



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

OSI MODEL

TCP/IP

UNIX/HP/Sun

Novell

Microsoft

SAN

IBM

ISO

VoIP

VPN/Security

Apple

Layer 7: Application Layer

- Defines interface to user processes for communication and data transfer in network
- Provides standardized services such as virtual terminal, file and job transfer and operation

Layer 6: Presentation Layer

- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data, encrypts and decrypts data, compresses and decompresses data

Layer 5: Session Layer

- Manages user sessions and dialogues
- Controls establishment and termination of logical links between users
- Reports upper layer errors

Layer 4: Transport Layer

- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
- Provides connectionless oriented packet delivery

Layer 3: Network Layer

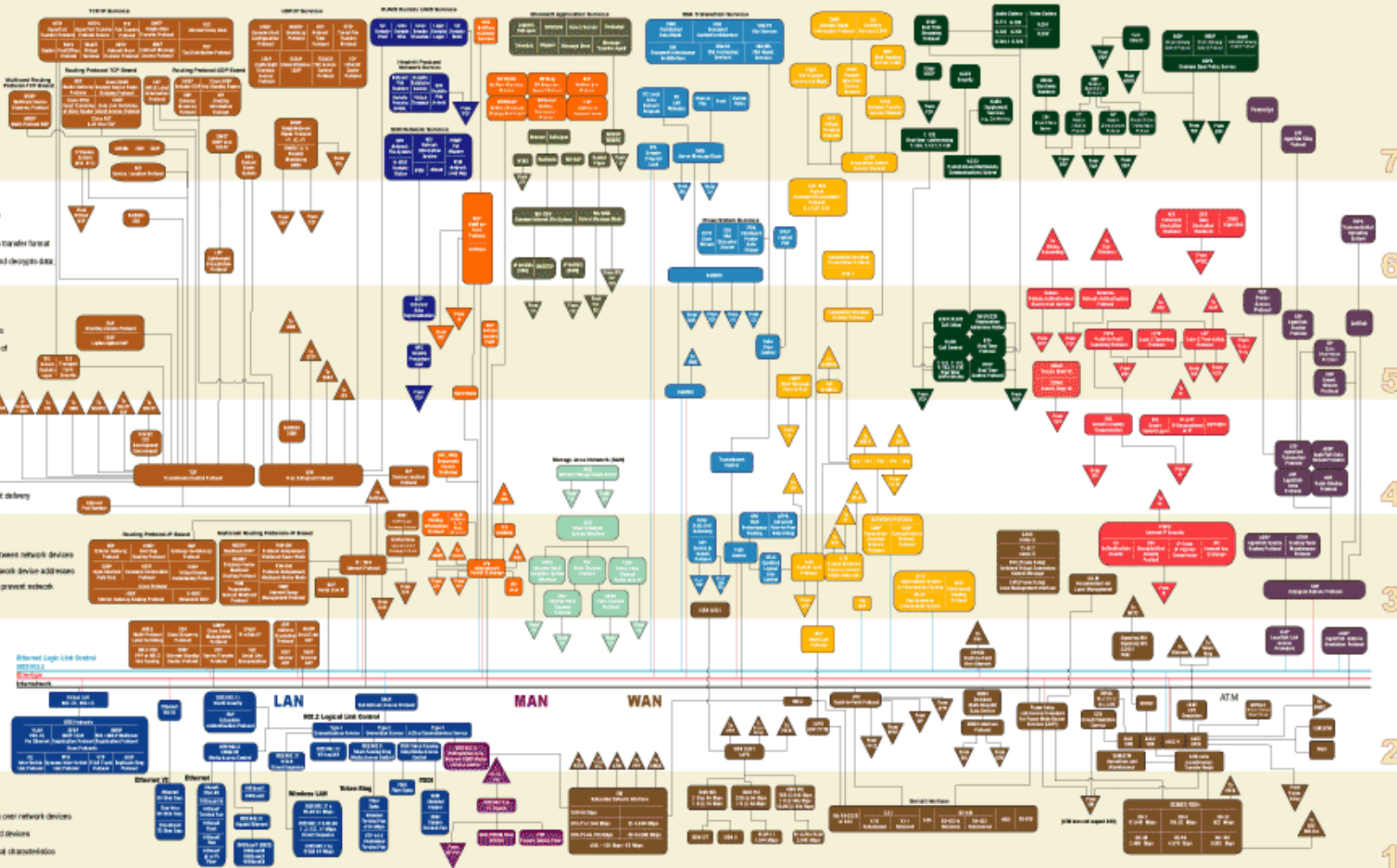
- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer

- Defines procedures for operating the communication link
- Frames packets
- Detects and corrects packets transfer errors

Layer 1: Physical Layer

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics



ANSI
American National Standards Institute
11 West 42nd Street
New York, NY 10036 USA
Tel: 212-512-1800
www.ansi.org

ETSI
European Telecommunications Standards Institute
Route des Lucioles
F-91061 Evry-Courcouronnes, France
Tel: 33 (0)4 67 41 42 00
www.etsi.org

FCI
Federal Communications Commission
1915 M Street NW
Washington, DC 20554
Tel: 202-418-0100
www.fcc.gov

IEEE
Institute of Electrical and Electronics Engineers, Inc.
445 Roca Lane
P.O. Box 1331
Piscataway, NJ 08854-1331 USA
Tel: 908-981-0000
www.ieee.org

ISO
International Organization for Standardization
One rue de Vanille CH-1211
Geneve 20, Switzerland
Tel: 41-22-719-1111
www.iso.ch

ITU
International Telecommunications Union
Place des Nations
CH-1211 Geneva 20, Switzerland
Tel: 41 22 919 51 11
www.itu.ch

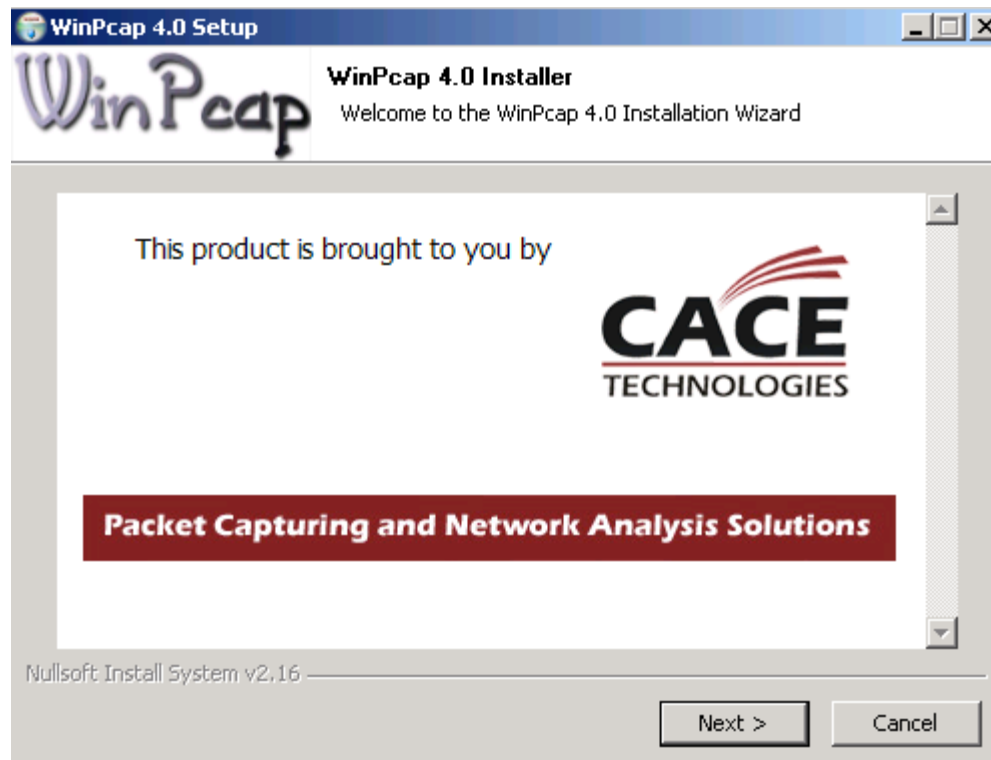
ISO/IEC
International Society
www.iso.org
www.iec.org
ISO/IEC Joint Technical Group
1715, Route de la Gare
CH-1211 Geneva 20, Switzerland
Tel: 41-22-919-60-11
www.iso.org

IEC
International Electrotechnical Commission
1, rue de Vanille
CH-1211 Geneva 20, Switzerland
Tel: 41-22-919-60-11
www.iec.ch

Javvin

Network Communication Protocols Map Copyright © 2004 Javvin Group www.javvin.com info@javvin.com

Instalação



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 Web Test Bauer Ask The Admin >>

WIRESHARK

Wireshark Get Help Develop Tools Buy



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...



Taking Wireshark Into Uncharted Waters

- Analysis
- Charting
- Reporting
- Integrated with Wireshark





Enriching

News

Wireshark is 10! (Plus two bonus announcements)

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

```
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] ...

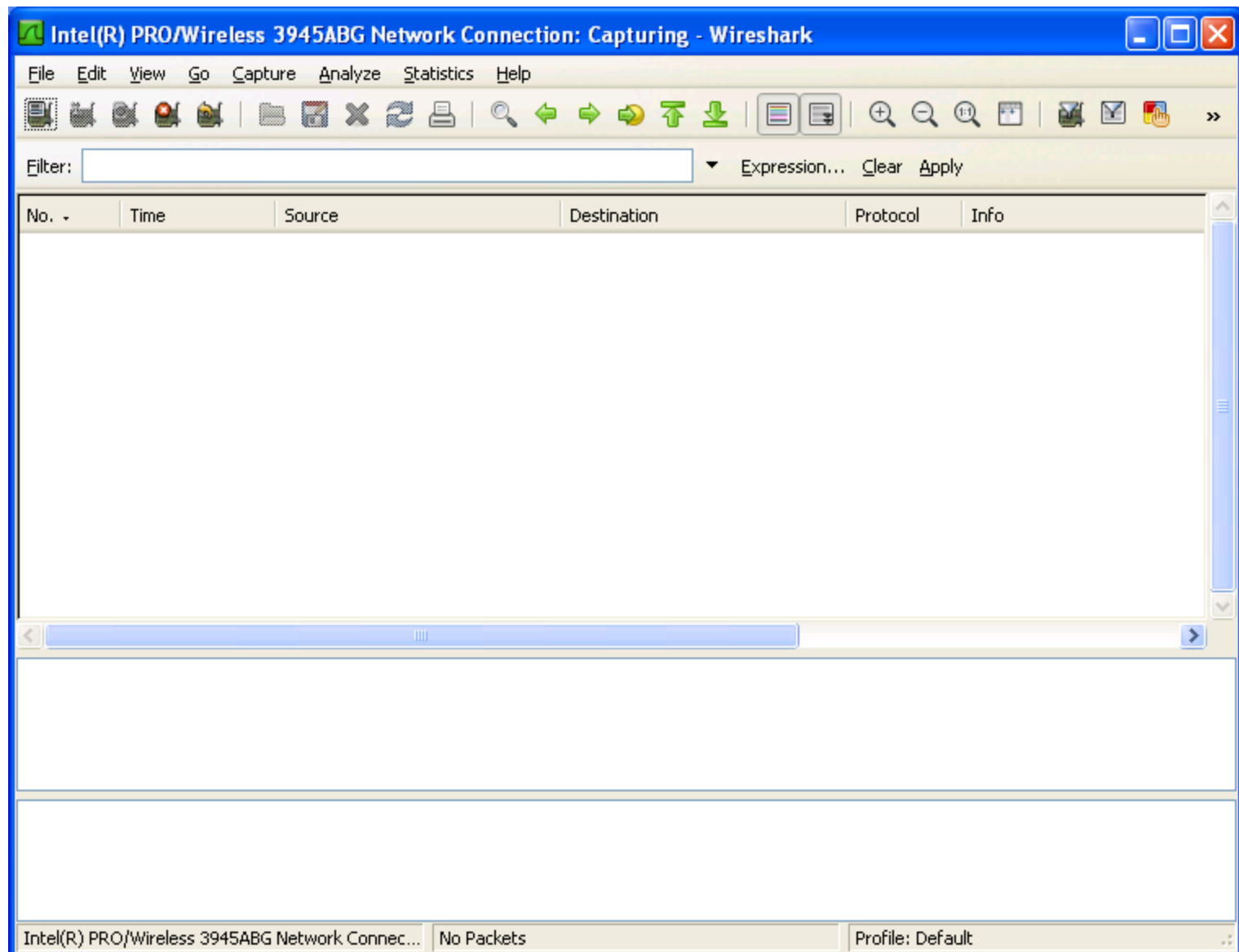
Capture interface:

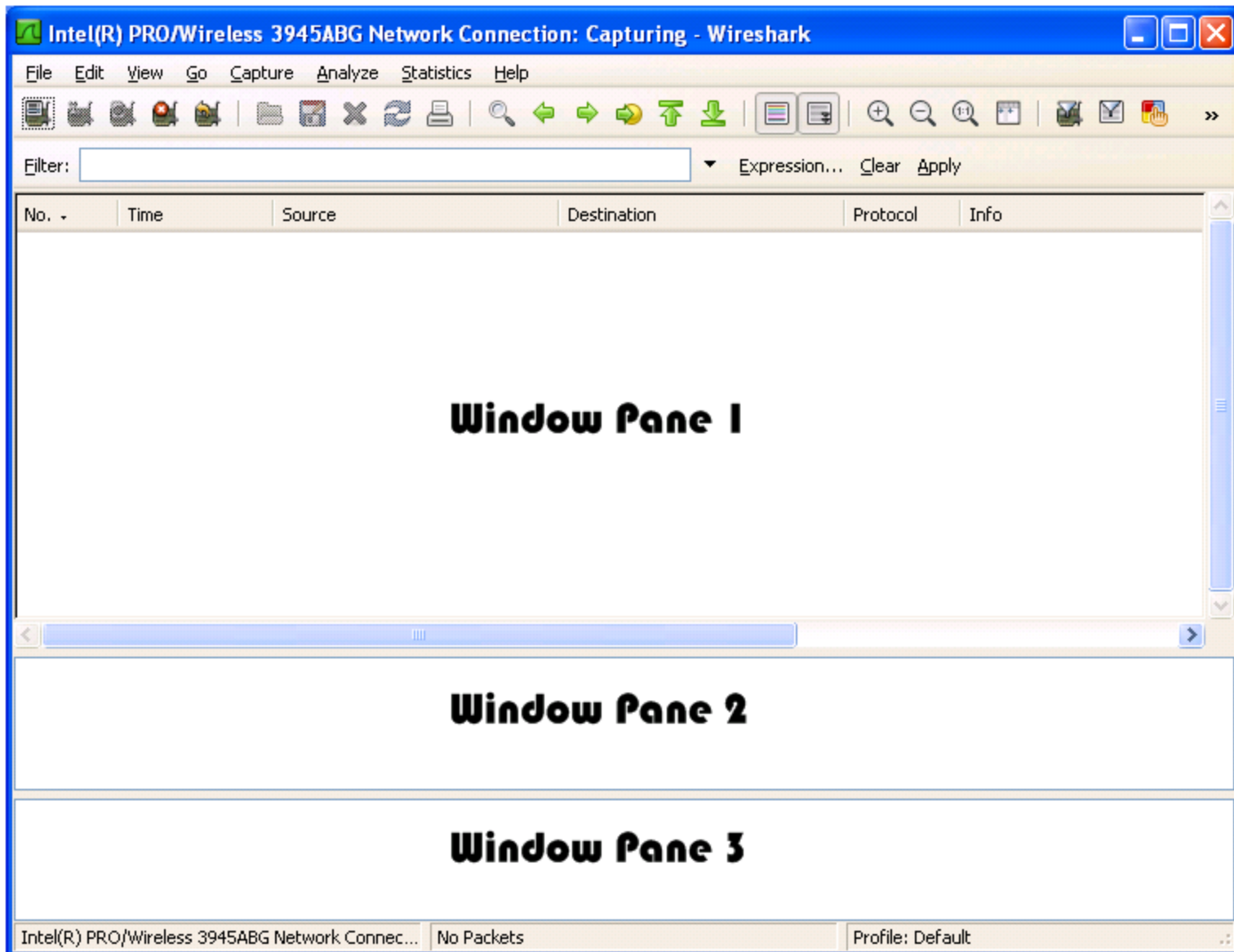
```
-i <interface>      name or idx of interface (def: first non-loopback)
-f <capture filter>  packet filter in libpcap filter syntax
-s <snaplen>         packet snapshot length (def: 65535)
-p                  don't capture in promiscuous mode
-B <buffer size>     size of kernel buffer (def: 1MB)
-y <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
```

.....





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/PAqP/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 aar6.....

0010 03 00 00 0c 20 00 02 b4 a4 63 00 01 00 16 43 4cc....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 0aFas tEtherne

0040 0e 00 03 00 16 46 61 73 74 45 74 68 65 72 6e 65 t1/0/21.(. ..Cisco Interne

0050 74 31 2f 30 2f 32 31 00 04 00 08 00 00 00 28 00 ...Cisco Interne

0060 05 00 dc 43 69 73 63 6f 20 49 6e 74 65 72 6e 65 twork op erating

0070 74 77 6f 72 6b 20 4f 70 65 72 61 74 69 6e 67 20 system s oftware

0080 53 79 73 74 65 6d 20 53 6f 66 74 77 61 72 65 20 .IOS (tm) C3750

0090 0a 49 4f 53 20 28 74 6d 29 20 43 33 37 35 30 20

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Tem... Packets: 51 Displayed: 51 Marked: 0 Dropped: 0 Profile: Default

Janela HEX

The image shows a Wireshark window titled "Tucker Ellis & West aaa.pcap - Wireshark". The packet list on the left shows 19 packets. Packets 2, 3, and 4 are highlighted in yellow. The packet details pane shows the IP header of packet 2, with the Identification field (0x698c) highlighted in blue. A red arrow points from the text "Highlighted packets here" to the yellow-highlighted packets in the list, and another red arrow points from the same text to the blue-highlighted Identification field. The hex dump pane shows the raw data of packet 2, with the first 10 bytes (0000 ff ff ff ff ff ff 00 e0) highlighted in blue. A red arrow points from the text "Are shown here as well" to this blue-highlighted area.

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 1
19	0.001640	192.168.1.2	212.242.33.35	SIP	Request: REGISTER sip:sip.cyt

Header length: 20 bytes
+ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 78
Identification: 0x698c (27020)
+ Flags: 0x00
Fragment offset: 0

0000 ff ff ff ff ff ff 00 e0 ed 01 6e bd 08 00 45 00n...E.
0010 00 4e 69 8c 00 34 56 11 4c c1 c0 a8 01 02 c0 a8 .Ni...L.....
0020 01 ff 00 89 00 34 56 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 45E FEDEJFPE
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43 FEENE EEOCACAL
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

Menu

The image shows the Wireshark network traffic analysis tool. The main window displays a list of captured packets. The first packet is an ARP request from DellComp_4f:36:23 to Broadcast, asking for the MAC address of 192.168.1.1. Subsequent packets are ICMP Echo (ping) requests and replies between 192.168.1.101 and 143.89.14.34.

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 00:06:00:08:74:4f
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

The packet details pane for the first packet shows the following structure:

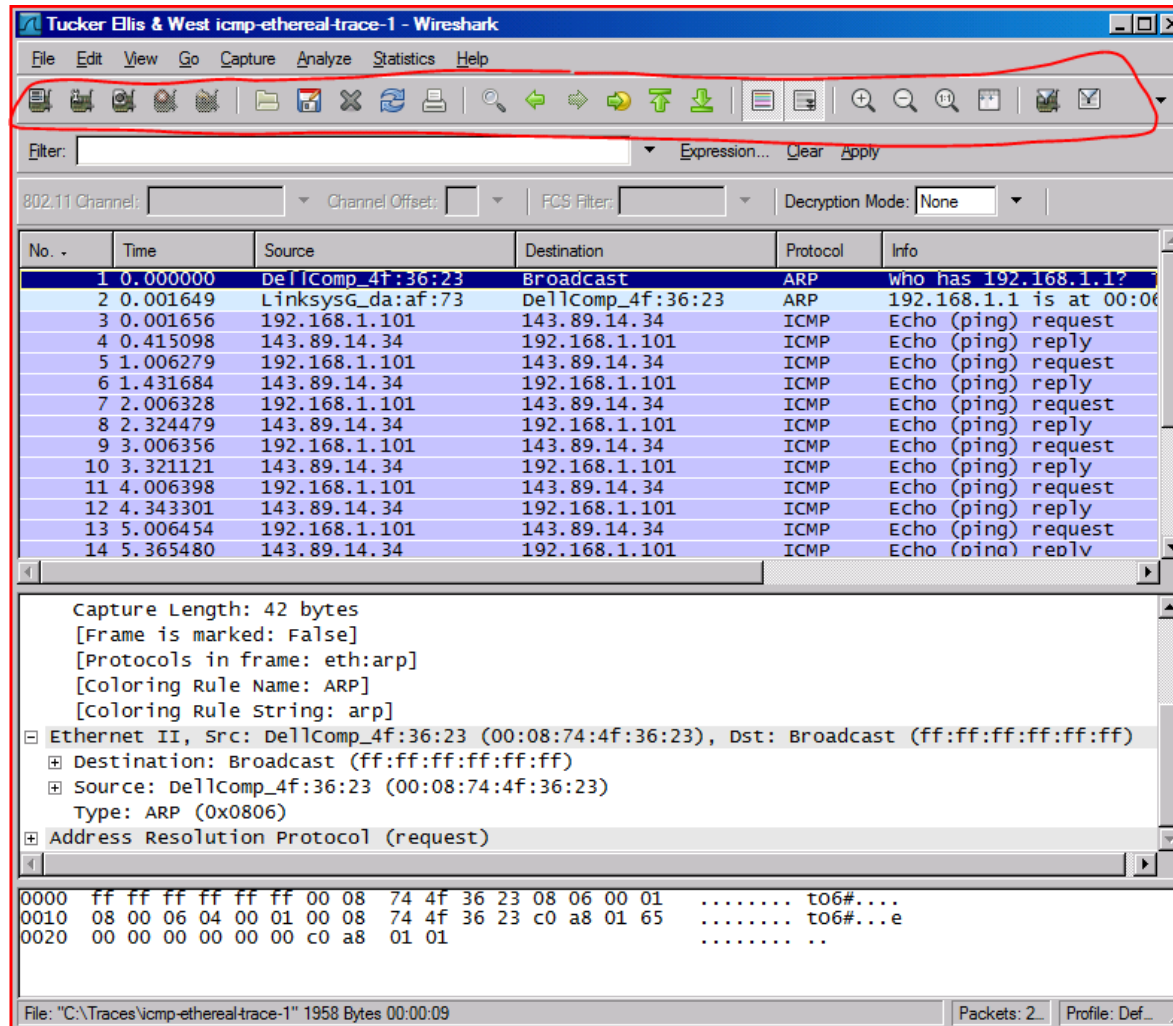
- Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: DellComp_4f:36:23 (00:08:74:4f:36:23)
 - Type: ARP (0x0806)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  ff ff ff ff ff ff 00 08 74 4f 36 23 08 06 00 01  .... t06#....
0010  08 00 06 04 00 01 00 08 74 4f 36 23 c0 a8 01 65  .... t06#...e
0020  00 00 00 00 00 00 c0 a8 01 01  .... ..
```

The status bar at the bottom indicates: File: "C:\Traces\icmp-ethereal-trace-1" 1958 Bytes 00:00:09, Packets: 2, Profile: Def...

Barra de Buttons



Status Bar

The image shows a Wireshark window titled "Tucker Ellis & West icmp-ethereal-trace-1 - Wireshark". The main display area shows a list of 14 captured packets. The first packet is an ARP request from DellComp_4f:36:23 to Broadcast. The second packet is an ARP reply from LinksysG_da:af:73 to DellComp_4f:36:23. The remaining packets are ICMP Echo (ping) requests and replies between 192.168.1.101 and 143.89.14.34.

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 00:08:74:4f:36:23
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

The packet details pane shows the following information for the selected packet (No. 1):

- 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)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 ff ff ff ff ff ff 00 08 74 4f 36 23 08 06 00 01 ..... t06#....
0010 08 00 06 04 00 01 00 08 74 4f 36 23 c0 a8 01 65 ..... t06#...e
0020 00 00 00 00 00 00 c0 a8 01 01 ..... ..
```

The status bar at the bottom of the window is circled in red and displays the following information:

File: "C:\Traces\icmp-ethereal-trace-1" 1958 Bytes 00:00:09 Packets: 2 Profile: Def...

Status Bar

The image shows a Wireshark window titled "Tucker Ellis & West aaa.pcap - Wireshark". The main pane displays a list of 19 network packets. The details pane for the selected packet (No. 19) shows the following information:

- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
- Total Length: 78
- Identification: 0x698c (27020)
- Flags: 0x00
- Fragment offset: 0

The packet data is shown in hexadecimal and ASCII. The status bar at the bottom indicates "Identification (ip.id), 2 bytes" and "Packets: 691 Displayed: 691 Marked: 0".

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 1
19	0.001640	192.168.1.2	212.242.33.35	SIP	Request: REGISTER sip:sip.cyt

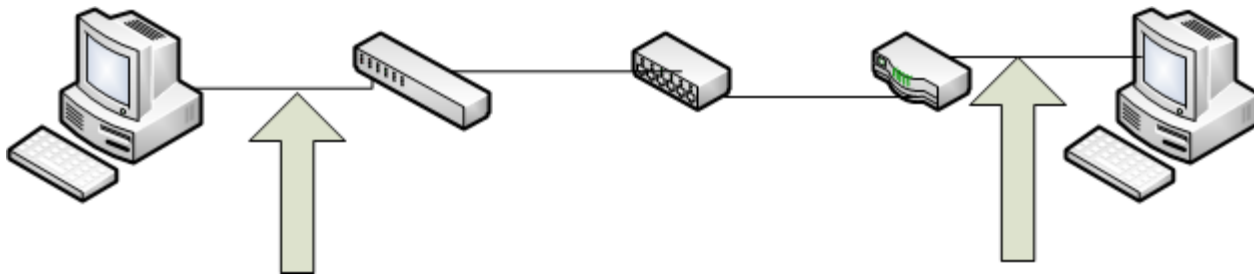
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 78
Identification: 0x698c (27020)
Flags: 0x00
Fragment offset: 0

0000 ff ff ff ff ff ff 00 e0 ed 01 6e bd 08 00 45 00n...E.
0010 00 4e 69 8c 00 00 80 11 4c c1 c0 a8 01 02 c0 a8 .N....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 45E 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. ...

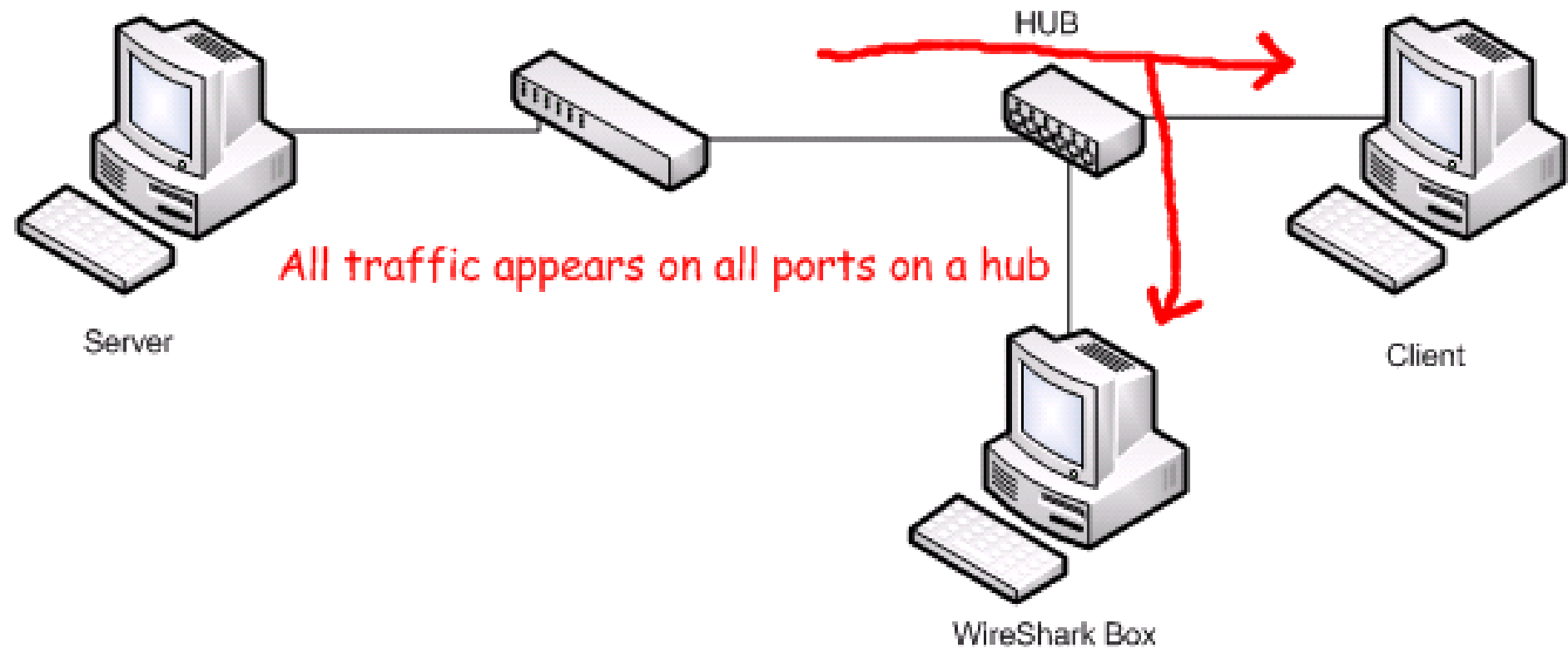
Identification (ip.id), 2 bytes
Packets: 691 Displayed: 691 Marked: 0
Profile: Default

Onde eu devo usar o
WireShark?

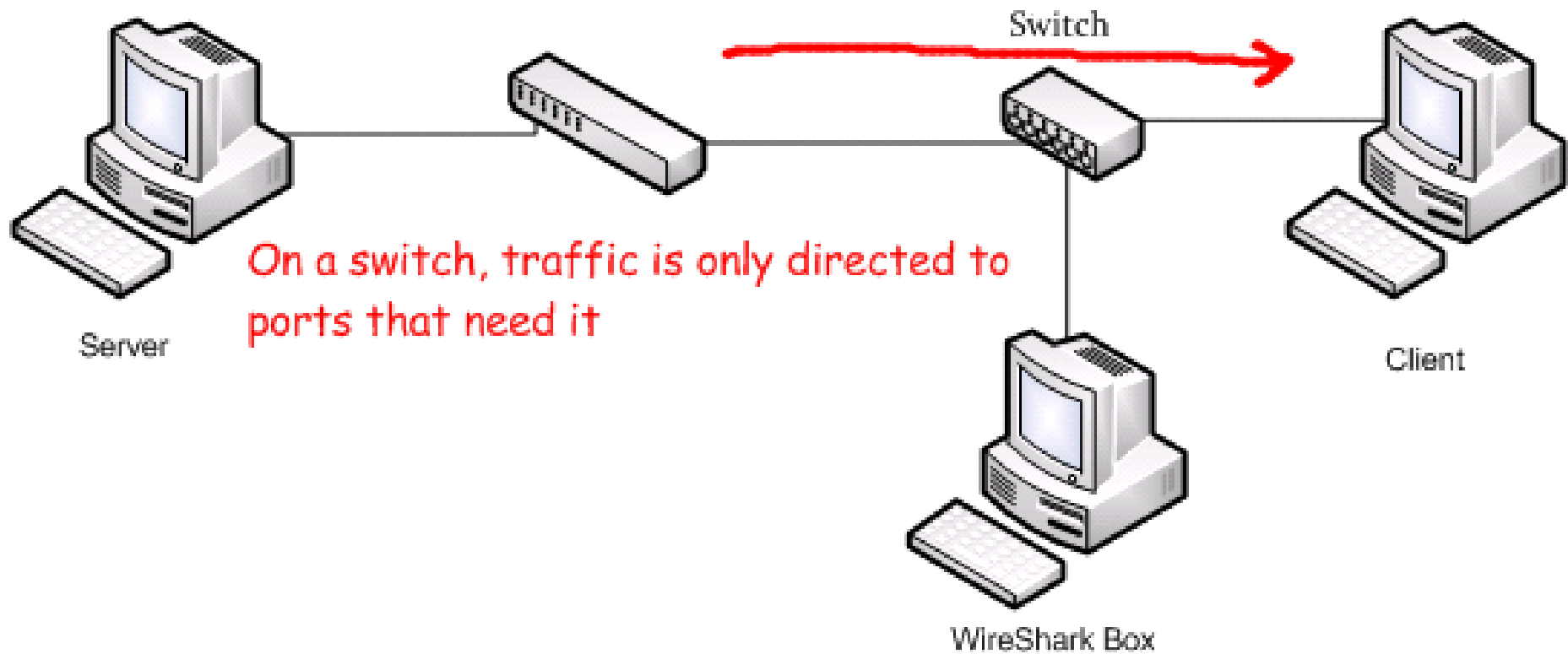
A localização muda TUDO !



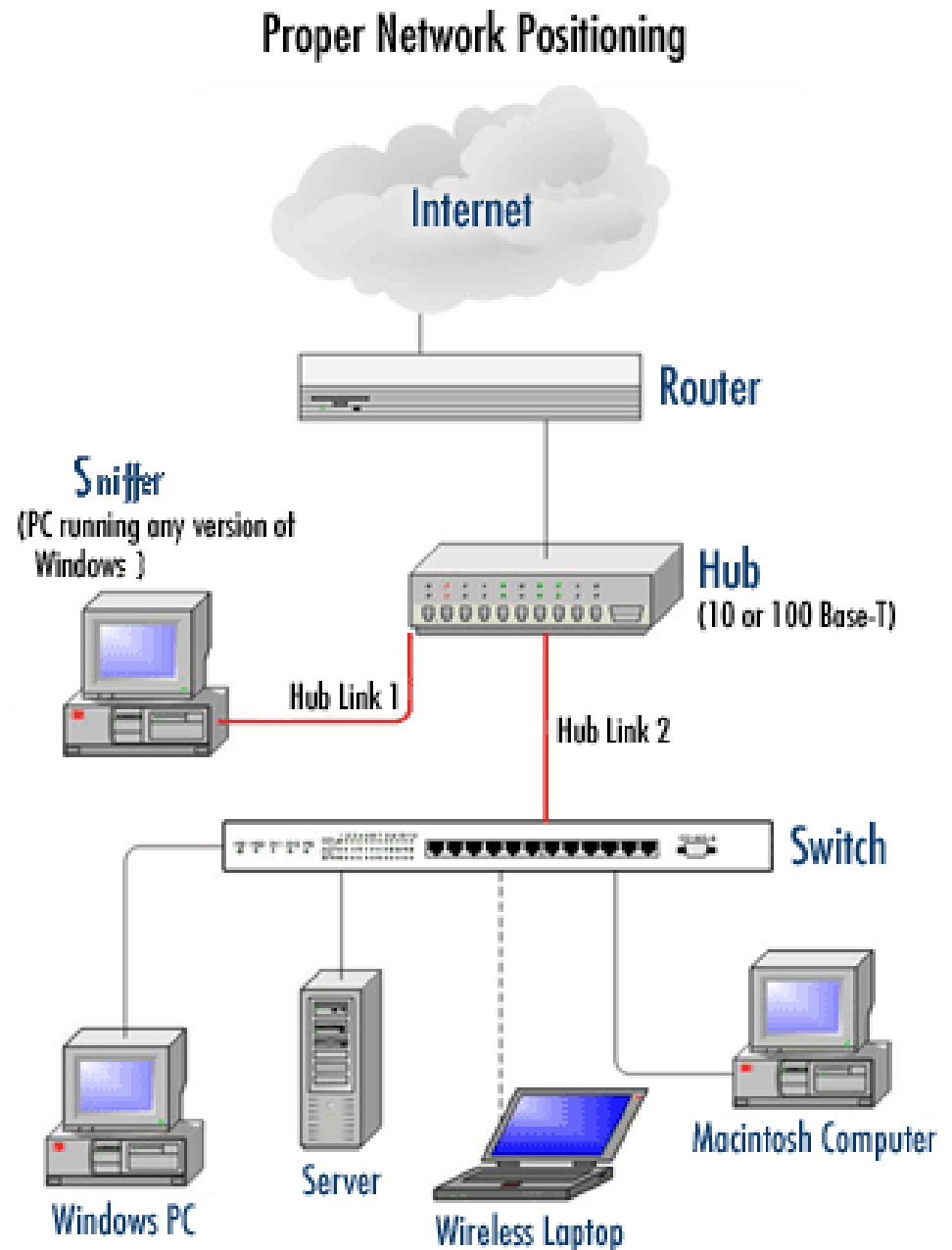
Hub



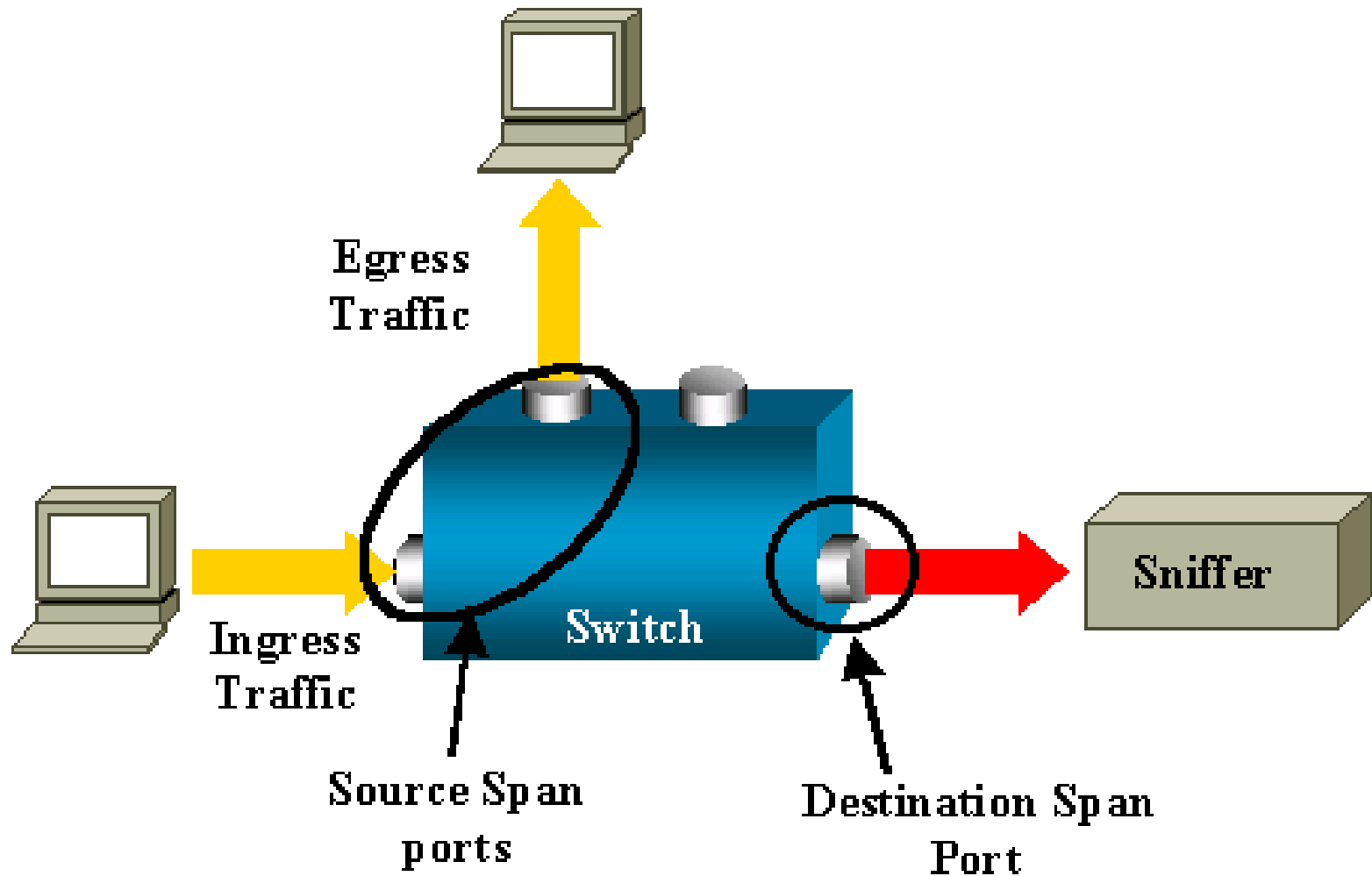
Switches



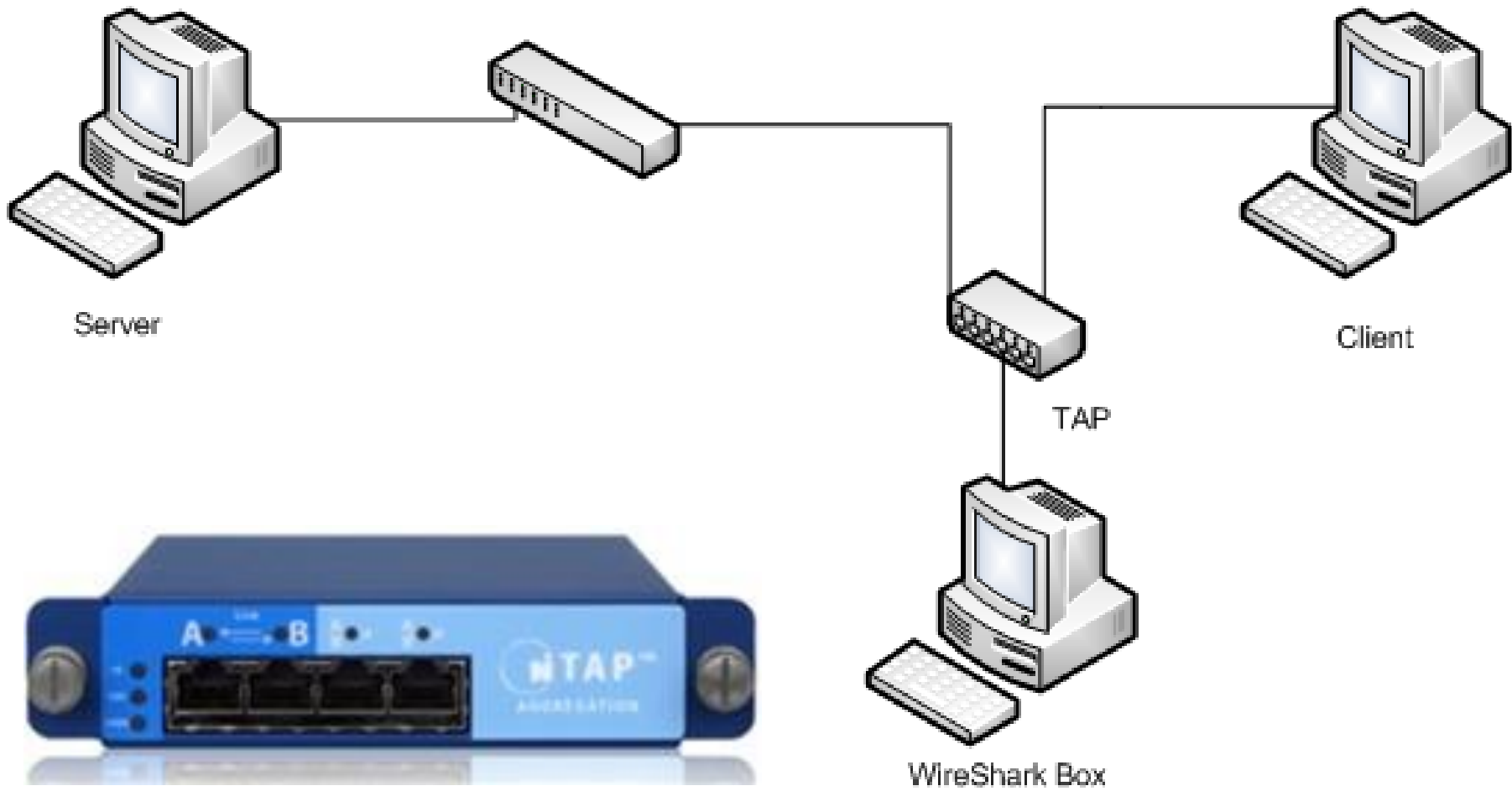
Não é o ideal, mas funciona



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//

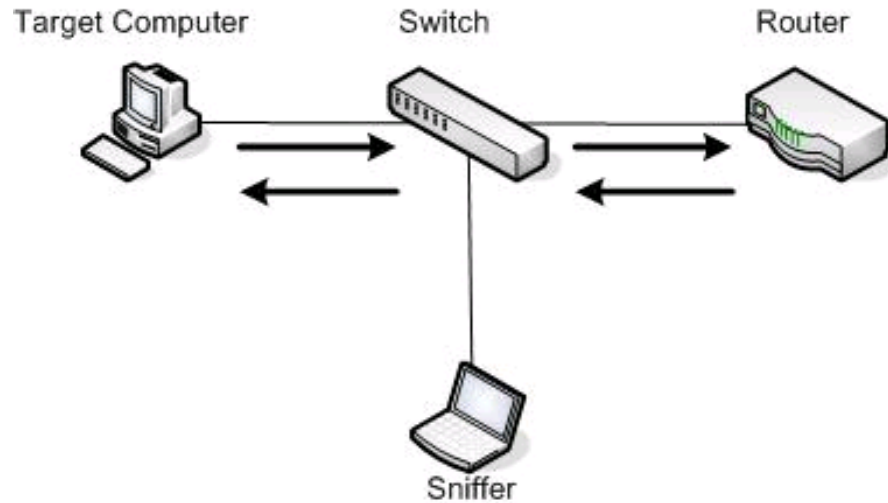
- switch(config-if)#**port monitor FastEthernet 0/3** //especificar a porta que será espelhada//

- switch(config-if)#**exit**

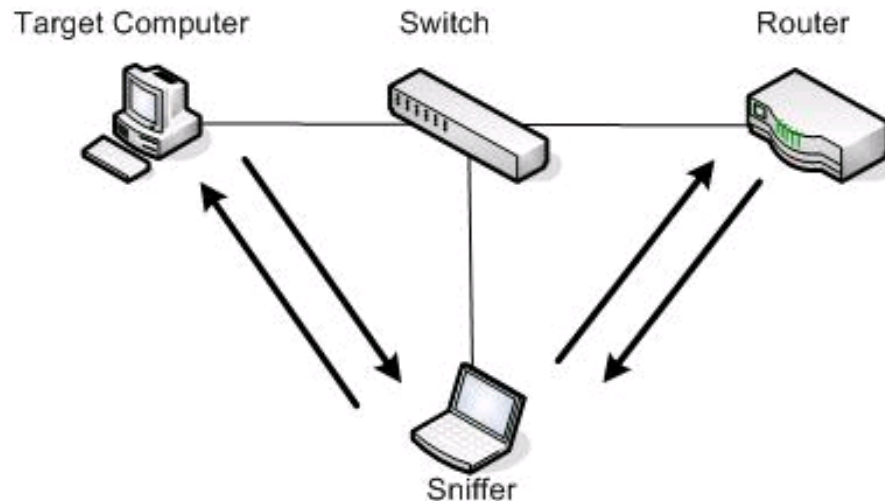
- switch(config)#**exit**

ARP Cache Poisoning

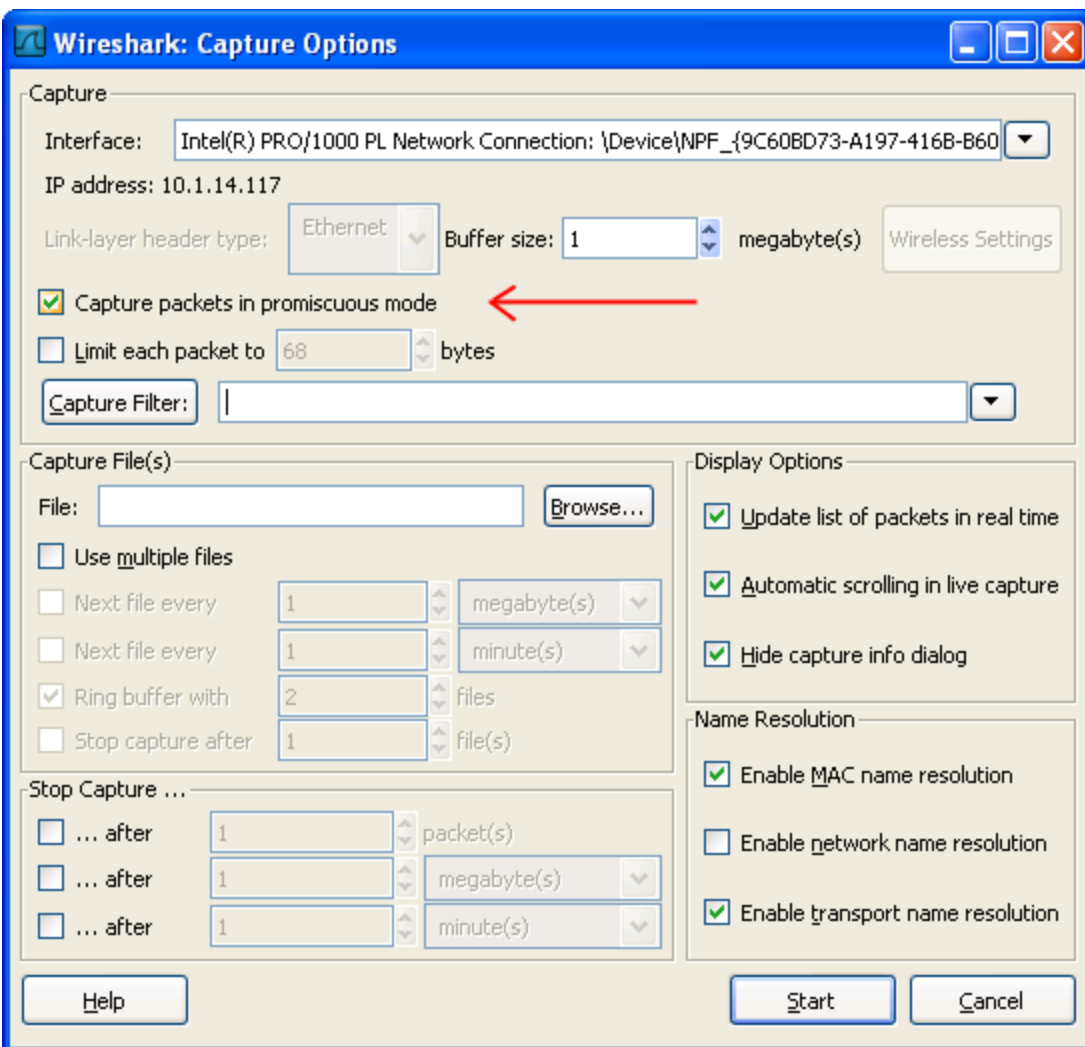
Normal Traffic Pattern



Poisoned ARP Cache

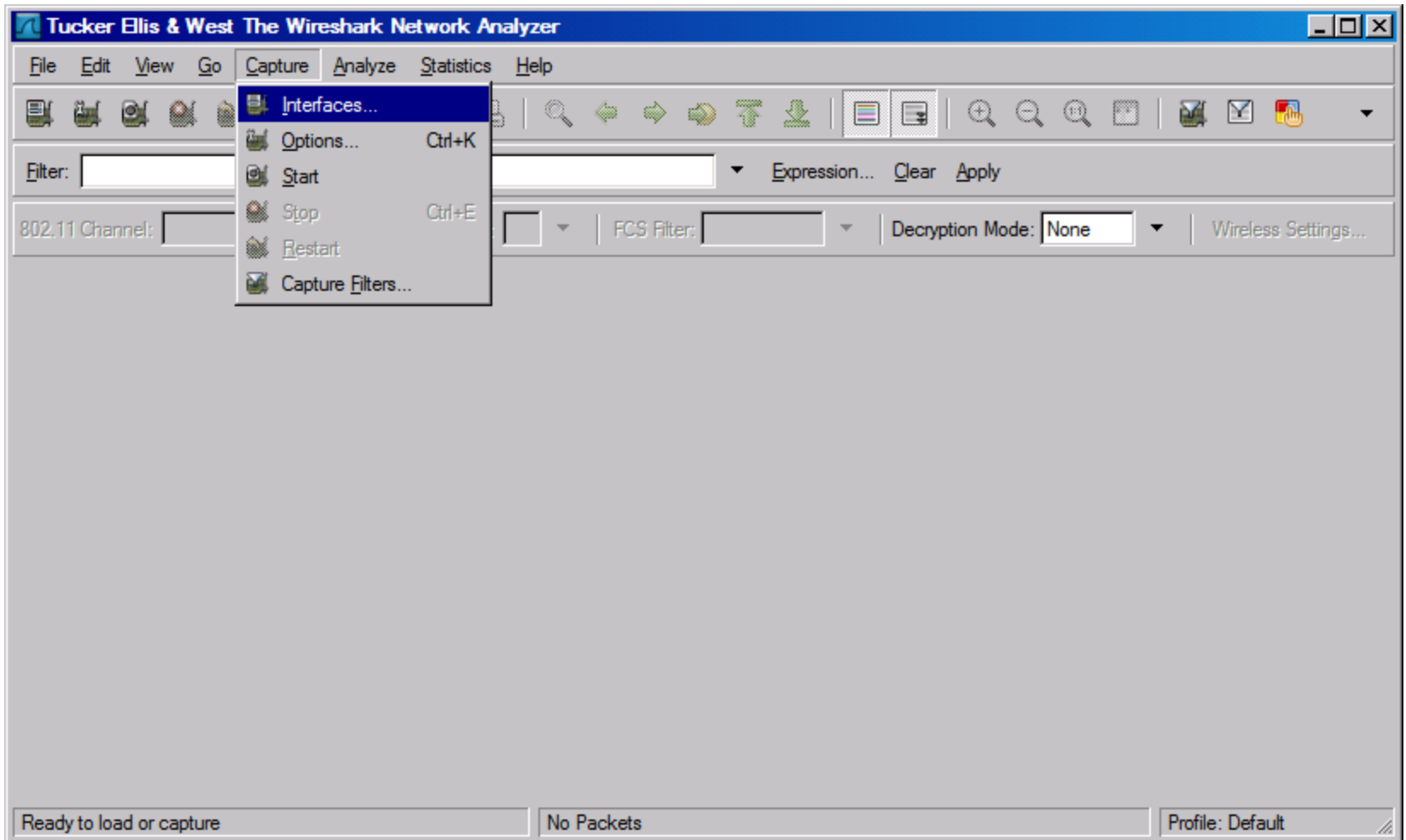


Promiscuous Mode

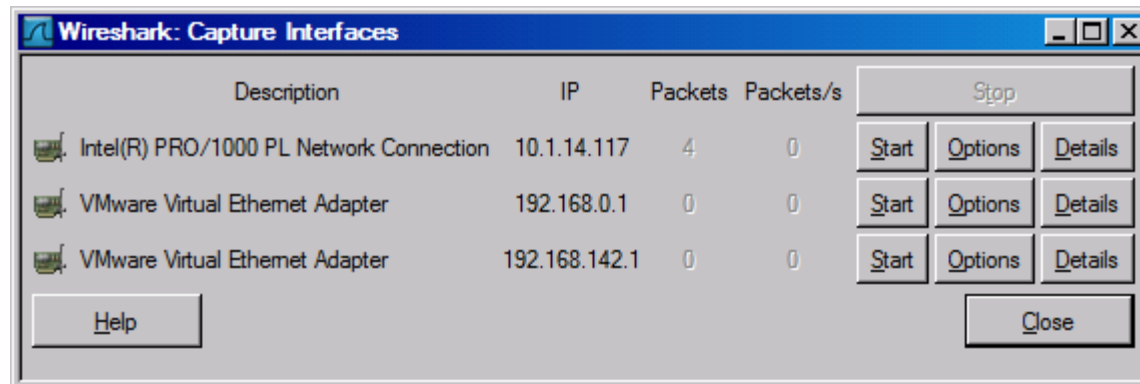


Marcando este box, estamos determinando que a interface escolhida fique em MODO PROMÍSCUO durante a captura. Se isso não for feito, o Wireshark apenas capturarão quadros broadcast e os que saem e entram na máquina onde está o sniffer.

Captura Simples



Escolha da Interface



Opções de Captura

Tucker Ellis & West Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/1000 PL Network Connection: \Device\NPF_{97708CAB-FF09-4180-S} ▼

IP address: 10.1.14.117

Link-layer headertype: Ethernet ▼ Buffer size: 1 megabyte(s) Wireless Settings

☒ 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)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s) ▼

☐ ... after 1 minute(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

Help Start Cancel

Filtragem de Tráfego

Exemplos de Filtros

host 10.1.11.24

host 192.168.0.1 and host 10.1.11.1

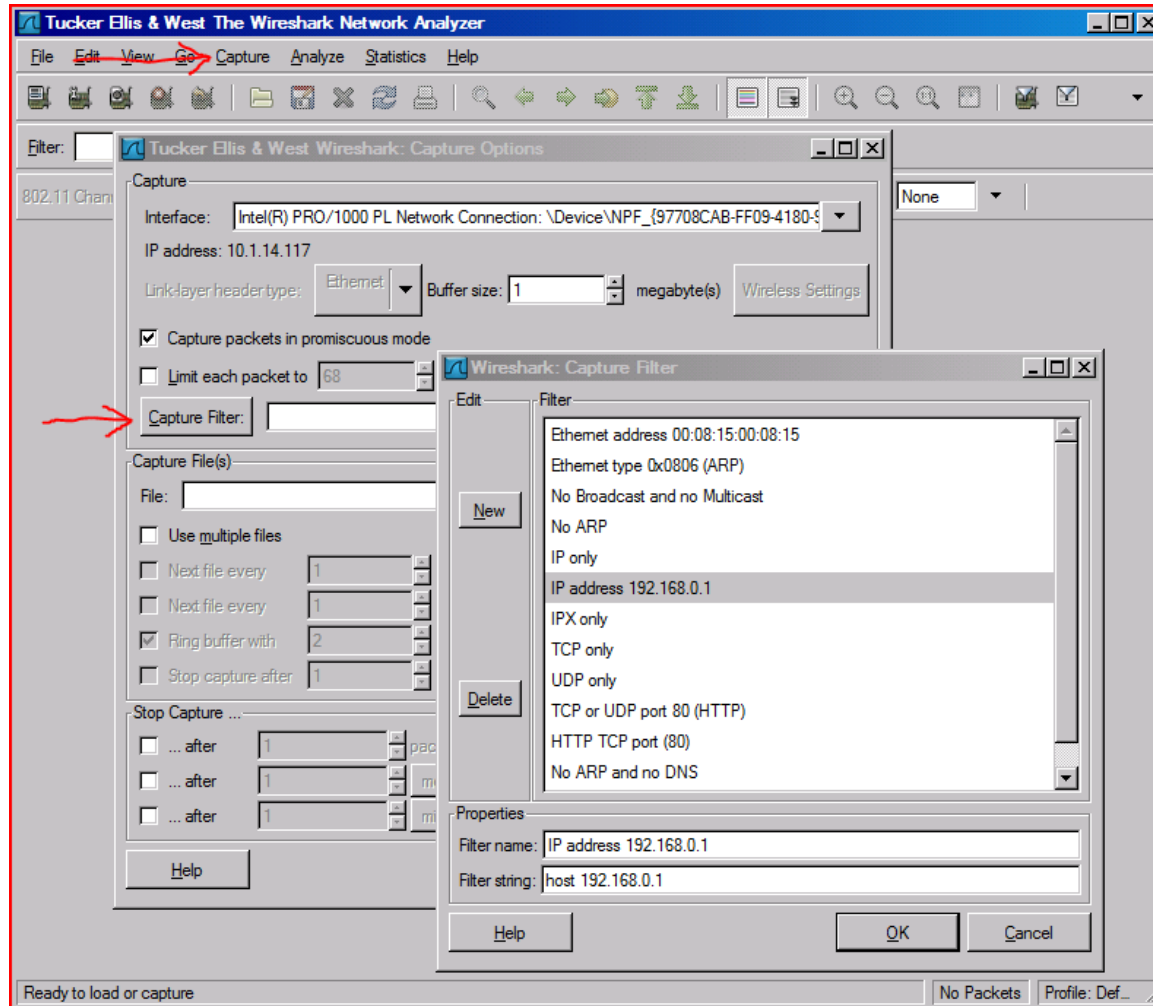
tcp port http

ip

not broadcast not multicast

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

Capture Filter



Capture Options

Tucker Ellis & West Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/1000 PL Network Connection: \Device\NPF_{97708CAB-FF09-4180-9...}

IP address: 10.1.14.117

Linklayer headertype: Ethernet Buffer size: 1 megabyte(s) [Wireless Settings](#)

☒ Capture packets in promiscuous mode

☐ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File: c:\cap1.pcap [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)

Stop Capture ...

☐ ... after 1 packet(s)

☐ ... after 1 megabyte(s)

☐ ... after 1 minute(s)

Display Options

☒ Update list of packets in real time

☒ Automatic scrolling in live capture

☒ Hide capture info dialog

Name Resolution

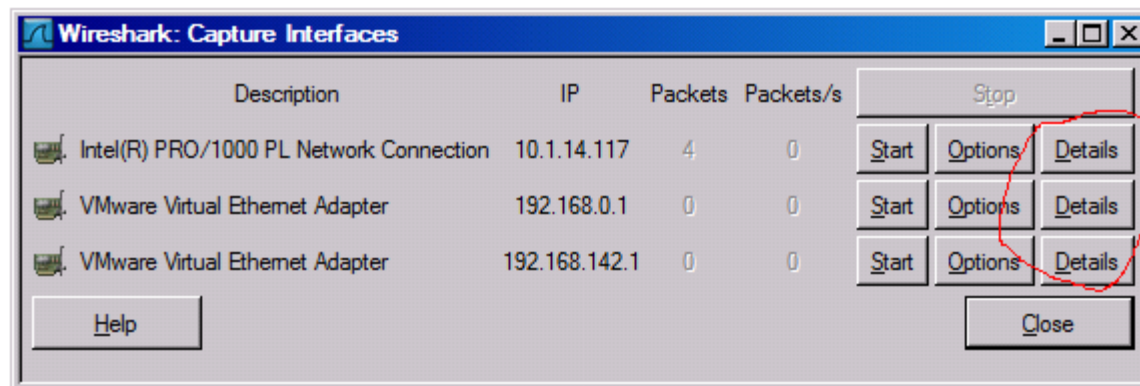
☒ Enable MAC name resolution

☐ Enable network name resolution

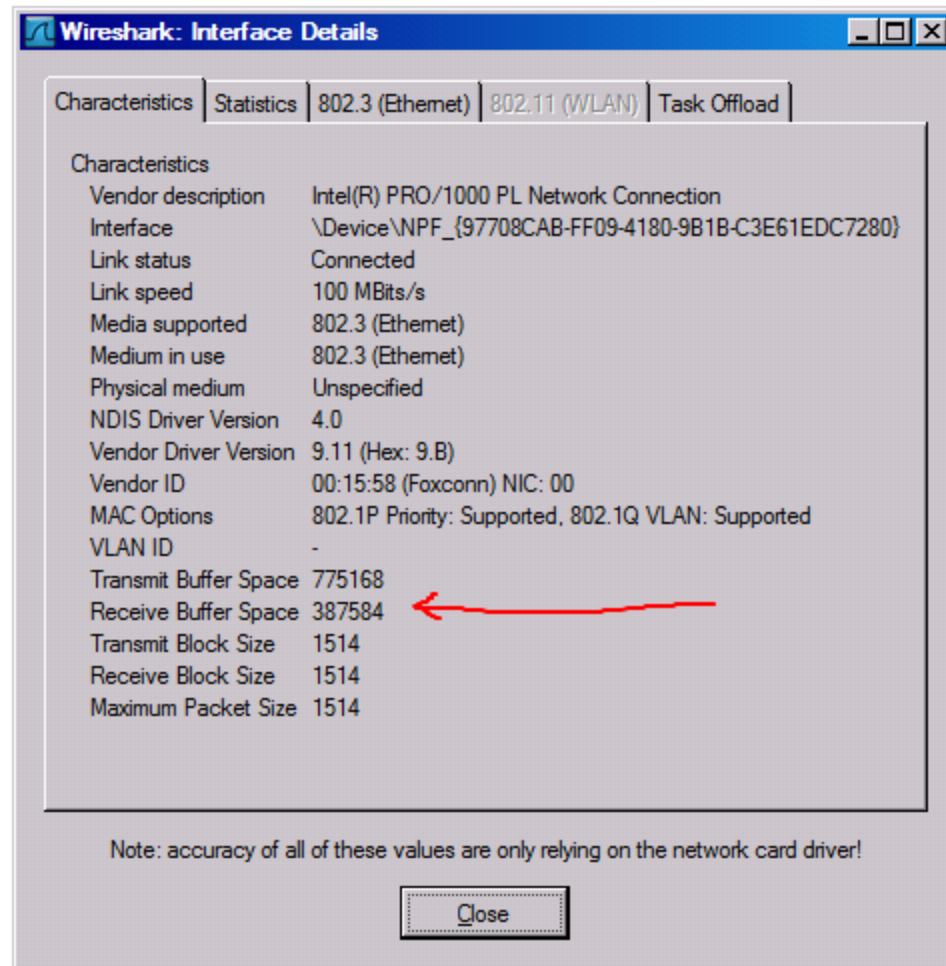
☒ Enable transport name resolution

[Help](#) [Start](#) [Cancel](#)

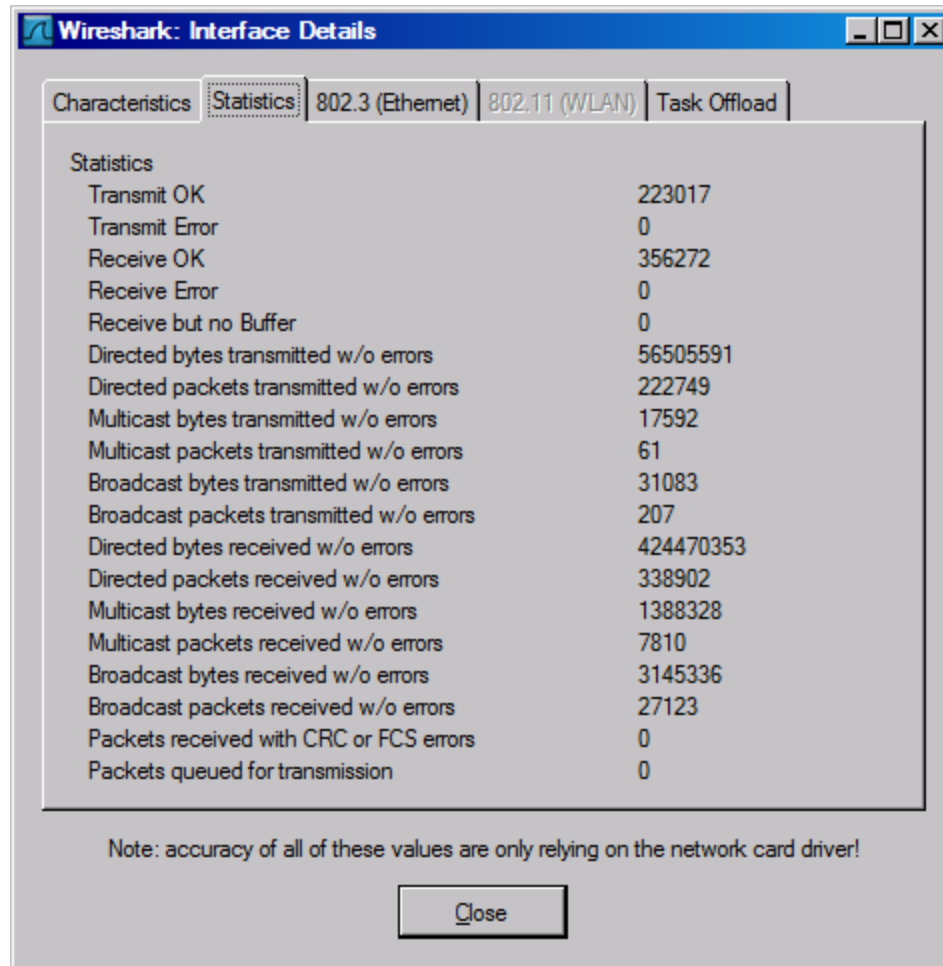
Capture Interfaces



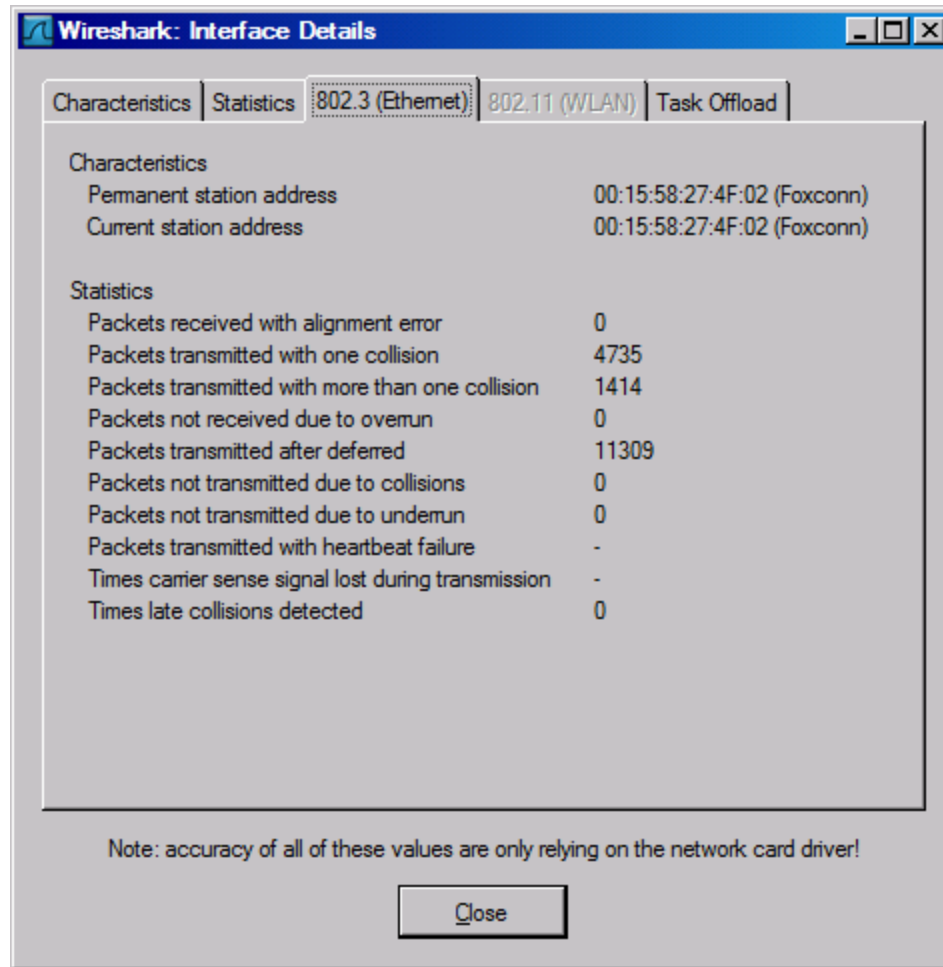
Interface Details: Characteristics



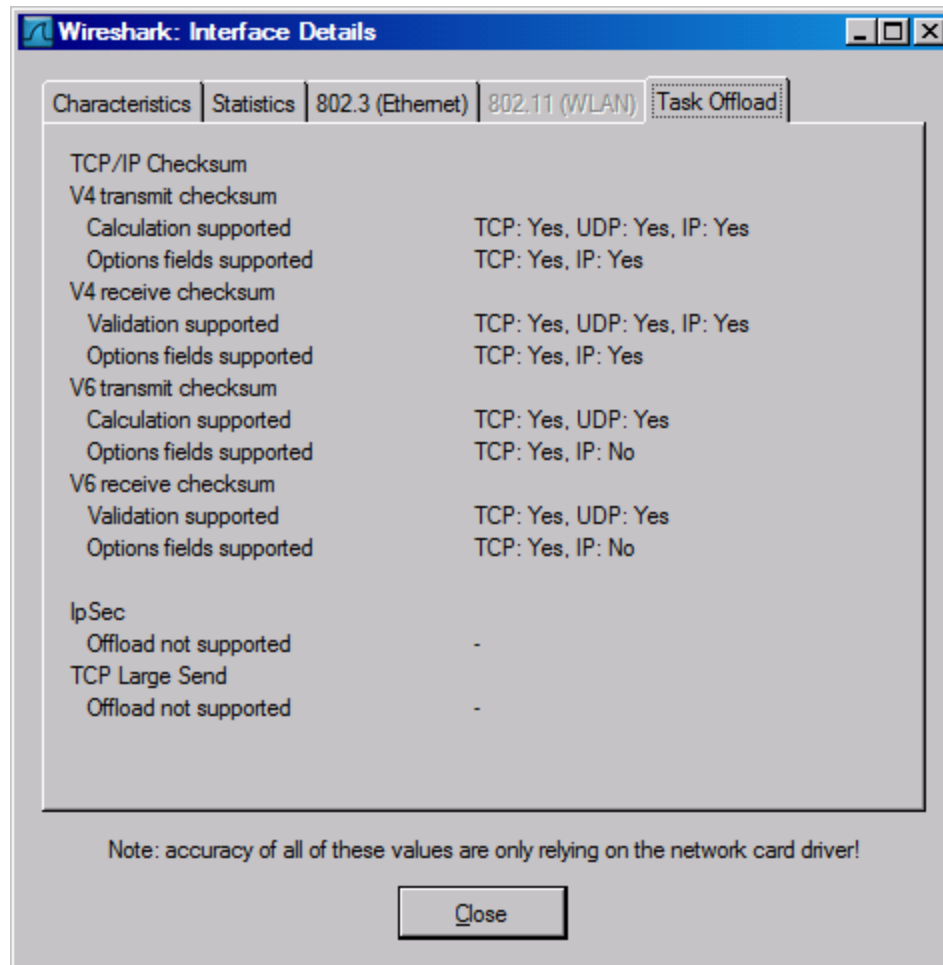
Interface Details: Statistics



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):

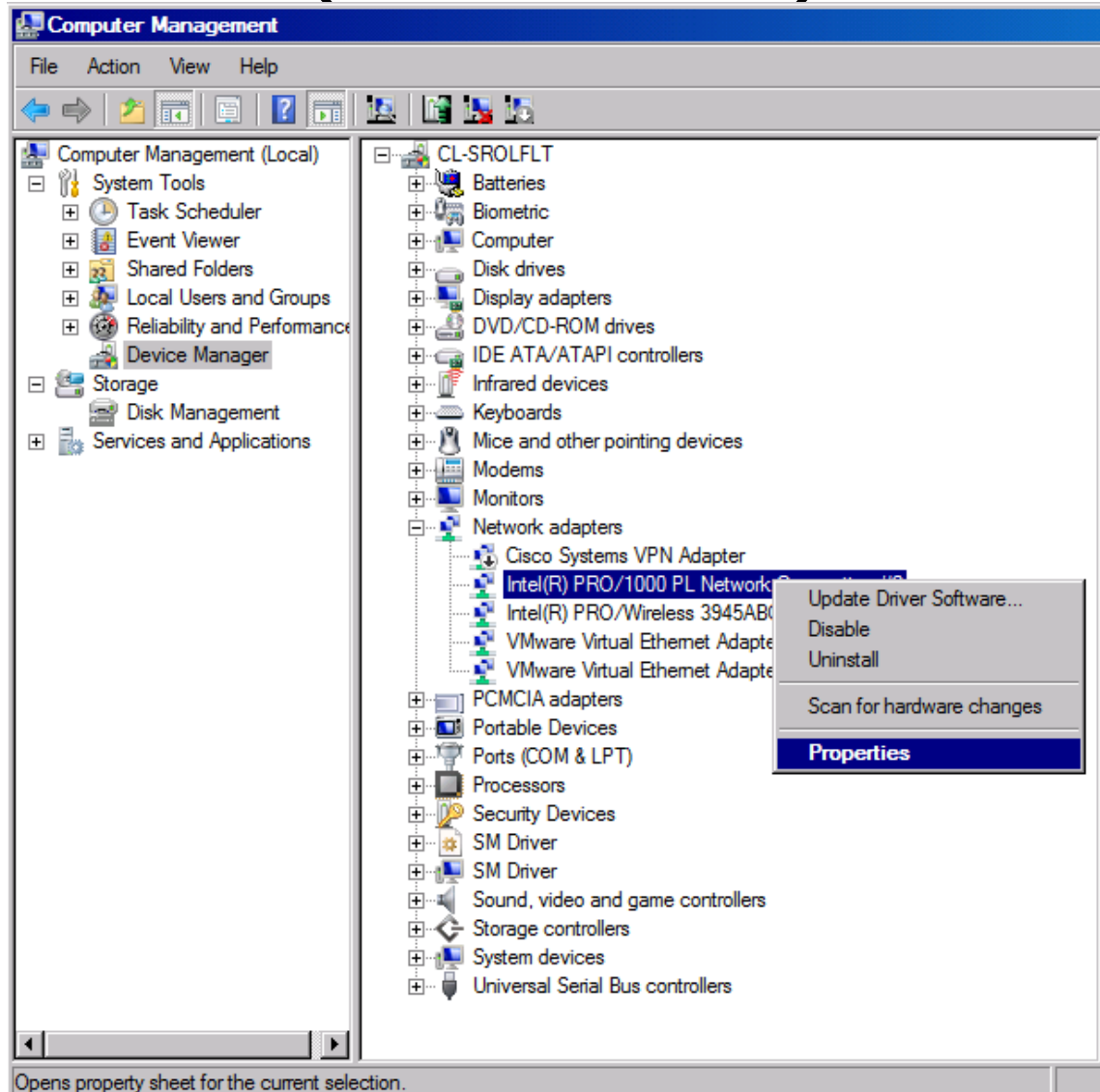
```
ifconfig em0 -rcxsum -tcxsum (choose correct network interface if not em0)
```

On MacOS (as root):

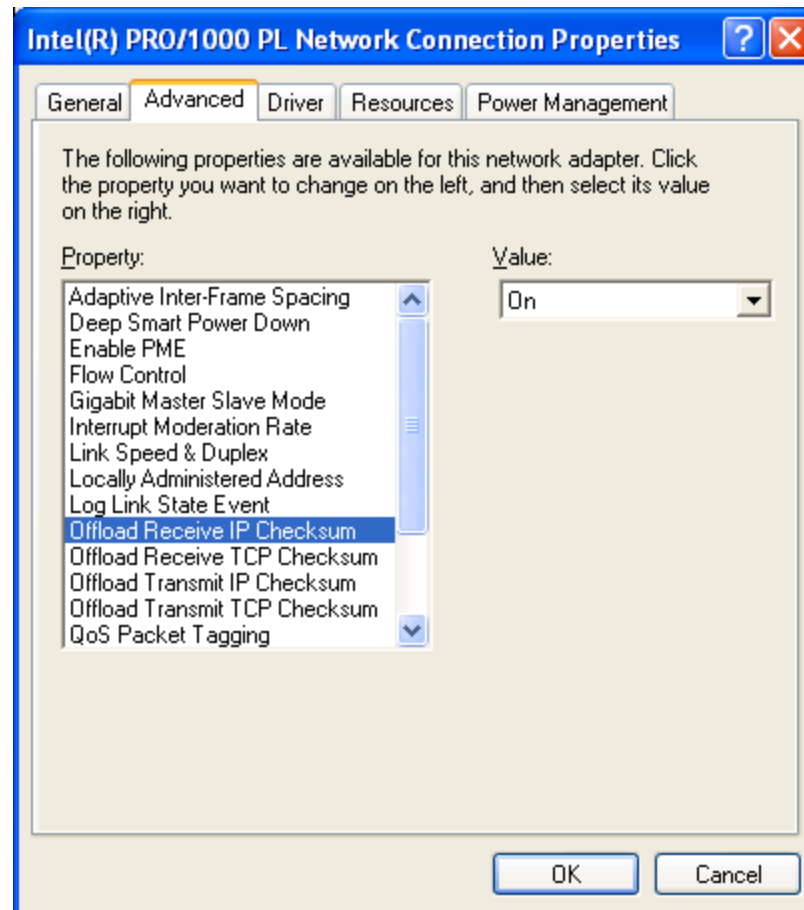
```
sysctl -w net.link.ether.inet.apple_hwcksum_tx=0
```

```
sysctl -w net.link.ether.inet.apple_hwcksum_rx=0
```

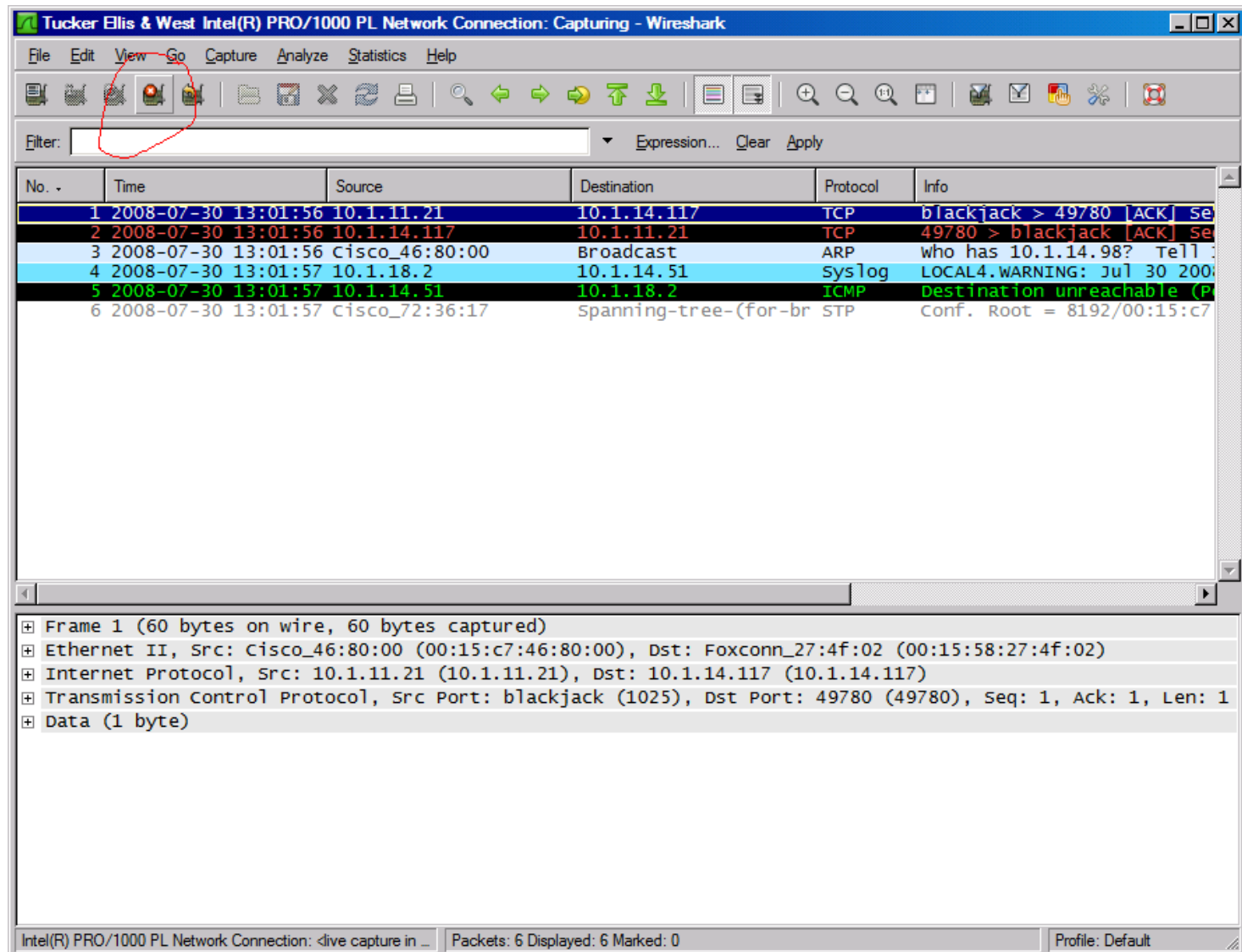
Turning off Checksum offload (Windows)



Turning off Checksum offload



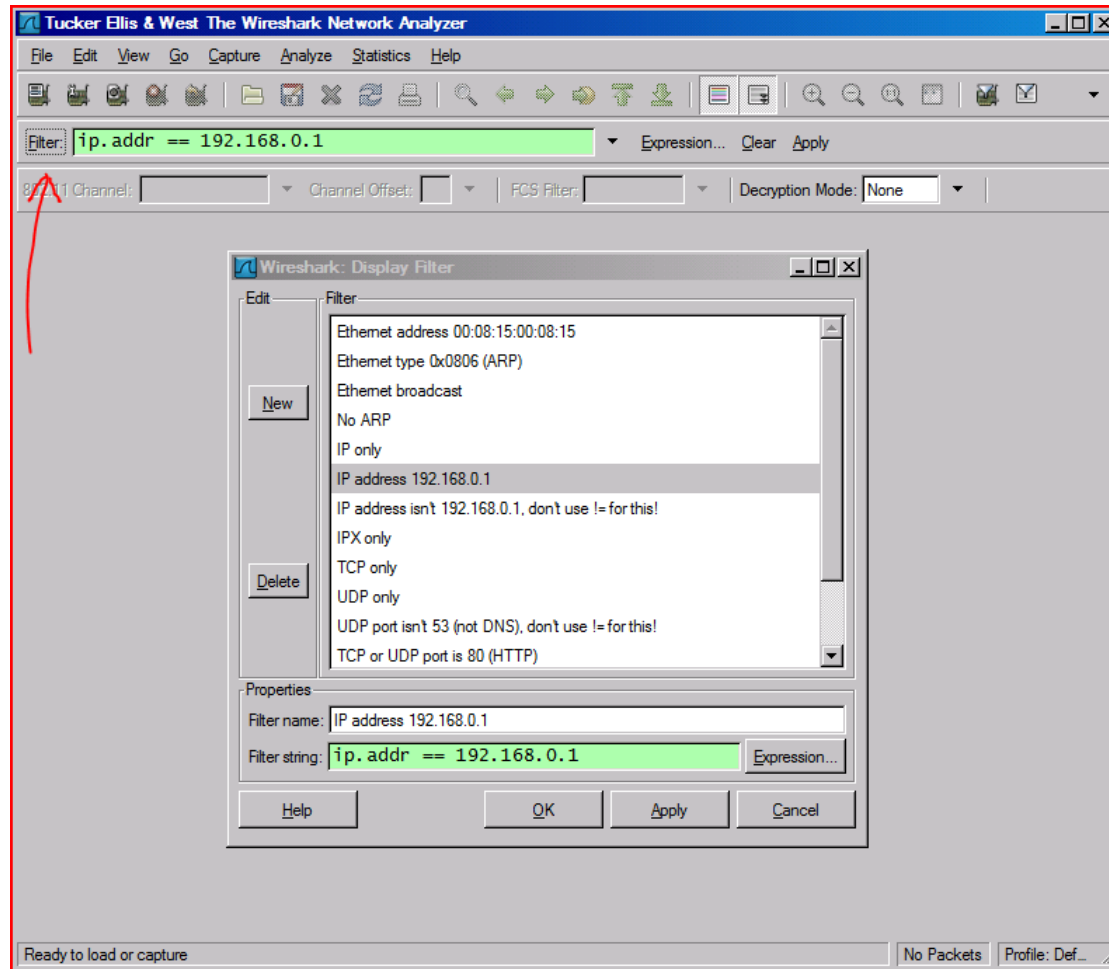
Interrompendo a Captura



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

The image shows the Wireshark network protocol analyzer interface. The title bar reads "Tucker Ellis & West Obsolete_Packets.cap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains icons for file operations, capture, and analysis. The left pane shows a filter field and a list of captured packets. The middle pane displays the "Protocol Hierarchy" menu, which is expanded to show various protocol categories and sub-protocols. The right pane shows a detailed view of the selected packet, including its protocol stack and raw data.

Protocol Hierarchy Menu:

- 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...
- SMTP Operations...
- TCP Stream Graph
- WLAN Traffic...

Packet List:

No.	Time	Source
1	0.000000	::
2	0.000010	::
3	2.179063	192.168.1.1
4	2.439522	192.168.1.1
5	2.715733	192.168.1.1
6	2.821401	192.168.1.1
7	2.821546	192.168.1.1
8	2.824683	192.168.1.1
9	2.990859	192.168.1.1
10	3.266913	192.168.1.1
11	3.495707	fe80::20c
12	3.495727	fe80::20c
13	3.542893	192.168.1.1
14	3.543088	192.168.1.1

Packet Details:

- Frame 1 (88 bytes on wire, 88 bytes captured)
- Linux cooked capture
- Internet Protocol Version 4
- Internet Control Message Protocol

Packet Bytes:

Offset	Hex	ASCII
0000	00 04 00 01 00 06 00 0c	
0010	60 00 00 00 00 20 00 01	
0020	00 00 00 00 00 00 00 00	
0030	00 00 00 01 ff 0d 56 e3	
0040	83 00 d2 c2 00 00 00 00	
0050	00 00 00 01 ff 0d 56 e3	

Packet Info:

Protocol	Info
ICMPv6	Multicast listener report
ICMPv6	Multicast listener report
NBNS	Name query NB LOCALHOST
NBNS	Name query NB LOCALHOST
NBNS	Name query NB LOCALHOST
DNS	Standard query PTR 66.1
DNS	Standard query PTR 255.
DNS	Standard query response
NBNS	Name query NB LOCALHOST
NBNS	Name query NB LOCALHOST
ICMPv6	Router solicitation
ICMPv6	Router solicitation
DNS	Standard query A DoCoMo
NBNS	Name query NB LOCALHOST

Status Bar: File: "C:\Users\vo2.TEW\Downloads\Obsolete_Packets.cap" Packets: 10949 Displayed: 10949 Marked: 0 Profile: Default

Protocol Hierarchy

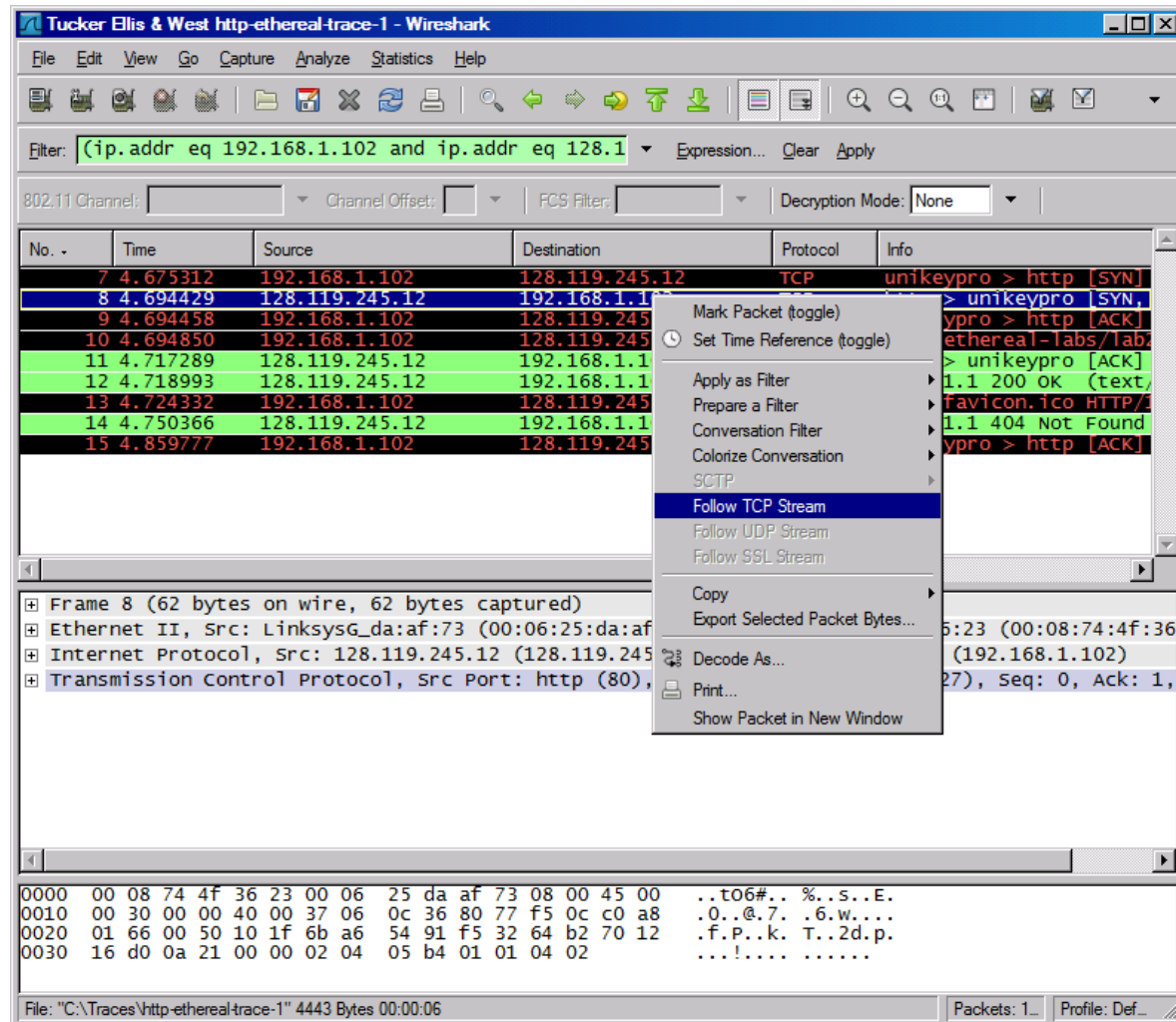
Wireshark: Protocol Hierarchy Statistics

Display filter: none

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

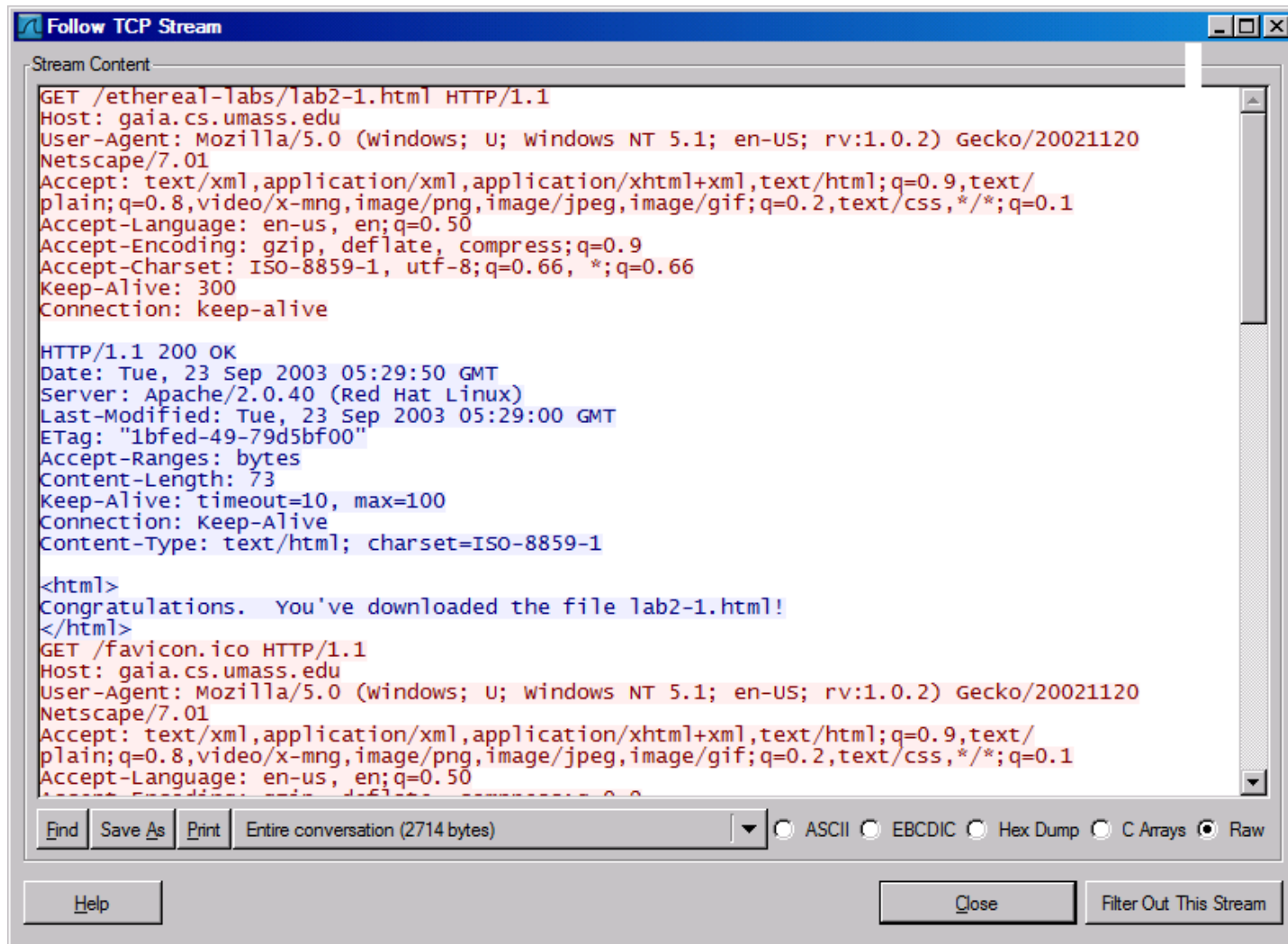
Help Close

Follow TCP Stream



Follow TCP Stream

As cores diferenciam os usuários em uma conexão



Expert Info

The screenshot shows the Wireshark interface with the 'Expert Info' pane open for frame 8. The main packet list shows a sequence of protocols: SNMP, DNS, TCP, and HTTP. The selected frame 8 is an HTTP 200 OK response from 128.119.245.12 to 192.168.1.102.

Expert Info Details:

- 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:36:23)
- 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,

Packet Bytes:

```
0000  00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00  ..t06#.. %..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+Wam+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

The screenshot shows the Wireshark interface with the 'Conversations' pane selected. The left pane shows a list of captured packets, with packet 2 selected. The middle pane shows a list of conversations, with the 'HTTP' conversation selected. The right pane shows a detailed view of the selected conversation, displaying the HTTP 404 error response.

Conversations Pane:

No.	Time	Source
1	0.000000	192.168.1.104
2	0.017162	192.168.1.102
3	3.017086	192.168.1.104
4	3.034572	192.168.1.102
5	4.626878	192.168.1.104
6	4.663785	63.240.76.19
7	4.675312	192.168.1.102
8	4.694429	128.119.2.104
9	4.694458	192.168.1.102
10	4.694850	192.168.1.104
11	4.717289	128.119.2.104
12	4.718993	128.119.2.104
13	4.724332	192.168.1.104
14	4.750366	128.119.2.104

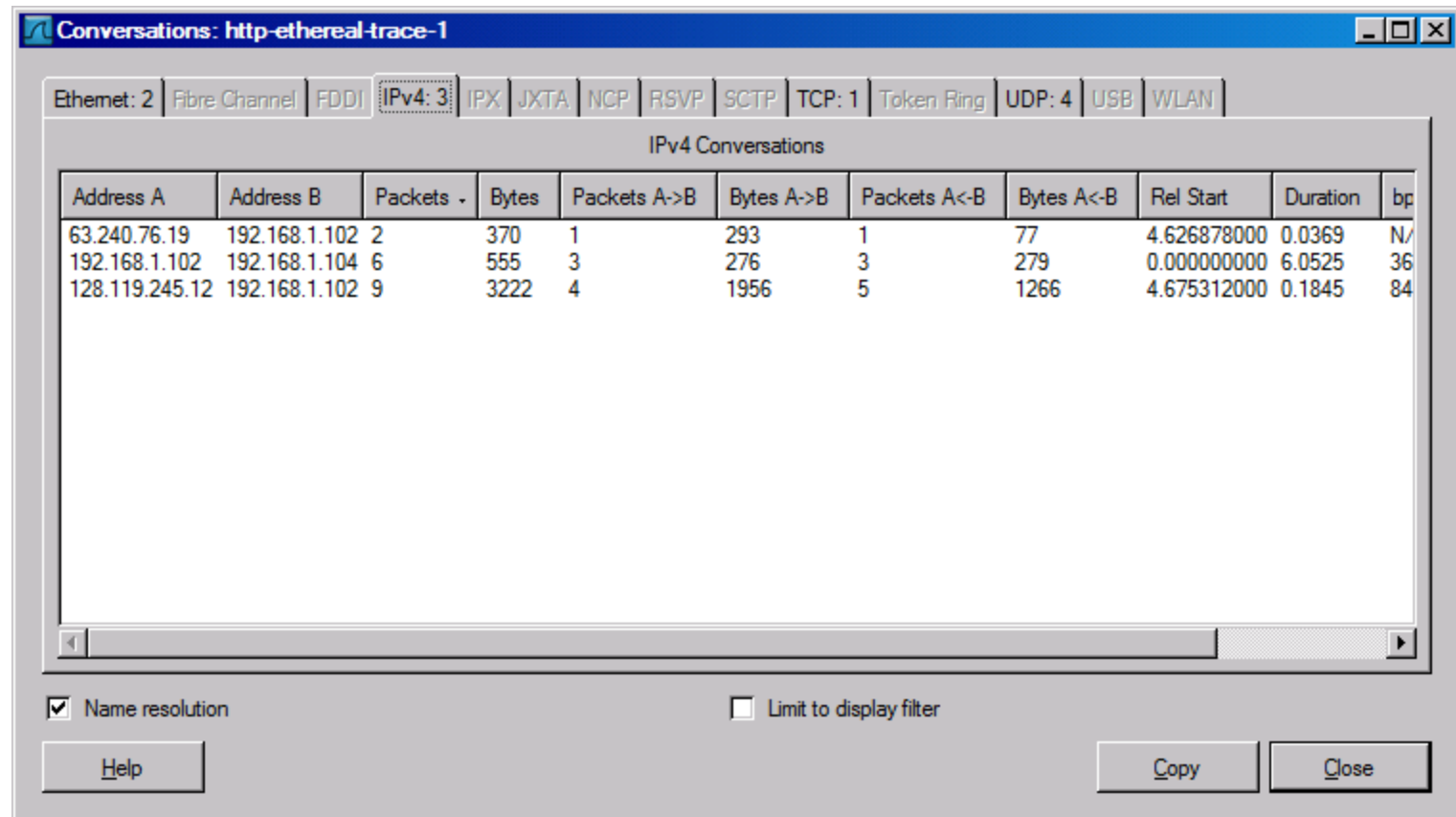
HTTP Conversation Details:

Protocol	Info
SNMP	get-request SNMPv2-SMI
SNMP	get-response SNMPv2-SMI
SNMP	get-request SNMPv2-SMI
SNMP	get-response SNMPv2-SMI
DNS	Standard query A gaia.d
DNS	Standard query response
TCP	unikeypro > http [SYN]
TCP	http > unikeypro [SYN]
TCP	unikeypro > http [ACK]
HTTP	GET /ethereal-labs/lab
TCP	http > unikeypro [ACK]
HTTP	HTTP/1.1 200 OK (text)
HTTP	GET /favicon.ico HTTP/1
HTTP	HTTP/1.1 404 Not Found

HTTP 404 Error Details:

eb:ed), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
104), Dst: 192.168.1.102 (192.168.1.102)
Port: opsview-envoy (4125)

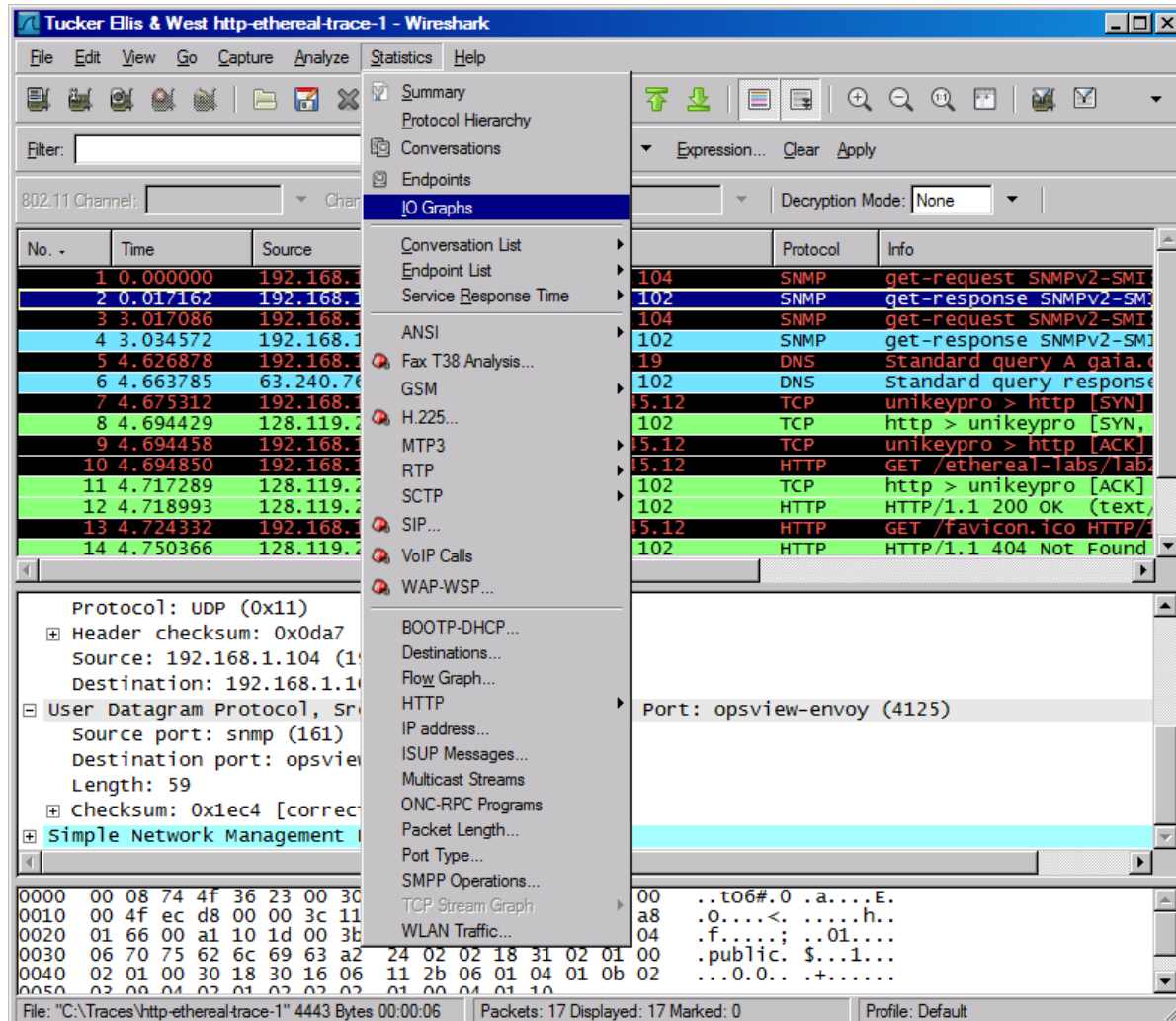
Conversations



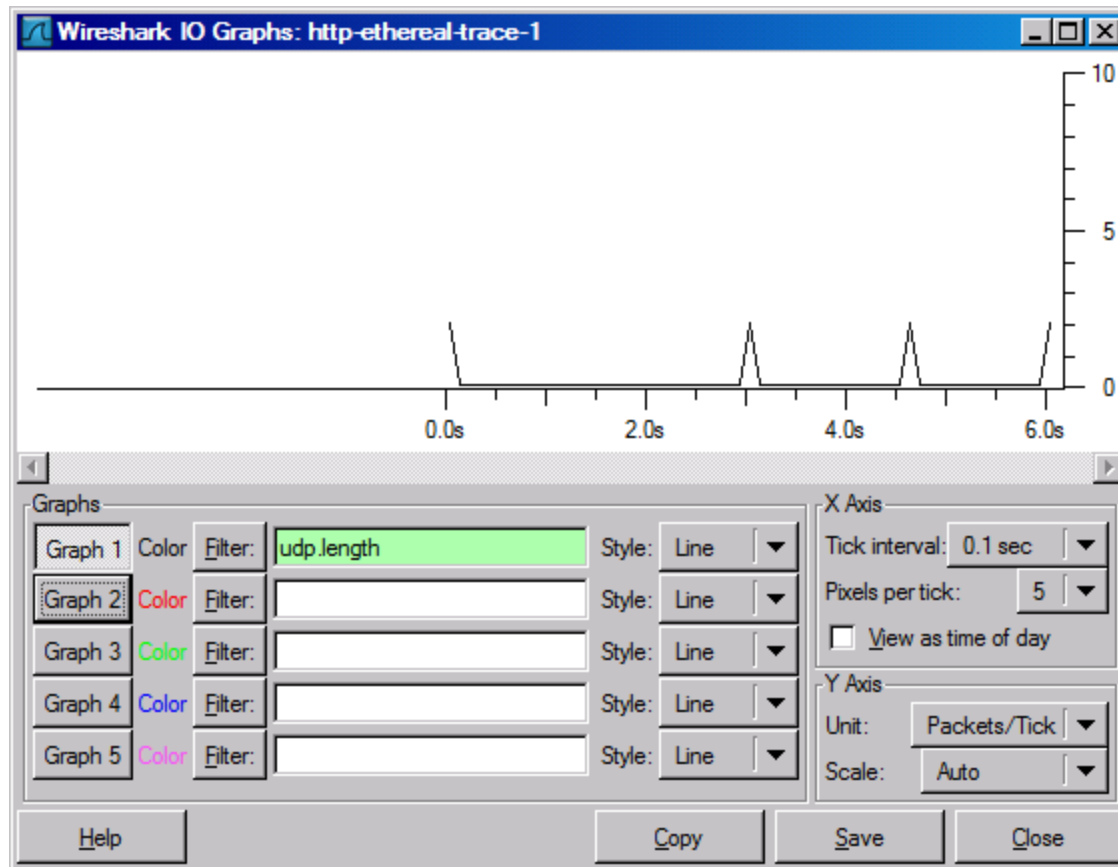
The screenshot shows the 'Conversations' window in Wireshark, titled 'Conversations: http-ethereal-trace-1'. The 'IPv4: 3' tab is selected, displaying a table of IPv4 conversations. The table has columns for Address A, Address B, Packets, Bytes, and bidirectional traffic statistics. Three conversations are listed, involving IP addresses 63.240.76.19, 192.168.1.102, and 192.168.1.104. At the bottom, there are checkboxes for 'Name resolution' (checked) and 'Limit to display filter' (unchecked), along with 'Help', 'Copy', and 'Close' buttons.

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bp
63.240.76.19	192.168.1.102	2	370	1	293	1	77	4.626878000	0.0369	N/
192.168.1.102	192.168.1.104	6	555	3	276	3	279	0.000000000	6.0525	36
128.119.245.12	192.168.1.102	9	3222	4	1956	5	1266	4.675312000	0.1845	84

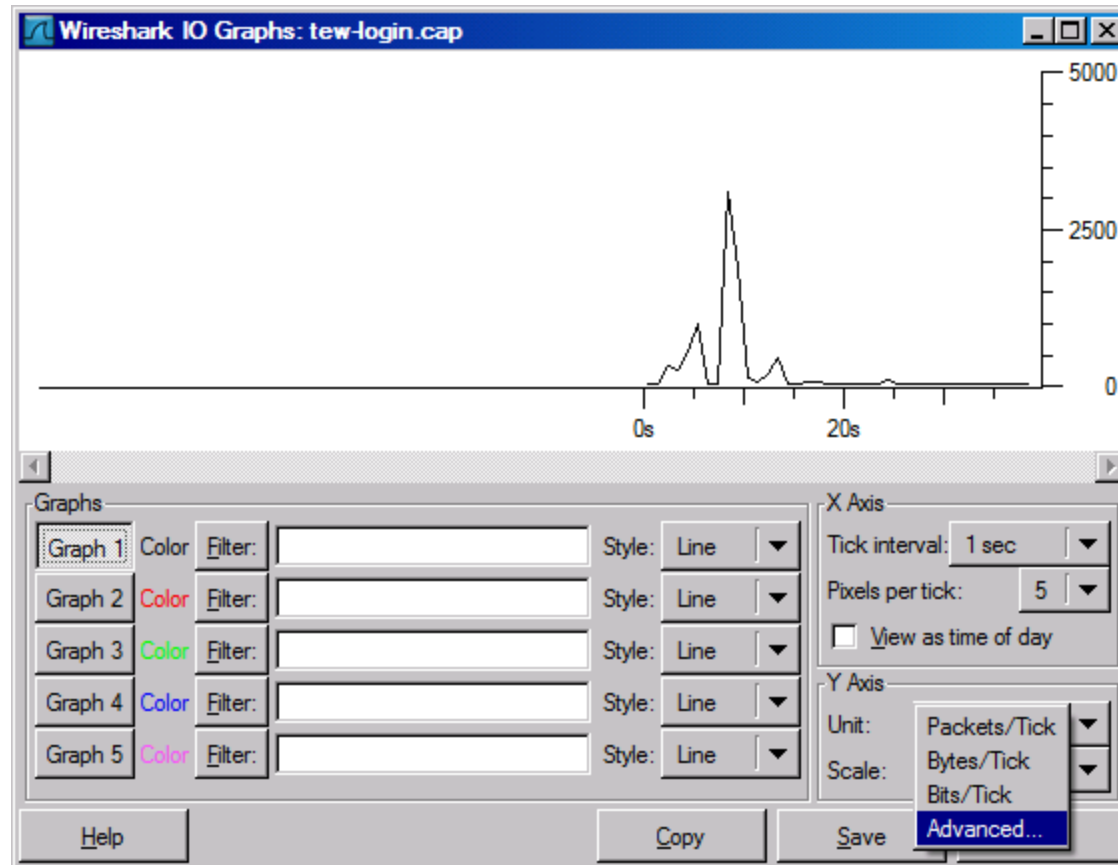
IOGraphs



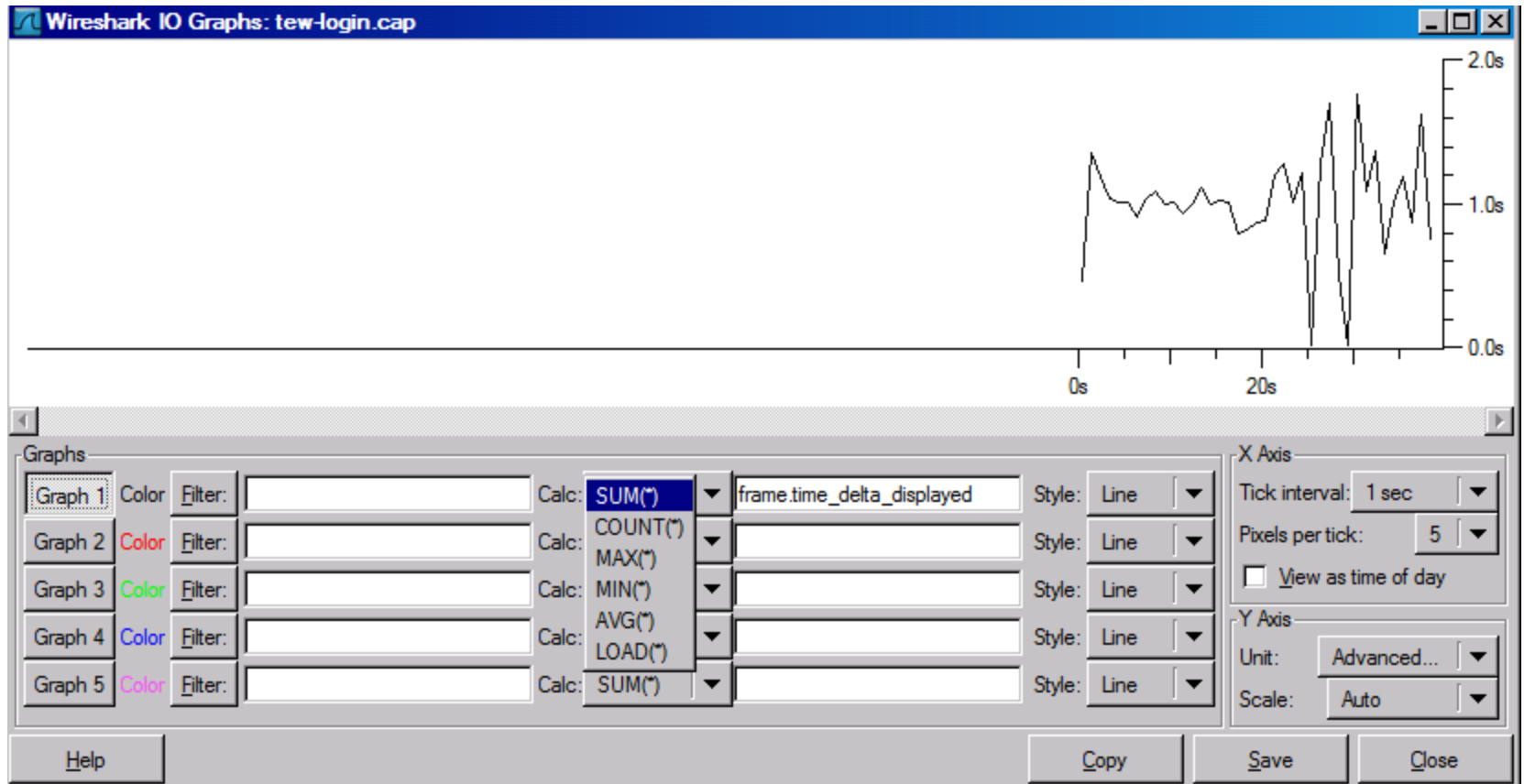
IOGraphs



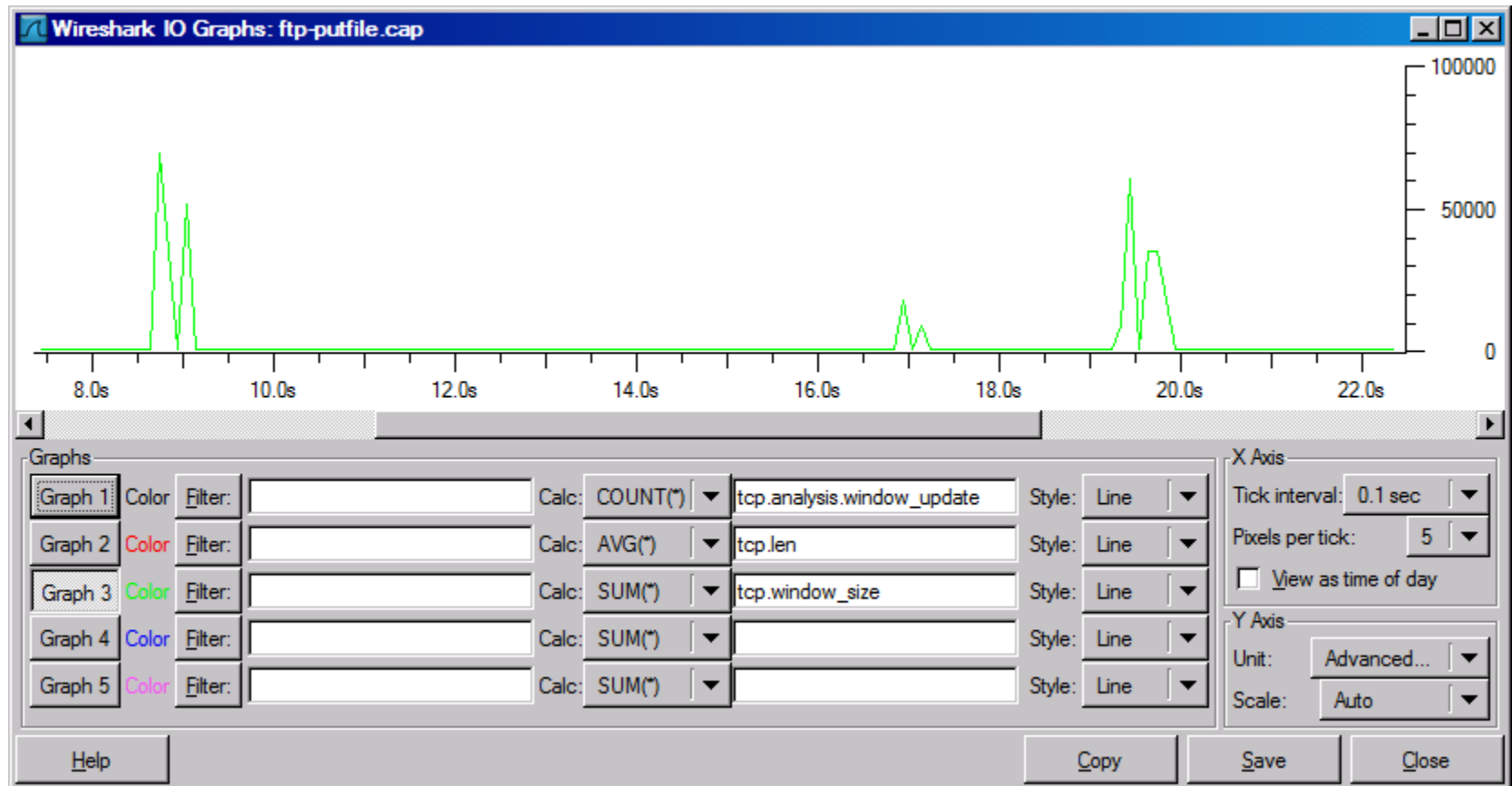
IOGraphs



IOGraphs



IOGraphs



Flow Graphs

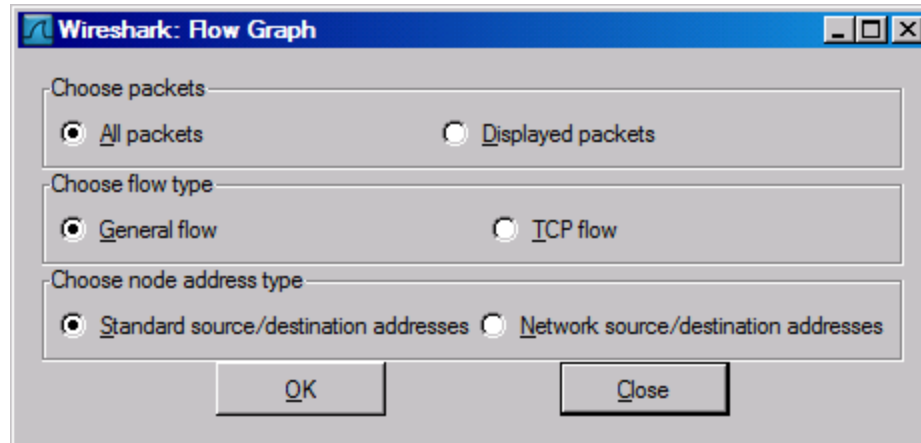
The image shows the Wireshark network protocol analyzer interface. The title bar reads "Tucker Ellis & West http-ethereal-trace-1 - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains icons for file operations, capture, and analysis. The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. The first 14 packets are highlighted in green, and the last 14 are highlighted in blue. The list includes columns for No., Time, and Source.
- Packet Details:** Shows the details of the selected packet (No. 14). It includes sections for Protocol (UDP), User Datagram Protocol, and Simple Network Management Protocol.
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

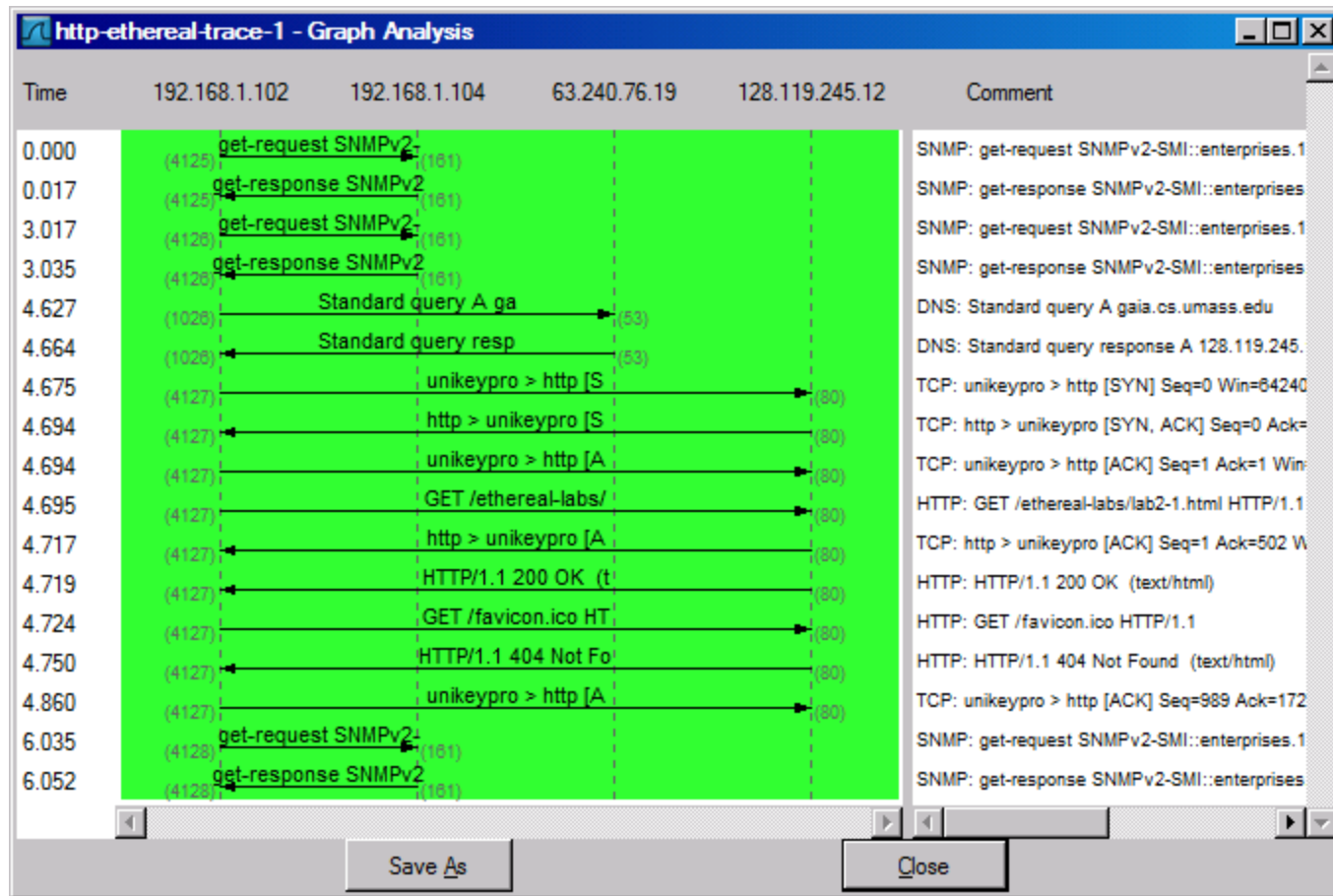
The "Statistics" menu is open, showing options like Summary, Protocol Hierarchy, Conversations, Endpoints, and IO Graphs. The "Flow Graph..." option is highlighted under the "IO Graphs" section.

The status bar at the bottom indicates: File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06, Packets: 17 Displayed: 17 Marked: 0, Profile: Default.

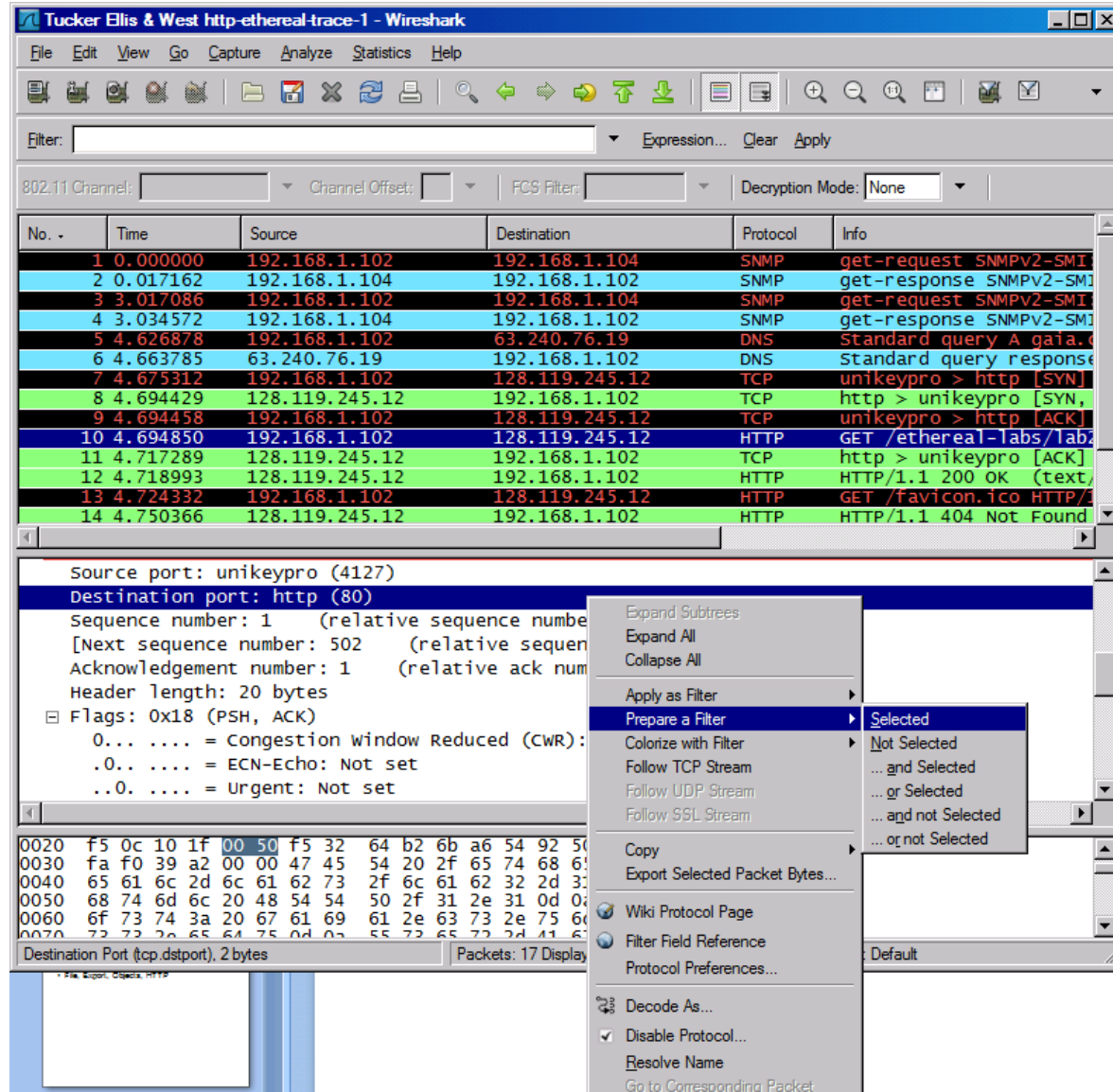
Flow Graphs



Flow Graphs



Right Click Filtering



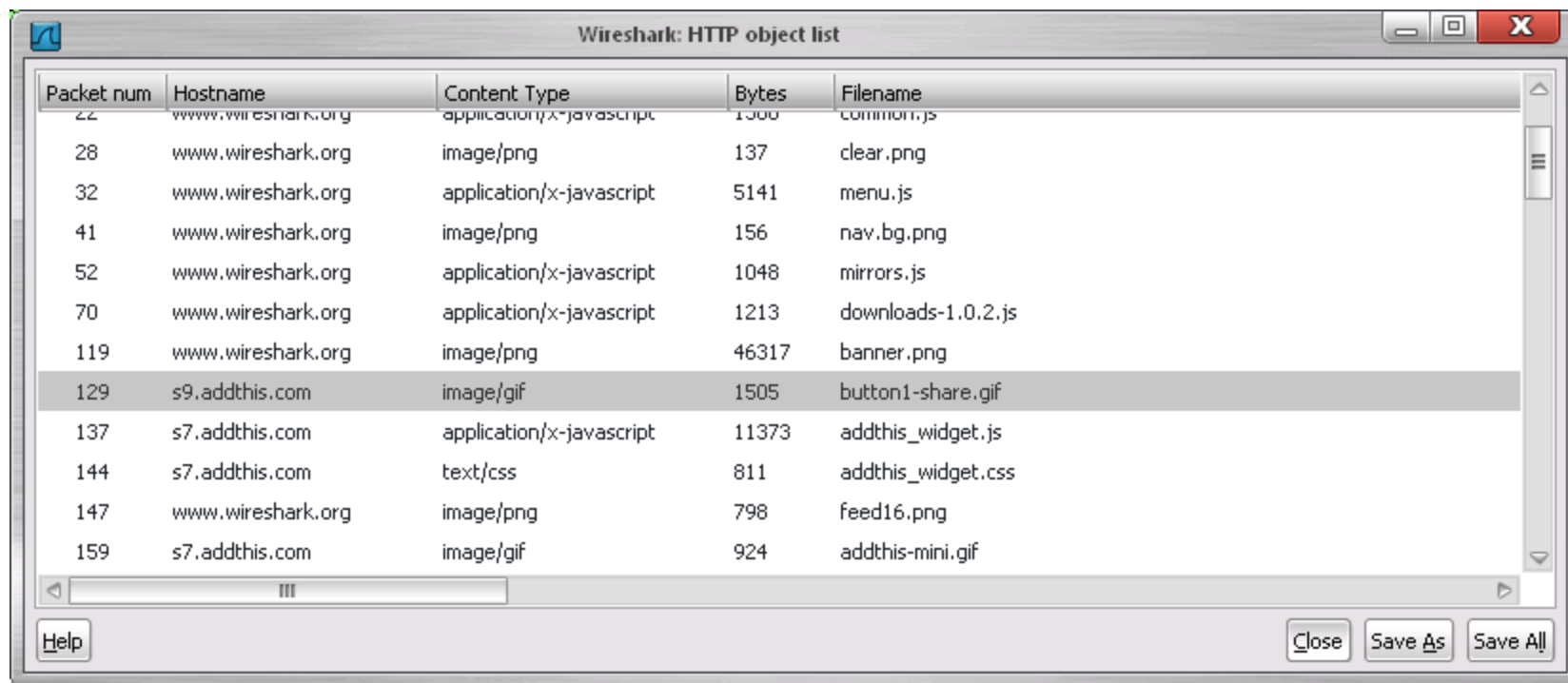
Export HTTP

The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "Tucker Ellis & West http-ethereal-trace-1 - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, packet navigation, and analysis. Below the toolbar, there are fields for "Channel Offset", "FCS Filter", and "Decryption Mode". The main packet list displays several packets, with packet 14 selected. The details pane for packet 14 shows the following information:

- 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

The packet bytes pane at the bottom shows the raw data of the selected packet, including the destination port (tcp.dstport), the number of packets displayed (17), and the profile (Default).

Export HTTP Objects



VOIP

Tucker Ellis & West aaa.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:

802.11 Channel: Char

No.	Time	Source	Destination	Protocol	Info
1	2005-07-04 05:32:20.1	192.168.1.255	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
2	2005-07-04 05:32:21.1	192.168.1.255	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
3	2005-07-04 05:32:22.1	192.168.1.255	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
4	2005-07-04 05:32:31.1	192.168.1.1	192.168.1.1	ARP	who has 192.168.1.1? Tell
5	2005-07-04 05:32:31.1	192.168.1.1	192.168.1.1	ARP	192.168.1.1 is at 00:30:54
6	2005-07-04 05:32:31.1	192.168.1.1	192.168.1.1	DNS	Standard query A sip.cyber
7	2005-07-04 05:32:32.1	192.168.1.1	192.168.1.1	DNS	Standard query A sip.cyber
8	2005-07-04 05:32:34.1	192.168.1.1	192.168.1.2	DNS	Standard query response A
9	2005-07-04 05:32:34.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
10	2005-07-04 05:32:35.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
11	2005-07-04 05:32:36.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
12	2005-07-04 05:32:38.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
13	2005-07-04 05:32:39.1	192.168.1.1	192.168.1.2	ARP	who has 192.168.1.2? Tell
14	2005-07-04 05:32:39.1	192.168.1.1	192.168.1.2	ARP	192.168.1.2 is at 00:e0:ed
15	2005-07-04 05:32:40.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
16	2005-07-04 05:32:44.1	192.168.1.1	192.168.1.1	DNS	Standard query SRV _sip._u
17	2005-07-04 05:32:52.1	192.168.1.1	192.168.1.1	DNS	Standard query PTR 1.0.0.1
18	2005-07-04 05:32:52.1	192.168.1.2	192.168.1.2	DNS	Standard query response PTR
19	2005-07-04 05:32:52.1	192.168.1.2	192.168.1.2	SIP	Request: REGISTER sip:sip.

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...

Frame 1 (92 bytes on wire)
Ethernet II, Src: Silicom...
Internet Protocol, Src: 19...
User Datagram Protocol, Src...
NetBIOS Name Service

0000 ff ff ff ff ff ff 00 e0
0010 00 4e 69 8c 00 00 80 11
0020 01 ff 00 89 00 89 00 3a
0030 00 00 00 00 00 00 20 45
0040 45 45 50 45 4e 45 42 45
0050 41 42 41 42 41 42 41 00

File: "C:\Users\vo2.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	C
508.349	575.439	192.168.1.2	sip:816666@voip.bruiula.net	sip:97239287044@voip.bruiula.net	SIP	18	CANCELLED	
692.955	727.341	192.168.1.2	sip:voi18062@sip.cybercity.dk	sip:0097239287044@sip.cybercity.dk	SIP	8	REJECTED	
1307.689	1359.221	192.168.1.2	sip:35104723@sip.cybercity.dk	sip:0097239287044@sip.cybercity.dk	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.pcap - VoIP Calls

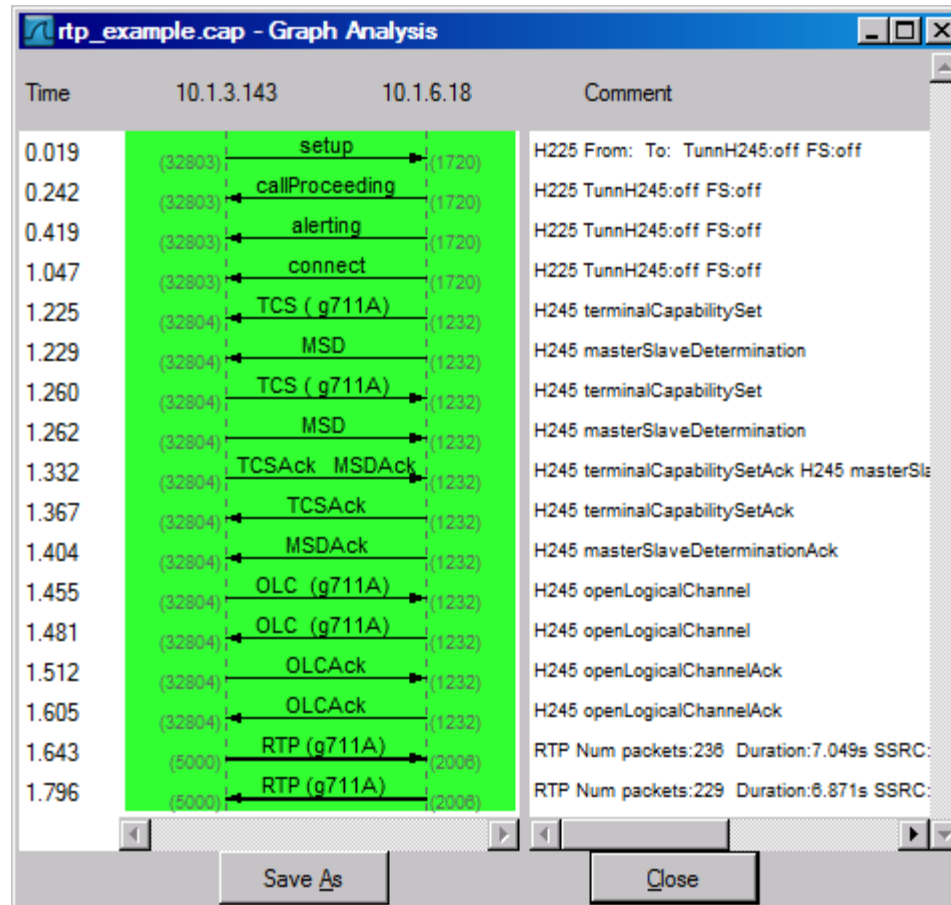
Detected 1 VoIP Call. Selected 1 Call.

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

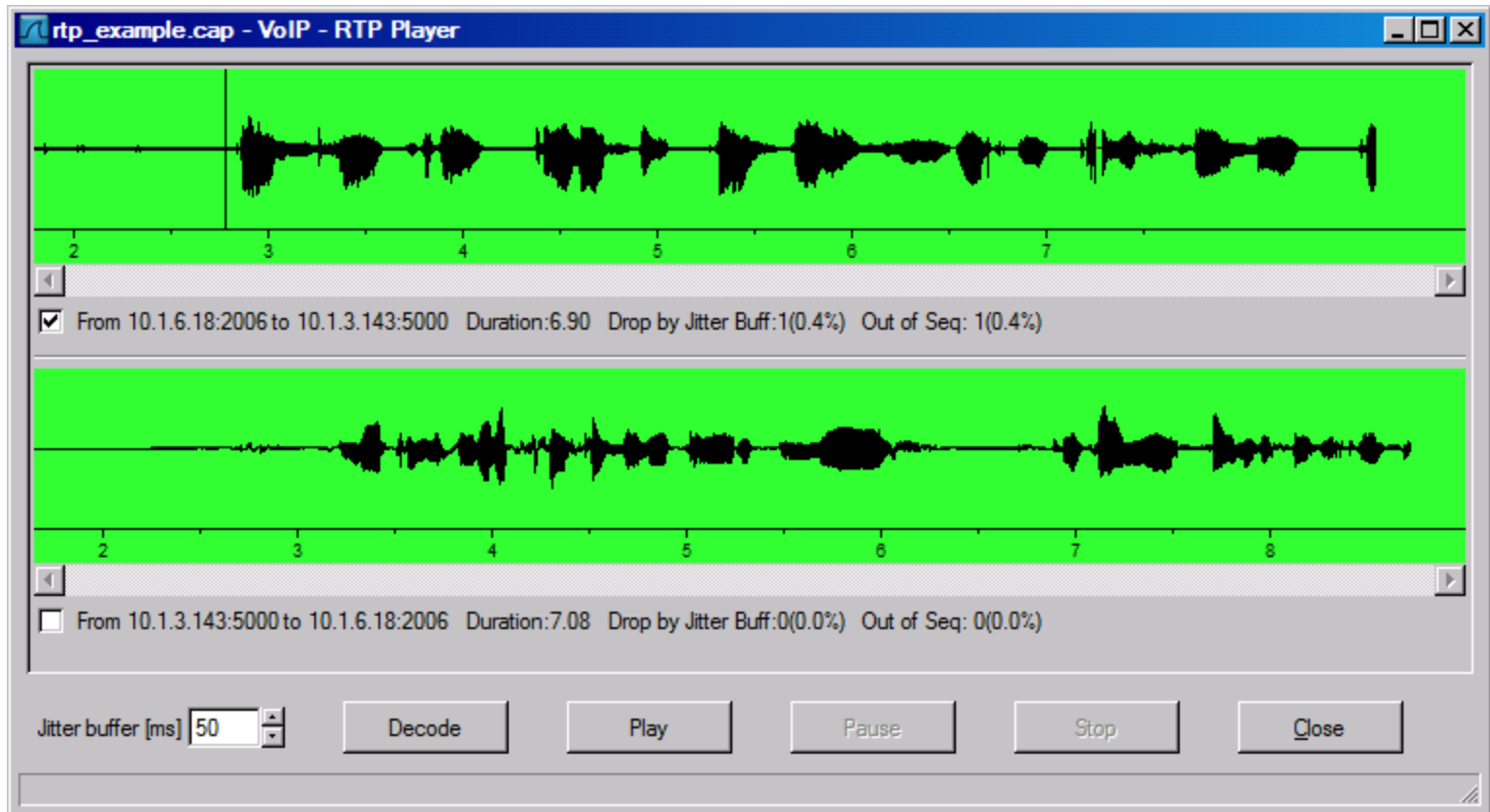
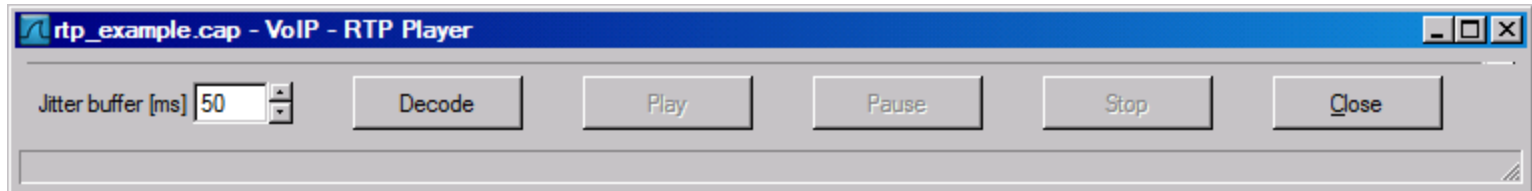
Total: Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 0

Prepare Filter Graph Player Select All Close

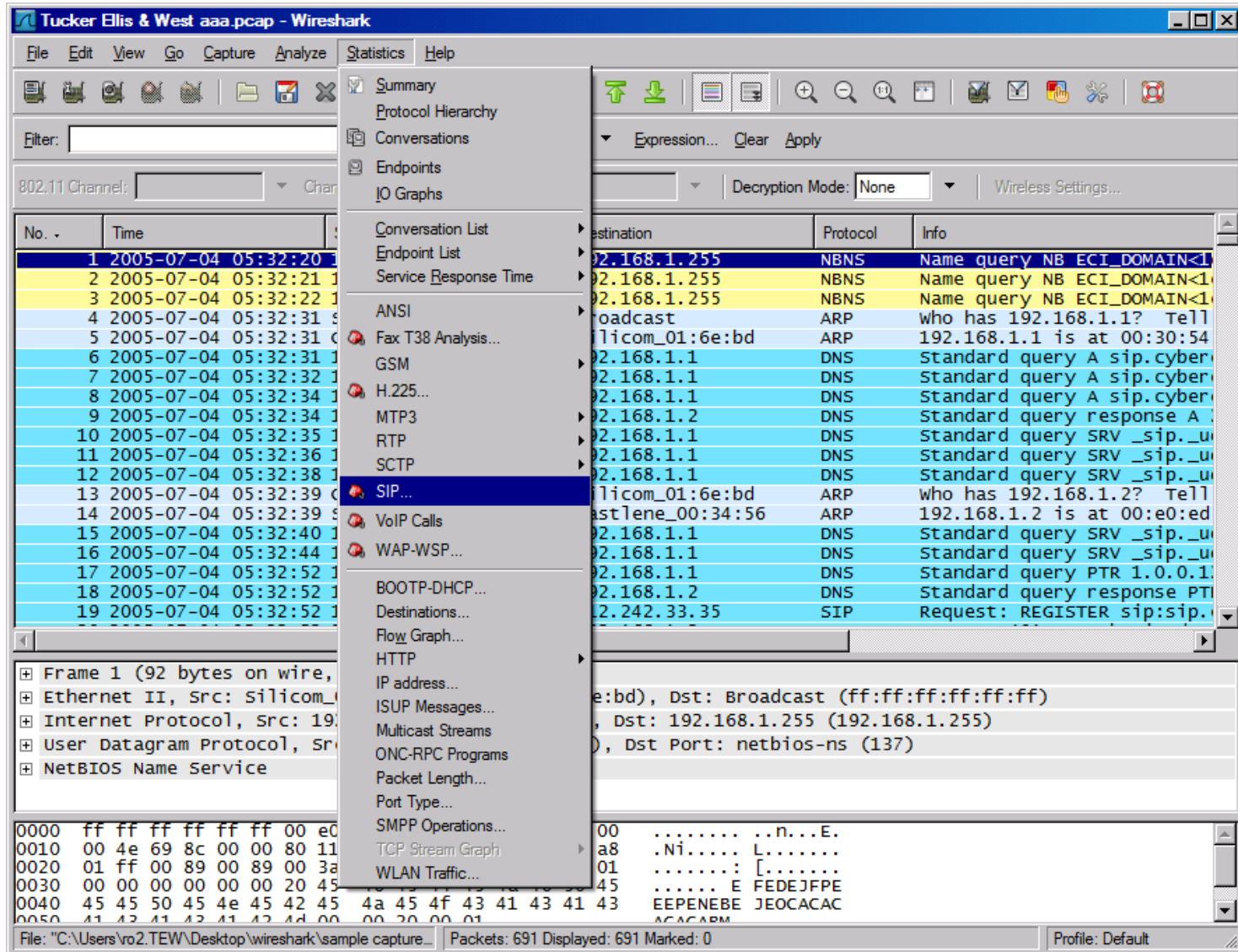
VOIP Call Graph



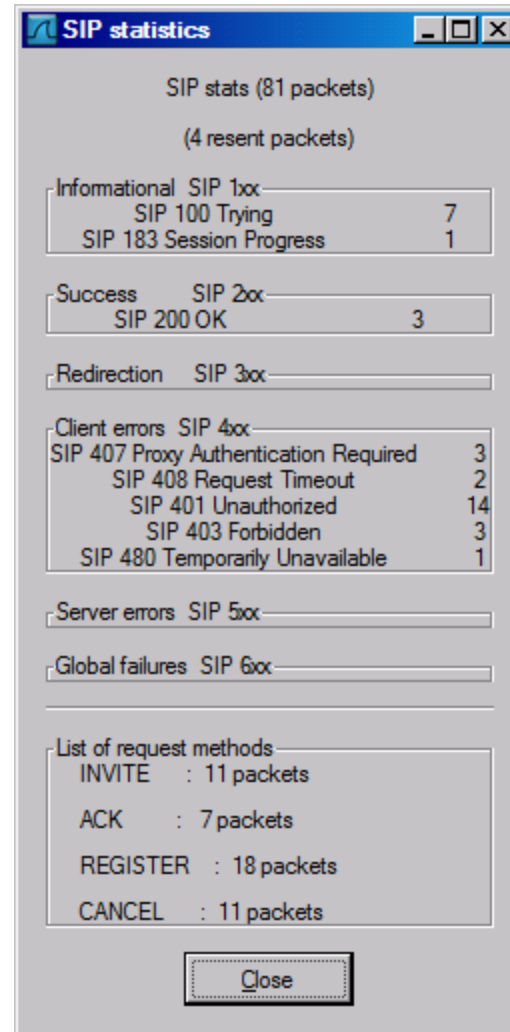
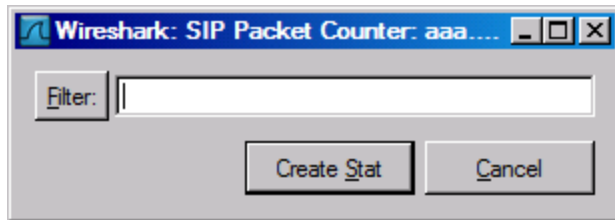
VOIP RTP Player



SIP Analysis



SIP Analysis



HTTP Analysis

The screenshot shows the Wireshark interface with a capture file named "Tucker Ellis & West internet-capture-113pm-07242008.cap". The packet list on the left shows 19 packets. The packet details pane on the right shows the selected packet (No. 18) as an HTTP packet. A context menu is open over the packet list, showing options for analyzing the selected HTTP packet.

Packet List:

No.	Time	Destination	Protocol	Info
1	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
2	2008-07-24 13:12:59.1	10.1.15.104	TCP	acc-raid > http [ACK] Seq=
3	2008-07-24 13:12:59.1	10.1.15.104	HTTP	GET /p/s/sm_vrt_3thumb_scr
4	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
5	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
6	2008-07-24 13:12:59.1	10.1.15.104	TCP	acc-raid > http [ACK] Seq=
7	2008-07-24 13:12:59.1	10.1.15.104	DNS	Standard query A a632.g.ak
8	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
9	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
10	2008-07-24 13:12:59.1	10.1.15.104	TCP	acc-raid > http [ACK] Seq=
11	2008-07-24 13:12:59.1	10.1.15.104	HTTP	GET /customer/advance/9/.o
12	2008-07-24 13:12:59.1	10.1.15.104	HTTP	GET /customer/advance/9/.o
13	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP t
14	2008-07-24 13:12:59.2	10.1.11.13	DNS	Standard query response CN
15	2008-07-24 13:12:59.1	10.1.11.13	TCP	mcs-calypsoicf > http [SYN
16	2008-07-24 13:12:59.1	10.1.12.67	HTTP	Continuation or non-HTTP t
17	2008-07-24 13:12:59.1	10.2.101.36	TCP	3325 > http [ACK] Seq=1 Ac
18	2008-07-24 13:12:59.1	10.1.12.67	HTTP	[TCP Out-Of-Order] Continu
19	2008-07-24 13:12:59.1	10.2.101.36	TCP	3325 > http [ACK] Seq=1 Ac

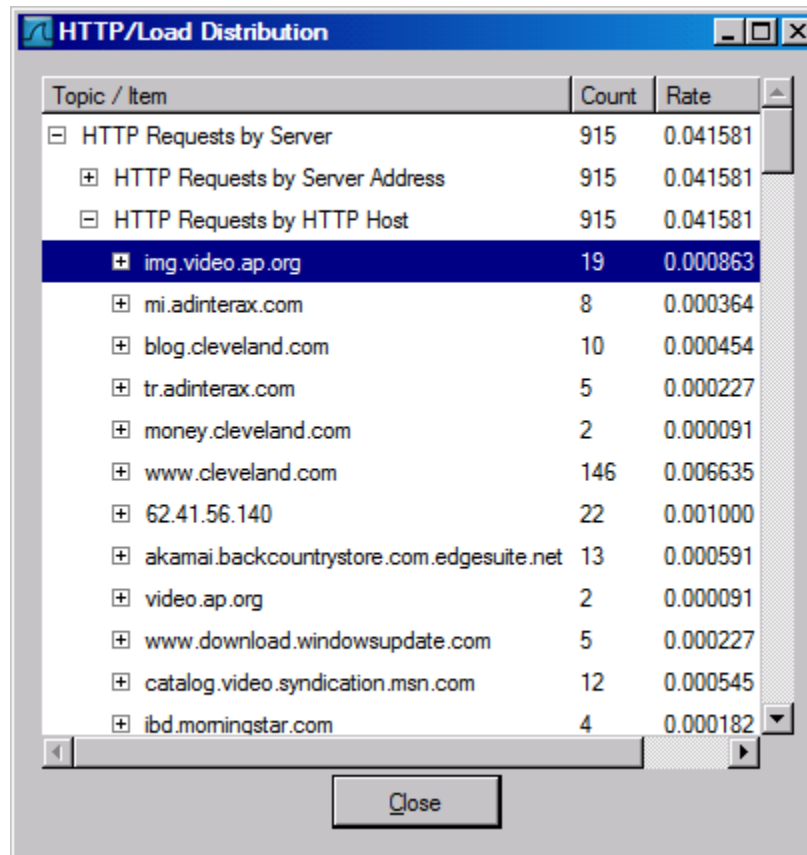
Packet Details (Frame 18):

- Frame 1 (1514 bytes on wire)
- Ethernet II, Src: Cisco_f7
- Internet Protocol, Src: 20
- Transmission Control Proto
- Hypertext Transfer Proto

Context Menu Options:

- 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**
 - Load Distribution...
 - Packet Counter...
 - Requests...
- IP address...
- ISUP Messages...
- Multicast Streams
- ONC-RPC Programs
- Packet Length...
- Port Type...
- SMPP Operations...
- TCP Stream Graph
- WLAN Traffic...

HTTP Analysis – Load Distribution

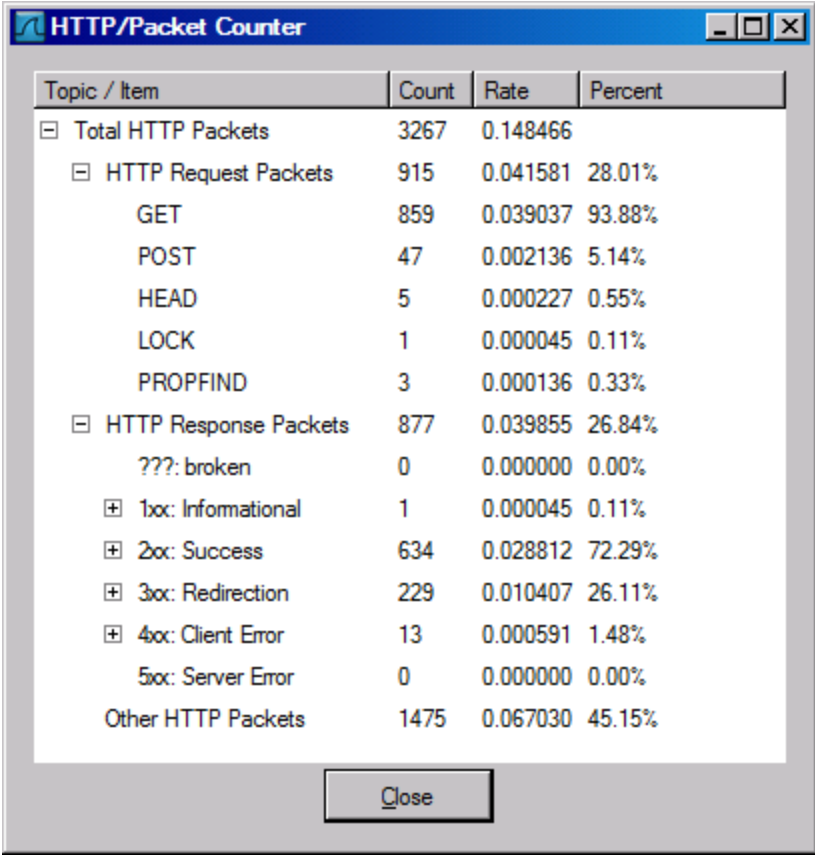


The screenshot shows a window titled "HTTP/Load Distribution" with a table of HTTP requests. The table has three columns: "Topic / Item", "Count", and "Rate". The data is organized into a tree structure. The "img.video.ap.org" item is highlighted in blue.

Topic / Item	Count	Rate
[-] HTTP Requests by Server	915	0.041581
[+] HTTP Requests by Server Address	915	0.041581
[-] HTTP Requests by HTTP Host	915	0.041581
 img.video.ap.org	19	0.000863
[+] mi.adinterax.com	8	0.000364
[+] blog.cleveland.com	10	0.000454
[+] tr.adinterax.com	5	0.000227
[+] money.cleveland.com	2	0.000091
[+] www.cleveland.com	146	0.006635
[+] 62.41.56.140	22	0.001000
[+] akamai.backcountrystore.com.edgesuite.net	13	0.000591
[+] video.ap.org	2	0.000091
[+] www.download.windowsupdate.com	5	0.000227
[+] catalog.video.syndication.msn.com	12	0.000545
[+] ibd.morningstar.com	4	0.000182

Close

HTTP Analysis – Packet Counter

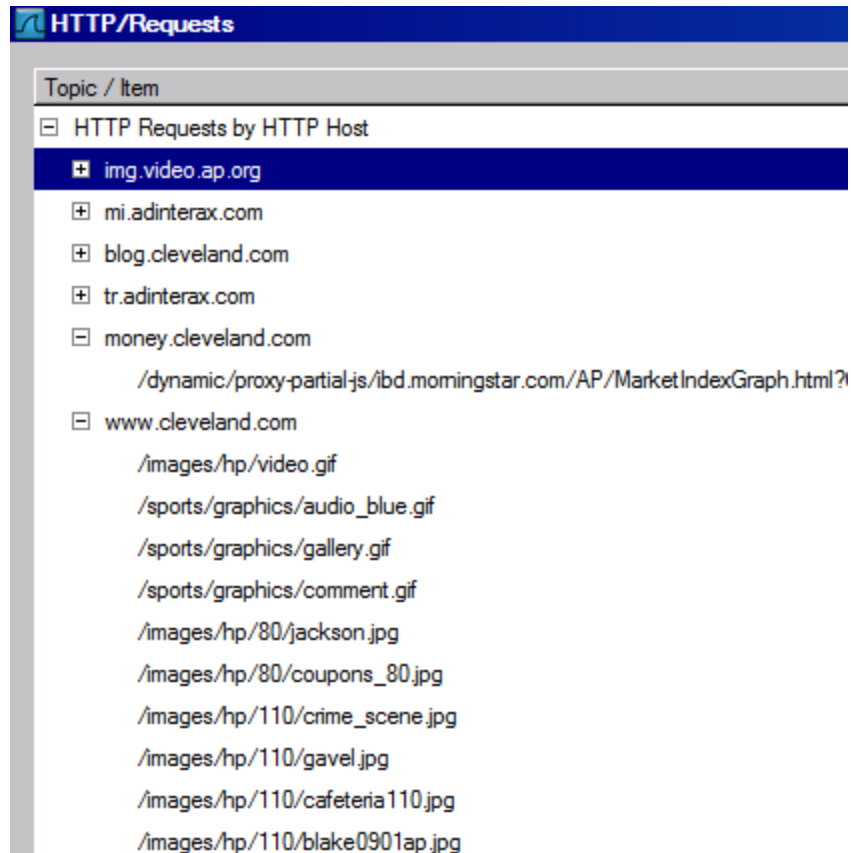


The screenshot shows a window titled "HTTP/Packet Counter" with a table of statistics. The table has four columns: "Topic / Item", "Count", "Rate", and "Percent". The data is organized hierarchically, starting with "Total HTTP Packets" and branching into "HTTP Request Packets" and "HTTP Response Packets". Under "HTTP Request Packets", there are sub-items for HTTP methods: GET, POST, HEAD, LOCK, and PROPFIND. Under "HTTP Response Packets", there are sub-items for response status codes: 1xx: Informational, 2xx: Success, 3xx: Redirection, 4xx: Client Error, and 5xx: Server Error, along with "Other HTTP Packets". A "Close" button is located at the bottom right of the window.

Topic / Item	Count	Rate	Percent
☒ Total HTTP Packets	3267	0.148466	
☒ HTTP Request Packets	915	0.041581	28.01%
GET	859	0.039037	93.88%
POST	47	0.002136	5.14%
HEAD	5	0.000227	0.55%
LOCK	1	0.000045	0.11%
PROPFIND	3	0.000136	0.33%
☒ HTTP Response Packets	877	0.039855	26.84%
??? : broken	0	0.000000	0.00%
☒ 1xx: Informational	1	0.000045	0.11%
☒ 2xx: Success	634	0.028812	72.29%
☒ 3xx: Redirection	229	0.010407	26.11%
☒ 4xx: Client Error	13	0.000591	1.48%
5xx: Server Error	0	0.000000	0.00%
Other HTTP Packets	1475	0.067030	45.15%

Close

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”