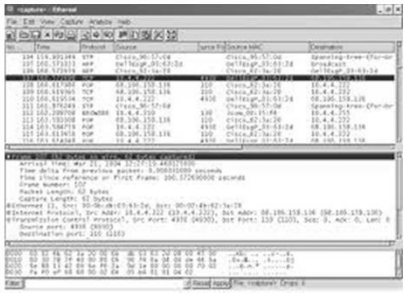
Tools

Foundations of computer networks

Analysers

- Network protocol analyser



- Traffic analyser

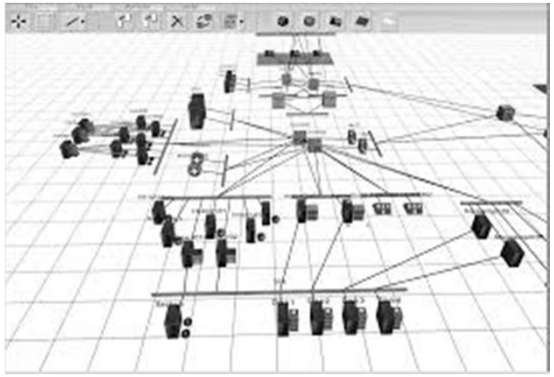
- Software
- Hardware

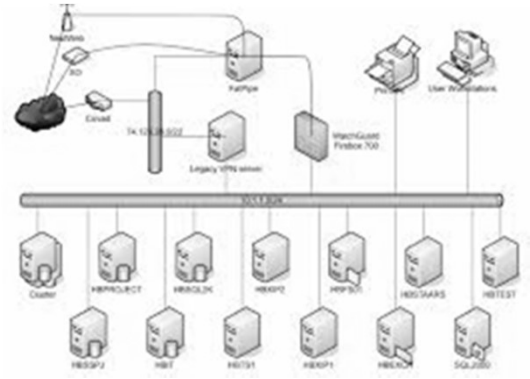
dedicated computer

980 Protocol Analyzer

Network diagramming software

- Lan MapShot
- Lab Network

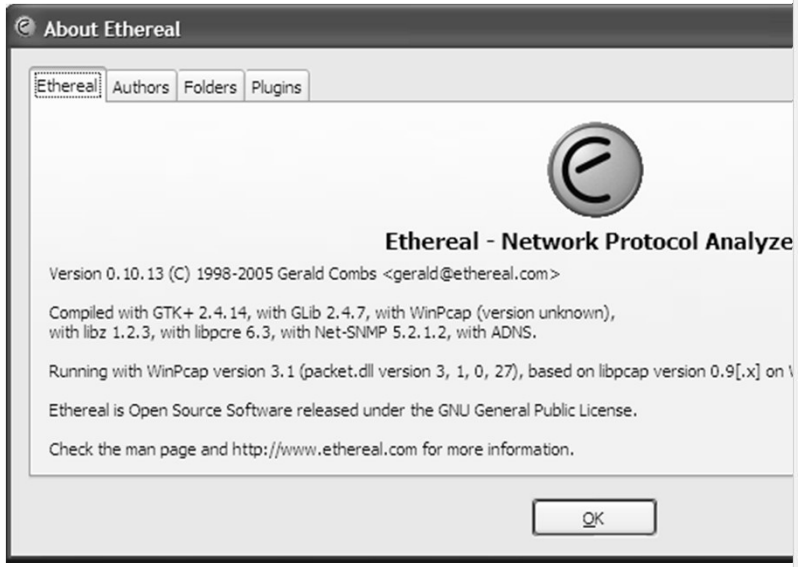


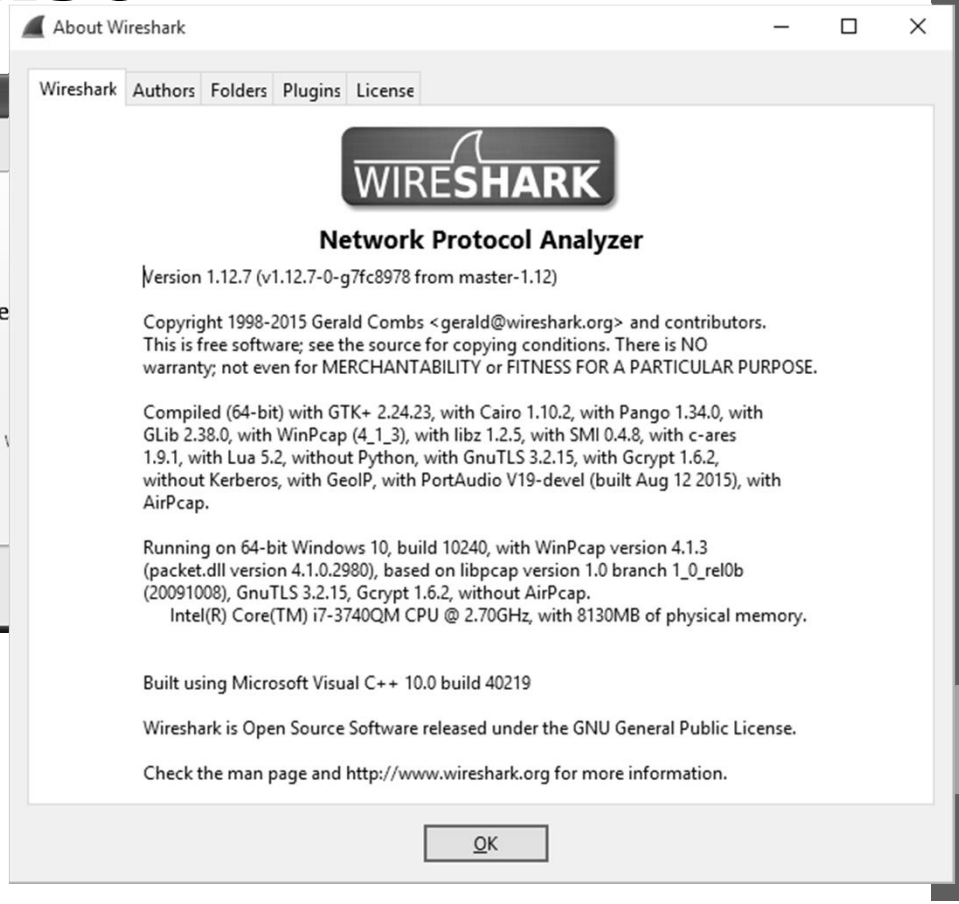


Ethereal - Wireshark

Foundations of computer networks

Software - license





www.wireshark.org

Systems

- Windows
- OS X
- Linux

Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
OS X 10.6 and later Intel 64-bit .dmg
OS X 10.6 and later Intel 32-bit .dmg

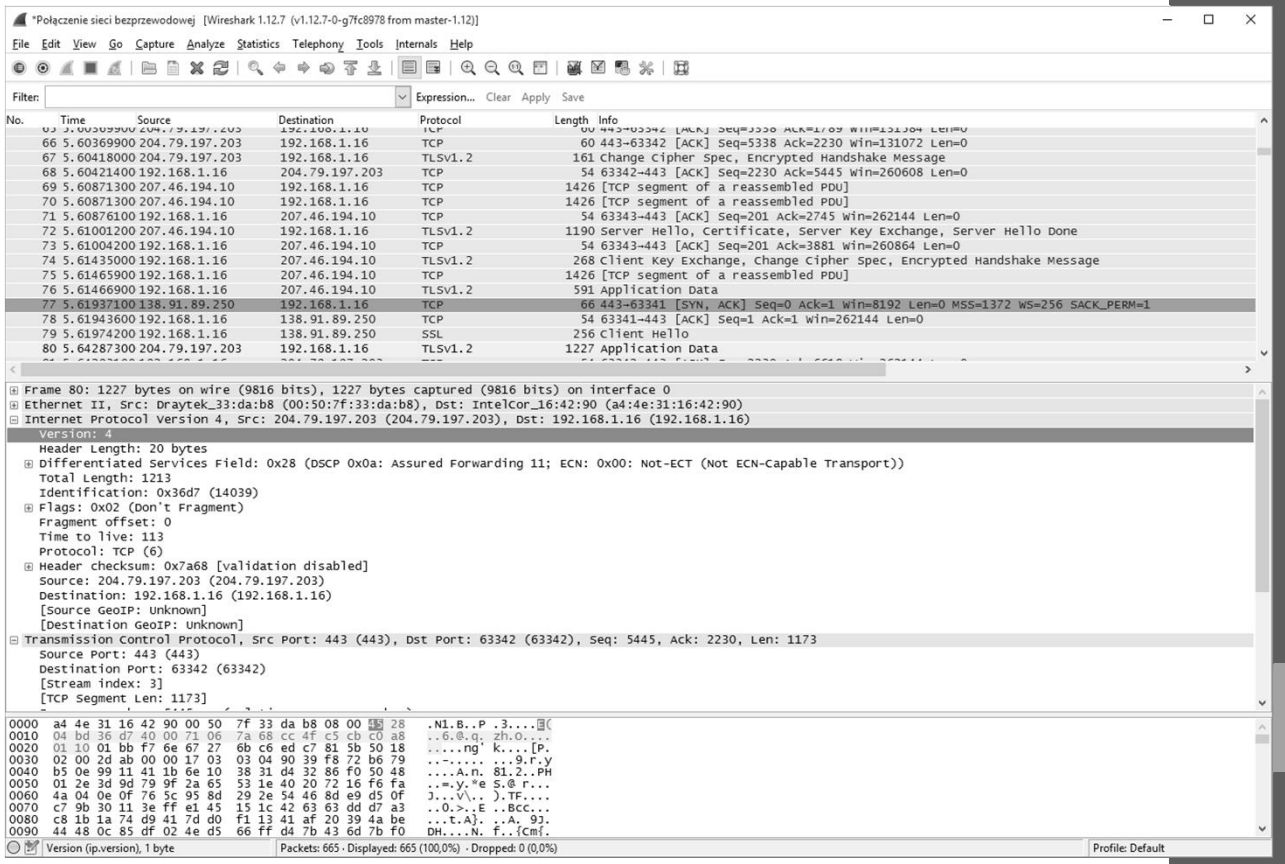
Source Code

Data flow

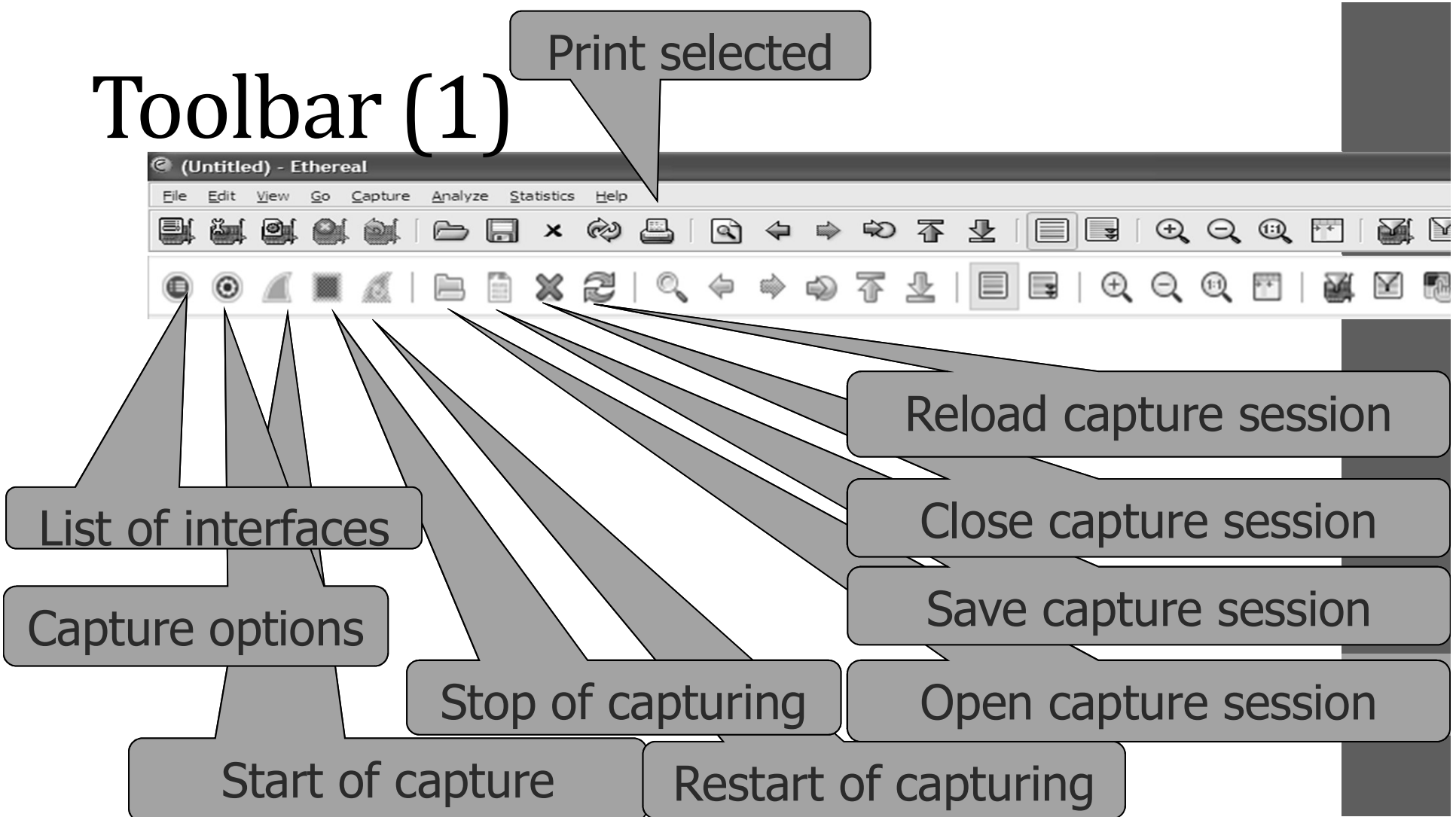
- Medium
- Interface
- Real time statistics
- Capture filter
- Time marking
- Buffer
- Display filter
- Decoding and analysing
- Save/print filter
- Saving/printing

Main window

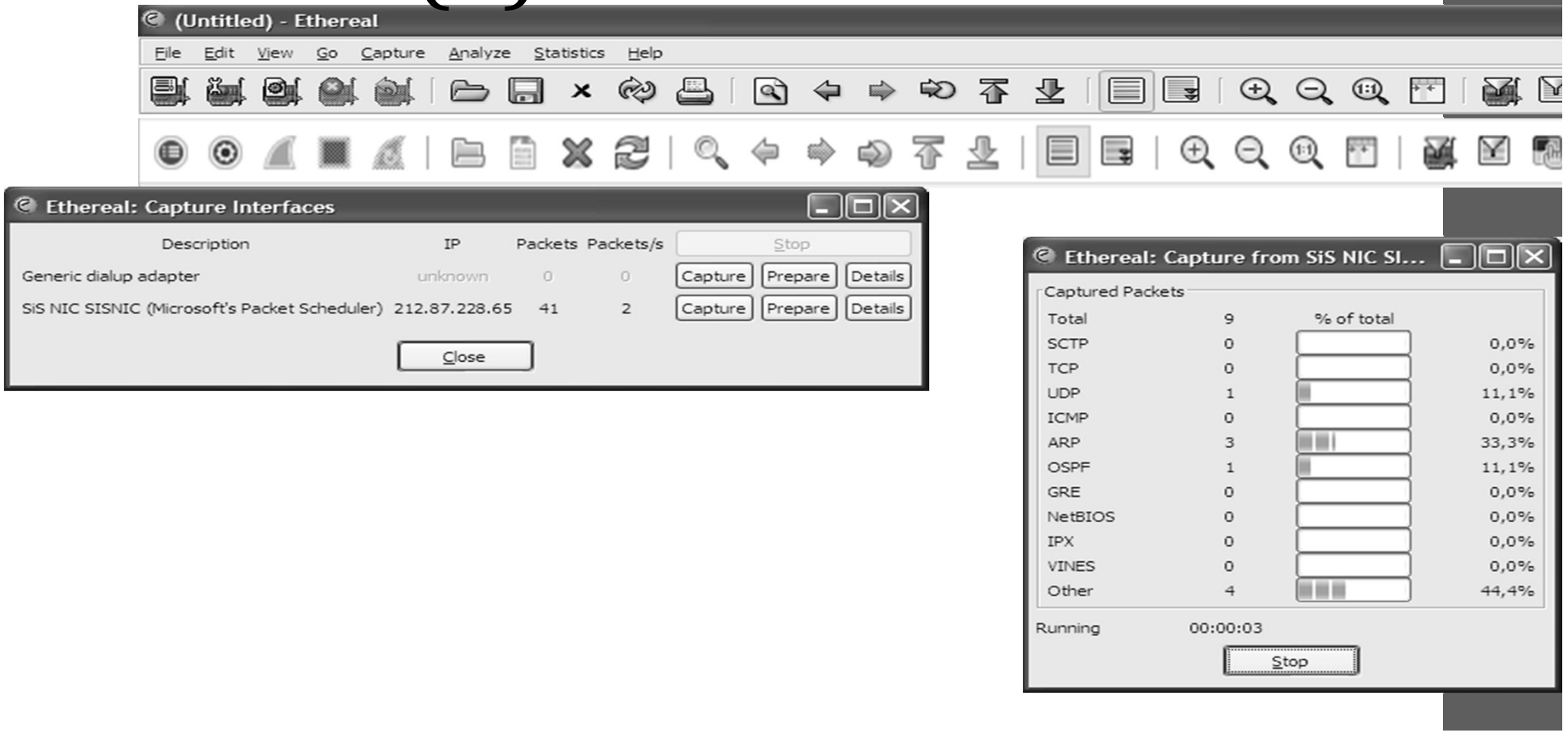
- menu,
- toolbar,
- display filter bar,
- packet list,
- packet details,
- packet bytes (hex and ASCII),
- status bar



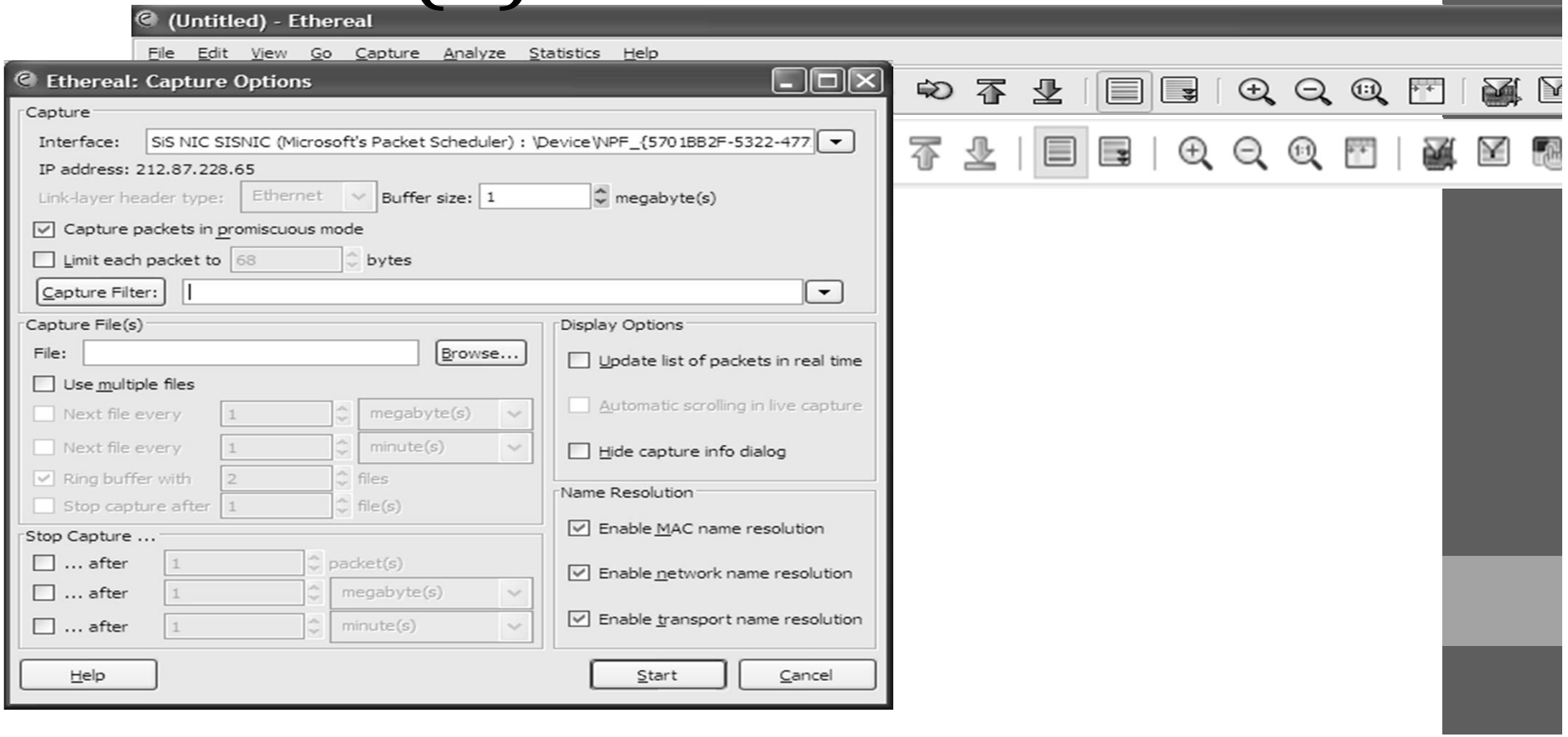
Toolbar (1)


Print selected
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Reload capture session
List of interfaces
Close capture session
Capture options
Save capture session
Stop of capturing
Open capture session
Start of capture
Restart of capturing

Toolbar (1)

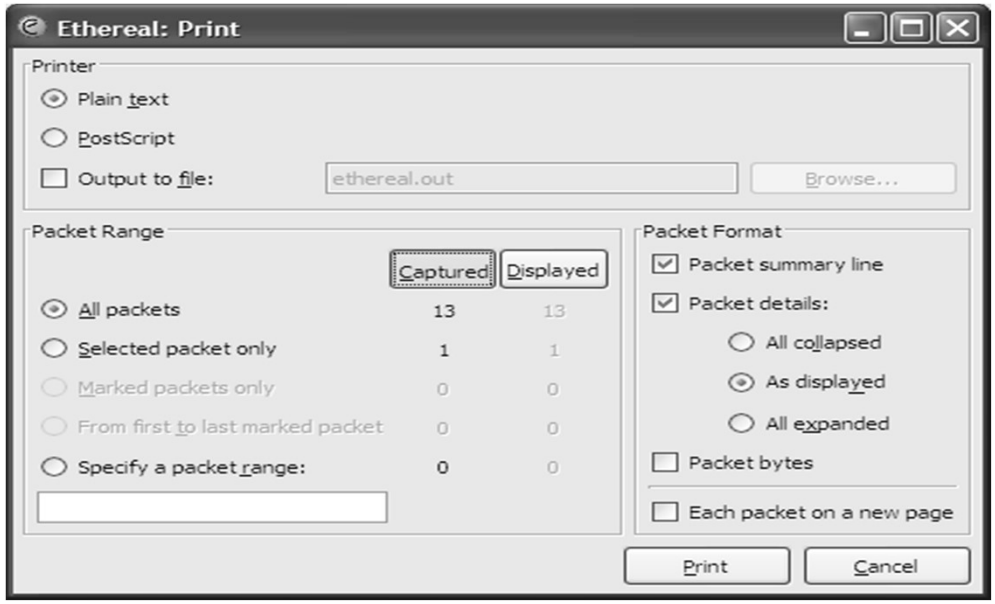

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Ethereal: Capture Interfaces
Description IP Packets Packets/s Stop
Generic dialup adapter unknown 0 0 Capture Prepare Details
SiS NIC SISNIC (Microsoft's Packet Scheduler) 212.87.228.65 41 2 Capture Prepare Details
Close
Ethereal: Capture from SiS NIC SI...
Captured Packets
Total 9 % of total
SCTP 0 0,0%
TCP 0 0,0%
UDP 1 11,1%
ICMP 0 0,0%
ARP 3 33,3%
OSPF 1 11,1%
GRE 0 0,0%
NetBIOS 0 0,0%
IPX 0 0,0%
VINES 0 0,0%
Other 4 44,4%
Running 00:00:03
Stop

Toolbar (1)

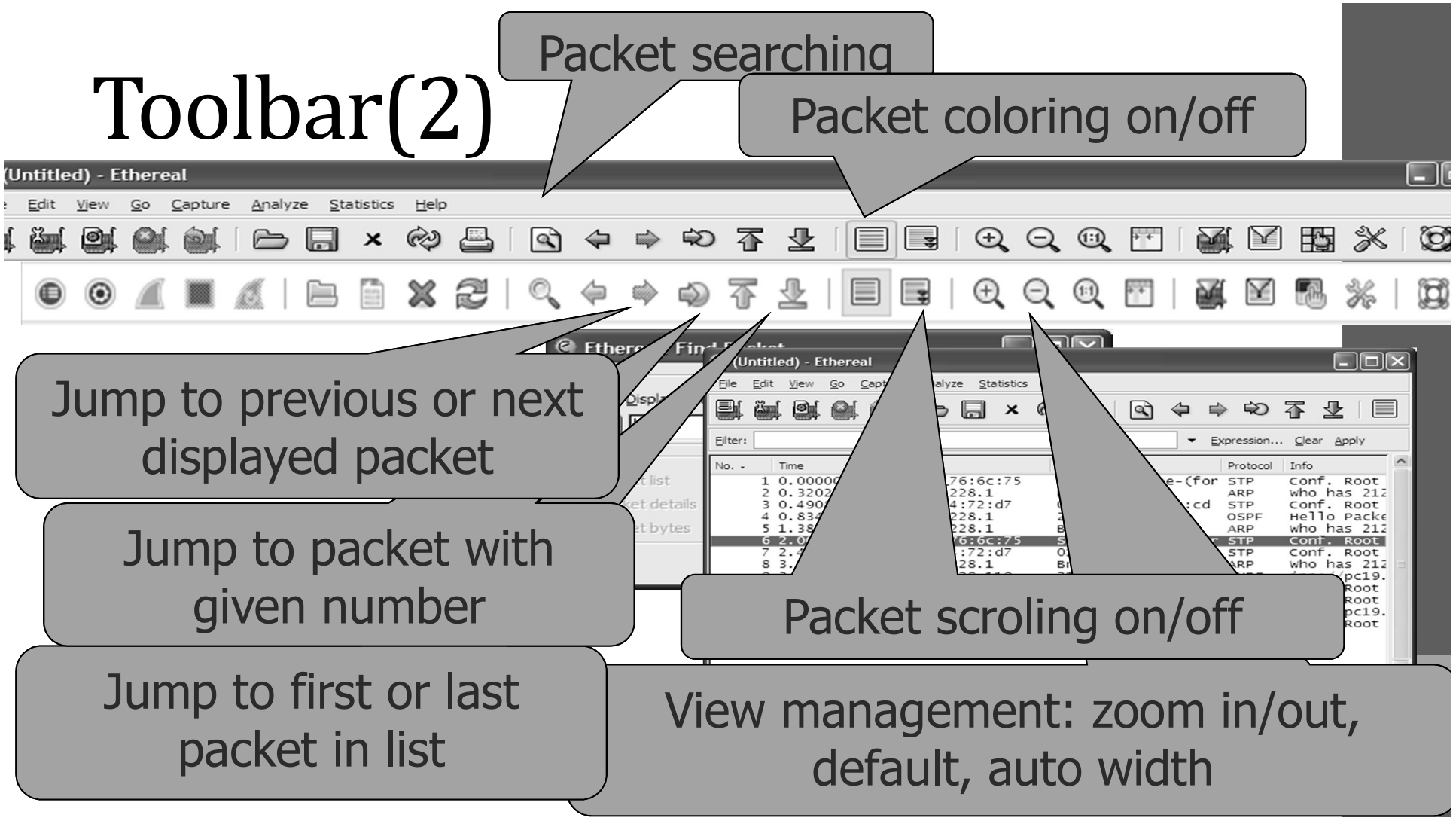

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Ethereal: Capture Options
Capture
Interface: SiS NIC SISNIC (Microsoft's Packet Scheduler) : \Device\NPF_{5701BB2F-5322-477
IP address: 212.87.228.65
Link-layer header type: Ethernet
Buffer size: 1 megabyte(s)
Capture packets in promiscuous mode
Limit each packet to 68 bytes
Capture Filter:
Capture File(s)
File:
Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Help
Start
Cancel

Toolbar (1)

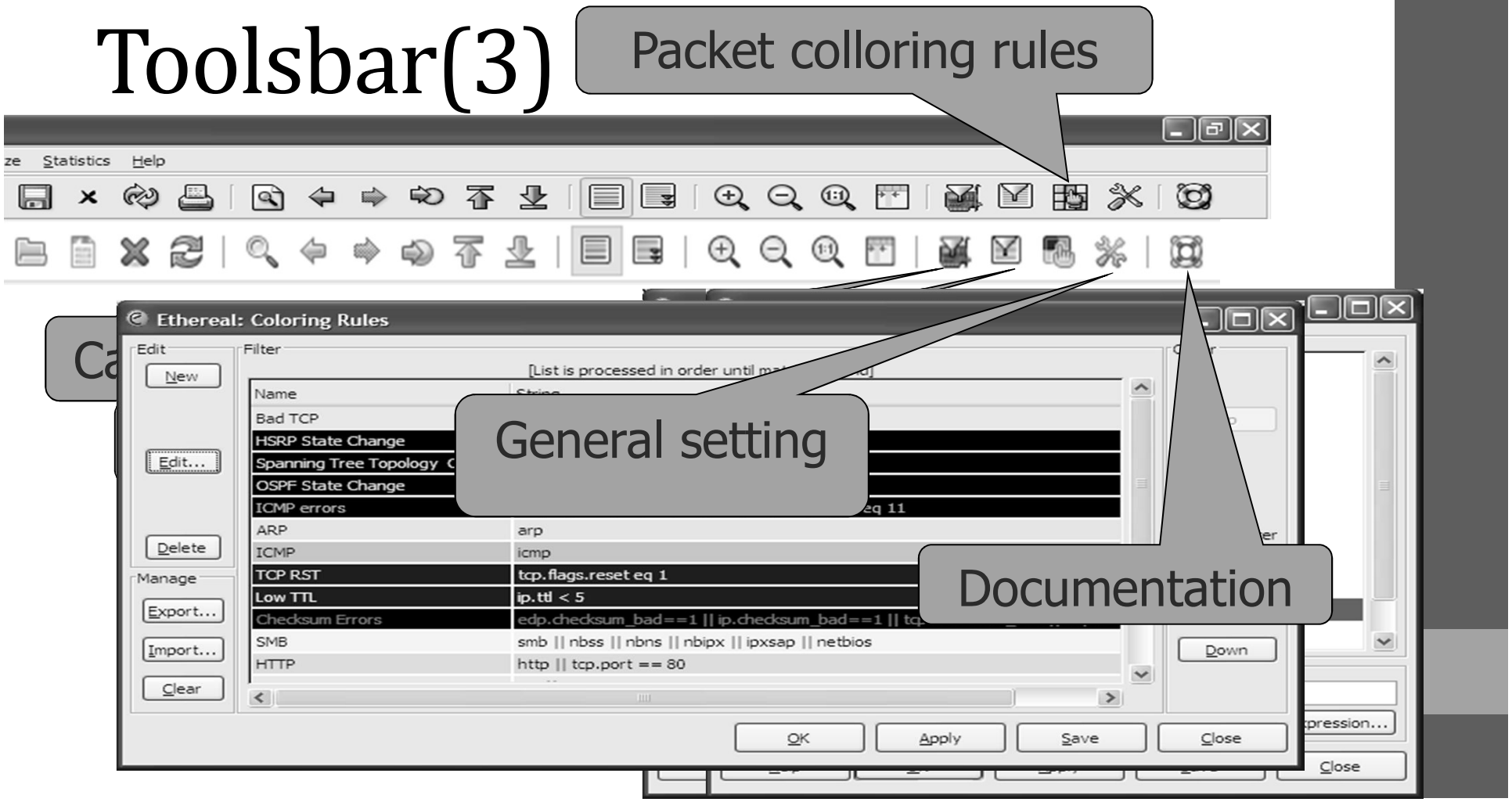

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help


Ethereal: Print
Printer
Plain text
PostScript
Output to file:
ethereal.out
Browse...
Packet Range
Captured
Displayed
All packets 13 13
Selected packet only 1 1
Marked packets only 0 0
From first to last marked packet 0 0
Specify a packet range: 0 0
Packet Format
Packet summary line
Packet details:
All collapsed
As displayed
All expanded
Packet bytes
Each packet on a new page
Print
Cancel

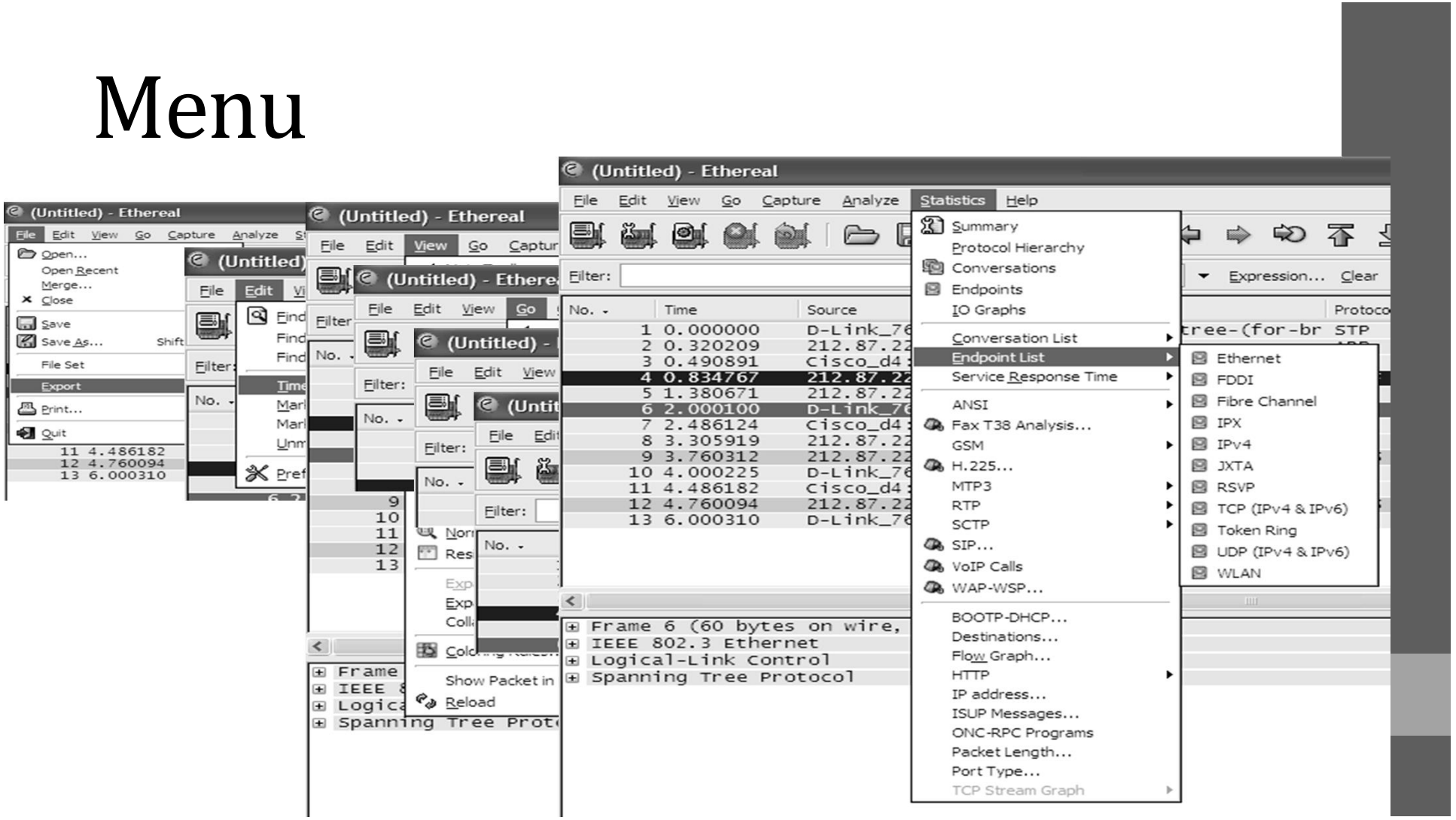
Toolbar(2)

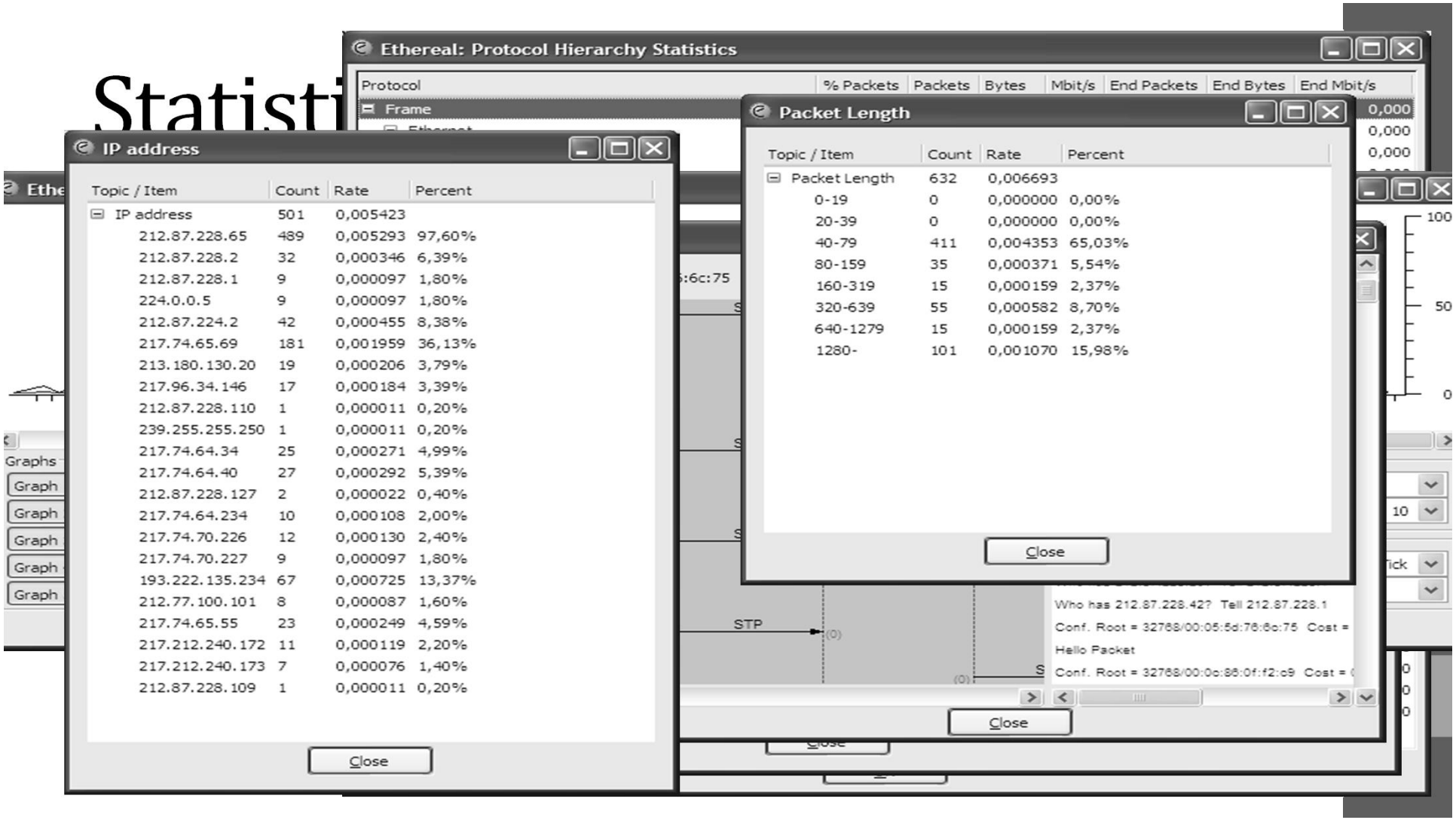

Packet searching
Packet coloring on/off
(Untitled) - Ethereal
Edit View Go Capture Analyze Statistics Help
Jump to previous or next displayed packet
Jump to packet with given number
Jump to first or last packet in list
Packet scroling on/off
View management: zoom in/out, default, auto width

Toolsbar(3)

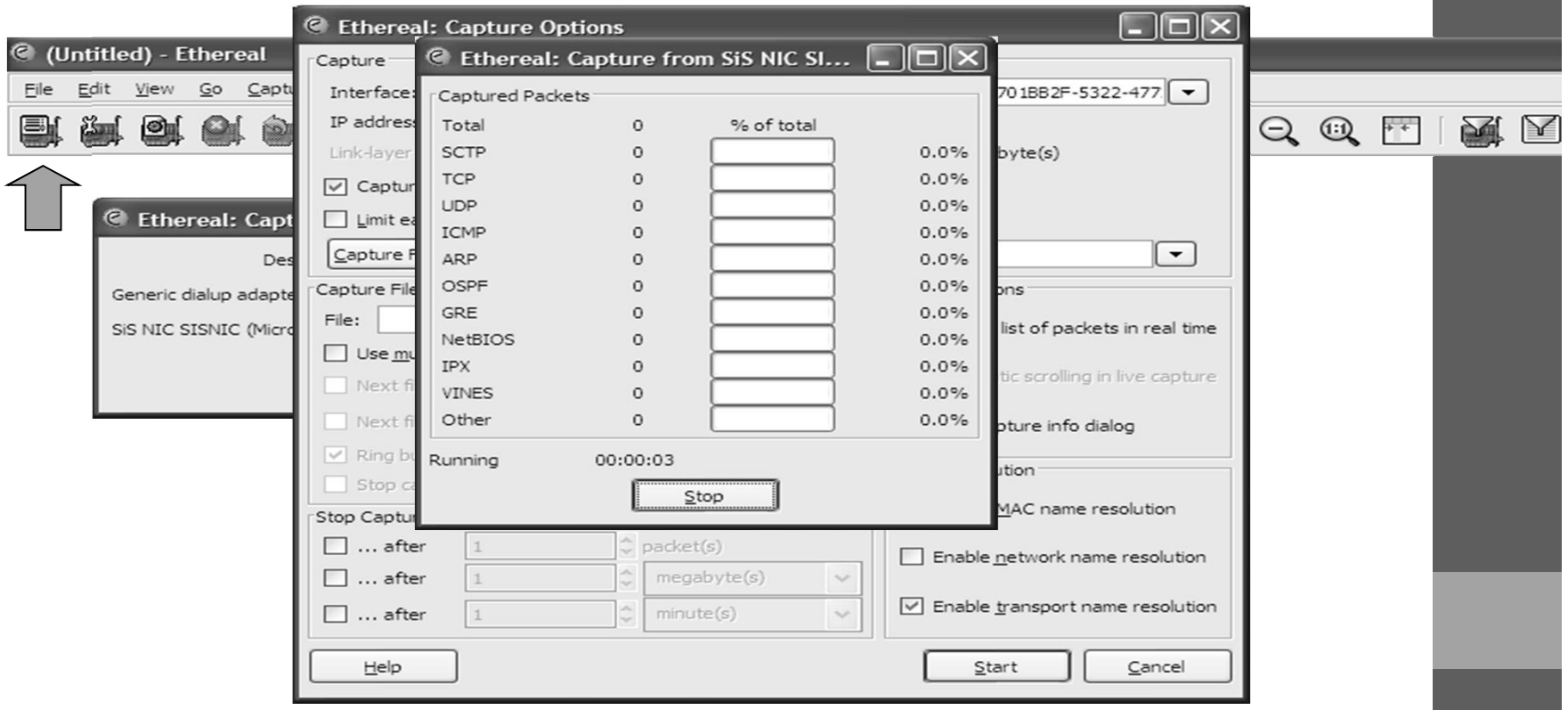

Packet colloring rules
General setting
Documentation
Ethereal: Coloring Rules
Edit
New
Edit...
Delete
Manage
Export...
Import...
Clear
Filter
Name
Bad TCP
HSRP State Change
Spanning Tree Topology
OSPF State Change
ICMP errors
ARP
arp
ICMP
icmp
TCP RST
tcp.flags.reset eq 1
Low TTL
ip.ttl < 5
Checksum Errors
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80
Down
OK
Apply
Save
Close
Statistics
Help

Menu


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Summary
Protocol Hierarchy
Conversations
Endpoints
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANSI
Fax T38 Analysis...
GSM
H.225...
MTP3
RTP
SCTP
SIP...
VoIP Calls
WAP-WSP...
BOOTP-DHCP...
Destinations...
Flow Graph...
HTTP
IP address...
ISUP Messages...
ONC-RPC Programs
Packet Length...
Port Type...
TCP Stream Graph
Ethernet
FDDI
Fibre Channel
IPX
IPv4
JXTA
RSVP
TCP (IPv4 & IPv6)
Token Ring
UDP (IPv4 & IPv6)
WLAN
Filter:
Expression... Clear
No. Time Source
Frame 6 (60 bytes on wire,
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol


Statisti
Ethereal: Protocol Hierarchy Statistics
Protocol
% Packets
Packets
Bytes
Mbit/s
End Packets
End Bytes
End Mbit/s
Frame
0,000
0,000
0,000
IP address
Topic / Item
Count
Rate
Percent
IP address 501 0,005423
212.87.228.65 489 0,005293 97,60%
212.87.228.2 32 0,000346 6,39%
212.87.228.1 9 0,000097 1,80%
224.0.0.5 9 0,000097 1,80%
212.87.224.2 42 0,000455 8,38%
217.74.65.69 181 0,001959 36,13%
213.180.130.20 19 0,000206 3,79%
217.96.34.146 17 0,000184 3,39%
212.87.228.110 1 0,000011 0,20%
239.255.255.250 1 0,000011 0,20%
217.74.64.34 25 0,000271 4,99%
217.74.64.40 27 0,000292 5,39%
212.87.228.127 2 0,000022 0,40%
217.74.64.234 10 0,000108 2,00%
217.74.70.226 12 0,000130 2,40%
217.74.70.227 9 0,000097 1,80%
193.222.135.234 67 0,000725 13,37%
212.77.100.101 8 0,000087 1,60%
217.74.65.55 23 0,000249 4,59%
217.212.240.172 11 0,000119 2,20%
217.212.240.173 7 0,000076 1,40%
212.87.228.109 1 0,000011 0,20%
Close
Packet Length
Topic / Item
Count
Rate
Percent
Packet Length 632 0,006693
0-19 0 0,000000 0,00%
20-39 0 0,000000 0,00%
40-79 411 0,004353 65,03%
80-159 35 0,000371 5,54%
160-319 15 0,000159 2,37%
320-639 55 0,000582 8,70%
640-1279 15 0,000159 2,37%
1280- 101 0,001070 15,98%
Close
Graphs
Graph
Graph
Graph
Graph
Graph
STP
Who has 212.87.228.42? Tell 212.87.228.1
Conf. Root = 32768/00:05:5d:76:6c:75 Cost =
Hello Packet
Conf. Root = 32768/00:0c:86:0f:f2:c9 Cost =
Close
100
50
0
10

Capturing


(Untitled) - Ethereal
File Edit View Go Capt
Ethereal: Capt
Generic dialup adapte
SiS NIC SISNIC (Micro
Ethereal: Capture Options
Capture
Interfaces
IP address
Link-layer
Capture
Limit ea
Capture F
Capture File
File:
Use mu
Next fi
Next fi
Ring bu
Stop ca
Stop Capture
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Help
Ethereal: Capture from SiS NIC SI...
Captured Packets
Total 0 % of total
SCTP 0 0.0%
TCP 0 0.0%
UDP 0 0.0%
ICMP 0 0.0%
ARP 0 0.0%
OSPF 0 0.0%
GRE 0 0.0%
NetBIOS 0 0.0%
IPX 0 0.0%
VINES 0 0.0%
Other 0 0.0%
Running 00:00:03
Stop
701BB2F-5322-477
byte(s)
list of packets in real time
tic scrolling in live capture
pture info dialog
MAC name resolution
Enable network name resolution
Enable transport name resolution
Start
Cancel

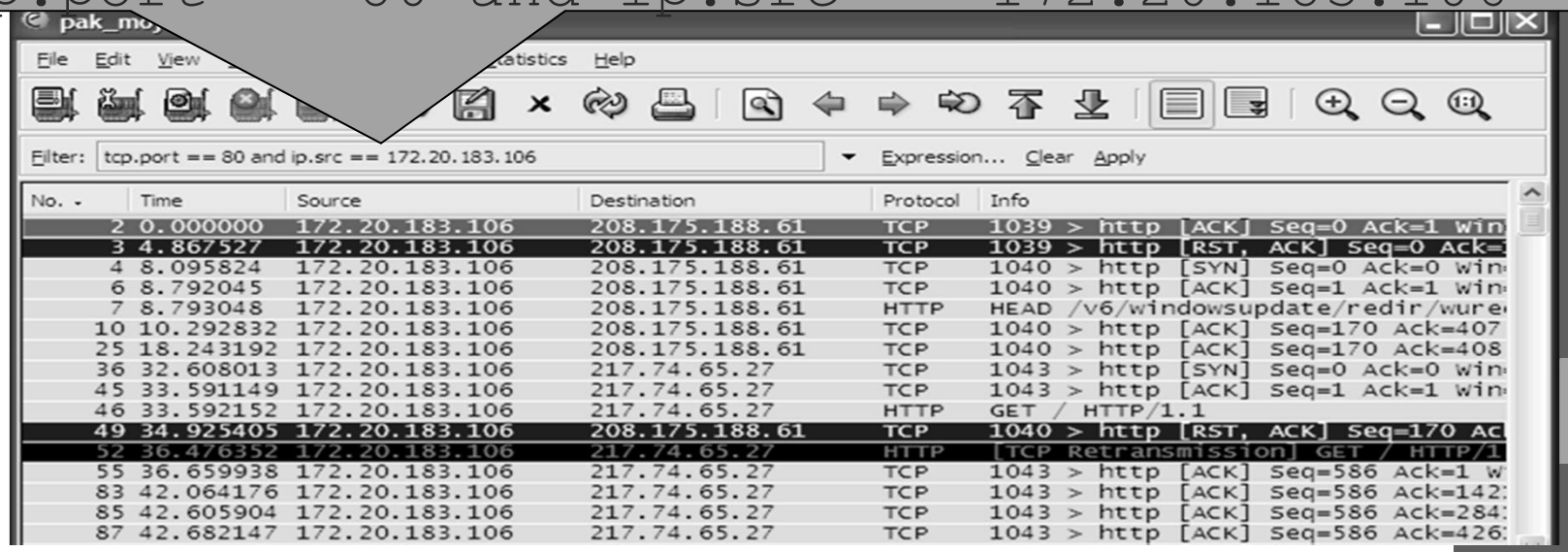
Filters – relations

- eq, == equal
- ne, != not equal
- gt, > greater than
- lt, < lower than
- ge, >= greater or equal
- le, <= lower or equal

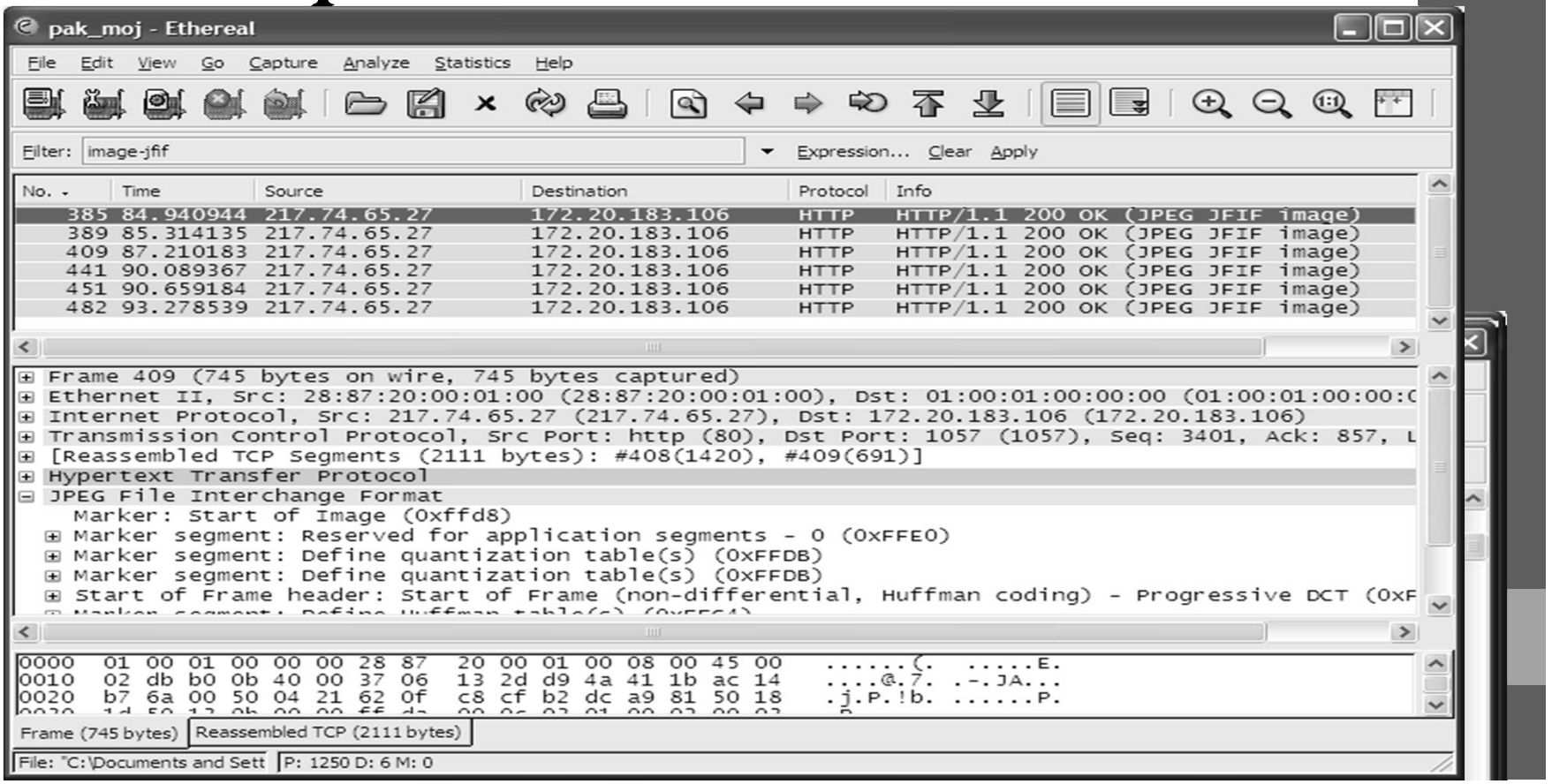
Filters – logical

- and, && logical AND
- or, || logical OR

```
tcp.port == 80 and ip.src == 172.20.183.106
```



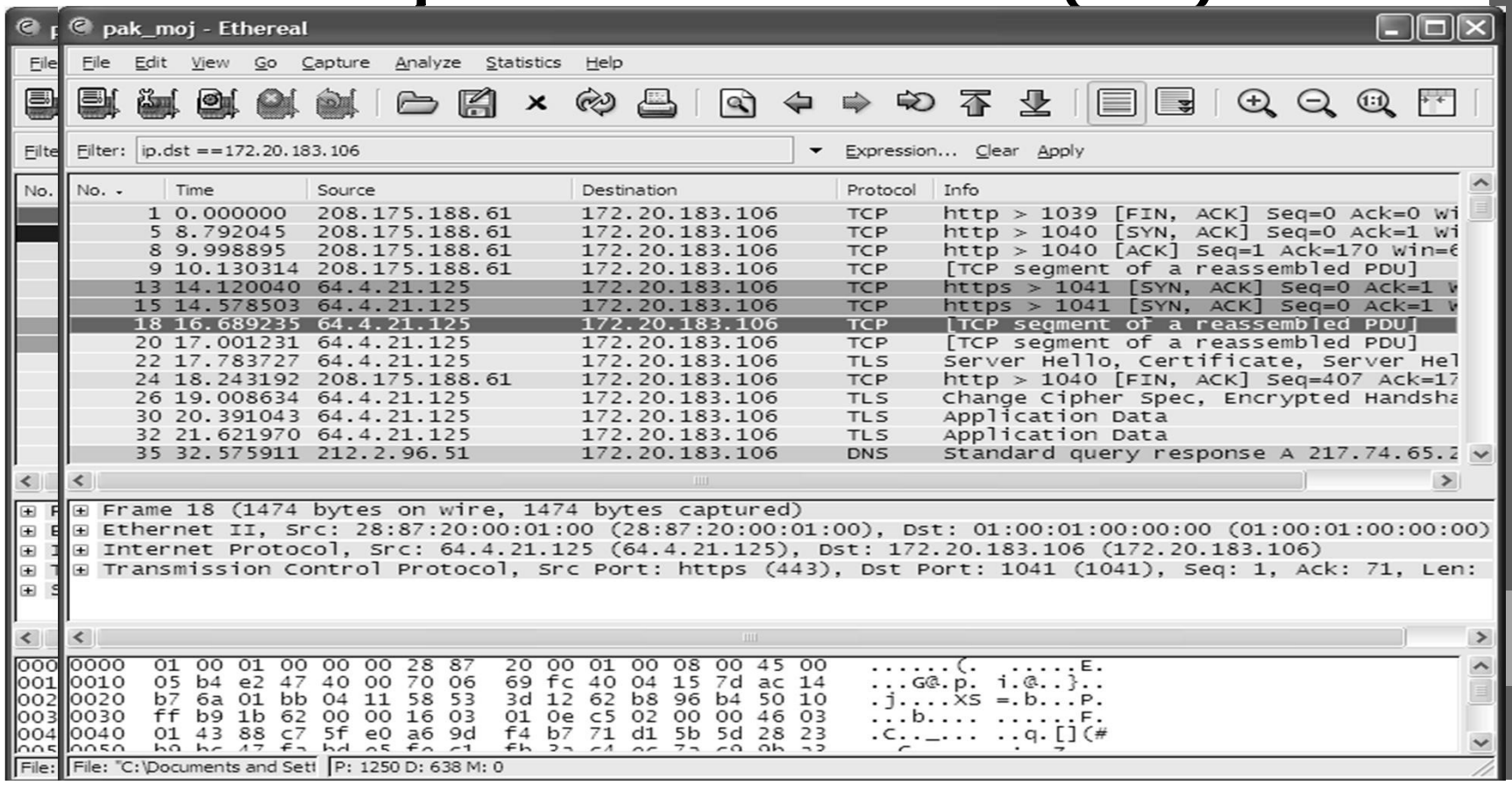
Filters - protocols

- 

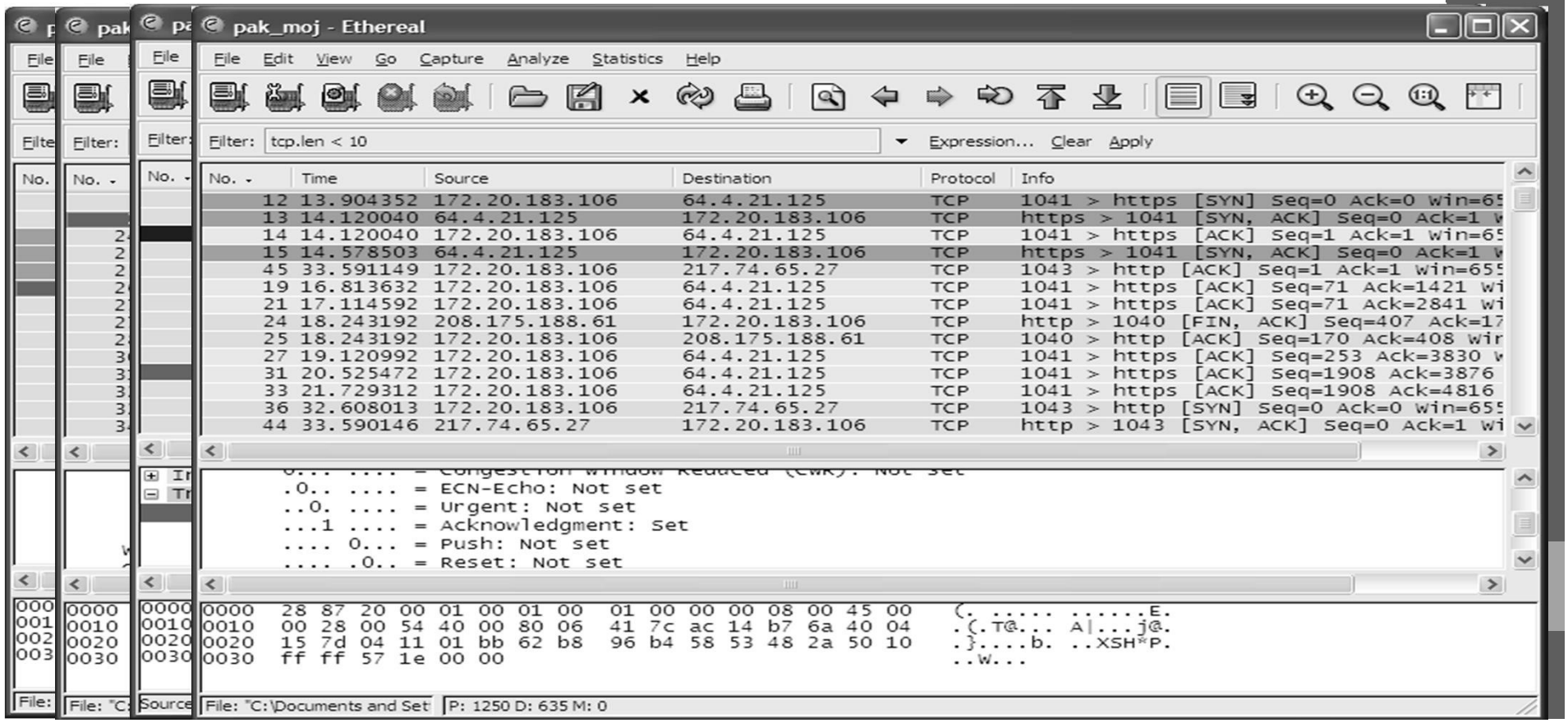
Filters – protocol fields (eth)

- eth
  - eth.addr ==
  - eth.dst ==
  - eth.len ==
  - eth.src ==
  - eth.trailer ==
  - eth.type ==

Filters – protocol fields (IP)



Filters – protocol fields (TCP)



Filters – protocol fields (UDP)

- udp
  - udp.checksum
  - udp.checksum_bad Bad
  - udp.dstport
  - udp.length
  - udp.port
  - udp.srcport

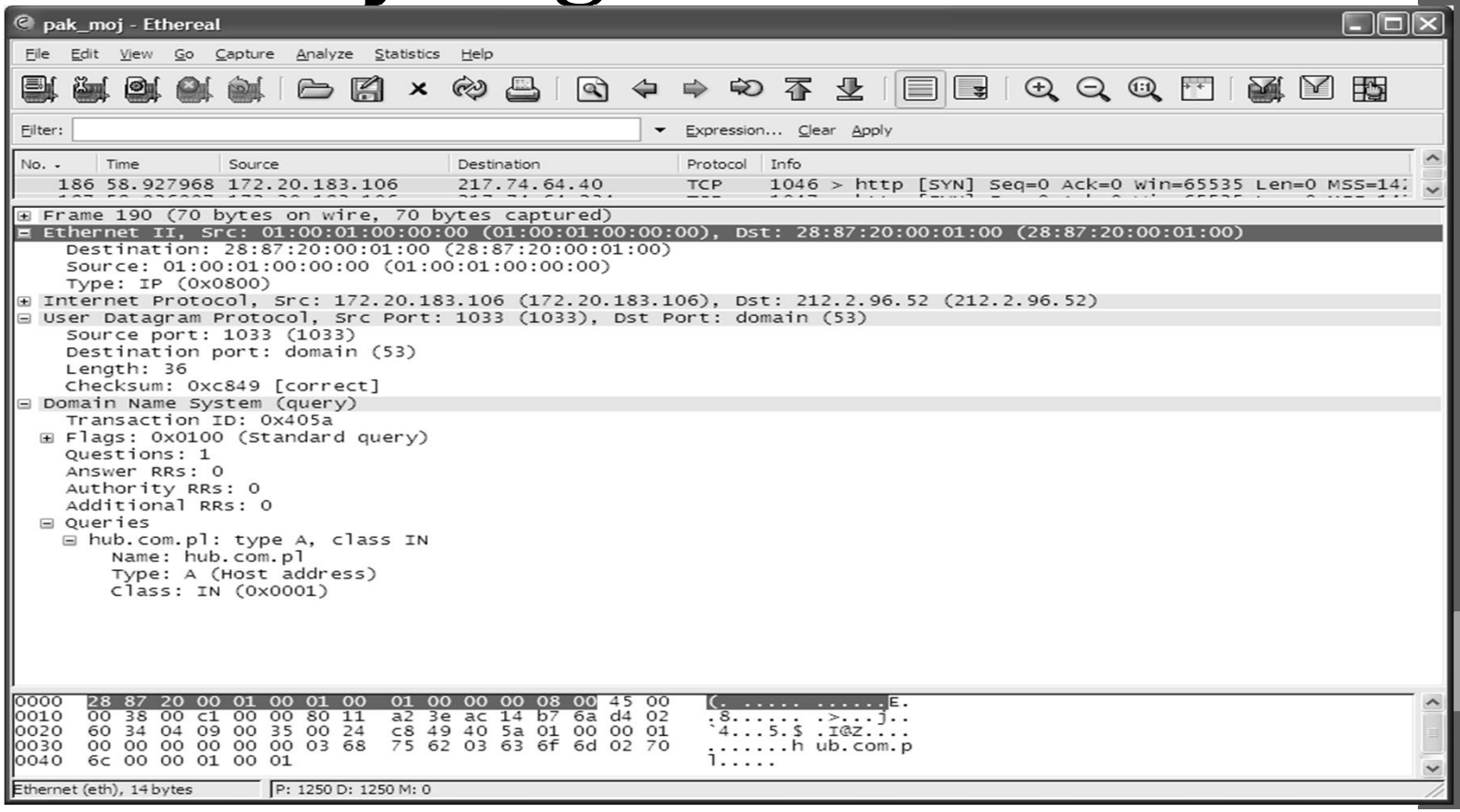
Filters – protocols fields (HTTP)

- http
  - http.cookie ==
  - http.host ==

Filters – protocols fields (echo)

- echo
  - echo.data ==
  - echo.request
  - echo.response

Paket analysing



Bibliography

- http://www.ethereal.com
- http://www.wireshark.org
- Richard Sharpe, Ed Warnicke, Ulf Lamping, *Ethereal User's Guide V2.0.2 (16586) for Ethereal 0.10.12*,