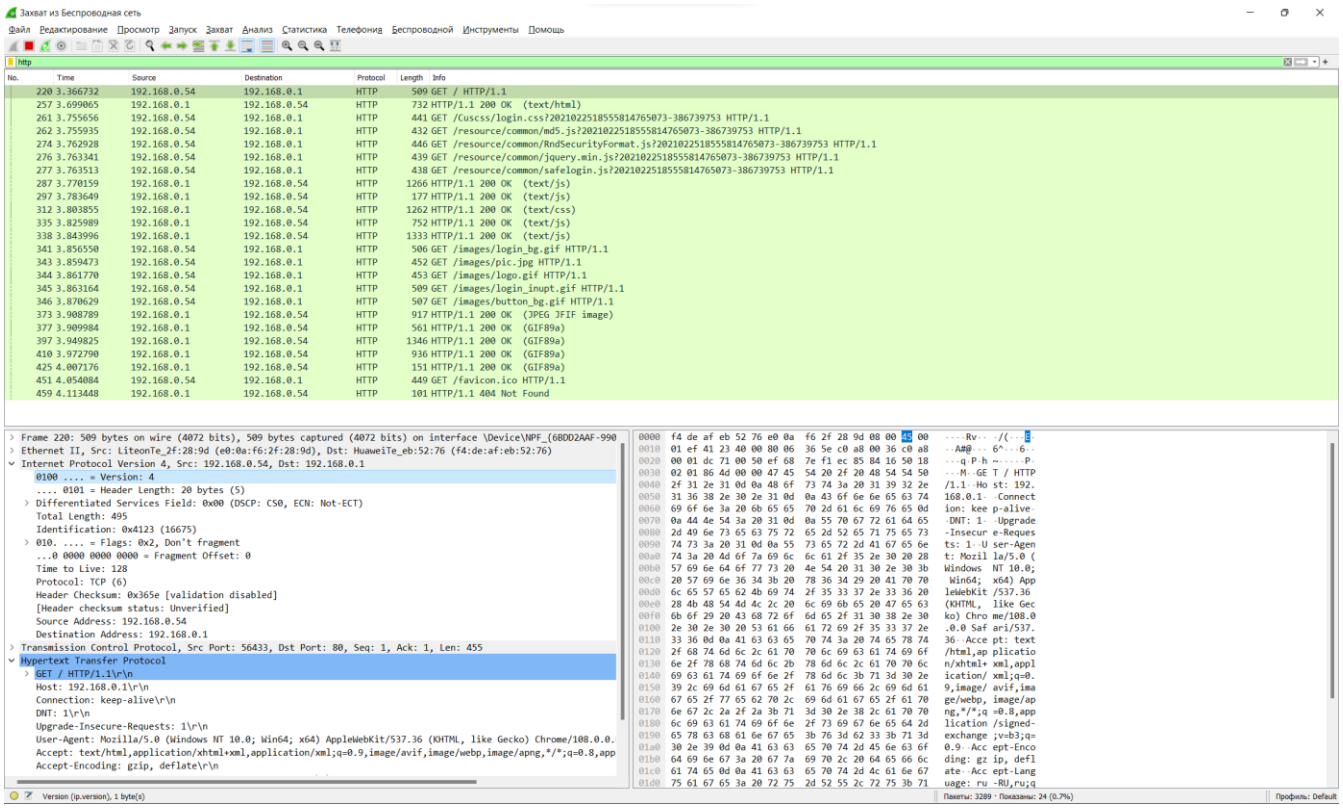
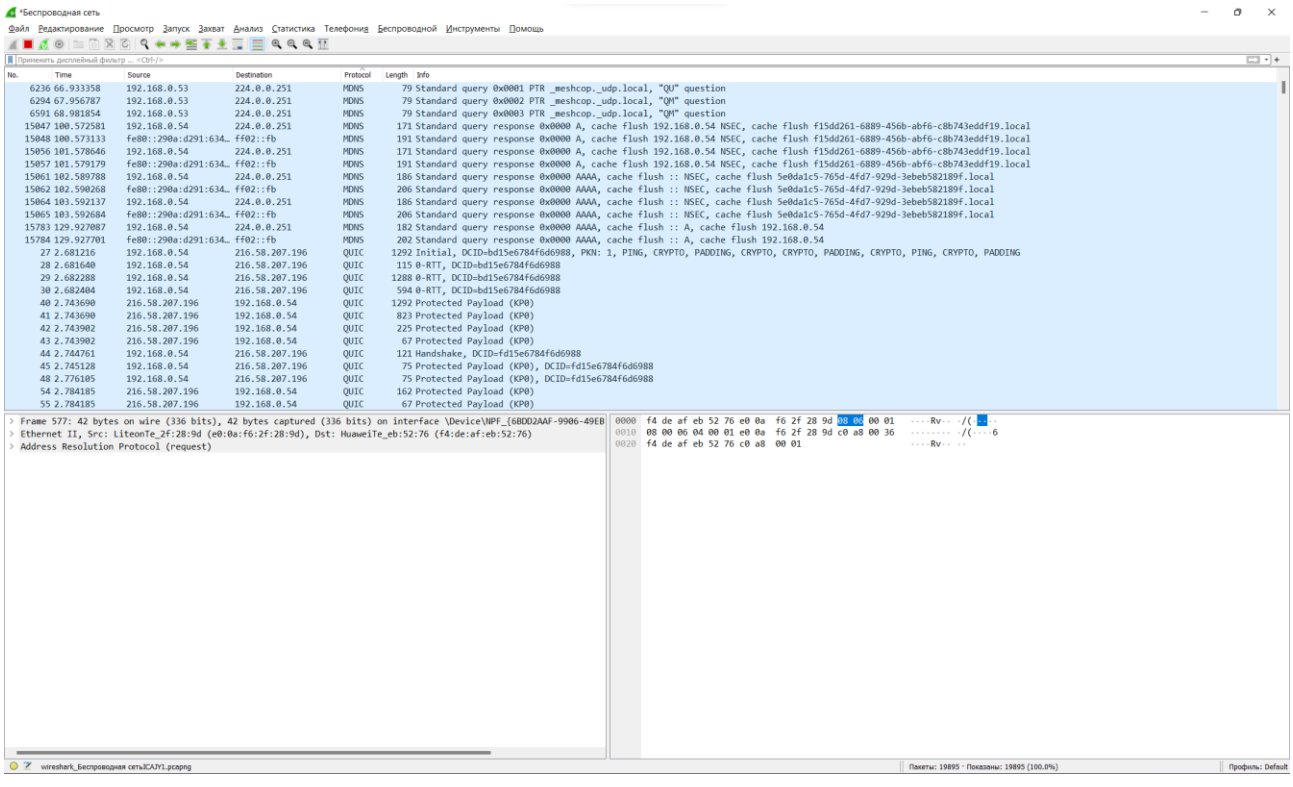
Собинин Егор Яковлевич 3 курс ИВТ1(2)

С помощьюй программы Wireshark исследуем сетевую активность. Можно найти некоторое количество HTTP запросов. Эти запросы, вероятно, делались в управление роутером.

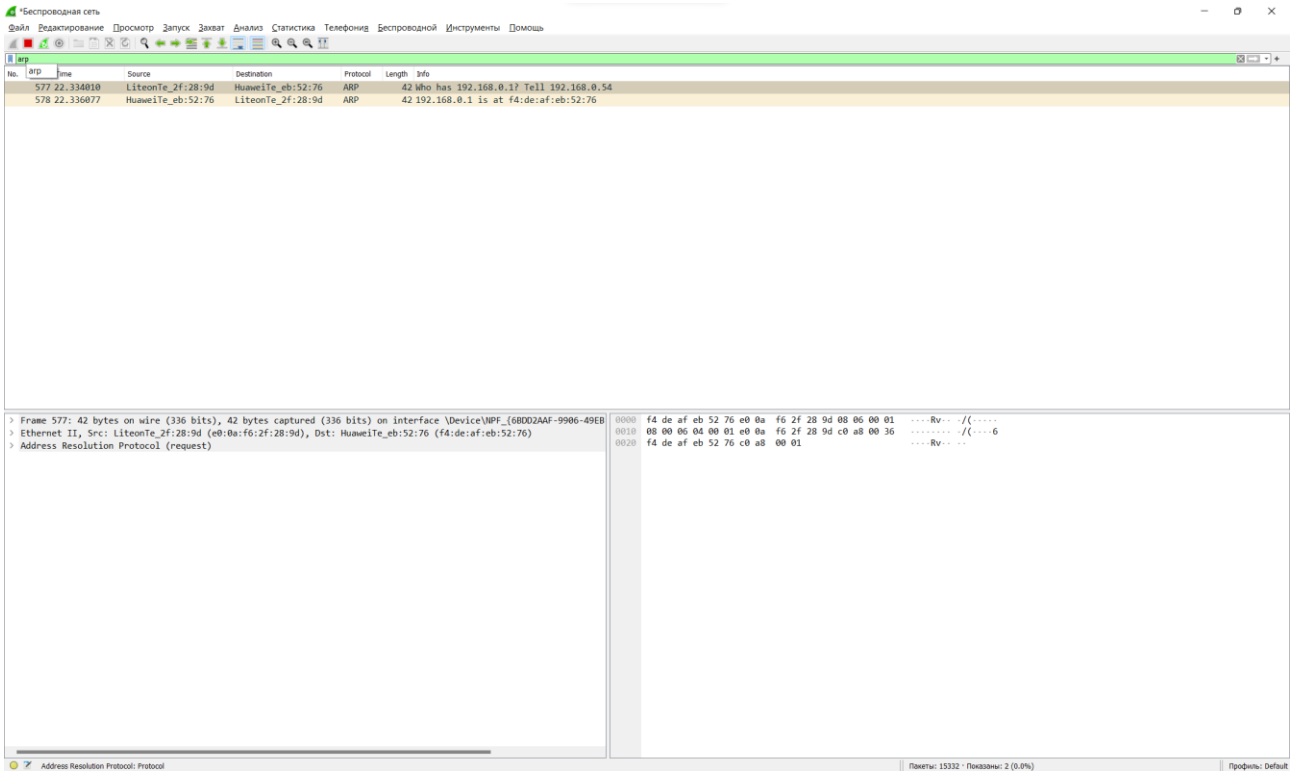


Кроме того, было найдено много записей с протоколом QUIC. По интернет запросу из активных сессий, вероятно, это общение с серверами ВКонтакте.

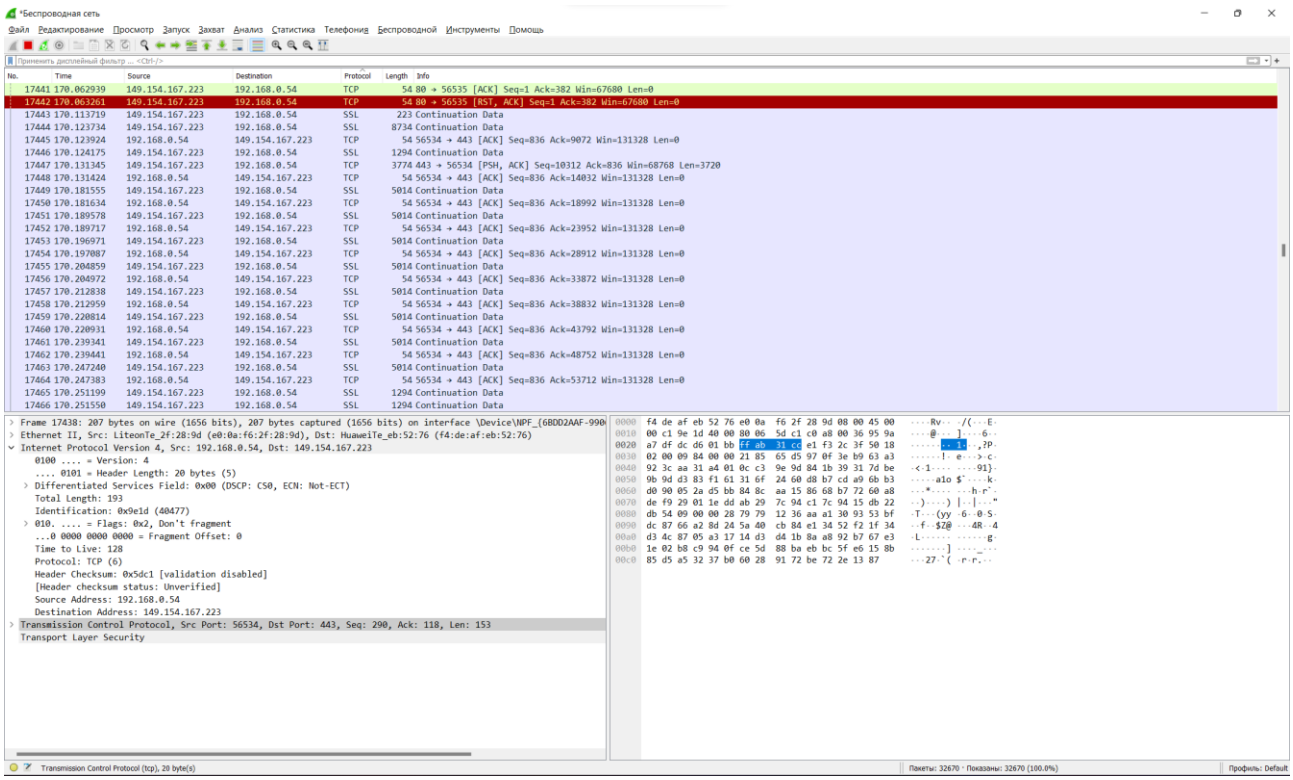


Собинин Егор Яковлевич 3 курс ИВТ1(2)

Так же были замечены 2 запроса по ARP протоколу. Судя по источнику и IP-адресу, это роутер.



Общение через TCP и SSL судя по IP-адресам происходит с серверами Telegram.



Собинин Егор Яковлевич 3 курс ИВТ1(2)

Сделав POST запрос по протоколу HTTP к административной панели роутера мы отправляем логин администратора и пароль. Средствами WireShark, а именно «Следовать» -> «Поток TCP» можно найти логин и хеш-код пароля

```
POST /login.cgi HTTP/1.1
Host: 192.168.0.1
Connection: keep-alive
Content-Length: 89
Cache-Control: max-age=0
Origin: http://192.168.0.1
DNT: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.1/
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: Cookie=body:Language:russian:id=-1

UserName=qqq&PassWord=cXFx&Language=russian&x.X_HW_Token=cd8ad20ade4182689d11436017efaa14HTTP/1.1 200 OK
Cache-control:no-cache, no-store, max-age=0
Content-Type:text/html
Content-Language:ru
Pragma:no-cache
Transfer-Encoding:chunked
X-Frame-Options:SAMEORIGIN
Connection:Keep-Alive
```

В крайней правой строке можно найти некоторые незашифрованные данные, что доказывает, что данные передавались в открытом виде. Кроме того, в той же строке указана версия HTTP.