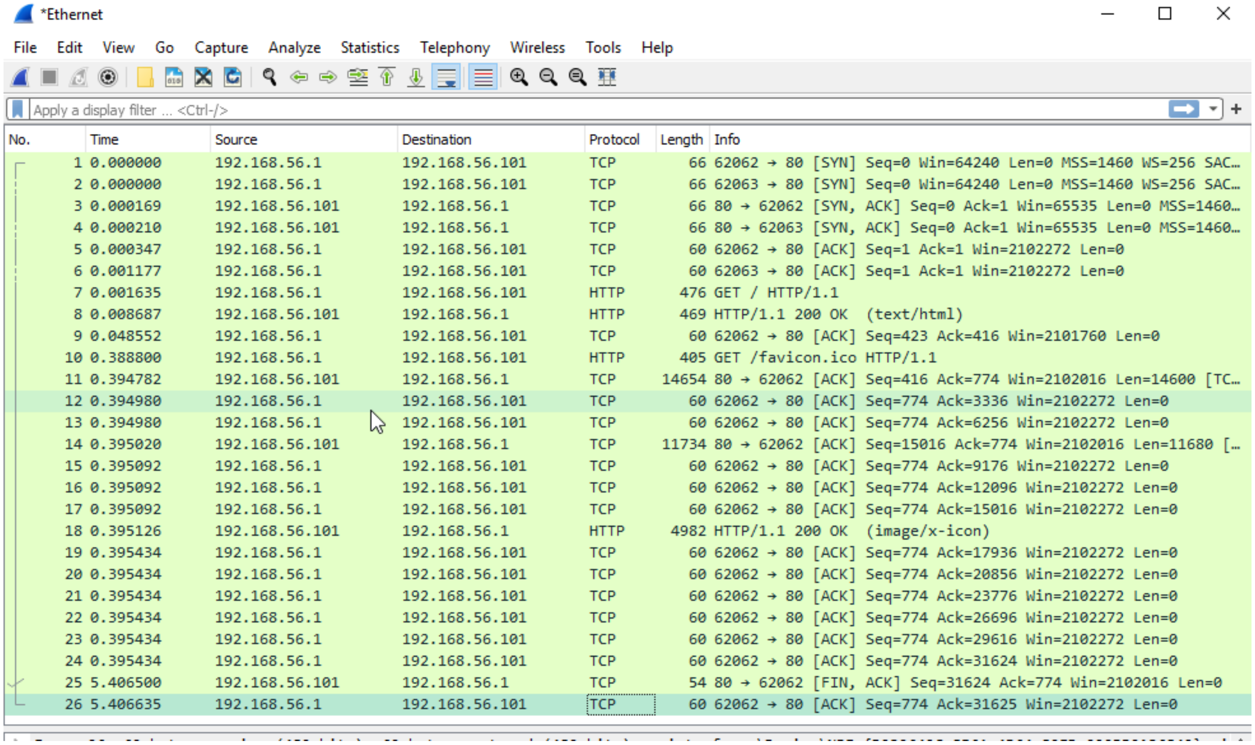
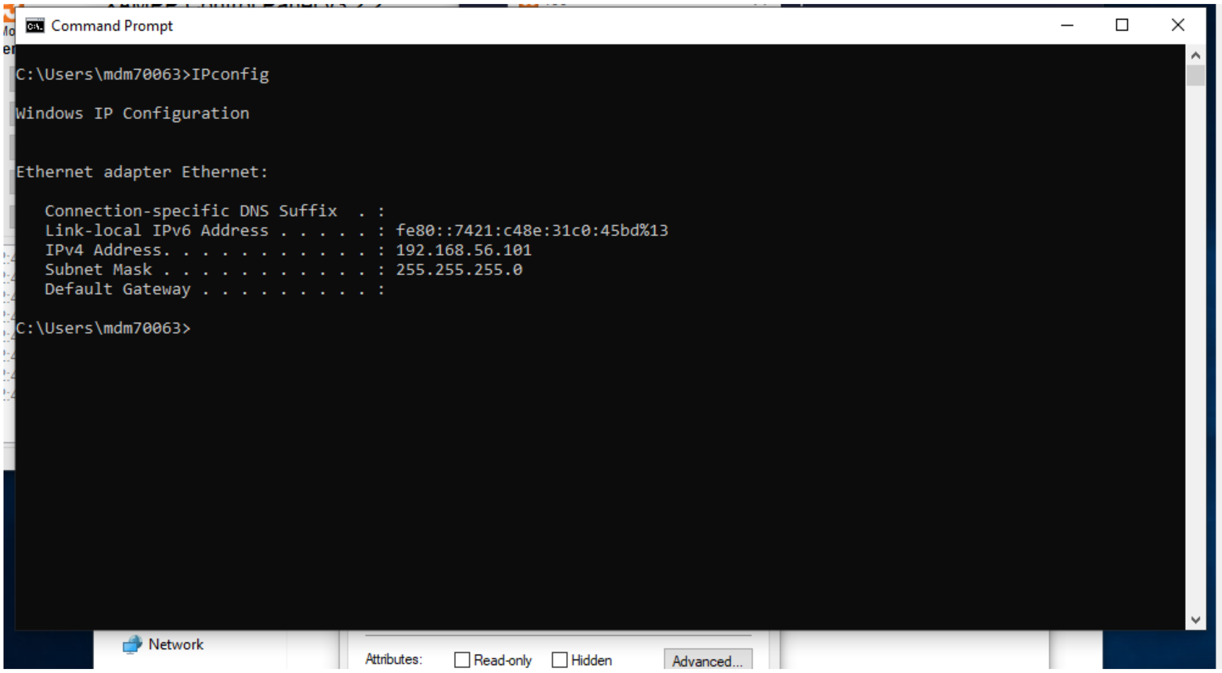

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	192.168.56.101	TCP	66	62062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC…
2	0.000000	192.168.56.1	192.168.56.101	TCP	66	62063 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC…
3	0.000169	192.168.56.101	192.168.56.1	TCP	66	80 → 62062 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
4	0.000210	192.168.56.101	192.168.56.1	TCP	66	80 → 62063 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
5	0.000347	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
6	0.001177	192.168.56.1	192.168.56.101	TCP	60	62063 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
7	0.001635	192.168.56.1	192.168.56.101	HTTP	476	GET / HTTP/1.1
8	0.008687	192.168.56.101	192.168.56.1	HTTP	469	HTTP/1.1 200 OK (text/html)
9	0.048552	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=423 Ack=416 Win=2101760 Len=0
10	0.388800	192.168.56.1	192.168.56.101	HTTP	405	GET /favicon.ico HTTP/1.1
11	0.394782	192.168.56.101	192.168.56.1	TCP	14654	80 → 62062 [ACK] Seq=416 Ack=774 Win=2102016 Len=14600 [TC…
12	0.394980	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=3336 Win=2102272 Len=0
13	0.394980	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=6256 Win=2102272 Len=0
14	0.395020	192.168.56.101	192.168.56.1	TCP	11734	80 → 62062 [ACK] Seq=15016 Ack=774 Win=2102016 Len=11680 […
15	0.395092	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=9176 Win=2102272 Len=0
16	0.395092	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=12096 Win=2102272 Len=0
17	0.395092	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=15016 Win=2102272 Len=0
18	0.395126	192.168.56.101	192.168.56.1	HTTP	4982	HTTP/1.1 200 OK (image/x-icon)
19	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=17936 Win=2102272 Len=0
20	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=20856 Win=2102272 Len=0
21	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=23776 Win=2102272 Len=0
22	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=26696 Win=2102272 Len=0
23	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=29616 Win=2102272 Len=0
24	0.395434	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=31624 Win=2102272 Len=0
25	5.406500	192.168.56.101	192.168.56.1	TCP	54	80 → 62062 [FIN, ACK] Seq=31624 Ack=774 Win=2102016 Len=0
26	5.406635	192.168.56.1	192.168.56.101	TCP	60	62062 → 80 [ACK] Seq=774 Ack=31625 Win=2102272 Len=0

8) WHAT IS THE FULL PATH OF DocumentRoot DIRECTORY ON YOUR WINDOWS 10 VM?

- C:\xampp\htdocs\index.html

9) WHAT IS THE IP ADDRESS OF YOUR HOST COMPUTER (the lab computer), and HOW DID YOU FIND THIS INFORMATION?

- 

```
C:\Users\mdm70063>IPconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7421:c48e:31c0:45bd%13
   IPv4 Address. . . . . . . . . . . : 192.168.56.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\mdm70063>
```

13) IN THE TCP THREE-WAY HANDSHAKE THAT BEGINS THE EXCHANGE OF THIS WEB PAGE, WHICH IP ADDRESS INITIATES COMMUNICATION (sends the first packet)? Hence, we will refer to this as packet 0.

(Hint: The TCP Three-Way Handshake can be identified from the TCP Flags used in the first 2 packets… SYN, SYN/ACK)

- 192.168.56.1

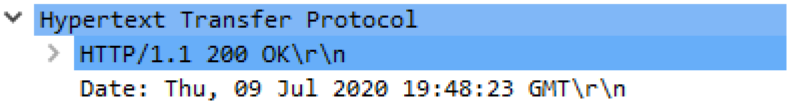
14) WHAT ARE THE INITIAL TCP SEQUENCE NUMBERS USED BY EACH SIDE OF THE WEB PAGE EXCHANGE?

- 0 and 1

15) HOW MANY PACKETS INTO THE CONVERSATION (how many packets after “packet 0”) IS THE PACKET WHICH CONTAINS THE TEXT OF THE WEB PAGE index.html?

- seven

16) a. WHAT IS THE FIRST LINE OF THE HTTP HEADER IN THE PACKET WHICH CONTAINS THE TEXT OF THE WEB PAGE index.html?

- 

```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 09 Jul 2020 19:48:23 GMT\r\n
```

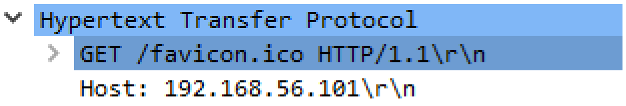
b. DOES THIS LINE OF THE HEADER INDICATE SUCCESS OR FAILURE?

- success

17) a. HOW MANY PACKETS INTO THE CONVERSATION CONVERSATION (how many packets after “packet 0”) IS THE PACKET WHICH CONTAINS THE GET REQUEST FROM THE Host Computer TO THE Windows 10 VM?

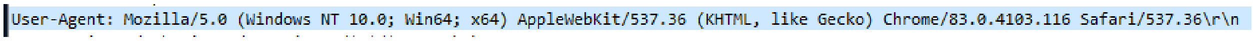
- nine

b. WHAT IS THE FIRST LINE OF THE GET REQUEST HTTP HEADER (starts with the word “GET”)?

- 

```
v Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    Host: 192.168.56.101\r\n
```

c. WHAT TEXT IS IN THE “User-Agent” FIELD OF THIS HEADER? (What do you think this User-Agent field indicates?)

- 

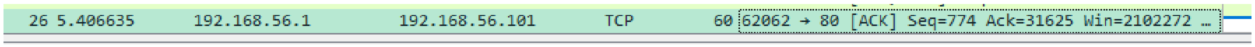
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36\r\n
```

- This tells you what os and web browser is used to view the HTML

18) WHICH SIDE (Host Computer or Windows 10 VM) IS THE FIRST TO SIGNAL AN END TO THE CONVERSATION (in other words, sends the TCP Fin flag)?

- Windows VM signals first to end the conversation. IP 192.168.56.101

19) WHAT ARE THE TCP FLAGS OF THE LAST PACKET SENT IN THE CONVERSATION? WHICH COMPUTER (Host or VM) SENDS THIS PACKET?

- 

```
26 5.406635      192.168.56.1        192.168.56.101      TCP        60 62062 → 80 [ACK] Seq=774 Ack=31625 Win=2102272 …
```

20) NOW THAT THE Windows 10 VM IS ON THE “INTERNAL NETWORKING,” OPEN A BROWSER INSIDE THE VM AND ACCESS http://www.csun.edu

DOES THIS SUCCEED? WHY OR WHY NOT?

- It will not work because there is no route from the VM to the internet.