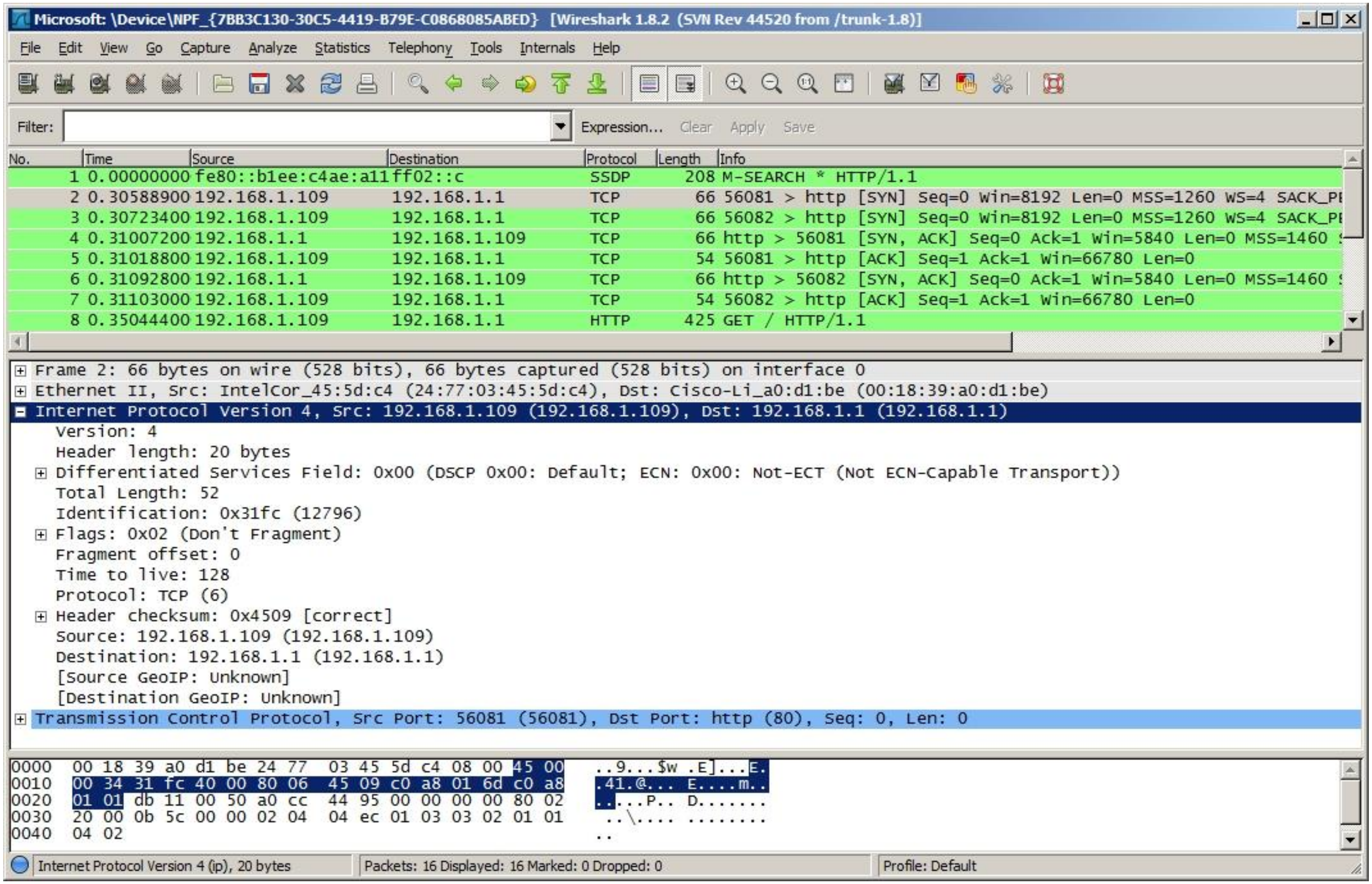

Microsoft: \Device\NPF_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Filter:
Expression...
Clear
Apply
Save

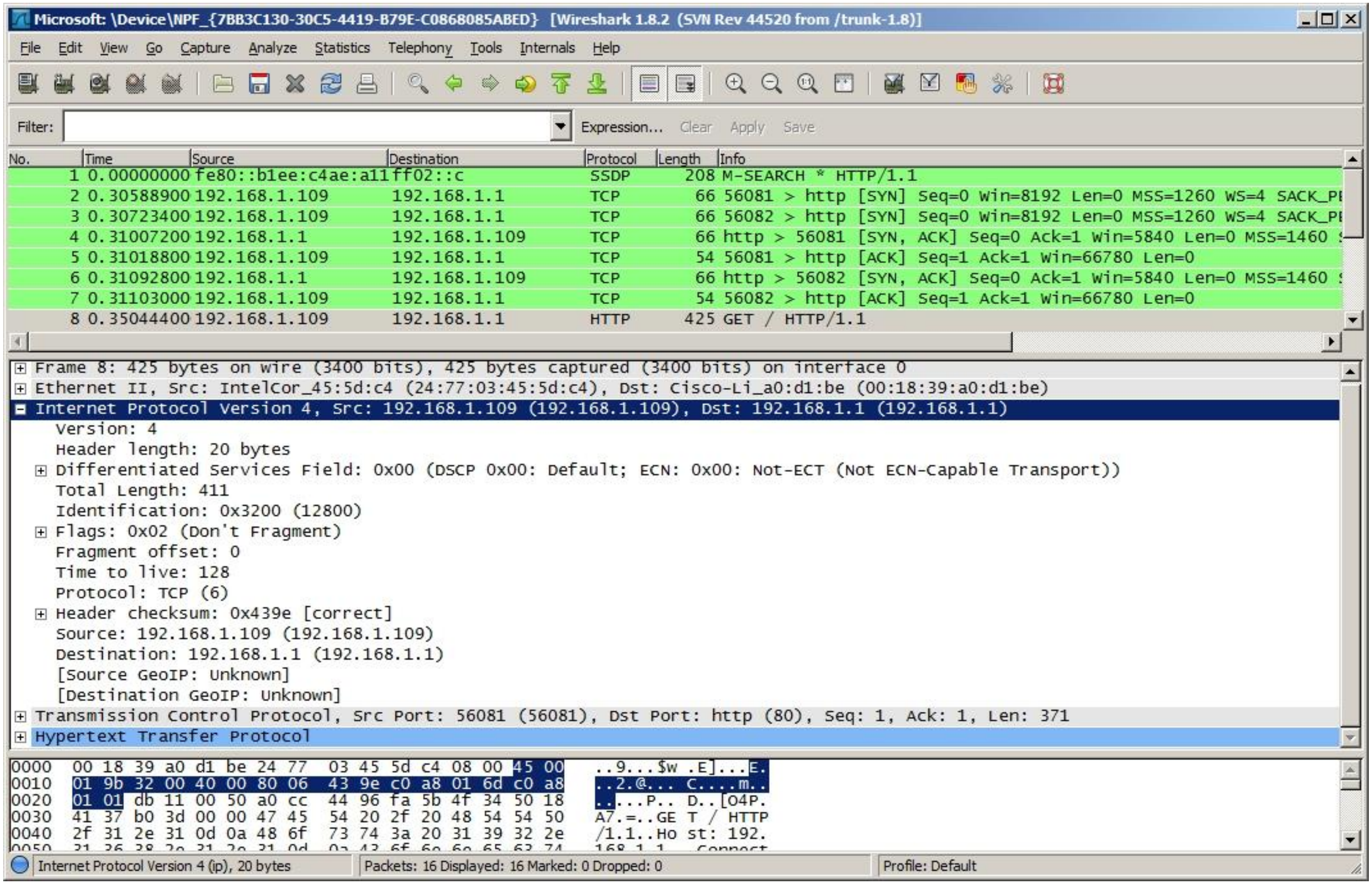
```
No.     Time       Source                 Destination    Protocol Length Info
      1 0.00000000 fe80::b1ee:c4ae:a11 ff02::c        SSDP        208 M-SEARCH * HTTP/1.1
      2 0.30588900 192.168.1.109          192.168.1.1    TCP          66 56081 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PI
      3 0.30723400 192.168.1.109          192.168.1.1    TCP          66 56082 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PI
      4 0.31007200 192.168.1.1            192.168.1.109  TCP          66 http > 56081 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
      5 0.31018800 192.168.1.109          192.168.1.1    TCP          54 56081 > http [ACK] Seq=1 Ack=1 Win=66780 Len=0
      6 0.31092800 192.168.1.1            192.168.1.109  TCP          66 http > 56082 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
      7 0.31103000 192.168.1.109          192.168.1.1    TCP          54 56082 > http [ACK] Seq=1 Ack=1 Win=66780 Len=0
      8 0.35044400 192.168.1.109          192.168.1.1    HTTP        425 GET / HTTP/1.1
```

```
⊞ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)
⊟ Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 52
    Identification: 0x31fc (12796)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x4509 [correct]
    Source: 192.168.1.109 (192.168.1.109)
    Destination: 192.168.1.1 (192.168.1.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Transmission Control Protocol, Src Port: 56081 (56081), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 18 39 a0 d1 be 24 77  03 45 5d c4 08 00 45 00   ..9...$w .E]...E.
0010  00 34 31 fc 40 00 80 06  45 09 c0 a8 01 6d c0 a8   .41.@... E....m..
0020  01 01 db 11 00 50 a0 cc  44 95 00 00 00 00 80 02   .....P.. D.......
0030  20 00 0b 5c 00 00 02 04  04 ec 01 03 03 02 01 01    ..\.... ........
0040  04 02                                              ..
```

```
Internet Protocol Version 4 (ip), 20 bytes | Packets: 16 Displayed: 16 Marked: 0 Dropped: 0 | Profile: Default
```

Capture 1 displays the contents of packet number 2 in this sample capture. Note that the Source is listed as 192.168.1.109 and the Destination is listed as 192.168.1.1. The middle window contains information about the IPv4 header, such as the header length, total length, and any flags that are set.



Microsoft: \Device\NPF_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

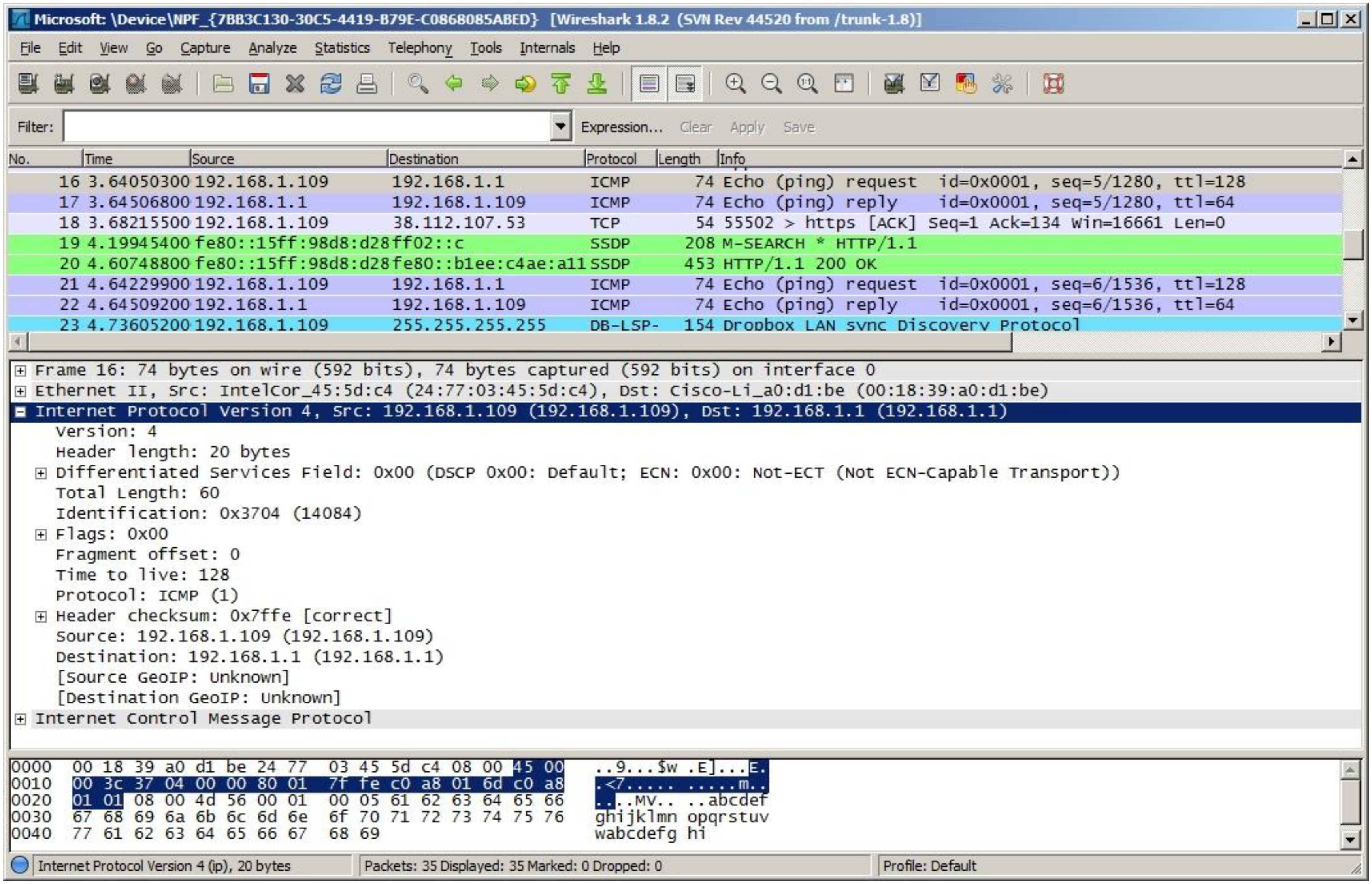
```
No.  Time        Source                Destination      Protocol Length Info
  1 0.00000000 fe80::b1ee:c4ae:a11 ff02::c          SSDP     208 M-SEARCH * HTTP/1.1
  2 0.30588900 192.168.1.109       192.168.1.1      TCP       66 56081 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_P
  3 0.30723400 192.168.1.109       192.168.1.1      TCP       66 56082 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_P
  4 0.31007200 192.168.1.1         192.168.1.109    TCP       66 http > 56081 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  5 0.31018800 192.168.1.109       192.168.1.1      TCP       54 56081 > http [ACK] Seq=1 Ack=1 Win=66780 Len=0
  6 0.31092800 192.168.1.1         192.168.1.109    TCP       66 http > 56082 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
  7 0.31103000 192.168.1.109       192.168.1.1      TCP       54 56082 > http [ACK] Seq=1 Ack=1 Win=66780 Len=0
  8 0.35044400 192.168.1.109       192.168.1.1      HTTP     425 GET / HTTP/1.1
```

```
⊞ Frame 8: 425 bytes on wire (3400 bits), 425 bytes captured (3400 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)
⊟ Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 411
    Identification: 0x3200 (12800)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x439e [correct]
    Source: 192.168.1.109 (192.168.1.109)
    Destination: 192.168.1.1 (192.168.1.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Transmission Control Protocol, Src Port: 56081 (56081), Dst Port: http (80), Seq: 1, Ack: 1, Len: 371
⊞ Hypertext Transfer Protocol
```

```
0000   00 18 39 a0 d1 be 24 77  03 45 5d c4 08 00 45 00    ..9...$w .E]...E.
0010   01 9b 32 00 40 00 80 06  43 9e c0 a8 01 6d c0 a8    ..2.@... C....m..
0020   01 01 db 11 00 50 a0 cc  44 96 fa 5b 4f 34 50 18    .....P.. D..[O4P.
0030   41 37 b0 3d 00 00 47 45  54 20 2f 20 48 54 54 50    A7.=..GE T / HTTP
0040   2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e    /1.1..Ho st: 192.
0050   31 36 38 2e 31 2e 31 0d  0a 43 6f 6e 6e 65 63 74    168.1.1. .Connect
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 16 Displayed: 16 Marked: 0 Dropped: 0
Profile: Default

Capture 2 displays the contents of packet number 8 in this sample capture. This is an HTTP packet. Also notice the presence of information beyond the TCP section.


Microsoft: \Device\NPF_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.    Time        Source                Destination         Protocol  Length Info
    16 3.64050300 192.168.1.109         192.168.1.1          ICMP        74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128
    17 3.64506800 192.168.1.1           192.168.1.109        ICMP        74 Echo (ping) reply    id=0x0001, seq=5/1280, ttl=64
    18 3.68215500 192.168.1.109         38.112.107.53        TCP         54 55502 > https [ACK] Seq=1 Ack=134 Win=16661 Len=0
    19 4.19945400 fe80::15ff:98d8:d28ff02::c                 SSDP       208 M-SEARCH * HTTP/1.1
    20 4.60748800 fe80::15ff:98d8:d28fe80::b1ee:c4ae:a11     SSDP       453 HTTP/1.1 200 OK
    21 4.64229900 192.168.1.109         192.168.1.1          ICMP        74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128
    22 4.64509200 192.168.1.1           192.168.1.109        ICMP        74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=64
    23 4.73605200 192.168.1.109         255.255.255.255      DB-LSP-    154 Dropbox LAN sync Discovery Protocol
```

```
⊞ Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)
⊟ Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x3704 (14084)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x7ffe [correct]
    Source: 192.168.1.109 (192.168.1.109)
    Destination: 192.168.1.1 (192.168.1.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊞ Internet Control Message Protocol
```

```
0000  00 18 39 a0 d1 be 24 77  03 45 5d c4 08 00 45 00   ..9...$w .E]...E.
0010  00 3c 37 04 00 00 80 01  7f fe c0 a8 01 6d c0 a8   .<7..... .....m..
0020  01 01 08 00 4d 56 00 01  00 05 61 62 63 64 65 66   ....MV.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 35 Displayed: 35 Marked: 0 Dropped: 0 | Profile: Default

Capture 3 displays the contents of packet number 16 in this sample capture. The sample packet is a ping request from host 192.168.1.109 to host 192.168.1.1. Notice how there is no TCP or UDP information because this is an Internet Control Message Protocol (ICMP) packet.