**Homework 0: Wireshark with Web Traffic**

**8) WHAT IS THE FULL PATH OF Document Root DIRECTORY ON YOUR WINDOWS 10 VM?**

The path is

C:\xampp\htdocs

**9) WHAT IS THE IP ADDRESS OF YOUR HOST COMPUTER (your physical laptop/desktop), and HOW DID YOU FIND THIS INFORMATION?**

My host ip is 192.168.0.40 I am on ubuntu so I used ip addr show in the terminal if I was on windows I could have used ipconfig as well

**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.**

my host with ip 192.168.56.1 (in the virtual box virtual network) will start the exchange with a SYN packet

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

The sequence number is 0 for both sides of the exchange

**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?**

4 packets into the conversation

**16)**

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

HTTP/1.1 200 OK

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

It indicate Success

**17)**

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

3 packets into the conversation

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

GET / HTTP/1.1

**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 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36

it indicates what browser I am using.

**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)?**

The web server (windows 10 VM) ends the conversation and sends the FIN package.

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

The flag of the last packet is ACK. Sent from the server (VM)

**20) NOW THAT THE Windows 10 VM IS ON THE “VIRTUAL HOST-ONLY ADAPTER,”OPEN A BROWSER INSIDE THE VM AND ACCESS** [**http://www.csun.edu**](http://www.csun.edu) **DOES THIS SUCCEED? WHY OR WHY NOT?**

No, we can’t reach the internet because in host only adapter the VM is virtually connected only to the host.