Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Компьютерные сети»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2

«Анализ трафика компьютерных сетей утилитой Wireshark»

Выполнили:

Бардышев Артём Антонович,

студент группы N3346

(подпись)

Проверил:

Ярошевский Дмитрий Сергеевич,

Ведущий инженер, ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

Введение 4
1 Подготовка 5
2 Анализ полученных пакетов 6
2.1 DNS-запрос 6
2.2 TCP 7
2.3 TLS-Handshake 7
2.4 HTTP 8
2.5 ARP 8
2.6 ICMP 9
2.7 nslookup 9
3 Ответы на вопросы 11
3.1 Имеет ли место фрагментация исходного пакета? 11
3.2 Какая информация указывает, является ли фрагмент последним или промежуточным? 11
3.3 Чему равно количество фрагментов при передаче ping-пакетов? 11
3.4 Как изменить поле TTL? 11
3.5 Что содержится в поле данных ping-пакета? 12
3.6 Сколько байт в заголовке IP и в данных? 12
3.7 Как и почему изменяется TTL в последовательных ICMP-пакетах tracert? 12
3.8 Чем отличаются ICMP-пакеты tracert и ping? 12
3.9 Чем отличаются ICMP reply и ICMP error? 12
3.10 Что изменится, если убрать ключ -d? 13
3.11 Как выглядит HTTP-запрос и ответ? 13
3.12 Что означает строка состояния HTTP 200 OK? 13
3.13 Что происходит при повторном обращении к странице? 13
3.14 Почему адрес DNS-запроса не совпадает с адресом сайта? 13
3.15 Какие бывают типы DNS-запросов? 13
3.16 Почему браузер делает дополнительные DNS-запросы? 14
3.17 Какие MAC-адреса есть в ARP-пакетах и что они означают? 14
3.18 Почему в ARP-запросе указан IP-адрес источника? 14
3.19 Чем различаются DNS-запросы типа A и NS? 14
3.20 Что содержится в поле “Answers” DNS-ответа? 14

3.21 Является ли ответ DNS-сервера авторитативным? 15
3.22 Почему адрес DNS-сервера отличается от адреса сайта? 15
3.23 Что содержится в поле “Authority” DNS-ответа? 15
3.24 Что произойдёт, если очистить ARP-кэш? 15
Заключение 16
Список использованных источников 17

ВВЕДЕНИЕ

Цель работы – Изучить структуру протокольных блоков данных (PDU), проанализировав реальный сетевой трафик на своём компьютере при помощи Wireshark.

В процессе выполнения учебно-исследовательской работы (УИР) необходимо: − Освоить базовые навыки работы с анализатором трафика Wireshark: захват, фильтрация и анализ пакетов. − Исследовать работу служебных протоколов ICMP, DNS и ARP на примере системных утилит ping, tracert и nslookup.

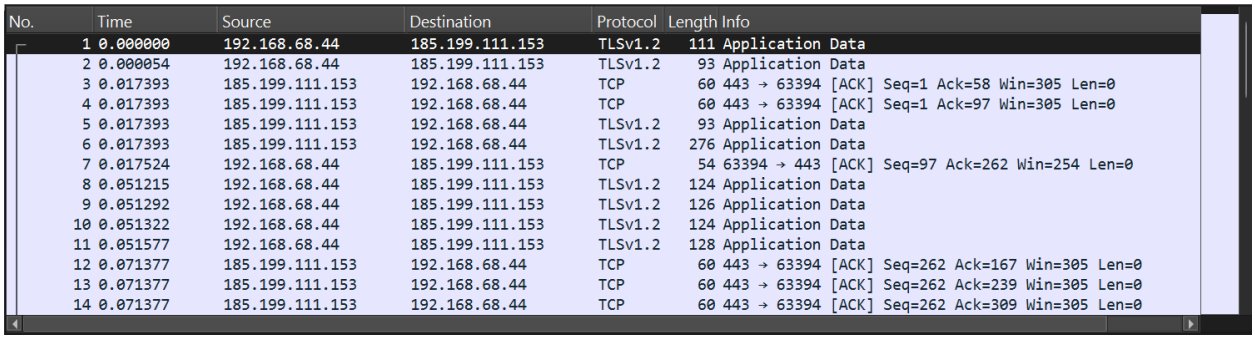
1 ПОДГОТОВКА

Устанавливаем Wireshark, настраиваем фильтр захвата

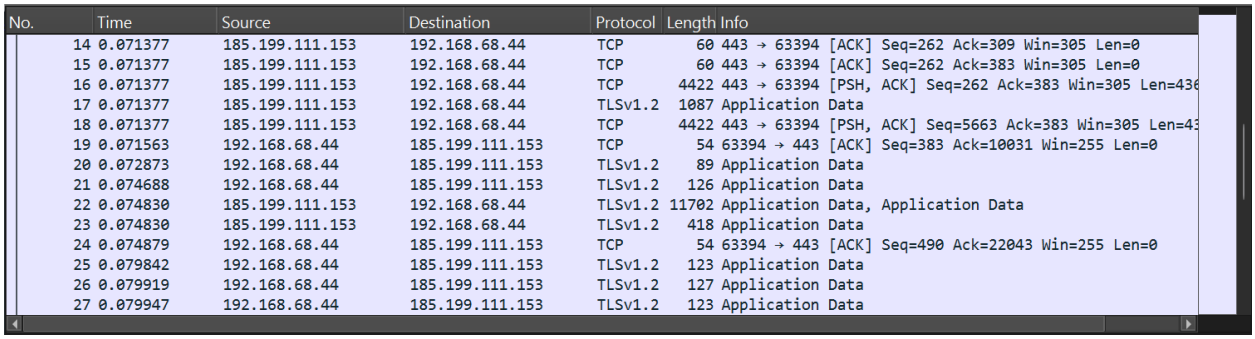
host baatraining.com (т.к. для анализа было решено взять сайт содержащий мои инициалы – Бардышев Артём Антонович baatraining.com)

Выбираем активный интерфейс – беспроводная сеть

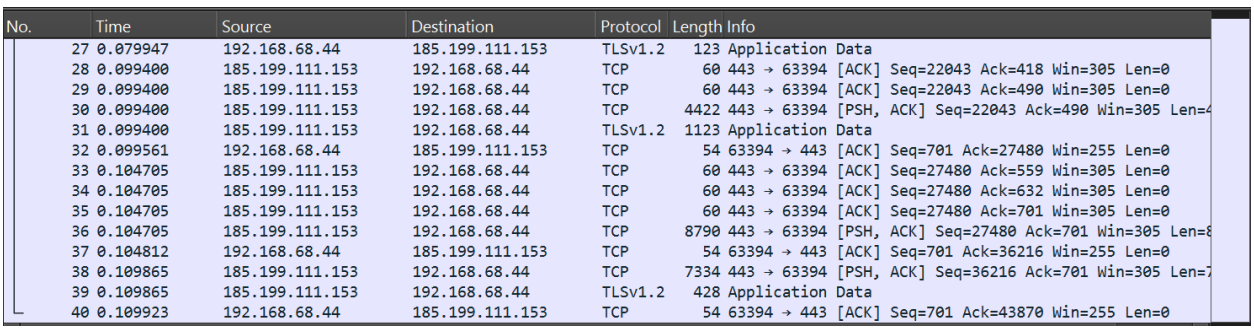
При запуске захвата открываем сайт в браузере, как только страница загрузится полностью захват можно останавливать.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.68.44	185.199.111.153	TLSv1.2	111	Application Data
2	0.000054	192.168.68.44	185.199.111.153	TLSv1.2	93	Application Data
3	0.017393	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=1 Ack=58 Win=305 Len=0
4	0.017393	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=1 Ack=97 Win=305 Len=0
5	0.017393	185.199.111.153	192.168.68.44	TLSv1.2	93	Application Data
6	0.017393	185.199.111.153	192.168.68.44	TLSv1.2	276	Application Data
7	0.017524	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=97 Ack=262 Win=254 Len=0
8	0.051215	192.168.68.44	185.199.111.153	TLSv1.2	124	Application Data
9	0.051292	192.168.68.44	185.199.111.153	TLSv1.2	126	Application Data
10	0.051322	192.168.68.44	185.199.111.153	TLSv1.2	124	Application Data
11	0.051577	192.168.68.44	185.199.111.153	TLSv1.2	128	Application Data
12	0.071377	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=262 Ack=167 Win=305 Len=0
13	0.071377	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=262 Ack=239 Win=305 Len=0
14	0.071377	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=262 Ack=309 Win=305 Len=0



No.	Time	Source	Destination	Protocol	Length	Info
14	0.071377	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=262 Ack=309 Win=305 Len=0
15	0.071377	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=262 Ack=383 Win=305 Len=0
16	0.071377	185.199.111.153	192.168.68.44	TCP	4422	443 → 63394 [PSH, ACK] Seq=262 Ack=383 Win=305 Len=436
17	0.071377	185.199.111.153	192.168.68.44	TLSv1.2	1087	Application Data
18	0.071377	185.199.111.153	192.168.68.44	TCP	4422	443 → 63394 [PSH, ACK] Seq=5663 Ack=383 Win=305 Len=43
19	0.071563	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=383 Ack=10031 Win=255 Len=0
20	0.072873	192.168.68.44	185.199.111.153	TLSv1.2	89	Application Data
21	0.074688	192.168.68.44	185.199.111.153	TLSv1.2	126	Application Data
22	0.074830	185.199.111.153	192.168.68.44	TLSv1.2	11702	Application Data, Application Data
23	0.074830	185.199.111.153	192.168.68.44	TLSv1.2	418	Application Data
24	0.074879	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=490 Ack=22043 Win=255 Len=0
25	0.079842	192.168.68.44	185.199.111.153	TLSv1.2	123	Application Data
26	0.079919	192.168.68.44	185.199.111.153	TLSv1.2	127	Application Data
27	0.079947	192.168.68.44	185.199.111.153	TLSv1.2	123	Application Data



No.	Time	Source	Destination	Protocol	Length	Info
27	0.079947	192.168.68.44	185.199.111.153	TLSv1.2	123	Application Data
28	0.099400	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=22043 Ack=418 Win=305 Len=0
29	0.099400	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=22043 Ack=490 Win=305 Len=0
30	0.099400	185.199.111.153	192.168.68.44	TCP	4422	443 → 63394 [PSH, ACK] Seq=22043 Ack=490 Win=305 Len=4
31	0.099400	185.199.111.153	192.168.68.44	TLSv1.2	1123	Application Data
32	0.099561	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=701 Ack=27480 Win=255 Len=0
33	0.104705	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=27480 Ack=559 Win=305 Len=0
34	0.104705	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=27480 Ack=632 Win=305 Len=0
35	0.104705	185.199.111.153	192.168.68.44	TCP	60	443 → 63394 [ACK] Seq=27480 Ack=701 Win=305 Len=0
36	0.104705	185.199.111.153	192.168.68.44	TCP	8790	443 → 63394 [PSH, ACK] Seq=27480 Ack=701 Win=305 Len=8
37	0.104812	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=701 Ack=36216 Win=255 Len=0
38	0.109865	185.199.111.153	192.168.68.44	TCP	7334	443 → 63394 [PSH, ACK] Seq=36216 Ack=701 Win=305 Len=7
39	0.109865	185.199.111.153	192.168.68.44	TLSv1.2	428	Application Data
40	0.109923	192.168.68.44	185.199.111.153	TCP	54	63394 → 443 [ACK] Seq=701 Ack=43870 Win=255 Len=0

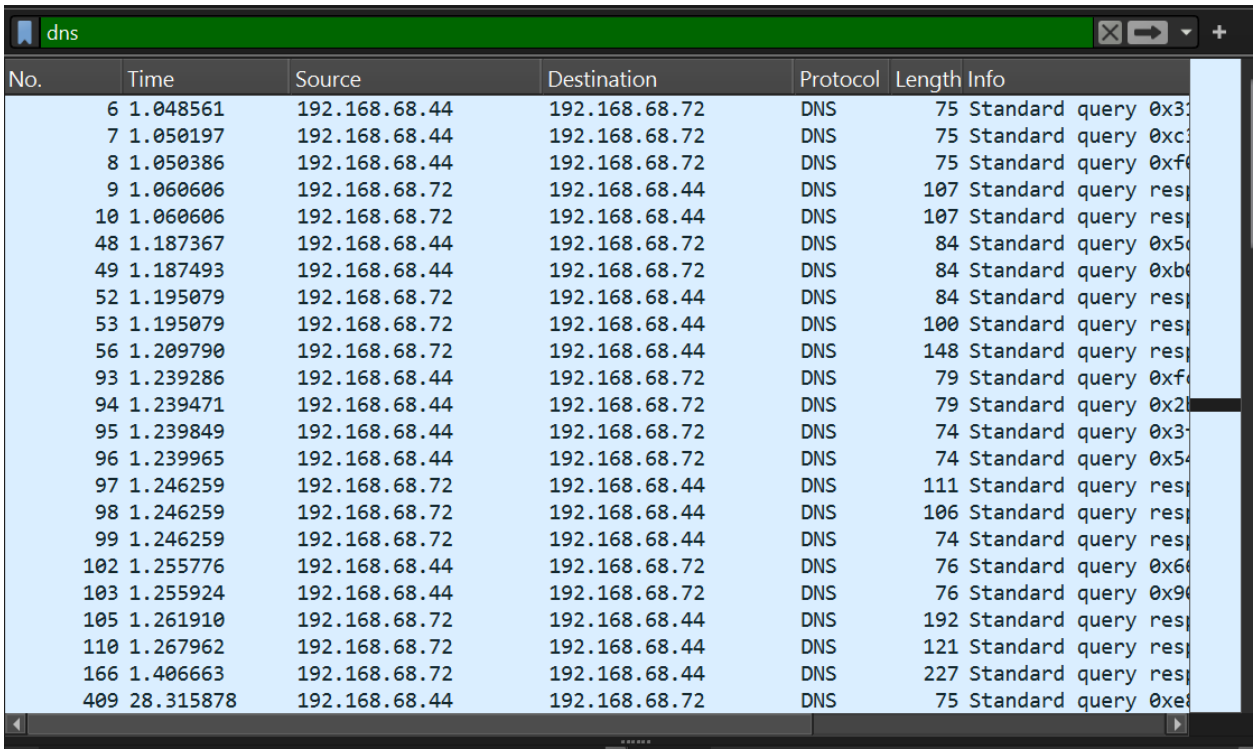
2 АНАЛИЗ ПОЛУЧЕННЫХ ПАКЕТОВ

Теперь нужно **разобрать типы пакетов**, которые появились в моем захвате.

2.1 DNS-запрос

В фильтре Wireshark вводим:

Dns

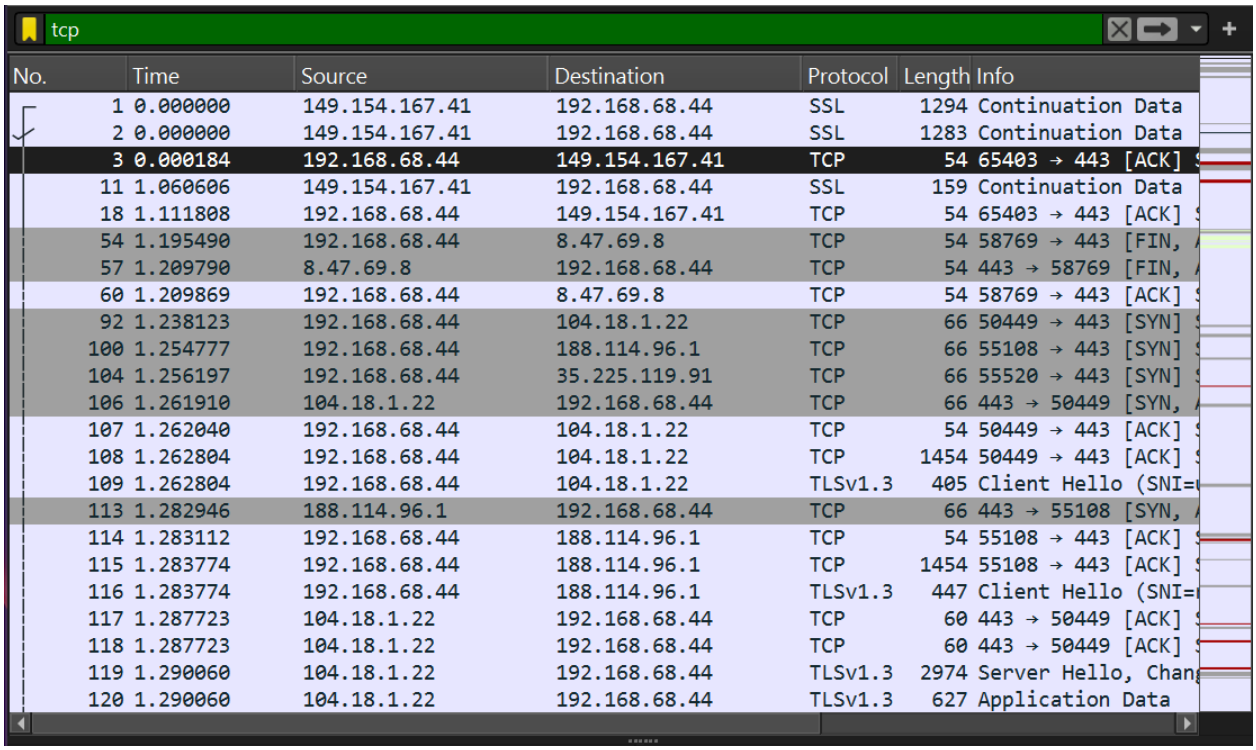


При обращении к сайту baatraining.com выполняется DNS запрос на получение IP – адреса, в запросе указан тип A (IPv4), в ответе возвращается ip адрес нужного сайта.

2.2 TCP

В фильтре Wireshark вводим:

tcp

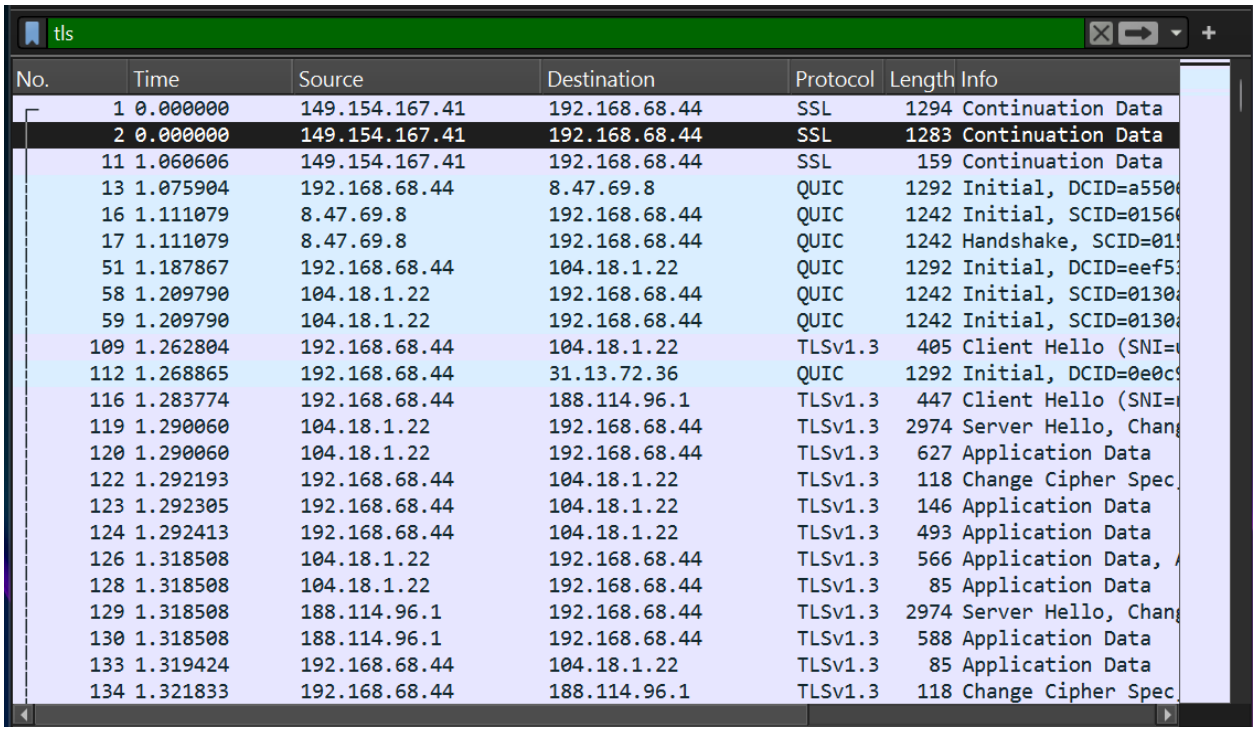


TCP – соединение устанавливается по стандартной трёхфазной схеме: клиент отправляет SYN, сервер отвечает SYN, если отправляется ACK, то и в ответ приходит ACK, таким образом устанавливается надежное соединение для дальнейшей передачи данных.

2.3 TLS-Handshake

В фильтре Wireshark вводим:

tls



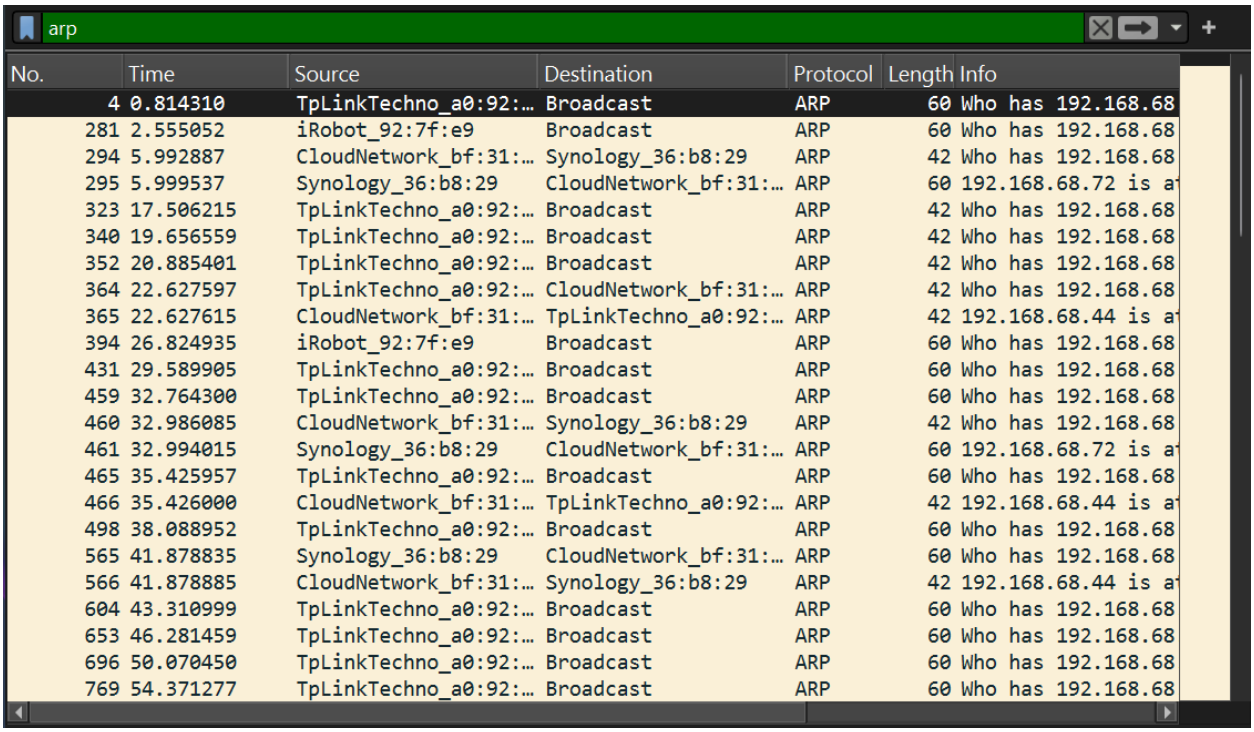
После установления TCP-соединения начинается TLS-рукопожатие, в ходе которого клиент и сервер договариваются о параметрах шифрования. Сервер передает сертификат подвтерждающий подлинность сайта.

2.4 HTTP

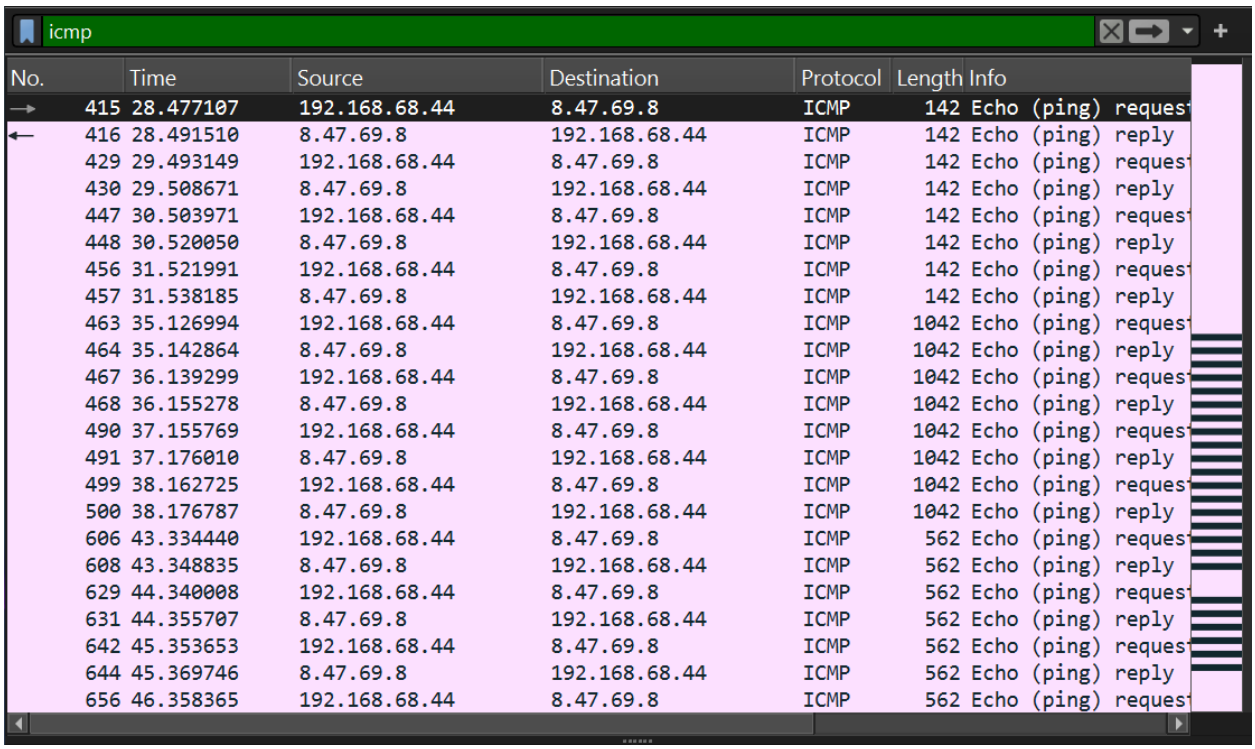
Клиент отправляет запрос GET /, сервер отвечает HTTP/1.1 200 OK, это означает что сейчас будет открыта HTML страница и соединение установлено успешно, так же в этот момент передаются вспомогательные файлы css, js, изображения.

2.5 ARP

ARP используется для определения физического MAC адресаустройства в локальной сети.
Клиент отправляет запрос: Кто имеет IP-адресс шлюза?
Приходит ответ с MAC-адресом маршрутизатора.



2.6 ICMP



При увеличении размера ICMP-пакета наблюдается фрагментация IP-датаграмм. Максимальный размер без фрагментации – 1500 байт

2.7 nslookup

в командной строке выполняем команды:

nslookup baatraining.com

nslookup -type=NS baatraining.com

- При выполнении первой команды nslookup baatraining.com был отправлен запрос **типа A** (Address), предназначенный для получения IPv4-адреса веб-сайта.
  В ответе от DNS-сервера были получены записи:
  Name: baatraining.com
  Address: 104.26.7.125
  Address: 104.26.6.125
  Эти IP-адреса принадлежат инфраструктуре Cloudflare, через которую обслуживается сайт.
- При выполнении второй команды nslookup -type=NS baatraining.com был отправлен запрос **типа NS** (Name Server), возвращающий список авторитативных DNS-серверов домена.
  В ответ были получены записи:
  baatraining.com nameserver = ray.ns.cloudflare.com
  baatraining.com nameserver = dawn.ns.cloudflare.com
  В заголовке DNS-пакетов в Wireshark видно:
  Source IP: IP-адрес моего компьютера (например, 192.168.0.102)
  Destination IP: адрес DNS-сервера (например, 192.168.0.1 — локальный маршрутизатор)
  Protocol: UDP
  Destination Port: 53

3 ОТВЕТЫ НА ВОПРОСЫ

3.1 Имеет ли место фрагментация исходного пакета?

Да, фрагментация возникает, когда размер пакета превышает **MTU (Maximum Transmission Unit)**, обычно равный 1500 байт.

Пакеты ping -l 100 и ping -l 1000 проходят без фрагментации,

а начиная с ping -l 2000 пакет разбивается на несколько частей.

На фрагментацию указывают поля:

- Flags: More fragments = 1 — пакет не последний;
- Fragment offset > 0 — смещение следующего фрагмента.

3.2 Какая информация указывает, является ли фрагмент последним или промежуточным?

Поле **More Fragments** в заголовке IP.

- Если Set, значит фрагмент **промежуточный**.
- Если Not set, но Offset > 0 — это **последний** фрагмент.

3.3 Чему равно количество фрагментов при передаче ping-пакетов?

Пример расчёта при MTU = 1500 байт:

(1480 — полезная нагрузка на фрагмент)

Размер пакета – кол-во фрагментов

100 – 1

1000 – 1

2000 – 2

4000 – 3

8000 – 6

3.4 Как изменить поле TTL?

Команда:

```
ping -i <значение> baatraining.com
```

Например:

```
ping -i 10 baatraining.com
```

установит TTL = 10.

3.5 Что содержится в поле данных ping-пакета?

В Windows по умолчанию поле данных содержит повторяющуюся последовательность символов латинского алфавита (ASCII):

```
abcdefghijklmnopqrstuvwabcdefghi...
```

которая заполняет пространство до указанного размера пакета.

3.6 Сколько байт в заголовке IP и в данных?

- **Заголовок IP:** 20 байт (без опций).
- **Поле данных:** 64 байта (в ICMP Echo Request).

3.7 Как и почему изменяется TTL в последовательных ICMP-пакетах tracert?

tracert отправляет серию пакетов с TTL = 1, 2, 3…

Каждый маршрутизатор уменьшает TTL на единицу.

Когда TTL = 0, маршрутизатор отбрасывает пакет и отправляет обратно ICMP-сообщение

Time to live exceeded.

Это позволяет определить IP каждого промежуточного узла.

3.8 Чем отличаются ICMP-пакеты tracert и ping?

- **ping** использует фиксированный TTL (обычно 128) и ждёт `Echo Reply`.

- **tracert** искусственно снижает TTL (1, 2, 3 …), чтобы получить от каждого маршрутизатора `Time Exceeded`.

Обе утилиты используют ICMP, но цели разные: ping проверяет доступность, tracert строит маршрут.

3.9 Чем отличаются ICMP reply и ICMP error?

- **ICMP Reply** (`Echo Reply`, тип 0) — нормальный ответ от конечного хоста.

- **ICMP Error** (`Time Exceeded`, тип 11) — сообщает, что TTL пакета истёк на промежуточном узле.

Tracert использует **оба** типа ответов: первые показывают маршрут, последний — достижение цели.

3.10 Что изменится, если убрать ключ -d?

Tracert начнёт отправлять **обратные DNS-запросы** (PTR-записи),
чтобы узнать доменные имена маршрутизаторов по их IP.
Это создаст дополнительный **DNS-трафик**.

3.11 Как выглядит HTTP-запрос и ответ?

Видна последовательность:

```
Client Hello → Server Hello → Certificate → Encrypted Application Data
```

Обычных строк `GET` и `HTTP/1.1 200 OK` нет, так как данные шифруются.

3.12 Что означает строка состояния HTTP 200 OK?

Эта строка указывает, что запрос клиента успешно обработан,
и сервер отправил содержимое страницы.
(Если бы сайт использовал HTTP, а не HTTPS, в Wireshark было бы видно
HTTP/1.1 200 OK.)

3.13 Что происходит при повторном обращении к странице?

Браузер использует **кэш**.
Если данные не изменились, отправляется **Conditional GET** с заголовком:

```
If-Modified-Since: <дата>
```

Сервер отвечает:

```
304 Not Modified
```

и страница берётся из кэша.

3.14 Почему адрес DNS-запроса не совпадает с адресом сайта?

DNS-запрос идёт на **адрес DNS-сервера** (например, 192.168.0.1 или 8.8.8.8),
а не на сайт baatraining.com.
Клиент спрашивает у DNS-сервера: *«Какой IP у baatraining.com?»*,
а уже затем обращается к этому IP.

3.15 Какие бывают типы DNS-запросов?

- **A** — IPv4-адрес;

- **AAAA** — IPv6-адрес;
- **CNAME** — псевдоним;
- **NS** — имя авторитативного DNS-сервера.

Для сайта `baatraining.com` зафиксированы запросы типа **A** и **AAAA**.

3.16 Почему браузер делает дополнительные DNS-запросы?

Потому что страница сайта подгружает ресурсы (скрипты, картинки)
с других доменов (например, cdn.ba.com, static.cloudflare.com).
Каждый новый домен требует отдельного DNS-запроса.

3.17 Какие MAC-адреса есть в ARP-пакетах и что они означают?

- **Source MAC:** MAC твоего компьютера.
- **Destination MAC:** широковещательный (ff:ff:ff:ff:ff:ff) — в ARP Request.
- **Target MAC:** в ARP Reply — MAC твоего шлюза (роутера).

Таким образом, ARP определяет физический адрес устройства в локальной сети.

3.18 Почему в ARP-запросе указан IP-адрес источника?

Чтобы принимающее устройство знало, куда отправить ответ.
Например, твой компьютер указывает свой IP (192.168.x.x),
а роутер использует его, чтобы вернуть ARP-ответ напрямую

3.19 Чем различаются DNS-запросы типа A и NS?

Запрос типа **A** возвращает IP-адреса хоста (ресурсные записи с типом Address).
Запрос типа **NS** возвращает имена серверов, обслуживающих доменную зону.

3.20 Что содержится в поле “Answers” DNS-ответа?

В поле *Answers* содержатся ресурсные записи (Resource Records), запрошенные клиентом.
Для запроса типа A — это IP-адреса,
для типа NS — имена серверов зоны (ray.ns.cloudflare.com, dawn.ns.cloudflare.com).

3.21 Является ли ответ DNS-сервера авторитативным?

Нет, флаг Authoritative Answer (AA) в заголовке DNS-пакета **сброшен**,

что указывает на неавторитативный ответ.

Ответ предоставлен локальным кэширующим DNS-сервером (роутером).

3.22 Почему адрес DNS-сервера отличается от адреса сайта?

Потому что запрос направляется не на сам сайт, а на DNS-сервер, который выполняет разрешение имени в IP-адрес.
Сайт — это конечный ресурс, а DNS-сервер — посредник, выполняющий поиск IP по имени.

3.23 Что содержится в поле “Authority” DNS-ответа?

В поле *Authority* указаны авторитативные DNS-серверы,
ответственные за зону `baatraining.com` —
в нашем случае это **ray.ns.cloudflare.com** и **dawn.ns.cloudflare.com**.

3.24 Что произойдёт, если очистить ARP-кэш?

При следующем обращении к интернету компьютер не найдёт сохранённый MAC-адрес шлюза и **выполнит новый ARP-запрос**.
В Wireshark сразу появится пакет вида:

```
Who has 192.168.0.1? Tell 192.168.0.100
```

ЗАКЛЮЧЕНИЕ

В ходе работы была проведена запись и анализ сетевого трафика при обращении к веб-сайту baatraining.com

Были исследованы DNS-, TCP-, TLS-, HTTP- и ARP-пакеты, установлены их структура и взаимодействие.

Анализ показал, что передача данных осуществляется по модели TCP/IP, а шифрование выполняется с использованием протокола TLS 1.3.

Программа Wireshark позволяет детально изучить каждый уровень сетевой модели и выявить особенности обмена данными в Интернет.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алиев Т.И., Соснин В.В., Шинкарук Д.Н. Компьютерные сети и телекоммуникации: задания и тесты. – СПб: Университет ИТМО – 2018. – 112 с.

2. Куроуз Дж. Ф., Росс К. В. Компьютерные сети: Нисходящий подход / пер. с англ. – 6-е изд. – М.: Эксмо, 2016. – 912 с.