
Packet Analysis with Wireshark

A. Using Wireshark to Capture Packets

A.1 Introduction

Wireshark is a protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. It allows the user to see all traffic being passed over the network by putting the network card into promiscuous mode. (from wikipedia.org)

A.2 Capturing Packets with Wireshark

In this exercise, you will learn how to capture and analyze packets using Wireshark. You need two computers, PCa and PCb. **Perform the following steps only in PCa** and do not use PCb at this moment.

- 1) Open **Internet Explorer** and minimize it. Do not close it, you will use Internet Explorer in this exercise.
- 2) Find **Wireshark** icon on the Desktop and double-click it to start **Wireshark**.
- 3) From the **Capture** menu, select **Interfaces**.
- 4) Click on **Start** for **VMware Accelerated ADM PCNET Adaptor**
- 5) You will connect to PCb's website to create network traffic. In the Internet Explorer URL window, type "**http://192.168.1.102**" and press **Enter**.
- 6) Stop capturing packets as soon as possible. Go back to Wireshark, and from the **Capture** menu, select **Stop** to stop capturing packets. Then, look at the content of the captured packets.

Review Questions:

- In the Wireshark menu, select **Analyze**, and then select **Display Filters**. In the filter windows, find **No ARP**, and click on it and then click **Apply**. This way you will filter out all ARP packets. In the packet headers window click + to expand the content of individual header (see the picture below) and fill the following table.

Packet	Source IP	Source Port	Destination IP	Protocol	TCP Flag	Sequence

The screenshot shows the Wireshark interface. The packet list pane at the top shows several packets. A blue arrow labeled "Packet" points to the first packet in the list. The packet details pane below shows the expanded headers for a selected packet. Blue arrows labeled "IP Header", "TCP Header", and "TCP Flags" point to the corresponding sections in the details pane. A blue box labeled "Click+ to expand headers" is positioned near the bottom of the details pane. The packet list shows the following entries:

Source	Destination	Protocol	Info
vmware_99:00:e4	vmware_99:39:78	ARP	192.168.1.102 is at 00:50:56:99:00:e4
192.168.1.101	192.168.1.102	TCP	ff-annunc > http [SYN, ACK] Seq=0 win=65535
192.168.1.102	192.168.1.101	TCP	http > ff-annunc [SYN, ACK] Seq=0 Ack=1
192.168.1.101	192.168.1.102	TCP	ff-annunc > http [ACK] Seq=1 Ack=1 win=0
192.168.1.101	192.168.1.102	HTTP	GET / HTTP/1.1
192.168.1.102	192.168.1.101	HTTP	HTTP/1.1 200 OK (text/html)
192.168.1.101	192.168.1.102	TCP	ff-annunc > http [ACK] Seq=286 Ack=34

The packet details pane for the selected packet (Frame 3) shows:

- Ethernet II, Src: vmware_99:39:78 (00:50:56:99:39:78), Dst: vmware_99:0b:e4 (00:50:56:99:0b:e4)
- Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 192.168.1.102 (192.168.1.102)
- Transmission Control Protocol, Src Port: ff-annunc (1089), Dst Port: http (80), Seq: 0, Len: 28
 - Source port: ff-annunc (1089)
 - Destination port: http (80)
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x02 (SYN)
 - Window size: 65535
 - Checksum: 0x088a [correct]

- Find the first HTTP protocol from 192.168.1.102 to 192.168.1.101. This packet's payload should be the content of the website. Can you see the content of the website?