ESET Tech Center

How to create a Wireshark log

Steef | ESET Nederland - 2020-01-07 - Comments (0) - Diagnostics

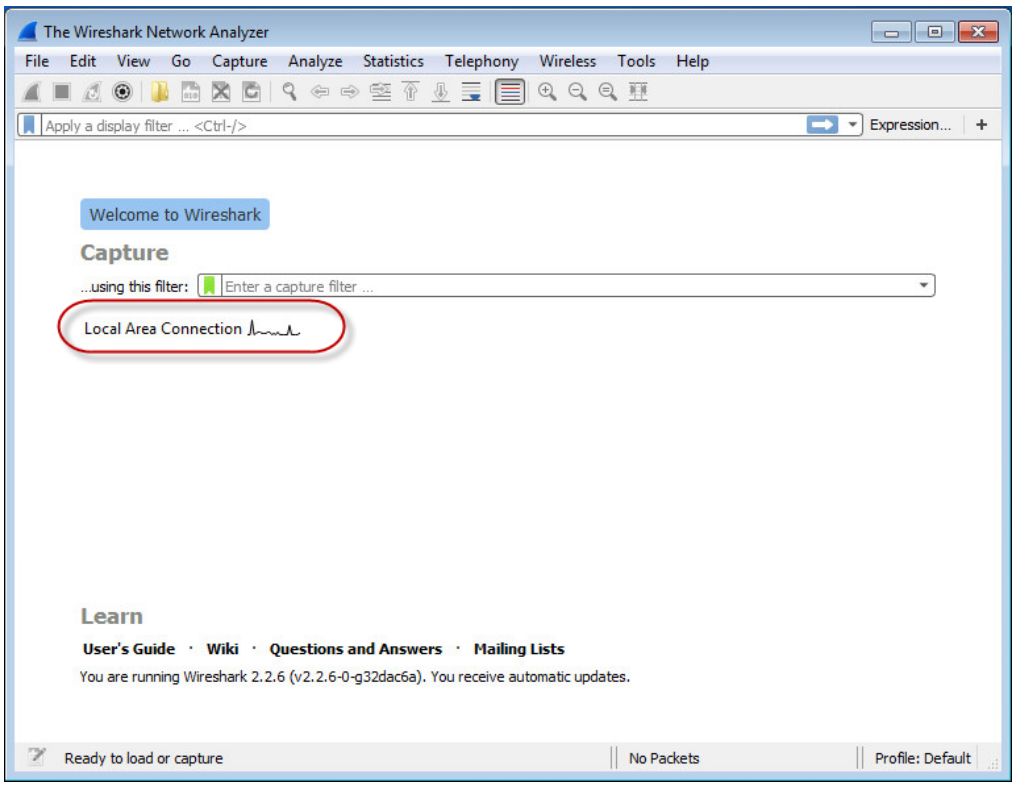
Issue

After contacting ESET support, you might be asked to recreate your problem and provide us with Wireshark log file. To do this, you will need Wireshark software.

> When is Wireshark log file needed?
>
> Wireshark log file is typically required to diagnose network related issues (for example Update, Activation issues, etc.).

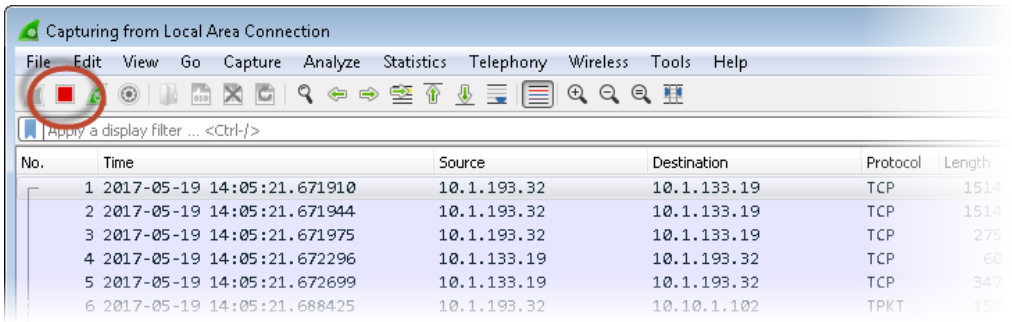
Solution

1. Download Wireshark utility: https://www.wireshark.org/#download
2. When your download is complete, execute the installation file and install the Wireshark (you can use default settings)
3. Run Wireshark utility
4. Double-click on the network adapter that you are using, it will automatically start capturing network traffic



5. Reproduce the problematic issue

6. After issue is reproduced, stop capturing communication by clicking on the red button



7. Click on **File → Save As...** and save the log file in native ***.pcapng** format

Related Content

- Create a full memory dump of a VMware virtual machine
- How do I generate a memory dump manually?
- Run the Info_get.command on a Linux machine and send the logs to ESET Technical Support
- Using tcpdump on a MacOS
- Using Process Monitor to create log files

- Using tcpdump on a Virtual Appliance
- How do I use ESET Log Collector?