**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО 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»**

Лабораторная работа № 4   
по курсу «Криптография»

Группа: М8О-310Б-21

Студент: А. С. Личковаха

Преподаватель: А. В. Борисов

Оценка:

Дата: 12.05.2024

Москва, 2024

**ОГЛАВЛЕНИЕ**

[**1** **Тема** 3](#_Toc166588233)

[**2** **Задание** 3](#_Toc166588234)

[**3** **Ход лабораторной работы** 4](#_Toc166588235)

[**4** **Выводы** 6](#_Toc166588236)

# **Тема**

Аутентификация с асимметричными алгоритмами шифрования

# **Задание**

1. Выбрать не менее 2-ух веб-серверов сети Интернет различной организационной и государственной принадлежности.
2. Запустить Wireshark и используя Firefox установить https соединение с выбранным сервером.
3. Провести анализ соединения.
4. Сохранить данные необходимые 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)

1. Если список исследуемых серверов не исчерпан выбрать другой сервер и повторить соединение.
2. 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).
3. Провести сравнительный анализ полученной информации.

В качестве отчета представить результаты сравнительного анализа, выводы в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и государственной принадлежности.

# **Ход лабораторной работы**

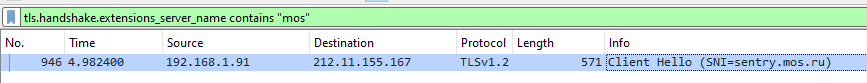
Я установил Wireshark на свой пк и запустил. Чтобы проводить анализ

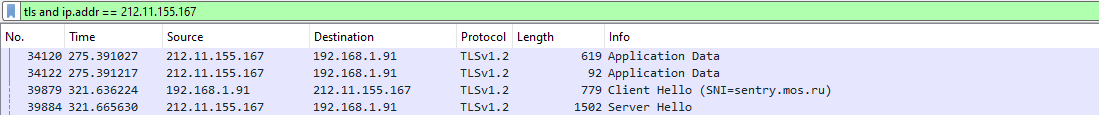
я выбрал интерфейс для беспроводного соединения, так как через wifi подключен к сети. В качестве сайтов для анализа я выбрал

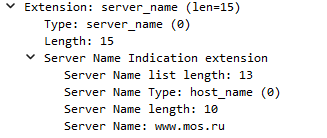
mos.ru и ya.ru .

Далее требуется установить hhtps-соединение с сайтами, для этого введём URL веб серверов, начиная с "https://". После захода остановим захват, чтобы провести анализ пакетов. Разберём на примере работы с сервером профи, а для mos.ru просто соберём информацию.

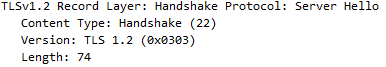
Для начала в поле фильтра введём команду: «tls.handshake.extensions\_server\_name contains "mos"» чтобы узнать ip сервера в столбце destination.

Далее отфильтруем пакеты по протоколу tls и ip адресу ”tls and ip.addr == 185.186.186.140”





Проанализируем пакет с сообщение Client Hello. Перейдём в Transport Layer Security/Handshake Protocol/Extension чтобы увидеть имя сервера, с которым происходит коммуникация.

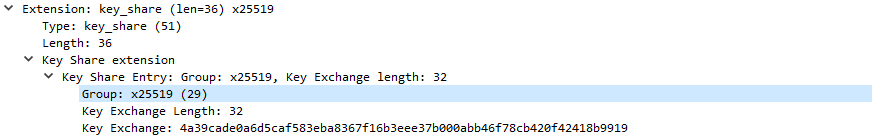


Чтобы посмотреть версию TLS, а также алгоритмы шифрования, нужно найти пакет с сообщением Server Hello и в параметрах пакета в Transport Layer Security можно увидеть набор шифров для использования

Выбранный алгоритмы шифрования

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

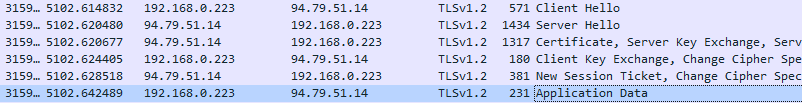
В параметрах также указано, что для генерации ключей симметричного шифрования будет использоваться группа эллиптических кривых — x25519



Информацию о сертификате можно получить из пакета с сообщением Certificate.



Время установки соединения это разница во времени между сообщениями client hello и finished (0,027657).



Подведём итоги:

mos.ru

1. Имя сервера: mos.ru
2. Версия TLS: 1.2
3. Алгоритмы шифрования: SHA-256 with RSA Encryption
4. Сертификат:
   * version — v3
   * Serial number — 31676e550a63262efe51e6c7
   * Validity:

notBefore: utcTime (0)

utcTime: 2023-11-15 09:40:06 (UTC)

notAfter: utcTime (0)

utcTime: 2024-12-16 09:40:05 (UTC)

* + Удостоверяющий центр - GlobalSign RSA OV SSL CA 2018

ya.ru

1. Имя сервера: ya.ru
2. Версия TLS: 1.3
3. Алгоритмы шифрования: SHA-384 with RSA Encryption
4. Сертификат:
   * version — v3
   * Serial number — 49431cbe2139a733c0067370
   * Validity

notBefore: utcTime (0)

utcTime: 2023-12-27 07:18:05 (UTC)

notAfter: utcTime (0)

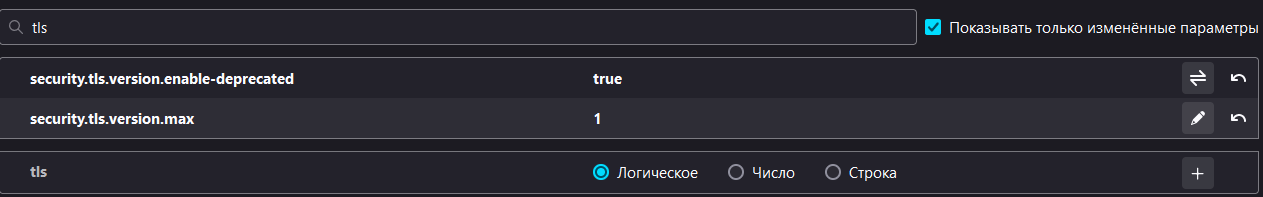
utcTime: 2024-07-28 07:18:05 (UTC)

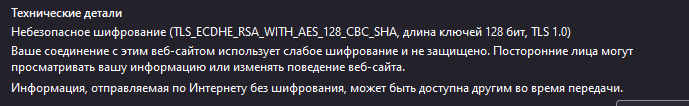
* + Удостоверяющий центр - GlobalSign RSA OV SSL CA 2018

5. Время установки соединения: 0,007535 сек

Из собранных характеристик видно, что все серверы работают с TLSv1.3, это действительно хорошо, так как применяются современные алгоритмы шифрования и установленное соединение более защищенное.

Поставим версию TLS 1.0, для этого по адресу about:config поменял значение у поля security.tls.version.max на 1 а также security.tls.version.enable-deprecated на true.



Попробуем снова установить соединение с сайтами. В итоге при заходе на сайт ya.ru браузер предупредил нас о том что соединение незащищено:  


# **Выводы**

В процессе выполнения лабораторной работы я научился работать с утилитой Wireshark, которая предоставляет мощные инструменты для анализа трафика, и захватывать пакеты данных, проходящие через мой сетевой интерфейс, освоил фильтрацию пакетов, изучил аспекты протокола TLS, методы извлечения и интерпретации данных из захваченных пакетов. Этот опыт помог мне лучше понять механизм работы соединения через HTTPS и какие факторы влияют на его безопасность и корректность настроек.