Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Lab Exercise 05 – Using Wireshark to Examine the Transport Layer

Objectives

Part 1: Use Wireshark to familiarize yourself with the TCP Protocol.

Part 2: Use Wireshark to familiarize yourself with the UDP Protocol.

Background / Scenario

To complete this Lab Exercise you must download the sample Wireshark Capture files from Blackboard. The filenames are `http_witp_jpegs.cap` and `dns.cap`. For your reference, these are sample capture files provided through the Wireshark Wiki: https://wiki.wireshark.org/SampleCaptures where many more interesting sample capture files are available.

These sample captures will illustrate the functionality of the Transport Layer and how the information in the header is used to move information between the Application Layer and the lower layers of the OSI Model.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access with Wireshark installed)
- Sample Capture Files.

Part 1: The TCP Protocol

In Part 1, you will examine the header fields and content in a TCP Segment (A Layer 4 PDU is called a segment). A Wireshark capture will be used to examine the contents in those fields.

The contents of this file have been captured using Wireshark running on the client PC. The network traffic has been filtered so that it only contains the one type of traffic we want to inspect.

Step 1: Open the capture file `http_witp_jpegs.cap` in Wireshark

The screen is split in 3. We will focus on the top section (it should be colour-coded right now). Using your knowledge of the Transport Layer and with reference to this capture file, answer the following questions.

Using the Numbering on the left side, which segments contain the three-way handshake (only refer to the first time you encounter the three-way handshake)?

```
1    0.000000 10.1.1.101       10.1.1.1 TCP      62       3177 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1

2    0.000651 10.1.1.1 10.1.1.101       TCP      62       80 → 3177 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
SACK_PERM=1

3    0.000697 10.1.1.101       10.1.1.1 TCP      54       3177 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
```

What is/are the source port(s) (list all that you find)?

1. 80
2. 3177
3. 3179
4. 3183
5. 3184
6. 3185

7. 3187
8. 3188
9. 3189
10. 3190
11. 3191
12. 3192
13. 3193
14. 3194
15. 3195
16. 3196
17. 3197
18. 3198
19. 3199
20. 3200

What is/are the destination port(s) (list all that you find)? Which one appears most frequently?

1. 80

Port 80 appears to be the most frequent

What Application Layer protocol is associated with the most frequent destination port number (the official list of port numbers is here https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt)?

HTTP

What RFC(s) is/are associated with this Application Layer Protocol (there are several RFCs that apply here, list one)?

RFC 7325

Step 2: **From the Statistics Menu, select Conversations. When the Conversations window opens, select the TCP Tab.**

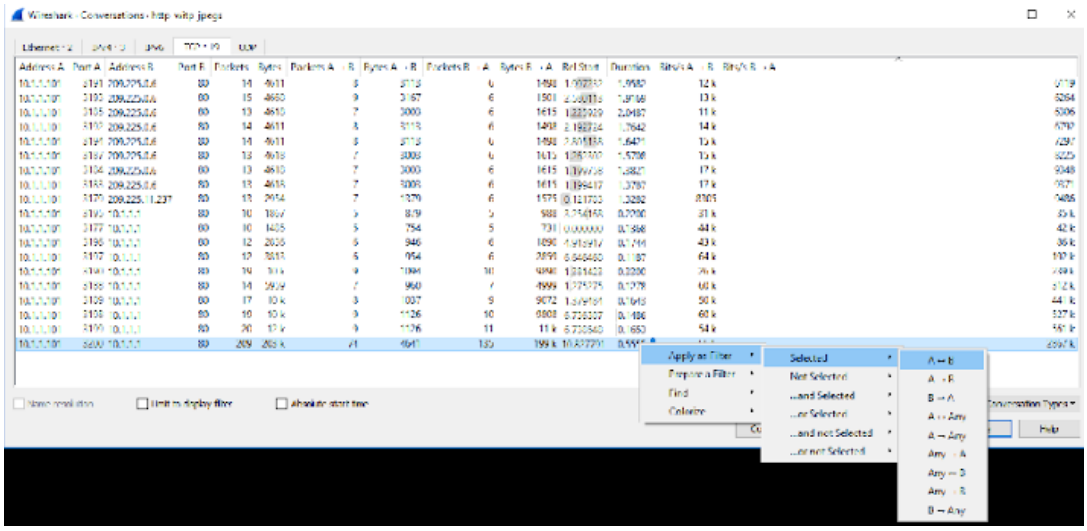
How many Transport Layer Conversations/Sessions are there? 19

The information in this view can be sorted by clicking on the column header. Try clicking on the headers (Address A, Port A, Address B, Port B, etc.) to see how this works.

Which computer, Address A or Address B, do you think is the client? Address A

How Many different Servers is this client connecting to? 3

Click on the Column Header “Bits/s B -> A”, the largest value at the bottom (or top, depending on your sort direction) should be 2867k. Click somewhere on this line so that the entire line is highlighted. Right-click on this line and select “Apply As Filter” from the menu. Then select “Selected” and “A<->B” from the sub-menus. It should look like this:



When you have selected “A<->B”, click Close to close the Conversations Window. You should be back at the main Wireshark screen with only the Filtered conversation displayed. The numbers on the left side should start at 275 and end at 483.

The displayed traffic represents a single complete TCP “conversation” between two hosts: a client and a server. Note the three-way handshake before any application data is exchanged.

What is the source port for this conversation? 3200

What is the destination port for this conversation? 80

What is being requested by the client? an image (GET /Websidan/2004-07-SeaWorld/fullsize/DSC07858.JPG)

Reflection Question (no wrong answer, give it your best shot): Was the request successfully fulfilled? How might we know, based on this trace, if a problem has occurred?

The request was fulfilled as we see in row 479: a 200 (All OK) http status is returned by the server with the image in the response payload. We can easily know if a problem has occurred by looking at the http status code.

Part 2: The UDP Protocol

In Part 2, you will examine the header fields and content in a UDP Segment (recall that a Layer 4 PDU is called a segment). A Wireshark capture will be used to examine the contents in those fields.

The contents of this file have been captured using Wireshark running on the client PC. The network traffic has been filtered so that it only contains the one type of traffic we want to inspect.

Step 1: Open the capture file `dns.cap` in Wireshark.

The screen is split in 3. We will focus on the top section (it should be colour-coded right now). Using your knowledge of the Transport Layer and with reference to this capture file, answer the following questions.

How do we begin communication between a client and a server when we use UDP?

The communication begins when the client sends a datagram to the server.

What is/are the source port(s) (list all that you find)?

1. 32795
2. 32796
3. 32797

What is/are the destination port(s) (list all that you find)? Which appears most frequently?

1. 53

Port 53 appears to be the most frequent

What Application Layer protocol is associated with the most frequent destination port number? DNS

What RFC(s) is/are associated with this Application Layer Protocol? RFC 1034

Step 2: **From the Statistics Menu, select Conversations. When the Conversations window opens, select the UDP Tab.**

How many Transport Layer Conversations/Sessions are there? 8

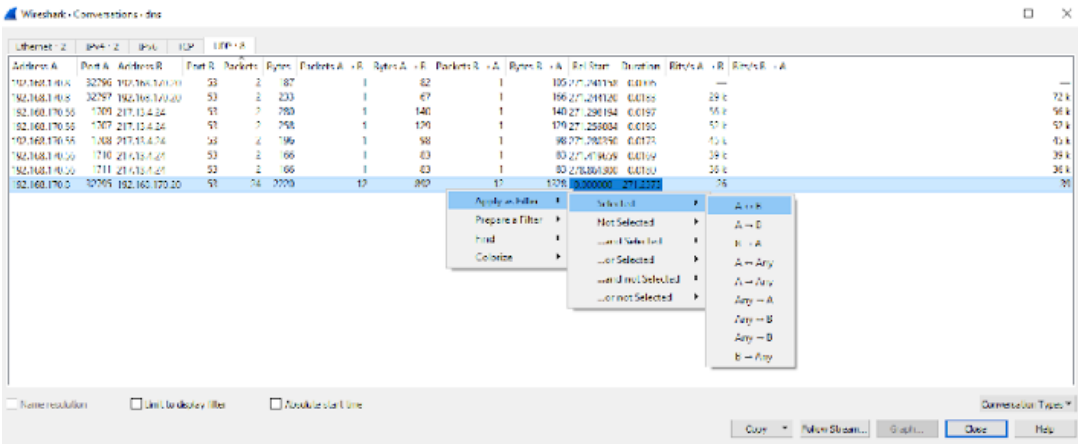
In the context of UDP, what does a “session” mean (remember, UDP does not build a session before communicating, so what do these rows represent)? Conversations in the form of datagrams sent by the client to the server and vice-versa

Which computer, Address A or Address B, do you think is the client? Address A

How many different client addresses are there in this capture? 2

How many different server addresses are there in this capture? 2

Click on the Column Header “Packets”, the largest value at the bottom (or top, depending on your sort direction) should be 24. Click somewhere on this line so that the entire line is highlighted. Right-click on this line and select “Apply As Filter” from the menu. Then select “Selected” and “A<->B” from the sub-menus. It should look like this:



When you have selected “A<->B”, click Close to close the Conversations Window. You should be back at the main Wireshark screen with only the Filtered conversation displayed. The numbers on the left side should start at 1 and end at 24.

What is the source port for this conversation? 32795

What is the destination port for this conversation? 53

Although UDP does not establish a session and maintain a connection like TCP does, we view this as a "conversation" in Wireshark because the application is using consistent source and destination numbers. How might this be useful when managing or troubleshooting the application or our network connectivity?

Helps narrow down the issue to either the client or the server helping identify the source of the issue.

Reflection Question (no wrong answer, give it your best shot): What other information available in this view might be useful for managing or troubleshooting applications?

The time column can help identify bottlenecks in the network probably

Reflection

The middle section of the three sections in Wireshark presents an analysis of each protocol layer. Select any row in the top section of wireshark and then view the information at each layer of the OSI model in the middle section. What does this analysis tell you about how the layers of the OSI model inter-relate with each other?

The analysis reveals that despite having specific responsibilities, each layer depends, in one or more capacity, on layers that are immediately on top and bottom of the layer itself.