Wireshark Guide

This guide shows how to troubleshoot the issues when an application or a domain, and Stats are not working properly.

Installation

Please download and install Wireshark. Choose x32 version, if you don't know the architecture of your operating system:

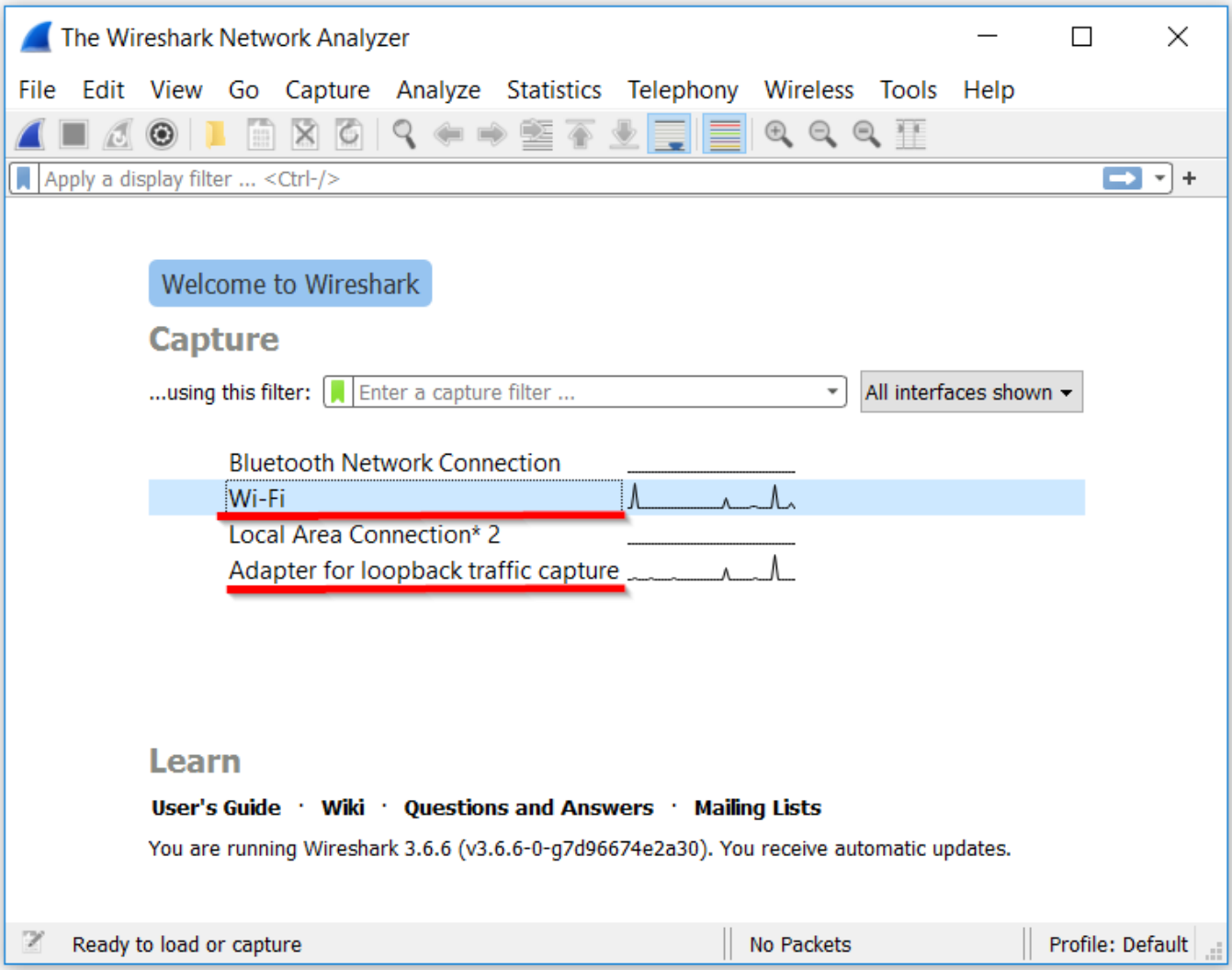
https://www.wireshark.org/download.html

According to Wireshark requirements, you will need to install either WinPcap or Npcap capture driver. Please select the option most suitable for you.

How to use the app

Once Wireshark is installed, the system should be restarted.

Please run the Wireshark application with the administrator rights. During the first run you will be prompted to select the source interface. Please select one of the network adapters:
Adapter for loopback traffic capture – if you are using SafeDNS Agent.
Wi-Fi or Local Area Connection – if the settings are configured on the network level.

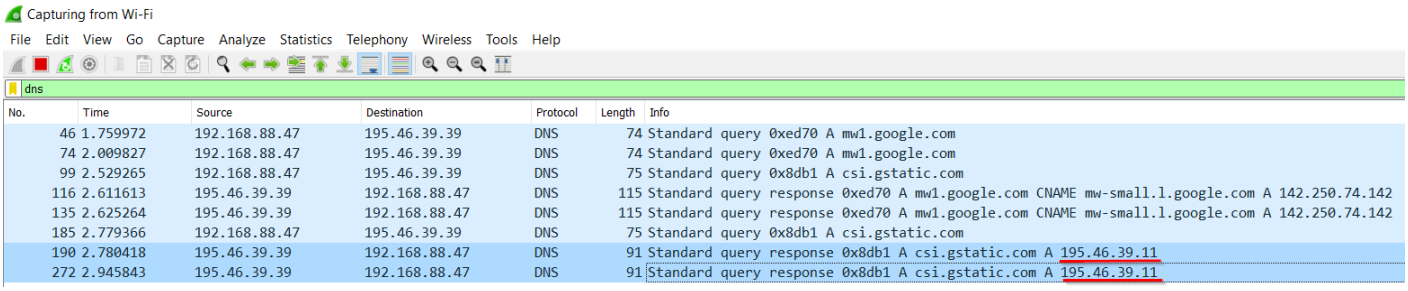


Configure the capture protocol by typing the **dns** in the Display Filter field and press the Enter button.

This step will filter all network requests to show DNS requests only.

Start the application that requires troubleshooting.

The screen of Wireshark shows the list of the hostname addresses, their corresponding IP addresses, and additional service information.



In the example above, the domain csi.gstatic.com was resolved to the IP address 195.46.39.13 - SafeDNS BlockPage address.
This means that the domain csi.gstatic.com is currently blocked either because its category is blocked or because it is on the Denylist.

Please note, that SafeDNS BlockPages can use the following addresses:
195.46.39.1, 195.46.39.2, 195.46.39.3, 195.46.39.11, 195.46.39.12, and 195.46.39.13.

How to solve the issue?

Please look up for the category of the domain with the SafeDNS online tool:

https://www.safedns.com/check-website

After that, check if this category is not blocked in your SafeDNS Dashboard or is not on the Denylist.

Using Wireshark to capture DNS requests is usually enough to solve any issues related to DNS web filtering. However, you can also try advanced Wireshark features - network packet capture, packet analyzer, and USB traffic capture.

Revision #3
Created 11 September 2022 00:40:11
Updated 15 September 2023 21:45:42 by Leo Nagano