CS 252 Spring 2017- Lab Quiz 1

Feb 2nd, 2017. Time: Upto 5pm (HARD DEADLINE). Max weight: 15%

Total marks scored : 35.9

You are given a trace file trace4.pcap. The trace has been taken by running **`tcpdump`** *on a host with IP address 192.168.0.106.*
Open this trace in wireshark and answer the following questions.

Justify all your answers briefly, *stating the packet IDs, fields and values of fields from which you made your inferences. If you did any calculations, show the expression which is resulting in the final answer. Only writing a final number or word answer will get zero marks.*

Section-1

Q

1. The trace has all sorts of packets but is overwhelmingly made of a trace of a connection related to one particular activity or command. What is that?

Ans. The host is downloading a pdf file. An HTTP request is sent to the IP address 128.171.224.109 in packet #14. The file transfer happens over TCP.

1

---

2. What is the IP address, port number of the two ends of this connection? How many packets do you see of this connection (hint: filter properly and see bottom right of wireshark window). Let us call this Connection X. The following questions are about this Connection X.
    a. At which IP address and port number is the "server" running? What type of server is this (i.e. is it FTP server, SSH server, Web server, NFS server..)
    b. At which IP address and port number is the client running? What possible terminal command at the client could generate such a trace? Write the whole command.
    c. Can you see the client hostname in the trace? If yes what is it? The server hostname? If yes, what is it?

Ans. The host receiving the file has the IP address 192.168.0.106 and the port is 50718. The other end of the connection has the IP address 128.171.224.109 and the port is 80. We can see this from the TCP(Source Port, Destination Port) and IP headers(Source, Destination) in packet #14.

The number of packets for this connection are 948. We can see this by applying the filter as `ip.addr == 192.168.0.106 && tcp.port == 80 && ip.addr == 128.171.224.109`

a. The server is running on the IP address 128.171.224.109 and port 80. We can see this from packet #14(TCP and IP headers give the destination port and destination IP

address respectively) where the client send the request to the server to GET the pdf. It is a web server since the service being used is HTTP(again can be inferred from the Hypertext Transfer Protocol header present in packet #14)

1.5

b. The client is running on the IP address 192.168.0.106 and the port is 50718. We can see this from packet #14(TCP and IP headers give the destination port and destination IP address respectively) where the client send the request to the server to GET the pdf.
The command used for generating this trace is
`wget http://www.honolulu.hawaii.edu/sites/www2.honolulu.hawaii.edu/files/policies-nondiscrimination.pdf`

2

We can get the Full Request URI from the Hypertext Transfer Protocol header of packet #14.

c. The client's hostname is Sandips-iMac-3 . We can't get the hostname of the server though we have its URI.

0

---

3. Look at packets 5 and 6. What question is Packet 5 asking? What answer did it get in Packet 6?

Ans. Packet 5 is sending an ARP request to find the MAC address linked to the IP 192.168.0.1. "Who has 192.168.0.1? Tell 192.168.0.106"
It gets answer that "192.168.0.1 is at 48:ee:0c:46:ab:2c". Thus it now has the MAC address of 192.168.0.1

1

---

4. Look at packets 7,8,9,10. Describe what they are doing and which is the client, which is the server, and what is this kind of server called.

Ans. The client 192.168.0.106 is asking for the A and AAAA DNS records from the server 192.168.0.1 for the url www.honolulu.hawaii.edu in packet #7 and #8 respectively. In packet #9 and #10, the server replies with the answers. This kind of server is called Domain Name Server. We know that 192.168.0.106 is the client since that is the one initiating the query.

2

5. For packet number 14 (which is of Connection X), answer the following questions.
   a. The headers of which layers can you see clearly? Write 3 header field names and their values for each of the layers that you can see in this packet. E.g. For each layer, you can answer in the following format:
   Layer name:
   Field Name1 = value1
   Field Name2 = value2
   Field Name3 = value3
   b. The packet number 14 is going from which host (IP addr) to which host (IP addr)?
   c. The packet number 14 is going from which network interface (MAC address) to which network interface (MAC addr)?

Ans. a. Application Layer
User-Agent: Wget/1.17.1 (linux-gnu)\r\n
Accept-Encoding: identity\r\n
Connection: Keep-Alive\r\n

Transport layer:
Source Port: 50718
Destination Port: 80
Header Length: 32 bytes

Network Layer”
Time to live: 64
Source: 192.168.0.106
Destination: 128.171.224.109
Link Layer
Destination: 192.168.0.1 (48:ee:0c:46:ab:2c)
Source: IntelCor_9d:a9:cc (cc:3d:82:9d:a9:cc)
Type: IPv4 (0x0800)

2.4

b. Packet 14 goes from 192.168.0.106 to 128.171.224.109.

1

c. Packet 14 goes from cc:3d:82:9d:a9:cc to 48:ee:0c:46:ab:2c

1

---

6. Using information in packet numbers 5,6 and 14 (and answers to above questions) can you infer whether there is a direct link between the two end-hosts of Connection X. Justify your answer. Do not use any reasoning other than what is evident in these packets.
    a. If there is no direct link, what is the IP address and MAC address of the next hop from the client?

Ans. From packet #6 we can see that 192.168.0.1 has the MAC address 48:ee:0c:46:ab:2c. From packet #14 we see that the next hop is 48:ee:0c:46:ab:2c which is not the end-host. So there is no direct link.

a. Mac address of the next hop is 48:ee:0c:46:ab:2c as we can see from the Link layer header of packet #14. The IP address linked to it is 192.168.0.1 which we can see by reverse mapping using packet #6

3

Section-2: *The following questions need you to look at timestamps and do some calculations. You are advised to use a spreadsheet (e.g. Libreoffice calc) for all these otherwise the calculations will take time, and will have to be repeated. Also, it might be a good idea to filter the trace on the server IP address.*

Q

7. Find packet pairs in the setup and tear down of Connection X that represent roundtrips from the client to server to client. Find 3 such packet pairs. Write the packet number pairs.

a. Calculate the RTT (roundtrip) you are getting from each of these 3 (write which packet pair gives which time). Write the min, max and average.

Ans. 1. (11,12) – 2.632139 – 2.222949 = 0.40919 sec
(12,13) -
(970,971) - 16.967975 – 16.560798 = 0.407177

Min = 0.407177 s
Max = 0.40919 s
Avg. = 0.4081835s

2

8. Now look at packets from the server to client in packet number range 18 to 32. How many packets came **to** the client **from** the server in this range?
9. What is the interarrival time of packets coming **to** the client **from** the server? Write all the times, the average, min and max.

Ans.

0.000038
0.008825
0.00019
0.002674
0.000041
0.001798
0.00004

Max = 0.427991, Min = 0.000038, Average = 0.001943714

- interarrival times obtained by subtracting the time stamps of the consecutive received packets. Packets received were 18,20,22,24,26,28,30,32

2.5

Section-3: Now observe packets 32 onwards

Q

10. Packet numbers 32 and 34 are sequential arrivals to the client. What is their interarrival time?
    a. What inference can you make from this and the interarrival time of packets 18 to 32? Specifically, do you think the server is using stop and wait protocol to send its data? (You may assume that RTT from server-client-server will have a similar value to client-server-client RTT). If not, what might be the window size (in units of packets). Justify your inference.
    b. How much data in bytes do you think the server sent without waiting for an acknowledgement? (Hint: for this you can use the TCP sequence number seen in the packets. TCP numbers its packet sequence numbers in units of bytes. E.g. The first data packet has sequence number 1. Now, if Packet P_k has Sequence number S_k (bytes) and size L bytes, the next packet P(k+1) will have Sequence number S_k +L bytes.

Ans. Interarrival time – (time stamp 43 – time stamp 32) 0.427991 sec

a. No the server is not using stop and wait protocol. We can say this because the packets in 18 to 32 came in quick succession but packet 34 came late. First window ended at packet #32. The window size is probably 8 packets since 8 packets(sent together in the first window) were received in quick succession b/w packets 18-32.

4.5

b. Packet #32. TCP headers. The data sent till now equals the sequence number of the upcoming packet(#34 – Field Next Sequence Number - 12843 bytes.

0.5 – forgot to subtract seq number of window start (=1)

11. Find series of packets with the same arrival pattern as packets 18 to 34. Find three more such series. Using TCP sequence numbers, figure out how much data the sender is sending (essentially its window size in bytes) without waiting for an ack. Fill in the following table:
    Packet series start packet number| series end packet number | Window size in bytes.
    What inference can you draw from this table about the window size (in bytes) the sender is using?

Ans.

a. 34 | 52 | 36963-12843 = 24120
b. 52 | 64 | 74611 – 36963 = 37648
c. 64 | 76 | 115155 - 74611= 40544
d. 76 | 88 | 155699 - 115155= 40544

The sender is increasing the window size till 40544 bytes.

5.5 – window size changes, increases further later

---

12. What is the “raw” throughput achieved in this connection? (Raw throughput can be calculated e.g. by bytes sent in packets 18-32 and time in which they were received).

Ans.

12843 - 307(sequence number on 34 – sequence number on 20) / 3.023480 – 3.009874(time stamp 32 – time stamp 18) = 921358.224312803 bytes/sec

0.5 – same window size in bytes that you calculated above

13. What is the latency from the connection setup request by the client (“SYN”), to getting the first packet of the file?

Ans. 3.009874 – 2.222949 (time stamp #18 - #11) = 0.786925s

1

14. What is the latency from the connection setup request by the client (“SYN”), to getting the last packet of the file?

Ans. (time stamp #968 - #11) = 16.559410 – 2.222949 = 14.336461 sec

1

15. What is the effective throughput of the whole connection? [Data received / (Receiving time of Last packet of file - connection setup request time)]

Ans. According to the formula given,

Data received = size of pdf file = 2560032 bytes
effective througput = 2560032/14.336461 = 178567.918540008 bytes/s

1

16. What do you think is dominating the latency? (slow data rate of some bottleneck link? Or large Round Trip Time? Justify your answer.)

Ans. The large round trip time. This is because even the syn-ack response time was large. If it had been a bottleneck, time would have been lesser since syn ack packets are very small.

2.5 – try to give numbers when you make such comparisons