Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Безопасность компьютерных сетей»

Лабораторная работа №4  
«Специальные техники анализа трафика в Wireshark»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Знакомство с интерфейсом приложения 3](file:///D:\Документы\Клоченко\УРФУ\Учеба\3%20kurs\Labs\CNS\Отчеты\Lab_Net_2.docx#_Toc132967636)

[2. Фильтрация пакетов 5](file:///D:\Документы\Клоченко\УРФУ\Учеба\3%20kurs\Labs\CNS\Отчеты\Lab_Net_2.docx#_Toc132967637)

[3. Анализ служебных протоколов 8](file:///D:\Документы\Клоченко\УРФУ\Учеба\3%20kurs\Labs\CNS\Отчеты\Lab_Net_2.docx#_Toc132967638)

[4. Обращение к *web*-сайту 15](file:///D:\Документы\Клоченко\УРФУ\Учеба\3%20kurs\Labs\CNS\Отчеты\Lab_Net_2.docx#_Toc132967639)

[Вывод 20](file:///D:\Документы\Клоченко\УРФУ\Учеба\3%20kurs\Labs\CNS\Отчеты\Lab_Net_2.docx#_Toc132967640)

**Цель работы:**

Знакомство с сетевым анализатором трафика *Wireshark*, изучение приемов анализа трафика.

**Ход работы:**

## Просмотр TLS-трафика

* 1. Откроем браузер FireFox. В консоли выполним команды:
* set SSLKEYLOGFILE=%HOMEDRIVE%%HOMEPATH%\keys.log
* “%ProgramFiles%\Mozilla Firefox\firefox.exe”

Первая строка в файле keys.log:

# SSL/TLS secrets log file, generated by NSS.

* 1. Запустим захват трафика и откроем в FireFox страницу <https://max.zolotyh.su/lab03>. В открывшейся форме введем свой псевдоним в качестве имени пользователя и пароль. Остановим захват трафика. Отфильтруем трафик отправки данных на сайт по его IP-адресу, а затем отобразим содержимое TCP-потока.

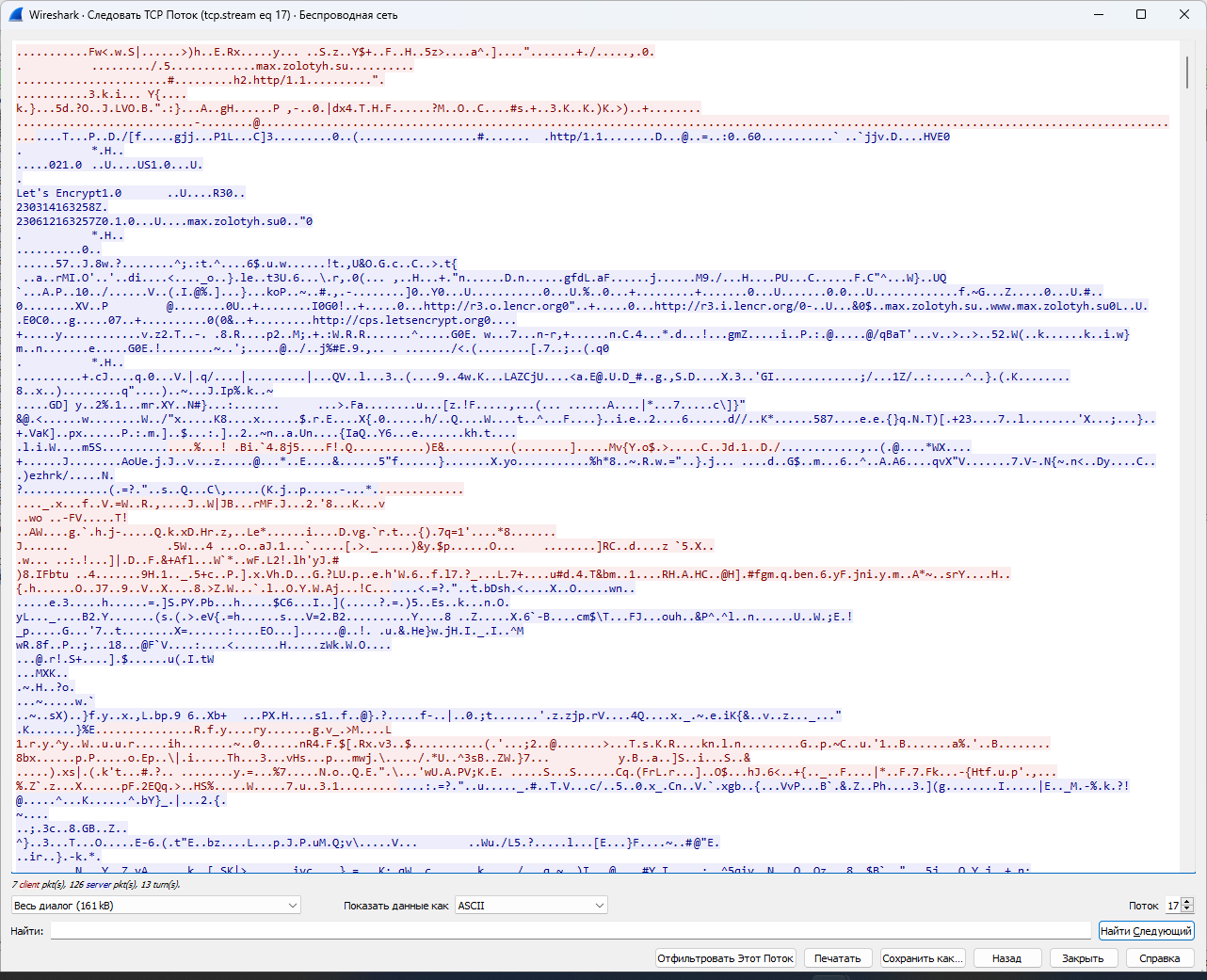


Рисунок 1. Содержимое TCP потока

Передаваемая информация не распознаваема.

* 1. Переходим «Edit – Preferences – Protocols – TLS». В поле «(Pre)-Master-Secret log filename» указываем полный путь к файлу ключей, созданному в п1.1.

Уберем фильтр по TCP потоку и вернем фильтр по IP адресу.

В силу большого количества захваченных пакетов, зафиксируем только первые видимые в списке:

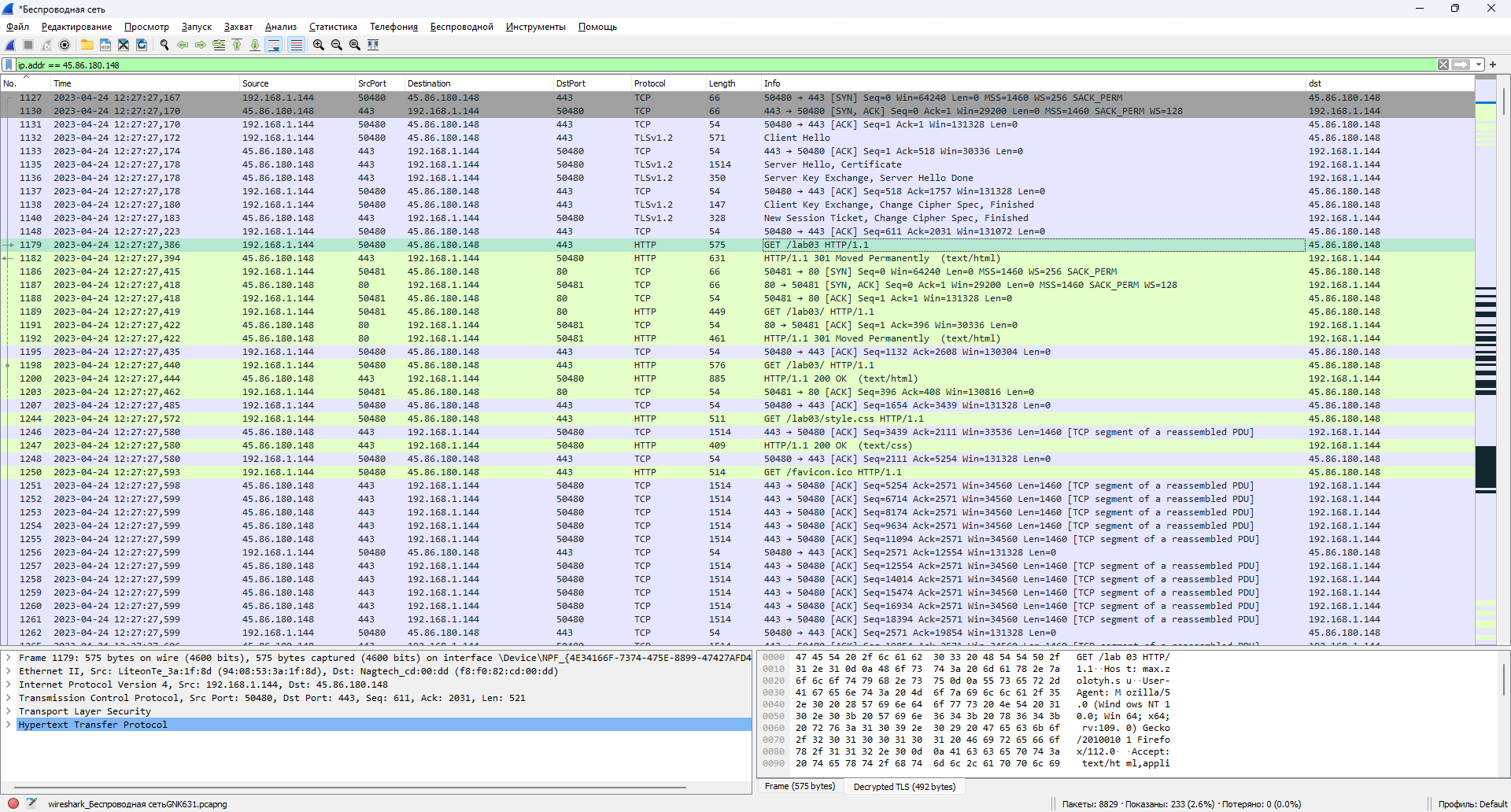


Рисунок 2. Захваченные пакеты

* 1. В списке захваченных пакетов найдем http пакет с POST запросом. Следуем по TLS потоку.

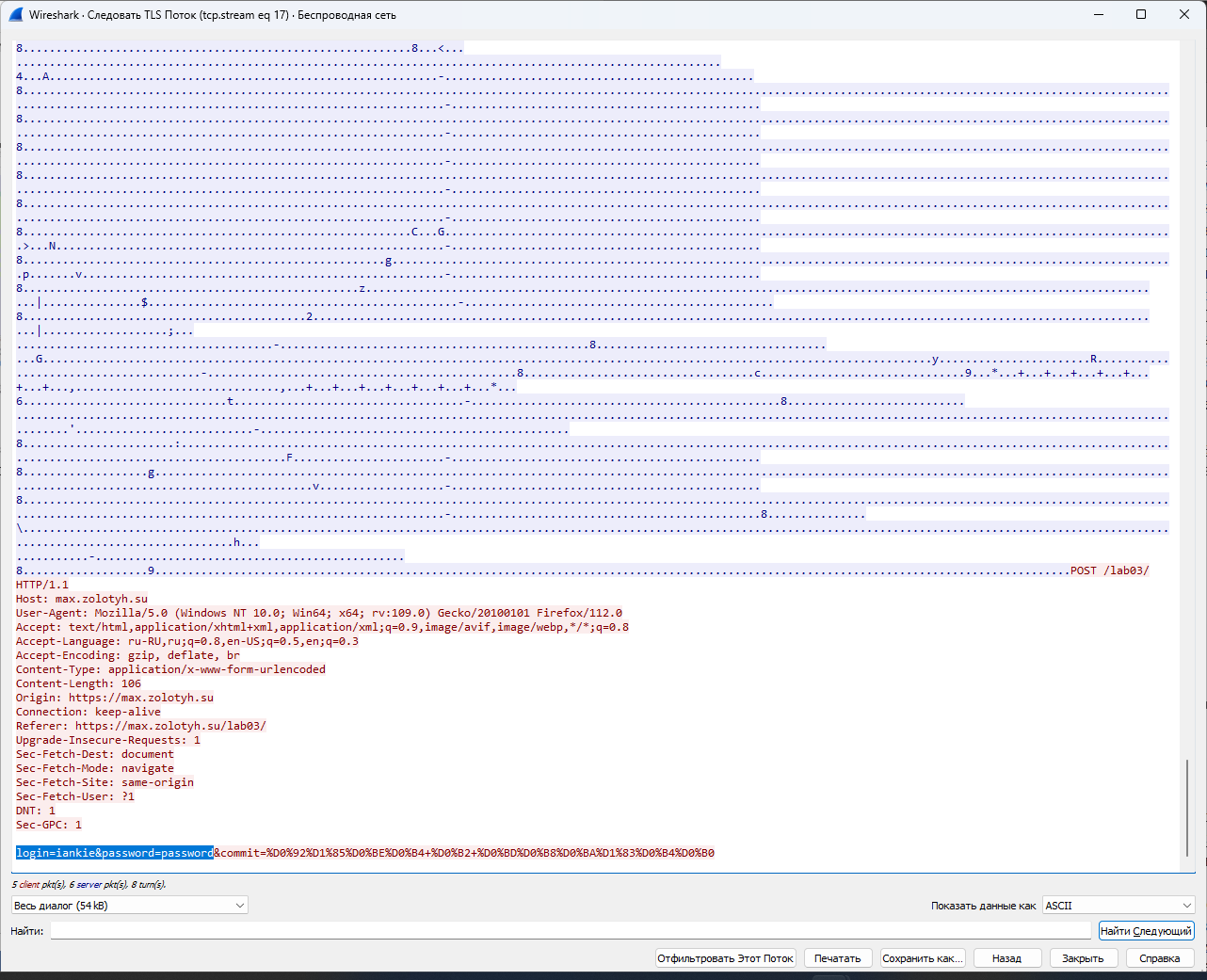


Рисунок 3. TLS поток

## Работа с HTTP2 потоком

* 1. Запустим захват трафика и откроем в FireFox страницу <https://ya.ru>. В поисковой форме введем любую комбинацию из латинских символов и выполняем поиск. Останавливаем захват трафика. Восстанавливаем TLS поток отправки поискового запроса.

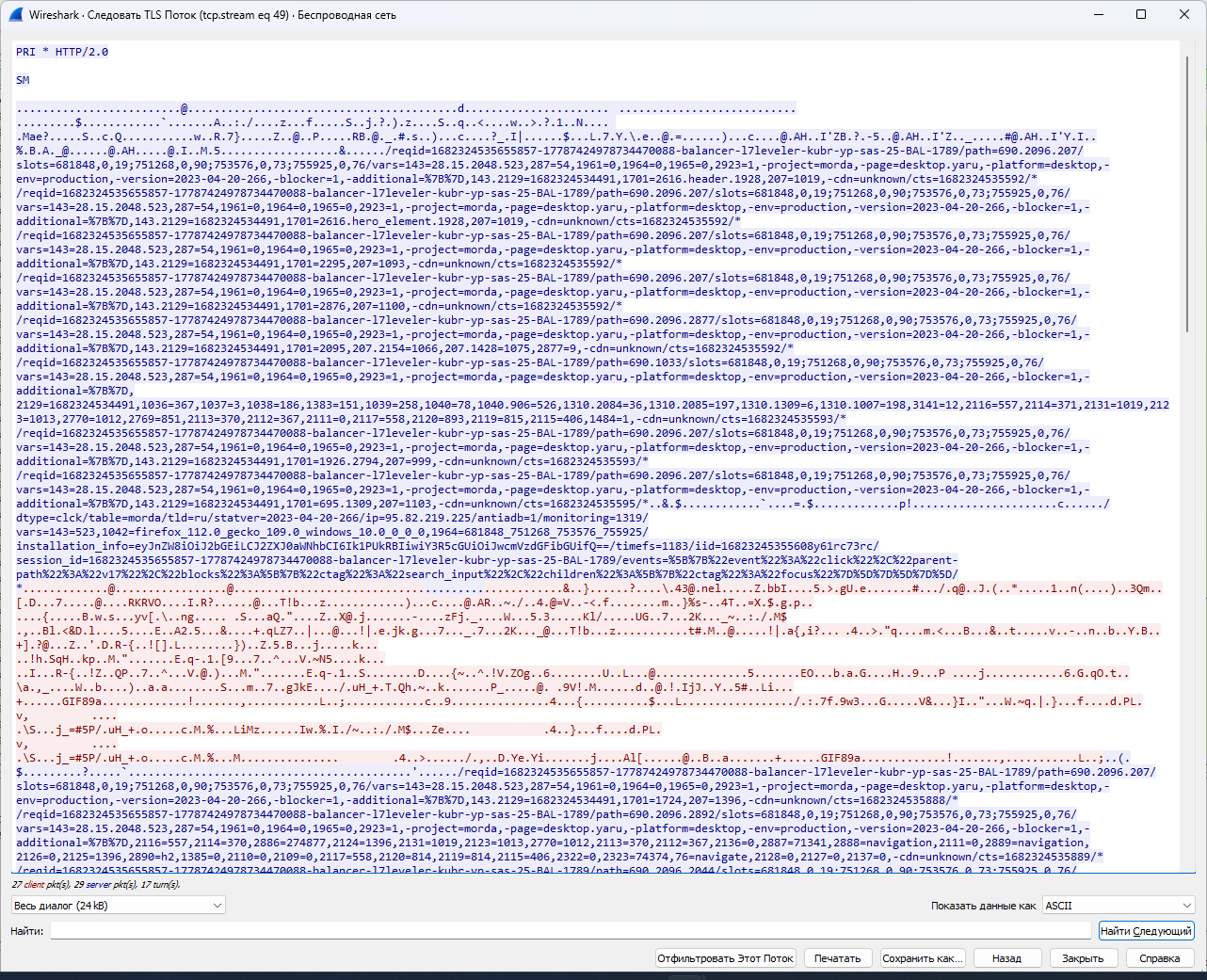


Рисунок 4. TLS поток (HTTP2)

* 1. Применим в качестве фильтра отображения выражение «http2». Далее ищем пакет, в котором содержится строка, которая была введена в предыдущем пункте с методом HTTP запроса POST.

При анализе сайта max.zolotyh.su нам встречались похожие заголовки, например Accept, Accept-Language, Accept-Encoding.

* 1. Составим фильтр отображения, который будет отображать только HTTP2 заголовки, содержащие методы POST и GET:

(http2.flags == 0x24) or (http2.flags == 0x25)

В столбце Info можно увидеть различные относительные URL, для некоторых из них можно попытаться объяснить их роль:

* /click/click (или /click/counter) идут в связке с методом POST и, возможно, связаны с «кликами» пользователя в поисковой системе, например нажатие на кнопку «Поиск», переключение по вкладкам «Поиск», «Картинки», «Видео» и тд.
* /search/text=<some text>… - собственно перенаправление на страницу поиска по введенному тексту. Тоже идет в связке с методом POST.
  1. Применим фильтр отображения «http2 || http», затем вызовем статистику по отправителям и получателям трафика. Путем перехода на вкладку IPv4, включения ограничения отображения фильтра и сортировки по убыванию байт получаем рейтинг узлов.

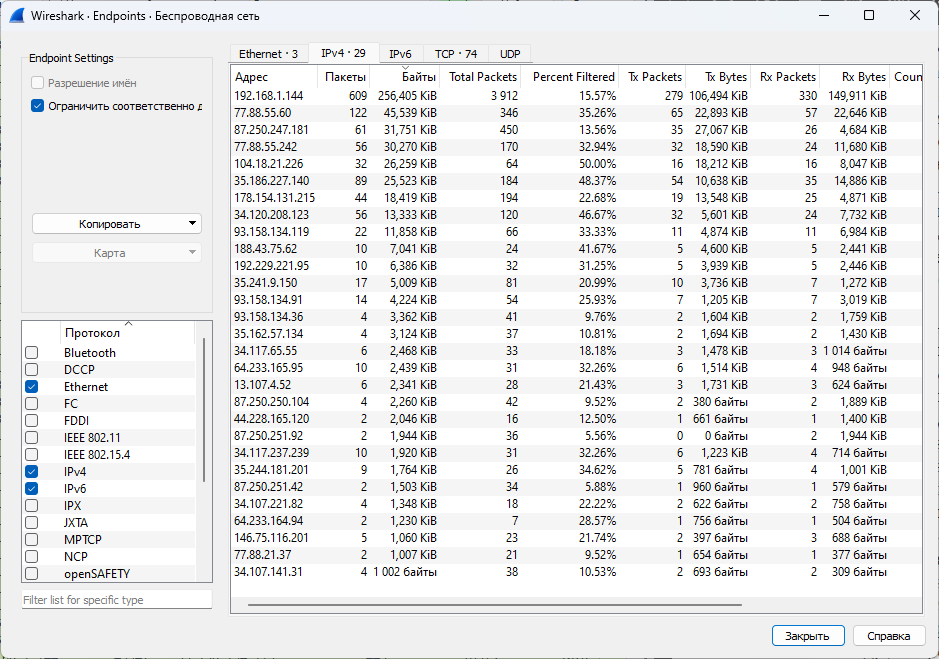


Рисунок 5. Рейтинг узлов по байтам (IPv4)

* 1. Откроем анализатор DNS пакетов в захваченном трафике. Найдем имена узлов из рейтинга, полученного на предыдущем шаге.

Таблица 1. Соответствие IP адресов узлов именам узлов

|  |  |
| --- | --- |
| **IP адрес узла** | **Имя узла** |
| 93.158.134.119 | mc.yandex.ru |
| 93.158.134.36 | favicon.yandex.ru |
| 93.158.134.91 | yabs.yandex.ru |
| 87.250.251.92 | cryprox.yandex.net |
| 87.250.251.42 | egress.yandex.net |
| 87.250.250.104 | csp.yandex.net |
| 87.250.247.181 | avatars.mds.yandex.net |
| 77.88.21.60 | yandex.ru |
| 77.88.21.37 | mail.yandex.ru |

## Дополнительная информация об IP адресах