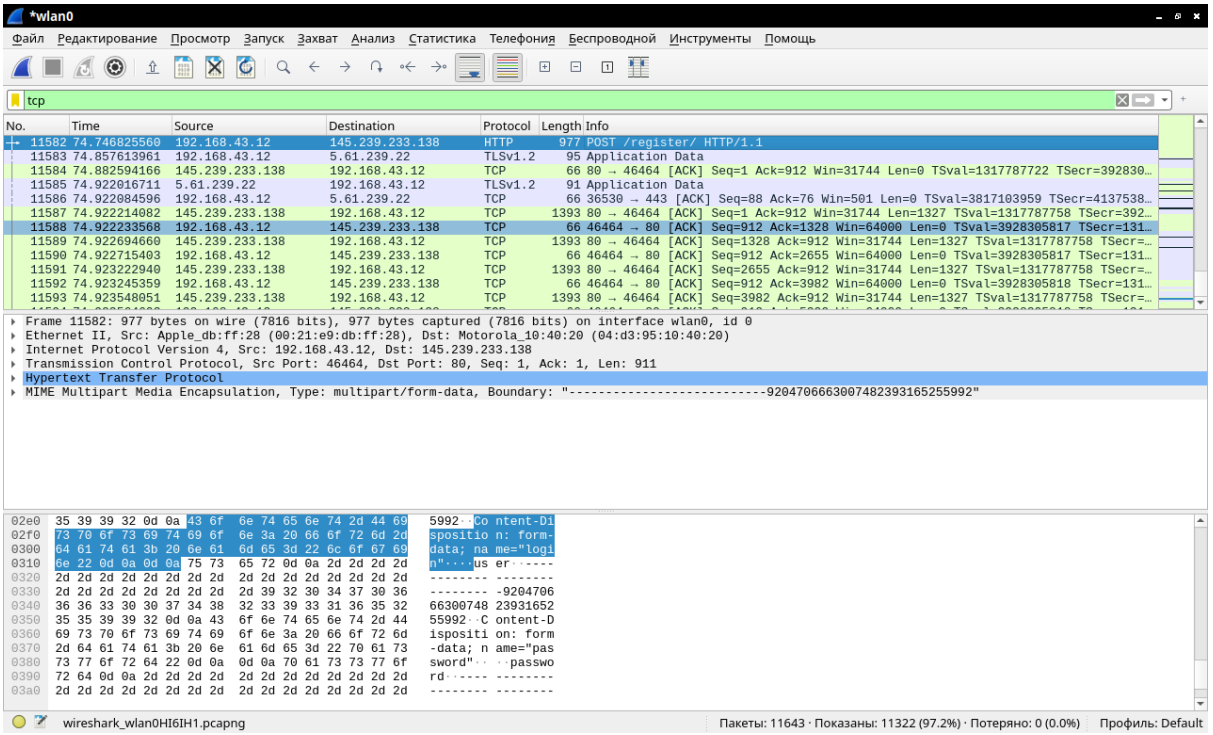
1.Найти нешифрованный HTTP-сайт, где есть регистрация и логин. Отправить фейковые данные. Сможет ли злоумышленник перехватить пароль?

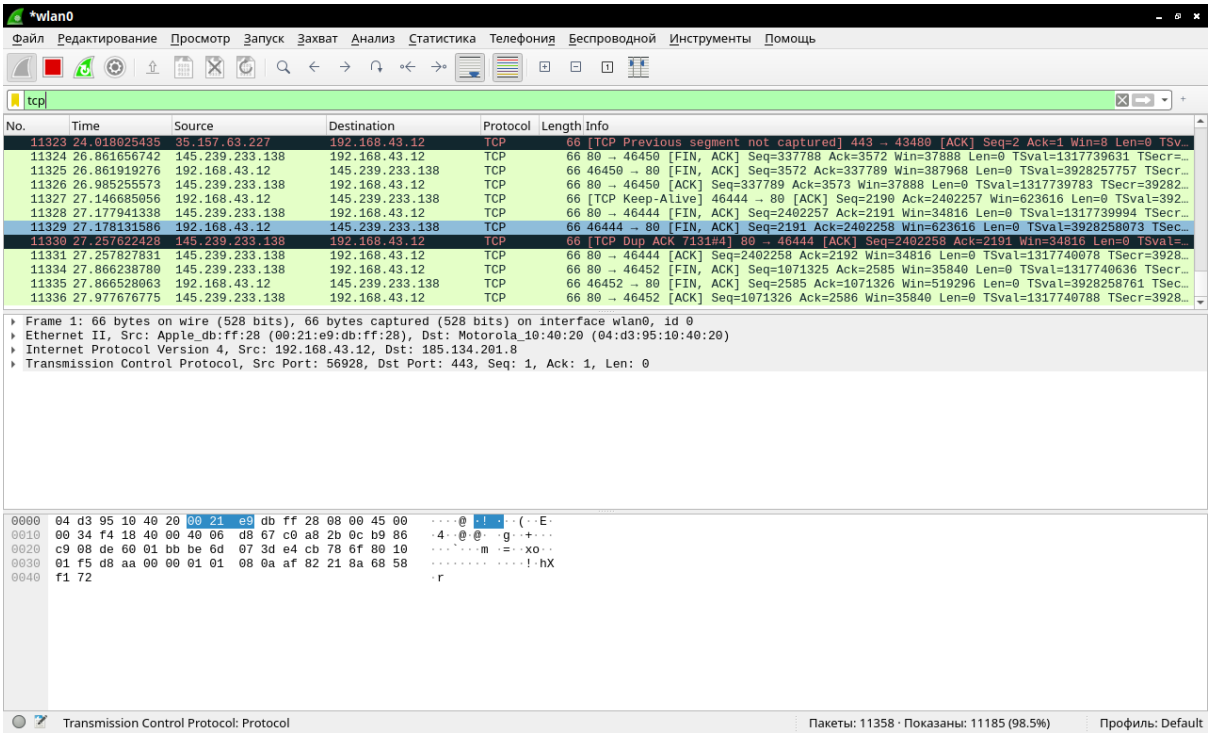
Да, сможет. Пароль уходит в открытом виде.



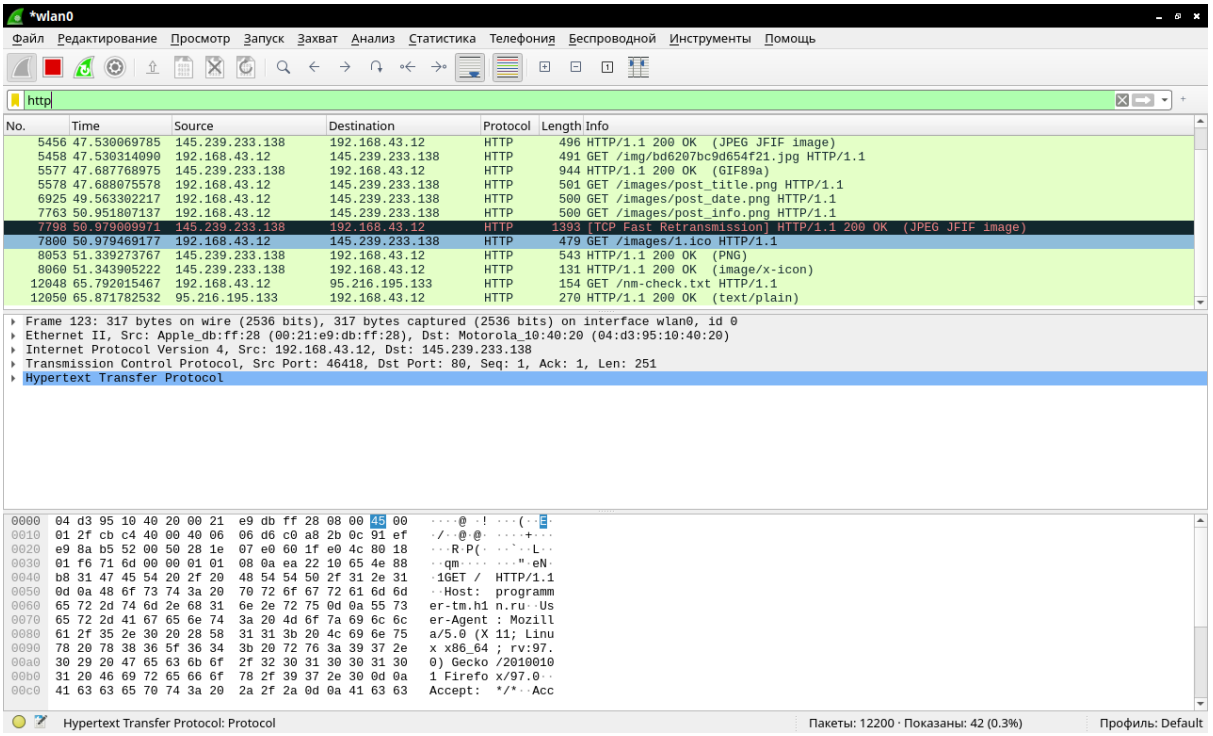
Тут мы явно видим логин и пароль которые ввели (естественно не верные)

P.S. При соединении через TLS данные шифруются и получить их в открытом виде для новичка не реально.

2. Найти не шифрованный HTTP-сайт со множеством картинок. Рекомендуется использовать Google Chrome. Сколько TCP-соединений будет открыто и почему?



Соединений TCP порядка 10 - 11 тысяч. Чтобы загрузить весь материал (6 картинок + подложка сайта)



42 http запроса/ответа Так же мы можем наблюдать весь процесс построения страницы через собранный запрос.

3. Повторите п.1 с TLS. Вопрос тот же.

Через TLS сходу не удалось найти пару логин и пароль. (как это было с TCP)

4. ** Какие интересные протоколы можно обнаружить, если зайти при помощи Google Chrome на YouTube? (Сработать может не у всех.)

TLS1.2 - 1.3, UDP, TCP, SSDP, QUIC, OSSP, ARP, DNS, HTTP

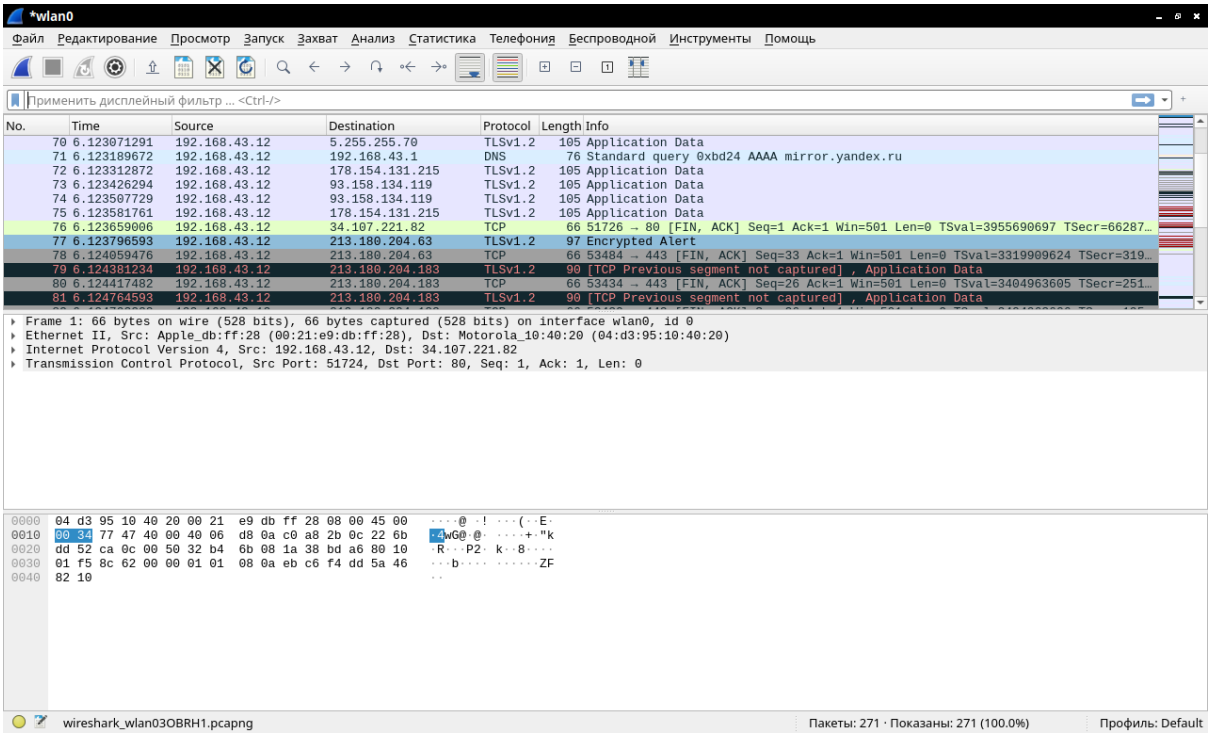
Мы получаем страницу по HTTP, DNS (определяем где она), ARP (Куда отправить запрос) TSP, TLS

OCSP - похоже на получение видео в окошках (фреймах)

TLS, UDP, QUIC - похоже на передачу видео.

SSDP - передает информацию о клиенте.

5 ** Если хочется совсем сложное задание, то попробуйте изучить трафик при подключении к FTP-серверу (достаточно любого публичного нешифрованного FTP-сервера, например Yandex.Mirror)



Нашел http вариант только и тут все банально, TLS - шифрование, tcp, dns (и прочее, по мелочи) прогрузка странички.

WireShark работал под Linux. Сайт - мой проект programmer-tm.h1n.ru