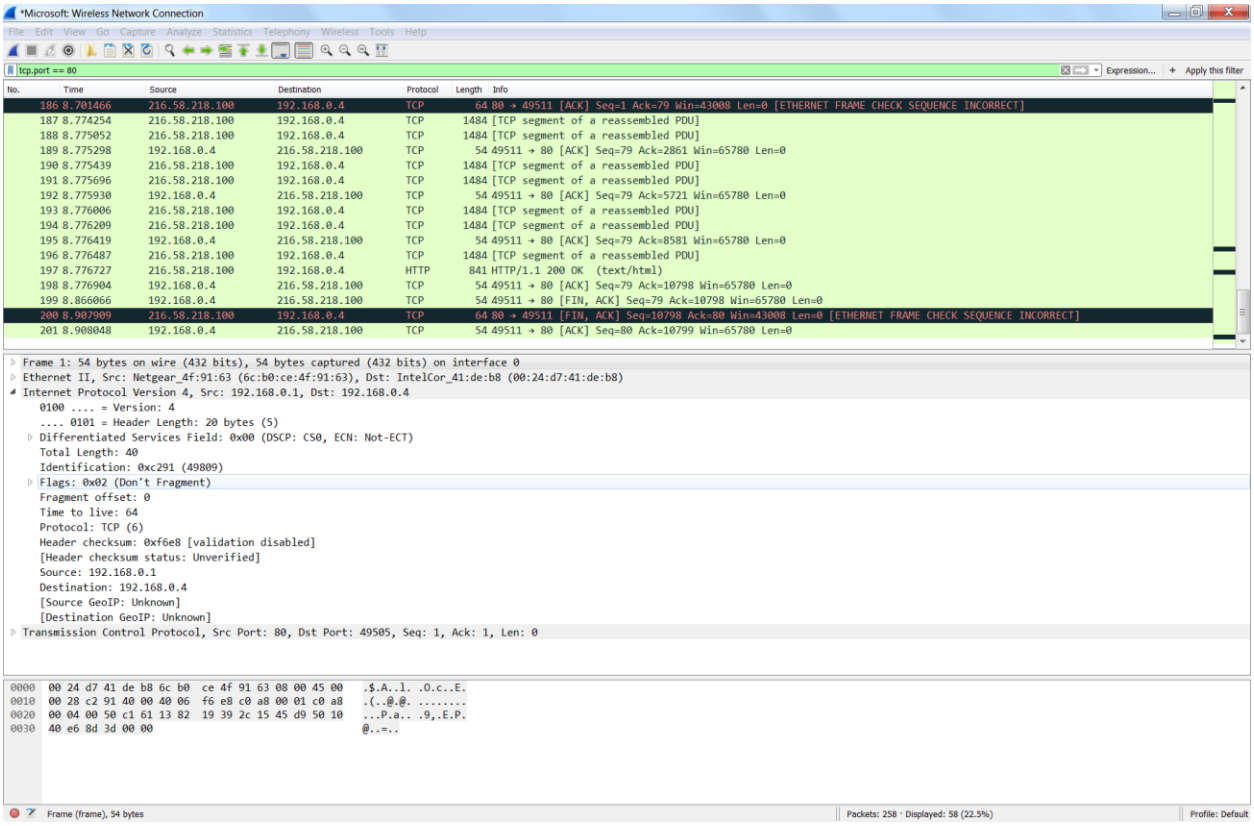
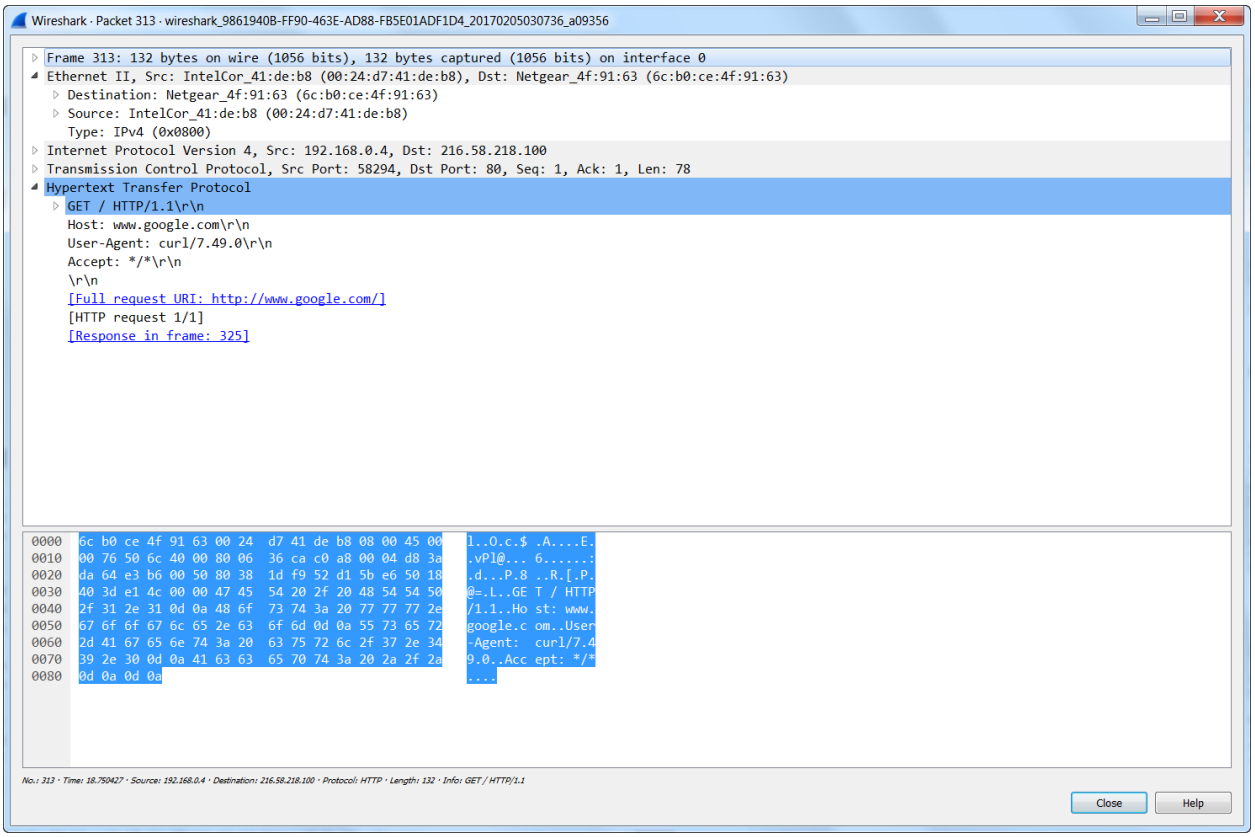
By: Kyle Killion

First Traced Captured – www.google.com 216.58.218.100

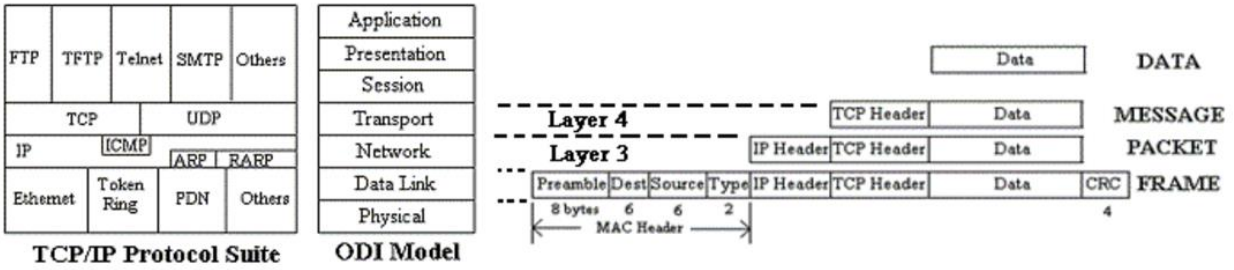


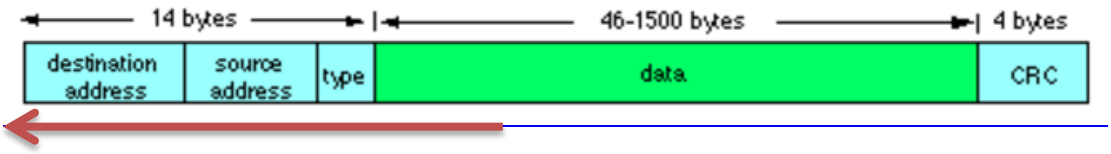
Wireshark packet structure screen:



Ethernet II Diagram

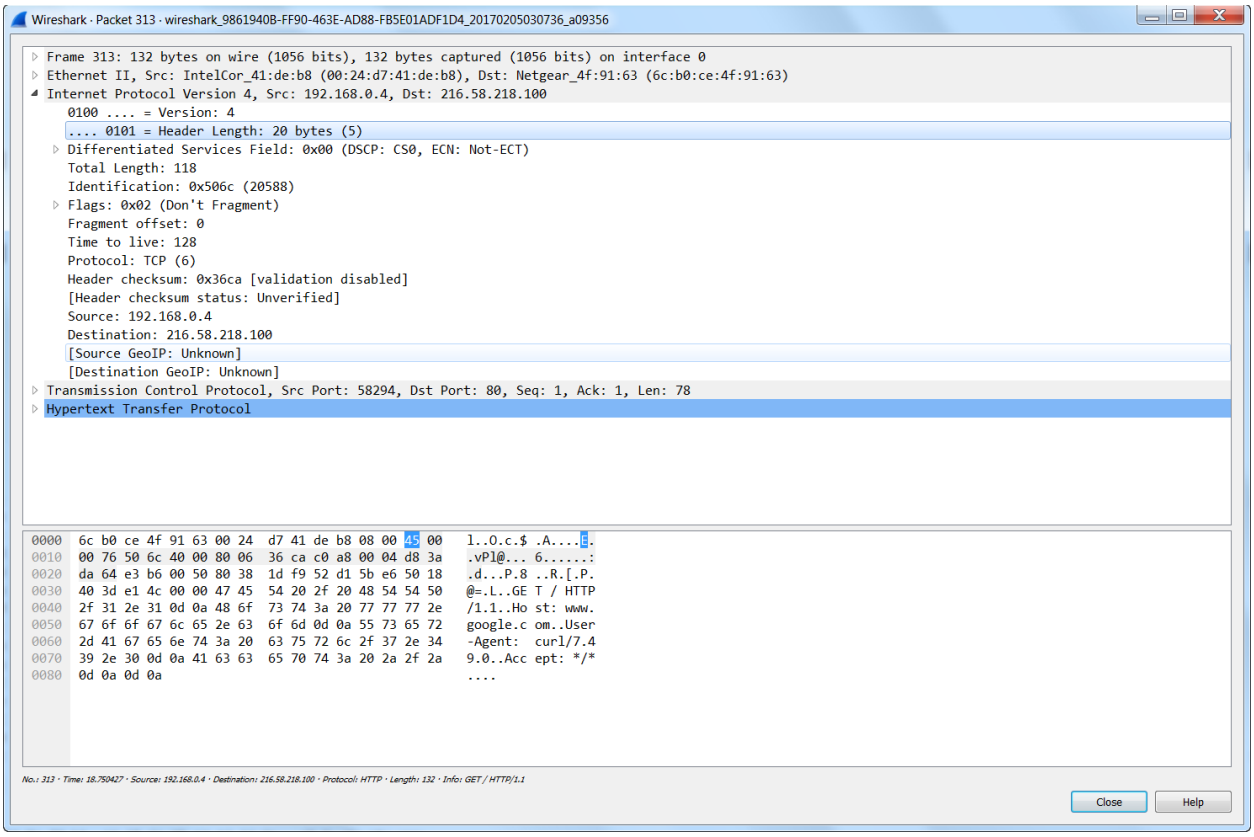
Source: http://www.infocellar.com/networks/ethernet/frame.htm



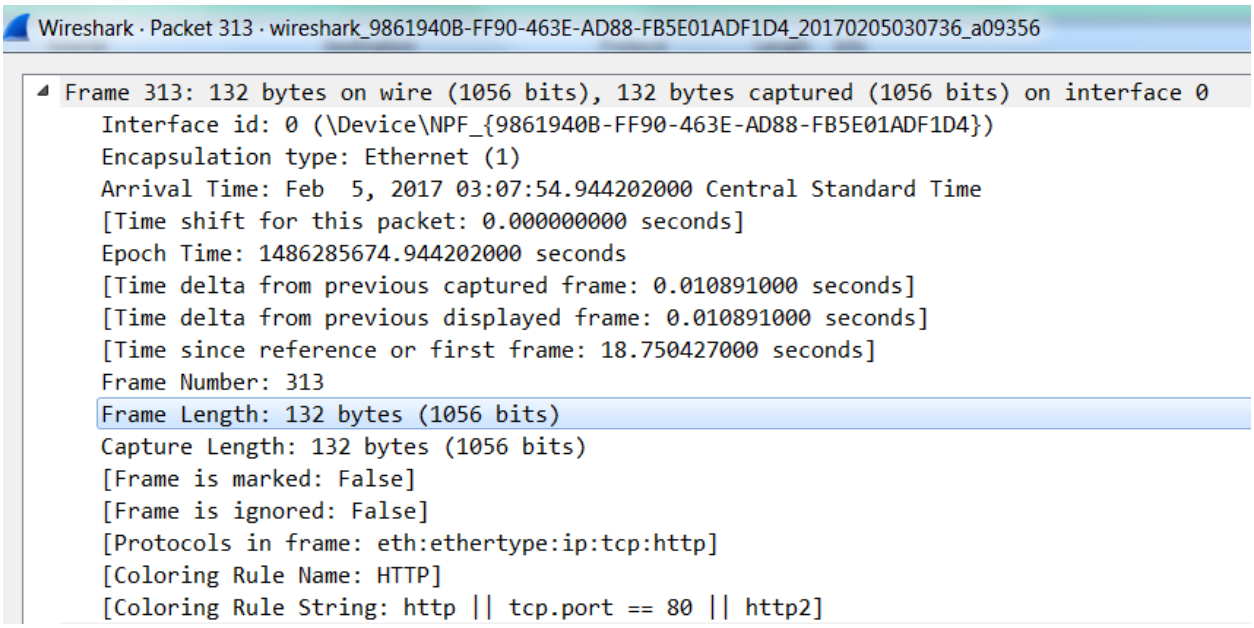


Data Flow

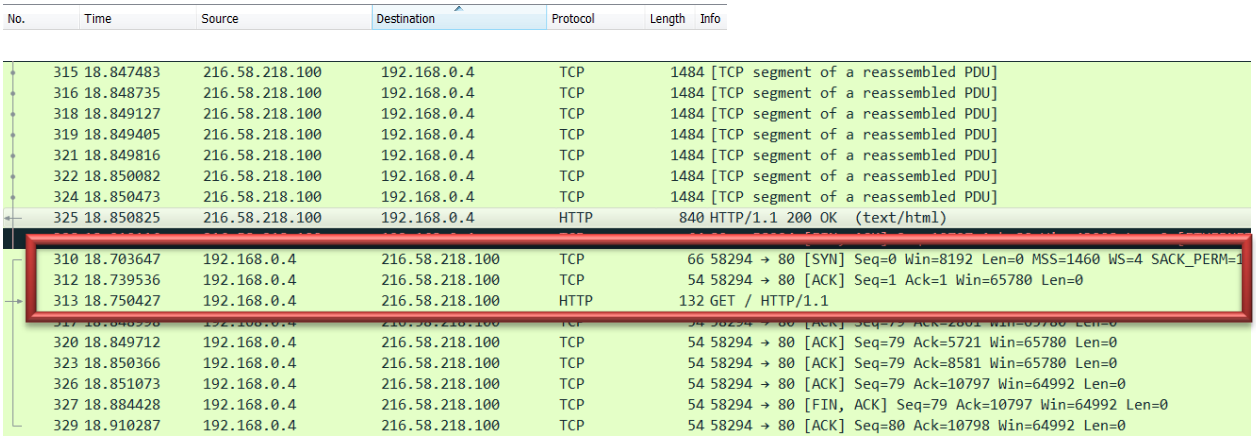
Header Length:



Frame or Packet Length:



Protocol Overhead



HTTP Packet: 132 Bytes

TCP SYN and ACK: Sum of 120 Bytes

Total overhead approximately: 90%

Demultiplexing

1) The “Type” field / (0x0800) used for IP
   a. `Type: IPv4 (0x0800)`
2) `Protocol: TCP (6)` “Protocol” field / “TCP(6)” value is used

Traceroute Exercise

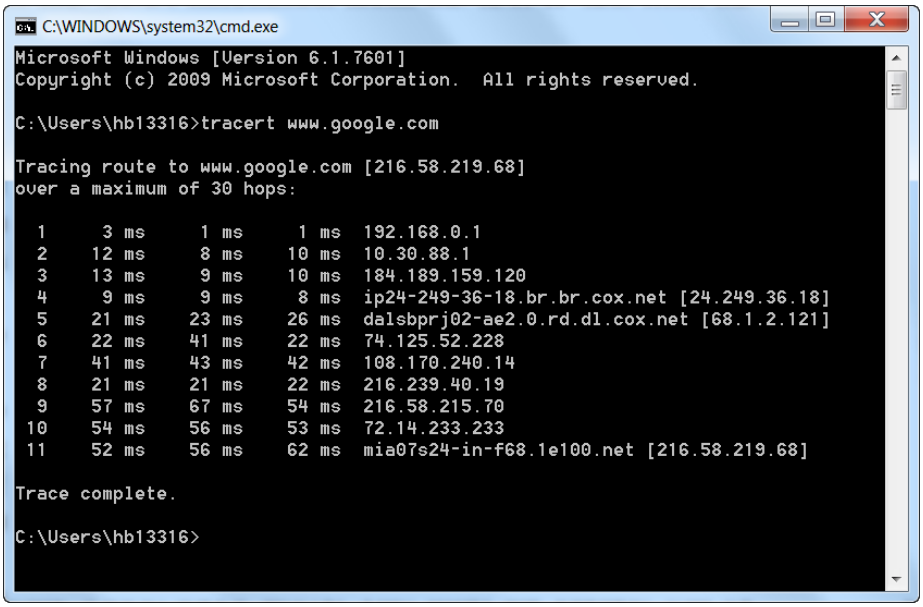
Capture Trace

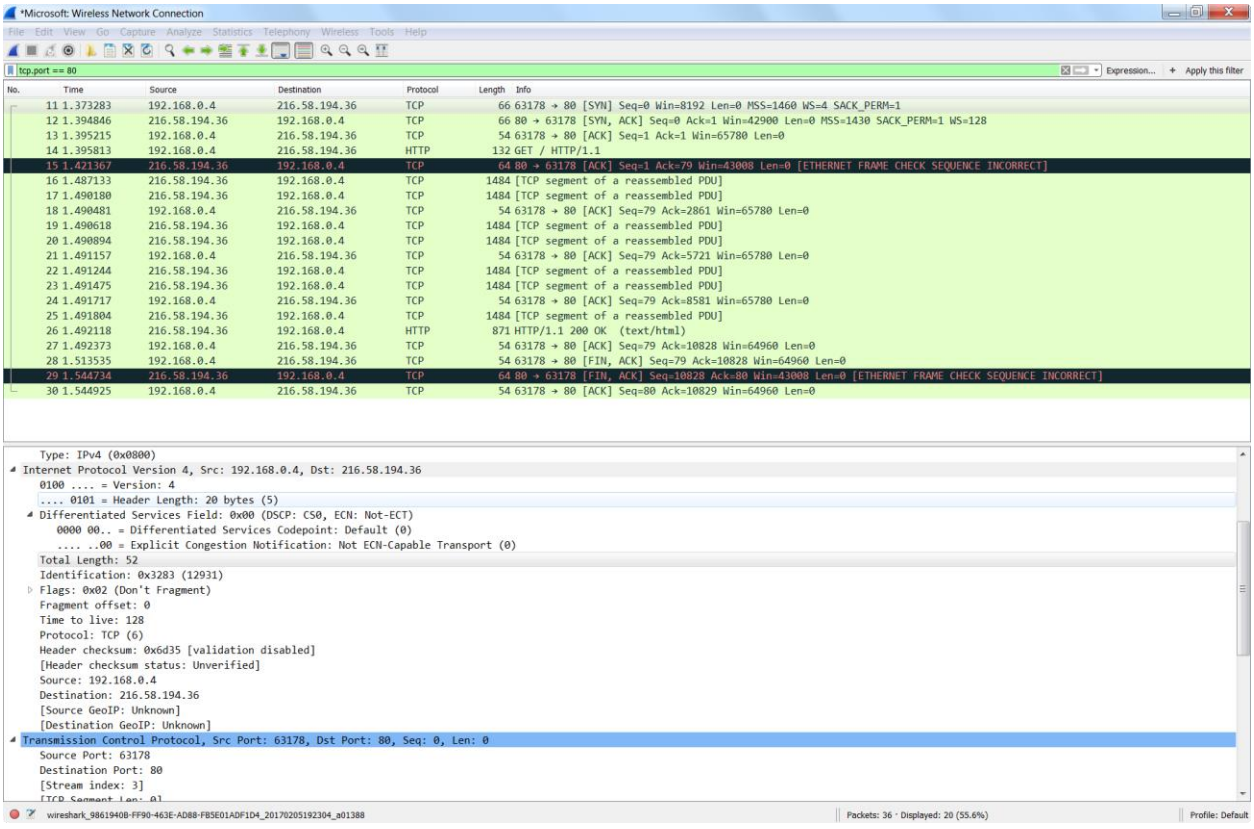
```
C:\Users\hb13316>tracert www.uwa.edu.au

Tracing route to www.uwa.edu.au.cdn.cloudflare.net [104.20.11.164]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  34.153.21.254
  2     1 ms     1 ms     1 ms  us-bro-460-e-r1.network.halliburton.com [34.38.1
47.254]
  3     7 ms     6 ms     6 ms  34.251.242.161
  4    14 ms    19 ms    14 ms  34.251.240.81
  5    12 ms    12 ms    12 ms  us-hal-np2-r1-mpls.network.halliburton.com [34.2
51.240.82]
  6    12 ms    12 ms    12 ms  us-hal-np2-core1.network.halliburton.com [34.36.
248.1]
  7    13 ms    12 ms    12 ms  us-hal-np2-r7-twc10g.network.halliburton.com [34
.36.248.98]
  8    19 ms    18 ms    18 ms  us-hal-np1-r101-man-h1.network.halliburton.com [
10.250.0.25]
  9    19 ms    19 ms    21 ms  us-hal-np3-core1-rcore1.network.halliburton.com
[10.192.1.21]
 10    19 ms    18 ms    18 ms  us-hal-np1-igw103-nat-h9.network.halliburton.com
 [134.132.52.2]
 11    19 ms    19 ms    19 ms  us-hal-np1-igw101-inap-h3.network.halliburton.co
m [10.192.255.252]
 12    21 ms    19 ms    19 ms  border3.te7-1.halliburton-12.dal006.pnap.net [21
6.52.184.121]
 13    23 ms    20 ms    23 ms  core2.po2-20g-bbnet2.dal006.pnap.net [216.52.191
.71]
 14    20 ms    20 ms    20 ms  bbr2.ae9.inapvox-26.dal006.pnap.net [64.95.158.2
42]
 15    20 ms    20 ms    19 ms  bbr1.ae7.dal006.pnap.net [64.95.158.201]
 16    21 ms    21 ms    20 ms  13335.dal.equinix.com [206.223.118.145]
 17    22 ms    21 ms    20 ms  104.20.11.164

Trace complete.
```

Was on the Halliburton Network which didn’t allow me to curl

```
C:\Users\hb13316>curl https://www.google.com
curl: (7) Failed to connect to www.google.com port 443: Connection refused
```

Back to home on my home network:





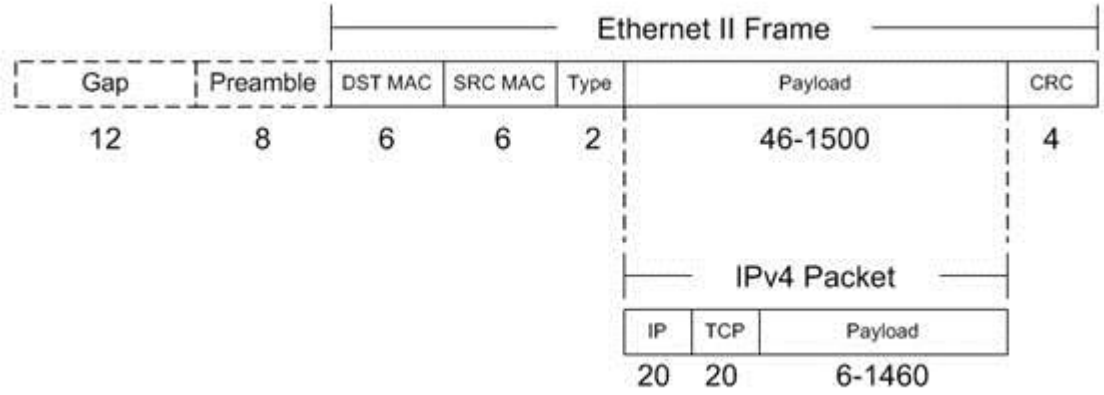
Inspect the Trace

```
Frame 14: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
Ethernet II, Src: IntelCor_41:de:b8 (00:24:d7:41:de:b8), Dst: Netgear_4f:91:63 (6c:b0:ce:4f:91
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 216.58.194.36
    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: 118
    Identification: 0x3285 (12933)
  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: 0x6cf1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.0.4
    Destination: 216.58.194.36
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 63178, Dst Port: 80, Seq: 1, Ack: 1, Len: 78
Hypertext Transfer Protocol
```

```
0000  6c b0 ce 4f 91 63 00 24  d7 41 de b8 08 00 45 00   l..O.c.$ .A....E.
0010  00 76 32 85 40 00 80 06  6c f1 c0 a8 00 04 d8 3a   .v2.@... l......:
0020  c2 24 f6 ca 00 50 35 72  7a e4 59 42 bf 35 50 18   .$...P5r z.YB.5P.
0030  40 3d 6a 93 00 00 47 45  54 20 2f 20 48 54 54 50   @=j...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  67 6f 6f 67 6c 65 2e 63  6f 6d 0d 0a 55 73 65 72   google.c om..User
0060  2d 41 67 65 6e 74 3a 20  63 75 72 6c 2f 37 2e 34   -Agent:  curl/7.4
0070  39 2e 30 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   9.0..Acc ept: */*
0080  0d 0a 0d 0a                                       ....
```

Packet Structure

Source: http://www.tamos.net/~rhay/overhead/ip-packet-overhead.htm

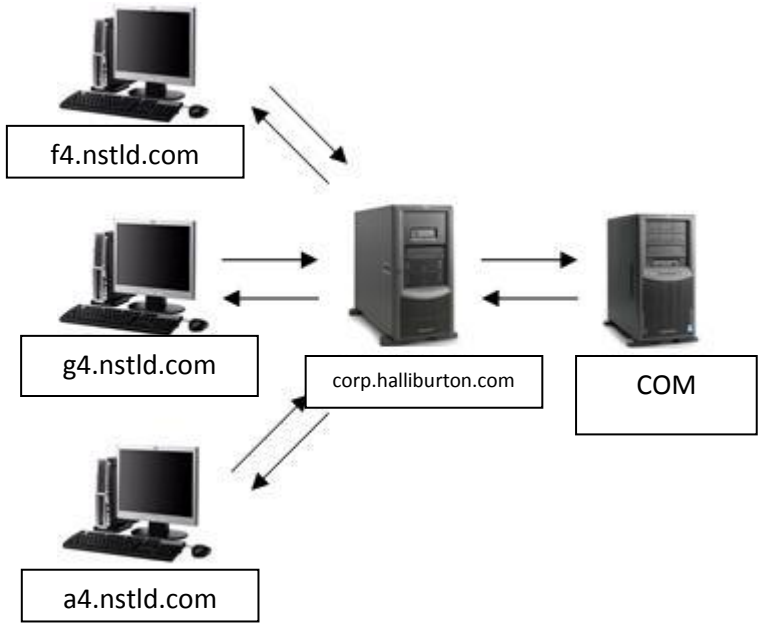


1) `Internet Protocol Version 4, Src: 192.168.0.4, Dst: 216.58.194.36`
   a. My Computer = 192.168.0.4
   b. Remote Server = 216.58.194.36
2) Header + Payload
3) No, it's different for different packets and no it's not the same in both directions between server client. With considering a pattern, yes, very interesting to see the same length and Identification increment by one from the previous packet.

4) 128 initial value for TTL packets sent from my computer. This is not the maximum possible that being the infamous 255 which makes up one byte.
   Source: https://www.quora.com/Why-is-the-maximum-TTL-value-in-an-IP-header-255
5) More Fragments = 0
6) 4 Bits and indicated by **IHL**

Manual Name Resolution

7)



corp.halliburton.com.	71347	IN	NS	f4.nstld.com
corp.halliburton.com.	71347	IN	NS	g4.nstld.com
corp.halliburton.com.	71347	IN	NS	a4.nstld.com

Capture and Inspect Trace – DNS

8) 2 bytes
9) Flag Response – Message is a Query (dns.flags.response) 2 bytes
10) DNS Header - 49 bytes
11) Yes – Type A
12) Yes – Type A
13) IP Address is carried in “Answers: Address”