Инструкция по работе с WireShark

В этом руководстве показано, как устранять проблемы, когда приложение или домен не работают должным образом и не имеют доступ по сети.

Установка

Загрузите и установите Wireshark. Выберите версию x32, если вы не знаете архитектуру своей операционной системы: https://www.wireshark.org/download.html

Согласно требованиям Wireshark, вам необходимо будет установить драйвер захвата WinPcap или Npcap. Пожалуйста, выберите наиболее подходящий для вас вариант.

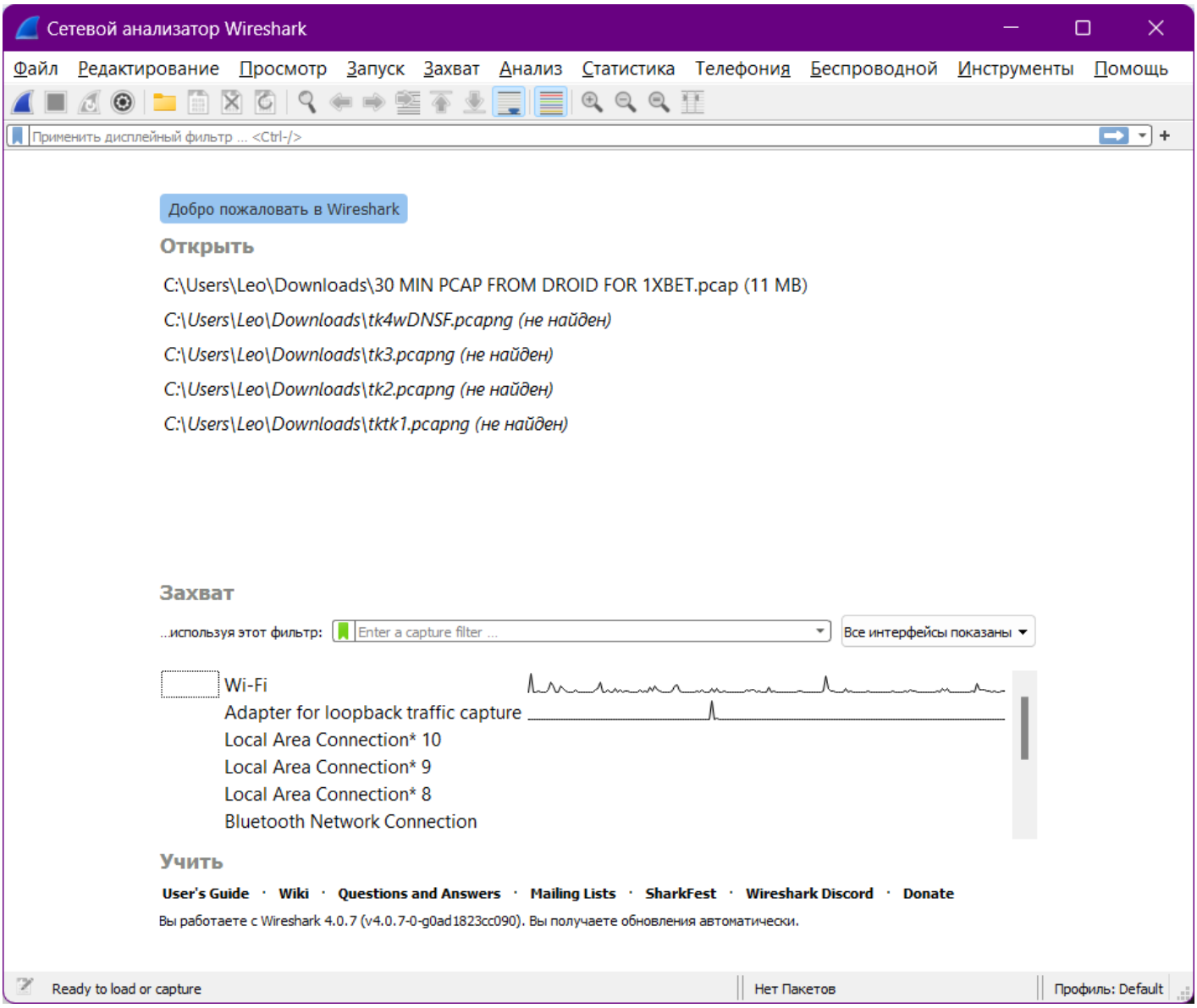
Как использовать приложение

После установки Wireshark систему следует перезагрузить.

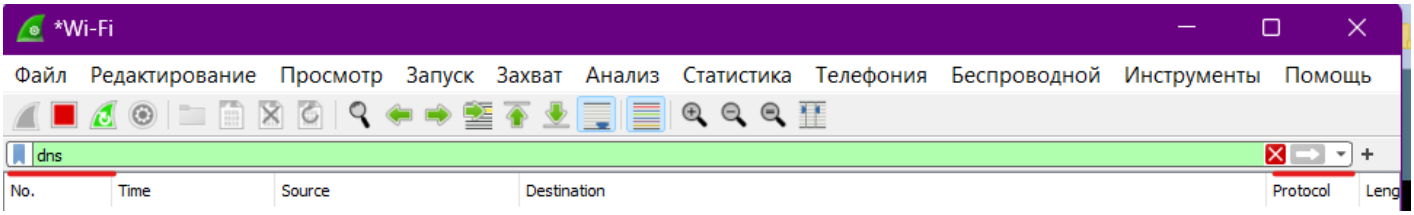
Пожалуйста, запустите приложение Wireshark с правами администратора. При первом запуске вам будет предложено выбрать интерфейс для захвата трафика. Пожалуйста, выберите один из сетевых адаптеров:

Adapter for loopback traffic capture - если вы используете агент SkyDNS.

Wi-Fi или Local Area Connection - если фильтрация настроена на сетевом уровне.



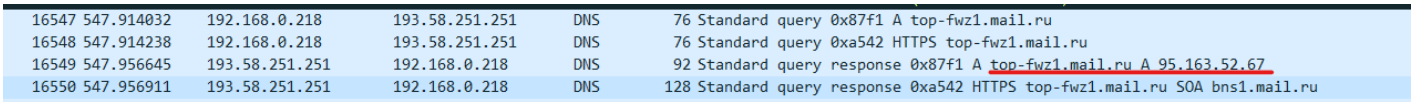
После запуска процесса отслеживания пакетов, настройте протокол захвата, введя DNS в поле **Фильтр отображения** и нажав кнопку **Ввод**.



На этом шаге все сетевые запросы будут фильтроваться, чтобы отображались только DNS-запросы.

Запустите приложение, требующее устранения неполадок.

На экране Wireshark отобразится список адресов имен хостов, соответствующие им IP-адреса и дополнительная служебная информация.



В приведенном выше примере, домен top-fwz1.mail.ru был разрешен в IP-адрес 95.163.52.67 - адрес запрашиваемого ресурса. Это означает, что вышеуказанный домен сервиса Mail.ru успешно резолвится через сервера фильтрации СкайДНС. Если вместо реального адреса запрашиваемого ресурса вы увидите адрес страницы блокировки СкайДНС, это означает что доступ к запрашиваемому ресурсу был заблокирован.

Ниже указаны адреса страниц блокировок СкайДНС:

```
193. 58. 251. 1
193. 58. 251. 2
193. 58. 251. 3
193. 58. 251. 4
193. 58. 251. 12
```

Как решить проблему?

Найдите категорию домена с помощью онлайн-инструмента SkyDNS: https://www.skydns.ru/check/

После этого проверьте, не заблокирована ли эта категория на панели управления SkyDNS или нет ли домена в списке запрещенных.

Использование Wireshark для захвата DNS-запросов обычно достаточно для решения любых проблем, связанных с веб-фильтрацией DNS. Однако вы также можете попробовать расширенные функции Wireshark — захват сетевых пакетов, анализатор пакетов и захват USB-трафика.

Revision #5
Created 13 December 2023 06:56:04 by Leo
Updated 18 July 2025 11:21:20 by Виктор