Web

Что такое и зачем?

Web

Что такое и зачем?

Что мы рассмотрим?

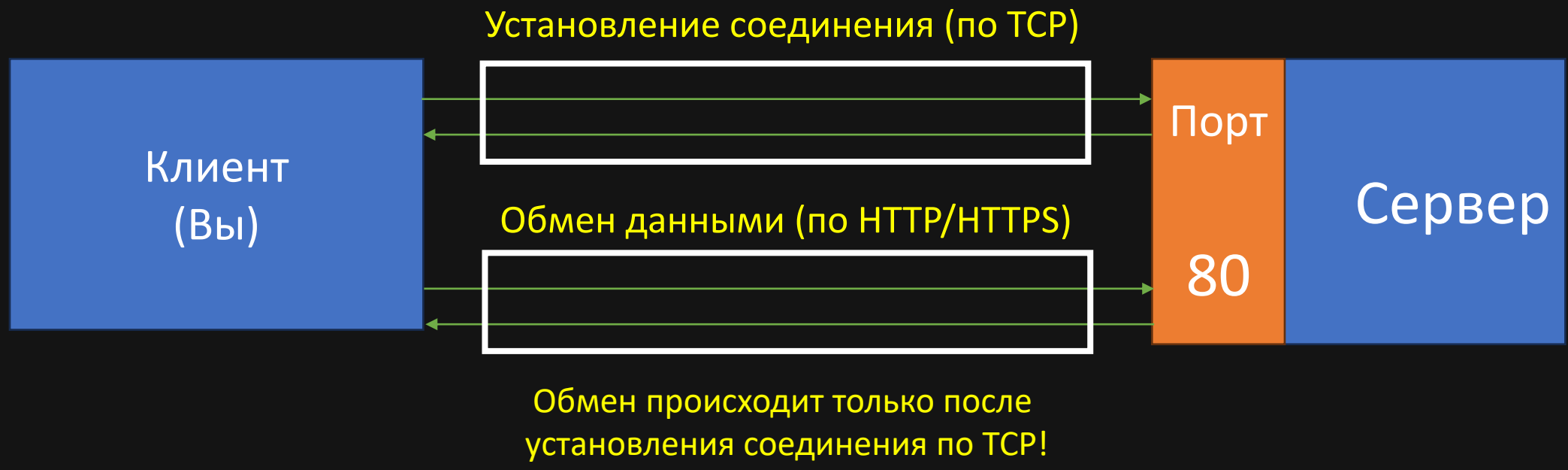
- Как работает сайт:
  - Как происходит подключение к сайту?
  - Что такое порт?
  - Какие есть протоколы и зачем нам прокси?
  - Как создать сайт и что нам искать?

Зачем это знать?

Ответ дня

Хачу взламать хексагон (зачем взламывать пентагон, ведь 5<6)

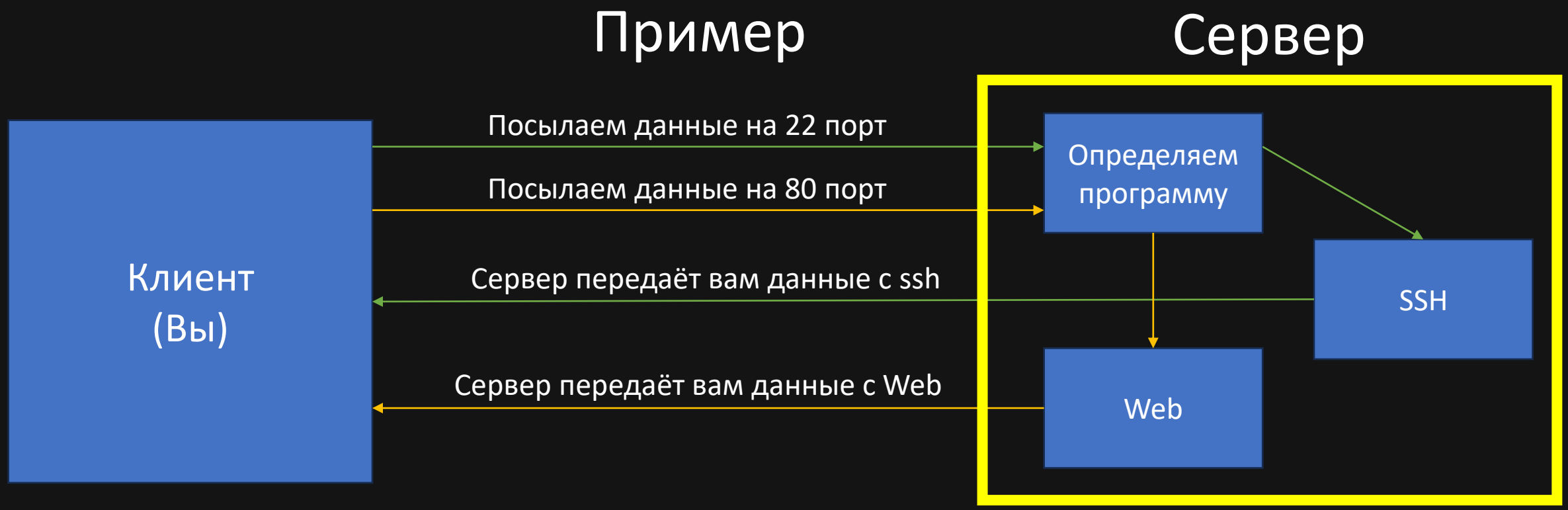
Как происходит подключение к сайту?



* Порт может быть любым, не обязательно 80 или 443

Что такое порт?

* Грубо говоря, порт – это номер программы, зарезервированный компьютером. На порт будут приходить данные, а компьютер в свою очередь соотносит данные с порта и программу, которой выделили порт и направляет их в программу



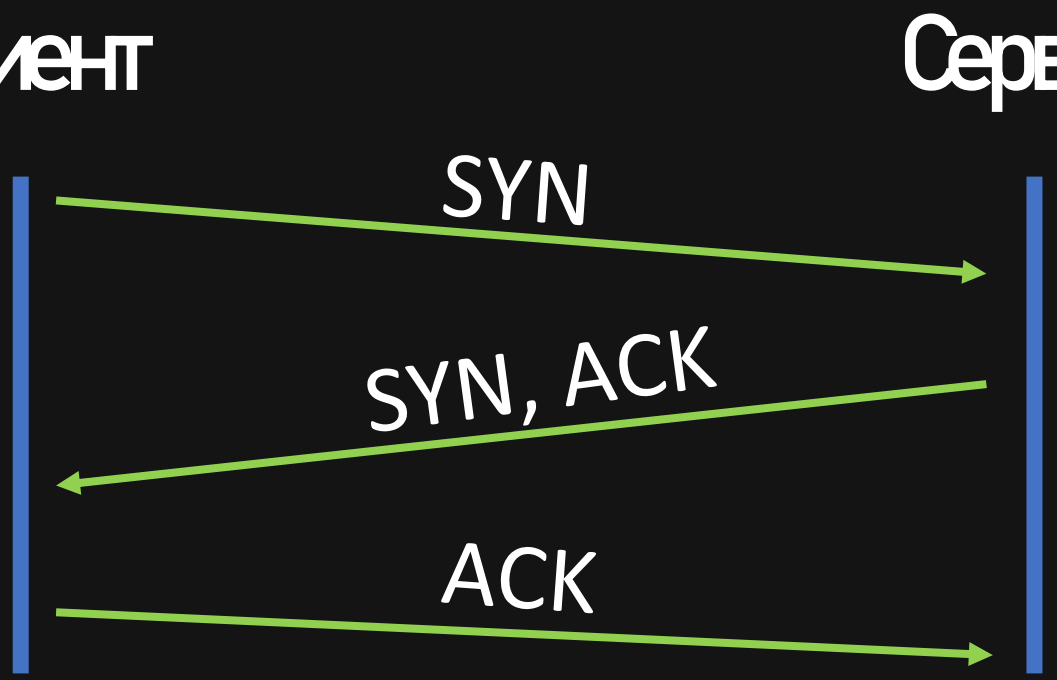
Какие есть протоколы и зачем нам прокси?

Главные протоколы (на данный момент) :

- TCP
- UDP
- HTTP
- HTTPS (HTTP + SSL)

Какие есть протоколы и зачем нам прокси?

TCP



Какие есть протоколы и зачем нам прокси?

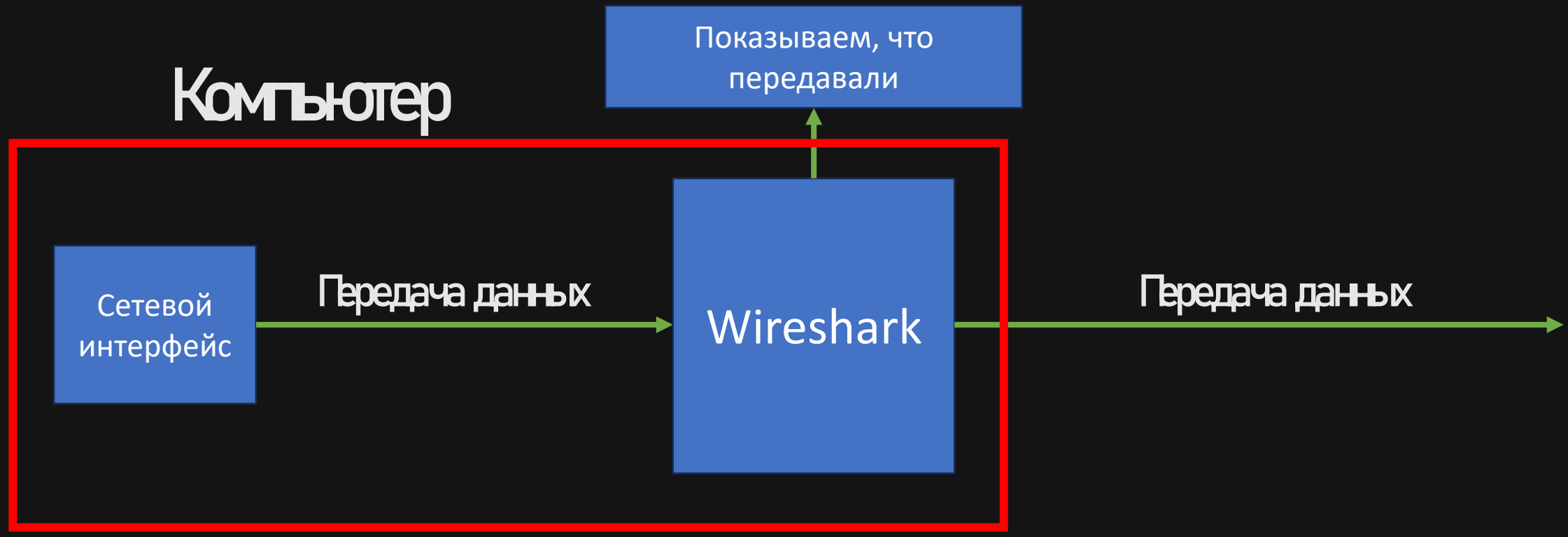
Как увидеть это?

-> Через перехват трафика

* Мы используем wireshark для перехвата трафика

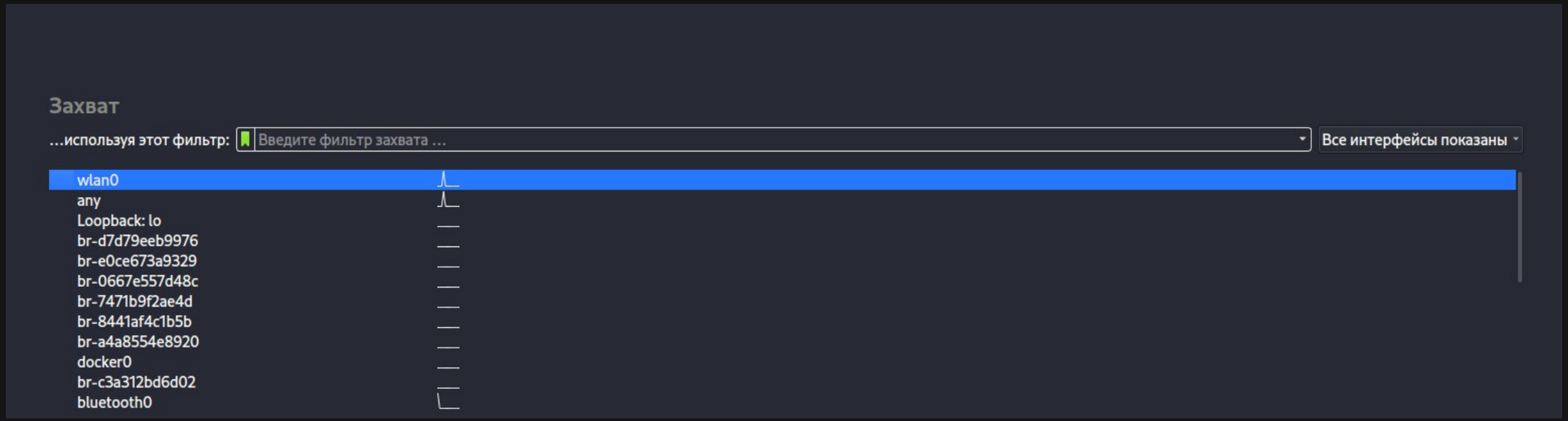
Какие есть протоколы и зачем нам прокси?

Как работает wireshark?



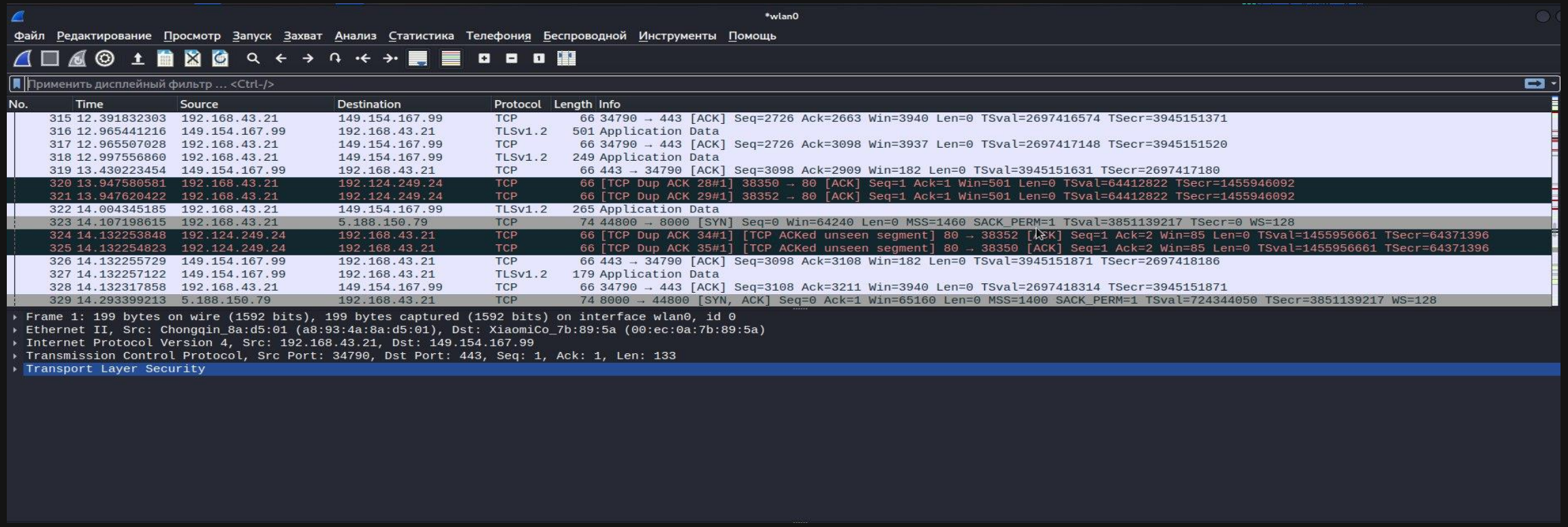
Какие есть протоколы и зачем нам прокси?

Открываем wireshark и выбираем интерфейс (с которого будем снимать трафик) (wlan0 / eth0)



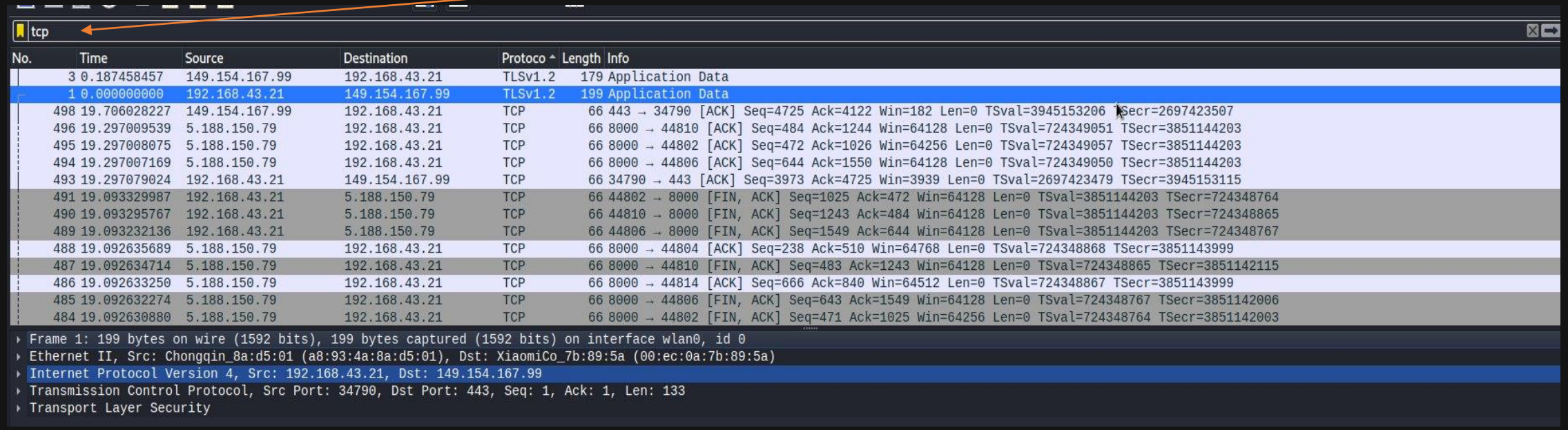
Какие есть протоколы и зачем нам прокси?

Wireshark начинает перехватывать трафик. Появляется следующее:



Какие есть протоколы и зачем нам прокси?

Wireshark перехватывает многие протоколы. Введём фильтр TCP (чтобы видеть передачи только по нему)



Какие есть протоколы и зачем нам прокси?

Значение столбцов (в wireshark):

Source – источник (кто отправляет данные)

Destination – приёмник (кто принимает данные)

Protocol – какой протокол передачи используется

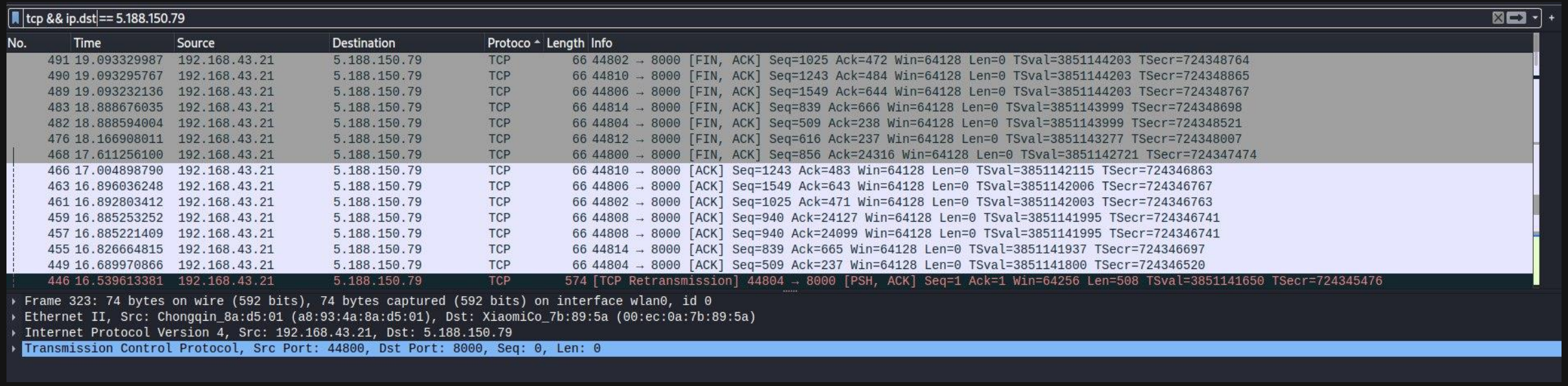
Info – краткая информация(какие флаги, порты...)

Какие есть протоколы и зачем нам прокси?

Фильтры можно комбинировать при помощи логических выражений.

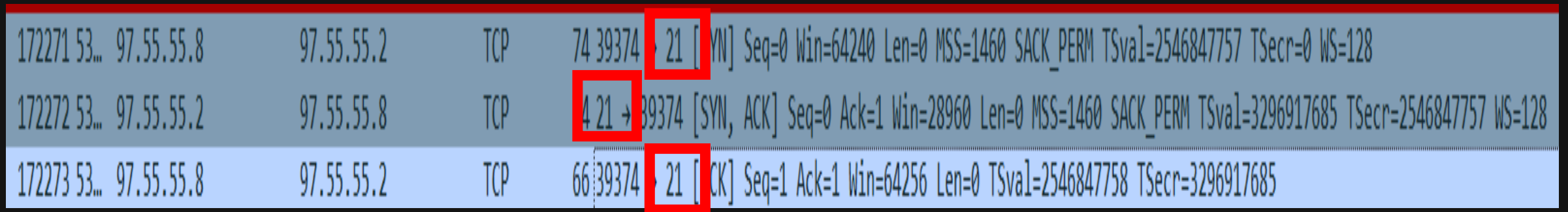
Пример: tcp && ip.dst == 5.188.150.79 (Hashctf)

(Мы ищем все данные, переданные по TCP к ip-адрессу 5.188.150.79)



Какие есть протоколы и зачем нам прокси?

Как выглядит подключение по TCP в wireshark



На какой порт сервера мы передаём данные?

21

Какие есть протоколы и зачем нам прокси?

UDP

Какие есть протоколы и зачем нам прокси?

udp

No.	Time	Source	Destination	Protocol	Lengtl	Info
1311…	8.…	97.55.55.8	97.55.55.2	UDP	342	48579 → 43100 Len=300
1311…	8.…	97.55.55.2	97.55.55.8	ICMP	370	Destination unreachable (Port unreachable)
2647…	10…	97.55.55.2	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
3954…	36…	97.55.55.2	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question

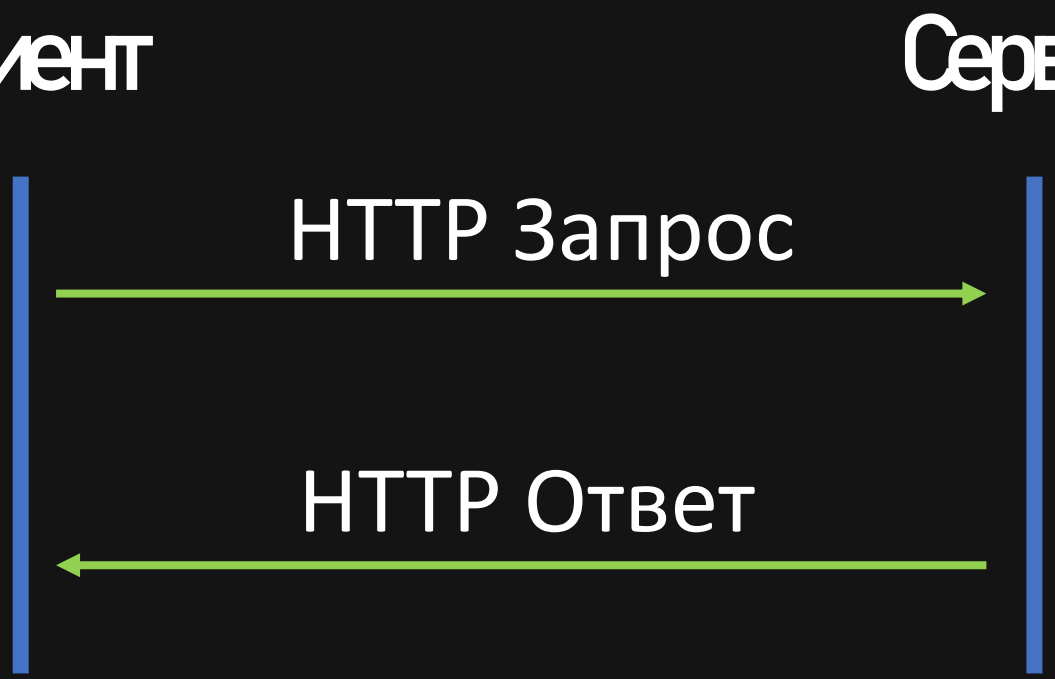
TCP используется для передачи данных без повреждения(CRC), а UDP – с повреждением данных, но с большой скоростью

-> TCP – Используем для критически важных данных везде (нам не нужно, чтобы на сайте появилось что-то внеземное)

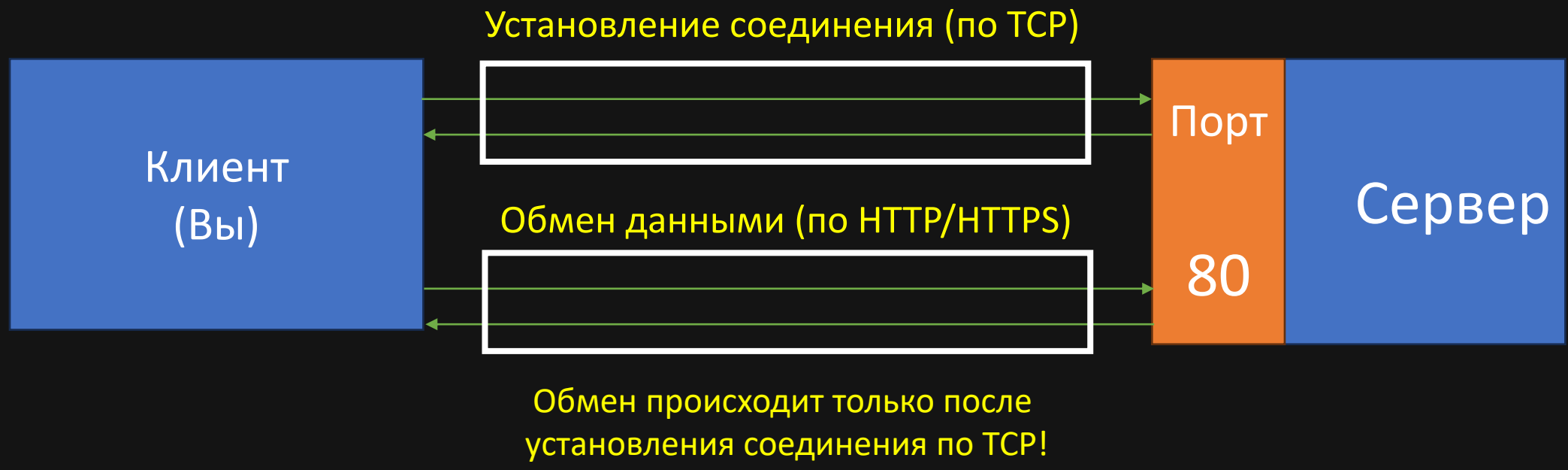
-> UDP – Используем где нужна скорость, а не качество данных (Видеоролики например)

Какие есть протоколы и зачем нам прокси?

Протокол HTTP (используется для сайтов) | HTTPS - актуальнее



Вспоминаем



* Порт может быть любым, не обязательно 80 или 443

Какие есть протоколы и зачем нам прокси?

Используем фильтр http и смотрим весь трафик по http

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
131097	7.…	97.55.55.8	97.55.55.2	HTTP	84	GET / HTTP/1.0
131099	7.…	97.55.55.2	97.55.55.8	HTTP	513	HTTP/1.1 200 OK (text/html)
131156	9.…	97.55.55.8	97.55.55.2	HTTP	238	GET /nmaplowercheck1681850705 HTTP/1.1
131158	9.…	97.55.55.8	97.55.55.2	HTTP	84	GET / HTTP/1.0
131160	9.…	97.55.55.8	97.55.55.2	HTTP	680	POST /sdk HTTP/1.1
131162	9.…	97.55.55.2	97.55.55.8	HTTP	513	HTTP/1.1 200 OK (text/html)
131164	9.…	97.55.55.2	97.55.55.8	HTTP	544	HTTP/1.1 404 Not Found (text/html)
131165	9.…	97.55.55.2	97.55.55.8	HTTP	523	HTTP/1.1 404 Not Found (text/html)
131182	9.…	97.55.55.8	97.55.55.2	HTTP	219	GET /HNAP1 HTTP/1.1
131185	9.…	97.55.55.8	97.55.55.2	HTTP	224	GET /evox/about HTTP/1.1
131187	9.…	97.55.55.2	97.55.55.8	HTTP	525	HTTP/1.1 404 Not Found (text/html)
131188	9.…	97.55.55.2	97.55.55.8	HTTP	530	HTTP/1.1 404 Not Found (text/html)
131200	9.…	97.55.55.8	97.55.55.2	HTTP	84	GET / HTTP/1.0
131202	9.…	97.55.55.2	97.55.55.8	HTTP	513	HTTP/1.1 200 OK (text/html)
131210	9.…	97.55.55.8	97.55.55.2	HTTP	102	GET / HTTP/1.1
131212	9.…	97.55.55.2	97.55.55.8	HTTP	494	HTTP/1.1 200 OK (text/html)

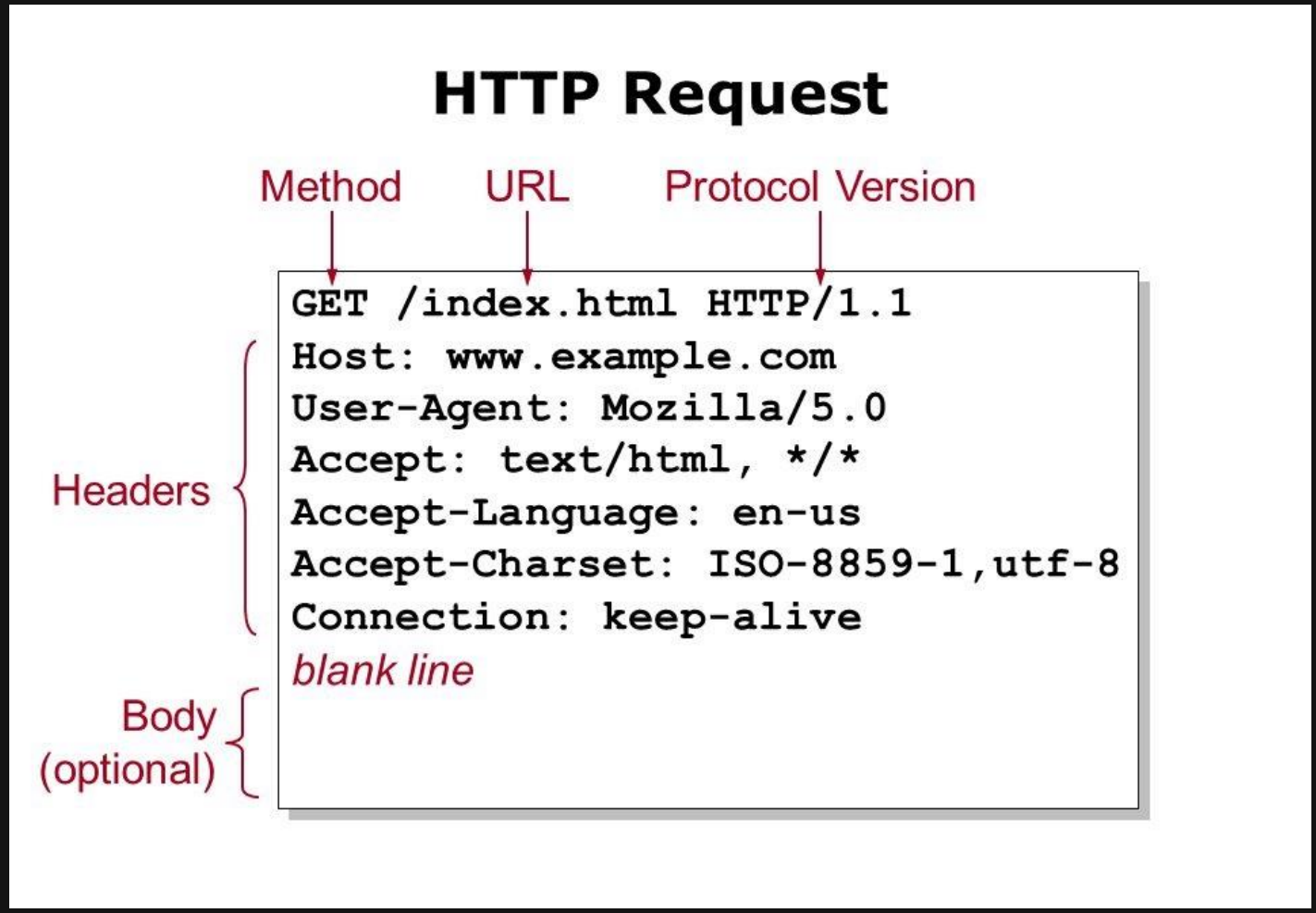
Какие есть протоколы и зачем нам прокси?

Структура HTTP запроса:

Метод URL Версия протокола

Заголовки (Указывают на доп.информацию)

Тело (в нём находятся данные)



Какие есть протоколы и зачем нам прокси?

Методы (говорят, что мы хотим)

GET

Получение веб-ресурса
(запрашиваем страничку. Простая загрузка сайта)

POST

Отправление данных на веб-ресурс
(Авторизация, регистрация. Всё, куда мы вводим данные)

* Есть ещё методы, но на данный момент ограничимся этими

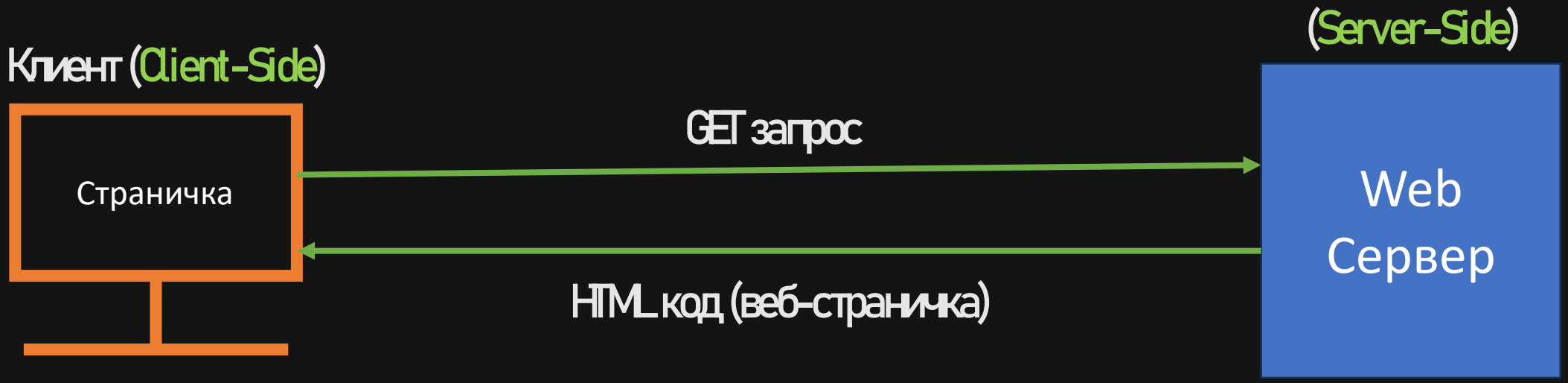
Какие есть протоколы и зачем нам прокси?

А теперь сравните трафик по TCP и HTTP. Какой из этих протоколов нам интересен с точки зрения атаки на сайты?

(Откройте wireshark и посмотрите пакеты TCP и HTTP. Где информация, которую вы передаёте для сайта)

Какие есть протоколы и зачем нам прокси?

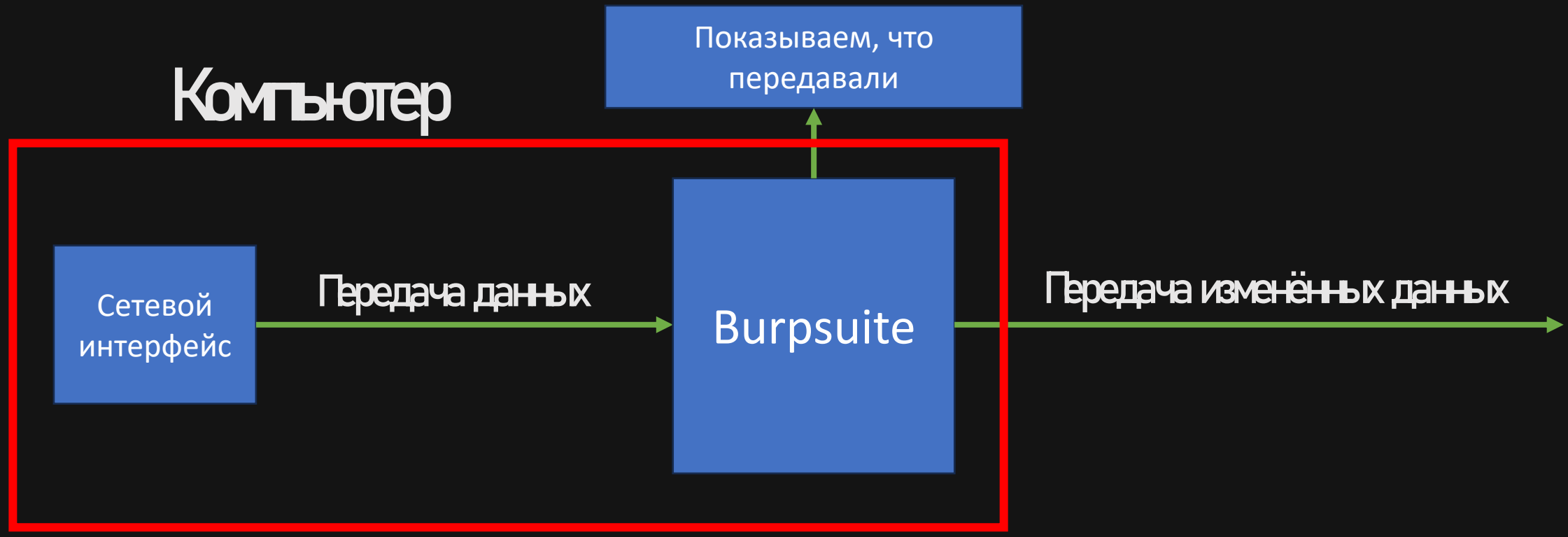
Как мы получаем сайт?



Браузер обрабатывает HTML код и выдаёт страничку

Какие есть протоколы и зачем нам прокси?

Как работает burpsuite?



Как создать сайт и что нам искать?

Создание сайта:

-> Создаём файл index.html

-> Запускаем PHP или XAMPP

Исмотрим, как все работает в wireshark и burpsuite

Как создать сайт и что нам искать?

Создание сайта:

-> Создаём файл index.html

-> Запускаем PHP или XAMPP

Исмотрим, как все работает в wireshark и burpsuite

Как создать сайт и что нам искать?

HTML – язык разметки

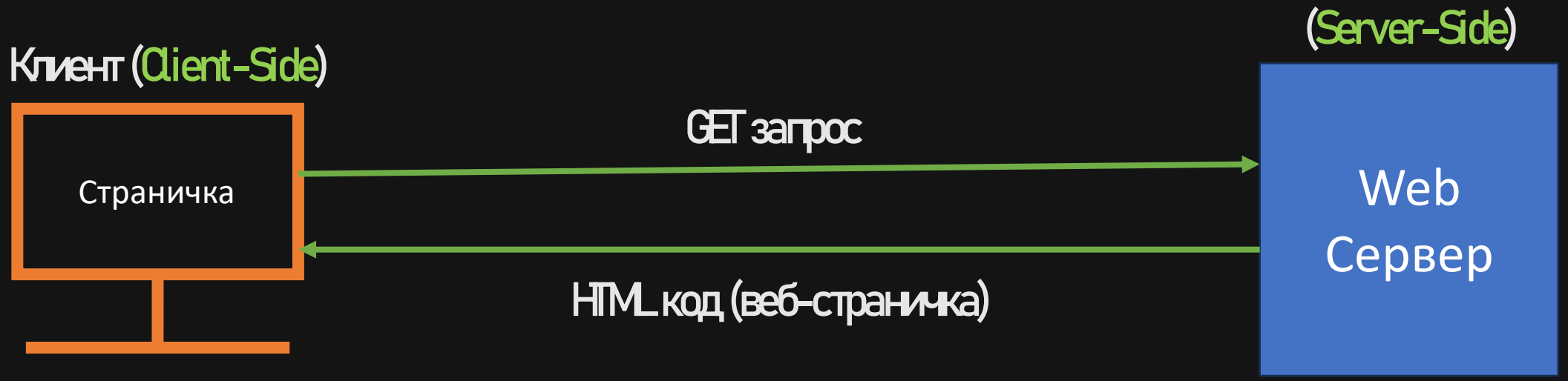
(НЕ ПРОГРАММИРОВАНИЯ!!!)

(Он определяет расположение элементов и структуру страницы)

```
1
2   <!DOCTYPE html>
3
4   <html>
5
6       <head>
7
8           <title>JS</title>
9           <meta charset="utf-8">
10
11      </head>
12
13      <body>
14
15          <script src="main.js"></script>
16
17      </body>
18
19  </html>
20
```

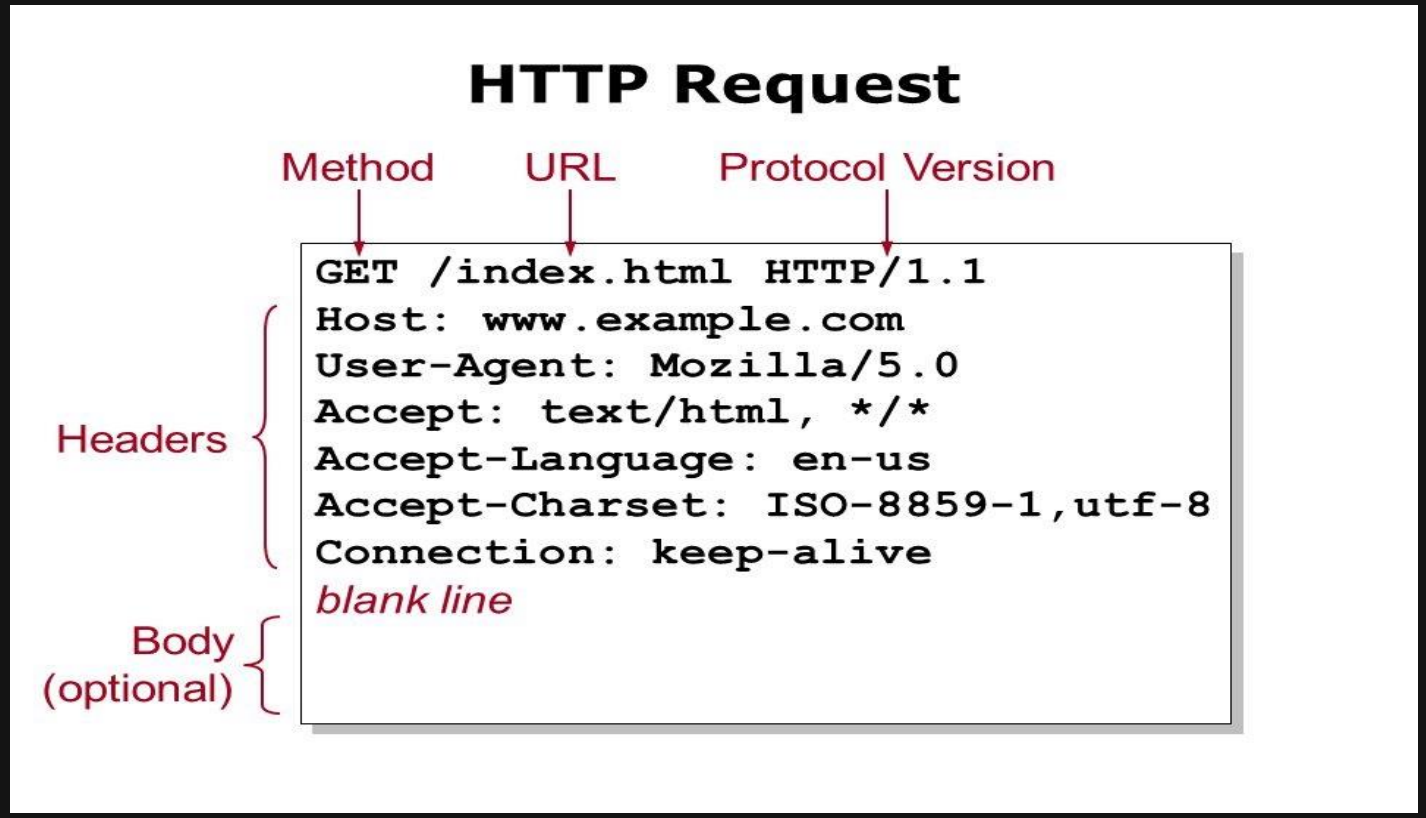
Ёщё раз

Как мы получаем сайт?



Браузер обрабатывает HTML код и выдаёт страничку

Как создать сайт и что нам искать?



Как создать сайт и что нам искать?

Если занятие ещё не закончилось – рассказываю про html, cookie и прочее. Решаем natas

Наш чат во вконтакте

Наш чат во телеграмме

Как меня найти