
Uma Ferramenta Essencial !

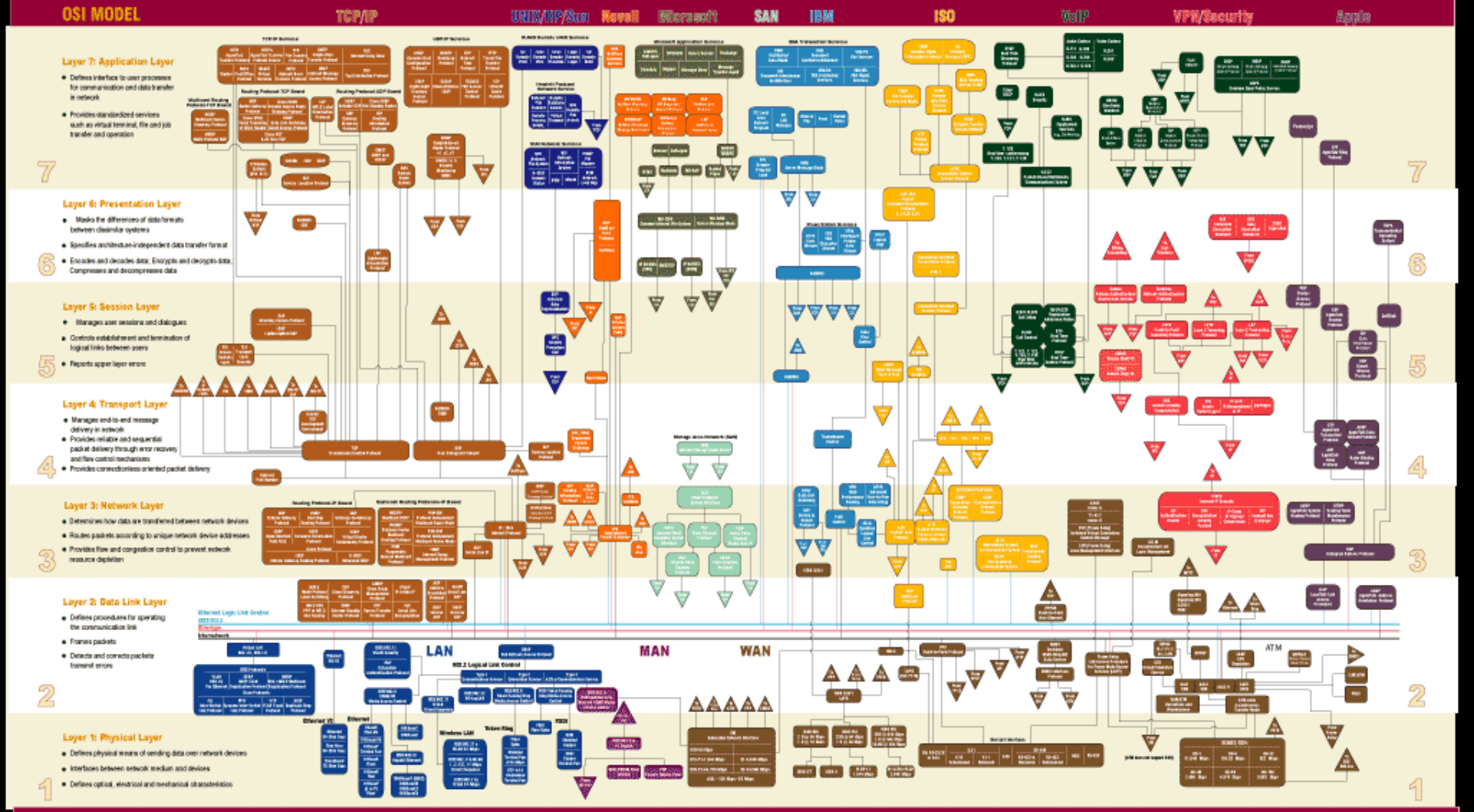
Prof. Fred Sauer, D.Sc.

fsauer@gmail.com

# Quem é WireShark?

- Packet sniffer/protocol analyzer
- Ferramenta de Rede de código aberto
- Evolução do Ethereal

# NETWORK COMMUNICATION PROTOCOLS MAP




**ANSI**
American National Standard Institute
11 west 42nd Street
New York NY 10036 USA
Tel: 212-642-4900
www.ansi.org

**ETSI**
European Telecommunications Standards Institute
Route des Lucioles
F-06921 Sophia Antipolis Cedex, France
Tel: 33 (0)4 92 94 42 00
www.etsi.org

**FCC**
Federal Communications Commission
1919 M Street NW
Washington DC USA
Tel: 202-418-0200
www.fcc.gov

**IEEE**
Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331 USA
Tel: 908-981-0060
www.ieee.org

**ISO**
International Organization for Standardization
Case postale 56
Geneva 20, Switzerland
Tel: 41-22-749-0111
www.iso.ch

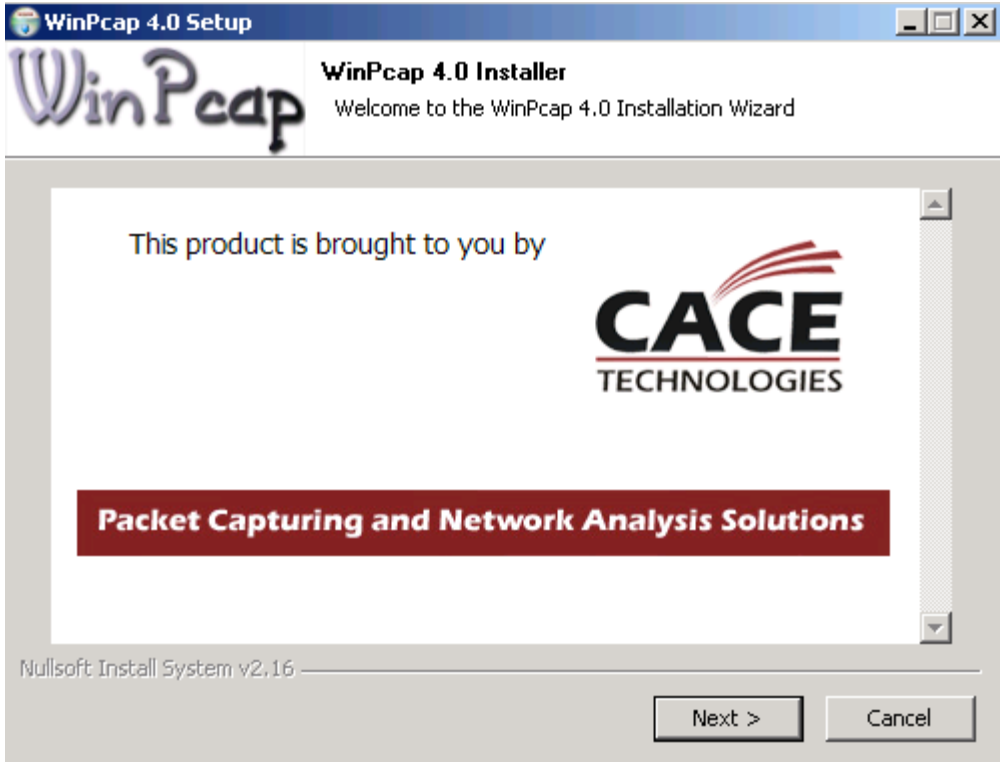
**ITU**
International Telecommunications Union
Place des Nations
CH-1211 Geneva 20, Switzerland
Tel: 41 22 99 51 11
www.itu.ch

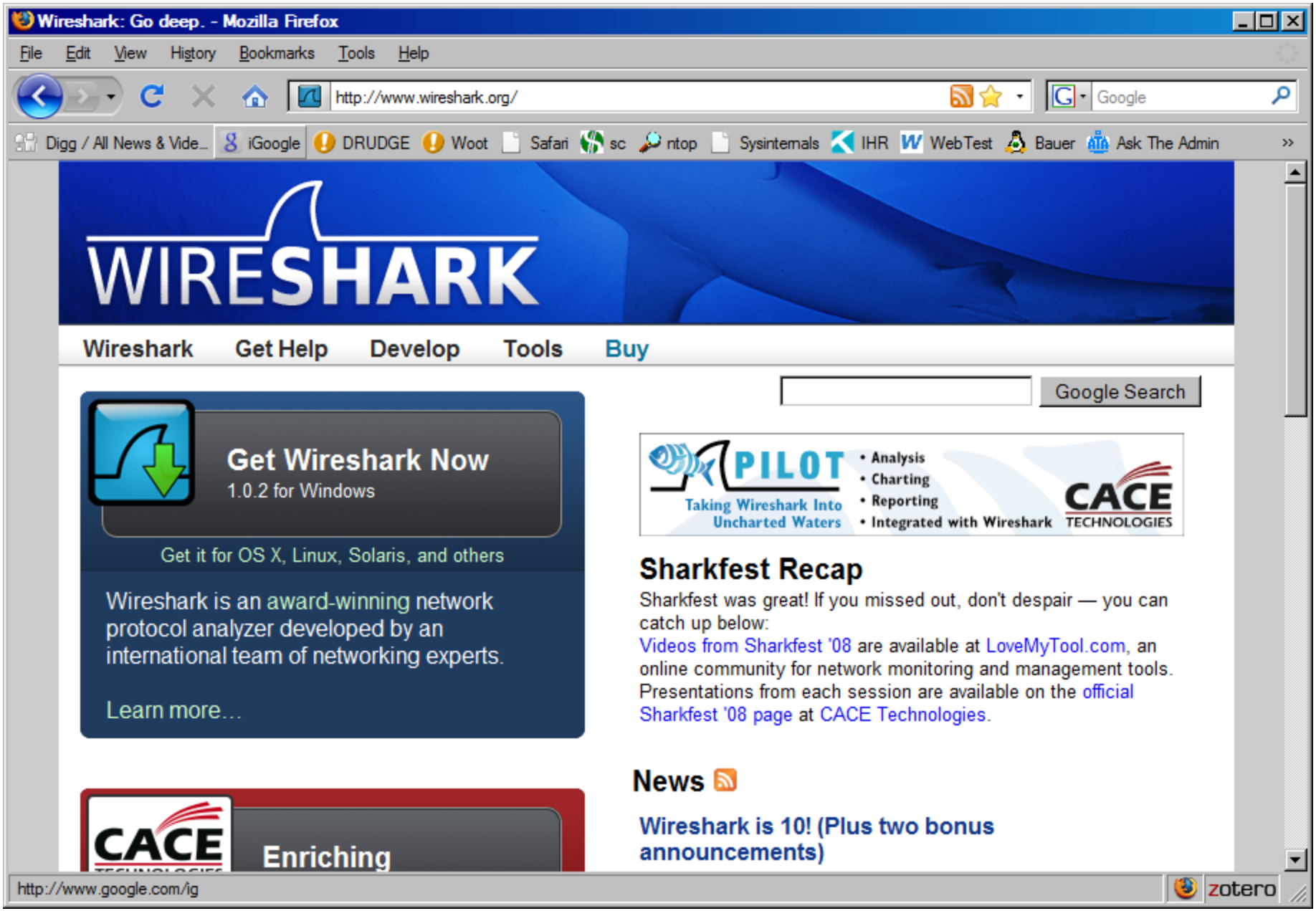
**ISOC:** Internet Society
www.isoc.org
**IETF:** Internet Engineering Task Force
www.ietf.org
1775 Wiehle Ave, Suite 102
Reston VA 20190 USA
Tel: 703-326-9880

**IEC**
International Electrotechnical Commission
3, rue de Varembe
P.O. Box 131
1211 Geneva 20, Switzerland
Tel: 41-22-919-02-11
www.iec.ch

Javvin

# Instalação


WinPcap 4.0 Setup
WinPcap
WinPcap 4.0 Installer
Welcome to the WinPcap 4.0 Installation Wizard
This product is brought to you by
CACE
TECHNOLOGIES
Packet Capturing and Network Analysis Solutions
Nullsoft Install System v2.16
Next >
Cancel


Wireshark: Go deep. - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.wireshark.org/
Google
Digg / All News & Vide... iGoogle DRUDGE Woot Safari sc ntop Sysinternals IHR WebTest Bauer Ask The Admin
WIRESHARK
Wireshark Get Help Develop Tools Buy
Google Search
Get Wireshark Now
1.0.2 for Windows
Get it for OS X, Linux, Solaris, and others
Wireshark is an award-winning network protocol analyzer developed by an international team of networking experts.
Learn more…
PILOT
Taking Wireshark Into Uncharted Waters
• Analysis
• Charting
• Reporting
• Integrated with Wireshark
CACE TECHNOLOGIES
Sharkfest Recap
Sharkfest was great! If you missed out, don't despair — you can catch up below:
Videos from Sharkfest '08 are available at LoveMyTool.com, an online community for network monitoring and management tools.
Presentations from each session are available on the official Sharkfest '08 page at CACE Technologies.
News
Wireshark is 10! (Plus two bonus announcements)
CACE
Enriching
http://www.google.com/ig
zotero

# Instalação no Linux

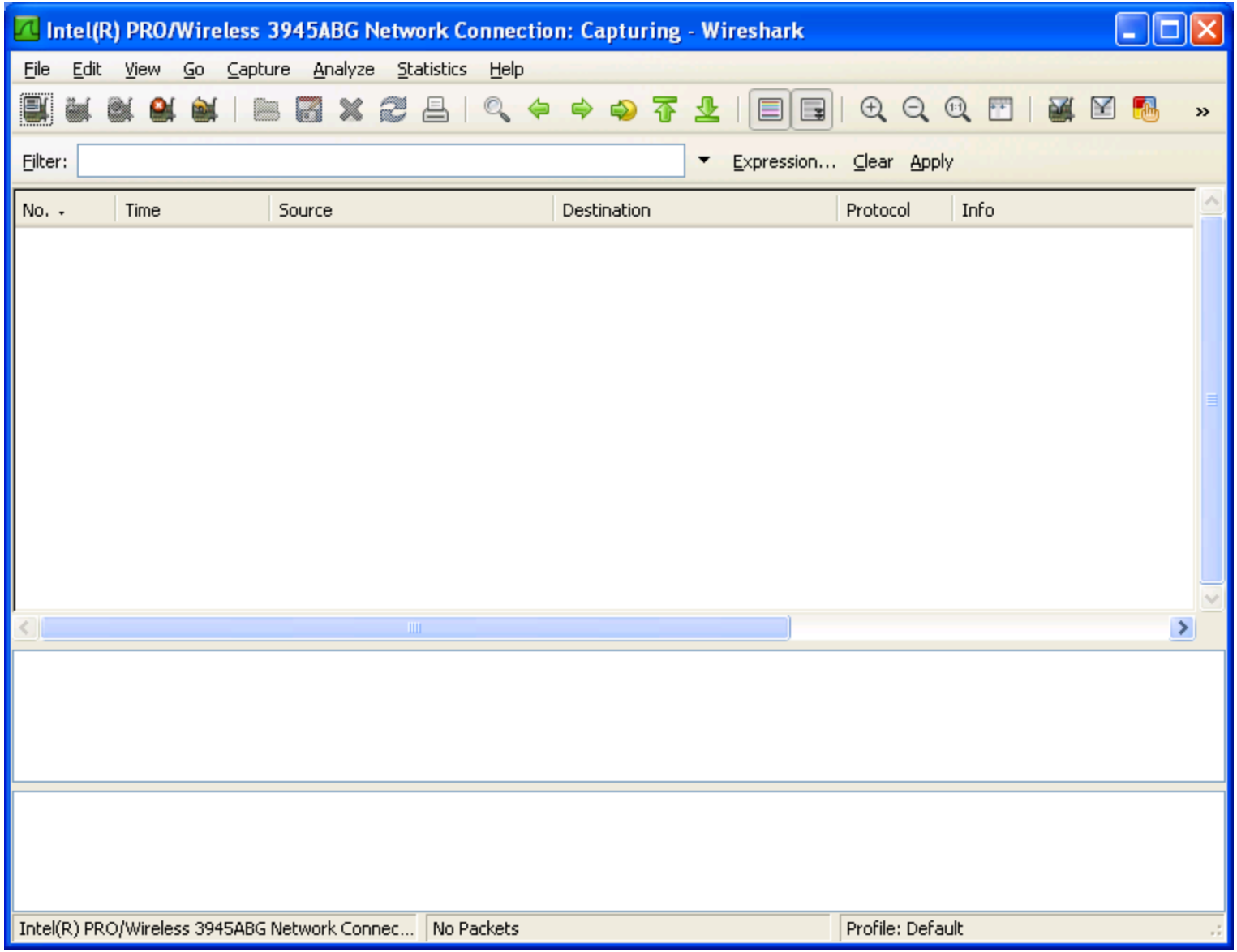
- CENTOS – yum install wireshark
- Ubuntu – apt-get install wireshark
- Red Hat – rpm –iv wireshark*rpm

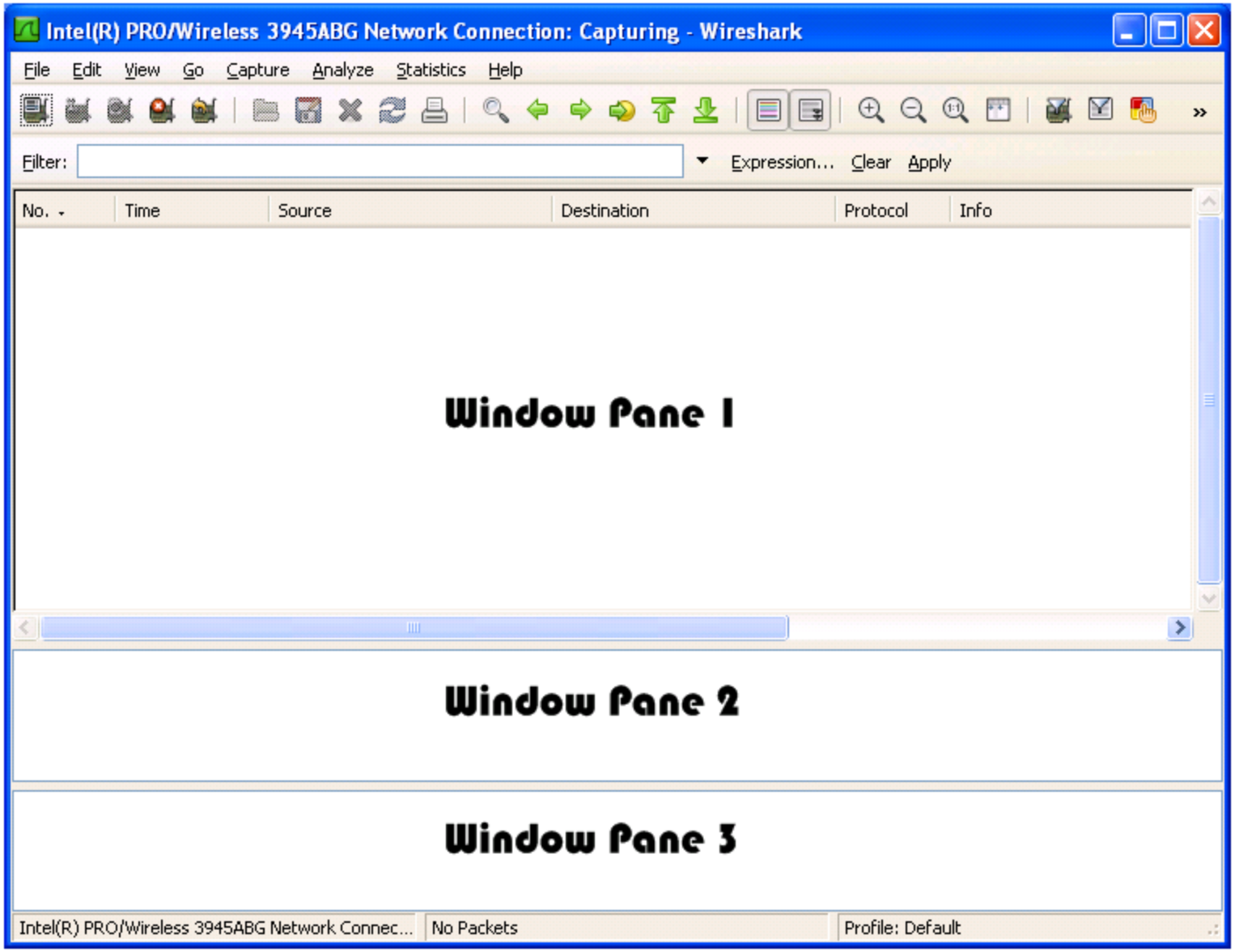
- Na maioria dos casos as dependências (como libpcap) são automaticamente instaladas


tshark
Wireshark
GUI

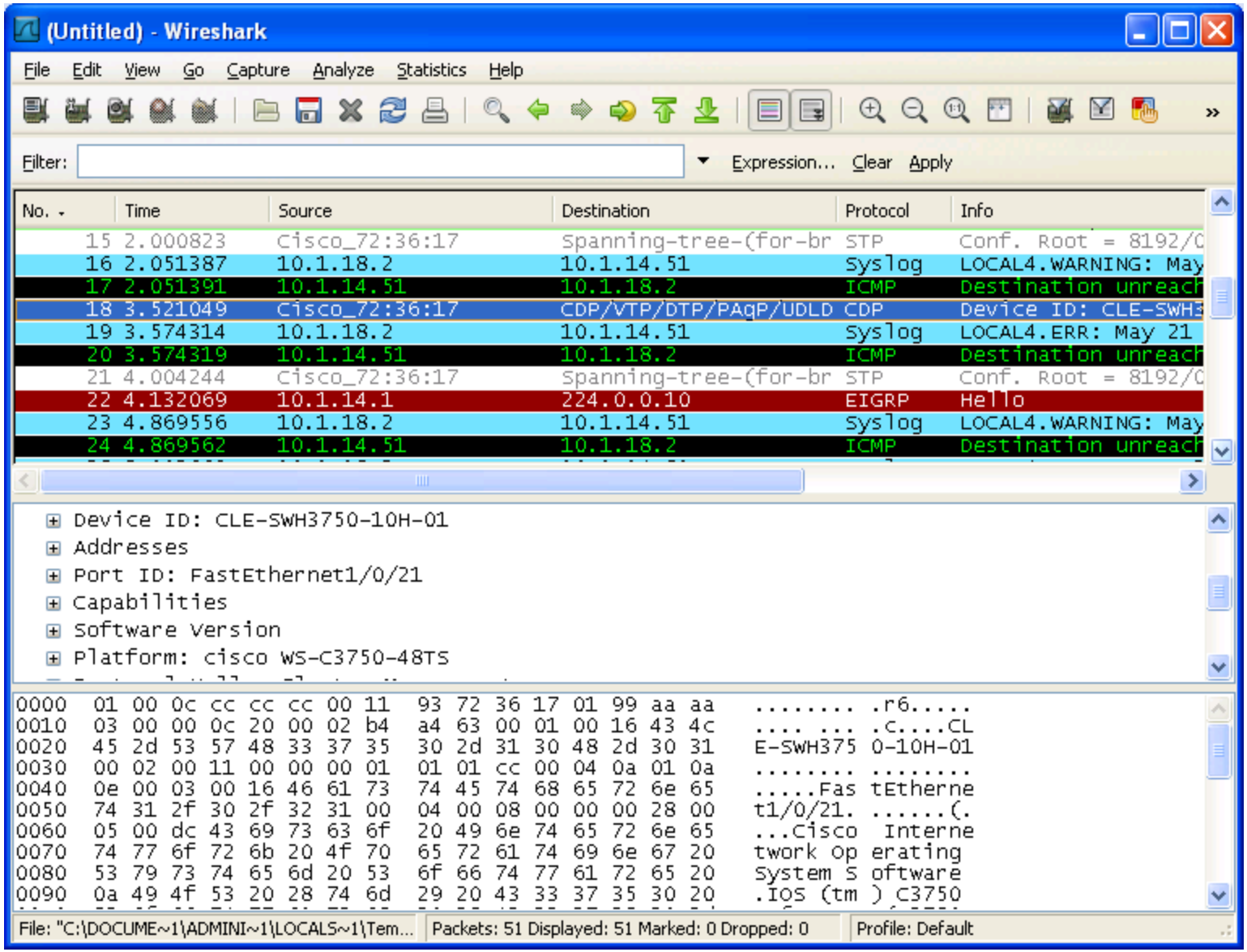
# tshark

```
C:\Program Files\Wireshark>tshark -help
TShark 1.0.0
Dump and analyze network traffic.
See http://www.wireshark.org for more information.

Copyright 1998-2008 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Usage: tshark [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -B <buffer size>         size of kernel buffer (def: 1MB)
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                             files:NUM - stop after NUM files
……..
```

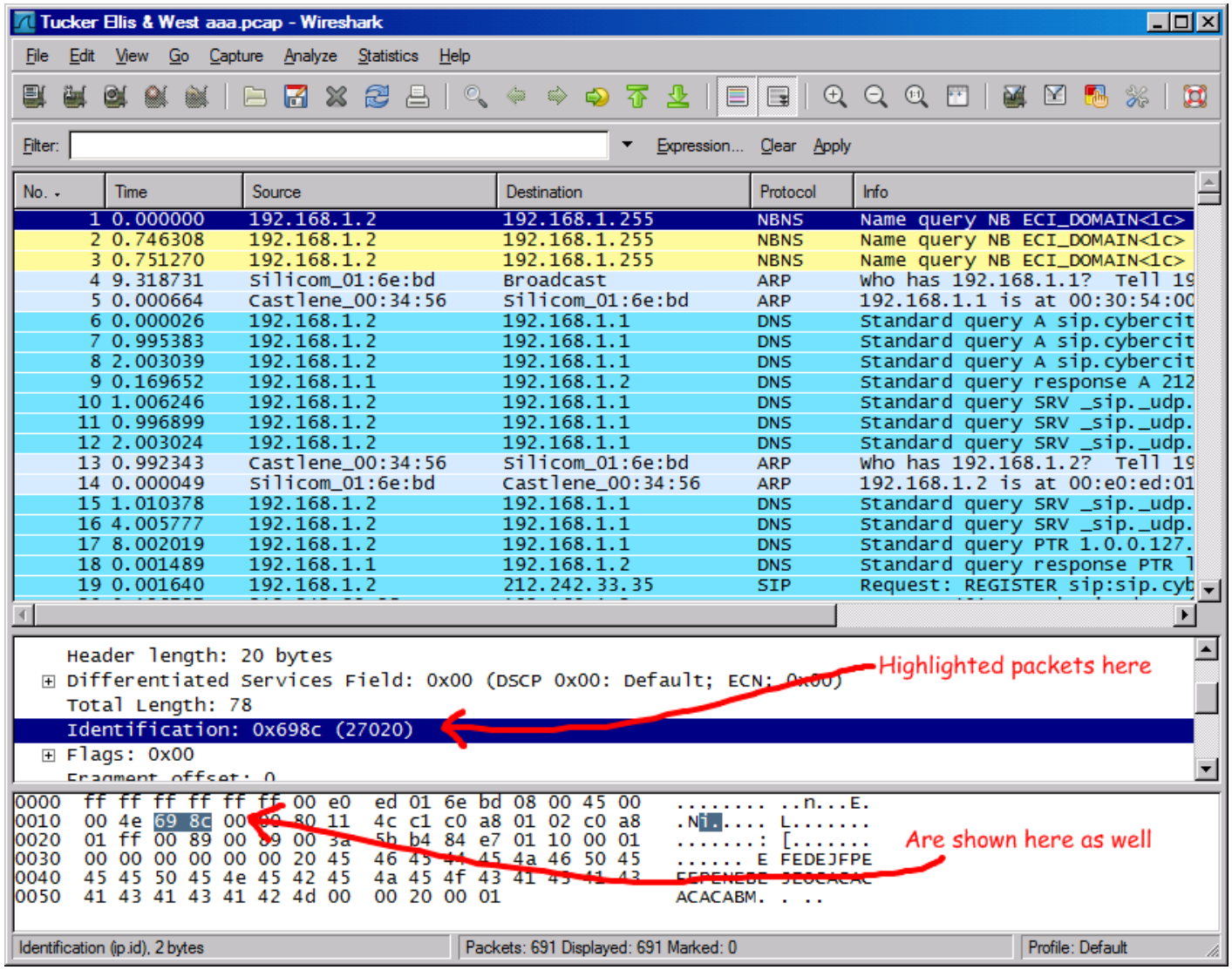

Intel(R) PRO/Wireless 3945ABG Network Connection: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
Intel(R) PRO/Wireless 3945ABG Network Connec...
No Packets
Profile: Default


Intel(R) PRO/Wireless 3945ABG Network Connection: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
Window Pane 1
Window Pane 2
Window Pane 3
Intel(R) PRO/Wireless 3945ABG Network Connec...
No Packets
Profile: Default

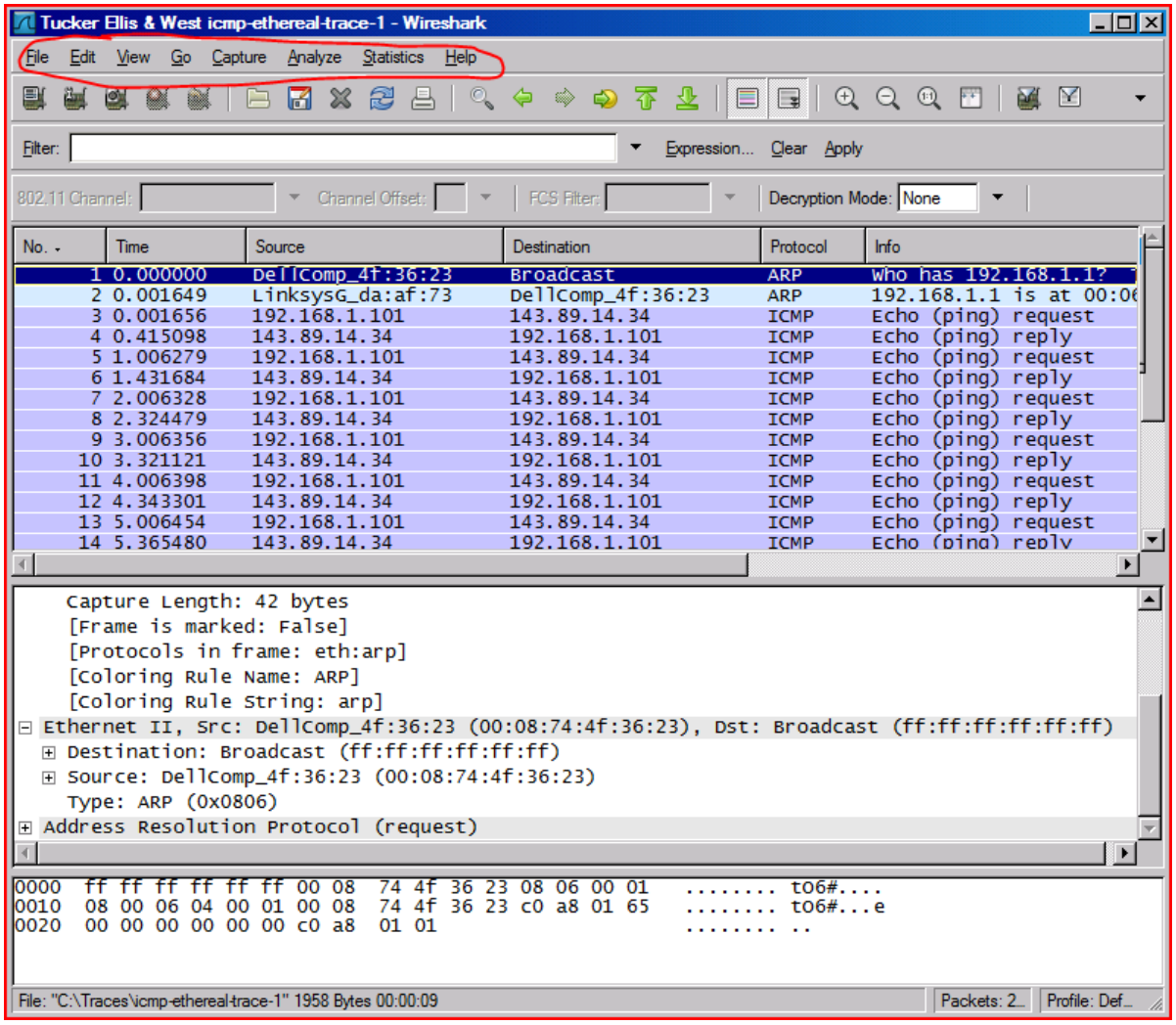
# Com tráfego…


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
15 2.000823 Cisco_72:36:17 Spanning-tree-(for-br STP Conf. Root = 8192/C
16 2.051387 10.1.18.2 10.1.14.51 Syslog LOCAL4.WARNING: May
17 2.051391 10.1.14.51 10.1.18.2 ICMP Destination unreach
18 3.521049 Cisco_72:36:17 CDP/VTP/DTP/PAgP/UDLD CDP Device ID: CLE-SWH3
19 3.574314 10.1.18.2 10.1.14.51 Syslog LOCAL4.ERR: May 21
20 3.574319 10.1.14.51 10.1.18.2 ICMP Destination unreach
21 4.004244 Cisco_72:36:17 Spanning-tree-(for-br STP Conf. Root = 8192/C
22 4.132069 10.1.14.1 224.0.0.10 EIGRP Hello
23 4.869556 10.1.18.2 10.1.14.51 Syslog LOCAL4.WARNING: May
24 4.869562 10.1.14.51 10.1.18.2 ICMP Destination unreach
Device ID: CLE-SWH3750-10H-01
Addresses
Port ID: FastEthernet1/0/21
Capabilities
Software Version
Platform: cisco WS-C3750-48TS
0000 01 00 0c cc cc cc 00 11 93 72 36 17 01 99 aa aa ..... .r6.....
0010 03 00 00 0c 20 00 02 b4 a4 63 00 01 00 16 43 4c .... ... .c....CL
0020 45 2d 53 57 48 33 37 35 30 2d 31 30 48 2d 30 31 E-SWH375 0-10H-01
0030 00 02 00 11 00 00 00 01 01 01 cc 00 04 0a 01 0a ..... .....
0040 0e 00 03 00 16 46 61 73 74 45 74 68 65 72 6e 65 .....Fas tEtherne
0050 74 31 2f 30 2f 32 31 00 04 00 08 00 00 00 28 00 t1/0/21. .....(.
0060 05 00 dc 43 69 73 63 6f 20 49 6e 74 65 72 6e 65 ...Cisco Interne
0070 74 77 6f 72 6b 20 4f 70 65 72 61 74 69 6e 67 20 twork Op erating
0080 53 79 73 74 65 6d 20 53 6f 66 74 77 61 72 65 20 System S oftware
0090 0a 49 4f 53 20 28 74 6d 29 20 43 33 37 35 30 20 .IOS (tm ) C3750
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... Packets: 51 Displayed: 51 Marked: 0 Dropped: 0 Profile: Default

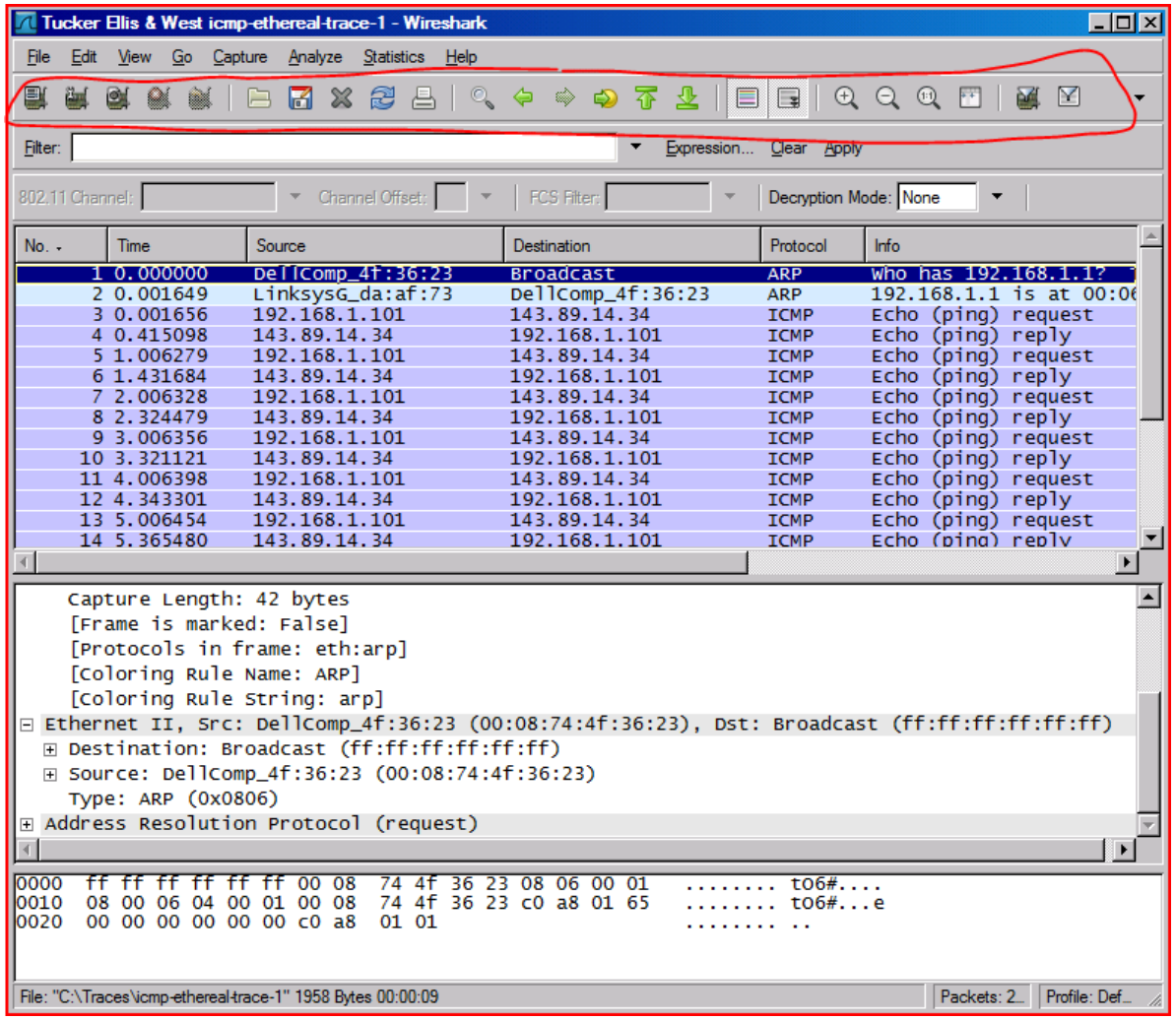
# Janela HEX


Tucker Ellis & West aaa.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
2 0.746308 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
3 0.751270 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
4 9.318731 Silicom_01:6e:bd Broadcast ARP who has 192.168.1.1? Tell 19
5 0.000664 Castlene_00:34:56 Silicom_01:6e:bd ARP 192.168.1.1 is at 00:30:54:00
6 0.000026 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
7 0.995383 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
8 2.003039 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
9 0.169652 192.168.1.1 192.168.1.2 DNS Standard query response A 212
10 1.006246 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
11 0.996899 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
12 2.003024 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
13 0.992343 Castlene_00:34:56 Silicom_01:6e:bd ARP who has 192.168.1.2? Tell 19
14 0.000049 Silicom_01:6e:bd Castlene_00:34:56 ARP 192.168.1.2 is at 00:e0:ed:01
15 1.010378 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
16 4.005777 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
17 8.002019 192.168.1.2 192.168.1.1 DNS Standard query PTR 1.0.0.127.
18 0.001489 192.168.1.1 192.168.1.2 DNS Standard query response PTR l
19 0.001640 192.168.1.2 212.242.33.35 SIP Request: REGISTER sip:sip.cyb
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 78
Identification: 0x698c (27020)
Flags: 0x00
Highlighted packets here
0000 ff ff ff ff ff ff 00 e0 ed 01 6e bd 08 00 45 00 ..... ..n...E.
0010 00 4e 69 8c 00 00 80 11 4c c1 c0 a8 01 02 c0 a8 .Ni..... L.....
0020 01 ff 00 89 00 89 00 3a 5b b4 84 e7 01 10 00 01 ..... [.....
0030 00 00 00 00 00 00 20 45 46 45 44 45 4a 46 50 45 ..... E FEDEJFPE
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43 EEPENEBE JEOCACAC
0050 41 43 41 43 41 42 4d 00 00 20 00 01 ACACABM. . ..
Are shown here as well
Identification (ip.id), 2 bytes
Packets: 691 Displayed: 691 Marked: 0
Profile: Default

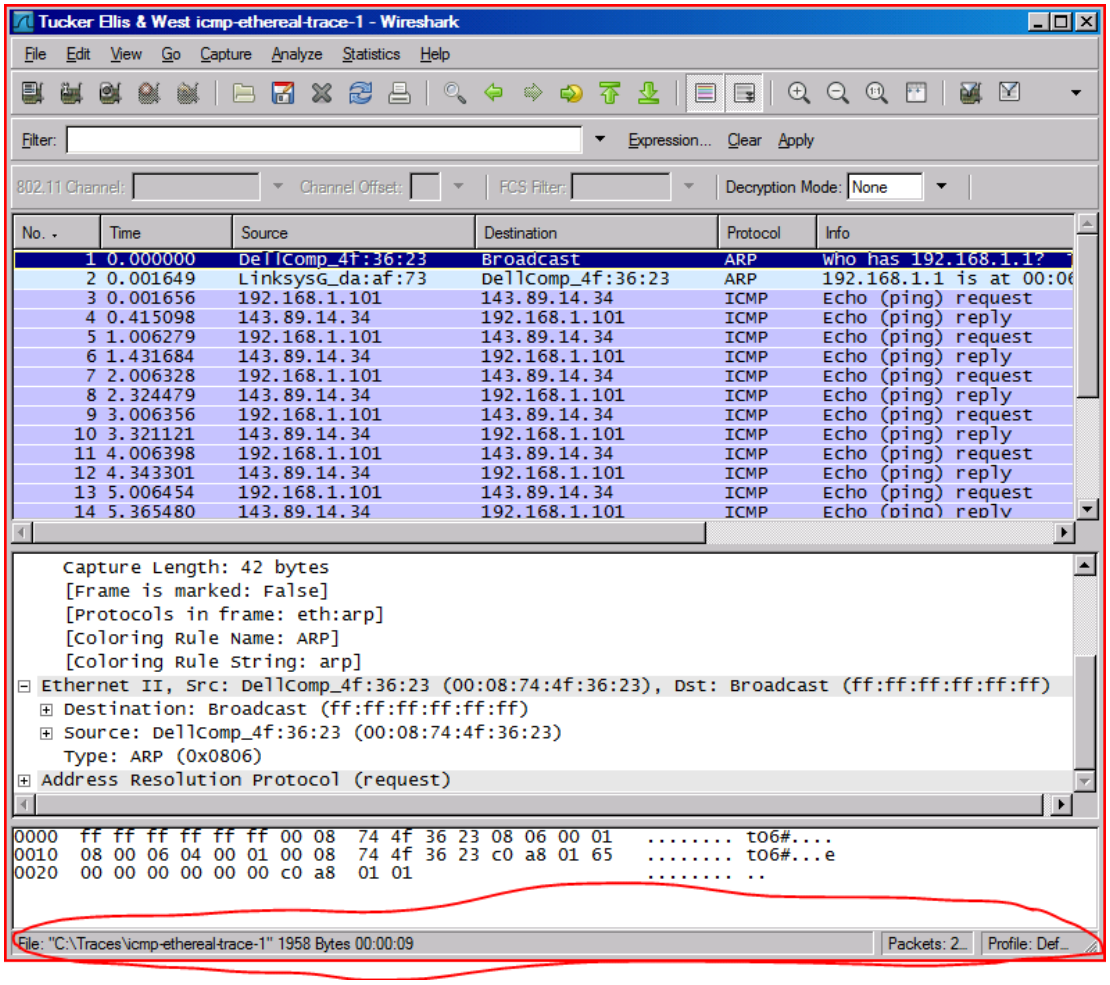
# Menu


Tucker Ellis & West icmp-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None
No. Time Source Destination Protocol Info
1 0.000000 DellComp_4f:36:23 Broadcast ARP Who has 192.168.1.1?
2 0.001649 LinksysG_da:af:73 DellComp_4f:36:23 ARP 192.168.1.1 is at 00:0
3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
5 1.006279 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
6 1.431684 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
7 2.006328 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
8 2.324479 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
9 3.006356 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
10 3.321121 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
11 4.006398 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
12 4.343301 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
13 5.006454 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
14 5.365480 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
Capture Length: 42 bytes
[Frame is marked: False]
[Protocols in frame: eth:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: DellComp_4f:36:23 (00:08:74:4f:36:23)
Type: ARP (0x0806)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 08 74 4f 36 23 08 06 00 01 ........ tO6#....
0010 08 00 06 04 00 01 00 08 74 4f 36 23 c0 a8 01 65 ........ tO6#...e
0020 00 00 00 00 00 00 c0 a8 01 01 ........ ..
File: "C:\Traces\icmp-ethereal-trace-1" 1958 Bytes 00:00:09
Packets: 2...
Profile: Def...

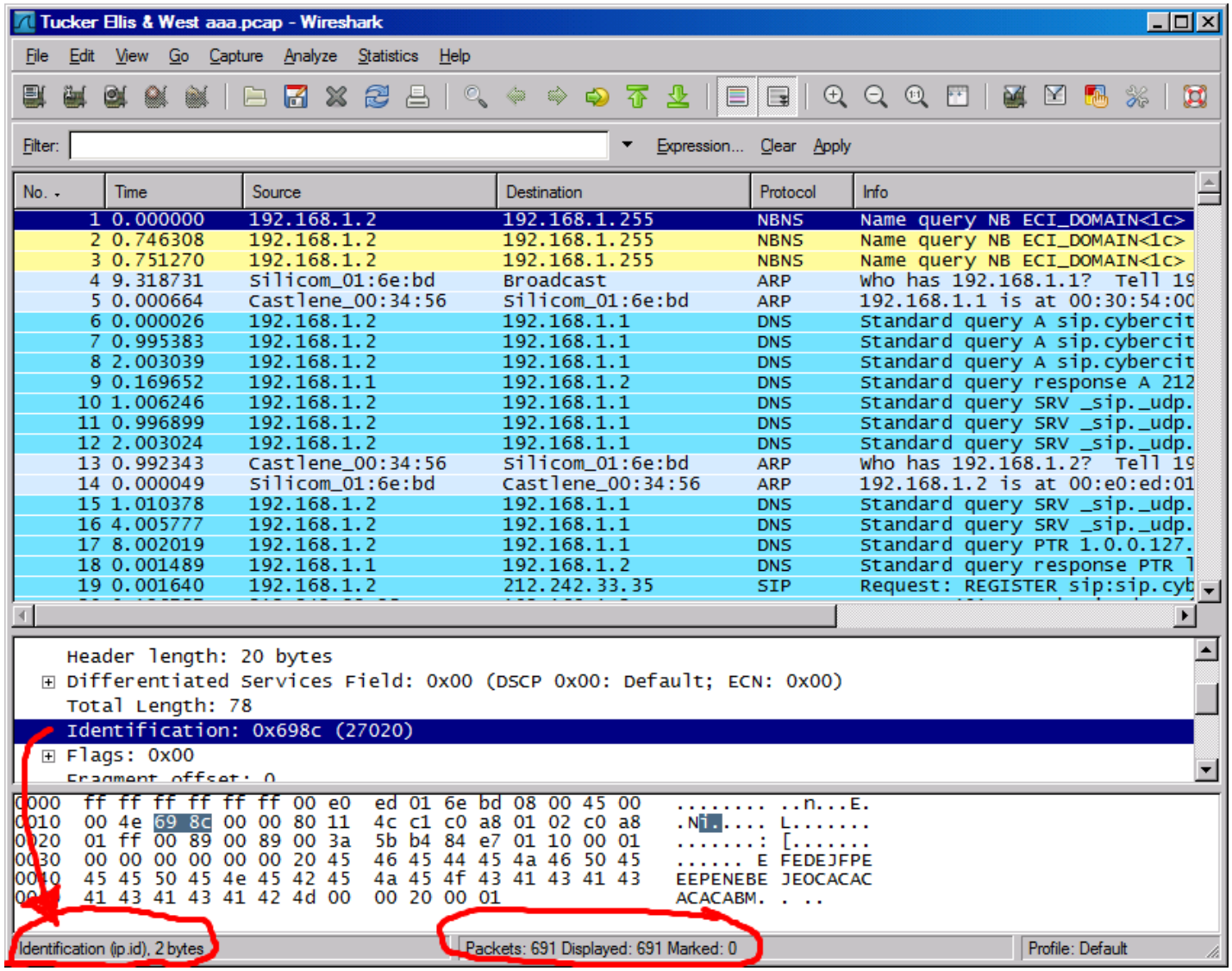
# Barra de Buttons



# Status Bar

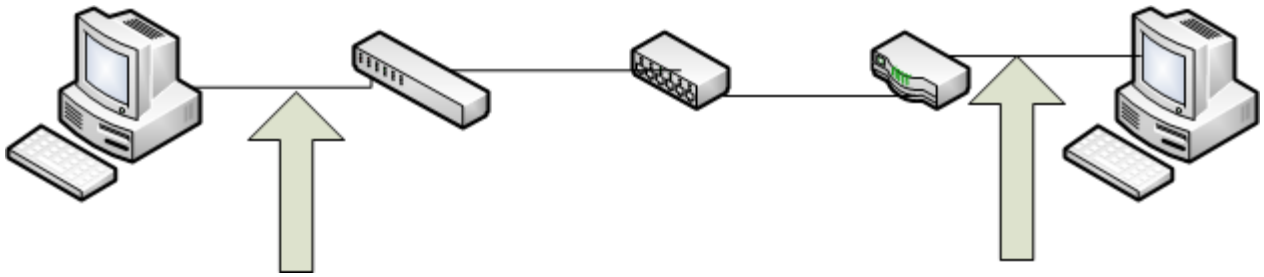

Tucker Ellis & West icmp-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None
No. Time Source Destination Protocol Info
1 0.000000 DellComp_4f:36:23 Broadcast ARP Who has 192.168.1.1?
2 0.001649 LinksysG_da:af:73 DellComp_4f:36:23 ARP 192.168.1.1 is at 00:06
3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
5 1.006279 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
6 1.431684 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
7 2.006328 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
8 2.324479 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
9 3.006356 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
10 3.321121 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
11 4.006398 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
12 4.343301 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
13 5.006454 192.168.1.101 143.89.14.34 ICMP Echo (ping) request
14 5.365480 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
Capture Length: 42 bytes
[Frame is marked: False]
[Protocols in frame: eth:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: DellComp_4f:36:23 (00:08:74:4f:36:23)
Type: ARP (0x0806)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 08 74 4f 36 23 08 06 00 01 ........ to6#....
0010 08 00 06 04 00 01 00 08 74 4f 36 23 c0 a8 01 65 ........ to6#...e
0020 00 00 00 00 00 00 c0 a8 01 01 ........ ..
File: "C:\Traces\icmp-ethereal-trace-1" 1958 Bytes 00:00:09
Packets: 2...
Profile: Def...

# Status Bar

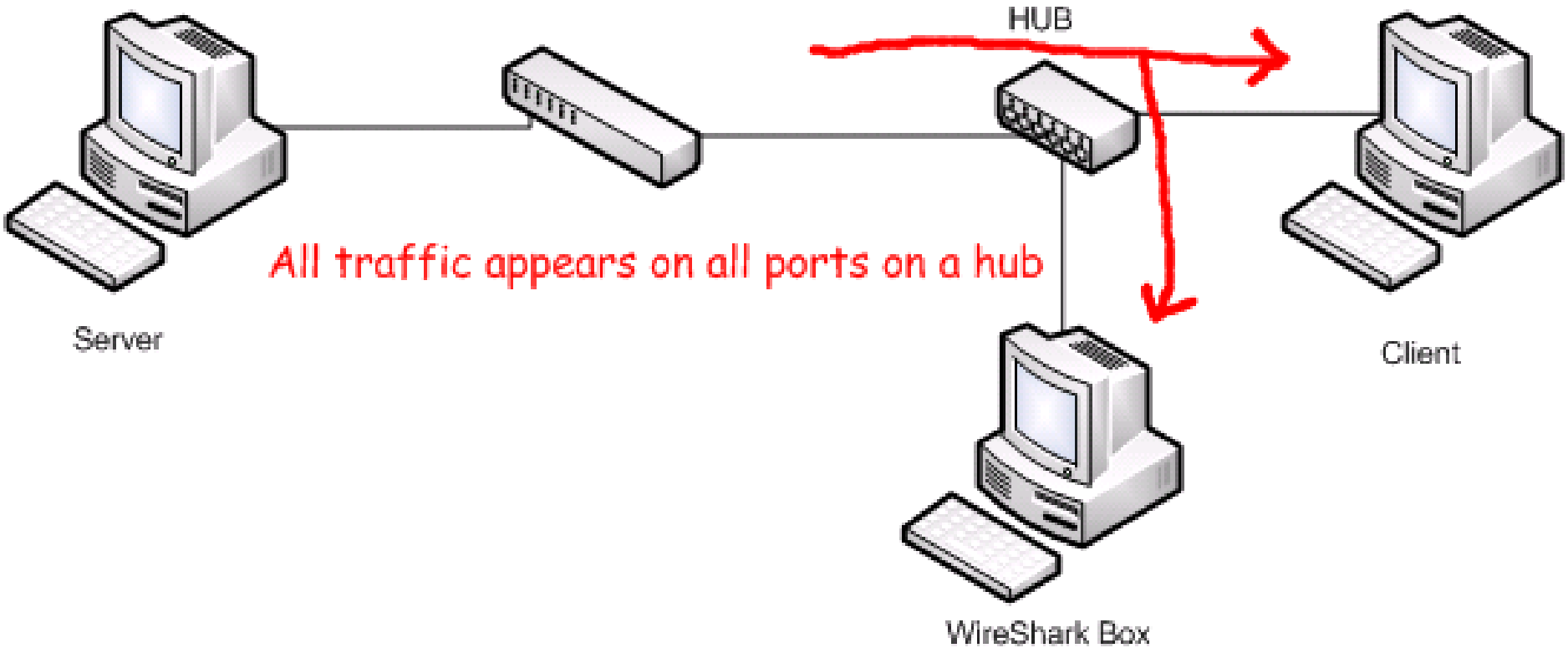

Tucker Ellis & West aaa.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
2 0.746308 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
3 0.751270 192.168.1.2 192.168.1.255 NBNS Name query NB ECI_DOMAIN<1c>
4 9.318731 Silicom_01:6e:bd Broadcast ARP Who has 192.168.1.1? Tell 19
5 0.000664 Castlene_00:34:56 Silicom_01:6e:bd ARP 192.168.1.1 is at 00:30:54:00
6 0.000026 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
7 0.995383 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
8 2.003039 192.168.1.2 192.168.1.1 DNS Standard query A sip.cybercit
9 0.169652 192.168.1.1 192.168.1.2 DNS Standard query response A 212
10 1.006246 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
11 0.996899 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
12 2.003024 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
13 0.992343 Castlene_00:34:56 Silicom_01:6e:bd ARP Who has 192.168.1.2? Tell 19
14 0.000049 Silicom_01:6e:bd Castlene_00:34:56 ARP 192.168.1.2 is at 00:e0:ed:01
15 1.010378 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
16 4.005777 192.168.1.2 192.168.1.1 DNS Standard query SRV _sip._udp.
17 8.002019 192.168.1.2 192.168.1.1 DNS Standard query PTR 1.0.0.127.
18 0.001489 192.168.1.1 192.168.1.2 DNS Standard query response PTR l
19 0.001640 192.168.1.2 212.242.33.35 SIP Request: REGISTER sip:sip.cyb
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 78
Identification: 0x698c (27020)
Flags: 0x00
0000 ff ff ff ff ff ff 00 e0 ed 01 6e bd 08 00 45 00 ..... ..n...E.
0010 00 4e 69 8c 00 00 80 11 4c c1 c0 a8 01 02 c0 a8 .Ni..... L.....
0020 01 ff 00 89 00 89 00 3a 5b b4 84 e7 01 10 00 01 ..... : [.....
0030 00 00 00 00 00 00 20 45 46 45 44 45 4a 46 50 45 ..... E FEDEJFPE
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43 EEPENEBE JEOCACAC
0050 41 43 41 43 41 42 4d 00 00 20 00 01 ACACABM. . ..
Identification (ip.id), 2 bytes
Packets: 691 Displayed: 691 Marked: 0
Profile: Default

# Onde eu devo usar o WireShark?

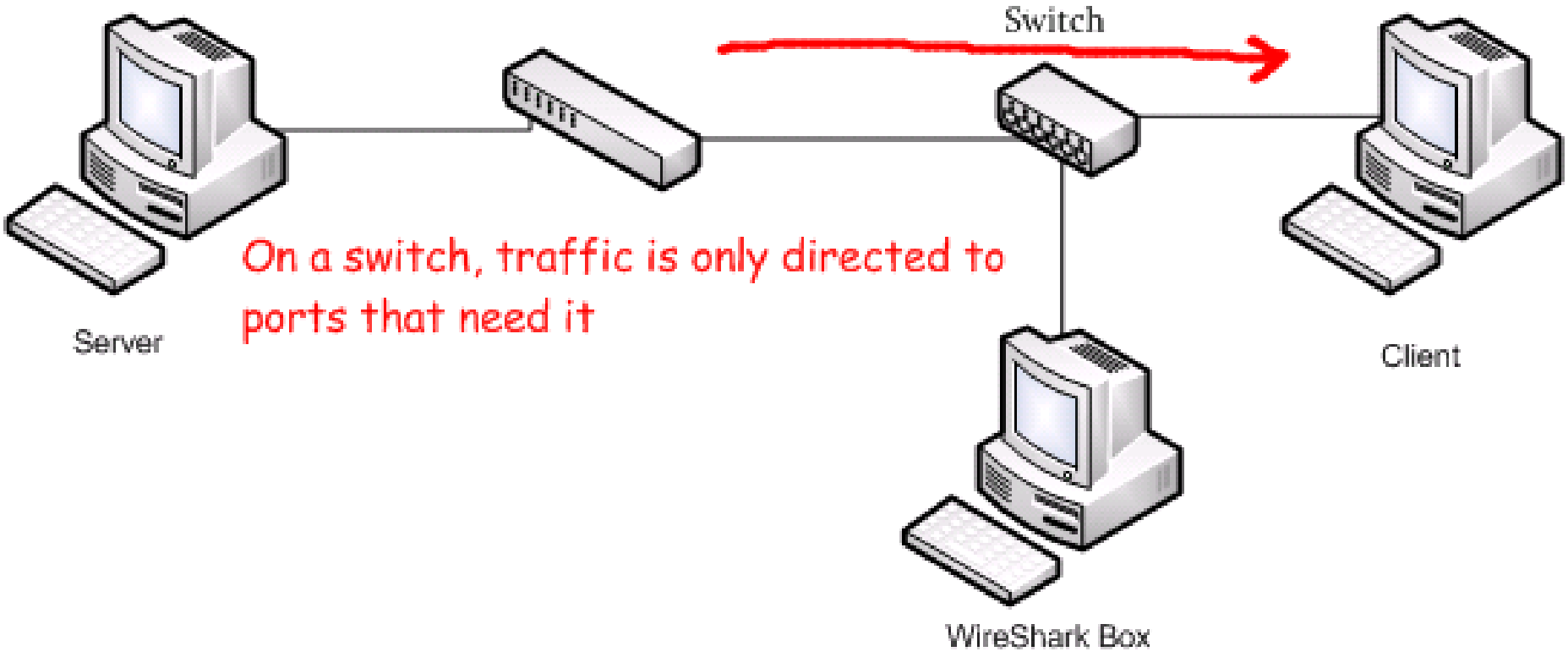
# A localização muda TUDO !



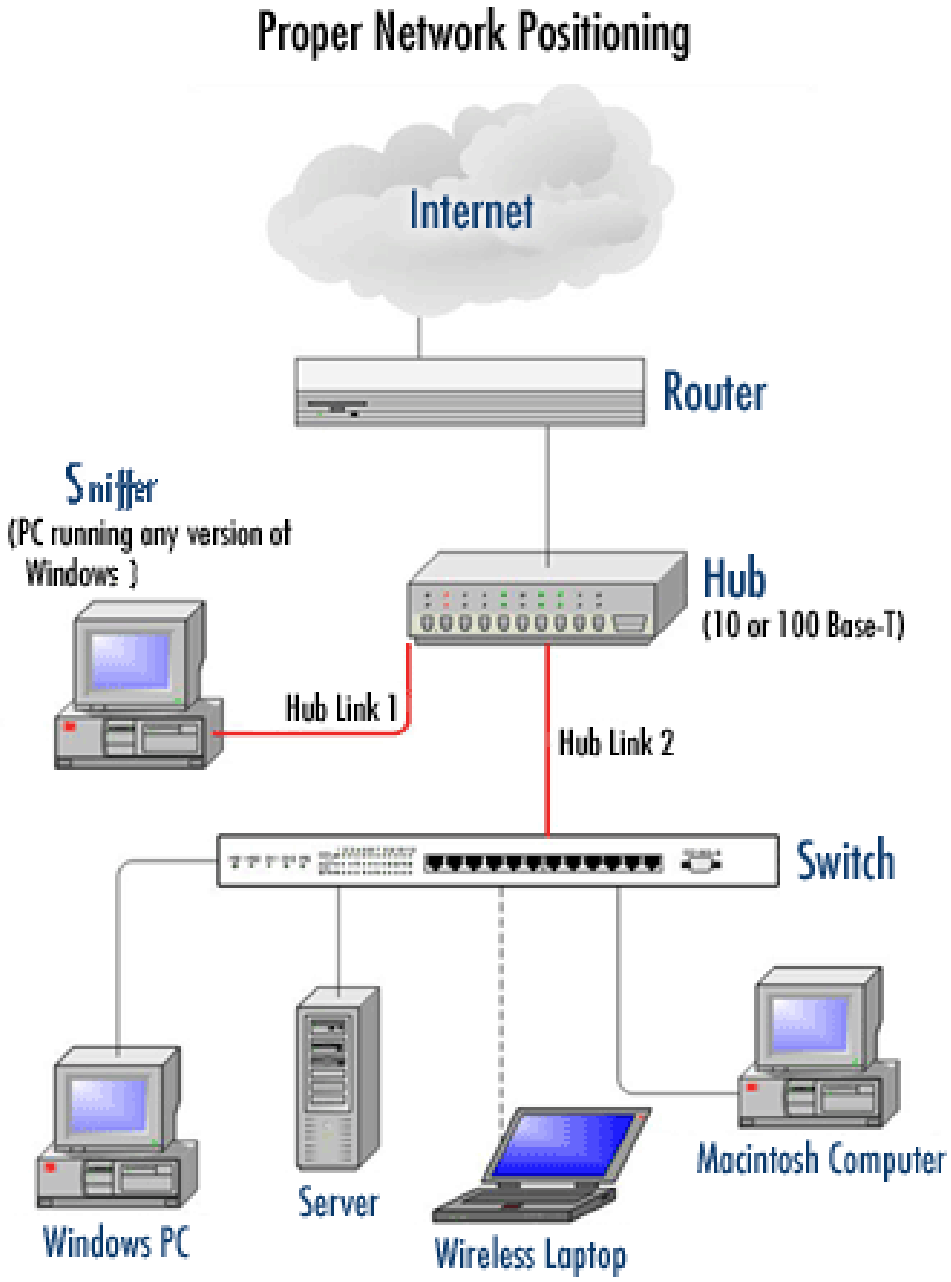
# Hub


HUB
All traffic appears on all ports on a hub
Server
Client
WireShark Box

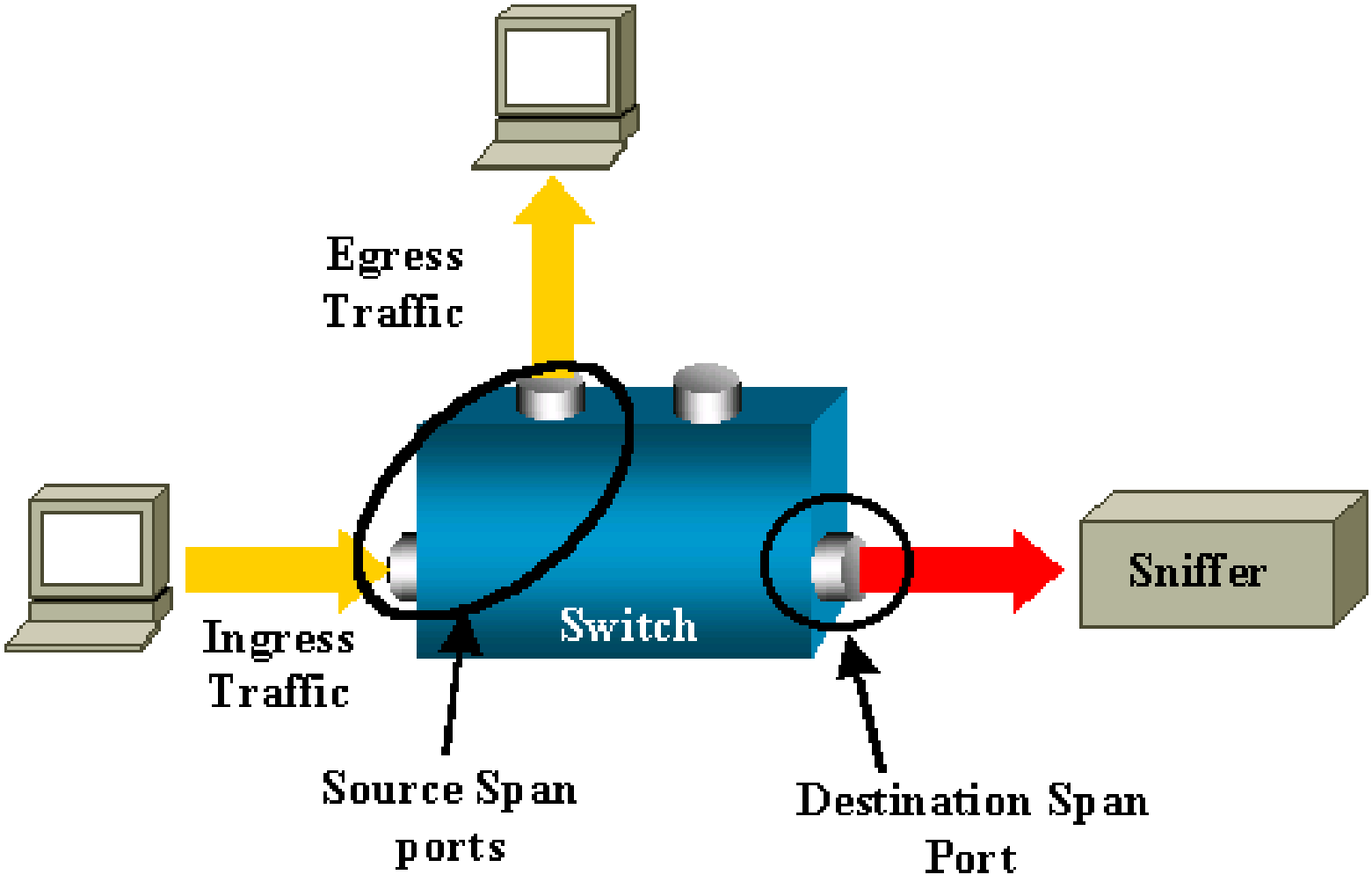
# Switches


Switch
Server
On a switch, traffic is only directed to ports that need it
Client
WireShark Box

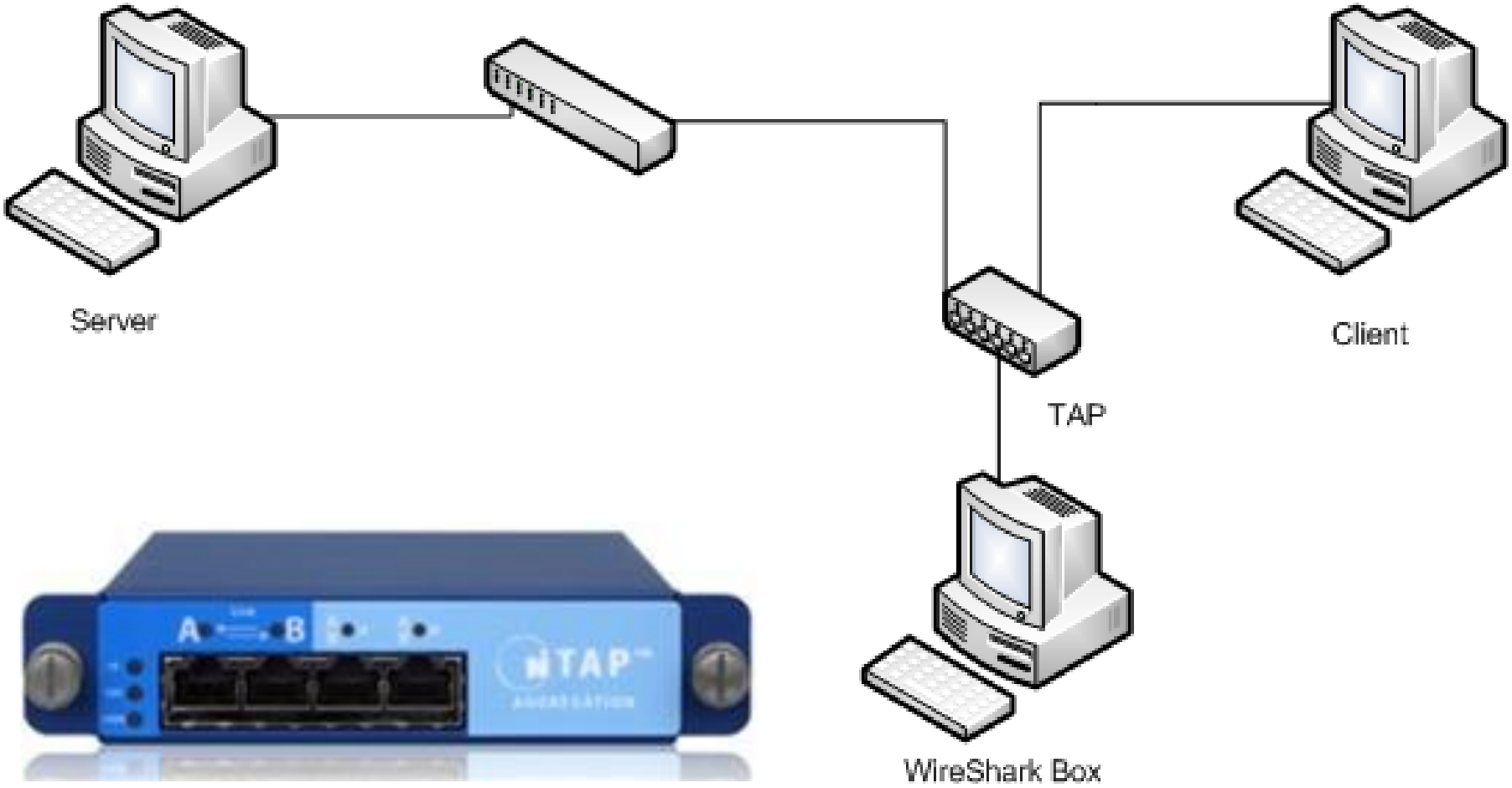
# Não é o ideal, mas funciona



# Switch com porta SPAN



# TAP



# Switch em modo SPAN

interface FastEthernet0/1

port monitor FastEthernet0/2

# Cisco - Exemplo

✓Espelhando as portas 1, 2 e 3 para a porta 10:

switch#config t  //entrar no modo de configuração//

•Enter configuration commands, one per line.  End with CNTL/Z.

•switch(config)#  **interface fastEthernet 0/10 //**entrar  no modo de configuração da interface onde os dados serão coletados//

•switch(config-if)#**port monitor FastEthernet 0/1**  //especificar a porta que será espelhada//

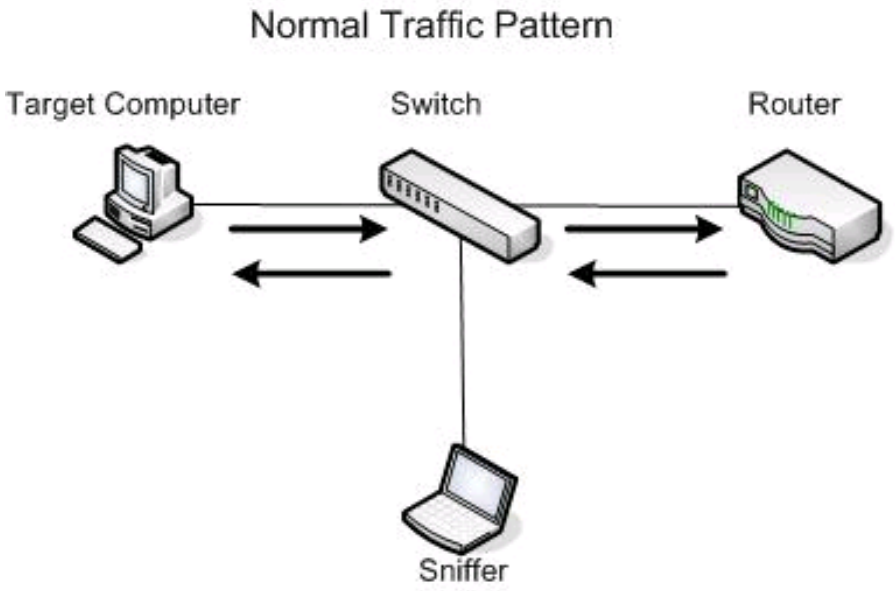
•switch(config-if)#**port monitor FastEthernet 0/2** //especificar a porta que será espelhada//

•switch(config-if)#**port monitor FastEthernet 0/3** //especificar a porta que será espelhada//

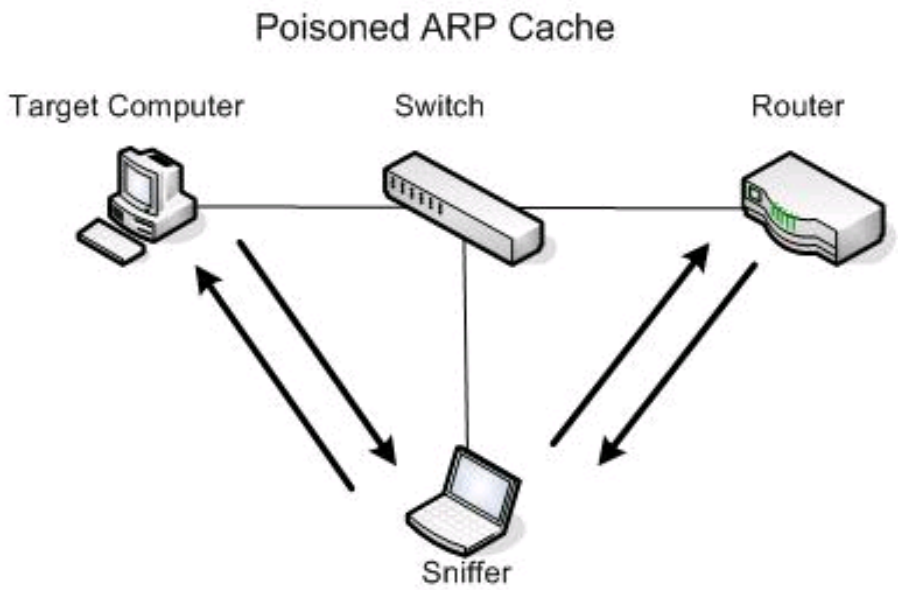
•switch(config-if)#**exit**

•switch(config)#**exit**

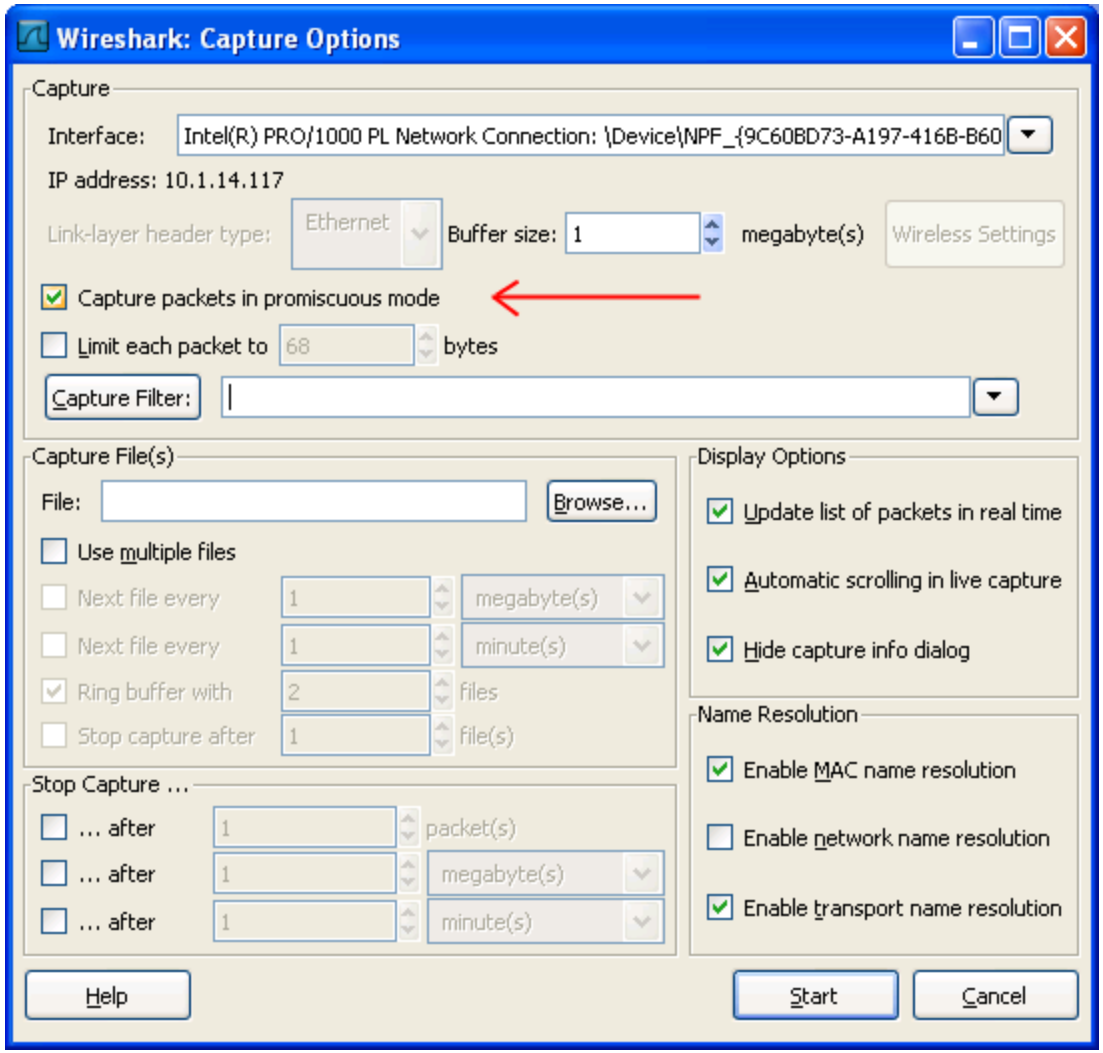
# ARP Cache Poisoning





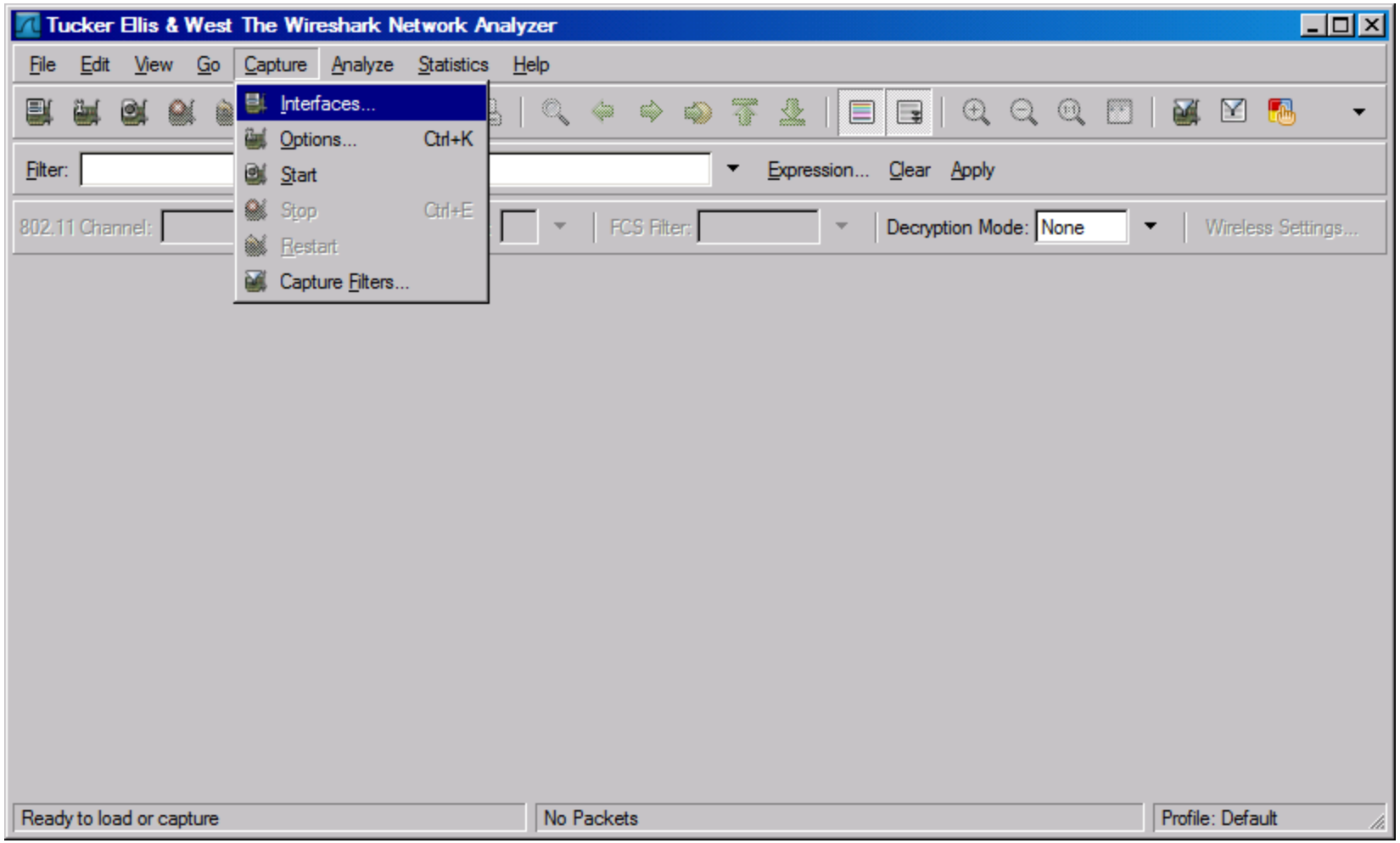


# Promiscuous Mode

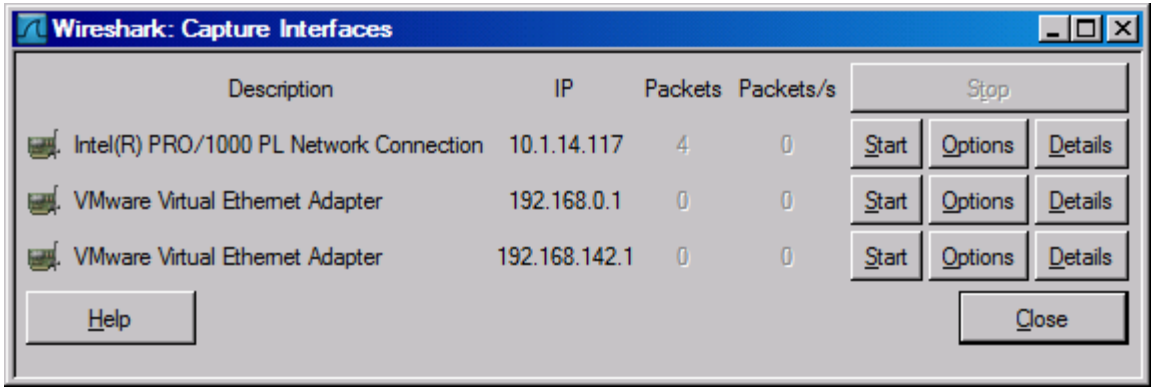



Marcando este box, estamos determinando que a interface escolhida fique em MODO PROMÍSCUO durante a captura. Se isso não for feito, o Wireshark apenas capturará quadros broadcast e os que saem e entram na máquina onde está o sniffer.

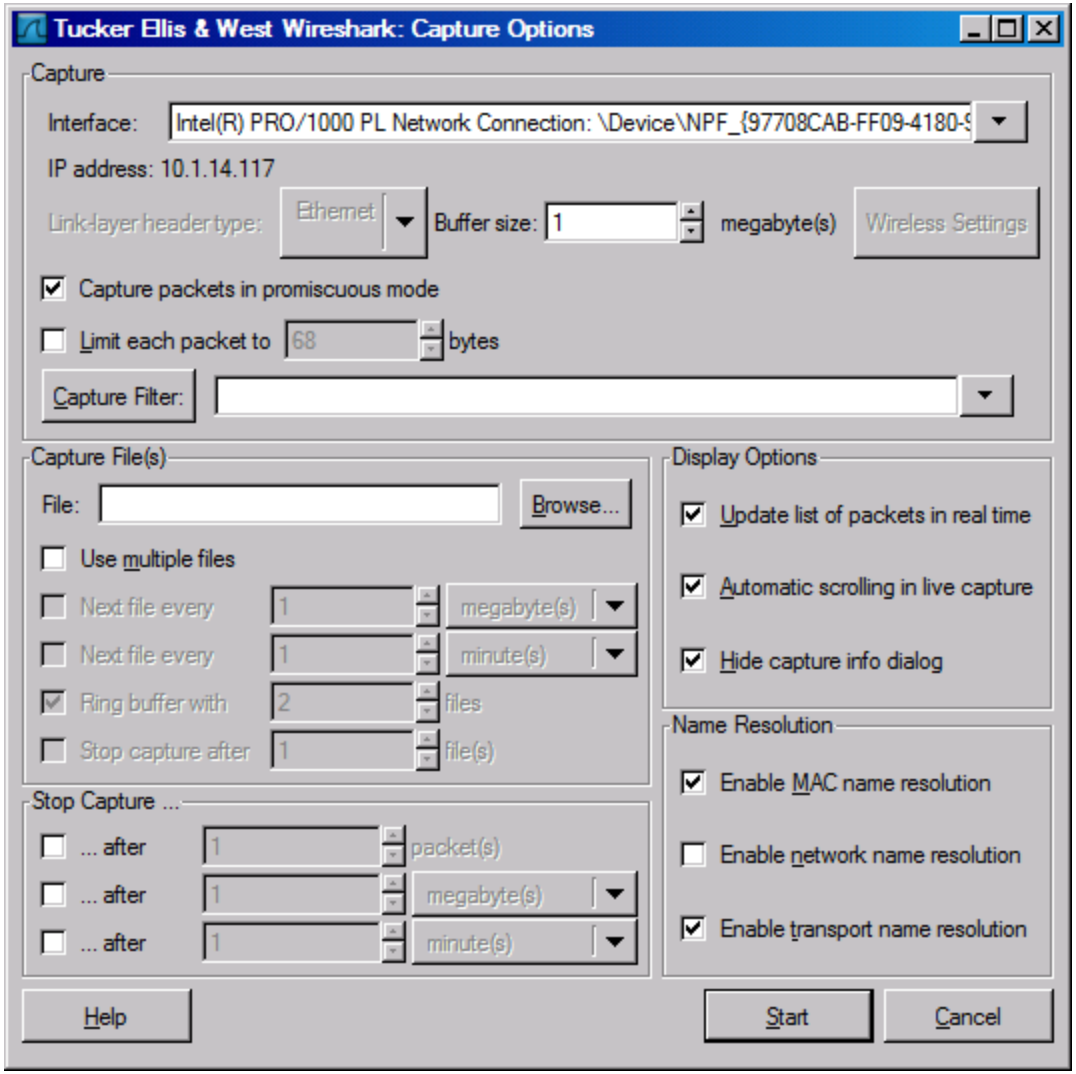
# Captura Simples



# Escolha da Interface



# Opções de Captura



# Filtragem de Tráfego

# Exemplos de Filtros

host 10.1.11.24

host 192.168.0.1 and host 10.1.11.1

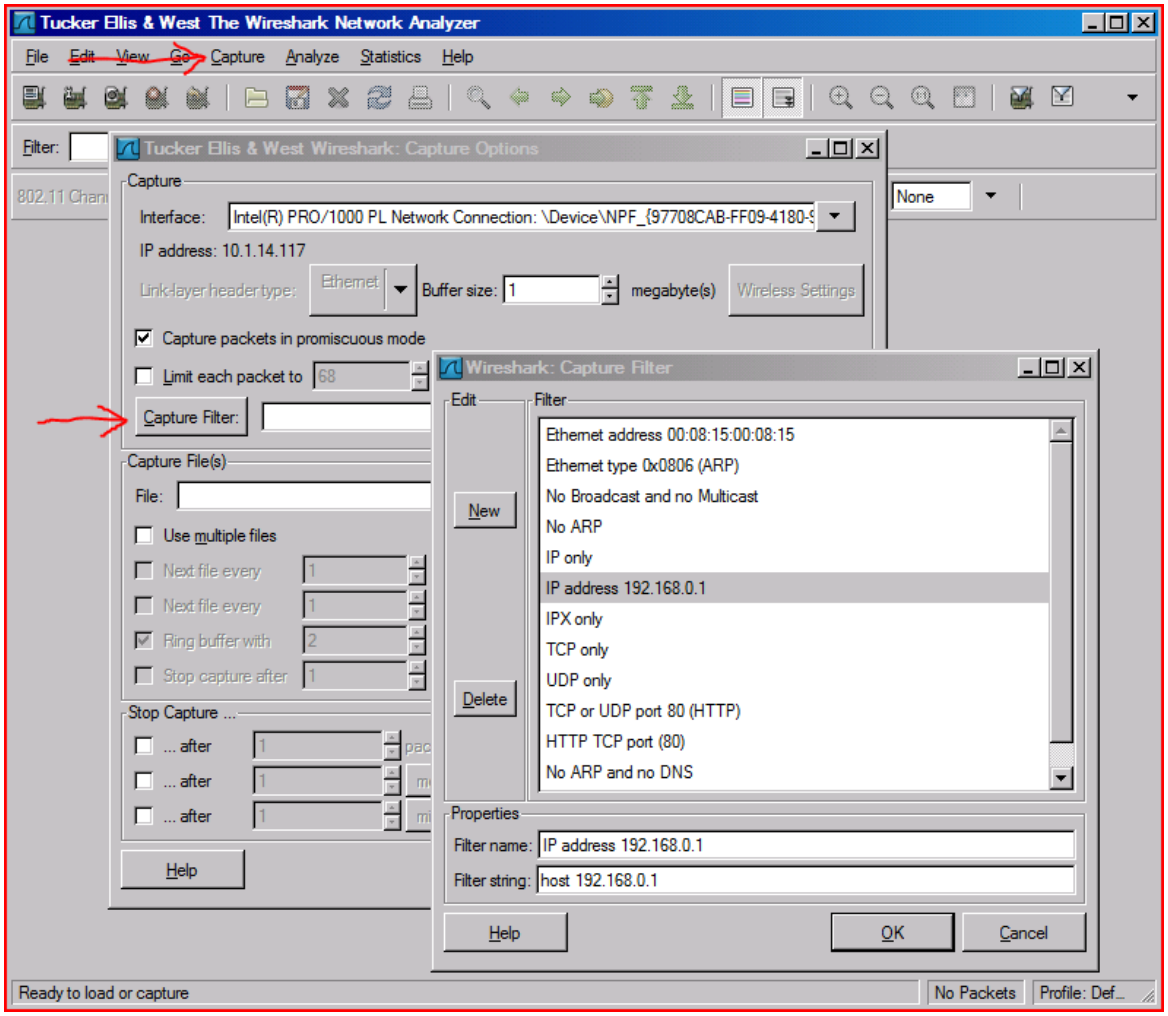
tcp port http

ip

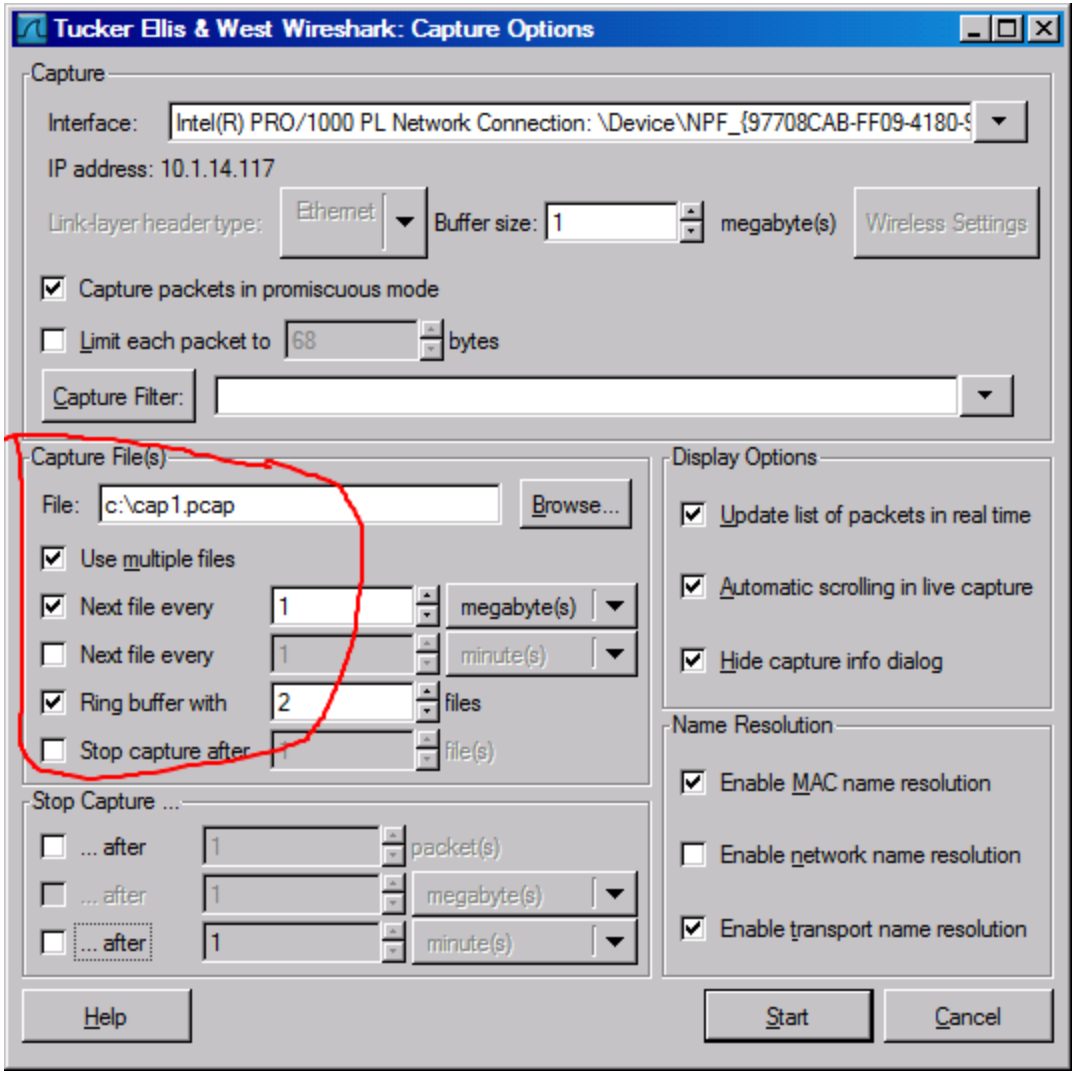
not broadcast not multicast

ether host 00:04:13:00:09:a3

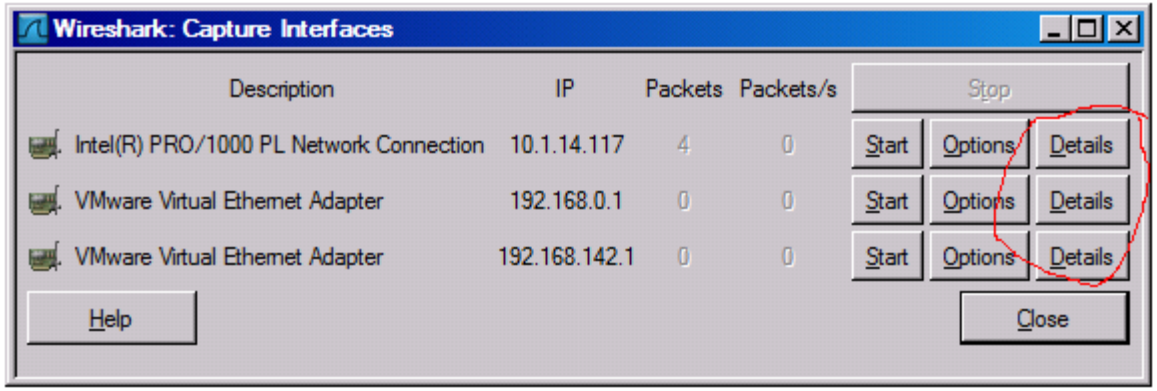
# Capture Filter



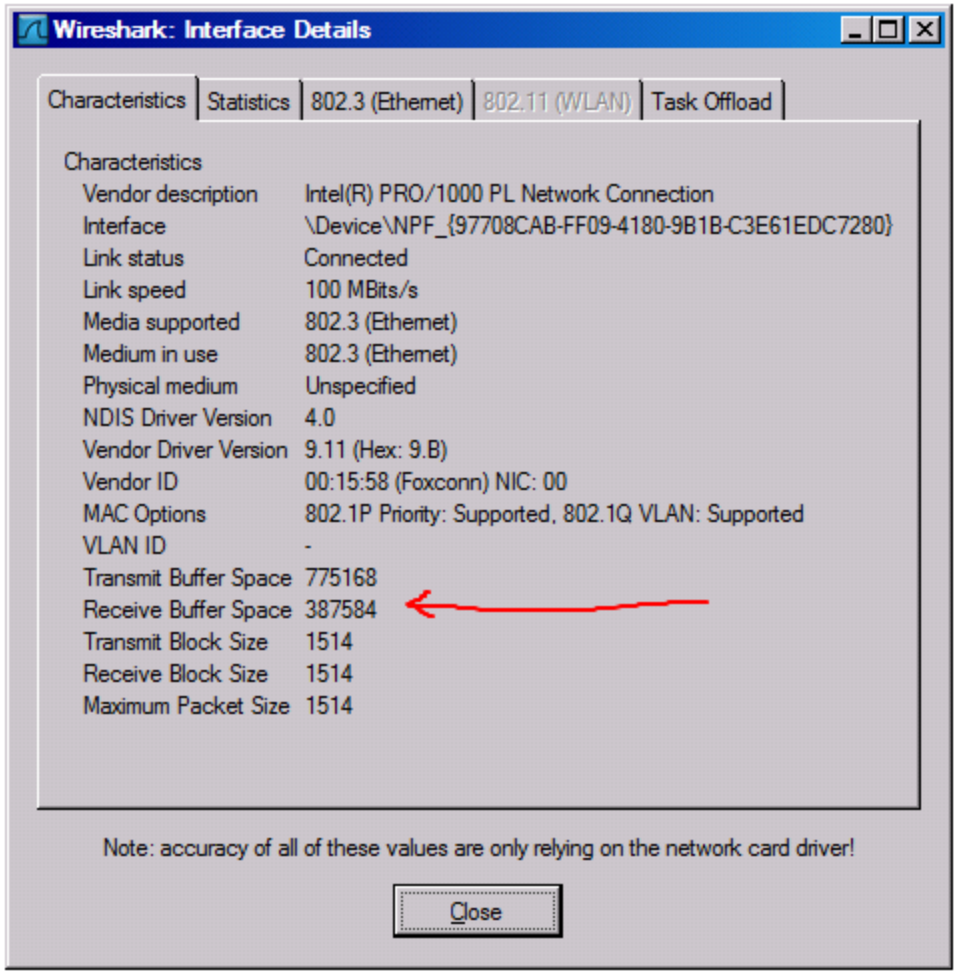
# Capture Options



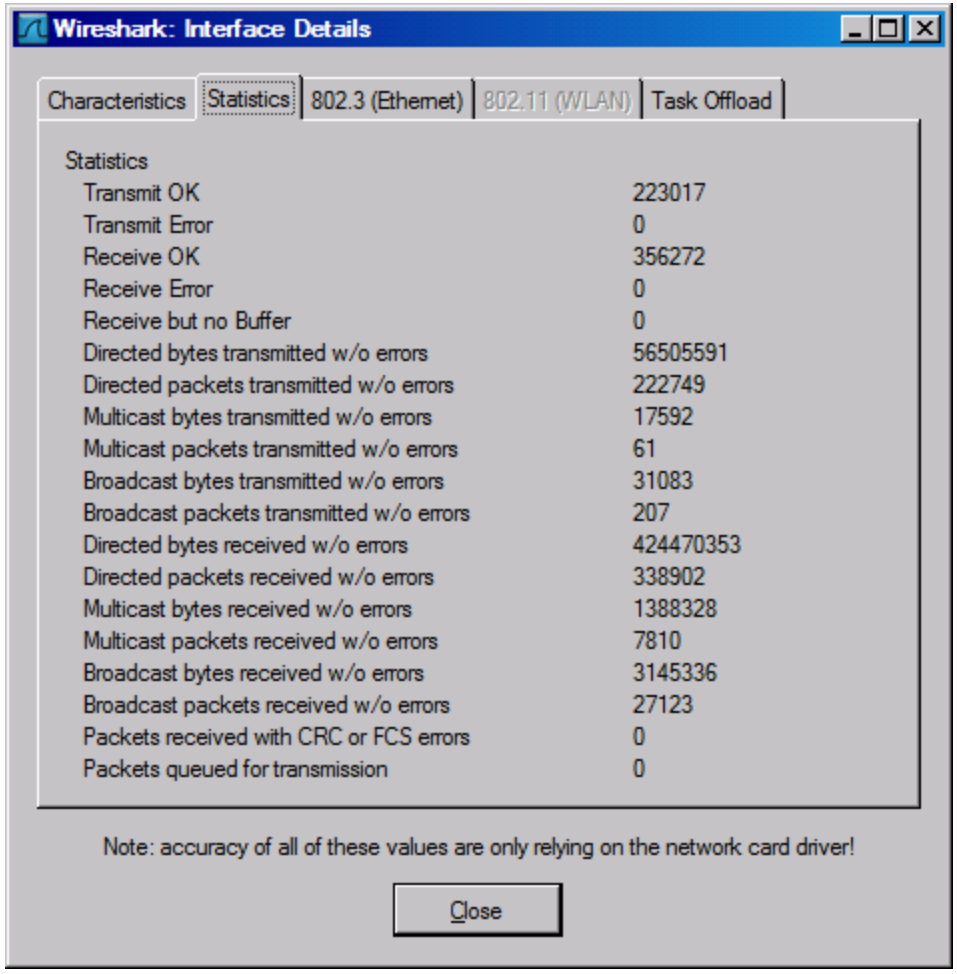
# Capture Interfaces



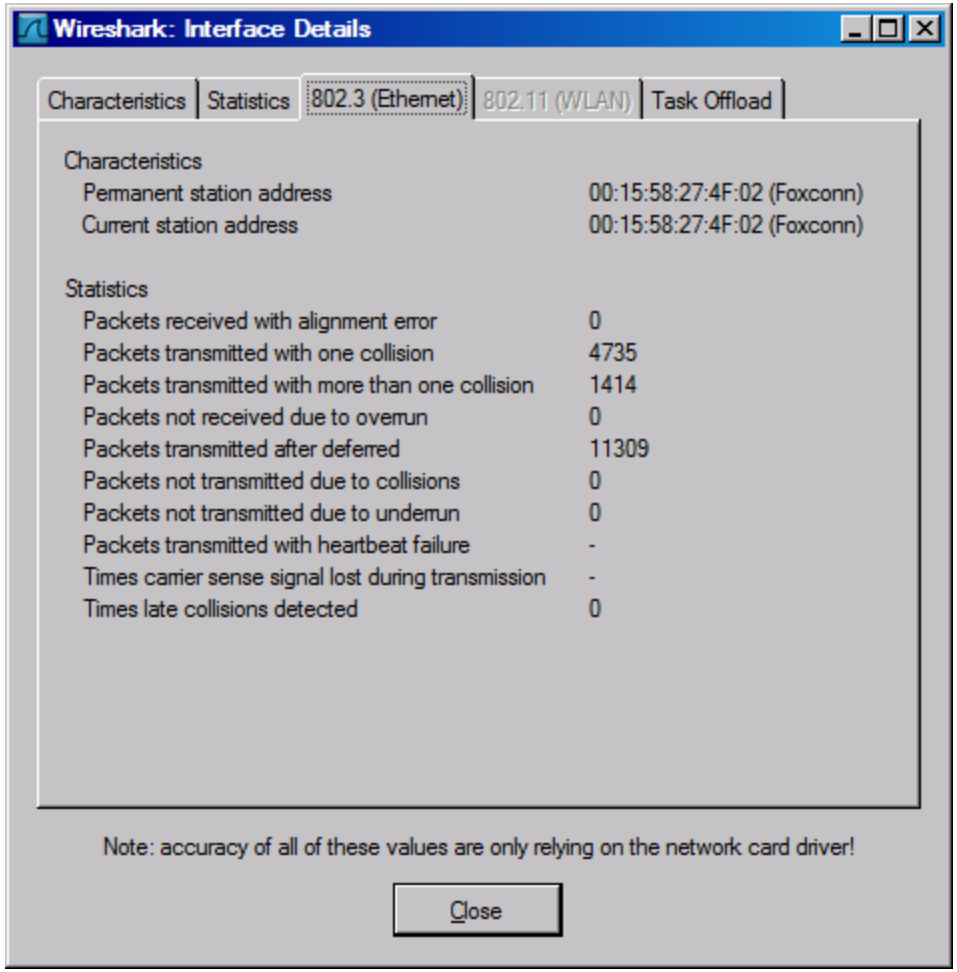
# Interface Details: Characteristics



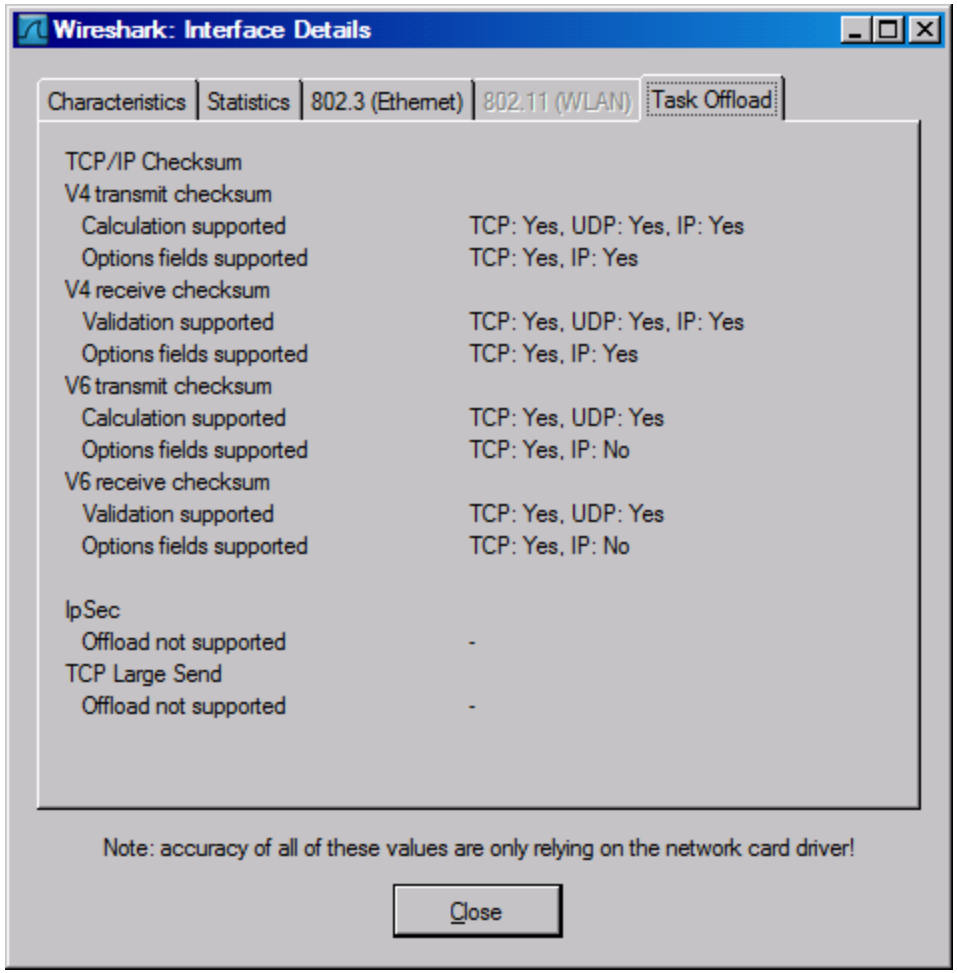
# Interface Details: Statistics



# Interface Details: 802.3 (Ethernet)



# Interface Details: Task Offload



# Checksum

Forma  de verificar a integridade dos dados através do cálculo sobre os dados recebidos e comparação com o **checksum** calculado no momento de seu envio. O IP e o TCP/UDP usam checksum de 16 bits.

# Checksum offload

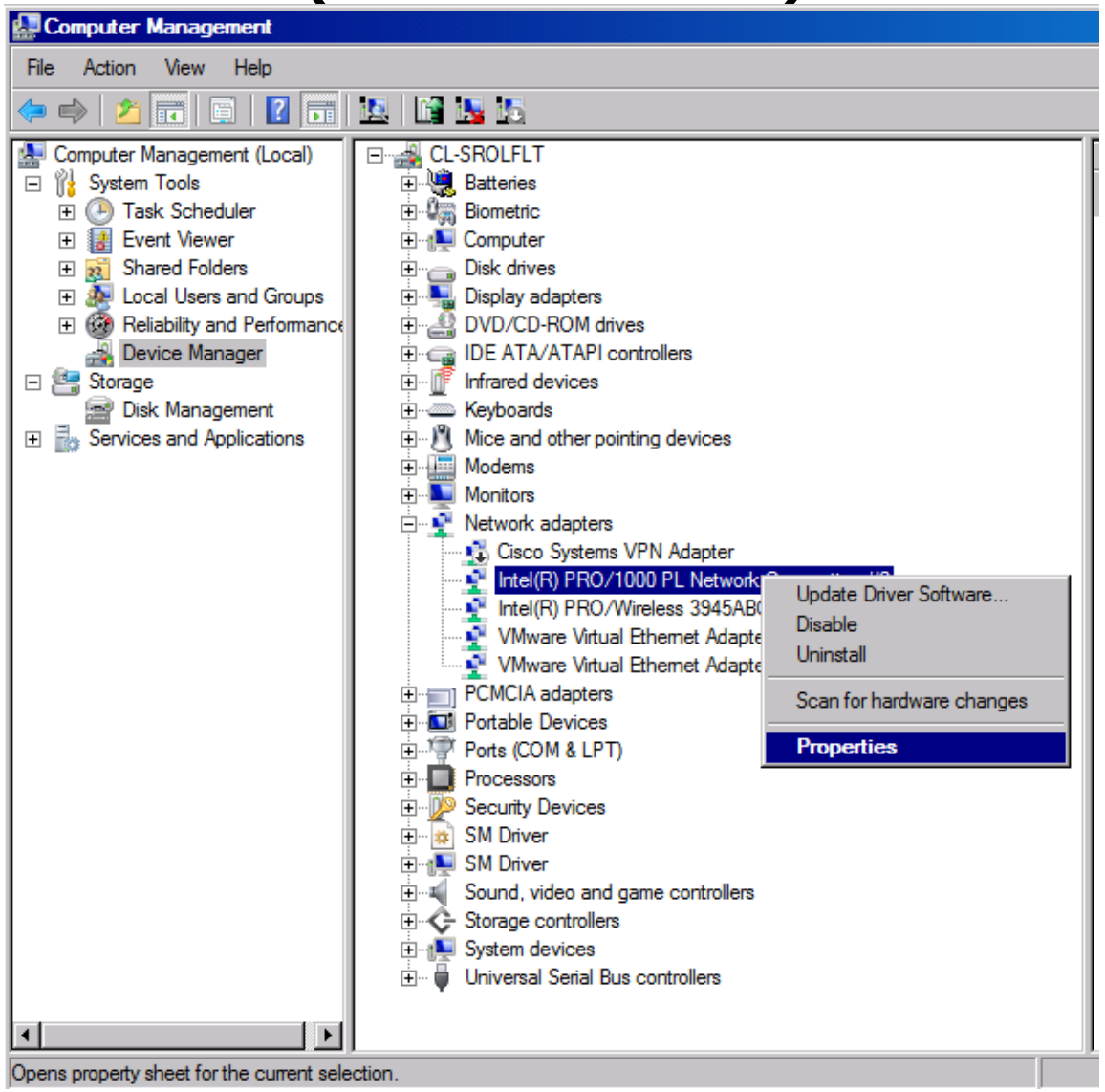
# Turning off Checksum offload

On Linux (as root)
ethtool -K eth0 rx off tx off (choose correct network interface if not eth0)

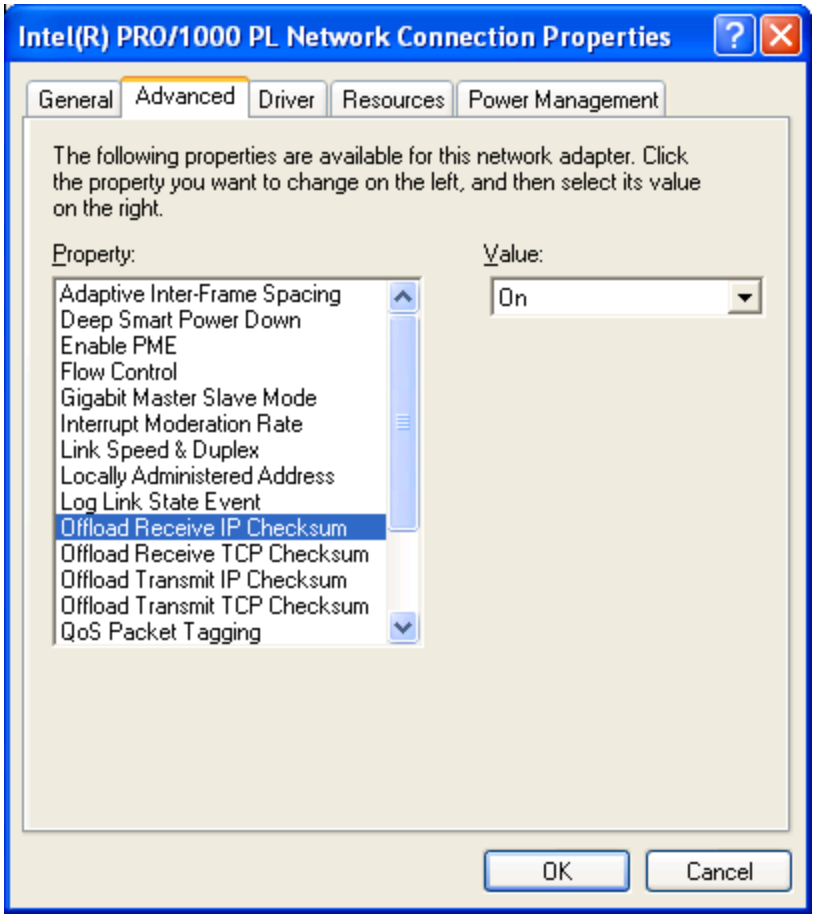
On FreeBSD (as root):
ifconfig em0 -rcxsum -tcxsum (choose correct network interface if not em0)

On MacOS (as root):
sysctl -w net.link.ether.inet.apple_hwcksum_tx=0
sysctl -w net.link.ether.inet.apple_hwcksum_rx=0

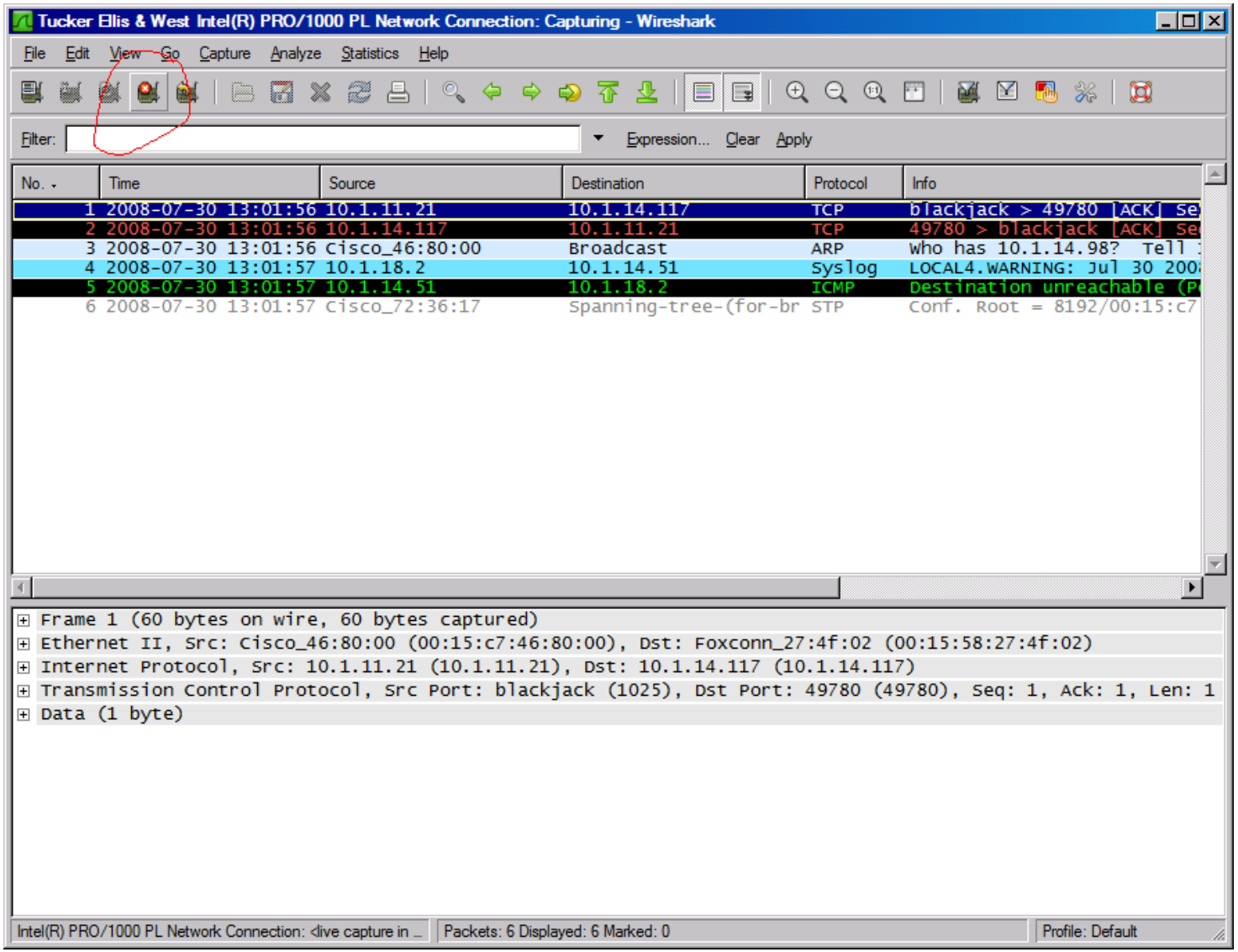
# Turning off Checksum offload (Windows)



# Turning off Checksum offload



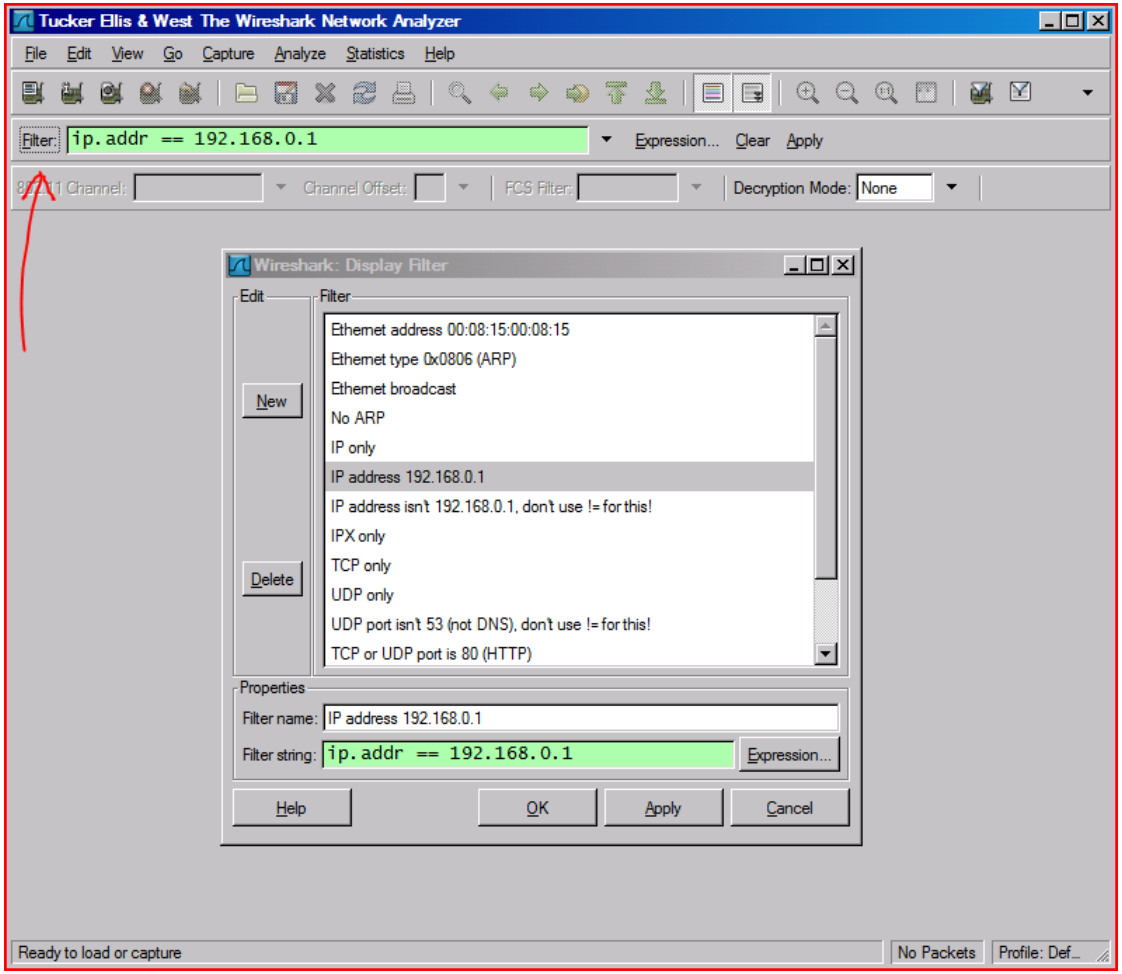
# Interrompendo a Captura



# Display Filters (Post-Filters)

- Display filters (também chamados post-filters, porque opera após a captura) são úteis para diagnóstico inicial.
- Display filters usam uma sintaxe diferente e mais poderosa que a dos filtros de captura.

# Display Filter



# Exemplos de Display Filter

**ip.src==10.1.11.24**

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

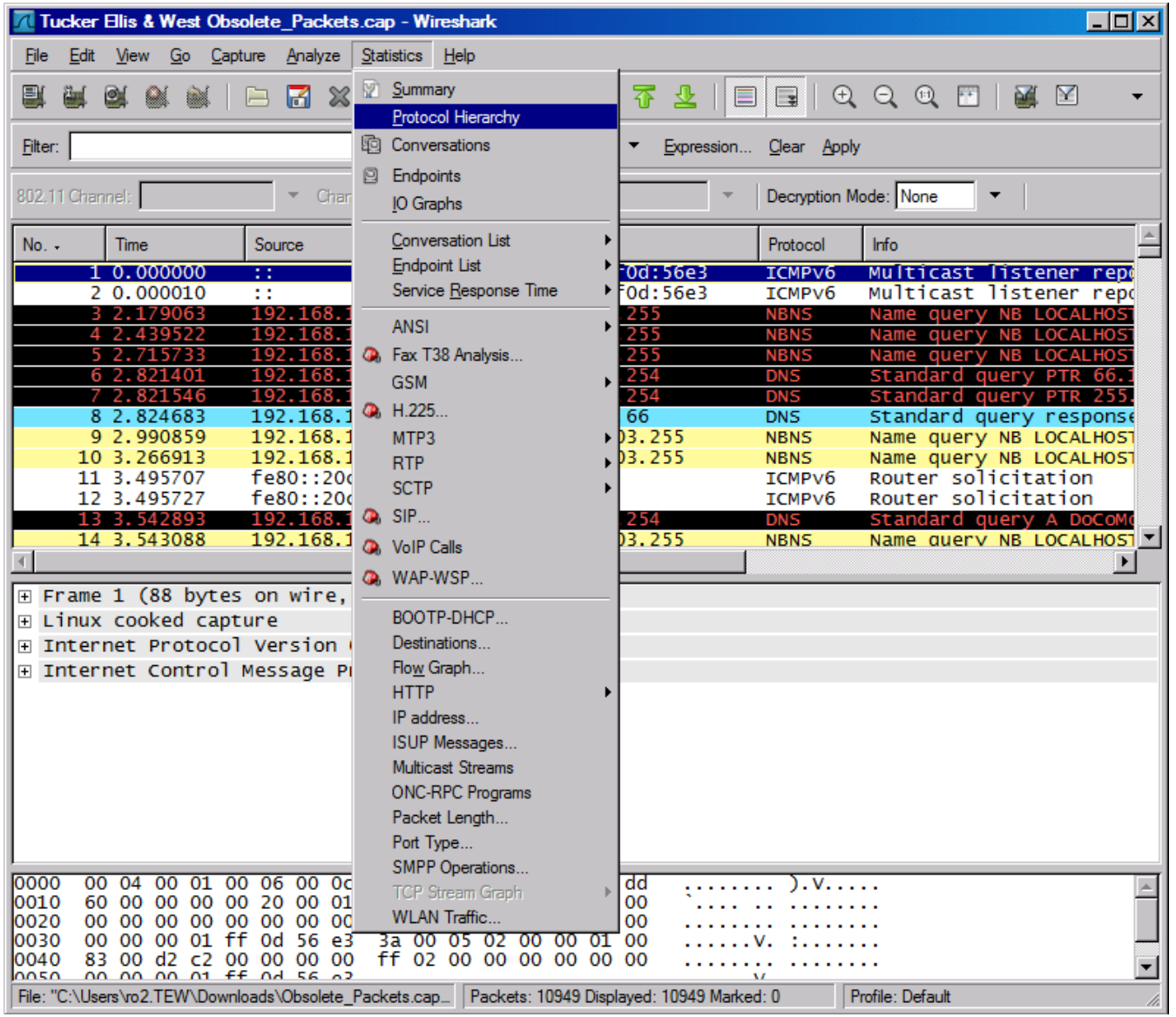
**tcp.port==80 || tcp.port==3389**

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

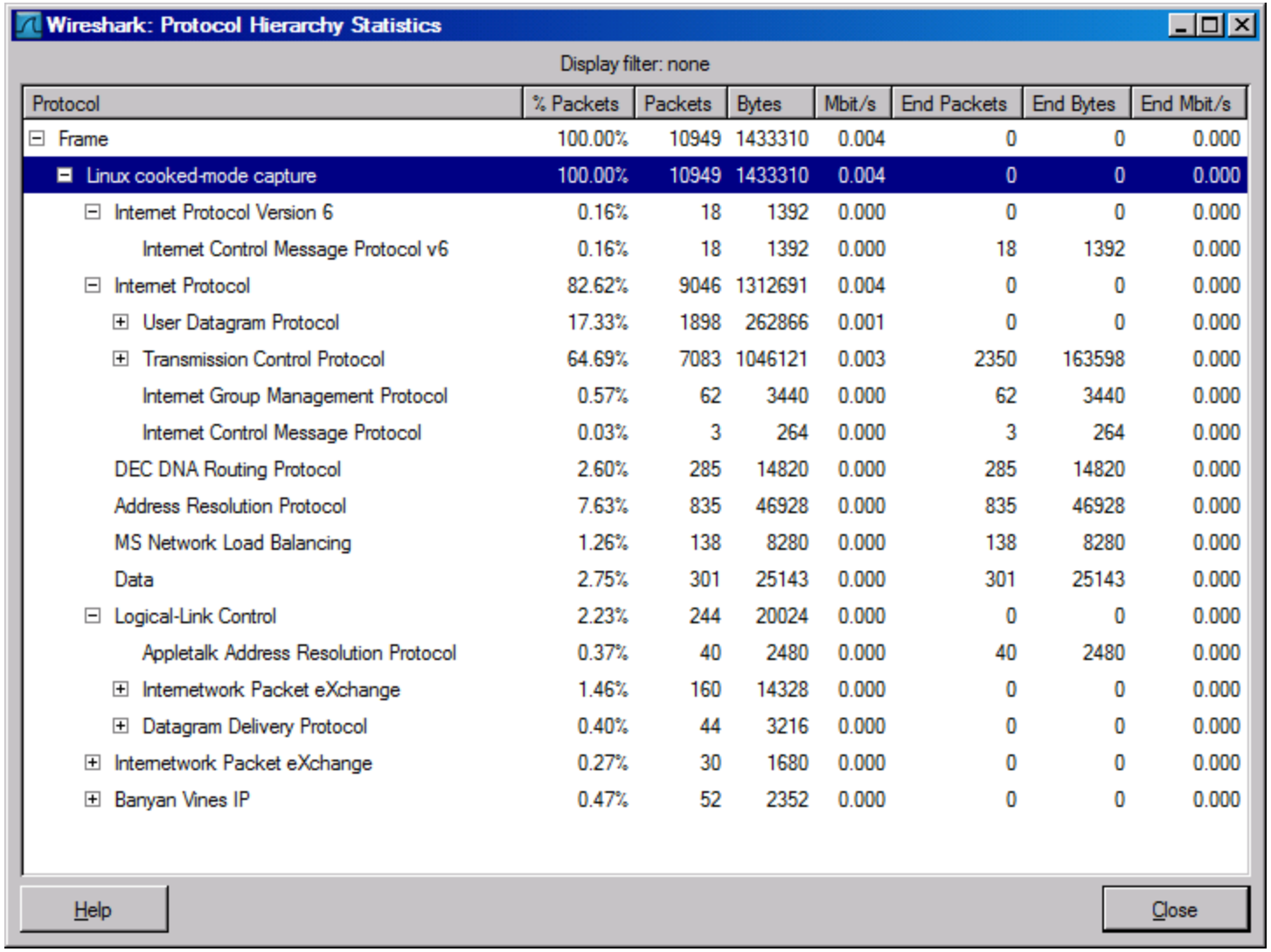
**(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) && (tcp.port==445 || tcp.port==139)**

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

# Protocol Hierarchy

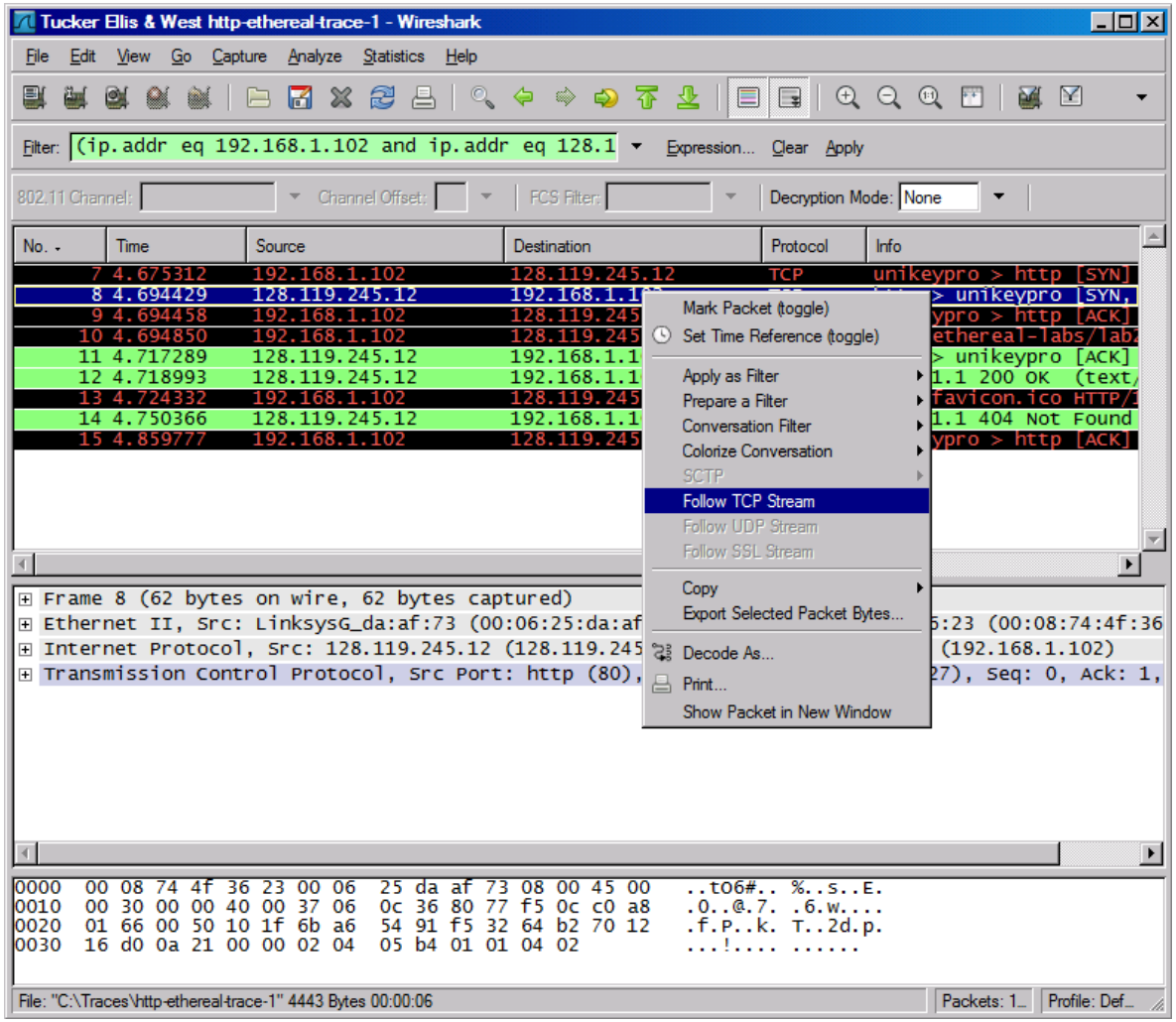


# Protocol Hierarchy



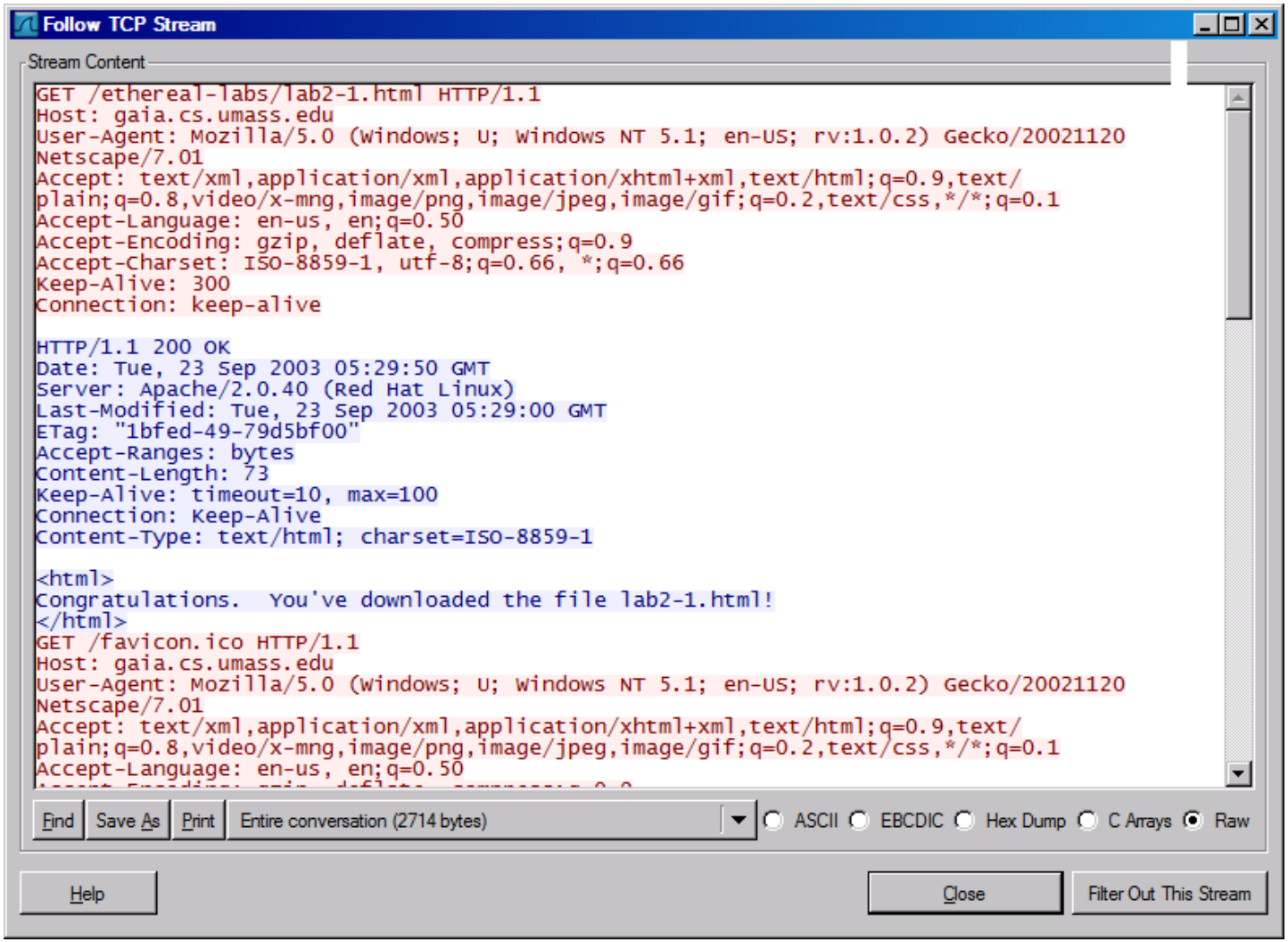

| Protocol | % Packets | Packets | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|
| Frame | 100.00% | 10949 | 1433310 | 0.004 | 0 | 0 | 0.000 |
| Linux cooked-mode capture | 100.00% | 10949 | 1433310 | 0.004 | 0 | 0 | 0.000 |
| Internet Protocol Version 6 | 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

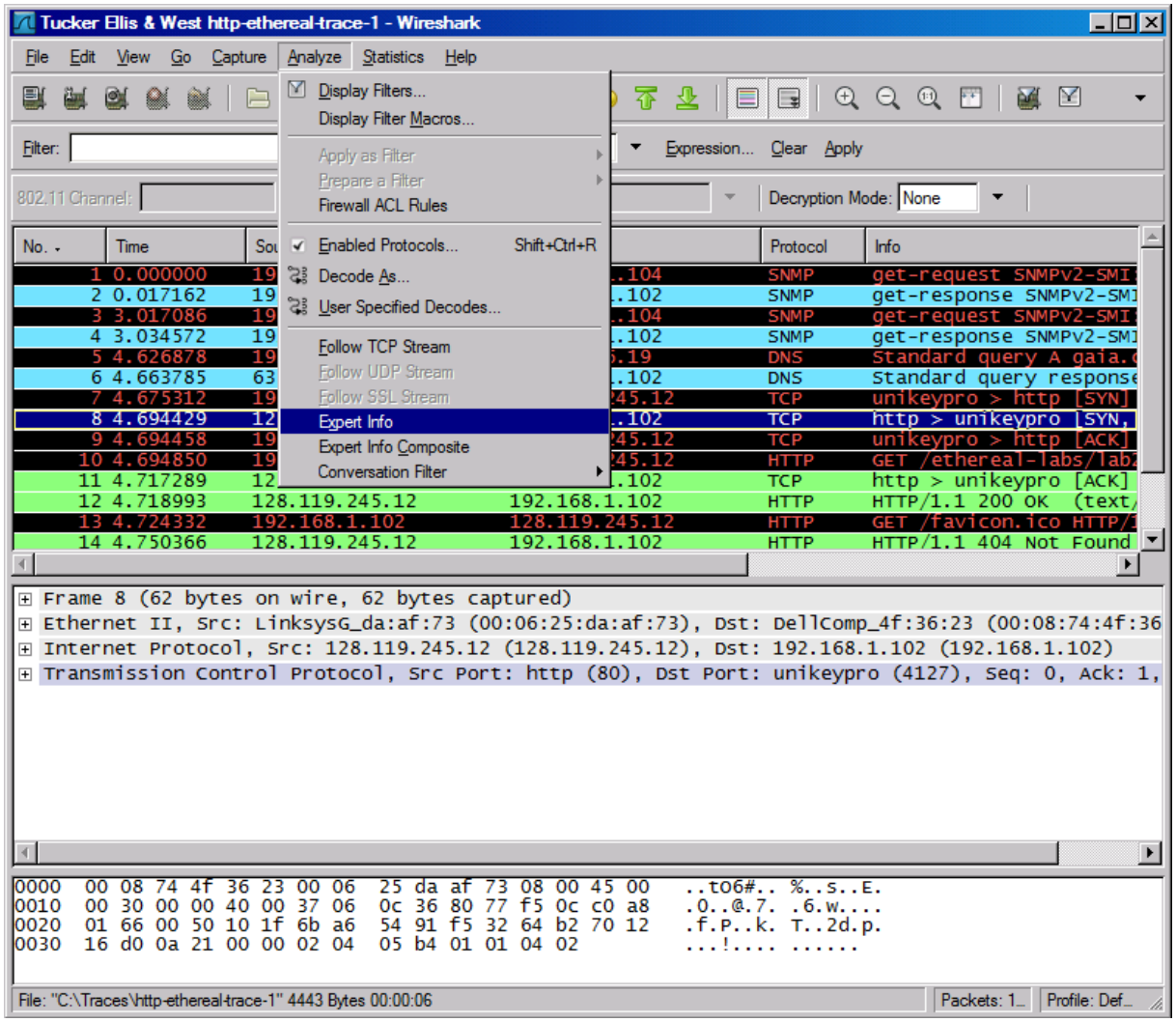


# Follow TCP Stream

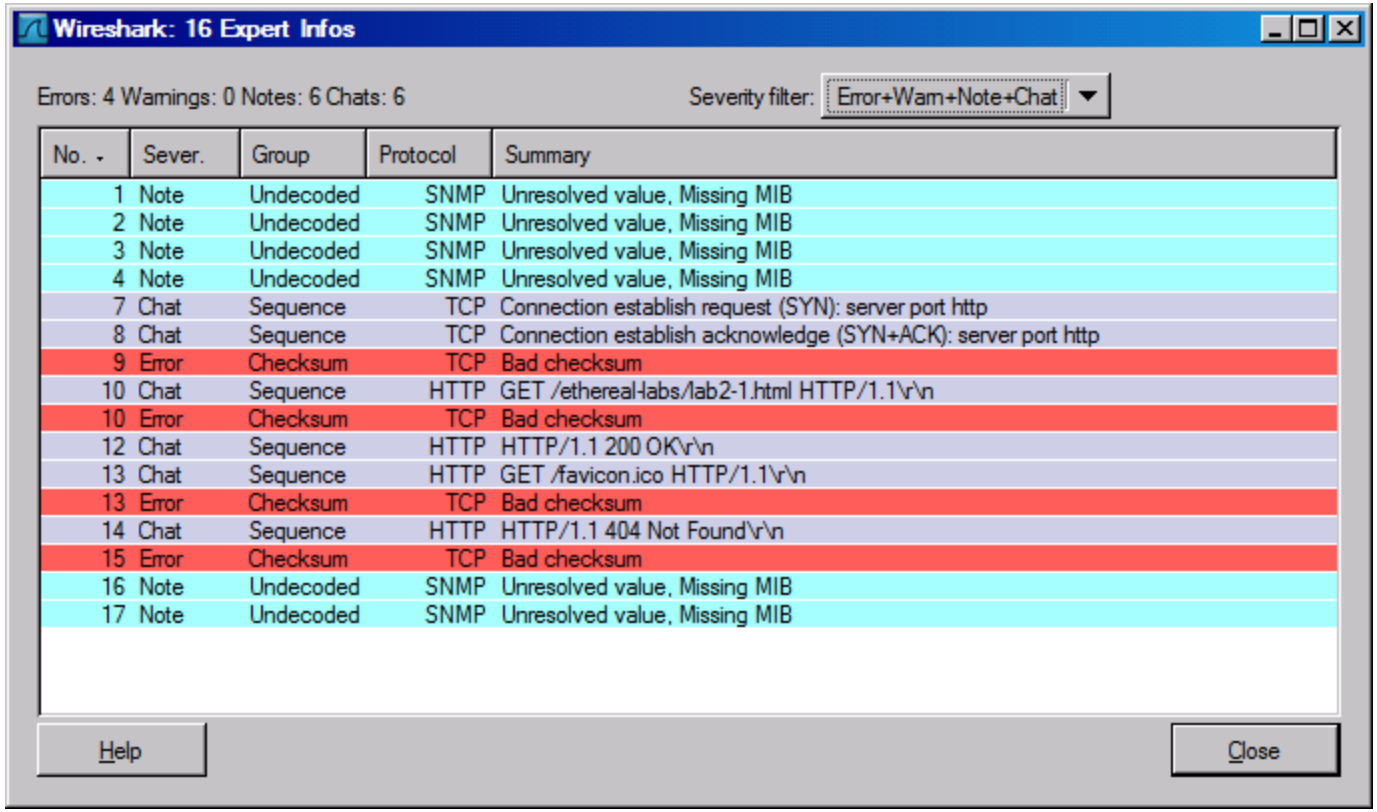
As cores diferenciam os usuários em uma conexão



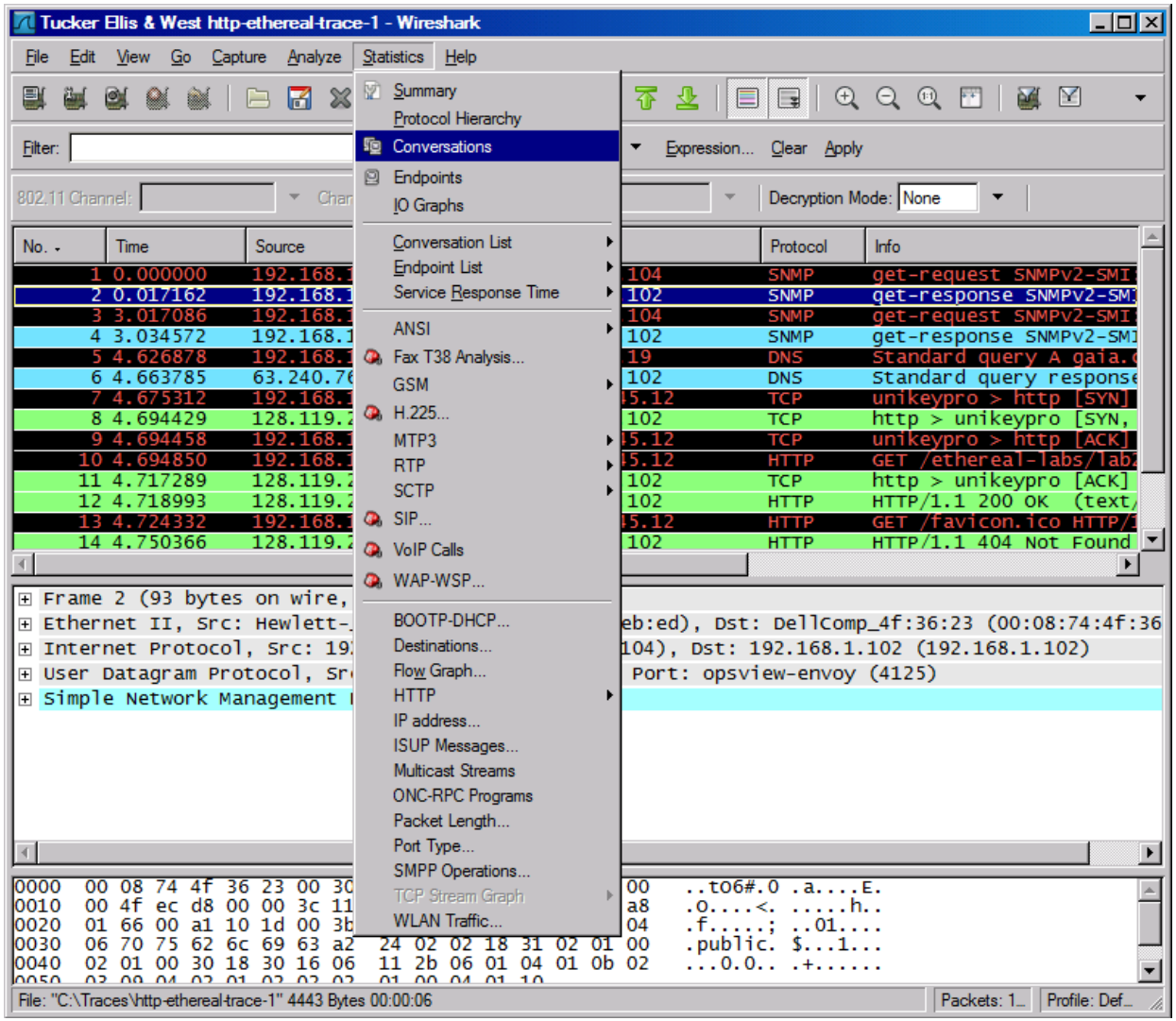
# Expert Info


Tucker Ellis & West http-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Display Filters...
Display Filter Macros...
Apply as Filter
Prepare a Filter
Firewall ACL Rules
Enabled Protocols... Shift+Ctrl+R
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Expert Info Composite
Conversation Filter
Filter:
Expression... Clear Apply
802.11 Channel:
Decryption Mode: None
No. Time Protocol Info
1 0.000000 SNMP get-request SNMPv2-SMI
2 0.017162 SNMP get-response SNMPv2-SMI
3 3.017086 SNMP get-request SNMPv2-SMI
4 3.034572 SNMP get-response SNMPv2-SMI
5 4.626878 DNS Standard query A gaia.
6 4.663785 DNS Standard query response
7 4.675312 TCP unikeypro > http [SYN]
8 4.694429 TCP http > unikeypro [SYN,
9 4.694458 TCP unikeypro > http [ACK]
10 4.694850 HTTP GET /ethereal-labs/lab
11 4.717289 TCP http > unikeypro [ACK]
12 4.718993 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 200 OK (text/
13 4.724332 192.168.1.102 128.119.245.12 HTTP GET /favicon.ico HTTP/
14 4.750366 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 404 Not Found
Frame 8 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 0, Ack: 1,
0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..tO6#.. %..s..E.
0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8 .0..@.7. .6.w....
0020 01 66 00 50 10 1f 6b a6 54 91 f5 32 64 b2 70 12 .f.P..k. T..2d.p.
0030 16 d0 0a 21 00 00 02 04 05 b4 01 01 04 02 ...!.... ......
File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06
Packets: 1...
Profile: Def...

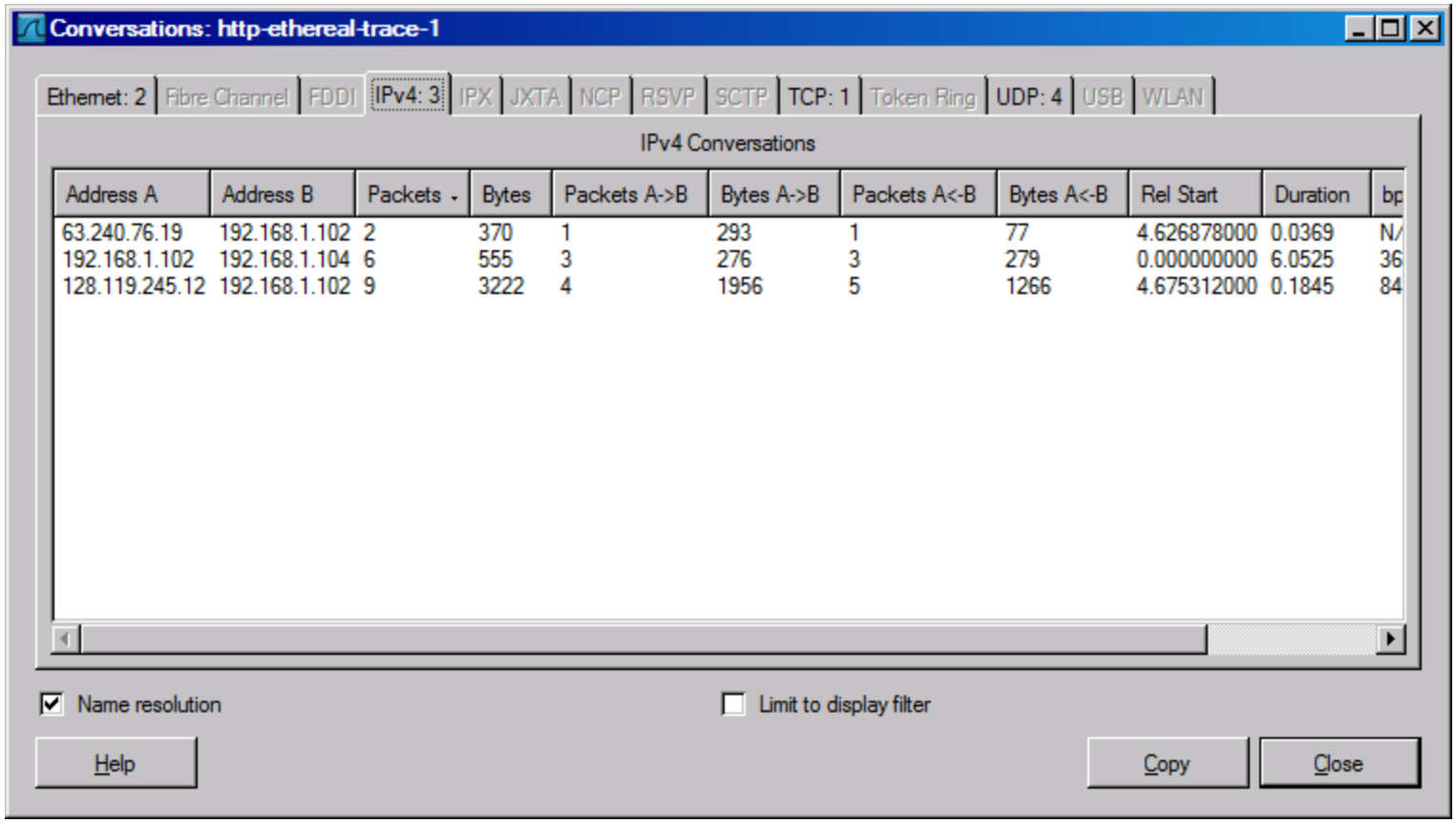
# Expert Info


Wireshark: 16 Expert Infos
Errors: 4 Warnings: 0 Notes: 6 Chats: 6
Severity filter: Error+Warn+Note+Chat
No. Sever. Group Protocol Summary
1 Note Undecoded SNMP Unresolved value, Missing MIB
2 Note Undecoded SNMP Unresolved value, Missing MIB
3 Note Undecoded SNMP Unresolved value, Missing MIB
4 Note Undecoded SNMP Unresolved value, Missing MIB
7 Chat Sequence TCP Connection establish request (SYN): server port http
8 Chat Sequence TCP Connection establish acknowledge (SYN+ACK): server port http
9 Error Checksum TCP Bad checksum
10 Chat Sequence HTTP GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
10 Error Checksum TCP Bad checksum
12 Chat Sequence HTTP HTTP/1.1 200 OK\r\n
13 Chat Sequence HTTP GET /favicon.ico HTTP/1.1\r\n
13 Error Checksum TCP Bad checksum
14 Chat Sequence HTTP HTTP/1.1 404 Not Found\r\n
15 Error Checksum TCP Bad checksum
16 Note Undecoded SNMP Unresolved value, Missing MIB
17 Note Undecoded SNMP Unresolved value, Missing MIB
Help
Close

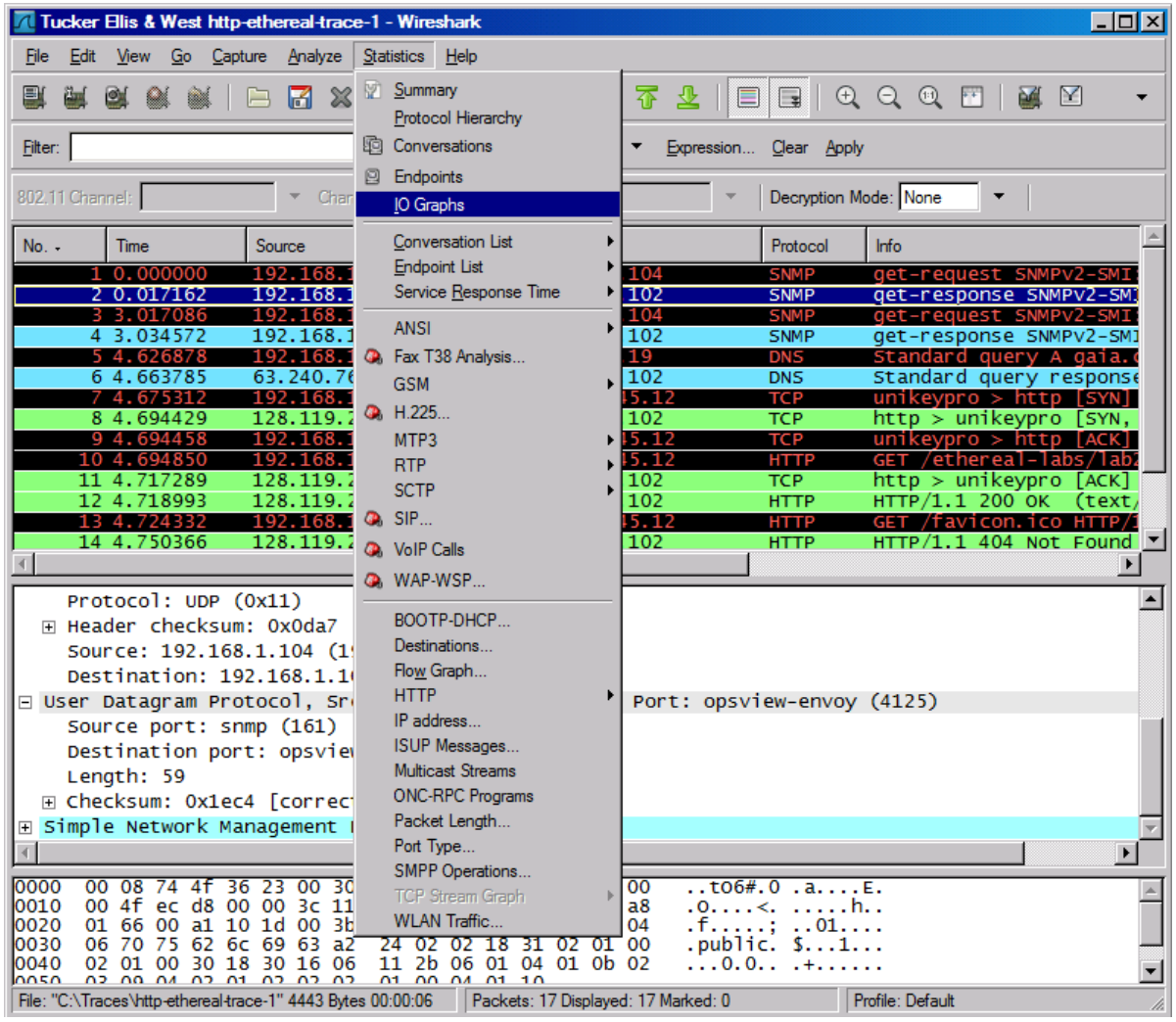
# Conversations



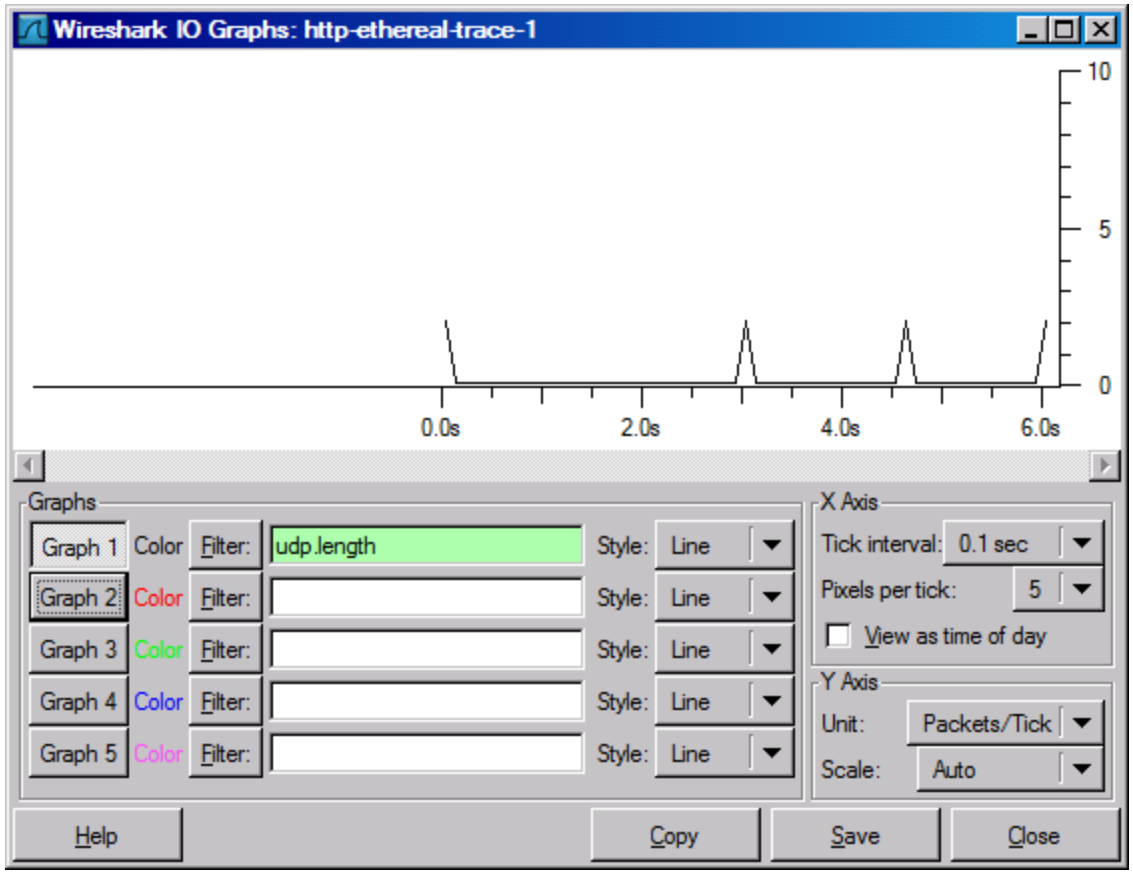
# Conversations



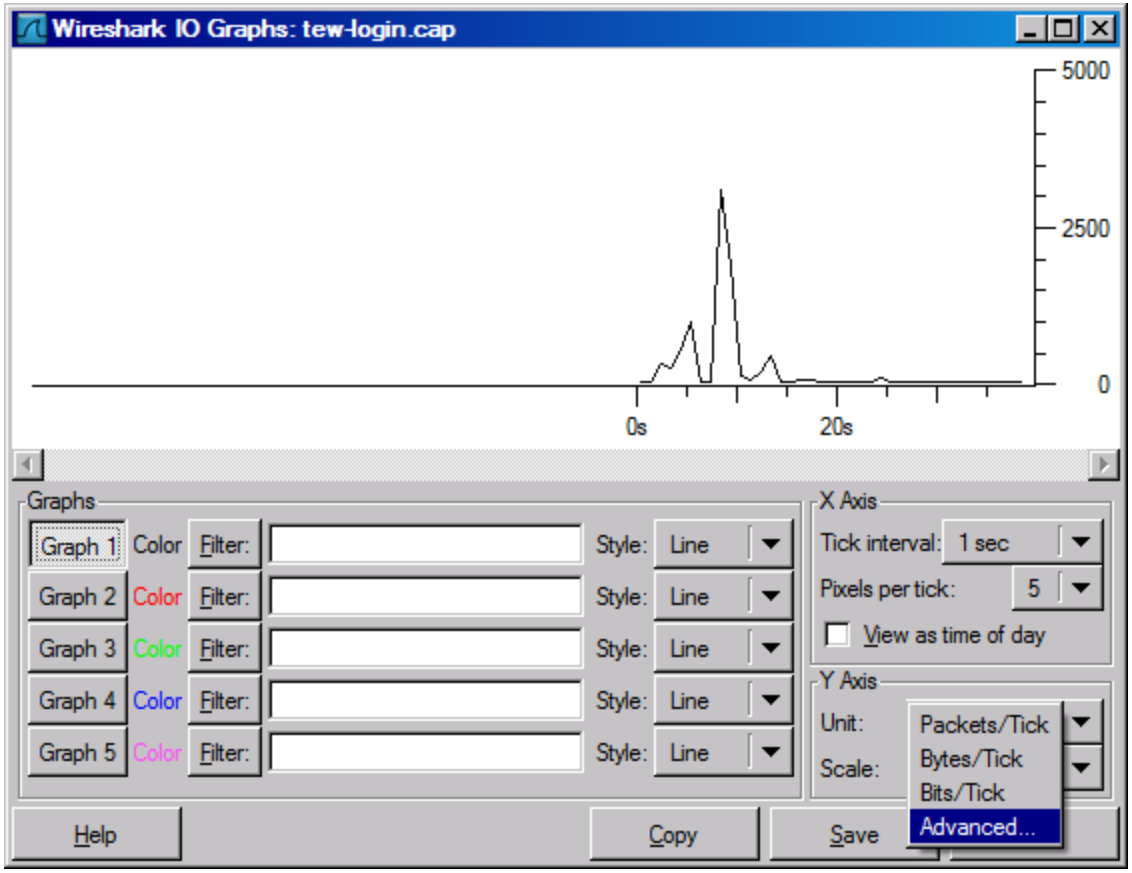
# IOGraphs


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
802.11 Channel:
Decryption Mode: None
No. Time Source Protocol Info
1 0.000000 192.168.1 SNMP get-request SNMPv2-SMI
2 0.017162 192.168.1 SNMP get-response SNMPv2-SMI
3 3.017086 192.168.1 SNMP get-request SNMPv2-SMI
4 3.034572 192.168.1 SNMP get-response SNMPv2-SMI
5 4.626878 192.168.1 DNS Standard query A gaia.
6 4.663785 63.240.76 DNS Standard query response
7 4.675312 192.168.1 TCP unikeypro > http [SYN]
8 4.694429 128.119.2 TCP http > unikeypro [SYN,
9 4.694458 192.168.1 TCP unikeypro > http [ACK]
10 4.694850 192.168.1 HTTP GET /ethereal-labs/lab
11 4.717289 128.119.2 TCP http > unikeypro [ACK]
12 4.718993 128.119.2 HTTP HTTP/1.1 200 OK (text/
13 4.724332 192.168.1 HTTP GET /favicon.ico HTTP/
14 4.750366 128.119.2 HTTP HTTP/1.1 404 Not Found
Protocol: UDP (0x11)
Header checksum: 0x0da7
Source: 192.168.1.104 (1
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)
0000 00 08 74 4f 36 23 00 30 ..tO6#.0
0010 00 4f ec d8 00 00 3c 11 .O....<.
0020 01 66 00 a1 10 1d 00 3b .f.....;
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 31 02 01 00 .public. $...1...
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02 ...0.0.. .+......
File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06
Packets: 17 Displayed: 17 Marked: 0
Profile: Default

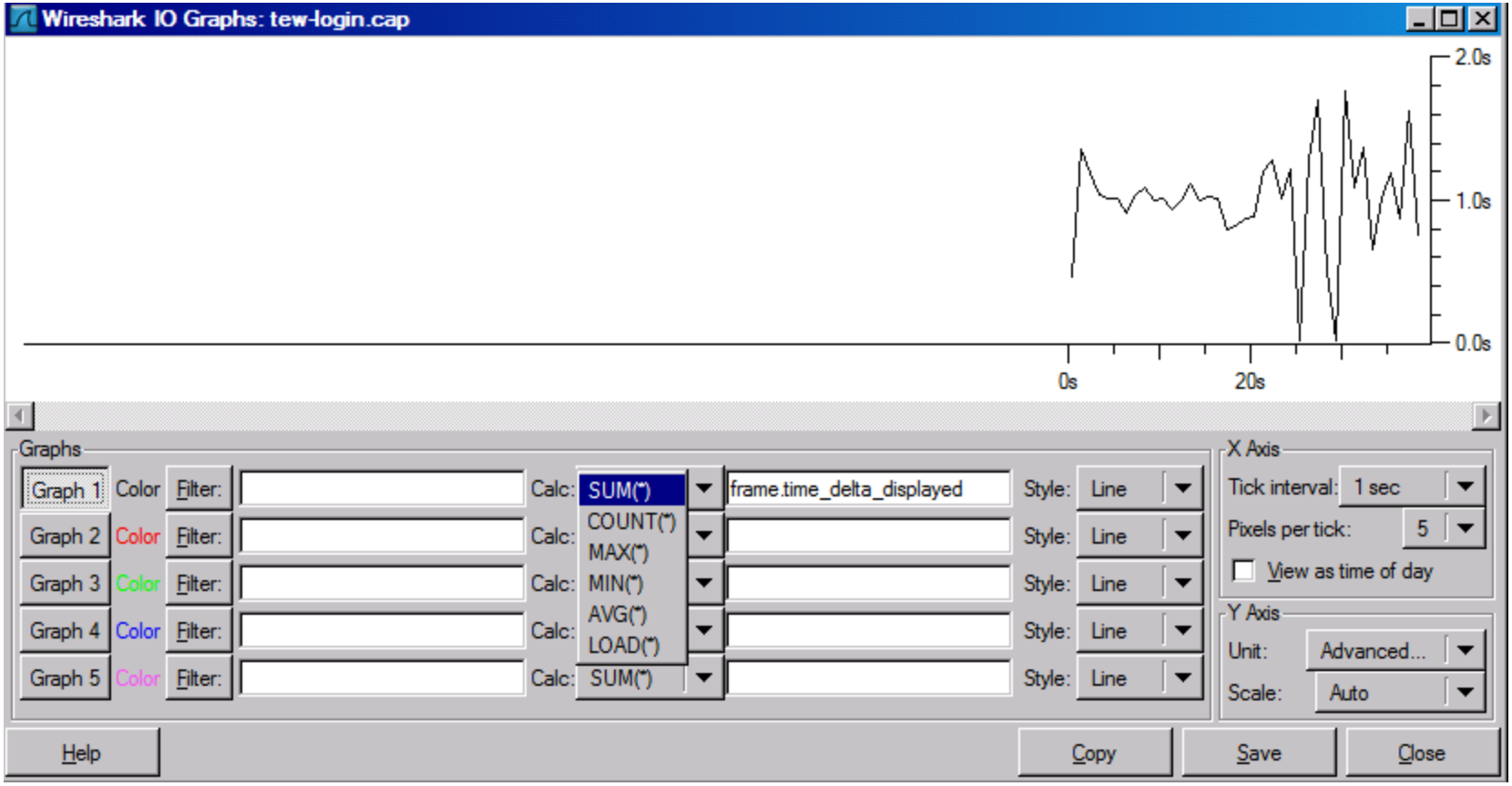
# IOGraphs


Wireshark IO Graphs: http-ethereal-trace-1
10
5
0
0.0s
2.0s
4.0s
6.0s
Graphs
Graph 1
Color
Filter:
udp.length
Style:
Line
Graph 2
Color
Filter:
Style:
Line
Graph 3
Color
Filter:
Style:
Line
Graph 4
Color
Filter:
Style:
Line
Graph 5
Color
Filter:
Style:
Line
X Axis
Tick interval:
0.1 sec
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Packets/Tick
Scale:
Auto
Help
Copy
Save
Close

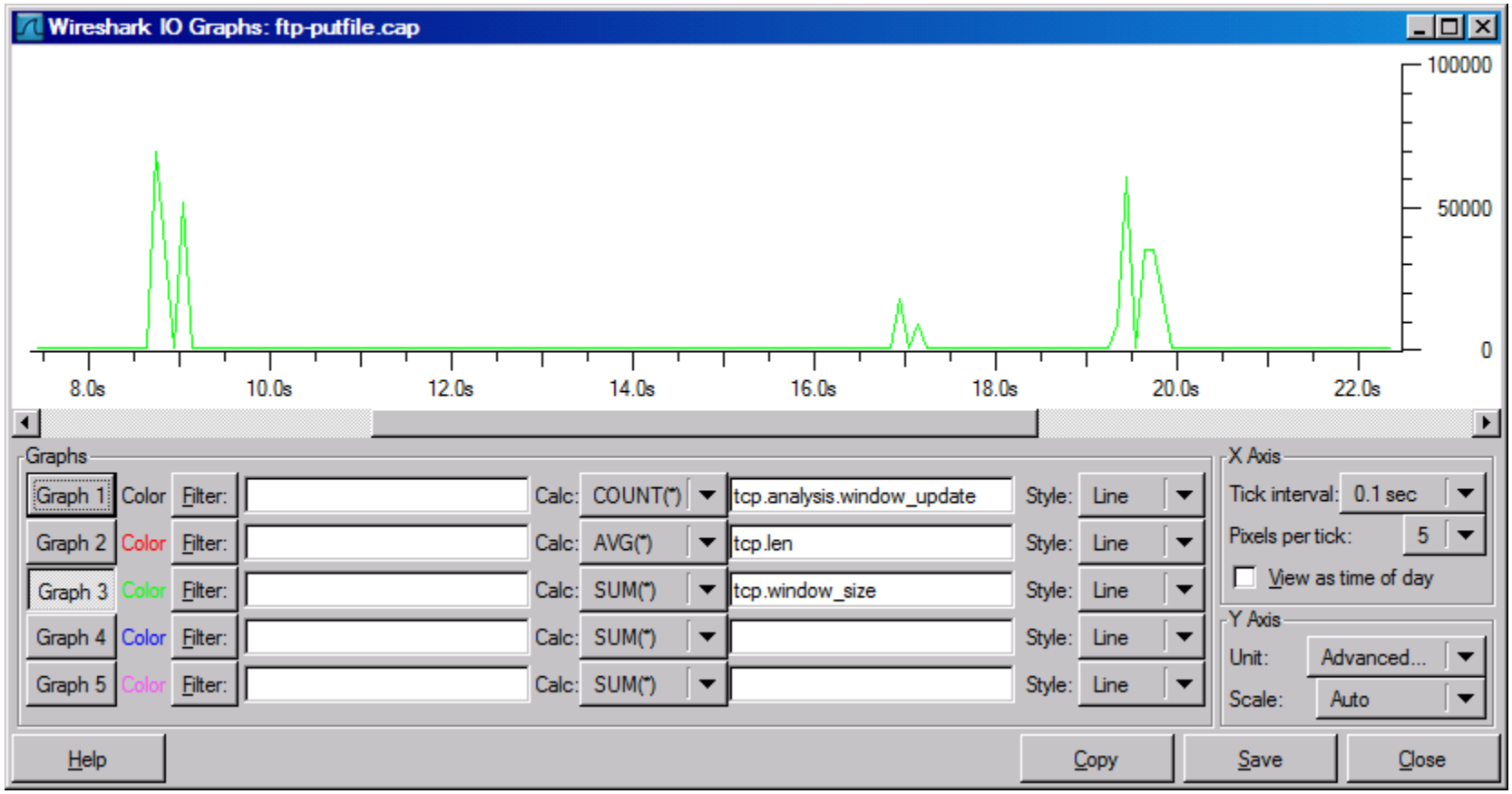
# IOGraphs


Wireshark IO Graphs: tew-login.cap
5000
2500
0
0s
20s
Graphs
Graph 1
Color
Filter:
Style:
Line
Graph 2
Color
Filter:
Style:
Line
Graph 3
Color
Filter:
Style:
Line
Graph 4
Color
Filter:
Style:
Line
Graph 5
Color
Filter:
Style:
Line
X Axis
Tick interval:
1 sec
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Packets/Tick
Bytes/Tick
Bits/Tick
Advanced...
Scale:
Help
Copy
Save

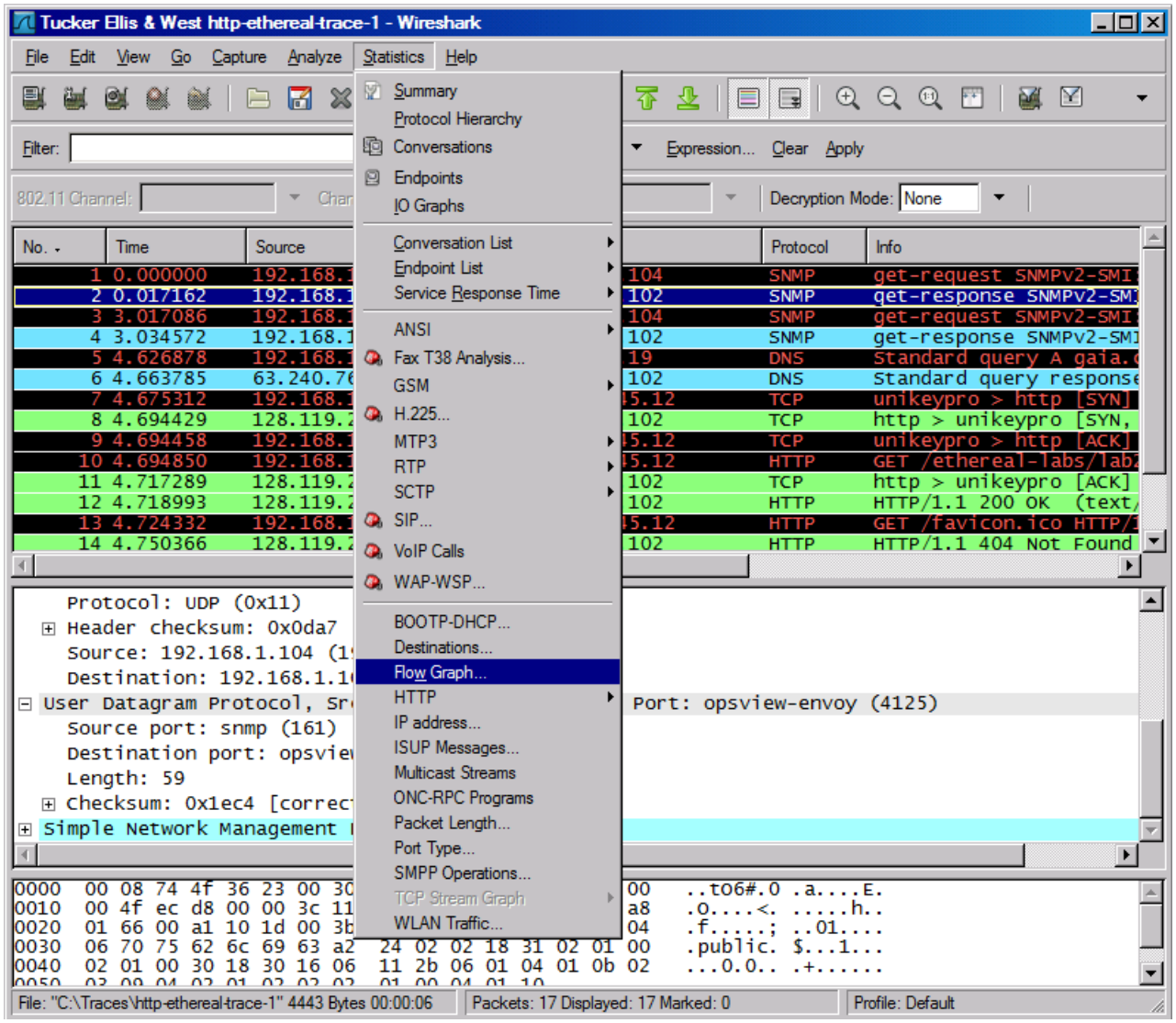
# IOGraphs


Wireshark IO Graphs: tew-login.cap
2.0s
1.0s
0.0s
0s
20s
Graphs
Graph 1
Color
Filter:
Calc:
SUM(*)
frame.time_delta_displayed
Style:
Line
Graph 2
Color
Filter:
Calc:
COUNT(*)
MAX(*)
MIN(*)
AVG(*)
LOAD(*)
Style:
Line
Graph 3
Color
Filter:
Calc:
Style:
Line
Graph 4
Color
Filter:
Calc:
Style:
Line
Graph 5
Color
Filter:
Calc:
SUM(*)
Style:
Line
X Axis
Tick interval:
1 sec
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Advanced...
Scale:
Auto
Help
Copy
Save
Close

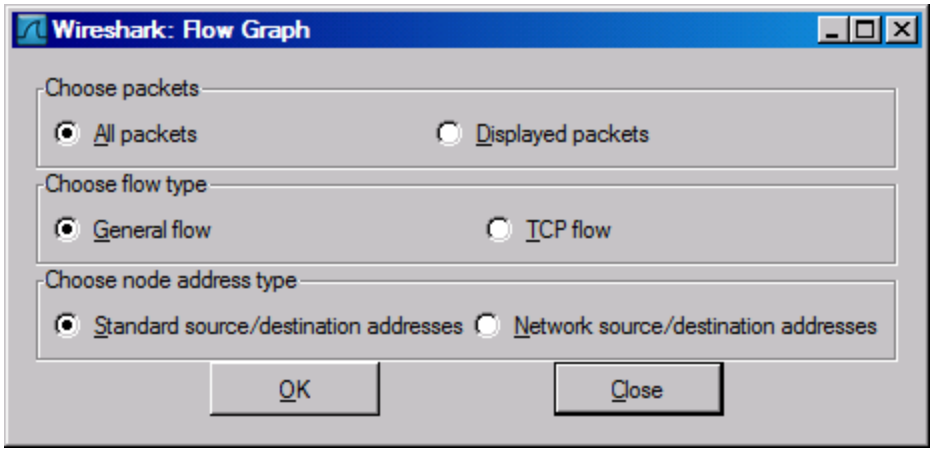
# IOGraphs


Wireshark IO Graphs: ftp-putfile.cap
100000
50000
0
8.0s
10.0s
12.0s
14.0s
16.0s
18.0s
20.0s
22.0s
Graphs
Graph 1 Color Filter: Calc: COUNT(*) tcp.analysis.window_update Style: Line
Graph 2 Color Filter: Calc: AVG(*) tcp.len Style: Line
Graph 3 Color Filter: Calc: SUM(*) tcp.window_size Style: Line
Graph 4 Color Filter: Calc: SUM(*) Style: Line
Graph 5 Color Filter: Calc: SUM(*) Style: Line
X Axis
Tick interval: 0.1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Advanced...
Scale: Auto
Help
Copy
Save
Close

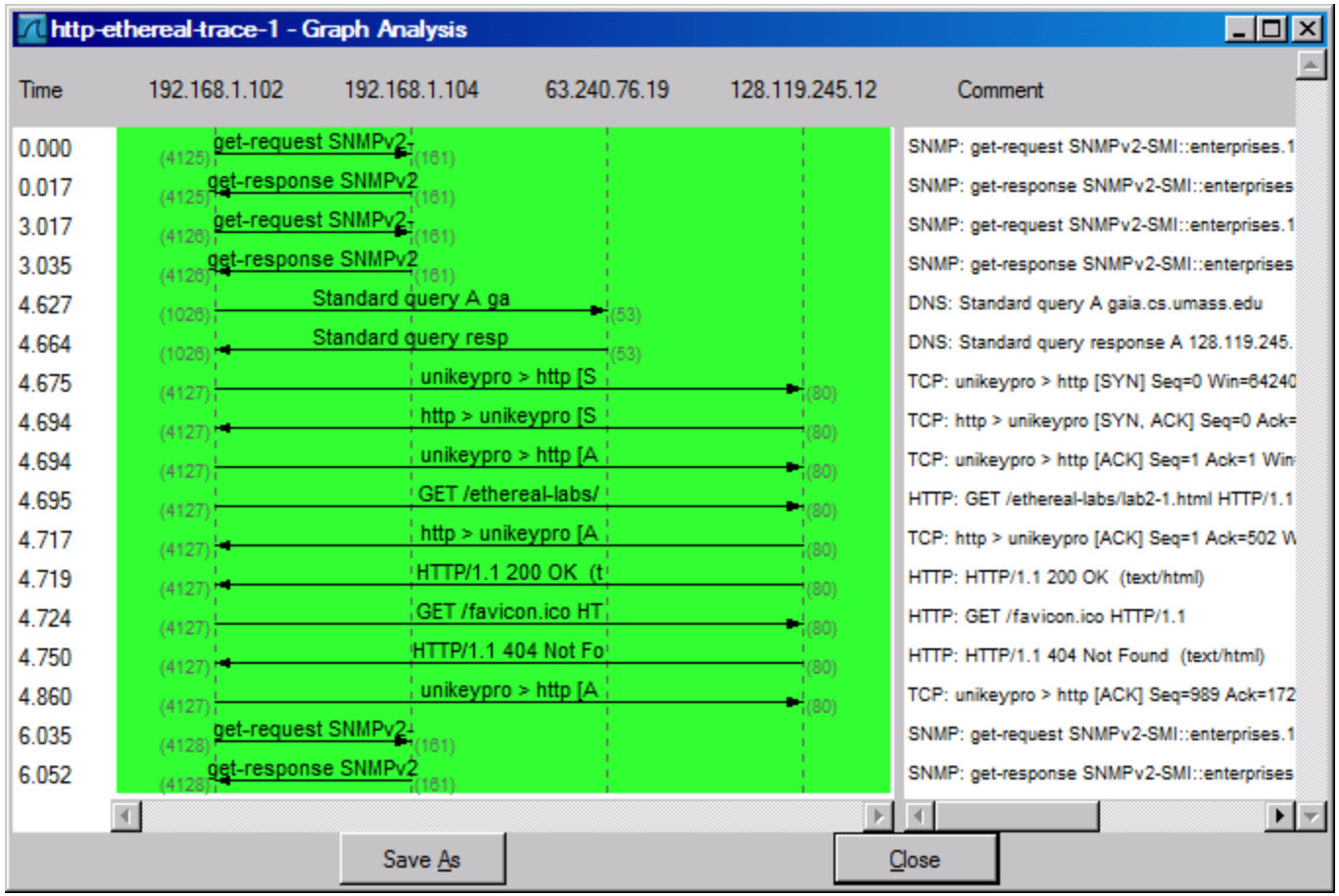
# Flow Graphs


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
802.11 Channel:
Decryption Mode: None
No. Time Source Protocol Info
1 0.000000 192.168.1 SNMP get-request SNMPv2-SMI
2 0.017162 192.168.1 SNMP get-response SNMPv2-SMI
3 3.017086 192.168.1 SNMP get-request SNMPv2-SMI
4 3.034572 192.168.1 SNMP get-response SNMPv2-SMI
5 4.626878 192.168.1 DNS Standard query A gaia.
6 4.663785 63.240.76 DNS Standard query response
7 4.675312 192.168.1 TCP unikeypro > http [SYN]
8 4.694429 128.119.2 TCP http > unikeypro [SYN,
9 4.694458 192.168.1 TCP unikeypro > http [ACK]
10 4.694850 192.168.1 HTTP GET /ethereal-labs/lab
11 4.717289 128.119.2 TCP http > unikeypro [ACK]
12 4.718993 128.119.2 HTTP HTTP/1.1 200 OK (text/
13 4.724332 192.168.1 HTTP GET /favicon.ico HTTP/1
14 4.750366 128.119.2 HTTP HTTP/1.1 404 Not Found
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)
0000 00 08 74 4f 36 23 00 30 00 ..to6#.0 .a...E.
0010 00 4f ec d8 00 00 3c 11 a8 .o....<. .....h..
0020 01 66 00 a1 10 1d 00 3b 04 .f.....; ..01....
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 31 02 01 00 .public. $...1...
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02 ...0.0.. .+......
File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06
Packets: 17 Displayed: 17 Marked: 0
Profile: Default

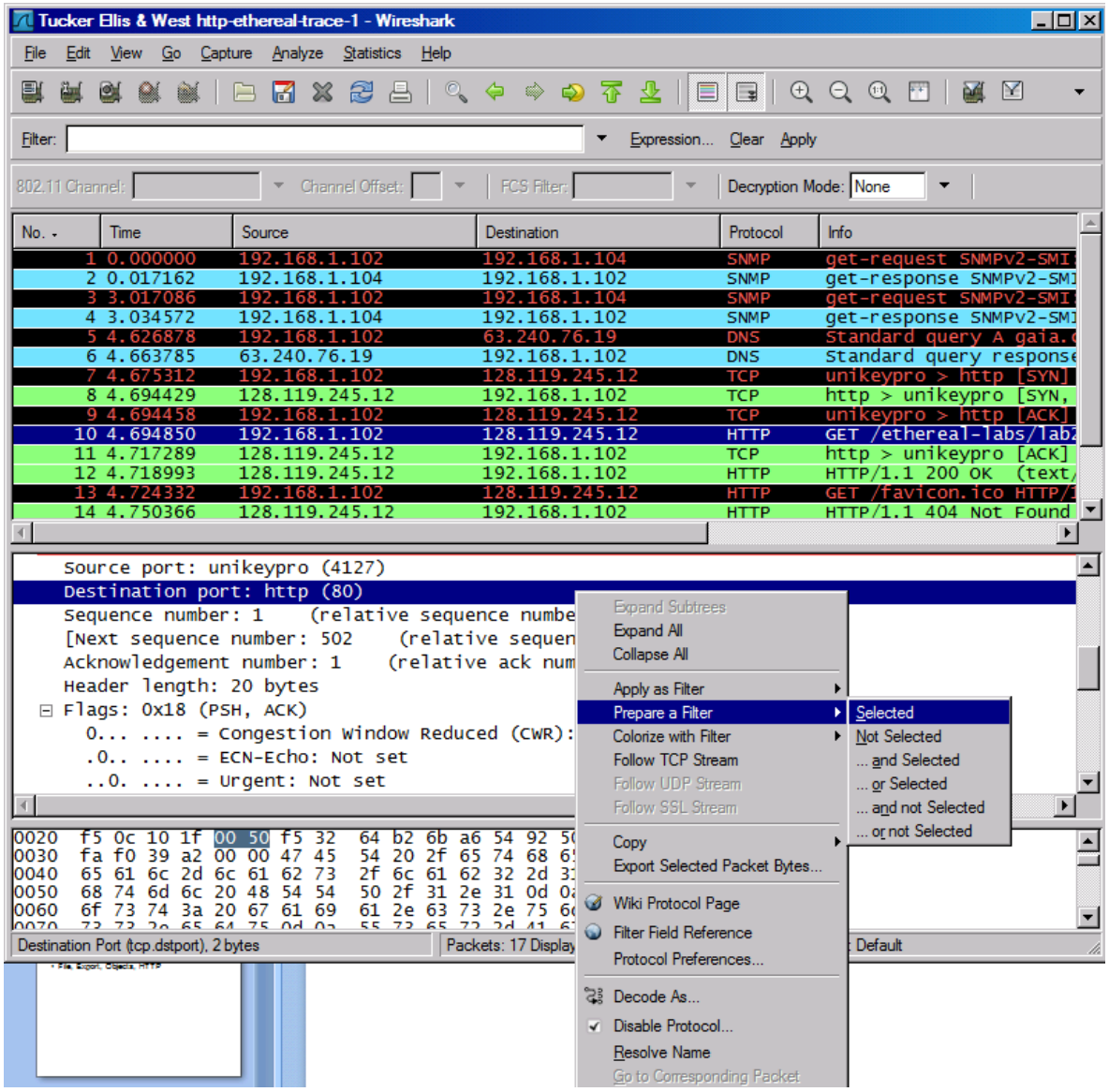
# Flow Graphs


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

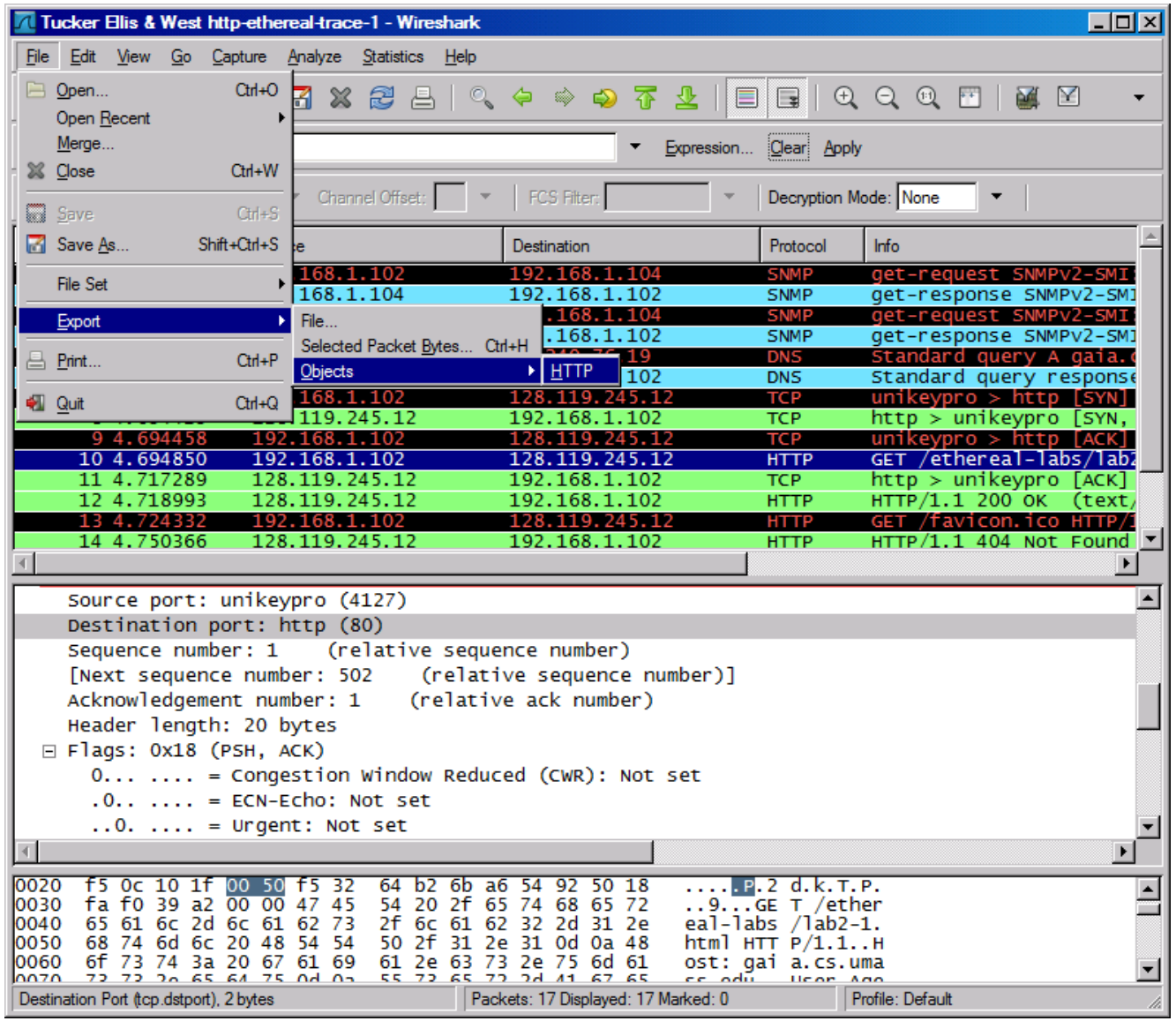
# Flow Graphs


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 get-request SNMPv2 (4125) (161) SNMP: get-request SNMPv2-SMI::enterprises.1
0.017 get-response SNMPv2 (4125) (161) SNMP: get-response SNMPv2-SMI::enterprises
3.017 get-request SNMPv2 (4126) (161) SNMP: get-request SNMPv2-SMI::enterprises.1
3.035 get-response SNMPv2 (4126) (161) SNMP: get-response SNMPv2-SMI::enterprises
4.627 Standard query A ga (1026) (53) DNS: Standard query A gaia.cs.umass.edu
4.664 Standard query resp (1026) (53) DNS: Standard query response A 128.119.245.
4.675 unikeypro > http [S (4127) (80) TCP: unikeypro > http [SYN] Seq=0 Win=64240
4.694 http > unikeypro [S (4127) (80) TCP: http > unikeypro [SYN, ACK] Seq=0 Ack=
4.694 unikeypro > http [A (4127) (80) TCP: unikeypro > http [ACK] Seq=1 Ack=1 Win
4.695 GET /ethereal-labs/ (4127) (80) HTTP: GET /ethereal-labs/lab2-1.html HTTP/1.1
4.717 http > unikeypro [A (4127) (80) TCP: http > unikeypro [ACK] Seq=1 Ack=502 W
4.719 HTTP/1.1 200 OK (t (4127) (80) HTTP: HTTP/1.1 200 OK (text/html)
4.724 GET /favicon.ico HT (4127) (80) HTTP: GET /favicon.ico HTTP/1.1
4.750 HTTP/1.1 404 Not Fo (4127) (80) HTTP: HTTP/1.1 404 Not Found (text/html)
4.860 unikeypro > http [A (4127) (80) TCP: unikeypro > http [ACK] Seq=989 Ack=172
6.035 get-request SNMPv2 (4128) (161) SNMP: get-request SNMPv2-SMI::enterprises.1
6.052 get-response SNMPv2 (4128) (161) SNMP: get-response SNMPv2-SMI::enterprises
Save As
Close

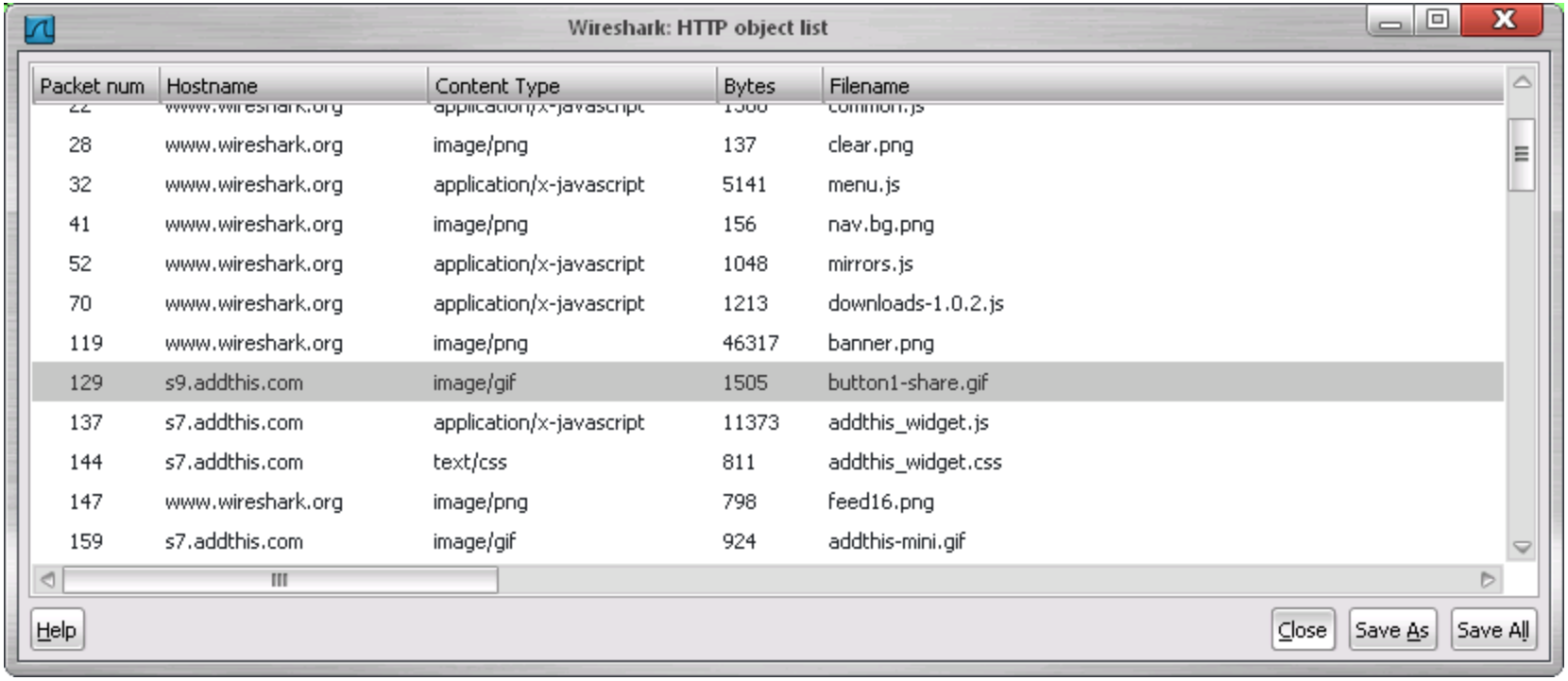
# Right Click Filtering



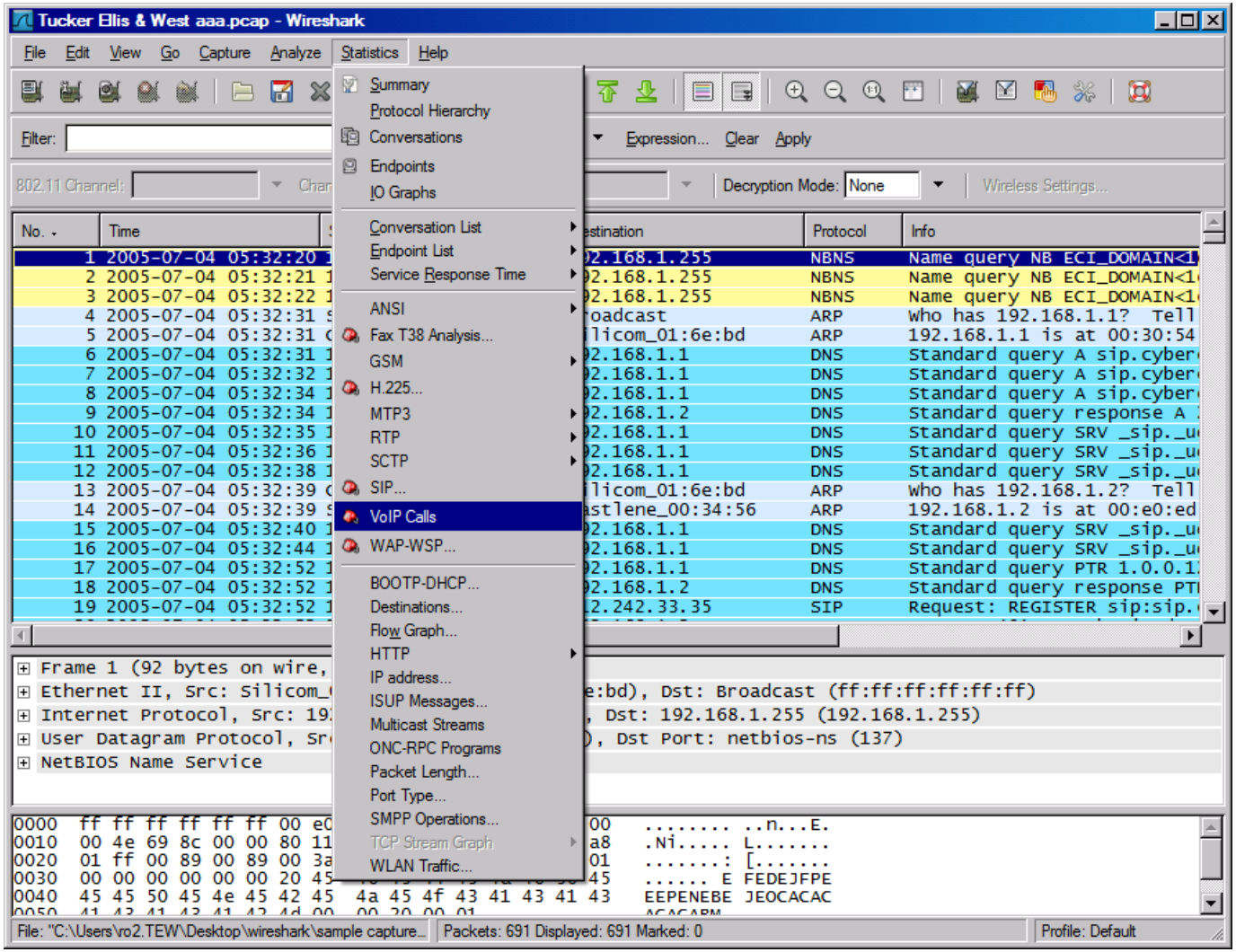
# Export HTTP


Tucker Ellis & West http-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Open... Ctrl+O
Open Recent
Merge...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export
Print... Ctrl+P
Quit Ctrl+Q
File...
Selected Packet Bytes... Ctrl+H
Objects
HTTP
Expression... Clear Apply
Channel Offset: FCS Filter: Decryption Mode: None
Destination Protocol Info
168.1.102 192.168.1.104 SNMP get-request SNMPv2-SMI
168.1.104 192.168.1.102 SNMP get-response SNMPv2-SMI
.168.1.104 SNMP get-request SNMPv2-SMI
.168.1.102 SNMP get-response SNMPv2-SMI
19 DNS Standard query A gaia.
102 DNS Standard query response
168.1.102 128.119.245.12 TCP unikeypro > http [SYN]
119.245.12 192.168.1.102 TCP http > unikeypro [SYN,
9 4.694458 192.168.1.102 128.119.245.12 TCP unikeypro > http [ACK]
10 4.694850 192.168.1.102 128.119.245.12 HTTP GET /ethereal-labs/lab
11 4.717289 128.119.245.12 192.168.1.102 TCP http > unikeypro [ACK]
12 4.718993 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 200 OK (text,
13 4.724332 192.168.1.102 128.119.245.12 HTTP GET /favicon.ico HTTP/1
14 4.750366 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 404 Not Found
Source port: unikeypro (4127)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
[Next sequence number: 502 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
0020 f5 0c 10 1f 00 50 f5 32 64 b2 6b a6 54 92 50 18 .....P.2 d.k.T.P.
0030 fa f0 39 a2 00 00 47 45 54 20 2f 65 74 68 65 72 ..9...GE T /ether
0040 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 32 2d 31 2e eal-labs /lab2-1.
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1..H
0060 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
Destination Port (tcp.dstport), 2 bytes
Packets: 17 Displayed: 17 Marked: 0
Profile: Default

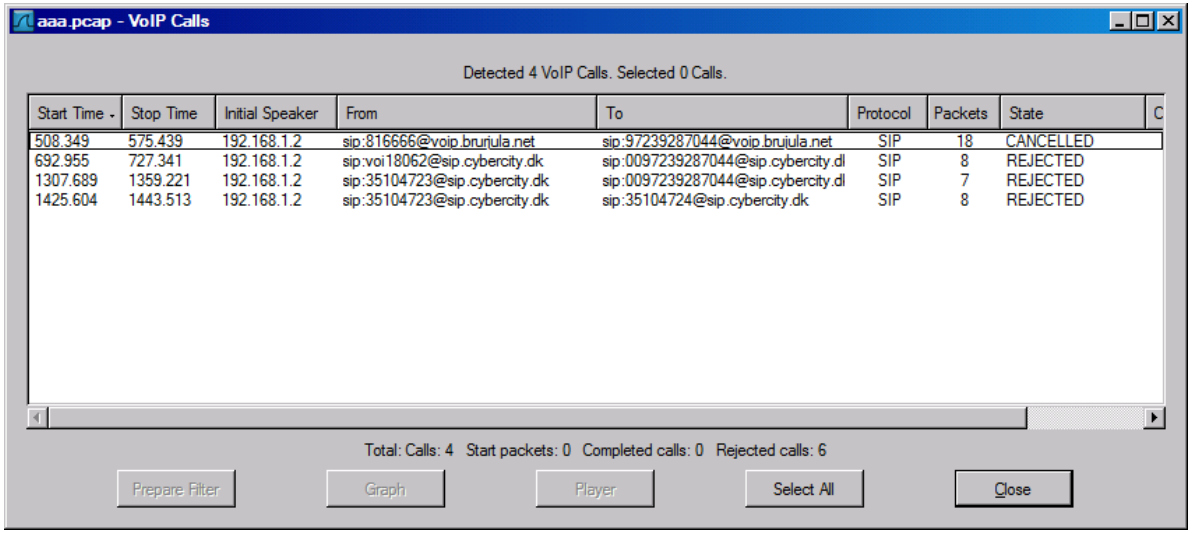
# Export HTTP Objects

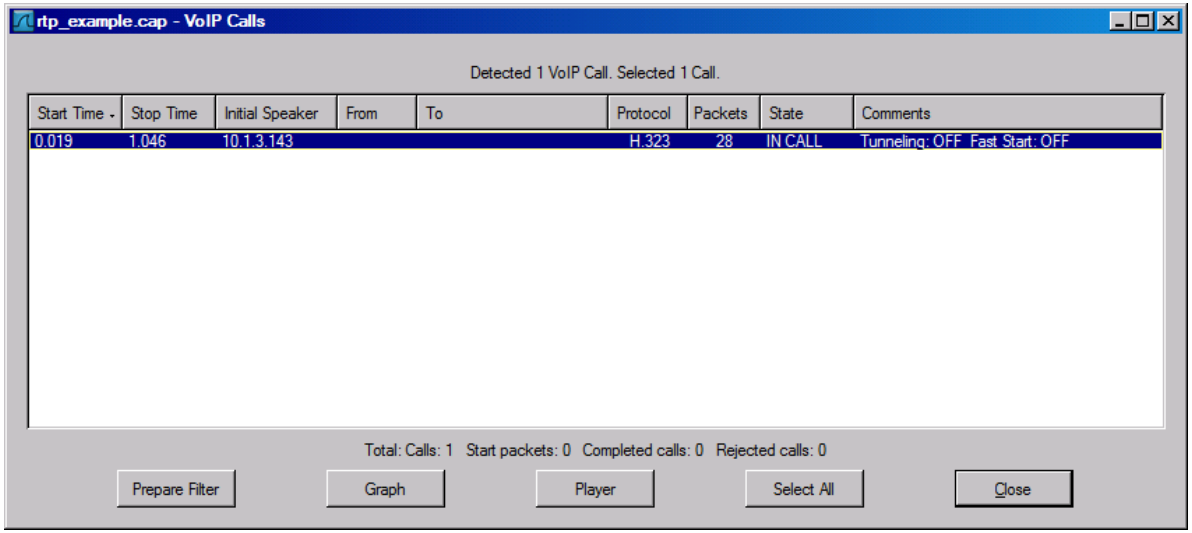


# VOIP

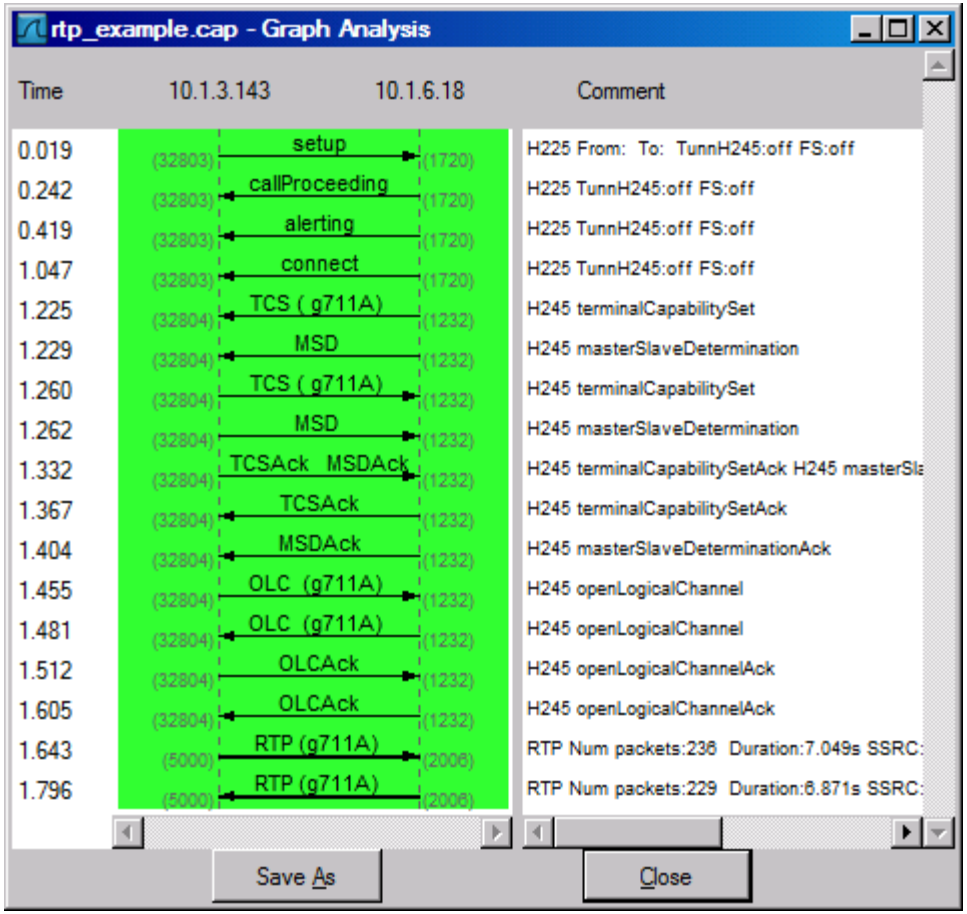

Tucker Ellis & West aaa.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Summary
Protocol Hierarchy
Conversations
Endpoints
IO Graphs
Conversation List
Endpoint List
Service Response Time
ANSI
Fax T38 Analysis...
GSM
H.225...
MTP3
RTP
SCTP
SIP...
VoIP Calls
WAP-WSP...
BOOTP-DHCP...
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
Wireless Settings...
No. Time Destination Protocol Info
Frame 1 (92 bytes on wire,
Ethernet II, Src: Silicom_
Internet Protocol, Src: 19
User Datagram Protocol, Sr
NetBIOS Name Service
File: "C:\Users\ro2.TEW\Desktop\wireshark\sample capture...
Packets: 691 Displayed: 691 Marked: 0
Profile: Default

# VOIP Calls

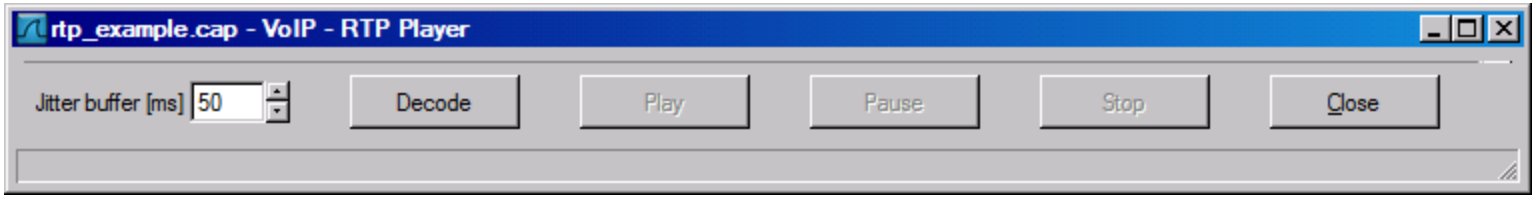

aaa.pcap - VoIP Calls
Detected 4 VoIP Calls. Selected 0 Calls.
Start Time | Stop Time | Initial Speaker | From | To | Protocol | Packets | State
508.349 | 575.439 | 192.168.1.2 | sip:816666@voip.brujula.net | sip:97239287044@voip.brujula.net | SIP | 18 | CANCELLED
692.955 | 727.341 | 192.168.1.2 | sip:voi18062@sip.cybercity.dk | sip:0097239287044@sip.cybercity.dl | SIP | 8 | REJECTED
1307.689 | 1359.221 | 192.168.1.2 | sip:35104723@sip.cybercity.dk | sip:0097239287044@sip.cybercity.dl | SIP | 7 | REJECTED
1425.604 | 1443.513 | 192.168.1.2 | sip:35104723@sip.cybercity.dk | sip:35104724@sip.cybercity.dk | SIP | 8 | REJECTED
Total: Calls: 4 Start packets: 0 Completed calls: 0 Rejected calls: 6
Prepare Filter
Graph
Player
Select All
Close

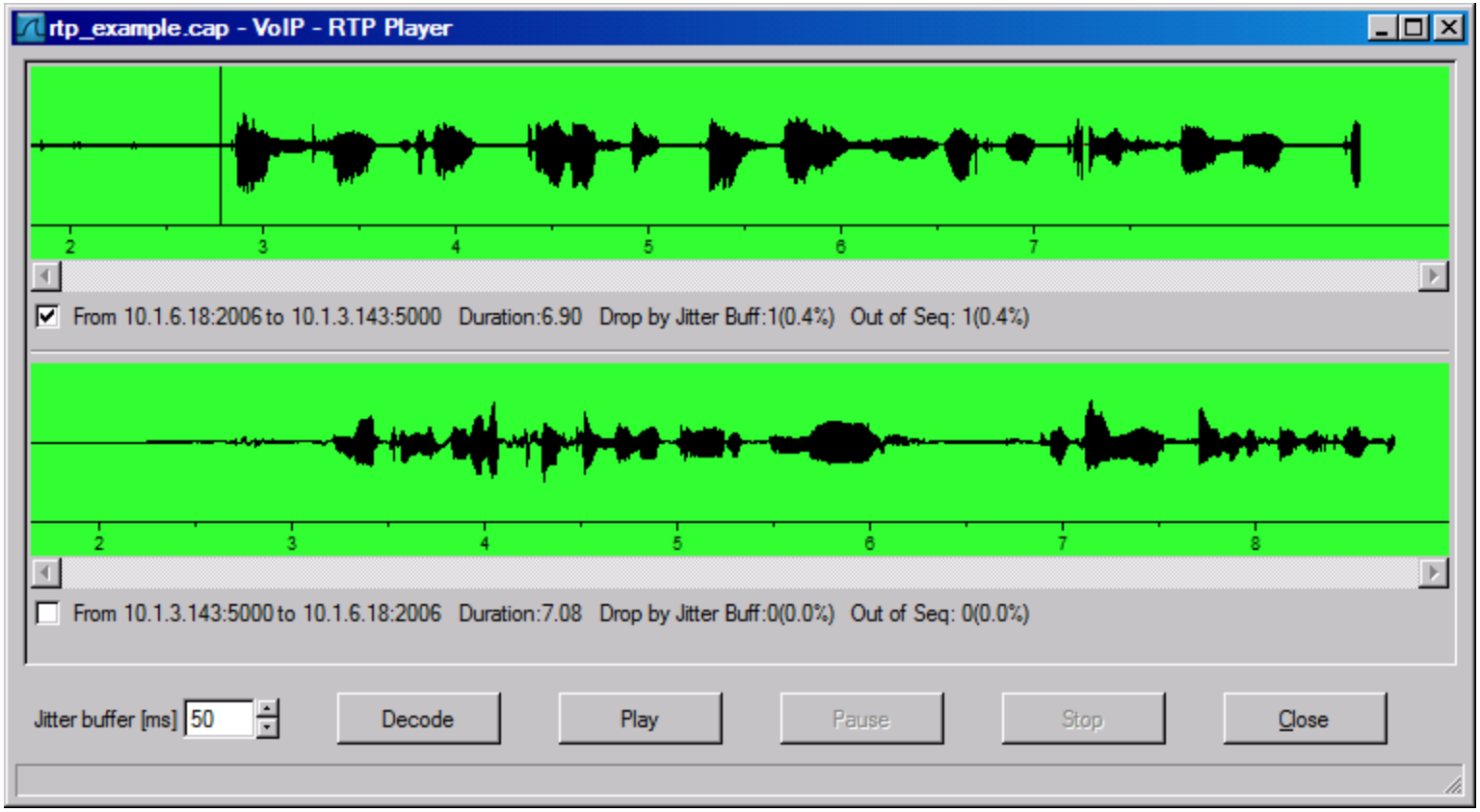

rtp_example.cap - VoIP Calls
Detected 1 VoIP Call. Selected 1 Call.
Start Time | Stop Time | Initial Speaker | From | To | Protocol | Packets | State | Comments
0.019 | 1.046 | 10.1.3.143 | | | H.323 | 28 | IN CALL | Tunneling: OFF Fast Start: OFF
Total: Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 0
Prepare Filter
Graph
Player
Select All
Close

# VOIP Call Graph

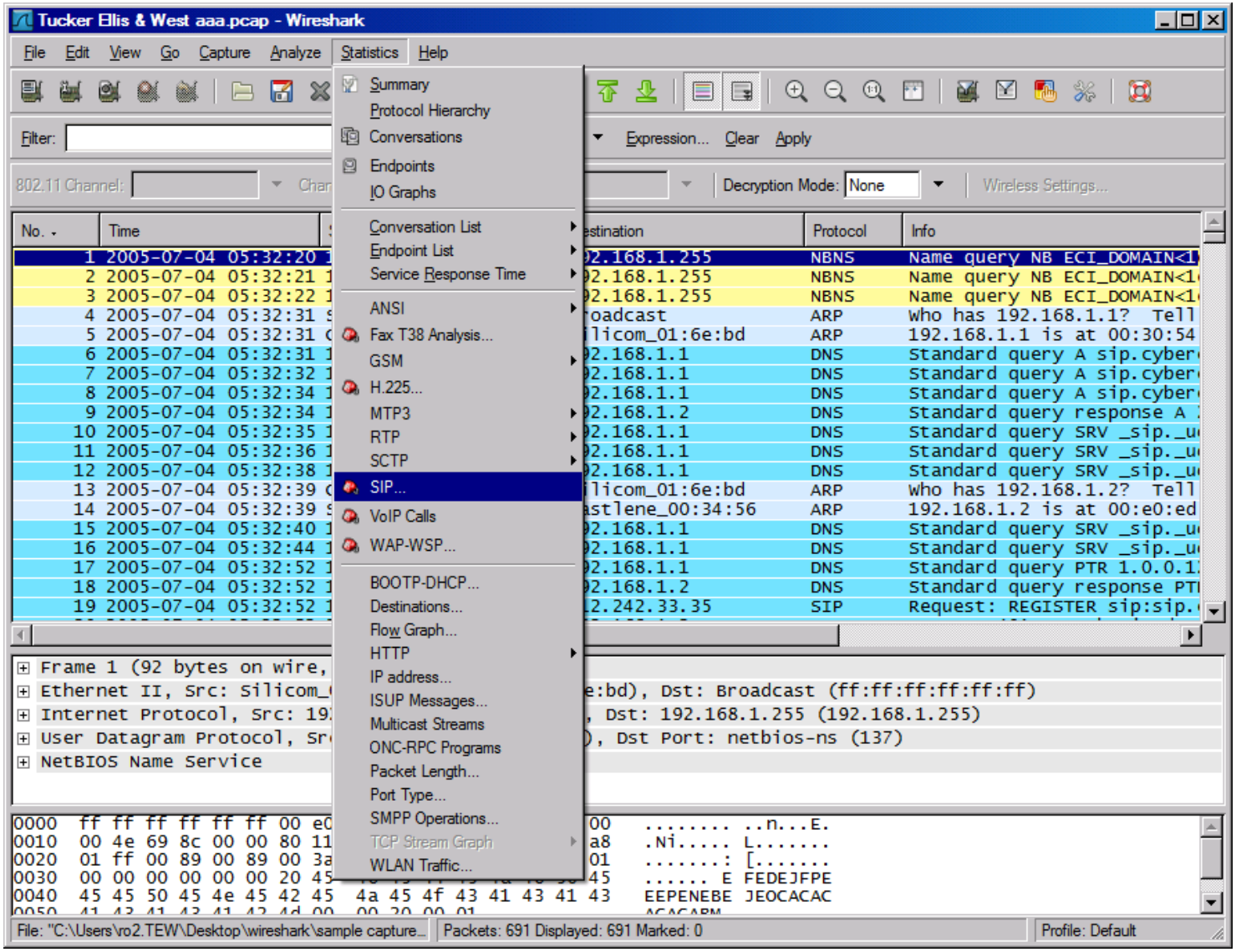


# VOIP RTP Player

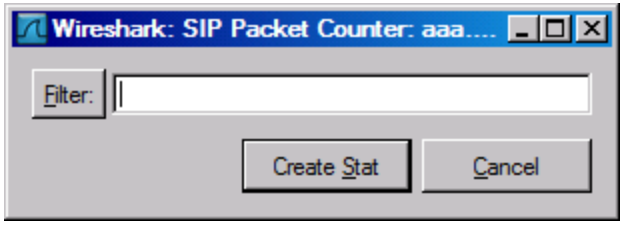


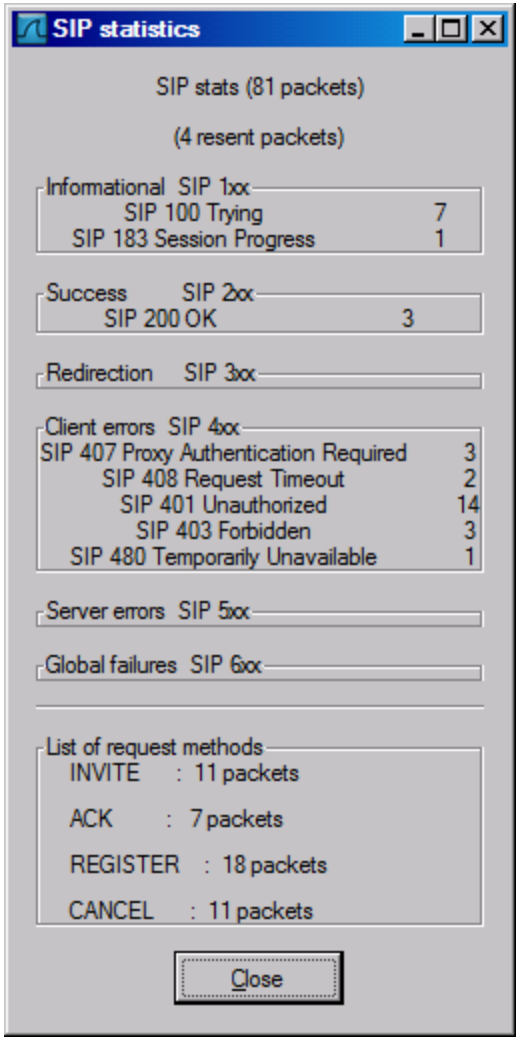



# SIP Analysis

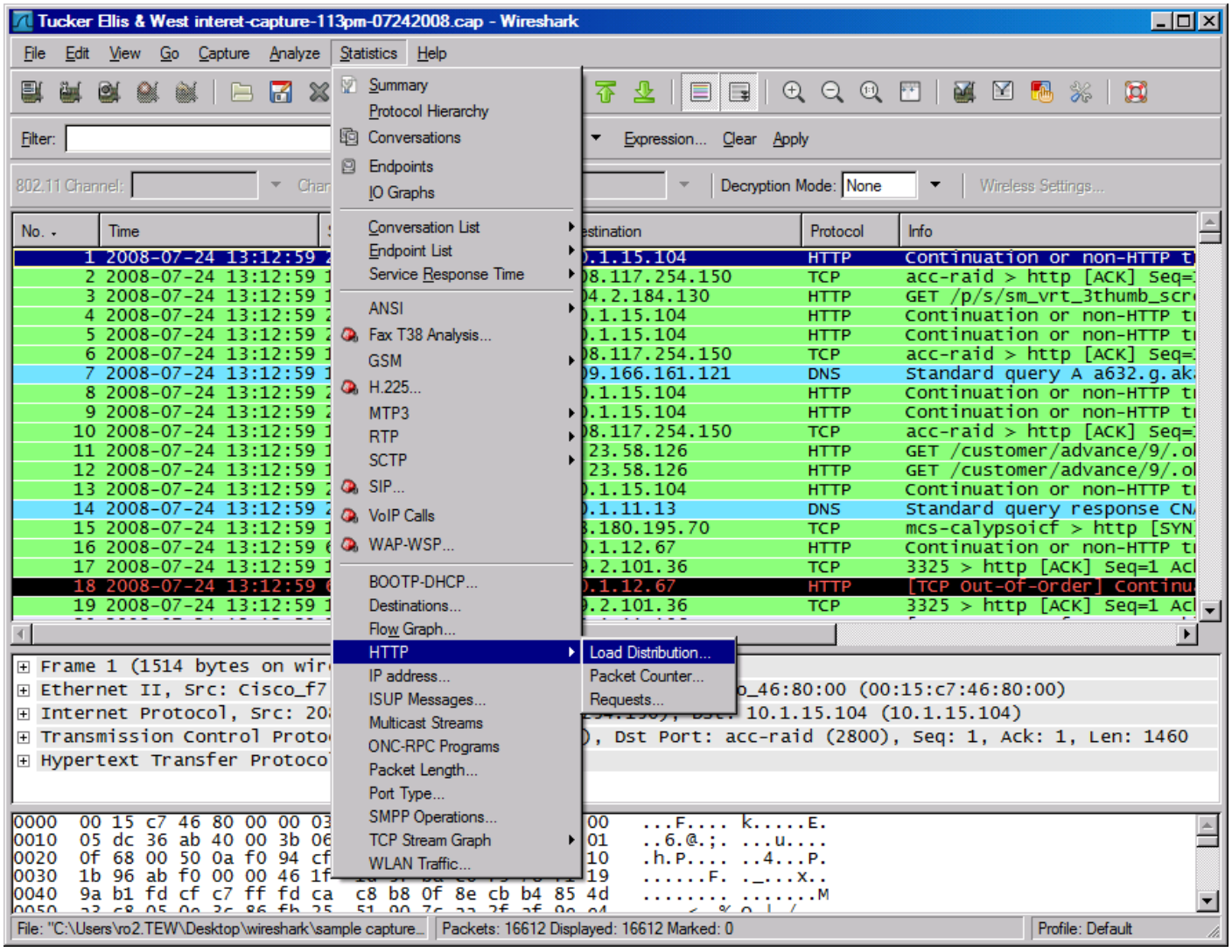


# SIP Analysis

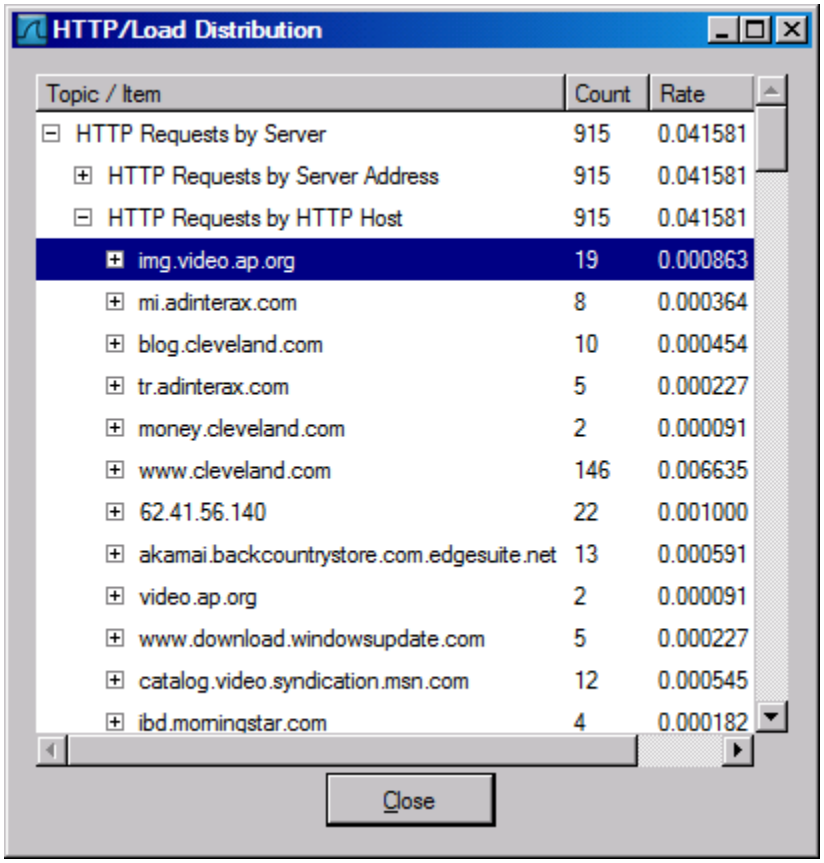


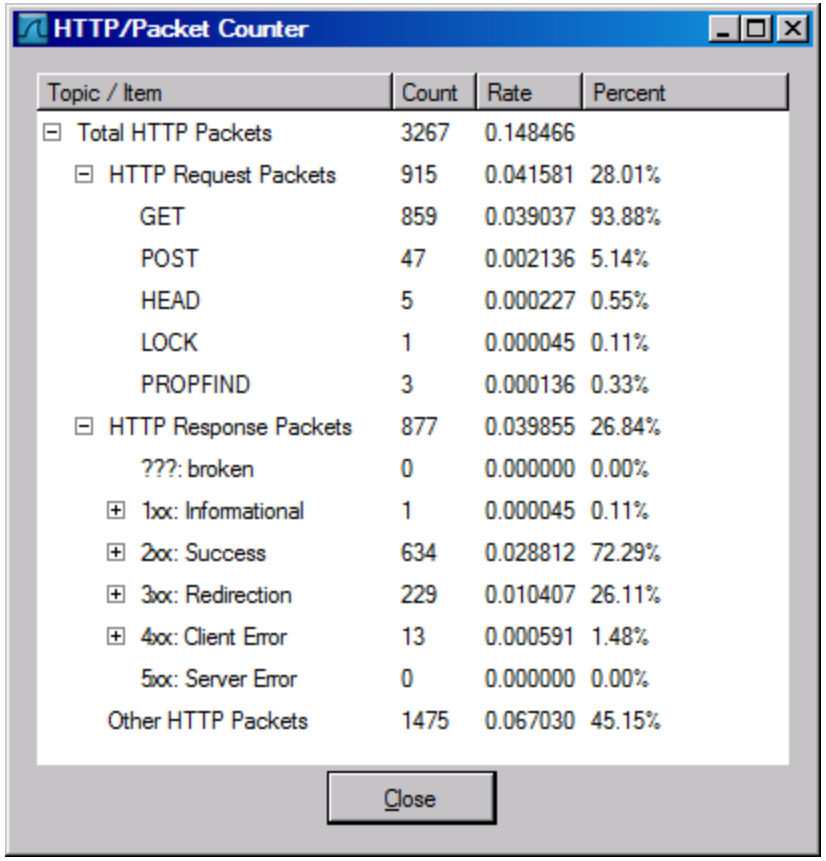
# HTTP Analysis



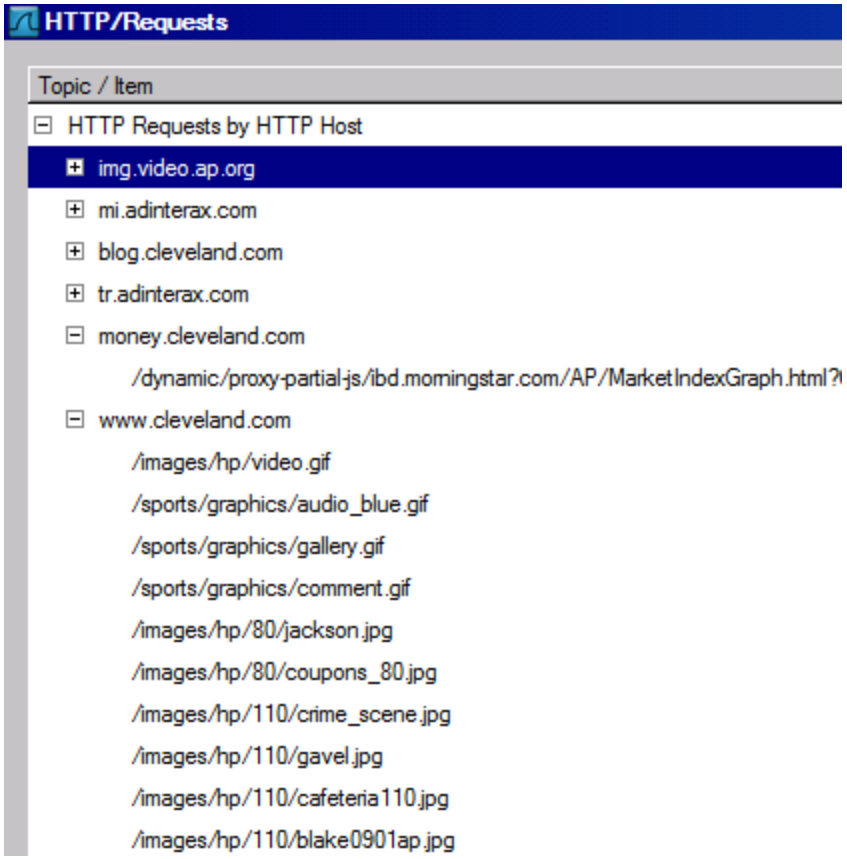
# HTTP Analysis – Load Distribution



# HTTP Analysis – Packet Counter



# HTTP Analysis – Requests



# Melhoria do Desempenho do WireShark

- Não use capture filters
- Aumente o read buffer size
- Evite usar a atualização dinâmica da tela
- Use um bom computador
- Use um TAP
- Não resolva os “names”