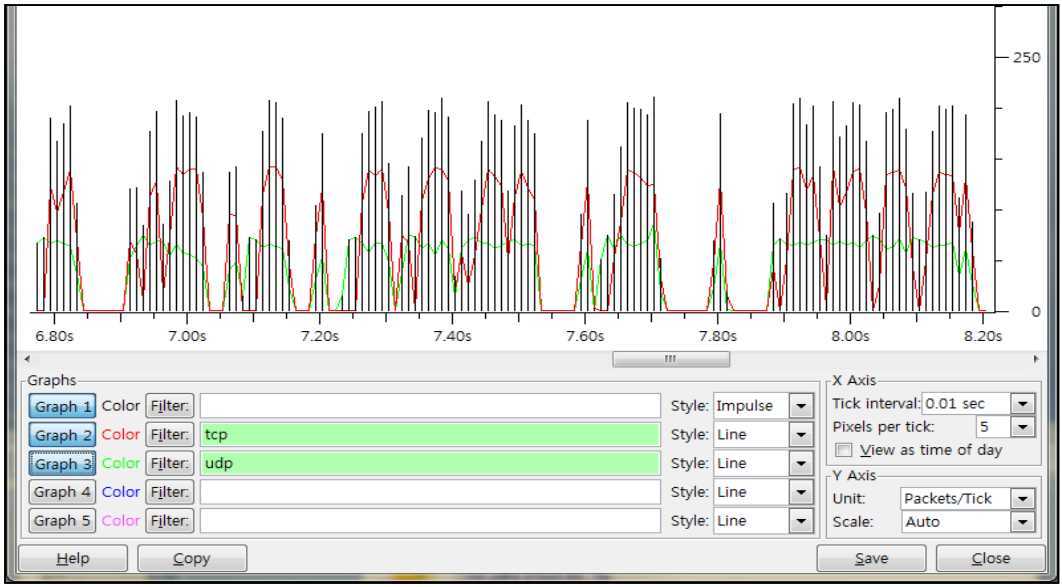
Demo: Filtering Packets

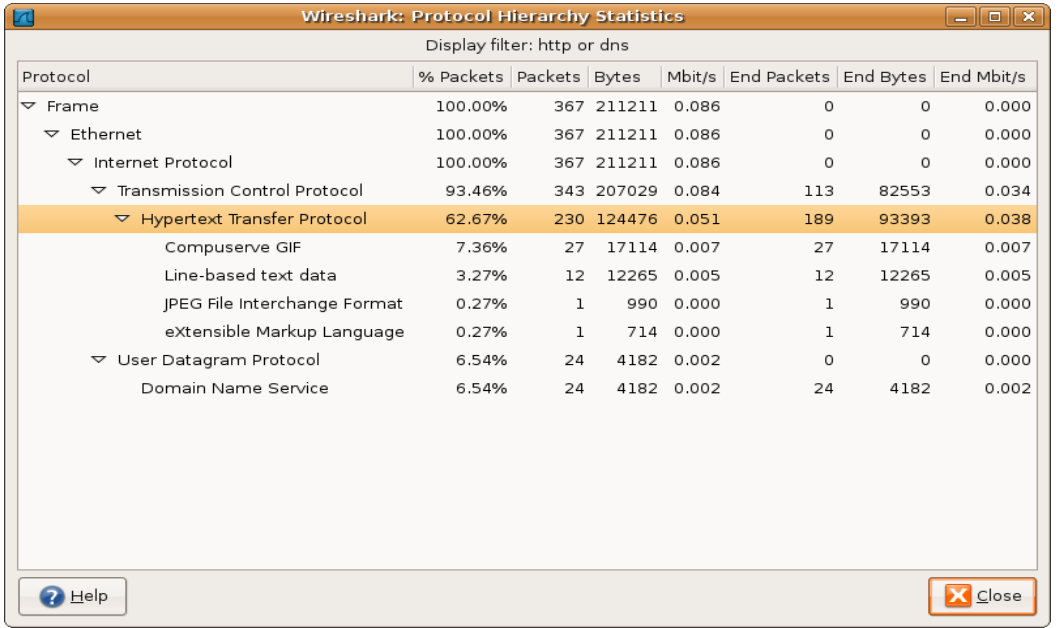
- **Use “Filter”**
  - **Rule : write field name and relation**
    - Check the Expression button → this button shows filtering rules



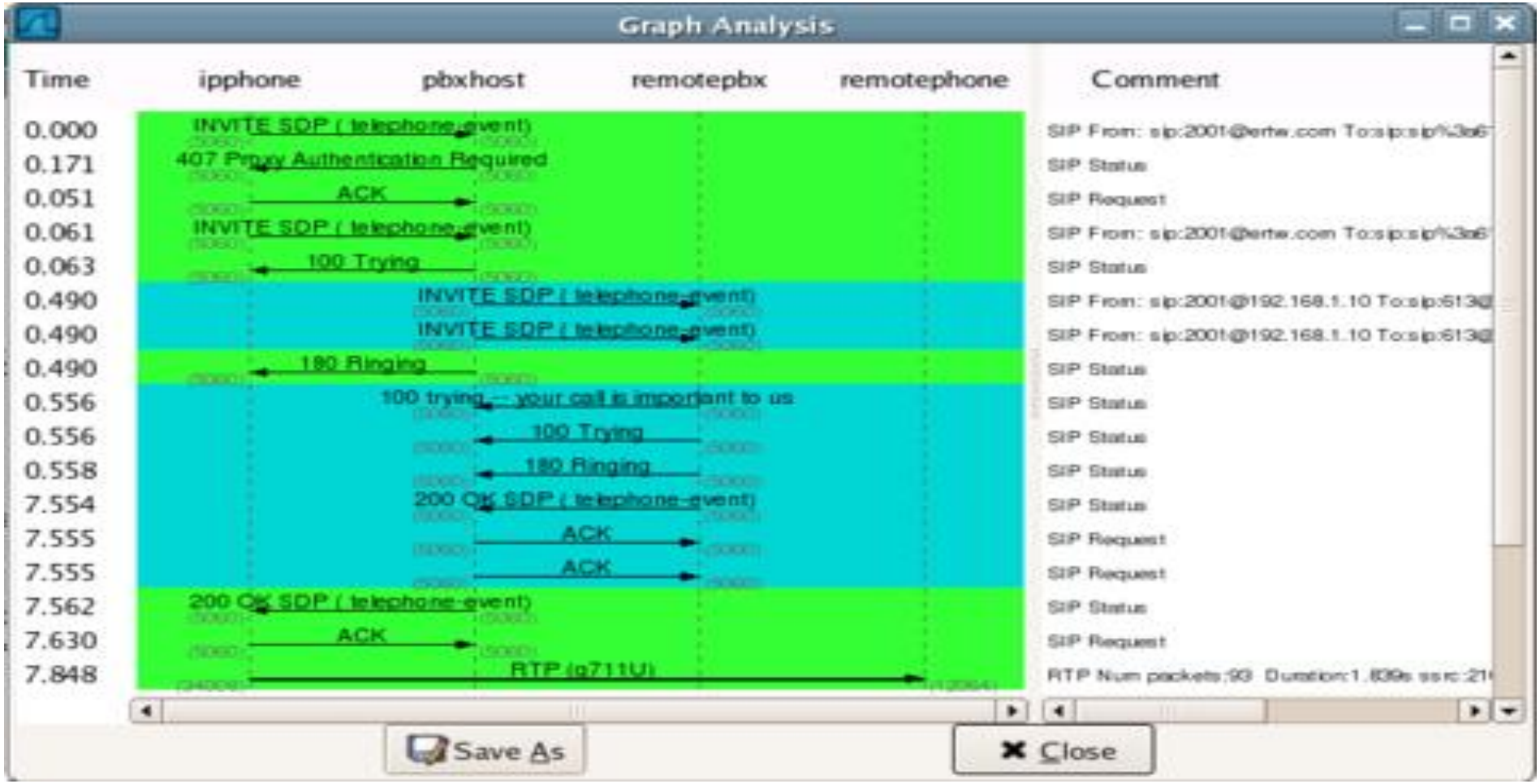
Demo: Statistics

- **IO graphs**
  - Visualizing the number of packets (or similar) in time
- **Protocol Hierarchy**
  - The protocol hierarchy of the captured packets
- **Summary**
  - General statistics about the current capture file
- **Flow graph**
  - Show the flow of packets



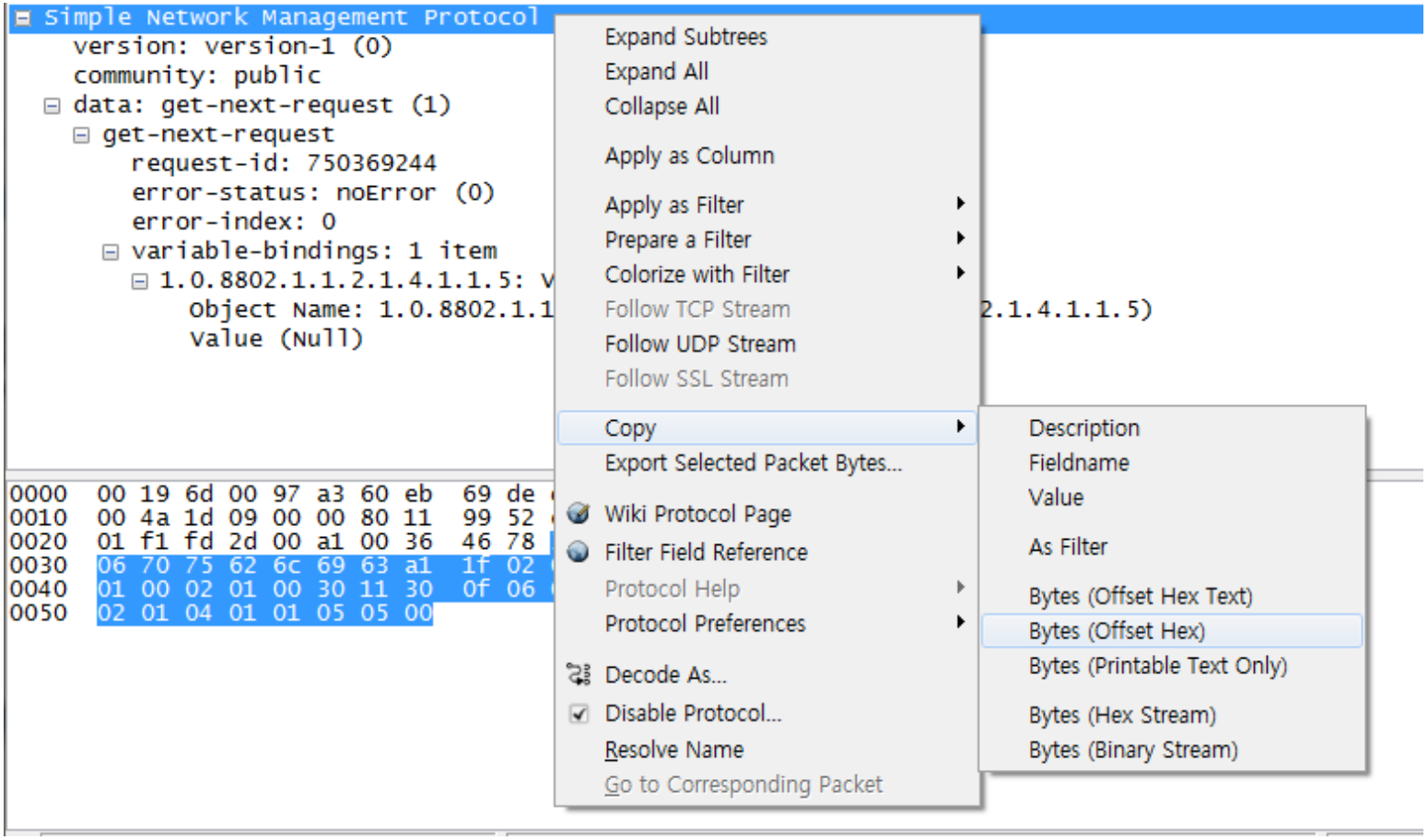


Demo: Graphical Interpretation



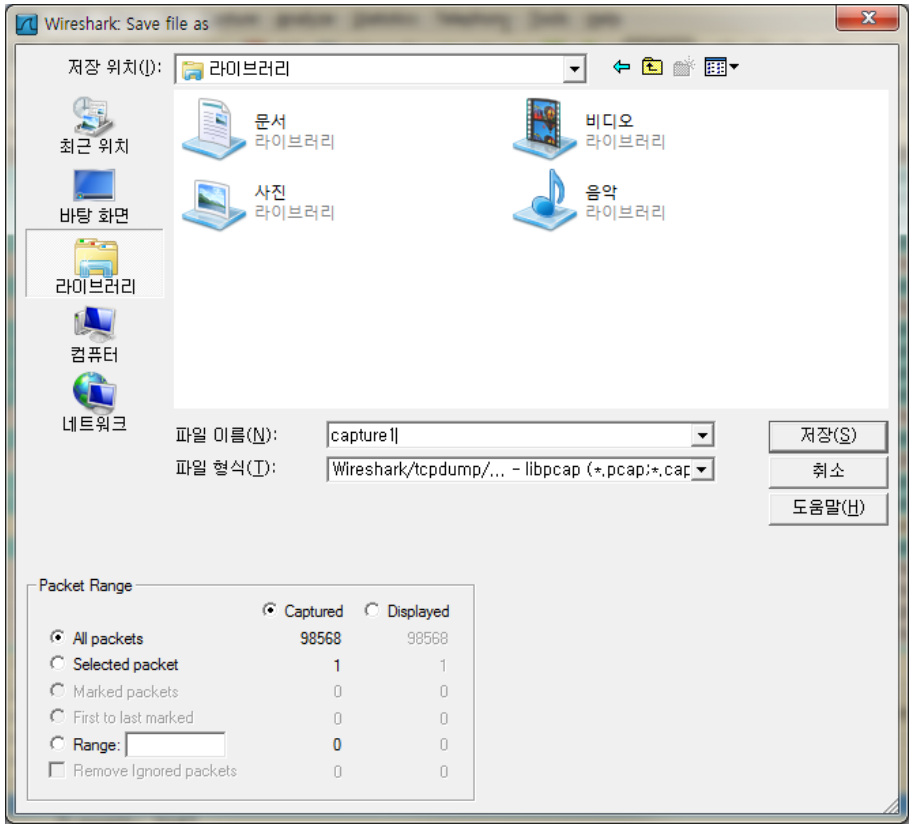
Demo: Dump Data

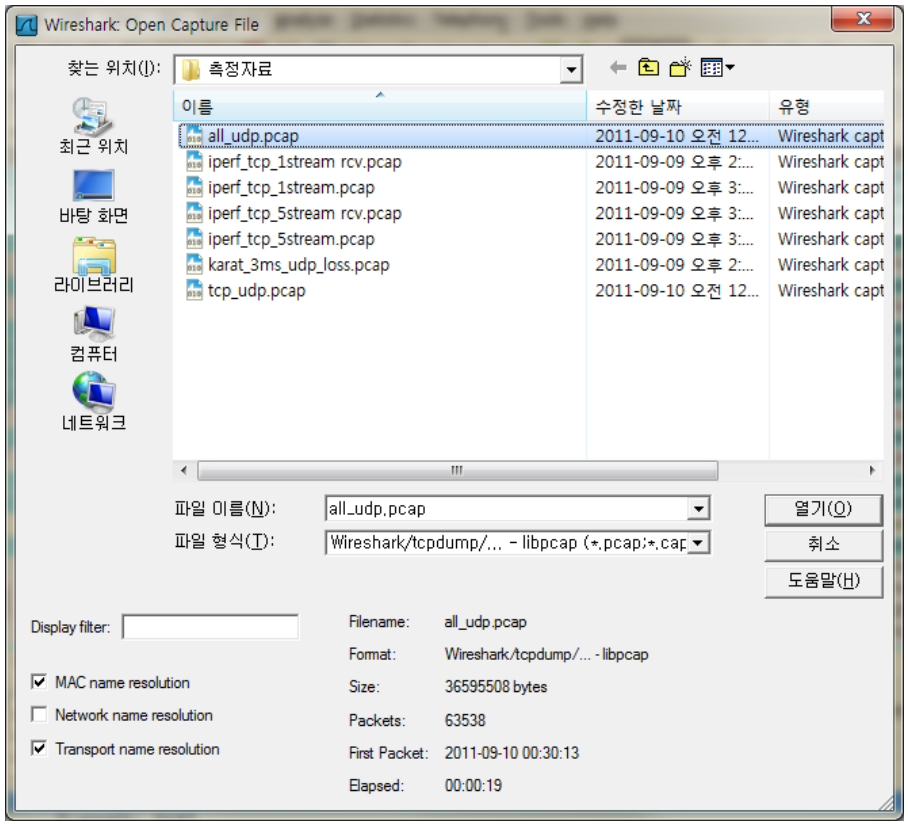
- **Copy & Paste raw data**



Demo: Save & Load

- File → Save as : save captured file
- File → Open *.pcap file





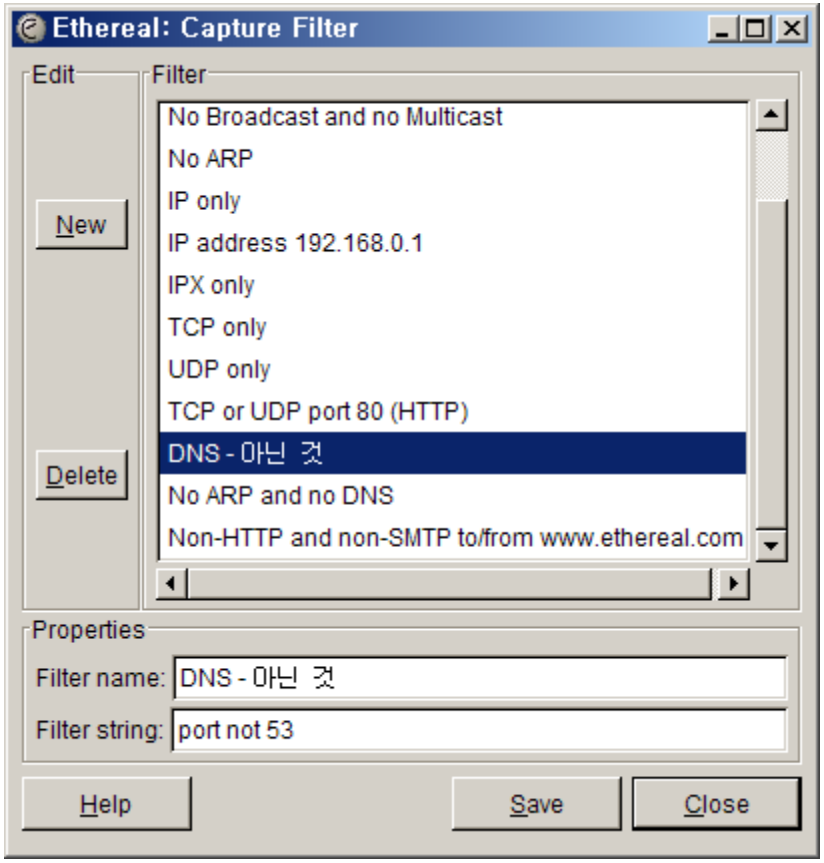
Capture filter (libpcap 방식)

- 모든 HTTP 패킷
  - tcp port 80
- Non-HTTP 패킷:
  - not tcp port 80 또는 !tcp port 80 또는 tcp port not 80
- www.inzen.com HTTP browsing
  - tcp port 80 || dst www.inzen.com
- www.inzen.com 아닌 HTTP browsing
  - tcp port 80 and not dst www.inzen.com
- TCP 패킷:
  - tcp 또는 ip proto 6
- TCP SYN 패킷
  - tcp[tcpflag] & tcp-syn == tcp-syn

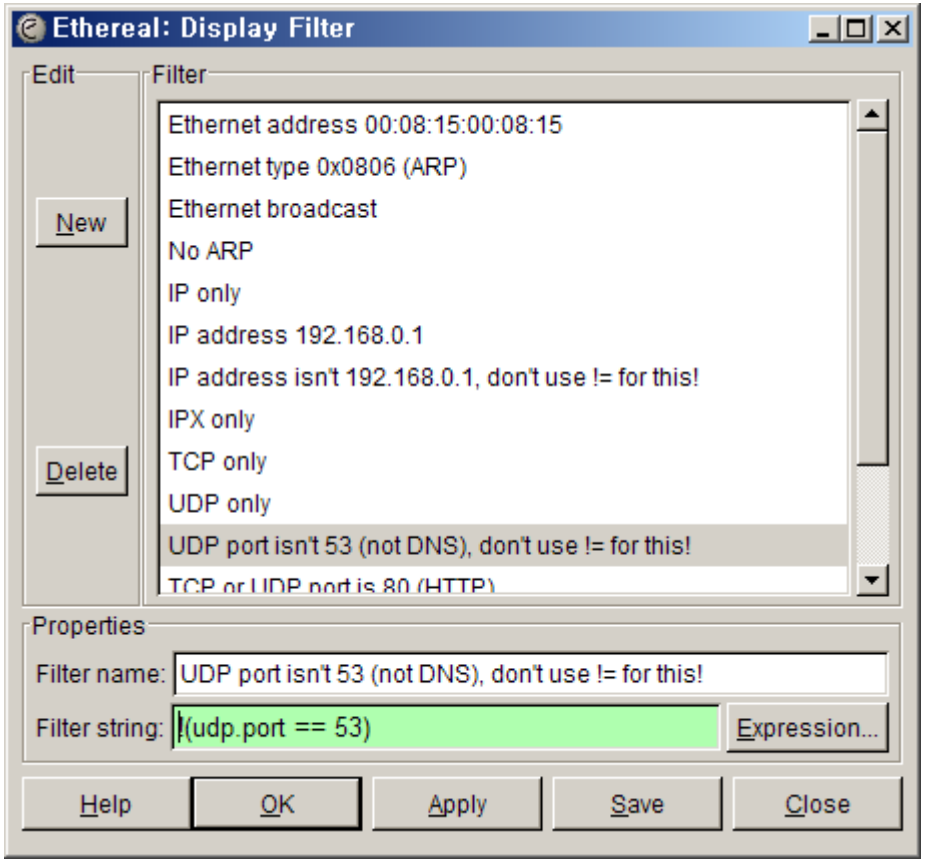
Capture filter (libpcap 방식)

- IP 패킷 with total length > 255
  - ip[2:2] > 0xff
- ICMP echo request and reply
  - icmp[icmptype] == icmp-echo or icmp[icmptype] == icmp-echoreply
- IP 또는 IPX 패킷
  - ip or ipx
- IPX 패킷
  - ipx
- IPX 패킷 destined for IPX network 00:01:F0:EE
  - ipx는 일부 주소만 지정 불가능

Capture/Display Filter – 주의 필요



Libpcap 입력 방식
다중 조건 경우 OR 확장



입력과 동시에 자동 문법 체크
다중 조건 경우 OR로 확장

캡처 및 캡처 필터
데모

Working with captured 패킷

- 패킷 보기
- Display Filter
- Finding 패킷
  - "Find Packet", "Find Next", "Find Previous"
- Go to a specific packet
  - "Go Back", "Go Forward", "Go to Packet", "Go to Corresponding Packet", "Go to First Packet", "Go to Last Packet"
- Marking 패킷 표시
- 시간 표시 형식 and 시간 참조
  - 패킷 시간 참조

실제 예제 (Display 필터)

- 스캐닝 – TCP 커넥션
  - tcp.flags.syn==1&&tcp.flags.ack==1 또는 tcp.flags==18
- 트로이잔 – SubSeven
  - tcp.port == 27374
- 트로이잔 – Netbus
  - tcp.port == 12345 || tcp.port == 12346
- 웹 – SQL Slammer
  - udp.port==1434 and ip.len < 384
- Nmap 스캐닝 확인
  - nmap -sS -O 10.3.100.231/24

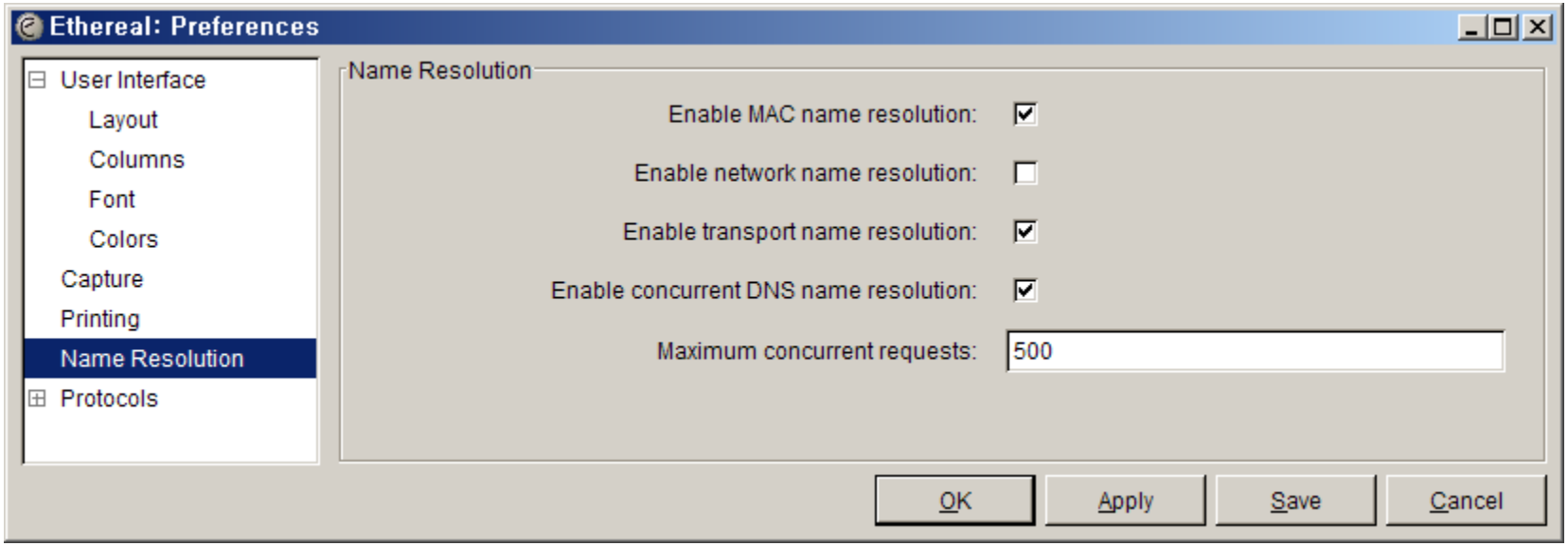
화면 필터
데모

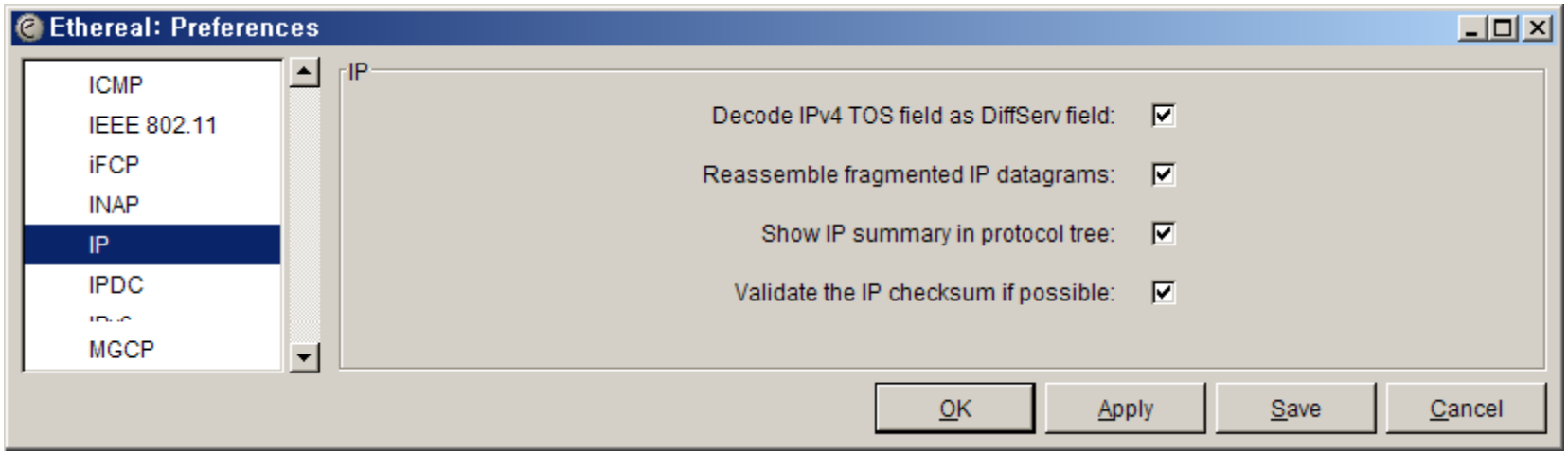
Advanced Features – 화면 표시 제어

- **Following TCP streams**
  - **특정 세션에 대한 프로토콜 흐름 분석**
- **Name Resolution**
  - **Ethernet name resolution (MAC)**
  - **IP name resolution (network)**
  - **TCP/UDP port name resolution (transport)**
  - **IPX name resolution (network)**
- **Packet Reassembling - enabled by default ?**

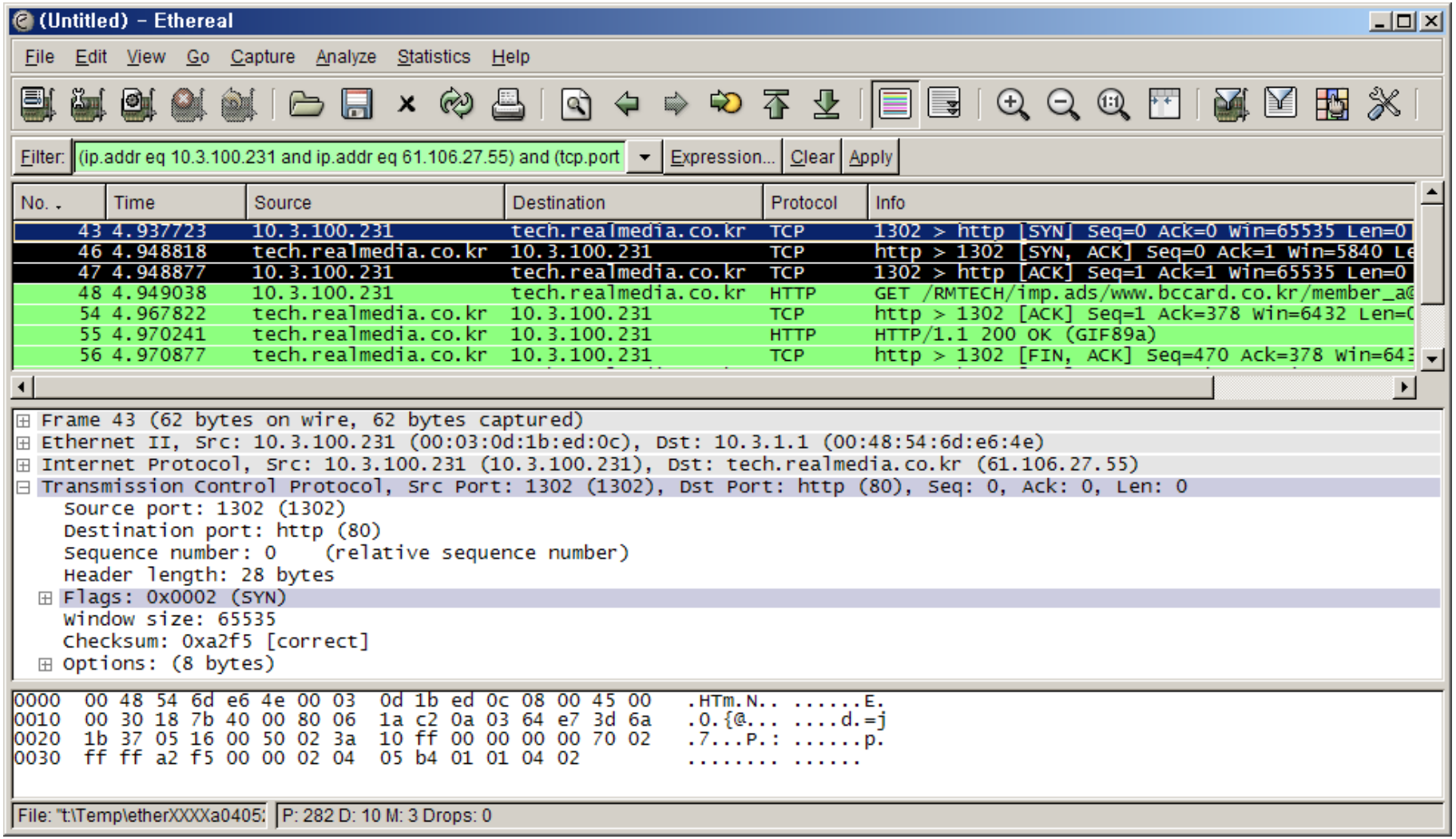
소스 epan/dissectors/

Name resolution, Fragment Reassembly

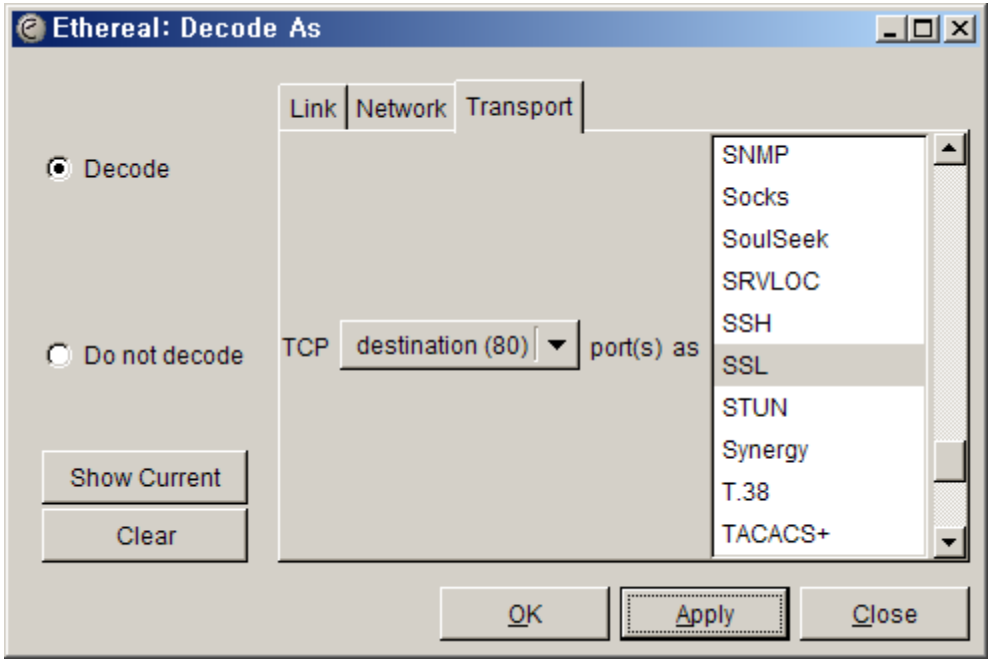


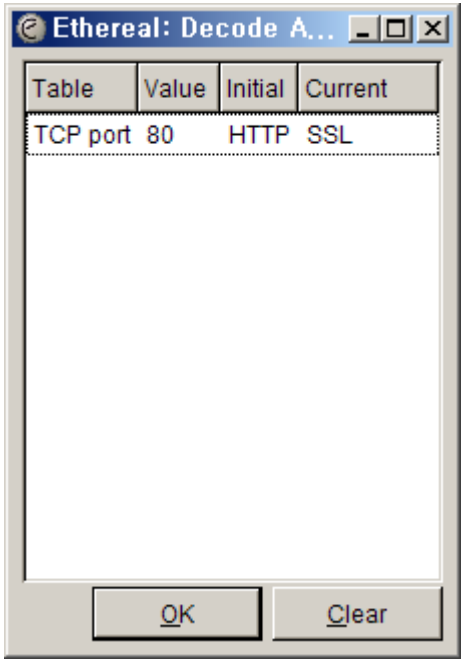


캡처 화면 – 필터, 이름 변환, 재조함



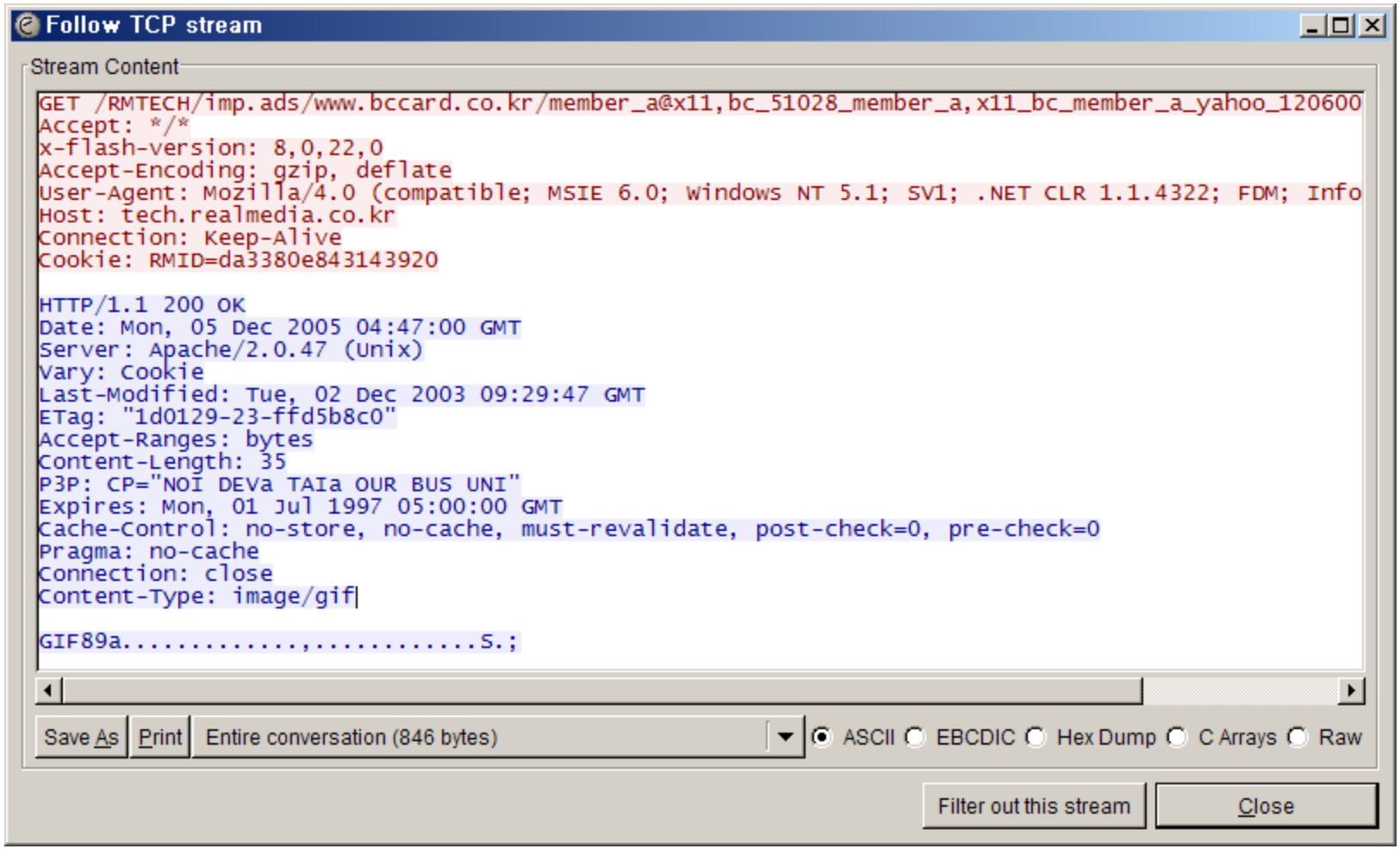
디코더 선택 (Dissector)





소스 epan/dissectors/

Follow stream



More Resources

- **Search “wireshark tutorial”**
- **http://wiki.wireshark.org**
- **http://wiki.wireshark.org/SampleCaptures**