UIC UNIVERSITY OF ILLINOIS AT CHICAGO Department of Computer Science
COLLEGE OF ENGINEERING

CS450 – Introduction to Networking
Lecture 15 – Wireshark & Assignment 3

Phu Phung

Feb 16, 2015

Information

- Website:

  https://www.wireshark.org/

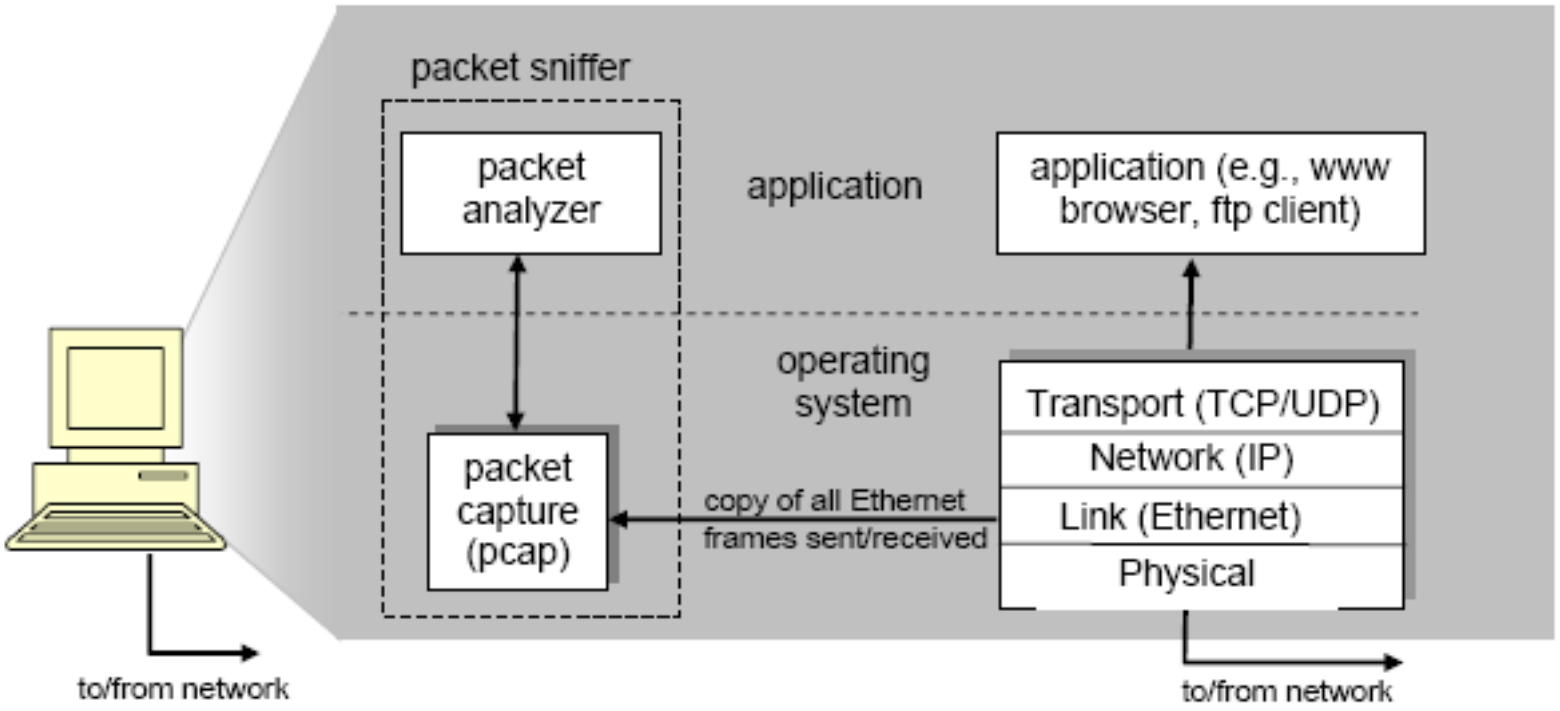
- Labs from Textbook

  http://www-net.cs.umass.edu/wireshark-labs/

What is Wireshark?

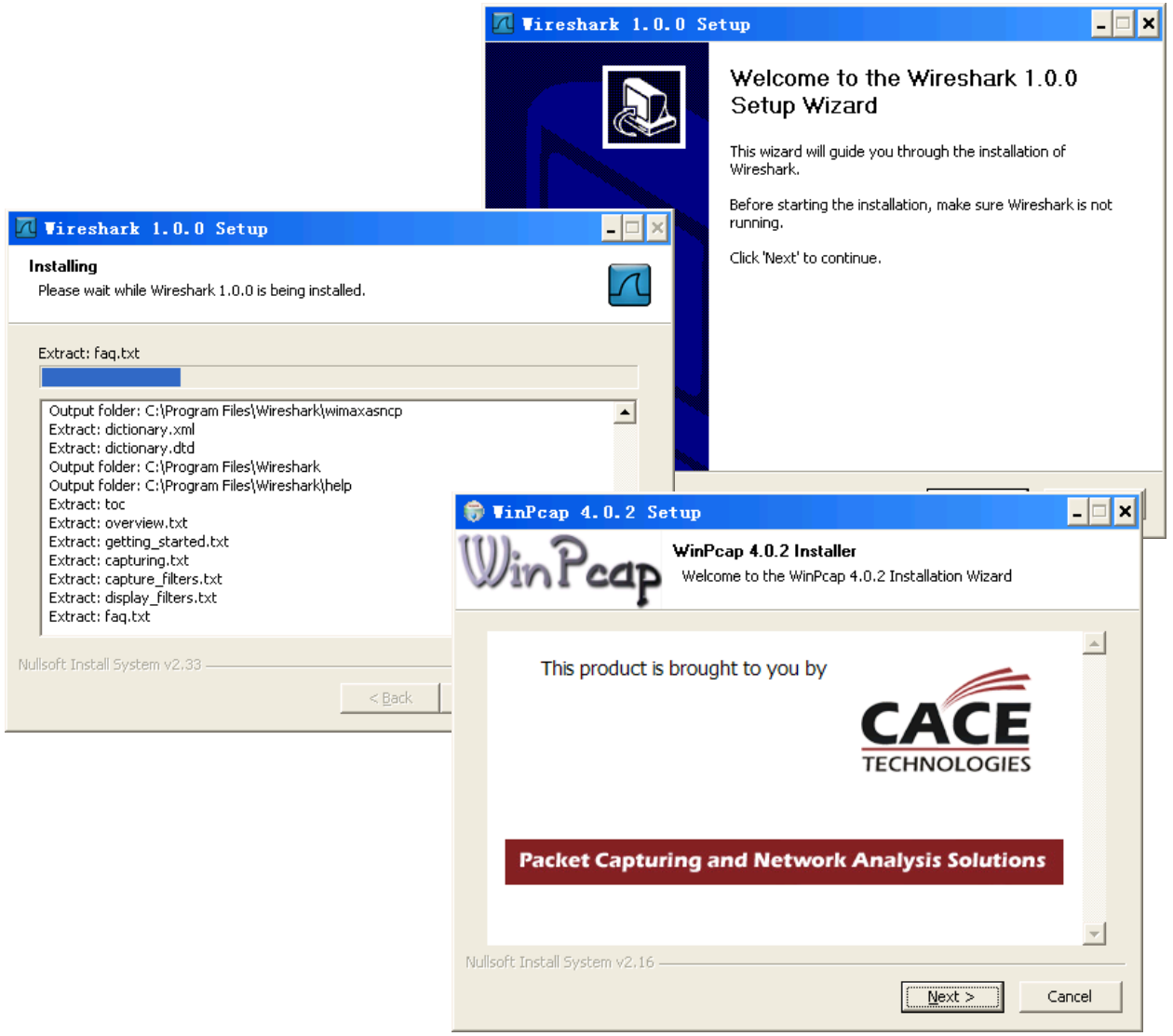
- Wireshark is a network packet/protocol analyzer.
  - A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- “The World's Most Popular Network Protocol Analyzer”

Wireshark System Overview



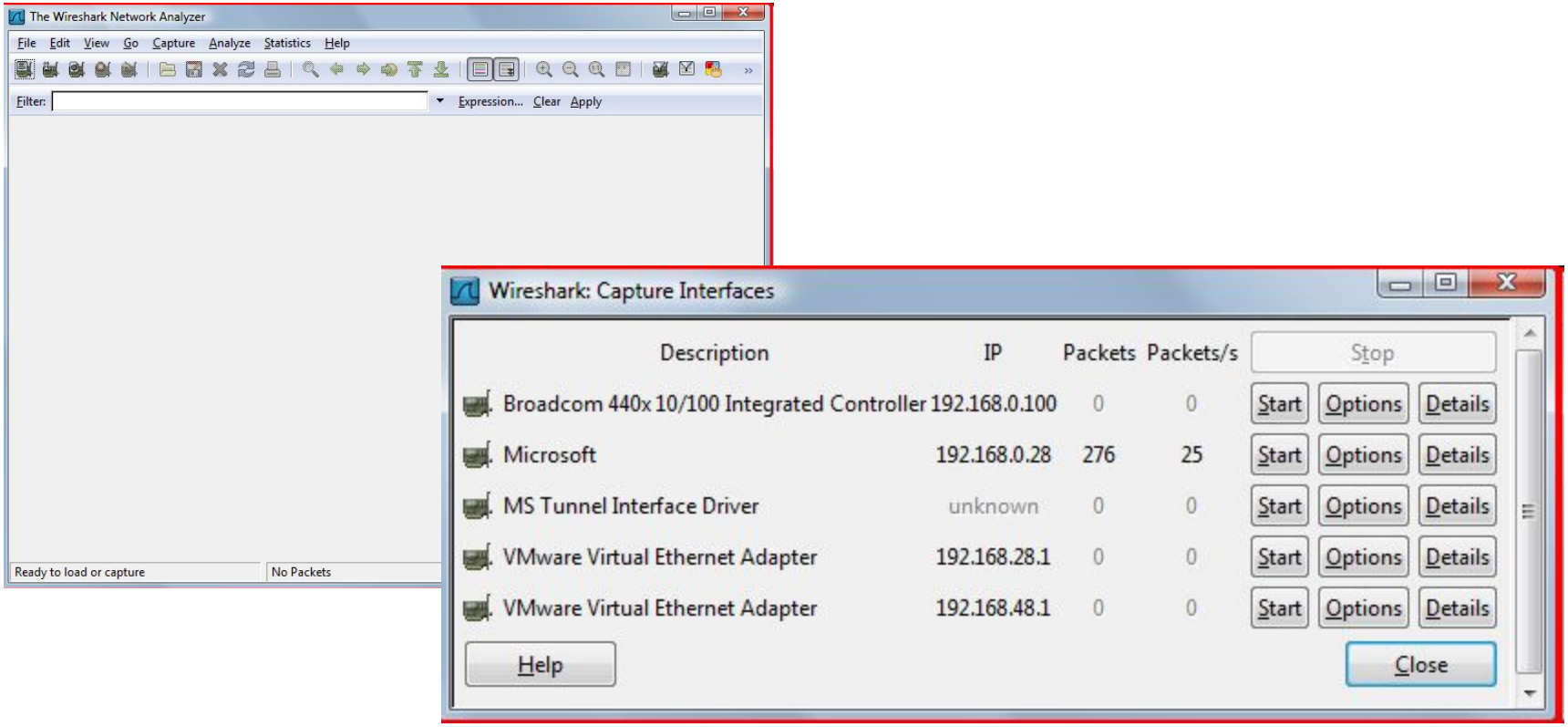
Install under Windows

- Download
- Install



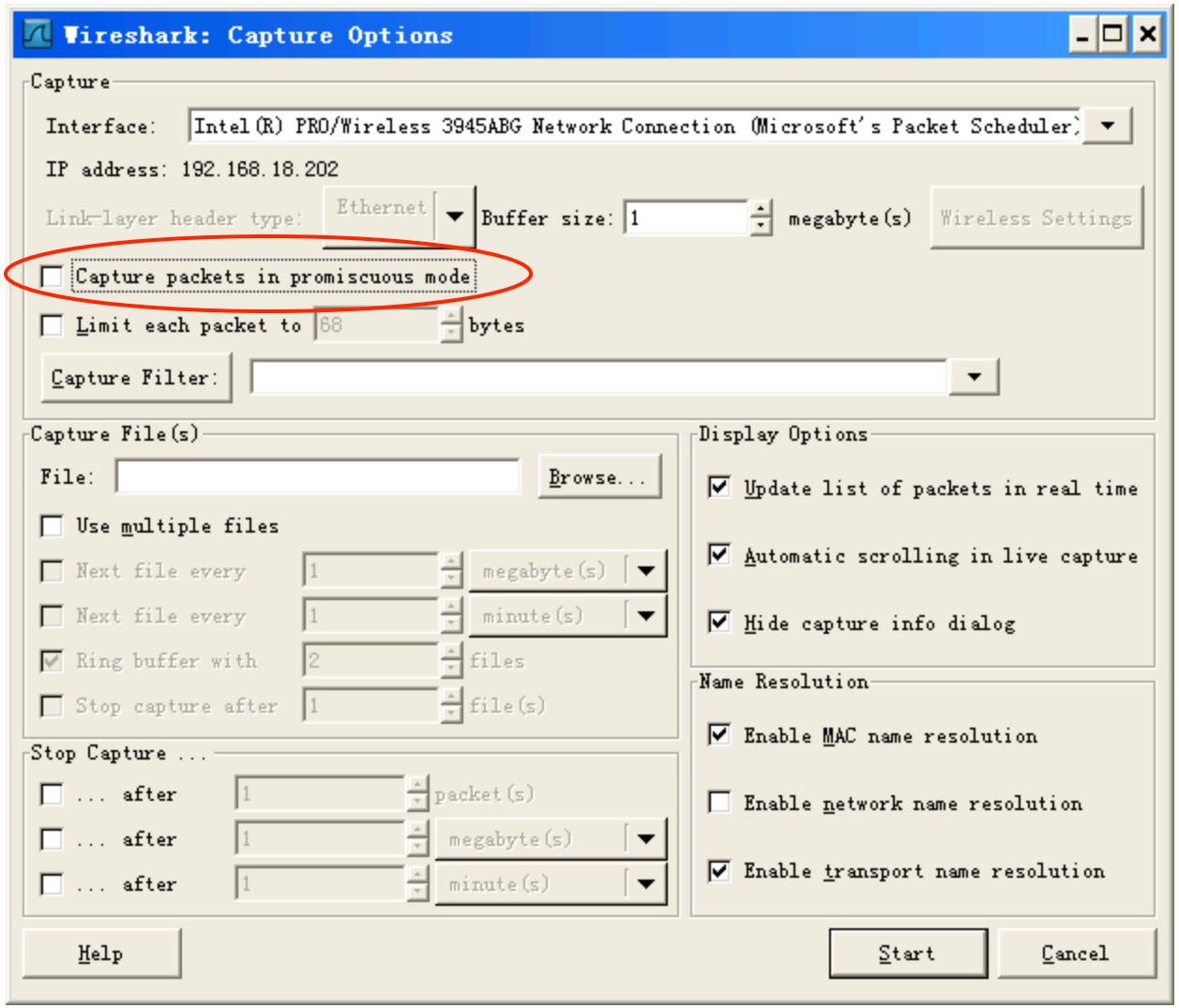
Install under Debian/ Ubuntu

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

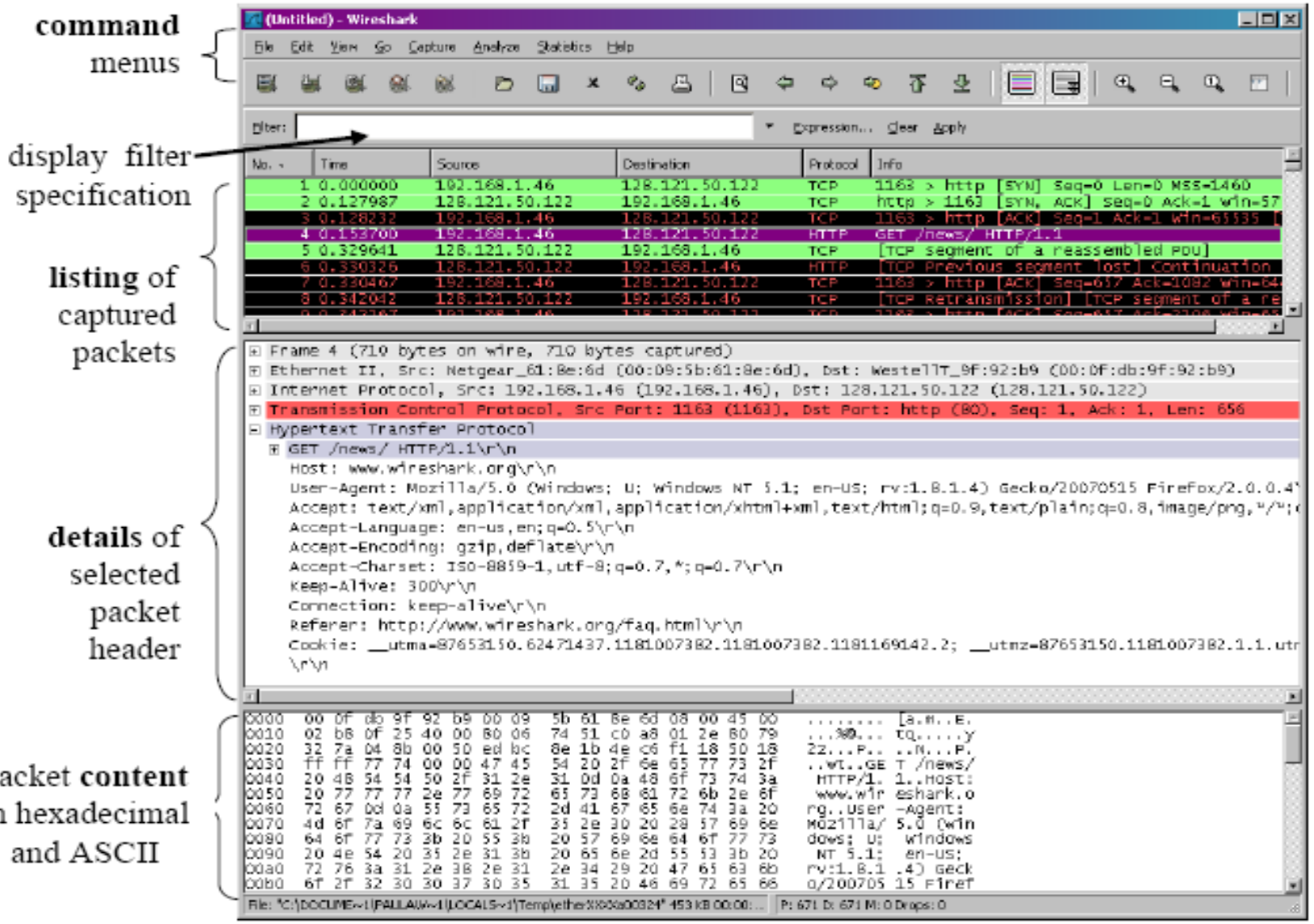


Configuration

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).



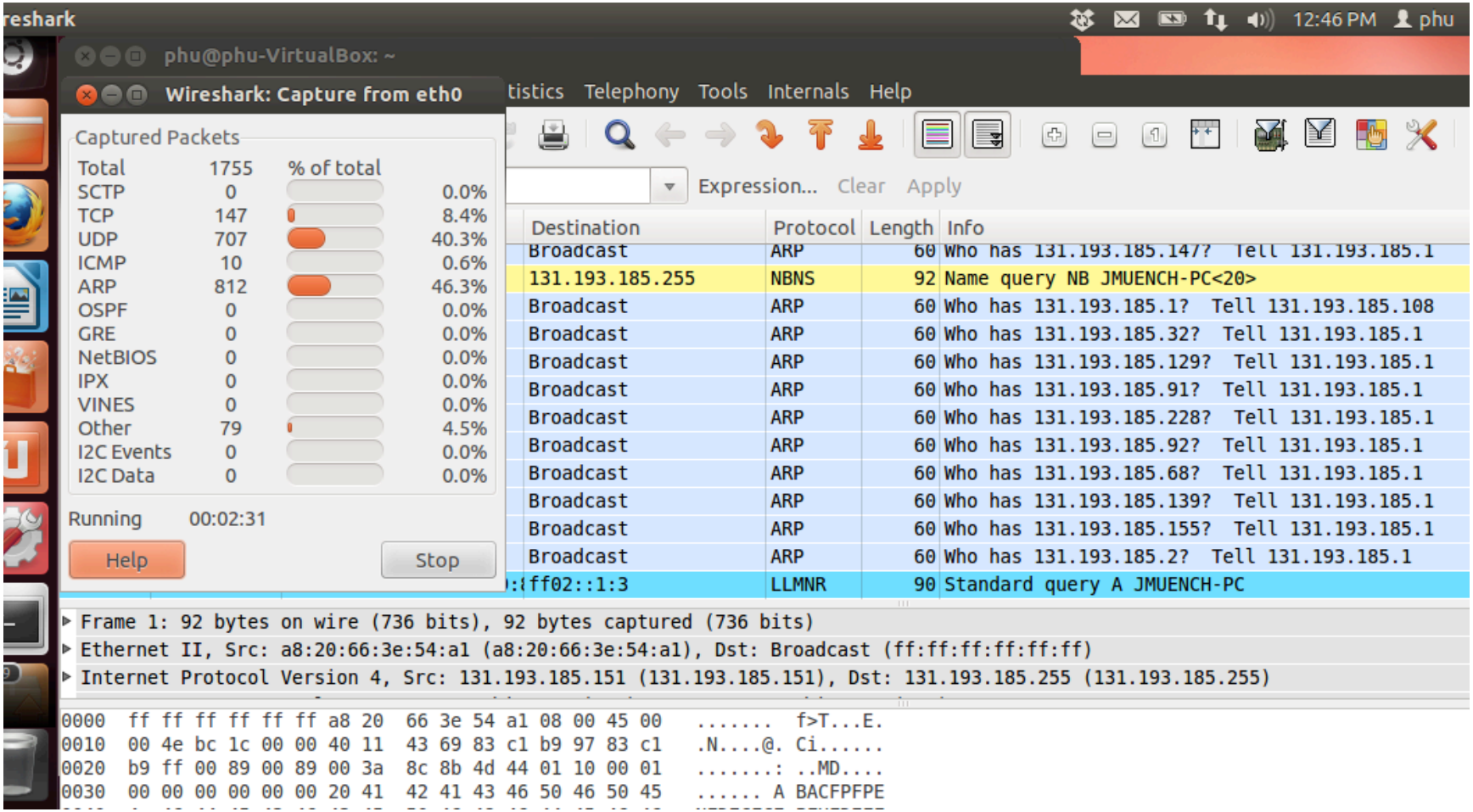
Wireshark Interface



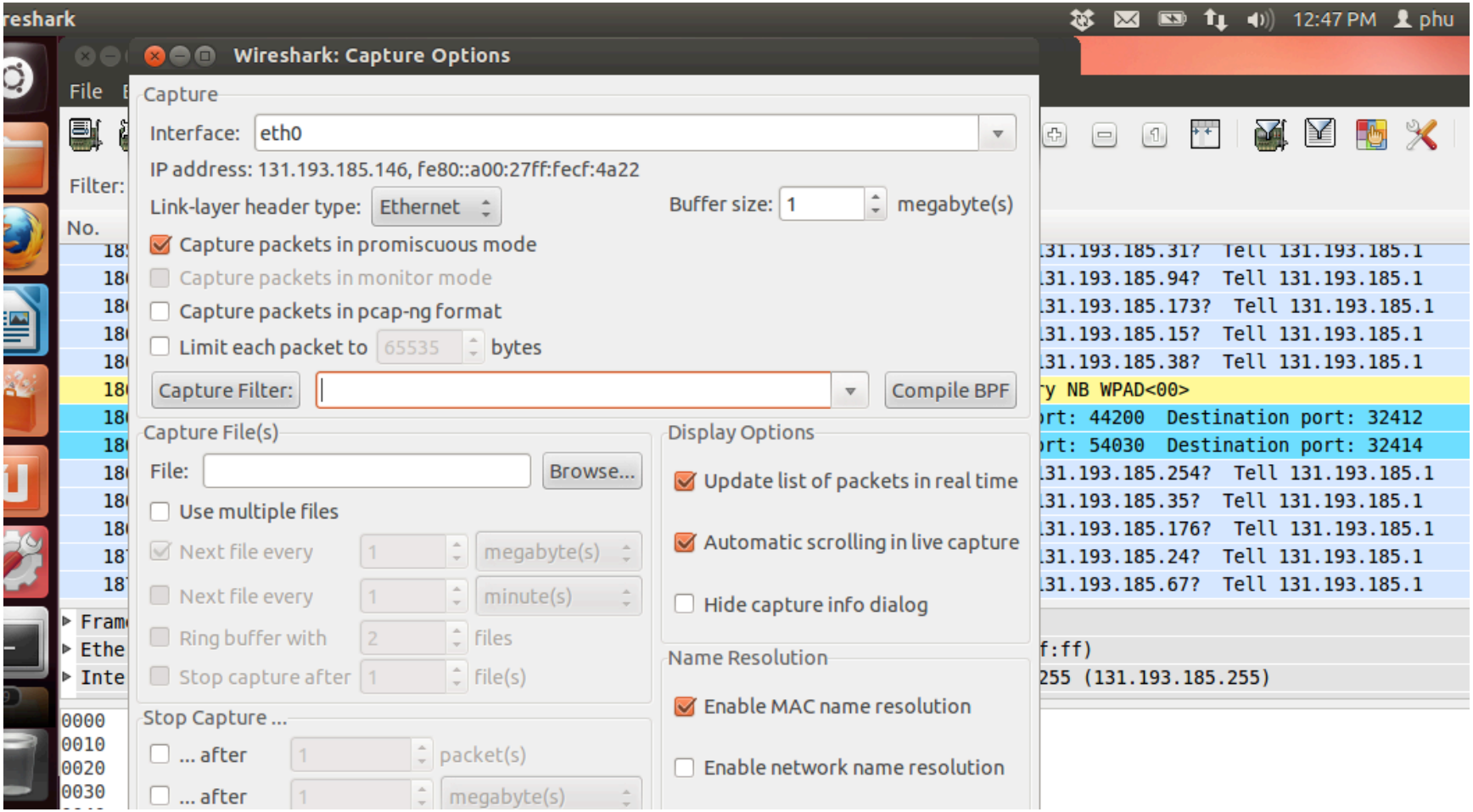
Wireshark on VirtualBox

- Only work with Ethernet interface
  - Bridge Adapter
  - Run with root permission:
    $sudo wireshark

Wireshark on VirtualBox



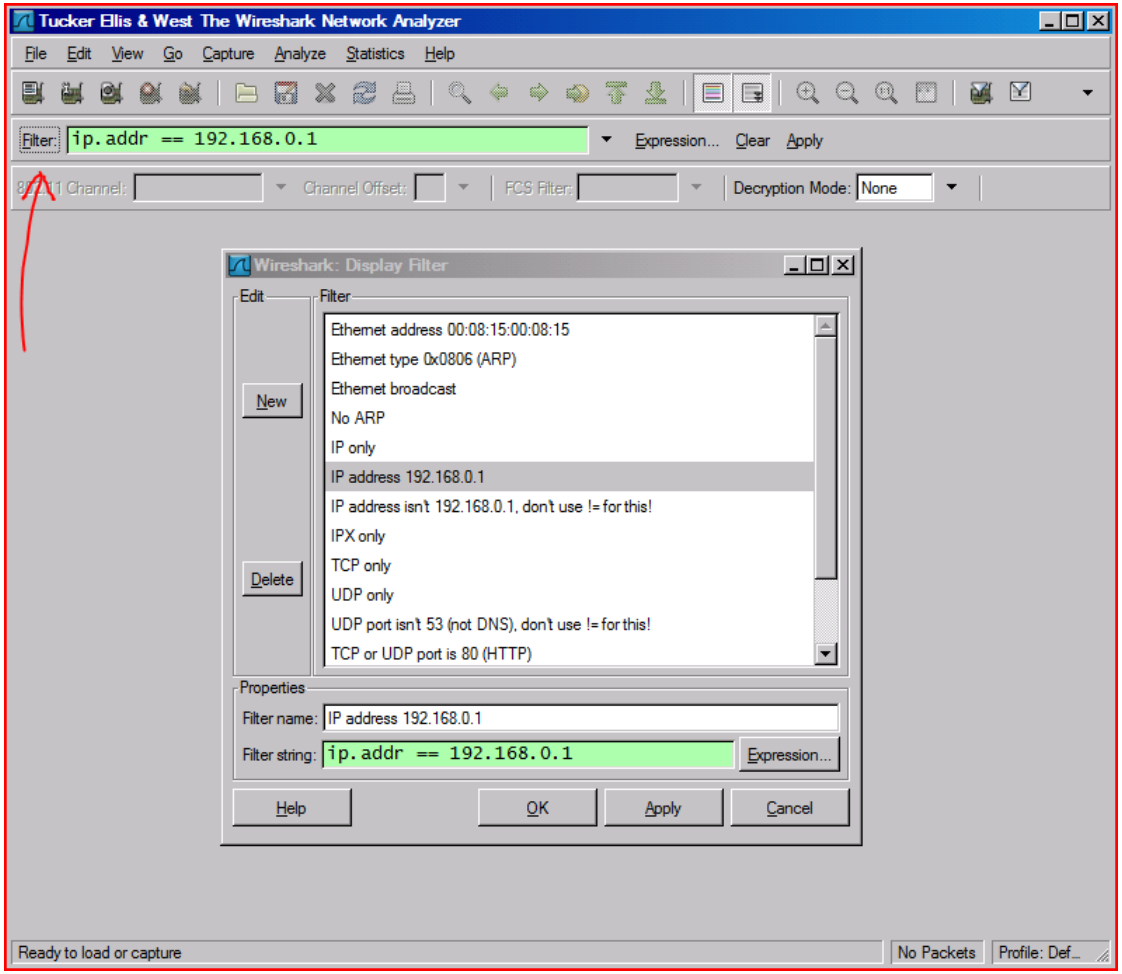
Wireshark on VirtualBox



Display Filters (Post-Filters)

- Display filters (also called post-filters) only filter the view of what you are seeing. All packets in the capture still exist in the trace
- Display filters use their own format and are much more powerful then capture filters

Display Filter



Display Filter Examples

ip.src==10.1.11.24

ip.addr==192.168.1.10 && ip.addr==192.168.1.20

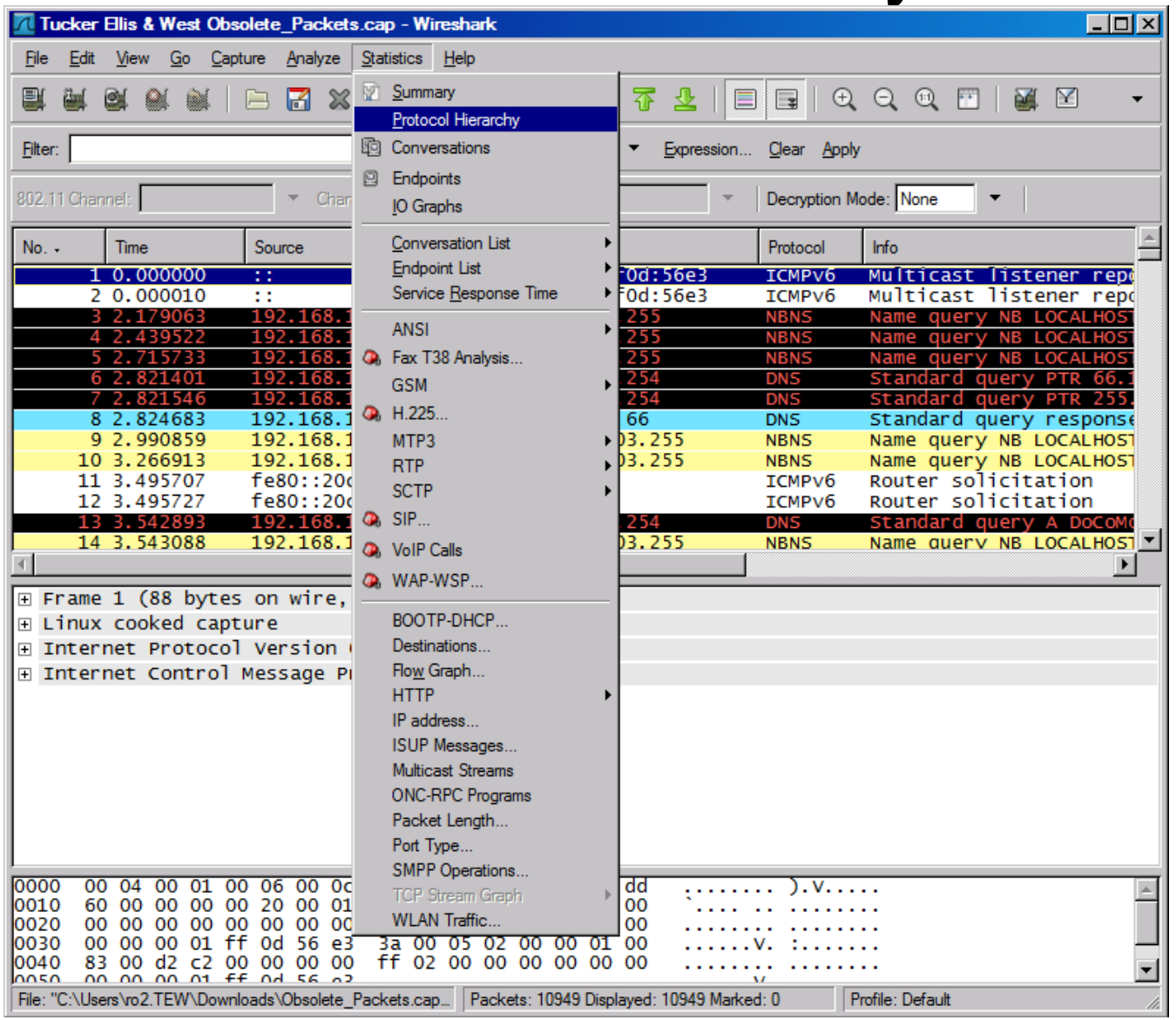
tcp.port==80 || tcp.port==3389

!(ip.addr==192.168.1.10 && ip.addr==192.168.1.20)

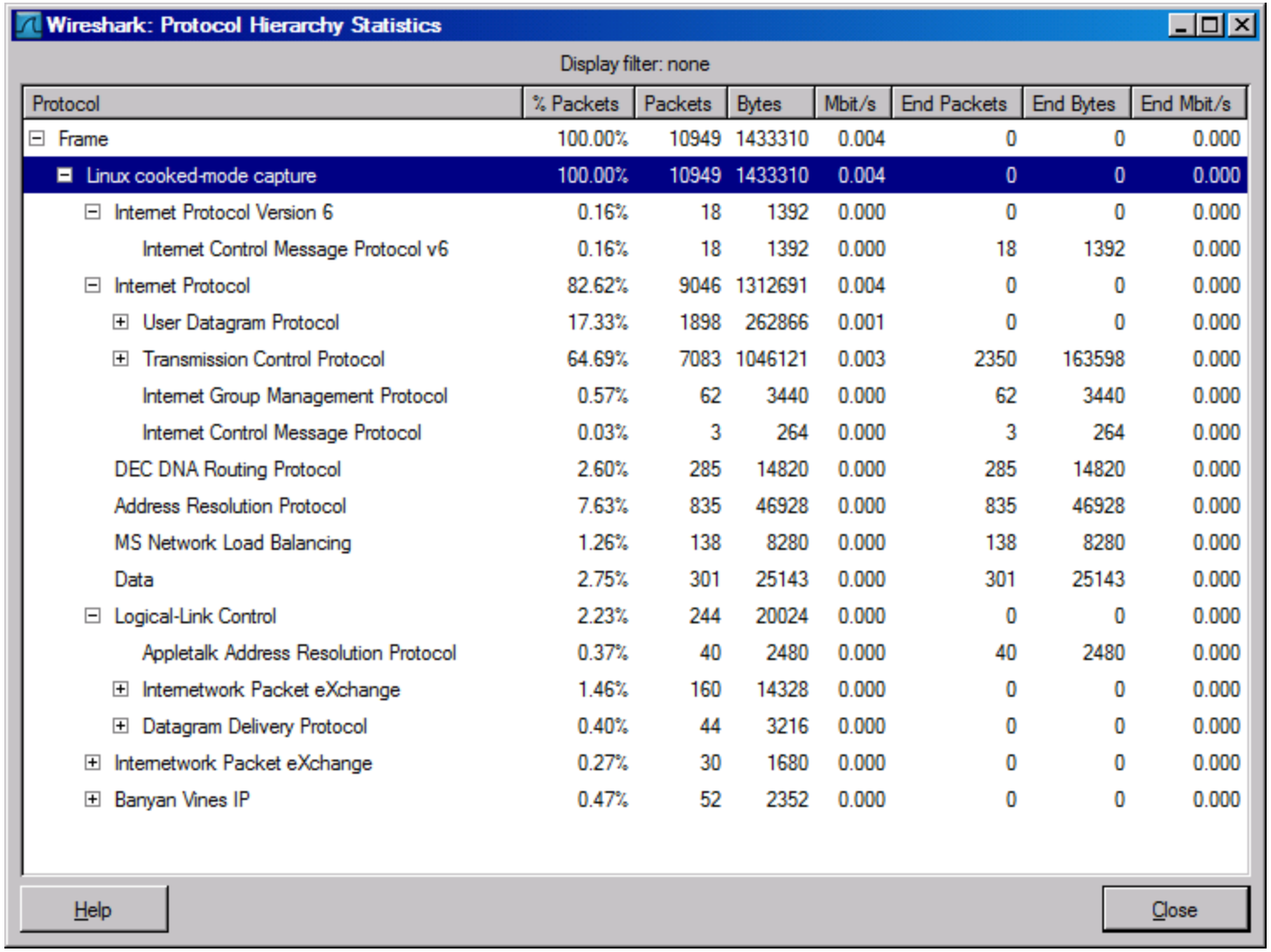
(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) && (tcp.port==445 || tcp.port==139)

(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) && (udp.port==67 || udp.port==68)

Protocol Hierarchy

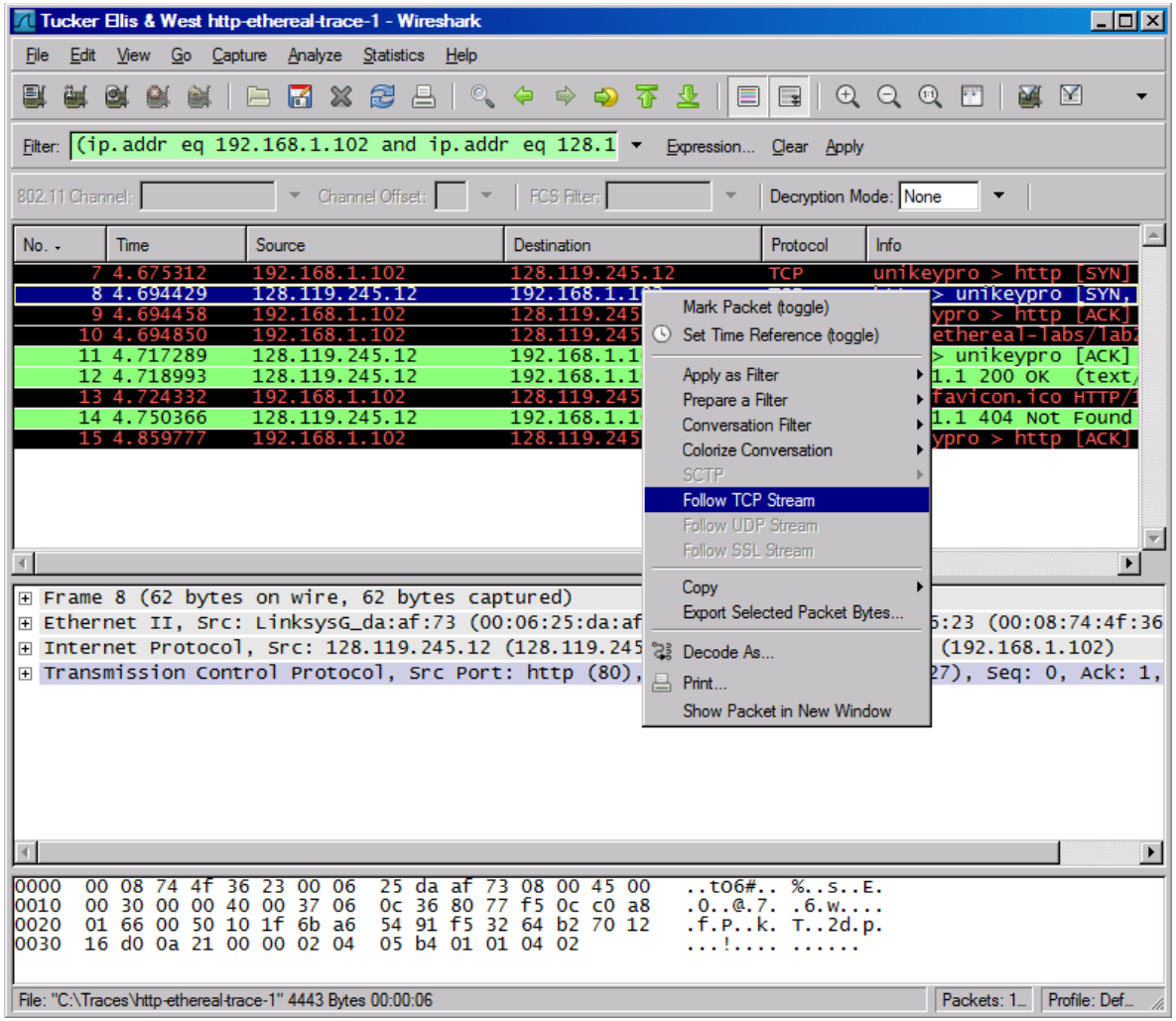


Protocol Hierarchy



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	10949	1433310	0.004	0	0	0.000
Linux cooked-mode capture	100.00%	10949	1433310	0.004	0	0	0.000
Internet Protocol Version 6	0.16%	18	1392	0.000	0	0	0.000
Internet Control Message Protocol v6	0.16%	18	1392	0.000	18	1392	0.000
Internet Protocol	82.62%	9046	1312691	0.004	0	0	0.000
User Datagram Protocol	17.33%	1898	262866	0.001	0	0	0.000
Transmission Control Protocol	64.69%	7083	1046121	0.003	2350	163598	0.000
Internet Group Management Protocol	0.57%	62	3440	0.000	62	3440	0.000
Internet Control Message Protocol	0.03%	3	264	0.000	3	264	0.000
DEC DNA Routing Protocol	2.60%	285	14820	0.000	285	14820	0.000
Address Resolution Protocol	7.63%	835	46928	0.000	835	46928	0.000
MS Network Load Balancing	1.26%	138	8280	0.000	138	8280	0.000
Data	2.75%	301	25143	0.000	301	25143	0.000
Logical-Link Control	2.23%	244	20024	0.000	0	0	0.000
Appletalk Address Resolution Protocol	0.37%	40	2480	0.000	40	2480	0.000
Internetwork Packet eXchange	1.46%	160	14328	0.000	0	0	0.000
Datagram Delivery Protocol	0.40%	44	3216	0.000	0	0	0.000
Internetwork Packet eXchange	0.27%	30	1680	0.000	0	0	0.000
Banyan Vines IP	0.47%	52	2352	0.000	0	0	0.000

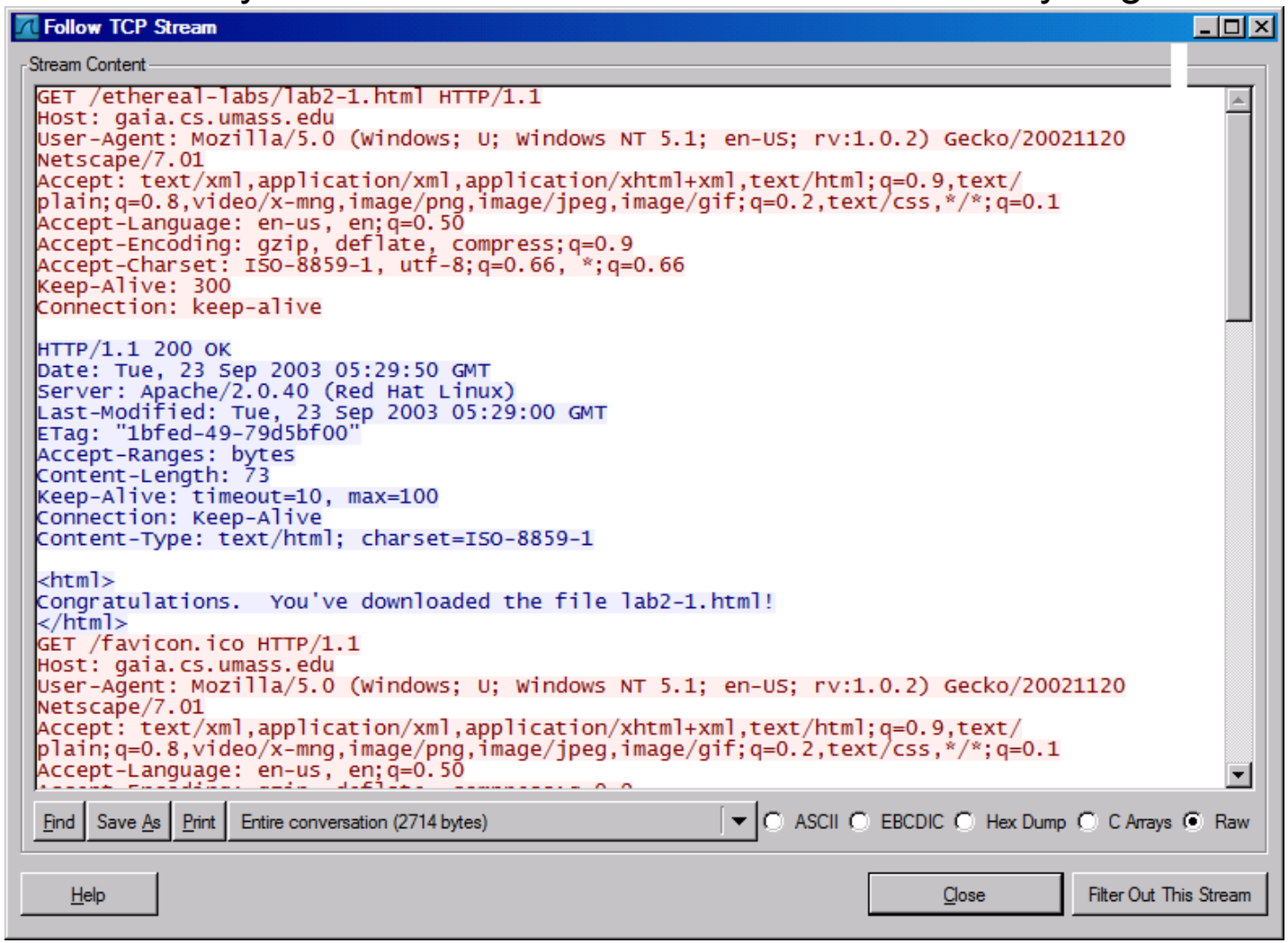
Follow TCP Stream



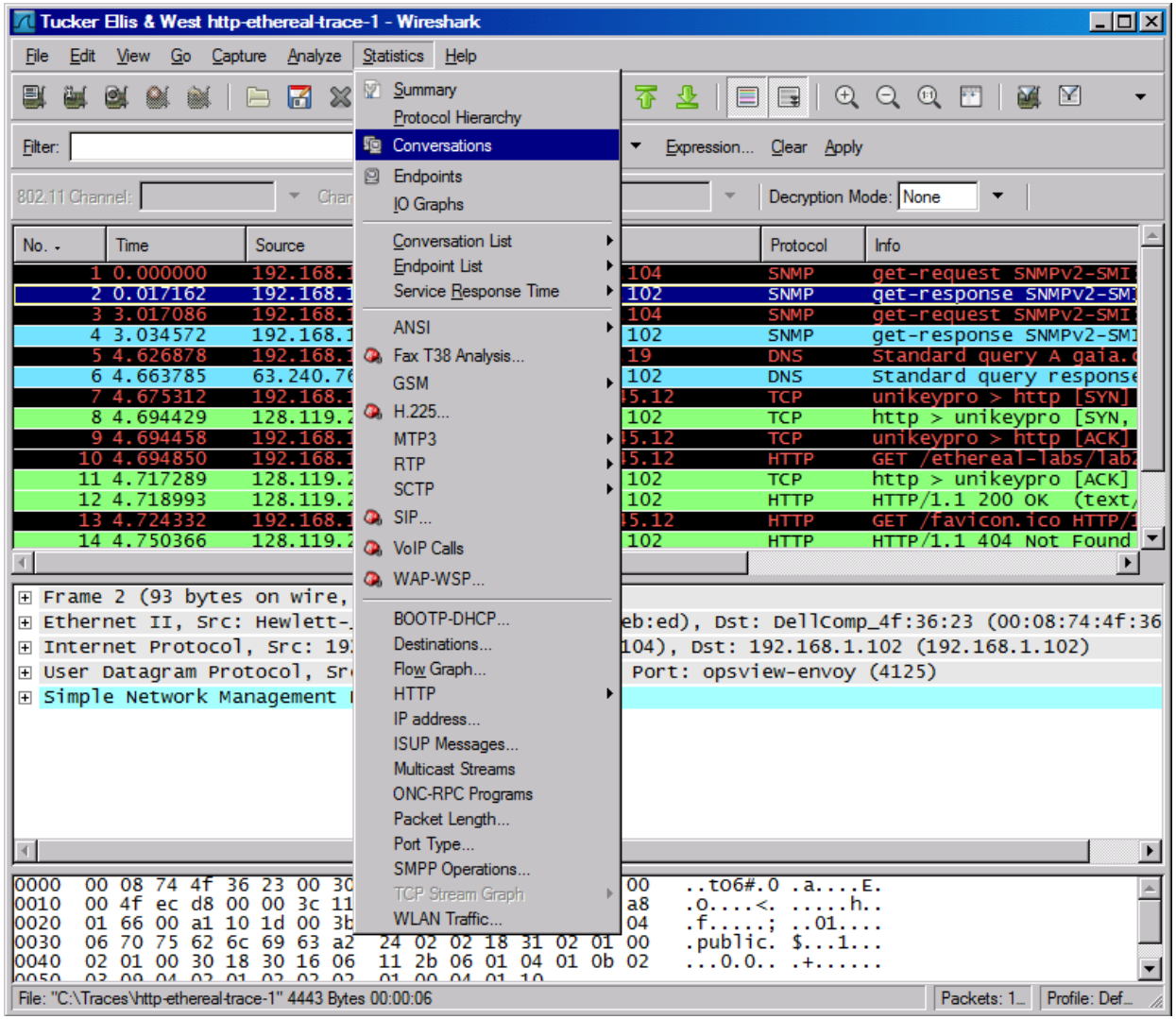
Follow TCP Stream

red - stuff you sent

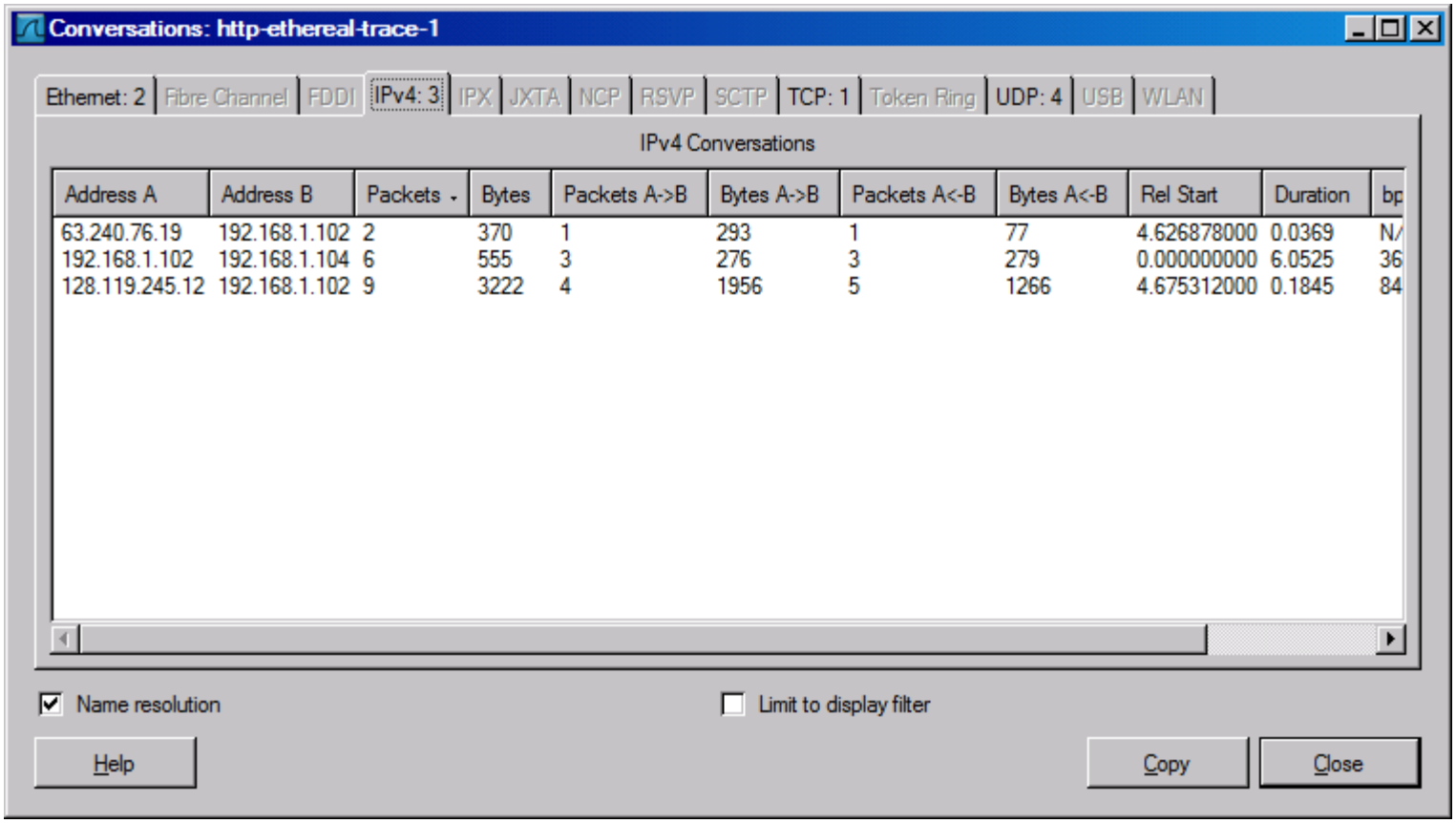
blue - stuff you get



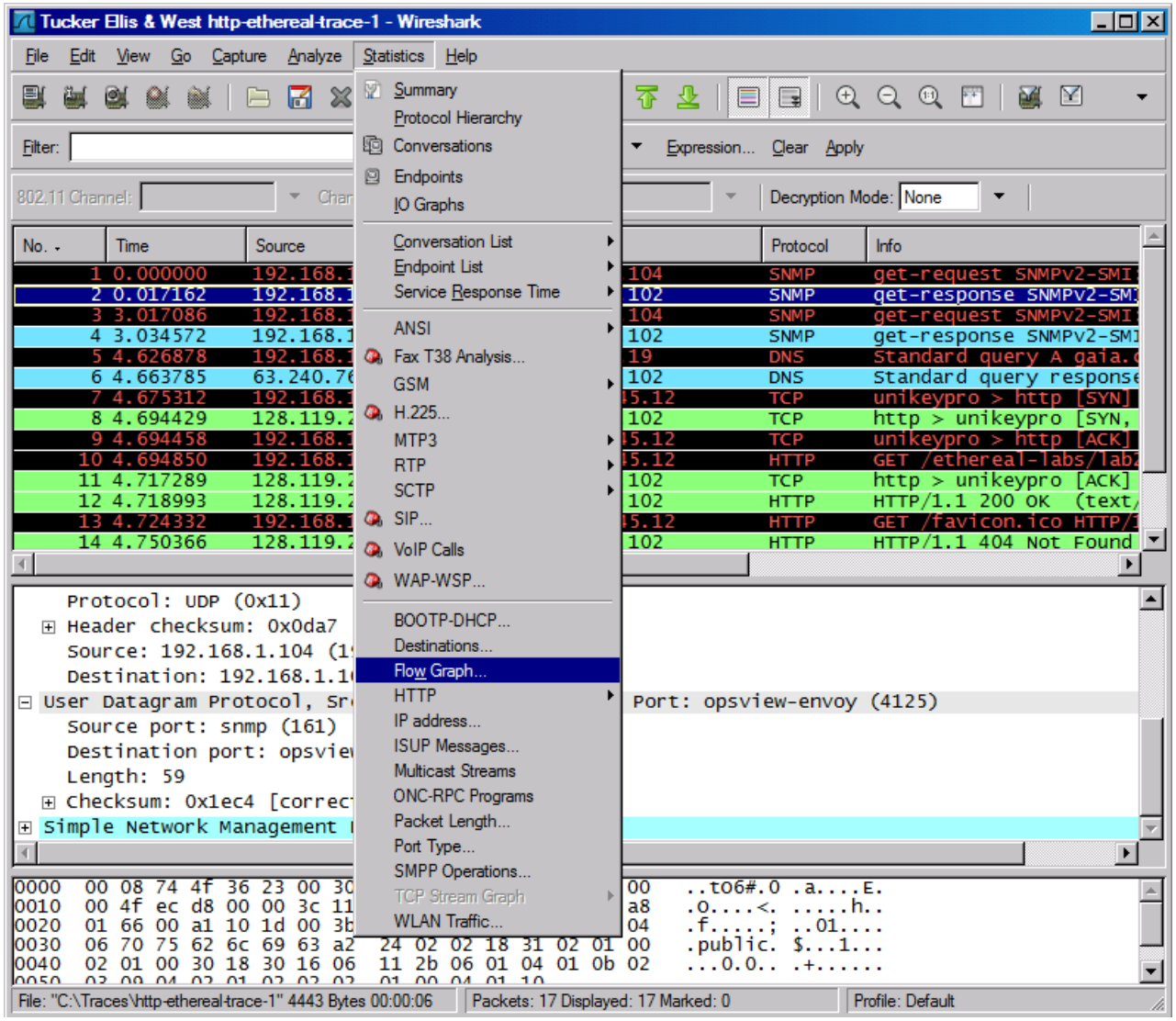
Conversations



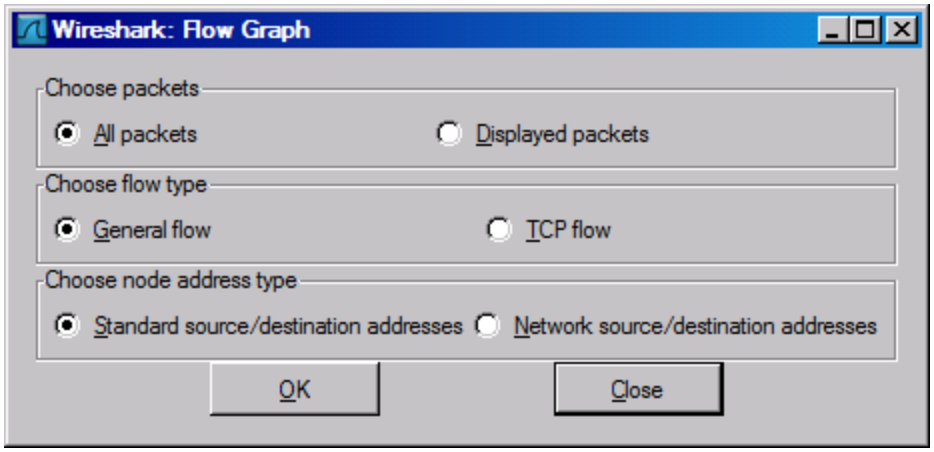
Conversations



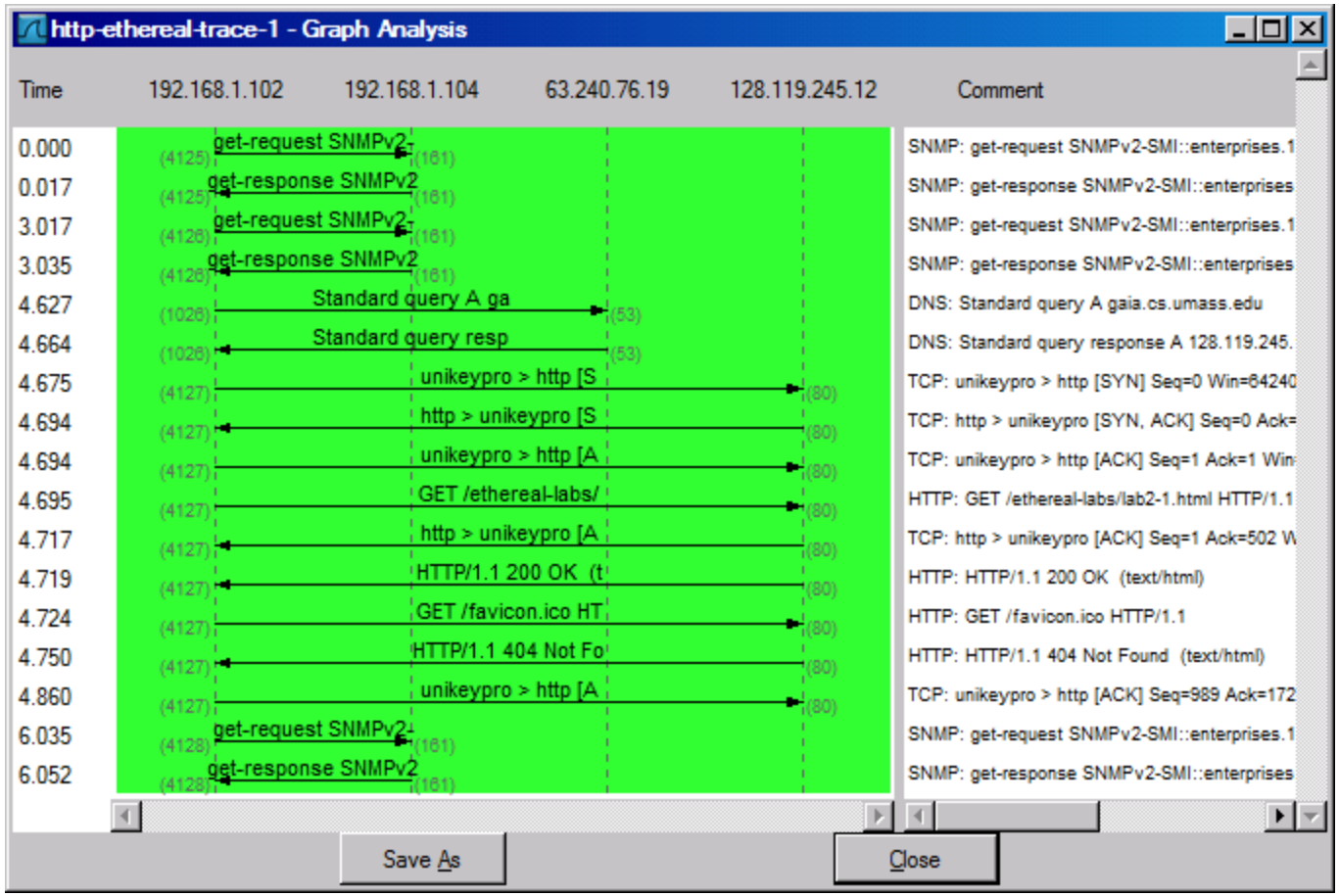
Flow Graphs


Tucker Ellis & West http-ethereal-trace-1 - Wireshark
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...
Multicast Streams
ONC-RPC Programs
Packet Length...
Port Type...
SMPP Operations...
TCP Stream Graph
WLAN Traffic...
Filter:
Expression... Clear Apply
Decryption Mode: None
No. Time Source Protocol Info
Protocol: UDP (0x11)
Header checksum: 0x0da7
Source: 192.168.1.104
Destination: 192.168.1.1
User Datagram Protocol, Sr
Source port: snmp (161)
Destination port: opsvie
Length: 59
Checksum: 0x1ec4 [correc
Simple Network Management
Port: opsview-envoy (4125)
File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06
Packets: 17 Displayed: 17 Marked: 0
Profile: Default

Flow Graphs


Wireshark: Flow Graph
Choose packets
All packets
Displayed packets
Choose flow type
General flow
TCP flow
Choose node address type
Standard source/destination addresses
Network source/destination addresses
OK
Close

Flow Graphs


http-ethereal-trace-1 - Graph Analysis
Time
192.168.1.102
192.168.1.104
63.240.76.19
128.119.245.12
Comment
0.000
0.017
3.017
3.035
4.627
4.664
4.675
4.694
4.694
4.695
4.717
4.719
4.724
4.750
4.860
6.035
6.052
get-request SNMPv2
get-response SNMPv2
get-request SNMPv2
get-response SNMPv2
Standard query A ga
Standard query resp
unikeypro > http [S
http > unikeypro [S
unikeypro > http [A
GET /ethereal-labs/
http > unikeypro [A
HTTP/1.1 200 OK (t
GET /favicon.ico HT
HTTP/1.1 404 Not Fo
unikeypro > http [A
get-request SNMPv2
get-response SNMPv2
SNMP: get-request SNMPv2-SMI::enterprises.1
SNMP: get-response SNMPv2-SMI::enterprises
SNMP: get-request SNMPv2-SMI::enterprises.1
SNMP: get-response SNMPv2-SMI::enterprises
DNS: Standard query A gaia.cs.umass.edu
DNS: Standard query response A 128.119.245.
TCP: unikeypro > http [SYN] Seq=0 Win=64240
TCP: http > unikeypro [SYN, ACK] Seq=0 Ack=
TCP: unikeypro > http [ACK] Seq=1 Ack=1 Win
HTTP: GET /ethereal-labs/lab2-1.html HTTP/1.1
TCP: http > unikeypro [ACK] Seq=1 Ack=502 W
HTTP: HTTP/1.1 200 OK (text/html)
HTTP: GET /favicon.ico HTTP/1.1
HTTP: HTTP/1.1 404 Not Found (text/html)
TCP: unikeypro > http [ACK] Seq=989 Ack=172
SNMP: get-request SNMPv2-SMI::enterprises.1
SNMP: get-response SNMPv2-SMI::enterprises
Save As
Close

Assignment 3 – Understanding Network Traffic using Wireshark

- Deadline Sunday Feb 22, 11:59 PM
  - 1 bonus point for submission 24 hours before deadline
  - Firm deadline -> Start early

Understanding Network Traffic using Wireshark

- Download the trace files, open with Wireshark and answer Q1-12 accordingly

- Q13 requires a real capture
  - Install Wireshark on your own machine

Next lecture

- TCP
  - Readings 3.5
- Guest lecture on Monday Feb 23rd
  - DNS Security
- Midterm exam in 4 weeks
  - In class: 1 PM Friday, March 6th