Franklin Nuth
Professor Ronny Bull
CSC323-A
9 October 2017

IP

1) The IP address of my computer is 192.168.1.102.
2) The value in the upper layer protocol field is 1.
3) There are 20 bytes in the IP header. There are 64 bytes in the payload of the IP datagram. I determined this by subtracting the total length and the header length.
4) The IP datagram has not been fragmented, because the More fragments bit = 0.
5) From one datagram to the next in the series of ICMP messages, the field in the IP datagram that always changes is Source IP.
6) The fields that stay constant are Version and Header length because it keeps the data whole. The fields that must change are Time to live and Checksums because it keeps the data moving between the messages.
7) The pattern I observed in the identification field is that it decreases to 0x0000.
8) The value in the identification field is 42029, and the TTL field is 224.
9) Identification changes because two or more packets with same ID indicates presence of a larger piece of data. TTL does not change because the TTL for the first hop router is always the same.
10) Yes, the message has been fragmented.
11) The information that indicates the packet has been fragmented is the offset of 0. We can indicate this is the first or last fragment is by checking the More Fragments flag. This IP datagram is 1500.
12) We know this is not the first datagram fragment because the offset is 0, and there are more fragments because the More Fragments number is higher than 0.
13) The fields that change between the first and second fragment is total length, flags, and segment offset.
14) Only one fragment was created from the original datagram.
15) The fields that change from are fragment offset and checksum.

```
      8 6.163045       192.168.1.102         128.59.23.100         ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1
(no response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 21:48:02.821397000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093139282.821397000 seconds
    [Time delta from previous captured frame: 0.297584000 seconds]
    [Time delta from previous displayed frame: 0.297584000 seconds]
    [Time since reference or first frame: 6.163045000 seconds]
    Frame Number: 8
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
    Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        Address: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ca [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence number (BE): 20483 (0x5003)
    Sequence number (LE): 848 (0x0350)
    [No response seen]
        [Expert Info (Warning/Sequence): No response seen to ICMP request]
            [No response seen to ICMP request]
            [Severity level: Warning]
            [Group: Sequence]
    Data (56 bytes)
0000  37 32 20 aa aa aa aa aa aa aa aa aa aa aa aa aa   72 ..............
0010  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0020  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0030  aa aa aa aa aa aa aa aa                          ........
        Data: 373220aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
        [Length: 56]
```

```
    347 53.626815      192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=0, ID=3344)
[Reassembled in #349]
Frame 347: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 18:48:50.285167000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093139330.285167000 seconds
    [Time delta from previous captured frame: 0.011736000 seconds]
    [Time delta from previous displayed frame: 0.011736000 seconds]
    [Time since reference or first frame: 53.626815000 seconds]
    Frame Number: 347
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
    Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        Address: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x3344 (13124)
    Flags: 0x01 (More Fragments)
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 7
    Protocol: ICMP (1)
    Header checksum: 0x0130 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 349
Data (1480 bytes)
0000  08 00 88 cb 03 00 be 03 38 31 20 aa aa aa aa aa   ........81 .....
0010  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0020  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0030  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0040  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0050  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0060  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0070  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0080  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0090  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0100  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0110  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0120  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0130  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0140  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0150  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0160  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0170  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0180  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0190  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0200  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
```

```
0210  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0220  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0230  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0240  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0250  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0260  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0270  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0280  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0290  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0300  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0310  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0320  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0330  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0340  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0350  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0360  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0370  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0380  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0390  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0400  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0410  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0420  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0430  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0440  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0450  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0460  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0470  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0480  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0490  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0500  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0510  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0520  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0530  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0540  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0550  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0560  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0570  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0580  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0590  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05c0  aa aa aa aa aa aa aa aa                         ........
    Data: 080088cb0300be03383120aaaaaaaaaaaaaaaaaaaaaaaaa...
    [Length: 1480]
```

```
     92 28.441511      192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)
[Reassembled in #93]
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 21:48:25.099863000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093139305.099863000 seconds
    [Time delta from previous captured frame: 5.488773000 seconds]
    [Time delta from previous displayed frame: 5.488773000 seconds]
    [Time since reference or first frame: 28.441511000 seconds]
    Frame Number: 92
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
    [Coloring Rule Name: TTL low or unexpected]
    [Coloring Rule String: ( ! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251
&& ip.ttl != 1 && !(vrrp || carp))]
Ethernet II, Src: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
    Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        Address: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    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: 1500
    Identification: 0x32f9 (13049)
    Flags: 0x01 (More Fragments)
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 1
        [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
    Protocol: ICMP (1)
    Header checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 93
Data (1480 bytes)
0000  08 00 d0 c6 03 00 77 03 37 36 20 aa aa aa aa aa   ......w.76 .....
0010  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0020  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0030  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0040  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0050  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0060  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0070  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0080  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0090  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0100  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0110  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0120  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0130  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0140  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0150  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0160  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0170  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
```

```
0180  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0190  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0200  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0210  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0220  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0230  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0240  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0250  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0260  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0270  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0280  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0290  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0300  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0310  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0320  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0330  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0340  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0350  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0360  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0370  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0380  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0390  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0400  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0410  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0420  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0430  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0440  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0450  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0460  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0470  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0480  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0490  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0500  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0510  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0520  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0530  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0540  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0550  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0560  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0570  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0580  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0590  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05c0  aa aa aa aa aa aa aa aa                         ........
    Data: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaa...
    [Length: 1480]
```

```
    379 54.967184      128.59.23.100         192.168.1.102         IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=1480,
ID=0959) [Reassembled in #380]
Frame 379: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 21, 2004 21:48:51.625536000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093139331.625536000 seconds
    [Time delta from previous captured frame: 0.008797000 seconds]
    [Time delta from previous displayed frame: 0.008797000 seconds]
    [Time since reference or first frame: 54.967184000 seconds]
    Frame Number: 379
    Frame Length: 1514 bytes (12112 bits)
    Capture Length: 1514 bytes (12112 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:data]
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
    Destination: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        Address: PremaxPe_8a:70:1a (00:20:e0:8a:70:1a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.59.23.100, Dst: 192.168.1.102
    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: 1500
    Identification: 0x0959 (2393)
    Flags: 0x03 (Don't Fragment) (More Fragments)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..1. .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 242
    Protocol: ICMP (1)
    Header checksum: 0xff60 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.59.23.100
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 380
Data (1480 bytes)
0000  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0010  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0020  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0030  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0040  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0050  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0060  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0070  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0080  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0090  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
00f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0100  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0110  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0120  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0130  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0140  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0150  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0160  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0170  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0180  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0190  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
01e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
```

```
01f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0200  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0210  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0220  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0230  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0240  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0250  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0260  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0270  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0280  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0290  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
02f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0300  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0310  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0320  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0330  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0340  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0350  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0360  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0370  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0380  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0390  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
03f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0400  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0410  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0420  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0430  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0440  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0450  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0460  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0470  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0480  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0490  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04c0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04d0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04e0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
04f0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0500  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0510  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0520  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0530  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0540  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0550  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0560  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0570  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0580  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
0590  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05a0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05b0  aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa   ................
05c0  aa aa aa aa aa aa aa aa                         ........
    Data: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
    [Length: 1480]
```

Franklin Nuth
Professor Ronny Bull
CSC323-A
9 September 2017

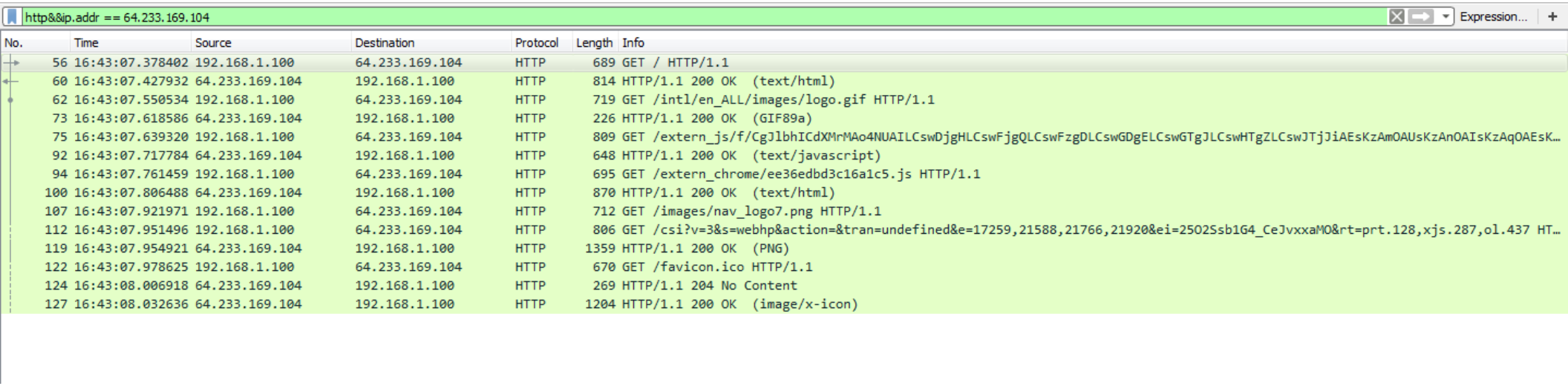
NAT

1) The IP address of the client is 192.168.1.100.
2) See screenshot.
3) On the IP datagram carrying the HTTP GET, the source IP is 192.168.1.100, the destination IP is 64.233.169.04, the TCP source is 4335, and the destination port is 80.
4) The time the 200 OK HTTP message was received was 7.158797. On the IP datagram, the source IP is 64.233.169.104, the destination IP is 192.168.1.100, the destination port is 80, and the TCP source is 4335.
5) The client-to-server TCP SYN segment that sets up the connection is set up at the time is 7.108986. In the TCP SYN the source IP is 64.223.169.104, the destination IP is 192.168.1.100, the source port is 80, and the destination port is 4335. The client received the ACK at 7.108986.
6) The time this message appeared in the trace file is 6.664397.The source IP is 71.192.34.104, the destination IP is 64.233.169.104, the TCP source is 4338, and the destination port is 80. The fields that changed are source IP.
7) The fields that changed in the HTTP GET message are Flags and Checksum. These fields needed to change because of differing packet types.
8) The time the first 200 OK HTTP message was received from the Google server is 0.636388. The source IP is 74.125.106.31, the destination IP was 71.192.34.104, the TCP source is 80, and the destination IP is 4331. The fields that are the same are Version, Header Length, and Flags. The fields that changed is Checksum.
9) The time the TCP SYN segment and the TCP ACK was received was 6.641926. The source and destination IP of both of these segments are 71.192.34.104. Both of their destination ports are 80. The SYN segment has a destination port of 4338, and 4337 for the ACK segment. The fields that are the same are Version, Header Length, and Flags. The one field that changed is Checksum.
10)

WAN		LAN	
IP	Port	IP	Port
71.192.34.104	4331	192.168.1.100	1028

```
    20 16:43:01.841450    192.168.1.100         74.125.106.31         HTTP     767    GET /safebrowsing/rd/goog-malware-
shavar_s_15361-15365.15361-15365.: HTTP/1.1
Frame 20: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:01.841450000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479381.841450000 seconds
    [Time delta from previous captured frame: 0.000087000 seconds]
    [Time delta from previous displayed frame: 0.043667000 seconds]
    [Time since reference or first frame: 1.572315000 seconds]
    Frame Number: 20
    Frame Length: 767 bytes (6136 bits)
    Capture Length: 767 bytes (6136 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: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
    Destination: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        Address: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        Address: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 74.125.106.31
    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: 753
    Identification: 0xa27e (41598)
    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: 128
    Protocol: TCP (6)
    Header checksum: 0xdedf [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 74.125.106.31
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 4331, Dst Port: 80, Seq: 1, Ack: 1, Len: 713
    Source Port: 4331
    Destination Port: 80
    [Stream index: 1]
    [TCP Segment Len: 713]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 714    (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: 0x798c [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.022008000 seconds]
        [Bytes in flight: 713]
        [Bytes sent since last PSH flag: 713]
```

```
    TCP payload (713 bytes)
Hypertext Transfer Protocol
    GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.:
        Request Version: HTTP/1.1
    Host: safebrowsing-cache.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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\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://safebrowsing-cache.google.com/safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.:]
    [HTTP request 1/4]
    [Response in frame: 39]
    [Next request in frame: 41]
```


http&&ip.addr == 64.233.169.104
Expression...
No. Time Source Destination Protocol Length Info
56 16:43:07.378402 192.168.1.100 64.233.169.104 HTTP 689 GET / HTTP/1.1
60 16:43:07.427932 64.233.169.104 192.168.1.100 HTTP 814 HTTP/1.1 200 OK (text/html)
62 16:43:07.550534 192.168.1.100 64.233.169.104 HTTP 719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
73 16:43:07.618586 64.233.169.104 192.168.1.100 HTTP 226 HTTP/1.1 200 OK (GIF89a)
75 16:43:07.639320 192.168.1.100 64.233.169.104 HTTP 809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKzAnOAIsKzAqOAEsK…
92 16:43:07.717784 64.233.169.104 192.168.1.100 HTTP 648 HTTP/1.1 200 OK (text/javascript)
94 16:43:07.761459 192.168.1.100 64.233.169.104 HTTP 695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100 16:43:07.806488 64.233.169.104 192.168.1.100 HTTP 870 HTTP/1.1 200 OK (text/html)
107 16:43:07.921971 192.168.1.100 64.233.169.104 HTTP 712 GET /images/nav_logo7.png HTTP/1.1
112 16:43:07.951496 192.168.1.100 64.233.169.104 HTTP 806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=25O2Ssb1G4_CeJvxxaMO&rt=prt.128,xjs.287,ol.437 HT…
119 16:43:07.954921 64.233.169.104 192.168.1.100 HTTP 1359 HTTP/1.1 200 OK (PNG)
122 16:43:07.978625 192.168.1.100 64.233.169.104 HTTP 670 GET /favicon.ico HTTP/1.1
124 16:43:08.006918 64.233.169.104 192.168.1.100 HTTP 269 HTTP/1.1 204 No Content
127 16:43:08.032636 64.233.169.104 192.168.1.100 HTTP 1204 HTTP/1.1 200 OK (image/x-icon)

```
     56 7.109267       192.168.1.100         64.233.169.104        HTTP     689    GET / HTTP/1.1
Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:07.378402000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.378402000 seconds
    [Time delta from previous captured frame: 0.000214000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 7.109267000 seconds]
    Frame Number: 56
    Frame Length: 689 bytes (5512 bits)
    Capture Length: 689 bytes (5512 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: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
    Destination: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        Address: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        Address: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.100, 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: 675
    Identification: 0xa2ac (41644)
    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: 128
    Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 64.233.169.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 635]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 636    (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: 0xaef3 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.033396000 seconds]
        [Bytes in flight: 635]
        [Bytes sent since last PSH flag: 635]
    TCP payload (635 bytes)
```

```
Hypertext Transfer Protocol
    GET / HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
            [GET / HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /
        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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\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/]
    [HTTP request 1/5]
    [Response in frame: 60]
    [Next request in frame: 62]
```

```
     53 7.075657       192.168.1.100         64.233.169.104        TCP      66     4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
SACK_PERM=1
Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:07.344792000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.344792000 seconds
    [Time delta from previous captured frame: 0.001760000 seconds]
    [Time delta from previous displayed frame: 4.897061000 seconds]
    [Time since reference or first frame: 7.075657000 seconds]
    Frame Number: 53
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
    Destination: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        Address: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        Address: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.100, 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: 52
    Identification: 0xa2aa (41642)
    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: 128
    Protocol: TCP (6)
    Header checksum: 0xabbb [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 64.233.169.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 4335
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
            [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
                [Connection establish request (SYN): server port 80]
                [Severity level: Chat]
                [Group: Sequence]
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x8262 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```

```
     54 7.108986       64.233.169.104        192.168.1.100         TCP      66     80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0
MSS=1430 SACK_PERM=1 WS=64
Frame 54: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:07.378121000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.378121000 seconds
    [Time delta from previous captured frame: 0.033329000 seconds]
    [Time delta from previous displayed frame: 0.033329000 seconds]
    [Time since reference or first frame: 7.108986000 seconds]
    Frame Number: 54
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
    Destination: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        Address: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        Address: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
        0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0xf61a (63002)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 50
    Protocol: TCP (6)
    Header checksum: 0xe62b [validation disabled]
    [Header checksum status: Unverified]
    Source: 64.233.169.104
    Destination: 192.168.1.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 4335
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x012 (SYN, 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
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
            [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
                [Connection establish acknowledge (SYN+ACK): server port 80]
                [Severity level: Chat]
                [Group: Sequence]
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····A··S·]
    Window size value: 5720
    [Calculated window size: 5720]
    Checksum: 0x4a2f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
    [SEQ/ACK analysis]
```

[This is an ACK to the segment in frame: 53]
[The RTT to ACK the segment was: 0.033329000 seconds]
[iRTT: 0.033396000 seconds]

```
    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]
```

```
     38 0.636388       74.125.106.31         71.192.34.104         HTTP     651    HTTP/1.1 200 OK  (application/
vnd.google.safebrowsing-chunk)
Frame 38: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:02.367452000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479382.367452000 seconds
    [Time delta from previous captured frame: 0.000106000 seconds]
    [Time delta from previous displayed frame: 0.104299000 seconds]
    [Time since reference or first frame: 0.636388000 seconds]
    Frame Number: 38
    Frame Length: 651 bytes (5208 bits)
    Capture Length: 651 bytes (5208 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:media]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
    Destination: 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)
    Source: 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)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 74.125.106.31, Dst: 71.192.34.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
        0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 637
    Identification: 0x819a (33178)
    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: 54
    Protocol: TCP (6)
    Header checksum: 0xa1fc [validation disabled]
    [Header checksum status: Unverified]
    Source: 74.125.106.31
    Destination: 71.192.34.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 4331, Seq: 17521, Ack: 714, Len: 597
    Source Port: 80
    Destination Port: 4331
    [Stream index: 1]
    [TCP Segment Len: 597]
    Sequence number: 17521    (relative sequence number)
    [Next sequence number: 18118    (relative sequence number)]
    Acknowledgment number: 714    (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: 114
    [Calculated window size: 7296]
    [Window size scaling factor: 64]
    Checksum: 0xe762 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
        [iRTT: 0.021885000 seconds]
        [Bytes in flight: 3517]
        [Bytes sent since last PSH flag: 6437]
```

```
    TCP payload (597 bytes)
    TCP segment data (597 bytes)
[13 Reassembled TCP Segments (18117 bytes): #21(1460), #22(1460), #23(1460), #25(1460), #26(1460), #27(1460), #30(1460), #31(1460),
#32(1460), #33(1460), #35(1460), #37(1460), #38(597)]
    [Frame: 21, payload: 0-1459 (1460 bytes)]
    [Frame: 22, payload: 1460-2919 (1460 bytes)]
    [Frame: 23, payload: 2920-4379 (1460 bytes)]
    [Frame: 25, payload: 4380-5839 (1460 bytes)]
    [Frame: 26, payload: 5840-7299 (1460 bytes)]
    [Frame: 27, payload: 7300-8759 (1460 bytes)]
    [Frame: 30, payload: 8760-10219 (1460 bytes)]
    [Frame: 31, payload: 10220-11679 (1460 bytes)]
    [Frame: 32, payload: 11680-13139 (1460 bytes)]
    [Frame: 33, payload: 13140-14599 (1460 bytes)]
    [Frame: 35, payload: 14600-16059 (1460 bytes)]
    [Frame: 37, payload: 16060-17519 (1460 bytes)]
    [Frame: 38, payload: 17520-18116 (597 bytes)]
    [Segment count: 13]
    [Reassembled TCP length: 18117]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a43616368652d43...]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Cache-Control: private,max-age=21600\r\n
    Content-Type: application/vnd.google.safebrowsing-chunk\r\n
    Expires: Sun, 20 Sep 2009 20:02:44 GMT\r\n
    Date: Sun, 20 Sep 2009 20:43:01 GMT\r\n
    Server: HTTP server (unknown)\r\n
    Content-Length: 17872\r\n
        [Content length: 17872]
    \r\n
    [HTTP response 1/4]
    [Time since request: 0.104299000 seconds]
    [Request in frame: 19]
    [Next request in frame: 41]
    [Next response in frame: 42]
    File Data: 17872 bytes
Media Type
    Media type: application/vnd.google.safebrowsing-chunk (17872 bytes)
```

```
    141 6.614792       71.192.34.104         64.233.169.104        TCP      66     4338 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4
SACK_PERM=1
Frame 141: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:08.345856000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479388.345856000 seconds
    [Time delta from previous captured frame: 0.001102000 seconds]
    [Time delta from previous displayed frame: 0.001102000 seconds]
    [Time since reference or first frame: 6.614792000 seconds]
    Frame Number: 141
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [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: 52
    Identification: 0xa2eb (41707)
    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: 0x045f [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: 0, Len: 0
    Source Port: 4338
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
            [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
                [Connection establish request (SYN): server port 80]
                [Severity level: Chat]
                [Group: Sequence]
        .... .... ...0 = Fin: Not set
        [TCP Flags: ··········S·]
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0xc034 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
        TCP Option - Maximum segment size: 1460 bytes
```

```
    TCP Option - No-Operation (NOP)
    TCP Option - Window scale: 2 (multiply by 4)
    TCP Option - No-Operation (NOP)
    TCP Option - No-Operation (NOP)
    TCP Option - SACK permitted
```

```
    143 6.641926       71.192.34.104         64.233.169.104        TCP      60     4337 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
Frame 143: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 20, 2009 16:43:08.372990000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479388.372990000 seconds
    [Time delta from previous captured frame: 0.000787000 seconds]
    [Time delta from previous displayed frame: 0.000787000 seconds]
    [Time since reference or first frame: 6.641926000 seconds]
    Frame Number: 143
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [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)
    Padding: 000020202020
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: 40
    Identification: 0xa2ed (41709)
    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: 0x0469 [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: 4337, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 4337
    Destination Port: 80
    [Stream index: 4]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (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
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····A····]
    Window size value: 65044
    [Calculated window size: 260176]
    [Window size scaling factor: 4]
    Checksum: 0x23fd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
```