

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-306Б-21

Студент(ка): О. А. Мезенин

Преподаватель: А. В. Борисов

Оценка:

Дата: 14.04.2024

Москва, 2024

ОГЛАВЛЕНИЕ

| | | |
|---|-------------------------------------|----|
| 1 | Тема | 3 |
| 2 | Задание | 3 |
| 3 | Теория..... | 4 |
| 4 | Ход лабораторной работы..... | 5 |
| 5 | Выводы..... | 13 |
| 6 | Список используемой литературы..... | 14 |

1 Тема

Аутентификация с асимметричными алгоритмами шифрования

2 Задание

1. Выбрать не менее 2-ух web-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 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 соединение.

6. Если браузер поддерживал соединение TLS 1.2 принудительно изменить параметры TLS соединения в Firefox на TLS 1.0 (в браузере перейти по адресу “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.

3 Теория

Проблема протокола HTTP заключается в том, что данные передаются по сети в открытом виде, что делает возможным для злоумышленника прослушивать передаваемые пакеты и извлекать информацию из параметров, заголовков и тела сообщений. Для устранения этой уязвимости был разработан HTTPS, который представляет собой HTTP поверх SSL (а затем и TLS), позволяющий безопасный обмен данными. В отличие от HTTP, использующего стандартный TCP/IP порт 80, HTTPS использует порт 443.

Secure Sockets Layer (SSL) — это криптографический протокол, обеспечивающий безопасное взаимодействие между пользователем и сервером в небезопасной сети. Сегодня он считается устаревшим.

Transport Layer Security (TLS) — это развитие идей, лежащих в основе протокола SSL. Этот протокол обеспечивает приватность, целостность и аутентификацию. Он использует гибридное шифрование, сочетающее асимметричное и симметричное шифрование: общий ключ для симметричного шифрования данных передаётся от клиента к серверу зашифрованным открытым ключом сервера, после чего сервер расшифровывает его своим закрытым ключом и использует для обмена данными с клиентом.

4 Ход лабораторной работы

В качестве web-серверов были выбраны два ресурса: <https://lkfl2.nalog.ru> — личный кабинет налогоплательщика и <https://ya.ru/> — главная страница поискового сервиса «Яндекс».

Первый ресурс

Начнем с первого сайта. Зайдем через Firefox на lkfl2.nalog.ru и в Wireshark выставим фильтрацию *ip.addr == 213.24.64.175*.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|--|
| 64 | 4.794424092 | 192.168.1.25 | 213.24.64.175 | TCP | 74 | 60304 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=955932658 TSecr=0 WS=128 |
| 65 | 4.794553395 | 192.168.1.25 | 213.24.64.175 | TCP | 74 | 60306 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=955932658 TSecr=0 WS=128 |
| 62 | 4.812647399 | 213.24.64.175 | 192.168.1.25 | TCP | 70 | 443 → 60306 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=3714129173 TSecr=955932658 |
| 64 | 4.812690791 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60306 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSval=955932676 TSecr=3714129173 |
| 65 | 4.813714218 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 728 | Client Hello |
| 66 | 4.836941562 | 213.24.64.175 | 192.168.1.25 | TCP | 66 | 443 → 60306 [ACK] Seq=1 Ack=663 Win=5042 Len=0 TSval=3714129197 TSecr=955932677 |
| 67 | 4.839448832 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1514 | Server Hello |
| 68 | 4.839472336 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60306 → 443 [ACK] Seq=663 Ack=1449 Win=63712 Len=0 TSval=955932703 TSecr=3714129199 |
| 69 | 4.839497544 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 2763 | Certificate, Server Key Exchange, Server Hello Done |
| 70 | 4.839506361 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60306 → 443 [ACK] Seq=663 Ack=4146 Win=62264 Len=0 TSval=955932703 TSecr=3714129199 |
| 71 | 4.841473856 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 192 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 73 | 4.856245933 | 213.24.64.175 | 192.168.1.25 | TCP | 66 | 443 → 60306 [ACK] Seq=4146 Ack=789 Win=5168 Len=0 TSval=3714129216 TSecr=955932705 |
| 74 | 4.856456662 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 72 | Change Cipher Spec |
| 75 | 4.856480196 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 111 | Encrypted Handshake Message |
| 76 | 4.856525060 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60306 → 443 [ACK] Seq=789 Ack=4197 Win=63712 Len=0 TSval=955932720 TSecr=3714129217 |
| 77 | 4.856742801 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 871 | Application Data |
| 80 | 4.874052088 | 213.24.64.175 | 192.168.1.25 | TCP | 66 | 443 → 60306 [ACK] Seq=4197 Ack=1594 Win=5973 Len=0 TSval=3714129235 TSecr=955932720 |
| 81 | 4.875657151 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 481 | Application Data |
| 86 | 4.922358390 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60306 → 443 [ACK] Seq=1594 Ack=4612 Win=63712 Len=0 TSval=955932786 TSecr=3714129236 |
| 87 | 5.062673786 | 192.168.1.25 | 213.24.64.175 | TCP | 74 | 60308 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=955932926 TSecr=0 WS=128 |
| 88 | 5.078735243 | 213.24.64.175 | 192.168.1.25 | TCP | 70 | 443 → 60308 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1 TSval=3714129439 TSecr=955932926 |
| 89 | 5.078765790 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60308 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSval=955932942 TSecr=3714129439 |
| 90 | 5.079943328 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 728 | Client Hello |
| 91 | 5.094450187 | 213.24.64.175 | 192.168.1.25 | TCP | 66 | 443 → 60308 [ACK] Seq=1 Ack=663 Win=5042 Len=0 TSval=3714129455 TSecr=955932943 |
| 92 | 5.097377891 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1514 | Server Hello |
| 93 | 5.097388712 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60308 → 443 [ACK] Seq=663 Ack=1449 Win=63712 Len=0 TSval=955932961 TSecr=3714129457 |
| 94 | 5.097446991 | 213.24.64.175 | 192.168.1.25 | TCP | 1514 | 443 → 60308 [ACK] Seq=1449 Ack=663 Win=5042 Len=1448 TSval=3714129457 TSecr=955932943 [TCP segment of a reassembled PDU] |
| 95 | 5.097455247 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60308 → 443 [ACK] Seq=663 Ack=2897 Win=62264 Len=0 TSval=955932961 TSecr=3714129457 |
| 96 | 5.098054155 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1315 | Certificate, Server Key Exchange, Server Hello Done |
| 97 | 5.099060903 | 192.168.1.25 | 213.24.64.175 | TCP | 66 | 60308 → 443 [ACK] Seq=663 Ack=4146 Win=63712 Len=0 TSval=955932961 TSecr=3714129457 |
| 98 | 5.099090607 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 192 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 101 | 5.116017403 | 213.24.64.175 | 192.168.1.25 | TCP | 66 | 443 → 60308 [ACK] Seq=4146 Ack=789 Win=5168 Len=0 TSval=3714129476 TSecr=955932962 |
| 102 | 5.116784508 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 72 | Change Cipher Spec |
| 103 | 5.116784708 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 111 | Encrypted Handshake Message |

Первый этап соединения — сообщение от клиента Client Hello.

| | | | | | | |
|---|-------------|---------------|---------------|---------|----------------|--------------|
| 65 | 4.813714218 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 728 | Client Hello |
| 66 | 4.836841562 | 213.24.64.175 | 192.168.1.25 | TCP | 66 443 → 60306 | [ACK] |
| 67 | 4.839448832 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1514 | Server Hello |
| ▶ Transmission Control Protocol, Src Port: 60306, Dst Port: 443, Seq: 1, Ack: 1, Len: 662 | | | | | | |
| ▼ Transport Layer Security | | | | | | |
| ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello | | | | | | |
| Content Type: Handshake (22) | | | | | | |
| Version: TLS 1.0 (0x0301) | | | | | | |
| Length: 657 | | | | | | |
| ▼ Handshake Protocol: Client Hello | | | | | | |
| Handshake Type: Client Hello (1) | | | | | | |
| Length: 653 | | | | | | |
| Version: TLS 1.2 (0x0303) | | | | | | |
| ▶ Random: a64759d56efb5e39042540dec5300d336e9850da54991d250803a6c06a561dfc | | | | | | |
| Session ID Length: 32 | | | | | | |
| Session ID: 0047a075e3de3c75799edebc81b1bef15ff74721750e2b50585b01c12b819e9a | | | | | | |
| Cipher Suites Length: 34 | | | | | | |
| ▼ Cipher Suites (17 suites) | | | | | | |
| Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) | | | | | | |
| Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) | | | | | | |
| Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) | | | | | | |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) | | | | | | |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | | | | | | |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) | | | | | | |
| Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | | | | | | |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) | | | | | | |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | | | | | | |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) | | | | | | |
| Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) | | | | | | |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | | | | | | |
| Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | | | | | | |
| Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) | | | | | | |
| Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) | | | | | | |
| Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) | | | | | | |
| Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) | | | | | | |
| Compression Methods Length: 1 | | | | | | |

Здесь можно увидеть версию протокола — TLSv1.2, также набор поддерживаемых клиентом алгоритмов шифрования (Cipher Suites) и случайное число (Random), которое будет использоваться для создания сеансового ключа.

Второй этап — сообщение от сервера Server Hello.

| | | | | | |
|----|-------------|---------------|---------------|---------|--|
| 67 | 4.839448832 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1514 Server Hello |
| 68 | 4.839472336 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] |
| 69 | 4.839497544 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 2763 Certificate, Server Key Exchange, Server Hello Done |
| 70 | 4.839506381 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] |

▶ Frame 67: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface eno1
 ▶ Ethernet II, Src: Sagemcom_b7:82:ac (30:24:78:b7:82:ac), Dst: Giga-Byt_92:05:69 (b4:2e:99:92:05:69)
 ▶ Internet Protocol Version 4, Src: 213.24.64.175, Dst: 192.168.1.25
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 60306, Seq: 1, Ack: 663, Len: 1448

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 91
- ▼ Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 87
 - Version: TLS 1.2 (0x0303)
 - ▶ Random: 5a1981e959b1454ee4a3754abc0712288ecaddfae537df2b618f5552458d760e
 - Session ID Length: 32
 - Session ID: e4f3b69c58d74b200dfba559025f32eb32569ab56a5b93ea0505f213506f0279
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Compression Method: null (0)
 - Extensions Length: 15
 - ▶ Extension: renegotiation_info (len=1)
 - ▶ Extension: ec_point_formats (len=2)
 - ▶ Extension: extended_master_secret (len=0)

[JA3S Fullstring: 771,49199,65281-11-23]
 [JA3S: 76c691f46143bf86e2d1bb73c6187767]

Здесь можно увидеть выбранный алгоритм шифрования (Cipher Suite) — TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 и рандомное число (Random) для создания сеансового ключа.

Третий этап — сообщение от сервера Certificate, Server Key Exchange, Server Hello Done.

| | | | | | |
|----|-------------|---------------|---------------|---------|--|
| 67 | 4.839448832 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 1514 Server Hello |
| 68 | 4.839472336 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] Seq=663 Ack=1449 Win=63712 Len=0 TSval=955932703 TSecr=3714129199 |
| 69 | 4.839497544 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 2763 Certificate, Server Key Exchange, Server Hello Done |
| 70 | 4.839506381 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] Seq=663 Ack=1446 Win=62264 Len=0 TSval=955932703 TSecr=3714129199 |

▶ Frame 69: 2763 bytes on wire (22104 bits), 2763 bytes captured (22104 bits) on interface eno1, id 0
 ▶ Ethernet II, Src: Sagemcom_b7:82:ac (30:24:78:b7:82:ac), Dst: Giga-Byt_92:05:69 (b4:2e:99:92:05:69)
 ▶ Internet Protocol Version 4, Src: 213.24.64.175, Dst: 192.168.1.25
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 60306, Seq: 1449, Ack: 663, Len: 2697
 ▶ [2 Reassembled TCP Segments (3702 bytes): #67(1352), #69(2350)]

▼ Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3697
- ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3693
 - Certificates Length: 3690
 - Certificates (3690 bytes)
 - ▶ Certificate Length: 1610
 - ▶ Certificate: 3082040b30820398a093020102020c99e255c3407668044dd5cf2a390d96092a864886f7... (id-at-commonName=.nalog.ru)
 - ▶ Certificate Length: 1204
 - ▶ Certificate: 3082040b30820398a093020102021077bd9e6742d5d9e9d049d774d02a6f9a300d06092a... (id-at-commonName=GlobalSign GCC R3 DV TLS CA 2020,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)
 - ▶ Certificate Length: 867
 - ▶ Certificate: 3082035f30820247a093020102020b04000000000121585308a2300d06092a864886f70d... (id-at-commonName=GlobalSign,id-at-organizationName=GlobalSign,id-at-organizationalUnitName=GlobalSign Root CA - R3)
- ▼ Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 333
 - ▼ Handshake Protocol: Server Key Exchange
 - Handshake Type: Server Key Exchange (12)
 - Length: 329
 - EC Diffie-Hellman Server Params
 - Curve Type: named_curve (0x03)
 - Named Curve: secp256r1 (0x0017)
 - Pubkey Length: 65
 - Pubkey: 0493f517b390222f07ecf46c9190e1c8ba5dfca8f4cee3852e5575d902ba708c443b3a...
 - Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
 - Signature Length: 256
 - Signature: 217d37195eb044dd3614387563bf30e6a71ed3155fee73cf7a04ffa0854b2d75518ebd27...
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 4
 - Handshake Protocol: Server Hello Done
 - Handshake Type: Server Hello Done (14)
 - Length: 0

Здесь есть цепочка сертификатов (Certificate): первый — сервера, последний — центра сертификации. Server Key Exchange содержит публичный ключ

для создания pre-master secret, который тоже используется для создания сессионного симметричного ключа. Server Hello Done говорит, что начальный этап установки соединения завершен.

Четвертый этап — сообщение от клиента Client Key Exchange, Change Cipher Spec, Finished.

| | | | | | |
|----|-------------|---------------|---------------|---------|--|
| 69 | 4.839497544 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 2763 Certificate, Server Key Exchange, Server Hello Done |
| 70 | 4.839506381 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] Seq=663 Ack=4146 Win=62264 Len=0 TSval=955932703 TS |
| 71 | 4.841473856 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 192 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 73 | 4.856245033 | 213.24.64.175 | 192.168.1.25 | TCP | 66 443 → 60306 [ACK] Seq=4146 Ack=789 Win=5168 Len=0 TSval=3714129216 TS |

Frame 71: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface eno1, id 0

Ethernet II, Src: Giga-Byt_92:05:69 (b4:2e:99:92:05:69), Dst: Sagemcom_b7:82:ac (30:24:78:b7:82:ac)

Internet Protocol Version 4, Src: 192.168.1.25, Dst: 213.24.64.175

Transmission Control Protocol, Src Port: 60306, Dst Port: 443, Seq: 663, Ack: 4146, Len: 126

Transport Layer Security

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 70
 - ▼ Handshake Protocol: Client Key Exchange
 - Handshake Type: Client Key Exchange (16)
 - Length: 66
 - ▼ EC Diffie-Hellman Client Params
 - Pubkey Length: 65
 - Pubkey: 042f65077976e5ae15d2f438530b9ee0108e69913049ede65295dd5b24d1b79de283632...
 - ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: TLS 1.2 (0x0303)
 - Length: 1
 - Change Cipher Spec Message
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 40
 - Handshake Protocol: Encrypted Handshake Message

В Client Key Exchange клиент передает свою часть публичного ключа для pre-master secret. В Change Cipher Spec клиент говорит, что готов перейти на защищенное соединение. В Finished (Encrypted Handshake Message) содержится первое зашифрованное сообщение.

Пятый этап — сообщения от сервера Change Cipher Spec и Finished.

| | | | | | |
|----|-------------|---------------|---------------|---------|------------------------------|
| 74 | 4.856456662 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 72 Change Cipher Spec |
| 75 | 4.856480196 | 213.24.64.175 | 192.168.1.25 | TLSv1.2 | 111 Encrypted Handshake Mess |
| 76 | 4.856525060 | 192.168.1.25 | 213.24.64.175 | TCP | 66 60306 → 443 [ACK] Seq=78 |
| 77 | 4.856742801 | 192.168.1.25 | 213.24.64.175 | TLSv1.2 | 871 Application Data |

Frame 74: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eno1, id 0

Ethernet II, Src: Sagemcom_b7:82:ac (30:24:78:b7:82:ac), Dst: Giga-Byt_92:05:69 (b4:2e:99:92:05:69)

Internet Protocol Version 4, Src: 213.24.64.175, Dst: 192.168.1.25

Transmission Control Protocol, Src Port: 443, Dst Port: 60306, Seq: 4146, Ack: 789, Len: 6

Transport Layer Security

- ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 - Content Type: Change Cipher Spec (20)
 - Version: TLS 1.2 (0x0303)
 - Length: 1
 - Change Cipher Spec Message

После этого этапа соединение считается установленным.

Запишем информацию для этого сайта:

- Имя сервера: lkfl2.nalog.ru
- IP-адрес: 213.24.64.175
- Версия TLS: 1.2
- Выбранные алгоритмы шифрования:
TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256
- Сертификаты:



Common name: *.nalog.ru
SANs: *.nalog.ru, nalog.ru
Valid from November 17, 2023 to December 18, 2024
Serial Number: 09e255c3407668044dd5cf2a
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign GCC R3 DV TLS CA 2020



Common name: GlobalSign GCC R3 DV TLS CA 2020
Organization: GlobalSign nv-sa
Location: BE
Valid from July 27, 2020 to March 17, 2029
Serial Number: 77bd0e0742d5d9e9d049d774d02a6f9a
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign



Common name: GlobalSign
Organization: GlobalSign **Org. Unit:** GlobalSign Root CA - R3
Valid from March 18, 2009 to March 18, 2029
Serial Number: 04000000000121585308a2
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign

- Время установки соединения (от ClientHello до Finished): 0.042765978 секунды.

Второй ресурс

Перейдем ко второму сайту — ya.ru с ip 5.255.255.242.

| ip.addr == 5.255.255.242 | | | | | | |
|--------------------------|--------------|---------------|---------------|----------|--------|--|
| o. | Time | Source | Destination | Protocol | Length | Info |
| 3085 | 97.655879900 | 5.255.255.242 | 192.168.1.25 | TCP | 74 | 443 → 46758 [SYN, ACK] Seq=0 Ack=1 Win=43338 Len=0 MSS=1410 SACK_PERM=1 TSval=179099053 |
| 3086 | 97.655937909 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46758 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4170438025 TSecr=1790990536 |
| 3087 | 97.657210897 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 719 | Client Hello |
| 3092 | 97.670755521 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=1 Ack=654 Win=42752 Len=0 TSval=1718563701 TSecr=4170438023 |
| 3093 | 97.671398893 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1274 | Server Hello, Change Cipher Spec, Application Data |
| 3094 | 97.671422517 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=654 Ack=1209 Win=64128 Len=0 TSval=4170438041 TSecr=1718563701 |
| 3095 | 97.671930744 | 5.255.255.242 | 192.168.1.25 | TCP | 1274 | 443 → 46746 [PSH, ACK] Seq=1209 Ack=654 Win=42752 Len=1208 TSval=1718563701 TSecr=41704 |
| 3096 | 97.671951383 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=654 Ack=2417 Win=63744 Len=0 TSval=4170438041 TSecr=1718563701 |
| 3097 | 97.671986880 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1692 | Application Data, Application Data, Application Data |
| 3100 | 97.672009413 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=654 Ack=4043 Win=62208 Len=0 TSval=4170438042 TSecr=1718563701 |
| 3105 | 97.674621132 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46758 [ACK] Seq=1 Ack=654 Win=42752 Len=0 TSval=1790990554 TSecr=4170438027 |
| 3106 | 97.676053631 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1274 | Server Hello, Change Cipher Spec, Application Data |
| 3107 | 97.676064151 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46758 → 443 [ACK] Seq=654 Ack=1209 Win=64128 Len=0 TSval=4170438046 TSecr=1790990554 |
| 3108 | 97.676551058 | 5.255.255.242 | 192.168.1.25 | TCP | 1274 | 443 → 46758 [PSH, ACK] Seq=1209 Ack=654 Win=42752 Len=1208 TSval=1790990554 TSecr=41704 |
| 3109 | 97.676557510 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46758 → 443 [ACK] Seq=654 Ack=2417 Win=63744 Len=0 TSval=4170438046 TSecr=1790990554 |
| 3110 | 97.676646157 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1692 | Application Data, Application Data, Application Data |
| 3111 | 97.676654232 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46758 → 443 [ACK] Seq=654 Ack=4043 Win=62208 Len=0 TSval=4170438046 TSecr=1790990554 |
| 3141 | 97.926305540 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 146 | Change Cipher Spec, Application Data |
| 3142 | 97.926740830 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 236 | Application Data |
| 3143 | 97.926765296 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 778 | Application Data |
| 3144 | 97.937839537 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=4043 Ack=734 Win=42752 Len=0 TSval=1718563968 TSecr=4170438296 |
| 3145 | 97.938464124 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 576 | Application Data, Application Data |
| 3146 | 97.938464374 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 127 | Application Data |
| 3147 | 97.938489612 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=1616 Ack=4553 Win=64128 Len=0 TSval=4170438308 TSecr=1718563968 |
| 3148 | 97.938505121 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=1616 Ack=4614 Win=64128 Len=0 TSval=4170438308 TSecr=1718563968 |
| 3149 | 97.938973834 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 97 | Application Data |
| 3150 | 97.942398946 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=4614 Ack=904 Win=42752 Len=0 TSval=1718563973 TSecr=4170438296 |
| 3151 | 97.942440924 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=4614 Ack=1616 Win=42240 Len=0 TSval=1718563973 TSecr=4170438296 |
| 3152 | 97.942461933 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 110 | Application Data |
| 3158 | 97.956976345 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 999 | Application Data |
| 3159 | 97.957014868 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=1647 Ack=5591 Win=64128 Len=0 TSval=4170438327 TSecr=1718563973 |
| 3160 | 97.958709099 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46758 → 443 [FIN, ACK] Seq=654 Ack=4043 Win=64128 Len=0 TSval=4170438328 TSecr=179099055 |
| 3161 | 97.959770379 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 220 | Application Data |
| 3165 | 97.974288135 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=5591 Ack=1801 Win=42496 Len=0 TSval=1718564004 TSecr=4170438329 |

Сервер использует TLSv1.3. Здесь в отличии от TLSv1.2 будут три этапа.

Первая этап соединения — сообщение от клиента Client Hello.

| | | | | | | |
|------|--------------|---------------|---------------|---------|------|------------------------|
| 3087 | 97.657210897 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 719 | Client Hello |
| 3092 | 97.670755521 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq= |
| 3093 | 97.671398893 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1274 | Server Hello, Change C |
| 3094 | 97.671422517 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq= |
| 3095 | 97.671930744 | 5.255.255.242 | 192.168.1.25 | TCP | 1274 | 443 → 46746 [PSH, ACK] |

```

▶ Frame 3087: 719 bytes on wire (5752 bits), 719 bytes captured (5752 bits) on interface eno1, id 0
▶ Ethernet II, Src: Giga-Byt_92:05:69 (b4:2e:99:92:05:69), Dst: Sagemcom_b7:82:ac (30:24:78:b7:82:ac)
▶ Internet Protocol Version 4, Src: 192.168.1.25, Dst: 5.255.255.242
▶ Transmission Control Protocol, Src Port: 46758, Dst Port: 443, Seq: 1, Ack: 1, Len: 653
▼ Transport Layer Security
  ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 648
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 644
      Version: TLS 1.2 (0x0303)
      Random: 01bec8756157d02efa07d4a3f3820ca37630e378e86bee99df4f942e0ea6ef01
      Session ID Length: 32
      Session ID: 5b19e156b70ede0c060de18477f905a81e4e31a991fcea8362b1457381271617
      Cipher Suites Length: 34
      ▶ Cipher Suites (17 suites)
      Compression Methods Length: 1
      ▶ Compression Methods (1 method)
      Extensions Length: 537
      ▶ Extension: server_name (len=10)
      ▶ Extension: extended_master_secret (len=0)
      ▶ Extension: renegotiation_info (len=1)
      ▶ Extension: supported_groups (len=14)
      ▶ Extension: ec_point_formats (len=2)
      ▶ Extension: session_ticket (len=0)
      ▶ Extension: application_layer_protocol_negotiation (len=14)
      ▶ Extension: status_request (len=5)
      ▶ Extension: delegated_credentials (len=10)
      ▶ Extension: key_share (len=107)

```

Здесь всё то же самое, как и в TLSv1.2. Но стоит обратить внимание на key_share — это поле будет и в ответе сервера, это значение используется для создания pre-master secret.

Второй этап — сообщение от сервера Server Hello, Change Cipher Spec, Finished.

| | | | | | | |
|------|--------------|---------------|---------------|---------|------|---|
| 3093 | 97.671398893 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1274 | Server Hello, Change Cipher Spec, Application Data |
| 3094 | 97.671422517 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=654 Ack=1209 Win=64128 Len=0 |
| 3095 | 97.671930744 | 5.255.255.242 | 192.168.1.25 | TCP | 1274 | 443 → 46746 [PSH, ACK] Seq=1209 Ack=654 Win=42752 Len=0 |
| 3096 | 97.671951383 | 192.168.1.25 | 5.255.255.242 | TCP | 66 | 46746 → 443 [ACK] Seq=654 Ack=2417 Win=63744 Len=0 |
| 3097 | 97.671986880 | 5.255.255.242 | 192.168.1.25 | TLSv1.3 | 1692 | Application Data, Application Data |

▶ Frame 3093: 1274 bytes on wire (10192 bits), 1274 bytes captured (10192 bits) on interface eno1, id 0

▶ Ethernet II, Src: Sagemcom_b7:82:ac (30:24:78:b7:82:ac), Dst: Giga-Byt_92:05:69 (b4:2e:99:92:05:69)

▶ Internet Protocol Version 4, Src: 5.255.255.242, Dst: 192.168.1.25

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 46746, Seq: 1, Ack: 654, Len: 1208

▼ Transport Layer Security

 ▼ 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: 37576b2ffa38aba9d0857bb9a03ad618194cbcf7fdee212bad79ef10ab8f93a0

 Session ID Length: 32

 Session ID: 22b6f4c447158d64420406f2bb1d791807c3aa4e307123abeb3a98f782398e58

 Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

 Compression Method: null (0)

 Extensions Length: 46

 ▶ Extension: supported_versions (len=2)

 ▶ Extension: key_share (len=36)

 [JA3S Fullstring: 771,4866,43-51]

 [JA3S: 15af977ce25de452b96affa2addb1036]

 ▼ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

 Content Type: Change Cipher Spec (20)

 Version: TLS 1.2 (0x0303)

 Length: 1

 Change Cipher Spec Message

 ▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls

 Opaque Type: Application Data (23)

 Version: TLS 1.2 (0x0303)

 Length: 32

 Encrypted Application Data: 0da6e03e8b84d65643804d56eb41df079c3f7e318bde8b0150f27de00520f71d

 [Application Data Protocol: http-over-tls]

Видим здесь Change Cipher Spec. Значит, все остальные сообщения (например, Certificate, Finished) будут зашифрованы.

Третий этап — сообщение от клиента Change Cipher Spec, Finished.

| | | | | | | |
|------|--------------|---------------|---------------|---------|-----|--|
| 3141 | 97.926305540 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 146 | Change Cipher Spec, Application Data |
| 3142 | 97.926740830 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 236 | Application Data |
| 3143 | 97.926765296 | 192.168.1.25 | 5.255.255.242 | TLSv1.3 | 778 | Application Data |
| 3144 | 97.927820527 | 5.255.255.242 | 192.168.1.25 | TCP | 66 | 443 → 46746 [ACK] Seq=1209 Ack=724 Win=0 |

▶ Frame 3141: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface eno1, id 0

▶ Ethernet II, Src: Giga-Byt_92:05:69 (b4:2e:99:92:05:69), Dst: Sagemcom_b7:82:ac (30:24:78:b7:82:ac)

▶ Internet Protocol Version 4, Src: 192.168.1.25, Dst: 5.255.255.242

▶ Transmission Control Protocol, Src Port: 46746, Dst Port: 443, Seq: 654, Ack: 4043, Len: 80

▼ Transport Layer Security

 ▼ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

 Content Type: Change Cipher Spec (20)

 Version: TLS 1.2 (0x0303)

 Length: 1

 Change Cipher Spec Message

 ▼ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls

 Opaque Type: Application Data (23)

 Version: TLS 1.2 (0x0303)

 Length: 69

 Encrypted Application Data: fdad86f69dee58455d179dc1af733b0cf855203799bfdb754075b0e723a0b95fb2c5f6d9...

 [Application Data Protocol: http-over-tls]

Клиент тоже начинает шифровать сообщения и отправляет Finished.

Запишем информацию для этого сайта:

- Имя сервера: ya.ru
- IP-адрес: 5.255.255.242

- Версия TLS: 1.3
- Выбранные алгоритмы шифрования: TLS_AES_256_GCM_SHA384
- Сертификаты:



Common name: *.xn--d1acp3f.xn--p1ai
SANs: *.xn--d1acp3f.xn--p1ai, *.yandex.az, yandex.az, *.yandex.by, yandex.by, *.yandex.co.il, yandex.co.il, *.yandex.com, yandex.com, *.yandex.com.am, yandex.com.am, *.yandex.com.ge, yandex.com.ge, *.yandex.com.tr, yandex.com.tr, *.yandex.ee, yandex.ee, *.yandex.fr, yandex.fr, *.yandex.kz, yandex.kz, *.yandex.lt, yandex.lt, *.yandex.lv, yandex.lv, *.yandex.md, yandex.md, *.yandex.ru, yandex.ru, *.yandex.tj, yandex.tj, *.yandex.tm, yandex.tm, *.yandex.uz, yandex.uz, *.ya.ru, ya.ru, *.yandex.de, yandex.de, *.yandex.org, yandex.org, *.yandex.net, yandex.net, *.yandex.jobs, yandex.jobs, *.yandex.aero, yandex.aero, xn--d1acp3f.xn--p1ai
Organization: YANDEX LLC
Location: Moscow, Moscow, RU
Valid from March 4, 2024 to September 1, 2024
Serial Number: 7097913e97c436858de28d6c
Signature Algorithm: ecdsa-with-SHA384
Issuer: GlobalSign ECC OV SSL CA 2018



Common name: GlobalSign ECC OV SSL CA 2018
Organization: GlobalSign nv-sa
Location: BE
Valid from November 20, 2018 to November 20, 2028
Serial Number: 01ee5f2295424905f90191a8dc
Signature Algorithm: ecdsa-with-SHA384
Issuer: GlobalSign



Common name: GlobalSign
Organization: GlobalSign Org. Unit: GlobalSign ECC Root CA - R5
Valid from June 18, 2019 to January 28, 2028
Serial Number: 751e3f53e3185933e95f08eceed0297
Signature Algorithm: sha384WithRSAEncryption
Issuer: GlobalSign Root CA

- Время установки соединения (от ClientHello до Finished): 0.269094643 секунды.

TLS 1.0

При смене версии TLS на клиенте удалось подключиться к обоим ресурсам. Но на сайте ya.ru появилось предупреждение о «незащищённом соединении». А на сайте lkfl2.nalog.ru никакого предупреждения не было.



5 Выводы

В ходе лабораторной работы ознакомился с протоколом TLS, в частности со структурой и работой его версий: TLS 1.2 и TLS 1.3. Научился с помощью программы Wireshark анализировать трафик сети.

В качестве примеров были выбраны два веб-сервера и проведён сравнительный анализ. На его основе можно сделать следующие выводы:

1) Максимальная версия TLS, поддерживаемая **государственным** сайтом lkfl2.nalog.ru — 1.2, т.е. не самая актуальная. При этом сайт поддерживает TLS 1.0 и никак об этом не предупреждает — хотя TLS 1.0 является deprecated. Кажется, что здесь есть проблема с безопасностью.

2) Сайт ya.ru поддерживает TLS 1.3 — актуальную версию протокола. При этом сервер поддерживает и TLS 1.0 (видимо, для большего охвата аудитории), но честно предупреждает, что используется «незащищённое соединение».

3) Было замерено время установки соединения для двух веб-серверов. Сайт ya.ru с TLS 1.3 устанавливал соединение гораздо дольше, чем сайт lkfl2.nalog.ru с TLS 1.2. Но это не означает, что работа TLS 1.2 быстрее, т.к. тут дело ещё в самом сервере — в частности его местоположении относительно клиента. Хотя и обе версии используют гибридное шифрование, TLS 1.3 требует на установку соединения меньше запросов, из чего можно предположить, что эта версия протокола может работать быстрее версии 1.2.

6 Список используемой литературы

1. Wireshark — подробное руководство по началу использования — <https://habr.com/ru/articles/735866/>
2. Основы HTTPS, TLS, SSL. Создание собственных X.509 сертификатов. Пример настройки TLSv1.2 в Spring Boot — <https://habr.com/ru/articles/593507/>
3. Decoding TLS v1.2 Protocol Handshake With Wireshark — <https://theseckmaster.com/blog/decoding-tls-v1-2-protocol-handshake-with-wireshark>
4. Decoding TLS 1.3 Protocol Handshake With Wireshark — <https://theseckmaster.com/blog/decoding-tls-1-3-protocol-handshake-with-wireshark>