

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ Ордена Трудового Красного Знамени
федеральное государственное бюджетное образовательное учреждение
высшего образования

МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И
ИНФОРМАТИКИ

Кафедра Информационной безопасности

Изучение основных функциональных возможностей программы-сниффера
WireShark

Задание:

1. Осуществить захват трафика
2. Изучить структуру IP-пакета, заголовки IP TCP UDP – пакета и его поля
3. Изучение функциональных возможностей
4. Графическое представление захваченного трафика

Выполнение задания

1) Осуществить захват трафика:

После запуска wireshark, выбираем необходимый источник трафика (в данном случае - Ethernet) и нажимаем на кнопку “начать захват пакетов”.

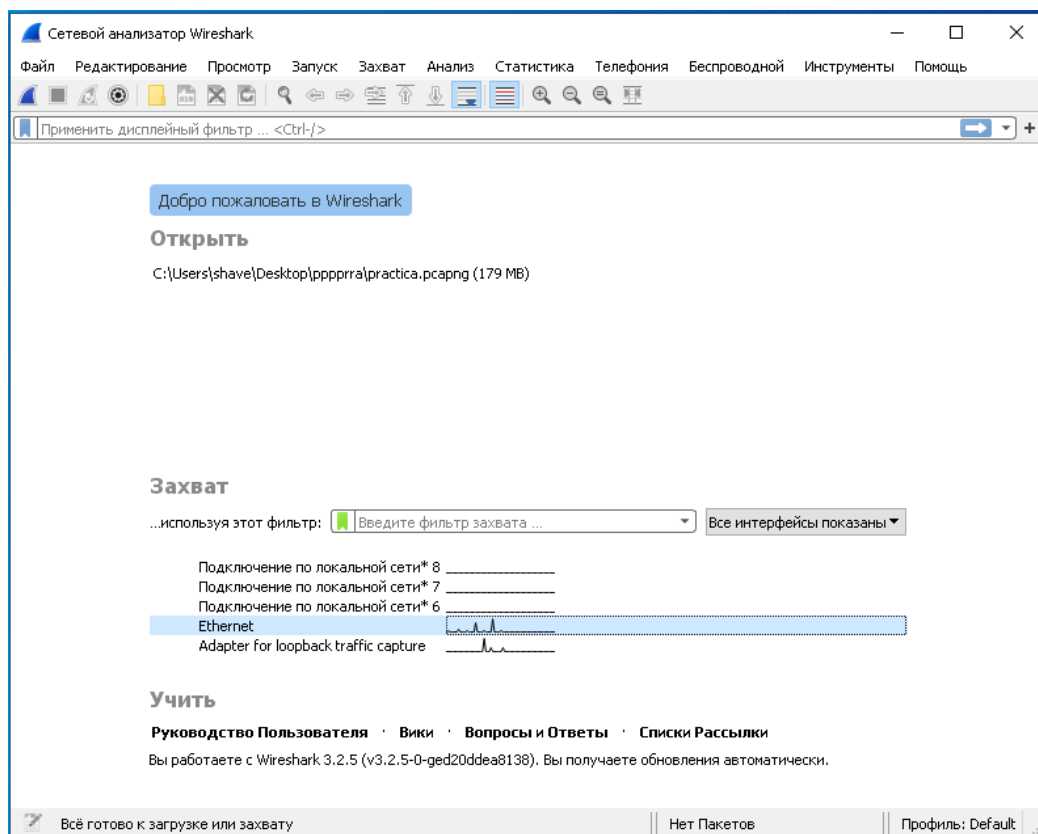


Рисунок 1 - стартовое окно wireshark

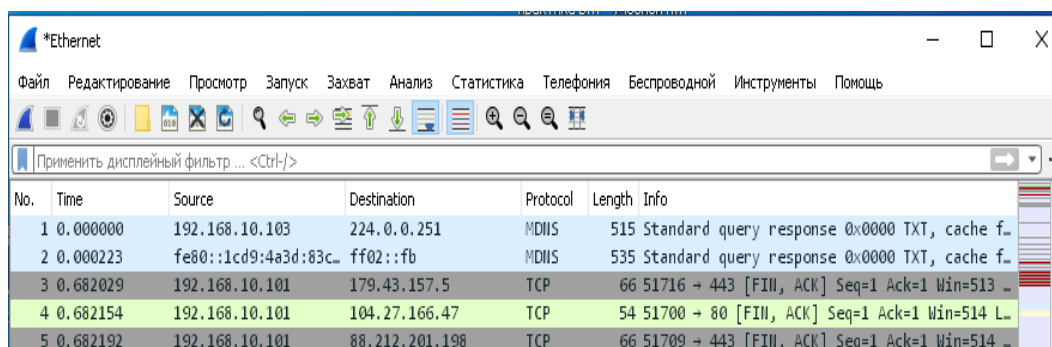


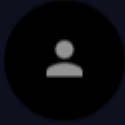
Рисунок 2 - начало захвата трафика


Для примера анализа трафика, выбран сайт <http://hd.kyberkino.ru>, на котором предварительно проведена регистрация.

В процессе работы программы:

- 1) Произведен переход на сайт <http://hd.kyberkino.ru>
- 2) Осуществлен вход в личную учетную запись
- 3) Осуществлен просмотр фильма в течении 20 минут

АВТОРИЗАЦИЯ





☒ Запомнить меня

Войти

[Регистрация](#) [Восстановить пароль](#)

Рисунок 3 – авторизация на сайте

За время просмотра, длительностью в 26 минут, было собрано 2272489 пакетов.

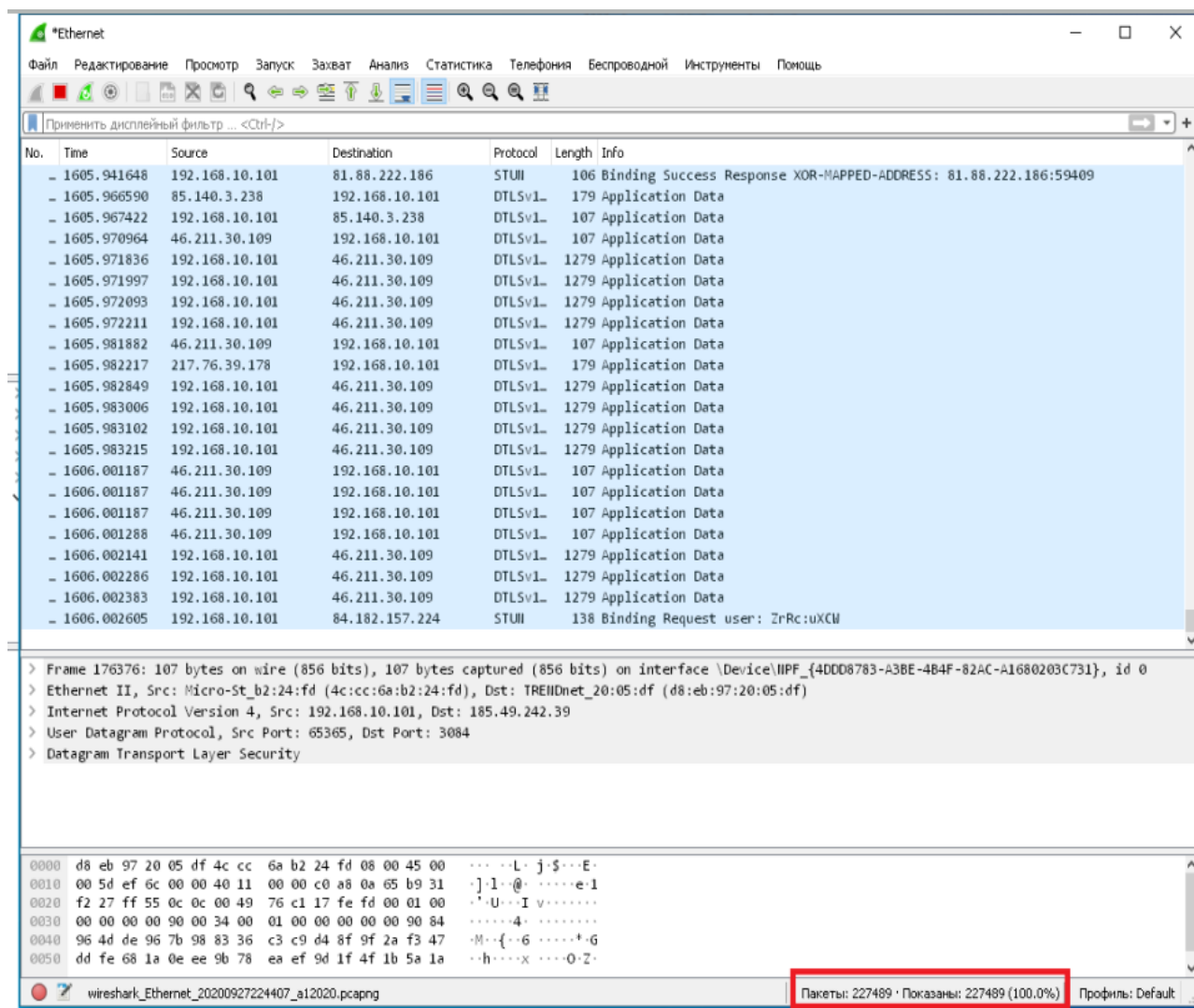


Рисунок 4 – конец захвата трафика

Для анализа конкретного пакета воспользуемся фильтром

http.request.method == "POST"

Из всех собранных пакетов, остаётся только 3. Из них нас интересует пакет, собранный на 13.906480 секунде. Выделим его и нам станет доступно дополнительное меню, в котором стоит обратить внимание на пункт HTML Form URL Encoded...

Так как сайт использует незащищенный протокол http, в захваченном пакете мы можем увидеть логин и пароль, использованные при авторизации на сайте.

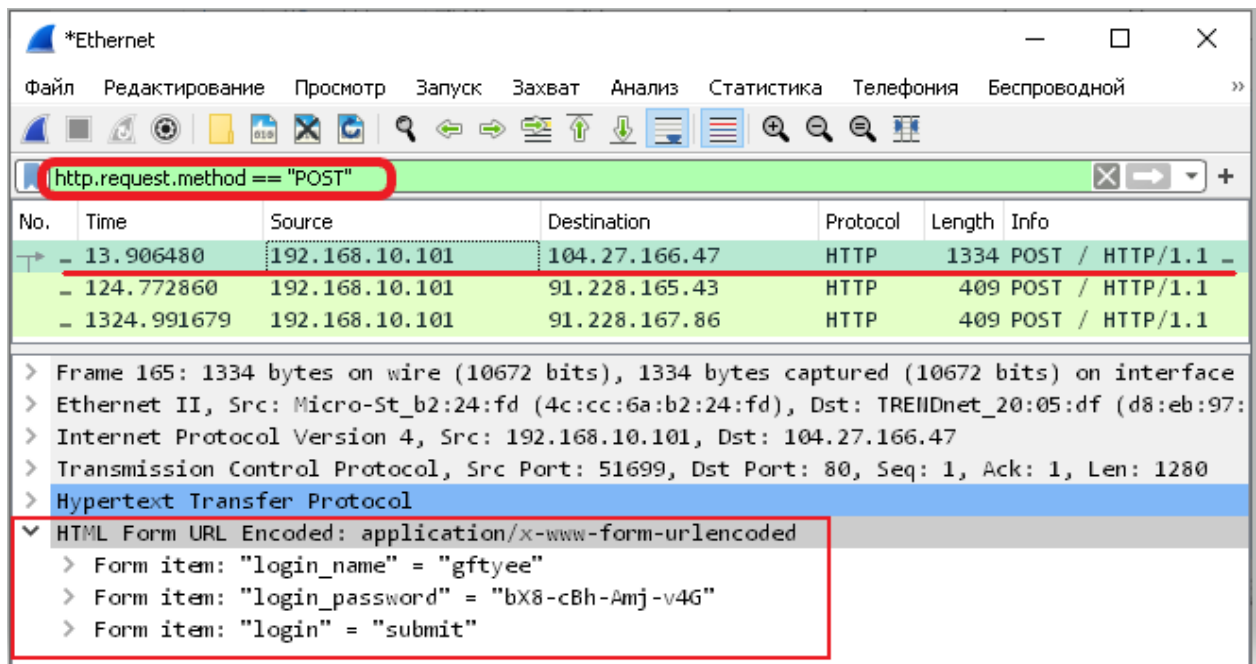


Рисунок 5 – анализ пакета

2) Изучить структуру IP-пакета, заголовки IP TCP UDP – пакета и его поля

IP-пакет состоит из заголовка и данных. Заголовок определяет функционал, а в поле данных передается какая-то информация. На рисунке 6 представлена таблица заголовков IP пакета.

| | | | | | |
|--------------|-------------------------------|--------------------------|--------------------------|--------------------------------------|-----------------------------|
| Заголовок IP | Версия (4 бита) | Длина заголовка (4 бита) | Тип обслуживания (8 бит) | Общая длина (16 бит) | |
| | Идентификация (16 бит) | | | Флаги (3 бита) | Смещение фрагмента (13 бит) |
| | Время жизни (8 бит) | Протокол (8 бит) | | Контрольная сумма заголовка (16 бит) | |
| | IP-адрес источника (32 бита) | | | | |
| | IP-адрес назначения (32 бита) | | | | |
| | | | | | |

Рисунок 6 – заголовок IP

Для начала выберем в wireshark пакет, содержащий протокол UDP. В появившемся меню, обратим внимание на пункт Internet Protocol...

В нем представлены все заголовки IP-пакета и их значения.

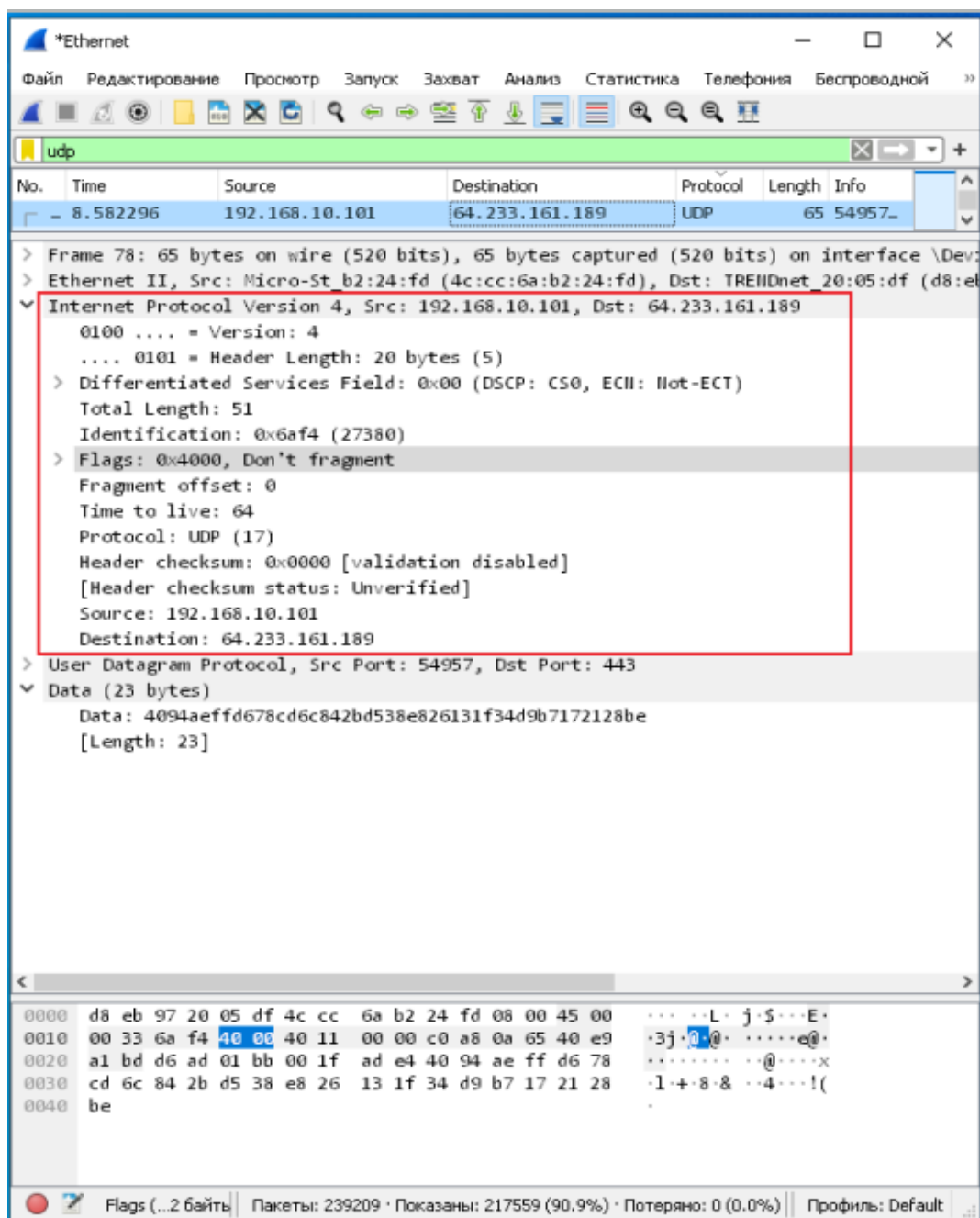


Рисунок 7 – заголовки IP в wireshark

Теперь ознакомимся с протоколом UDP. Таблица структуры UDP представлена на рисунке 8. Для просмотра заголовка UDP в wireshark развернем подменю с названием User Datagram Protocol...

| | |
|--------------------|-----------------------|
| Порт источника | Порт назначения |
| Длина UDP-сегмента | Контрольная сумма UDP |
| Данные | |

Рисунок 8 – UDP

```
User Datagram Protocol, Src Port: 54957, Dst Port: 443
  Source Port: 54957
  Destination Port: 443
  Length: 31
  Checksum: 0xade4 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  > [Timestamps]
```

Рисунок 9 – заголовок UDP в wireshark

Далее посмотрим структуру TCP. Её таблица представлена на рисунке 10.

В wireshark выделим пакет с TCP и откроем подменю Transmission Control Protocol...

| | | |
|---|--|--|
| Source Port (Адрес порта источника) | | Destination Port (Адрес порта назначения) |
| Sequence Number (Номер в последовательности) | | |
| Acknowledgment Number (Номер подтверждения) | | |
| Data Offset (Смещение данных) | Reserved/Control Bits (Зарезервировано/Биты управления) | Window (Размер окна) |
| Checksum (Контрольная сумма) | | Urgent Pointer (Указатель) |
| Options (Дополнительные данные заголовка) | | Padding (Выравнивание) |
| Data (Данные) | | |

Рисунок 10 – структура TCP

```
Transmission Control Protocol, Src Port: 443, Dst Port: 51711, Seq: 33, Ack: 2, Len: 0
  Source Port: 443
  Destination Port: 51711
  [Stream index: 8]
  [TCP Segment Len: 0]
  Sequence number: 33      (relative sequence number)
  Sequence number (raw): 1280445930
  [Next sequence number: 33      (relative sequence number)]
  Acknowledgment number: 2      (relative ack number)
  Acknowledgment number (raw): 2517688030
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
  Window size value: 64
  [Calculated window size: 64]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x1870 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
```

Рисунок 11 – заголовок TCP в wireshark

3) Изучение функциональных возможностей

Попробуем просмотреть данные, полученные пользователем при посещении сайта.

Для этого с помощью меню “файл” экспортируем объекты в HTTP.

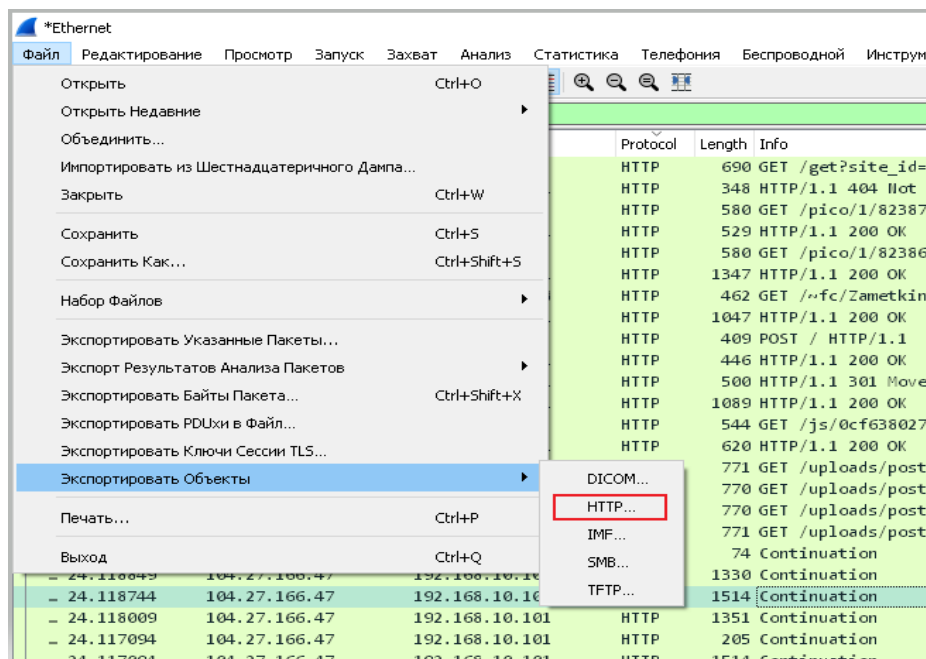


Рисунок 12 – экспорт объектов

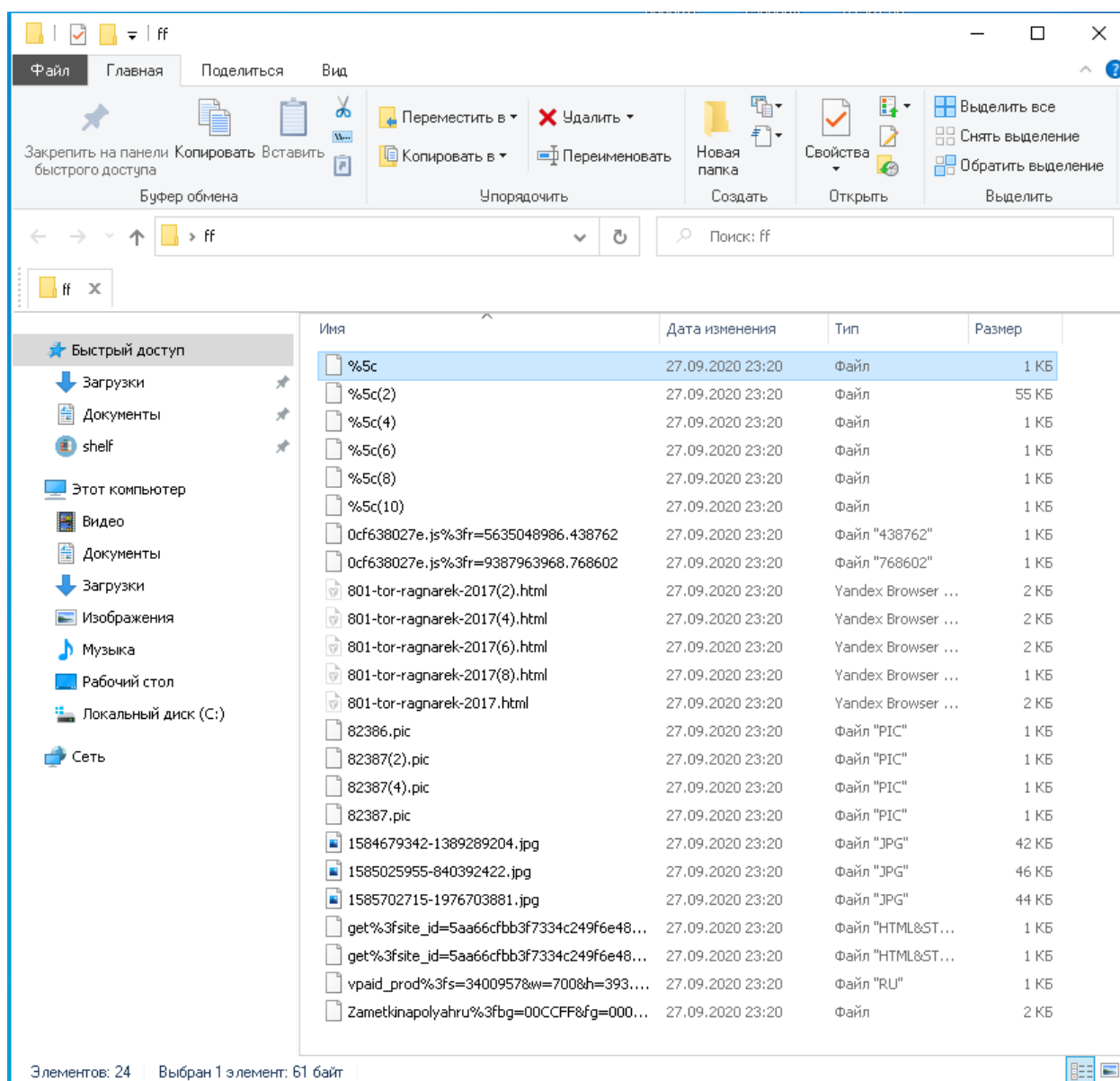


Рисунок 13 – экспортированные объекты в папке

Из экспортированных объектов возможно посмотреть, например, на изображения, которые были на сайте во время просмотра фильма.

Также можно построить график появления захваченных пакетов в зависимости от всего времени захвата. Для этого используем инструмент “График ввода/вывода”

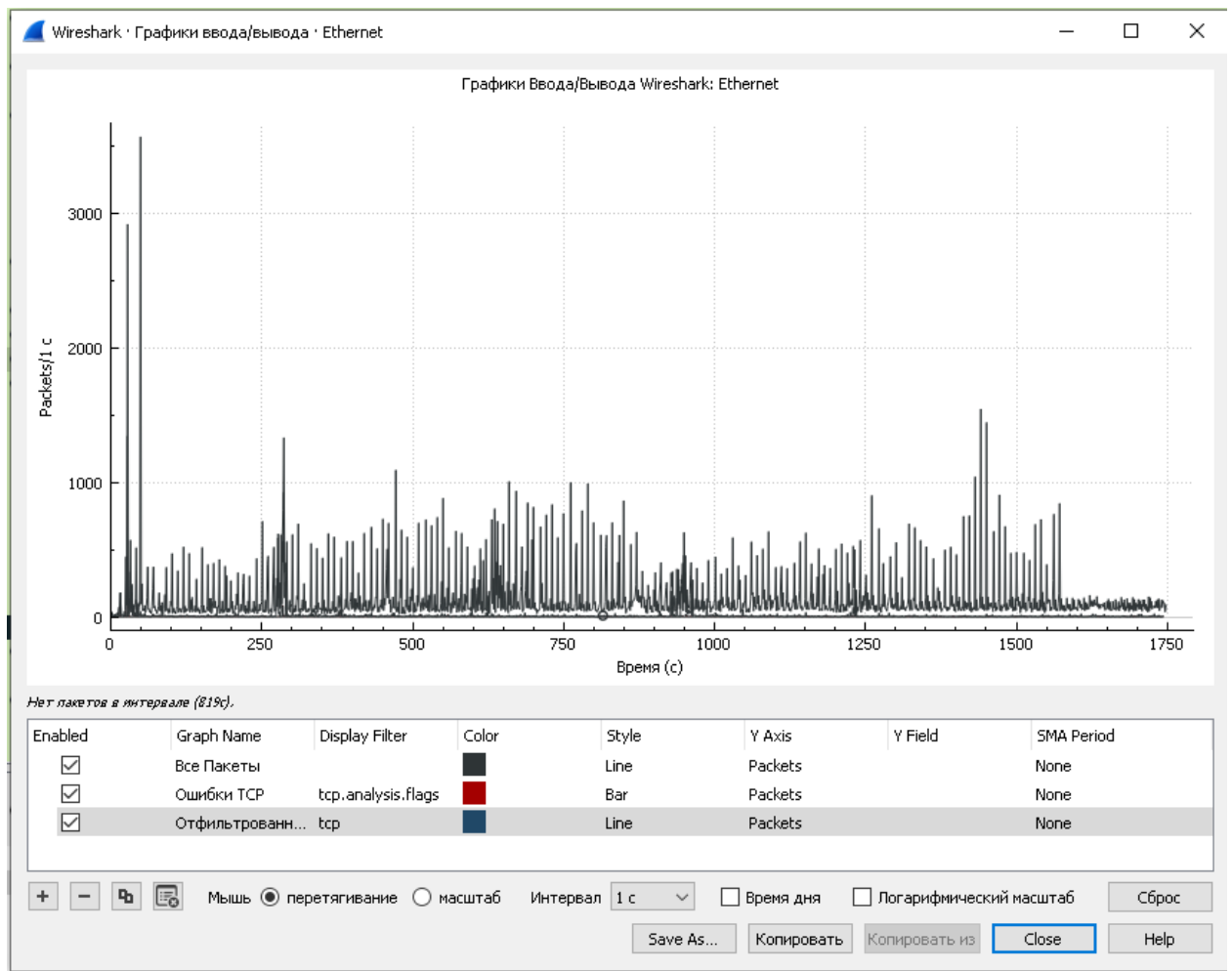


Рисунок 14 – График ввода/вывода