# Сетевые технологии. Лабораторный практикум

## Требования

* Среда для работы студента.
  + Для ОС Windows потребуются пакеты WinPcap и WinDump.
  + Для ОС Unix потребуется libpcap.
* ПО tcpdump.
* ПО Wireshark.
* Предварительно загруженные экземпляры сетевого трафика.
* Подключение к локальной сети или Internet.

## Блок 1. Захват трафика с интерфейса сетевой карты

В данном блоке предлагается изучить работу ПО tcpdump.

Требуется ознакомиться с возможными командами данного ПО, используя информацию, приведенную в дополнительных материалах (tcpdump.pdf).

Произвести предварительный обзор сетевого трафика. Направить icmp-пакеты в сторону DNS-сервера (8.8.8.8 или 8.8.4.4) или в сторону активного устройства в локальной сети. С помощью фильтра обнаружить данные пакеты.

Произвести запись не менее 1000 сетевых пакетов для последующего анализа (если подключение к локальной сети, то количество сетевых пакетов возможно уменьшить).

## Блок 2. Основы анализа сетевого трафика

В данном блоке предлагается изучить работу ПО Wireshark.

Записанный в блоке 1 сетевой трафик необходимо открыть с помощью ПО Wireshark и визуально изучить отображение в данном интерфейсе.

Изучить возможности отображения информации о фреймах (packets). Рассмотреть отображение заголовков TCP-фрейма с канального уровня по уровень приложения. С помощью механизмов фильтрации отобразить все датафреймы связанные с IP-адресом DNS-сервера или иного устройства, использованного как получатель в блоке 1.

Далее предлагается изучить средства визуализации агрегированной информации по записанной копии сетевого трафика. Для этого можно проследовать по пути: Статистика – Иерархия протоколов. Найти ICMP протокол и применить как фильтр для расследования инцидента.

После этого предлагается просмотреть функционал инструмента по пути: Статистика – Графики ввода/вывода. Будет полезно дополнительно добавить график ошибок TCP, как указано на рисунке Рисунок 1 или иной на усмотрение преподавателя.

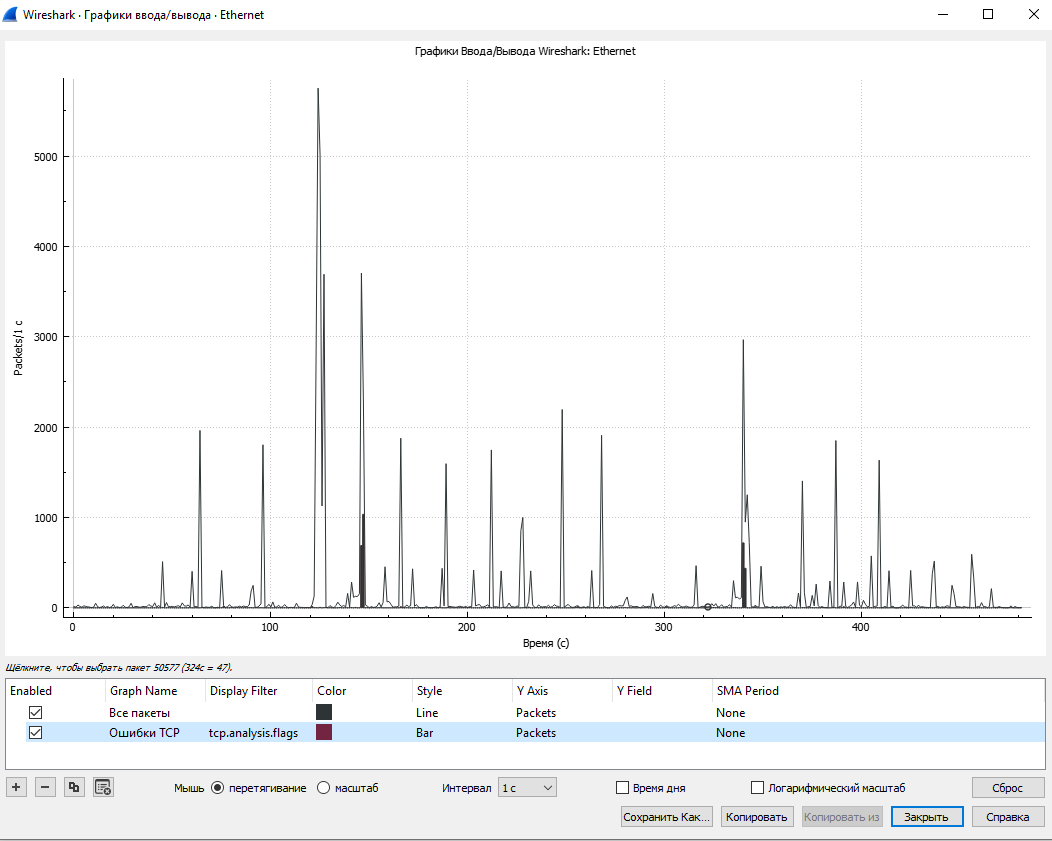


Рисунок 1 – Графики ввода/вывода Wireshark

## Блок 3. Анализ аномального трафика.

В данном блоке предлагается рассмотреть копию сетевого трафика TCP-сессии с потерей сегментов, провести анализ окна масштабирования и выявить переполнение буфера у пользователя, а также неверную настройку ОС (или установленного ПО).

Для работы предложены четыре копии сетевого трафика: SACK, First, Second-Client, Second-Server.

В копии SACK рекомендуется начать анализ с информации эксперта Wireshark, вызов которой приведен на рисунке Рисунок 2.

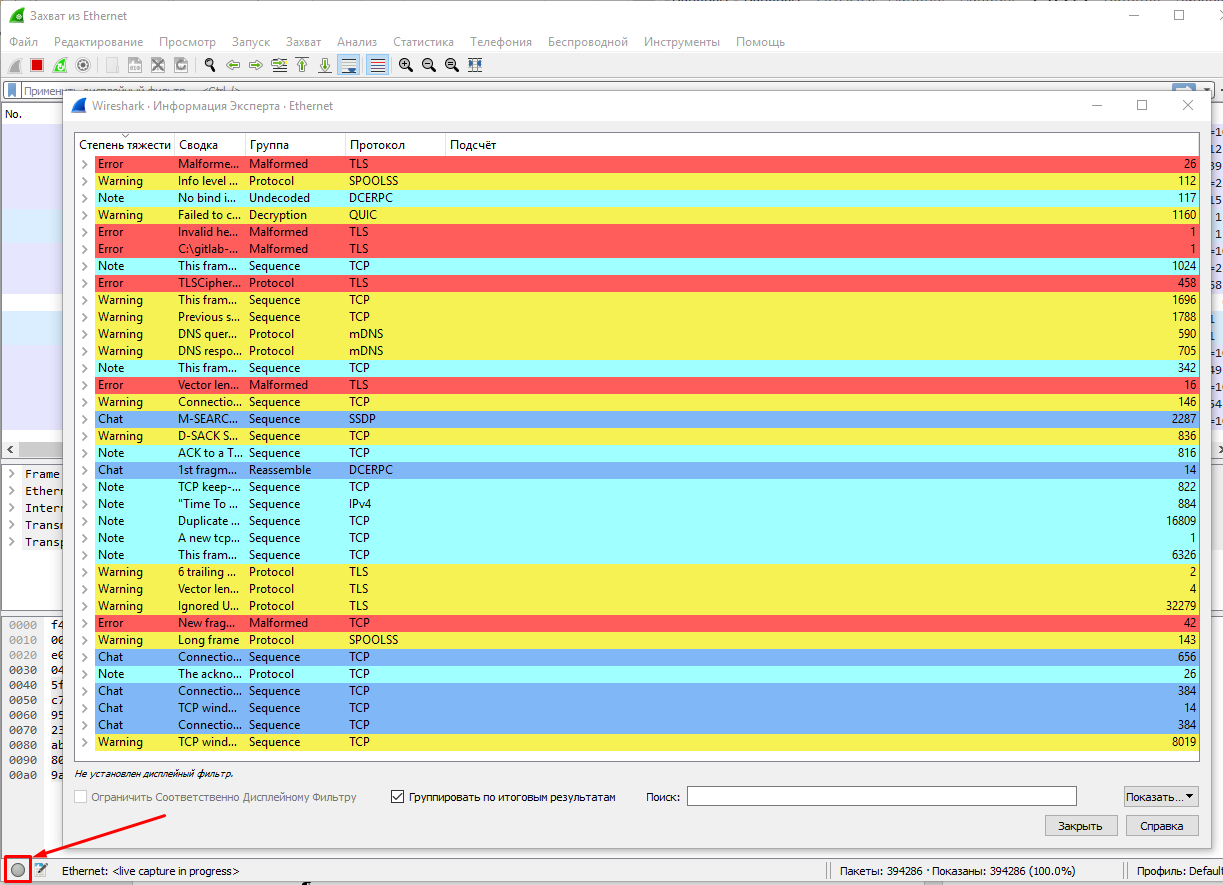


Рисунок 2 – Информация эксперта Wireshark

Далее просмотреть 30 TCP-фрейм, рассказать о потере сегмента, флагах неподтвержденного получения фрейма и опции SACK, которая направляет запрос продублировать сегмент снова.

После этого, предлагается перейти к выявлению переполнения буфера у пользователя путем просмотра информации о копии сетевого трафика под названием First.

После открытия файла необходимо перейти по пути: Статистика – Графики потока TCP – Масштабирование окна. Рассказать о процессе, реакции TCP на проблемы у пользователя.

Для обнаружения неверной настройки ОС (или установленного ПО) необходимо проанализировать сетевой трафик под названием Second-Client и Second-Server.

Первоначально просмотрев Графики потока TCP – Масштабирование окна у клиентской части можем сделать вывод, что трафик передается с маленьким размером окна, хотя ошибок в сессии нет.

Переходим к анализу серверной части. Обнаружим, что пакеты приходили без множителя окна. Видим ошибки c флагом TCP Window Full. Сервер готов отправлять фреймы с большим окном, но в рамках TCP handshake пользователь указал, что не поддерживает размер окна более 14600, причем SACK поддерживается, что является явной ошибкой настройки ОС (или установленного ПО).

## Блок 4. Анализ сетевой атаки.

Предлагается рассмотреть ресурс <https://www.netresec.com/?page=PcapFiles> в части сетевых атак и CTF. На усмотрение преподавателя возможно рассказать сценарий одной из атак и показать на примере копии сетевого трафика.

Каждому студенту необходимо выбрать задачу из предложенных на ресурсе <https://www.malware-traffic-analysis.net/training-exercises.html>.

Требуется просмотреть набор задач, выбрать уникальное (для исключения коллизий можно вести валидацию через преподавателя). После этого, необходимо ознакомиться со сценарием атаки, понять поставленную задачу.

На ресурсе предлагается конечный ответ к каждой задаче. Возможно использовать один из подходов:

* Предоставить студентам ссылку на ресурс и на выходе предложить произвести полное описание хода атаки (времязатратно для приема работ).
* Предварительно загрузить задачи без ответов (Перевод предлагается произвести используя ресурс [https://www.deepl.com](https://www.deepl.com/)). Успешным выполнением блока будет являться верный ответ на задачу.

Дополнительные ресурсы с экземплярами копий сетевого трафика:

* <https://wiki.wireshark.org/SampleCaptures>
* <https://packetlife.net/captures/>