

MSDS 7349 – Data and Network Security - Homework Wireshark

By: Kyle Killion

First Traced Captured – www.google.com 216.58.218.100

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the first packet (No. 186).

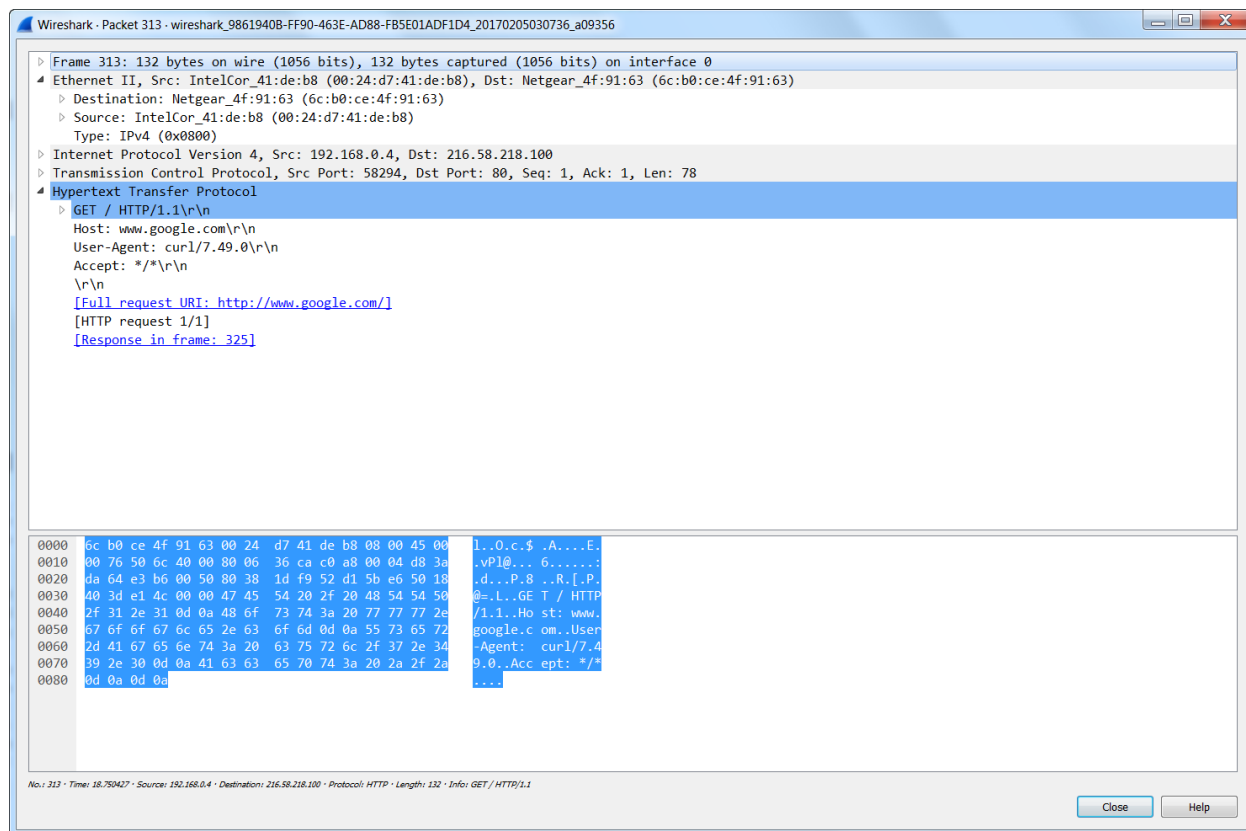
No.	Time	Source	Destination	Protocol	Length	Info
186	8.701466	216.58.218.100	192.168.0.4	TCP	64	80 → 49511 [ACK] Seq=1 Ack=79 Win=43008 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
187	8.774254	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
188	8.775052	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
189	8.775298	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [ACK] Seq=79 Ack=2861 Win=65780 Len=0
190	8.775439	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
191	8.775696	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
192	8.775930	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [ACK] Seq=79 Ack=5721 Win=65780 Len=0
193	8.776006	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
194	8.776209	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
195	8.776419	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [ACK] Seq=79 Ack=8581 Win=65780 Len=0
196	8.776487	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
197	8.776727	216.58.218.100	192.168.0.4	HTTP	841	HTTP/1.1 200 OK (text/html)
198	8.776994	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [ACK] Seq=79 Ack=10798 Win=65780 Len=0
199	8.856066	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [FIN, ACK] Seq=79 Ack=10798 Win=65780 Len=0
200	8.907909	216.58.218.100	192.168.0.4	TCP	64	80 → 49511 [FIN, ACK] Seq=10798 Ack=80 Win=43008 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
201	8.908048	192.168.0.4	216.58.218.100	TCP	54	49511 → 80 [ACK] Seq=80 Ack=10799 Win=65780 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Netgear_4f:91:63 (6c:b0:ce:4f:91:63), Dst: IntelCor_41:de:b8 (00:24:d7:41:de:b8)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.4
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xc291 (49809)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0xf6e8 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.1
Destination: 192.168.0.4
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 49505, Seq: 1, Ack: 1, Len: 0

0000 00 24 d7 41 de b8 6c b0 ce 4f 91 63 00 00 45 00 .\$.A..l..O.c..E.
0010 00 28 c2 91 40 00 40 06 f6 e8 c0 a8 00 01 c0 a8 .(.@.@.....
0020 00 04 00 50 c1 61 13 82 19 39 2c 15 45 d9 50 10 ...P.a..9,.E.P.
0030 40 e6 8d 3d 00 00 @... ..

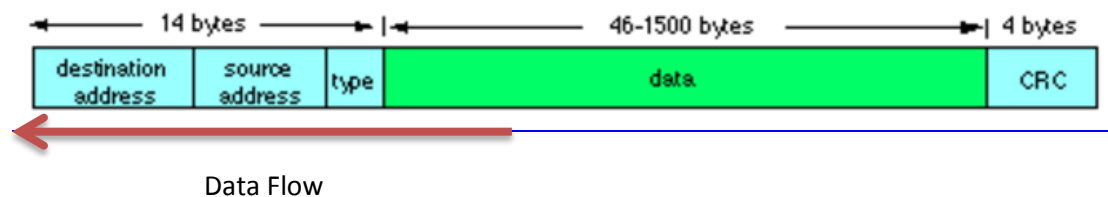
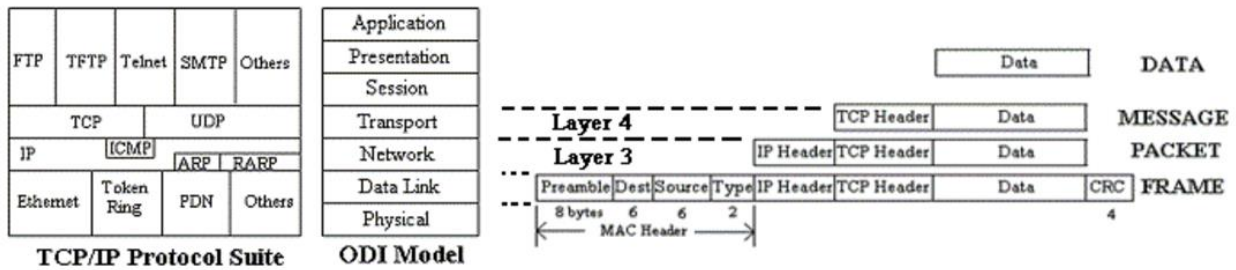
Frame (frame), 54 bytes | Packets: 258 · Displayed: 58 (22.5%) | Profile: Default

Wireshark packet structure screen:



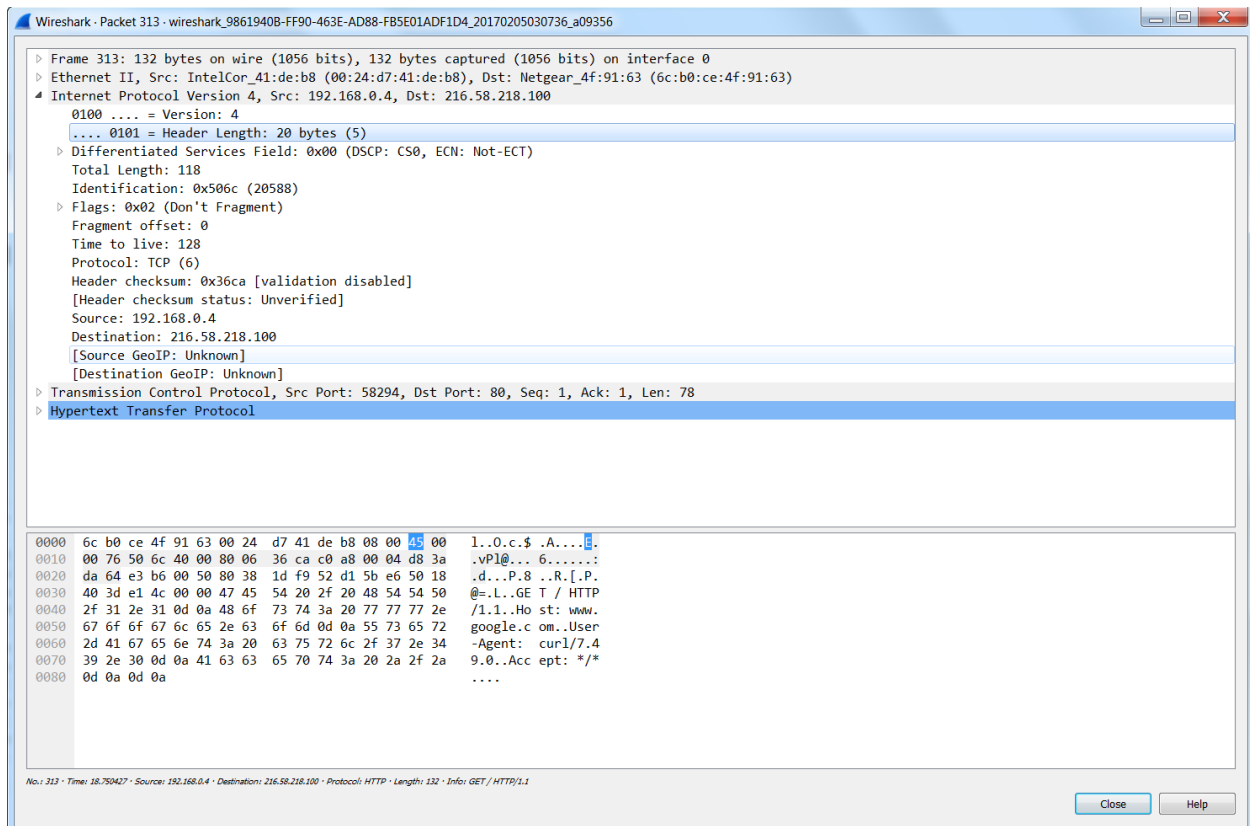
Ethernet II Diagram

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



Data Flow

Header Length:



MSDS 7349 – Data and Network Security - Homework Wireshark

Frame or Packet Length:

Wireshark · Packet 313 · wireshark_9861940B-FF90-463E-AD88-FB5E01ADF1D4_20170205030736_a09356

Frame 313: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
Interface id: 0 (\Device\NPF_{9861940B-FF90-463E-AD88-FB5E01ADF1D4})
Encapsulation type: Ethernet (1)
Arrival Time: Feb 5, 2017 03:07:54.944202000 Central Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1486285674.944202000 seconds
[Time delta from previous captured frame: 0.010891000 seconds]
[Time delta from previous displayed frame: 0.010891000 seconds]
[Time since reference or first frame: 18.750427000 seconds]
Frame Number: 313
Frame Length: 132 bytes (1056 bits)
Capture Length: 132 bytes (1056 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]

Protocol Overhead

No.	Time	Source	Destination	Protocol	Length	Info
315	18.847483	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
316	18.848735	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
318	18.849127	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
319	18.849405	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
321	18.849816	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
322	18.850082	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
324	18.850473	216.58.218.100	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
325	18.850825	216.58.218.100	192.168.0.4	HTTP	840	HTTP/1.1 200 OK (text/html)
310	18.703647	192.168.0.4	216.58.218.100	TCP	66	58294 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
312	18.739536	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0
313	18.750427	192.168.0.4	216.58.218.100	HTTP	132	GET / HTTP/1.1
317	18.848956	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=79 Ack=2001 Win=65780 Len=0
320	18.849712	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=79 Ack=5721 Win=65780 Len=0
323	18.850366	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=79 Ack=8581 Win=65780 Len=0
326	18.851073	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=79 Ack=10797 Win=64992 Len=0
327	18.884428	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [FIN, ACK] Seq=79 Ack=10797 Win=64992 Len=0
329	18.910287	192.168.0.4	216.58.218.100	TCP	54	58294 → 80 [ACK] Seq=80 Ack=10798 Win=64992 Len=0

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-mp1s.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
```

MSDS 7349 – Data and Network Security - Homework Wireshark

Back to home on my home network:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\hb13316>tracert www.google.com

Tracing route to www.google.com [216.58.219.68]
over a maximum of 30 hops:

  1    3 ms    1 ms    1 ms  192.168.0.1
  2   12 ms    8 ms   10 ms  10.30.88.1
  3   13 ms    9 ms   10 ms  184.189.159.120
  4    9 ms    9 ms    8 ms  ip24-249-36-18.br.br.cox.net [24.249.36.18]
  5   21 ms   23 ms   26 ms  dalsbprj02-ae2.0.rd.dl.cox.net [68.1.2.121]
  6   22 ms   41 ms   22 ms  74.125.52.228
  7   41 ms   43 ms   42 ms  108.170.240.14
  8   21 ms   21 ms   22 ms  216.239.40.19
  9   57 ms   67 ms   54 ms  216.58.215.70
 10   54 ms   56 ms   53 ms  72.14.233.233
 11   52 ms   56 ms   62 ms  mia07s24-in-f68.1e100.net [216.58.219.68]

Trace complete.

C:\Users\hb13316>
```

Microsoft Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
11	1.373283	192.168.0.4	216.58.194.36	TCP	66	63178 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
12	1.394846	216.58.194.36	192.168.0.4	TCP	66	80 → 63178 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0 MSS=1430 SACK_PERM=1 WS=128
13	1.395215	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0
14	1.395813	192.168.0.4	216.58.194.36	HTTP	132	GET / HTTP/1.1
15	1.421367	216.58.194.36	192.168.0.4	TCP	64	80 → 63178 [ACK] Seq=1 Ack=79 Win=43008 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
16	1.487133	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
17	1.490180	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
18	1.490481	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=79 Ack=2861 Win=65780 Len=0
19	1.490618	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
20	1.490894	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
21	1.491157	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=79 Ack=5721 Win=65780 Len=0
22	1.491244	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
23	1.491475	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
24	1.491717	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=79 Ack=8581 Win=65780 Len=0
25	1.491804	216.58.194.36	192.168.0.4	TCP	1484	[TCP segment of a reassembled PDU]
26	1.492118	216.58.194.36	192.168.0.4	HTTP	871	HTTP/1.1 200 OK (text/html)
27	1.492373	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=79 Ack=10828 Win=64960 Len=0
28	1.513535	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [FIN, ACK] Seq=79 Ack=10828 Win=64960 Len=0
29	1.544734	216.58.194.36	192.168.0.4	TCP	64	80 → 63178 [FIN, ACK] Seq=10828 Ack=80 Win=43008 Len=0 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
30	1.544925	192.168.0.4	216.58.194.36	TCP	54	63178 → 80 [ACK] Seq=80 Ack=10829 Win=64960 Len=0

Type: IPv4 (0x0800)

- 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: 52
 - Identification: 0x3283 (12931)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: TCP (6)
 - Header checksum: 0x6d35 [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: 0, Len: 0
 - Source Port: 63178
 - Destination Port: 80
 - [Stream index: 3]
 - [TCP Segment Len: 0]

wireshark_98619408-FF90-463E-A088-FB5E01ADF1D4_20170205192304_001388

Packets: 36 · Displayed: 20 (55.6%)

Profile: Default

Inspect the Trace

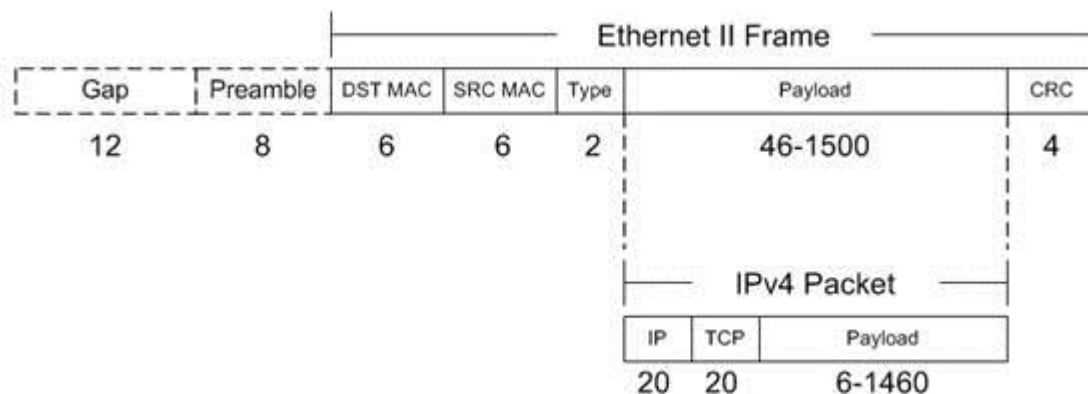
```

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:91:63)
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 1..0.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.SP.
  0030 40 3d 6a 93 00 00 47 45 54 20 2f 20 48 54 50 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>

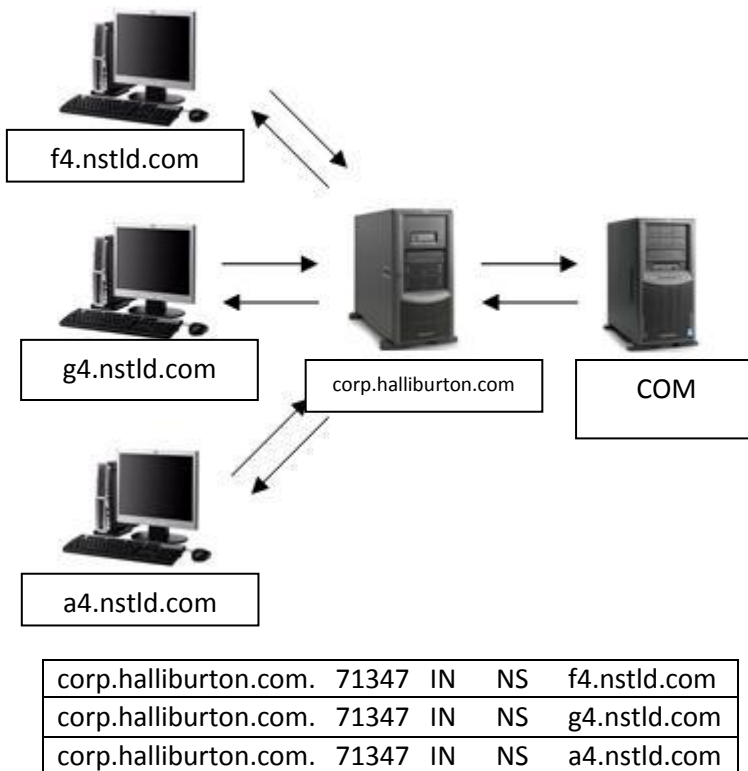


- 1) Internet Protocol Version 4, Src: 192.168.0.4, Dst: 216.58.194.36
 - a. My Computer = 192.168.0.4
 - b. Remote Server = 216.58.194.36
- 2) Header + Payload
- 3) No, it's different for different packets and no it's not the same in both directions between server client. With considering a pattern, 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)



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”