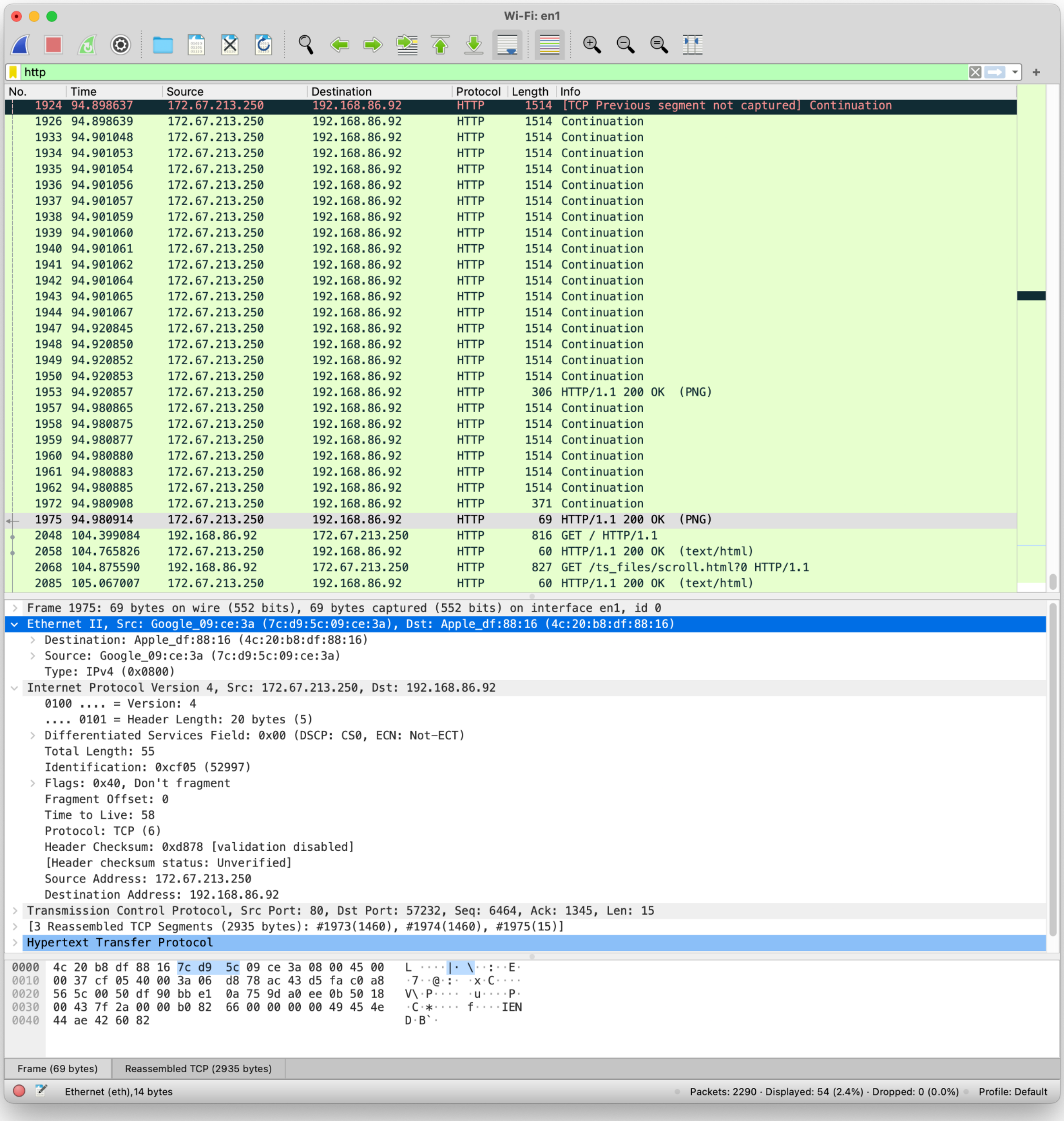
Ali Serdar Aydogdu
CS 2600 - X01
Lab 6
4/27/2021

Lab Exercise 6: IP Packet Header Dissection

See the last page for the screenshot.

1. What is the IP header length in bytes? (Wireshark translates the integer value in the Header length (HLen) field to the actual number of bytes for you.)
   Header length: 20 bytes
2. What is the integer value actually contained in the IP header's Header length field?
   (5)
3. What is the Total Length of the IP packet? Does this include the IP header? Does it include the Data-link layer (Ethernet or WiFi) frame header?
   Total Length: 45, It includes the IP header, it does not include the Data-link layer.
4. What is the Time To Live (TTL) value? What does this represent? Can you make an "educated guess" as to how many routers this packet has crossed on its way to your computer?
   58
5. Which Internet Layer 3 Transport protocol header is carried within this IP packet?
   TCP
6. Are there any options present at the end of the IP header (after the Destination Address)? If so, what are they?
   No
7. Clear the HTTP filter by clicking at the right of the Display Filter field, so that you are once again displaying all of the captured packets. Try Statistics | Packet Lengths again (without a filter). What are the most common packet length ranges? Why do you think this is the case?
   1500, the info section of them says "Continuation", most likely they are data streams of large files.



```
http
```

```
No.   Time        Source          Destination     Protocol Length Info
 1924 94.898637   172.67.213.250  192.168.86.92   HTTP     1514 [TCP Previous segment not captured] Continuation
 1926 94.898639   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1933 94.901048   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1934 94.901053   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1935 94.901054   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1936 94.901056   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1937 94.901057   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1938 94.901059   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1939 94.901060   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1940 94.901061   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1941 94.901062   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1942 94.901064   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1943 94.901065   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1944 94.901067   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1947 94.920845   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1948 94.920850   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1949 94.920852   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1950 94.920853   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1953 94.920857   172.67.213.250  192.168.86.92   HTTP      306 HTTP/1.1 200 OK  (PNG)
 1957 94.980865   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1958 94.980875   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1959 94.980877   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1960 94.980880   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1961 94.980883   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1962 94.980885   172.67.213.250  192.168.86.92   HTTP     1514 Continuation
 1972 94.980908   172.67.213.250  192.168.86.92   HTTP      371 Continuation
 1975 94.980914   172.67.213.250  192.168.86.92   HTTP       69 HTTP/1.1 200 OK  (PNG)
 2048 104.399084  192.168.86.92   172.67.213.250  HTTP      816 GET / HTTP/1.1
 2058 104.765826  172.67.213.250  192.168.86.92   HTTP       60 HTTP/1.1 200 OK  (text/html)
 2068 104.875590  192.168.86.92   172.67.213.250  HTTP      827 GET /ts_files/scroll.html?0 HTTP/1.1
 2085 105.067007  172.67.213.250  192.168.86.92   HTTP       60 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 1975: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface en1, id 0
v Ethernet II, Src: Google_09:ce:3a (7c:d9:5c:09:ce:3a), Dst: Apple_df:88:16 (4c:20:b8:df:88:16)
  > Destination: Apple_df:88:16 (4c:20:b8:df:88:16)
  > Source: Google_09:ce:3a (7c:d9:5c:09:ce:3a)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 172.67.213.250, Dst: 192.168.86.92
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 55
    Identification: 0xcf05 (52997)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 58
    Protocol: TCP (6)
    Header Checksum: 0xd878 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.67.213.250
    Destination Address: 192.168.86.92
> Transmission Control Protocol, Src Port: 80, Dst Port: 57232, Seq: 6464, Ack: 1345, Len: 15
> [3 Reassembled TCP Segments (2935 bytes): #1973(1460), #1974(1460), #1975(15)]
> Hypertext Transfer Protocol
```

```
0000  4c 20 b8 df 88 16 7c d9  5c 09 ce 3a 08 00 45 00   L ····|· \··:··E·
0010  00 37 cf 05 40 00 3a 06  d8 78 ac 43 d5 fa c0 a8   ·7··@·:· ·x·C····
0020  56 5c 00 50 df 90 bb e1  0a 75 9d a0 ee 0b 50 18   V\·P···· ·u····P·
0030  00 43 7f 2a 00 00 b0 82  66 00 00 00 00 49 45 4e   ·C·*···· f····IEN
0040  44 ae 42 60 82                                     D·B`·
```

Ethernet (eth),14 bytes

Packets: 2290 · Displayed: 54 (2.4%) · Dropped: 0 (0.0%)   Profile: Default