CSCI 2150 – Computer Architecture
Serial Protocol/Packetyzer Lab

Purpose

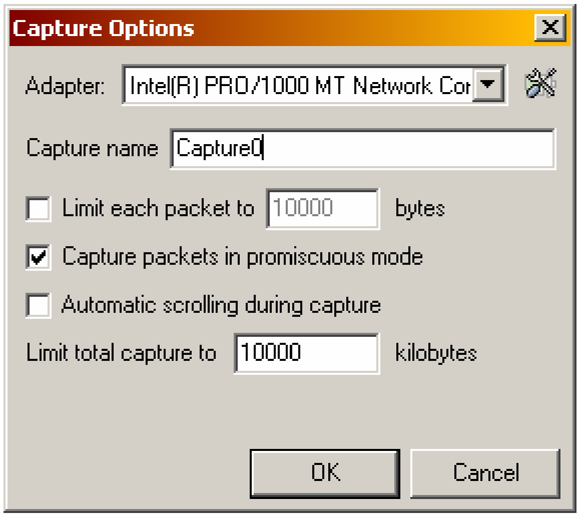
The purpose of this lab is to allow you to examine the raw data captured from an Ethernet port. It should reinforce the information presented during the serial protocols lecture by allowing you to examine the components that make up an Ethernet frame, an IP packet, and a TCP packet.

Starting Packetyzer

For this lab, we will be using a user interface for the Ethereal packet capture and dissection library called Packetyzer. It is licensed under the GNU General Public License and is free for download at http://www.networkchemistry.com/products/packetyzer.php.

Each of the laboratory PCs has an installation of Packetyzer which should have placed an icon on the desktop that looks like the icon in the figure to the right. Doubleclick on this icon to start Packetyzer.

Upon startup, Packetyzer prompts the user for the details of the capture session. These include the adaptor that will be monitored for packets, the name of the capture session, and any limits to be placed on the captured data. Even though we will be viewing captured data from a saved session, you should not hit cancel when this window appears.



Capture Options

Adapter: Intel(R) PRO/1000 MT Network Cor

Capture name Capture0

□ Limit each packet to 10000 bytes

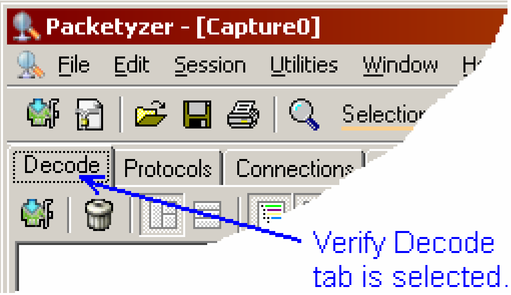
☑ Capture packets in promiscuous mode

□ Automatic scrolling during capture

Limit total capture to 10000 kilobytes

From the adapter window, an Ethernet adapter connected to an active TCP/IP network should be selected. In addition, to have a wide range of packets to examine, the box enabling promiscuous mode should be checked. This will allow Packetyzer to capture all messages seen by this adaptor. The capture name simply allows the user to identify the file name under which the captured data will be stored.

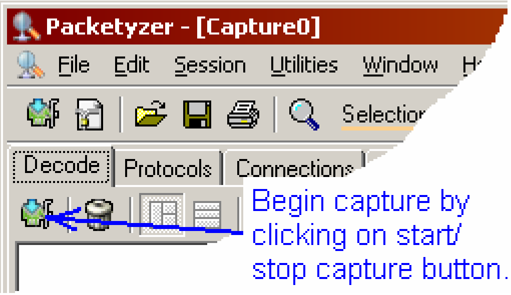
Once the user clicks on "OK", the Packetyzer main display screen appears. In order to begin a capture session, the decode tab should be selected.



Verify Decode tab is selected.

Capturing Live Data

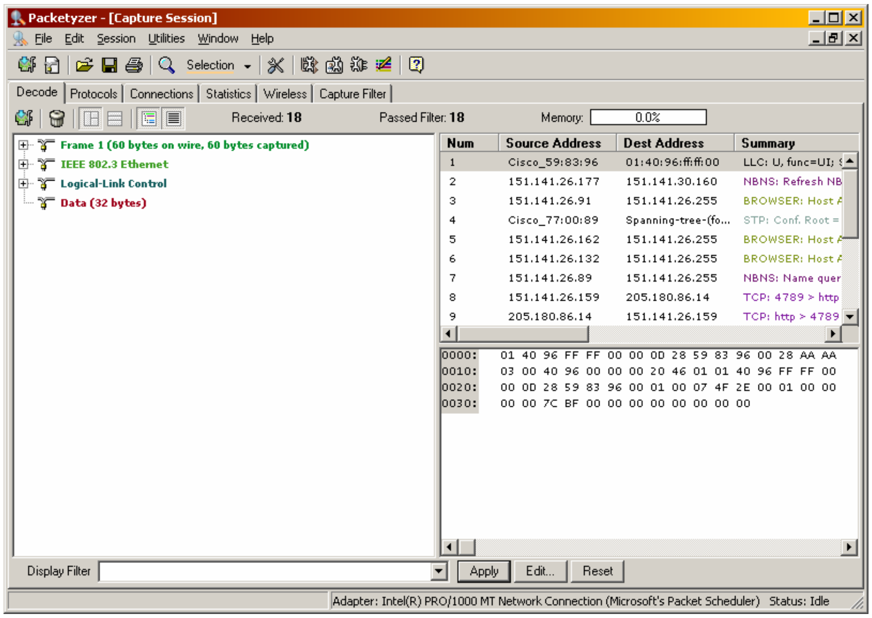
At this point, a simple capture can be performed by clicking on the start/stop capture button.



Begin capture by clicking on start/ stop capture button.

Once this button is pressed, packet information should begin to appear in the main display screen. In addition, the start/stop capture button should change such that a small red circle with a white "X" should appear. This button will now serve to stop the capture.

After a significant number of messages appear, the capture should be stopped in order to examine a specific message. The main display screen should look something like that shown in Figure A



Received: 18 Passed Filter: 18 Memory: 0.0%

- Frame 1 (60 bytes on wire, 60 bytes captured)
- IEEE 802.3 Ethernet
- Logical-Link Control
- Data (32 bytes)

Num	Source Address	Dest Address	Summary
1	Cisco_59:83:96	01:40:96:ff:ff:00	LLC: U, func=UI;
2	151.141.26.177	151.141.30.160	NBNS: Refresh NB
3	151.141.26.91	151.141.26.255	BROWSER: Host A
4	Cisco_77:00:89	Spanning-tree-(fo...	STP: Conf. Root =
5	151.141.26.162	151.141.26.255	BROWSER: Host A
6	151.141.26.132	151.141.26.255	BROWSER: Host A
7	151.141.26.89	151.141.26.255	NBNS: Name quer
8	151.141.26.159	205.180.86.14	TCP: 4789 > http
9	205.180.86.14	151.141.26.159	TCP: http > 4789

```
0000:   01 40 96 FF FF 00 00 0D 28 59 83 96 00 28 AA AA
0010:   03 00 40 96 00 00 00 20 46 01 01 40 96 FF FF 00
0020:   00 0D 28 59 83 96 00 01 00 07 4F 2E 00 01 00 00
0030:   00 00 7C BF 00 00 00 00 00 00 00 00
```

Adapter: Intel(R) PRO/1000 MT Network Connection (Microsoft's Packet Scheduler) Status: Idle

Figure A: Packetyzer Main Display Screen with Captured Data

Retrieving a Captured Session

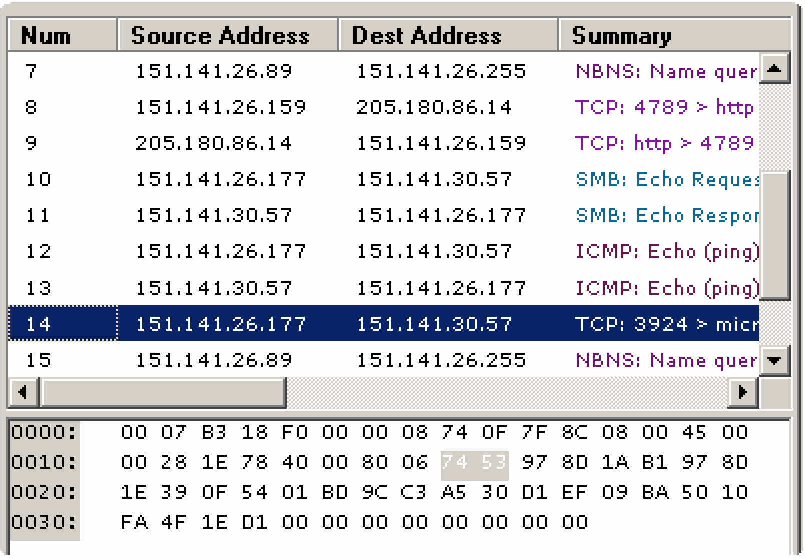
Since this lab will be run on the Wilson-Wallis machines where no live LAN connection is available, we will have to use a stored session. To retrieve a stored session, from the ***File*** menu, select ***Open***. Using the explorer window that appears, navigate to the root folder ***c:\***. You should see a file labeled "Sample Capture Session.cap". Select it and click on ***Open***. The data from this session should appear in the Packetyzer main display screen.

Evaluating a Frame

The three windows in the center of the main display screen present the statistics and data of the captured packets. The left window is the Tree Details view. You will use this view to examine the components of the received packets. (Note: Unless a packet has been selected from the top right window, the Tree Details view will be blank.)

The top right window, the Packet List view, presents a list of all of the packets received during the capture session. The bottom right window, the Hex and ASCII Details view, shows the octets of the captured packed selected in the Packet List view.

From the Packet List view, select a TCP packet. ***(If you are using the captured session, select the second packet.)*** This will allow the user to examine not only the Ethernet packet information, but also the TCP and IP packet information from the protocol stack. In Figure B, packet number 14, an acknowledge packet, has been selected.

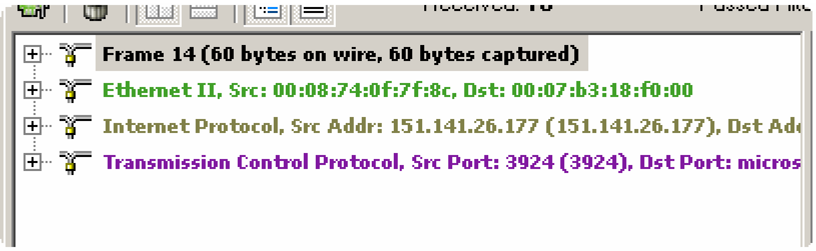


Num	Source Address	Dest Address	Summary
7	151.141.26.89	151.141.26.255	NBNS: Name quer
8	151.141.26.159	205.180.86.14	TCP: 4789 > http
9	205.180.86.14	151.141.26.159	TCP: http > 4789
10	151.141.26.177	151.141.30.57	SMB: Echo Reques
11	151.141.30.57	151.141.26.177	SMB: Echo Respor
12	151.141.26.177	151.141.30.57	ICMP: Echo (ping)
13	151.141.30.57	151.141.26.177	ICMP: Echo (ping)
14	151.141.26.177	151.141.30.57	TCP: 3924 > micr
15	151.141.26.89	151.141.26.255	NBNS: Name quer

```
0000:    00 07 B3 18 F0 00 00 08 74 0F 7F 8C 08 00 45 00
0010:    00 28 1E 78 40 00 80 06 74 53 97 8D 1A B1 97 8D
0020:    1E 39 0F 54 01 BD 9C C3 A5 30 D1 EF 09 BA 50 10
0030:    FA 4F 1E D1 00 00 00 00 00 00 00 00
```

Figure B: Packet List and Hex and ASCII Details Views with Message Selected

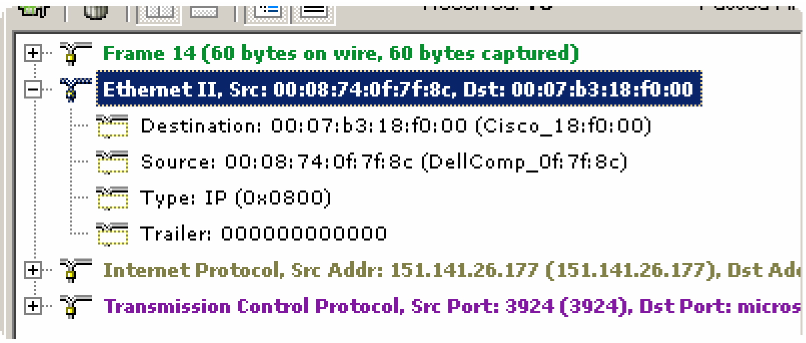
The Tree Details view now presents the parsed information from each of the protocols present in the packet. Figure C presents this view with each of the branches collapsed.



Frame 14 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:0f:7f:8c, Dst: 00:07:b3:18:f0:00
Internet Protocol, Src Addr: 151.141.26.177 (151.141.26.177), Dst Ad
Transmission Control Protocol, Src Port: 3924 (3924), Dst Port: micros

Figure C: Tree Details View with all Branches Collapsed

By clicking on the plus sign next to each of the protocols, the details of the frame are revealed. Figure D presents the Tree Details view with the details of the Ethernet frame revealed. Do this now for the Ethernet Frame.

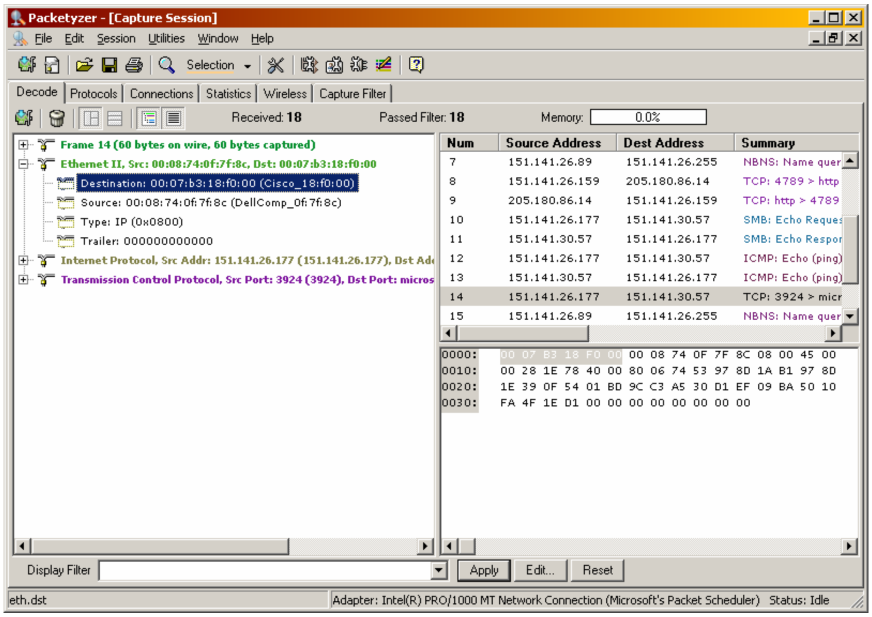


Frame 14 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:0f:7f:8c, Dst: 00:07:b3:18:f0:00
Destination: 00:07:b3:18:f0:00 (Cisco_18:f0:00)
Source: 00:08:74:0f:7f:8c (DellComp_0f:7f:8c)
Type: IP (0x0800)
Trailer: 000000000000
Internet Protocol, Src Addr: 151.141.26.177 (151.141.26.177), Dst Ad
Transmission Control Protocol, Src Port: 3924 (3924), Dst Port: micros

Figure D: Tree Details View with Ethernet Branch Expanded

Remember from the Ethernet frame discussion that the first three octets of the MAC address used by Ethernet identify the manufacturer. In the details revealed beneath the Ethernet identifier, it can be seen that the first three octets of the destination address in Figure D represents a Cisco NIC while the first three octets of the source address represents a Dell NIC.

From the frame selected in Figure D, we can see that Packetyzer has converted the raw data to user-friendly data in the Tree Details view. By highlighting an item of interest in the Tree Details view, you can see how the corresponding raw data is highlighted in the Hex and ASCII Details view. Notice in Figure E how by selecting the Ethernet destination, the corresponding raw data is highlighted in the Hex and ASCII Details view.


Packetyzer - [Capture Session]
File Edit Session Utilities Window Help
Selection
Decode Protocols Connections Statistics Wireless Capture Filter
Display Filter
Apply Edit... Reset

Received: 18 Passed Filter: 18 Memory: 0.0%

```
Frame 14 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:0f:7f:8c, Dst: 00:07:b3:18:f0:00
    Destination: 00:07:b3:18:f0:00 (Cisco_18:f0:00)
    Source: 00:08:74:0f:7f:8c (DellComp_0f:7f:8c)
    Type: IP (0x0800)
    Trailer: 000000000000
Internet Protocol, Src Addr: 151.141.26.177 (151.141.26.177), Dst Ad
Transmission Control Protocol, Src Port: 3924 (3924), Dst Port: micros
```

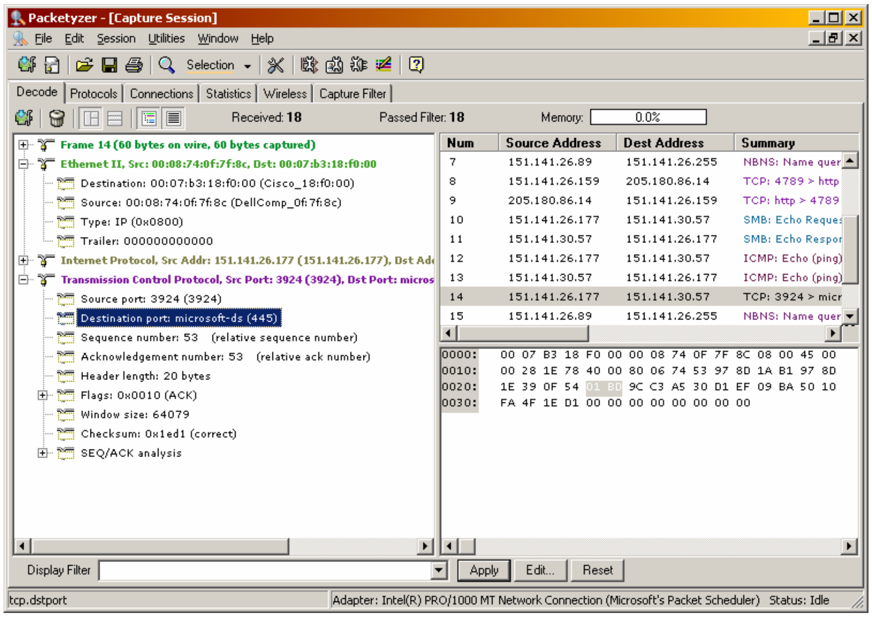
Num	Source Address	Dest Address	Summary
7	151.141.26.89	151.141.26.255	NBNS: Name quer
8	151.141.26.159	205.180.86.14	TCP: 4789 > http
9	205.180.86.14	151.141.26.159	TCP: http > 4789
10	151.141.26.177	151.141.30.57	SMB: Echo Reques
11	151.141.30.57	151.141.26.177	SMB: Echo Respor
12	151.141.26.177	151.141.30.57	ICMP: Echo (ping)
13	151.141.30.57	151.141.26.177	ICMP: Echo (ping)
14	151.141.26.177	151.141.30.57	TCP: 3924 > micr
15	151.141.26.89	151.141.26.255	NBNS: Name quer

```
0000:   00 07 B3 18 F0 00 00 08 74 0F 7F 8C 08 00 45 00
0010:   00 28 1E 78 40 00 80 06 74 53 97 8D 1A B1 97 8D
0020:   1E 39 0F 54 01 BD 9C C3 A5 30 D1 EF 09 BA 50 10
0030:   FA 4F 1E D1 00 00 00 00 00 00 00 00
```

eth.dst Adapter: Intel(R) PRO/1000 MT Network Connection (Microsoft's Packet Scheduler) Status: Idle

Figure E: Message with Raw Ethernet Destination Address Highlighted

Similarly, the raw data for each of the elements of the Ethernet frame and the IP and TCP packets can be identified. Figure F shows the TCP destination port highlighted in the Hex and ASCII Details view.


Packetyzer - [Capture Session]
File Edit Session Utilities Window Help
Selection
Decode Protocols Connections Statistics Wireless Capture Filter
Display Filter
Apply Edit... Reset

Received: 18 Passed Filter: 18 Memory: 0.0%

```
Frame 14 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:08:74:0f:7f:8c, Dst: 00:07:b3:18:f0:00
    Destination: 00:07:b3:18:f0:00 (Cisco_18:f0:00)
    Source: 00:08:74:0f:7f:8c (DellComp_0f:7f:8c)
    Type: IP (0x0800)
    Trailer: 000000000000
Internet Protocol, Src Addr: 151.141.26.177 (151.141.26.177), Dst Ad
Transmission Control Protocol, Src Port: 3924 (3924), Dst Port: micros
    Source port: 3924 (3924)
    Destination port: microsoft-ds (445)
    Sequence number: 53    (relative sequence number)
    Acknowledgement number: 53    (relative ack number)
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
    Window size: 64079
    Checksum: 0x1ed1 (correct)
    SEQ/ACK analysis
```

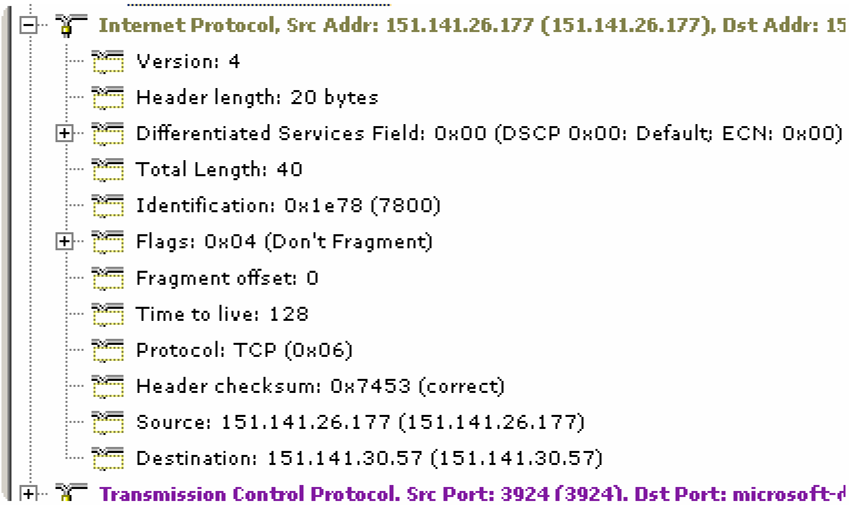
Num	Source Address	Dest Address	Summary
7	151.141.26.89	151.141.26.255	NBNS: Name quer
8	151.141.26.159	205.180.86.14	TCP: 4789 > http
9	205.180.86.14	151.141.26.159	TCP: http > 4789
10	151.141.26.177	151.141.30.57	SMB: Echo Reques
11	151.141.30.57	151.141.26.177	SMB: Echo Respor
12	151.141.26.177	151.141.30.57	ICMP: Echo (ping)
13	151.141.30.57	151.141.26.177	ICMP: Echo (ping)
14	151.141.26.177	151.141.30.57	TCP: 3924 > micr
15	151.141.26.89	151.141.26.255	NBNS: Name quer

```
0000:   00 07 B3 18 F0 00 00 08 74 0F 7F 8C 08 00 45 00
0010:   00 28 1E 78 40 00 80 06 74 53 97 8D 1A B1 97 8D
0020:   1E 39 0F 54 01 BD 9C C3 A5 30 D1 EF 09 BA 50 10
0030:   FA 4F 1E D1 00 00 00 00 00 00 00 00
```

tcp.dstport Adapter: Intel(R) PRO/1000 MT Network Connection (Microsoft's Packet Scheduler) Status: Idle

Figure F: Message with TCP Destination Port Identified

By expanding the branch for the IP header, the properties of the IP packet can be examined as shown in Figure G.



```
Internet Protocol, Src Addr: 151.141.26.177 (151.141.26.177), Dst Addr: 15
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0x1e78 (7800)
    Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x7453 (correct)
    Source: 151.141.26.177 (151.141.26.177)
    Destination: 151.141.30.57 (151.141.30.57)
Transmission Control Protocol, Src Port: 3924 (3924), Dst Port: microsoft-d
```

Figure G: Details of Internet Protocol Packet Revealed

From this expansion, the user can select the total length from the detailed view. This highlights the two octets from the IP packet 00 28 (hex). By highlighting the Internet Protocol heading, the beginning of the IP packet can be identified. If the user were to count the number of octets contained in the packet and subsequent data (the TCP packet) of this example, they would see that there are in fact 40 octets. (Note that in this example, the last six octets of the Ethernet frame are from the Ethernet trailer.) Do this now for your captured data. (IMPORTANT: You have a lot more to count than 40 bytes! Do yourself a favor and begin by counting the number of full lines, then multiplying this by 16. Then add in the number of bytes from the partial lines. You should get a value that equals the IP total length field.)

Finish the lab now by identifying the remaining fields and recording them on your laboratory worksheet. Before you leave, turn in your worksheet to the instructor.

References

Openxtra (2003), *Packetyzer User Guide*, West Yorkshire, UK, OPENXTRA Limited, October 2003.

Waters, Chris (project manager) (2003), Network Chemistry, *Packetyzer - Network Packet Analyzer*, *http://sourceforge.net/projects/packetyzer*. Retrieved May 26, 2005, from http://sourceforge.net/projects/packetyzer.