Brian Hert
Badruddoja, Syed
CSC 138
9th, February 2024

Lab 1 Introduction to Wireshark and Packet Capture

Task 4

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window? Attach screen shots of your observation. What are these protocols used for? (Hint: Scroll the protocol tab in the Wireshark tool)

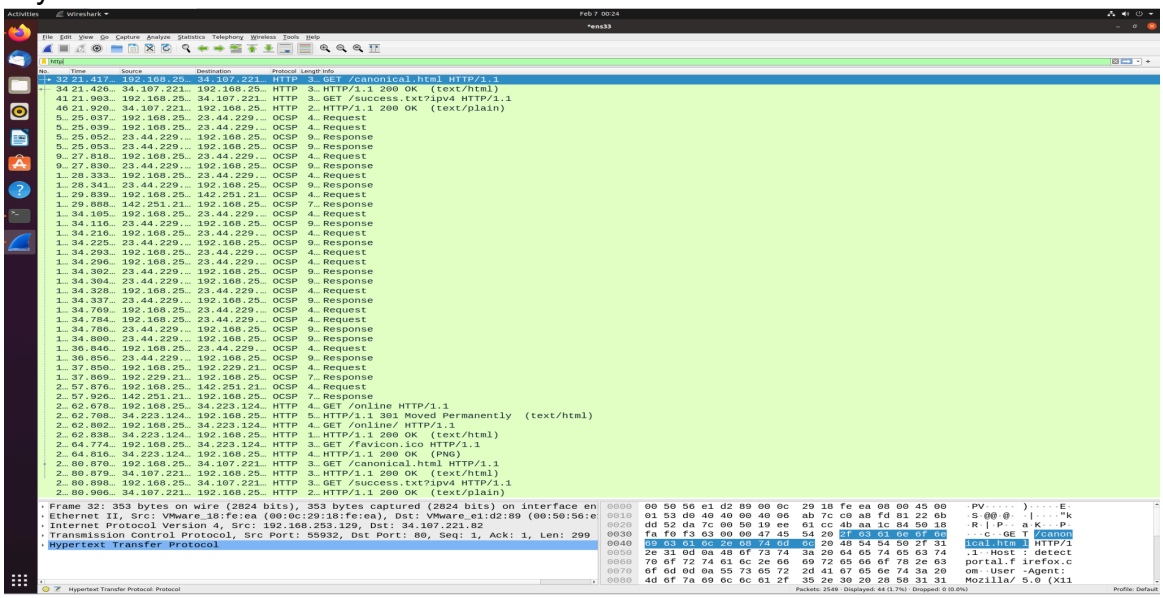
```
2… 84.426… 192.168.25… 192.168.25… NBNS  92 Name query NB WPAD<00>
2… 84.613… VMware_c0:… Broadcast   ARP   60 Who has 192.168.253.2? Tell 192.168.253.1
2… 84.677… 192.168.25… 224.0.0.251 MDNS  70 Standard query 0x0000 A wpad.local, "QM" question
```

- NetBIOS Name Service provides computer resolution and registration on the local area network. Design for creating an easy and ongoing method for sharing printers, files, and other resources.

- Address Resolution Protocol is a layer of two protocol designs to map MAC addresses to Ip addresses. This allows communication from different devices within the same network.

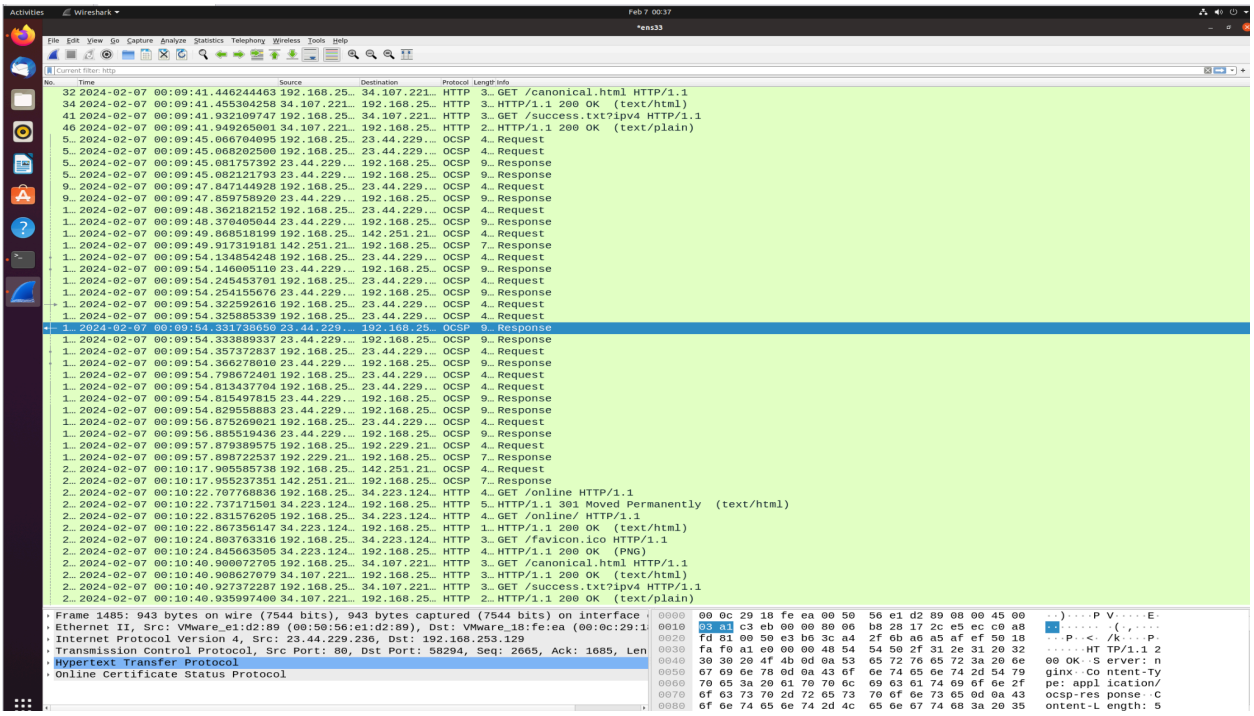
- Multicast Domain Name System is created for resolving host names to IP addresses within small networks that do not have a local DNS server such as small office environments.

2. On the display filter specification bar, type http and press enter. Attach a screenshot of your screen.



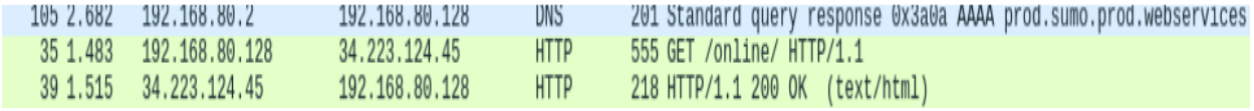
3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

It took me 0.023 Milliseconds to get the HTTP GET message sent until the HTTP OK was received.



4. What is the Internet address of www.neverssl.com? What is the Internet address of your computer? Attach a screenshot

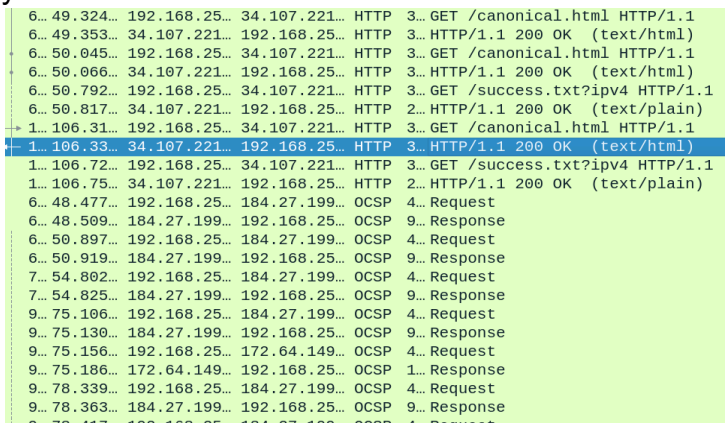
The internet address of the www.neverssl.com is: 34.223.124.45
My computer internet address: 192.680.80.128



5. What HTTP status codes do you see in the “info” column? What is the purpose of status codes?

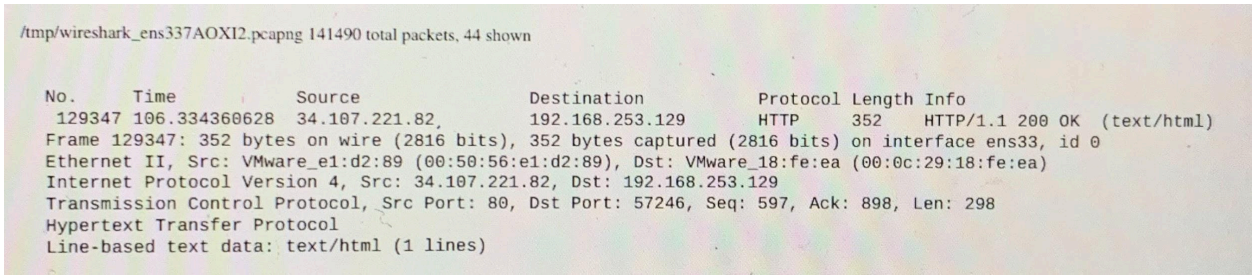
The status code shown is 200. The purpose of status codes is to display the status of

your connection to the website.



```
6… 49.324… 192.168.25… 34.107.221… HTTP  3… GET /canonical.html HTTP/1.1
6… 49.353… 34.107.221… 192.168.25… HTTP  3… HTTP/1.1 200 OK  (text/html)
6… 50.045… 192.168.25… 34.107.221… HTTP  3… GET /canonical.html HTTP/1.1
6… 50.066… 34.107.221… 192.168.25… HTTP  3… HTTP/1.1 200 OK  (text/html)
6… 50.792… 192.168.25… 34.107.221… HTTP  3… GET /success.txt?ipv4 HTTP/1.1
6… 50.817… 34.107.221… 192.168.25… HTTP  2… HTTP/1.1 200 OK  (text/plain)
1… 106.31… 192.168.25… 34.107.221… HTTP  3… GET /canonical.html HTTP/1.1
1… 106.33… 34.107.221… 192.168.25… HTTP  3… HTTP/1.1 200 OK  (text/html)
1… 106.72… 192.168.25… 34.107.221… HTTP  3… GET /success.txt?ipv4 HTTP/1.1
1… 106.75… 34.107.221… 192.168.25… HTTP  2… HTTP/1.1 200 OK  (text/plain)
6… 48.477… 192.168.25… 184.27.199… OCSP  4… Request
6… 48.509… 184.27.199… 192.168.25… OCSP  9… Response
6… 50.897… 192.168.25… 184.27.199… OCSP  4… Request
6… 50.919… 184.27.199… 192.168.25… OCSP  9… Response
7… 54.802… 192.168.25… 184.27.199… OCSP  4… Request
7… 54.825… 184.27.199… 192.168.25… OCSP  9… Response
9… 75.106… 192.168.25… 184.27.199… OCSP  4… Request
9… 75.130… 184.27.199… 192.168.25… OCSP  9… Response
9… 75.156… 192.168.25… 172.64.149… OCSP  4… Request
9… 75.186… 172.64.149… 192.168.25… OCSP  1… Response
9… 78.339… 192.168.25… 184.27.199… OCSP  4… Request
9… 78.363… 184.27.199… 192.168.25… OCSP  9… Response
```

6. Print the two HTTP messages (GET and OK) referred to question 3 above.



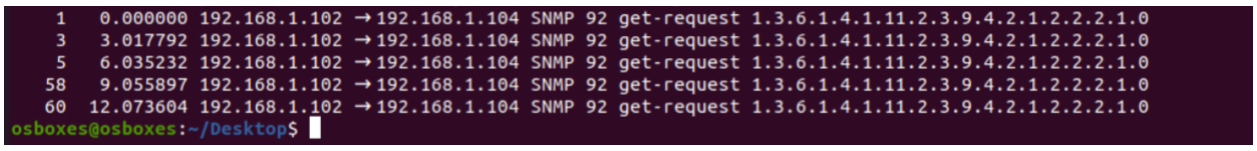
```
/tmp/wireshark_ens337AOXI2.pcapng 141490 total packets, 44 shown

No.     Time           Source                Destination           Protocol Length Info
 129347 106.334360628  34.107.221.82         192.168.253.129       HTTP     352    HTTP/1.1 200 OK  (text/html)
Frame 129347: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface ens33, id 0
Ethernet II, Src: VMware_e1:d2:89 (00:50:56:e1:d2:89), Dst: VMware_18:fe:ea (00:0c:29:18:fe:ea)
Internet Protocol Version 4, Src: 34.107.221.82, Dst: 192.168.253.129
Transmission Control Protocol, Src Port: 80, Dst Port: 57246, Seq: 597, Ack: 898, Len: 298
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
```

Task 6:

1. How many packets can you see when you run the command mentioned in option ‘c’. What protocols did you observe in the displayed window? Attach a screenshot.

I saw 5 packets when running the command. I observed SNMP as the protocol displayed.



```
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    3   3.017792 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    5   6.035232 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   58   9.055897 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   60  12.073604 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
osboxes@osboxes:~/Desktop$
```

2. How many packets are sourced from host 192.168.1.102?

27 packets are sourced from the host

```
osboxes@osboxes:~/Desktop$ tshark -r http-ethereal-trace-4 ip.src==192.168.1.102
    1   0.000000 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    3   3.017792 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    5   6.035232 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    7   7.196100 192.168.1.102 → 128.119.245.12 TCP 62 4307 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    9   7.236533 192.168.1.102 → 128.119.245.12 TCP 54 4307 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10   7.236929 192.168.1.102 → 128.119.245.12 HTTP 555 GET /ethereal-labs/lab2-4.html HTTP/1.1
   13   7.284335 192.168.1.102 → 165.193.123.218 TCP 62 4308 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   14   7.285795 192.168.1.102 → 134.241.6.82 TCP 62 4309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   16   7.305115 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=1 Ack=1 Win=64860 Len=0
   17   7.305485 192.168.1.102 → 165.193.123.218 HTTP 625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
   19   7.308503 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20   7.308803 192.168.1.102 → 134.241.6.82 HTTP 609 GET /~kurose/cover.jpg HTTP/1.1
   24   7.331386 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=572 Ack=2761 Win=64860 Len=0
   27   7.382784 192.168.1.102 → 128.119.245.12 TCP 54 4307 → 80 [ACK] Seq=502 Ack=1004 Win=63237 Len=0
   28   7.483377 192.168.1.102 → 165.193.123.218 TCP 54 4308 → 80 [ACK] Seq=572 Ack=3619 Win=64002 Len=0
   31   7.509396 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=69 Win=64172 Len=0
   34   7.510362 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=135 Win=64106 Len=0
   37   7.511335 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=184 Win=64057 Len=0
   40   7.532274 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=1646 Win=64240 Len=0
   43   7.539319 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=4566 Win=64240 Len=0
   46   7.557810 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=7486 Win=64240 Len=0
   49   7.566807 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=10406 Win=64240 Len=0
   52   7.581642 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=13326 Win=64240 Len=0
   55   7.589918 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=15829 Win=64240 Len=0
   56   7.601393 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [FIN, ACK] Seq=556 Ack=15829 Win=64240 Len=0
   58   9.055897 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   60  12.073604 192.168.1.102 → 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
osboxes@osboxes:~/Desktop$
```

3. How many packets are destined to the host 134.241.6.82

There are 13 packets destined for the host.

```
osboxes@osboxes:~/Desktop$ tshark -r http-ethereal-trace-4 ip.dst==134.241.6.82
   14   7.285795 192.168.1.102 → 134.241.6.82 TCP 62 4309 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   19   7.308503 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20   7.308803 192.168.1.102 → 134.241.6.82 HTTP 609 GET /~kurose/cover.jpg HTTP/1.1
   31   7.509396 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=69 Win=64172 Len=0
   34   7.510362 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=135 Win=64106 Len=0
   37   7.511335 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=184 Win=64057 Len=0
   40   7.532274 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=1646 Win=64240 Len=0
   43   7.539319 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=4566 Win=64240 Len=0
   46   7.557810 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=7486 Win=64240 Len=0
   49   7.566807 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=10406 Win=64240 Len=0
   52   7.581642 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=13326 Win=64240 Len=0
   55   7.589918 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [ACK] Seq=556 Ack=15829 Win=64240 Len=0
   56   7.601393 192.168.1.102 → 134.241.6.82 TCP 54 4309 → 80 [FIN, ACK] Seq=556 Ack=15829 Win=64240 Len=0
```

4. Attach screenshot of output from task 5.f.

```
================================================================================
TCP Conversations
Filter:<No Filter>
                                                |       <-      | |       ->      | |     Total     |    Relative    |   Duration   |
                                                | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |      Start     |              |
192.168.1.102:4309      <-> 134.241.6.82:80         21 16 kB          13 1,265 bytes      34 18 kB        7.285795000         0.3345
192.168.1.102:4308      <-> 165.193.123.218:80       5 3,902 bytes       5 849 bytes      10 4,751 bytes     7.284335000         0.1990
192.168.1.102:4307      <-> 128.119.245.12:80        3 1,179 bytes       4 725 bytes       7 1,904 bytes     7.196100000         0.1867
================================================================================
osboxes@osboxes:~/Desktop$
```