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

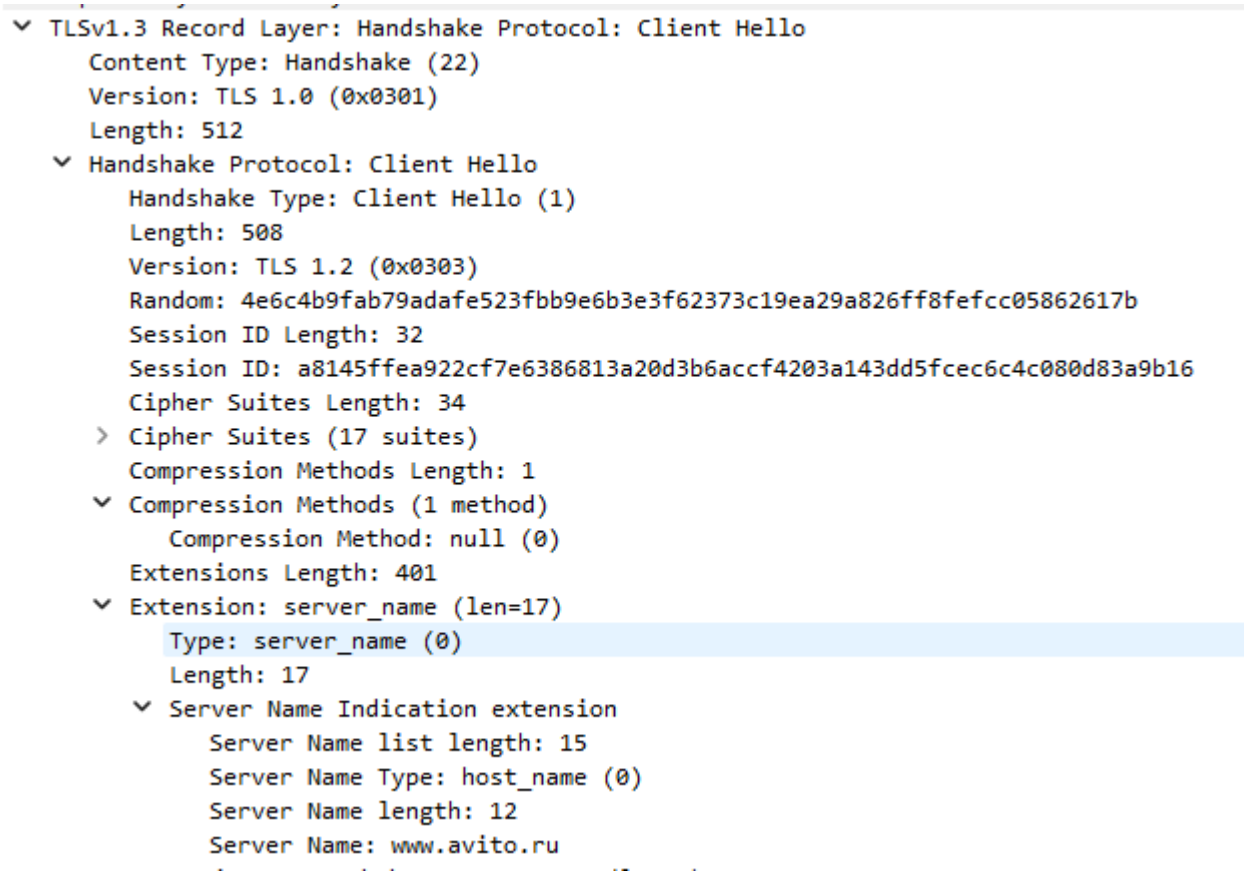
Задание:

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.

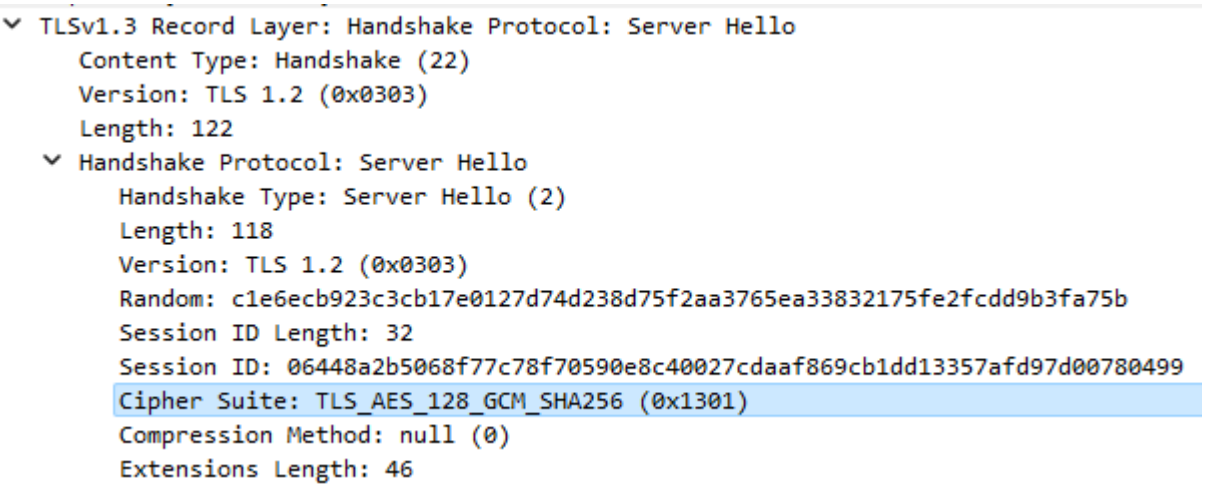
Ход выполнения работы

Веб сервер сайта www.avito.ru

Пакет ClienHello:



Имя сервера: 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

Пакет ClientHello:

```
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
      Random: 4152757fbb988d80650aa907ae42a4d2abf0d71dfb198025c23211979b2d1a78
      Session ID Length: 32
      Session ID: 45ba3c490fd8be33fa378fa17e9e5d0c5d4e7a996cbeae380040ff2450135e00
      Cipher Suites Length: 32
    > Cipher Suites (16 suites)
      Compression Methods Length: 1
    > Compression Methods (1 method)
      Extensions Length: 403
    > Extension: Reserved (GREASE) (len=0)
        Type: Reserved (GREASE) (43690)
        Length: 0
        Data: <MISSING>
    > Extension: server_name (len=18)
        Type: server_name (0)
        Length: 18
      > Server Name Indication extension
          Server Name list length: 16
          Server Name Type: host_name (0)
          Server Name length: 13
          Server Name: www.twitch.tv
    > Extension: extended master secret (len=0)
```

Имя сервера: www.twitch.tv
TLS версия: 1.2

ServerHello:

```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 118
      Version: TLS 1.2 (0x0303)
      Random: 0fa9fa2775b4e2af3f60d969ac75fe4ff51aa0d650176c8a58de1d5a6bf2aaaf
      Session ID Length: 32
      Session ID: 45ba3c490fd8be33fa378fa17e9e5d0c5d4e7a996cbeae380040ff2450135e00
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 46
```

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

Пакет ClentHello:

```
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 271
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 267
    Version: TLS 1.2 (0x0303)
    Random: c9c760a17d55c42f199c83699af2dcbcc1526b9aa44a74df414dc4e2c5ee16d8
    Session ID Length: 32
    Session ID: 93ac29e822b8d623cb3aa978c9fee98eba79e32da883f2c208fcf9890062da6d
    Cipher Suites Length: 36
  > Cipher Suites (18 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 158
  v Extension: server_name (len=10)
      Type: server_name (0)
      Length: 10
    v Server Name Indication extension
        Server Name list length: 8
        Server Name Type: host_name (0)
        Server Name length: 5
        Server Name: ya.ru
```

Имя сервера: ya.ru
TLS версия: 1.2

ServerHello:

```
v Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 118
    Version: TLS 1.2 (0x0303)
    Random: d2fce0bd38b63370ec6f3de5dff6f643ce9477b3b7cdb04407703b91d6bc86ac
    Session ID Length: 32
    Session ID: 14878908a5d22aaaf21d436315bdfa96f17a2cbc93112b71e643ddaa498e58be
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
    Extensions Length: 46
```

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

Пакет ClientHello:

```
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
  > Random: 434c3fa3a702e5f68c8aa81f2e151219c13d8d46b8489c0f8c243e823bc28bdc
    Session ID Length: 32
    Session ID: 9de928cb7274594fdb650d2c5a6f819a5b98256b236b0716a2c60486c1830eea
    Cipher Suites Length: 34
  > Cipher Suites (17 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 401
  v Extension: server_name (len=21)
      Type: server_name (0)
      Length: 21
    v Server Name Indication extension
        Server Name list length: 19
        Server Name Type: host_name (0)
        Server Name length: 16
        Server Name: www.gosuslugi.ru
```

Имя сервера: www.gosuslugi.ru
TLS версия: 1.2

ServerHello:

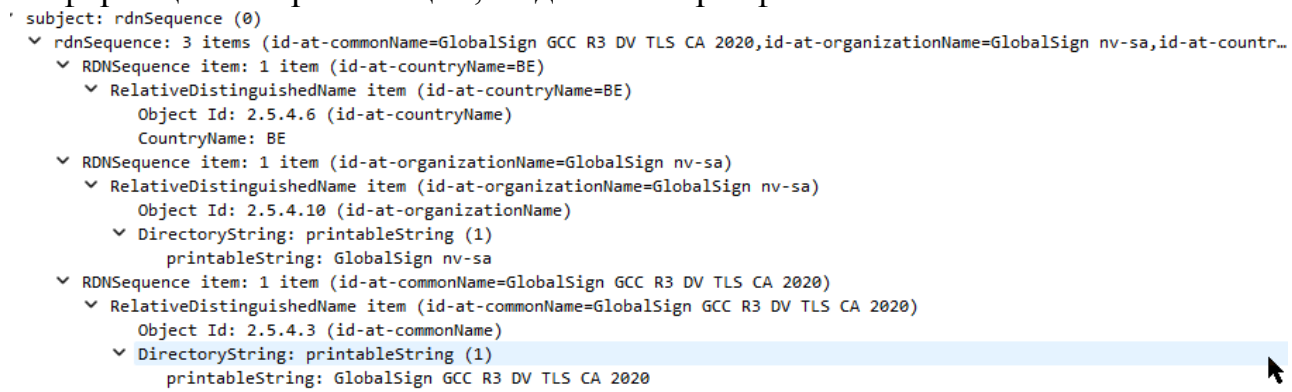
```
v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 100
  v Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 96
      Version: TLS 1.2 (0x0303)
    > Random: 36dab4b169e1a5a8608ccdddc736e1764b73bb9d76de0a0030359cd42064e145
      Session ID Length: 32
      Session ID: a5c11ef3a9f5c247ec681e2e731ccbae26f3d21f69ba61cee5ffd1ce016cdb7e
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Method: null (0)
      Extensions Length: 24
```

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

Пакет ClientHello:

```
Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
  > Random: 65bce0621c062bdf9c6badac87a229bd52dd9e9230ded9176d511fa188156508
    Session ID Length: 32
    Session ID: bf7b5bbdd9df0ae985f09d49d0729b58aa8725b7e7c59eb522739233bbd0353d
    Cipher Suites Length: 34
  > Cipher Suites (17 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 401
  v Extension: server_name (len=18)
        Type: server_name (0)
        Length: 18
      v Server Name Indication extension
            Server Name list length: 16
            Server Name Type: host_name (0)
            Server Name length: 13
            Server Name: s.sberbank.ru
```

Имя сервера: s.sberbank.ru
TLS версия: 1.2

ServerHello:

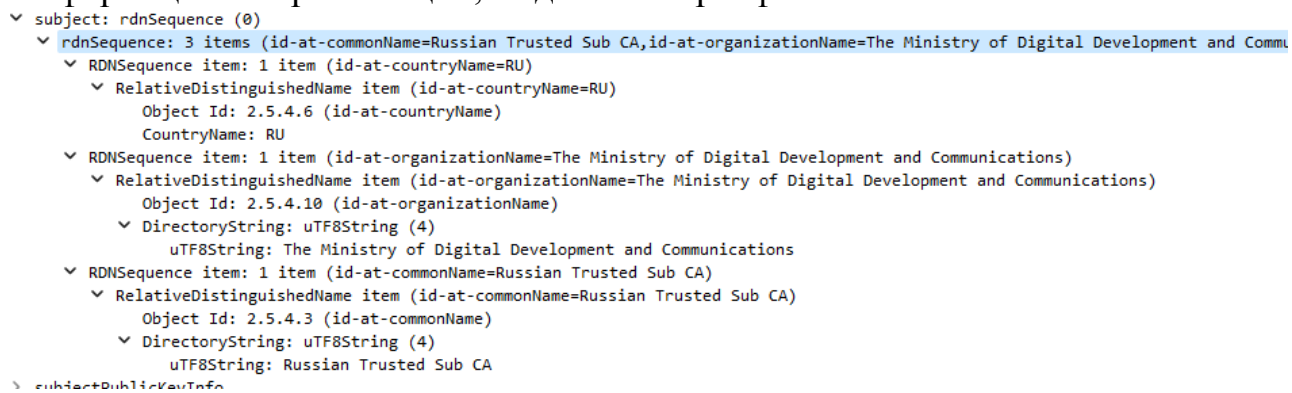
```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 100
    Version: TLS 1.2 (0x0303)
  > Random: 0ee4a386b0eb811497a8a5420a23d31fd90dac6679759eecaa5a72afbd67dba9
    Session ID Length: 32
    Session ID: 6258e4f2b79d58d74b2038bd1fe5004f2e6069dfcf858e3be4fe3a6fee75506f
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
    Extensions Length: 28
  v Extension: renegotiation_info (len=1)
        Type: renegotiation_info (65281)
        Length: 1
      > Renegotiation Info extension
```

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:

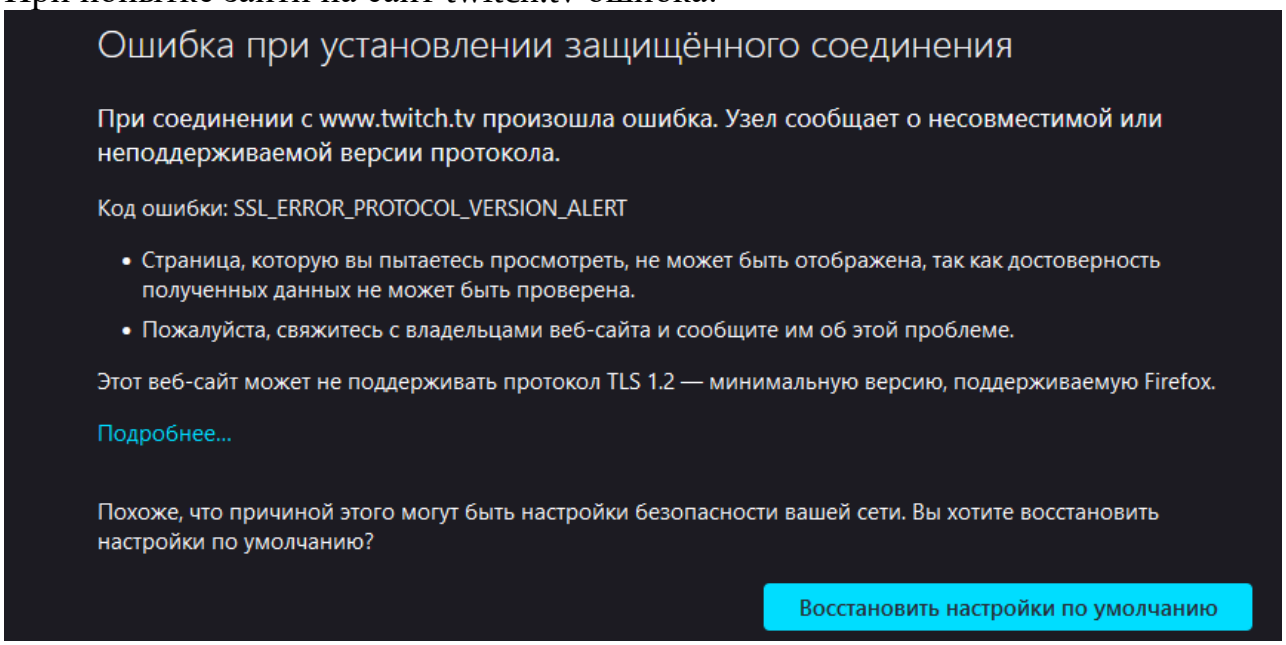


Информация о ключе:

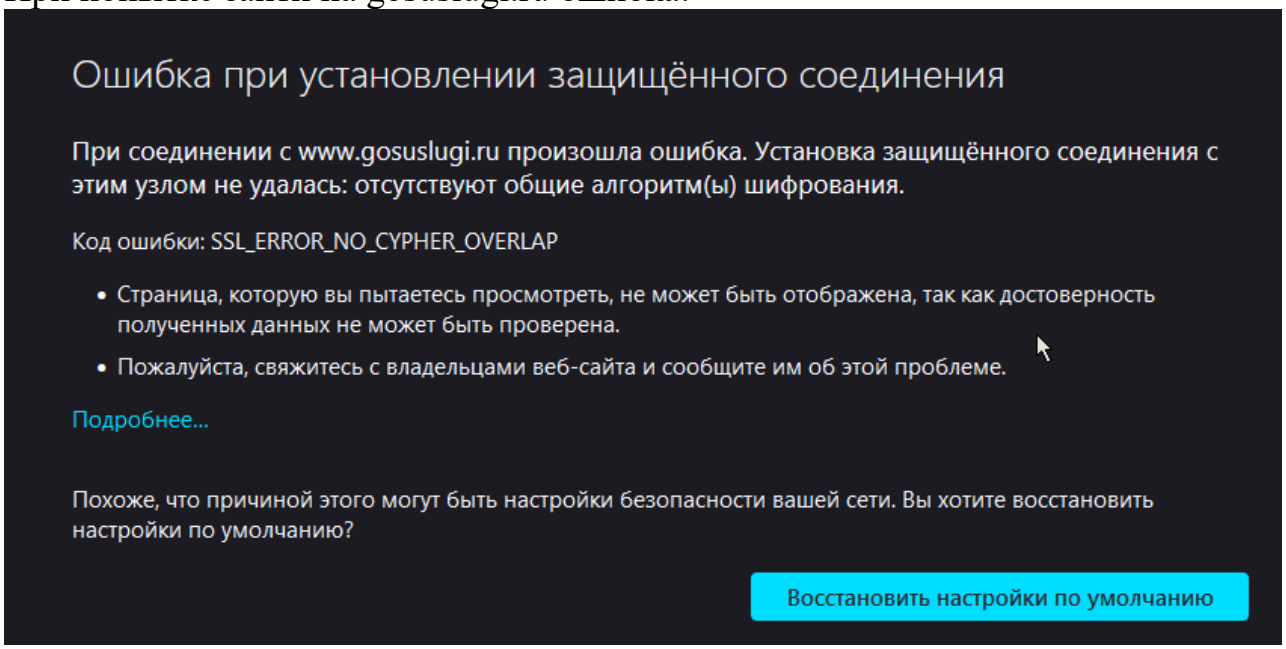
Время соединения: рассчитаем как разность между ClientHello и первым переданным пакетом: **455,208505 - 455,200092 = 0,008413**

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:

```
TLSv1 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 80
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 76
      Version: TLS 1.0 (0x0301)
    > Random: 268abd9fb942ef0ed8edf06f17c02c6d703965247e5422ad444f574e47524400
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      Compression Method: null (0)
      Extensions Length: 36
    > Extension: renegotiation_info (len=1)
```

Extensions Length уменьшился до 36.

Для сайта avito.ru ServerHello:

```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 96
    Version: TLS 1.0 (0x0301)
  > Random: c52749da07a2d346de28f18a9b32a8e8a75302164b638a1e444f574e47524400
    Session ID Length: 32
    Session ID: bfcbcca6ae35e9099ed4ff2130b69fb19cb5a0659de5e36d03ca2d47bf296401
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Compression Method: null (0)
    Extensions Length: 24
  > Extension: renegotiation_info (len=1)
```

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:

687	2.989980	192.168.0.10	194.54.14.168	TLSv1	201	Client Hello
691	2.996773	194.54.14.168	192.168.0.10	TLSv1	61	Alert (Level: Fatal, Description: Handshake Failure)
751	3.048395	192.168.0.10	194.54.14.168	TLSv1	201	Client Hello
760	3.054742	194.54.14.168	192.168.0.10	TLSv1	61	Alert (Level: Fatal, Description: Handshake Failure)

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.