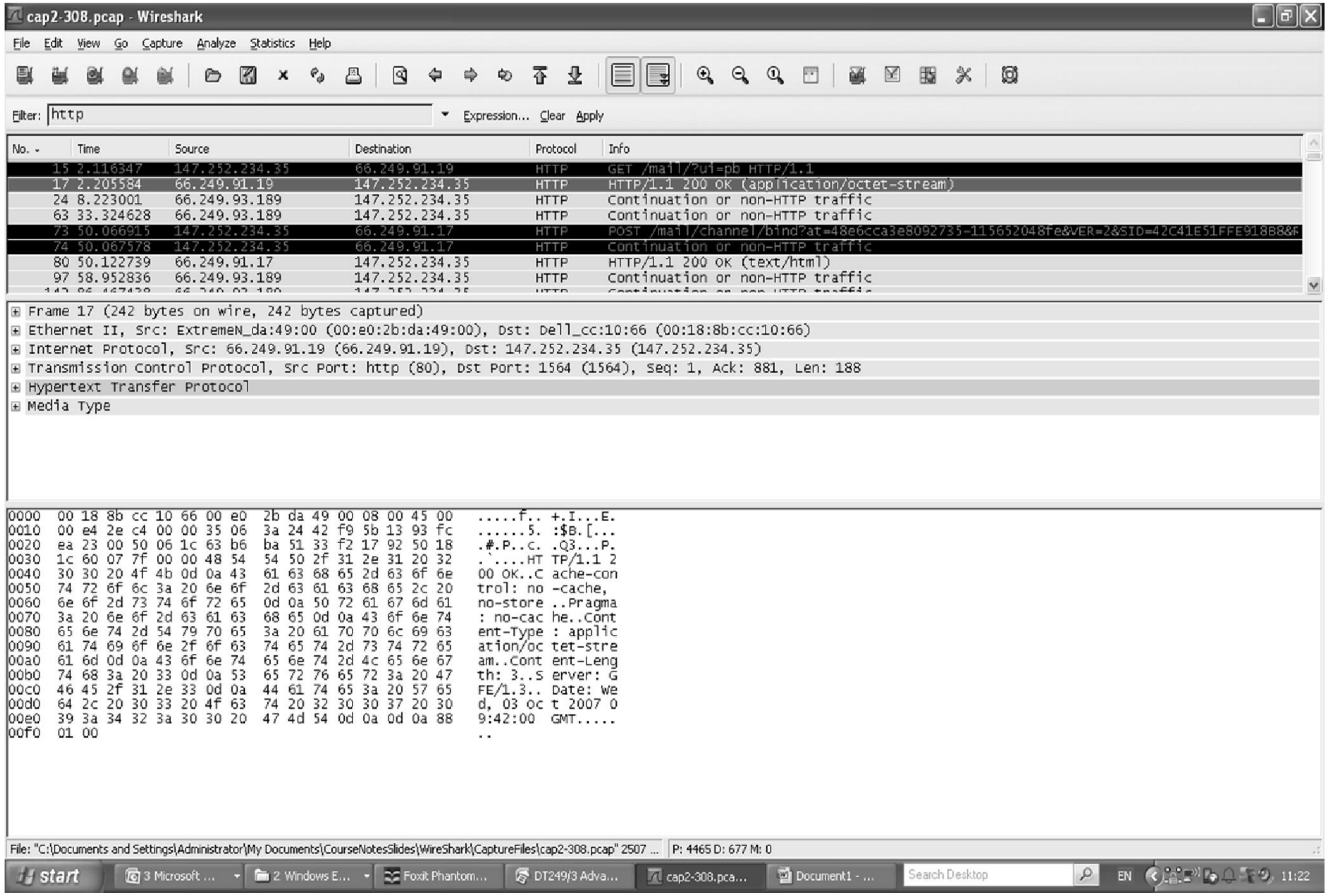
Wireshark - Protocols at Work

- The *Wireshark* Protocol Analyzer is used to capture and analyze *frames* from a Network Interface Card (NIC) d
- The following slide (screenshot 1) shows the opening screen with a captured frame highlighted:
  - Here a filter has been applied so as to only show frames carrying HTTP data
- The screen contains three sub-screens:
  - The top screen provides summary information for each *frame* captured.
  - The middle screen provides a breakdown of the frame showing the component parts (i.e. TCP segment header, IP datagram header, Ethernet frame header etc.).
  - The lower screen shows how the entire frame including its data field appears on the *wire* (transmission medium) i.e. the 1 and 0's (in HEX form).
- Packet 17 from the top screen will be considered in the following slides in order the demonstrate *encapsulation*:
  - This frame contains a HTTP 200 OK Response message.

Wireshark Opening Screen (screenshot 1)



Filter: http

```
No. -   Time        Source            Destination       Protocol  Info
     15 2.116347    147.252.234.35    66.249.91.19      HTTP      GET /mail/?ui=pb HTTP/1.1
     17 2.205584    66.249.91.19      147.252.234.35    HTTP      HTTP/1.1 200 OK (application/octet-stream)
     24 8.223001    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
     63 33.324628   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
     73 50.066915   147.252.234.35    66.249.91.17      HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
     74 50.067578   147.252.234.35    66.249.91.17      HTTP      Continuation or non-HTTP traffic
     80 50.122739   66.249.91.17      147.252.234.35    HTTP      HTTP/1.1 200 OK (text/html)
     97 58.952836   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
```

```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   .`....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

File: "C:\Documents and Settings\Administrator\My Documents\CourseNotesSlides\WireShark\CaptureFiles\cap2-308.pcap" 2507 ... P: 4465 D: 677 M: 0

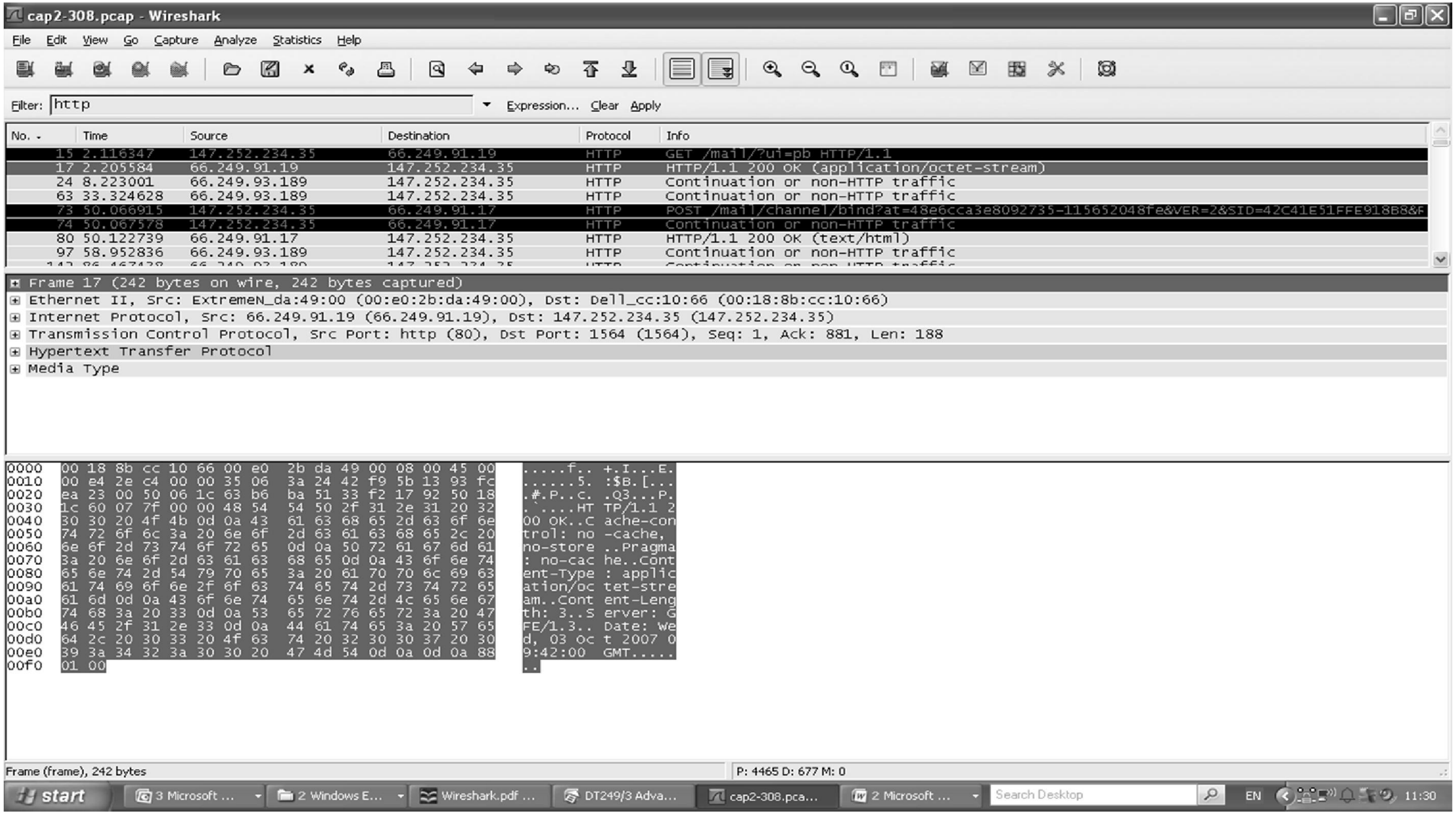
Encapsulation

- *Encapsulation* is a process whereby the PDUs from each protocol layer are carried inside the payload section of the next protocol layer down the protocol stack. For instance:
  - A HTTP request/response is carried inside a TCP *segment*,
  - A TCP segment is carried inside an IP *datagram*,
  - An IP datagram is carried inside an Ethernet *frame*.
- The following screenshots show examples of this process:
  - By clicking on the different component headers in the middle screen the location of the bytes associated with each PDU header type (Frame, IP and TCP) can be seen highlighted on the bottom screen.

Encapsulation

- Notice the order in which the PDU headers appear:
  - The entire frame is highlighted in screenshot 2
    - All bytes associated with the frame are highlighted in the lower screen as one would expect.
  - The HTTP header data is highlighted in screenshot 3
    - The bytes associated with the HTTP 200 response comprise the last part of the frame
  - The TCP header data is highlighted in screenshot 4
    - The bytes associated with the TCP segment header precede the HTTP response data
  - The IP header data is highlighted in screenshot 5
    - The bytes associated with the IP header precede the TCP segment header
  - The Frame header data is highlighted in screenshot 6
    - The bytes associated with the Frame header precede the IP datagram header

Screenshot 2 – The entire *Frame*



cap2-308.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: http

```
No. -  Time       Source           Destination      Protocol  Info
   15  2.116347   147.252.234.35   66.249.91.19     HTTP      GET /mail/?ui=pb HTTP/1.1
   17  2.205584   66.249.91.19     147.252.234.35   HTTP      HTTP/1.1 200 OK (application/octet-stream)
   24  8.223001   66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
   63  33.324628  66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
   73  50.066915  147.252.234.35   66.249.91.17     HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
   74  50.067578  147.252.234.35   66.249.91.17     HTTP      Continuation or non-HTTP traffic
   80  50.122739  66.249.91.17     147.252.234.35   HTTP      HTTP/1.1 200 OK (text/html)
   97  58.952836  66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
```

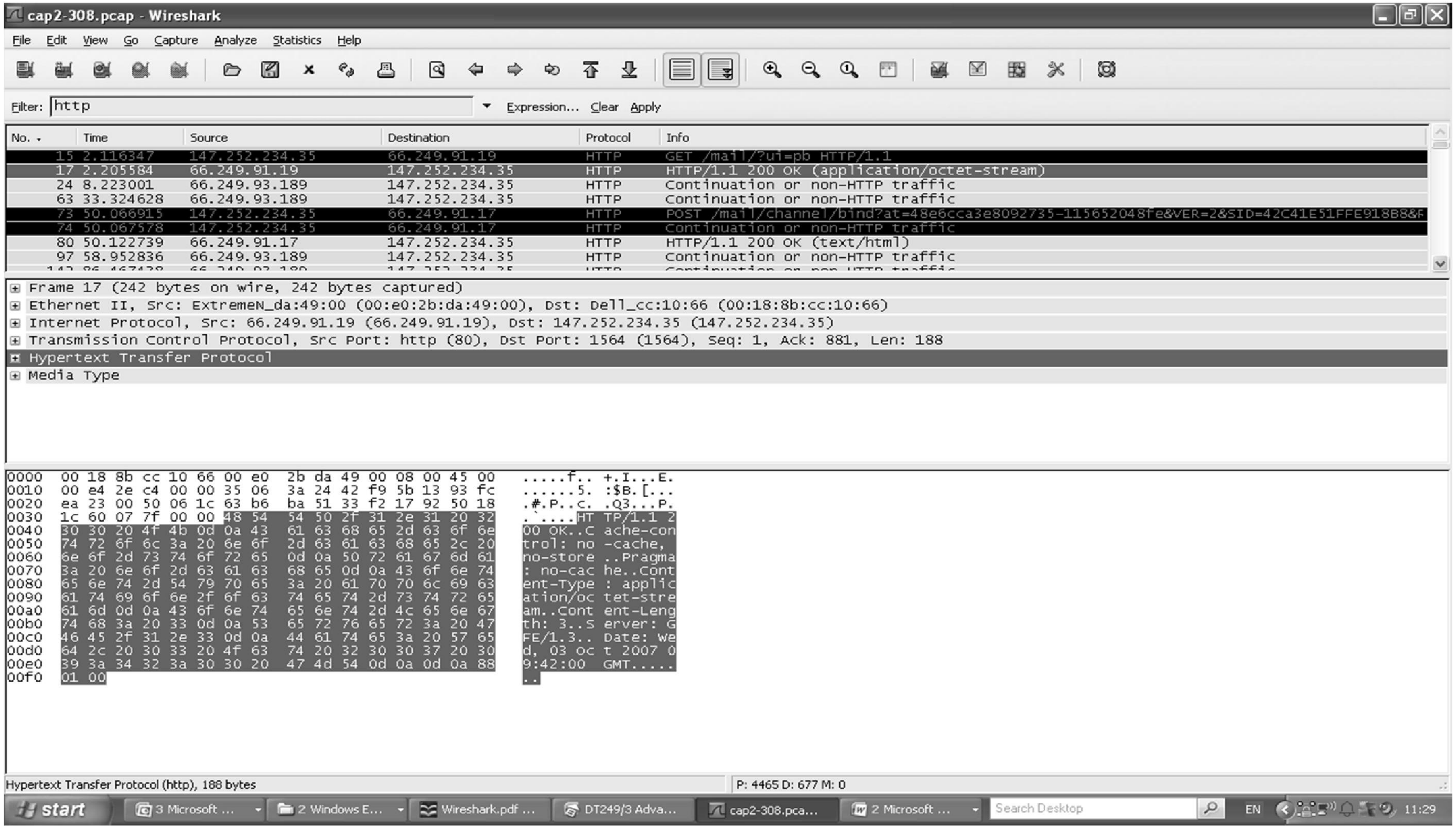
```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   .`....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

Frame (frame), 242 bytes

P: 4465 D: 677 M: 0

Screenshot 3 – The *HTTP* response data



Filter: http

```
No. -   Time        Source            Destination       Protocol  Info
   15 2.116347    147.252.234.35    66.249.91.19      HTTP      GET /mail/?ui=pb HTTP/1.1
   17 2.205584    66.249.91.19      147.252.234.35    HTTP      HTTP/1.1 200 OK (application/octet-stream)
   24 8.223001    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
   63 33.324628   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
   73 50.066915   147.252.234.35    66.249.91.17      HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
   74 50.067578   147.252.234.35    66.249.91.17      HTTP      Continuation or non-HTTP traffic
   80 50.122739   66.249.91.17      147.252.234.35    HTTP      HTTP/1.1 200 OK (text/html)
   97 58.952836   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
  143 86.467438   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
```

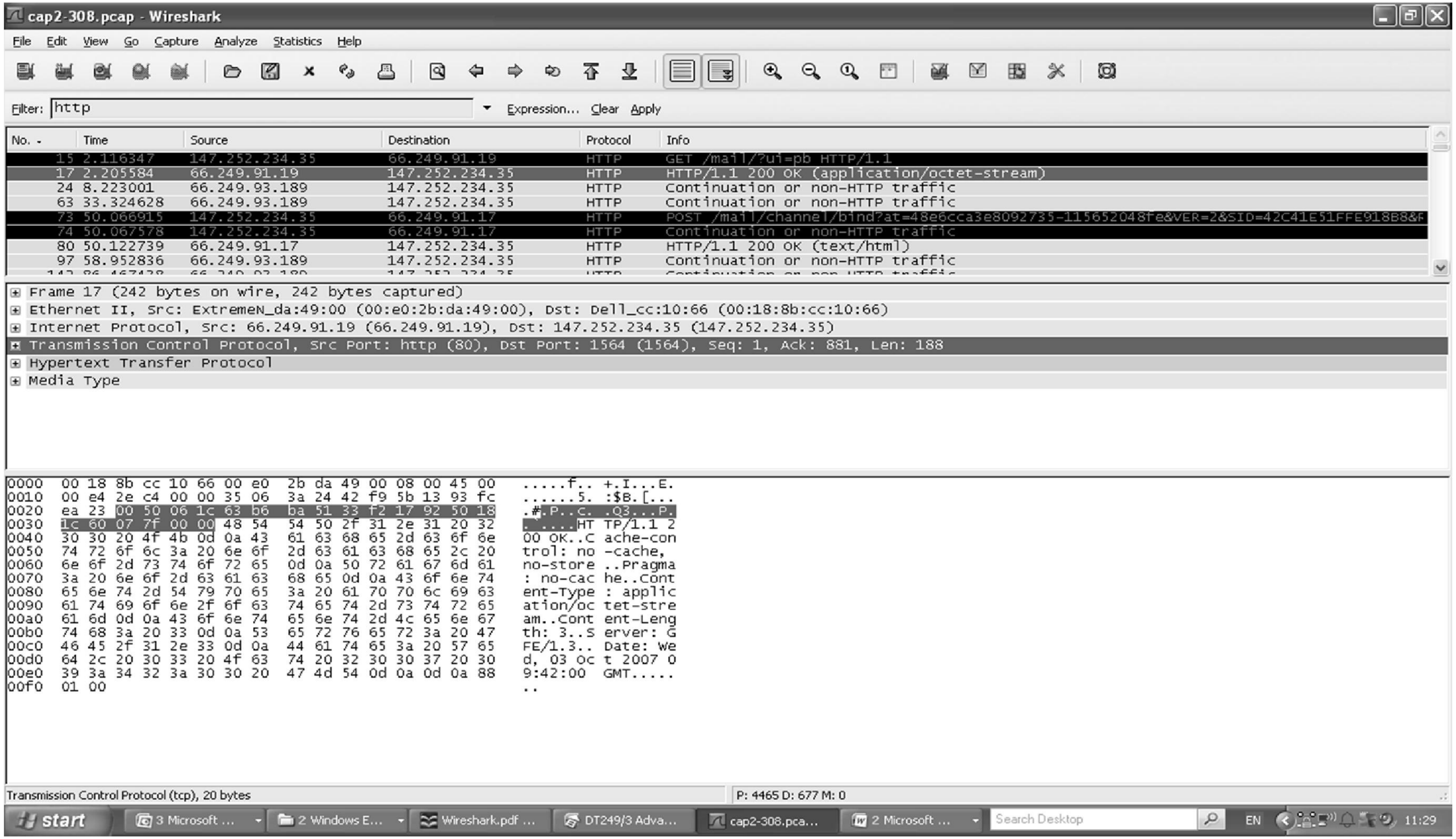
```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   .`....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache, 
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

Hypertext Transfer Protocol (http), 188 bytes

P: 4465 D: 677 M: 0

*S*creenshot 4 – The *TCP* segment header



```
No. -   Time        Source            Destination       Protocol  Info
     15 2.116347    147.252.234.35    66.249.91.19      HTTP      GET /mail/?ui=pb HTTP/1.1
     17 2.205584    66.249.91.19      147.252.234.35    HTTP      HTTP/1.1 200 OK (application/octet-stream)
     24 8.223001    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
     63 33.324628   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
     73 50.066915   147.252.234.35    66.249.91.17      HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
     74 50.067578   147.252.234.35    66.249.91.17      HTTP      Continuation or non-HTTP traffic
     80 50.122739   66.249.91.17      147.252.234.35    HTTP      HTTP/1.1 200 OK (text/html)
     97 58.952836   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
    143 86.467428   66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
```

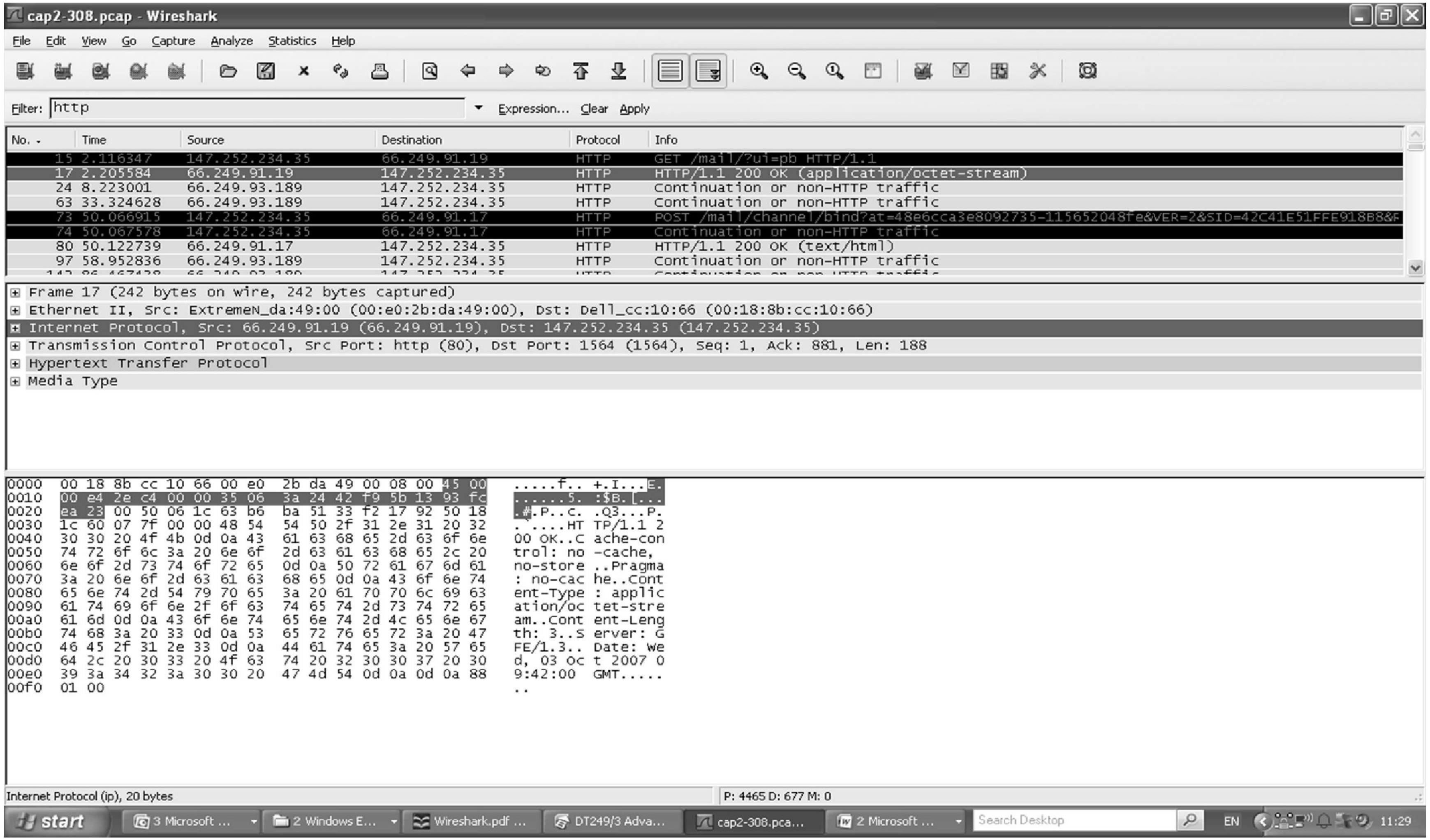
```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   ......HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

Transmission Control Protocol (tcp), 20 bytes

P: 4465 D: 677 M: 0

Screenshot 5 – The *IP* datagram header



Filter: http

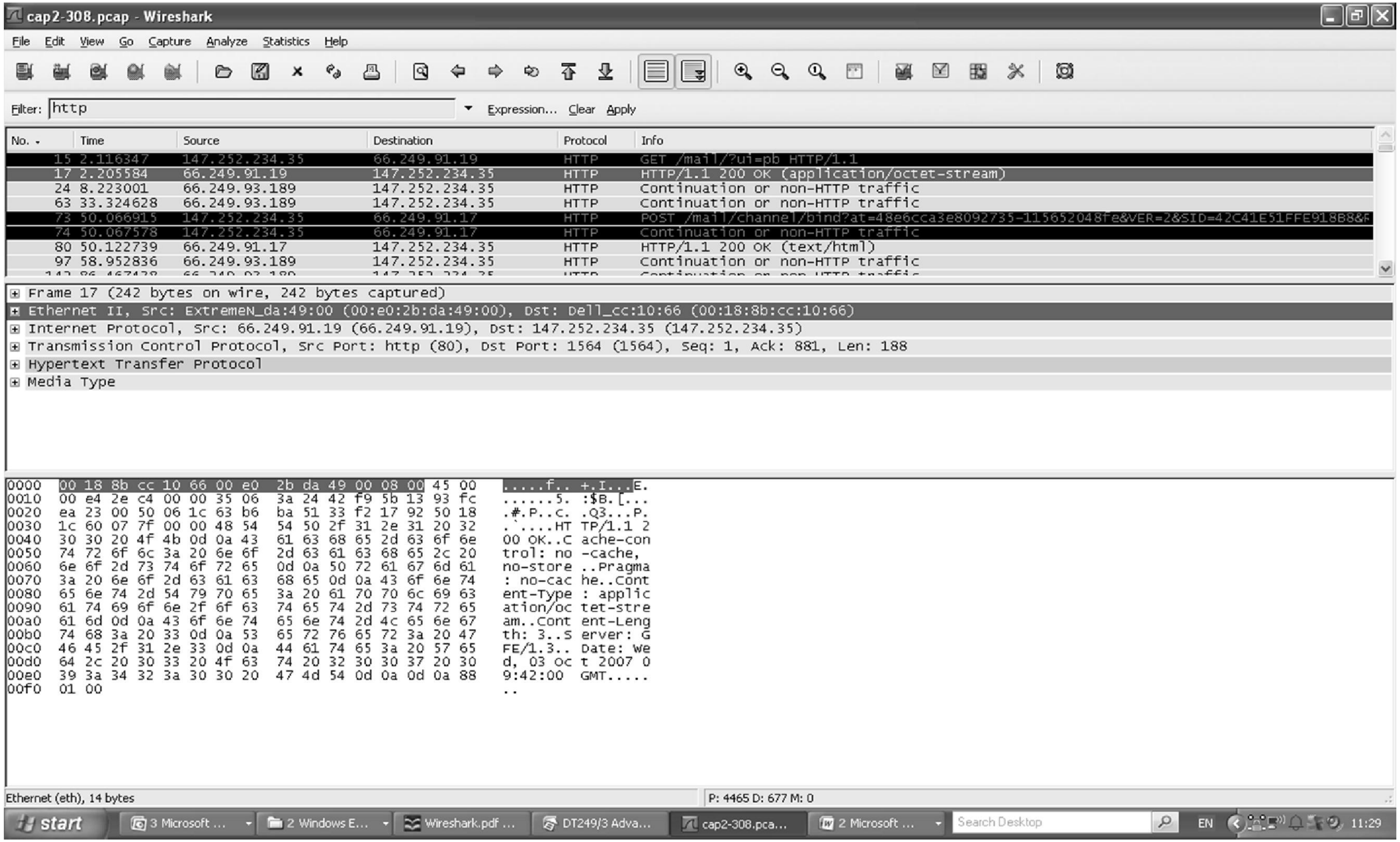
```
No. -  Time         Source            Destination       Protocol  Info
   15  2.116347     147.252.234.35    66.249.91.19      HTTP      GET /mail/?ui=pb HTTP/1.1
   17  2.205584     66.249.91.19      147.252.234.35    HTTP      HTTP/1.1 200 OK (application/octet-stream)
   24  8.223001     66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
   63  33.324628    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
   73  50.066915    147.252.234.35    66.249.91.17      HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
   74  50.067578    147.252.234.35    66.249.91.17      HTTP      Continuation or non-HTTP traffic
   80  50.122739    66.249.91.17      147.252.234.35    HTTP      HTTP/1.1 200 OK (text/html)
   97  58.952836    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
  143  86.467428    66.249.93.189     147.252.234.35    HTTP      Continuation or non-HTTP traffic
```

```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   .`....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

Internet Protocol (ip), 20 bytes | P: 4465 D: 677 M: 0

Screenshot 6 – The *Ethernet* frame header



Filter: http

```
No. -  Time          Source           Destination      Protocol  Info
    15 2.116347      147.252.234.35   66.249.91.19     HTTP      GET /mail/?ui=pb HTTP/1.1
    17 2.205584      66.249.91.19     147.252.234.35   HTTP      HTTP/1.1 200 OK (application/octet-stream)
    24 8.223001      66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
    63 33.324628     66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
    73 50.066915     147.252.234.35   66.249.91.17     HTTP      POST /mail/channel/bind?at=48e6cca3e8092735-115652048fe&VER=2&SID=42C41E51FFE918B8&F
    74 50.067578     147.252.234.35   66.249.91.17     HTTP      Continuation or non-HTTP traffic
    80 50.122739     66.249.91.17     147.252.234.35   HTTP      HTTP/1.1 200 OK (text/html)
    97 58.952836     66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
   143 86.467428     66.249.93.189    147.252.234.35   HTTP      Continuation or non-HTTP traffic
```

```
⊞ Frame 17 (242 bytes on wire, 242 bytes captured)
⊞ Ethernet II, Src: ExtremeN_da:49:00 (00:e0:2b:da:49:00), Dst: Dell_cc:10:66 (00:18:8b:cc:10:66)
⊞ Internet Protocol, Src: 66.249.91.19 (66.249.91.19), Dst: 147.252.234.35 (147.252.234.35)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1564 (1564), Seq: 1, Ack: 881, Len: 188
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0000  00 18 8b cc 10 66 00 e0  2b da 49 00 08 00 45 00   .....f.. +.I...E.
0010  00 e4 2e c4 00 00 35 06  3a 24 42 f9 5b 13 93 fc   ......5. :$B.[...
0020  ea 23 00 50 06 1c 63 b6  ba 51 33 f2 17 92 50 18   .#.P..c. .Q3...P.
0030  1c 60 07 7f 00 00 48 54  54 50 2f 31 2e 31 20 32   .`....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 63 6f 6e   00 OK..C ache-con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 2c 20   trol: no -cache,
0060  6e 6f 2d 73 74 6f 72 65  0d 0a 50 72 61 67 6d 61   no-store ..Pragma
0070  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 43 6f 6e 74   : no-cac he..Cont
0080  65 6e 74 2d 54 79 70 65  3a 20 61 70 70 6c 69 63   ent-Type : applic
0090  61 74 69 6f 6e 2f 6f 63  74 65 74 2d 73 74 72 65   ation/oc tet-stre
00a0  61 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   am..Cont ent-Leng
00b0  74 68 3a 20 33 0d 0a 53  65 72 76 65 72 3a 20 47   th: 3..S erver: G
00c0  46 45 2f 31 2e 33 0d 0a  44 61 74 65 3a 20 57 65   FE/1.3.. Date: We
00d0  64 2c 20 30 33 20 4f 63  74 20 32 30 30 37 20 30   d, 03 Oc t 2007 0
00e0  39 3a 34 32 3a 30 30 20  47 4d 54 0d 0a 0d 0a 88   9:42:00  GMT.....
00f0  01 00                                              ..
```

Ethernet (eth), 14 bytes

P: 4465 D: 677 M: 0