Московский Авиационный Институт

(Национальный Исследовательский Университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

**Курсовой проект по курсу**

**«Криптография»**

Студент: Почечура Артемий Андреевич

Группа: М80-306Б-20

Преподаватель: Борисов Август Валерьевич

Дата: 23.05.2023

Оценка:

Подпись: \_\_\_\_\_\_\_\_\_\_\_

Москва, 2023

**1. Выбор 5-ти веб-серверов различной организационной и государственной принадлежности**

Мною были выбраны следующие веб-сервисы:

* wildberries.ru
* terraria.fandom.com
* youtube.com
* hh.ru
* avito.ru

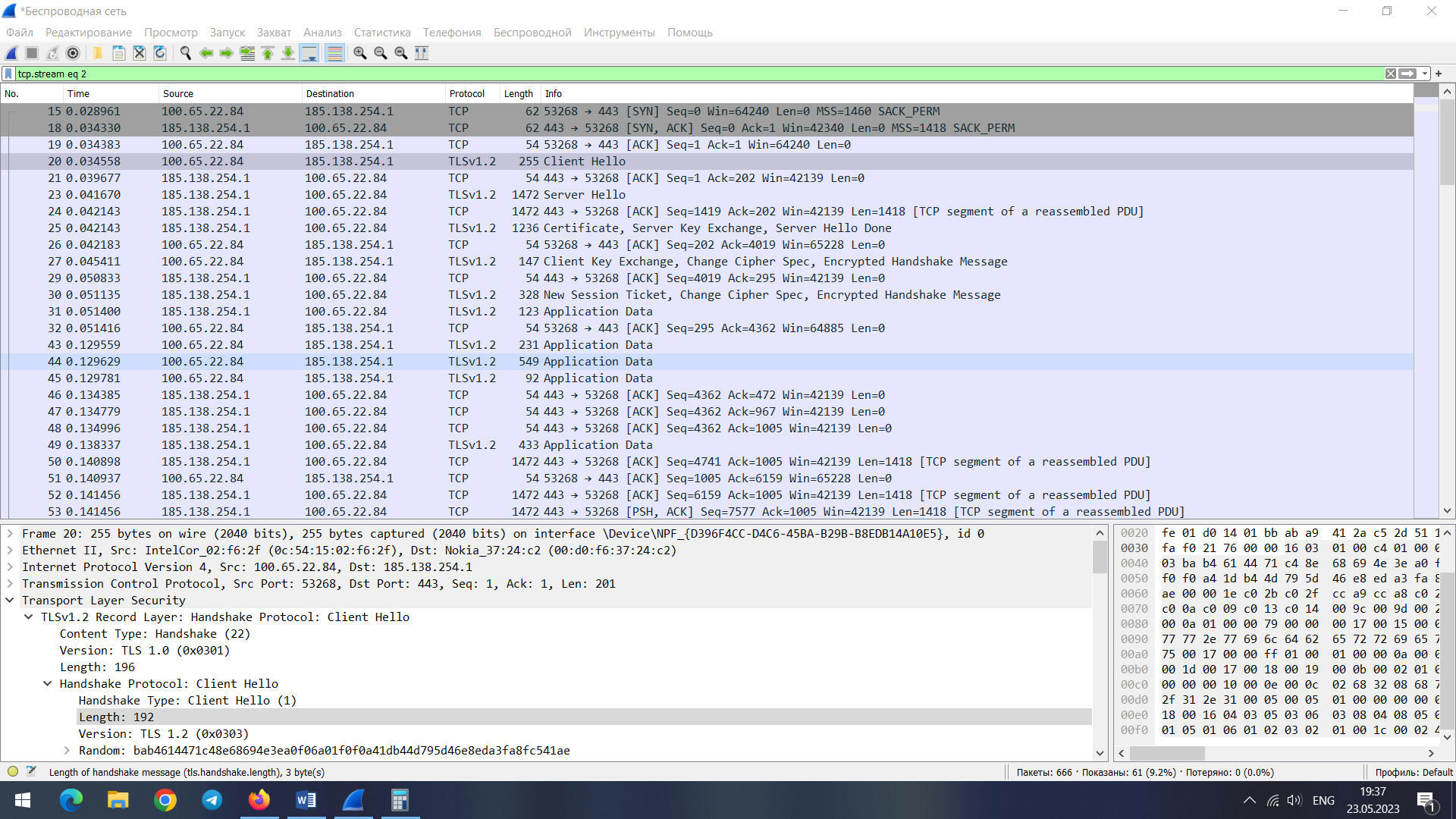
**2. Анализ соединения с выбранными серверами**

Для захвата трафика была использована программа Wireshark. Сам трафик захватывался из браузера Firefox. На нём можно легко менять минимальную и максимальную версии TLS, перейдя во вкладку about:config.

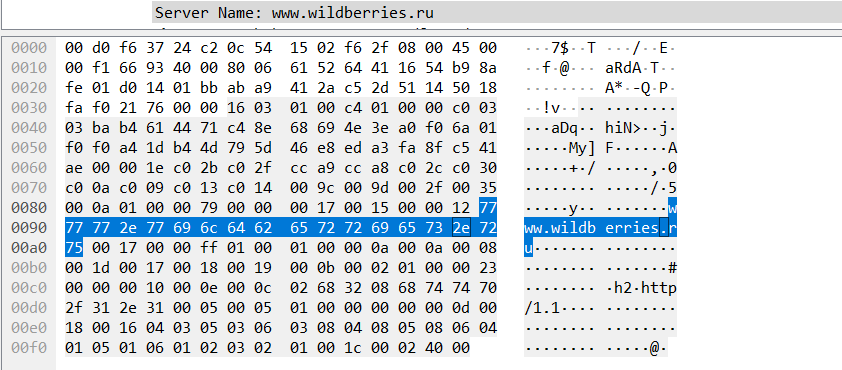
При работе с Wireshark лучше закрыть все посторонние приложения, так как их трафик может также захватываться, что усложнит поиск нужной нам информации.

Перейдём к самому анализу.

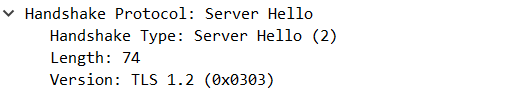
**1. Веб-сервер wildberries.ru**



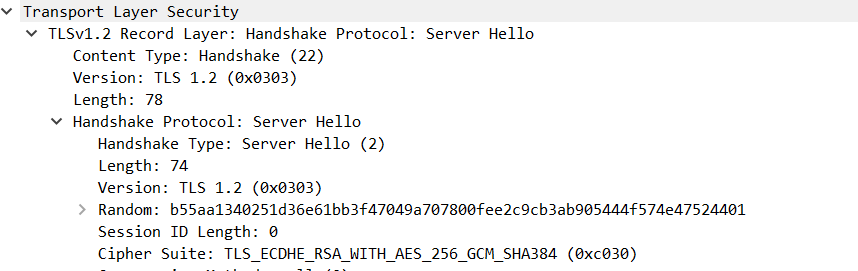
Имя серверабыло найдено в пакете Client hello**:**



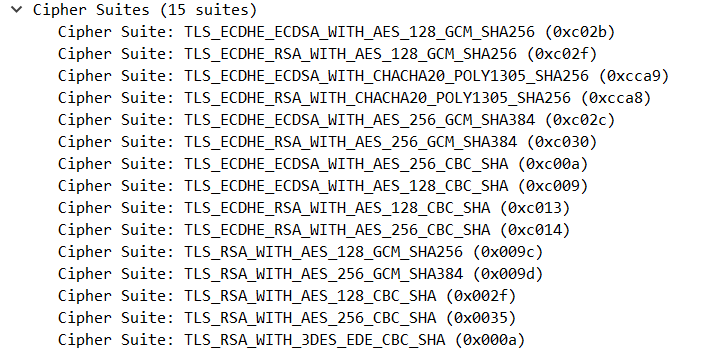
Версия TLS 1.2, информация была найдена в пакете Server Hello



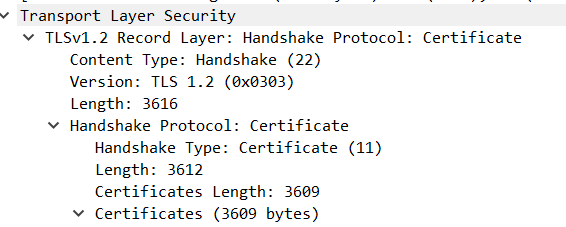
Для шифрования был выбран алгоритм Диффи-Хеллмана, информация также была найдена в Server Hello (Cipher Suite):



Информацию о всех возможных алгоритмах шифрования клиента, можно найти в Client hello:



Сертификат и его версия:



Валидность ключа и сертификата от/до:



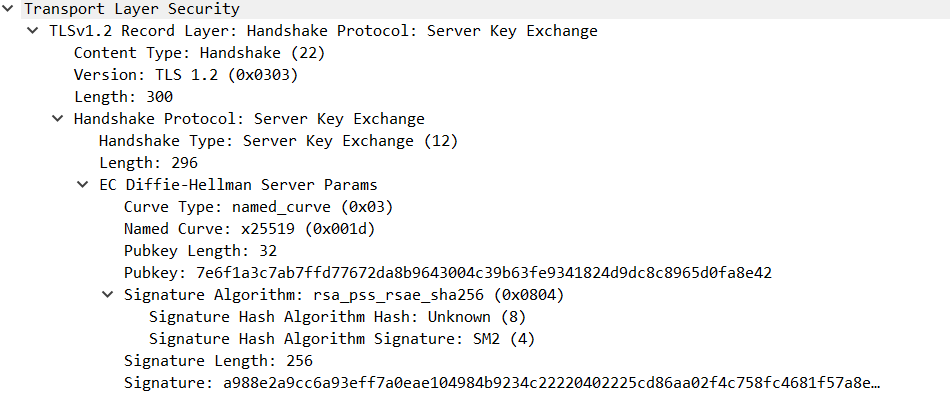
Организация, выдавшая сертификат:



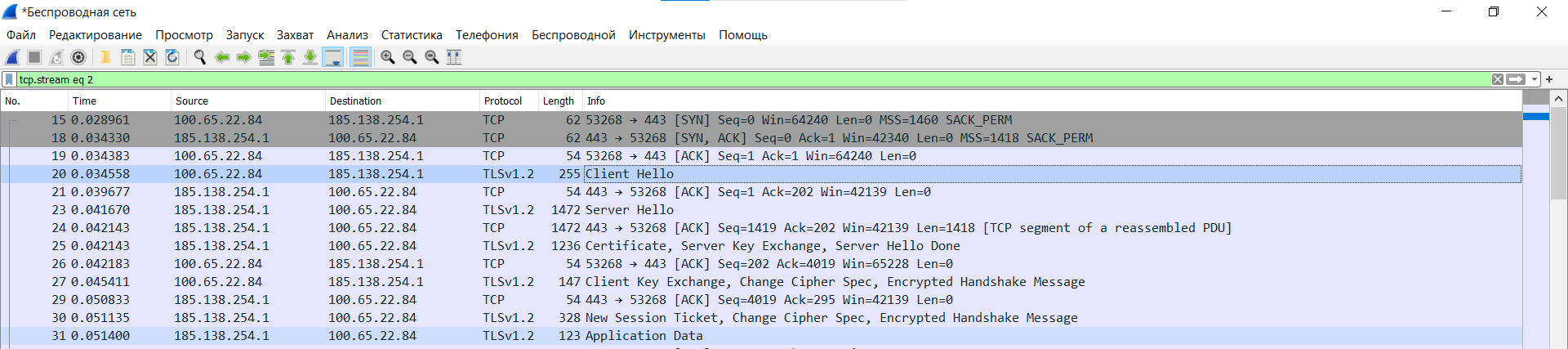
Статус сертификата для данного сервера не указан:



Информация о ключе:

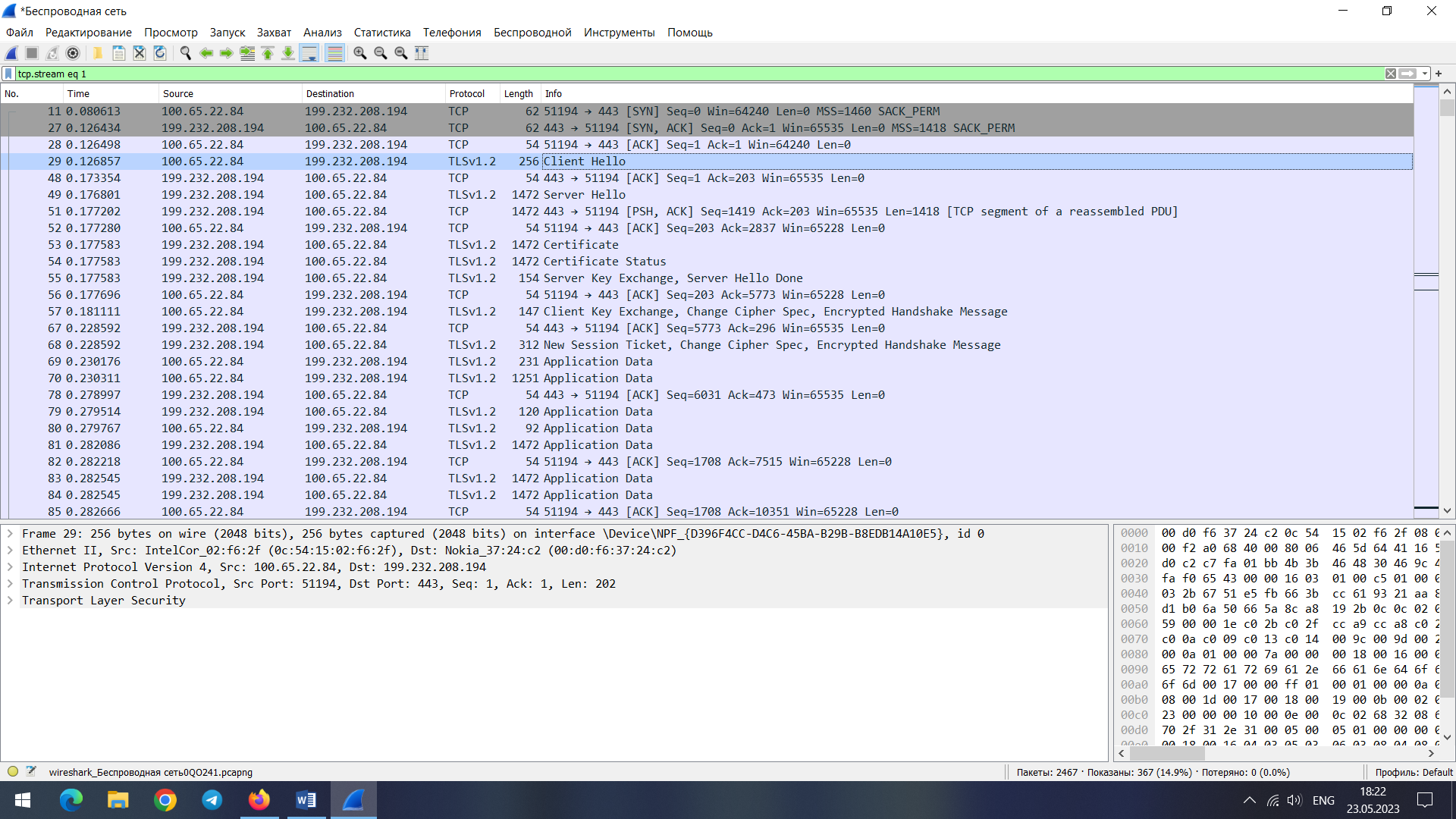


Время соединения считается как разность между Client Hello и первым переданным пакетом Application Data:

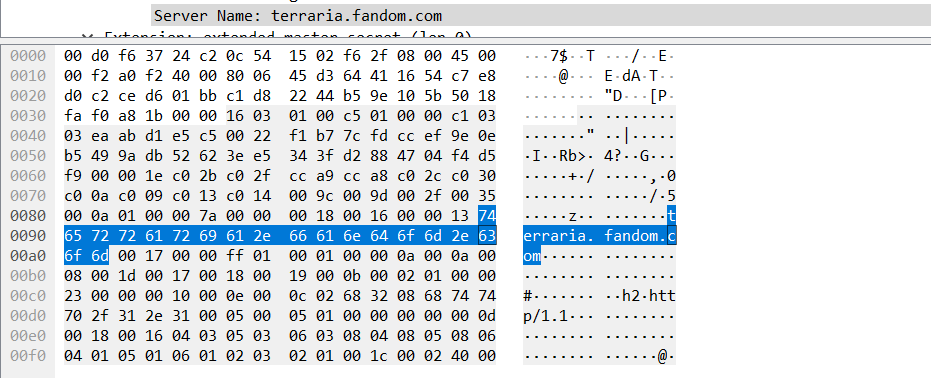


0,051400 – 0,034558 = 0,016842

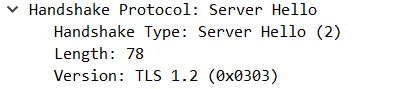
**2. Веб-сервер terraria.fandom.com**



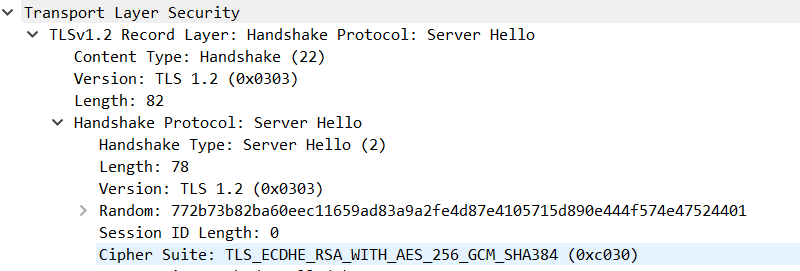
Имя серверабыло найдено в пакете Client hello**:**

****

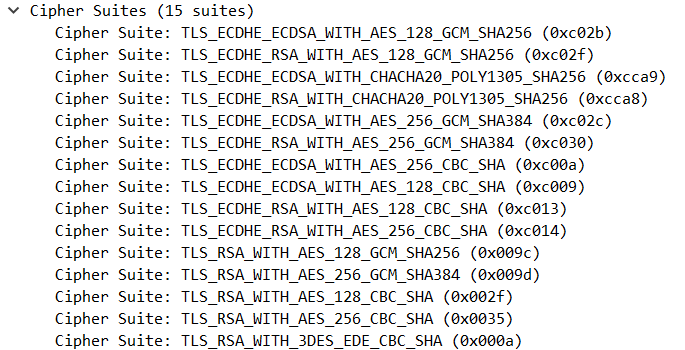
Версия TLS 1.2, информация была найдена в пакете Server Hello



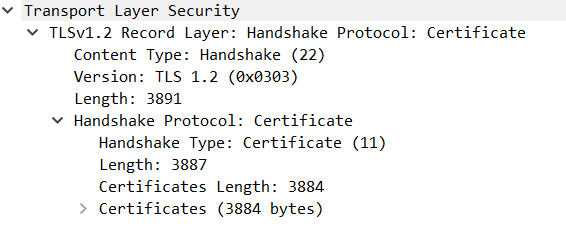
Для шифрования был выбран алгоритм Диффи-Хеллмана, информация также была найдена в Server Hello (Cipher Suite):



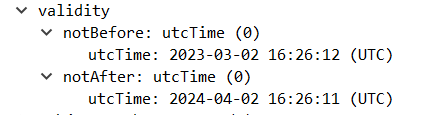
Информацию о всех возможных алгоритмах шифрования клиента, можно найти в Client hello:



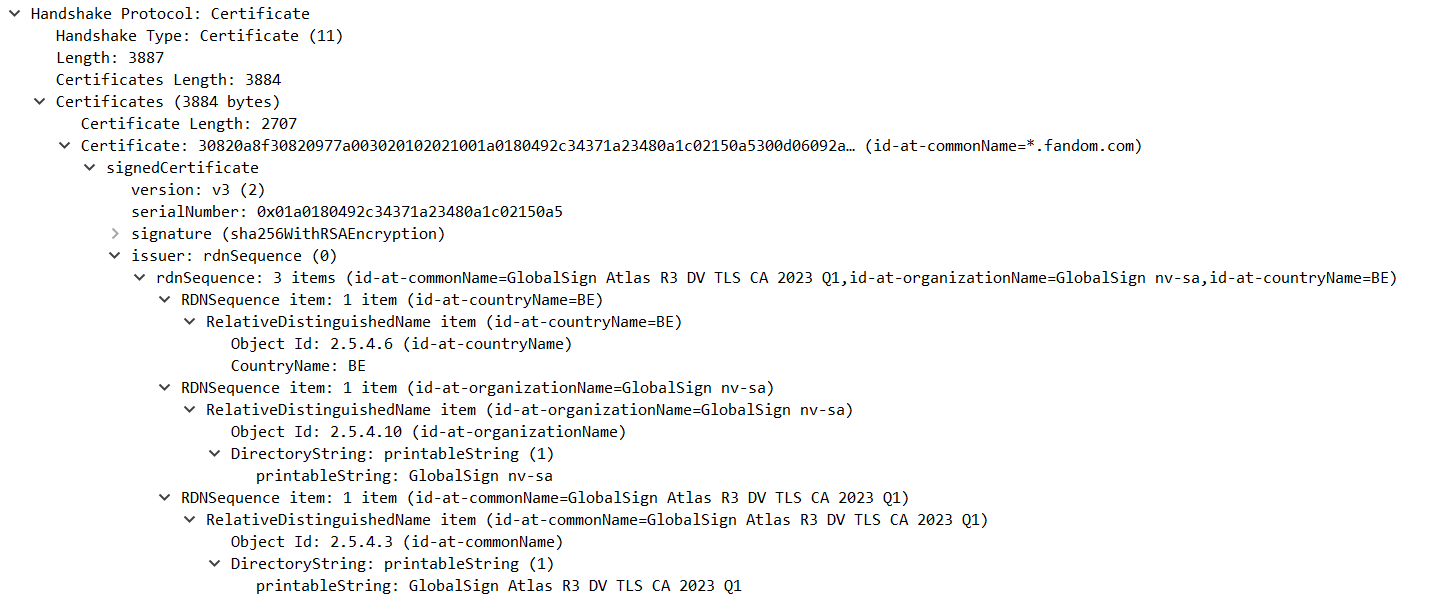
Сертификат и его версия:



Валидность ключа и сертификата от/до:



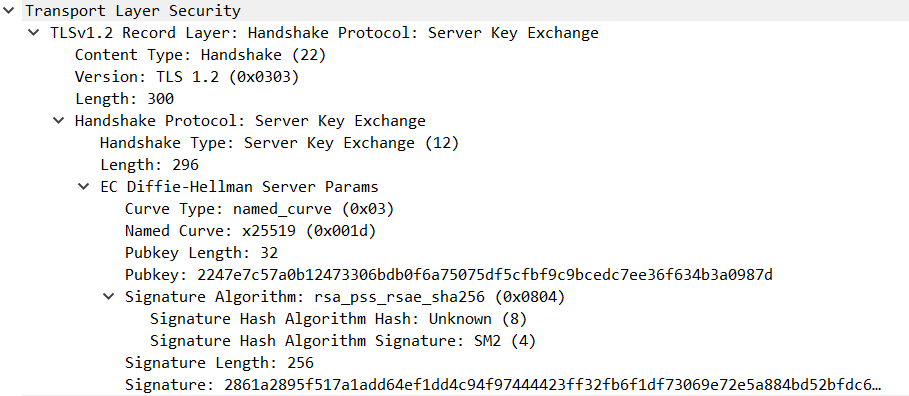
Организация, выдавшая сертификат:



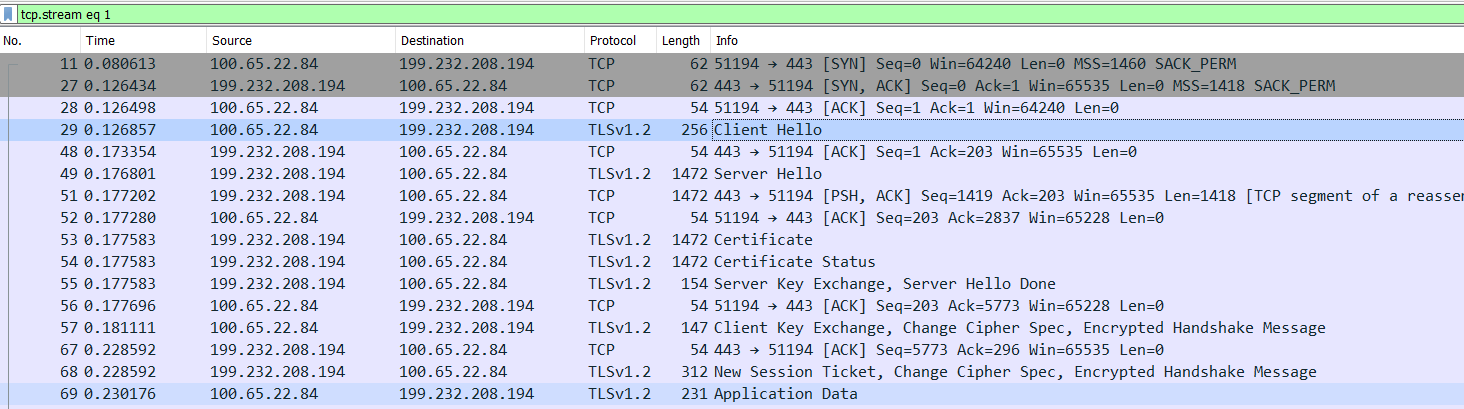
Статус сертификата:



Информация о ключе:

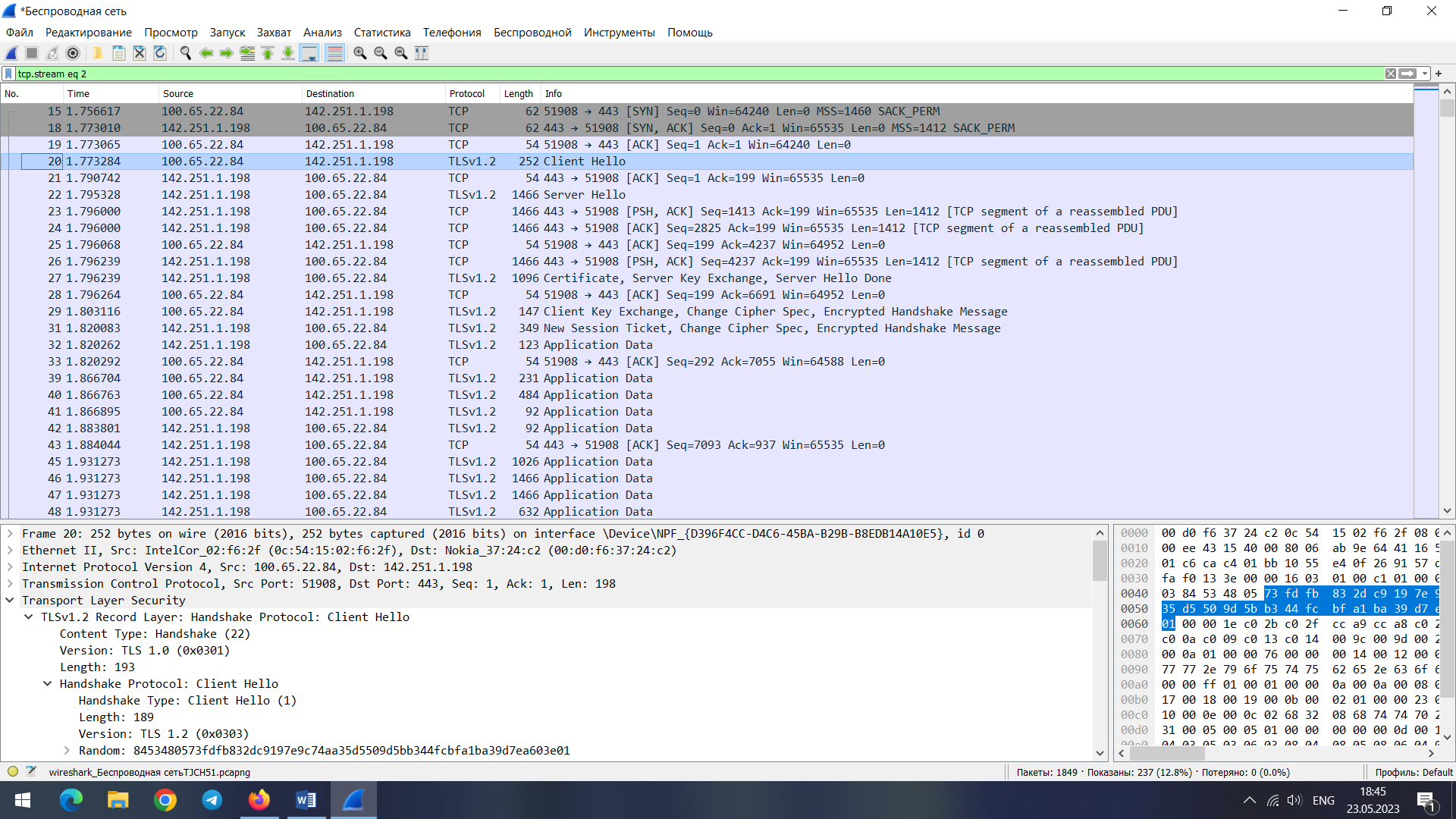


Время соединения считается как разность между Client Hello и первым переданным пакетом Application Data:

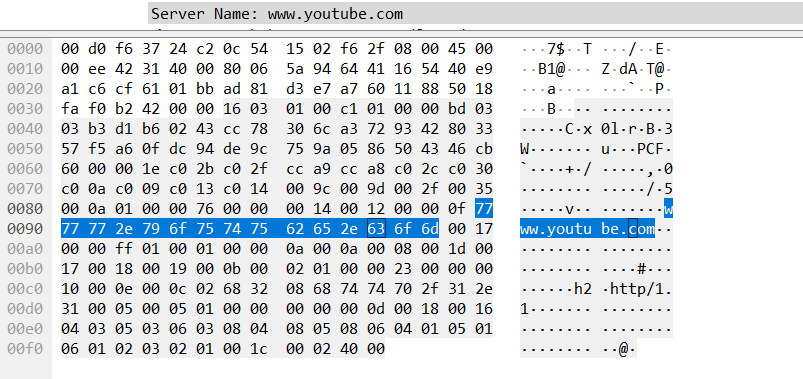


0,230176 – 0,126857 = 0,103319

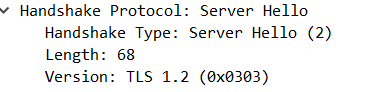
**3. Веб-сервер youtube.com**



Имя серверабыло найдено в пакете Client hello**:**

****

Версия TLS 1.2, информация была найдена в пакете Server Hello



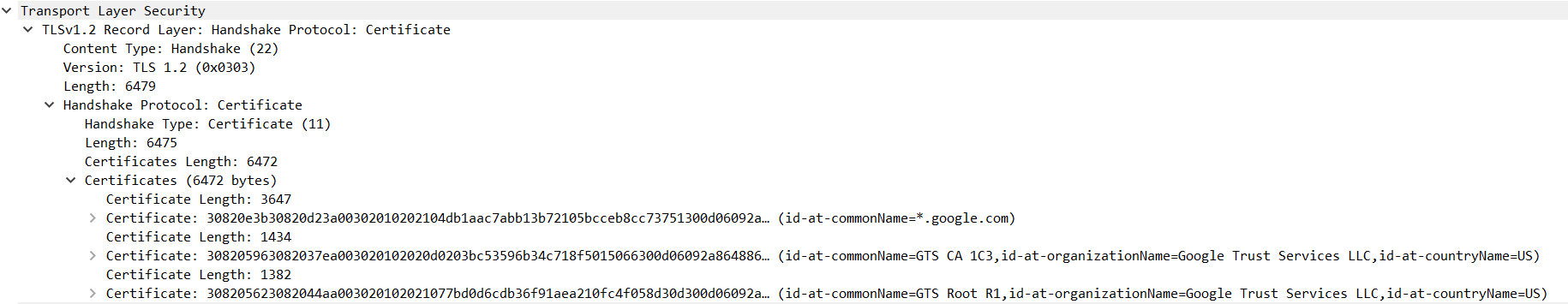
Для шифрования был выбран алгоритм Диффи-Хеллмана, информация также была найдена в Server Hello:



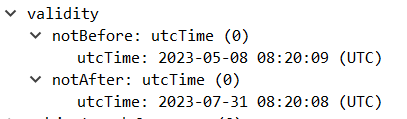
Информацию о всех возможных алгоритмах шифрования клиента, можно найти в Client hello:



Сертификат и его версия:



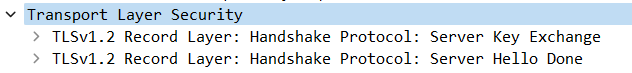
Валидность ключа и сертификата от/до:



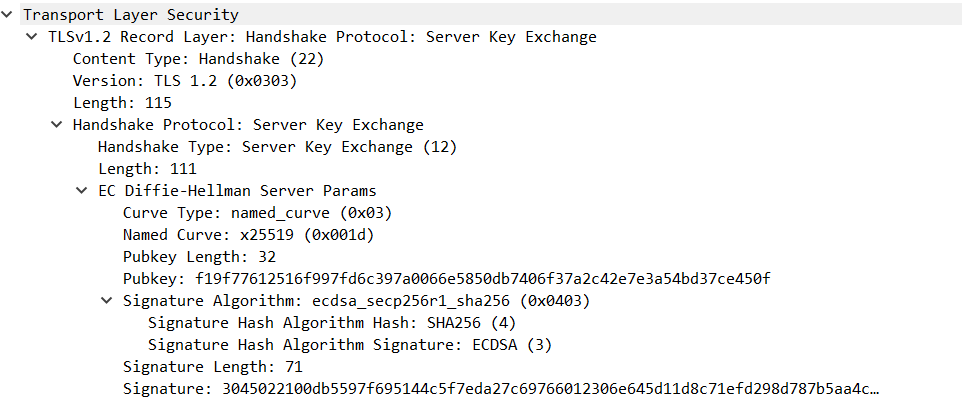
Организация, выдавшая сертификат:



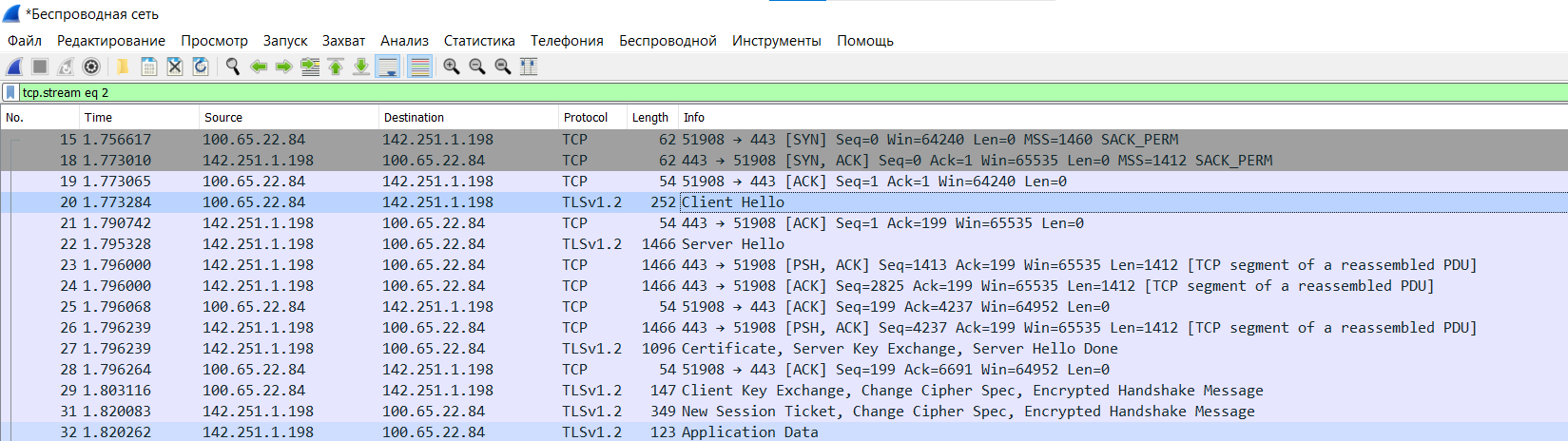
Статус сертификата для данного сервера не указан:



Информация о ключе:

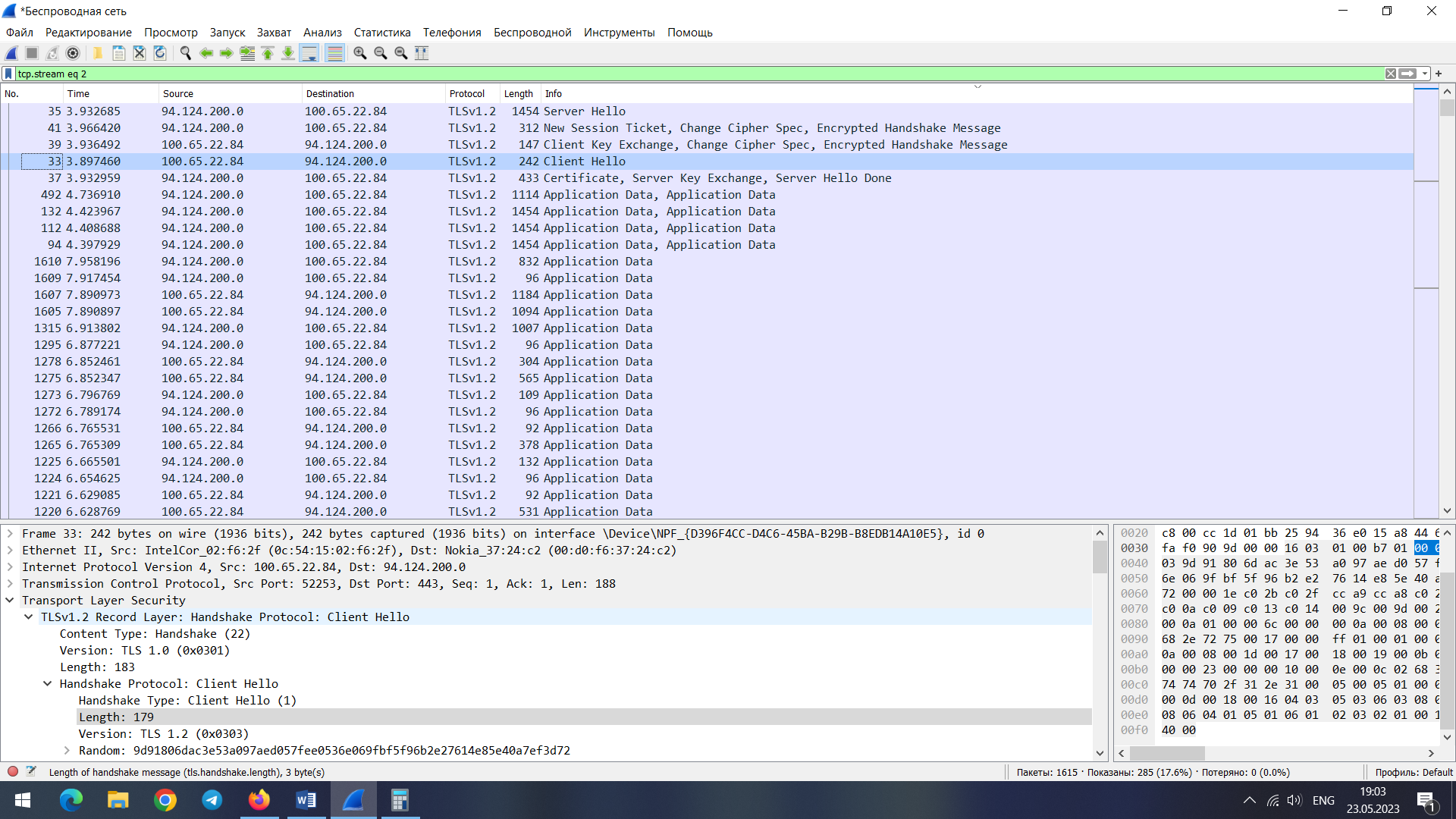


Время соединения считается как разность между Client Hello и первым переданным пакетом Application Data:

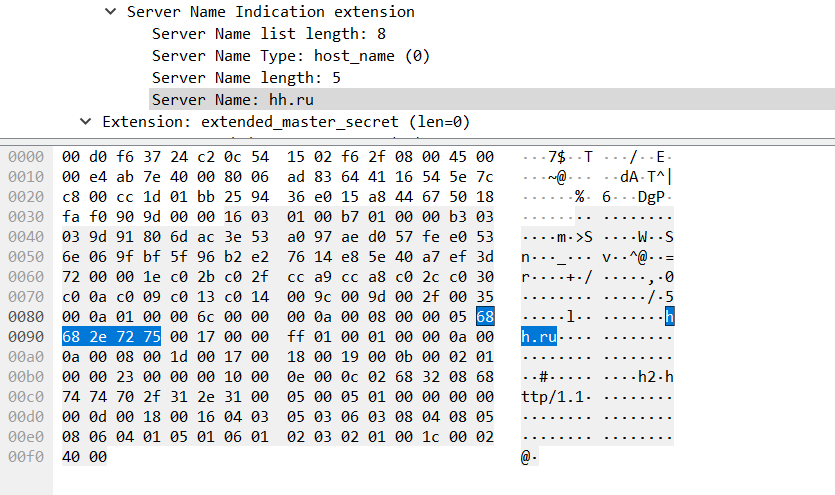


1.820262 – 1.773284 = 0.046978

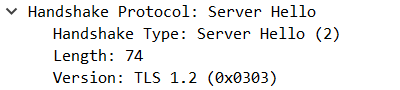
**4. Веб-сервер hh.ru**



Имя серверабыло найдено в пакете Client hello**:**

****

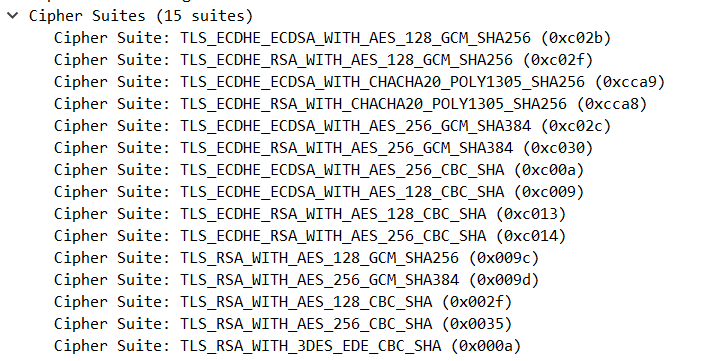
Версия TLS 1.2, информация была найдена в пакете Server Hello



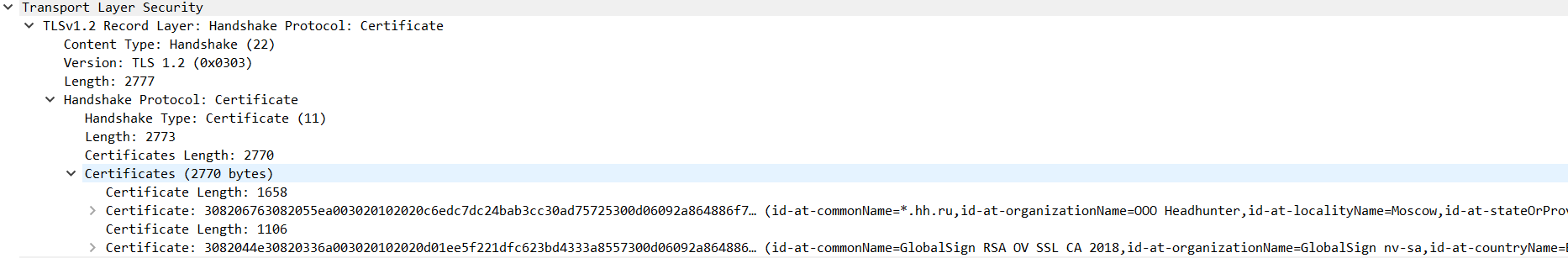
Для шифрования был выбран алгоритм Диффи-Хеллмана, информация также была найдена в Server Hello:



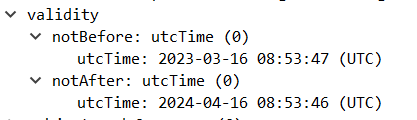
Информацию о всех возможных алгоритмах шифрования клиента, можно найти в Client hello:



Сертификат и его версия:



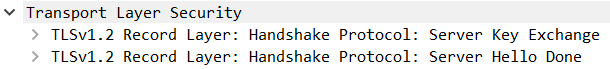
Валидность ключа и сертификата от/до:



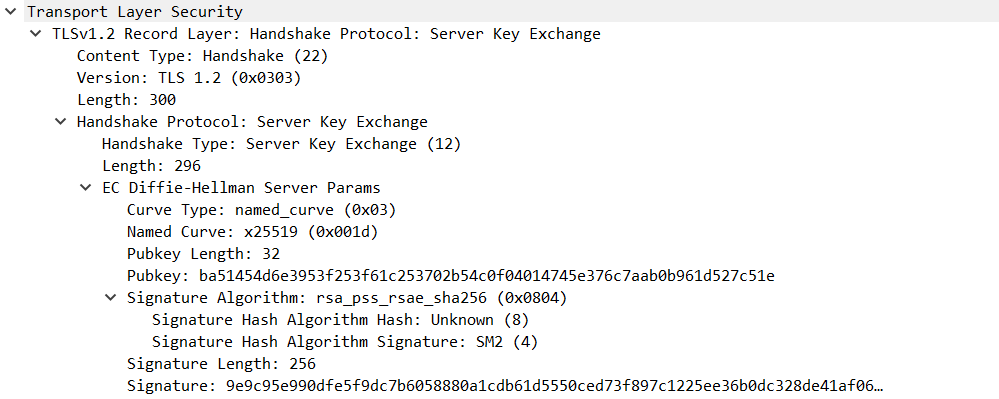
Организация, выдавшая сертификат:



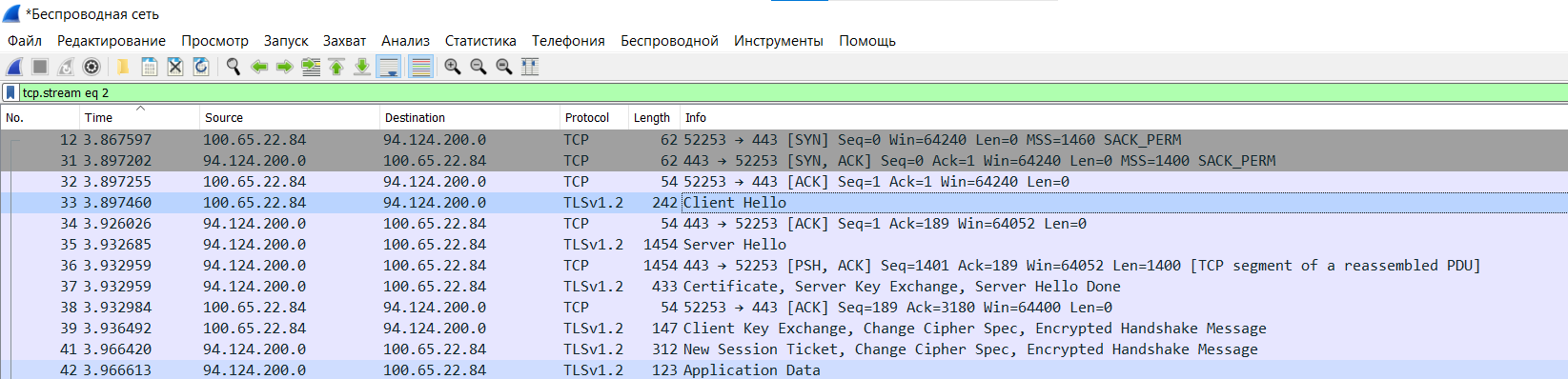
Статус сертификата для данного сервера не указан:



Информация о ключе:

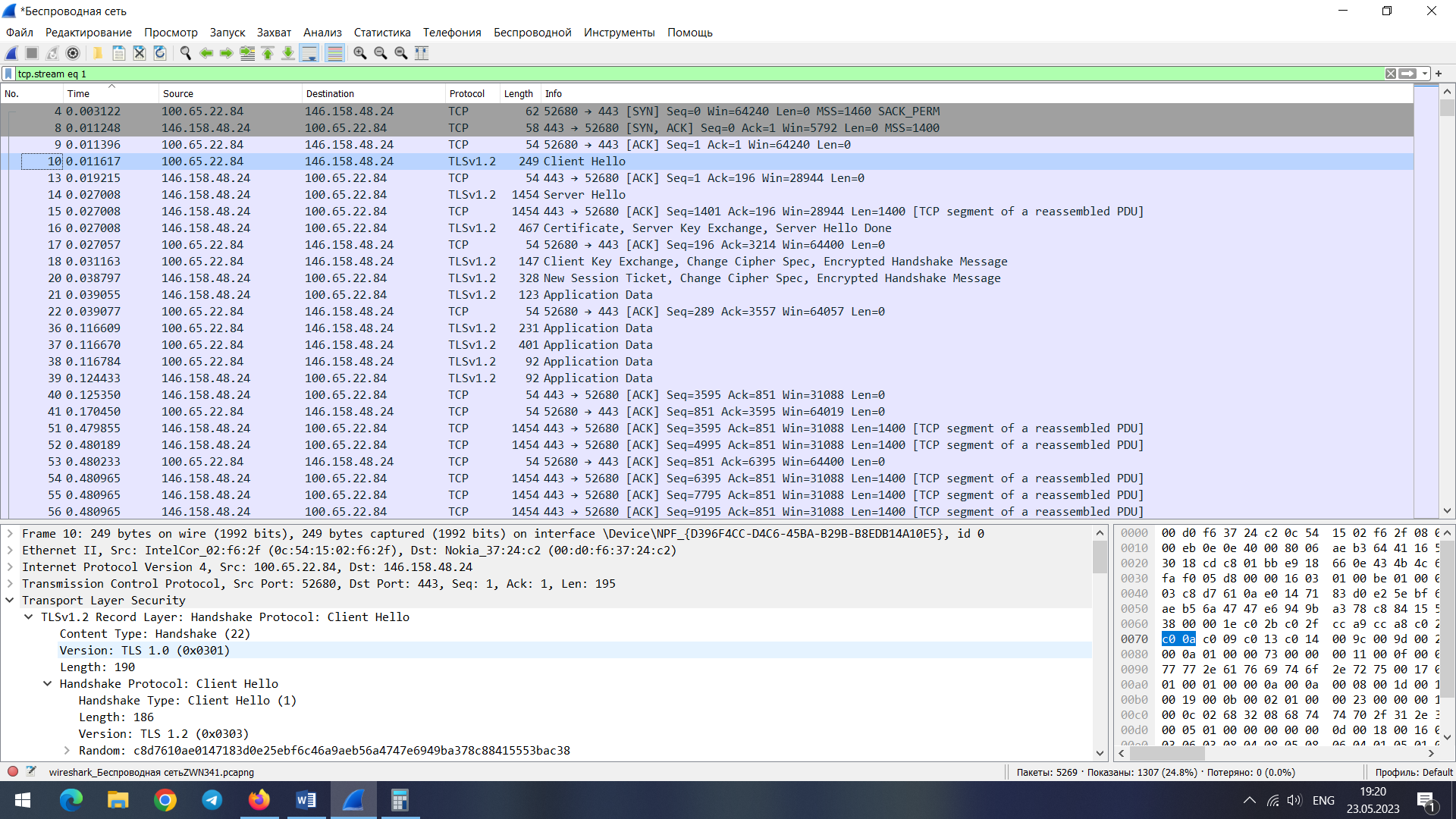


Время соединения считается как разность между Client Hello и первым переданным пакетом Application Data:

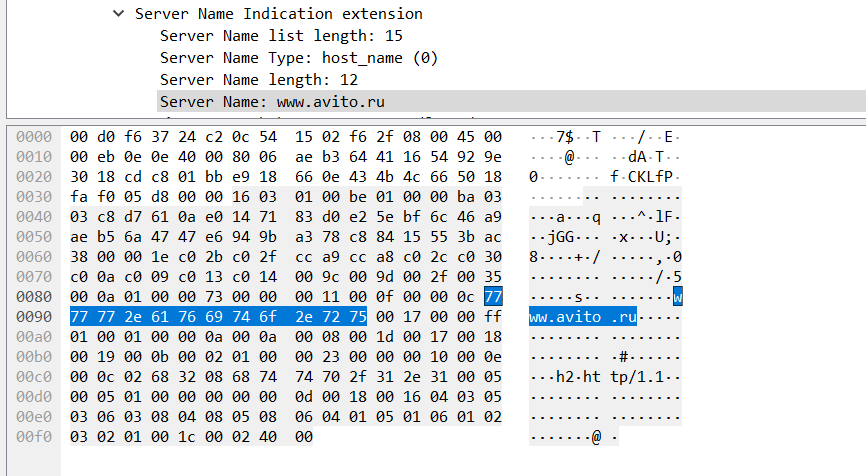


3.966613 – 3.897460 = 0.069153

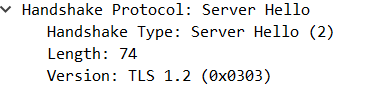
**5. Веб-сервер avito.ru**



Имя серверабыло найдено в пакете Client hello**:**

****

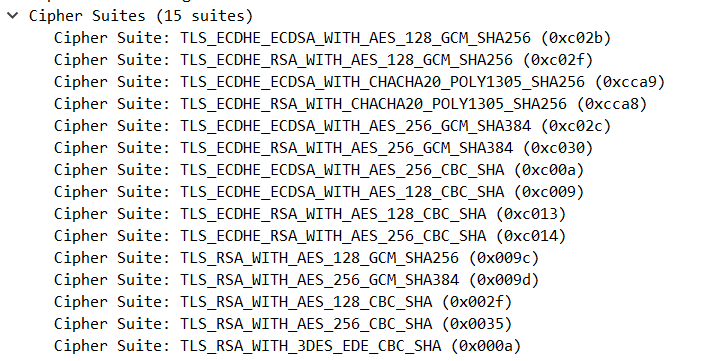
Версия TLS 1.2, информация была найдена в пакете Server Hello



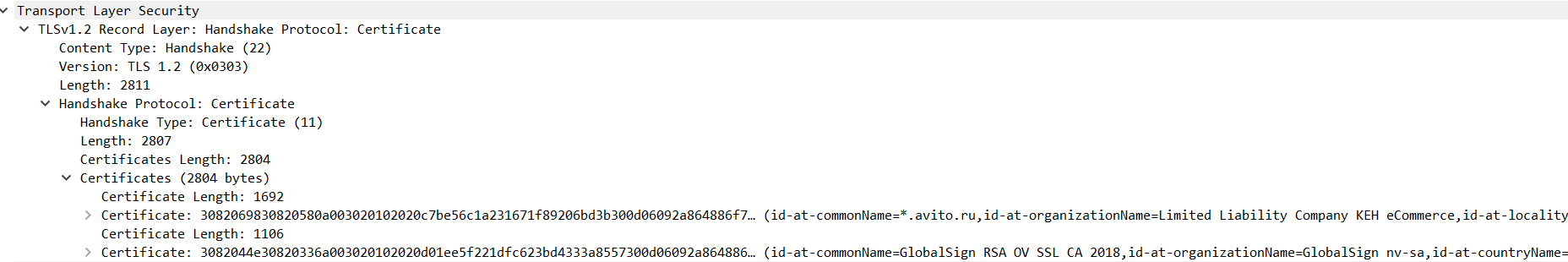
Для шифрования был выбран алгоритм Диффи-Хеллмана, информация также была найдена в Server Hello (Cipher Suite):



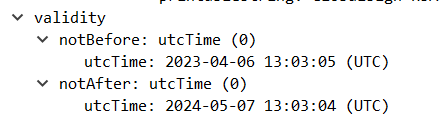
Информацию о всех возможных алгоритмах шифрования клиента, можно найти в Client hello:



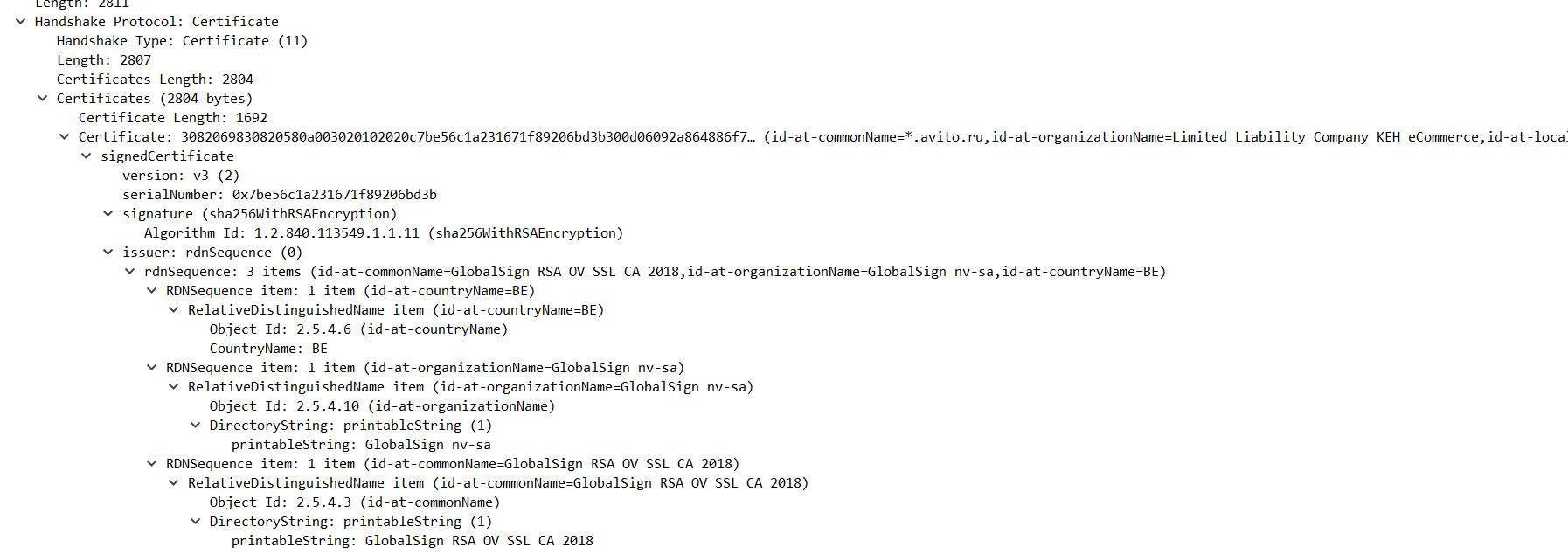
Сертификат и его версия:



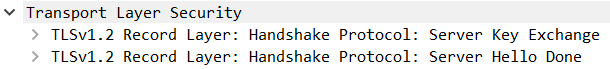
Валидность ключа и сертификата от/до:



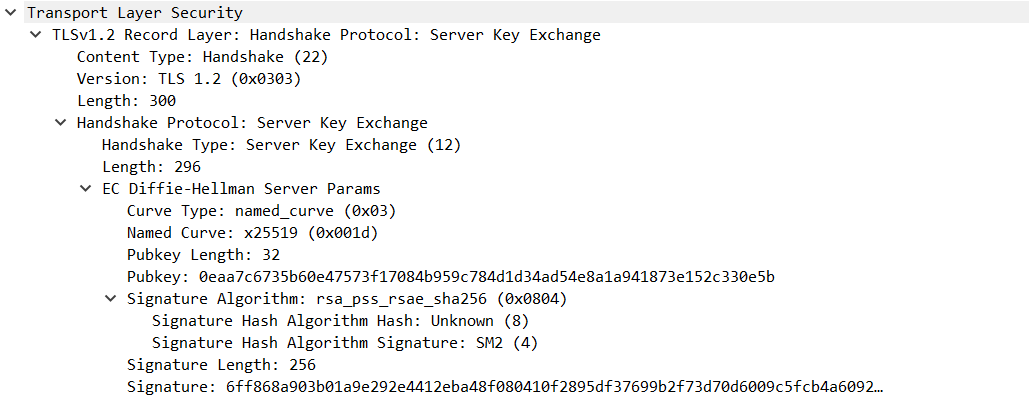
Организация, выдавшая сертификат:



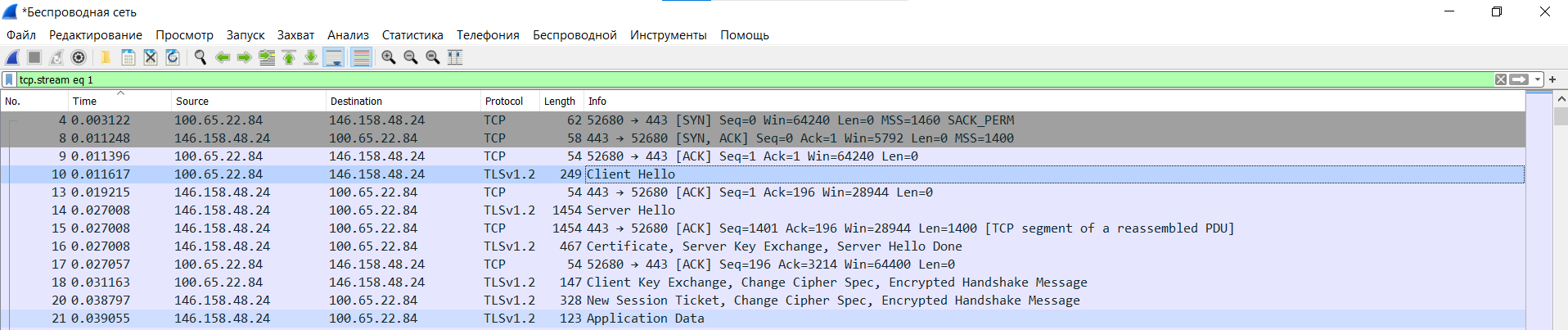
Статус сертификата для данного сервера не указан:



Информация о ключе:

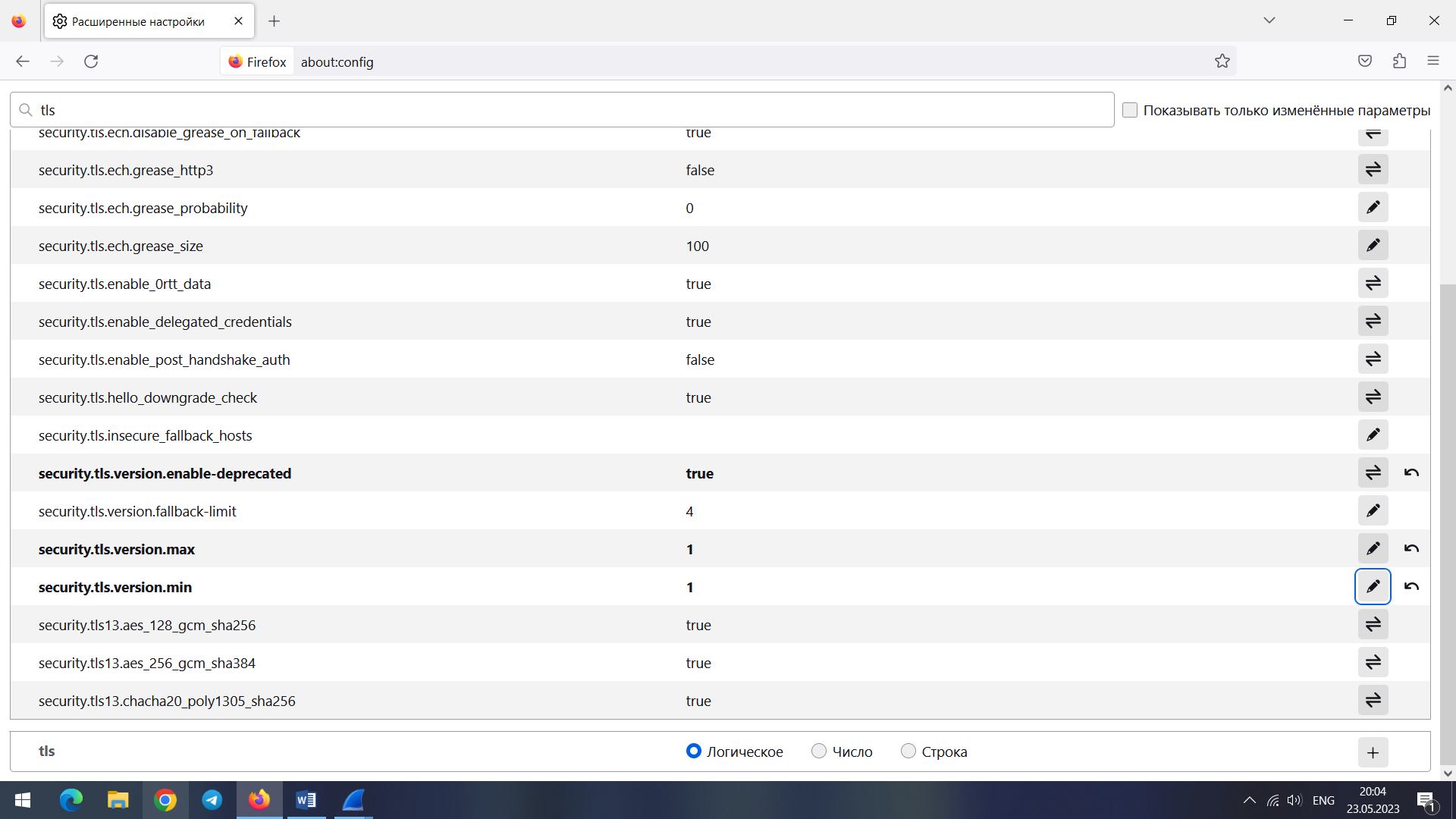


Время соединения считается как разность между Client Hello и первым переданным пакетом Application Data:



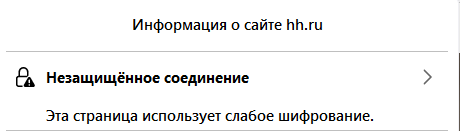
0.039055– 0,011617 = 0,027438

Теперь можно сменить версию TLS с 1.2 на 1.0 и посмотреть, что изменится на тех же веб-сервисах:

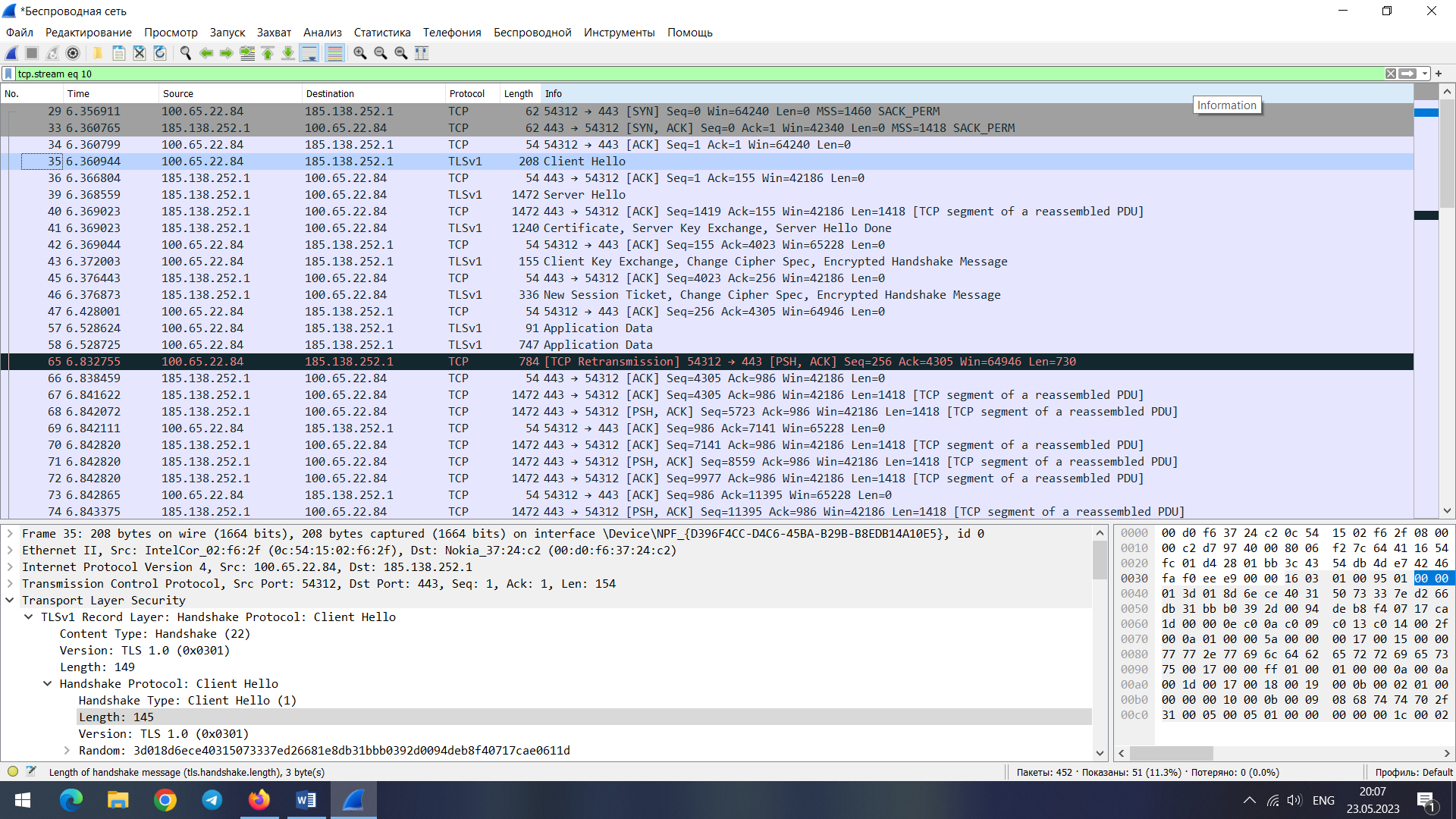


**1. Веб-сервер wildberries.ru**

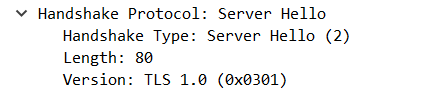
Сайт работает корректно, никаких проблем обнаружено не было. Однако, появилось сообщение о незащищённости соединения:



Wireshar смог успешно произвести захват трафика:



Версия TLS сменилась на 1.0:

****

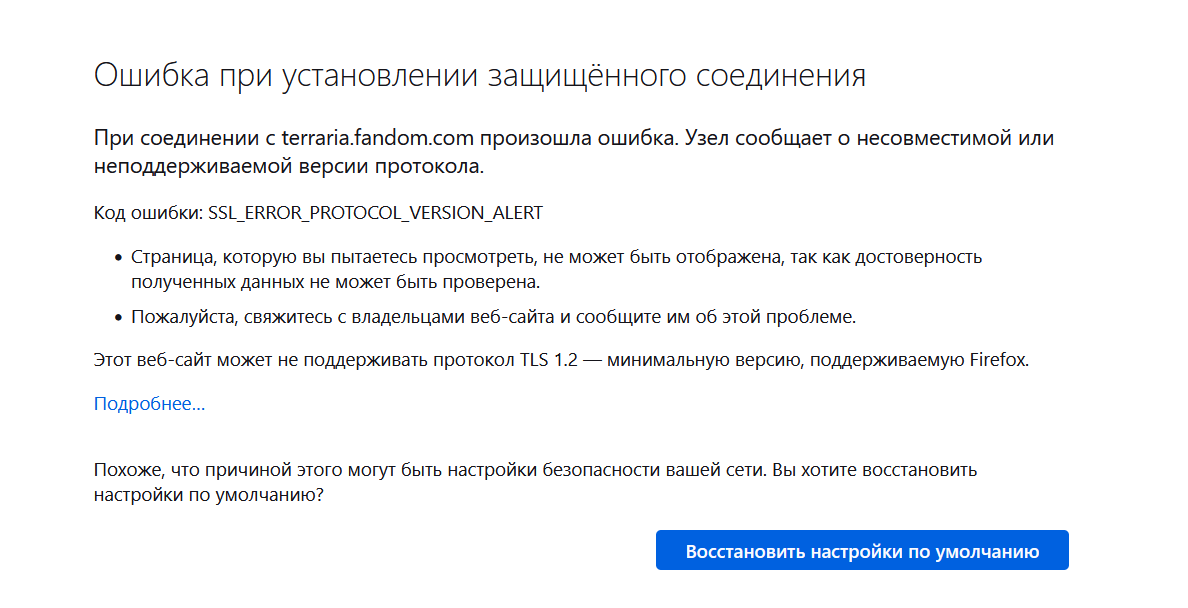
Способ шифрования также изменился:

****

В сертификатах и ключах видимые изменения замечены не были. Очевидно, что и в информации о сертификате также поменялся ключ.

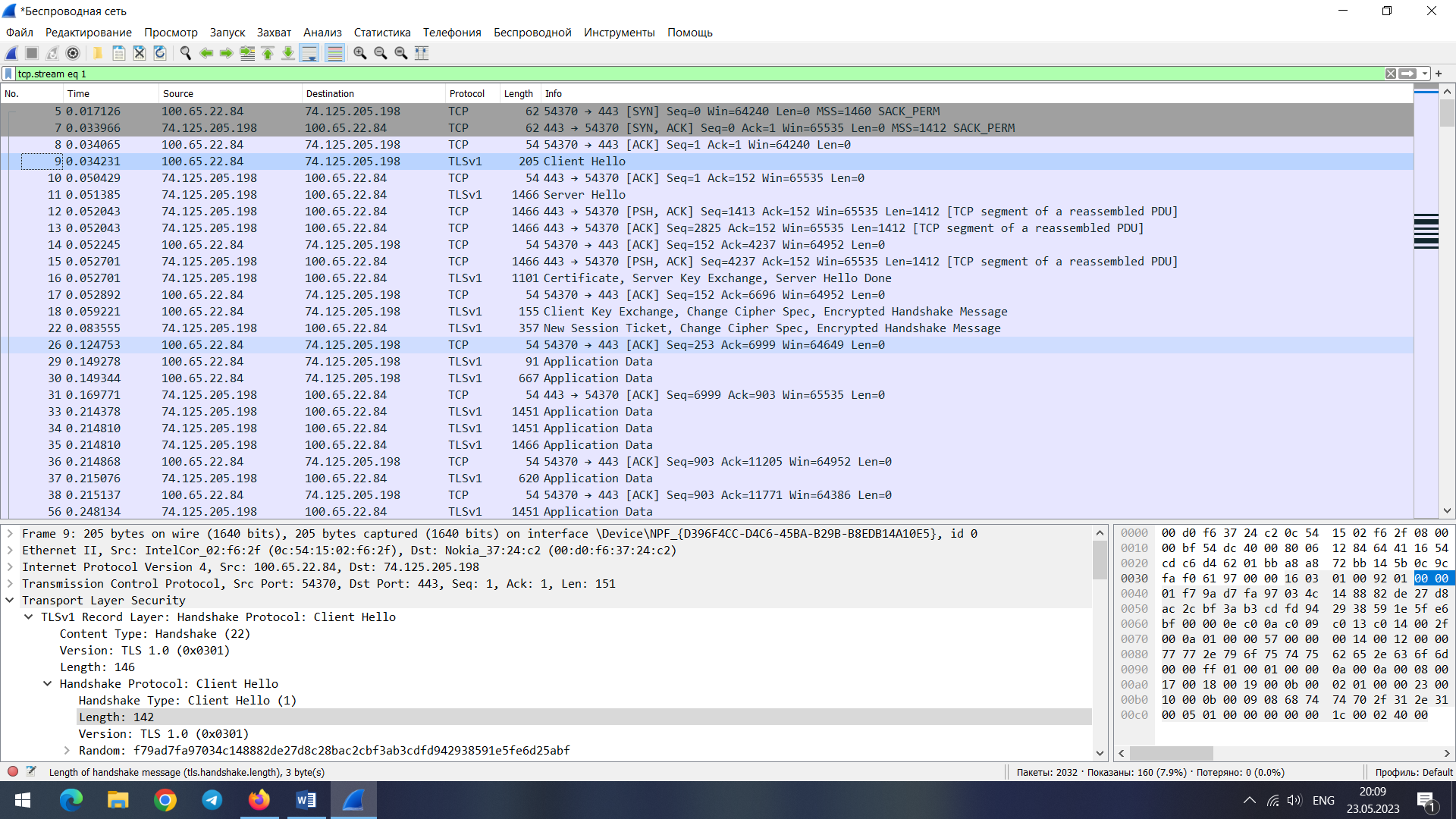
**2. Веб-сервер terraria.fandom.com**

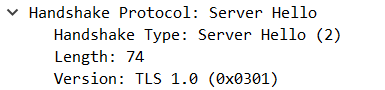
При попытке зайти на веб-сервер Террарии Вики возникает ошибка при установлении защищённого соединения. В Wireshark никакой информации о попытках соединения найдено не было. Данный сайт поддерживает только TLS версии 1.2 и 1.3.

****

**3. Веб-сервер youtube.com**

На данном и последующих сайтах захват трафика был успешно осуществлён, как и в первом случае. Изменения отражены на скриншотах ниже:

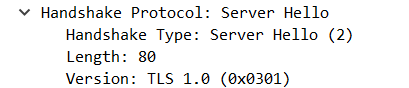


****

****

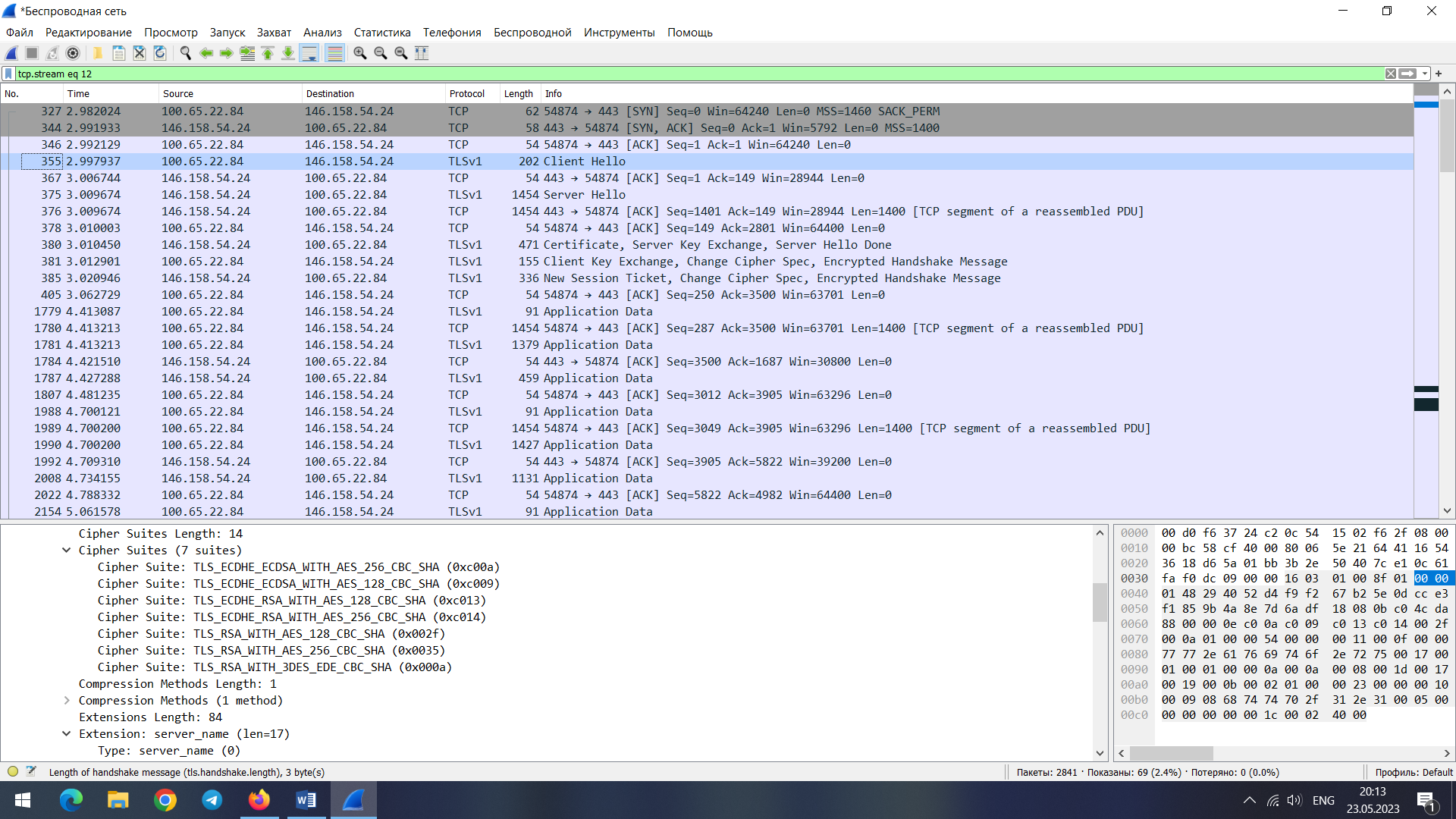
**4. Веб-сервер hh.ru**

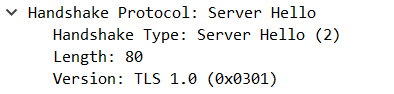


****

****

**5. Веб-сервер avito.ru**



****

****

**4. Вывод**

В процессе работы над данной работой я узнал, как осуществляется связь между сервером и клиентом на веб-серверах. В ходе анализа данных стало понятно, что алгоритм рукопожатия обеспечивает договорённость между сервером и клиентом о способе шифрования и дешифрования сообщений.

Многие сайты в настоящее время используют новые протоколы TLS 1.2 и 1.3 для шифрования сообщений. Протоколы версий 1.0 и 1.1 считаются устаревшими и на некоторые сайты зайти с их использованием нельзя, из-за проблем с безопасностью соединения или невозможности найти подходящий Cipher Suite. Это значит, что современные сайты достаточно надёжны.

Все сертификаты выданы давно существующими и крайне известными сертификационными центрами, что в очередной раз подтверждает надёжность этих сайтов.

На всех анализируемых мною сайтах в качестве алгоритма шифрования использовался алгоритм Диффи-Хеллмана. Данный алгоритм считается надёжнее, чем другие. Однако можно заметить, что использовался также RSA, но уже в качестве алгоритма активации.