**Collect data for protocol reverse engineering**

|  |
| --- |
| **Warning: the process described in this document collect personal data. These data are not kept and are deleted or anonymized after being used by the development team.**  **However, please consider all files containing the collected data as sensitives and treat them with all precaution it requires (do not share to third party, use a secured way to transfer them to development team, and delete them once transferred to development team).** |

# What is this document

This document described how to collect data in order to request a new protocol to be implemented in the tool UniversalScanner.

Please note that we cannot guarantee that your protocol integration requests will be fulfilled, especially if:

* The analysis is too hard, the protocol is ciphered or discovery not done on Layer 3 (IPv4 or IPv6);
* Some information are not provided or missing;
* The device manufacturer is small company with a non-significant number of units sold over the market;
* Lack of time or resource in the development team;
* Any other reason that development team would judge acceptable.

There is no warranty at all about the result.

# What is needed

You will need:

* The device(s) that should be detected powered up and reachable on a network;
* A computer with connected on the same network than the device(s);
* The discovery software tool from the manufacturer of the device(s);
* The software Wireshark.

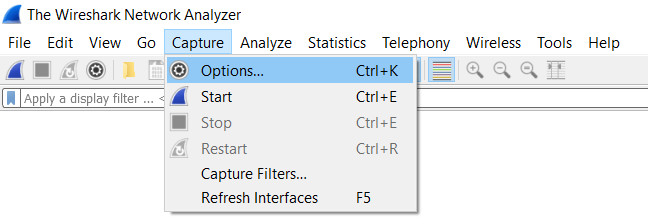
Wireshark can be downloaded here: <https://www.wireshark.org/download.html>

**Important note: Please download setup version, do not choose the portable version to capture as it does not contain the service NPcap which is used to make the capture.**

# How to proceed

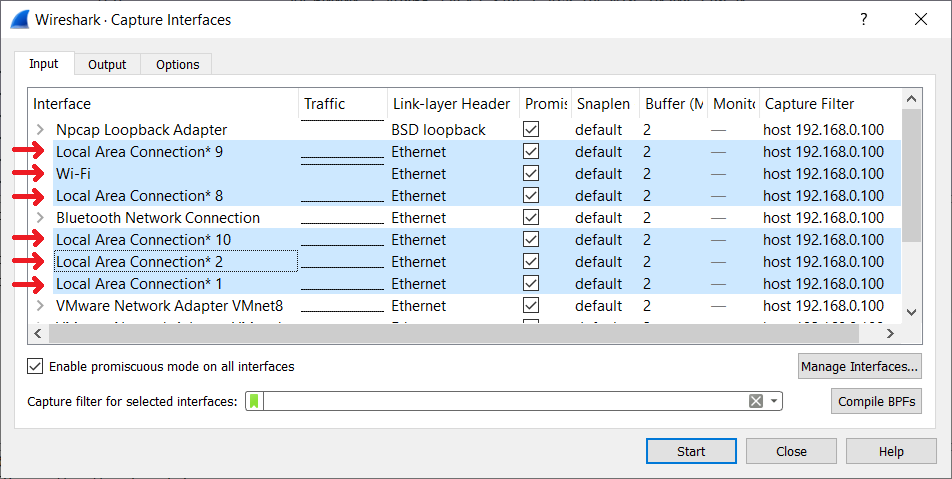
On the computer, close all running programs (especially video recording software, browsers, etc.).

Install and run Wireshark; go in the **Capture** / **Option**:

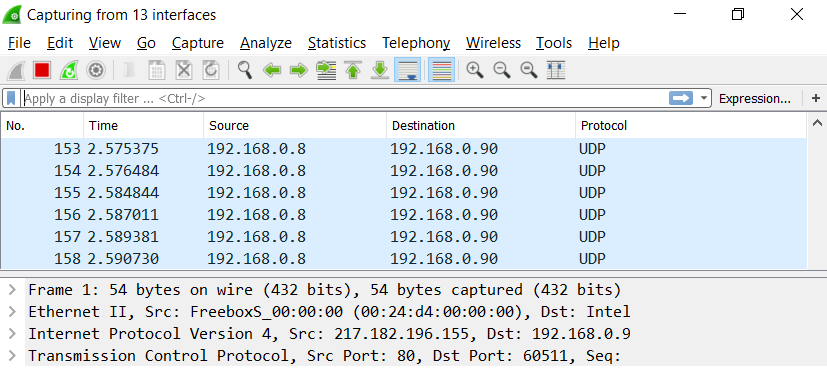


Select the relevant interface(s) on which you would like to make the capture, you can select several by keeping the key Control pressed on your keyboard at same time. Warning, to select the interface, the line must be highlighted in light blue (the checkbox indicates only that we want to listen the foreign traffic).

If you don’t know on which interface to make the capture, select all interfaces.

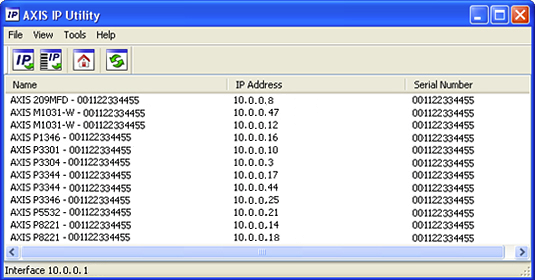


Then click on the button , Wireshark will automatically start the capture in real time.



**Do not close Wireshark**, let the program capturing while we do the discovery query and see response(s).

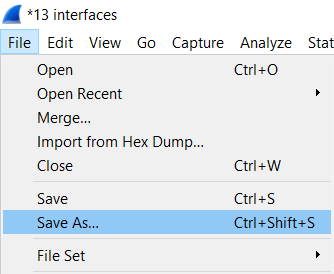
Run the discovery software tool from the manufacturer and perform a discovery query:



Once the discovery is done, go back to Wireshark and stop the capture clicking on the button **.**



Save the Wireshark capture file going into menu **File** / **Save As**.



Make a print screen of the discovery software with the visible results.

# What I should transfer and to whom

You should transfer one archive (zip for example) the following data:

☐ The Wireshark capture file save while discovery is done;

☐ The screenshot of discovery software with the visible results of found devices and details (IP address, serial, etc.);

☐ The discovery program from the manufacturer (download link or included in the archive);

☐ The name of the manufacturer.

You can send results to Julien Blitte via a transfer website (such as Google Drive, WeTransfer, OneDrive, etc.) to this e-mail: julienblittegmailcom

