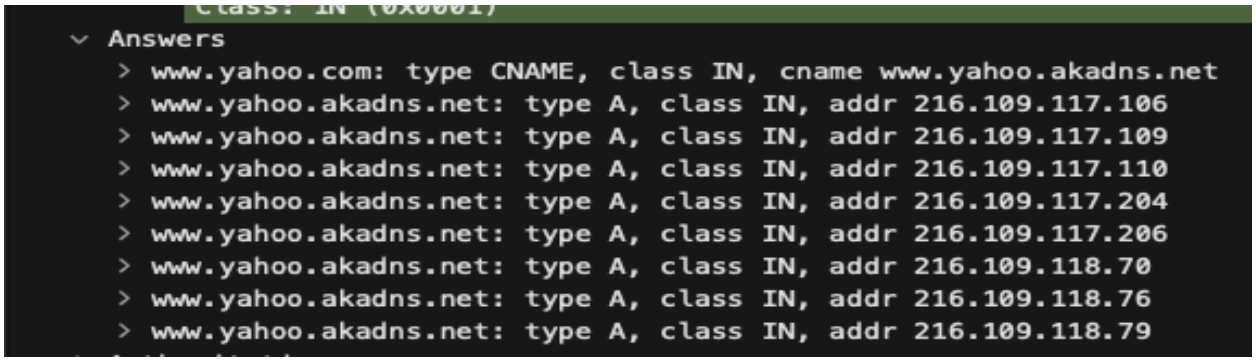
Ruben Valdez
Assignment: Lab 1
Basic Wireshark Network Analysis

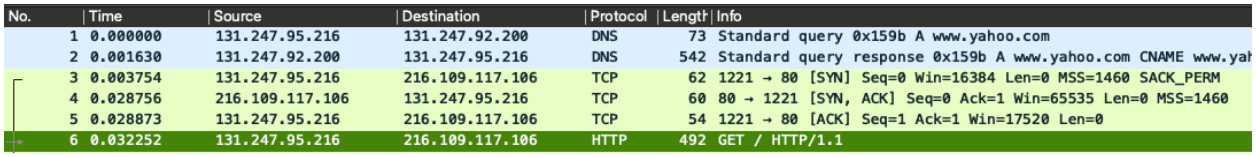
Spring 2025 | CSEC 5306
Computer Networks and Security
Prof. Alsmadi

Date: January 19, 2025

a) The following indicate the CNAME, “www.yahoo.akadns.net”. In the below screenshot, there are multiple IP addresses listed for this website.

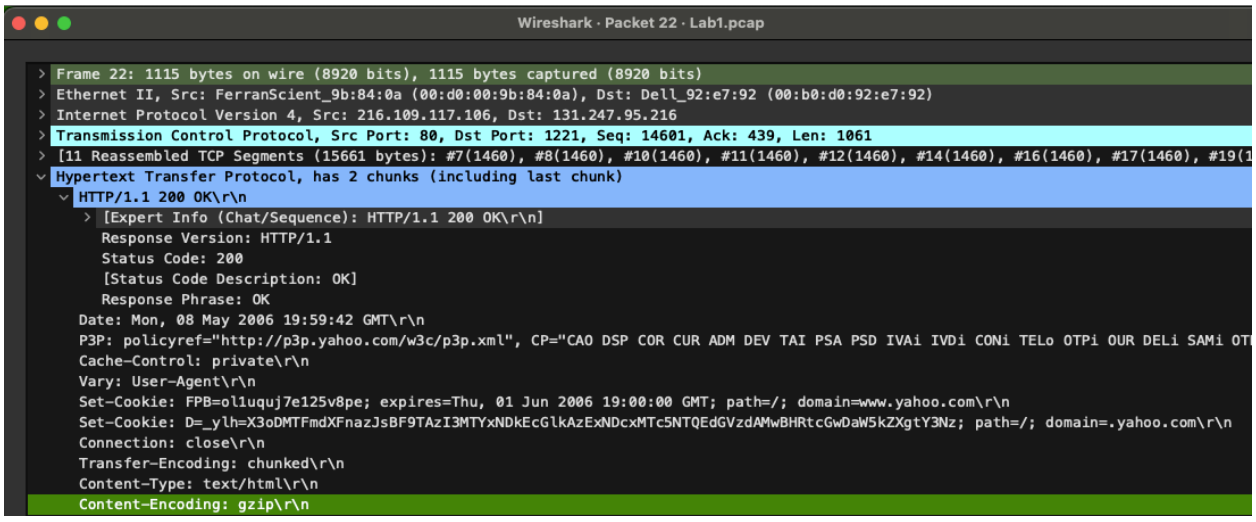


b) On the 6th packet/frame is when the web pages is received.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	131.247.95.216	131.247.92.200	DNS	73	Standard query 0x159b A www.yahoo.com
2	0.001630	131.247.92.200	131.247.95.216	DNS	542	Standard query response 0x159b A www.yahoo.com CNAME www.yah
3	0.003754	131.247.95.216	216.109.117.106	TCP	62	1221 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
4	0.028756	216.109.117.106	131.247.95.216	TCP	60	80 → 1221 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
5	0.028873	131.247.95.216	216.109.117.106	TCP	54	1221 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
6	0.032252	131.247.95.216	216.109.117.106	HTTP	492	GET / HTTP/1.1

c) Packet 22, proves the website uses gzip to compress its data for sending. It also writes cookies.



d) In packets 26 and 27, I believe there is a DNS redirect.

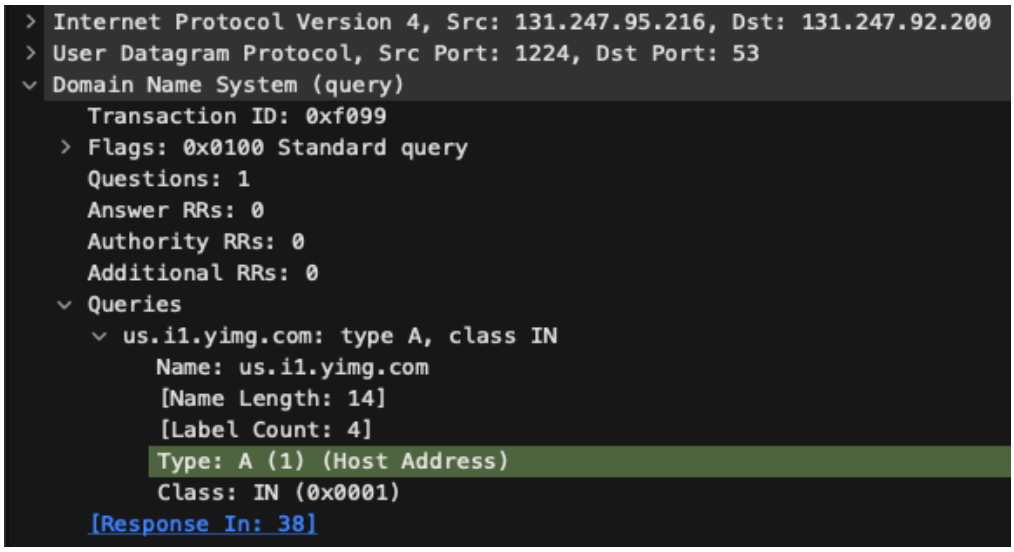
```
> Internet Protocol Version 4, Src: 131.247.95.216, Dst: 131.247.92.200
> User Datagram Protocol, Src Port: 1222, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x409b
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v us.js2.yimg.com: type A, class IN
        Name: us.js2.yimg.com
        [Name Length: 15]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 27]
```

```
> Internet Protocol Version 4, Src: 131.247.92.200, Dst: 131.247.95.216
> User Datagram Protocol, Src Port: 53, Dst Port: 1222
v Domain Name System (response)
    Transaction ID: 0x409b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v us.js2.yimg.com: type A, class IN
        Name: us.js2.yimg.com
        [Name Length: 15]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Answers
    > us.js2.yimg.com: type CNAME, class IN, cname a321.yimg.com.georedirector.akadns.net
    > a321.yimg.com.georedirector.akadns.net: type CNAME, class IN, cname a321.x.a.yimg.com
    > a321.x.a.yimg.com: type A, class IN, addr 64.21.46.151
    > a321.x.a.yimg.com: type A, class IN, addr 64.21.46.134
    > a321.x.a.yimg.com: type A, class IN, addr 64.21.46.150
    [Request In: 26]
    [Time: 0.002442000 seconds]
```

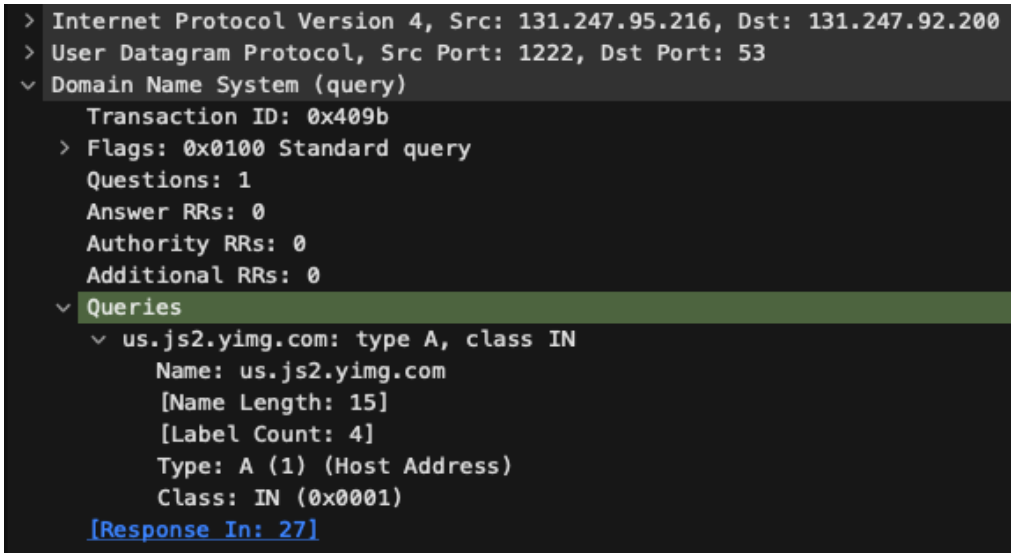
e)

This DNS request is for image
The address in frame 37, “us.i1.yimg.com” was not listed in frame 26. The address listed in frame 26 was “us.js2.yimg.com”.

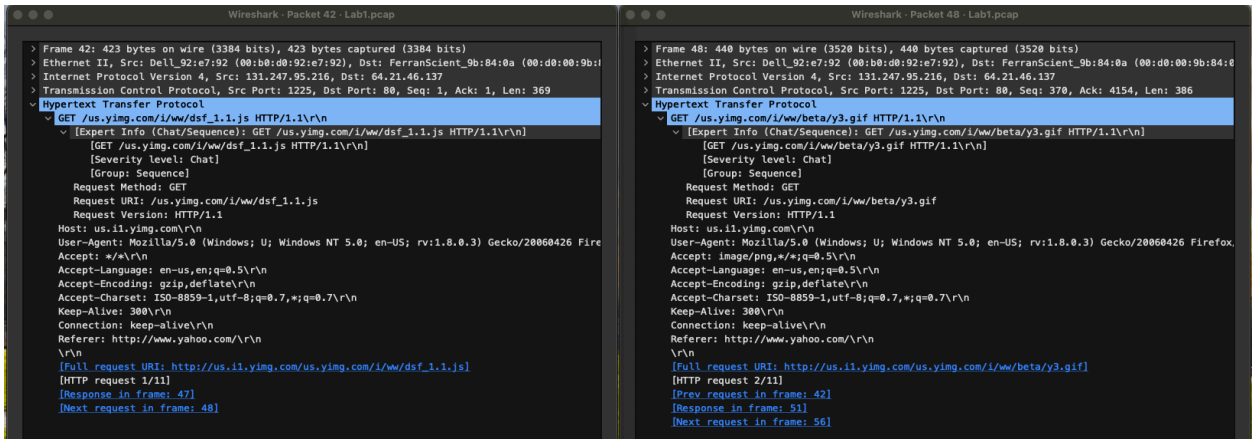
Frame 37



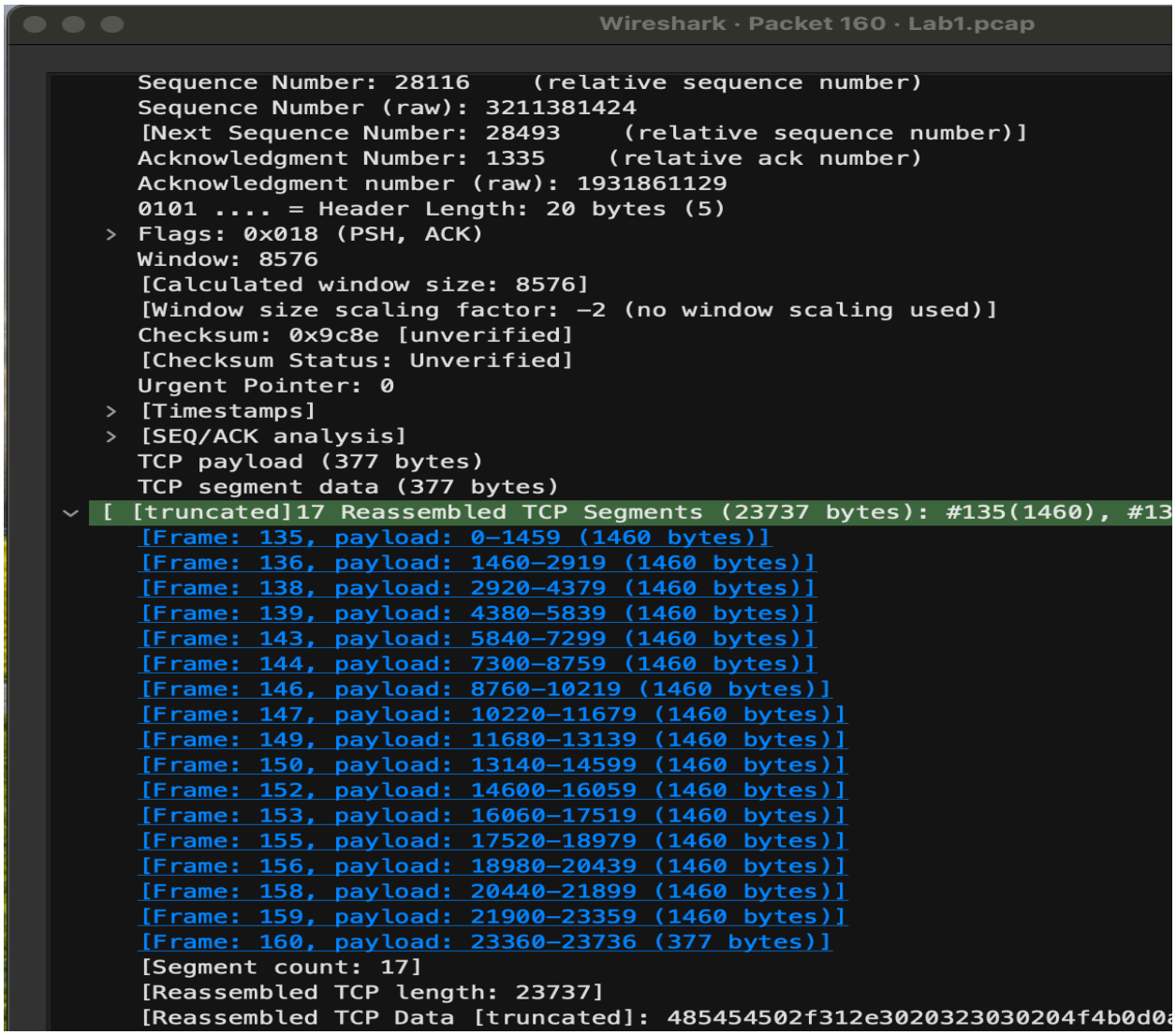
Frame 26



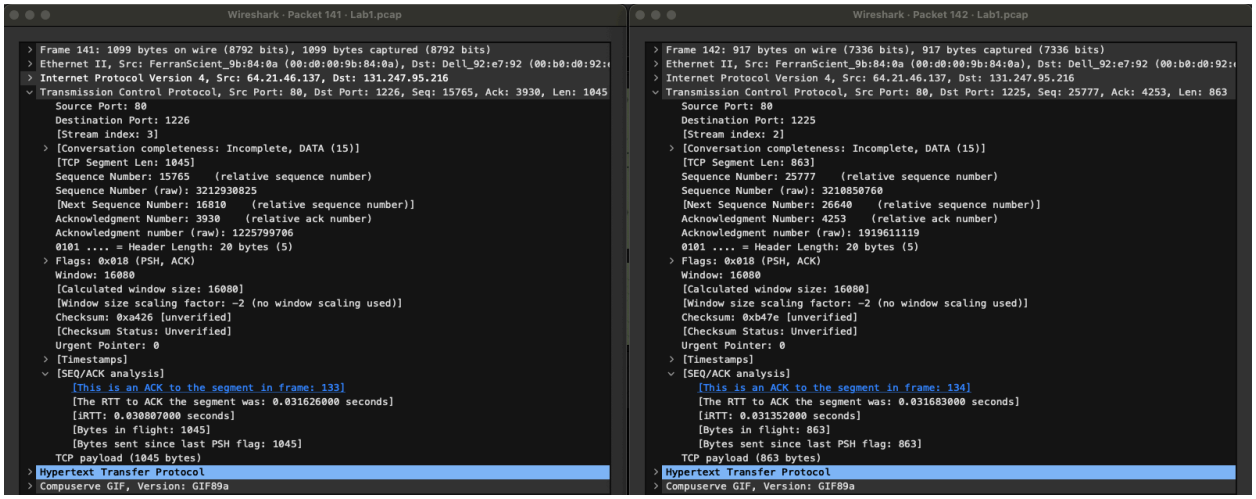
f) I would think, that the reason for this was because the IPs were the same. In addition, the Host value were the same “us.i1.yimg.com”.



g) Below is frame 160. The screen shot shows a summary of the segmentation of frames. Here, frames 139 and 143 are shown but NOT frames 141 and 142.



h) Frame 141 is ACK to segment in frame 133. Frame 142 Is an ACK to the segment in frame 134.



133	1.036937	131.247.95.216	64.21.46.137	HTTP	442	GET /us.yimg.com/i/ww/trfc_bckt.gif HTTP/1.1
134	1.037005	131.247.95.216	64.21.46.137	HTTP	440	GET /us.yimg.com/i/ww/answers.gif HTTP/1.1