МИНИСТЕРСТВО НАУКИ И ВЫШСЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский Авиационный Институт»

(Национальный Исследовательский Университет)

**Институт** №8 «Информационные технологии и прикладная математика»

**Кафедра** 806 «Вычислительная математика и программирование»

**Курсовая работа**

**по курсу «Криптография»**

|  |  |
| --- | --- |
| Студент: | Семин А. В. |
| Группа: | М8О-306Б-20 |
| Преподаватель: | А. В. Борисов |
| Оценка: |  |
| Дата: |  |

Москва, 2023

# Курсовая работа

**Тема:** Аутентификация с асимметричными алгоритмами шифрования

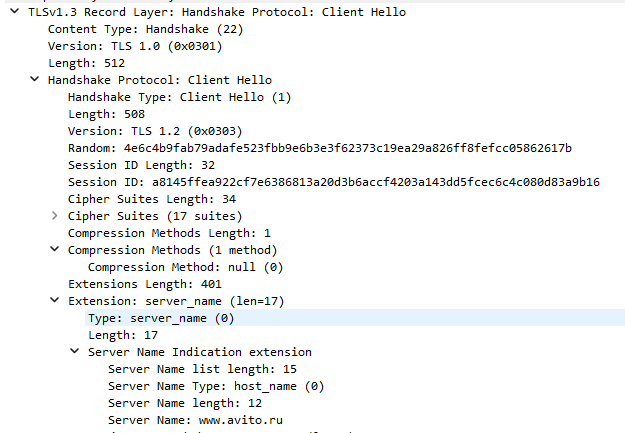
**Задание:**

1. Выбрать не менее 5-ти веб-серверов различной организационной и государственной принадлежности.
2. Запустить Wireshark и используя Firefox установить https соединение с выбранным сервером.
3. Провести анализ соединения.
4. Сохранить данные необходимы для последующего сравнительного анализа: Имя сервера, его характеристики. Версия TLS. Выбранные алгоритмы шифрования. Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр. Время установки соединения (от ClientHello до Finished)
5. Если список исследуемых серверов не исчерпан выбрать другой сервер и повторить соединие.
6. Если браузер поддерживал соединение TLS 1.2 принудительно изменить параметры TLS соединения в Firefox на TLS 1.0 (в браузере перейти по “about:config” и изменить раздел SSL\TLS) и провести попытки соединения с выбранными серверами).
7. Провести сравнительный анализ полученной информации.
8. В качестве отчета представить результаты сравнительного анализа, выводы в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и государственной принадлежности.

# Ход выполнения работы

**Веб сервер сайта** [**www.avito.ru**](http://www.avito.ru)

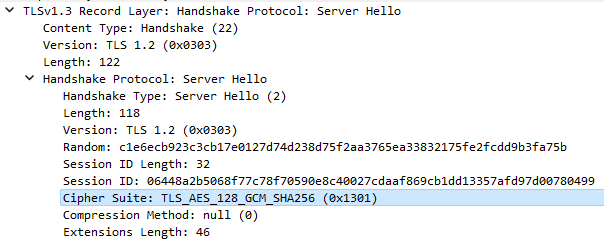
­­Пакет ClienHello:



Имя сервера: [www.avito.ru](http://www.avito.ru)

TLS версия: 1.2

ServerHello:



Алгоритм шифрования: AES 128-bit (Advanced Encryption Standard).

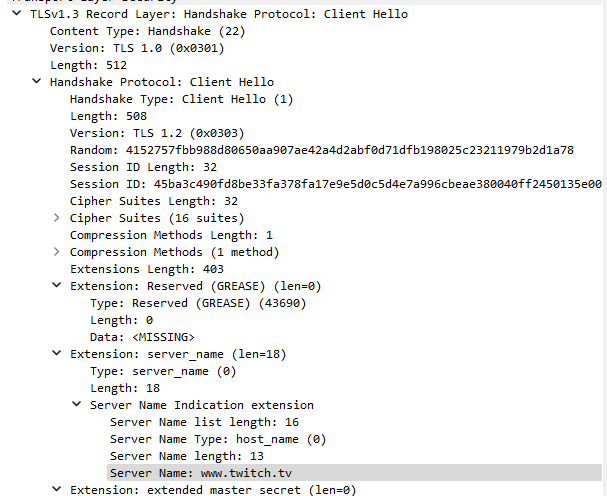
Пакет сертификата отсутствует.

Время соединения: рассчитаем как разность между ClientHello и первым

переданным пакетом: **263,589435 - 263,580866 = 0,008569**

**Веб сервер сайта** [**www.twitch.tv**](http://www.twitch.tv)

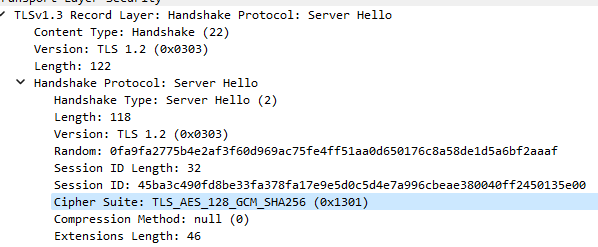
Пакет ClientHello:



Имя сервера: [www.twitch.tv](http://www.twitch.tv)

TLS версия: 1.2

ServerHello:



Алгоритм шифрования: AES 128-bit (Advanced Encryption Standard).

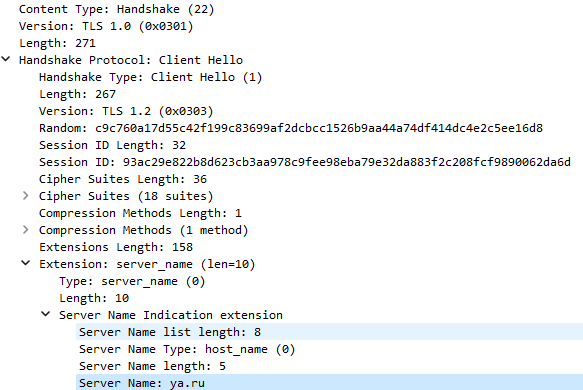
Пакет сертификата отсутствует.

Время соединения: рассчитаем как разность между ClientHello и первым

переданным пакетом: **8,377751 - 8,335916 = 0,041835**

**Веб сервер сайта** [**www.ya.ru**](http://www.ya.ru)

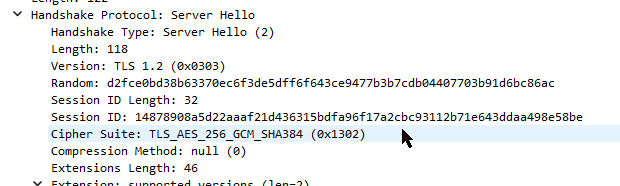
Пакет ClentHello:



Имя сервера: ya.ru

TLS версия: 1.2

ServerHello:



Алгоритм шифрования: AES 256-bit (Advanced Encryption Standard).

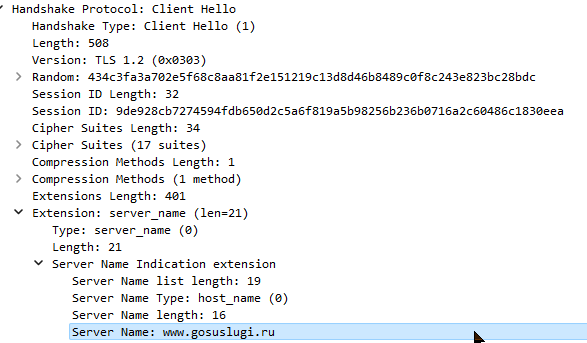
Пакет сертификата отсутствует.

Время соединения: рассчитаем как разность между ClientHello и первым

переданным пакетом: 8,320519 – 8,313512 = 0,007007

**Веб сервер** [**www.gosuslugi.ru**](http://www.gosuslugi.ru)

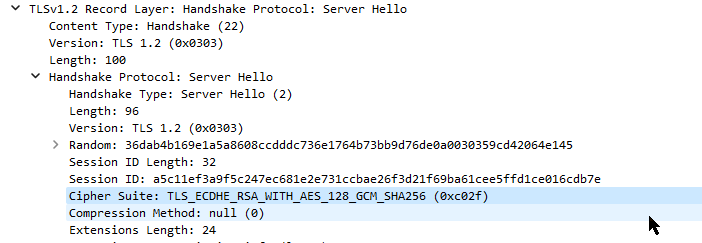
Пакет ClientHello:



Имя сервера: [www.gosuslugi.ru](http://www.gosuslugi.ru)

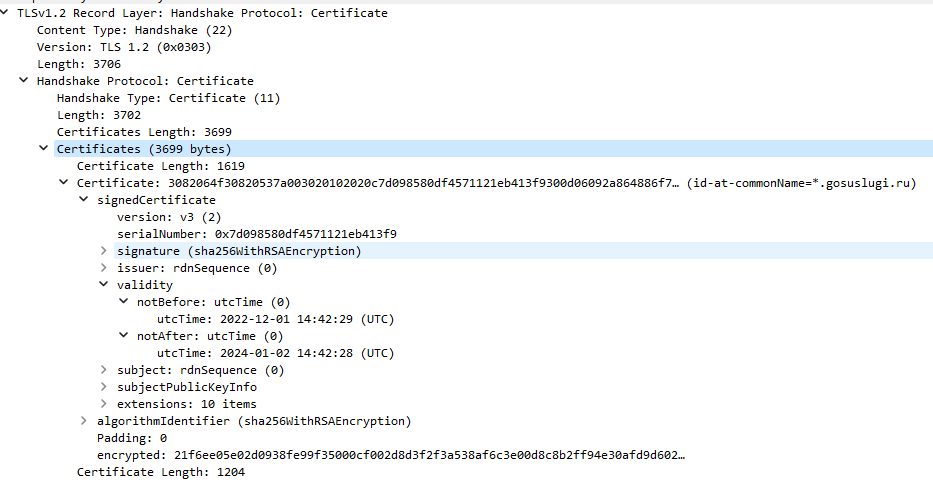
TLS версия: 1.2

ServerHello:

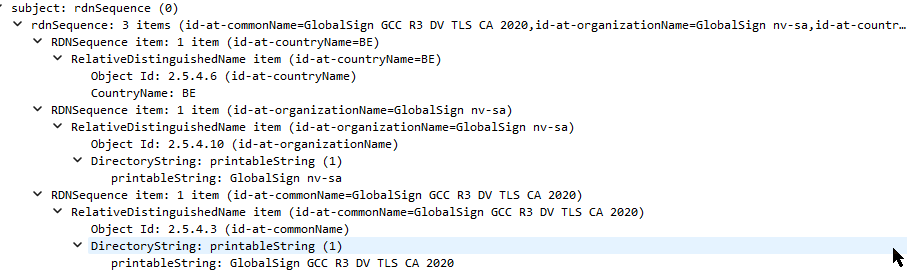


Алгоритм шифрования: ECDHE – алгоритм Диффи-Хеллмана на эллиптических кривых.

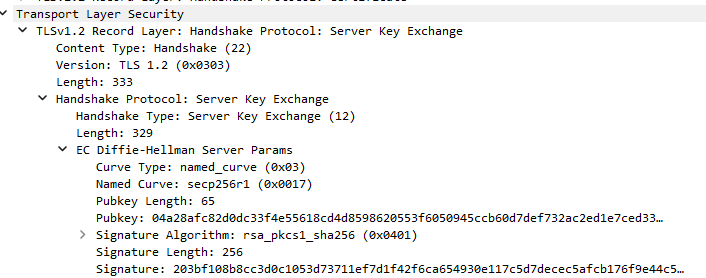
Изучим сертификат:



Валиден с 2022-12-01 по 2024-01-02

Информация об организации, выдавшей сертификат: 

Информация о ключе:

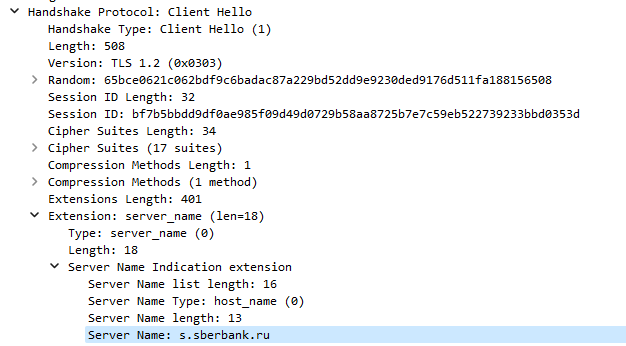


Время соединения: рассчитаем как разность между ClientHello и первым

переданным пакетом: **4,080135 - 4,066591 = 0,013544**

**Веб сервер** [**www.sberbank.ru**](http://www.sberbank.ru)

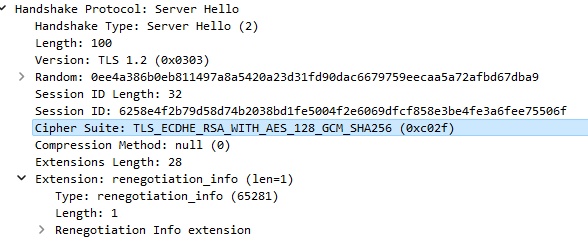
Пакет ClientHello:

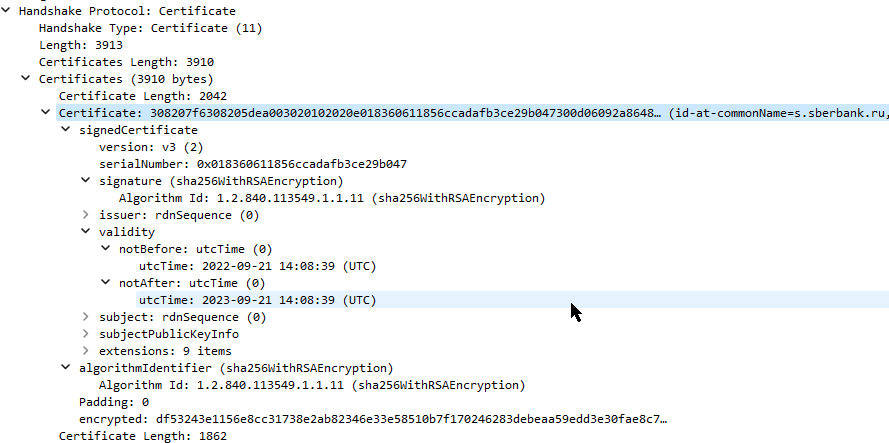


Имя сервера: s.sberbank.ru

TLS версия: 1.2

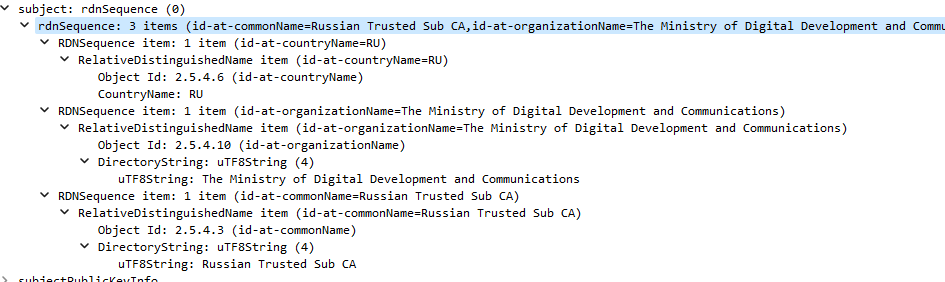
ServerHello:

 Алгоритм шифрования: ECDHE – алгоритм Диффи-Хеллмана на эллиптических кривых.

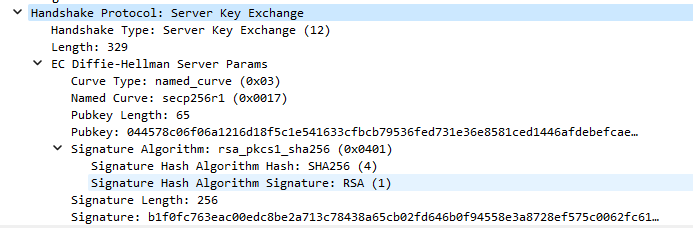
Изучим сертификат: 

Валиден с 2022-09-21 по 2023-09-21

Информация об организации, выдавшей сертификат:



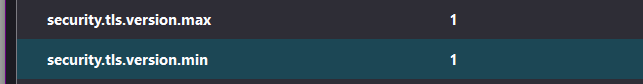
Информация о ключе:



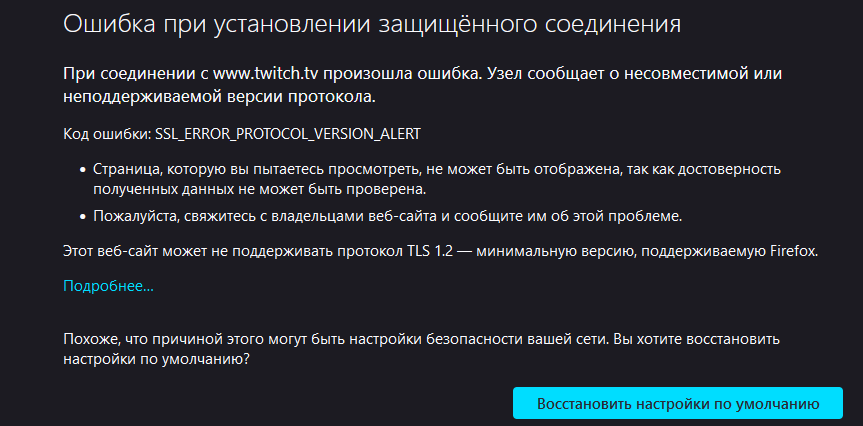
Время соединения: рассчитаем как разность между ClientHello и первым

переданным пакетом: **455,208505 - 455,200092 = 0,008413**

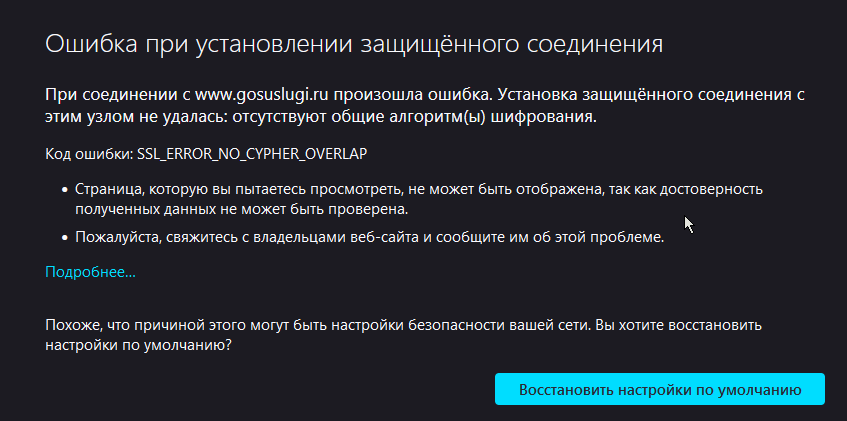
# Изменим версию TLS на 1.0



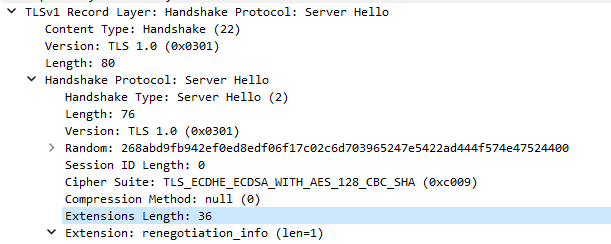
При попытке зайти на сайт twitch.tv ошибка:



При попытке зайти на gosuslugi.ru ошибка:

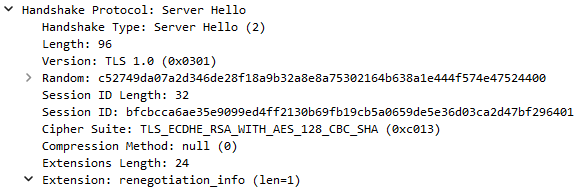


Однако на сайты ya.ru, avito.ru и sbebank.ru получилось успешно перейти, и они загрузились.

Но теперь, например, в пакете ServerHello сайта ya.ru: 

Extensions Length уменьшился до 36.

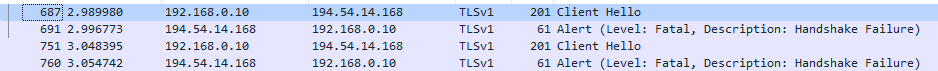
Для сайта avito.ru ServerHello:



Здесь Extension Length уменьшился до 24.

Также в обоих случаях алгоритм шифрования изменился на алгоритм Диффи-Хеллмана.

Для сайта sberbank.ru пакеты через TLS протокол теперь выглядят следующим образом:



# Выводы

В процессе выполнения данной лабораторной работы я разобрался в работе с инструментом Wireshark, а также изучил протокол защиты TLS. Протестировал, как себя поведут сайды при попытке подключения с разными версиями TLS. Среди изученных мною серверов три из пяти имели стандартный алгоритм шифрования AES для версии TLS 1.2, остальные два – алгоритм Диффи-Хеллмана. Проведя анализ путем сравнения работы серверов, можно предположить, что на время ответа сервера в большинстве случаев влияет его загруженность.