

# Computer Networks Lab - IT091IU

Lecture 0: Course introduction

Lecturer: Le Duy Tan, Ph.D.

# Instructor's Profile



**Lê Duy Tân, PhD**

- B.Eng. *Computer Network and Communications* (2016) – UIT – VNU-HCM
- M.IT (2018) and Ph.D. (2021) Information Science – JAIST - Japan
- Email: [ldtan@hcmiu.edu.vn](mailto:ldtan@hcmiu.edu.vn)
- <https://it.hcmiu.edu.vn/user/ldtan>

## Research Interests

- Smart Grid
- Internet of Things
- Network Security
- Computer Networks

## Teaching Courses at ITIU

- Computer Networks
- Internet of Things
- Introduction to Computing
- Computer Graphics

## Hobbies

- Japanese language and culture
- Running

# *Course Information*

- Course title: Computer Networks Lab (IT091), 01 credits
- Time: once a week
- Where: Due to the COVID-19 pandemic, all classes will be taught online via Zoom
- Instructor: Lê Duy Tân, Ph.D.
  - Email: [ldtan@hcmiu.edu.vn](mailto:ldtan@hcmiu.edu.vn)
  - Use your IU email
  - Use label [Computer Networks – Group Number – Lab Number] in the subject of the e-mails

# *Tentative schedule*

Part	Week	Topics
PART I. WIRESHARK	Week 1	Introduction to Wireshark
	Week 2	HTTP - TCP, UDP
	Week 3	IP
PART II. PACKET TRACER	Week 4	Introduction to Packet Tracer
	Week 5	VLSM, Static routing
	Week 6	Routing
	Week 7	Vlan
	Week 8	Exam

# Assessments

Item	Points	Percent
Lab Reports (weekly)	10	10%
Lab Exam (8 <sup>th</sup> week)	10	10%
<b>Total Points</b>	<b>20</b>	<b>20%</b>

- There are a total of 7 Lab Assignments in this course. 3/7 Lab Assignments will be randomly selected to score (~10% of your final score).
- There will be a test on the last week (8th week) of this course (10% of your final score).

# *Textbook*

- **WireShark Labs:** J. F. Kurose, K. Ross,  
**Computer Networking: A Top-Down Approach,**  
6ed.
- **Packet Tracer Labs:** Odom, Wendell. **CCNA 200-301 Official Cert Guide, Volume 2.** Cisco Press,  
2019.

# *Blackboard*

- Course information, announcements
- Download lectures
- Upload the assignments, lab reports  
(all files must be in pdf, pka format)

# Online classroom rules

## Be on time



sign in at least  
10 minutes  
before class

## Be prepared



all your things must  
be prepared before  
joining the class

## Turn on camera



always turn your  
camera on so we  
can see each other

## Do not eat



We do not eat  
during online  
class session

## Dress appropriately



Wear something  
comfortable but  
presentable

## Mute your mic



Mute your mic  
when you are  
not talking

## Raise your hand



Raise your hand  
to talk or to ask  
teacher for help

## Enjoy learning



Let's enjoy  
this new kind  
of learning

# Feedback and comment

- Email your instructor
  - Use your IU email
  - Use label **[Computer Networks – Group Number – Lab Number]** in the subject of the e-mails
- Blackboard IU Forum
- Google Form link
  - Post Message as Anonymous
  - Link: <https://forms.gle/JQpQ1Uy9erEMmdWE6>

The screenshot shows the International University Blackboard interface. On the left, there's a sidebar with various course links. The 'Discussions' link is highlighted with a red box. Below it, a specific discussion forum for 'Computer Networks\_S1\_2021-22\_G03' is selected, also with a red box around its name. This forum has 2 posts and 0 unread posts. The main content area shows a 'Discussion Board' section with a message about encouraging critical thinking and interacting with ideas. To the right, there's a large green box containing a feedback form titled 'Computer Networks - Feedback'. The form includes a message from the instructor, a 'Your comment \*' field with a 'Required' note, and a 'Submit' button.

INTERNATIONAL UNIVERSITY  
BLACKBOARD

Computer Networks\_S1\_2021-22\_G03 Discussion Board

Computer Networks\_S1\_2021-22\_G03

Home Page

Announcements

Content

Staff Contacts

**Discussions**

Assignments

Tools

Help

My Grades

Discussion Board

Discussions are a good way to encourage students to think critically about your coursework and interact with each others' ideas. You can start a discussion or reply to one in this board.

Create Forum

Delete FORUM DESCRIPTION TOTAL POSTS UNREAD POSTS

Computer Networks Forum Please feel free to ask anything related to our course Computer Networks 2 0

Delete

Your comment \*

Your answer

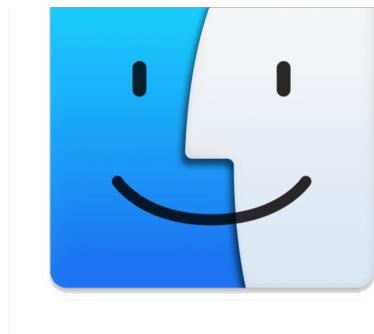
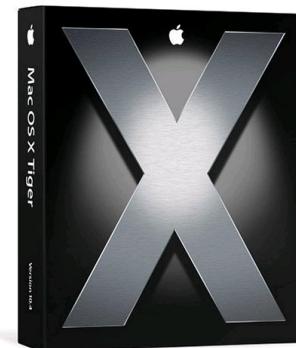
Submit



*Drinking straight from the network hose*

# So What is Wireshark?

- Packet sniffer/protocol analyzer
- Open Source Network Tool
- Latest version of the ethereal tool



Mac OS

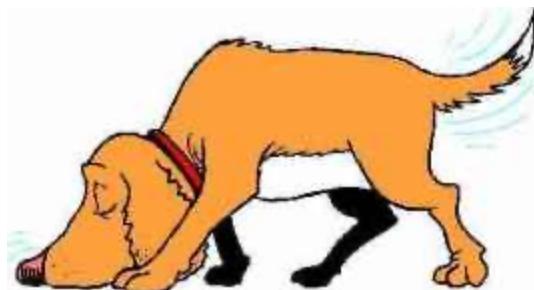


Microsoft Windows 2000



# Some intended purposes

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol internals*
- Hackers also use Wireshark



00101001001010111010101





Follow TCP Stream

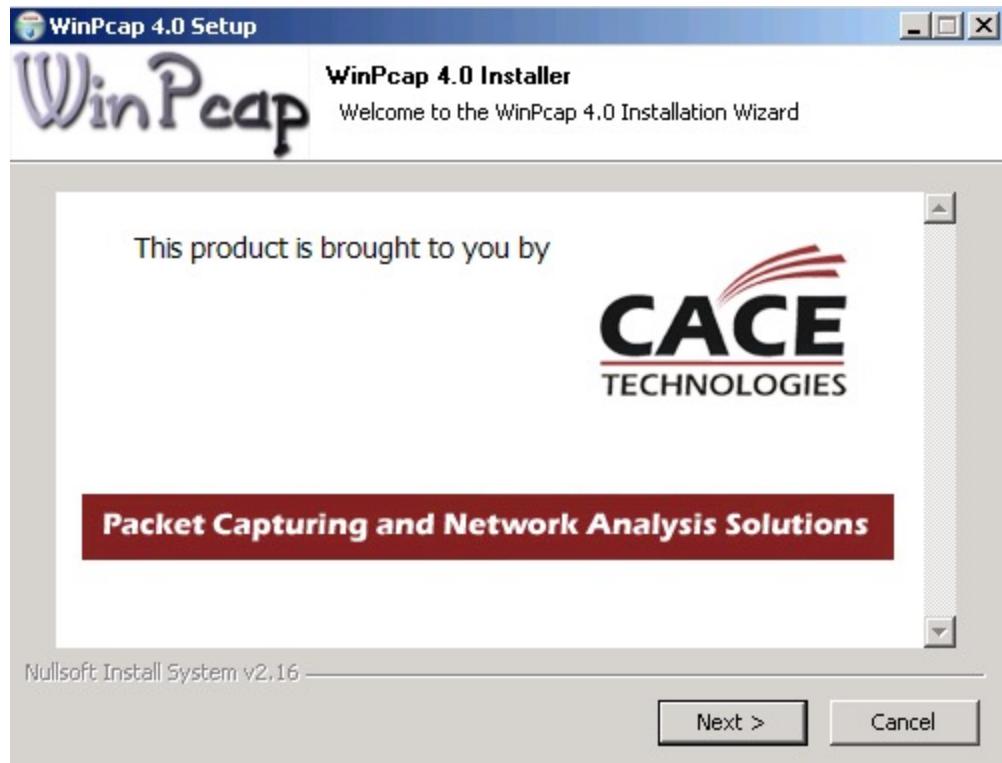
Stream Content

```
...&....user.oryx.database.mailstore..R.....D.Tp...
(md5ceffc01dcde7541829deef6b5e9c9142.R.....S....client_encoding.UNICODE.S....Datestyle.ISO,
MDY.S....is_superuser.off.S....server_version.7.4.6.S....session_authorization.oryx.K.....X.#....Z....I
.begin....B.....E.....P....1.select revision from mailstore for
update....B.....D....P.E.....S....1....2....C...
BEGIN.1....2....T....!..revision...C?.....D.....C....SELECT.Z....TP....commit...B....
u.id, u.address, u.inbox, n.name as parentspace, u.login, u.id, u.secret, a.name, a.localpart,
a.domain from users u, addresses a, namespaces n where u.login=$1 and u.id=a.id and
n.id=u.parentspace...B....4.....ams....D....P.E.....S....1....2....T....
id...CF.....address...CF.....inbox...CF.....parentspace...CR.....lo
id...CF.....address...CF.....inbox...CF.....parentspace...CR.....lo
```

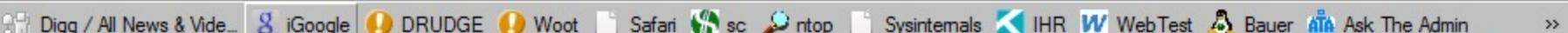
Find Save As Print Entire conversation (1430 bytes) ▾  ASCII  EBCDIC  Hex Dump  C Arrays  Raw

[Help](#) [Close](#) [Filter Out This Stream](#)

# Installation







# 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...



Enriching

Google Search



- Analysis
- Charting
- Reporting
- Integrated with Wireshark



## 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)

```
wireshark-setup.exe /S /desktopicon=yes /quicklaunchicon=no
```

# Installation on Linux

- CENTOS – yum install wireshark
- Ubuntu – apt-get install wireshark
- Red Hat – rpm –iv wireshark\*rpm
- In most cases dependencies (like libpcap) are installed automatically

...because Linux installers rock





# 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] ...

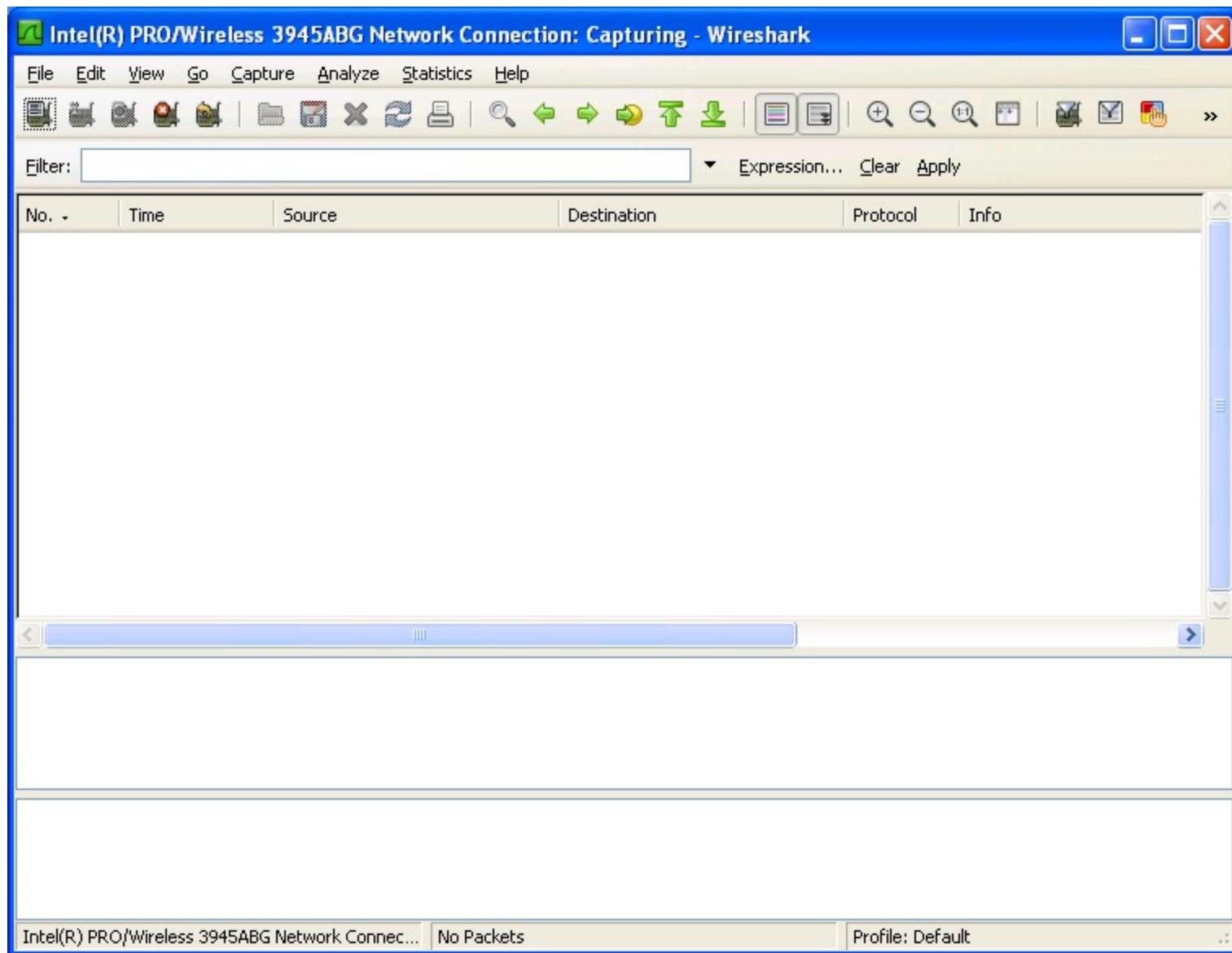
Capture interface:

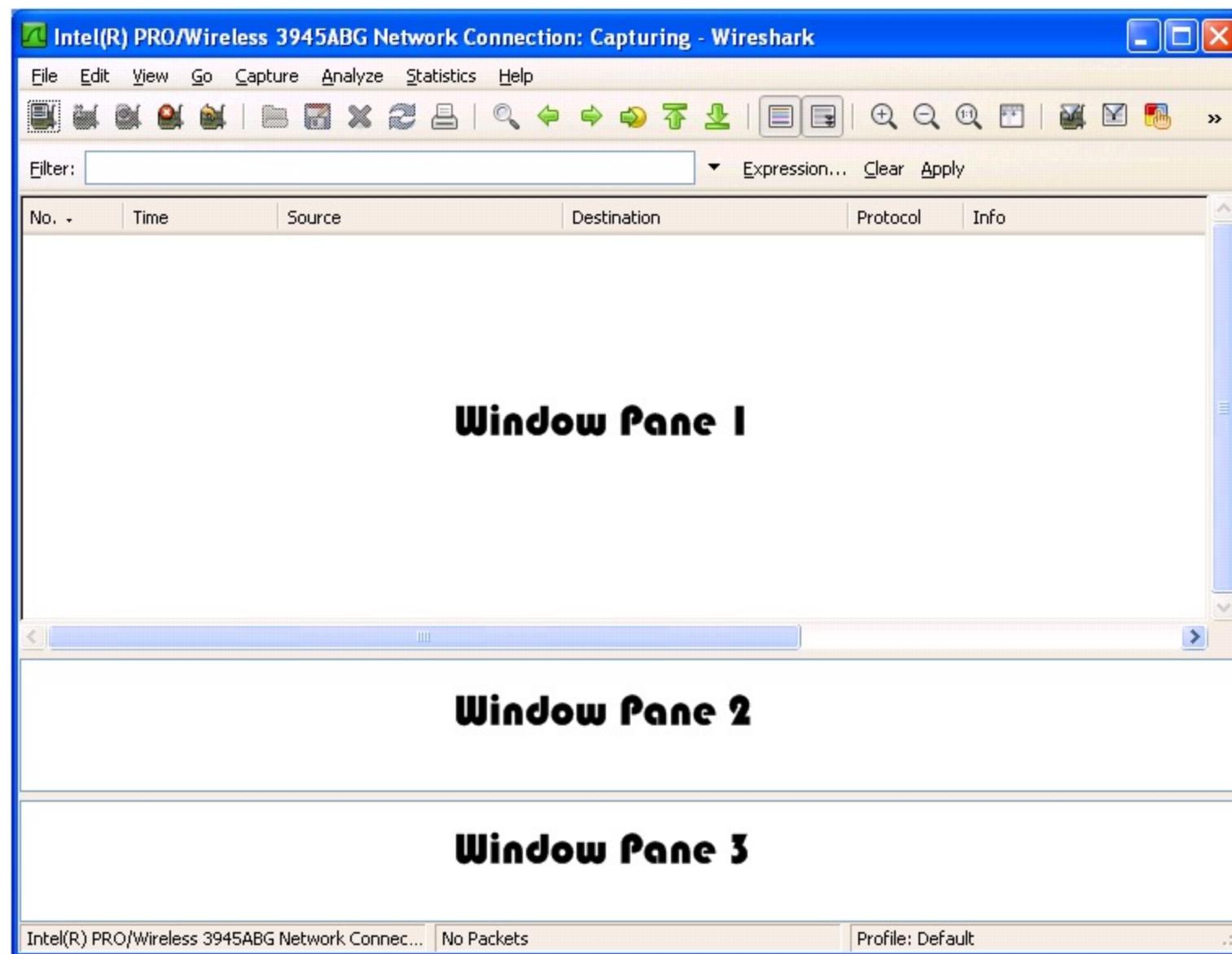
- i <interface> name or idx of interface (def: first non-loopback)
- f <capture filter> packet filter in libpcap filter syntax
- s <snaplen> packet snapshot length (def: 65535)
- p don't capture in promiscuous mode
- B <buffer size> size of kernel buffer (def: 1MB)
- y <link type> link layer type (def: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

.....





# With traffic...

The screenshot shows the Wireshark interface with a list of captured network packets. The packet details pane shows a single selected packet (packet 18) which is a CDP message. The bytes pane displays the raw hex and ASCII data for this packet.

**Packets List:**

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 unreachable
18	3.521049	Cisco_72:36:17	CDP/VTP/DTP/PAqP/UDLD	CDP	Device ID: CLE-SWH3750-10H-01
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 unreachable
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 unreachable

**Selected Packet Details:**

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

**Selected Packet Bytes:**

0000	01	00	0c	cc	cc	cc	00	11	93	72	36	17	01	99	aa	aa	.....	.r6.....
0010	03	00	00	0c	20	00	02	b4	a4	63	00	01	00	16	43	4c	.....	.c....CL
0020	45	2d	53	57	48	33	37	35	30	2d	31	30	48	2d	30	31	E-SWH3750-10H-01	
0030	00	02	00	11	00	00	00	01	01	01	cc	00	04	0a	01	0a	.....	.....
0040	0e	00	03	00	16	46	61	73	74	45	74	68	65	72	6e	65	.....	Fas tEtherne
0050	74	31	2f	30	2f	32	31	00	04	00	08	00	00	00	28	00	t1/0/21.	.....(.
0060	05	00	dc	43	69	73	63	6f	20	49	6e	74	65	72	6e	65	...Cisco	Interne
0070	74	77	6f	72	6b	20	4f	70	65	72	61	74	69	6e	67	20	twork	Op erating
0080	53	79	73	74	65	6d	20	53	6f	66	74	77	61	72	65	20	System	S oftware
0090	0a	49	4f	53	20	28	74	6d	29	20	43	33	37	35	30	20	.IOS (tm)	C3750

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

# HEX Window

Tucker Ellis & West aaa.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

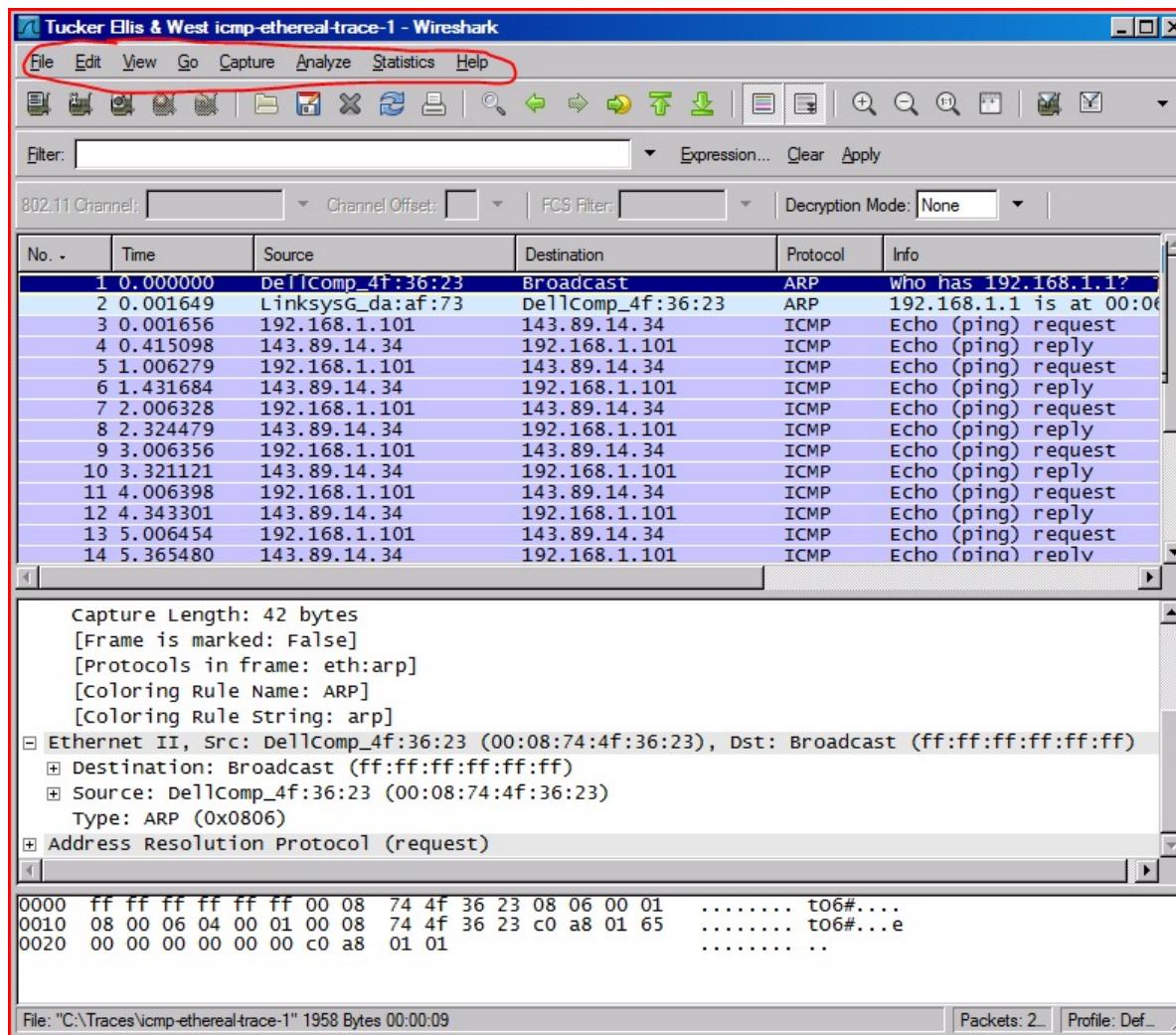
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
2	0.746308	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
3	0.751270	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
4	9.318731	Silicom_01:6e:bd	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.1 is at 00:30:54:00
5	0.000664	Castlrene_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	Castlrene_00:34:56	Silicom_01:6e:bd	ARP	who has 192.168.1.2? Tell 192.168.1.2 is at 00:e0:ed:01
14	0.000049	Silicom_01:6e:bd	Castlrene_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.cyb

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

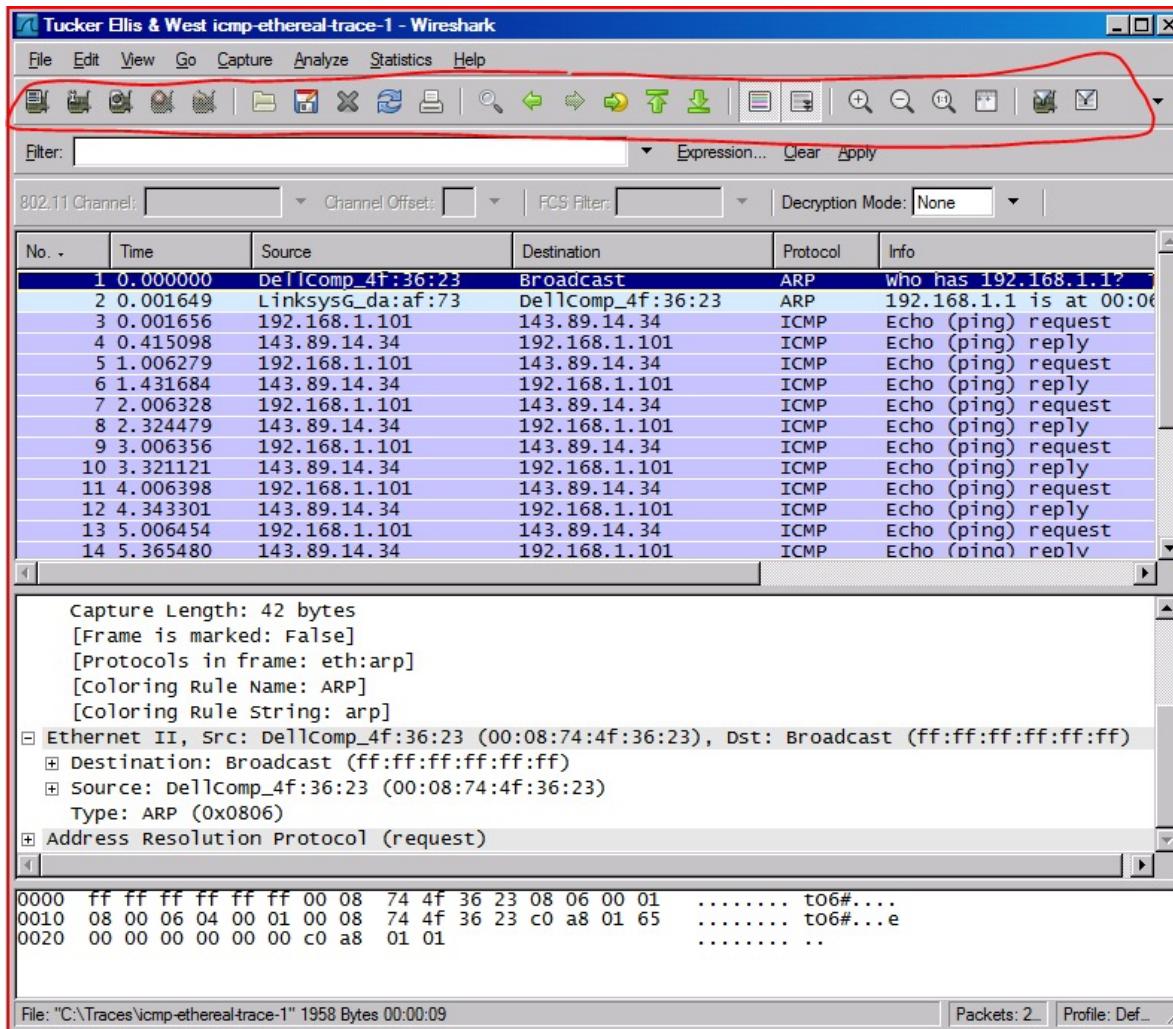
0000 ff ff ff ff ff ff 00 e0 ed 01 6e bd 08 00 45 00 .n...E.  
0010 00 4e 69 8c 00 00 80 11 4c c1 c0 a8 01 02 c0 a8 .Ni...L.....  
0020 01 ff 00 89 00 09 00 3a 5b b4 84 e7 01 10 00 01 .....[.....  
0030 00 00 00 00 00 00 20 45 46 45 41 45 4a 46 50 45 .....E FEDE]FPE  
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43 FEPENEBE 3ECAAC  
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

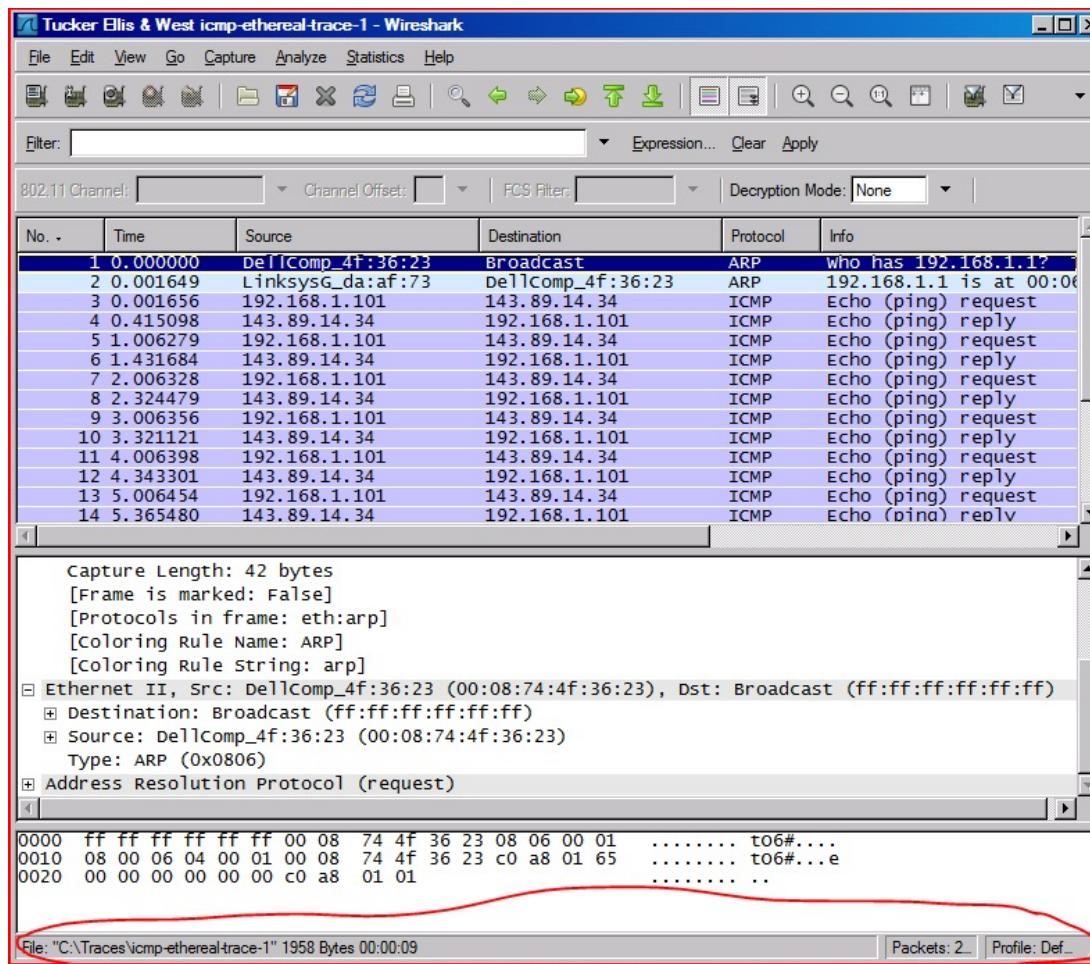
# Menu Bar



# Button Bar



# Status Bar



# Status Bar

Tucker Ellis & West aaa.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
2	0.746308	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
3	0.751270	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
4	9.318731	silicom_01:6e:bd	Broadcast	ARP	who has 192.168.1.1? Tell 19
5	0.000664	Castlene_00:34:56	silicom_01:6e:bd	ARP	192.168.1.1 is at 00:30:54:0C
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.cyb

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 00 e0 ed 01 6e bd 08 00 45 00 . . . . . n . . E.  
0010 00 4e 69 8d 00 00 80 11 4c c1 c0 a8 01 02 c0 a8 . N1 . . . L . . . .  
0020 01 ff 00 89 00 89 00 3a 5b b4 84 e7 01 10 00 01 . . . . . [ . . . .  
0030 00 00 00 00 00 20 45 46 45 44 45 4a 46 50 45 . . . . . E FEDEJFPE  
0040 45 45 50 45 4e 45 42 45 4a 45 4f 43 41 43 41 43 EEPENEBE JEOCACAC  
0050 41 43 41 43 41 42 4d 00 00 20 00 01 ACACABM. . .

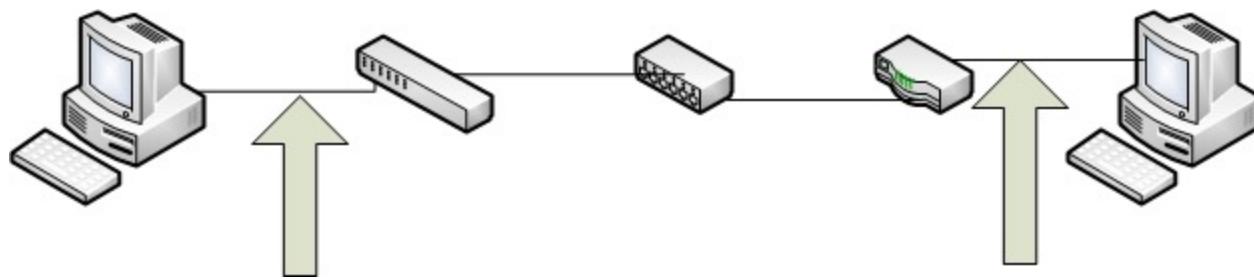
Identification (ip.id), 2 bytes

Packets: 691 Displayed: 691 Marked: 0

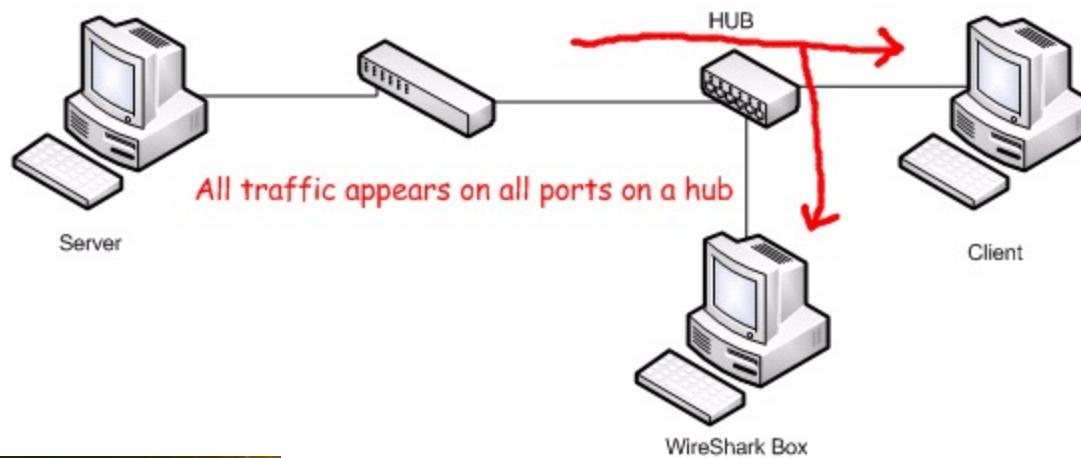
Profile: Default

Where do I put Wireshark?

# Location, Location, Location

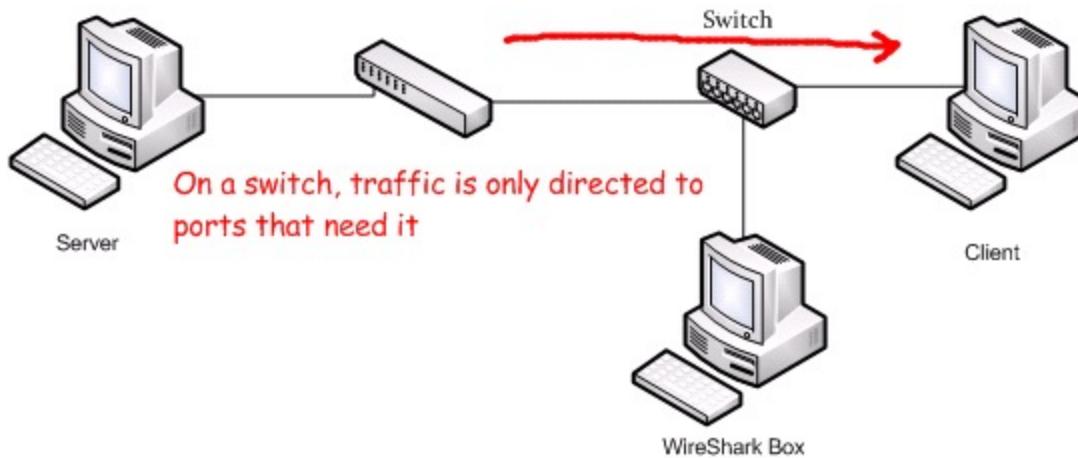


# Hub



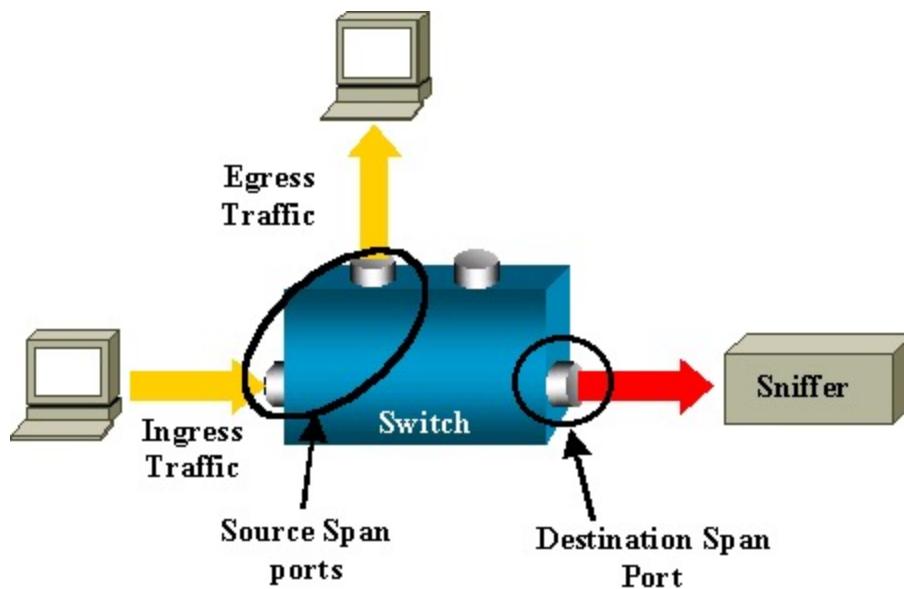
Hub

# Switches

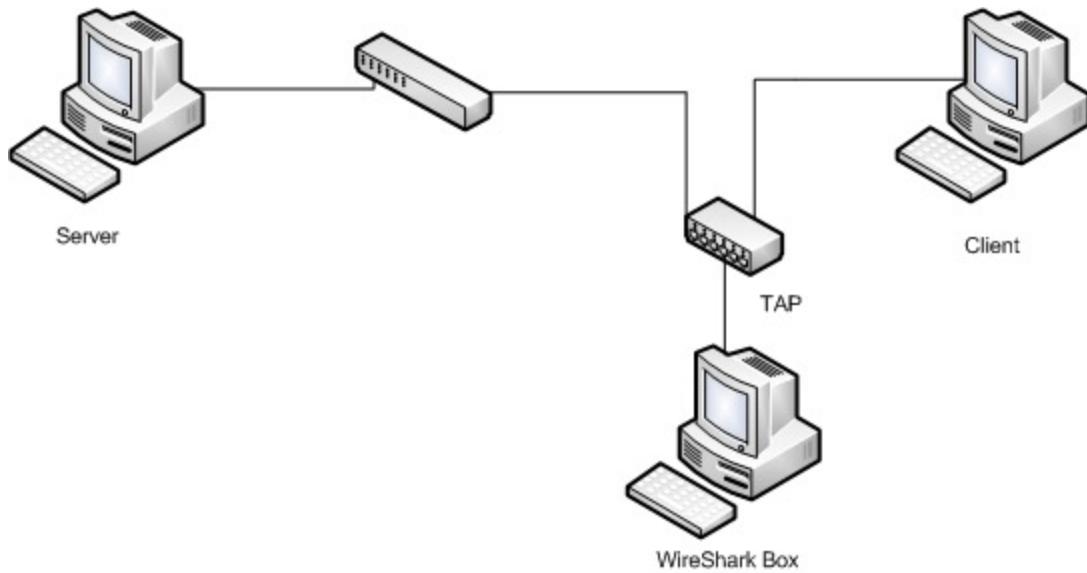


**Configure a switch port to be a monitoring port**

# Switch with a SPAN port



# TAP (Test Access Point)



# Switch

interface FastEthernet0/1

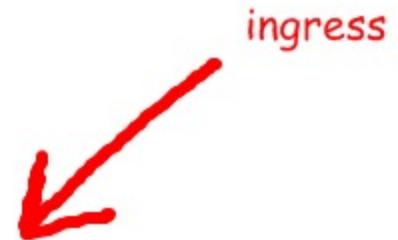
port monitor FastEthernet0/2



# Switch

interface FastEthernet0/1

port monitor FastEthernet0/2 rx



Interface FastEthernet0/3

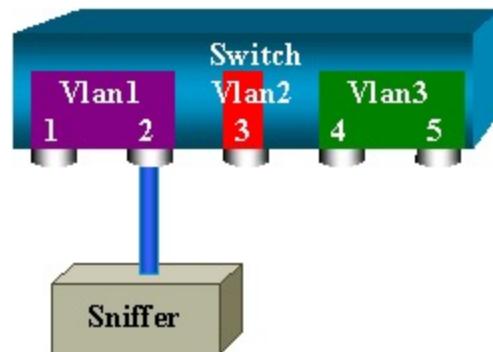
port monitor FastEthernet0/2 tx



# VLAN Monitoring

interface FastEthernet0/1

port monitor VLAN1



# Types of TAPs

- Copper & Optical
- Conversion TAPs
- Aggregator TAPs
- Full-Duplex TAPs
- Hub – Technically...a hub is a half duplex TAP, but you may miss critical layer 1 events



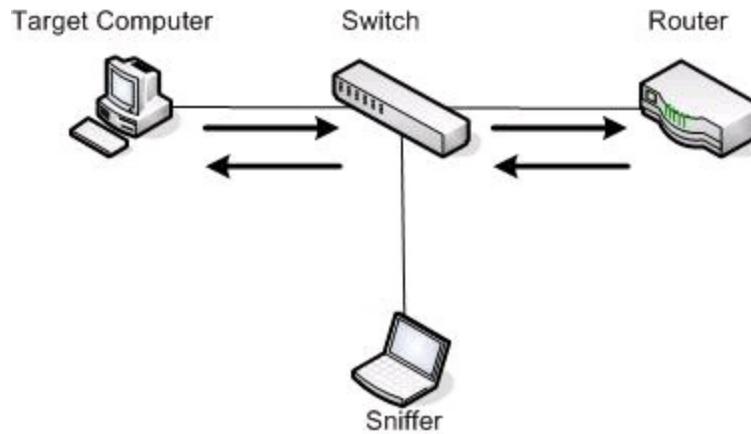
# Why to use a TAP

- Physical layer errors aren't seen by SPAN
- SPAN ports increase the CPU on your switch
- Timestamps are more accurate when using a TAP
- SPAN ports hide jitter (loss of synchronicity)
- After 50% port utilization you begin to drop packets (if you monitor both transmit & receive)
  - sometimes you can fix this
- They are non-intrusive
- It makes you look really cool

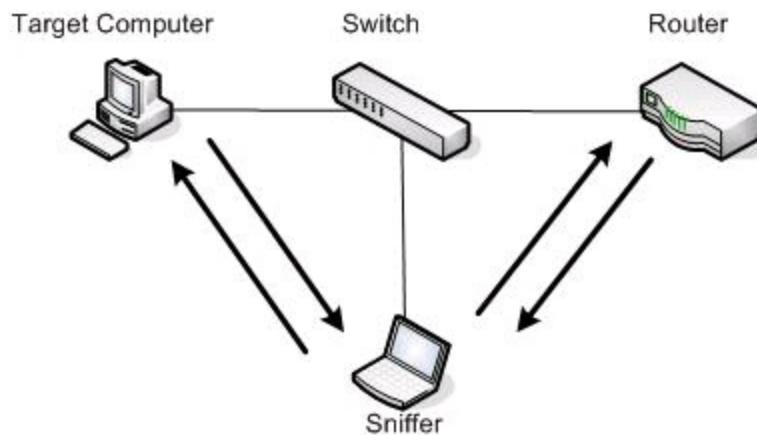


# ARP (Address Resolution Protocol) Cache Poisoning

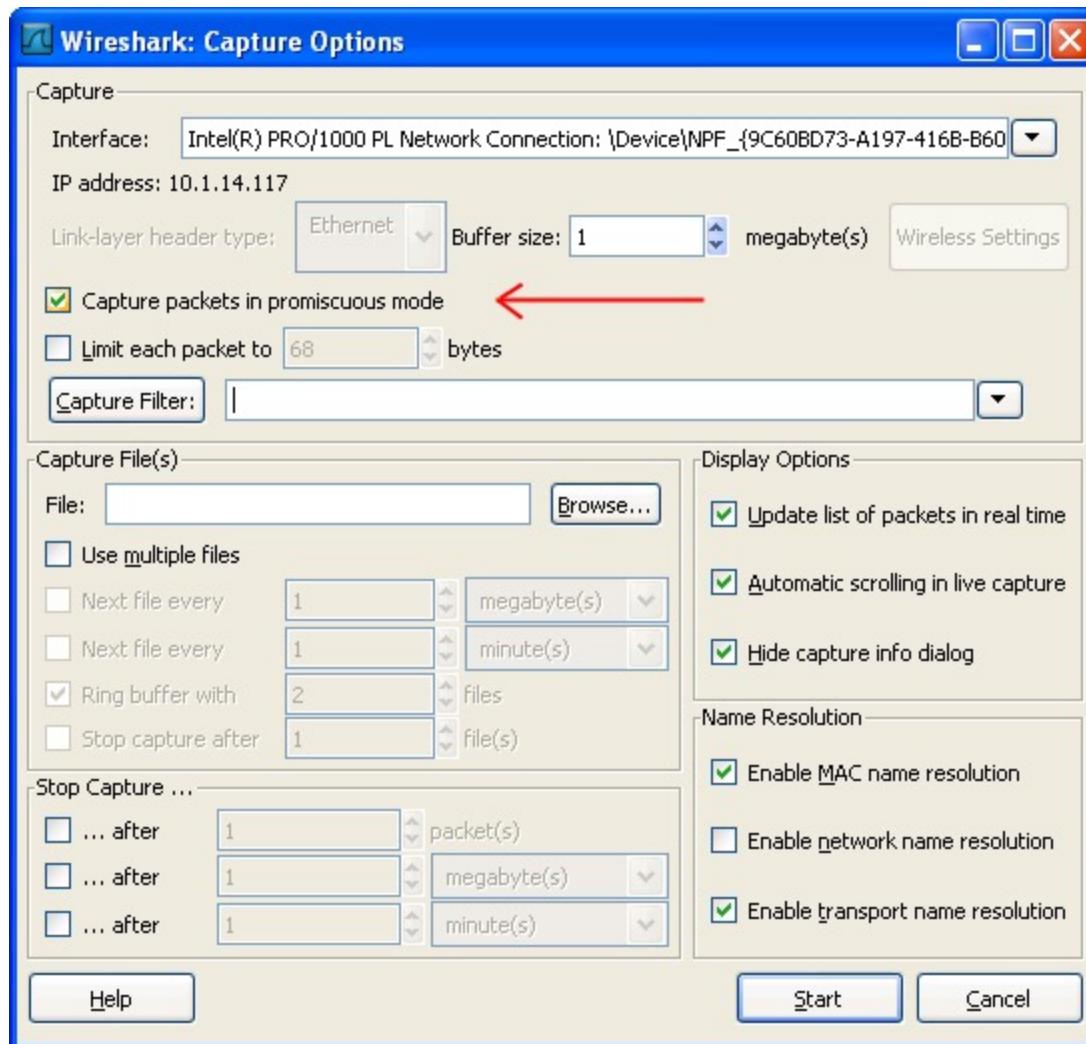
Normal Traffic Pattern



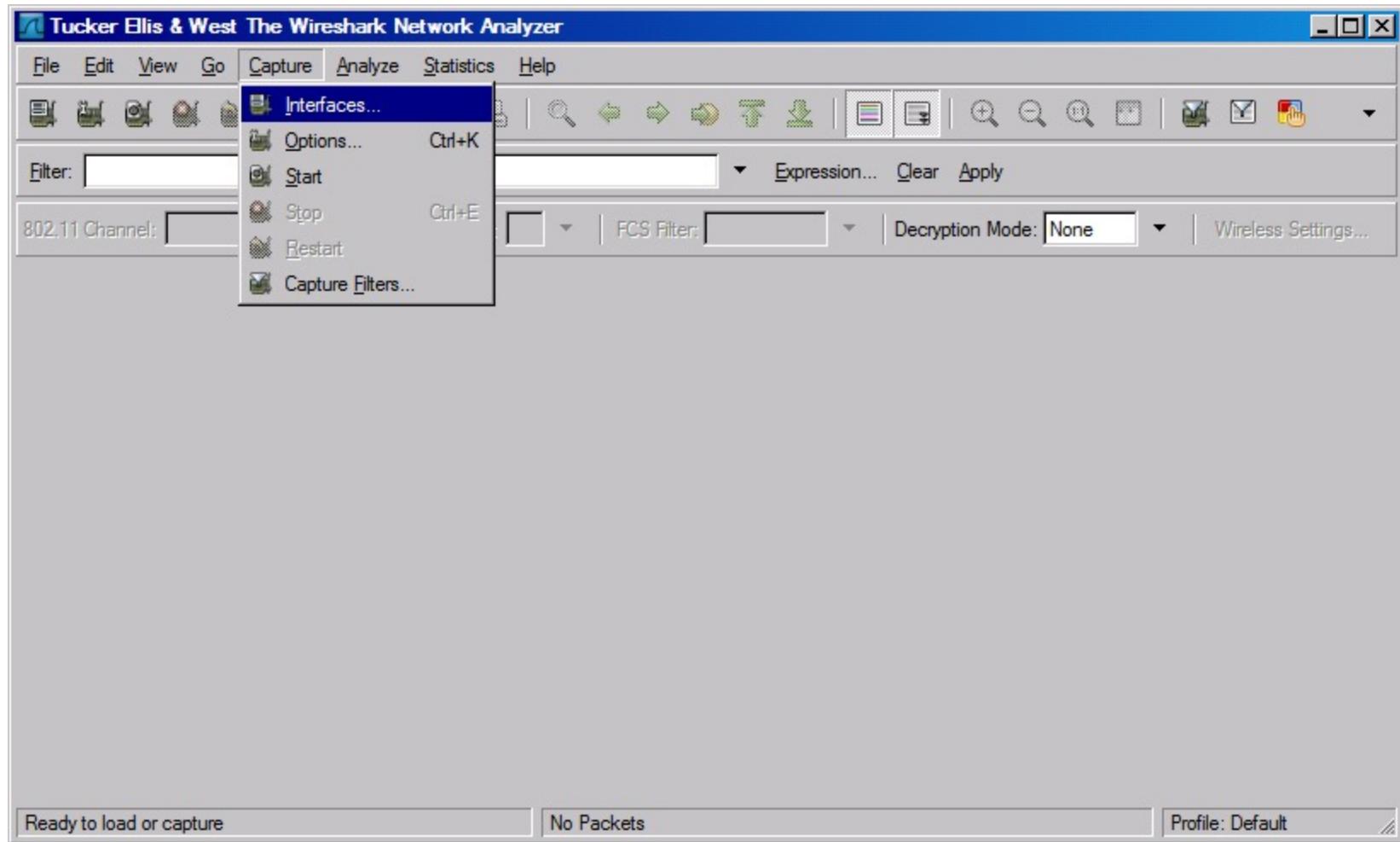
Poisoned ARP Cache



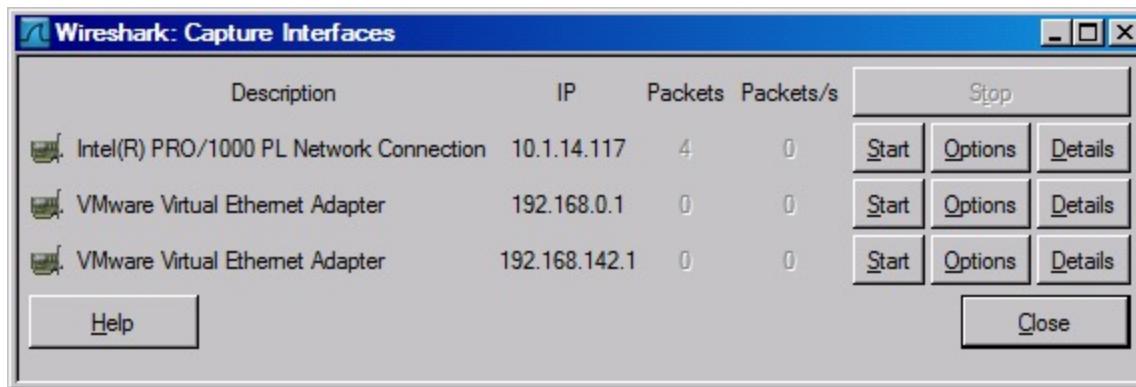
# Setting promiscuous mode



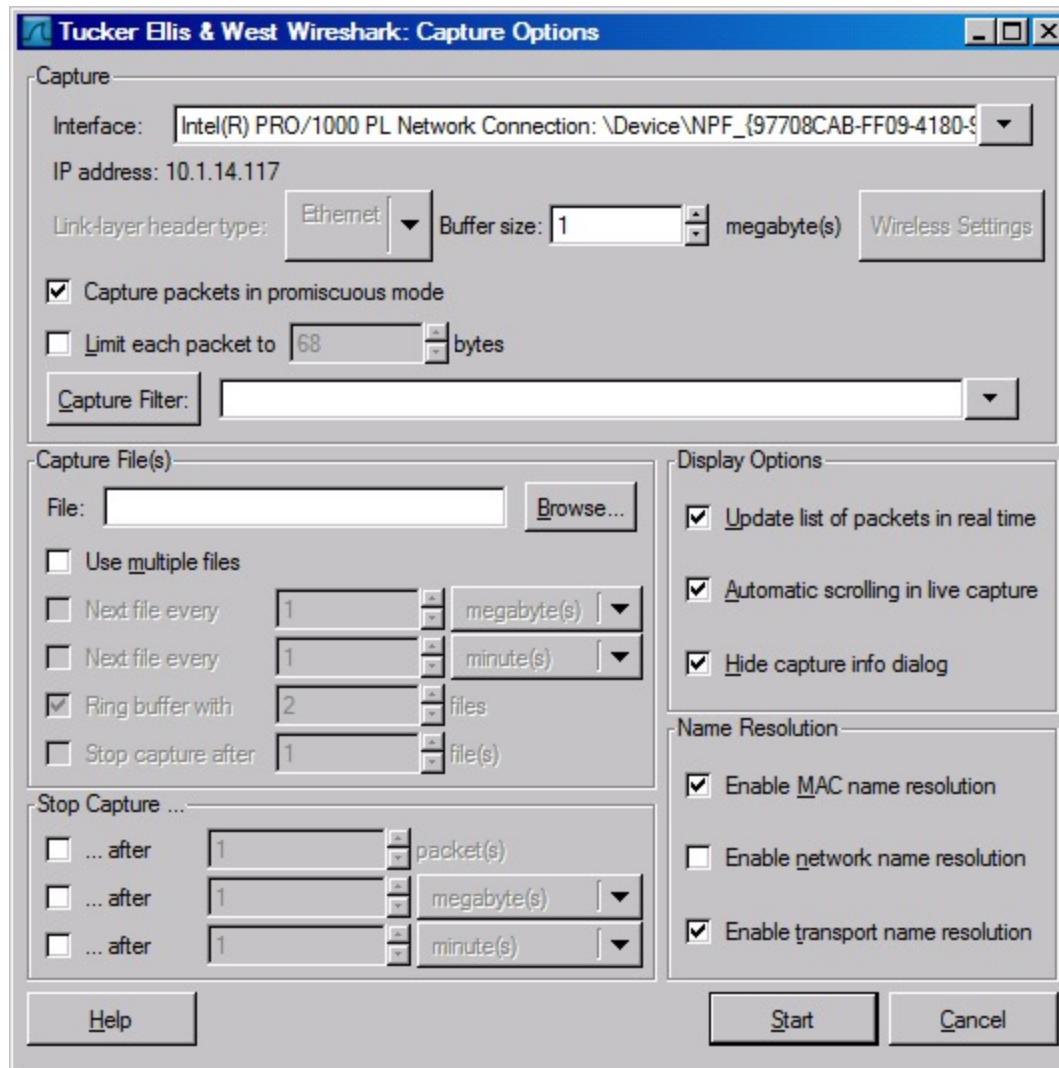
# Simple Capture



# Capture Interfaces



# Capture Options



selectively ignore traffic

# Capture Filter examples

host 10.1.11.24

host 192.168.0.1 and host 10.1.11.1

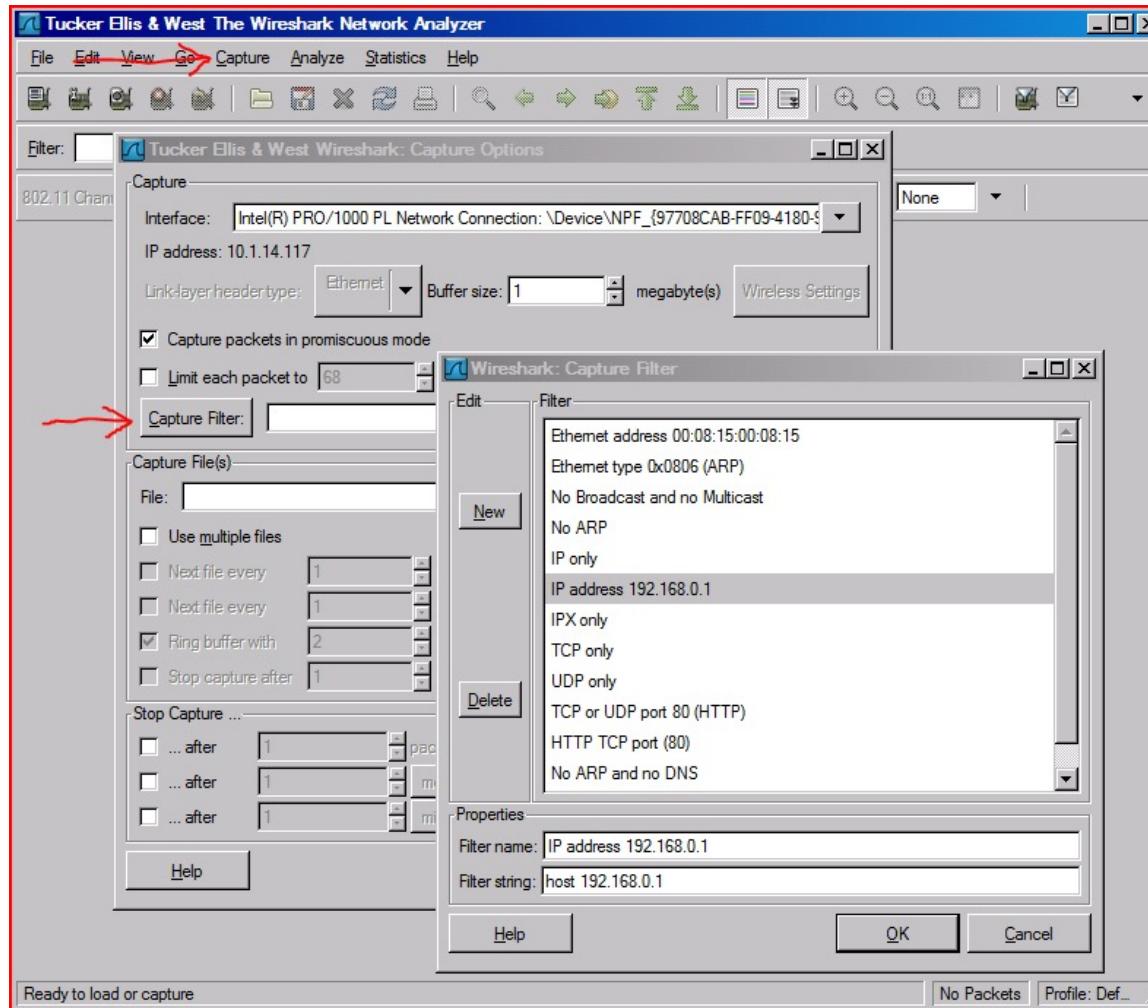
tcp port http

ip

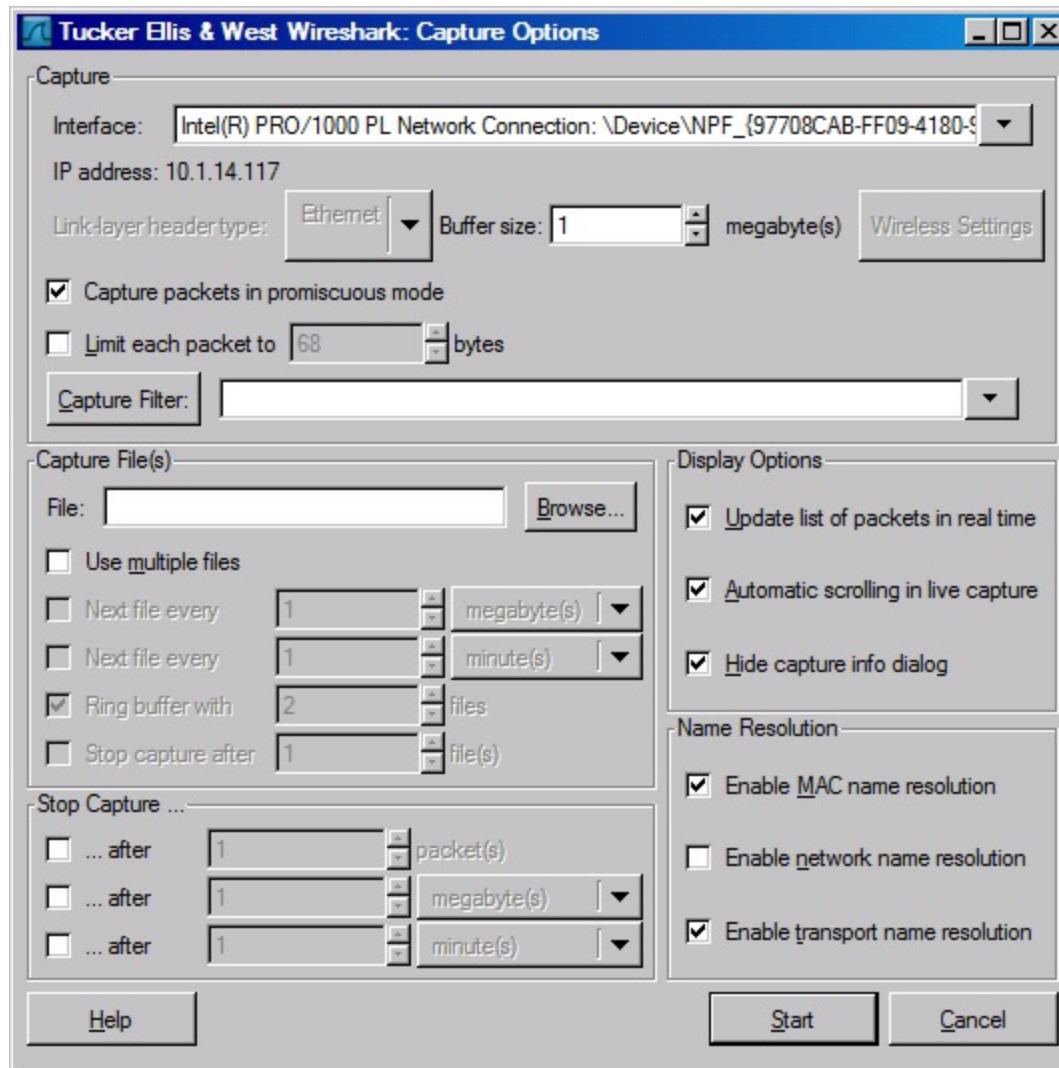
not broadcast not multicast

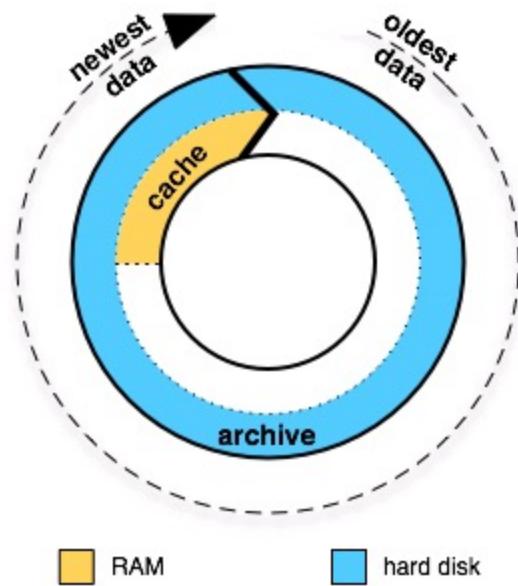
ether host 00:04:13:00:09:a3

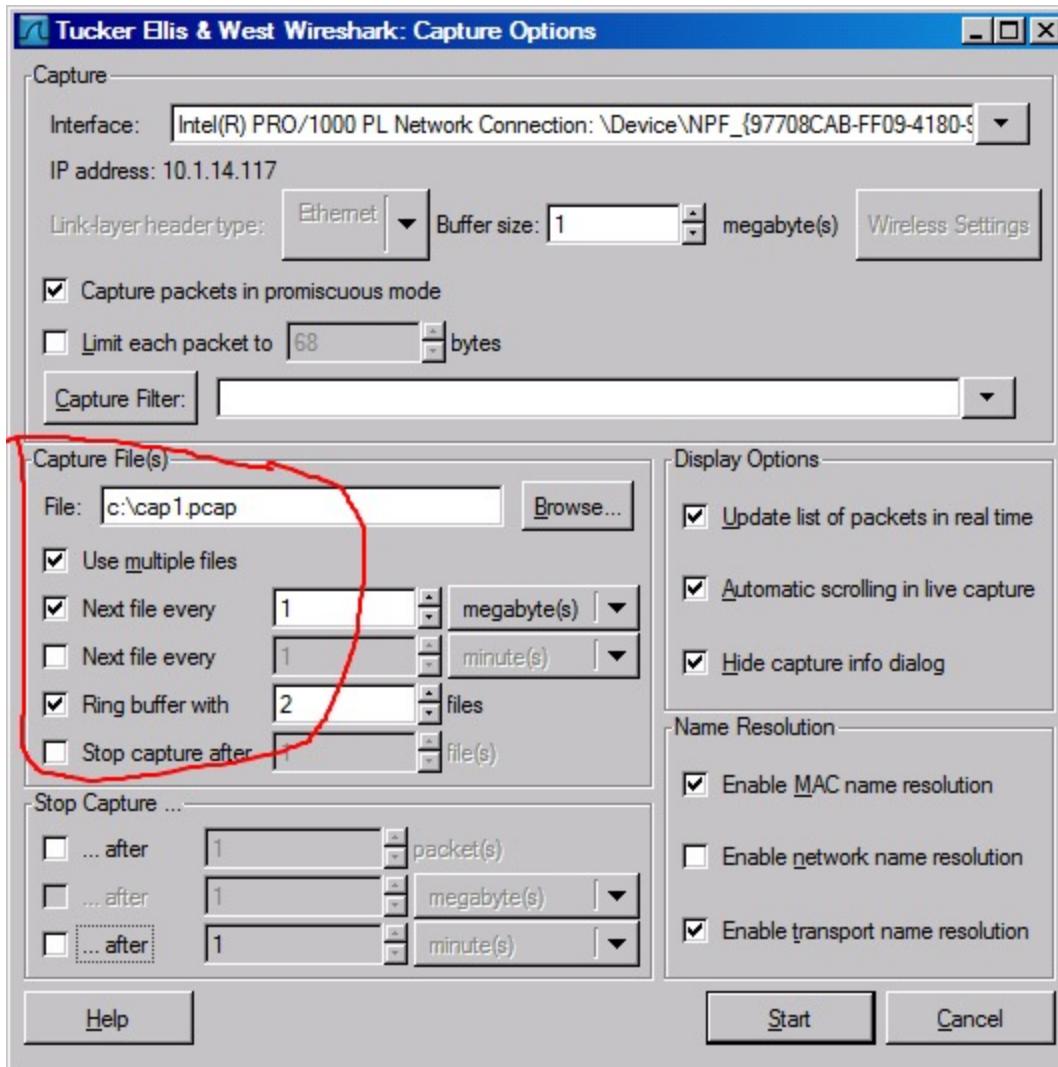
# Capture Filter



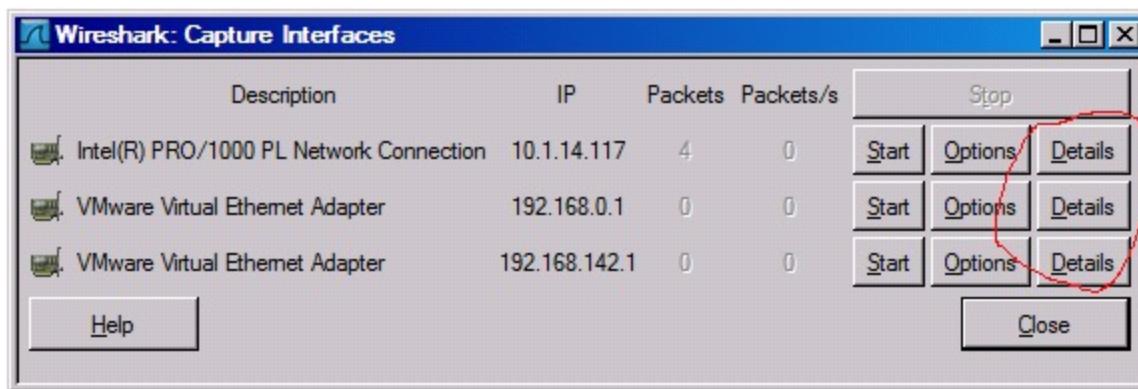
# Capture Options



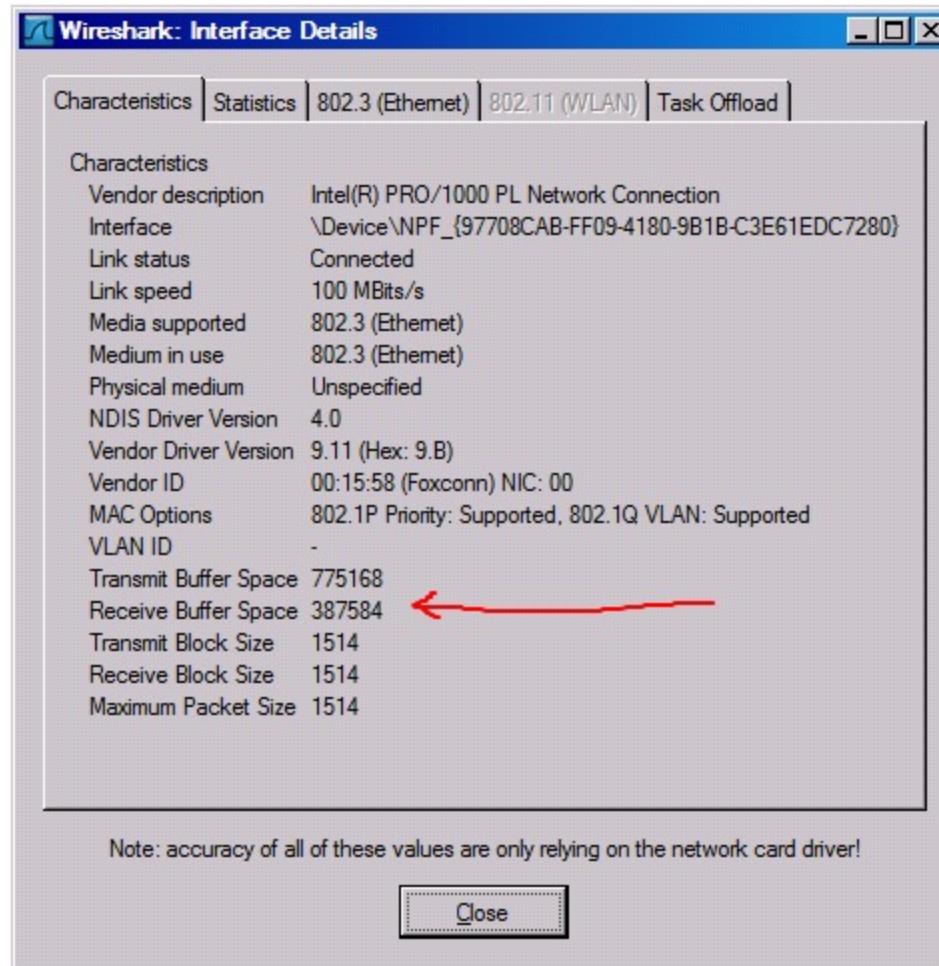




# Capture Interfaces



# Interface Details: Characteristics



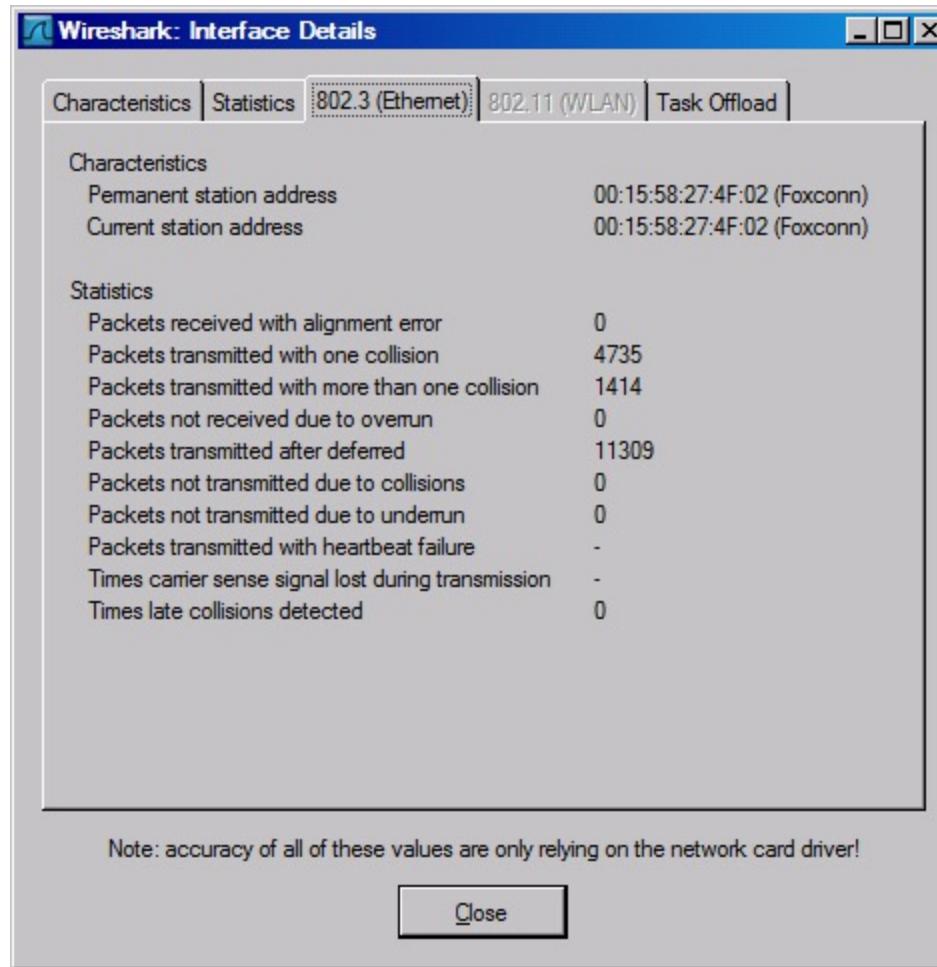
# Interface Details: Statistics

Statistics	
Transmit OK	223017
Transmit Error	0
Receive OK	356272
Receive Error	0
Receive but no Buffer	0
Directed bytes transmitted w/o errors	56505591
Directed packets transmitted w/o errors	222749
Multicast bytes transmitted w/o errors	17592
Multicast packets transmitted w/o errors	61
Broadcast bytes transmitted w/o errors	31083
Broadcast packets transmitted w/o errors	207
Directed bytes received w/o errors	424470353
Directed packets received w/o errors	338902
Multicast bytes received w/o errors	1388328
Multicast packets received w/o errors	7810
Broadcast bytes received w/o errors	3145336
Broadcast packets received w/o errors	27123
Packets received with CRC or FCS errors	0
Packets queued for transmission	0

Note: accuracy of all of these values are only relying on the network card driver!

[Close](#)

# Interface Details: 802.3 (Ethernet)



# Interface Details: Task Offload

Wireshark: Interface Details

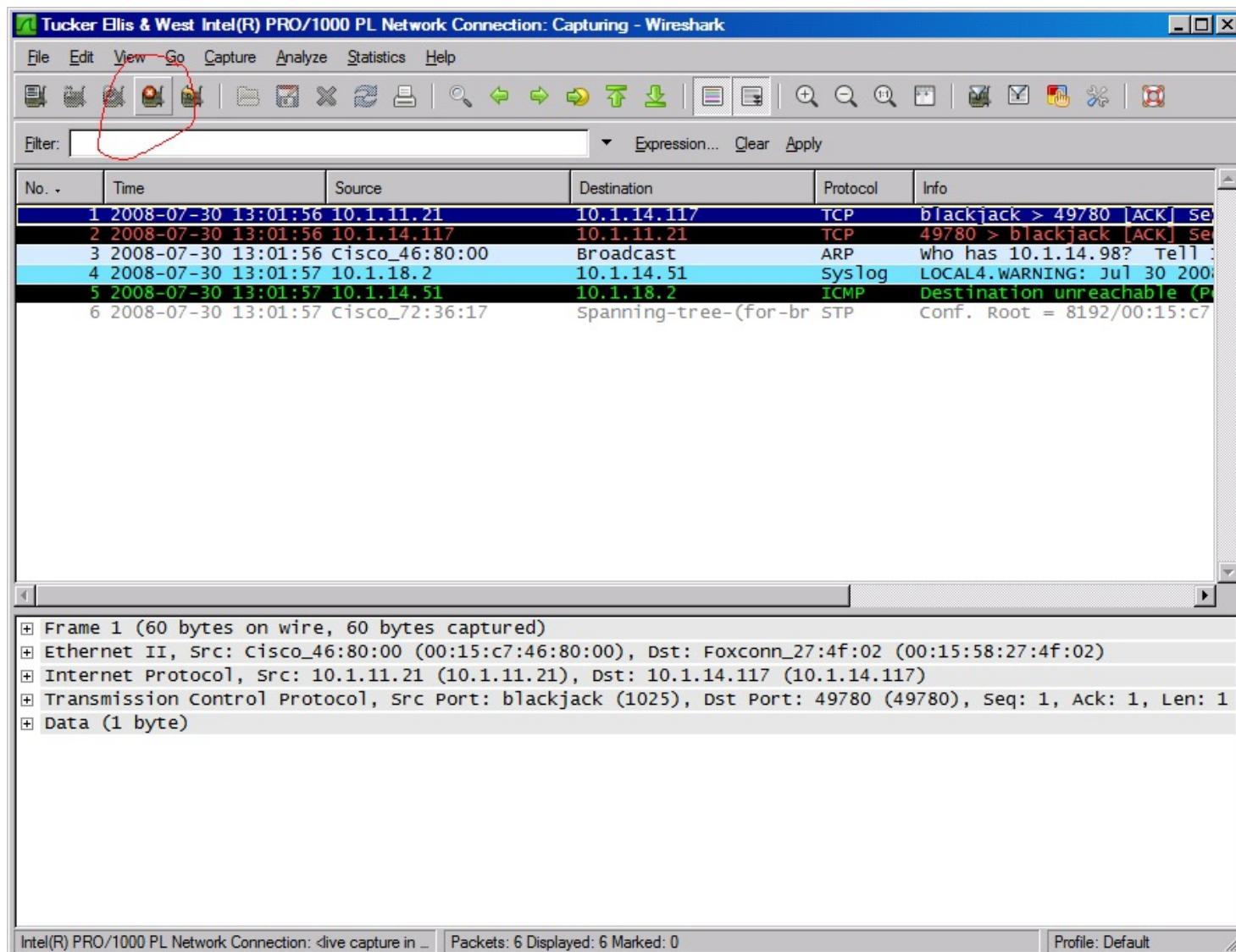
Characteristics | Statistics | 802.3 (Ethernet) | 802.11 (WLAN) | Task Offload

TCP/IP Checksum	
V4 transmit checksum	TCP: Yes, UDP: Yes, IP: Yes
Calculation supported	
Options fields supported	TCP: Yes, IP: Yes
V4 receive checksum	TCP: Yes, UDP: Yes, IP: Yes
Validation supported	
Options fields supported	TCP: Yes, IP: Yes
V6 transmit checksum	TCP: Yes, UDP: Yes
Calculation supported	
Options fields supported	TCP: Yes, IP: No
V6 receive checksum	TCP: Yes, UDP: Yes
Validation supported	
Options fields supported	TCP: Yes, IP: No
IpSec	
Offload not supported	-
TCP Large Send	
Offload not supported	-

Note: accuracy of all of these values are only relying on the network card driver!

[Close](#)

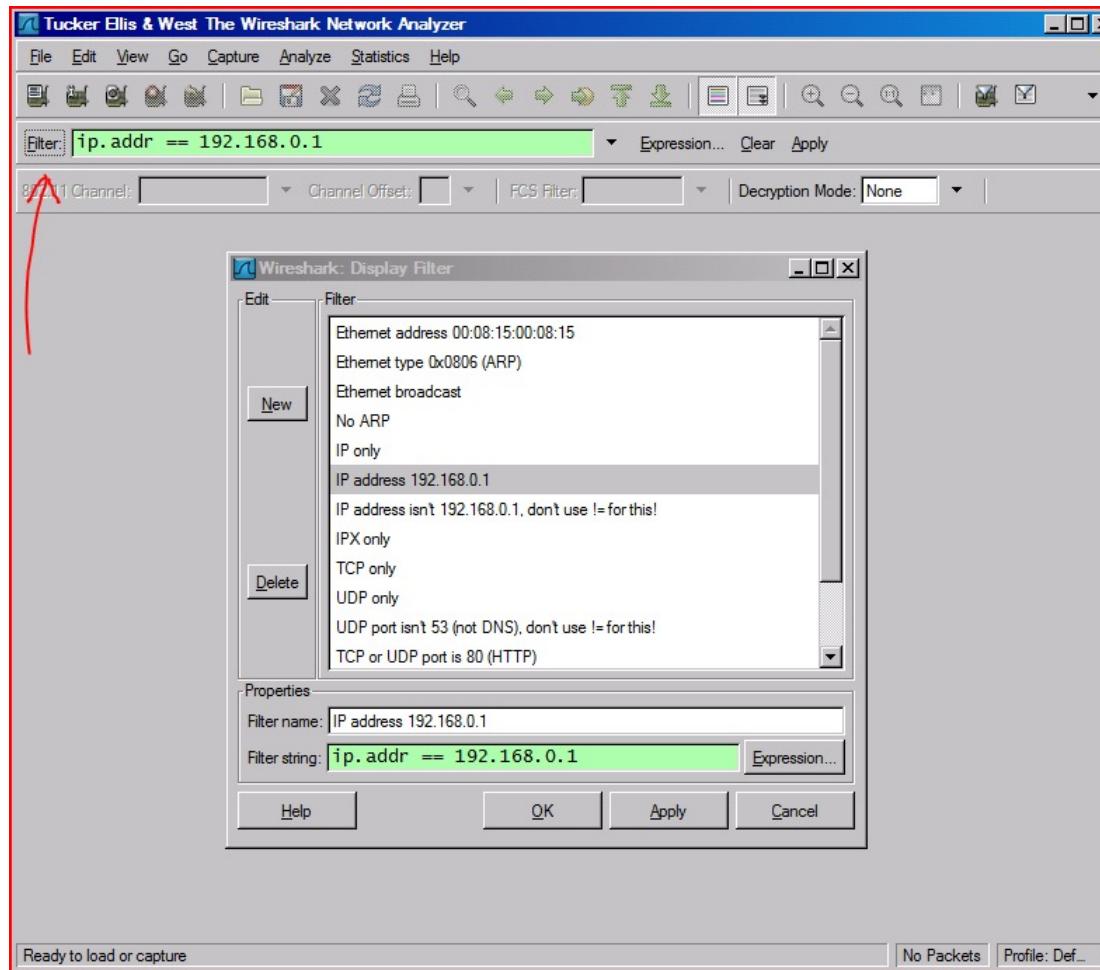
# Stopping the Packet Capture



# 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

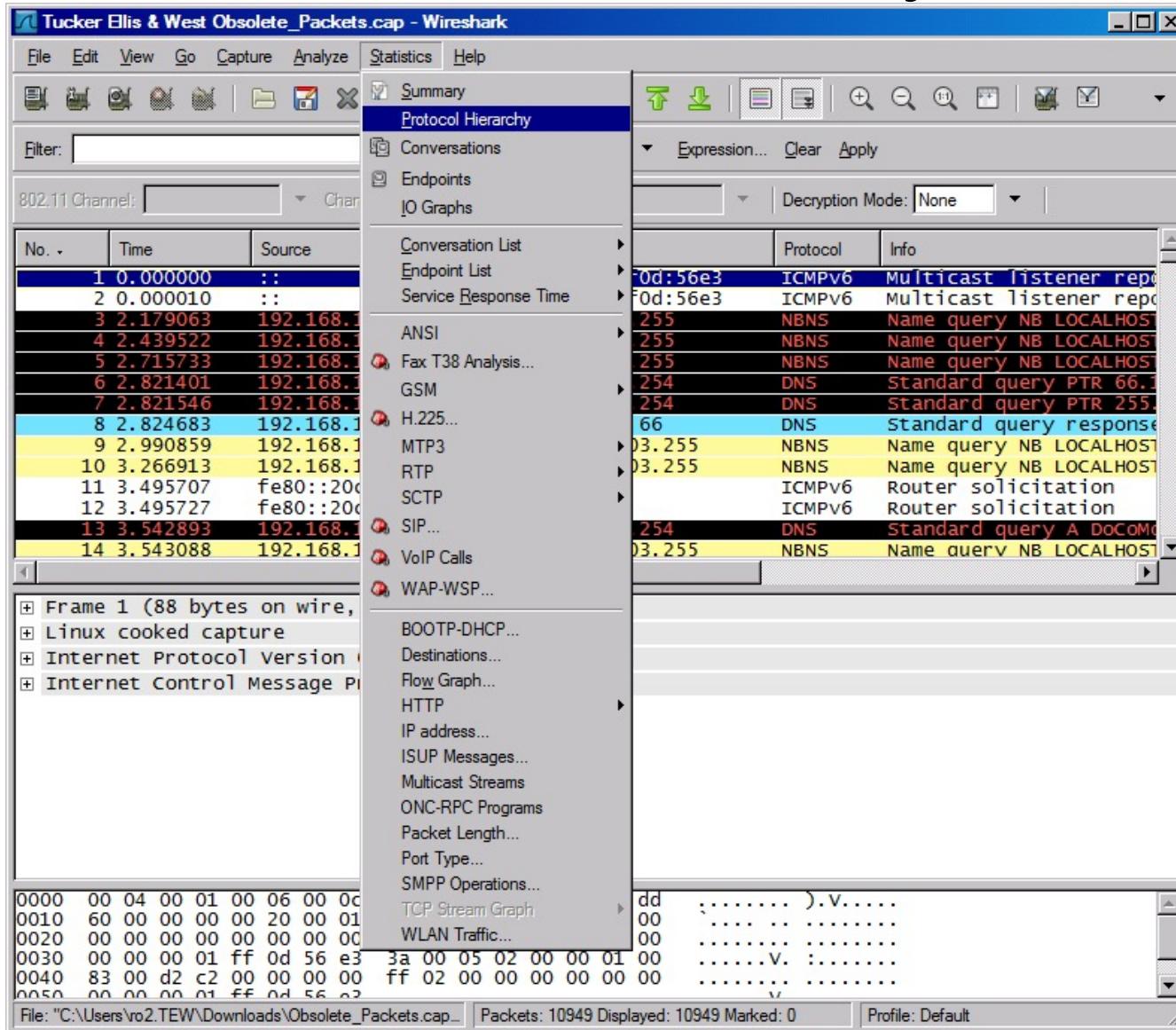
tcp.port==80 || tcp.port==3389

!(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)

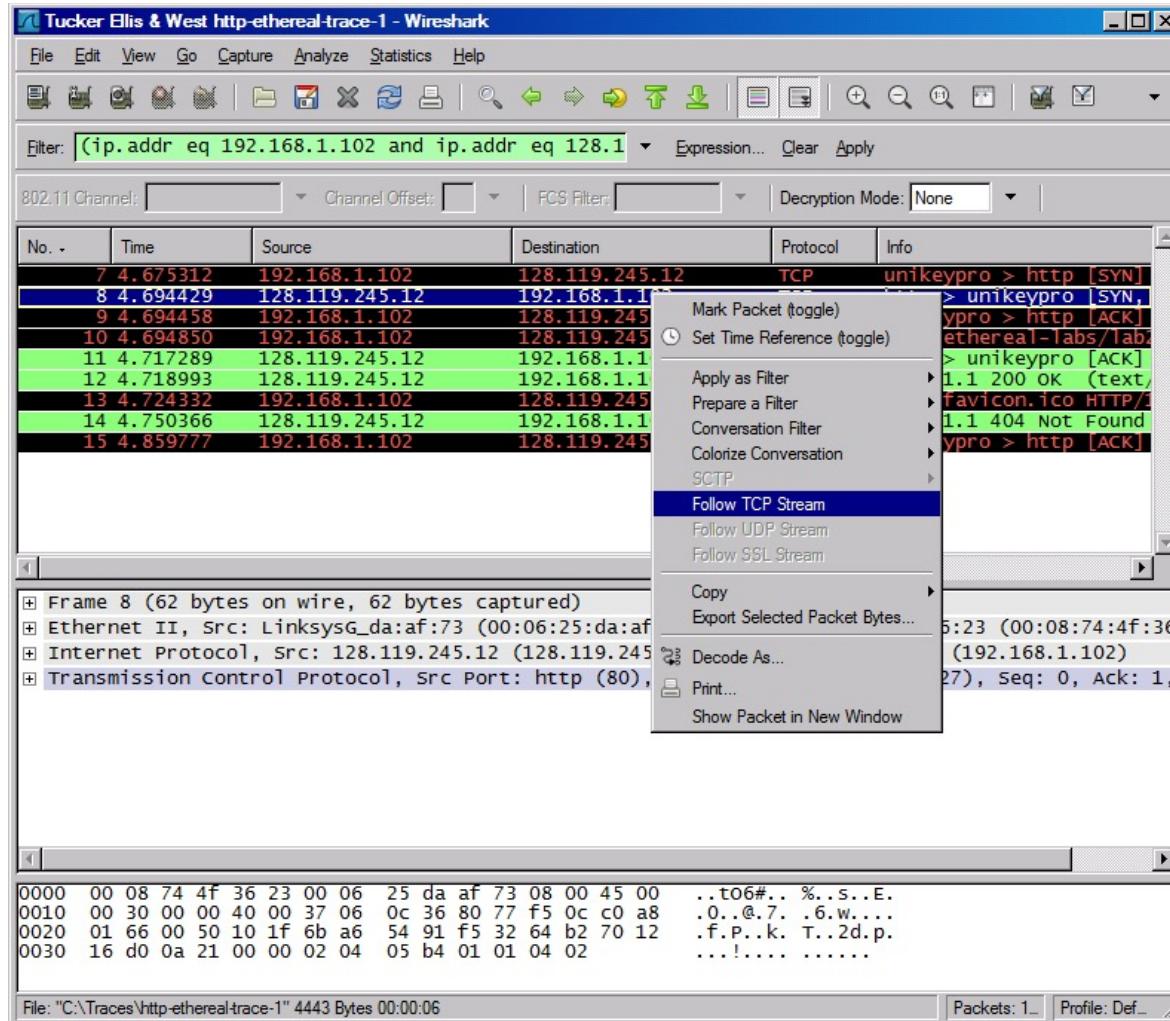
# Protocol Hierarchy



# 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	
Internet Protocol eXchange	1.46%	160	14328	0.000	0	0	0.000	
Datagram Delivery Protocol	0.40%	44	3216	0.000	0	0	0.000	
Internet Protocol eXchange	0.27%	30	1680	0.000	0	0	0.000	
Banyan Vines IP	0.47%	52	2352	0.000	0	0	0.000	

# Follow TCP Stream



# Follow TCP Stream

red - stuff you sent

blue - stuff you get

The screenshot shows a window titled "Follow TCP Stream" with a blue header bar. The main area is labeled "Stream Content" and contains a text representation of a network conversation. The text is color-coded: red for what the client sent and blue for what the server returned. The client's request (red) includes a GET request for "tab2-1.html" with various headers like Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Accept-Charset, Keep-Alive, and Connection. The server's response (blue) includes an HTTP/1.1 200 OK status with headers Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, and Content-Type. The response body (blue) contains the HTML content "<html>Congratulations. You've downloaded the file tab2-1.html!</html>". Below the text area is a toolbar with buttons for Find, Save As, Print, and Entire conversation (2714 bytes). To the right of the text area are several radio buttons for ASCII, EBCDIC, Hex Dump, C Arrays, and Raw, with "Raw" selected. At the bottom are buttons for Help, Close, and Filter Out This Stream.

```
GET /ethereal-Tabs/tab2-1.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 tab2-1.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
```

Find Save As Print Entire conversation (2714 bytes) ▾  ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help Close Filter Out This Stream

# Expert Info

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

File Edit View Go Capture Analyze Statistics Help

Filter: 802.11 Channel:

No. Time Source Destination Protocol Length Info

1	0.000000	19:00:00:00:00:00	..104	SNMP	get-request	SNMPV2-SMI
2	0.017162	19:00:00:00:00:00	..102	SNMP	get-response	SNMPV2-SMI
3	0.017086	19:00:00:00:00:00	..104	SNMP	get-request	SNMPV2-SMI
4	3.034572	19:00:00:00:00:00	..102	SNMP	get-response	SNMPV2-SMI
5	4.626878	19:00:00:00:00:00	..19	DNS	Standard query A	gaia.0.etherreal-labs.lan
6	4.663785	63:00:00:00:00:00	..102	DNS	Standard query response	unikeypro.0.etherreal-labs.lan
7	4.675312	19:00:00:00:00:00	45.12	TCP	unikeypro > http	[SYN]
8	4.694429	12:00:00:00:00:00	..102	TCP	http > unikeypro	[SYN, ACK]
9	4.694458	19:00:00:00:00:00	45.12	TCP	unikeypro > http	[ACK]
10	4.694850	19:00:00:00:00:00	45.12	HTTP	GET /ethereal-labs/lab	/index.html
11	4.717289	12:00:00:00:00:00	..102	TCP	http > unikeypro	[ACK]
12	4.718993	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 200 OK	(text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	GET /favicon.ico	HTTP/1.1 200 OK
14	4.750366	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 404	Not Found

Frame 8 (62 bytes on wire, 62 bytes captured)  
Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: DellComp\_4f:36:23 (00:08:74:4f:36)  
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)  
Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 0, Ack: 1,

0000 00 08 74 4F 36 23 00 06 25 da af 73 08 00 45 00 ..t06#.. %.5..E.  
0010 00 30 00 00 40 00 37 06 0c 36 80 77 f5 0c c0 a8 .0..@.7. .6.w....  
0020 01 66 00 50 10 1f 6b a6 54 91 f5 32 64 b2 70 12 .f.P..k. T..2d.p.  
0030 16 d0 0a 21 00 00 02 04 05 b4 01 01 04 02 ....!.....

File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06 Packets: 1 Profile: Def

# Expert Info

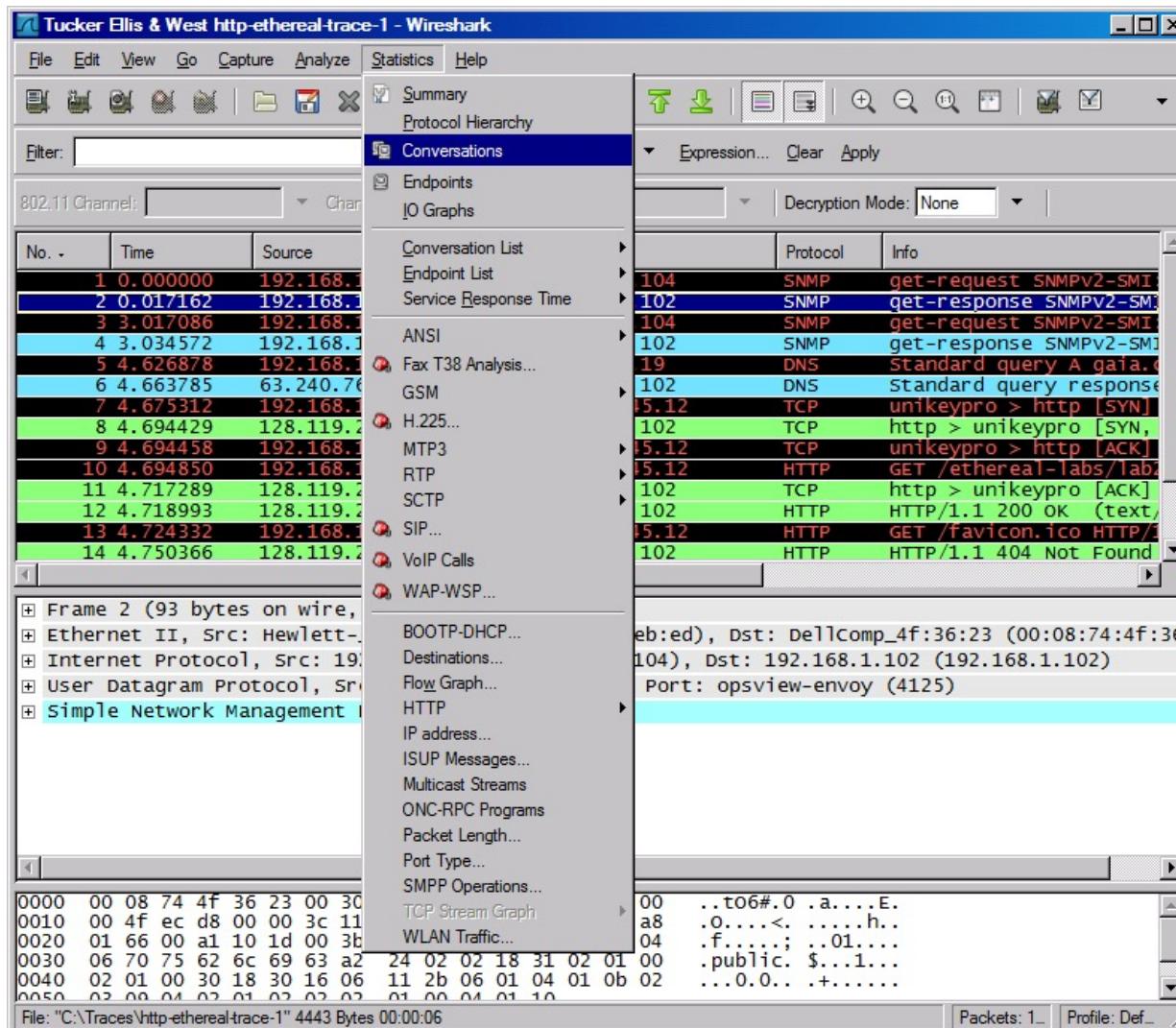
Wireshark: 16 Expert Infos

Errors: 4 Warnings: 0 Notes: 6 Chats: 6 Severity filter: Error+Warn+Note+Chat ▾

No. ▾	Sever.	Group	Protocol	Summary
1	Note	Undecoded	SNMP	Unresolved value, Missing MIB
2	Note	Undecoded	SNMP	Unresolved value, Missing MIB
3	Note	Undecoded	SNMP	Unresolved value, Missing MIB
4	Note	Undecoded	SNMP	Unresolved value, Missing MIB
7	Chat	Sequence	TCP	Connection establish request (SYN): server port http
8	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port http
9	Error	Checksum	TCP	Bad checksum
10	Chat	Sequence	HTTP	GET /ethereal-Habs/lab2-1.html HTTP/1.1\r\n
10	Error	Checksum	TCP	Bad checksum
12	Chat	Sequence	HTTP	HTTP/1.1 200 OK\r\n
13	Chat	Sequence	HTTP	GET /favicon.ico HTTP/1.1\r\n
13	Error	Checksum	TCP	Bad checksum
14	Chat	Sequence	HTTP	HTTP/1.1 404 Not Found\r\n
15	Error	Checksum	TCP	Bad checksum
16	Note	Undecoded	SNMP	Unresolved value, Missing MIB
17	Note	Undecoded	SNMP	Unresolved value, Missing MIB

Help Close

# Conversations



# Conversations

Conversations: http-ethereal-trace-1

Ethernet: 2 | Fibre Channel | FDDI | **IPv4: 3** | IPX | JXTA | NCP | RSVP | SCTP | TCP: 1 | Token Ring | UDP: 4 | USB | WLAN

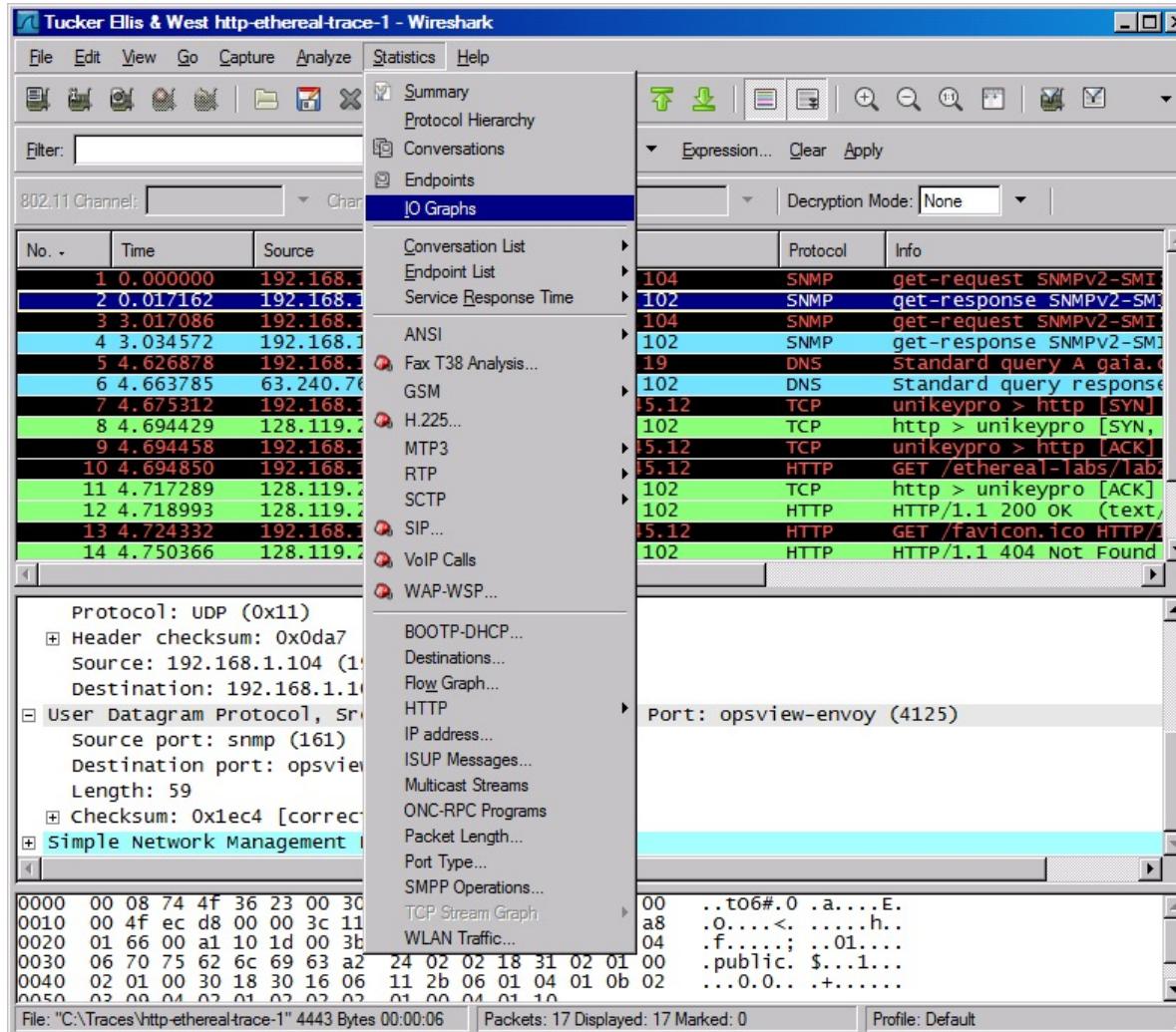
IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps
63.240.76.19	192.168.1.102	2	370	1	293	1	77	4.626878000	0.0369	N/A
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

Name resolution       Limit to display filter

[Help](#) [Copy](#) [Close](#)

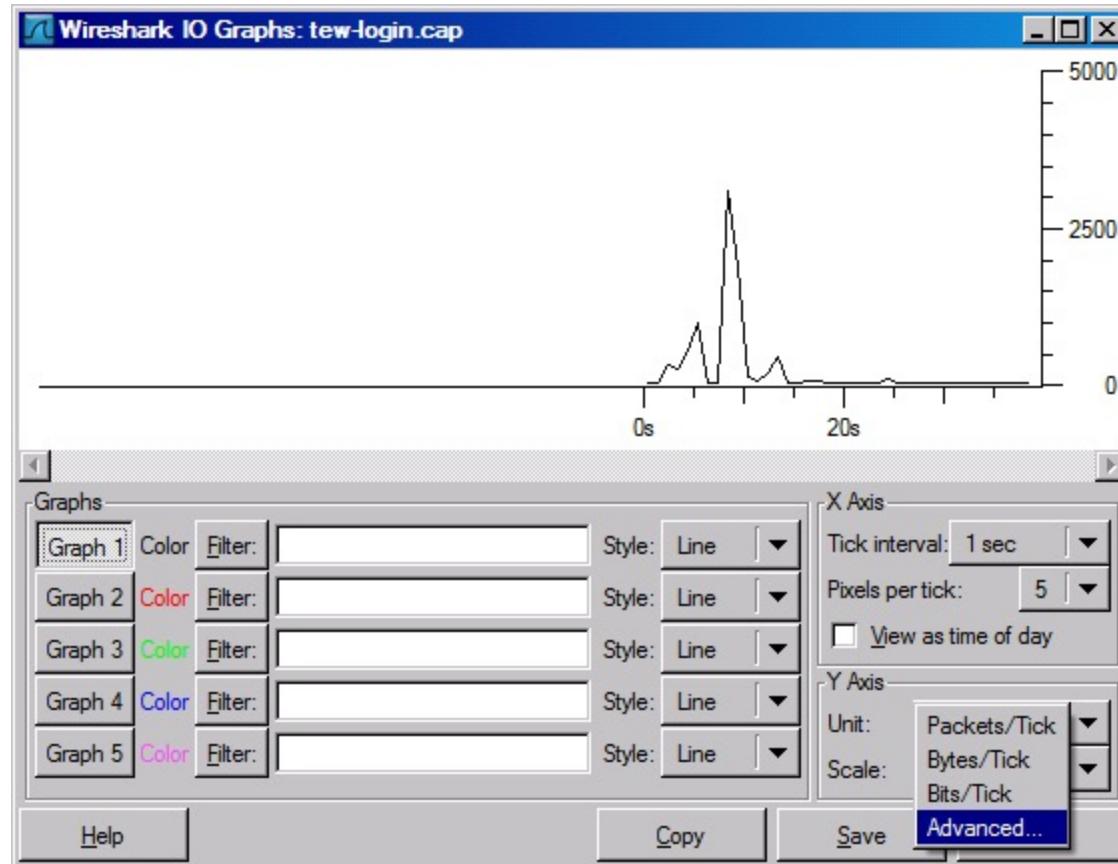
# IOGraphs



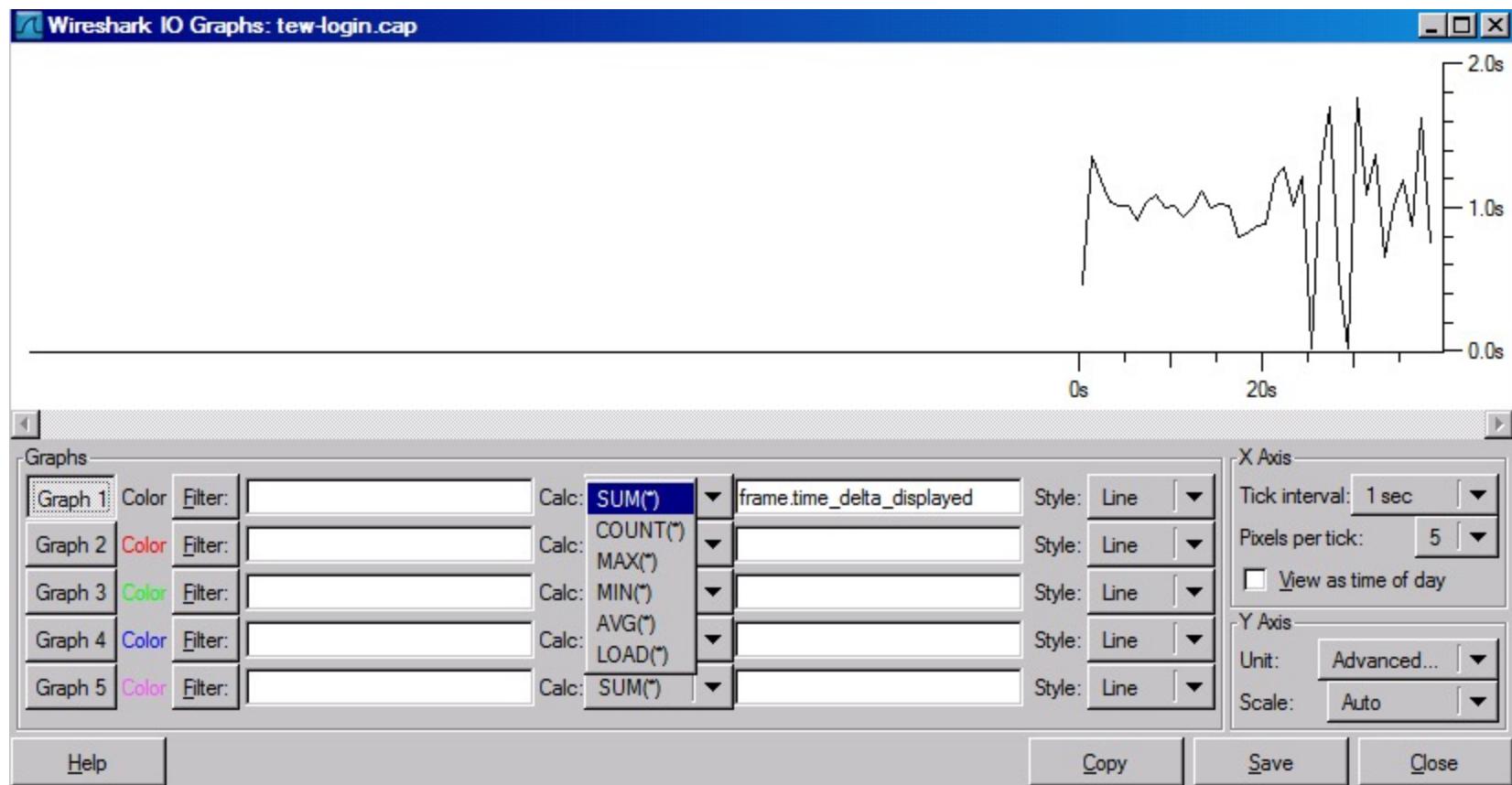
# IOGraphs



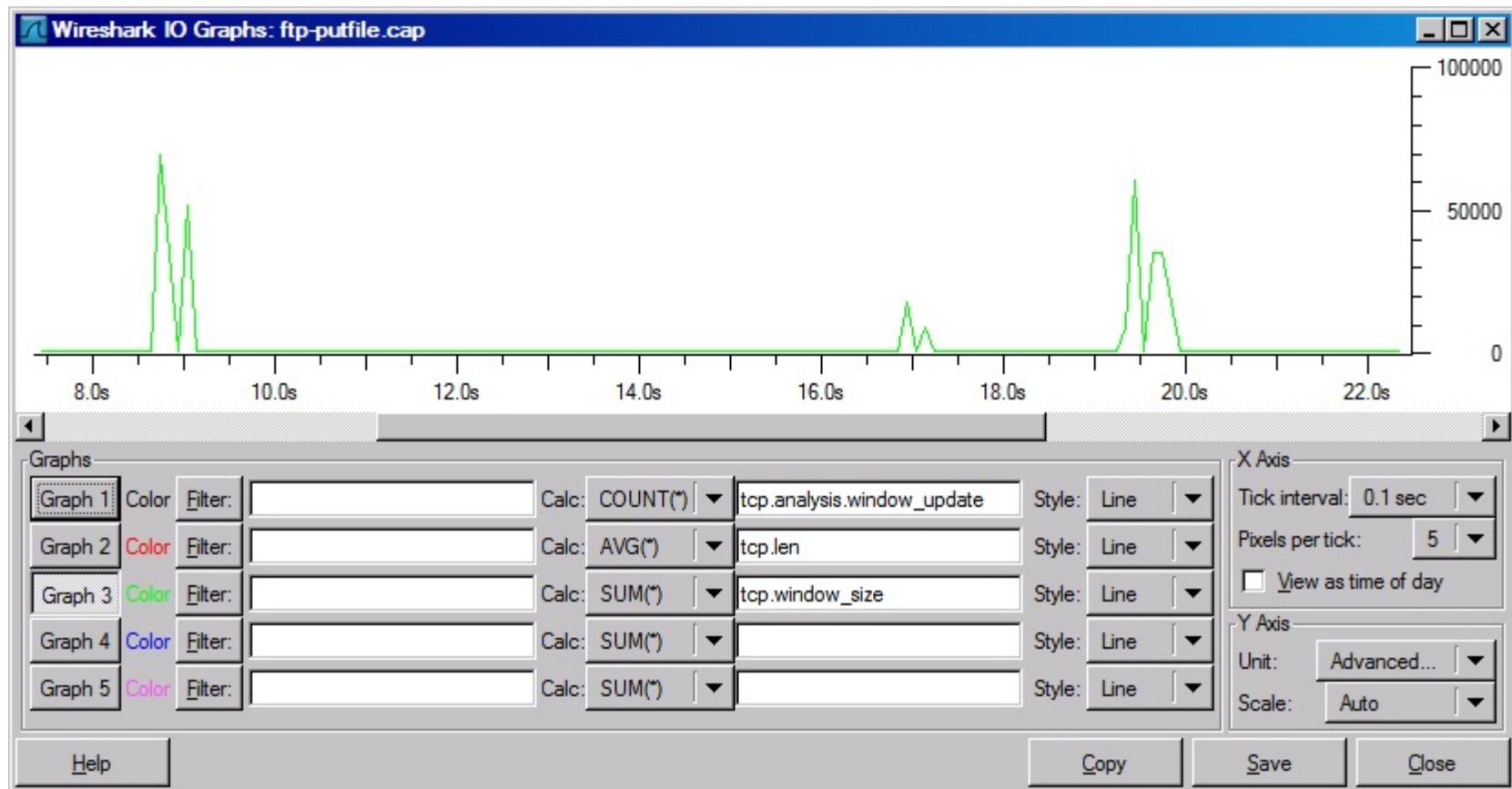
# IOGraphs



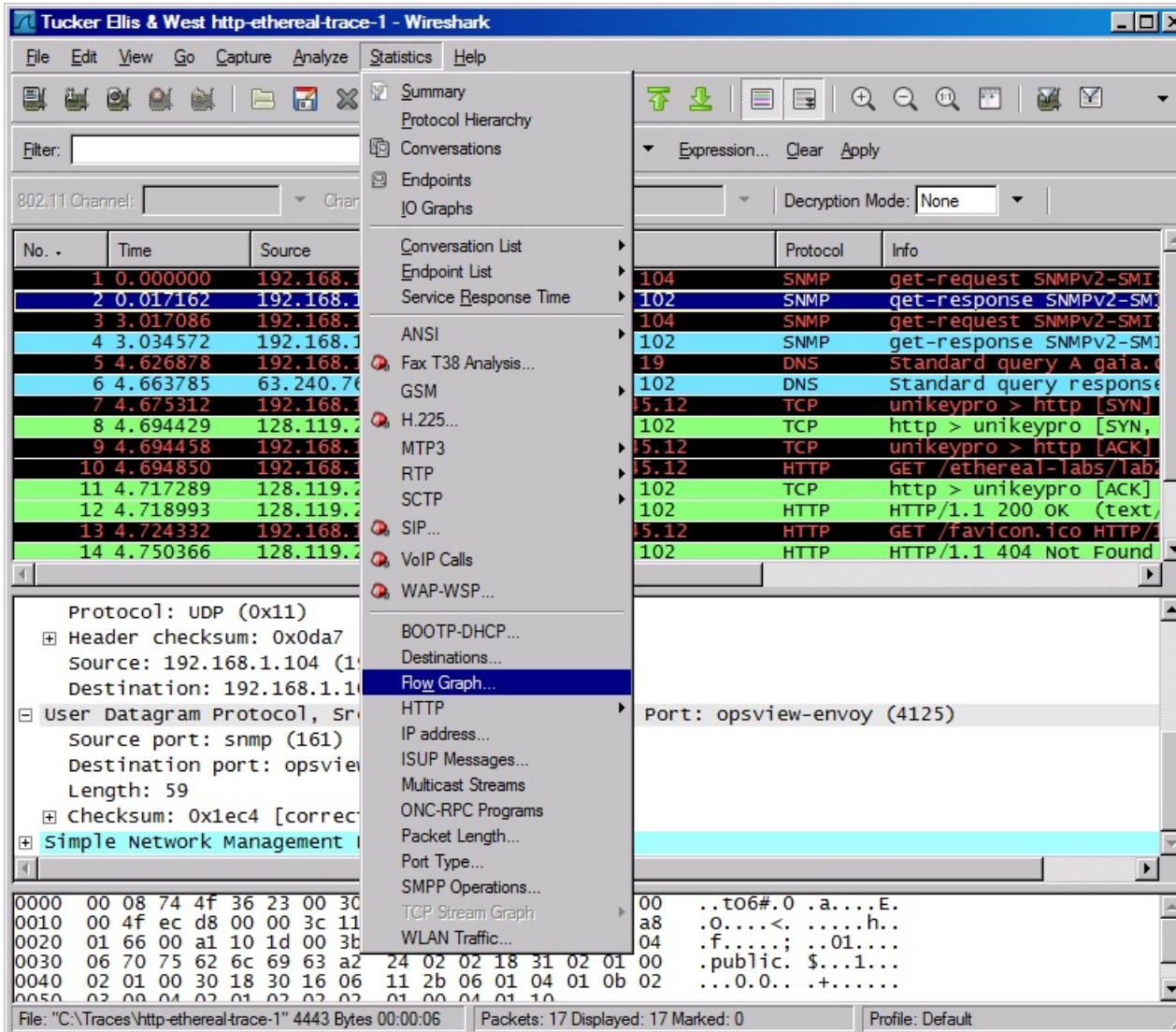
# IOGraphs



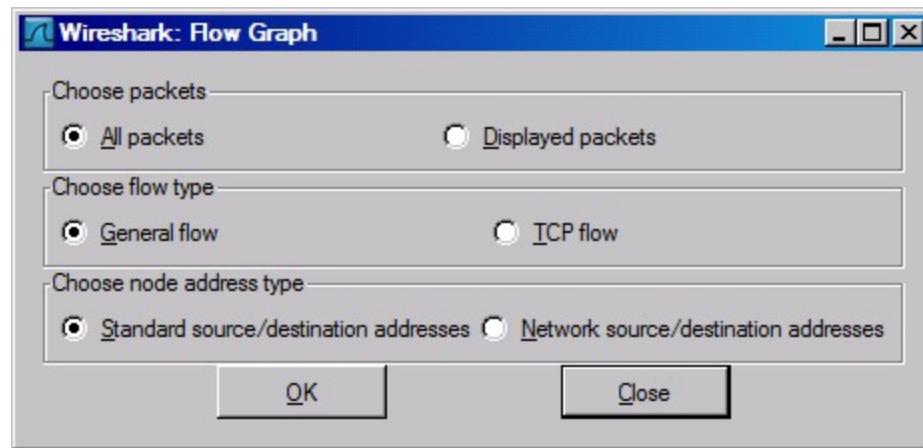
# IOGraphs



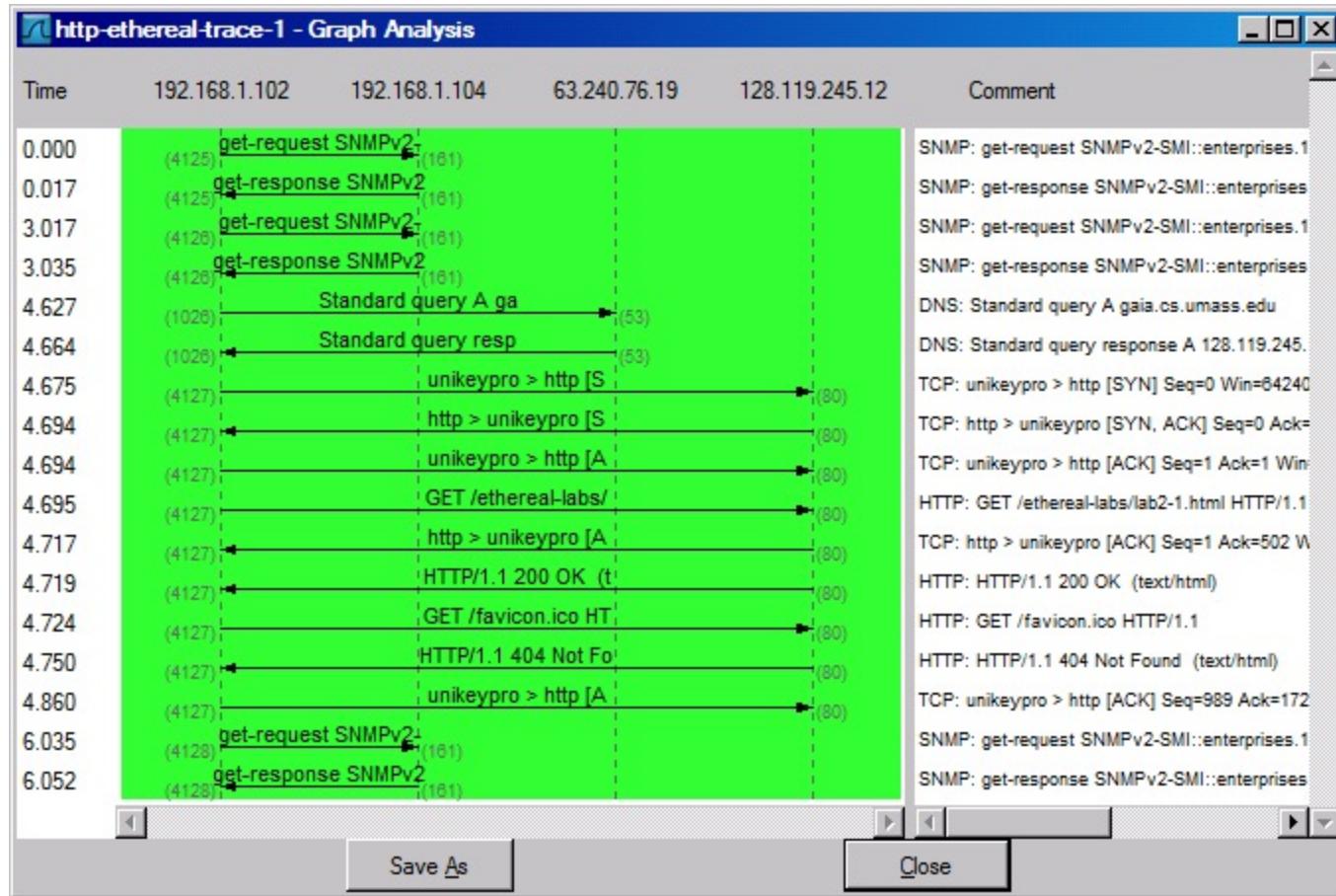
# Flow Graphs



# Flow Graphs



# Flow Graphs



# Right Click Filtering

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

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	get-request SNMPV2-SMI
2	0.017162	192.168.1.104	192.168.1.102	SNMP	get-response SNMPV2-SMI
3	3.017086	192.168.1.102	192.168.1.104	SNMP	get-request SNMPV2-SMI
4	3.034572	192.168.1.104	192.168.1.102	SNMP	get-response SNMPV2-SMI
5	4.626878	192.168.1.102	63.240.76.19	DNS	Standard query A gaia.o
6	4.663785	63.240.76.19	192.168.1.102	DNS	Standard query response
7	4.675312	192.168.1.102	128.119.245.12	TCP	unikeypro > http [SYN]
8	4.694429	128.119.245.12	192.168.1.102	TCP	http > unikeypro [SYN,
9	4.694458	192.168.1.102	128.119.245.12	TCP	unikeypro > http [ACK]
10	4.694850	192.168.1.102	128.119.245.12	HTTP	GET /ethereal-labs/lab2
11	4.717289	128.119.245.12	192.168.1.102	TCP	http > unikeypro [ACK]
12	4.718993	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 200 OK (text/
13	4.724332	192.168.1.102	128.119.245.12	HTTP	GET /favicon.ico HTTP/1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	HTTP/1.1 404 Not Found

Source port: unikeypro (4127)  
Destination port: http (80)  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 502 (relative sequence number)  
Acknowledgement number: 1 (relative ack number)  
Header length: 20 bytes  
Flags: 0x18 (PSH, ACK)  
0... .... = Congestion Window Reduced (CWR):  
.0... .... = ECN-Echo: Not set  
.00.... = Urgent: Not set

0020 f5 0c 10 1f 00 50 f5 32 64 b2 6b a6 54 92 50  
0030 fa f0 39 a2 00 00 47 45 54 20 2f 65 74 68 69  
0040 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 32 2d 3c  
0050 68 74 6d 2c 48 54 54 50 2f 31 2e 31 0d 0c  
0060 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 60  
0070 72 72 20 65 61 75 0d 0a 55 72 65 72 2d 41 60

Destination Port (tcp.dstport), 2 bytes | Packets: 17 Display

Expand Subtrees  
Expand All  
Collapse All  
Apply as Filter  
Prepare a Filter Selected  
Colorize with Filter  
Follow TCP Stream  
Follow UDP Stream  
Follow SSL Stream  
Copy  
Export Selected Packet Bytes...  
Wiki Protocol Page  
Filter Field Reference  
Protocol Preferences...  
Default  
Decode As...  
Disable Protocol...  
Resolve Name  
Go to Corresponding Packet

# Export HTTP

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

File Edit View Go Capture Analyze Statistics Help

Open... Ctrl+O  
Open Recent  
Merge...  
Close Ctrl+W  
Save Ctrl+S  
Save As... Shift+Ctrl+S  
File Set  
Export File... .168.1.104 SNMP get-request SNMPv2-SMI  
Selected Packet Bytes... Ctrl+H .168.1.102 SNMP get-response SNMPv2-SMI  
Print... Ctrl+P Objects HTTP 102 DNS Standard query A gaia.d  
Quit Ctrl+Q 168.1.102 128.119.245.12 TCP unikeypro > http [SYN]  
119.245.12 192.168.1.102 TCP http > unikeypro [SYN,  
9 4.694458 192.168.1.102 128.119.245.12 TCP unikeypro > http [ACK]  
10 4.694850 192.168.1.102 128.119.245.12 HTTP GET /ethereal-labs/lab2-1  
11 4.717289 128.119.245.12 192.168.1.102 TCP http > unikeypro [ACK]  
12 4.718993 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 200 OK (text/  
13 4.724332 192.168.1.102 128.119.245.12 HTTP GET /favicon.ico HTTP/  
14 4.750366 128.119.245.12 192.168.1.102 HTTP HTTP/1.1 404 Not Found

Source port: unikeypro (4127)  
Destination port: http (80)  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 502 (relative sequence number)]  
Acknowledgement number: 1 (relative ack number)  
Header length: 20 bytes  
Flags: 0x18 (PSH, ACK)  
0.... .... = Congestion window Reduced (CWR): Not set  
.0.... .... = ECN-Echo: Not set  
.0.... .... = Urgent: Not set

0020 f5 0c 10 1f 00 50 f5 32 64 b2 6b a6 54 92 50 18 ....P.2 d.k.T.P.  
0030 fa f0 39 a2 00 00 47 45 54 20 2f 65 74 68 65 72 ..9..GE T /ether  
0040 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 32 2d 31 2e eal-labs /lab2-1.  
0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1..H  
0060 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma  
0070 73 72 20 65 61 75 0d 07 55 72 65 72 2d 11 67 65 ee.edu User Agg

Destination Port (tcp.dstport), 2 bytes Packets: 17 Displayed: 17 Marked: 0 Profile: Default

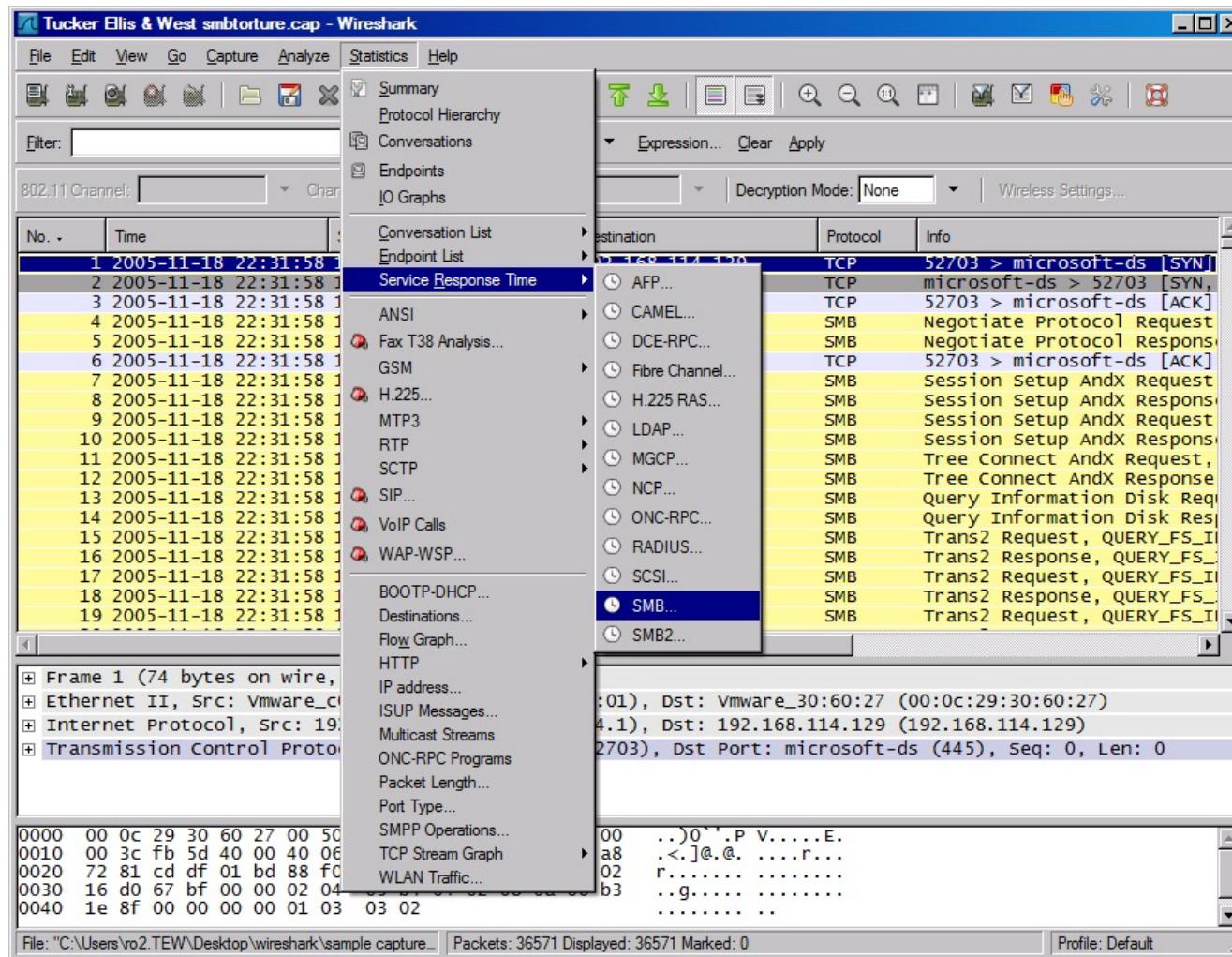
# Export HTTP Objects

Wireshark: HTTP object list

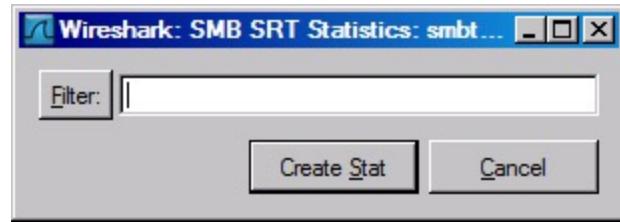
Packet num	Hostname	Content Type	Bytes	Filename
22	www.wireshark.org	application/x-javascript	1000	common.js
28	www.wireshark.org	image/png	137	clear.png
32	www.wireshark.org	application/x-javascript	5141	menu.js
41	www.wireshark.org	image/png	156	nav.bg.png
52	www.wireshark.org	application/x-javascript	1048	mirrors.js
70	www.wireshark.org	application/x-javascript	1213	downloads-1.0.2.js
119	www.wireshark.org	image/png	46317	banner.png
129	s9.addthis.com	image/gif	1505	button1-share.gif
137	s7.addthis.com	application/x-javascript	11373	addthis_widget.js
144	s7.addthis.com	text/css	811	addthis_widget.css
147	www.wireshark.org	image/png	798	feed16.png
159	s7.addthis.com	image/gif	924	addthis-mini.gif

Help      Close      Save As      Save All

# Service Response Time - SMB



# Service Response Time - SMB



# Service Response Time - SMB

SMB Service Response Time statistics: smbture.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

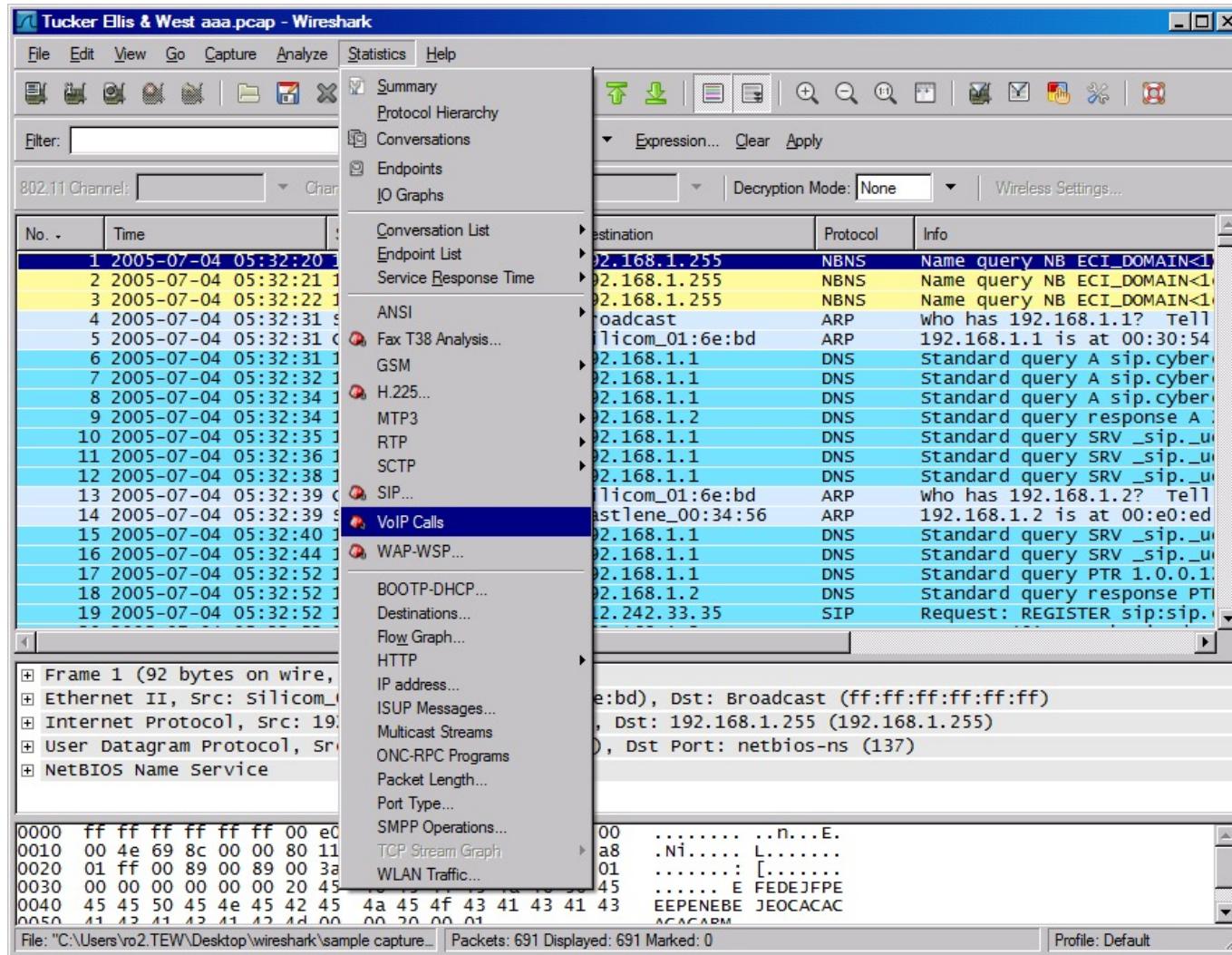
Index	Procedure	Calls ^	Min SRT	Max SRT	Avg SRT
2	FIND_NEXT2	240	0.00098	0.03823	0.00245
5	QUERY_PATH_INFO	200	0.00030	0.02970	0.00176
1	FIND_FIRST2	183	0.00087	0.04908	0.00330
7	QUERY_FILE_INFO	152	0.00030	0.04077	0.00187
8	SET_FILE_INFO	90	0.00019	0.26765	0.00548
6	SET_PATH_INFO	35	0.00031	0.02258	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



# VOIP Calls

aaa.pcap - VoIP Calls

Detected 4 VoIP Calls. Selected 0 Calls.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
508.349	575.439	192.168.1.2	sip:816666@voip.brujula.net	sip:97239287044@voip.brujula.net	SIP	18	CANCELLED	
692.955	727.341	192.168.1.2	sip:voi18062@sip.cybercity.dk	sip:0097239287044@sip.cybercity.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.cap - VoIP Calls

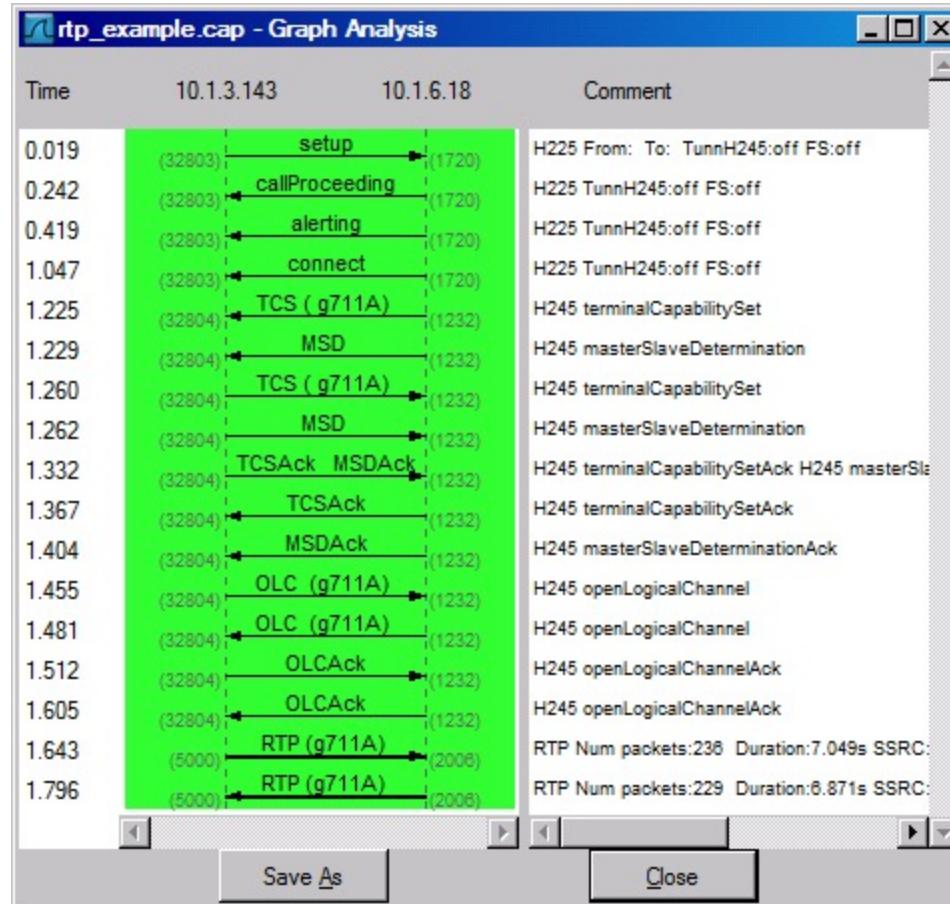
Detected 1 VoIP Call. Selected 1 Call.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
0.019	1.046	10.1.3.143			H.323	28	IN CALL	Tunneling: OFF Fast Start: OFF

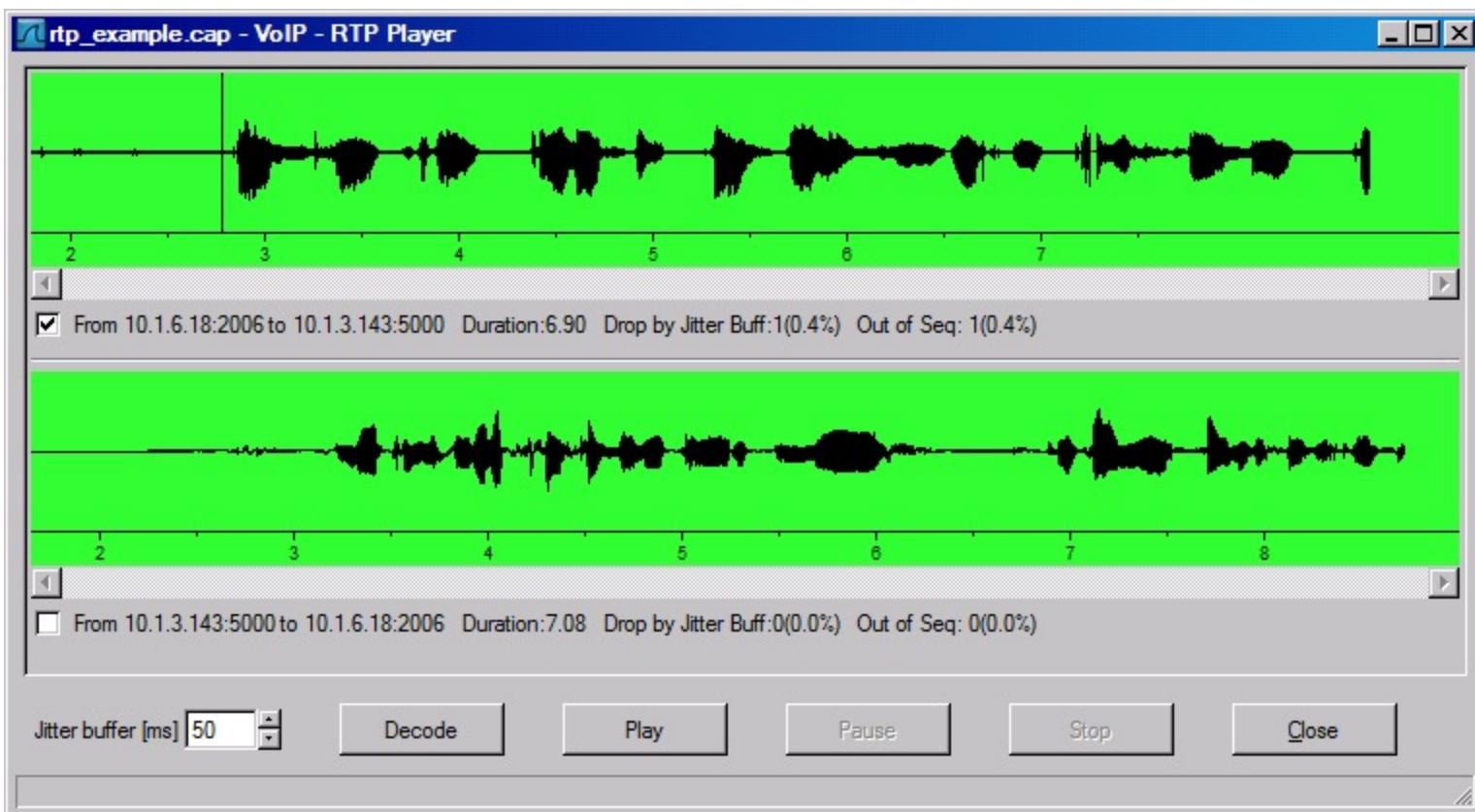
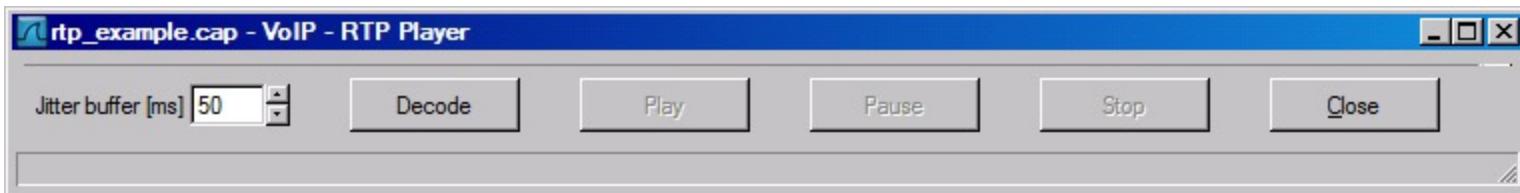
Total: Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 0

Prepare Filter Graph Player Select All Close

# VOIP Call Graph



# VOIP RTP Player



# SIP Analysis

Tucker Ellis & West aaa.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: [ ]

802.11 Channel: [ ] | Char

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

Expression... Clear Apply

Decryption Mode: None | Wireless Settings...

Conversation List

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
astlenet_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 PTR
12.242.33.35	SIP	Request: REGISTER sip:sip.

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, 92 bytes captured) at 0:0:0:0 (0.000000 - 0.000000 seconds) on wire (144 bits, 18 bytes) at interface "Silicom\_01:6e:bd" (Intel PRO/100 MT Desktop Adapter) (eth0)

Ethernet II, Src: Silicom\_01:6e:bd (00:4e:69:8c:00:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

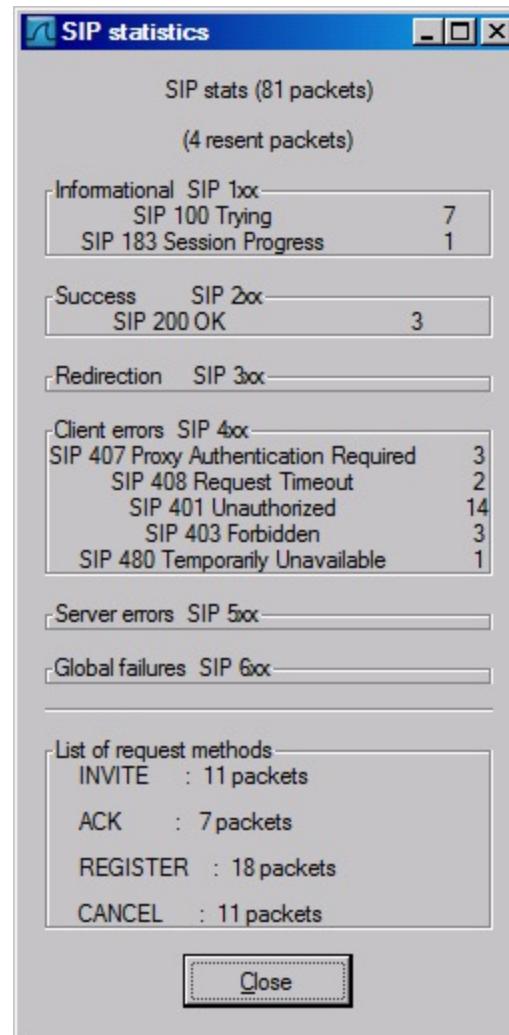
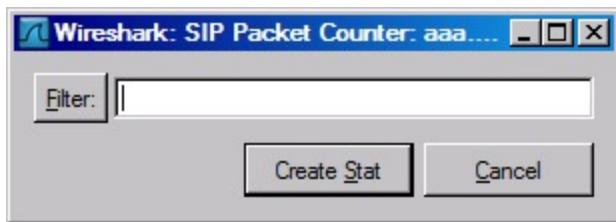
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.255 (192.168.1.255)

User Datagram Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: Port: netbios-ns (137)

NetBIOS Name Service

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

# SIP Analysis



# HTTP Analysis

Tucker Ellis & West internet-capture-113pm-07242008.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: [ ]

802.11 Channel: [ ] Channel

No. Time: 1 2008-07-24 13:12:59.121000 2 2008-07-24 13:12:59.121000 3 2008-07-24 13:12:59.121000 4 2008-07-24 13:12:59.121000 5 2008-07-24 13:12:59.121000 6 2008-07-24 13:12:59.121000 7 2008-07-24 13:12:59.121000 8 2008-07-24 13:12:59.121000 9 2008-07-24 13:12:59.121000 10 2008-07-24 13:12:59.121000 11 2008-07-24 13:12:59.121000 12 2008-07-24 13:12:59.121000 13 2008-07-24 13:12:59.121000 14 2008-07-24 13:12:59.121000 15 2008-07-24 13:12:59.121000 16 2008-07-24 13:12:59.121000 17 2008-07-24 13:12:59.121000 18 2008-07-24 13:12:59.121000 19 2008-07-24 13:12:59.121000

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...

Expression... Clear Apply Decryption Mode: None Wireless Settings...

Destination	Protocol	Info
1.1.15.104	HTTP	Continuation or non-HTTP t
08.117.254.150	TCP	acc-raid > http [ACK] Seq=
04.2.184.130	HTTP	GET /p/s/sm_vrt_3thumb_scri
0.1.15.104	HTTP	Continuation or non-HTTP ti
0.1.15.104	HTTP	Continuation or non-HTTP ti
08.117.254.150	TCP	acc-raid > http [ACK] Seq=
09.166.161.121	DNS	Standard query A a632.g.ak
0.1.15.104	HTTP	Continuation or non-HTTP ti
0.1.15.104	HTTP	Continuation or non-HTTP ti
08.117.254.150	TCP	acc-raid > http [ACK] Seq=
23.58.126	HTTP	GET /customer/advance/9/.ol
23.58.126	HTTP	GET /customer/advance/9/.ol
0.1.15.104	HTTP	Continuation or non-HTTP ti
0.1.11.13	DNS	Standard query response CN
0.180.195.70	TCP	mcs-calypsoicf > http [SYN]
0.1.12.67	HTTP	Continuation or non-HTTP ti
0.2.101.36	TCP	3325 > http [ACK] Seq=1 Ac
0.1.12.67	HTTP	[TCP out-of-order] Continu
0.2.101.36	TCP	3325 > http [ACK] Seq=1 Ac

Frame 1 (1514 bytes on wire (1211 bits), 1514 bytes captured (1211 bits), 13:12:59.121000 to 13:12:59.121000) [槍]

Ethernet II, Src: Cisco\_f7 (08:00:00:00:00:f7) [槍]

Internet Protocol Version 4, Src: 20.1.15.104 (20.1.15.104) [槍]

Transmission Control Protocol [槍]

Hypertext Transfer Protocol [槍]

0000 00 15 c7 46 80 00 00 03

0010 05 dc 36 ab 40 00 3b 06

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 c8 b8 0f 8e cb b4 85 4d

0060 51 00 7c 72 f7 ff 00 04

File: "C:\Users\vo2.TEW\Desktop\wireshark\sample capture..." Packets: 16612 Displayed: 16612 Marked: 0 Profile: Default

# HTTP Analysis – Load Distribution

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

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

 **HTTP/Requests**

Topic / Item

- ⊖ HTTP Requests by HTTP Host
  - + [img.video.ap.org](#)
  - + [mi.adinterax.com](#)
  - + [blog.cleveland.com](#)
  - + [tr.adinterax.com](#)
  - ⊖ [money.cleveland.com](#)
    - [/dynamic/proxy-partial.js/ibd.morningstar.com/AP/MarketIndexGraph.html?!](#)
  - ⊖ [www.cleveland.com](#)
    - [/images/hp/video.gif](#)
    - [/sports/graphics/audio\\_blue.gif](#)
    - [/sports/graphics/gallery.gif](#)
    - [/sports/graphics/comment.gif](#)
    - [/images/hp/80/jackson.jpg](#)
    - [/images/hp/80/coupons\\_80.jpg](#)
    - [/images/hp/110/crime\\_scene.jpg](#)
    - [/images/hp/110/gavel.jpg](#)
    - [/images/hp/110/cafeteria110.jpg](#)
    - [/images/hp/110/blake0901ap.jpg](#)

# Password Hacking Demo

