WIRESHARK

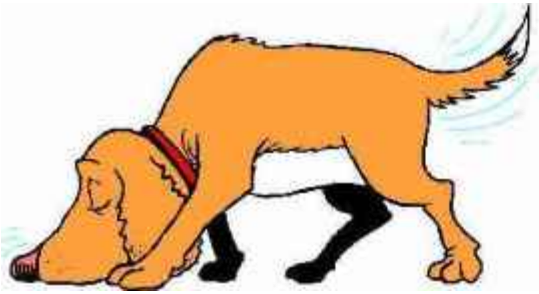
Drinking straight from the network hose

So What is WireShark?

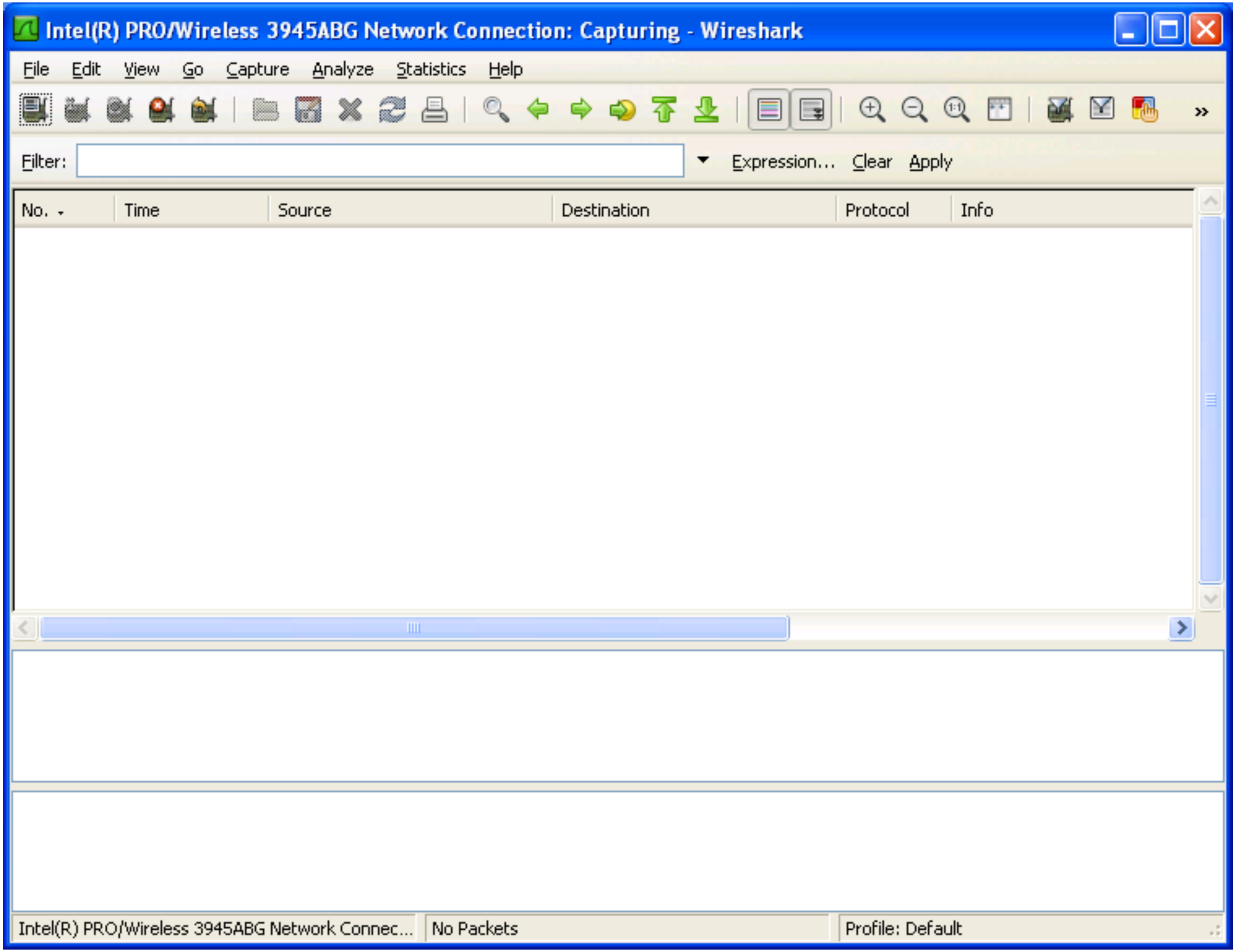
- Packet sniffer/protocol analyzer
- Open Source Network Tool
- Latest version of the ethereal tool

Stuff we won’t cover

- What’s a network?
- What’s an IP address?
- What’s a MAC address?
- What’s a router?
- What do you mean capture?
- Can this make Elite run faster?
- What’s open source?
- How can one man look so bald?



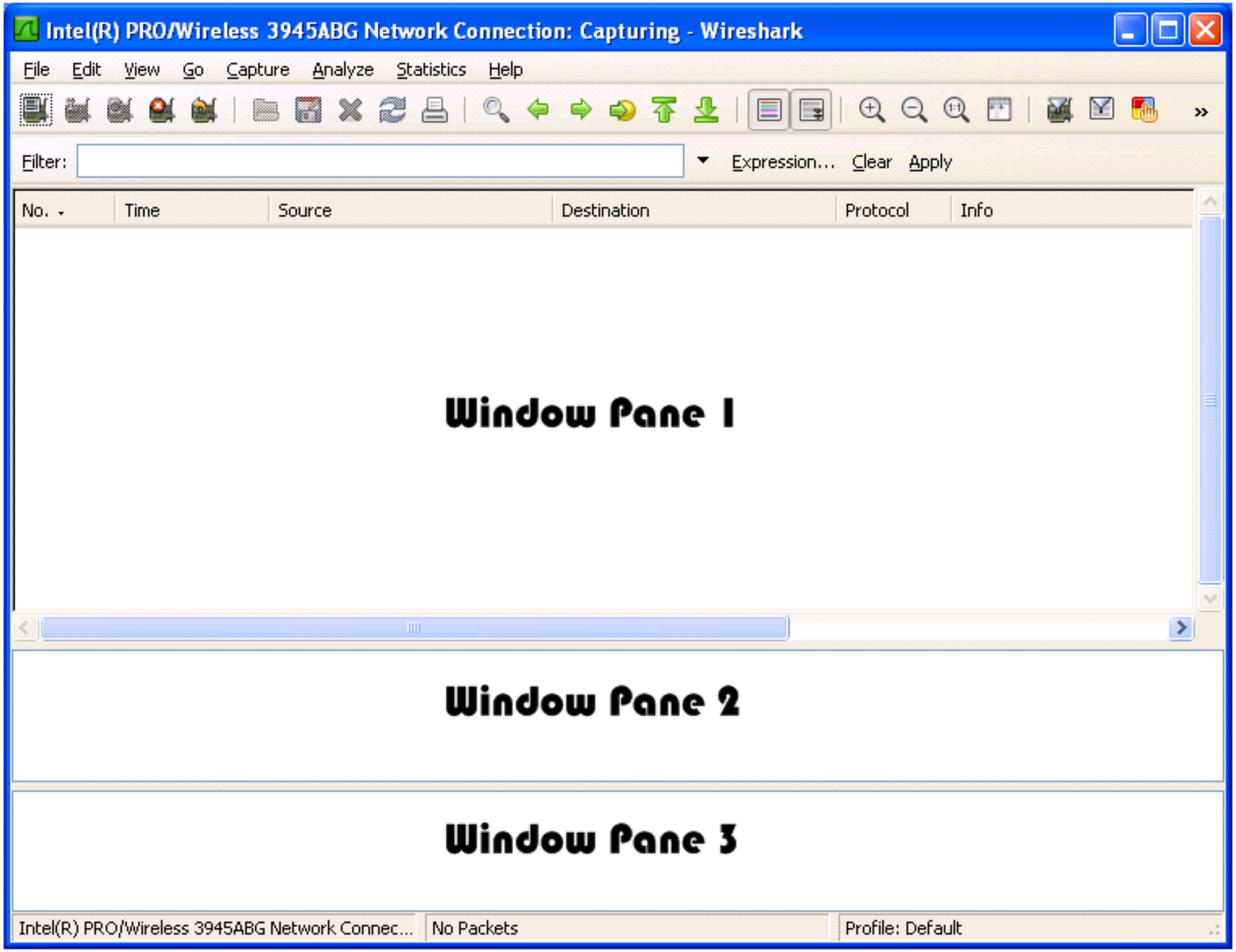
0010100100101011101010101



Intel(R) PRO/Wireless 3945ABG Network Connection: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info

Intel(R) PRO/Wireless 3945ABG Network Connec... No Packets Profile: Default

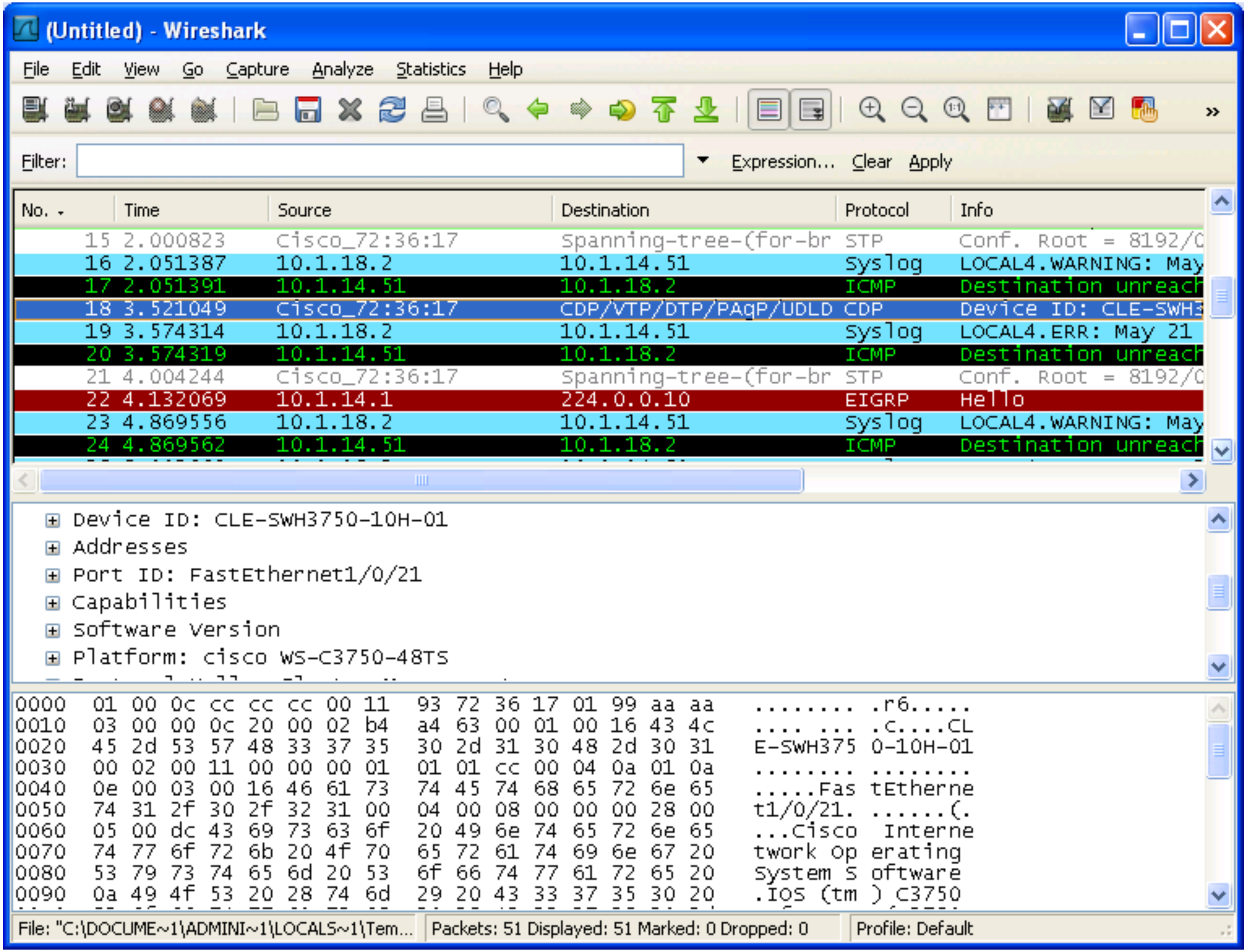


Window Pane 1

Window Pane 2

Window Pane 3

With traffic…



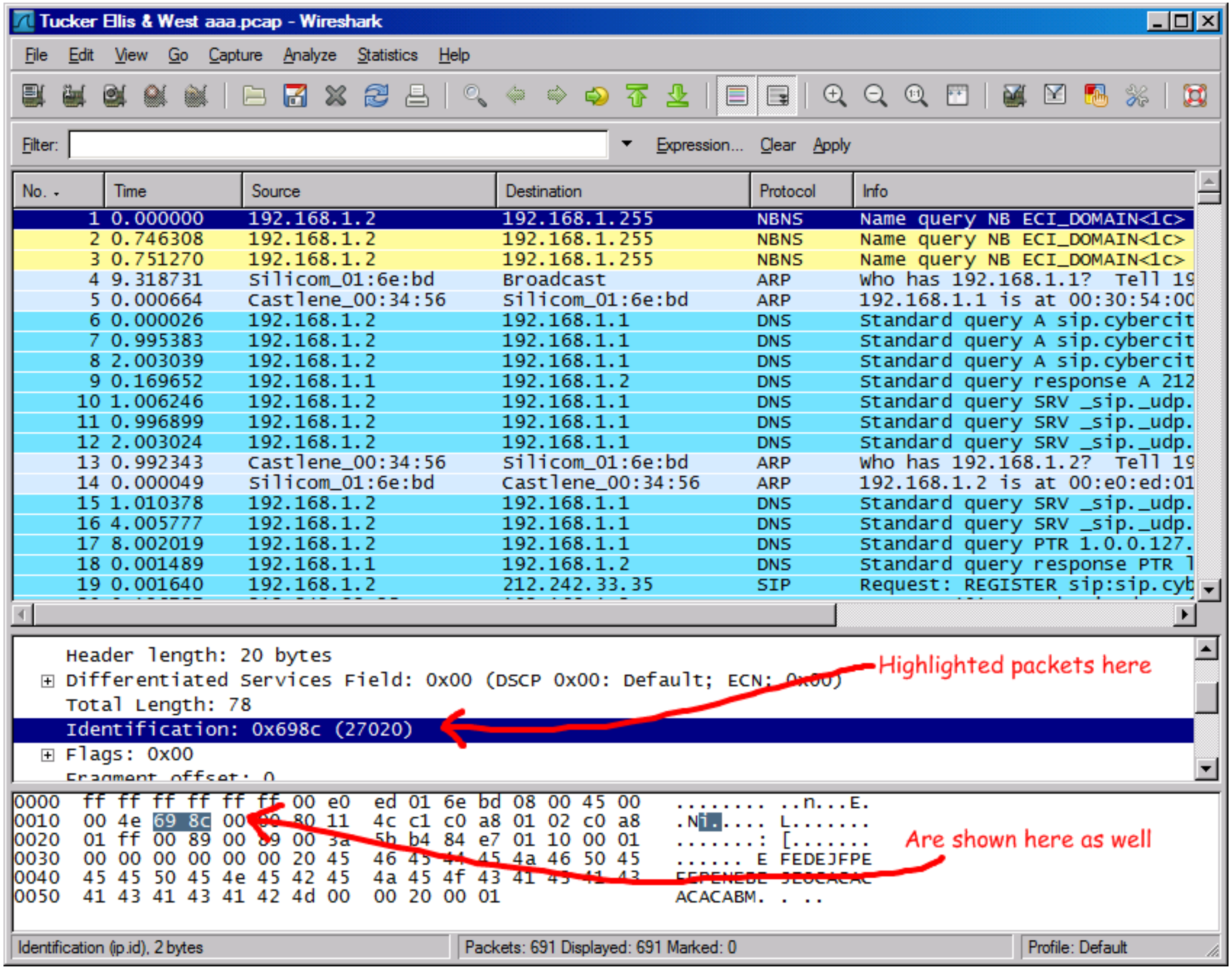
```
No. .  Time       Source          Destination             Protocol  Info
    15 2.000823   Cisco_72:36:17  Spanning-tree-(for-br   STP       Conf. Root = 8192/0
    16 2.051387   10.1.18.2       10.1.14.51              Syslog    LOCAL4.WARNING: May
    17 2.051391   10.1.14.51      10.1.18.2               ICMP      Destination unreach
    18 3.521049   Cisco_72:36:17  CDP/VTP/DTP/PAgP/UDLD   CDP       Device ID: CLE-SWH3
    19 3.574314   10.1.18.2       10.1.14.51              Syslog    LOCAL4.ERR: May 21
    20 3.574319   10.1.14.51      10.1.18.2               ICMP      Destination unreach
    21 4.004244   Cisco_72:36:17  Spanning-tree-(for-br   STP       Conf. Root = 8192/0
    22 4.132069   10.1.14.1       224.0.0.10              EIGRP     Hello
    23 4.869556   10.1.18.2       10.1.14.51              Syslog    LOCAL4.WARNING: May
    24 4.869562   10.1.14.51      10.1.18.2               ICMP      Destination unreach
```

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

```
0000  01 00 0c cc cc cc 00 11  93 72 36 17 01 99 aa aa   ........ .r6.....
0010  03 00 00 0c 20 00 02 b4  a4 63 00 01 00 16 43 4c   .... ... .c....CL
0020  45 2d 53 57 48 33 37 35  30 2d 31 30 48 2d 30 31   E-SWH375 0-10H-01
0030  00 02 00 11 00 00 00 01  01 01 cc 00 04 0a 01 0a   ........ ........
0040  0e 00 03 00 16 46 61 73  74 45 74 68 65 72 6e 65   .....Fas tEtherne
0050  74 31 2f 30 2f 32 31 00  04 00 08 00 00 00 28 00   t1/0/21. ......(.
0060  05 00 dc 43 69 73 63 6f  20 49 6e 74 65 72 6e 65   ...Cisco  Interne
0070  74 77 6f 72 6b 20 4f 70  65 72 61 74 69 6e 67 20   twork Op erating
0080  53 79 73 74 65 6d 20 53  6f 66 74 77 61 72 65 20   System S oftware
0090  0a 49 4f 53 20 28 74 6d  29 20 43 33 37 35 30 20   .IOS (tm ) C3750
```

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

HEX Window



```
No. -  Time        Source               Destination          Protocol  Info
    1 0.000000    192.168.1.2          192.168.1.255        NBNS      Name query NB ECI_DOMAIN<1c>
    2 0.746308    192.168.1.2          192.168.1.255        NBNS      Name query NB ECI_DOMAIN<1c>
    3 0.751270    192.168.1.2          192.168.1.255        NBNS      Name query NB ECI_DOMAIN<1c>
    4 9.318731    Silicom_01:6e:bd     Broadcast            ARP       Who has 192.168.1.1?  Tell 19
    5 0.000664    Castlene_00:34:56    Silicom_01:6e:bd     ARP       192.168.1.1 is at 00:30:54:00
    6 0.000026    192.168.1.2          192.168.1.1          DNS       Standard query A sip.cybercit
    7 0.995383    192.168.1.2          192.168.1.1          DNS       Standard query A sip.cybercit
    8 2.003039    192.168.1.2          192.168.1.1          DNS       Standard query A sip.cybercit
    9 0.169652    192.168.1.1          192.168.1.2          DNS       Standard query response A 212
   10 1.006246    192.168.1.2          192.168.1.1          DNS       Standard query SRV _sip._udp.
   11 0.996899    192.168.1.2          192.168.1.1          DNS       Standard query SRV _sip._udp.
   12 2.003024    192.168.1.2          192.168.1.1          DNS       Standard query SRV _sip._udp.
   13 0.992343    Castlene_00:34:56    Silicom_01:6e:bd     ARP       Who has 192.168.1.2?  Tell 19
   14 0.000049    Silicom_01:6e:bd     Castlene_00:34:56    ARP       192.168.1.2 is at 00:e0:ed:01
   15 1.010378    192.168.1.2          192.168.1.1          DNS       Standard query SRV _sip._udp.
   16 4.005777    192.168.1.2          192.168.1.1          DNS       Standard query SRV _sip._udp.
   17 8.002019    192.168.1.2          192.168.1.1          DNS       Standard query PTR 1.0.0.127.
   18 0.001489    192.168.1.1          192.168.1.2          DNS       Standard query response PTR l
   19 0.001640    192.168.1.2          212.242.33.35        SIP       Request: REGISTER sip:sip.cyb
```

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

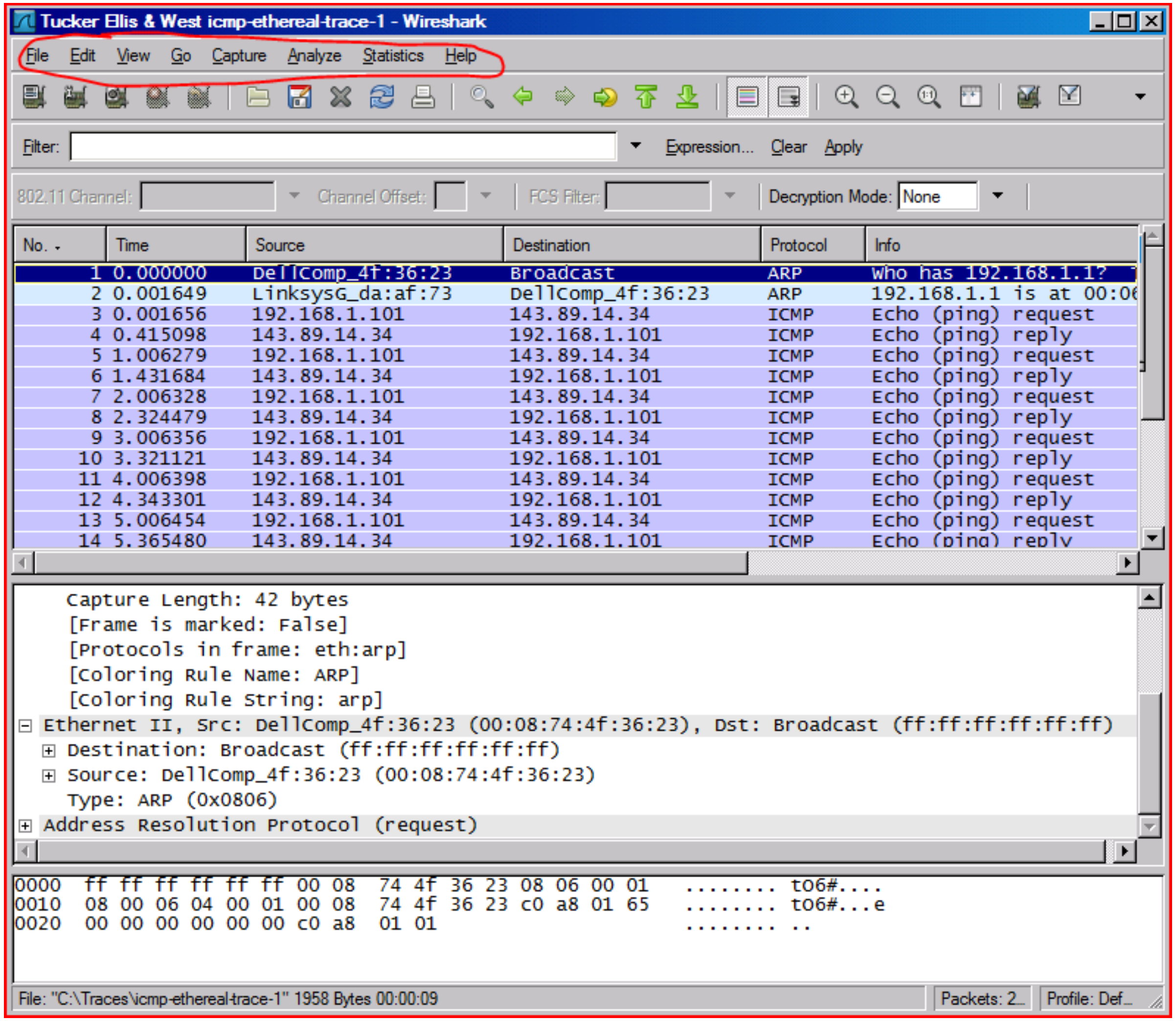
Highlighted packets here

```
0000  ff ff ff ff ff ff 00 e0  ed 01 6e bd 08 00 45 00   ........ ..n...E.
0010  00 4e 69 8c 00 00 80 11  4c c1 c0 a8 01 02 c0 a8   .Ni..... L.......
0020  01 ff 00 89 00 89 00 3a  5b b4 84 e7 01 10 00 01   .......: [.......
0030  00 00 00 00 00 00 20 45  46 45 44 45 4a 46 50 45   ...... E FEDEJFPE
0040  45 45 50 45 4e 45 42 45  4a 45 4f 43 41 43 41 43   EEPENEBE JEOCACAC
0050  41 43 41 43 41 42 4d 00  00 20 00 01               ACACABM. . ..
```

Are shown here as well

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

Menu Bar



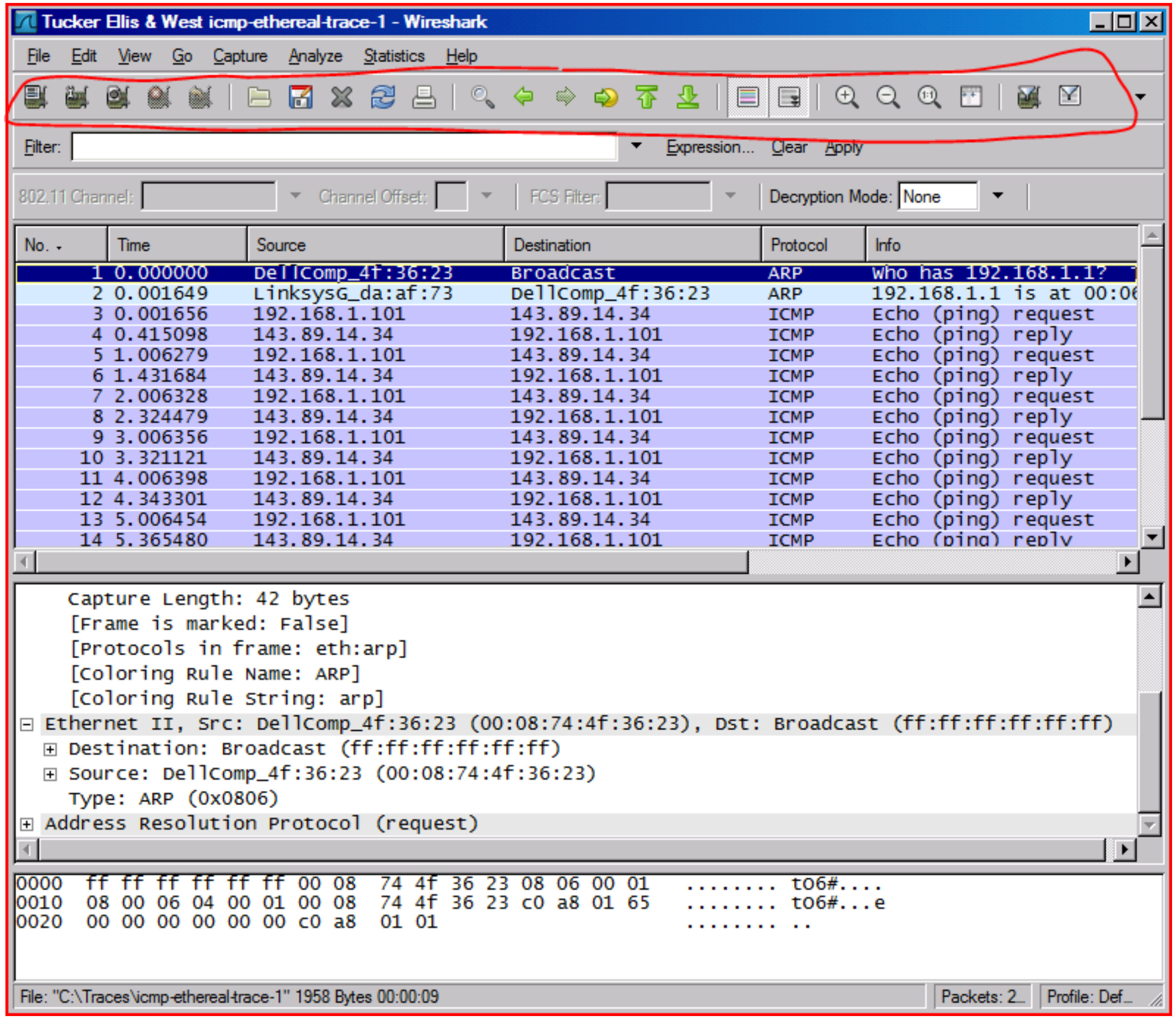
```
No. .  Time       Source              Destination         Protocol  Info
     1 0.000000   DellComp_4f:36:23   Broadcast           ARP       Who has 192.168.1.1?  T
     2 0.001649   LinksysG_da:af:73   DellComp_4f:36:23   ARP       192.168.1.1 is at 00:06
     3 0.001656   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
     4 0.415098   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
     5 1.006279   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
     6 1.431684   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
     7 2.006328   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
     8 2.324479   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
     9 3.006356   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
    10 3.321121   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
    11 4.006398   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
    12 4.343301   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
    13 5.006454   192.168.1.101       143.89.14.34        ICMP      Echo (ping) request
    14 5.365480   143.89.14.34        192.168.1.101       ICMP      Echo (ping) reply
```

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

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 06 00 01   ........ tO6#....
0010  08 00 06 04 00 01 00 08  74 4f 36 23 c0 a8 01 65   ........ tO6#...e
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

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

Button Bar



Decryption Mode: None

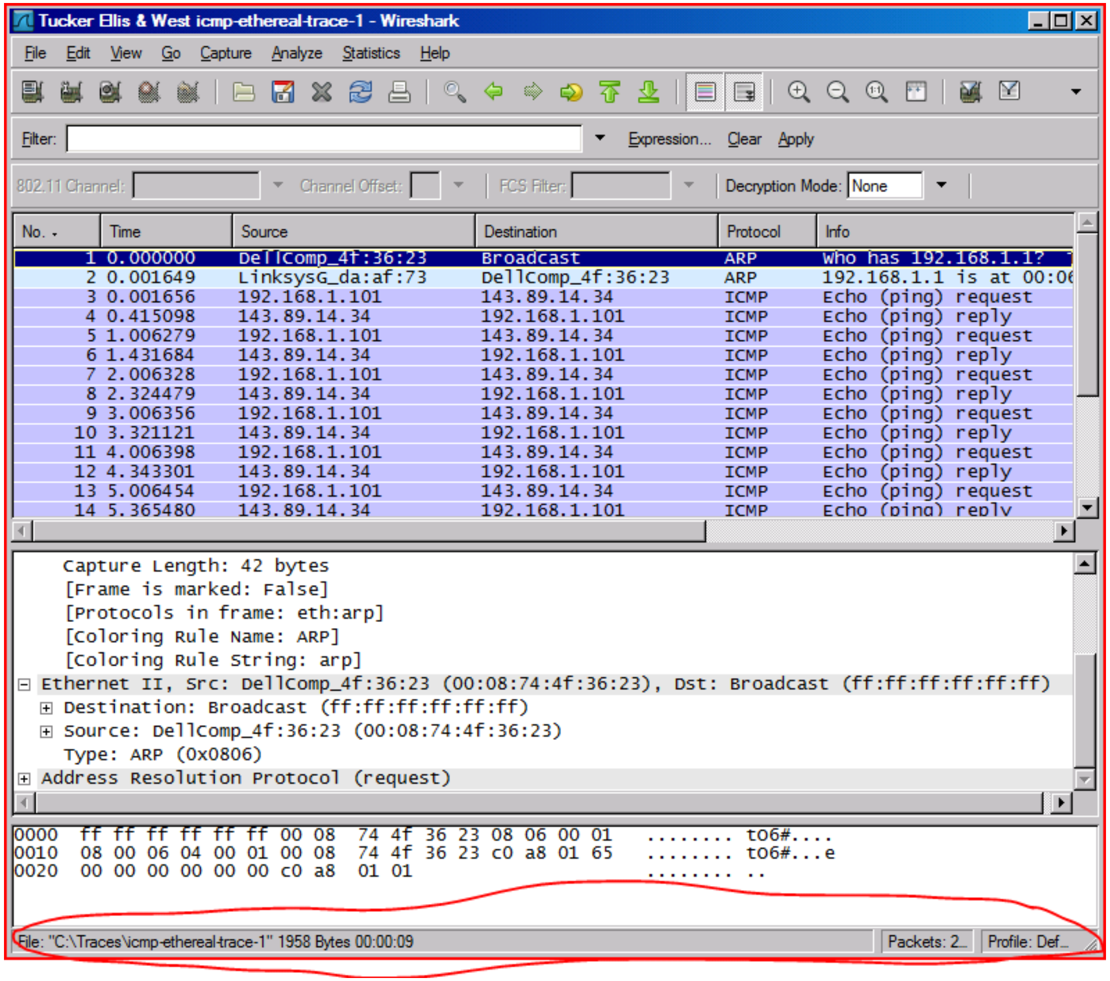
No.	Time	Source	Destination	Protocol	Info
1	0.000000	DellComp_4f:36:23	Broadcast	ARP	Who has 192.168.1.1?
2	0.001649	LinksysG_da:af:73	DellComp_4f:36:23	ARP	192.168.1.1 is at 00:06
3	0.001656	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
4	0.415098	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
5	1.006279	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
6	1.431684	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
7	2.006328	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
8	2.324479	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
9	3.006356	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
10	3.321121	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
11	4.006398	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
12	4.343301	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
13	5.006454	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
14	5.365480	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply

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

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 06 00 01   ........ tO6#....
0010  08 00 06 04 00 01 00 08  74 4f 36 23 c0 a8 01 65   ........ tO6#...e
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

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

Status Bar



Decryption Mode: None

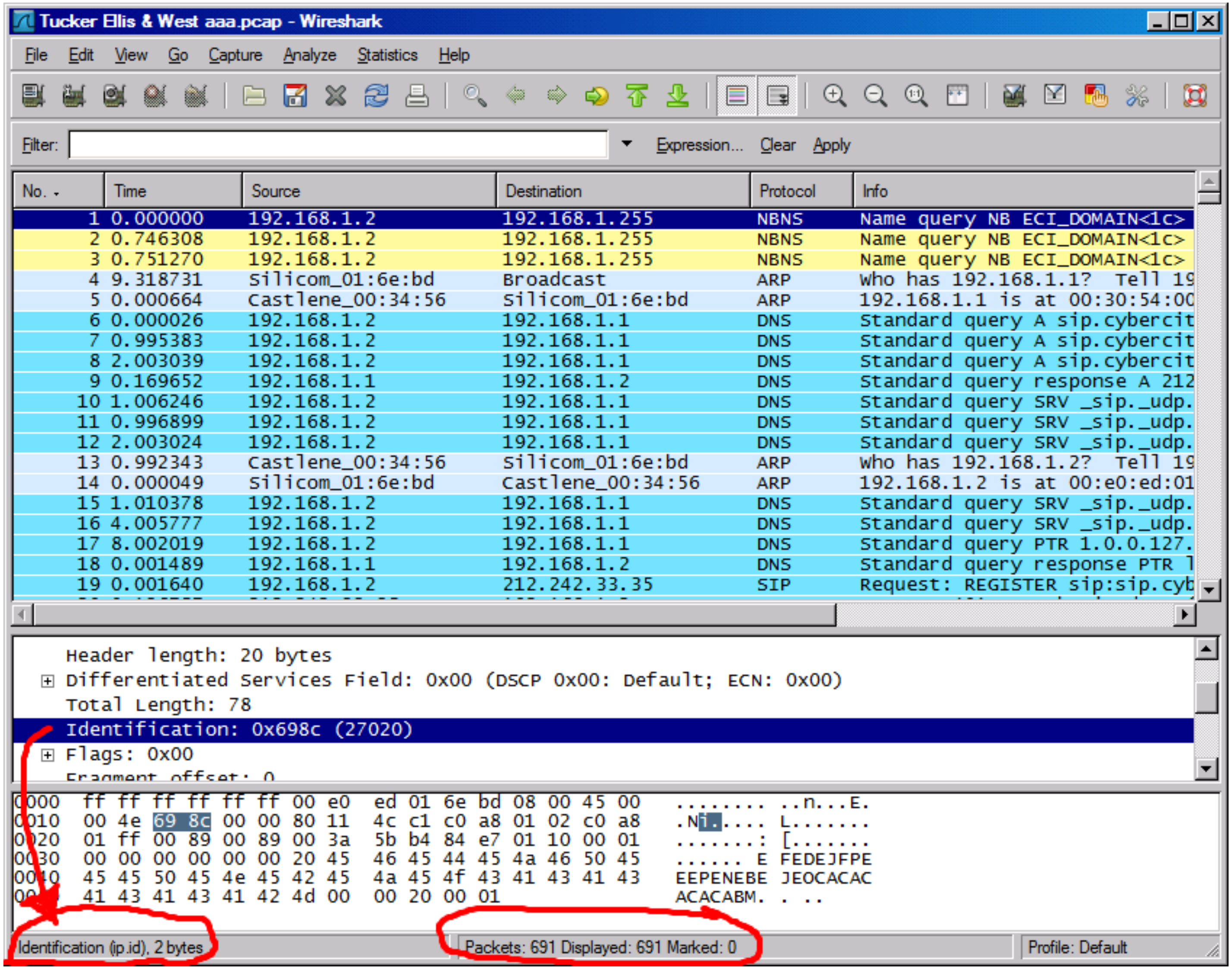
No.	Time	Source	Destination	Protocol	Info
1	0.000000	DellComp_4f:36:23	Broadcast	ARP	Who has 192.168.1.1?
2	0.001649	LinksysG_da:af:73	DellComp_4f:36:23	ARP	192.168.1.1 is at 00:06
3	0.001656	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
4	0.415098	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
5	1.006279	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
6	1.431684	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
7	2.006328	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
8	2.324479	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
9	3.006356	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
10	3.321121	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
11	4.006398	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
12	4.343301	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply
13	5.006454	192.168.1.101	143.89.14.34	ICMP	Echo (ping) request
14	5.365480	143.89.14.34	192.168.1.101	ICMP	Echo (ping) reply

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

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 06 00 01   ........ tO6#....
0010  08 00 06 04 00 01 00 08  74 4f 36 23 c0 a8 01 65   ........ tO6#...e
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

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

Status Bar



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
2	0.746308	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
3	0.751270	192.168.1.2	192.168.1.255	NBNS	Name query NB ECI_DOMAIN<1c>
4	9.318731	Silicom_01:6e:bd	Broadcast	ARP	Who has 192.168.1.1? Tell 19
5	0.000664	Castlene_00:34:56	Silicom_01:6e:bd	ARP	192.168.1.1 is at 00:30:54:00
6	0.000026	192.168.1.2	192.168.1.1	DNS	Standard query A sip.cybercit
7	0.995383	192.168.1.2	192.168.1.1	DNS	Standard query A sip.cybercit
8	2.003039	192.168.1.2	192.168.1.1	DNS	Standard query A sip.cybercit
9	0.169652	192.168.1.1	192.168.1.2	DNS	Standard query response A 212
10	1.006246	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.
11	0.996899	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.
12	2.003024	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.
13	0.992343	Castlene_00:34:56	Silicom_01:6e:bd	ARP	Who has 192.168.1.2? Tell 19
14	0.000049	Silicom_01:6e:bd	Castlene_00:34:56	ARP	192.168.1.2 is at 00:e0:ed:01
15	1.010378	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.
16	4.005777	192.168.1.2	192.168.1.1	DNS	Standard query SRV _sip._udp.
17	8.002019	192.168.1.2	192.168.1.1	DNS	Standard query PTR 1.0.0.127.
18	0.001489	192.168.1.1	192.168.1.2	DNS	Standard query response PTR l
19	0.001640	192.168.1.2	212.242.33.35	SIP	Request: REGISTER sip:sip.cyb

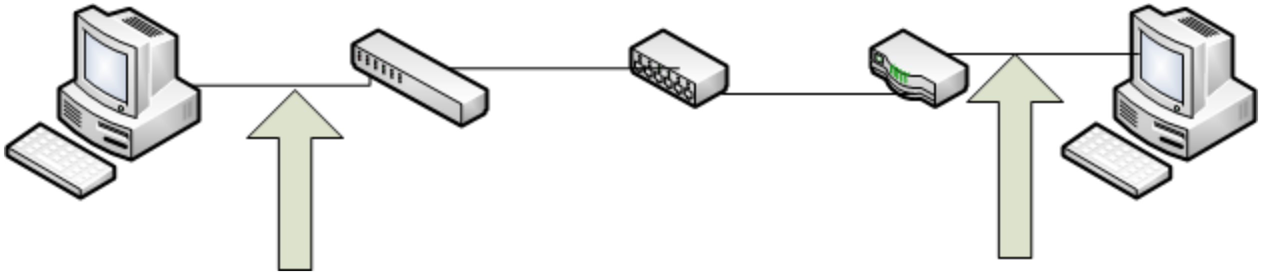
```
    Header length: 20 bytes
 ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 78
    Identification: 0x698c (27020)
 ⊞ Flags: 0x00
    Fragment offset: 0
```

```
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 89 00 3a  5b b4 84 e7 01 10 00 01   .......: [.......
0030  00 00 00 00 00 00 20 45  46 45 44 45 4a 46 50 45   ...... E FEDEJFPE
0040  45 45 50 45 4e 45 42 45  4a 45 4f 43 41 43 41 43   EEPENEBE JEOCACAC
0050  41 43 41 43 41 42 4d 00  00 20 00 01               ACACABM. . ..
```

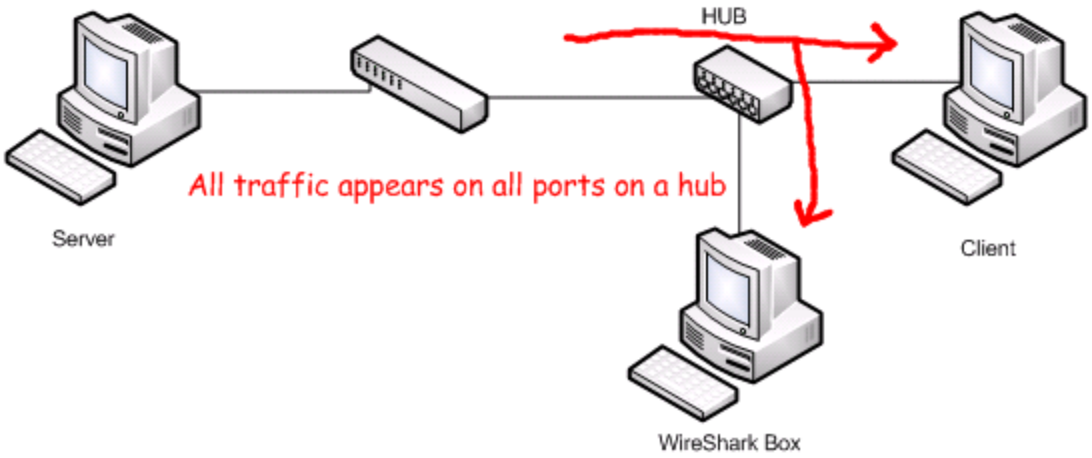
Identification (ip.id), 2 bytes | Packets: 691 Displayed: 691 Marked: 0 | Profile: Default

Where do I put WireShark?

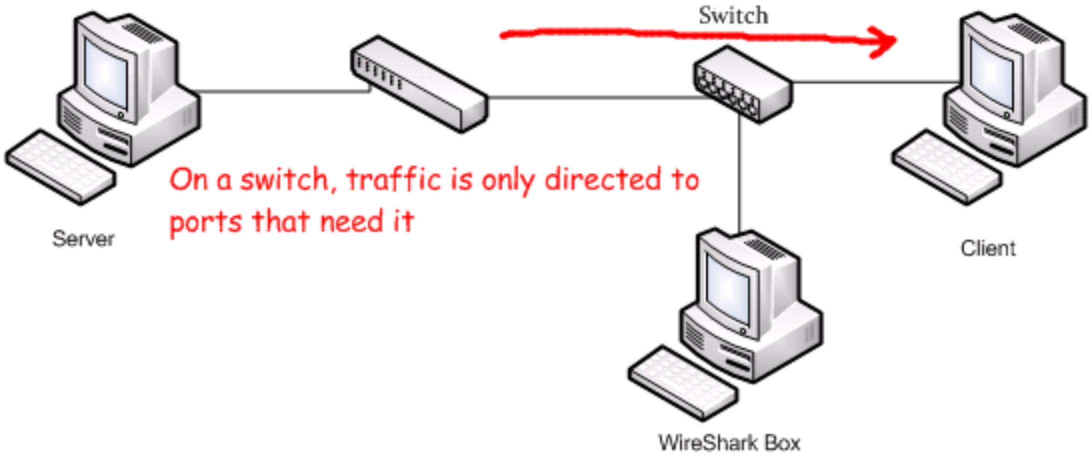
Location, Location, Location



Hub

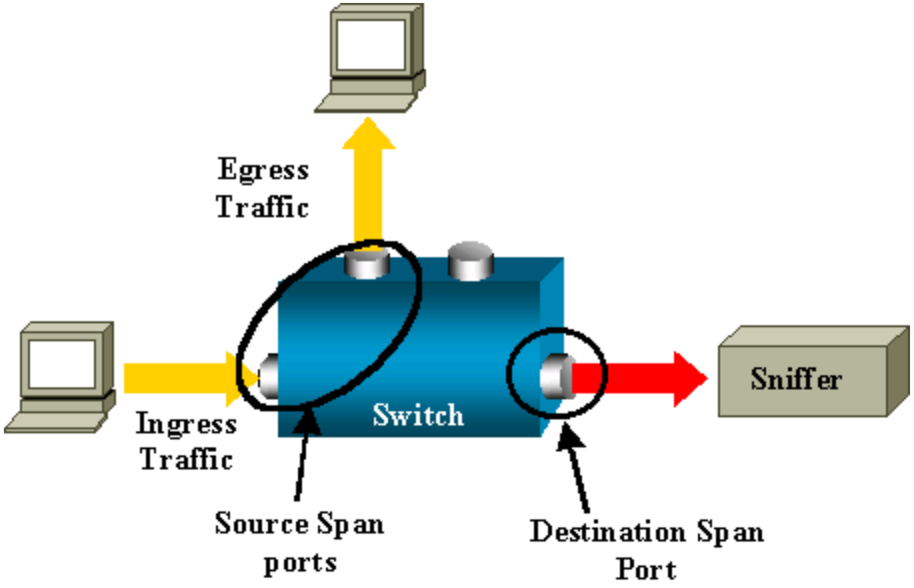

HUB
All traffic appears on all ports on a hub
Server
Client
WireShark Box

Switches



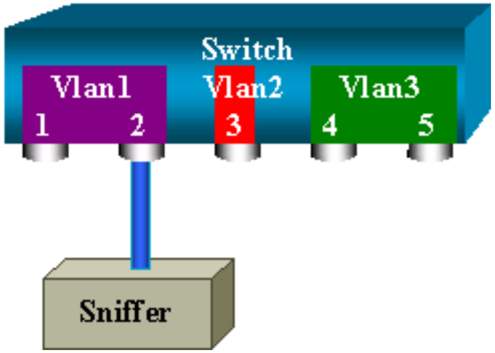
On a switch, traffic is only directed to ports that need it

Switch with a SPAN port



VLAN Monitoring

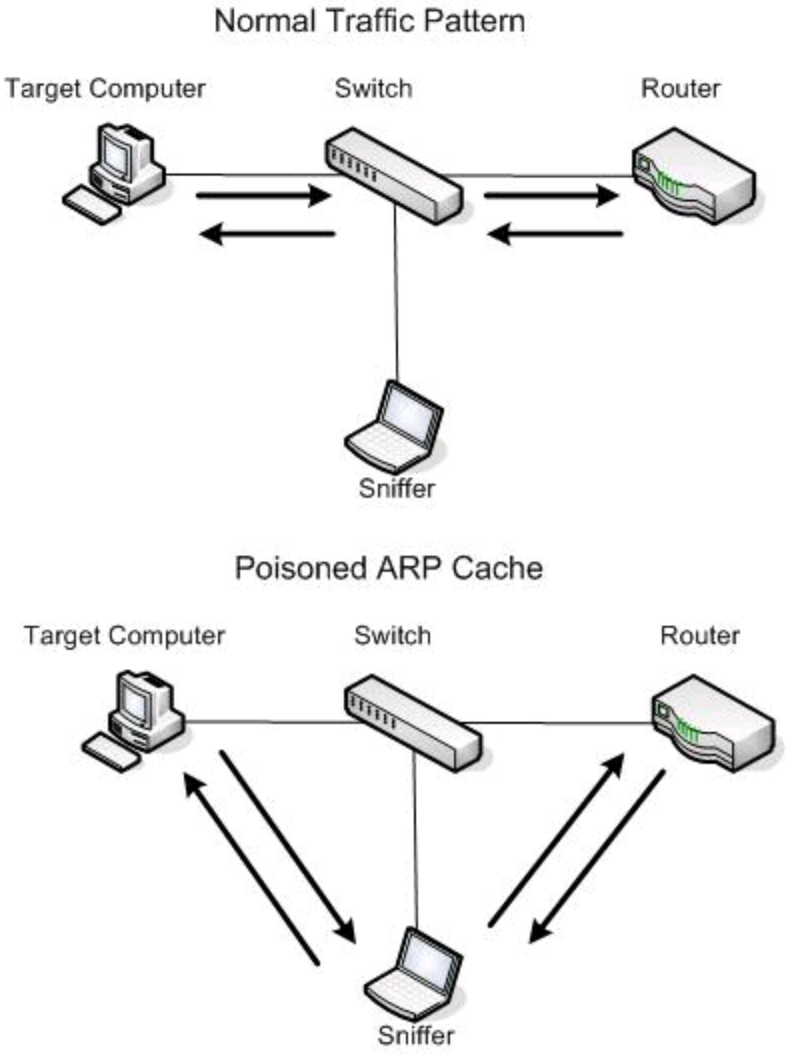
```
interface FastEthernet0/1
        port monitor VLAN1
```



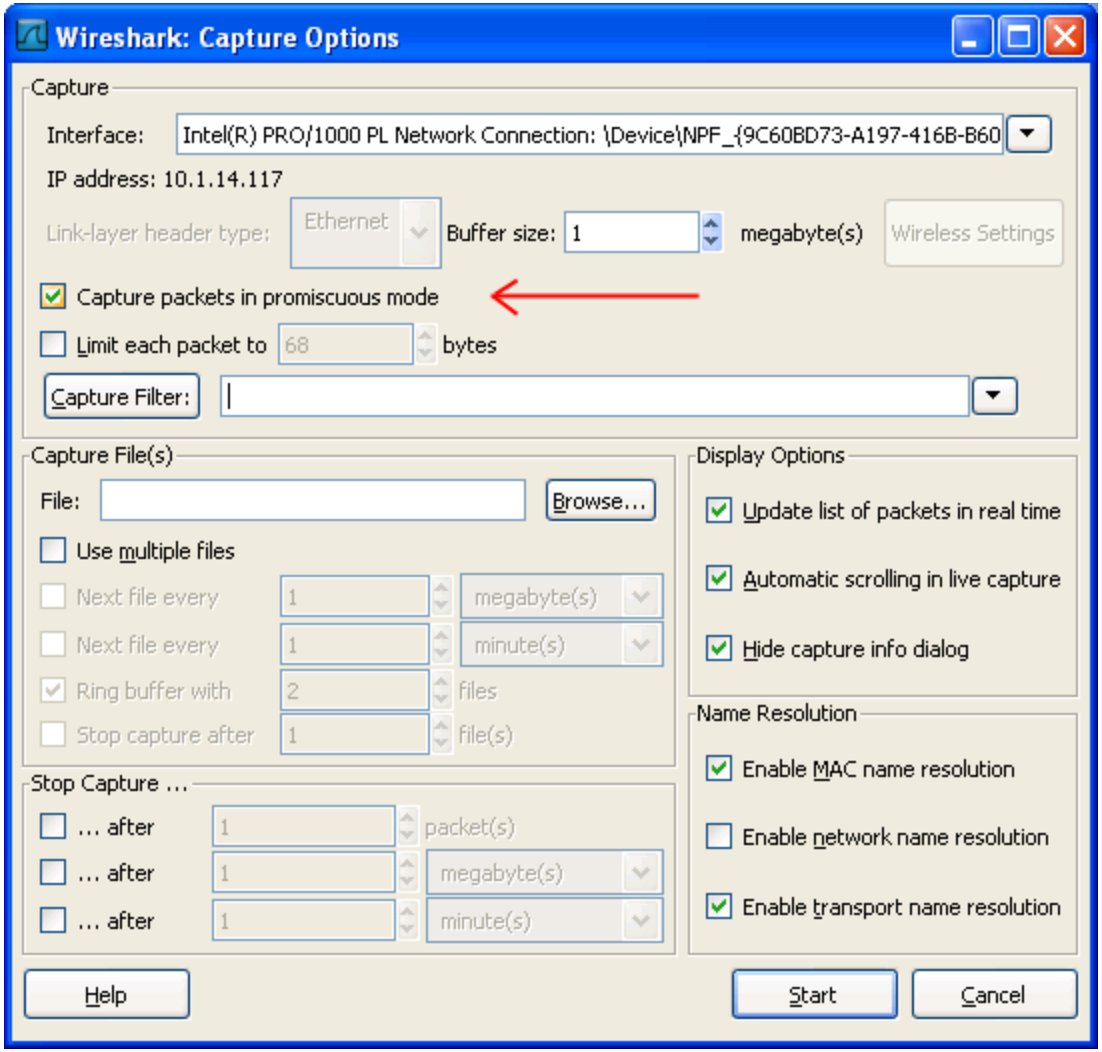
Types of TAPs

- 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

ARP Cache Poisoning



Setting promiscuous mode



Wireshark: Capture Options

Capture

Interface: Intel(R) PRO/1000 PL Network Connection: \Device\NPF_{9C60BD73-A197-416B-B60

IP address: 10.1.14.117

Link-layer header type: Ethernet

Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File:

□ 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

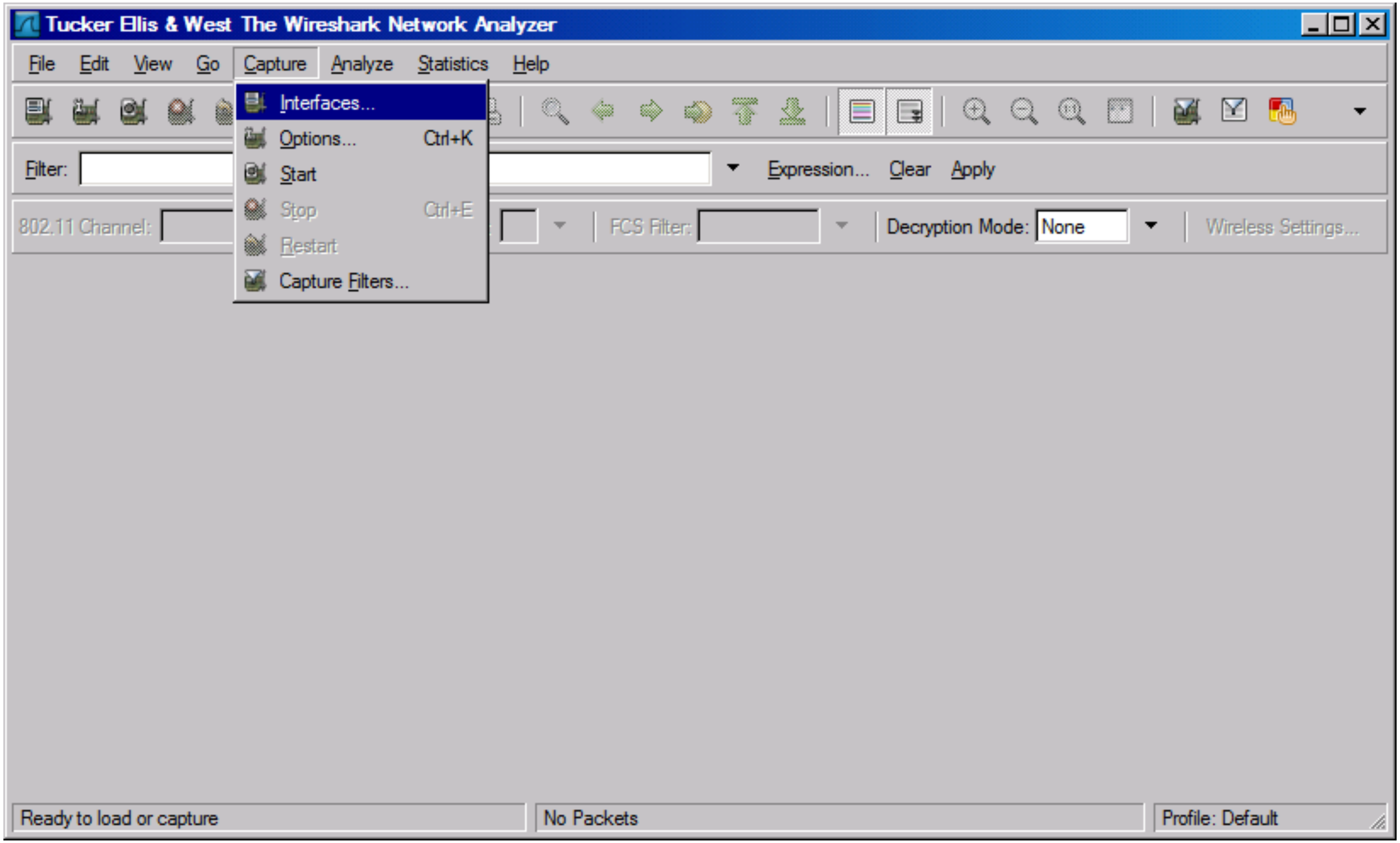
Name Resolution

☑ Enable MAC name resolution

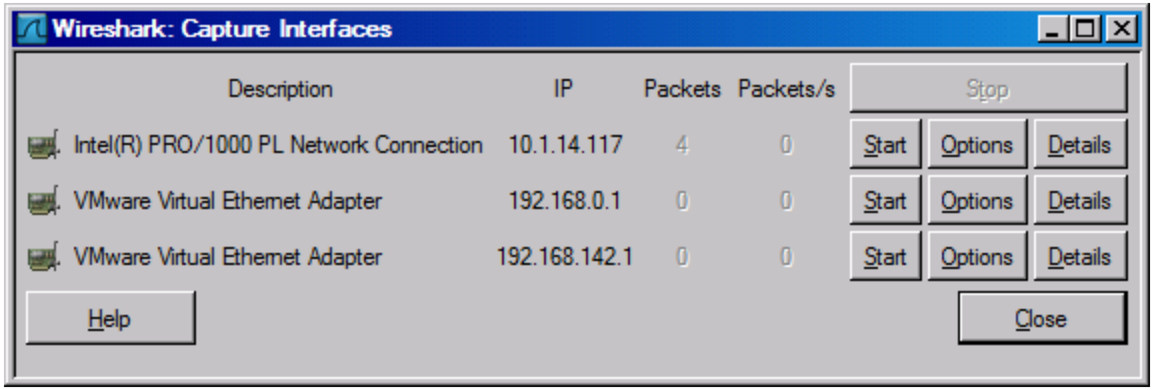
□ Enable network name resolution

☑ Enable transport name resolution

Simple Capture



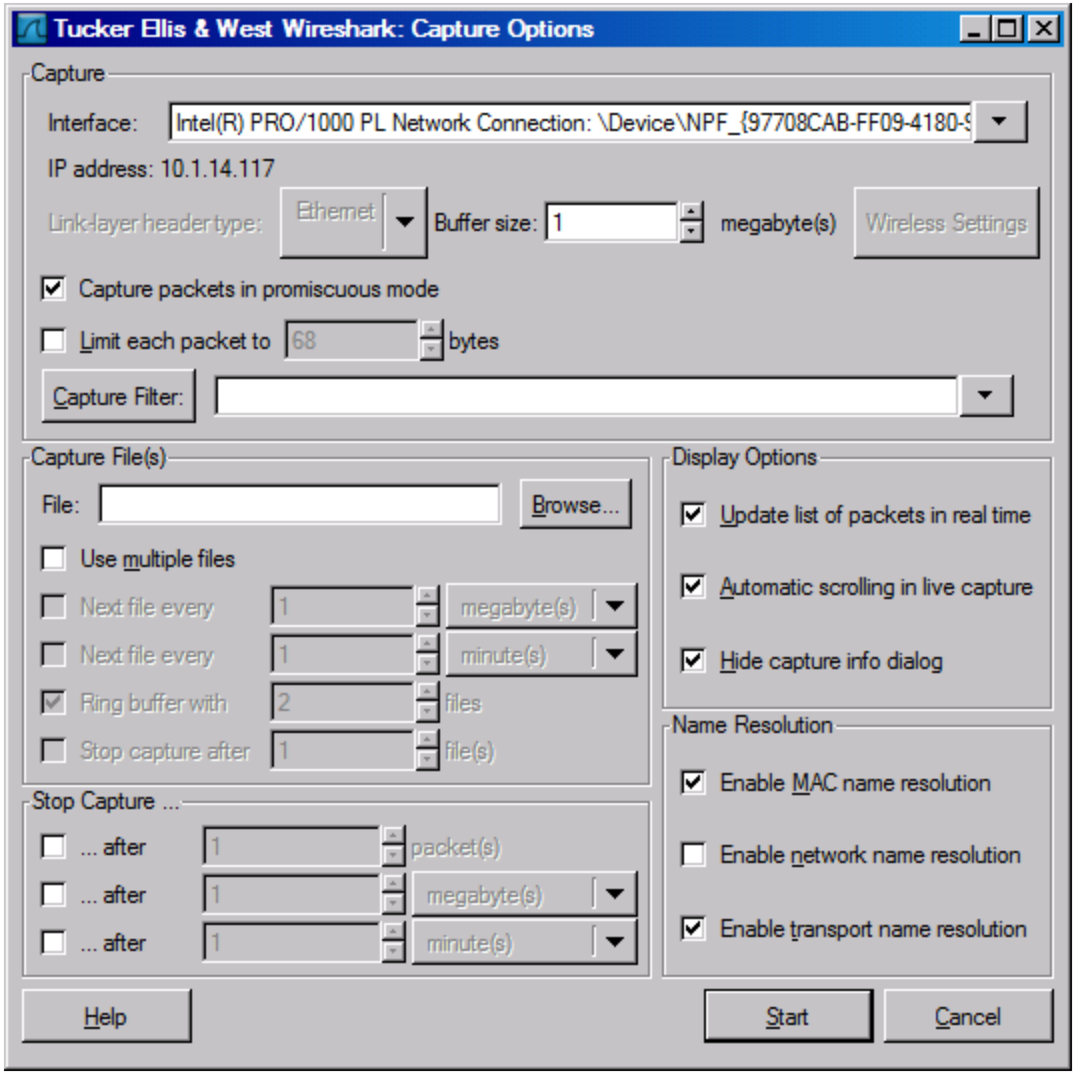
Capture Interfaces



Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s
Intel(R) PRO/1000 PL Network Connection	10.1.14.117	4	0
VMware Virtual Ethernet Adapter	192.168.0.1	0	0
VMware Virtual Ethernet Adapter	192.168.142.1	0	0

Capture Options



Tucker Ellis & West Wireshark: Capture Options

Capture

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

IP address: 10.1.14.117

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:

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

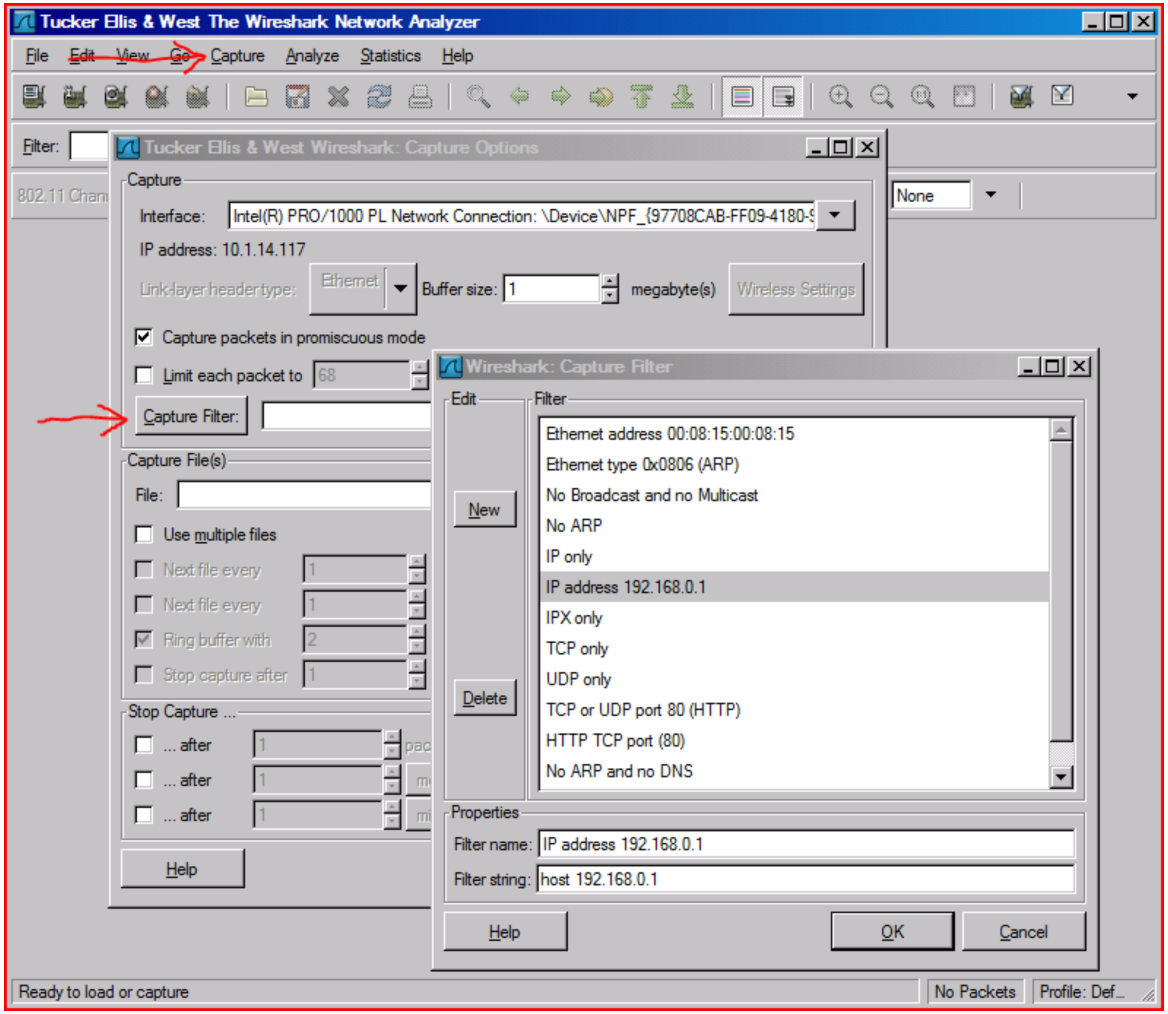
☑ Enable transport name resolution

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



Tucker Ellis & West The Wireshark Network Analyzer

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)

☑ Capture packets in promiscuous mode

□ Limit each packet to 68

Capture Filter:

Capture File(s)

File:

□ Use multiple files

□ Next file every 1

□ Next file every 1

☑ Ring buffer with 2

□ Stop capture after 1

Stop Capture ...

□ ... after 1 pac

□ ... after 1 m

□ ... after 1 mi

Wireshark: Capture Filter

Edit

Filter

- Ethernet address 00:08:15:00:08:15
- Ethernet type 0x0806 (ARP)
- No Broadcast and no Multicast
- No ARP
- IP only
- IP address 192.168.0.1
- IPX only
- TCP only
- UDP only
- TCP or UDP port 80 (HTTP)
- HTTP TCP port (80)
- No ARP and no DNS

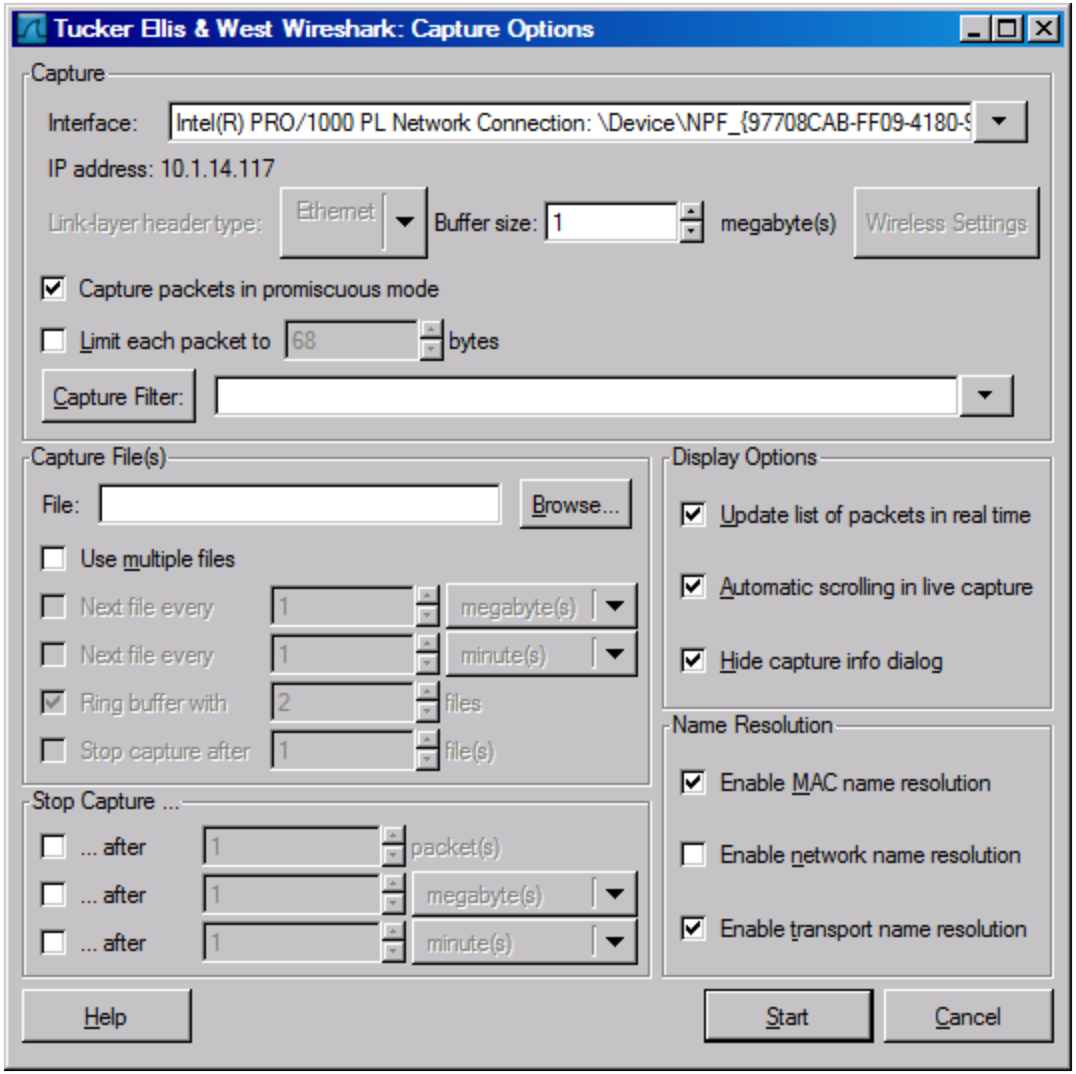
Properties

Filter name: IP address 192.168.0.1

Filter string: host 192.168.0.1

Ready to load or capture | No Packets | Profile: Def...

Capture Options



Tucker Ellis & West Wireshark: Capture Options

Capture

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

IP address: 10.1.14.117

Link-layer header type: Ethernet

Buffer size: 1 megabyte(s)

☑ Capture packets in promiscuous mode

☐ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File:

☐ 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

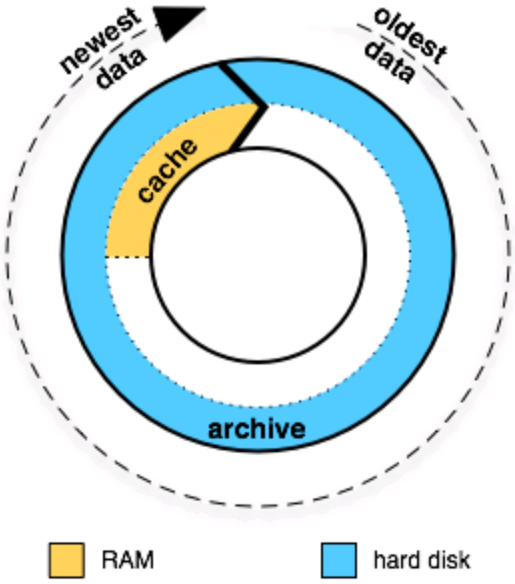
☑ Hide capture info dialog

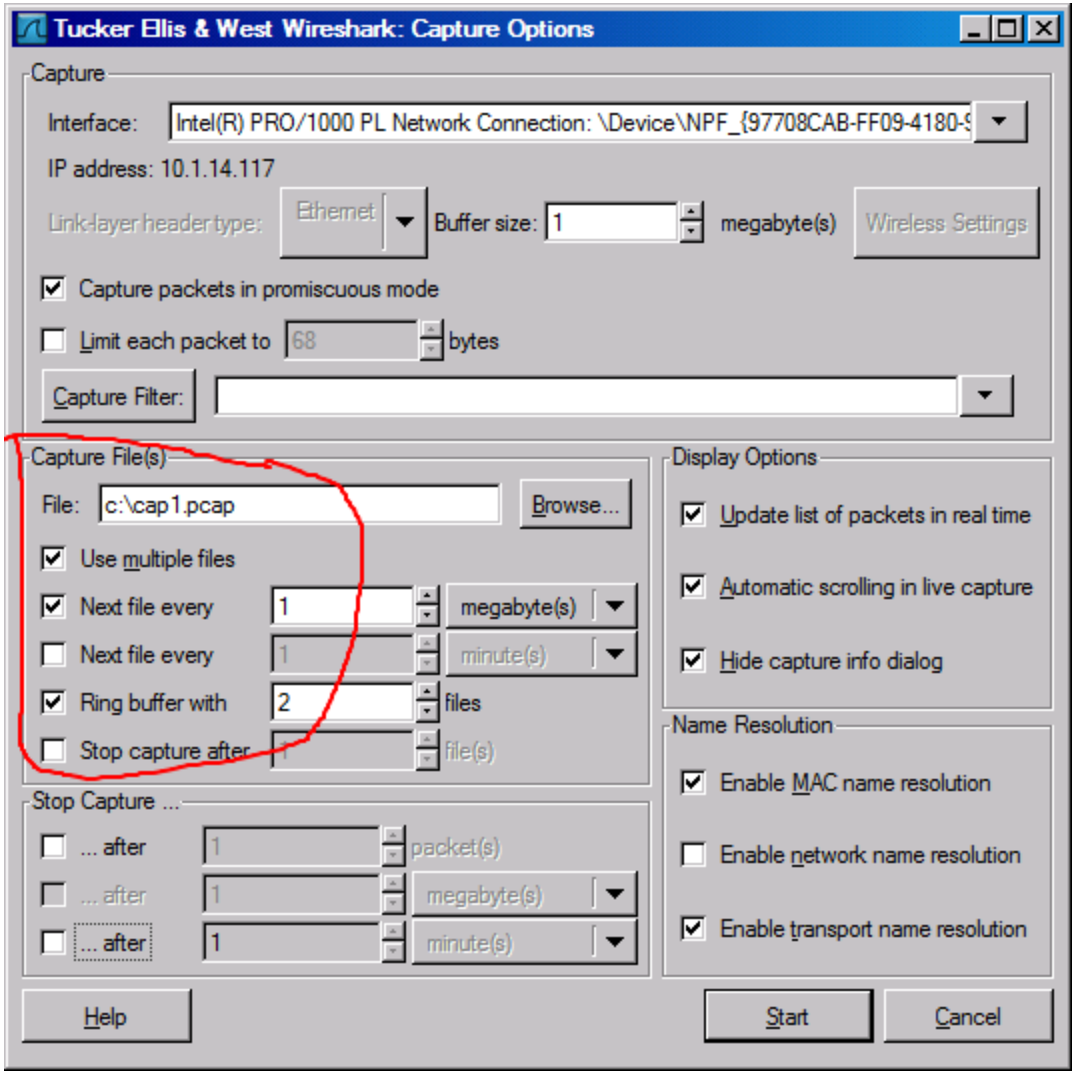
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution


newest data
oldest data
cache
archive
RAM
hard disk



Tucker Ellis & West Wireshark: Capture Options

Capture

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

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

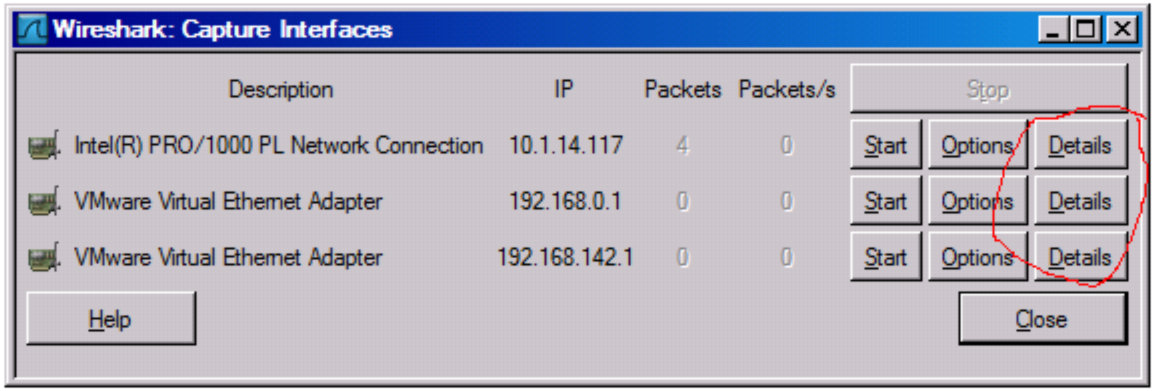
Name Resolution

☑ Enable MAC name resolution

□ Enable network name resolution

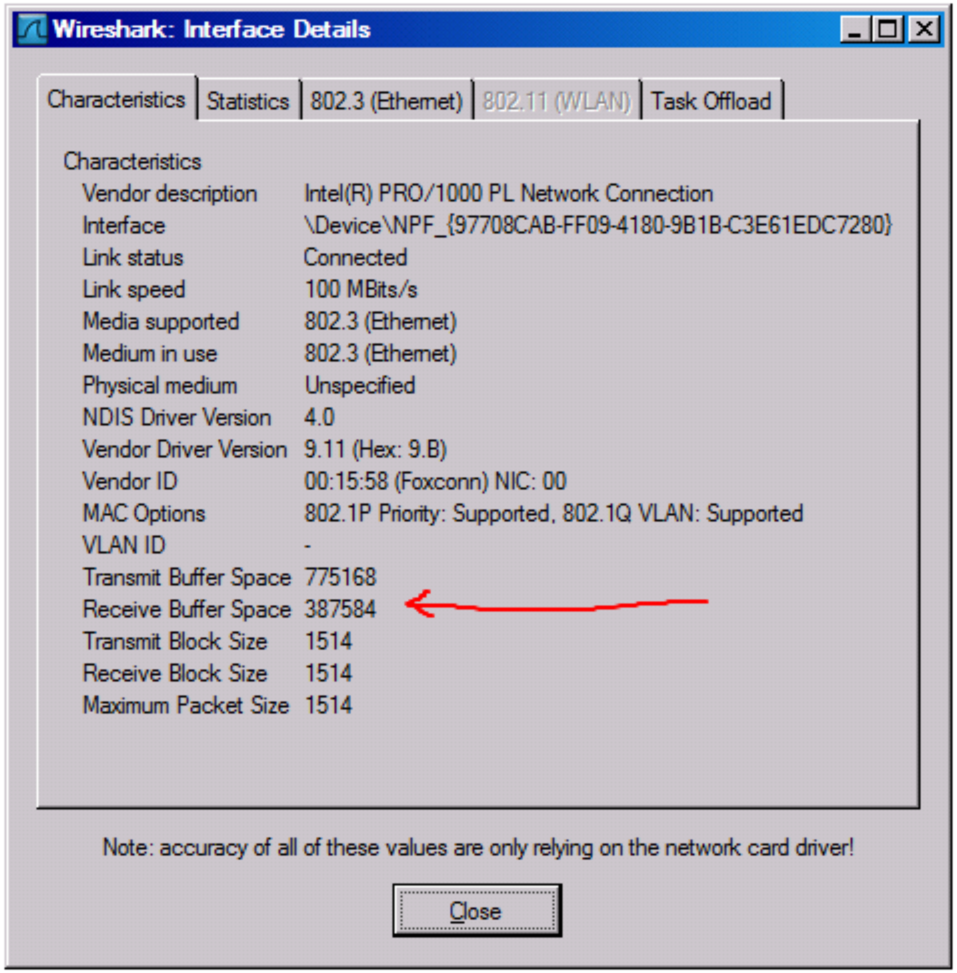
☑ Enable transport name resolution

Capture Interfaces



Description	IP	Packets	Packets/s
Intel(R) PRO/1000 PL Network Connection	10.1.14.117	4	0
VMware Virtual Ethernet Adapter	192.168.0.1	0	0
VMware Virtual Ethernet Adapter	192.168.142.1	0	0

Interface Details: Characteristics

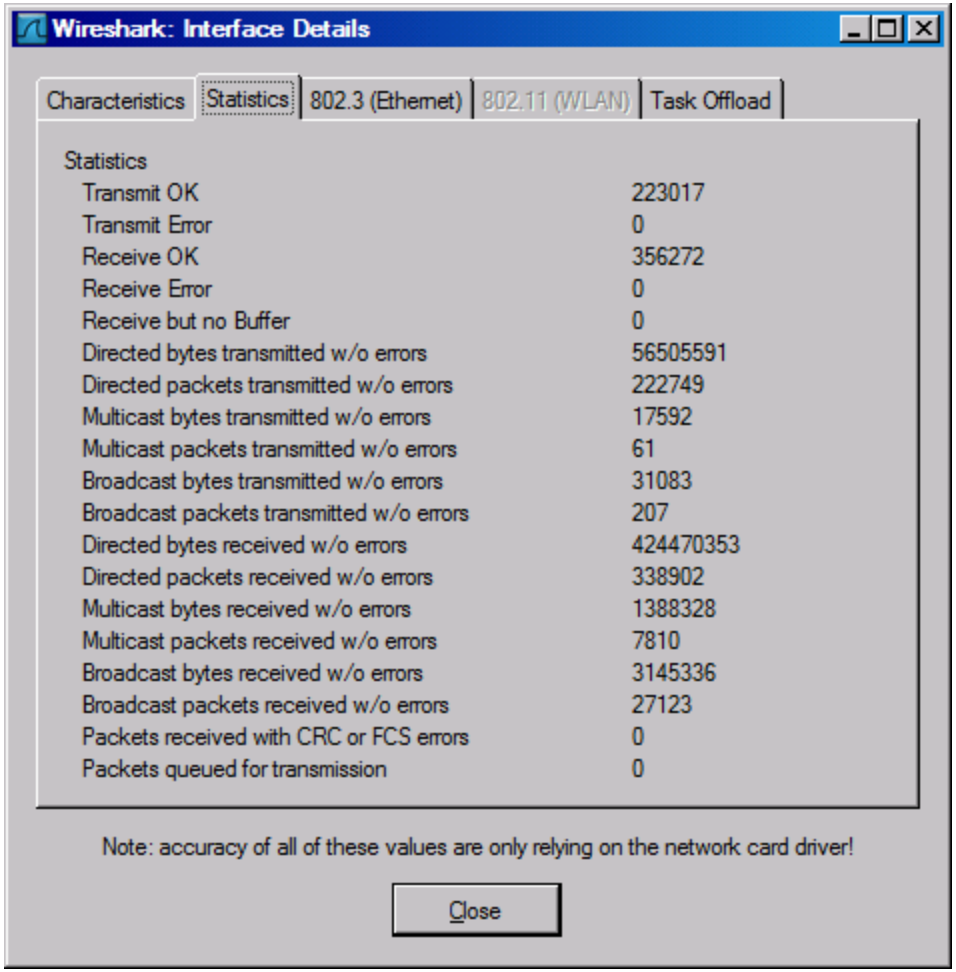


Characteristics

Vendor description	Intel(R) PRO/1000 PL Network Connection
Interface	\Device\NPF_{97708CAB-FF09-4180-9B1B-C3E61EDC7280}
Link status	Connected
Link speed	100 MBits/s
Media supported	802.3 (Ethernet)
Medium in use	802.3 (Ethernet)
Physical medium	Unspecified
NDIS Driver Version	4.0
Vendor Driver Version	9.11 (Hex: 9.B)
Vendor ID	00:15:58 (Foxconn) NIC: 00
MAC Options	802.1P Priority: Supported, 802.1Q VLAN: Supported
VLAN ID	-
Transmit Buffer Space	775168
Receive Buffer Space	387584
Transmit Block Size	1514
Receive Block Size	1514
Maximum Packet Size	1514

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

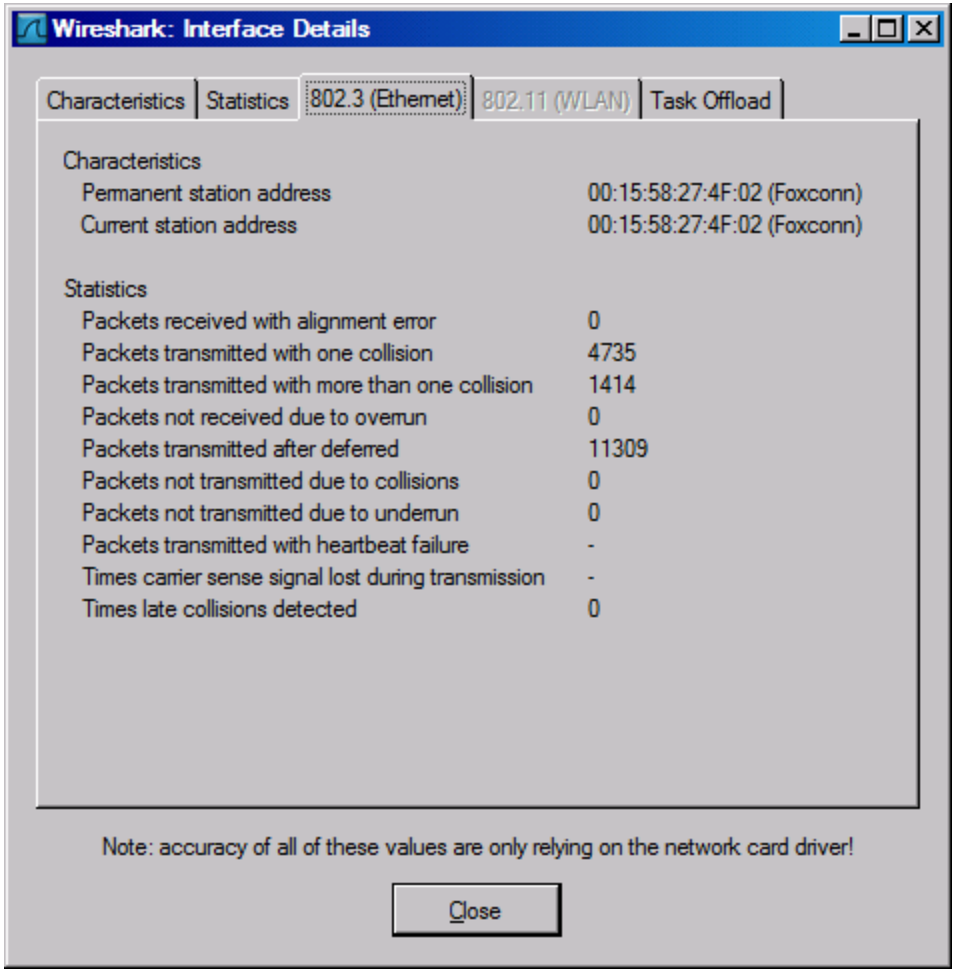
Interface Details: Statistics



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!

Interface Details: 802.3 (Ethernet)



Characteristics

Permanent station address	00:15:58:27:4F:02 (Foxconn)
Current station address	00:15:58:27:4F:02 (Foxconn)

Statistics

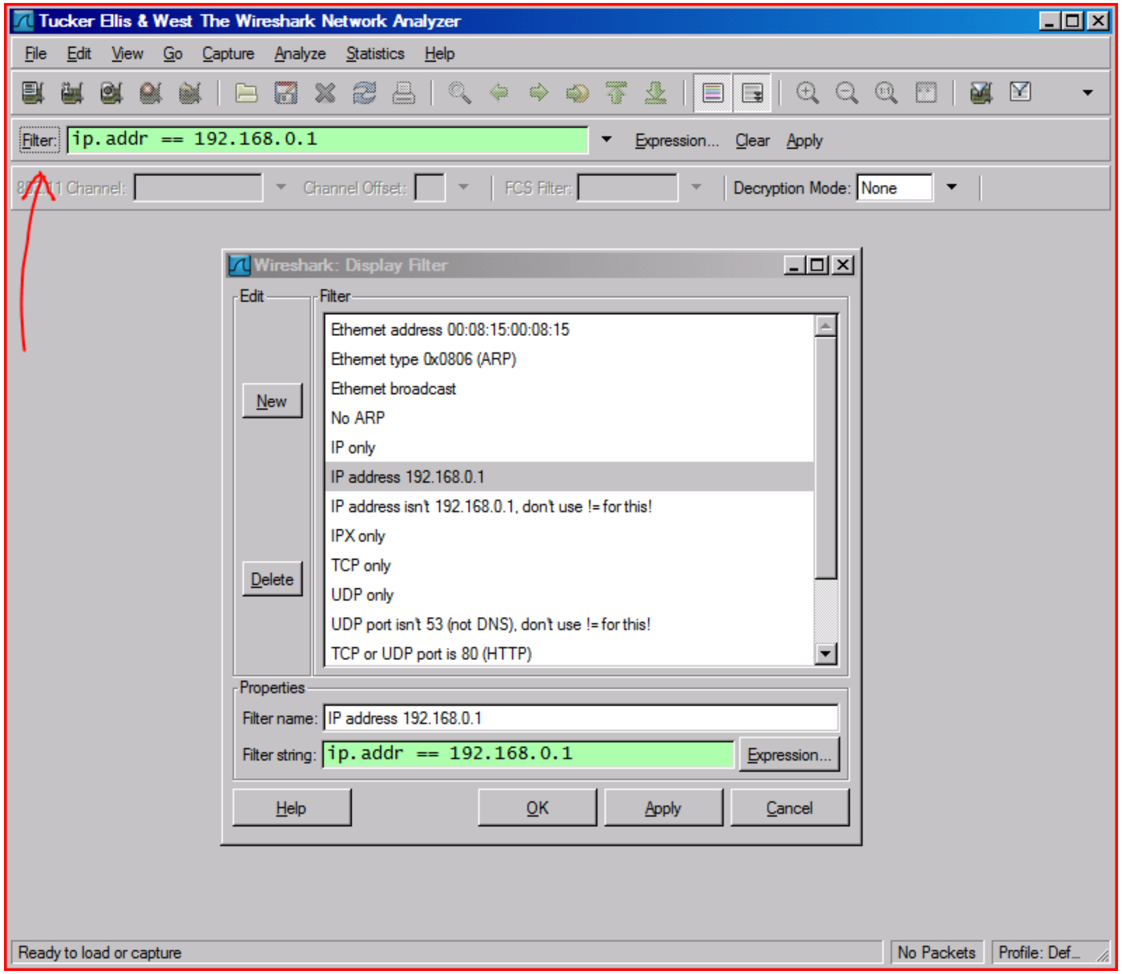
Packets received with alignment error	0
Packets transmitted with one collision	4735
Packets transmitted with more than one collision	1414
Packets not received due to overrun	0
Packets transmitted after deferred	11309
Packets not transmitted due to collisions	0
Packets not transmitted due to underrun	0
Packets transmitted with heartbeat failure	-
Times carrier sense signal lost during transmission	-
Times late collisions detected	0

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

Display Filters (Post-Filters)

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

Display Filter



Tucker Ellis & West The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
802.11 Channel: Channel Offset: FCS Filter:
Wireshark: Display Filter
Edit
New
Delete
Help OK Apply Cancel
Expression...

Filter: ip.addr == 192.168.0.1

Decryption Mode: None

Filter

- Ethernet address 00:08:15:00:08:15
- Ethernet type 0x0806 (ARP)
- Ethernet broadcast
- No ARP
- IP only
- IP address 192.168.0.1
- IP address isn't 192.168.0.1, don't use != for this!
- IPX only
- TCP only
- UDP only
- UDP port isn't 53 (not DNS), don't use != for this!
- TCP or UDP port is 80 (HTTP)

Properties

Filter name: IP address 192.168.0.1

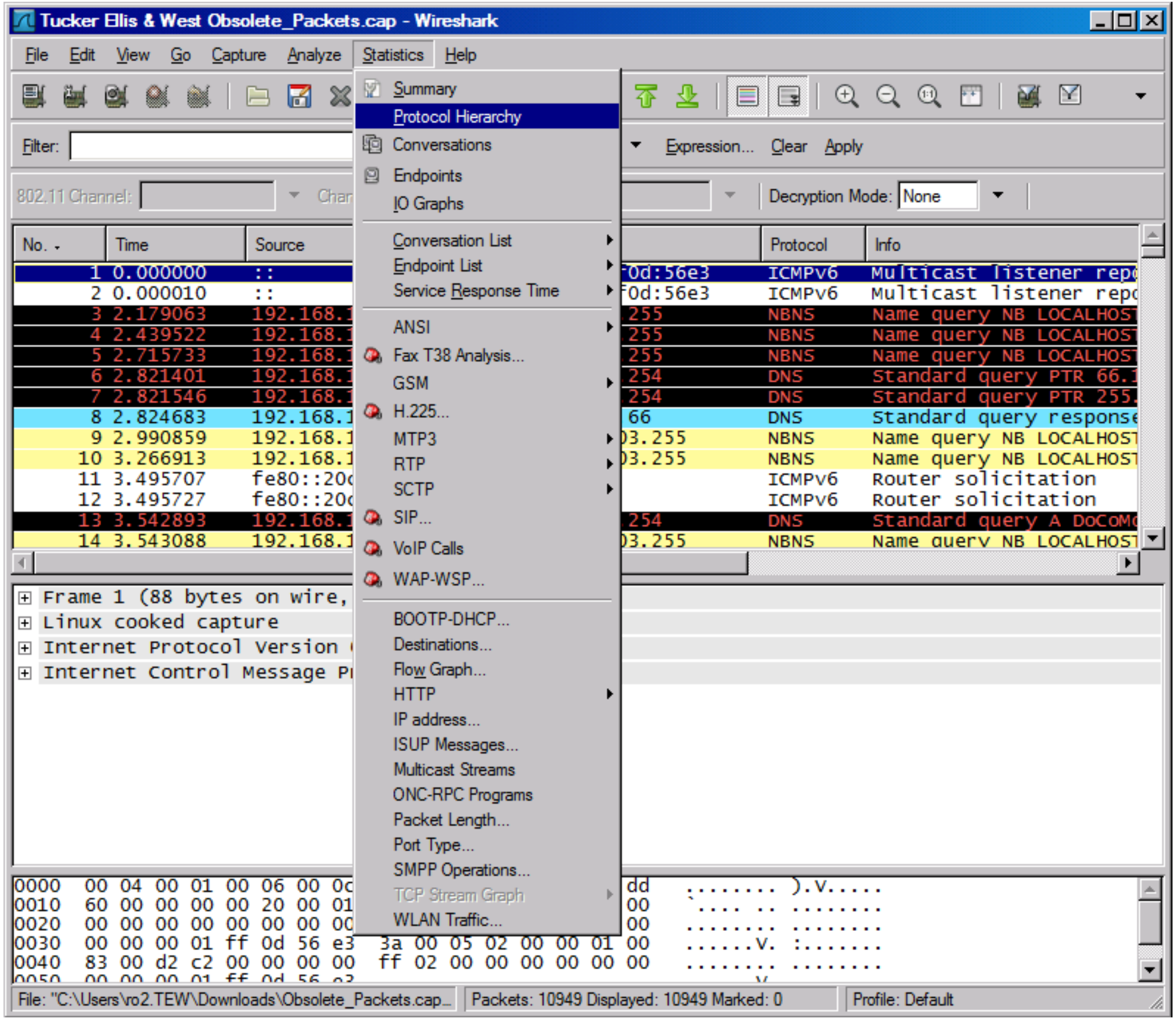
Filter string: ip.addr == 192.168.0.1

Ready to load or capture | No Packets | Profile: Def...

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



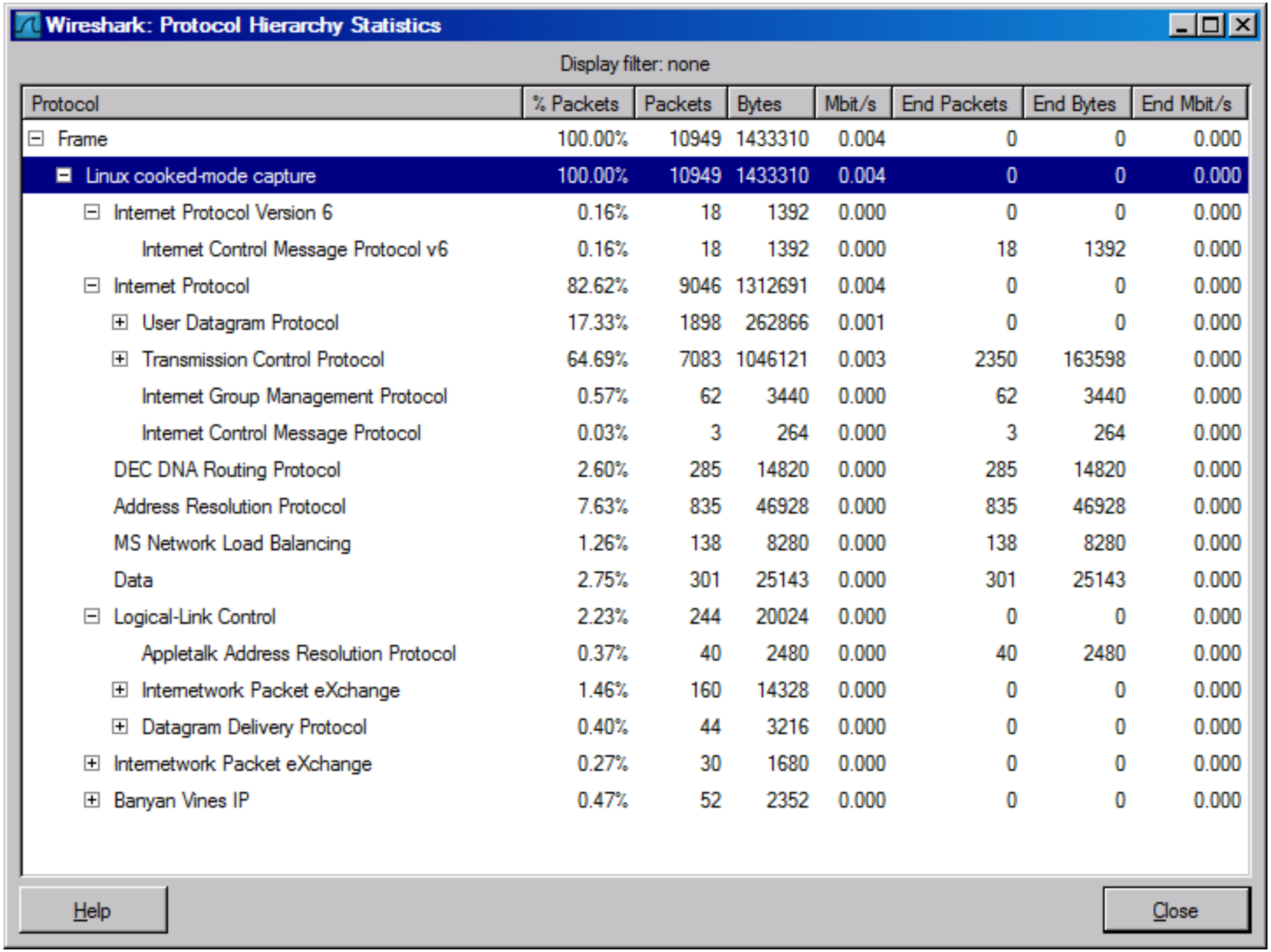
No.	Time	Source		Protocol	Info
1	0.000000	::	f0d:56e3	ICMPv6	Multicast listener repo
2	0.000010	::	f0d:56e3	ICMPv6	Multicast listener repo
3	2.179063	192.168.1	255	NBNS	Name query NB LOCALHOST
4	2.439522	192.168.1	255	NBNS	Name query NB LOCALHOST
5	2.715733	192.168.1	255	NBNS	Name query NB LOCALHOST
6	2.821401	192.168.1	254	DNS	Standard query PTR 66.1
7	2.821546	192.168.1	254	DNS	Standard query PTR 255.
8	2.824683	192.168.1	66	DNS	Standard query response
9	2.990859	192.168.1	03.255	NBNS	Name query NB LOCALHOST
10	3.266913	192.168.1	03.255	NBNS	Name query NB LOCALHOST
11	3.495707	fe80::20c		ICMPv6	Router solicitation
12	3.495727	fe80::20c		ICMPv6	Router solicitation
13	3.542893	192.168.1	254	DNS	Standard query A DoCoMo
14	3.543088	192.168.1	03.255	NBNS	Name query NB LOCALHOST

```
⊞ Frame 1 (88 bytes on wire,
⊞ Linux cooked capture
⊞ Internet Protocol Version
⊞ Internet Control Message Pr
```

```
0000  00 04 00 01 00 06 00 0c              dd    ........ ).V.....
0010  60 00 00 00 00 20 00 01              00    `....  .. ........
0020  00 00 00 00 00 00 00 00              00    ........ ........
0030  00 00 00 01 ff 0d 56 e3  3a 00 05 02 00 00 01 00    ......V. :.......
0040  83 00 d2 c2 00 00 00 00  ff 02 00 00 00 00 00 00    ........ ........
0050  00 00 00 01 ff 0d 56 e3
```

File: "C:\Users\ro2.TEW\Downloads\Obsolete_Packets.cap... Packets: 10949 Displayed: 10949 Marked: 0 Profile: Default

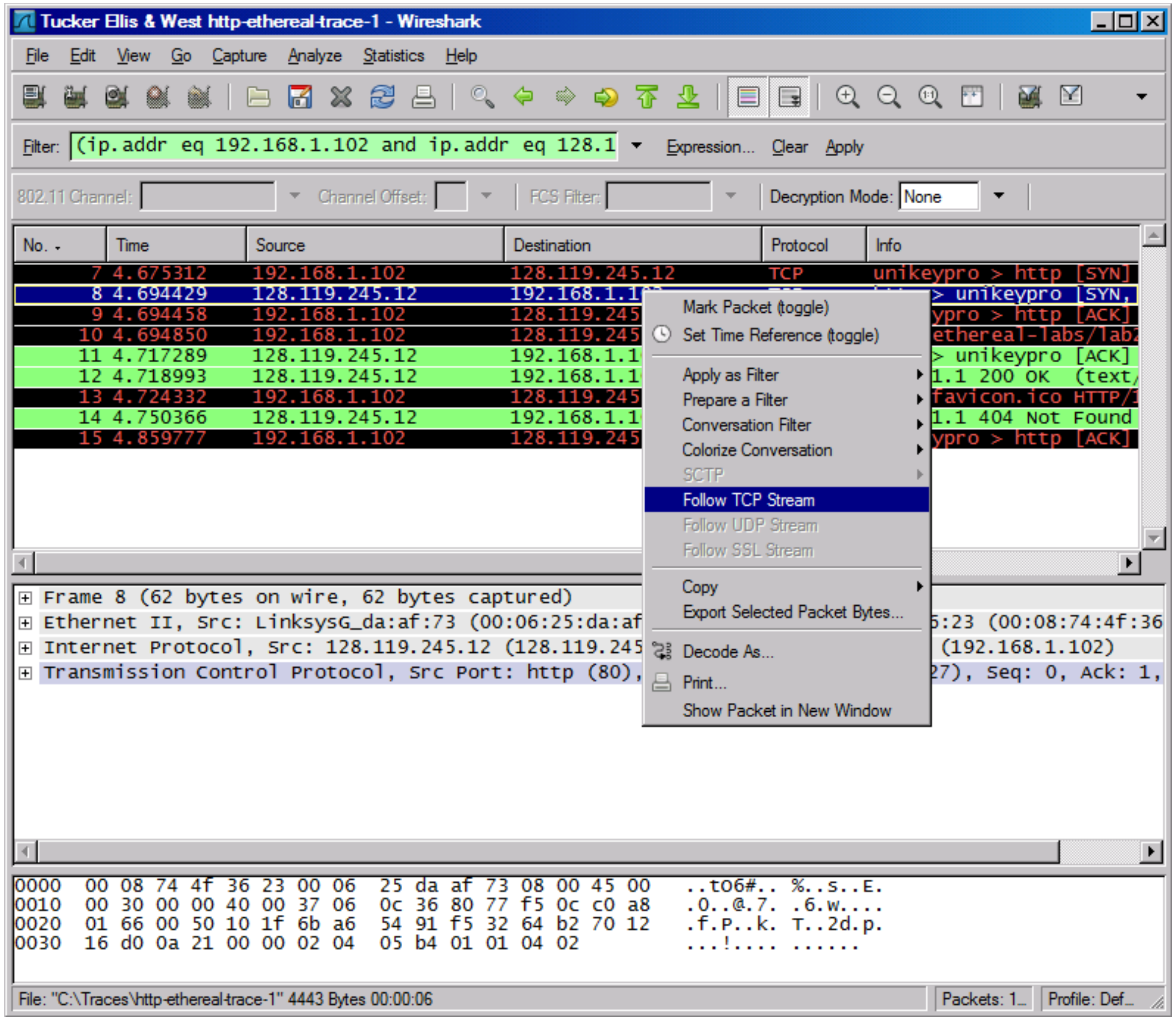
Protocol Hierarchy



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

Follow TCP Stream



Tucker Ellis & West http-ethereal-trace-1 - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
Mark Packet (toggle)
Set Time Reference (toggle)
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Decode As...
Print...
Show Packet in New Window

Filter: (ip.addr eq 192.168.1.102 and ip.addr eq 128.1

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

```
No. .   Time       Source          Destination     Protocol  Info
   7 4.675312   192.168.1.102   128.119.245.12  TCP       unikeypro > http [SYN]
   8 4.694429   128.119.245.12  192.168.1.1                > unikeypro [SYN,
   9 4.694458   192.168.1.102   128.119.245                ypro > http [ACK]
  10 4.694850   192.168.1.102   128.119.245                ethereal-labs/lab
  11 4.717289   128.119.245.12  192.168.1.1                > unikeypro [ACK]
  12 4.718993   128.119.245.12  192.168.1.1                1.1 200 OK  (text/
  13 4.724332   192.168.1.102   128.119.245                favicon.ico HTTP/1
  14 4.750366   128.119.245.12  192.168.1.1                1.1 404 Not Found
  15 4.859777   192.168.1.102   128.119.245                ypro > http [ACK]
```

```
⊞ Frame 8 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af          5:23 (00:08:74:4f:36
⊞ Internet Protocol, Src: 128.119.245.12 (128.119.245           (192.168.1.102)
⊞ Transmission Control Protocol, Src Port: http (80),          27), Seq: 0, Ack: 1,
```

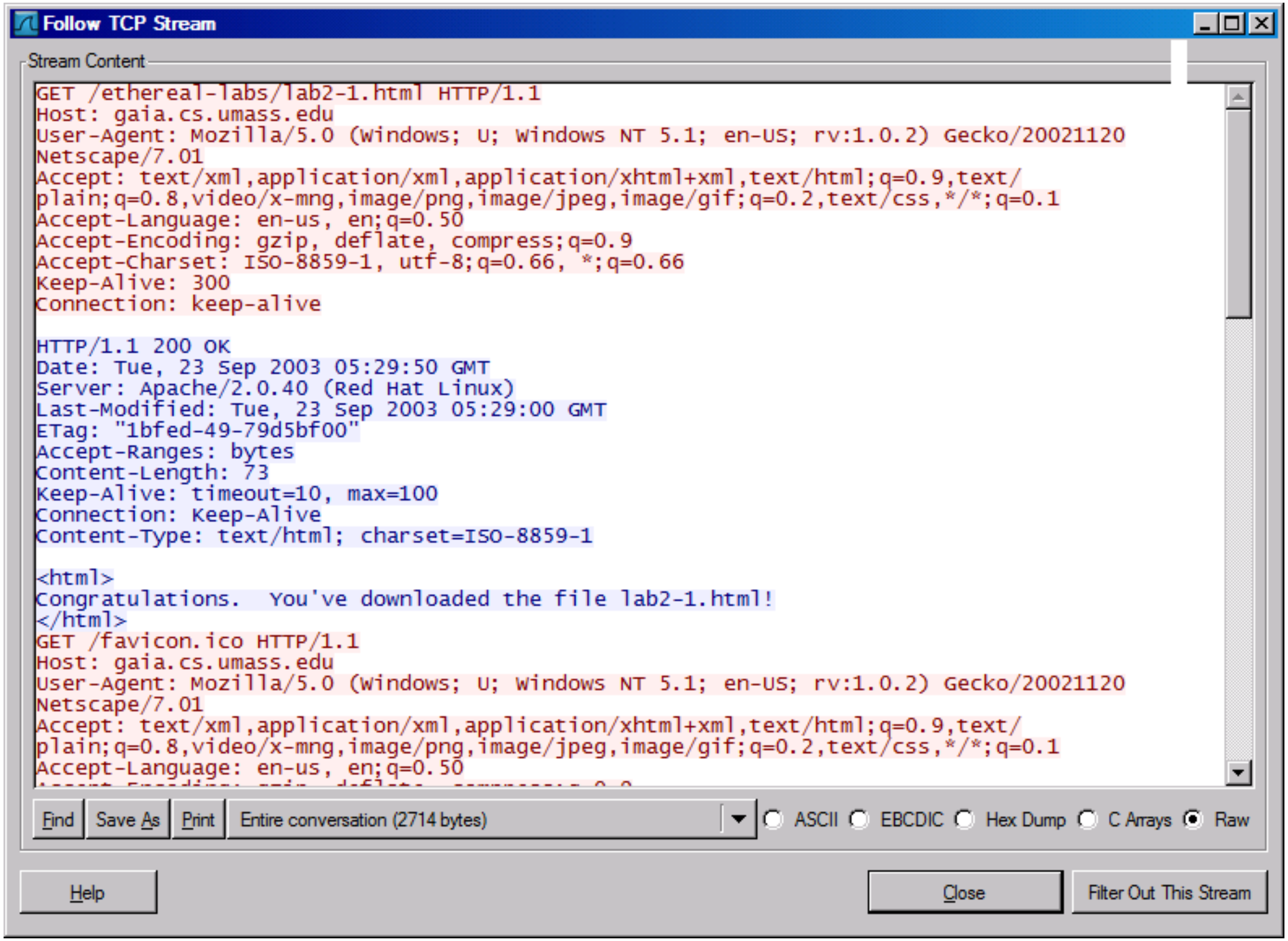
```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  00 30 00 00 40 00 37 06  0c 36 80 77 f5 0c c0 a8   .0..@.7. .6.w....
0020  01 66 00 50 10 1f 6b a6  54 91 f5 32 64 b2 70 12   .f.P..k. T..2d.p.
0030  16 d0 0a 21 00 00 02 04  05 b4 01 01 04 02         ...!.... ......
```

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

Follow TCP Stream

red - stuff you sent

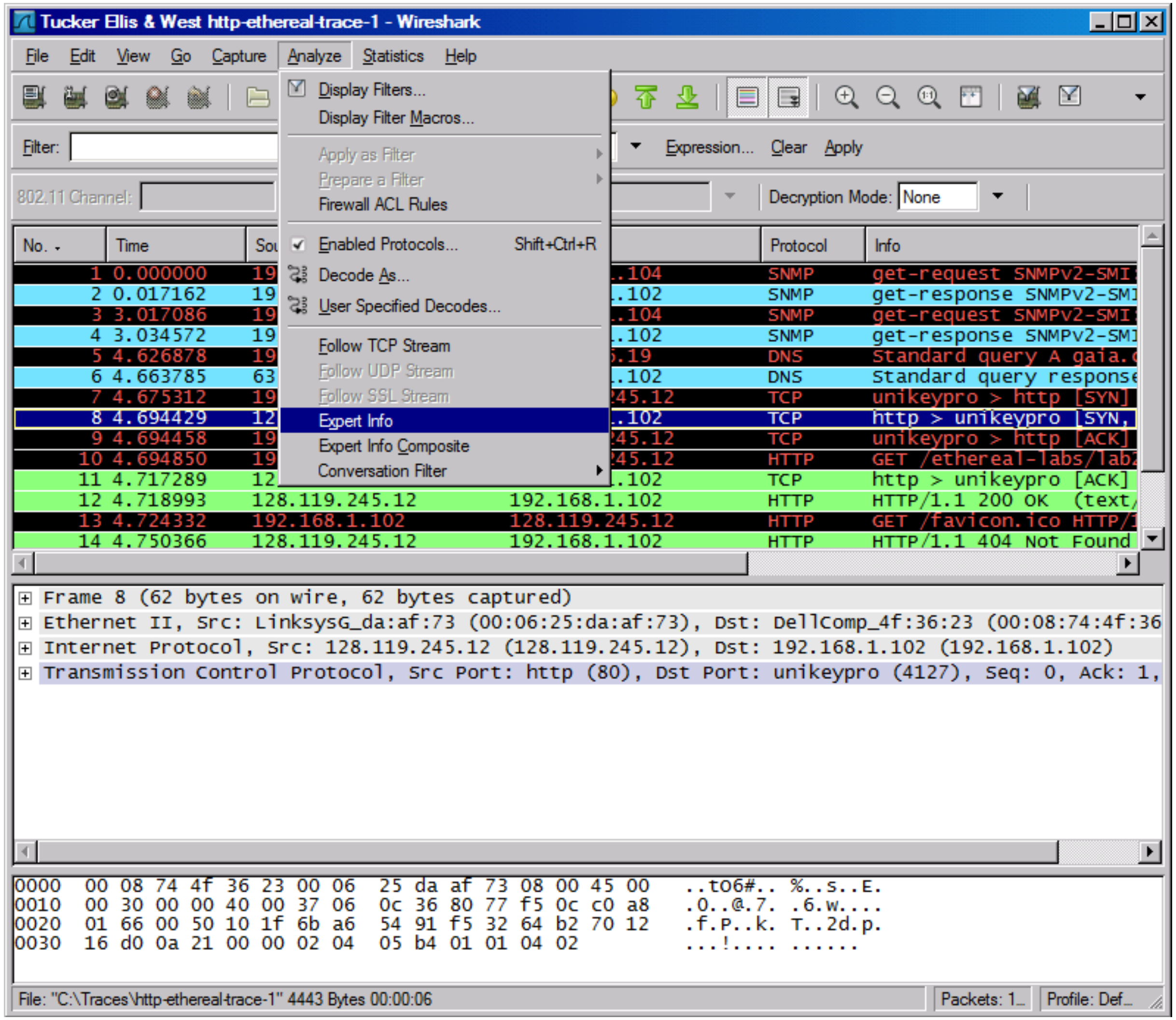
blue - stuff you get



```
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
```

Entire conversation (2714 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Expert Info



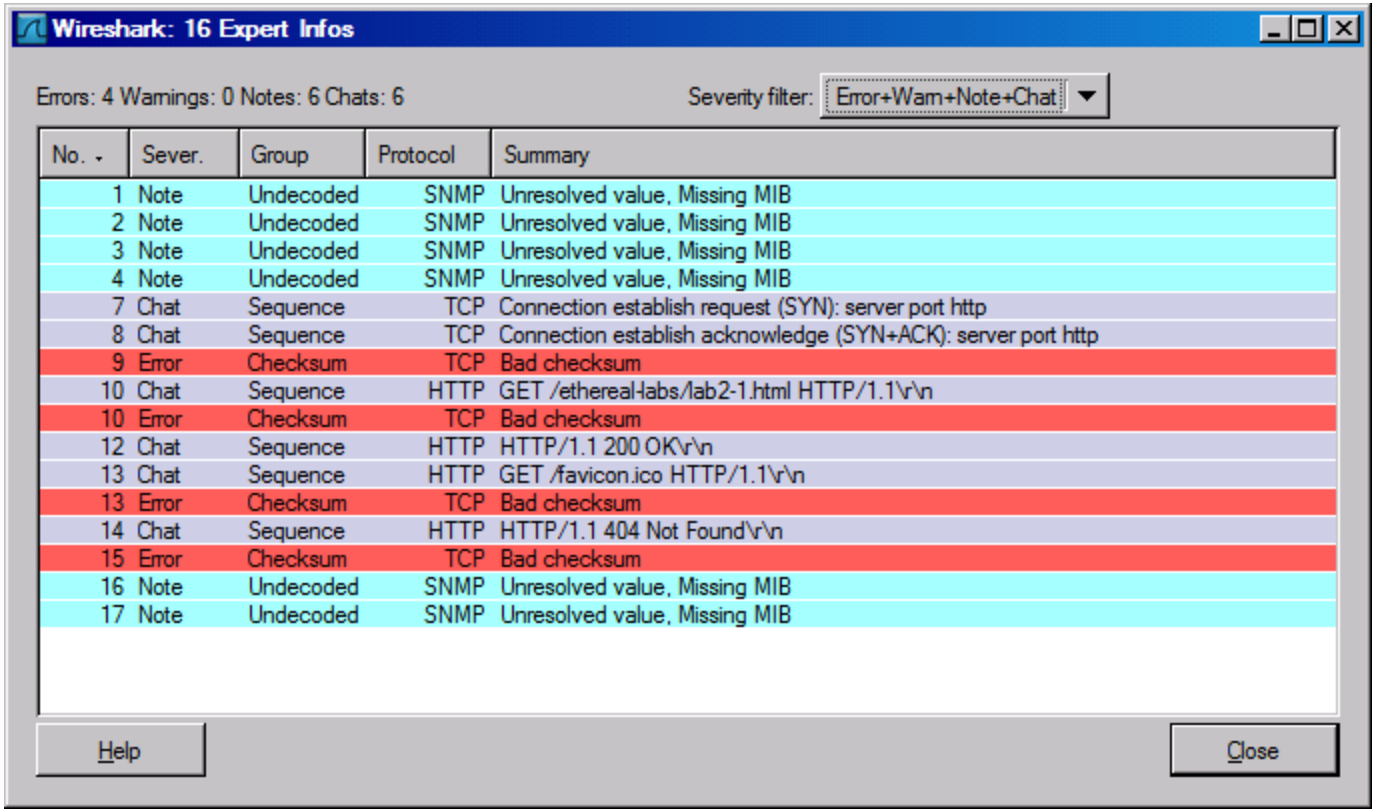
```
No. -  Time       Sou                            Protocol  Info
    1 0.000000   19          .104               SNMP      get-request SNMPv2-SMI
    2 0.017162   19          .102               SNMP      get-response SNMPv2-SMI
    3 3.017086   19          .104               SNMP      get-request SNMPv2-SMI
    4 3.034572   19          .102               SNMP      get-response SNMPv2-SMI
    5 4.626878   19          .19                DNS       Standard query A gaia.
    6 4.663785   63          .102               DNS       Standard query response
    7 4.675312   19          45.12              TCP       unikeypro > http [SYN]
    8 4.694429   12          .102               TCP       http > unikeypro [SYN,
    9 4.694458   19          45.12              TCP       unikeypro > http [ACK]
   10 4.694850   19          45.12              HTTP      GET /ethereal-labs/lab
   11 4.717289   12          .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
⊞ Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: unikeypro (4127), Seq: 0, Ack: 1,
```

```
0000   00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010   00 30 00 00 40 00 37 06  0c 36 80 77 f5 0c c0 a8   .0..@.7. .6.w....
0020   01 66 00 50 10 1f 6b a6  54 91 f5 32 64 b2 70 12   .f.P..k. T..2d.p.
0030   16 d0 0a 21 00 00 02 04  05 b4 01 01 04 02         ...!.... ......
```

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

Expert Info



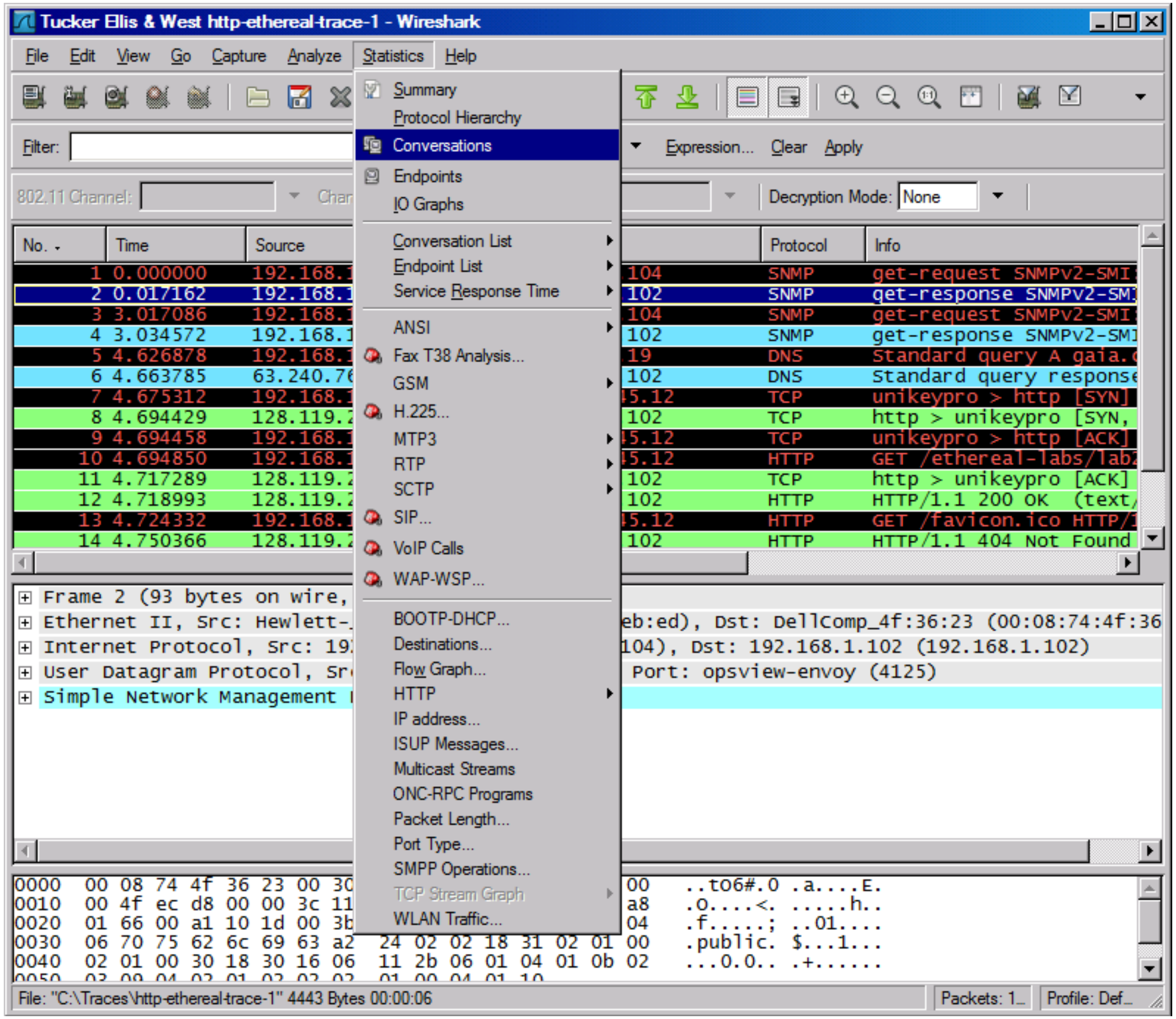
Wireshark: 16 Expert Infos

Errors: 4 Warnings: 0 Notes: 6 Chats: 6

Severity filter: Error+Warn+Note+Chat

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

Conversations



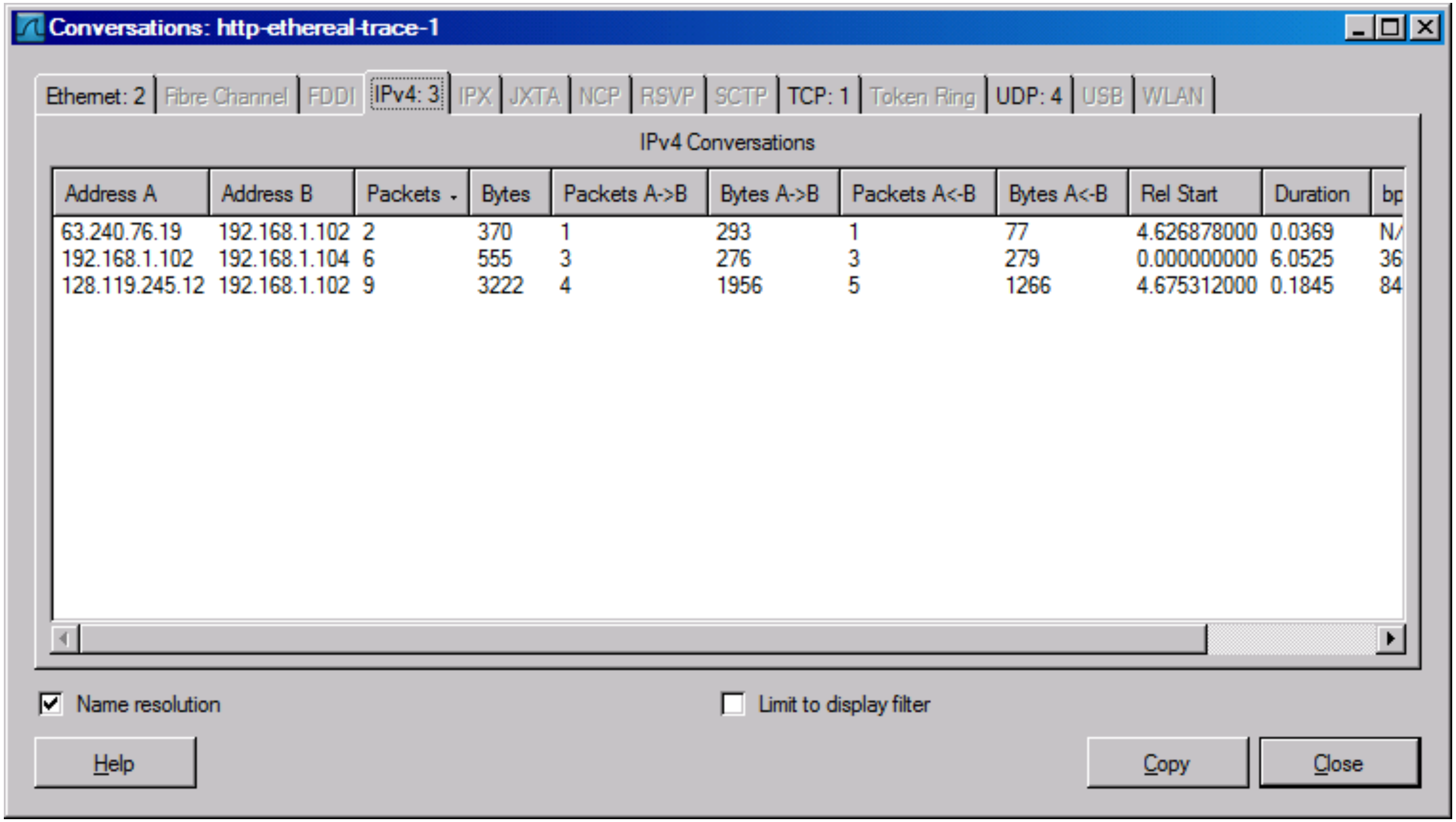
```
No. -     Time          Source                      Protocol   Info
     1 0.000000    192.168.1            104       SNMP       get-request SNMPv2-SMI
     2 0.017162    192.168.1            102       SNMP       get-response SNMPv2-SMI
     3 3.017086    192.168.1            104       SNMP       get-request SNMPv2-SMI
     4 3.034572    192.168.1            102       SNMP       get-response SNMPv2-SMI
     5 4.626878    192.168.1            19        DNS        Standard query A gaia.
     6 4.663785    63.240.76            102       DNS        Standard query response
     7 4.675312    192.168.1            5.12      TCP        unikeypro > http [SYN]
     8 4.694429    128.119.2            102       TCP        http > unikeypro [SYN,
     9 4.694458    192.168.1            5.12      TCP        unikeypro > http [ACK]
    10 4.694850    192.168.1            5.12      HTTP       GET /ethereal-labs/lab2
    11 4.717289    128.119.2            102       TCP        http > unikeypro [ACK]
    12 4.718993    128.119.2            102       HTTP       HTTP/1.1 200 OK  (text/
    13 4.724332    192.168.1            5.12      HTTP       GET /favicon.ico HTTP/1
    14 4.750366    128.119.2            102       HTTP       HTTP/1.1 404 Not Found
```

```
⊞ Frame 2 (93 bytes on wire,
⊞ Ethernet II, Src: Hewlett-      eb:ed), Dst: DellComp_4f:36:23 (00:08:74:4f:36
⊞ Internet Protocol, Src: 19      104), Dst: 192.168.1.102 (192.168.1.102)
⊞ User Datagram Protocol, Sr       Port: opsview-envoy (4125)
⊞ Simple Network Management
```

```
0000   00 08 74 4f 36 23 00 30         00    ..tO6#.0 .a....E.
0010   00 4f ec d8 00 00 3c 11         a8    .O....<. .....h..
0020   01 66 00 a1 10 1d 00 3b         04    .f.....; ..01....
0030   06 70 75 62 6c 69 63 a2  24 02 02 18 31 02 01 00    .public. $...1...
0040   02 01 00 30 18 30 16 06  11 2b 06 01 04 01 0b 02    ...0.0.. .+......
0050   03 09 04 02 01 02 02 02  01 00 04 01 10
```

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

Conversations



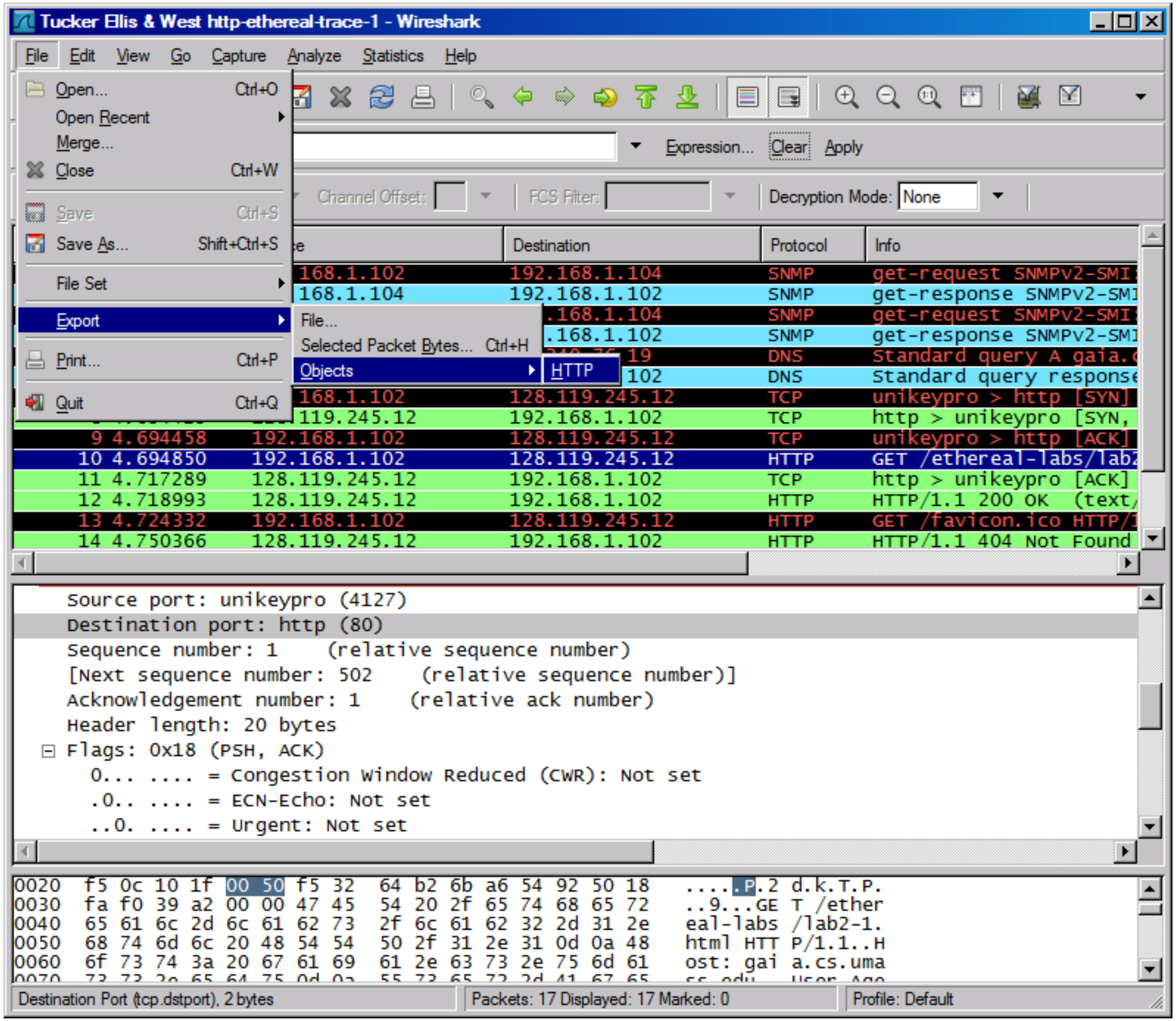
IPv4 Conversations

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

☑ Name resolution

☐ Limit to display filter

Export HTTP



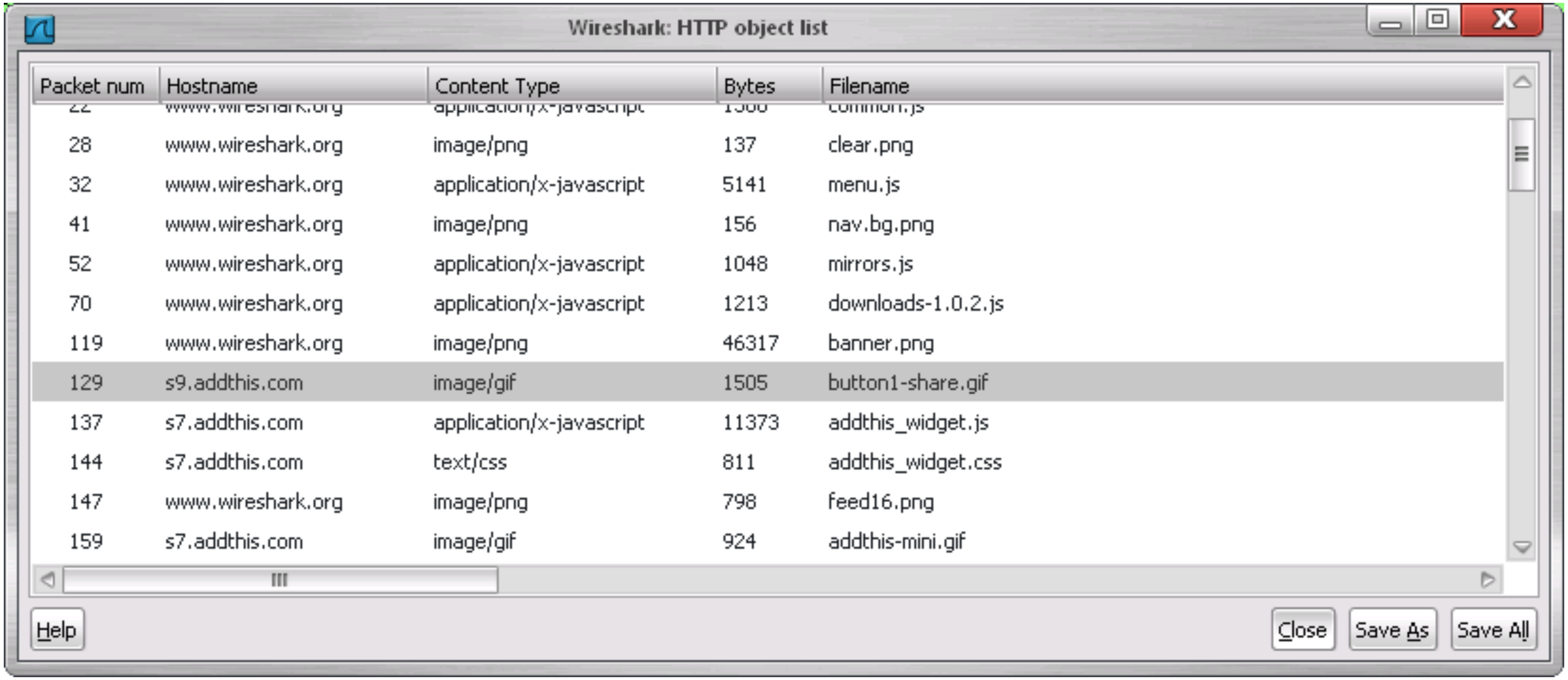
```
 e                    Destination        Protocol   Info
 168.1.102            192.168.1.104      SNMP       get-request SNMPv2-SMI
 168.1.104            192.168.1.102      SNMP       get-response SNMPv2-SMI
                      .168.1.104         SNMP       get-request SNMPv2-SMI
                      .168.1.102         SNMP       get-response SNMPv2-SMI
                      19                 DNS        Standard query A gaia.c
                      102                DNS        Standard query response
 168.1.102            128.119.245.12     TCP        unikeypro > http [SYN]
 119.245.12           192.168.1.102      TCP        http > unikeypro [SYN,
   9 4.694458   192.168.1.102   128.119.245.12   TCP    unikeypro > http [ACK]
  10 4.694850   192.168.1.102   128.119.245.12   HTTP   GET /ethereal-labs/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): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
```

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

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

Export HTTP Objects



Wireshark: HTTP object list

Packet num	Hostname	Content Type	Bytes	Filename
22	www.wireshark.org	application/x-javascript	[illegible]	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

Time for Fun!