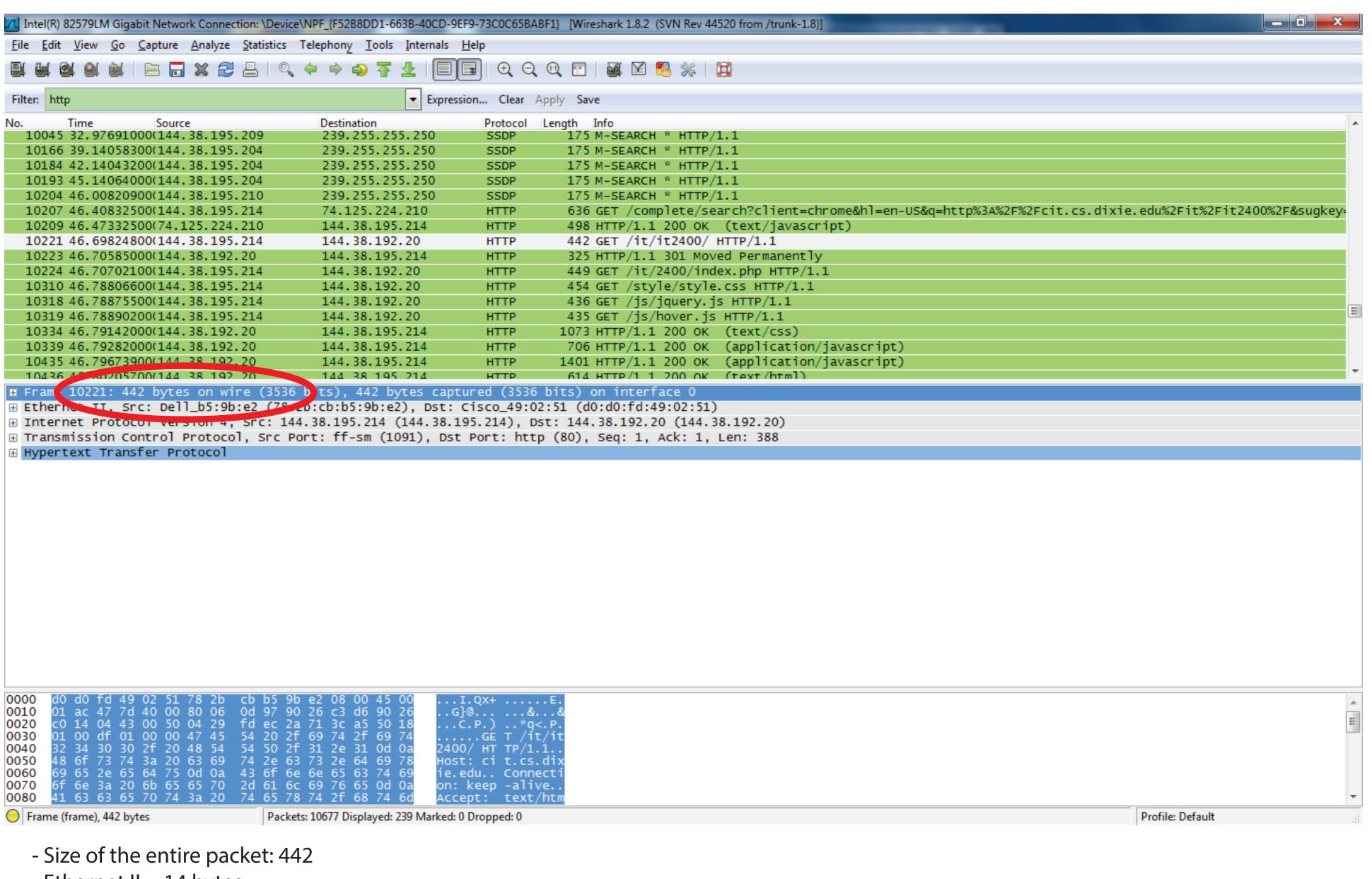
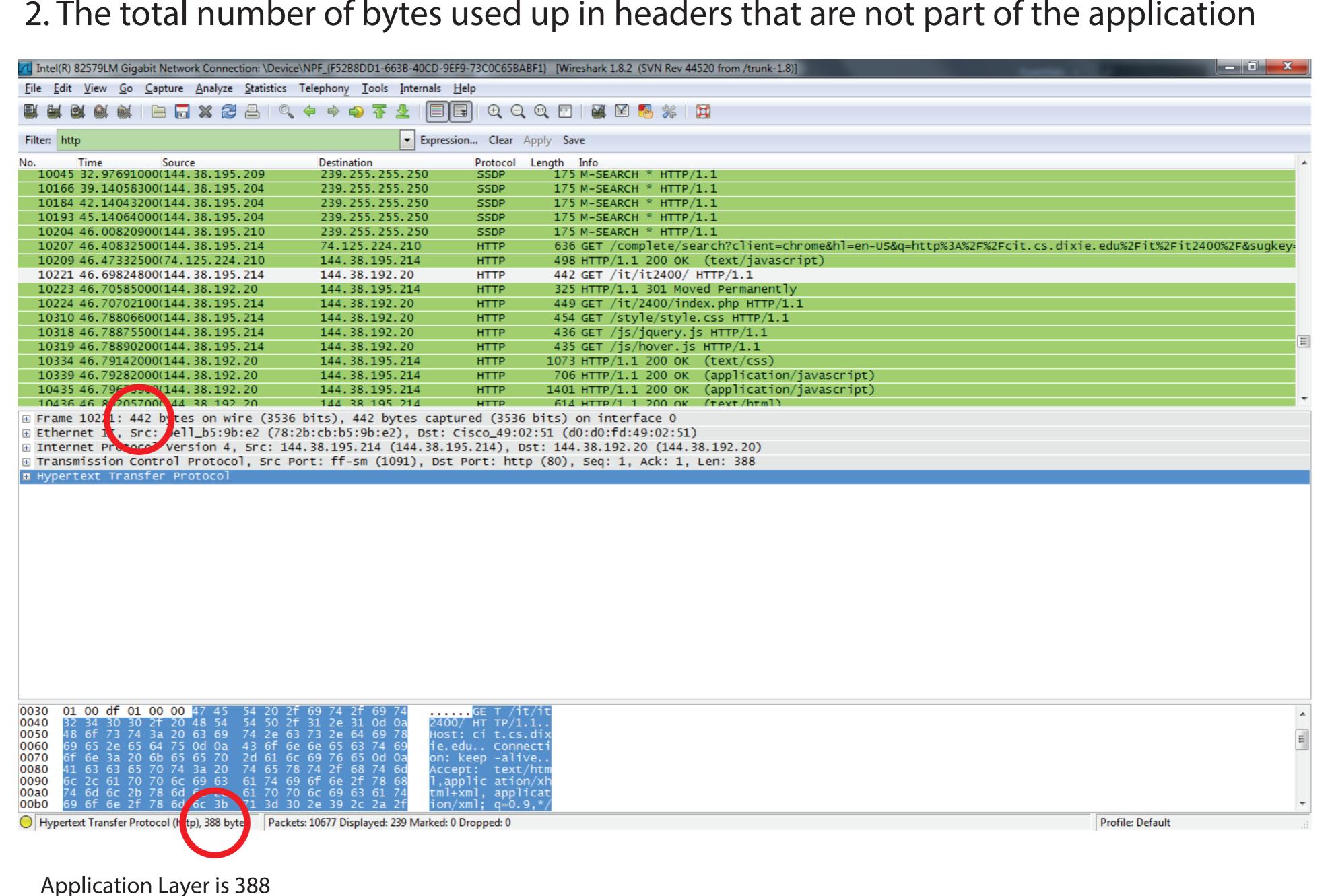
1. The size of the entire packet, and the size of the four layers.



- Ethernet II = 14 bytes
- -IP = 20 bytes
- -TCP = 20 bytes



3. Where "GET /it/it2400/" appears in the raw packet data (the bottom of the three panes).

Frame Layer is 442

442 - 388 = 54

QQQ T

Intel(R) 82579LM Gigabit Network Connection: \Device\NPF_{F52B8DD1-663B-40CD-9EF9-73C0C65BABF1} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

......GE T /it/it

ie.edu.. Connecti

on: keep -alive.

,applic ation/xh

tml+xml, applicat

Expression... Clear Apply Save

SSDP

SSDP

Protocol Length Info

ion/xml; q=0.9,*

<u>View Go Capture Analyze Statistics Telephony Tools Internals Help</u>

01 00 df 01 00 00 47 45 54 20 2f 69 74 2f

0040 0050 0060

0070

0080

Filter: http

Time

Source

10045 32.97691000(144.38.195.209

10166 39.14058300(144.38.195.204

10184 42.14043200(144.38.195.204

10193 45.14064000(144.38.195.204

32 34 30 30 2f 20 48 54 54 50 2f 31 2e 31 0d 48 6f 73 74 3a 20 63 69 74 2e 63 73 2e 64 69

69 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69

6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a

Hypertext Transfer Protocol (http), 388 bytes Packets: 10677 Displayed: 239 Marked: 0 Dropped: 0

Destination

239.255.255.250

239.255.255.250

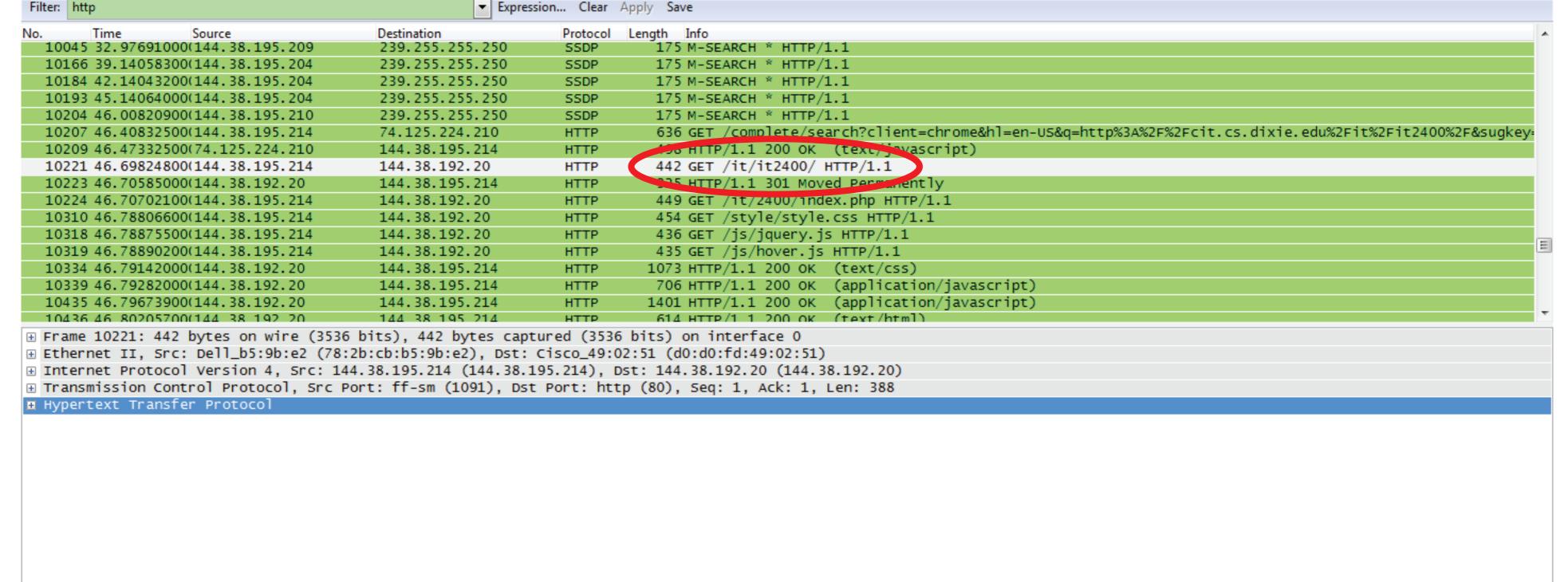
239.255.255.250

239.255.255.250

5c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78

74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61

69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a



4. The "Time to live" field in the IP header, and the amount of space it takes in the header. Intel(R) 82579LM Gigabit Network Connection: \Device\NPF_{F52B8DD1-663B-40CD-9EF9-73C0C65BABF1} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)] <u>File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help</u>

175 M-SEARCH * HTTP/1.1

175 M-SEARCH * HTTP/1.1

175 M-SEARCH * HTTP/1.1

175 M-SEARCH * HTTP/1.1

Profile: Default

Profile: Default

```
239.255.255.250
  10204 46.00820900(144.38.195.210
                                                              SSDP
                                                                        175 M-SEARCH * HTTP/1.1
                                                                        636 GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fcit.cs.dixie.edu%2Fit%2Fit2400%2F&sugkey=
   10207 46.40832500(144.38.195.214
                                         74.125.224.210
  10209 46.47332500(74.125.224.210
                                         144.38.195.214
                                                              HTTP
                                                                        498 HTTP/1.1 200 OK (text/javascript)
  10221 46.69824800(144.38.195.214
                                        144.38.192.20
                                                                        442 GET /it/it2400/ HTTP/1.1
                                                              HTTP
  10223 46.70585000(144.38.192.20
                                         144.38.195.214
                                                                        325 HTTP/1.1 301 Moved Permanently
  10224 46.70702100(144.38.195.214
                                         144.38.192.20
                                                              HTTP
                                                                        449 GET /it/2400/index.php HTTP/1.1
  10310 46.78806600(144.38.195.214
                                        144.38.192.20
                                                              HTTP
                                                                        454 GET /style/style.css HTTP/1.1
  10318 46.78875500(144.38.195.214
                                         144.38.192.20
                                                                        436 GET /js/jquery.js HTTP/1.1
  10319 46.78890200(144.38.195.214
                                         144.38.192.20
                                                              HTTP
                                                                        435 GET /js/hover.js HTTP/1.1
                                                                       1073 HTTP/1.1 200 OK (text/css)
  10334 46.79142000(144.38.192.20
                                        144.38.195.214
                                                              HTTP
  10339 46.79282000(144.38.192.20
                                         144.38.195.214
                                                                        706 HTTP/1.1 200 OK (application/javascript)
                                                              HTTP
   10435 46.79673900(144.38.192.20
                                         144.38.195.214
                                                              HTTP
                                                                       1401 HTTP/1.1 200 OK (application/javascript)
  10436 46 80205700(144 38 192 20
                                        144 38 195 214

    ⊞ Ethernet II, Src: Dell_b5:9b:e2 (78:2b:cb:b5:9b:e2), Dst: Cisco_49:02:51 (d0:d0:fd:49:02:51)

□ Internet Protocol Version 4, Src: 144.38.195.214 (144.38.195.214), Dst: 144.38.192.20 (144.38.192.20)
    Version: 4
    Header length: 20 bytes

→ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

    Total Length: 428
    Identification: 0x477d (18301)
  rragment offset.
    Time to live: 128
    Protocol: TCP (6)
  Source: 144.38.195.214 (144.38.195.214)
    Destination: 144.38.192.20 (144.38.192.20)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

    ⊕ Transmission Control Protocol, Src Port: ff-sm (1091), Dst Port: http (80), Seq: 1, Ack: 1, Len: 388

Hypertext Transfer Protocol
0010 01 ac 47 7d 40 00 🚻 06 0d 97 90 26 c3 d6 90 26
                                                        ..G}@.<mark>.</mark>. ...&...&
0020 c0 14 04 43 00 50 04 29 fd ec 2a 71 3c a5 50 18 0030 01 00 df 01 00 00 47 45 54 20 2f 69 74 2f 69 74
                                                       ...C.P.) ..*q<.P.
                                                       .....GE T /it/it
0040 32 34 30 30 2f 20 48 54 54 50 2f 31 2e 31 0d 0a
                                                       2400/ HT TP/1.1..
0050 48 6f 73 74 3a 20 63 69 74 2e 63 73 2e 64 69 78
                                                       Host: ci t.cs.dix
0060 69 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69
                                                       ie.edu.. Connecti
0070 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a
                                                       on: keep -alive..
0080 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d
                                                       Accept: text/htm
0090 6c 2. or /0 /0 oc 62 63 61 74 69 6f 6e 2f 78 68
                                                       l,applic ation/xh
Time to live (ip.ttl), 1 byte
                                 Packets: 10677 Displayed: 239 Marked: 0 Dropped: 0
                                                                                                                                                  Profile: Default
 Takes up 1 byte of space.
5. Five other protocols that you observed
```

Filter: Time Source 10183 42.03814200(144.38.192.20

144.38.195.214 60 http > startron [ACK] Seq=200466 Ack=2877 Win=12608 Len=0 175 M-SEARCH * HTTP/1.1 10184 42.14043200(144.38.195.204 239.255.255.250 10185 42.21906200(Cisco_54:ae:1e Spanning-tree-(for-br 10186 44.21862700(Cisco_54:ae:1e Spanning-tree-(for-STP

Destination

<u>File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help</u>

0070 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a

0080 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d

File: "C:\Users\NARMST~1\AppData\Local\... | Packets: 10677 Displayed: 10677 Marked: 0 Dropped: 0

Intel(R) 82579LM Gigabit Network Connection: \Device\NPF_{F52B8DD1-663B-40CD-9EF9-73C0C65BABF1} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

| 🗎 🔚 🗶 🥰 🖺 | 🔍 🗢 🕸 💫 7 🛂 | 🗐 📳 | 🗨 🔍 🔍 🖭 | 🖼 🗹 ங % | 💢

▼ Expression... Clear Apply Save

on: keep -alive..

Accept: text/htm

Length Info

```
60 RST. Root = 20480/306/d0:d0:fd:49:02:00 Cost = 3 Port = 0x815f
                                                                     60 RST. Root = 20480/306/d0:d0:fd:49:02:00 Cost = 3 Port = 0x815f
  10187 44.28381100(144.38.195.214
                                      144.38.192.86
                                                          SMB
                                                                     99 Close Request, FID: 0x4c8b
                                                          SMB
  10188 44.28402400(144.38.192.86
                                      144.38.195.214
                                                                     93 Close Response, FID: 0x4c8b
                                      144.38.192.86
                                                                     99 Close Request, FID: 0x4c09
  10189 44.28420900(144.38.195.214
                                                                     93 Close Response
  10190 44.28444500(144.38.192.86
                                      144.38.195.214
                                                          SMB
  10191 44.46749800(fe80::f8fe:b089:704a:!ff02::1:2
                                                          DHCPV6
                                                                    148 Solicit XID: 0xfef192 CID: 0001000118352774782bcbb622ef
                                                          TCP
                                                                     54 nsstp > microsoft-ds [ACK] Seq=162446 Ack=288699 Win=12564 Len=0
  10192 44.48364100(144.38.195.214
                                      144.38.192.86
                                                          SSDP
  10193 45.14064000(144.38.195.204
                                      239.255.255.250
                                                                    175 M-SEARCH * HTTP/1.1
  10194 45.72977400(fe80::48a7:7ec3:8370::ff02::16
                                                          ICMP (
                                                                     90 Multicast Listener Report Message v2
                                                          ARP
                                                                     60 Who has 144.38.195.193? Tell 144.38.195.210
  10195 45.74047300(Dell_ab:b5:0b
                                      Broadcast
                                                                     90 Multicast Listener Report Message v2
  10196 45.74128600(fe80::48a7:7ec3:8370::ff02::16
                                                                     90 Multicast Listener Report Message v2
  10197 45.74192700(fe80::48a7:7ec3:8370::ff02::16
  10198 45.74888900(fe80::48a7:7ec3:8370::ff02::16
                                                          ICMPv6
                                                                     90 Multicast Listener Report Message v2

    ⊞ Ethernet II, Src: Dell_b5:9b:e2 (78:2b:cb:b5:9b:e2), Dst: Cisco_49:02:51 (d0:d0:fd:49:02:51)

□ Internet Protocol Version 4, Src: 144.38.195.214 (144.38.195.214), Dst: 144.38.192.20 (144.38.192.20)
    Version: 4
    Header length: 20 bytes

■ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

   Total Length: 428
   Identification: 0x477d (18301)
  Fragment offset: 0
   Time to live: 128
   Protocol: TCP (6)
  Header checksum: 0x0d97 [correct]
    Source: 144.38.195.214 (144.38.195.214)
    Destination: 144.38.192.20 (144.38.192.20)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Hypertext Transfer Protocol
     d0 d0 fd 49 02 51 78 2b cb b5 9b e2 08 00 45 00
                                                    ...I.QX+ ....E.
                                                    ...G}@.... ....&....&
0010 01 ac 47 7d 40 00 80 06
                            0d 97 90 26 c3 d6 90 26
0020 c0 14 04 43 00 50 04 29 fd ec 2a 71 3c a5 50 18
                                                    ...C.P.) ..*q<.P.
0030 01 00 df 01 00 00 47 45 54 20 2f 69 74 2f 69 74
                                                    .....GE T /it/it
0040 32 34 30 30 2f 20 48 54 54 50 2f 31 2e 31 0d 0a
                                                    2400/ HT TP/1.1..
0050 48 6f 73 74 3a 20 63 69 74 2e 63 73 2e 64 69 78
                                                    Host: ci t.cs.dix
0060 69 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69
                                                    ie.edu.. Connecti
```