

```
154 6.669397      71.192.34.104      64.233.169.104      HTTP      670      GET /favicon.ico HTTP/1.1
Frame 154: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 20, 2009 16:43:08.400461000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1253479388.400461000 seconds
  [Time delta from previous captured frame: 0.000342000 seconds]
  [Time delta from previous displayed frame: 0.024788000 seconds]
  [Time since reference or first frame: 6.669397000 seconds]
  Frame Number: 154
  Frame Length: 670 bytes (5360 bits)
  Capture Length: 670 bytes (5360 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
  Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
    Destination: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
      Address: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
        .... 0. .... = LG bit: Globally unique address (factory default)
        .... 0 .... = IG bit: Individual address (unicast)
    Source: Dell_4f:36:23 (00:08:74:4f:36:23)
      Address: Dell_4f:36:23 (00:08:74:4f:36:23)
        .... 0. .... = LG bit: Globally unique address (factory default)
        .... 0 .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 656
    Identification: 0xa2f4 (41716)
    Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x01fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 71.192.34.104
    Destination: 64.233.169.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Transmission Control Protocol, Src Port: 4338, Dst Port: 80, Seq: 1, Ack: 1, Len: 616
    Source Port: 4338
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 616]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 617 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
      000. .... = Reserved: Not set
      ...0 .... = Nonce: Not set
      .... 0... = Congestion Window Reduced (CWR): Not set
      .... 0... = ECN-Echo: Not set
      .... ..0. = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP...]
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0x2eff [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
      [iRTT: 0.054263000 seconds]
      [Bytes in flight: 616]
      [Bytes sent since last PSH flag: 616]
    TCP payload (616 bytes)
```

Hypertext Transfer Protocol  
GET /favicon.ico HTTP/1.1\r\n  
[Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1\r\n]  
[GET /favicon.ico HTTP/1.1\r\n]  
[Severity level: Chat]  
[Group: Sequence]  
Request Method: GET  
Request URI: /favicon.ico  
Request Version: HTTP/1.1  
Host: www.google.com\r\n  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.14) Gecko/2009082707 Firefox/3.0.14 (.NET CLR 3.5.30729)\r\n  
Accept: image/png,image/\*;q=0.8,\*/\*;q=0.5\r\n  
Accept-Language: en-us,en;q=0.5\r\n  
Accept-Encoding: gzip,deflate\r\n  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n  
Keep-Alive: 300\r\n  
Connection: keep-alive\r\n  
[truncated]Cookie: PREF=ID=bf5d0bb622fc0544:U=f3b005fc50a5d6e7:TM=1248148747:LM=1250937140:GM=1:S=JrvbEJK\_1TdhMdJS;  
NID=27=nBKmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVAdIo4X26oEbAcAqAyesnEZccqTF0l3F7q549rdZPw588xqiEGBAwz\_7kPPbeoN5XQohmdQvgLcPFX  
Cookie pair: PREF=ID=bf5d0bb622fc0544:U=f3b005fc50a5d6e7:TM=1248148747:LM=1250937140:GM=1:S=JrvbEJK\_1TdhMdJS  
Cookie pair:  
NID=27=nBKmwWULTZsu7LjKEy9DazS3cvQEGC3qQJWZLVAdIo4X26oEbAcAqAyesnEZccqTF0l3F7q549rdZPw588xqiEGBAwz\_7kPPbeoN5XQohmdQvgLcPFXJ-3kk5h9JX2gD  
\r\n  
[Full request URI: http://www.google.com/favicon.ico]  
[HTTP request 1/1]  
[Response in frame: 160]