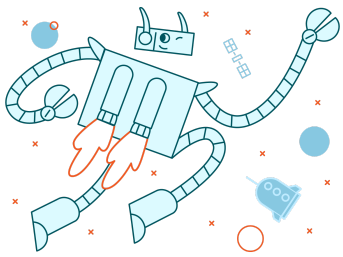
Ping & Shark



Goal

In this exercise we'll look at how Ping packets actually look like, in the wires.

Background

You already know of the cmd tool `ping`. What you don't know, is that ping is a part of a protocol called **ICMP**. It's a protocol that includes all kind of diagnostic messages, being used mostly by network IT people and routers. A ping request is called an **Echo Request**, and the response called an **Echo Reply**.

Step 1 - Capturing

1. Check your current IP and write it down.
2. Open Wireshark and a CMD window.
3. Start a new capture.
4. Now we'll try something cool - setting a display filter **at the start** of capture. Use the filter `ICMP` to see the ping traffic. It will be empty right now, that's fine.
5. Run 3 pings
    - to wikipedia.org
    - to 8.8.8.8
    - to 51.51.51.51
6. See the packets piling up in Wireshark? Without tons of irrelevant data? Sweet! 😎
7. Stop the capture.

Step 2 - Analyzing the packets

7. 📝 How many Echo Requests do you see? How many Echo replies?
8. 📝 What is the IP of wikipedia.org?
9. 📝 How long is the delay between every ping request? (in seconds)?
10. 📝 What happened when we pinged 51.51.51.51?
11. 📝 When a ping is sent, it usually contains a small text message (just to send *something*). What is the text message sent in those pings? (Hint: bottom pane)

To submit

Submit a document with answers for questions marked with 📝.