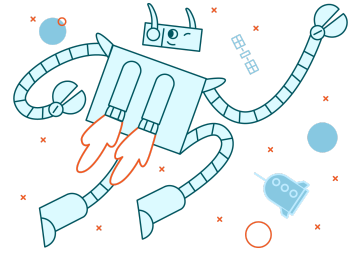# Agent Smith

Goal

Welcome to the User Agent investigation exercise! Today we'll capture HTTP requests in Wireshark, compare the User-Agent strings from a desktop and mobile view, and understand the difference between them.

Background

What is a User-Agent?

A User-Agent is a string sent by a web browser or other client application to identify itself to the server. It provides information about the client's software, operating system, and device, allowing the server to deliver an optimized response.

Why is the user-agent important?

- **Content optimization**: Servers use the User-Agent string to tailor content for different devices and browsers.
- **Analytics**: Helps in gathering data about the types of clients accessing a website.

Prerequisites

Wireshark Tool is needed for this assignment you can learn more about it and download the file here

Even though this exercise uses wireshark, the formal introduction of the tool will only be found in the next topic assignment "baby_shark"

Steps

Step 1 - Capturing on Desktop

1. Open Wireshark.

2. **Start a New Capture**:

   - Double-click the active interface to start capturing.
     - Hint: Look for Descriptive Names: Interfaces with names like "Wi-Fi" for your wireless connections or "Ethernet" for your wired connections.

3. **Browse to Example Website**:

   - Open your web browser and go to `http://www.example.com`.

4. **Stop Capturing**:

   - Stop the capturing in Wireshark using the red stop button 🟥 as soon as the page loads.

5. **Filter HTTP Packets**:

   - Use the filter `http` to display only HTTP packets.

6. **Identify the User-Agent String**:

   - Find the HTTP GET request for `www.example.com`.
   - Look for the User-Agent string in the request headers and copy the entire thing inside your submission text file.

7. **User-Agent Details**:

   - Within the user-agent string, what is the part that identifies your device type? Write the portion that identifies your device type in the same submission text file.

Hint: The User-Agent string typically begins with `Mozilla/5.0`. This originates from the early days of the web when the Netscape Navigator browser identified itself as `Mozilla` to ensure compatibility with web servers that were optimized for it. Modern browsers continue to use `Mozilla/5.0` as a convention for compatibility reasons, even though they are not related to the original Mozilla browser.

Step 2 - Capturing in Mobile Mode

8. **Enable Mobile Mode in Browser Dev Tools**:

   - Open your browser's developer tools (F12 or right-click and select "Inspect").

   - Click on the "Toggle Device Toolbar" (It is a button on the top left of your developer tools.)

     Alternatively, press `Ctrl` + `Shift` + `M`

9. **Start a New Capture in Wireshark on same interface**:

   - Click the blue shark button (top-left) to start a new capture.

10. **Browse to Example Website in Mobile Mode**:

    - With mobile mode enabled, go to `http://www.example.com` again.

11. **Stop Capturing**:

    - Stop the capturing in Wireshark using the red stop button ▮ as soon as the page loads.

12. **Filter HTTP Packets**:

    - Use the filter `http` to display only HTTP packets.

13. **Identify the User-Agent String once again**:

- Find the HTTP GET request for `www.example.com`.
- Look for the User-Agent string in the request headers and copy the entire thing inside your submission text file.

14. **User-Agent Comparison**:

- What are the main differences between this one and the earlier one (captured desktop mode vs mobile mode)?
- Why are they different?. Write all your answers inside the same submission text file.

To Submit

Submit your answers in a text file and upload it.

- User-Agent String for Desktop Mode
- Identification for Device Type
- User-Agent String for Mobile Mode
- Main Differences between the Desktop Mode and Mobile Mode
- Explanation for differences.

Sentinel