WireShark Lab

PREPARED BY: ER. SHARAT MAHARJAN

Latest version of Wireshark can be downloaded at no cost from the link

https://www.wireshark.org/download.html

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface

Test Run Do the following steps:

1. Start up the Wireshark program (select an interface and press start to capture packets).
2. Start up your favorite browser.
3. In your browser, go to Prime College homepage by typing www.primecollege.com.
4. After your browser has displayed the http://www.primecollege.com page, stop Wireshark packet capture by selecting stop in the Wireshark capture window.
5. Color Coding: You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

6. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the HTTP messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we have to use the filtering functionality of Wireshark by typing “http” in the filtering field.
7. To further filter packets in Wireshark, we need to use a more precise filter. By setting the http.host==www.primecollege.com, we are restricting the view to packets that have as an http host the www.primecollege.com website. Notice that we need two equal signs to perform the match “==” not just one.

To View and Analyze Packet Contents:

The captured data interface contains three main sections:

1. The packet list pane (the top section)
2. The packet details pane (the middle section)
3. The packet bytes pane (the bottom section)

1. Packet list:

It shows all packets found in the active capture file.

- **No.**: This field indicates which packets are part of the same conversation.
- **Time**: The timestamp of when the packet was captured is displayed in this column.
- **Source**: This column contains the address where the packet originated.
- **Destination**: This column contains the address that the packet is being sent to.
- **Protocol**: The packet's protocol name, such as TCP, can be found in this column.
- **Length**: The packet length, in bytes, is displayed in this column.
- **Info**: Additional details about the packet are presented here.

2. Packet details:

The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.

3. Packet bytes:

At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that can’t be printed are represented by a period.

To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.

THANK YOU!!!