Advanced Diploma of Industrial Data Communications, Networking and IT
(DIT)

Module 2
Industrial Ethernet

Lab Instructions for Ethernet Basics

V2

Created By:	Deon Reynders	Date:	15 July 2013

ENGINEERING INSTITUTE OF TECHNOLOGY

DIT Lab 2: Ethernet Basics

1.0 Overview

In these exercises we will focus on attributes of Ethernet, in particular the header structure and speed/duplex settings.

2.0 Hardware

You will perform these exercises on your own computer. If, for any reason, you are unable to install the software on your computer, or encounter any other technical difficulties, then you must immediately contact your course coordinator.

3.0 Software

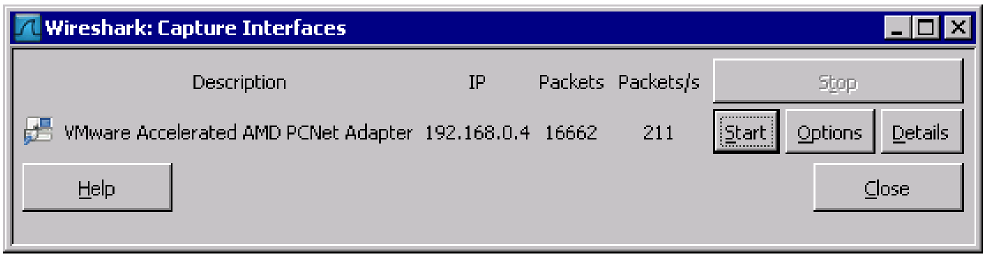
- Wireshark (download from http://www.wireshark.org/download.html)
- Screen capture software. Jing and Screenhunter Free are examples of free screen capturing software. When downloading or installing such software, please be careful not to install any unnecessary add-ons eg. Toolbars. Select 'advanced' installation and decline all offers.

4.0 Implementation

4.1 Capturing Ethernet frame and verifying type of frame

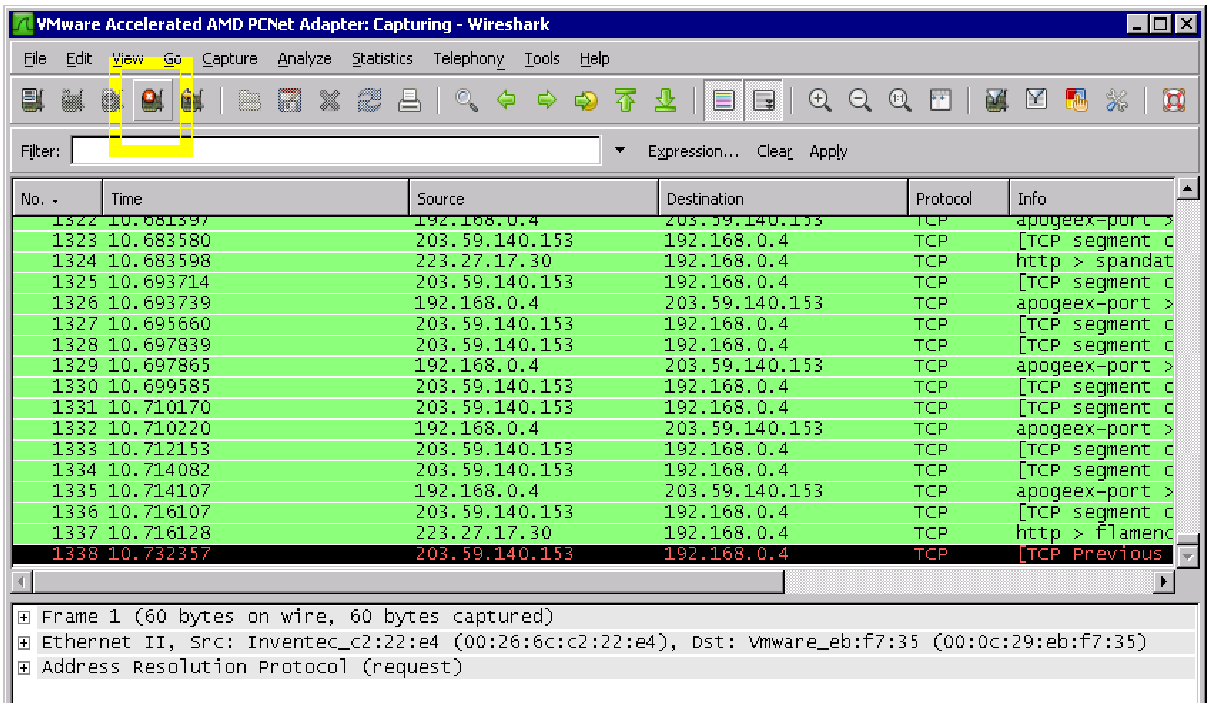
- Run Wireshark by clicking on the desktop icon

- Capture several frames by clicking Start-> Interfaces and then clicking the ‘Start’ button against the interface currently in use (i.e. the one that shows an increasing number of packets). On newer versions of Wireshark you first need to check the box against the desired interface before hitting ‘Start’



Description	IP	Packets	Packets/s
VMware Accelerated AMD PCNet Adapter	192.168.0.4	16662	211

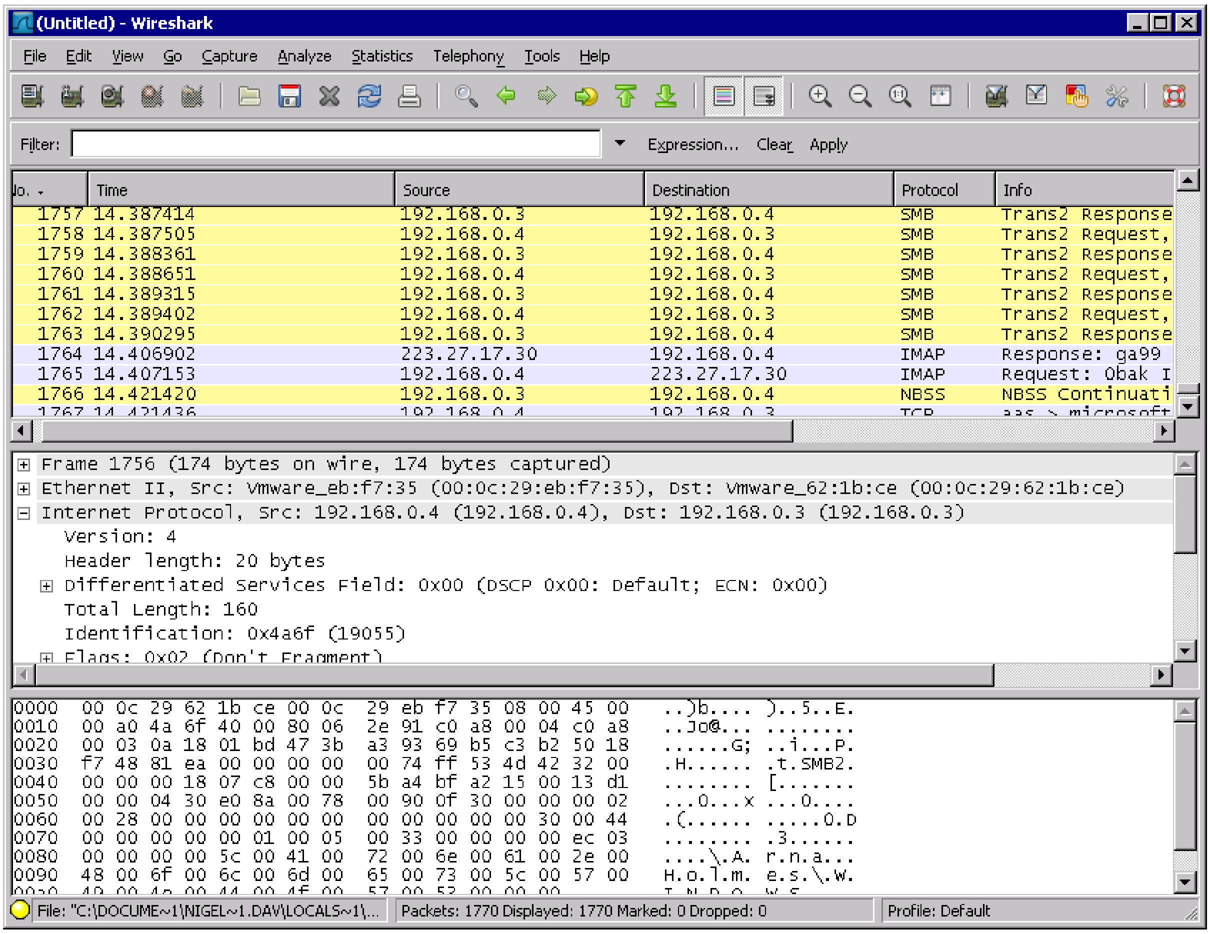
Capture a few packets, and then stop Wireshark



No.	Time	Source	Destination	Protocol	Info
1322	10.681397	192.168.0.4	203.59.140.153	TCP	apogeex-port >
1323	10.683580	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1324	10.683598	223.27.17.30	192.168.0.4	TCP	http > spandat
1325	10.693714	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1326	10.693739	192.168.0.4	203.59.140.153	TCP	apogeex-port >
1327	10.695660	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1328	10.697839	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1329	10.697865	192.168.0.4	203.59.140.153	TCP	apogeex-port >
1330	10.699585	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1331	10.710170	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1332	10.710220	192.168.0.4	203.59.140.153	TCP	apogeex-port >
1333	10.712153	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1334	10.714082	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1335	10.714107	192.168.0.4	203.59.140.153	TCP	apogeex-port >
1336	10.716107	203.59.140.153	192.168.0.4	TCP	[TCP segment c
1337	10.716128	223.27.17.30	192.168.0.4	TCP	http > flamenc
1338	10.732357	203.59.140.153	192.168.0.4	TCP	[TCP Previous

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Inventec_c2:22:e4 (00:26:6c:c2:22:e4), Dst: Vmware_eb:f7:35 (00:0c:29:eb:f7:35)
⊞ Address Resolution Protocol (request)
```

- Divide the screen into three equal parts. The upper part shows a summary of the packets captured, the middle part shows the contents of the selected frame (packet) in terms of headers etc., and the lower part shows the contents of the selected frame in Hex and ASCII



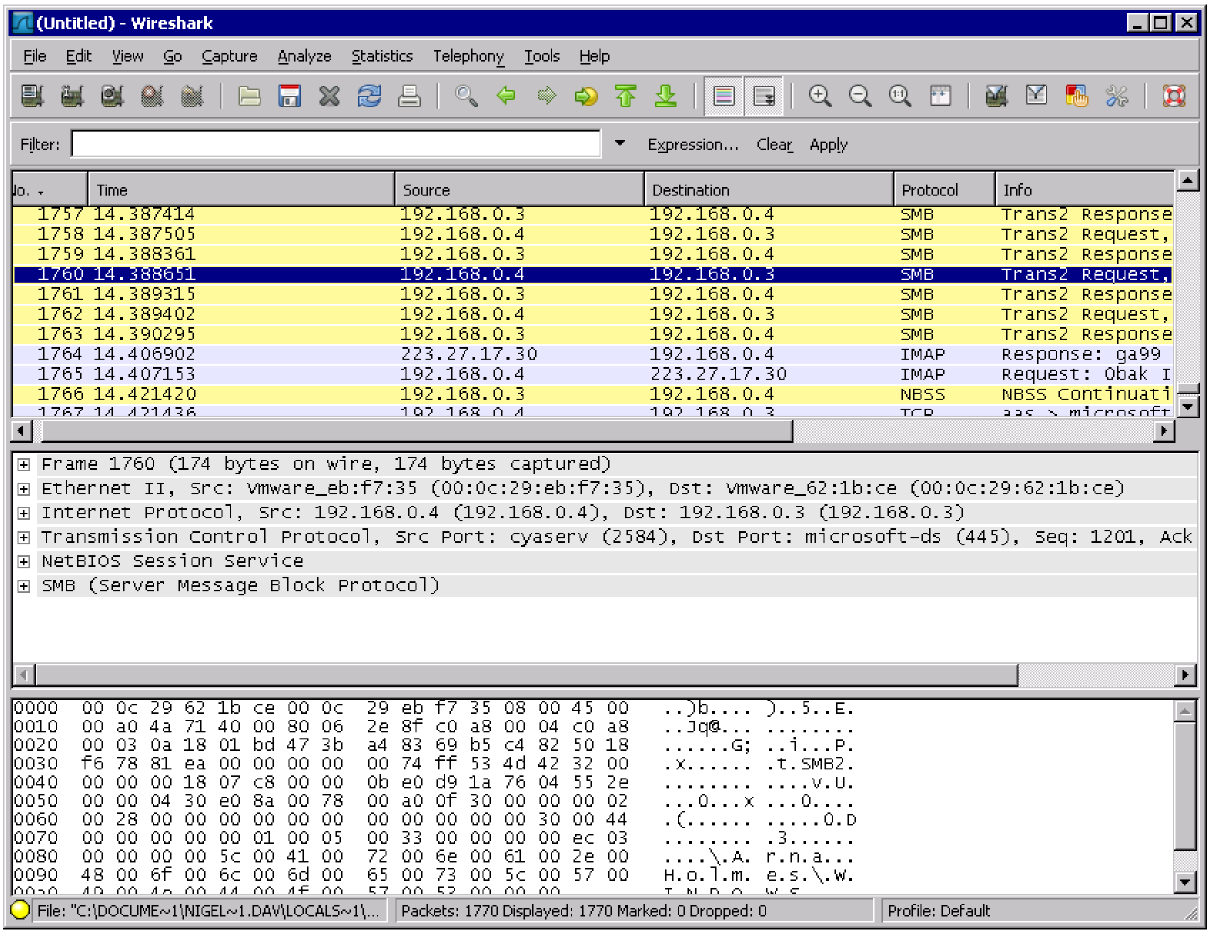
```
No. .  Time          Source          Destination     Protocol  Info
 1757 14.387414      192.168.0.3     192.168.0.4     SMB       Trans2 Response
 1758 14.387505      192.168.0.4     192.168.0.3     SMB       Trans2 Request,
 1759 14.388361      192.168.0.3     192.168.0.4     SMB       Trans2 Response
 1760 14.388651      192.168.0.4     192.168.0.3     SMB       Trans2 Request,
 1761 14.389315      192.168.0.3     192.168.0.4     SMB       Trans2 Response
 1762 14.389402      192.168.0.4     192.168.0.3     SMB       Trans2 Request,
 1763 14.390295      192.168.0.3     192.168.0.4     SMB       Trans2 Response
 1764 14.406902      223.27.17.30    192.168.0.4     IMAP      Response: ga99
 1765 14.407153      192.168.0.4     223.27.17.30    IMAP      Request: 0bak I
 1766 14.421420      192.168.0.3     192.168.0.4     NBSS      NBSS Continuati
 1767 14.421436      192.168.0.4     192.168.0.3     TCP       aas > microsoft
```

```
⊞ Frame 1756 (174 bytes on wire, 174 bytes captured)
⊞ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
⊟ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 160
    Identification: 0x4a6f (19055)
  ⊞ Flags: 0x02 (Don't Fragment)
```

```
0000  00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010  00 a0 4a 6f 40 00 80 06  2e 91 c0 a8 00 04 c0 a8   ..Jo@... ........
0020  00 03 0a 18 01 bd 47 3b  a3 93 69 b5 c3 b2 50 18   ......G; ..i...P.
0030  f7 48 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .H...... .t.SMB2.
0040  00 00 00 18 07 c8 00 00  5b a4 bf a2 15 00 13 d1   ........ [.......
0050  00 00 04 30 e0 8a 00 78  00 90 0f 30 00 00 00 02   ...0...x ...0....
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070  00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080  00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090  48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
00a0  49 00 4e 00 44 00 4f 00  57 00 53 00 00 00         I.N.D.O. W.S.
```

File: "C:\DOCUME~1\NIGEL~1.DAV\LOCALS~1\... | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

- Select any packet (frame) in the top section of the screen



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1757	14.387414	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1758	14.387505	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1759	14.388361	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1760	14.388651	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1761	14.389315	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1762	14.389402	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1763	14.390295	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1764	14.406902	223.27.17.30	192.168.0.4	IMAP	Response: ga99
1765	14.407153	192.168.0.4	223.27.17.30	IMAP	Request: 0bak I
1766	14.421420	192.168.0.3	192.168.0.4	NBSS	NBSS Continuati
1767	14.421436	192.168.0.4	192.168.0.3	TCP	aas > microsoft

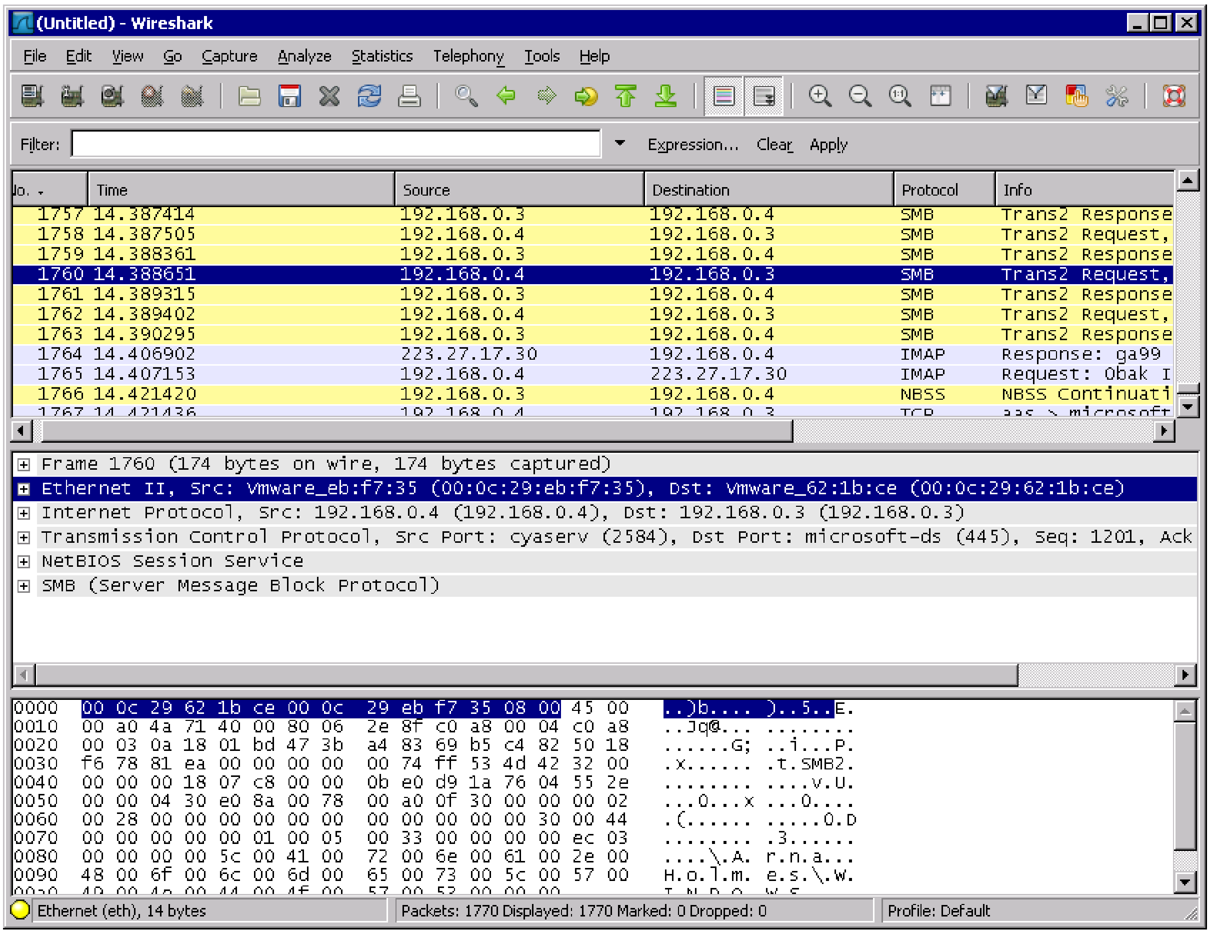
```
⊞ Frame 1760 (174 bytes on wire, 174 bytes captured)
⊞ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
⊞ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
⊞ Transmission Control Protocol, Src Port: cyaserv (2584), Dst Port: microsoft-ds (445), Seq: 1201, Ack
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010  00 a0 4a 71 40 00 80 06  2e 8f c0 a8 00 04 c0 a8   ..Jq@... ........
0020  00 03 0a 18 01 bd 47 3b  a4 83 69 b5 c4 82 50 18   ......G; ..i...P.
0030  f6 78 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .x...... .t.SMB2.
0040  00 00 00 18 07 c8 00 00  0b e0 d9 1a 76 04 55 2e   ........ ....v.U.
0050  00 00 04 30 e0 8a 00 78  00 a0 0f 30 00 00 00 02   ...0...x ...0....
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070  00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080  00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090  48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
```

File: "C:\DOCUME~1\NIGEL~1.DAV\LOCALS~1\... | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

- Go to the SECOND line in the centre section of the screen. This corresponds with Layer 2 (Data Link Layer) in the OSI model and hence, in ourcase, to Ethernet

Note that it is likely to be an Ethernet II (also known as Ethernet V2 or 'Bluebook) frame. Ethernet IEEE 802.3 frames will be labelled as such…but are fairly rare.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

lo.	Time	Source	Destination	Protocol	Info
1757	14.387414	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1758	14.387505	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1759	14.388361	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1760	14.388651	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1761	14.389315	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1762	14.389402	192.168.0.4	192.168.0.3	SMB	Trans2 Request,
1763	14.390295	192.168.0.3	192.168.0.4	SMB	Trans2 Response
1764	14.406902	223.27.17.30	192.168.0.4	IMAP	Response: ga99
1765	14.407153	192.168.0.4	223.27.17.30	IMAP	Request: 0bak I
1766	14.421420	192.168.0.3	192.168.0.4	NBSS	NBSS Continuati
1767	14.421436	192.168.0.4	192.168.0.3	TCP	aas > microsoft

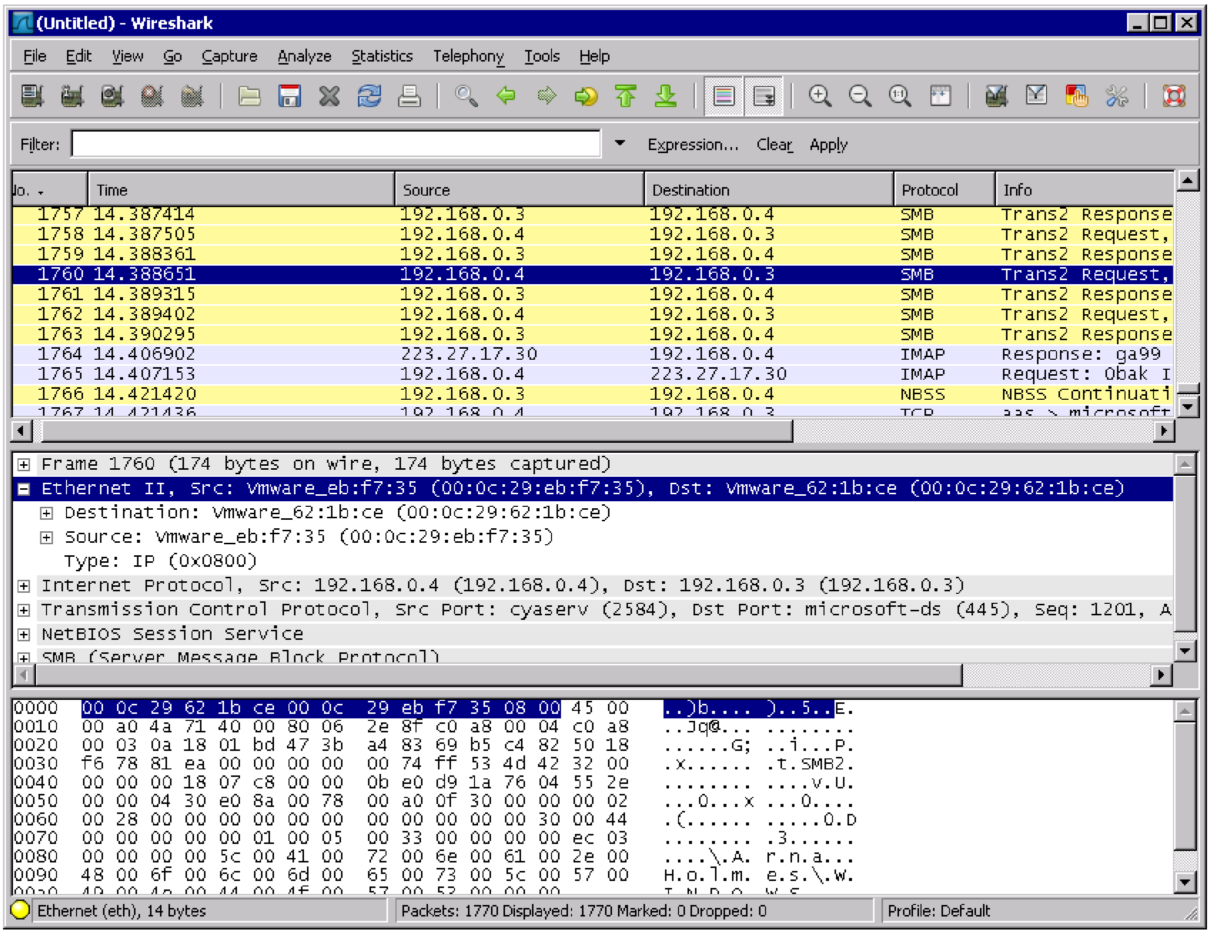
```
⊞ Frame 1760 (174 bytes on wire, 174 bytes captured)
⊞ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
⊞ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
⊞ Transmission Control Protocol, Src Port: cyaserv (2584), Dst Port: microsoft-ds (445), Seq: 1201, Ack
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010  00 a0 4a 71 40 00 80 06  2e 8f c0 a8 00 04 c0 a8   ..Jq@... ........
0020  00 03 0a 18 01 bd 47 3b  a4 83 69 b5 c4 82 50 18   ......G; ..i...P.
0030  f6 78 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .x...... .t.SMB2.
0040  00 00 00 18 07 c8 00 00  0b e0 d9 1a 76 04 55 2e   ........ ....v.U.
0050  00 00 04 30 e0 8a 00 78  00 a0 0f 30 00 00 00 02   ...0...x ...0....
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070  00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080  00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090  48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
00a0  49 00 4e 00 44 00 4f 00  57 00 53 00 00 00         I.N.D.O. W.S.
```

Ethernet (eth), 14 bytes | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

- Click the [+] ONCE so that the Ethernet header opens up. You will see the source and destination hardware ('MAC') addresses. Click on them individually, and observe the actual MAC addresses (hexadecimal) in the bottom pane on the screen.

They should resemble the example below.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

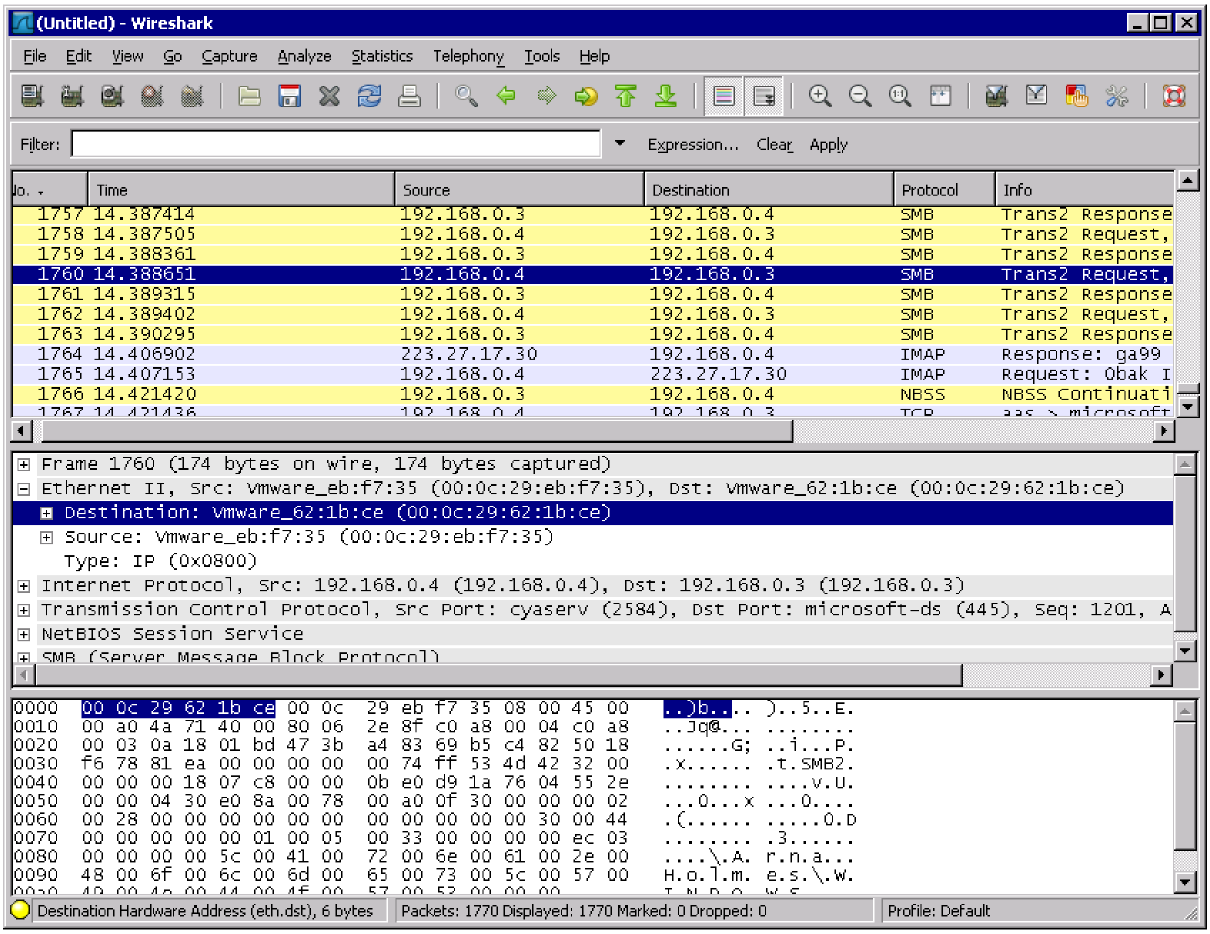
```
No. .  Time         Source         Destination    Protocol  Info
 1757 14.387414     192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1758 14.387505     192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1759 14.388361     192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1760 14.388651     192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1761 14.389315     192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1762 14.389402     192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1763 14.390295     192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1764 14.406902     223.27.17.30   192.168.0.4    IMAP      Response: ga99
 1765 14.407153     192.168.0.4    223.27.17.30   IMAP      Request: 0bak I
 1766 14.421420     192.168.0.3    192.168.0.4    NBSS      NBSS Continuati
 1767 14.421436     192.168.0.4    192.168.0.3    TCP       aas > microsoft
```

```
⊞ Frame 1760 (174 bytes on wire, 174 bytes captured)
⊟ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
  ⊞ Destination: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
  ⊞ Source: Vmware_eb:f7:35 (00:0c:29:eb:f7:35)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
⊞ Transmission Control Protocol, Src Port: cyaserv (2584), Dst Port: microsoft-ds (445), Seq: 1201, A
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010  00 a0 4a 71 40 00 80 06  2e 8f c0 a8 00 04 c0 a8   ..Jq@... ........
0020  00 03 0a 18 01 bd 47 3b  a4 83 69 b5 c4 82 50 18   ......G; ..i...P.
0030  f6 78 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .x...... .t.SMB2.
0040  00 00 00 18 07 c8 00 00  0b e0 d9 1a 76 04 55 2e   ........ ....v.U.
0050  00 00 04 30 e0 8a 00 78  00 a0 0f 30 00 00 00 02   ...0...x ...0....
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070  00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080  00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090  48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
```

Ethernet (eth), 14 bytes | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

Note that, if you select a particular field within the header (in the centre section of the display), the corresponding bytes in the 'raw' data captured from the network is highlighted as well, in the bottom section of the screen as in the following example


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source        Destination   Protocol Info
  1757 14.387414  192.168.0.3   192.168.0.4   SMB      Trans2 Response
  1758 14.387505  192.168.0.4   192.168.0.3   SMB      Trans2 Request,
  1759 14.388361  192.168.0.3   192.168.0.4   SMB      Trans2 Response
  1760 14.388651  192.168.0.4   192.168.0.3   SMB      Trans2 Request,
  1761 14.389315  192.168.0.3   192.168.0.4   SMB      Trans2 Response
  1762 14.389402  192.168.0.4   192.168.0.3   SMB      Trans2 Request,
  1763 14.390295  192.168.0.3   192.168.0.4   SMB      Trans2 Response
  1764 14.406902  223.27.17.30  192.168.0.4   IMAP     Response: ga99
  1765 14.407153  192.168.0.4   223.27.17.30  IMAP     Request: 0bak I
  1766 14.421420  192.168.0.3   192.168.0.4   NBSS     NBSS Continuati
  1767 14.421436  192.168.0.4   192.168.0.3   TCP      aas > microsoft
```

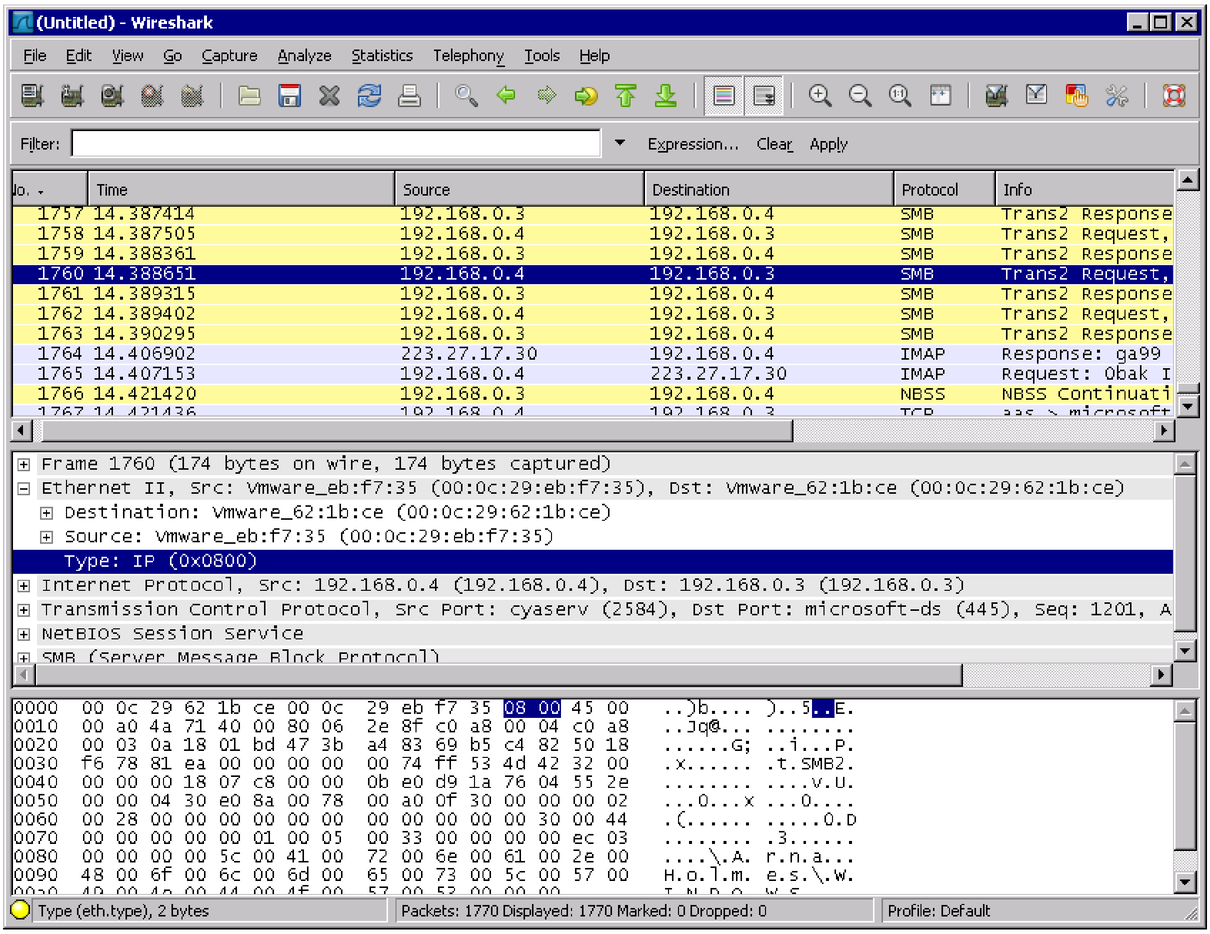
```
⊞ Frame 1760 (174 bytes on wire, 174 bytes captured)
⊟ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
  ⊞ Destination: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
  ⊞ Source: Vmware_eb:f7:35 (00:0c:29:eb:f7:35)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
⊞ Transmission Control Protocol, Src Port: cyaserv (2584), Dst Port: microsoft-ds (445), Seq: 1201, A
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000  00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010  00 a0 4a 71 40 00 80 06  2e 8f c0 a8 00 04 c0 a8   ..Jq@... ........
0020  00 03 0a 18 01 bd 47 3b  a4 83 69 b5 c4 82 50 18   ......G; ..i...P.
0030  f6 78 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .x...... .t.SMB2.
0040  00 00 00 18 07 c8 00 00  0b e0 d9 1a 76 04 55 2e   ........ ....v.U.
0050  00 00 04 30 e0 8a 00 78  00 a0 0f 30 00 00 00 02   ...0...x ...0....
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070  00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080  00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090  48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
00a0  49 00 4e 00 44 00 4f 00  57 00 53 00 00 00         I.N.D.O. W.S...
```

Destination Hardware Address (eth.dst), 6 bytes | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

Question 1: Snag the Ethernet header, but only the 4 lines comprising the header. In other words your snag should show the summary for the Ethernet header, plus the three fields comprising the header (as displayed in the centre part of the screen)

- Now observe the 3rd field.
  Since it contains a ‘Type’ number we know it is a V2 frame.
  For the IEEE 802.3 format this would be a ‘Length’ field.



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .   Time       Source         Destination    Protocol  Info
 1757 14.387414    192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1758 14.387505    192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1759 14.388361    192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1760 14.388651    192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1761 14.389315    192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1762 14.389402    192.168.0.4    192.168.0.3    SMB       Trans2 Request,
 1763 14.390295    192.168.0.3    192.168.0.4    SMB       Trans2 Response
 1764 14.406902    223.27.17.30   192.168.0.4    IMAP      Response: ga99
 1765 14.407153    192.168.0.4    223.27.17.30   IMAP      Request: 0bak I
 1766 14.421420    192.168.0.3    192.168.0.4    NBSS      NBSS Continuati
 1767 14.421436    192.168.0.4    192.168.0.3    TCP       aas > microsoft
```

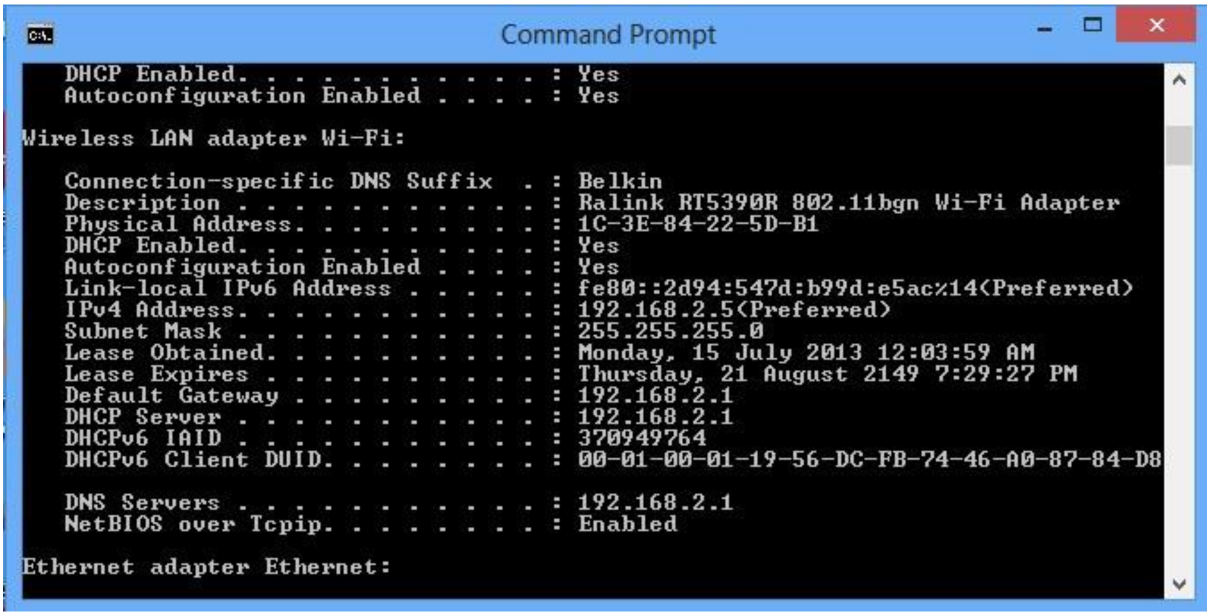
```
⊞ Frame 1760 (174 bytes on wire, 174 bytes captured)
⊟ Ethernet II, Src: Vmware_eb:f7:35 (00:0c:29:eb:f7:35), Dst: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
   ⊞ Destination: Vmware_62:1b:ce (00:0c:29:62:1b:ce)
   ⊞ Source: Vmware_eb:f7:35 (00:0c:29:eb:f7:35)
     Type: IP (0x0800)
⊞ Internet Protocol, Src: 192.168.0.4 (192.168.0.4), Dst: 192.168.0.3 (192.168.0.3)
⊞ Transmission Control Protocol, Src Port: cyaserv (2584), Dst Port: microsoft-ds (445), Seq: 1201, A
⊞ NetBIOS Session Service
⊞ SMB (Server Message Block Protocol)
```

```
0000   00 0c 29 62 1b ce 00 0c  29 eb f7 35 08 00 45 00   ..)b.... )..5..E.
0010   00 a0 4a 71 40 00 80 06  2e 8f c0 a8 00 04 c0 a8   ..Jq@... ........
0020   00 03 0a 18 01 bd 47 3b  a4 83 69 b5 c4 82 50 18   ......G; ..i...P.
0030   f6 78 81 ea 00 00 00 00  00 74 ff 53 4d 42 32 00   .x...... .t.SMB2.
0040   00 00 00 18 07 c8 00 00  0b e0 d9 1a 76 04 55 2e   ........ ....v.U.
0050   00 00 04 30 e0 8a 00 78  00 a0 0f 30 00 00 00 02   ...0...x ...0....
0060   00 28 00 00 00 00 00 00  00 00 00 00 00 30 00 44   .(...... .....0.D
0070   00 00 00 00 00 01 00 05  00 33 00 00 00 00 ec 03   ........ .3......
0080   00 00 00 00 5c 00 41 00  72 00 6e 00 61 00 2e 00   ....\.A. r.n.a...
0090   48 00 6f 00 6c 00 6d 00  65 00 73 00 5c 00 57 00   H.o.l.m. e.s.\.W.
00a0   49 00 4e 00 44 00 4f 00  57 00 53 00 00 00         I.N.D.O. W.S...
```

Type (eth.type), 2 bytes | Packets: 1770 Displayed: 1770 Marked: 0 Dropped: 0 | Profile: Default

- Check the type number (0x0800 meaning 0800 Hex) here to confirm that the payload (that follows) is IP (http://en.wikipedia.org/wiki/EtherType). Snag the expanded Ethernet header (3 lines) so that you include the two MAC addresses as well as the Type field.

- Go to the DOS(Command) prompt and type ipconfig /all. You will get something like this:



```
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Belkin
   Description . . . . . . . . . . . : Ralink RT5390R 802.11bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 1C-3E-84-22-5D-B1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2d94:547d:b99d:e5ac%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, 15 July 2013 12:03:59 AM
   Lease Expires . . . . . . . . . . : Thursday, 21 August 2149 7:29:27 PM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 370949764
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-19-56-DC-FB-74-46-A0-87-84-D8

   DNS Servers . . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:
```

Note your MAC address (a.k.a. Physical Address) for the connection you are currently using (Ethernet or Wi-Fi). In the example above it is 1C-3E-84-2-5D-B1.

Question 2: Snag the IPCONFIG display

Question 3: What is the MAC address on your own computer?

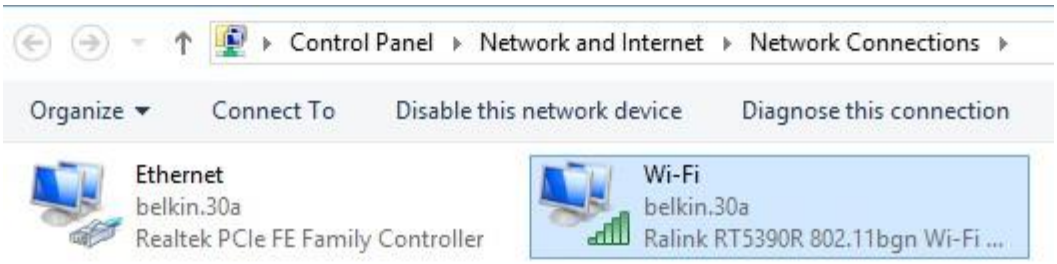
Question 4: Is the Ethernet packet you snagged earlier being sent to or from your machine? Justify your answer

4.2 Speed and duplex settings

The initial steps may vary slightly between operating systems.

- Go to your Control Panel. For Windows 7 and 8 you would select ‘Control Panel’ from the Start menu, in XP you would go Start->Settings->Control Panel.

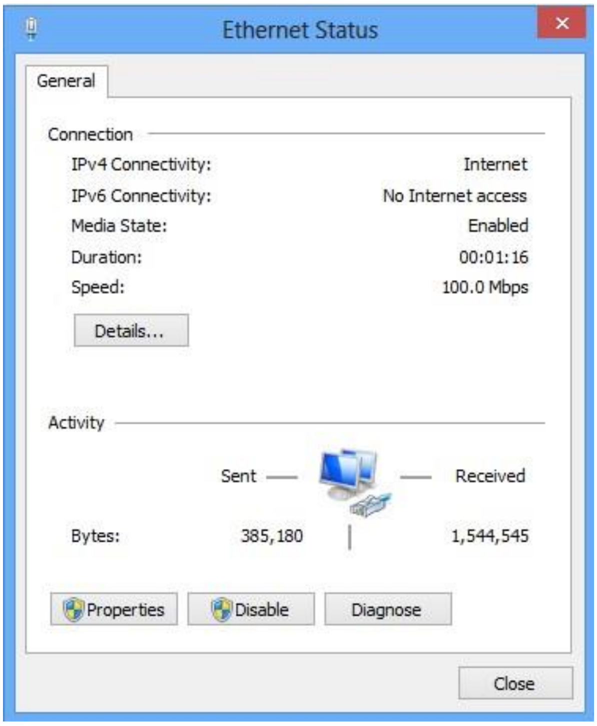
- From here you can select View Network Status and tasks->Change Adapter Settings, or in XP you could select Networks directly from the Control Panel display


Control Panel ▸ Network and Internet ▸ Network Connections ▸
Organize ▾
Connect To
Disable this network device
Diagnose this connection

Ethernet
belkin.30a
Realtek PCIe FE Family Controller

Wi-Fi
belkin.30a
Ralink RT5390R 802.11bgn Wi-Fi ...

- Click on the Ethernet connection to open up the Ethernet Status dialog box



Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:01:16

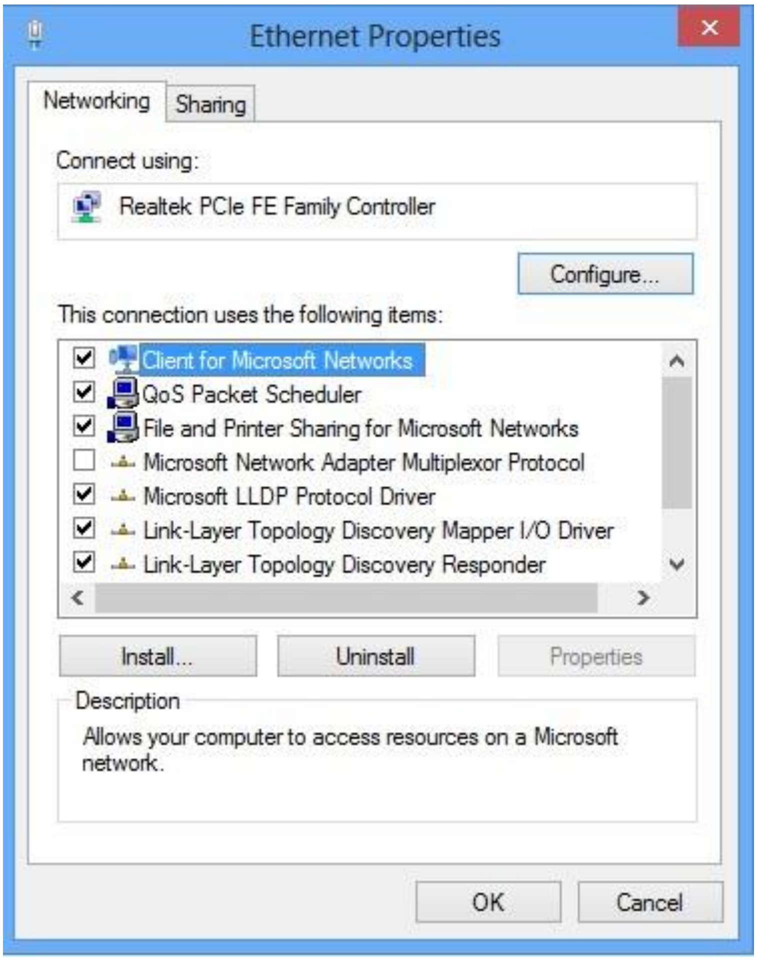
Speed: 100.0 Mbps

Activity

Sent — — Received

Bytes: 385,180 | 1,544,545

- Click on Properties to open up the Ethernet Properties dialog box



Connect using:

Realtek PCIe FE Family Controller

This connection uses the following items:

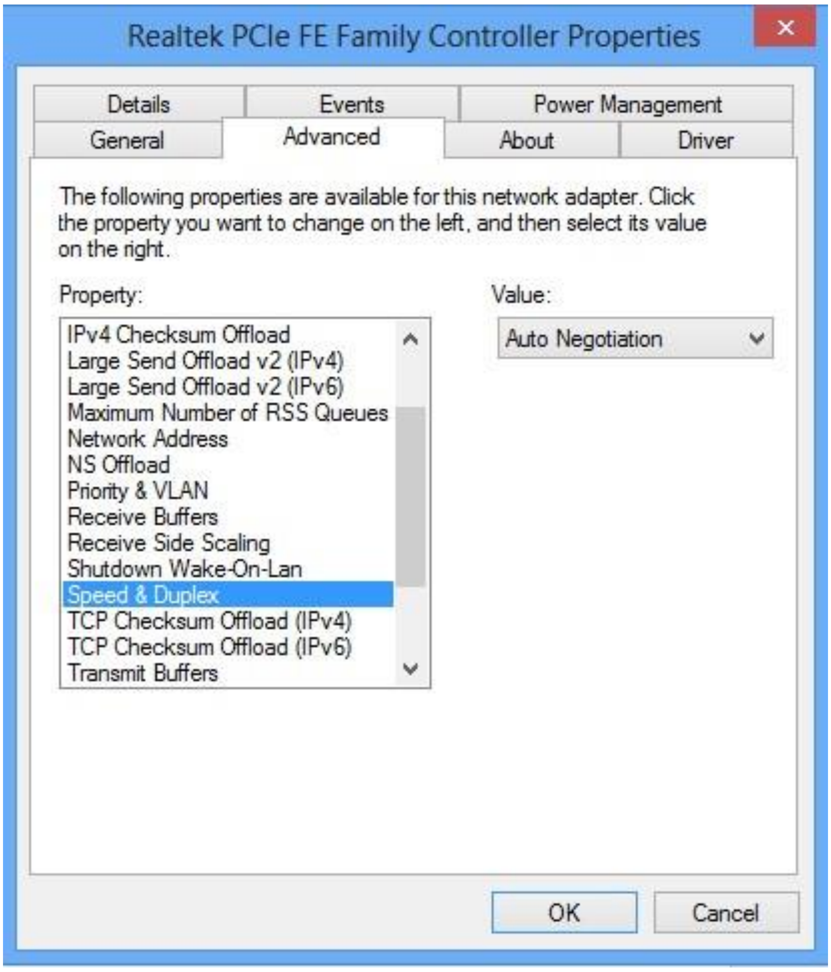
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

- Your Ethernet interface shows up under ‘Connect using:’. Now click on Configure and select the Advanced tab. From the Property box select Speed and Duplex, and then open the drop-down menu under Value.

- The current setting should be Auto-negotiation, but there are several other possibilities. DO NOT CHANGE THE SETTING at the present moment. You may need to do so if, for example, you attach your laptop to switch that fails to auto-negotiate a setting, at which point you might need to alter the setting



Realtek PCIe FE Family Controller Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- IPv4 Checksum Offload
- Large Send Offload v2 (IPv4)
- Large Send Offload v2 (IPv6)
- Maximum Number of RSS Queues
- Network Address
- NS Offload
- Priority & VLAN
- Receive Buffers
- Receive Side Scaling
- Shutdown Wake-On-Lan
- Speed & Duplex
- TCP Checksum Offload (IPv4)
- TCP Checksum Offload (IPv6)
- Transmit Buffers

Value: Auto Negotiation

- Question 5: Take a screenshot of the speed and duplex settings, with the Value dialog box open if possible. However, Screenhunter might insist on closing it, as in the snag above

End of DIT Lab 2.