Lab Assignments for Chapter 24

We have created two lab assignments for this chapter: Lab24-1 and Lab24-2. We have also included two lab-report sheets, which means that each assignment should be reported in a separate sheet. It is assumed that you have done the lab assignment for Chapter 1, which told you how to install the Wireshark software and how to use it.

24.1 LAB24-1: UDP

In this lab, we use Wireshark to capture and study UDP packets. We find the values of different fields of a UDP user datagram header. Using the values in these fields, we also find all the information about a user datagram and verify that the value in *total length* field matches with the total number of bytes in the user datagram (header and data). We also check to see whether a checksum has been calculated for the packet.

UDP is a connectionless protocol; no connection-establishment and connection-termination packets are issued by UDP. This means that UDP cannot be a source or sink protocol in a captured frame. To analyze UDP headers, we need to use a source or sink protocol at the application layer that uses the services of UDP. DNS is a good candidate. However, as we will learn in Chapter 26, DNS packets can be encapsulated in either UDP or TCP packets (depending on the size). We need to be careful to select only those DNS packets that use the service of UDP.

Since any client-server application program (except DNS itself) uses DNS as the first step, we can open any application to capture DNS packets. We recommend to access your favorite website for this purpose.

24.1.1 Assignment

- Start your web browser and clear the browser's cache memory, but do not access any website yet.
- Open Wireshark and start capturing.
- Go back to your web browser and retrieve any file from a website. Wireshark starts capturing packets.
- After enough packets have been captured, stop Wireshark and save the captured file.

- Using the captured file, select only those DNS packets that use the service of UDP. Type **udp** (lowercase) in the filter field and click **Apply**. The packet list pane of the Wireshark window should now display a bunch of DNS messages. Each DNS message is carried in a UDP packet.

Questions

Using the captured information, answer the following questions in your lab report.

1. In the packet list pane, select the first DNS packet. In the packet detail pane, select the **User Datagram Protocol**. The UDP hexdump will be highlighted in the packet byte lane. Using the hexdump and consulting Figure 24.2 in the textbook, determine
   - a. the source port number.
   - b. the destination port number.
   - c. the total length of the user datagram.
   - d. the length of the data.
   - e. whether the packet is directed from a client to a server or vice versa.
   - f. the application-layer protocol.
   - g. whether a checksum is calculated for this packet or not.
2. Using the information in the packet detail lane, verify your answers you obtained in question 1.
3. What are the source and destination IP addresses in the query message? What are those addresses in the response message? What is the relationship between the two?
4. What are the source and destination port numbers in the query message? What are those addresses in the response message? What is the relationship between the two? Which port number is a well-known port number?
5. What is the length of the first packet? How many bytes of payload are carried by the first packet?
6. In the packet detail pane, select the Domain Name System. The DNS message will be highlighted in the packet byte pane. Count the number of bytes highlighted in the packet byte pane. Does the count agree with the answer to question 5?
7. Is the checksum calculated for the first UDP packet? What is the value of the checksum?

24.1.2 Documents to Turn in

1. A copy of the Lab24-1 report sheet that contains answered questions.
2. A printout of the supporting captured information.

24.2 LAB24-2: TCP

In this lab, we use Wireshark to capture TCP packets to study many features of TCP protocol. Many applications such as HTTP, SMTP, TELNET, and FTP use the service of TCP. For this lab, we use HTTP application to download a rather long file.

The situation of TCP is different from UDP. TCP is a connection-oriented protocol; it uses packets for connection establishment, connection termination, and data transfer. This means that we can capture packets that use TCP as source or sink protocol as well as packets that use an application-layer protocol as the source or sink, but use TCP as the intermediate protocol. In this lab assignment, we capture both types of packets and distinguish between them.

24.2.3 Assignment

- Start your web browser and clear the browser's cache memory, but do not access any website yet.
- Open Wireshark and start capturing.
- Go back to your web browser and retrieve any file from a website. Wireshark starts capturing packets.
- After enough packets have been captured, stop Wireshark and save the captured file.
- Using the captured file, select only those packets that use the service of TCP. For this purpose, type **tcp** (lowercase) in the *filter field* and press **Apply**. The packet list pane of the Wireshark window should now display a bunch of packets.

Part I: Connection-Establishment Phase

Identify the TCP packets used for connection establishment. Note that the last packet used for connection establish may have the application-layer as the source protocol.

Questions

Using the captured information, answer the following question in your lab report about packets used for connection establishment.

1. What are the socket addresses for each packet?
2. What flags are set in each packet?
3. What are the sequence number and acknowledgment number of each packet?
4. What are the window size of each packet?

Part II: Data-Transfer Phase

The data-transfer phase starts with an HTTP GET request message and ends with an HTTP OK message.

Questions

Using the captured information, answer the following question in your lab report about packets used for data transfer.

1. What TCP flags are set in the first data-transfer packet (HTTP GET message)?
2. How many bytes are transmitted in this packet?
3. How often the receiver generates an acknowledgment? To which acknowledgment rule (defined in Page 769 in the textbook) does your answer corresponds to?
4. How many bytes are transmitted in each packet? How are the sequence and acknowledgment numbers related to number of bytes transmitted?
5. What are the original window sizes that are set by the client and the server? Are these numbers expected? How do they change as more segments are received by the client?
6. Explain how the window size is used in flow control?
7. What is purpose of the HTTP OK message in the data transfer phase?

Part III: Connection Termination Phase

The data-transfer phase is followed by the connection termination phase. Note that some packets used in the connection-termination phase may have the source or sink protocol at the application layer. Find the packets used for connection termination.

Questions

Using the captured information, answer the following question in your lab report about packets used for connection termination.

1. How many TCP segments are exchanged for this phase?
2. Which end point started the connection termination phase?
3. What flags are set in each of segments used for connection termination?

Part IV: General

This section relates to all TCP packets.

Questions

From the captured information, answer the following question in your lab report.

1. Using the hexdump and consulting Figure 24.7 in the text, determine the following for any TCP packet:
   a. the source port number.
   b. the destination port number.
   c. the sequence number.
   d. the acknowledgment number.
   e. the header length?
   f. the set flags (you may see two extra flag bits that are shown as reserved ones in the textbook).

   g. the window size.
   h. the urgent pointer value.
2. Using the information in the detail pane lane, verify your answers is question 1.
3. Does any of the TCP packet header carry options? Explain your answer.
4. What is the size of a TCP packet with no options. What is the size of a TCP packet with options?
5. Is window size in any of the TCP packet zero? Explain your answer.

24.2.4 Documents to Turn in

1. A copy of the Lab24-2 report sheet that contains answered questions.
2. A printout of the supporting captured information.