


Baby Shark

Goal

Welcome to our first Wireshark  exercise! We'll get familiar with the basic functionality and see some interesting stuff in the packets. Good luck!


Background

Wireshark is a packet analyzer. It captures traffic from our network interface and displays it. It's *a lot* of data, so our main challenge is finding just the interesting stuff. You are always welcome to use our filters cheat-sheet at all times (filters-cheatsheet.pdf can be found under this topic attachments).

Let's go!

Steps

Step 1 - Capturing

1. Open Wireshark. In the opening screen, look at the network interfaces' "heart-beat" and examine which one is the active one.
2. Start a new capture by double-clicking the active interface.
3. Go to <http://www.example.com>.
4. Stop the capturing (with the red stop button ) as fast as possible - A smaller capture means smaller haystack to go through :)
 - Wasn't very fast? Don't worry, you can start a new capture and do everything again. Just click on the blue shark button (top-left).

Step 2 - Basic filtering

5. How many packets were captured overall? (Hint: bottom of screen)
6. Use a filter to display only HTTP packets. Write your filter in your answers.
7. How many packets are displayed now?
8. Clear the filter, and now write a new filter to display only *outgoing* packets. Write your filter in your answers.
9. Now write a new filter to display only *outgoing HTTP* packets. Write your filter in your answers.

Step 3 - Looking for data

10. Use *Follow TCP Stream* option to see the full conversation between the client and the server. How many messages did each one of them send?
11. Look closely at the headers of the server's responses. Can you find out the server type and version?

To submit

- A text file containing your answers for:
 - Answers for Part 5 to 9 of **Step 2**
 - Answers for Part 10 to 11 of **Step 3**

