Introduction to Using a Protocol Analyzer: Ethereal

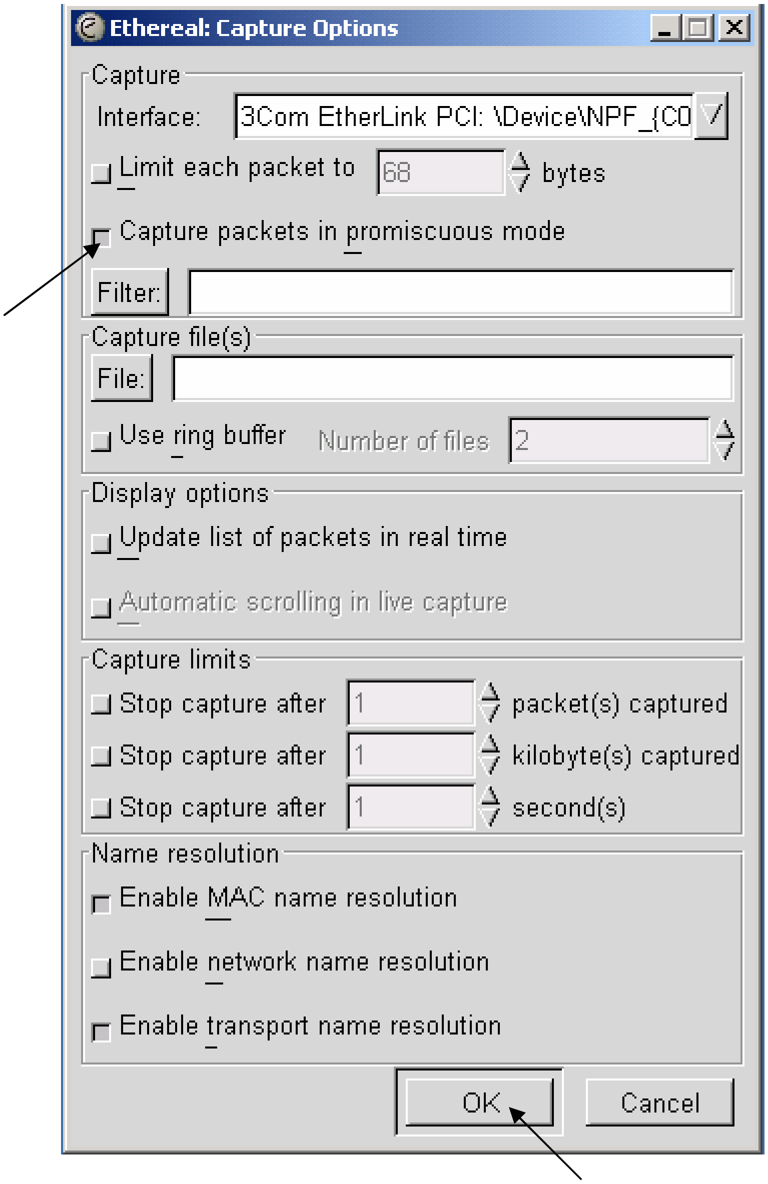
I. Downloading and Installing Ethereal

1. Go to: www.ethereal.com
2. From the left navigation bar choose: Download
3. Find "Microsoft: Windows (Intel, 32-bit)" under the Platform column, then click on the hyperlink: local archive under the Location column.
4. From step 1, click on the hyperlink WinPcap
5. From the left navigation bar select Downloads, then click on WinPcap auto-installer (driver +DLLs)
6. When the *Save as* window opens, save the plug to the desktop
7. Go back to the following link: http://www.ethereal.com/distribution/win32
8. Select: ethereal-setup-0.9.14.exe, which you will find towards the end of the screen.
9. Find Chapel Hill, NC in the location column, then click on the binary icon, in the same row, under the Download column, or click on the following link: http://prdownloads.sourceforge.net/ethereal/ethereal-setup-0.9.14.exe?use_mirror=unc
10. When the *Save as* window opens, download the application to your desktop.
11. Install WinPcap, using the default settings
12. Install Ethereal, Using the default settings

II. Capturing Packets with Ethereal

1. Double-click on the ethereal short-cut Icon on your desktop.
2. When the application opens select Start from the Capture menu.

3. Toggle off the “capture-packets-in promiscuous-mode” option(Figure1)



Ethereal: Capture Options

Capture

Interface: 3Com EtherLink PCI: \Device\NPF_{C0

☐ Limit each packet to 68 bytes

☑ Capture packets in promiscuous mode

Filter:

Capture file(s)

File:

☐ Use ring buffer Number of files 2

Display options

☐ Update list of packets in real time

☐ Automatic scrolling in live capture

Capture limits

☐ Stop capture after 1 packet(s) captured

☐ Stop capture after 1 kilobyte(s) captured

☐ Stop capture after 1 second(s)

Name resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

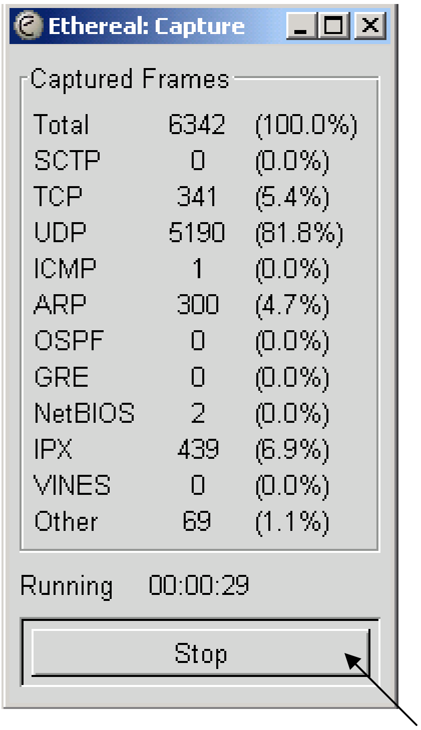
☑ Enable transport name resolution

Figure 1

4. Click on the OK command button

5. Open your browser and type www.cisco.com to generate some traffic.

6. Go back to the Ethereal: Capture window and click on the Stop command button(Figure 2)



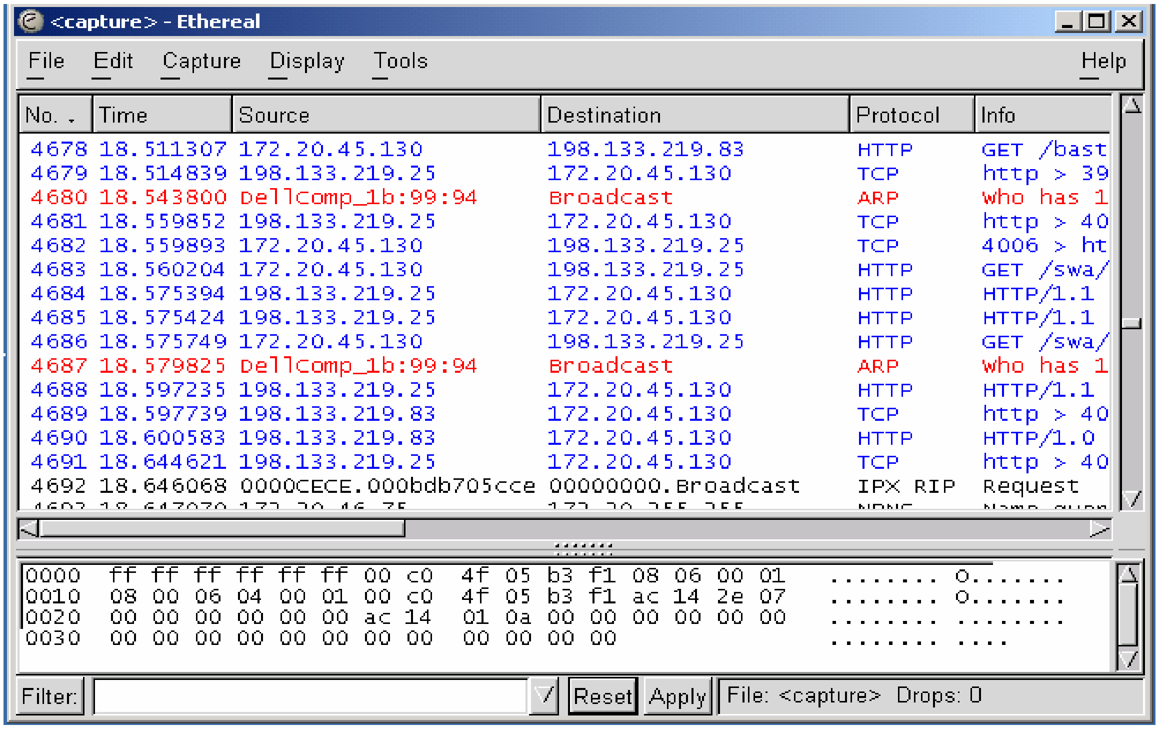
Captured Frames

Total	6342	(100.0%)
SCTP	0	(0.0%)
TCP	341	(5.4%)
UDP	5190	(81.8%)
ICMP	1	(0.0%)
ARP	300	(4.7%)
OSPF	0	(0.0%)
GRE	0	(0.0%)
NetBIOS	2	(0.0%)
IPX	439	(6.9%)
VINES	0	(0.0%)
Other	69	(1.1%)

Running 00:00:29

Figure 2

7. A similar screen to the one shown below will appear with all the captured frames



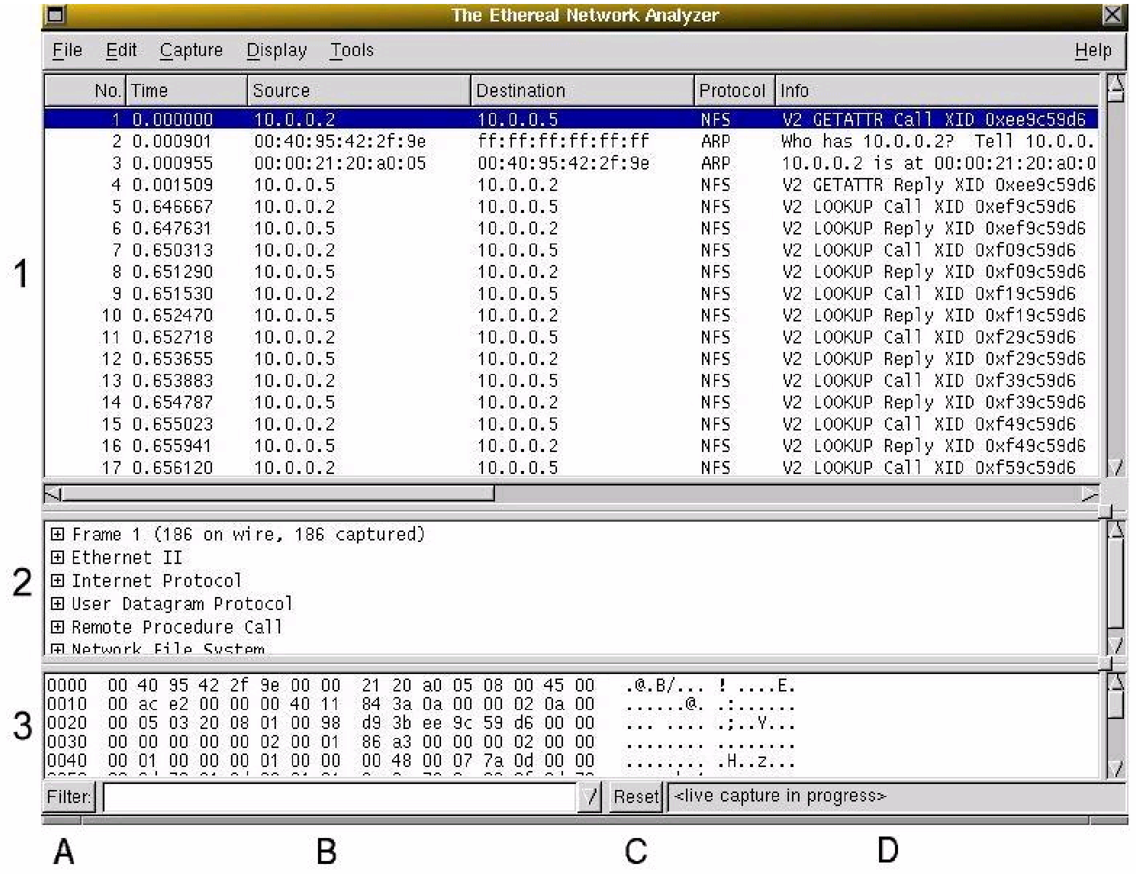
```
No.  Time      Source               Destination         Protocol Info
4678 18.511307 172.20.45.130        198.133.219.83      HTTP     GET /bast
4679 18.514839 198.133.219.25       172.20.45.130       TCP      http > 39
4680 18.543800 DellComp_1b:99:94    Broadcast           ARP      Who has 1
4681 18.559852 198.133.219.25       172.20.45.130       TCP      http > 40
4682 18.559893 172.20.45.130        198.133.219.25      TCP      4006 > ht
4683 18.560204 172.20.45.130        198.133.219.25      HTTP     GET /swa/
4684 18.575394 198.133.219.25       172.20.45.130       HTTP     HTTP/1.1
4685 18.575424 198.133.219.25       172.20.45.130       HTTP     HTTP/1.1
4686 18.575749 172.20.45.130        198.133.219.25      HTTP     GET /swa/
4687 18.579825 DellComp_1b:99:94    Broadcast           ARP      Who has 1
4688 18.597235 198.133.219.25       172.20.45.130       HTTP     HTTP/1.1
4689 18.597739 198.133.219.83       172.20.45.130       TCP      http > 40
4690 18.600583 198.133.219.83       172.20.45.130       HTTP     HTTP/1.0
4691 18.644621 198.133.219.25       172.20.45.130       TCP      http > 40
4692 18.646068 0000CECE.000bdb705cce 00000000.Broadcast IPX RIP  Request
4693 18.647070 172.20.46.75         172.20.255.255      NBNS     Name quer
```

```
0000   ff ff ff ff ff ff 00 c0  4f 05 b3 f1 08 06 00 01   ........ O.......
0010   08 00 06 04 00 01 00 c0  4f 05 b3 f1 ac 14 2e 07   ........ O.......
0020   00 00 00 00 00 00 ac 14  01 0a 00 00 00 00 00 00   ........ ........
0030   00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: <capture> Drops: 0

Figure 3

8. Examine Figure 4 to identify the components of the ethereal windo . You will notice that following:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.2	10.0.0.5	NFS	V2 GETATTR Call XID 0xee9c59d6
2	0.000901	00:40:95:42:2f:9e	ff:ff:ff:ff:ff:ff	ARP	Who has 10.0.0.2? Tell 10.0.0.
3	0.000955	00:00:21:20:a0:05	00:40:95:42:2f:9e	ARP	10.0.0.2 is at 00:00:21:20:a0:0
4	0.001509	10.0.0.5	10.0.0.2	NFS	V2 GETATTR Reply XID 0xee9c59d6
5	0.646667	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xef9c59d6
6	0.647631	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xef9c59d6
7	0.650313	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf09c59d6
8	0.651290	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xf09c59d6
9	0.651530	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf19c59d6
10	0.652470	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xf19c59d6
11	0.652718	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf29c59d6
12	0.653655	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xf29c59d6
13	0.653883	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf39c59d6
14	0.654787	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xf39c59d6
15	0.655023	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf49c59d6
16	0.655941	10.0.0.5	10.0.0.2	NFS	V2 LOOKUP Reply XID 0xf49c59d6
17	0.656120	10.0.0.2	10.0.0.5	NFS	V2 LOOKUP Call XID 0xf59c59d6

```
⊞ Frame 1 (186 on wire, 186 captured)
⊞ Ethernet II
⊞ Internet Protocol
⊞ User Datagram Protocol
⊞ Remote Procedure Call
⊞ Network File System
```

```
0000  00 40 95 42 2f 9e 00 00  21 20 a0 05 08 00 45 00   .@.B/... ! ....E.
0010  00 ac e2 00 00 00 40 11  84 3a 0a 00 00 02 0a 00   ......@. .:......
0020  00 05 03 20 08 01 00 98  d9 3b ee 9c 59 d6 00 00   ... .... .;..Y...
0030  00 00 00 00 00 02 00 01  86 a3 00 00 00 02 00 00   ........ ........
0040  00 01 00 00 00 01 00 00  00 48 00 07 7a 0d 00 00   ........ .H..z...
```

Figure 4

Ethereal is comprised of three main windows, or panes.

1. The top pane is the packet list pane. It displays a summary of each packet captured. By clicking on packets in this pane your control what is displayed in the other two panes.
2. The middle pane is the tree view pane. It displays the packet selected in the top pane in more detail.
3. The bottom pane is the data view pane. It displays the data from the packet selected in the top pane, and highlights the field selected in the tree view pane.

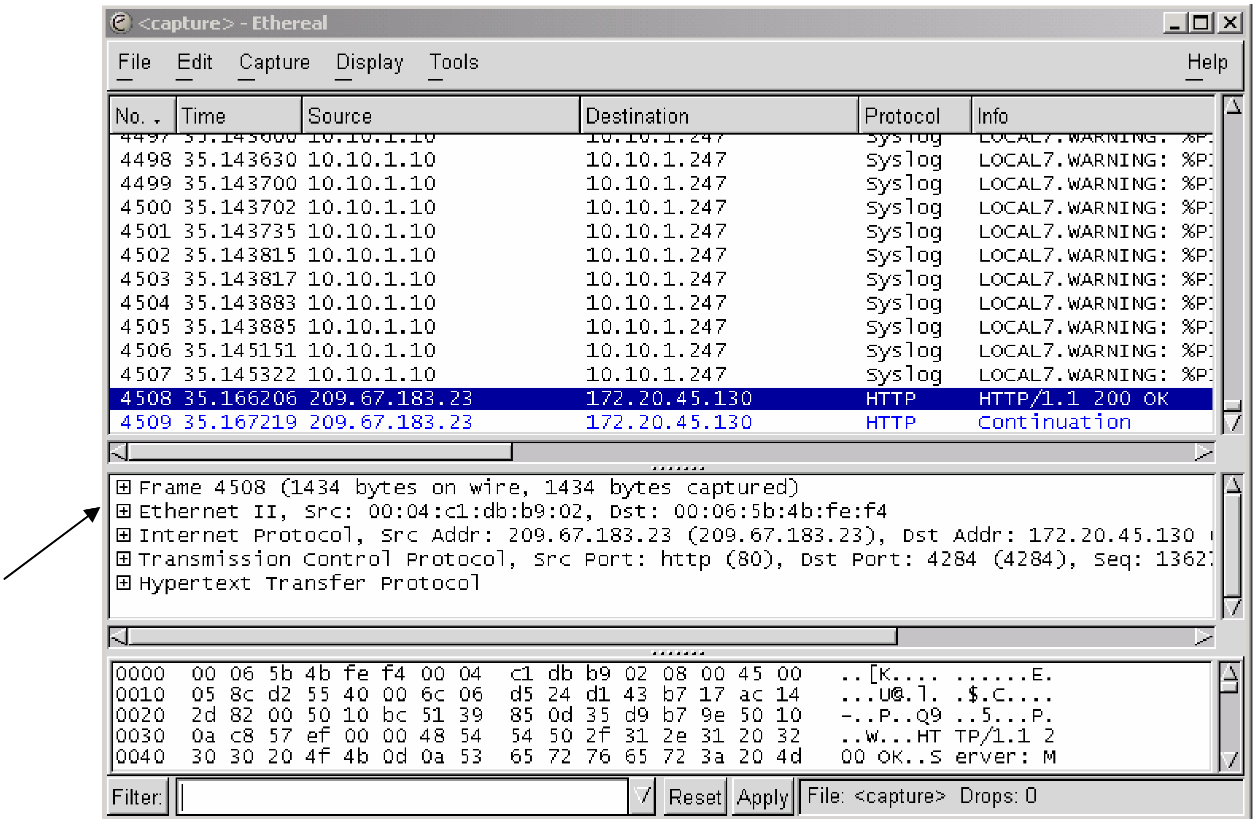
In addition to the three main panes, there are four elements of interest on the bottom of the ethereal main window.

A. The lower leftmost button labeled "Filter:" can be clicked to bring up the filter construction dialog.

B. The left middle text box provides an area to enter or edit filter strings. This is also where the current filter in effect it displayed. You can click on the pull down arrow to select past filter string from a list. More information on display filter strings is available in *the section called Filtering packets while viewing*
C. The right middle button labeled "Reset" clears the current filter.
D. The right text box displays informational messages. These message may indicate whether or not you are capturing, what file you have read into the packet list pane if you are not capturing. If you have selected a protocol field from the tree view pane and it is possible to filter on that field then the filter label for that protocol field will be displayed.

III. Analyzing Ethernet Encapsulation (RFC 894)

1. In the middle pane click on Ethernet II. (Figure 5)



```
No. .  Time      Source           Destination        Protocol  Info
4497 35.143600 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4498 35.143630 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4499 35.143700 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4500 35.143702 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4501 35.143735 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4502 35.143815 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4503 35.143817 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4504 35.143883 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4505 35.143885 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4506 35.145151 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4507 35.145322 10.10.1.10        10.10.1.247        Syslog    LOCAL7.WARNING: %P
4508 35.166206 209.67.183.23     172.20.45.130      HTTP      HTTP/1.1 200 OK
4509 35.167219 209.67.183.23     172.20.45.130      HTTP      Continuation
```

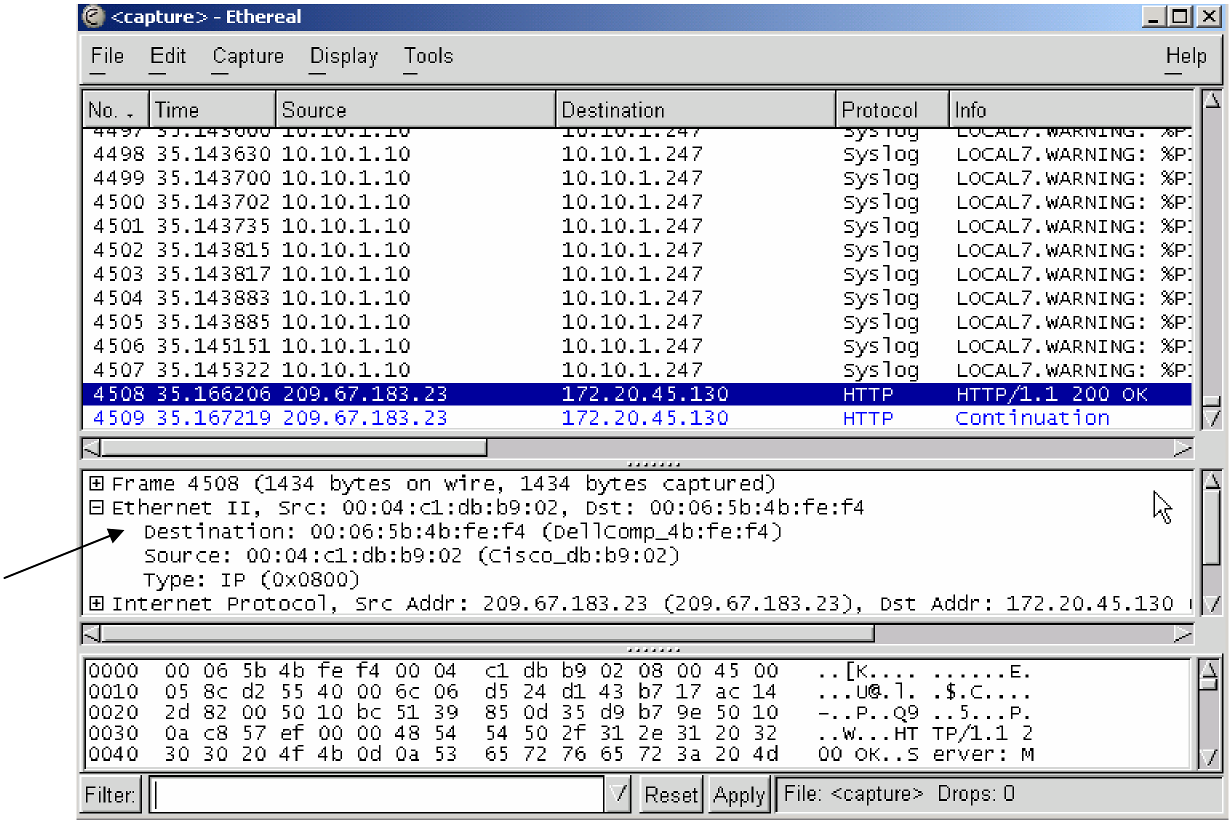
```
⊞ Frame 4508 (1434 bytes on wire, 1434 bytes captured)
⊞ Ethernet II, Src: 00:04:c1:db:b9:02, Dst: 00:06:5b:4b:fe:f4
⊞ Internet Protocol, Src Addr: 209.67.183.23 (209.67.183.23), Dst Addr: 172.20.45.130
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 4284 (4284), Seq: 1362
⊞ Hypertext Transfer Protocol
```

```
0000  00 06 5b 4b fe f4 00 04  c1 db b9 02 08 00 45 00   ..[K.... ......E.
0010  05 8c d2 55 40 00 6c 06  d5 24 d1 43 b7 17 ac 14   ...U@.l. .$.C....
0020  2d 82 00 50 10 bc 51 39  85 0d 35 d9 b7 9e 50 10   -..P..Q9 ..5...P.
0030  0a c8 57 ef 00 00 48 54  54 50 2f 31 2e 31 20 32   ..W...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 4d   00 OK..S erver: M
```

File: <capture> Drops: 0

Figure 5

2. Notice how the details of the Ethernet encapsulation collapses (Figure 6)



```
No.  Time      Source        Destination   Protocol  Info
4497 35.143600 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4498 35.143630 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4499 35.143700 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4500 35.143702 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4501 35.143735 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4502 35.143815 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4503 35.143817 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4504 35.143883 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4505 35.143885 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4506 35.145151 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4507 35.145322 10.10.1.10    10.10.1.247   Syslog    LOCAL7.WARNING: %P
4508 35.166206 209.67.183.23 172.20.45.130 HTTP      HTTP/1.1 200 OK
4509 35.167219 209.67.183.23 172.20.45.130 HTTP      Continuation
```

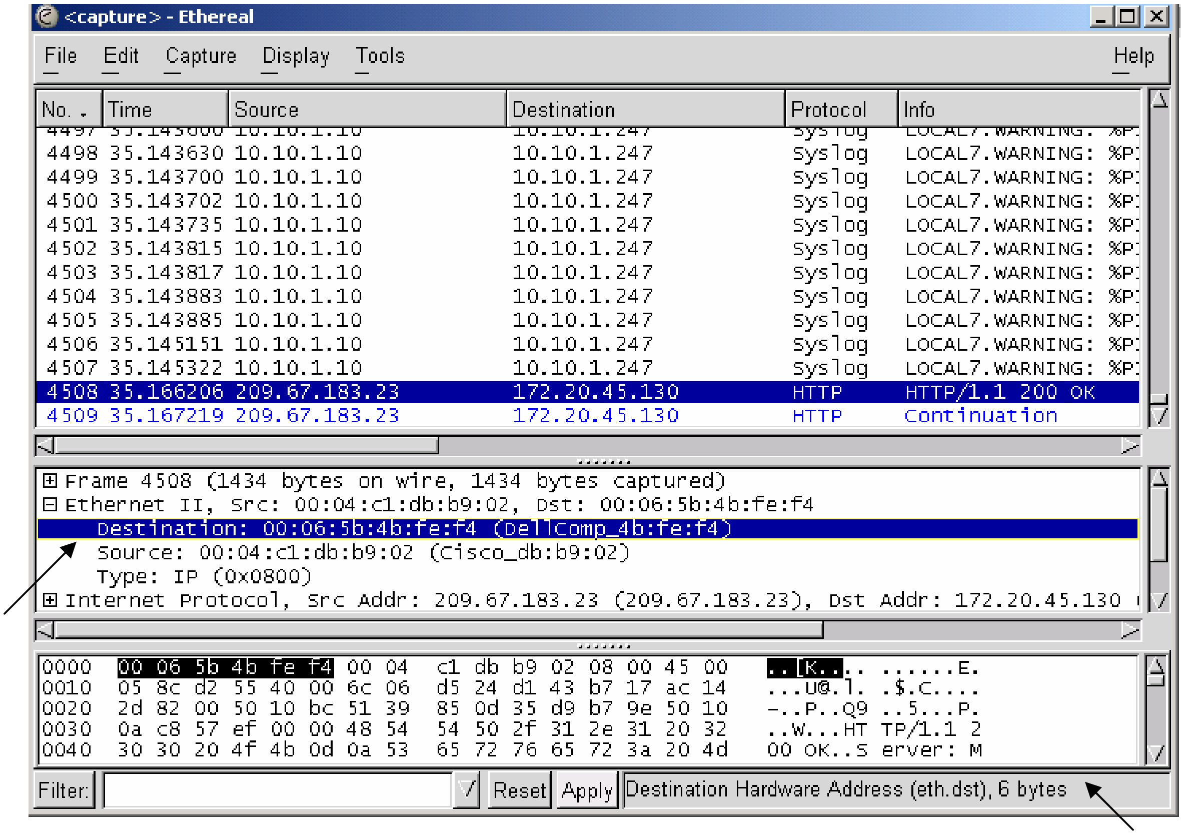
```
⊞ Frame 4508 (1434 bytes on wire, 1434 bytes captured)
⊟ Ethernet II, Src: 00:04:c1:db:b9:02, Dst: 00:06:5b:4b:fe:f4
    Destination: 00:06:5b:4b:fe:f4 (DellComp_4b:fe:f4)
    Source: 00:04:c1:db:b9:02 (Cisco_db:b9:02)
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 209.67.183.23 (209.67.183.23), Dst Addr: 172.20.45.130
```

```
0000  00 06 5b 4b fe f4 00 04  c1 db b9 02 08 00 45 00   ..[K.... ......E.
0010  05 8c d2 55 40 00 6c 06  d5 24 d1 43 b7 17 ac 14   ...U@.l. .$.C....
0020  2d 82 00 50 10 bc 51 39  85 0d 35 d9 b7 9e 50 10   -..P..Q9 ..5...P.
0030  0a c8 57 ef 00 00 48 54  54 50 2f 31 2e 31 20 32   ..W...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 4d   00 OK..S erver: M
```

File: <capture> Drops: 0

(Figure 6)

Select the Destination field from the Ethernet encapsulation. Can you tell the size of that field? (Figure 7). Hint: Check the right text box on the bottom of the ethereal main window.



No.	Time	Source	Destination	Protocol	Info
4497	35.143600	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4498	35.143630	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4499	35.143700	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4500	35.143702	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4501	35.143735	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4502	35.143815	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4503	35.143817	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4504	35.143883	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4505	35.143885	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4506	35.145151	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4507	35.145322	10.10.1.10	10.10.1.247	Syslog	LOCAL7.WARNING: %P
4508	35.166206	209.67.183.23	172.20.45.130	HTTP	HTTP/1.1 200 OK
4509	35.167219	209.67.183.23	172.20.45.130	HTTP	Continuation

```
⊞ Frame 4508 (1434 bytes on wire, 1434 bytes captured)
⊟ Ethernet II, Src: 00:04:c1:db:b9:02, Dst: 00:06:5b:4b:fe:f4
    Destination: 00:06:5b:4b:fe:f4 (DellComp_4b:fe:f4)
    Source: 00:04:c1:db:b9:02 (Cisco_db:b9:02)
    Type: IP (0x0800)
⊞ Internet Protocol, Src Addr: 209.67.183.23 (209.67.183.23), Dst Addr: 172.20.45.130
```

```
0000  00 06 5b 4b fe f4 00 04  c1 db b9 02 08 00 45 00   ..[K.... ......E.
0010  05 8c d2 55 40 00 6c 06  d5 24 d1 43 b7 17 ac 14   ...U@.l. .$.C....
0020  2d 82 00 50 10 bc 51 39  85 0d 35 d9 b7 9e 50 10   -..P..Q9 ..5...P.
0030  0a c8 57 ef 00 00 48 54  54 50 2f 31 2e 31 20 32   ..W...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 4d   00 OK..S erver: M
```

Destination Hardware Address (eth.dst), 6 bytes

Figure 7

3. Using ethereal identify the following Ethernet encapsulation fields and record their sizes in bytes in the provided boxes.

Destination Address	Source Address	Type	Data	CRC
□	□	□	□	□