



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

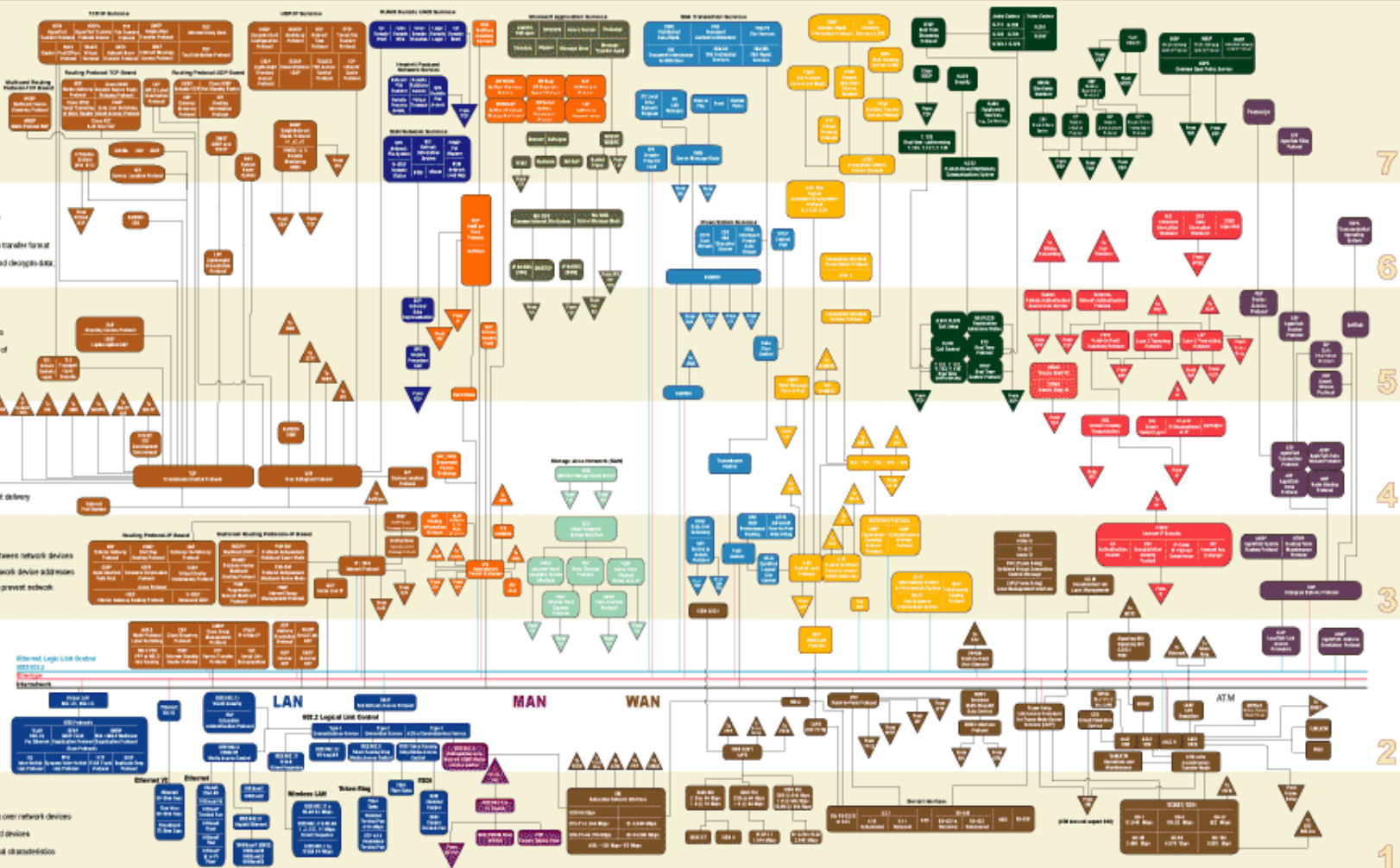
- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion

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)1 67 88 44 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 89 51 11
www.itu.ch

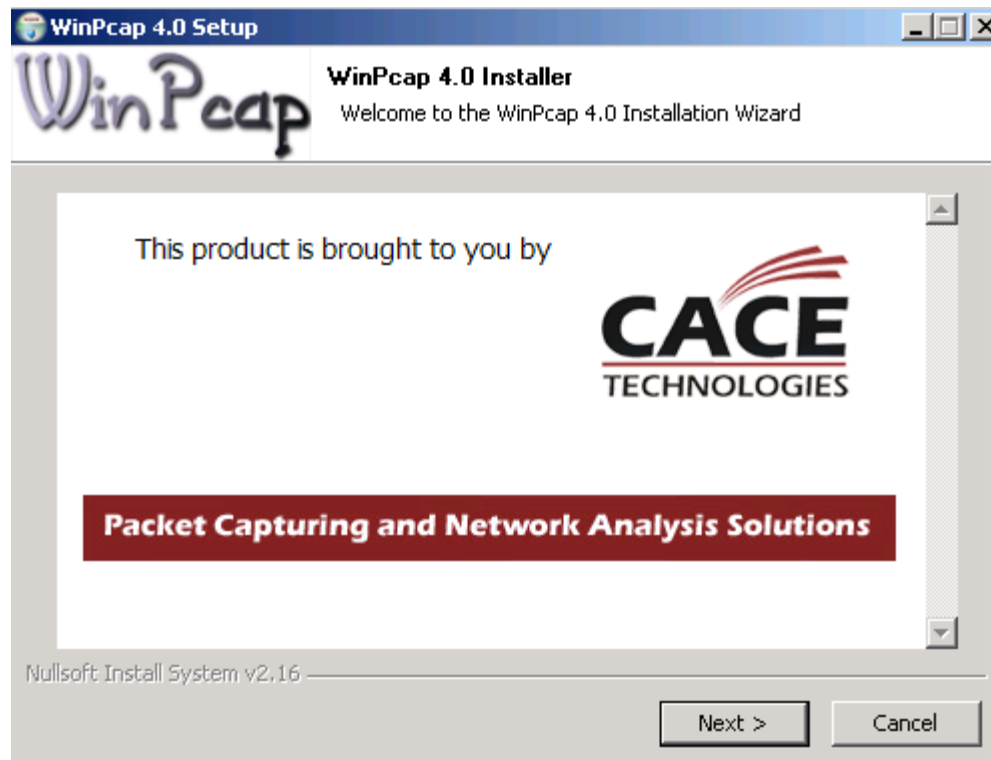
ISO/IEC
International Organization for Standardization
www.iso.org
www.iec.org
www.iso.org/IEC/Joint-Technical-Committee
1715, Route de la Gare
CH-1211 Geneva 20, Switzerland
Tel: 41-22-419-60-11
www.iso.org

IEC
International Electrotechnical Commission
3, rue de Vanille
CH-1211 Geneva 20, Switzerland
Tel: 41-22-419-60-11
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...




PILOT

Taking Wireshark Into Uncharted Waters

- Analysis
- Charting
- Reporting
- Integrated with Wireshark





Enriching


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)

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] ...

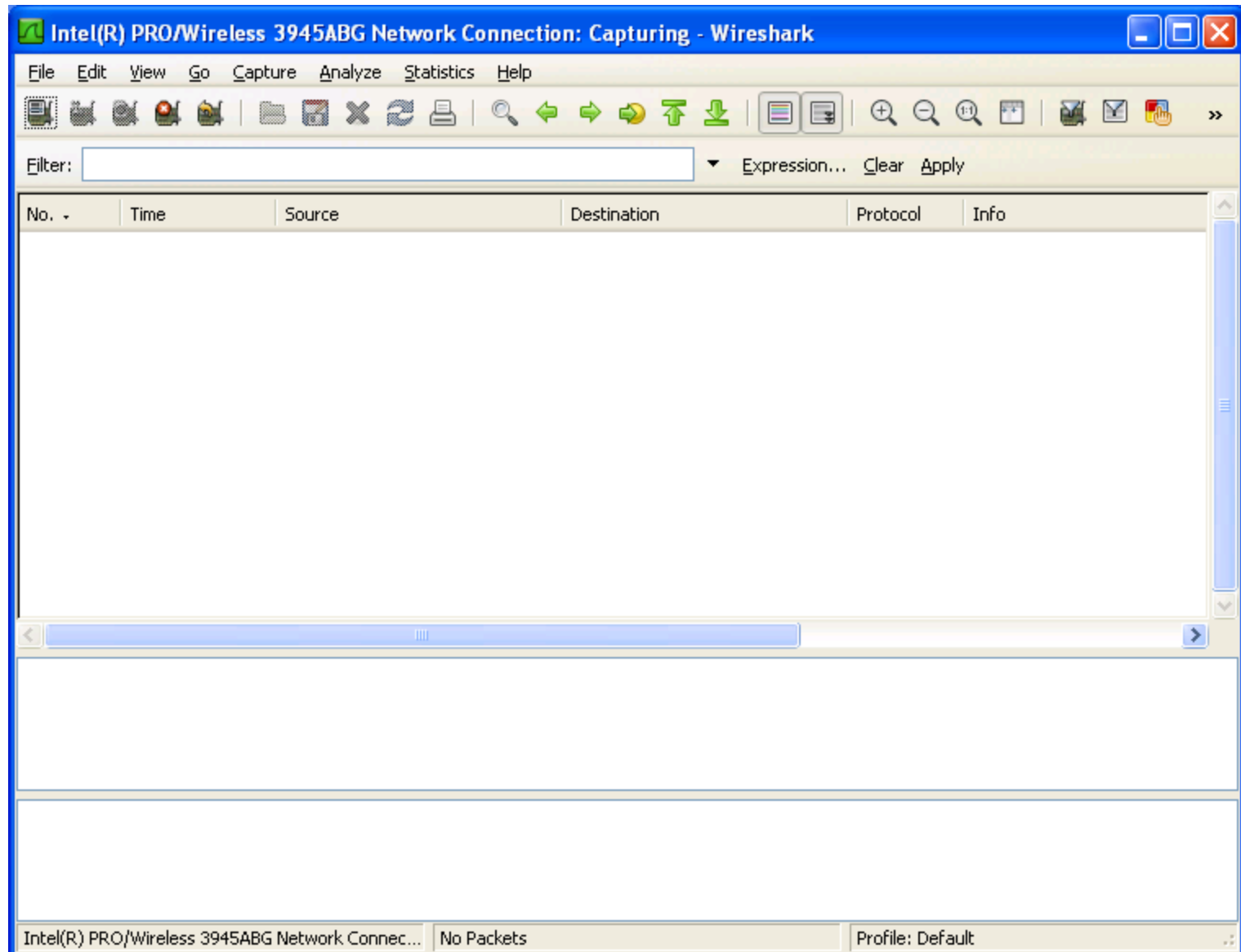
Capture interface:

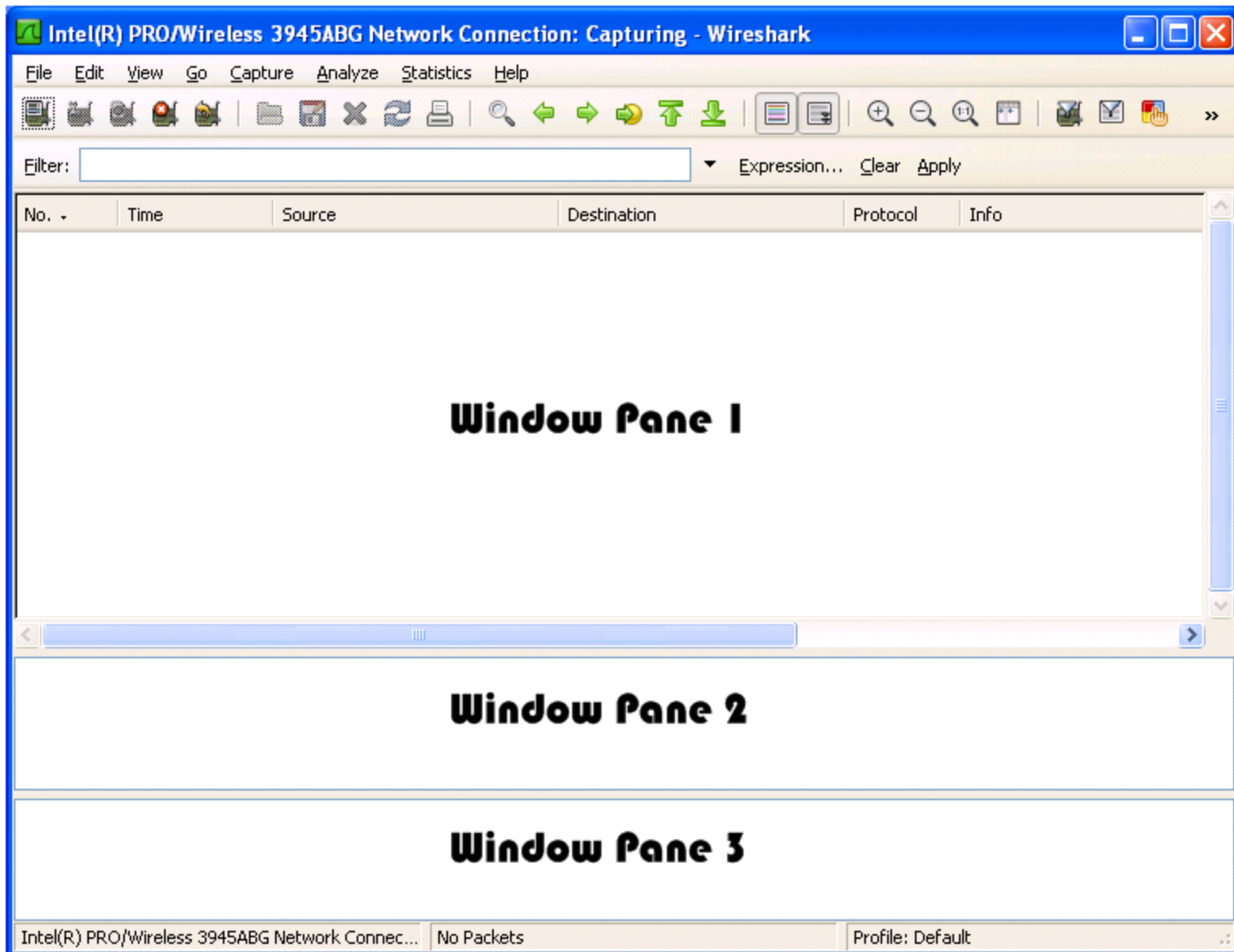
```
-i <interface>      name or idx of interface (def: first non-loopback)
-f <capture filter>  packet filter in libpcap filter syntax
-s <snaplen>         packet snapshot length (def: 65535)
-p                  don't capture in promiscuous mode
-B <buffer size>     size of kernel buffer (def: 1MB)
-y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

The image shows a Wireshark network traffic capture window titled "(Untitled) - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help) and a toolbar with icons for file operations, capture, and analysis. A filter bar is present above the packet list.

The packet list displays the following data:

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

Below the packet list, the packet details pane shows the following information for the selected packet (No. 22):

- Device ID: CLE-SWH3750-10H-01
- Addresses
- Port ID: FastEthernet1/0/21
- Capabilities
- Software version
- Platform: cisco WS-C3750-48TS

The packet bytes pane at the bottom displays the raw data in hexadecimal and ASCII format. The ASCII column shows the following text:

```
.r6.....  
...c....CL  
E-SWH375 0-10H-01  
.....  
.....FastEthernet  
t1/0/21. ....(.  
...Cisco Interne  
twork operating  
system software  
.IOS (tm) C3750
```

The status bar at the bottom indicates: 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 fields: Header length: 20 bytes, Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00), Total Length: 78, Identification: 0x698c (27020), Flags: 0x00, and Fragment offset: 0. A red arrow points from the text "Highlighted packets here" to the Identification field. The packet bytes pane shows the hex dump of the packet, with a red arrow pointing from the text "Are shown here as well" to the hex value 69 8c in the second line.

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 FEENEFE DEOCACAL
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 protocol analyzer interface. The title bar reads "Tucker Ellis & West icmp-ethereal-trace-1 - Wireshark". The menu bar, which is circled in red, includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. Below the menu bar is a toolbar with various icons for file operations, capture, and analysis. A filter bar is present with the text "Filter: Expression... Clear Apply". The main packet list pane shows a table of captured packets:

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 00:00
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

Below the packet list is the packet details pane, which shows the structure of the selected packet (packet 1):

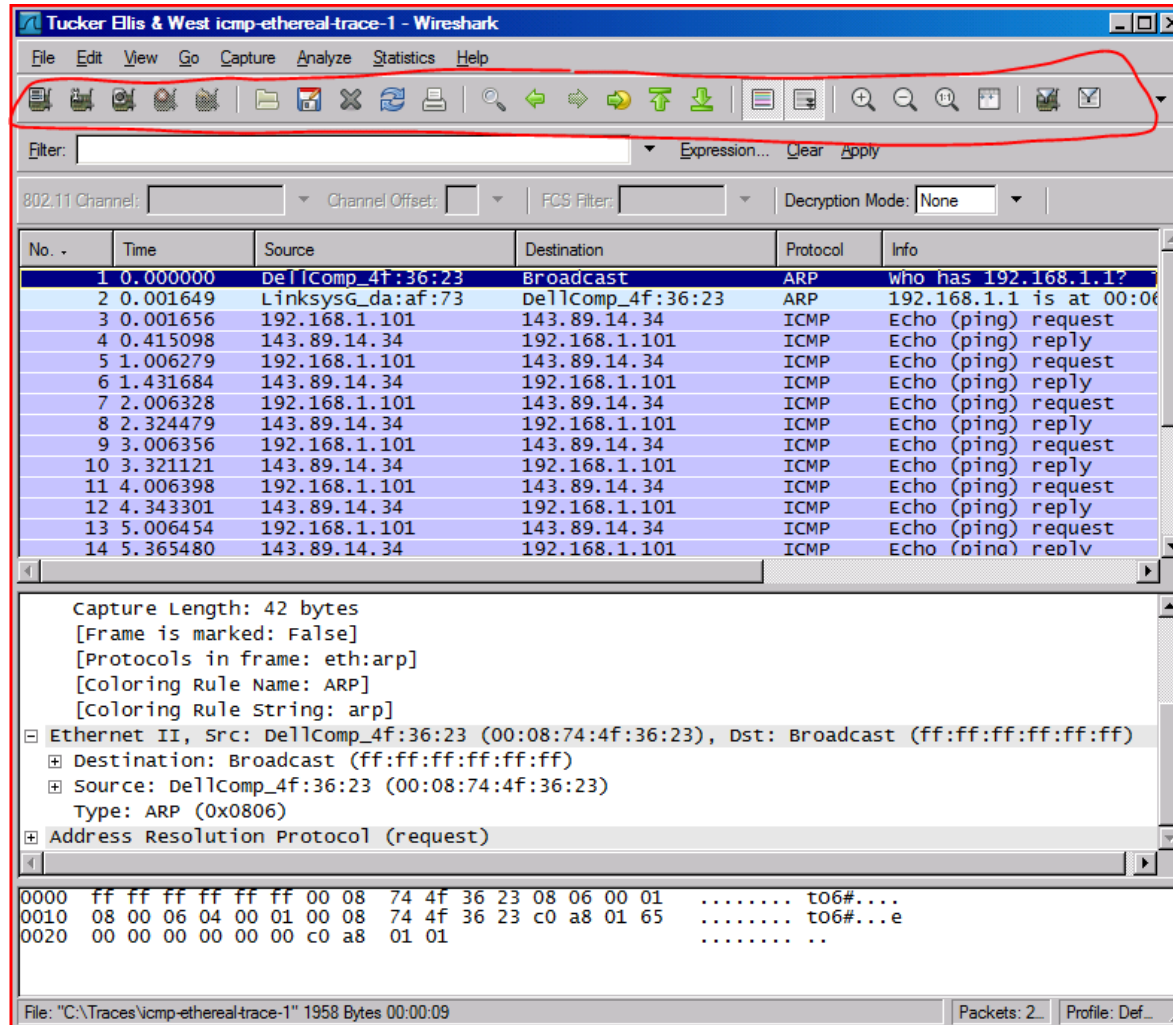
- Capture Length: 42 bytes
- [Frame is marked: False]
- [Protocols in frame: eth:arp]
- [Coloring Rule Name: ARP]
- [Coloring Rule String: arp]
- Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: DellComp_4f:36:23 (00:08:74:4f:36:23)
 - Type: ARP (0x0806)
- Address Resolution Protocol (request)

At the bottom is the packet bytes pane, showing 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 for the first packet shows the following information:

- 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

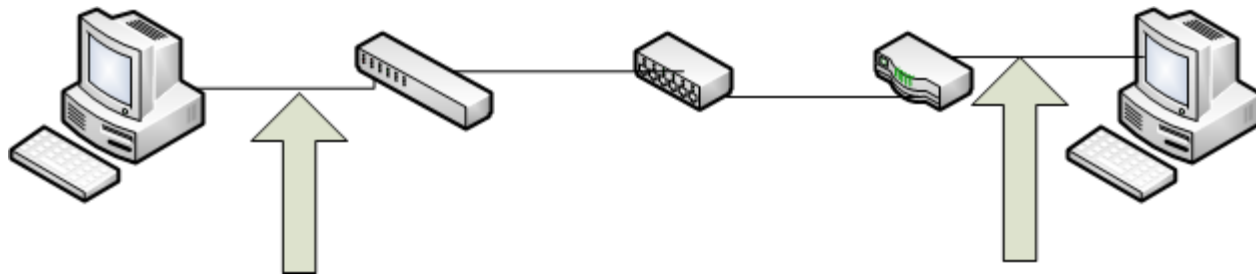
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 78
Identification: 0x698c (27020)
Flags: 0x00
Fragment offset: 0

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. ...

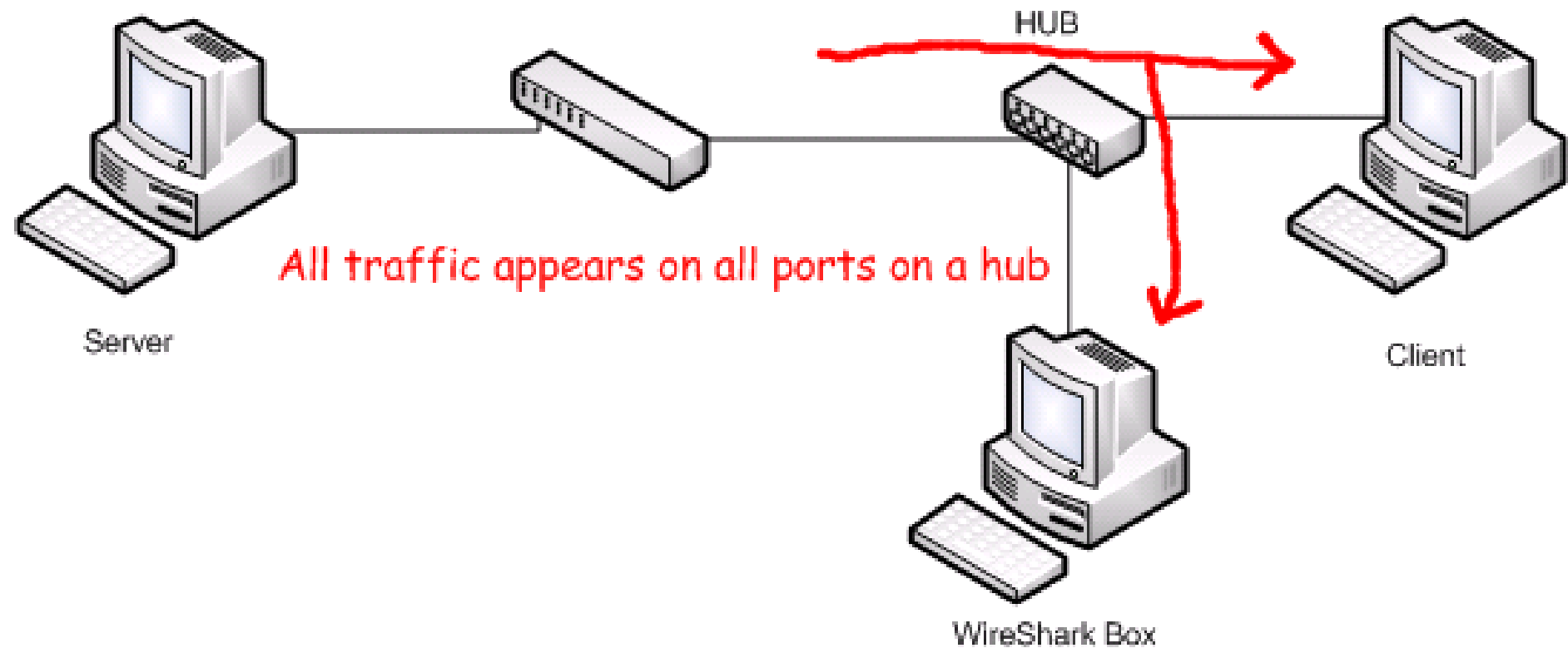
Identification (ip.id), 2 bytes
Packets: 691 Displayed: 691 Marked: 0
Profile: Default

Onde eu devo usar o
WireShark?

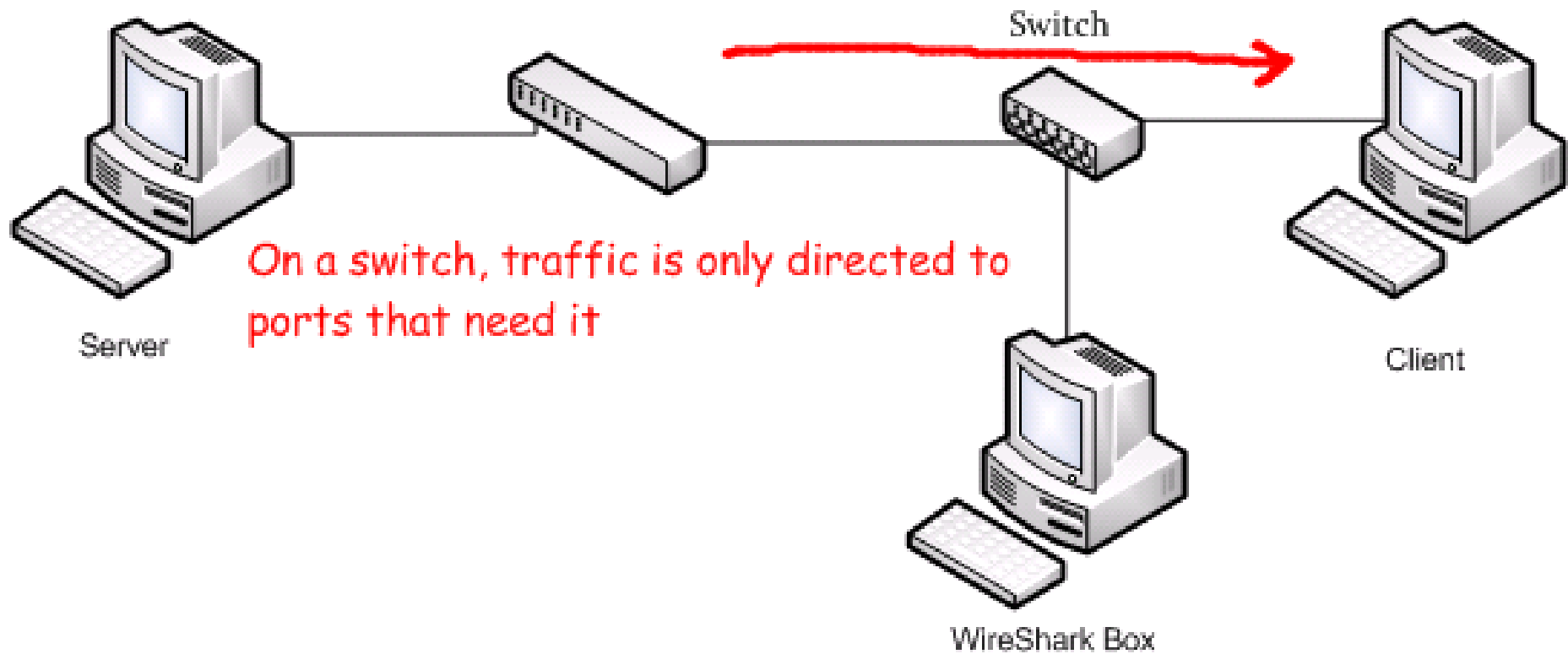
A localização muda TUDO !



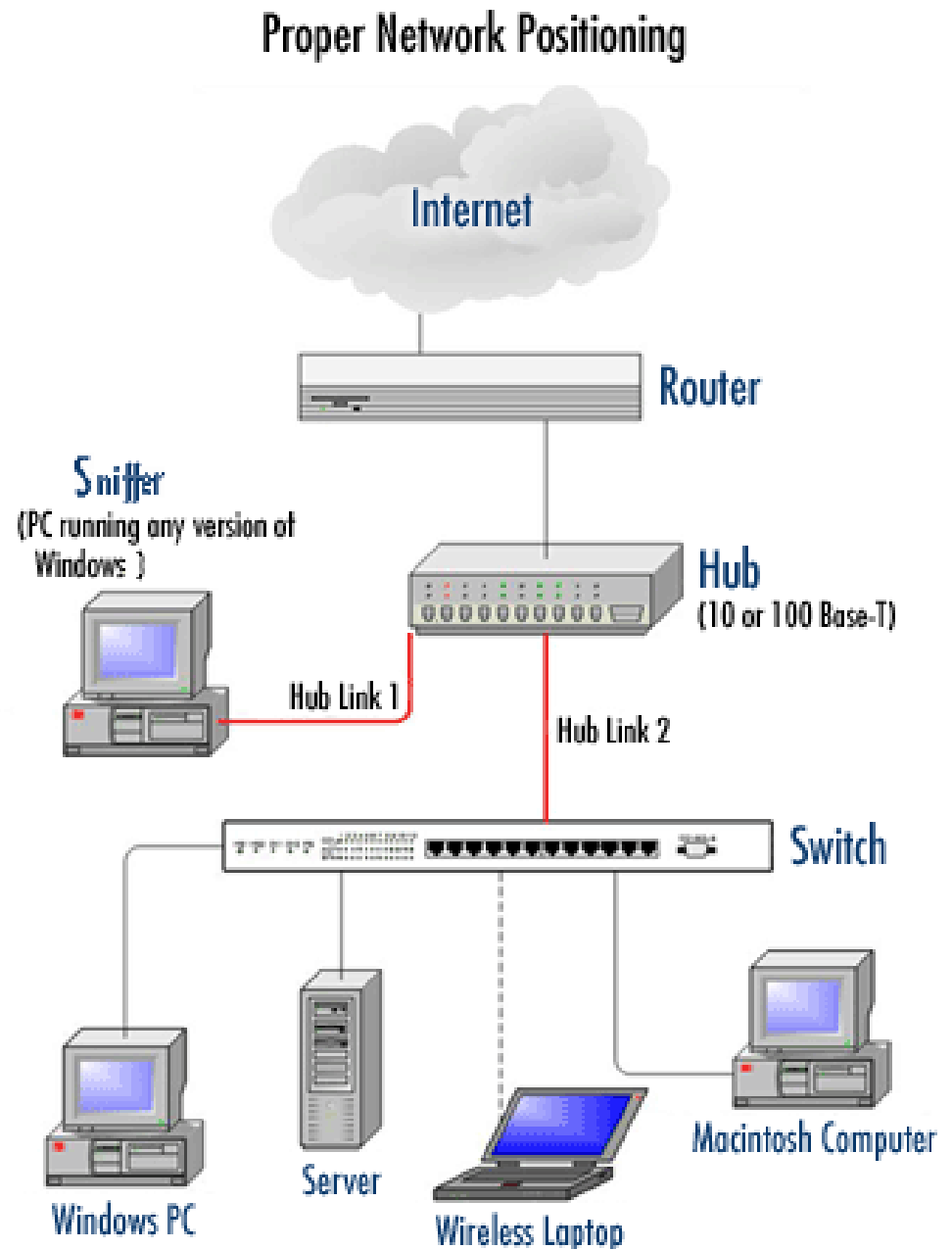
Hub



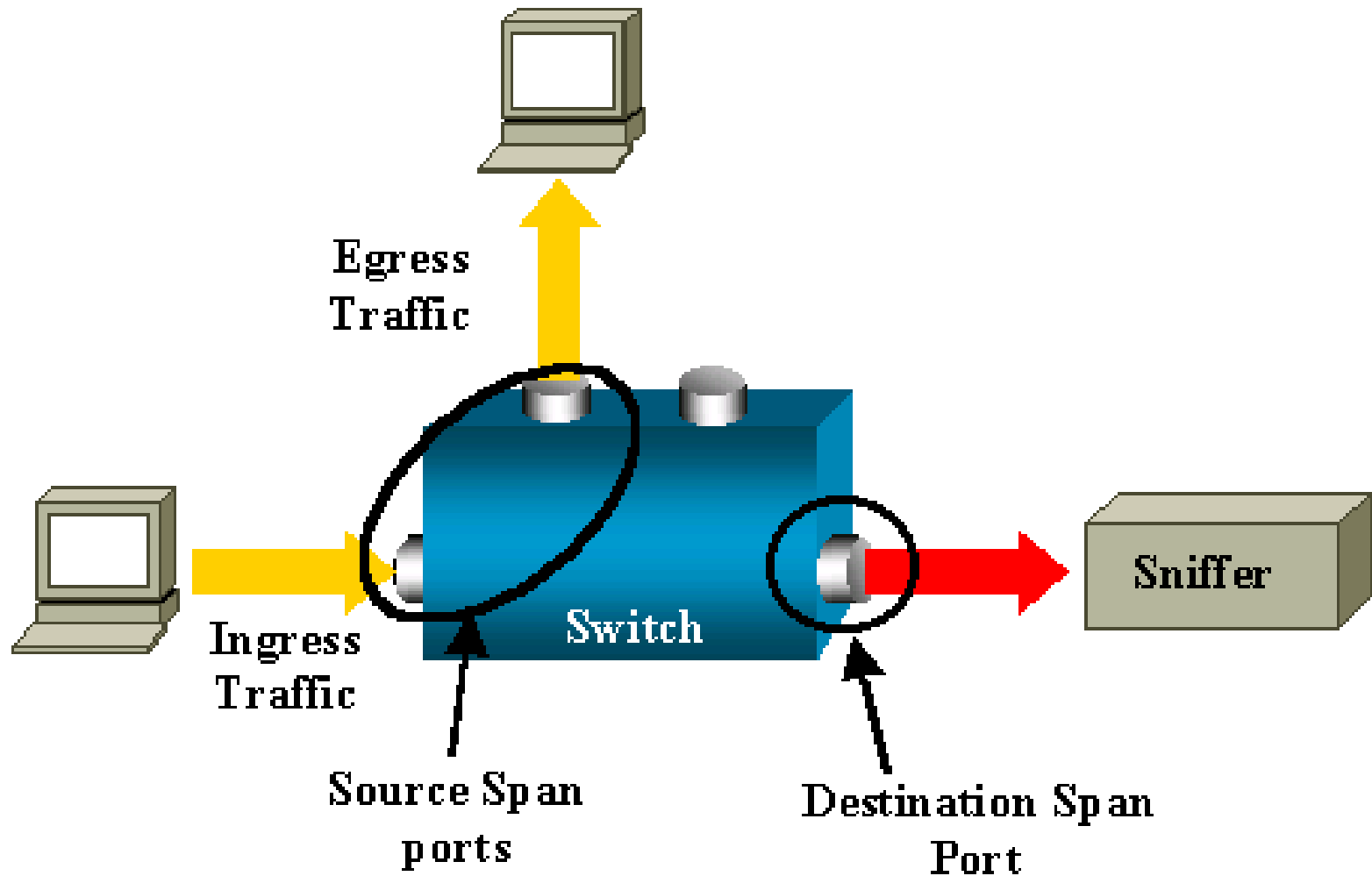
Switches



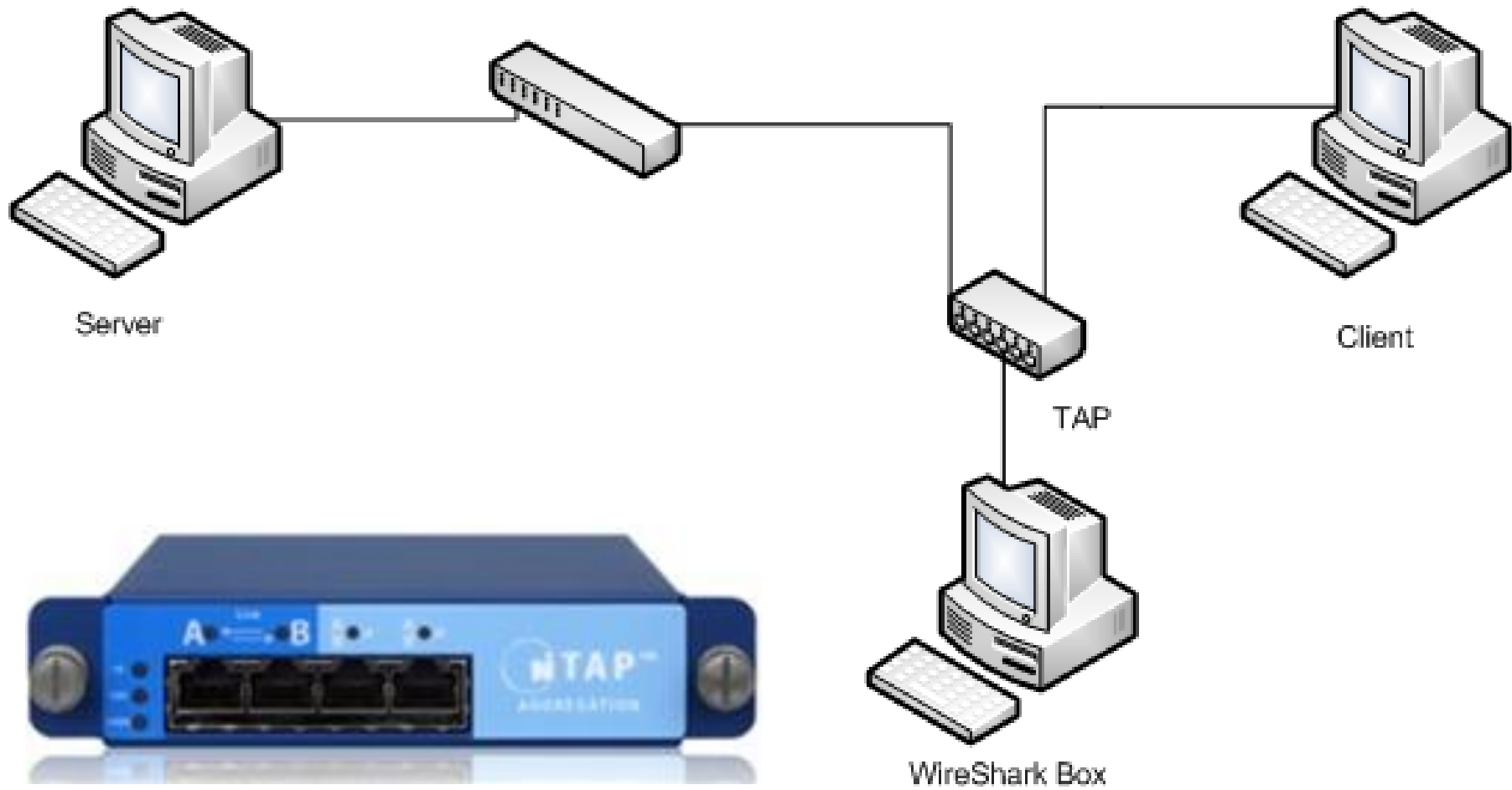
Não é o ideal, mas funciona



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//

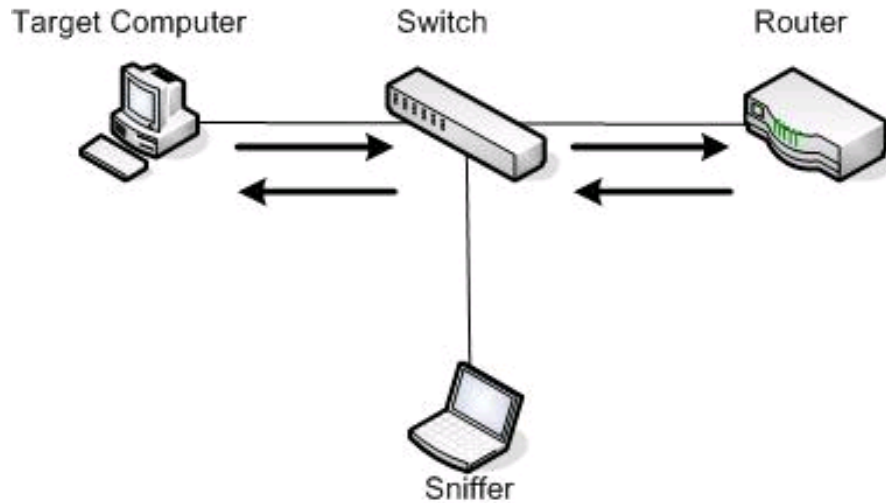
- switch(config-if)#**port monitor FastEthernet 0/3** //especificar a porta que será espelhada//

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

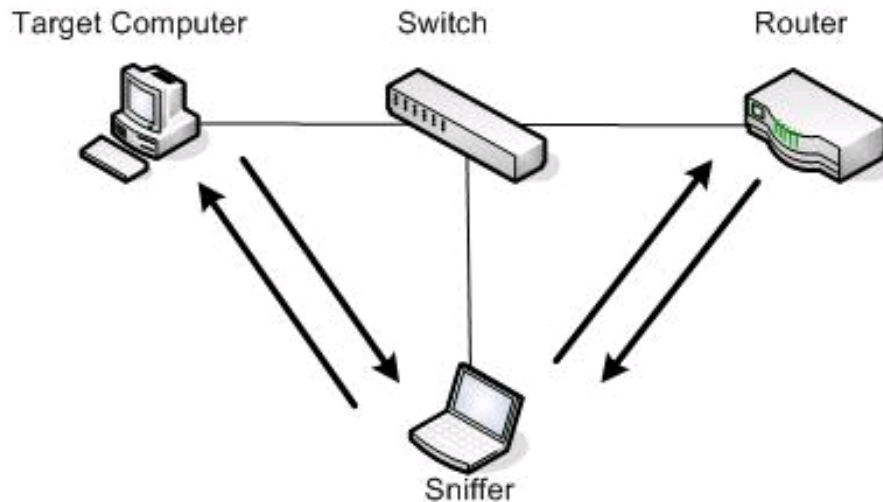
- switch(config)#**exit**

ARP Cache Poisoning

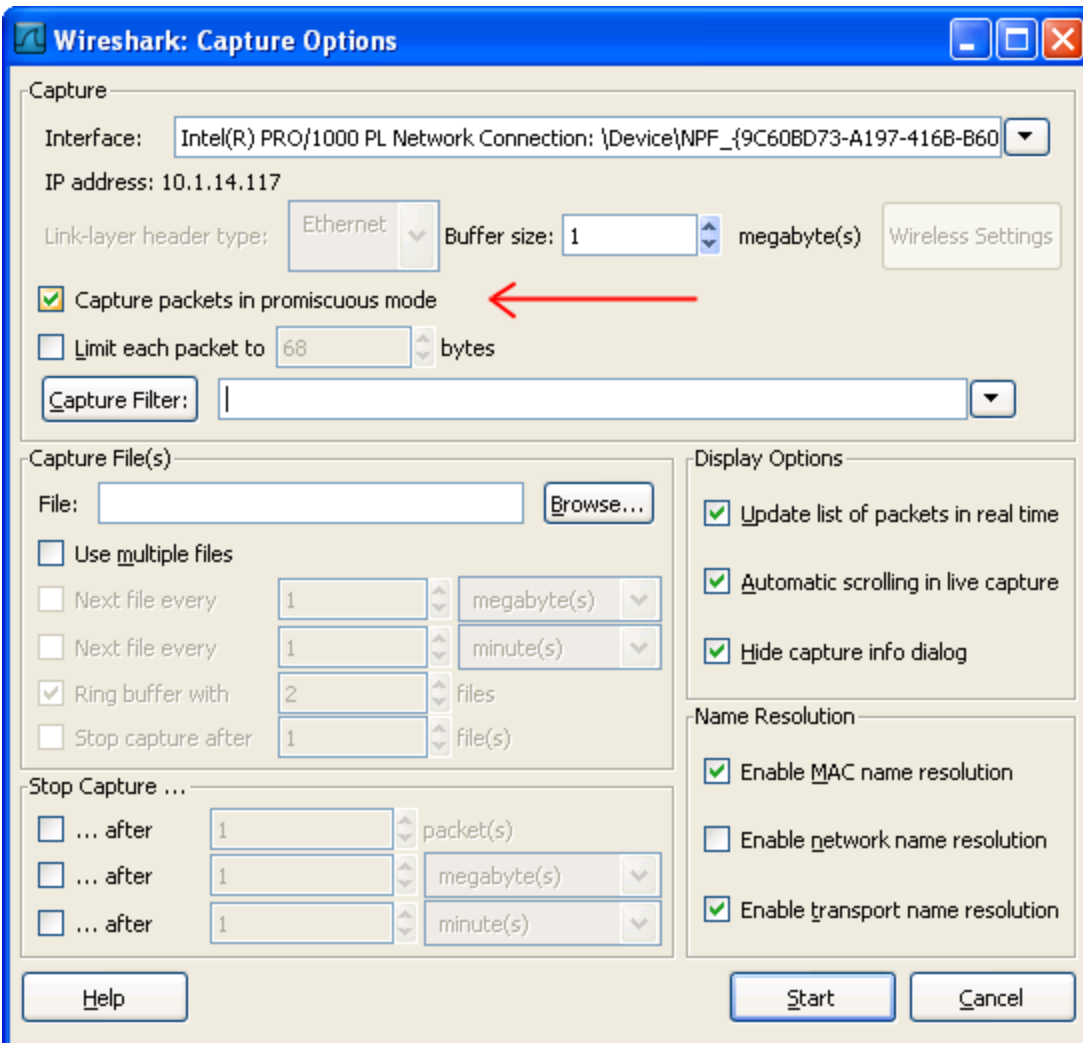
Normal Traffic Pattern



Poisoned ARP Cache

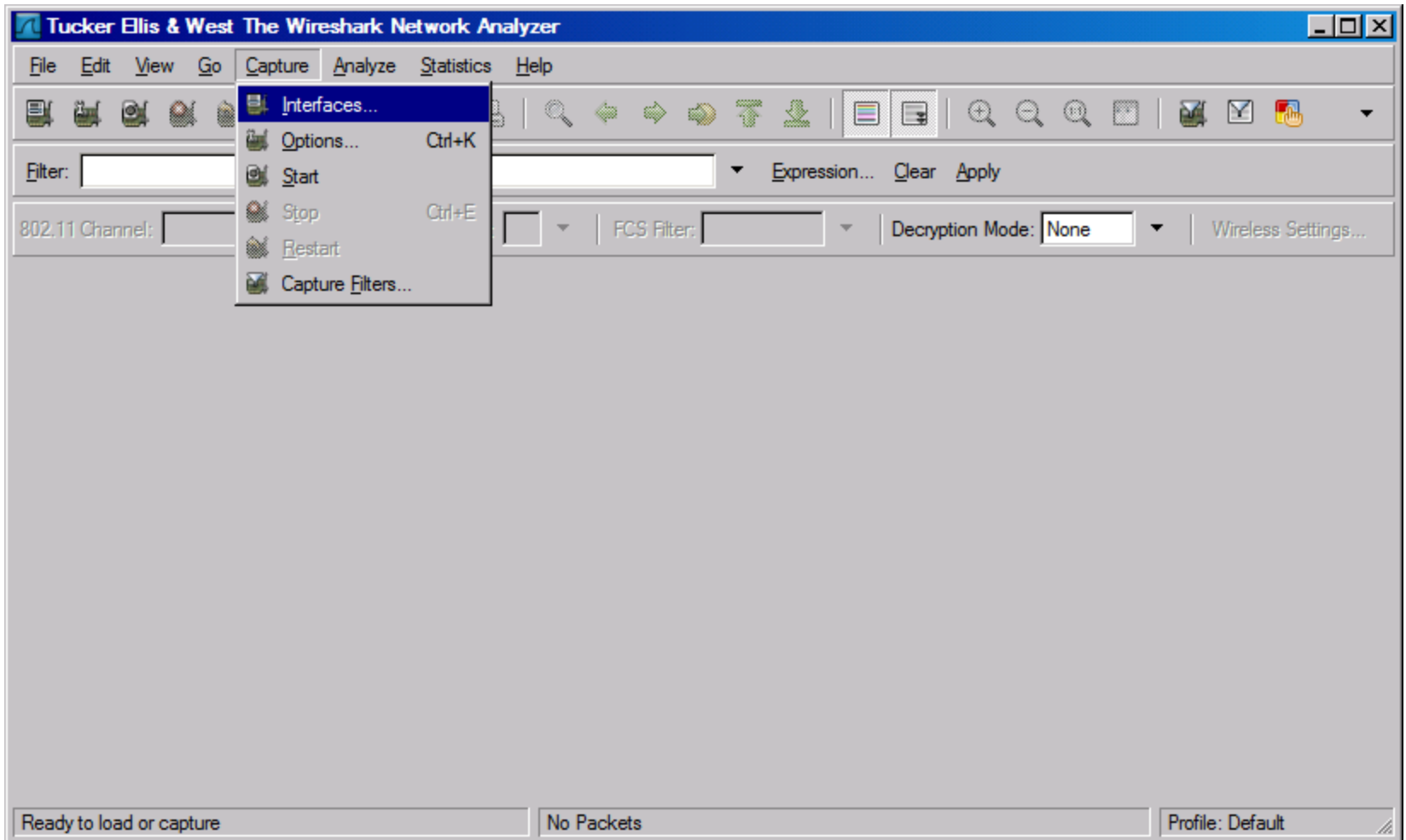


Setting promiscuous mode

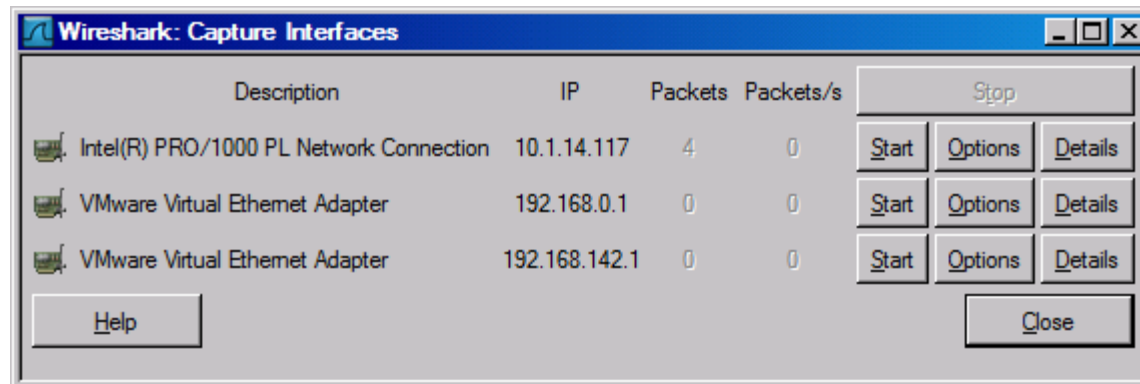


Marcando este box, estamos determinando que a interface escolhida fique em MODO PROMÍSCUO durante a captura. Se isso não for feito, o Wireshark apenas capturarão quadros broadcast e os que saem e entram na máquina onde está o sniffer.

Simple Capture



Capture Interfaces



Capture Options

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

selectively ignore traffic

Capture Filter examples

host 10.1.11.24

host 192.168.0.1 and host 10.1.11.1

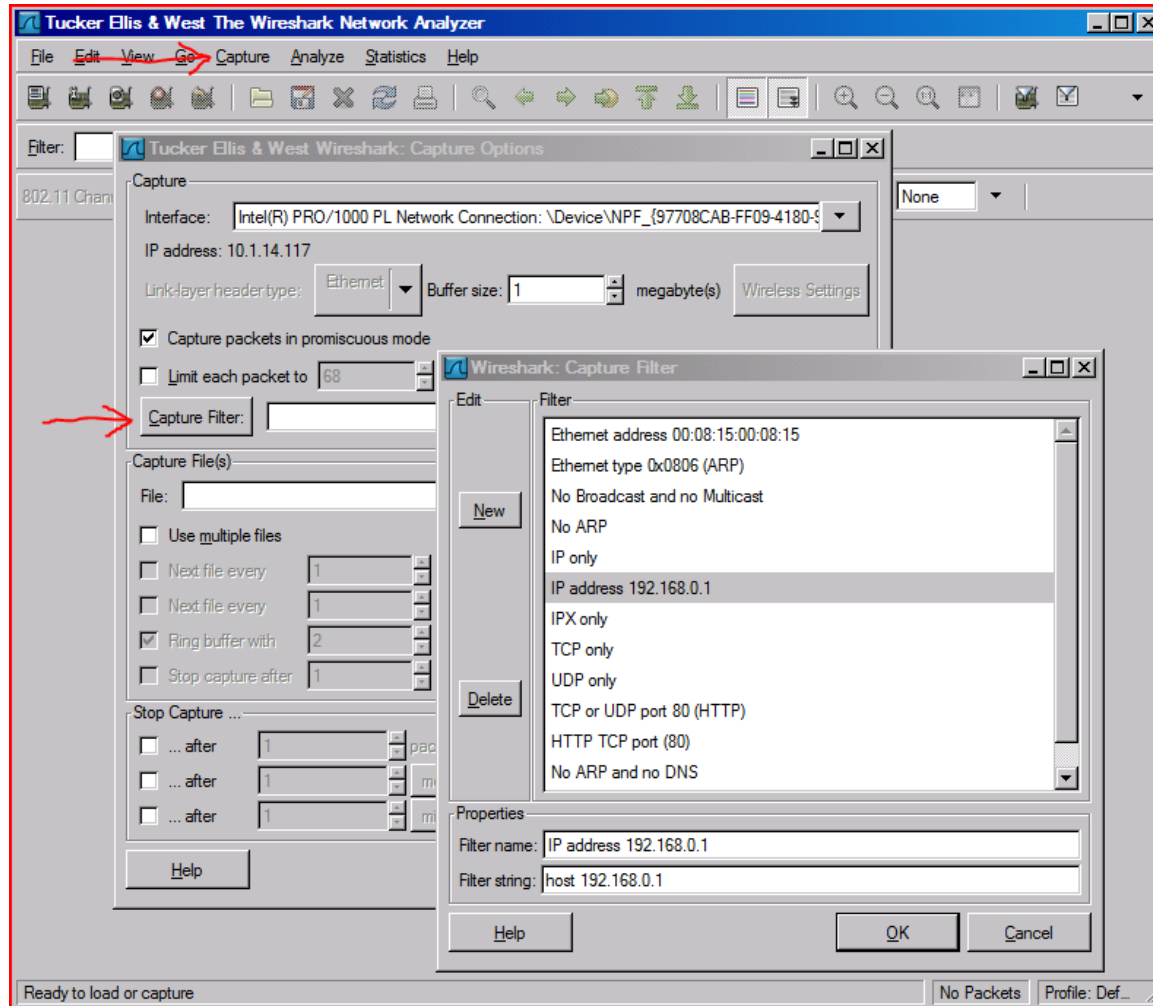
tcp port http

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-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

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

Link-layer header type: 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

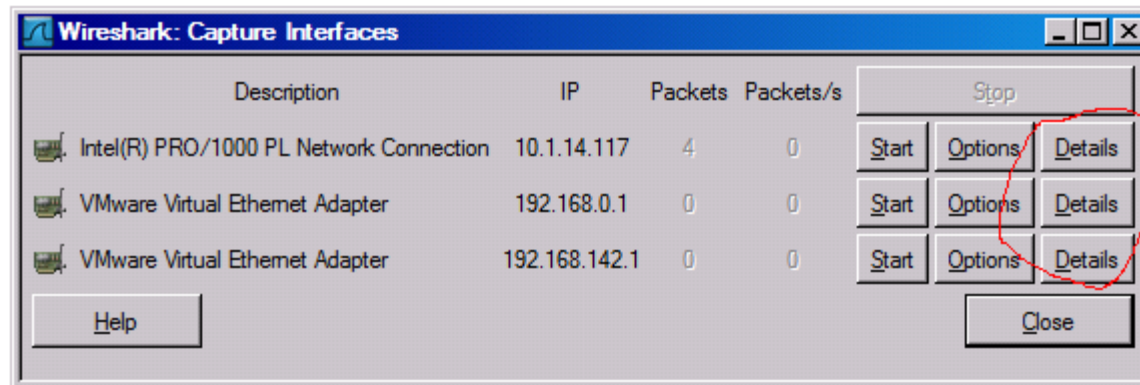
☒ Enable MAC name resolution

☐ Enable network name resolution

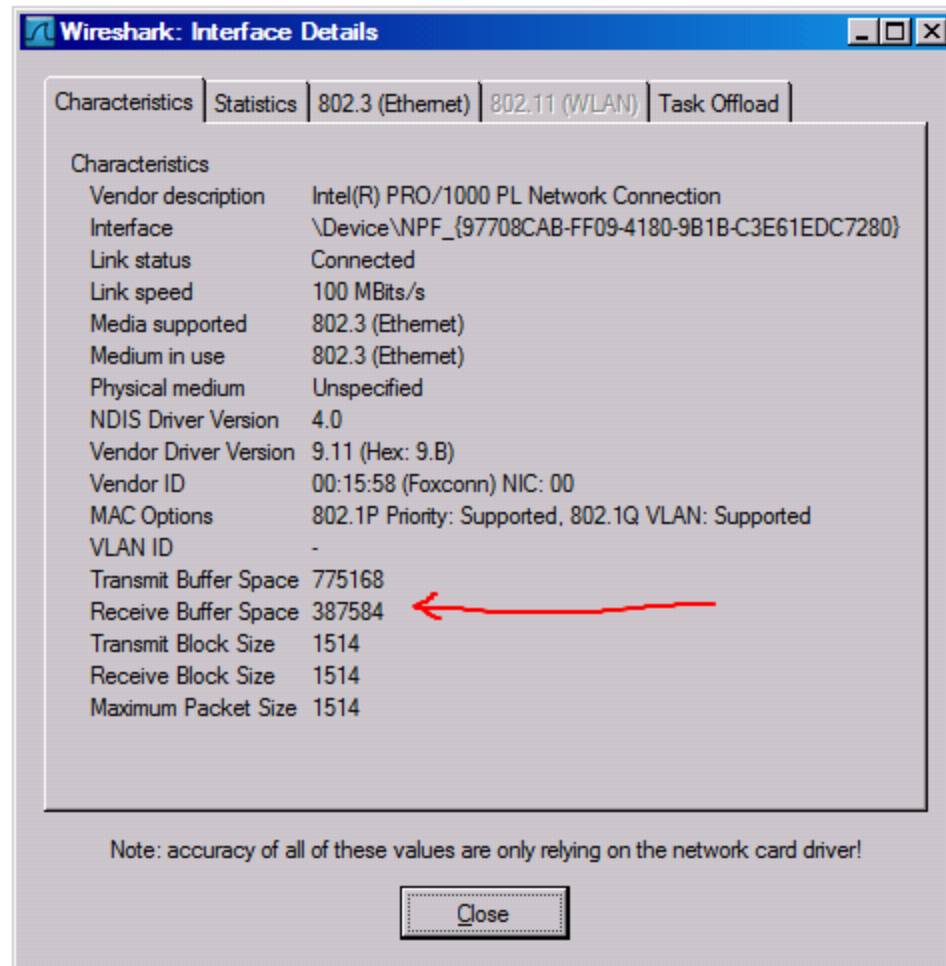
☒ Enable transport name resolution

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

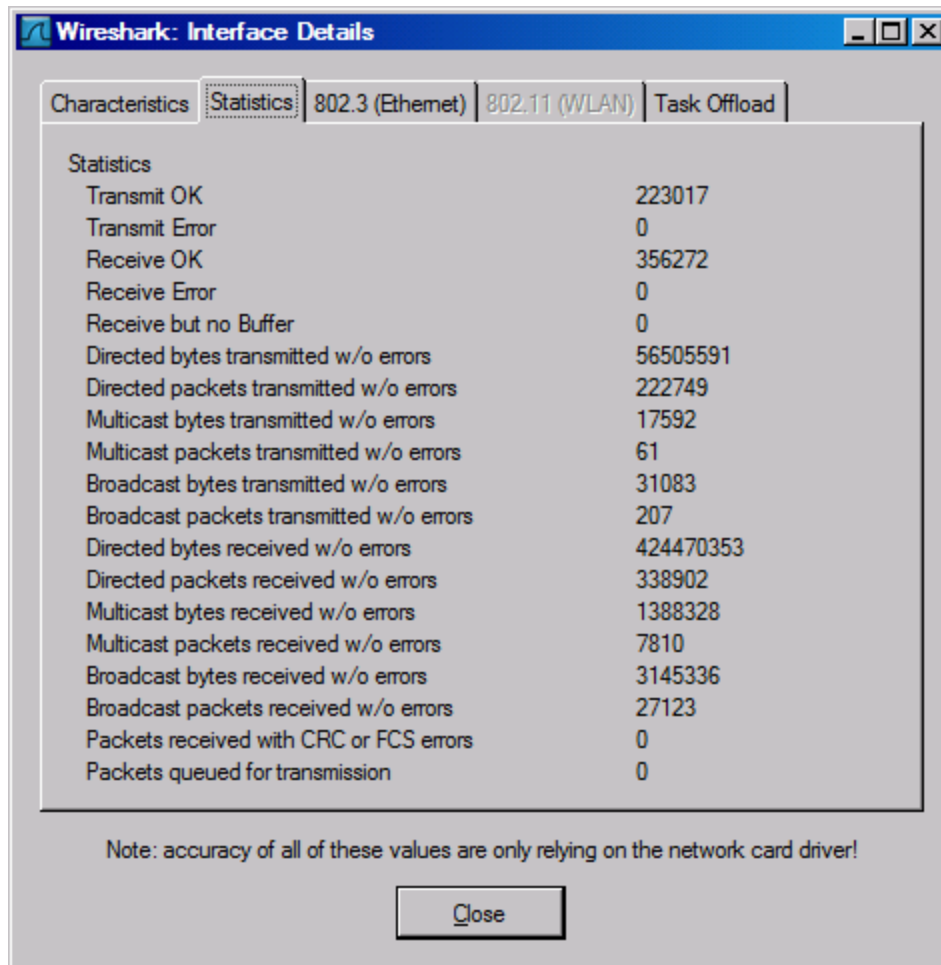
Capture Interfaces



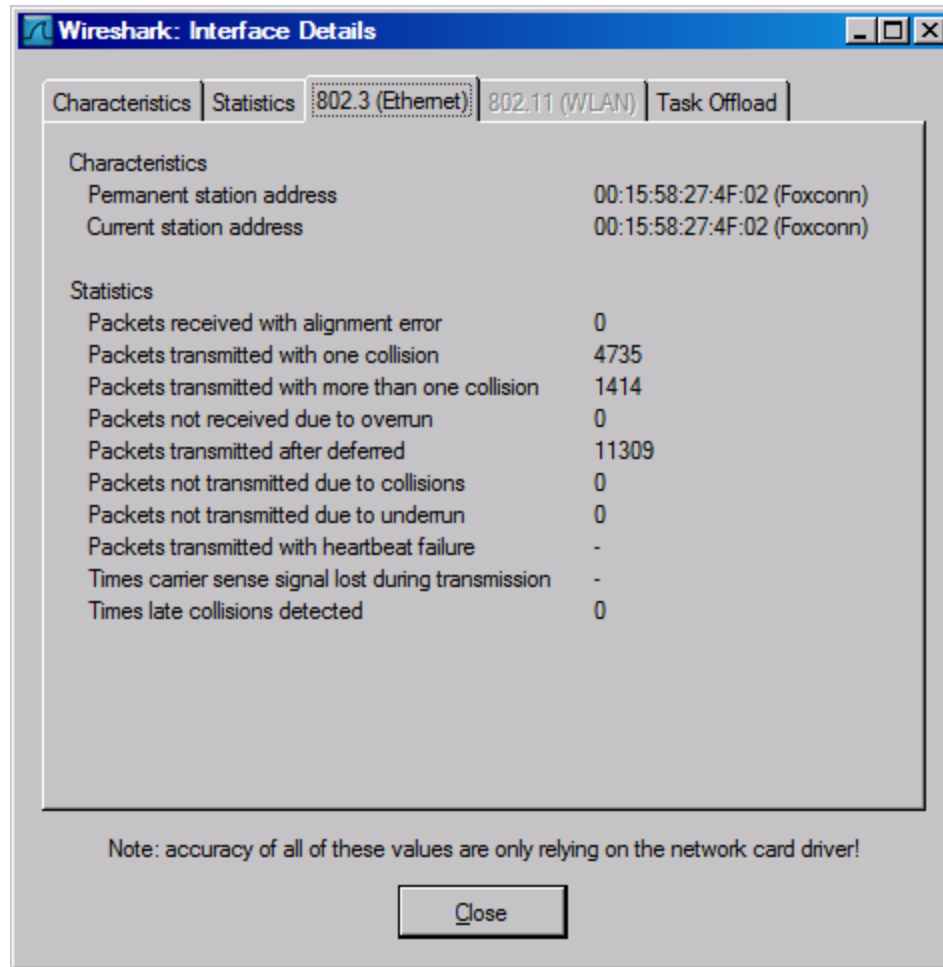
Interface Details: Characteristics



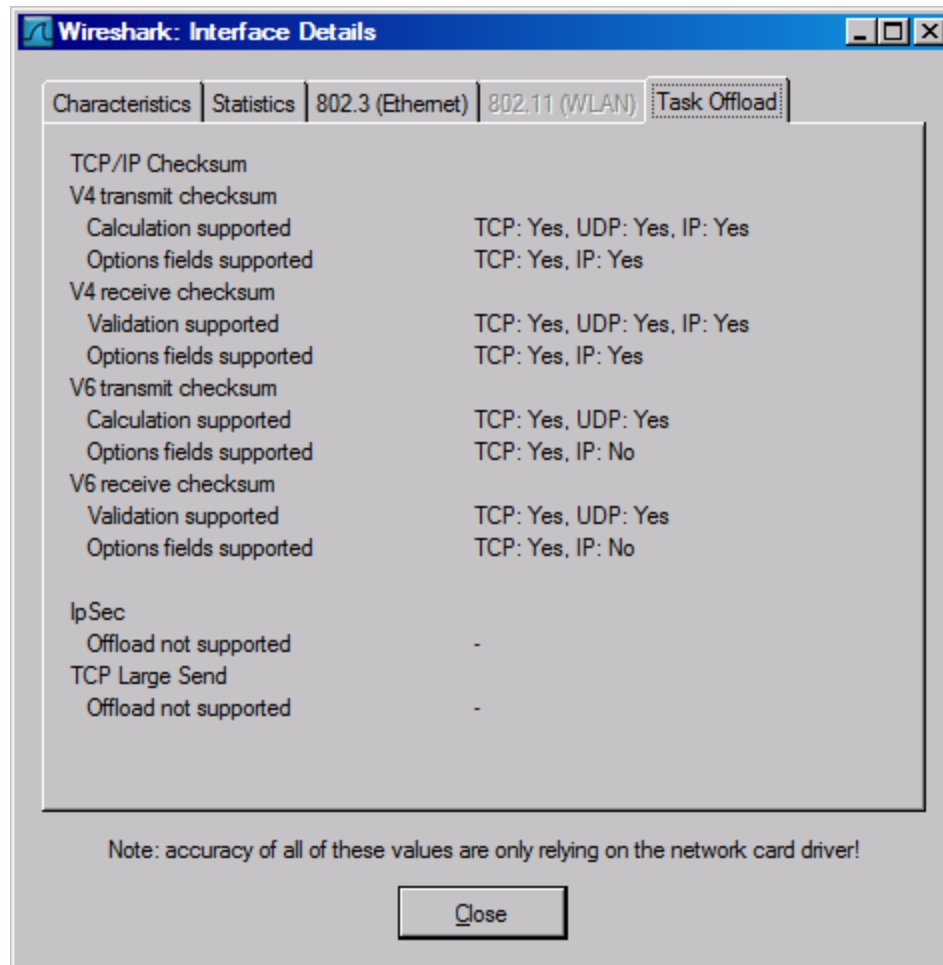
Interface Details: Statistics



Interface Details: 802.3 (Ethernet)



Interface Details: Task Offload



Checksum

A **checksum** is a form of redundancy check, a simple way to protect the integrity of data by detecting errors in data that are sent through space or time. It works by adding up the basic components of a message, typically the assorted bits, and storing the resulting value. Anyone can later perform the same operation on the data, compare the result to the authentic checksum, and (assuming that the sums match) conclude that the message was most likely not corrupted.

Source: [Wikipedia.com](https://en.wikipedia.org/wiki/Checksum)

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):

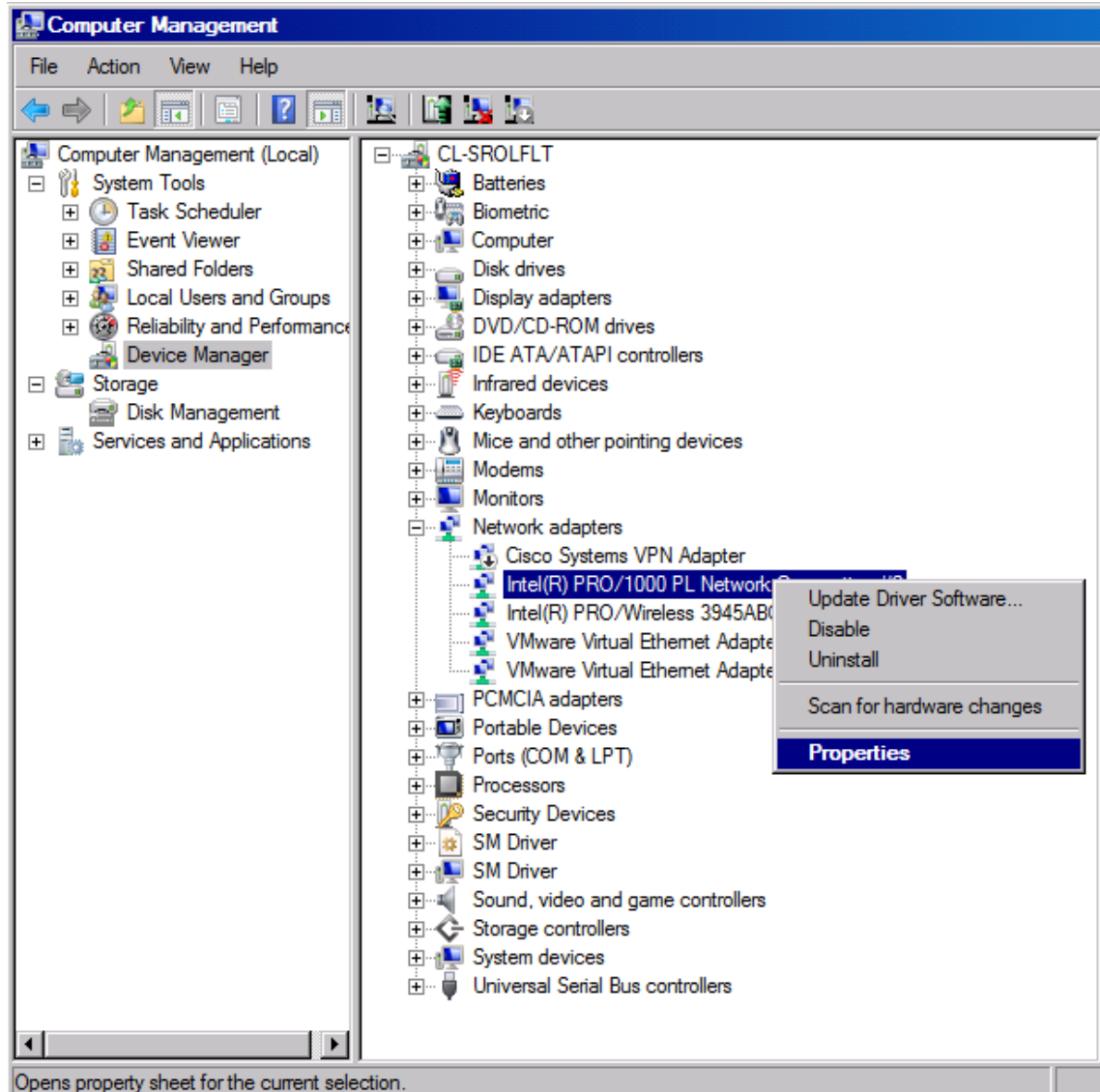
```
ifconfig em0 -rcxsum -tcxsum (choose correct network interface if not em0)
```

On MacOS (as root):

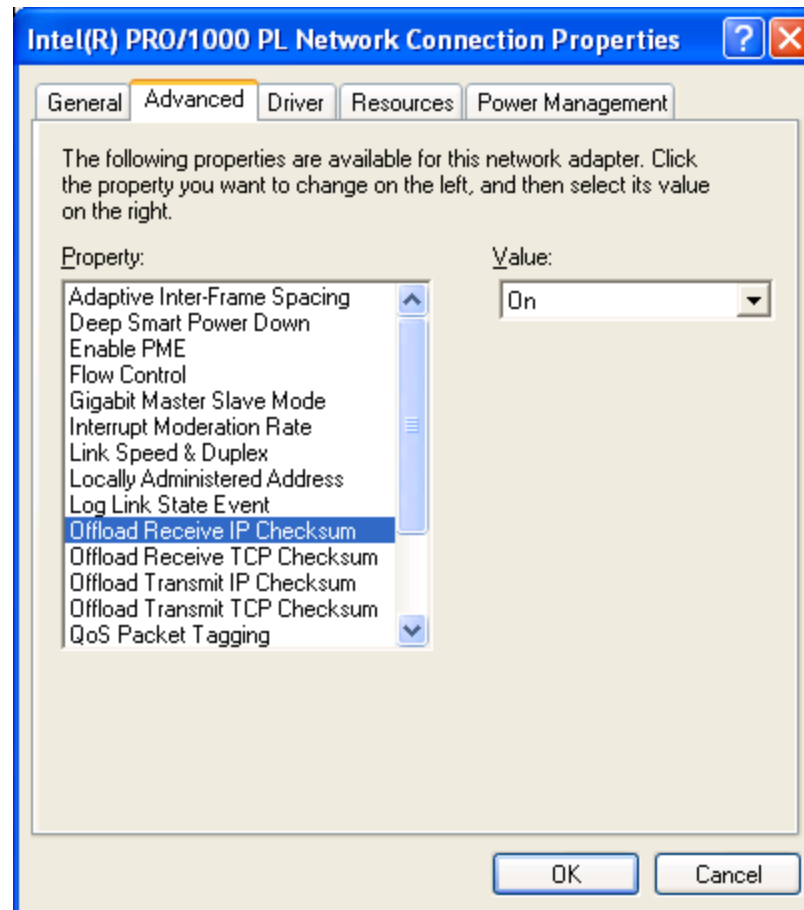
```
sysctl -w net.link.ether.inet.apple_hwcksum_tx=0
```

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

Turning off Checksum offload



Turning off Checksum offload



Capture Options

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

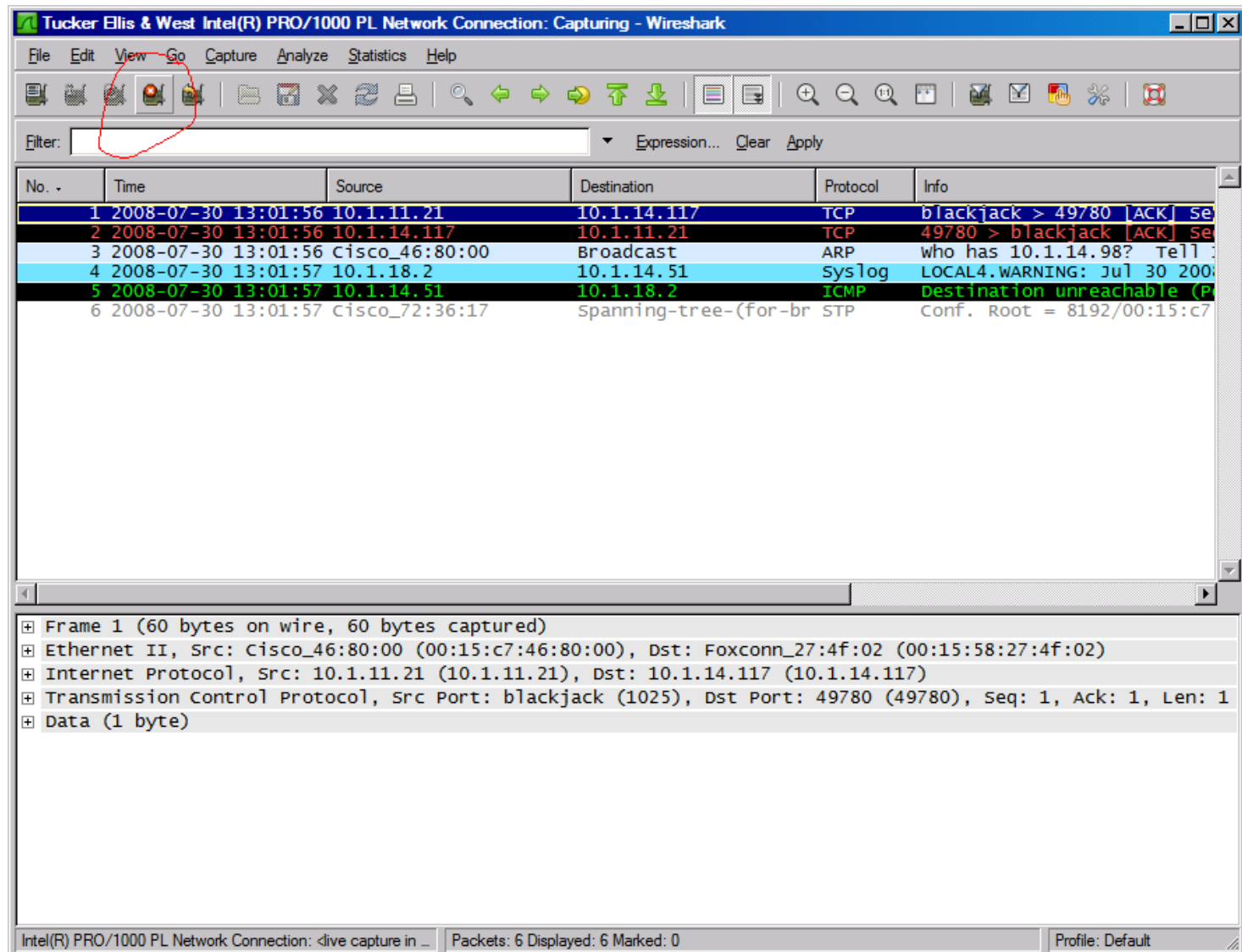
☒ Enable MAC name resolution

☐ Enable network name resolution

☒ Enable transport name resolution

Help Start Cancel

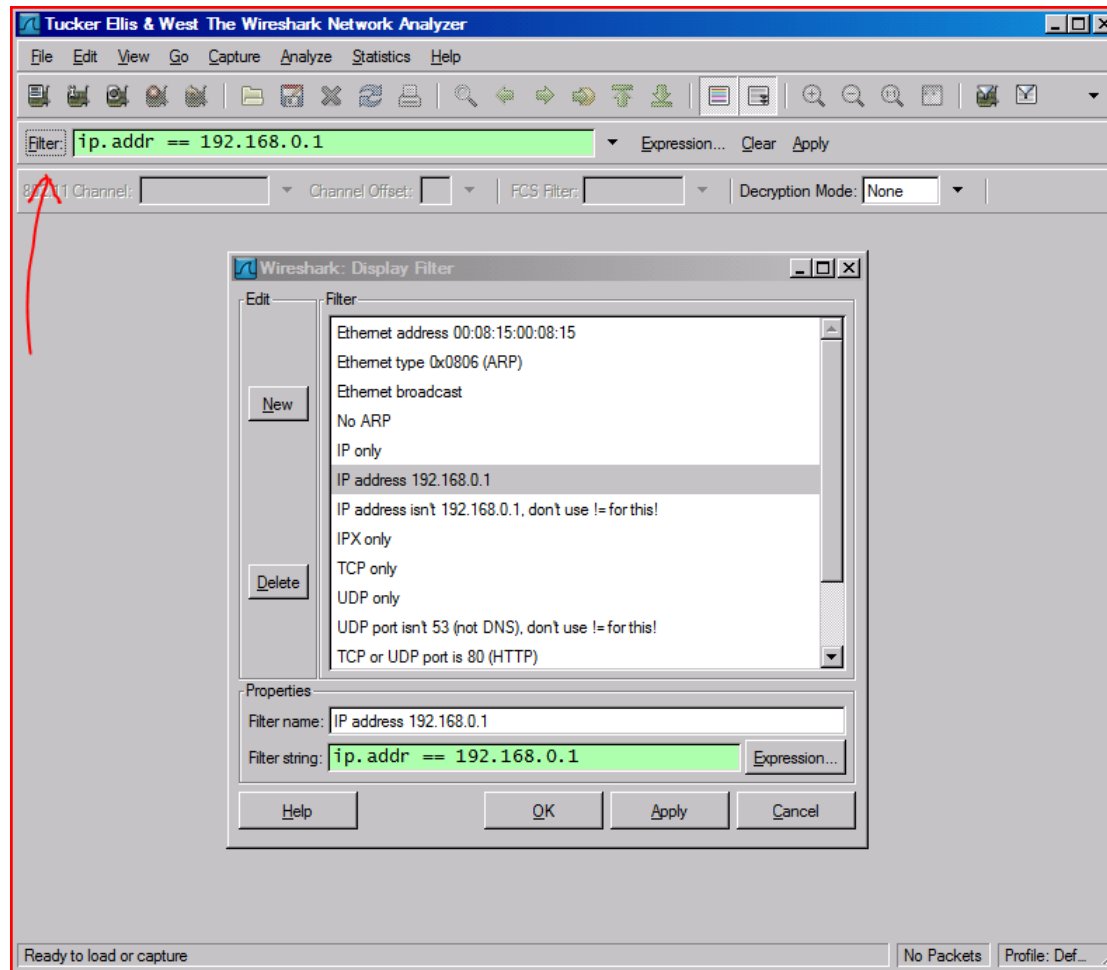
Stopping the Packet Capture



Display Filters (Post-Filters)

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

Display Filter



Display Filter Examples

`ip.src==10.1.11.24`

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

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

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

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

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

Protocol Hierarchy

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 various functions like opening files, saving, and zooming.

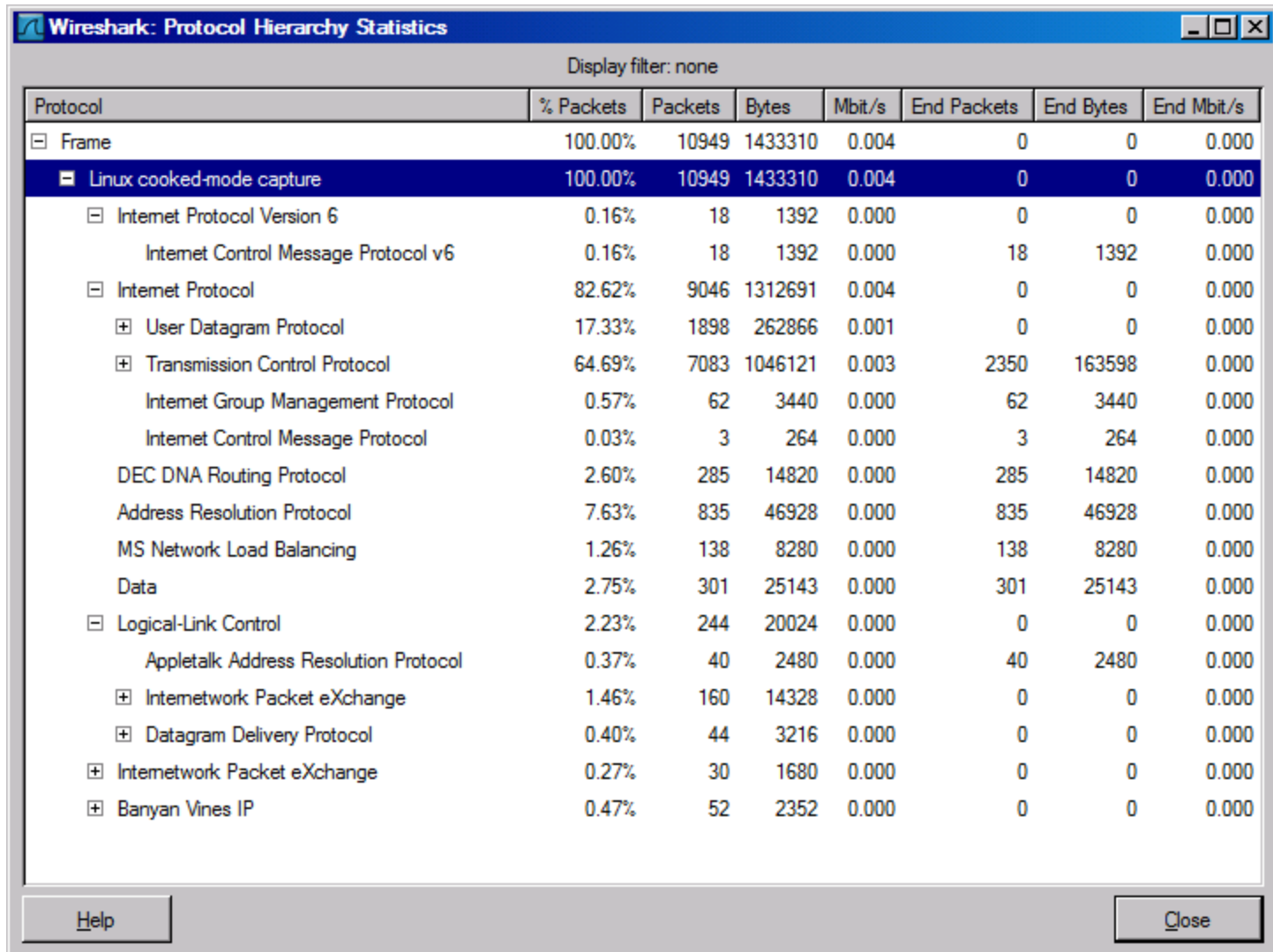
The left pane shows the "Filter:" field and a list of packets. The middle pane shows the "Protocol Hierarchy" pane, which is currently expanded. It displays a tree view of protocols: Summary, Conversations, Endpoints, and IO Graphs. Under "Conversations", a list of protocols is shown, including ICMPv6, NBNS, DNS, and RTP. The right pane shows the packet details for the selected packet (No. 14, Time 3.543088, Source 192.168.1.1). The details pane shows the protocol stack: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMPv6). The packet list at the bottom shows the raw packet data in hexadecimal and ASCII.

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

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

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

Protocol Hierarchy



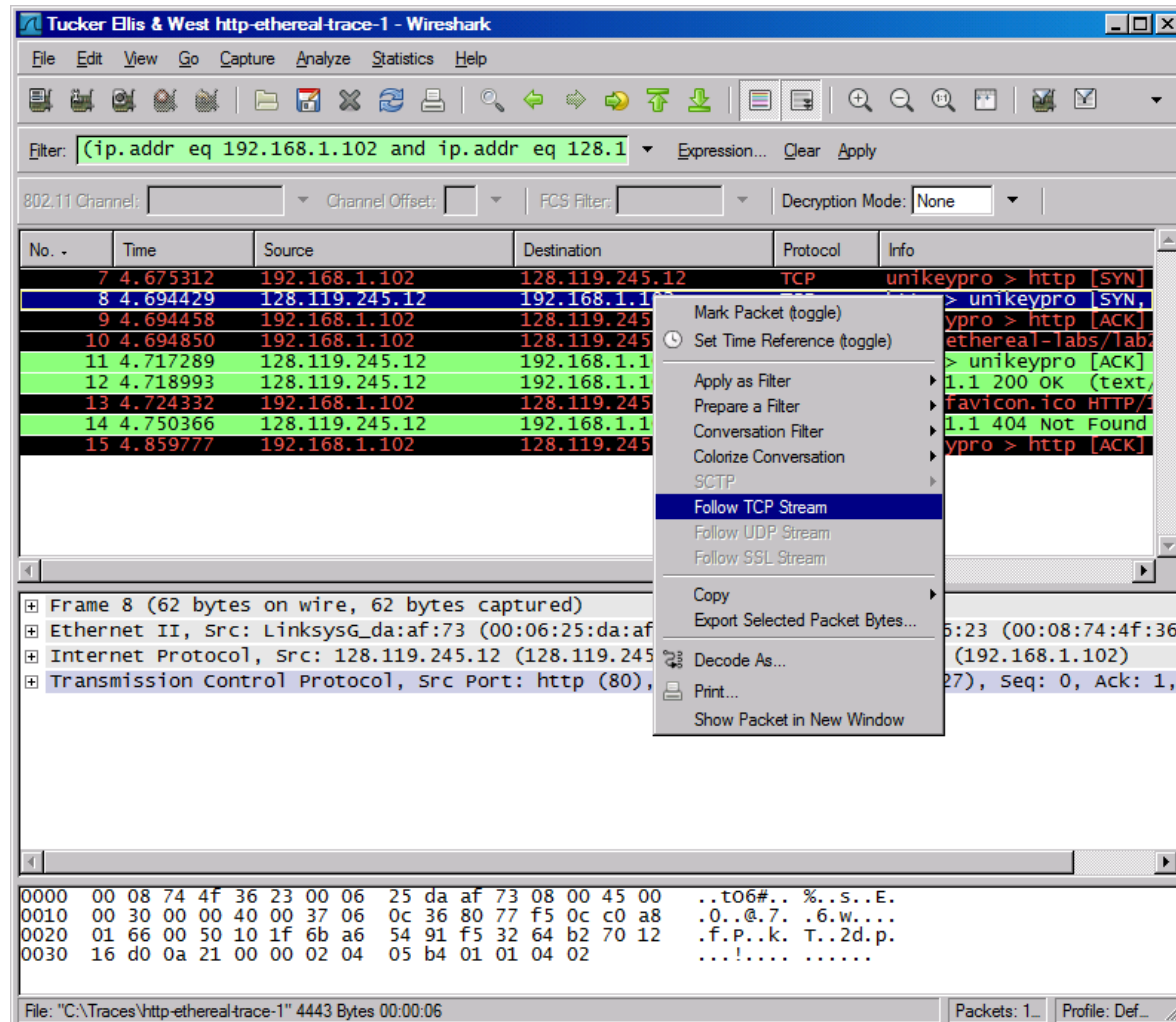
Wireshark: Protocol Hierarchy Statistics

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

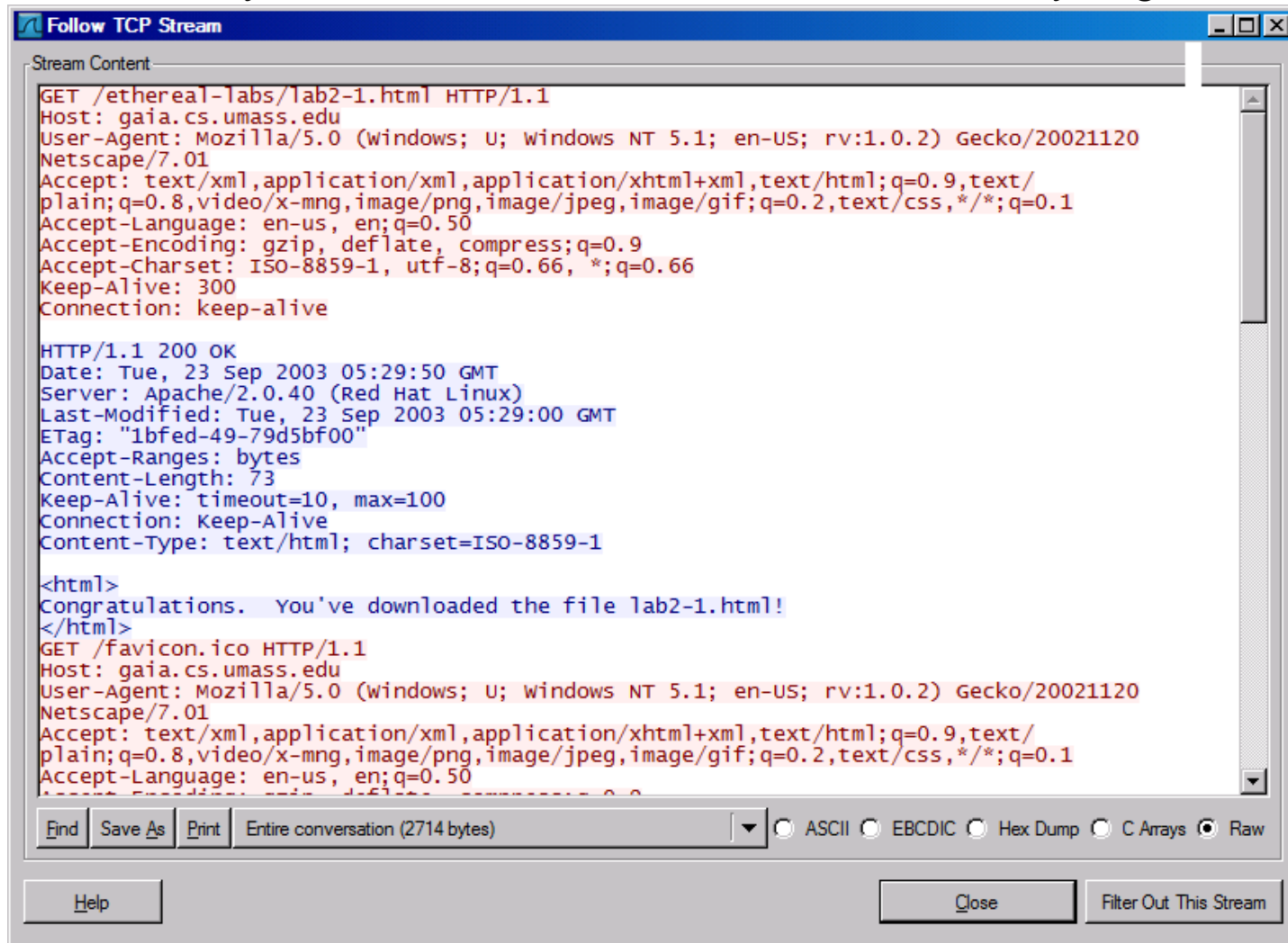
Follow TCP Stream



Follow TCP Stream

red - stuff you sent

blue - stuff you get



The screenshot shows a window titled "Follow TCP Stream" with a "Stream Content" pane. The pane displays a network conversation between a client (Netscape) and a server (gaia.cs.umass.edu). The client sends an HTTP GET request for "/ethereal-labs/lab2-1.html". The server responds with an HTTP 200 OK status and a content type of "text/html". The client then sends a GET request for "/favicon.ico". The server responds with an HTTP 200 OK status and a content type of "text/html". The client then sends a GET request for "/favicon.ico". The server responds with an HTTP 200 OK status and a content type of "text/html". The client then sends a GET request for "/favicon.ico". The server responds with an HTTP 200 OK status and a content type of "text/html".

```
GET /ethereal-labs/lab2-1.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120
Netscape/7.01
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en-us, en;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *,q=0.66
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 23 Sep 2003 05:29:50 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT
ETag: "1bfed-49-79d5bf00"
Accept-Ranges: bytes
Content-Length: 73
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<html>
Congratulations. You've downloaded the file lab2-1.html!
</html>

GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120
Netscape/7.01
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en-us, en;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *,q=0.66
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 23 Sep 2003 05:29:50 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT
ETag: "1bfed-49-79d5bf00"
Accept-Ranges: bytes
Content-Length: 73
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<html>
Congratulations. You've downloaded the file lab2-1.html!
</html>

GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120
Netscape/7.01
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1
Accept-Language: en-us, en;q=0.50
Accept-Encoding: gzip, deflate, compress;q=0.9
Accept-Charset: ISO-8859-1, utf-8;q=0.66, *,q=0.66
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 23 Sep 2003 05:29:50 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT
ETag: "1bfed-49-79d5bf00"
Accept-Ranges: bytes
Content-Length: 73
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=ISO-8859-1

<html>
Congratulations. You've downloaded the file lab2-1.html!
</html>
```

Find Save As Print Entire conversation (2714 bytes) [Dropdown] [Radio Buttons: ASCII, EBCDIC, Hex Dump, C Arrays, Raw]

Help Close Filter Out This Stream

Expert Info

The screenshot shows the Wireshark interface with the 'Expert Info' pane open. The main packet list shows frame 8 selected, which is an HTTP 200 OK response. The Expert Info pane displays details for this frame, including Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Wireshark Window: Tucker Ellis & West http-ethereal-trace-1 - Wireshark

Filter: 802.11 Channel: []

Expert Info:

- ☒ 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

Packet List:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.104	192.168.1.102	SNMP	get-request SNMPv2-SMI
2	0.017162	192.168.1.102	192.168.1.104	SNMP	get-response SNMPv2-SMI
3	3.017086	192.168.1.104	192.168.1.102	SNMP	get-request SNMPv2-SMI
4	3.034572	192.168.1.102	192.168.1.104	SNMP	get-response SNMPv2-SMI
5	4.626878	192.168.1.19	192.168.1.102	DNS	Standard query A qiaa.
6	4.663785	192.168.1.102	192.168.1.102	DNS	Standard query response
7	4.675312	192.168.1.45.12	192.168.1.102	TCP	unikeypro > http [SYN]
8	4.694429	192.168.1.102	192.168.1.45.12	TCP	http > unikeypro [SYN]
9	4.694458	192.168.1.45.12	192.168.1.102	TCP	unikeypro > http [ACK]
10	4.694850	192.168.1.45.12	192.168.1.102	HTTP	GET /ethereal-labs/lab
11	4.717289	192.168.1.102	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

Frame 8 (62 bytes on wire, 62 bytes captured)

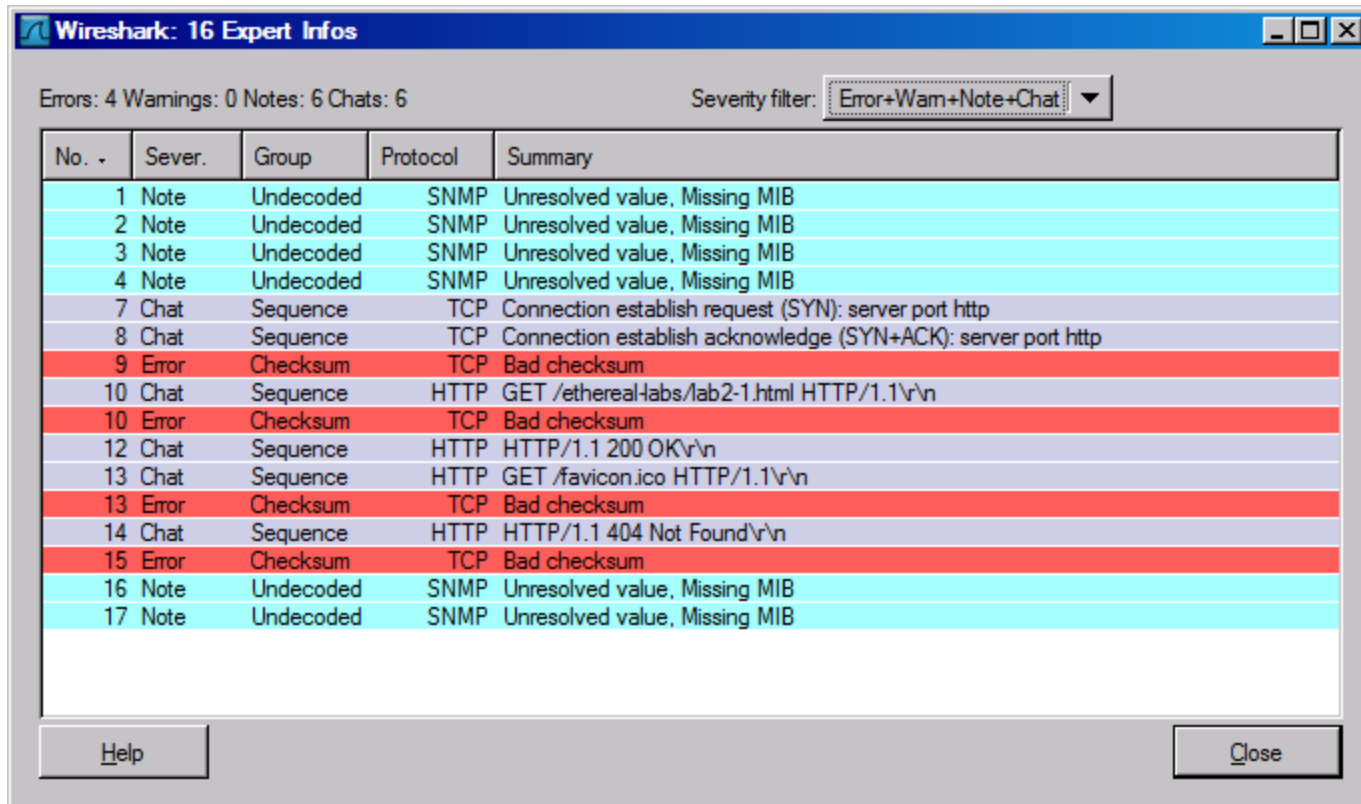
- Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
- Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
- Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 0, Ack: 1,

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 pane displays a list of network sessions, each with a number, time, and source IP address. The sessions are color-coded: blue for SNMP, green for DNS, and red for HTTP. The detailed view on the right shows the selected session (104) and its protocol (HTTP). The packet list on the left shows the selected packet (104) and its details (Ethernet II, Internet Protocol, User Datagram Protocol, Simple Network Management Protocol).

Conversations List:

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	192.168.1.19
6	4.663785	63.240.76.102
7	4.675312	192.168.1.102
8	4.694429	128.119.2.102
9	4.694458	192.168.1.102
10	4.694850	192.168.1.102
11	4.717289	128.119.2.102
12	4.718993	128.119.2.102
13	4.724332	192.168.1.102
14	4.750366	128.119.2.102

Selected Session (104):

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.4
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

Selected Packet (104):

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

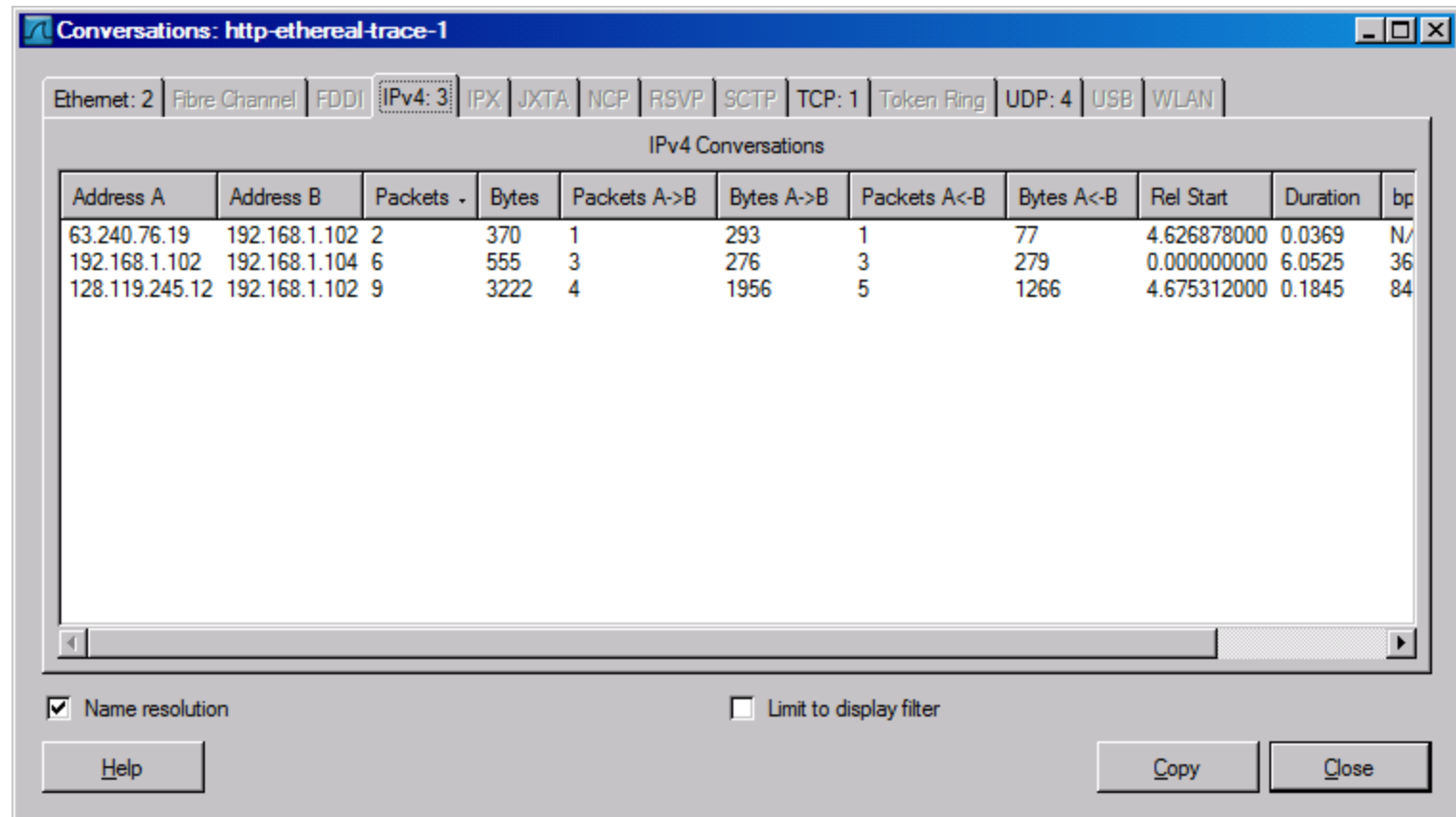
Packet Details:

- Ethernet II, Src: Hewlett-Packard (08:00:00:08:00:08), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
- Internet Protocol, Src: 192.168.1.102, Dst: 192.168.1.102
- User Datagram Protocol, Src Port: 4125, Dst Port: 4125
- Simple Network Management Protocol

Packet Data:

```
0000 00 08 74 4f 36 23 00 3c 00 08 00 00 00 00 00 00
0010 00 4f ec d8 00 00 3c 11 00 00 00 00 00 00 00 00
0020 01 66 00 a1 10 1d 00 3b 00 00 00 00 00 00 00 00
0030 06 70 75 62 6c 69 63 a2 24 02 02 18 31 02 01 00
0040 02 01 00 30 18 30 16 06 11 2b 06 01 04 01 0b 02
0050 02 00 04 02 01 02 02 01 00 04 01 10
```

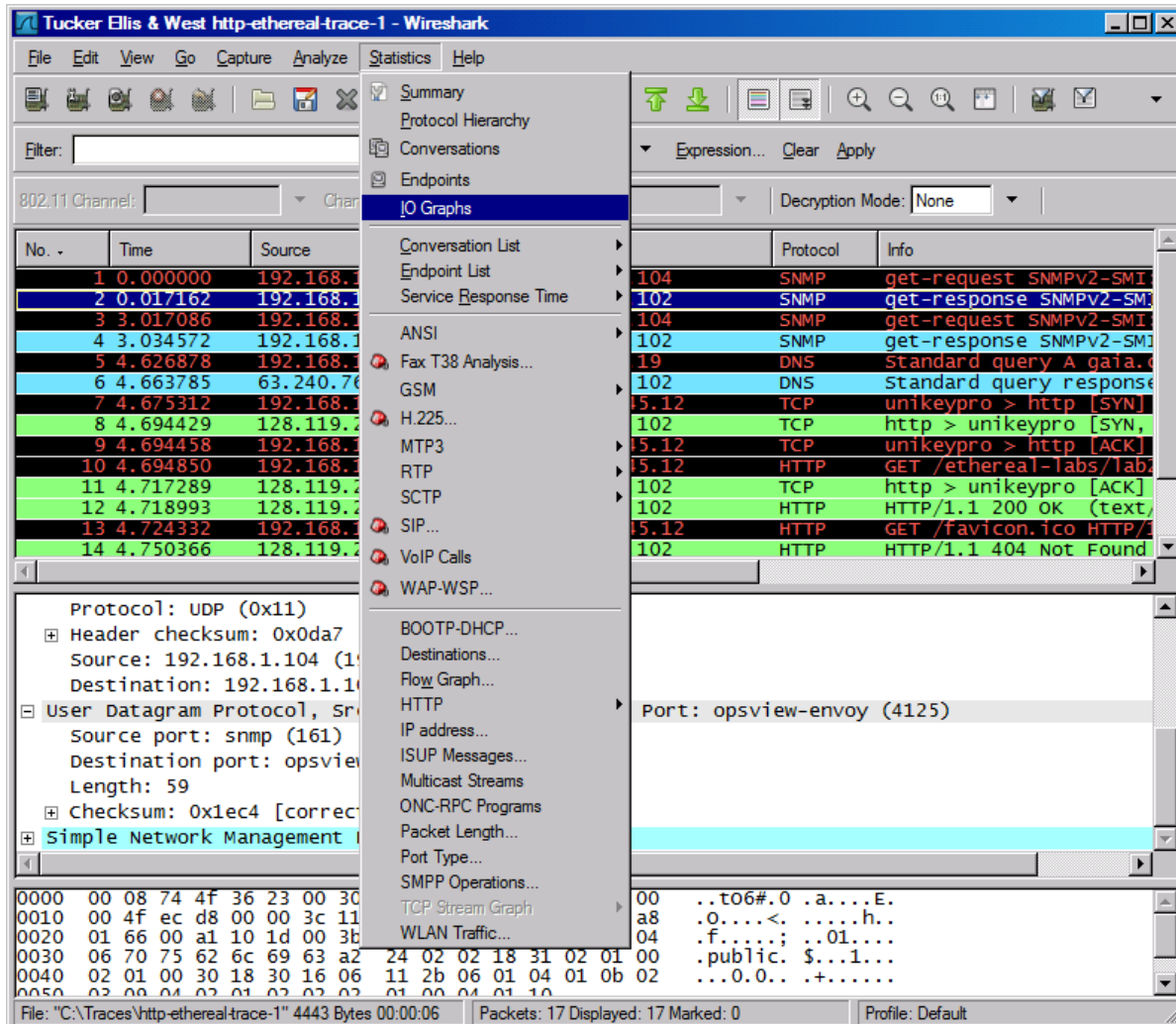
Conversations



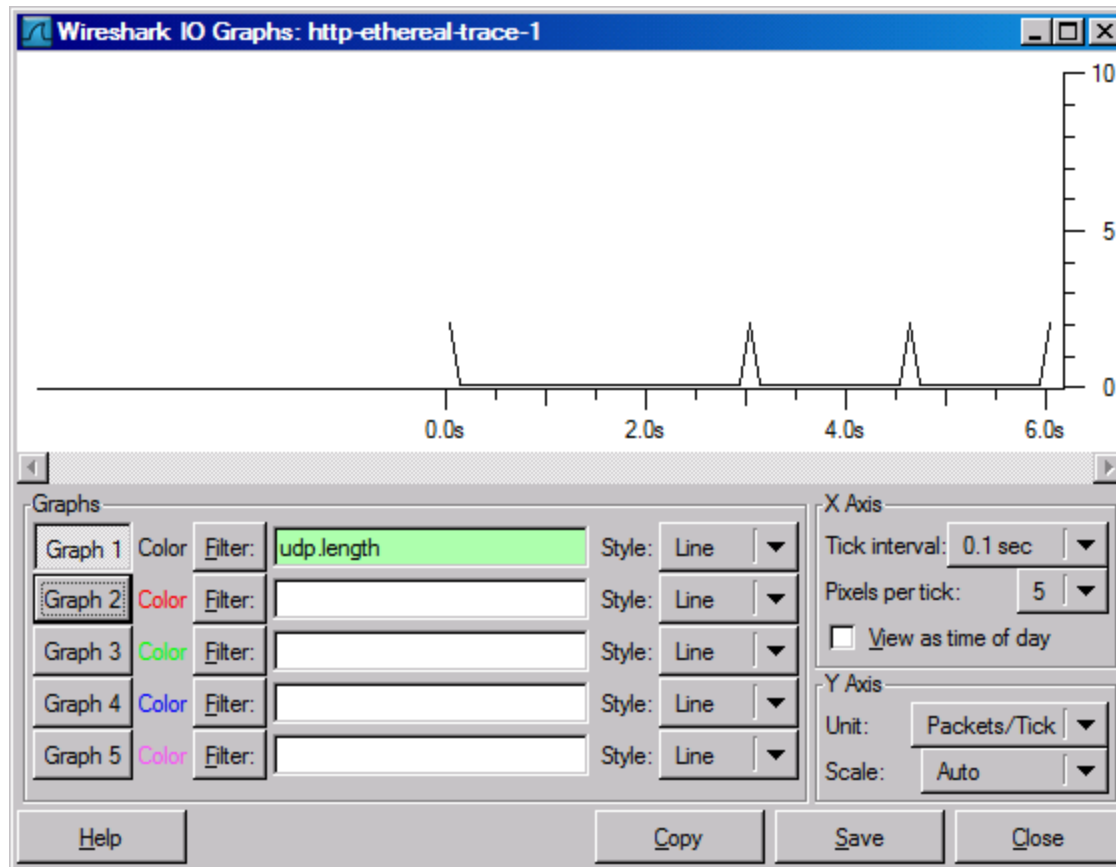
The image shows the 'Conversations' window in Wireshark, titled 'Conversations: http-ethereal-trace-1'. The 'IPv4: 3' tab is selected, showing a list of IPv4 conversations. The table has columns for Address A, Address B, Packets, Bytes, and direction-specific statistics. The data shows three distinct conversations: one between 63.240.76.19 and 192.168.1.102, another between 192.168.1.102 and 192.168.1.104, and a third between 128.119.245.12 and 192.168.1.102. 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

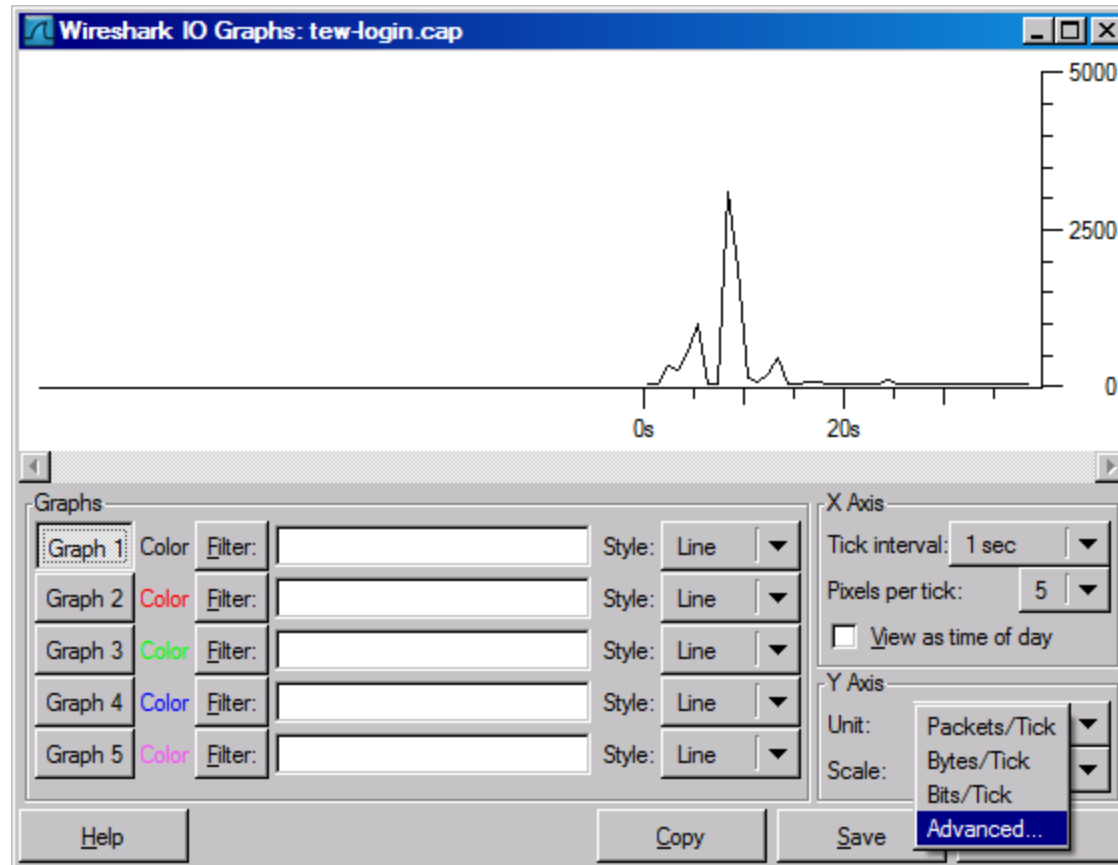
IOGraphs



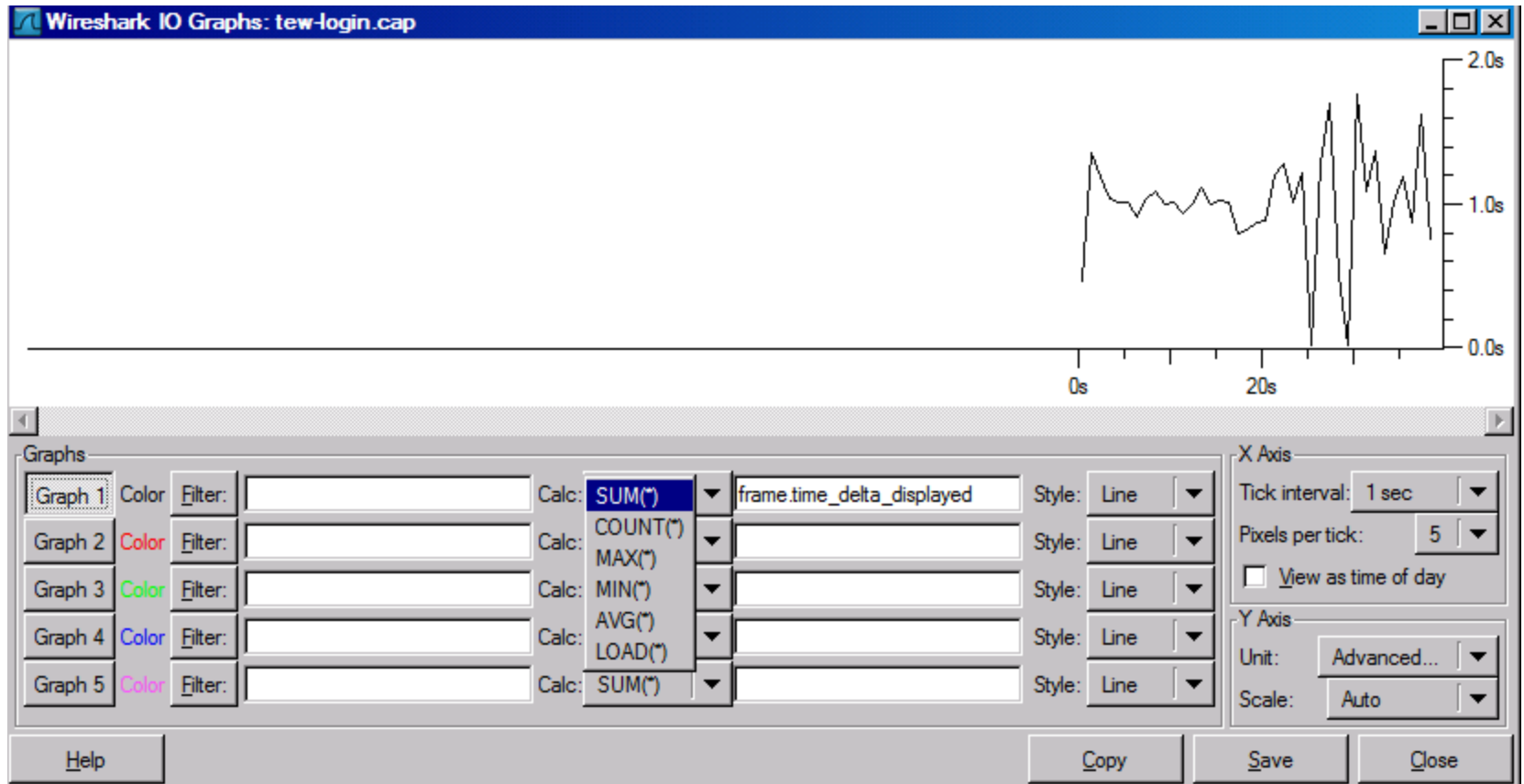
IOGraphs



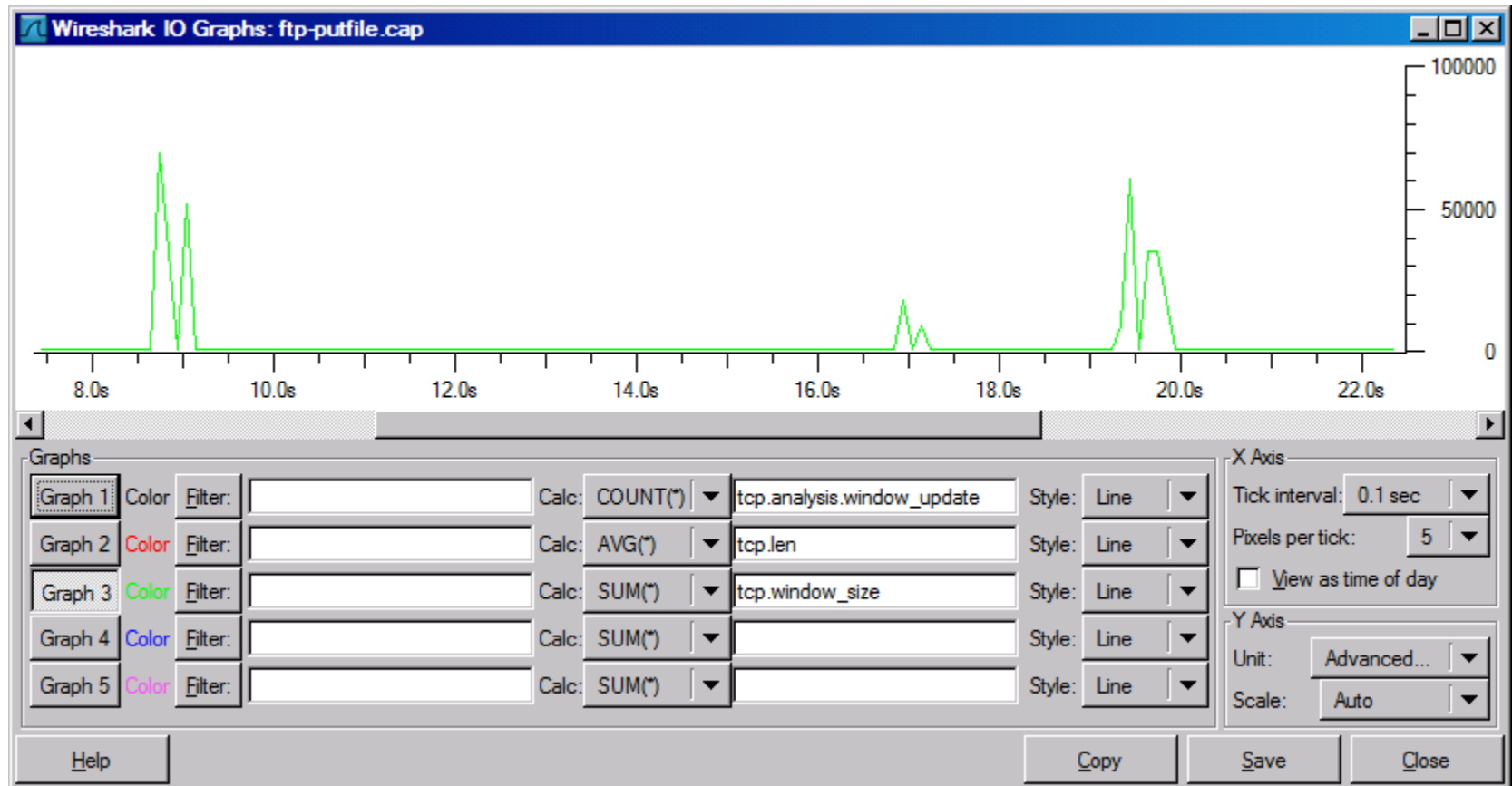
IOGraphs



IOGraphs



IOGraphs



Flow Graphs

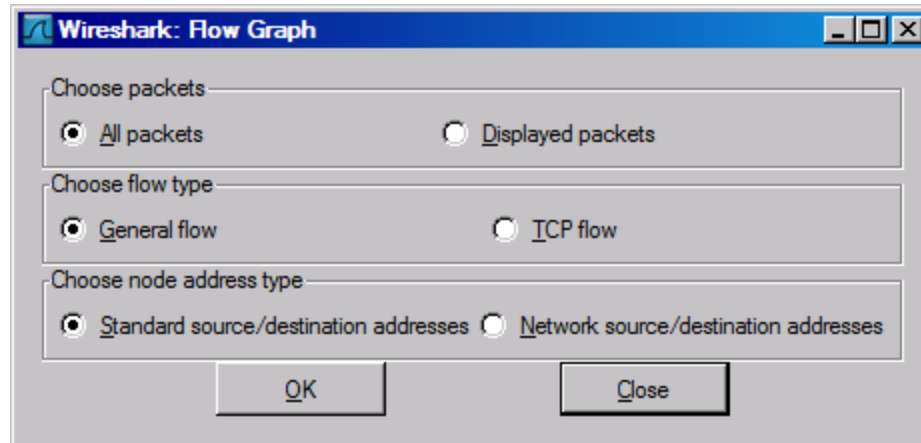
The image shows the Wireshark network protocol analyzer interface. The title bar reads "Tucker Ellis & West http-ethereal-trace-1 - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains icons for file operations, capture, and analysis. The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

- Filter:** A text field for applying filters to the packet list.
- 802.11 Channel:** A dropdown menu for selecting the channel.
- Packet List:** A table showing captured packets. The first 14 packets are listed, with columns for No., Time, and Source. The source IP addresses are 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102, 192.168.1.104, 192.168.1.102.
- Packet Details:** A pane showing the hierarchical structure of the selected packet (No. 14). It includes fields like Protocol (UDP), Header checksum, Source, Destination, User Datagram Protocol, Source port, Destination port, Length, Checksum, and Simple Network Management Protocol.
- Packet Bytes:** A pane showing the raw packet data in hexadecimal and ASCII.
- Statistics:** A pane showing various statistics, including Summary, Protocol Hierarchy, Conversations, Endpoints, and IO Graphs.
- Flow Graph:** A pane showing the flow graph of the selected packet, which is currently empty.

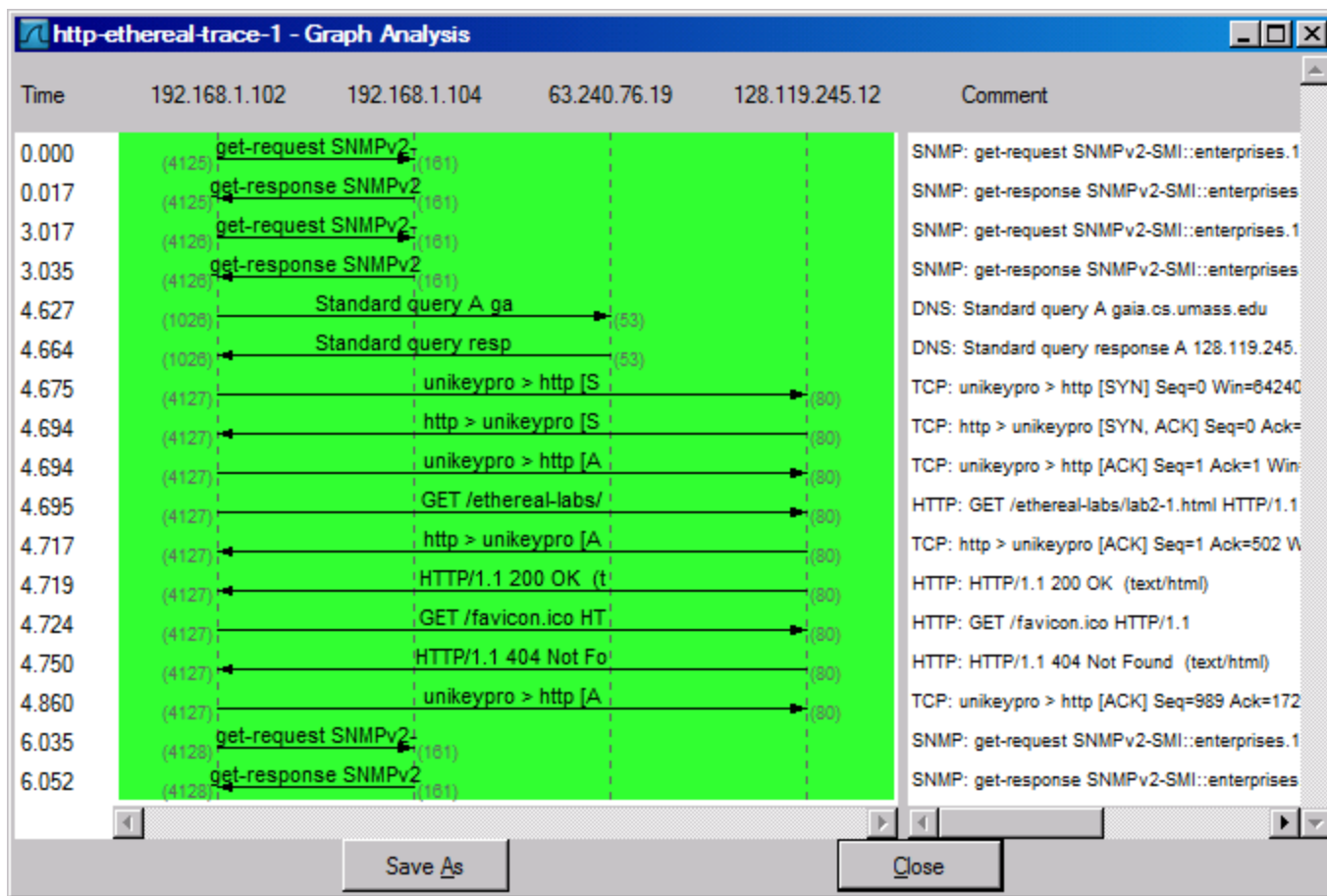
The context menu is open over the packet list, showing options like Summary, Protocol Hierarchy, Conversations, Endpoints, IO Graphs, Conversation List, Endpoint List, Service Response Time, ANSI, Fax T38 Analysis..., GSM, H.225..., MTP3, RTP, SCTP, SIP..., VoIP Calls, WAP-WSP..., BOOTP-DHCP..., Destinations..., Flow Graph..., HTTP, IP address..., ISUP Messages..., Multicast Streams, ONC-RPC Programs, Packet Length..., Port Type..., SMPP Operations..., TCP Stream Graph, and WLAN Traffic... The "Flow Graph..." option is highlighted.

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

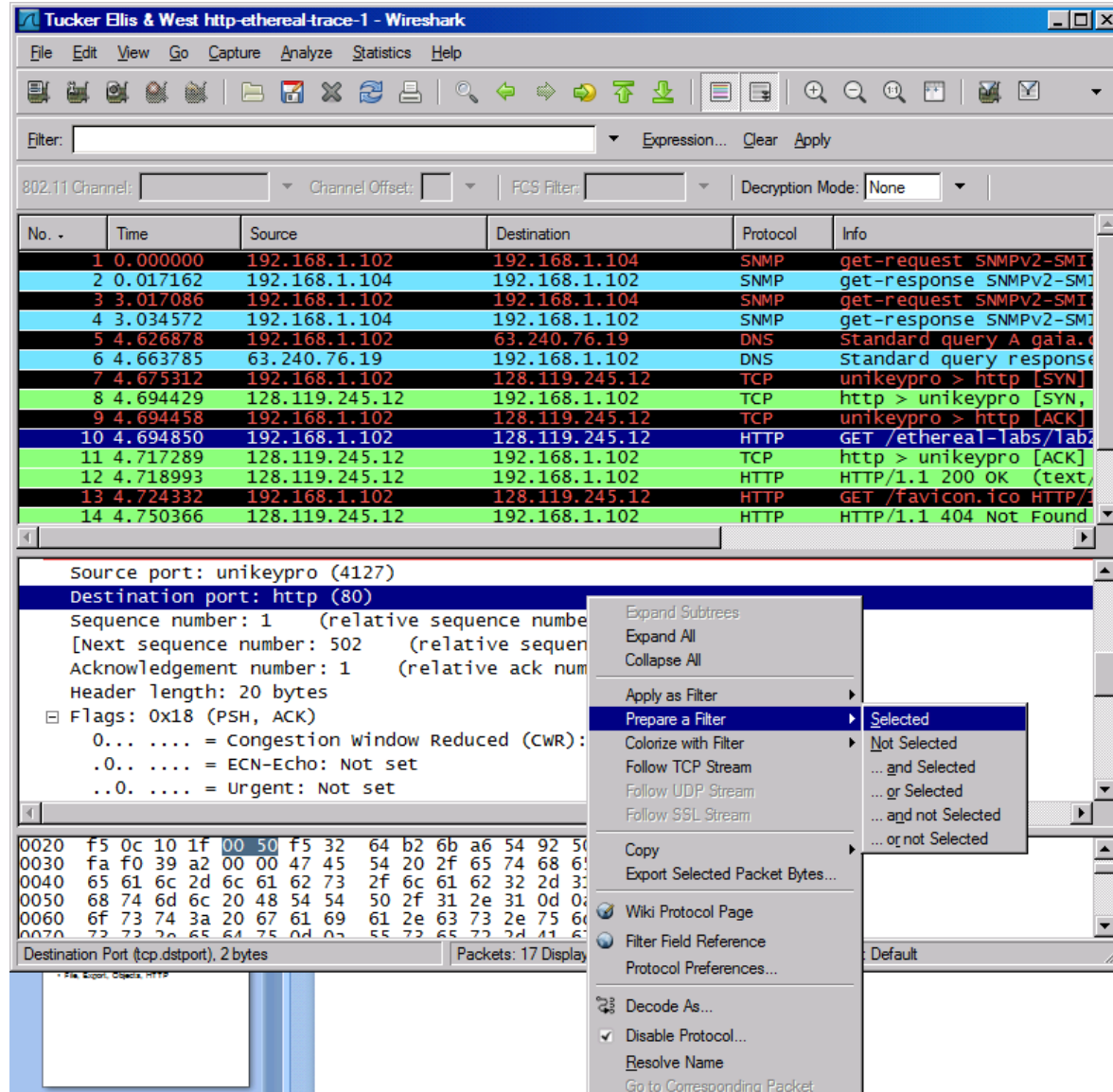
Flow Graphs



Flow Graphs



Right Click Filtering



Export HTTP

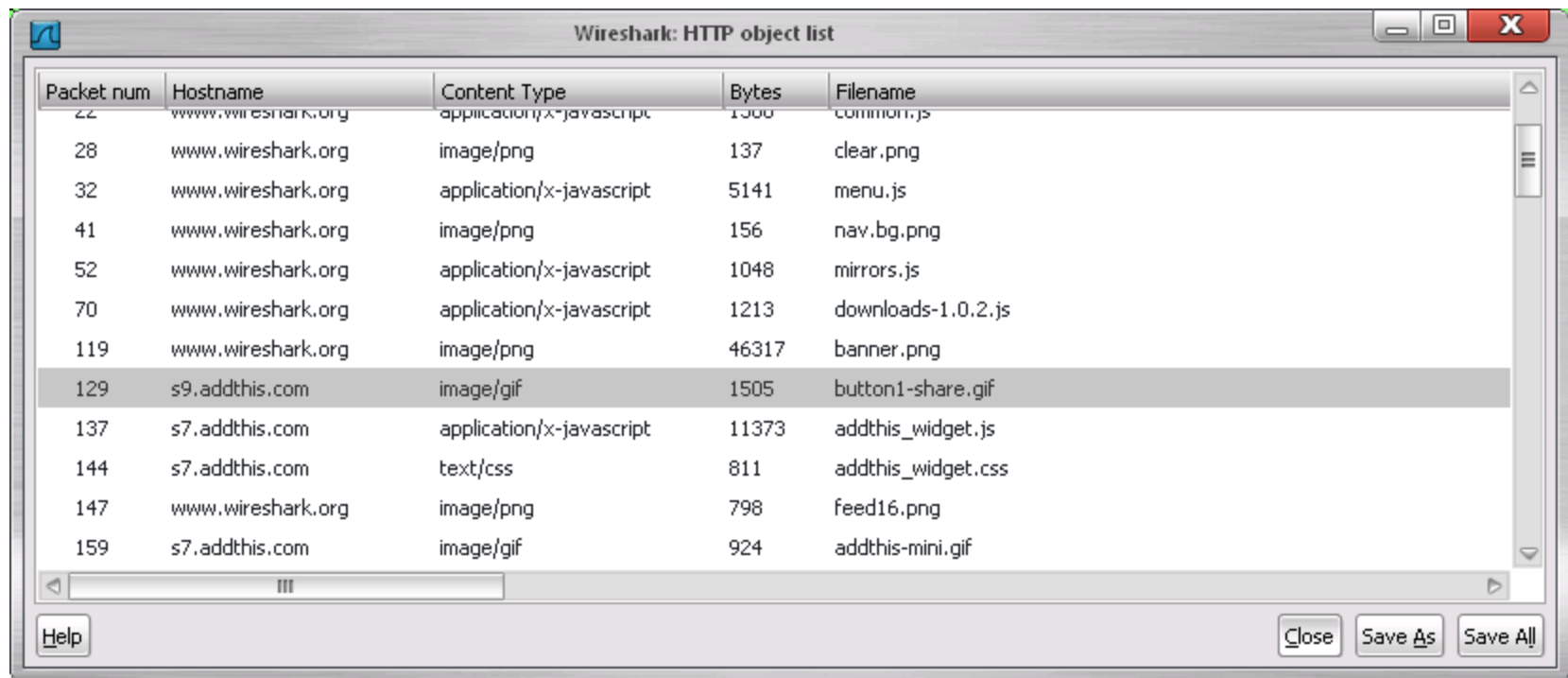
The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "Tucker Ellis & West http-ethereal-trace-1 - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, packet navigation, 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

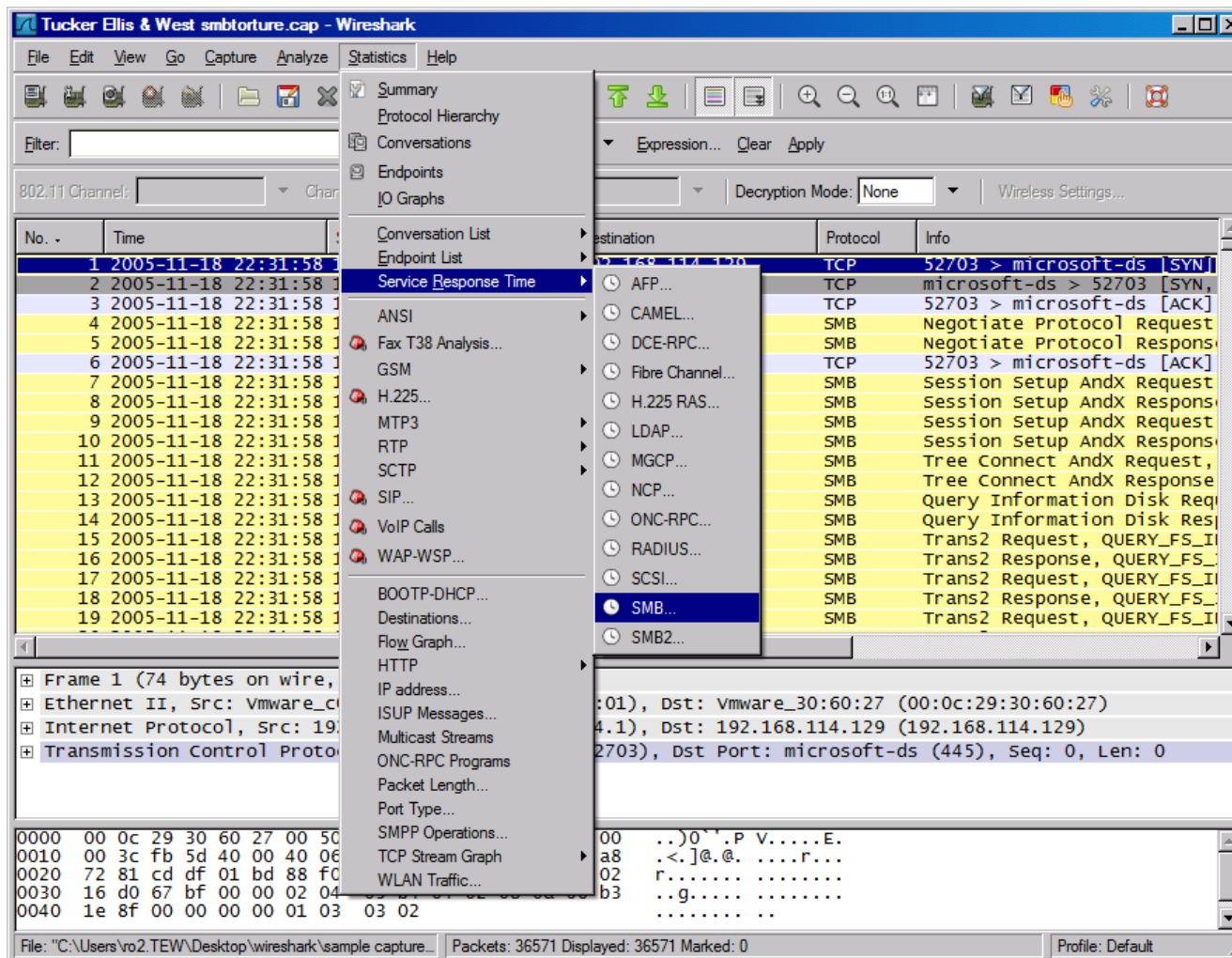
The packet bytes pane at the bottom shows the raw data of the selected packet, with the first few bytes highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
9	4.694458	192.168.1.102	128.119.245.12	TCP	60	unikeypro > http [SYN]
10	4.694850	192.168.1.102	128.119.245.12	HTTP	100	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	http > unikeypro [ACK]
12	4.718993	128.119.245.12	192.168.1.102	HTTP	100	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	100	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	100	HTTP/1.1 404 Not Found

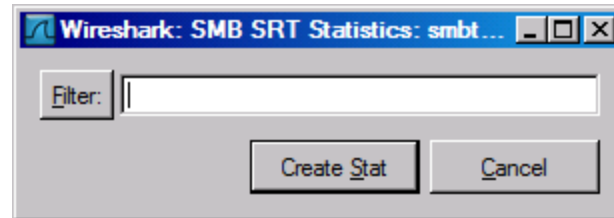
Export HTTP Objects



Service Response Time - SMB



Service Response Time - SMB



Service Response Time - SMB

SMB Service Response Time statistics: smbtorure.cap

SMB Service Response Time statistics

Filter:

SMB Commands

Index	Procedure	Calls ^	Min SRT	Max SRT	Avg SRT
113	Tree Disconnect	26	0.00019	0.02985	0.00235
19	Lock And Read	13	0.00026	0.21067	0.01892
7	Rename	12	0.00038	0.96396	0.08593
12	Lock Byte Range	11	0.00016	0.29542	0.04520
13	Unlock Byte Range	11	0.00016	0.00046	0.00028
116	Logoff AndX	11	0.00073	0.04617	0.00782
2	Open	10	0.00027	0.99055	0.09965
10	Read	9	0.00034	0.00121	0.00074
11	Write	9	0.00145	0.06665	0.02555

Transaction2 Sub-Commands

Index	Procedure	Calls ^	Min SRT	Max SRT	Avg SRT
2	FIND_NEXT2	240	0.00098	0.03823	0.00245
5	QUERY_PATH_INFO	200	0.00030	0.02970	0.00176
1	FIND_FIRST2	183	0.00087	0.04908	0.00330
7	QUERY_FILE_INFO	152	0.00030	0.04077	0.00187
8	SET_FILE_INFO	90	0.00019	0.26765	0.00548
6	SET_PATH_INFO	35	0.00031	0.02258	0.00167
3	QUERY_FS_INFO	23	0.00033	0.00450	0.00093
0	OPEN2	17	0.00026	1.00611	0.06069
13	CREATE_DIRECTORY	2	0.00218	0.00250	0.00234

NT Transaction Sub-Commands

Index	Procedure	Calls ^	Min SRT	Max SRT	Avg SRT
6	NT QUERY SECURITY DESC	58	0.00039	0.04631	0.00296
3	NT SET SECURITY DESC	44	0.00035	0.18661	0.00611
1	NT CREATE	21	0.00022	0.16868	0.00964
2	NT IOCTL	7	0.00041	0.05230	0.01348
4	NT NOTIFY	3	0.00326	0.00383	0.00354

Close

VOIP

Tucker Ellis & West aaa.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:

802.11 Channel: Char

No. Time

No.	Time
1	2005-07-04 05:32:20
2	2005-07-04 05:32:21
3	2005-07-04 05:32:22
4	2005-07-04 05:32:31
5	2005-07-04 05:32:31
6	2005-07-04 05:32:31
7	2005-07-04 05:32:32
8	2005-07-04 05:32:34
9	2005-07-04 05:32:34
10	2005-07-04 05:32:35
11	2005-07-04 05:32:36
12	2005-07-04 05:32:38
13	2005-07-04 05:32:39
14	2005-07-04 05:32:39
15	2005-07-04 05:32:40
16	2005-07-04 05:32:44
17	2005-07-04 05:32:52
18	2005-07-04 05:32:52
19	2005-07-04 05:32:52

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...

Destination Protocol Info

Destination	Protocol	Info
192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
Broadcast	ARP	who has 192.168.1.1? Tell
Silicom_01:6e:bd	ARP	192.168.1.1 is at 00:30:54
192.168.1.1	DNS	Standard query A sip.cyber
192.168.1.1	DNS	Standard query A sip.cyber
192.168.1.2	DNS	Standard query response A
192.168.1.1	DNS	Standard query SRV _sip._u
192.168.1.1	DNS	Standard query SRV _sip._u
192.168.1.1	DNS	Standard query SRV _sip._u
Silicom_01:6e:bd	ARP	who has 192.168.1.2? Tell
astlene_00:34:56	ARP	192.168.1.2 is at 00:e0:ed
192.168.1.1	DNS	Standard query SRV _sip._u
192.168.1.1	DNS	Standard query SRV _sip._u
192.168.1.1	DNS	Standard query PTR 1.0.0.1
192.168.1.2	DNS	Standard query response PT
192.242.33.35	SIP	Request: REGISTER sip:sip.

Frame 1 (92 bytes on wire, 120 bytes captured on interface 0) on interface 0
Ethernet II, Src: Silicom_01:6e:bd, Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.1, Dst: 192.168.1.255
User Datagram Protocol, Src Port: 5060, Dst Port: netbios-ns (137)
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

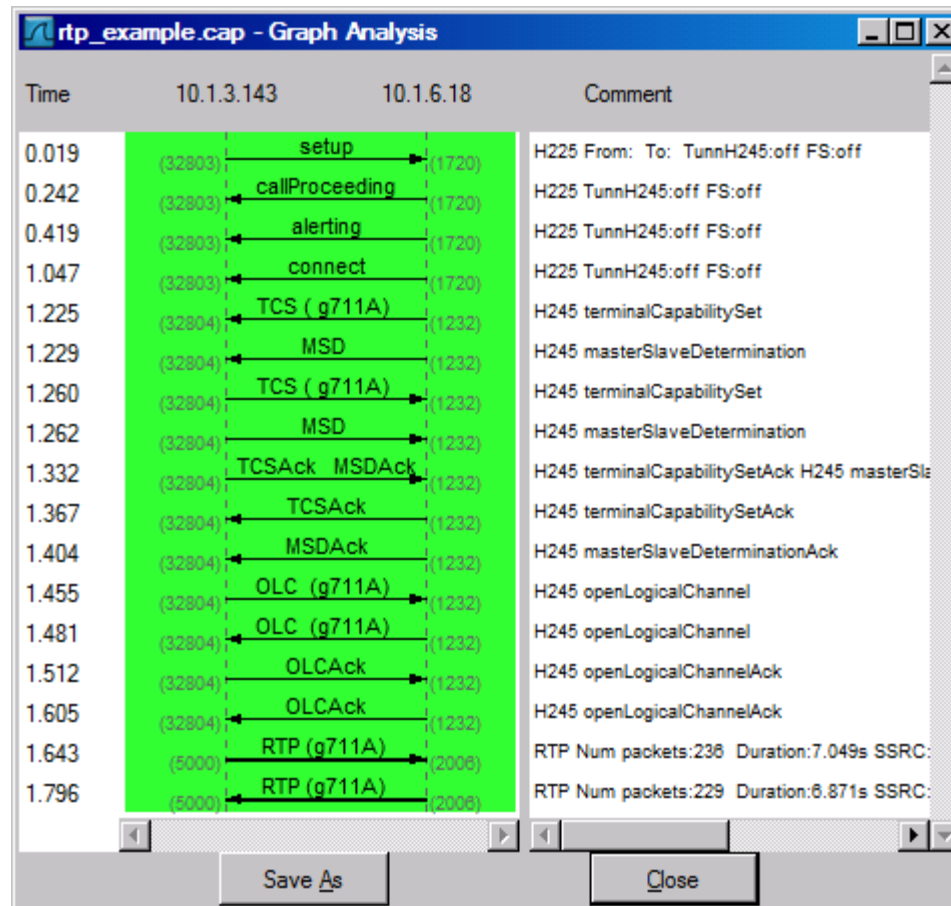
Detected 1 VoIP Call. Selected 1 Call.

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

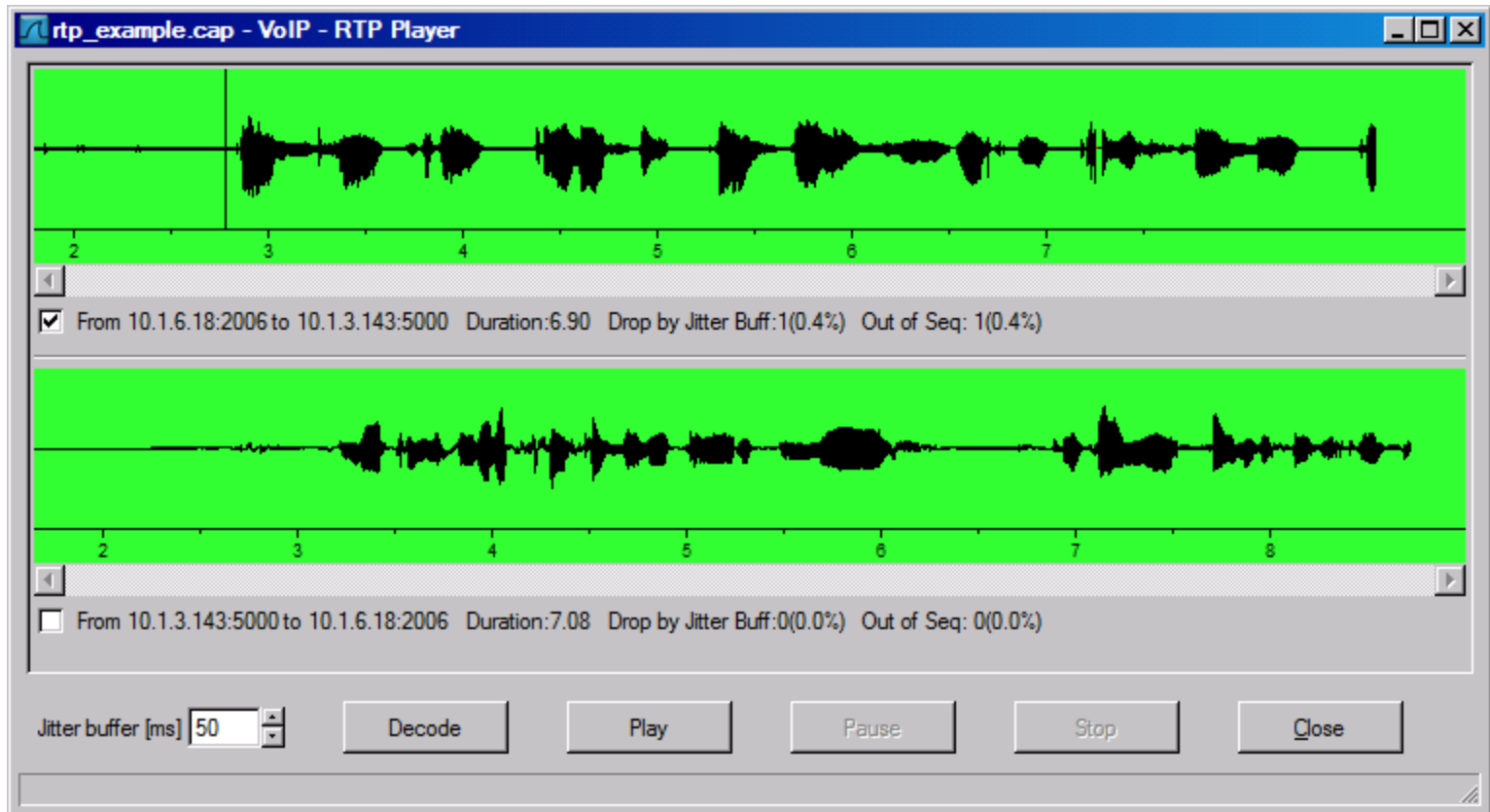
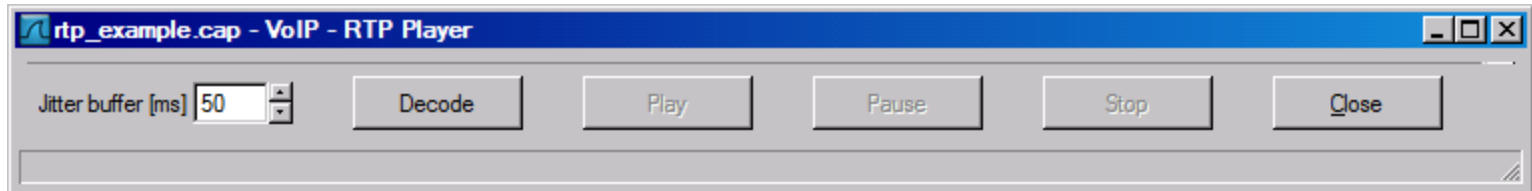
Total: Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 0

Prepare Filter Graph Player Select All Close

VOIP Call Graph



VOIP RTP Player



SIP Analysis

The screenshot shows the Wireshark interface with the 'Statistics' menu open. The 'SIP...' option is highlighted. The packet list on the right shows a sequence of network traffic including NBNS, ARP, DNS, and SIP messages.

Statistics 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...
- SMPP Operations...
- TCP Stream Graph
- WLAN Traffic...

Packet List:

No.	Time	Destination	Protocol	Info
1	2005-07-04 05:32:20	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
2	2005-07-04 05:32:21	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
3	2005-07-04 05:32:22	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1
4	2005-07-04 05:32:31	Broadcast	ARP	who has 192.168.1.1? Tell
5	2005-07-04 05:32:31	silicom_01:6e:bd	ARP	192.168.1.1 is at 00:30:54
6	2005-07-04 05:32:31	192.168.1.1	DNS	Standard query A sip.cyber
7	2005-07-04 05:32:32	192.168.1.1	DNS	Standard query A sip.cyber
8	2005-07-04 05:32:34	192.168.1.1	DNS	Standard query A sip.cyber
9	2005-07-04 05:32:34	192.168.1.2	DNS	Standard query response A
10	2005-07-04 05:32:35	192.168.1.1	DNS	Standard query SRV _sip._u
11	2005-07-04 05:32:36	192.168.1.1	DNS	Standard query SRV _sip._u
12	2005-07-04 05:32:38	192.168.1.1	DNS	Standard query SRV _sip._u
13	2005-07-04 05:32:39	silicom_01:6e:bd	ARP	who has 192.168.1.2? Tell
14	2005-07-04 05:32:39	astlene_00:34:56	ARP	192.168.1.2 is at 00:e0:ed
15	2005-07-04 05:32:40	192.168.1.1	DNS	Standard query SRV _sip._u
16	2005-07-04 05:32:44	192.168.1.1	DNS	Standard query SRV _sip._u
17	2005-07-04 05:32:52	192.168.1.1	DNS	Standard query PTR 1.0.0.1
18	2005-07-04 05:32:52	192.168.1.2	DNS	Standard query response PTR
19	2005-07-04 05:32:52	192.242.33.35	SIP	Request: REGISTER sip:sip.

Packet Details:

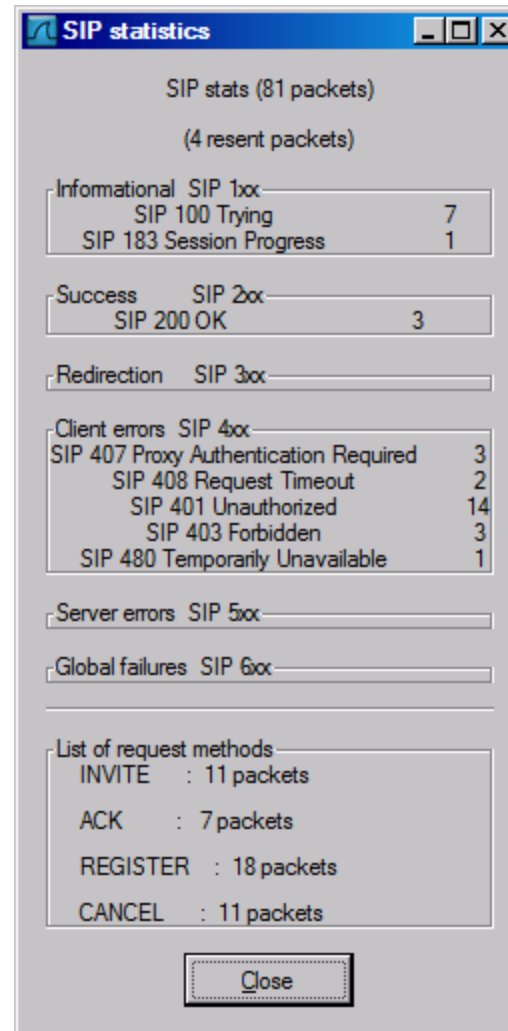
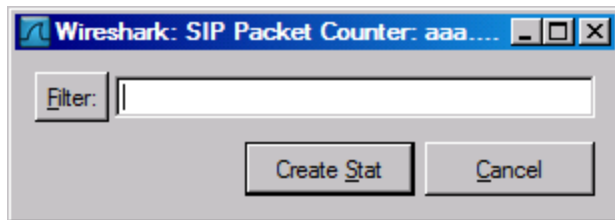
- Frame 1 (92 bytes on wire)
- Ethernet II, Src: silicom_01:6e:bd, Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol, Src: 192.168.1.1, Dst: 192.168.1.255
- User Datagram Protocol, Src Port: 54321, Dst Port: netbios-ns (137)

Packet Bytes:

```
0000 ff ff ff ff ff ff 00 e0 00 00 00 00 00 00 00 00
0010 00 4e 69 8c 00 00 80 11 00 00 00 00 00 00 00 00
0020 01 ff 00 89 00 89 00 3a 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 20 45 4a 45 4f 43 41 43 41 43
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43
0050 41 43 41 43 41 43 4d 00 00 20 00 01 00 00 00 00
```

File: "C:\Users\vo2.TEW\Desktop\wireshark\sample capture..." Packets: 691 Displayed: 691 Marked: 0 Profile: Default

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) with details for Ethernet II, Internet Protocol, and Hypertext Transfer Protocol. 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_scri
4	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP ti
5	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP ti
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 ti
9	2008-07-24 13:12:59.2	10.1.15.104	HTTP	Continuation or non-HTTP ti
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 ti
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-calyppoicf > http [SYN
16	2008-07-24 13:12:59.1	10.1.12.67	HTTP	Continuation or non-HTTP ti
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):

- Ethernet II, Src: Cisco_f7...
- Internet Protocol, Src: 10.1.15.104, Dst: 10.1.15.104
- Hypertext Transfer Protocol, Method: GET, URI: /customer/advance/9/.o...

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...

Packet Bytes:

0000 00 15 c7 46 80 00 00 03 c8 b8 0f 8e cb b4 85 4d

0010 05 dc 36 ab 40 00 3b 06 51 00 76 33 2f 0f 00 04

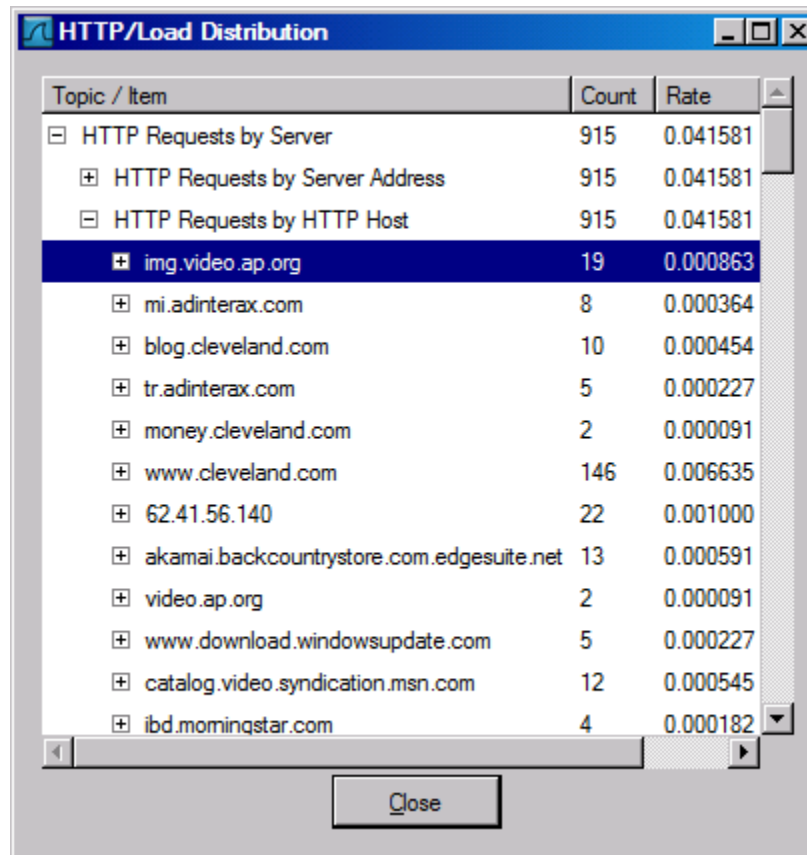
0020 0f 68 00 50 0a f0 94 cf

0030 1b 96 ab f0 00 00 46 1f


0040 9a b1 fd cf c7 ff fd ca

0050 23 c8 05 00 26 86 fb 25

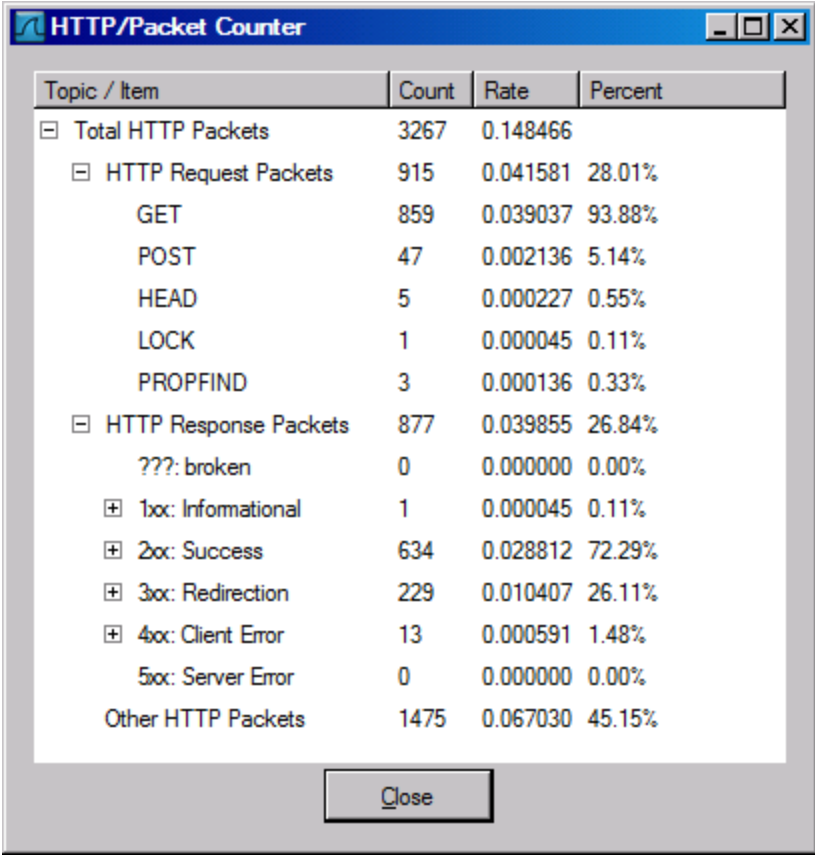
HTTP Analysis – Load Distribution



The screenshot shows a window titled "HTTP/Load Distribution" with a table of HTTP request data. The table has three columns: "Topic / Item", "Count", and "Rate". The data is organized hierarchically, starting with "HTTP Requests by Server" (915 requests, 0.041581 rate), which is expanded to show "HTTP Requests by Server Address" and "HTTP Requests by HTTP Host". The "HTTP Requests by HTTP Host" section is further expanded, showing a list of hosts with their respective counts and rates. The host "img.video.ap.org" is highlighted in blue, indicating it is the selected item. Other hosts include "mi.adinterax.com", "blog.cleveland.com", "tr.adinterax.com", "money.cleveland.com", "www.cleveland.com", "62.41.56.140", "akamai.backcountrystore.com.edgesuite.net", "video.ap.org", "www.download.windowsupdate.com", "catalog.video.syndication.msn.com", and "ibd.morningstar.com". A "Close" button is located at the bottom of the window.

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

HTTP Analysis – Packet Counter

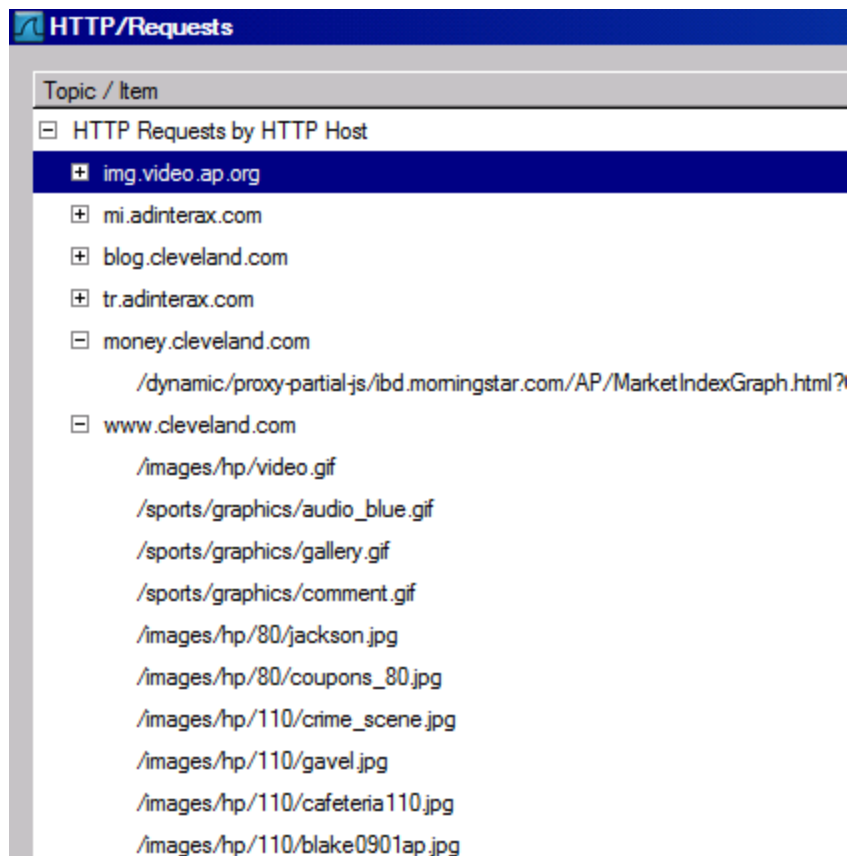


The screenshot shows a window titled "HTTP/Packet Counter" with a table of statistics. The table has four columns: "Topic / Item", "Count", "Rate", and "Percent". The data is organized hierarchically, starting with "Total HTTP Packets", followed by "HTTP Request Packets" (with sub-items for GET, POST, HEAD, LOCK, and PROPFIND), then "HTTP Response Packets" (with sub-items for status codes: 1xx, 2xx, 3xx, 4xx, 5xx, and 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



TroubleShooting TCP

- Latency
- Loss
- Jitter
- Jabber
- Small Packets

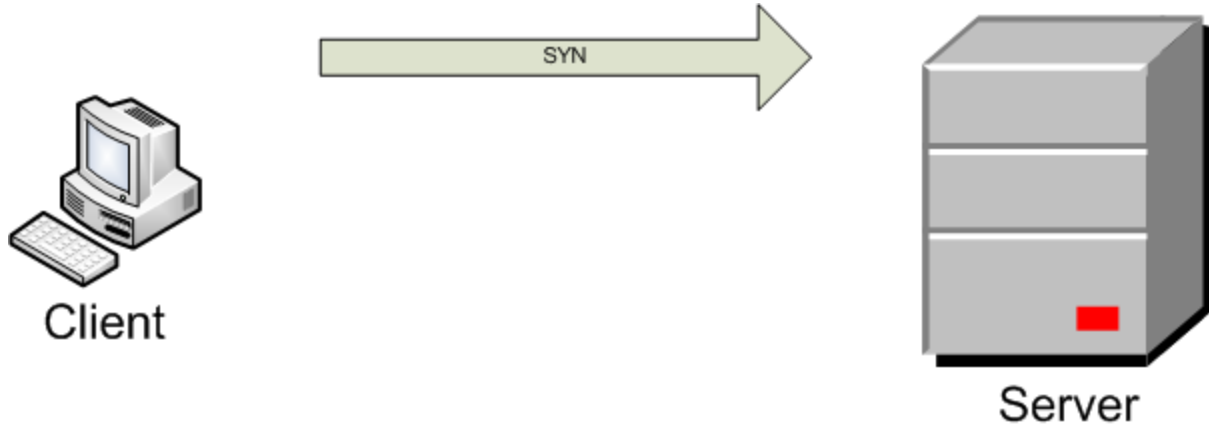
Latency

The time it takes for a packet to travel from point a to point b

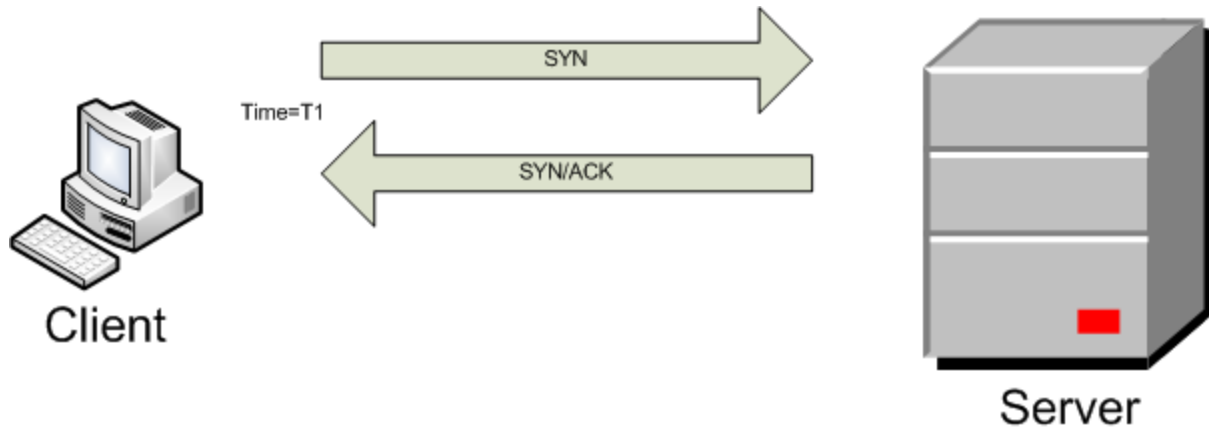
Latency is often the cause of “slow” networks



Troubleshooting TCP Latency



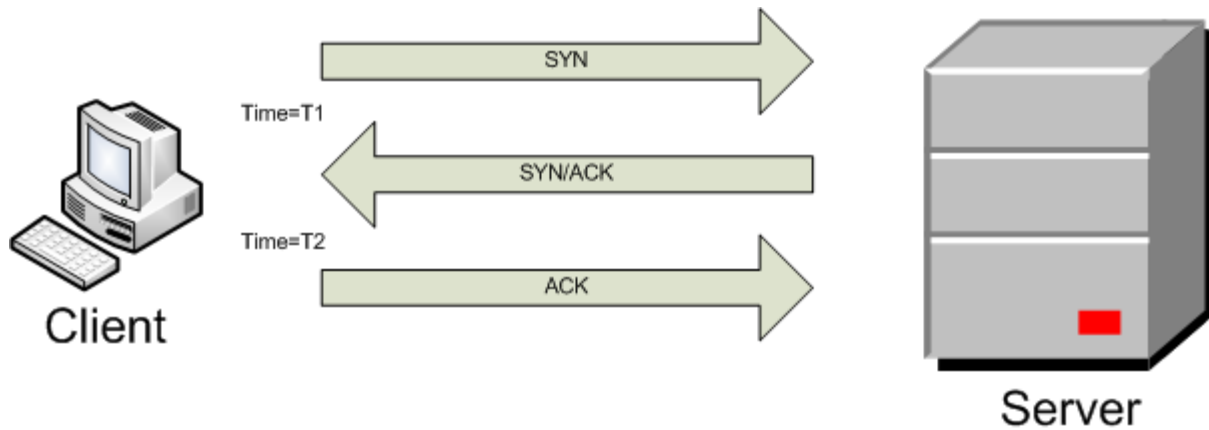
T1



T1 is the time it took from the moment the syn was sent until the client received the syn/ack

This time is due to the wire latency + processing time of the IP stack on the server

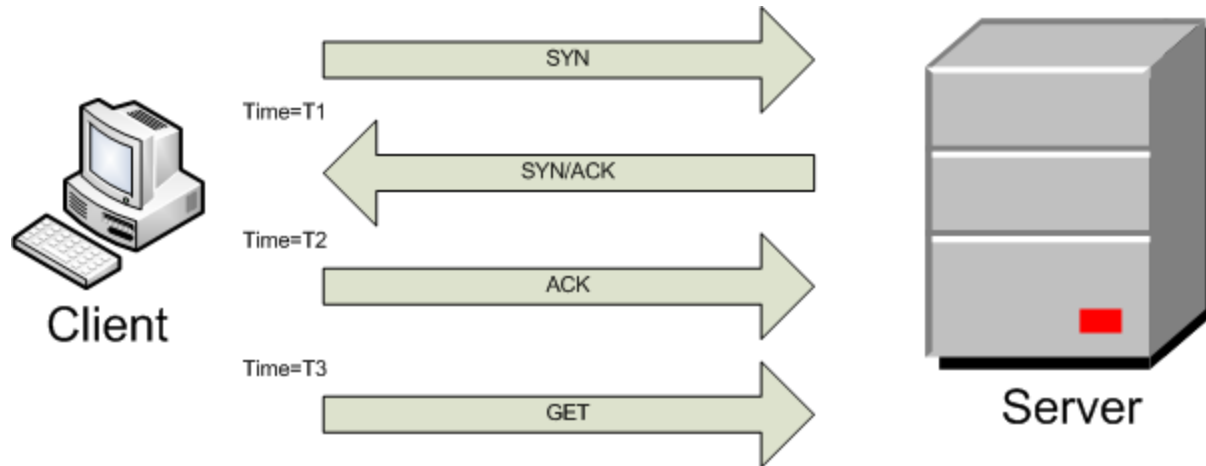
T2



T2 is the time it took from receiving the SYN/ACK until the ACK is sent.

This time is the processing time of the IP stack on the client

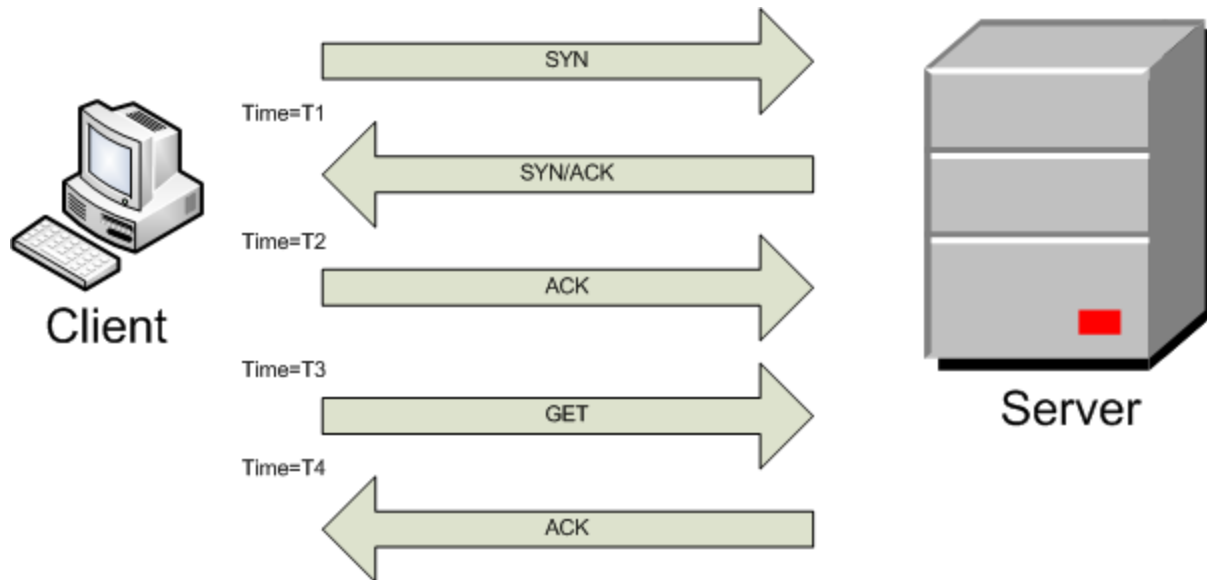
T3



T3 is the time it took from sending the ACK until the clients sends a GET.

This time is the processing time of the application on the client

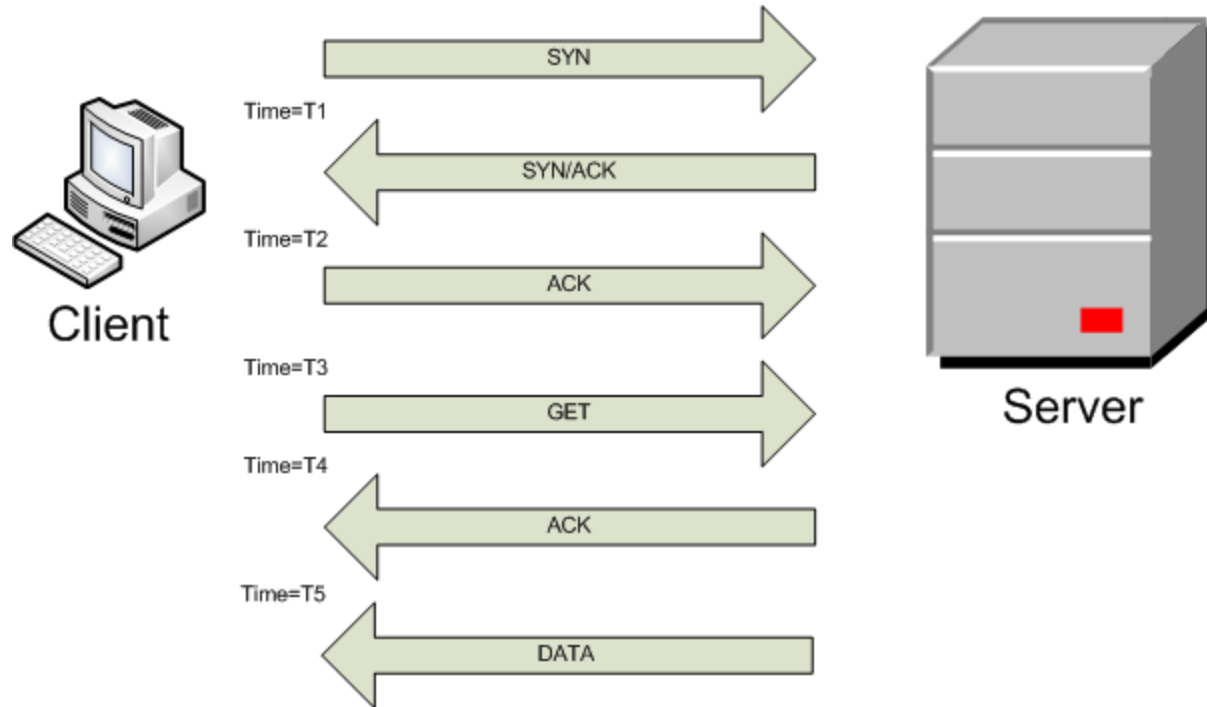
T4



T4 is the time it took from sending GET until an ACK is received at the client.

This time is due to wire latency.

T5



T5 is the time it took from getting the ACK until data is received at the client.

This time is due the server application.

TIPS

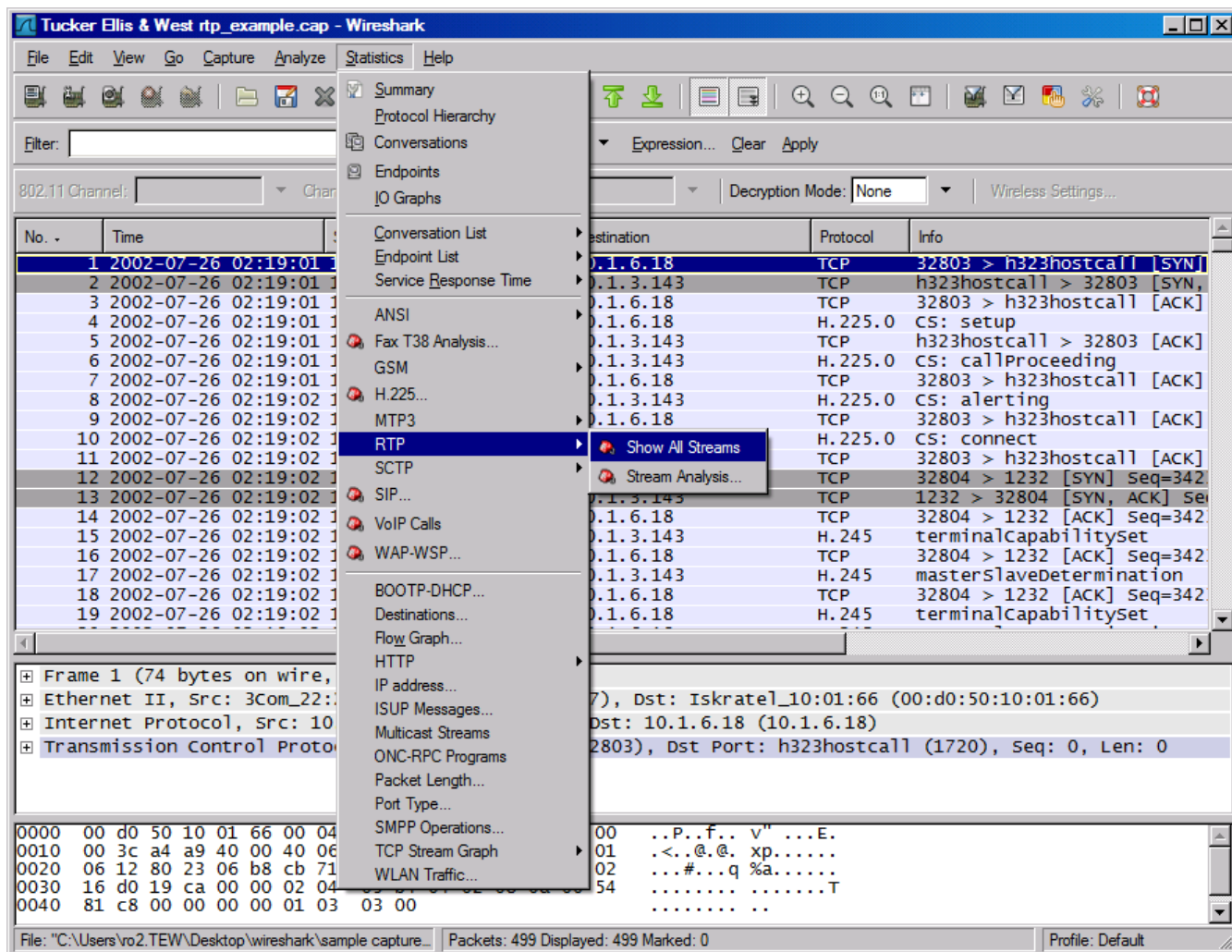
- Time #1 & #4 should be small on a LAN application. If not, check your network path, nic settings and throughput.
- Time #2 is the client ip stack. Should be minimal. If not, check the driver.
- Time #3 is the client application. This time will undoubtedly vary greatly between packets. Talk to your developers if you see an issue here.
- Time #5 is the server application. This time will also vary greatly, but generally if #5 is huge and #4 is really, really small look at delays caused by the server application. Start troubleshooting on the server by looking at CPU, bandwidth, memory and disk IO.

Jitter

Jitter is an unwanted variation of one or more characteristics of a periodic signal in electronics and telecommunications. Jitter may be seen in characteristics such as the interval between successive pulses, or the amplitude, frequency, or phase of successive cycles.

Source: [Wikipedia.com](https://en.wikipedia.org/wiki/Jitter)

Jitter



Jitter

Wireshark: RTP Streams

Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)
10.1.3.143	5000	10.1.6.18	2006	0xDEE0EE8F	ITU-T G.711 PCMA	236	0 (0.0%)	34.83
10.1.6.18	2006	10.1.3.143	5000	0xF3CB2001	ITU-T G.711 PCMA	229	1 (0.4%)	86.12

Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

Wireshark: RTP Streams

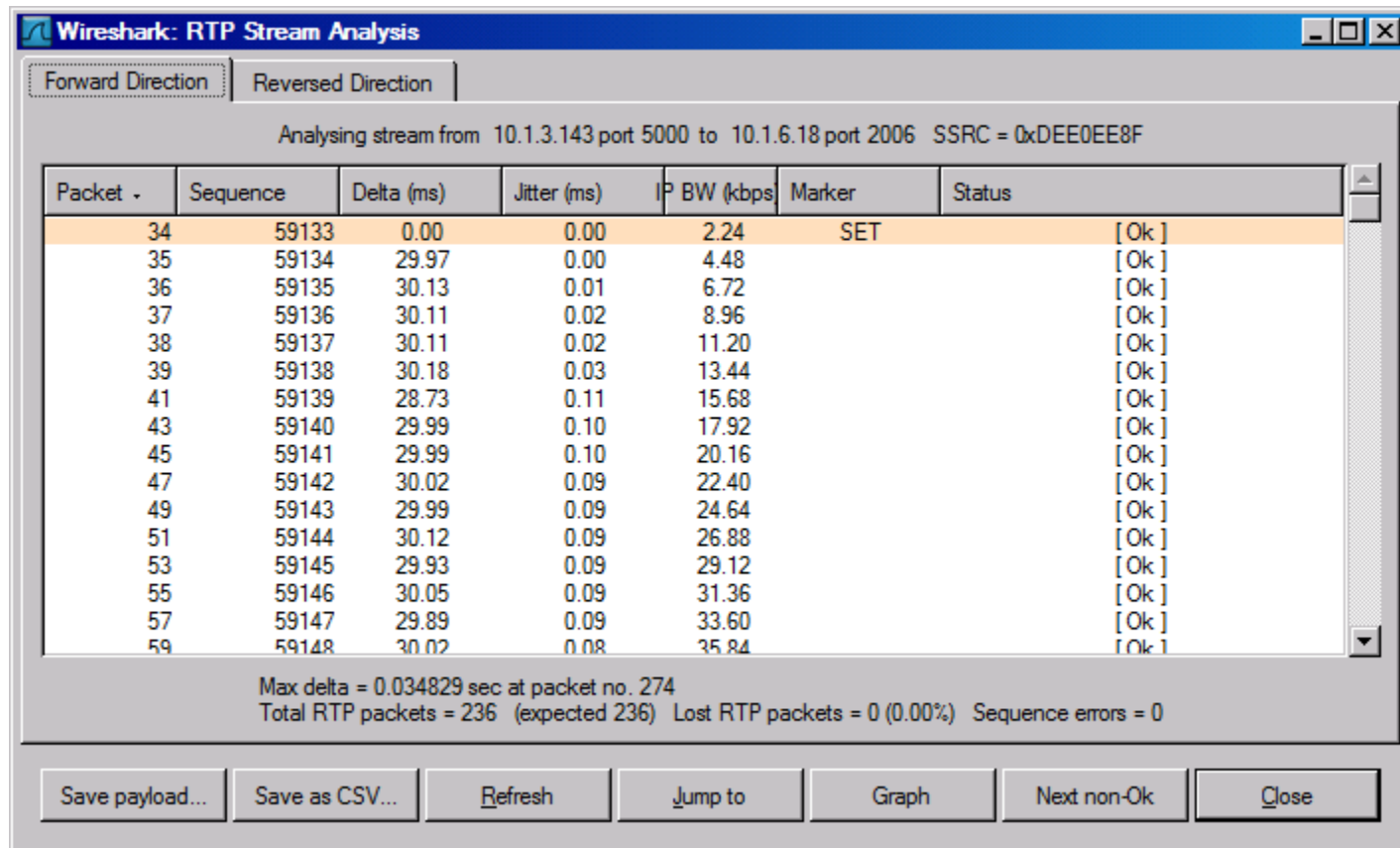
Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
	2006	0xDEE0EE8F	ITU-T G.711 PCMA	236	0 (0.0%)	34.83	0.83	0.37	
	5000	0xF3CB2001	ITU-T G.711 PCMA	229	1 (0.4%)	86.12	7.34	2.84	X

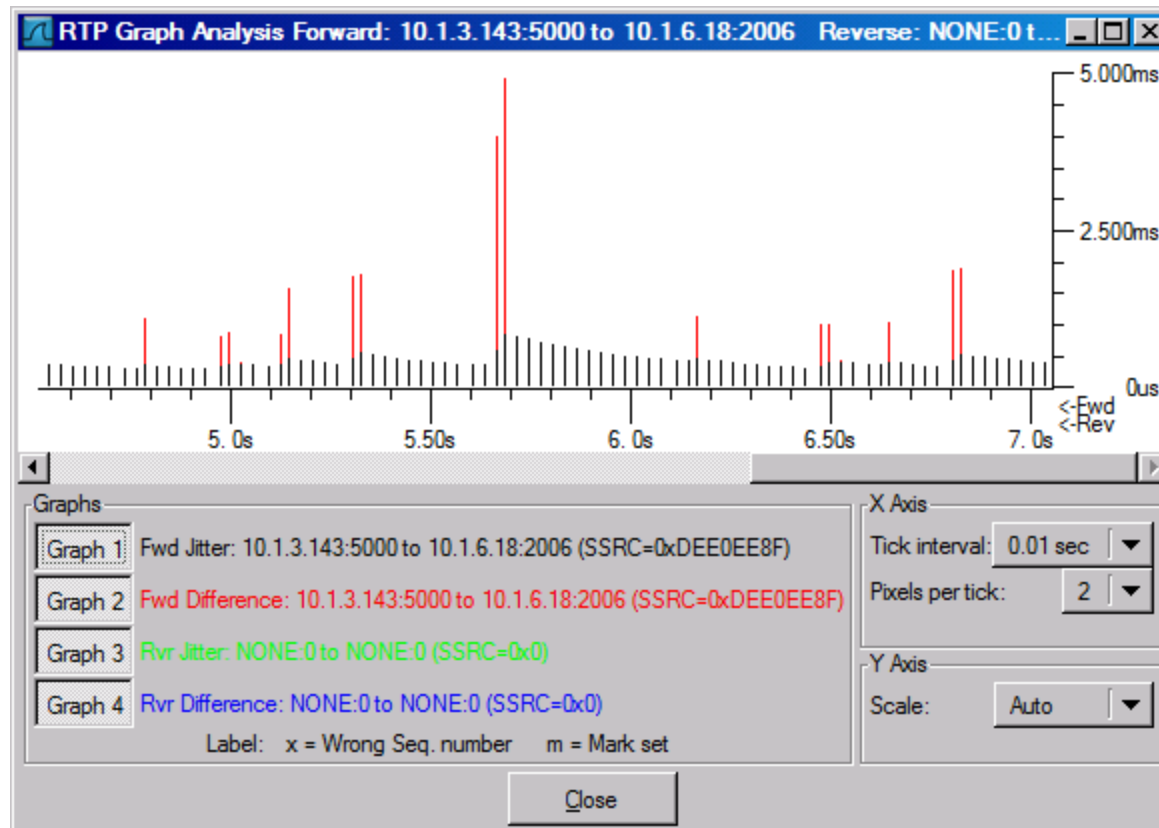
Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

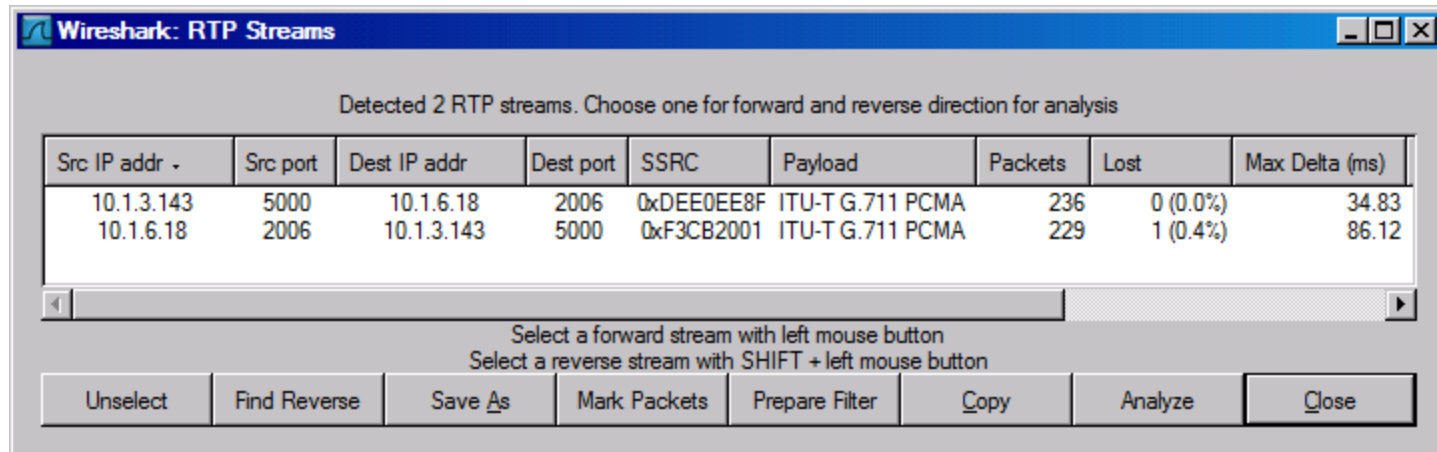
Jitter



Jitter



LOSS



Jabber

Jabber occurs when there are excessively long packets from a network device.

Packet Length

The image shows a Wireshark packet capture analysis window. The title bar reads "Tucker Ellis & West tew-cle-dc001-june423008-cap1.cap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, capture, and analysis. The left pane shows a list of packets with columns for No., Time, and a checkbox. Packet 184 is selected. The middle pane shows a tree view of the packet structure, with "Service Advertisement Protocol" expanded, showing "General Response" and "Server Name: TEW-SNAPNW". The right pane shows a table of packet details, including destination, protocol, and info. The "Packet Length..." option is highlighted in the menu.

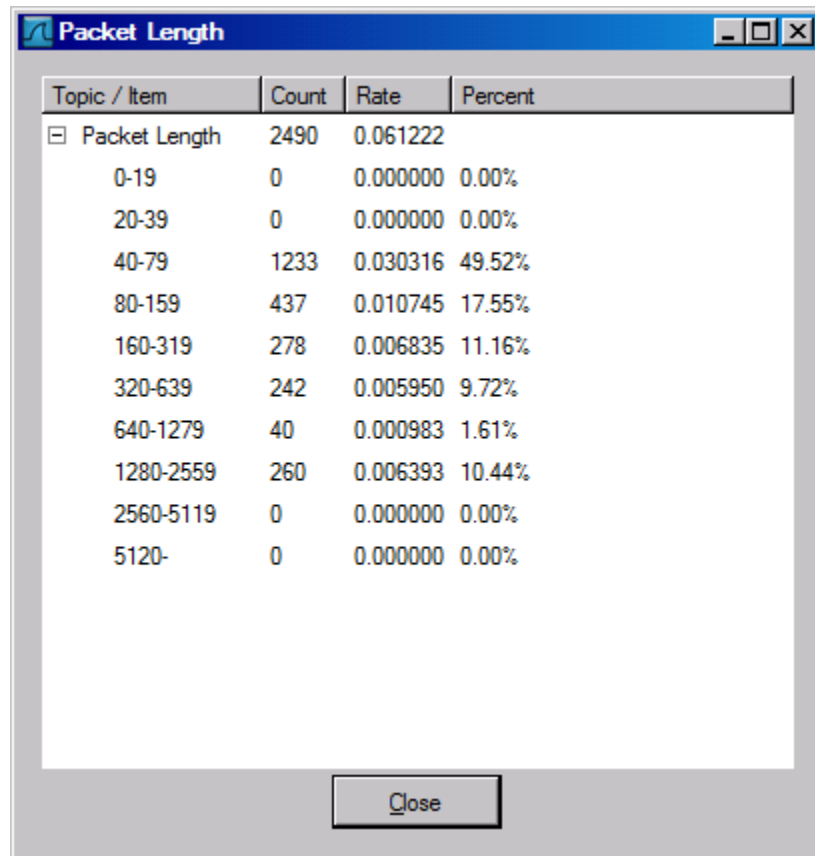
No.	Time	Destination	Protocol	Info
181	2008-06-04 16:38:49.1	0.1.11.21	DNS	Standard query A b1.ac-ima
182	2008-06-04 16:38:49.1	0.1.11.13	DNS	Standard query A a203.da2.
183	2008-06-04 16:38:49.1	0.1.11.21	DNS	Standard query A i247.phot
184	2008-06-04 16:38:49.1	0010111.ffffffffffff	IPX SAP	General Response
185	2008-06-04 16:38:49.1	0010111.ffffffffffff	IPX RIP	Response
186	2008-06-04 16:38:49.1	0.1.11.13	DNS	Standard query A i247.phot
187	2008-06-04 16:38:49.1	0.1.11.21	DNS	Standard query response A
188	2008-06-04 16:38:49.1	0.6.12.102	DNS	Standard query response A
189	2008-06-04 16:38:49.1	0.1.11.219	TCP	blackjack > 4392 [ACK] seq
190	2008-06-04 16:38:49.1	0.1.11.207	TCP	blackjack > skip-mc-gikreq
191	2008-06-04 16:38:49.1	0.1.11.21	TCP	4392 > blackjack [ACK] seq
192	2008-06-04 16:38:49.1	0.1.11.21	TCP	skip-mc-gikreq > blackjack
193	2008-06-04 16:38:49.1	0.1.11.21	DNS	Standard query response A
194	2008-06-04 16:38:49.1	0.6.12.102	DNS	Standard query response CN
195	2008-06-04 16:38:50.1	0.1.11.21	DNS	Standard query response CN
196	2008-06-04 16:38:50.1	0.6.12.102	DNS	Standard query response CN
197	2008-06-04 16:38:50.1	0.1.11.21	DNS	Standard query A i273.phot
198	2008-06-04 16:38:50.1	0.1.11.13	DNS	Standard query A i273.phot
199	2008-06-04 16:38:50.1	0.1.11.21	DNS	Standard query A i208.phot

Text item 0, 48 bytes

Packets: 2490 Displayed: 2490 Marked: 0

Profile: Default

Packet Length



The screenshot shows a window titled "Packet Length" with a table of statistics. The table has four columns: "Topic / Item", "Count", "Rate", and "Percent". The data is organized into a tree structure where "Packet Length" is the root, and various length ranges are its children. The "Rate" column for the root is 0.061222. The "Percent" column for the root is not explicitly shown, but the values for the children sum up to 100%.

Topic / Item	Count	Rate	Percent
[-] Packet Length	2490	0.061222	
0-19	0	0.000000	0.00%
20-39	0	0.000000	0.00%
40-79	1233	0.030316	49.52%
80-159	437	0.010745	17.55%
160-319	278	0.006835	11.16%
320-639	242	0.005950	9.72%
640-1279	40	0.000983	1.61%
1280-2559	260	0.006393	10.44%
2560-5119	0	0.000000	0.00%
5120-	0	0.000000	0.00%

Close

Improving WireShark Performance

- Don't use capture filters
- Increase your read buffer size
- Don't update the screen dynamically
- Get a faster computer
- Use a TAP
- Don't resolve names