Осипов Артём Максимович
ФИТУ, 1 курс, 020303 АИСа-о24

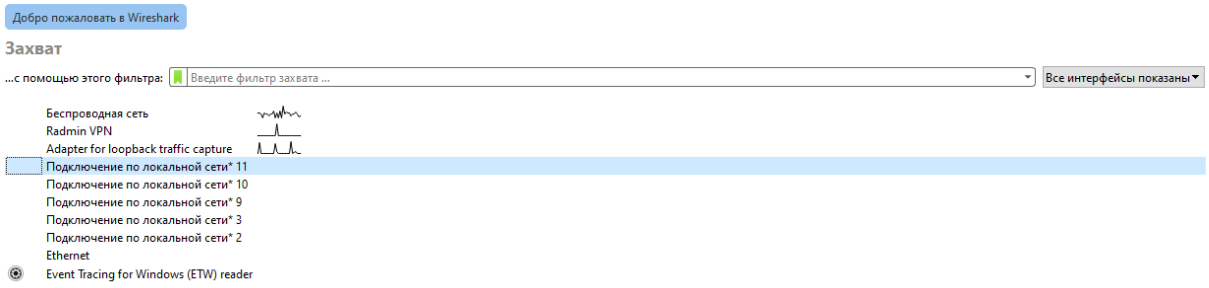
Практическое задание №1

Цель работы: Ознакомиться с различиями в работе протоколов HTTP и HTTPS при помощи анализатора пакетов Wireshark

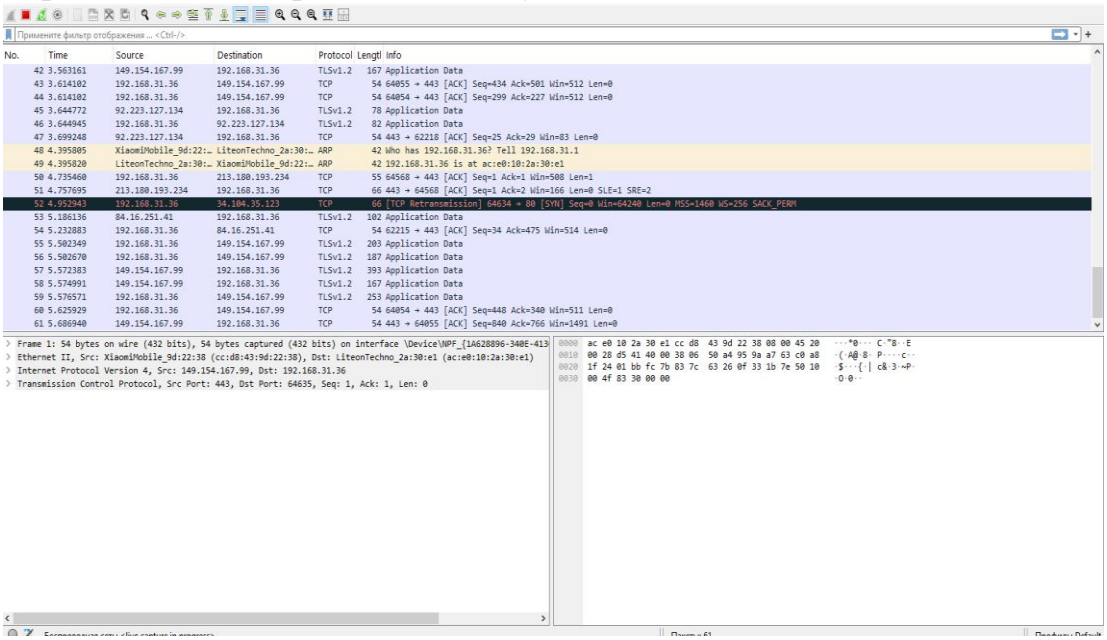
Задание: Запустить перехват сетевых пакетов в Wireshark, выполнить перехват сетевых пакетов для заданного узла для определения IP адреса целевого узла, выбрать любой пакет открыть HTTP Stream для просмотра убедиться, что заданный ресурс не использует шифрование, а содержимое пакетов представлено в открытом виде, выполнить перехват сетевых пакетов для заданного узла для определения IP адреса. Убедиться, что пакеты, передаваемые между клиентом и сервером зашифрованы выполнить анализ TLS рукопожатия (TLS Handshake). Отразить в отчете фазы Client Hello, Server Hello и то, какими данными клиент и сервер обмениваются в это время. Если имеет место быть повышение версии TLS - описать, как это происходит.

Ход работы:

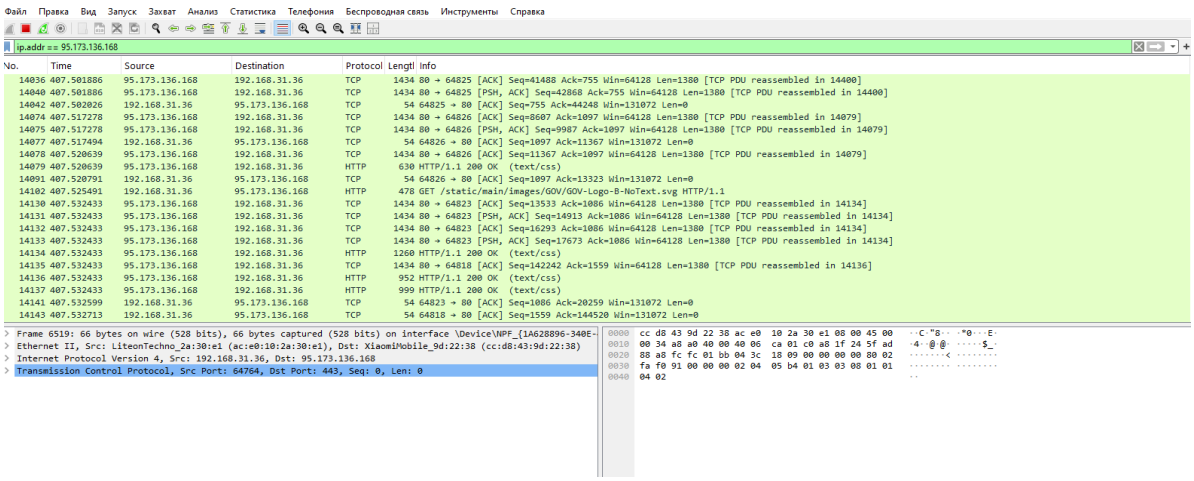
1. Запускаю Wireshark, на главной странице:



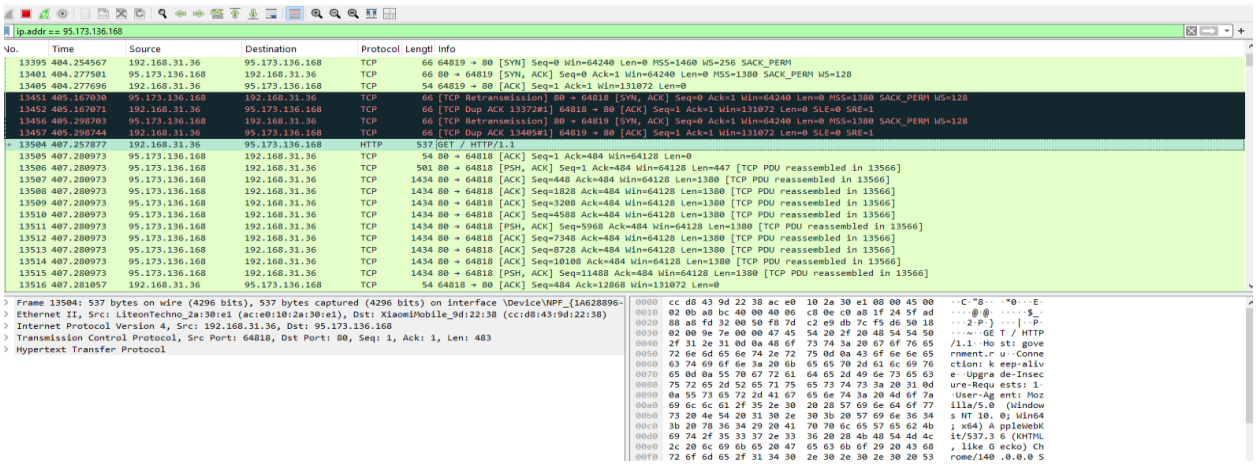
2. Выполняю перехват сетевых пакетов для заданного узла для определения IP адреса целевого узла:



3. Захожу на сайт правительства и прогружаю его, дальше с помощью улиты nslookup нахожу ip адрес, сортирую по нему и выполняю перехват сетевых пакетов для заданного узла для определения IP адреса:



4. Выбираю пакет `GET / HTTP/1.1`



5. Открываю HTTP Stream для просмотра, убеждаюсь что заданный пакет не использует шифрование

```
GET / HTTP/1.1
Host: government.ru
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7


HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 Sep 2025 23:11:31 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 67235
Connection: keep-alive
Keep-Alive: timeout=60
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: http://services.government.ru
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Authorization
Access-Control-Allow-Credentials: true
Vary: Origin

<!DOCTYPE html>
<html dir="ltr" lang="ru-RU">
<head>

    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <meta name="author" content="Government.ru">

    <!-- Stylesheets
    ============================================= -->
    <link rel="stylesheet" href="/static/main/css/bootstrap.css" type="text/css">
    <link rel="stylesheet" href="/static/main/style.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/dark.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/font-icons.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/animate.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/magnific-popup.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/responsive.css" type="text/css">
    <link rel="stylesheet" href="/static/main/css/components/bs-select.css" type="text/css">

    <!-- Range Slider CSS -->
    <link href="/static/main/css/components/ion.rangeslider.css" rel="stylesheet" type="text/css">
```

6. Захожу на сайт нпи, тыкже выполняю перехват сетевых пакетов и вижу что пакеты передоваемые между клиентом и сервером зашифрованы

```
22066 600.988170    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=12350 Ack=2616 Win=31872 Len=1440 [TCP PDU reassembled in 22067]
22067 600.988170    195.209.112.86    192.168.31.36     TLSv1.3   598 Application Data
22071 600.988318    192.168.31.36     195.209.112.86    TCP        54 64896 → 443 [ACK] Seq=2616 Ack=14334 Win=132352 Len=0
22076 601.007973    192.168.31.36     195.209.112.86    TLSv1.3   198 Application Data
22077 601.008480    192.168.31.36     195.209.112.86    TLSv1.3   175 Application Data
22079 601.011550    192.168.31.36     195.209.112.86    TLSv1.3   196 Application Data
22080 601.012168    192.168.31.36     195.209.112.86    TLSv1.3   135 Application Data
22081 601.016852    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=14334 Ack=2881 Win=31872 Len=1440 [TCP PDU reassembled in 22085]
22082 601.016852    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=15774 Ack=2881 Win=31872 Len=1440 [TCP PDU reassembled in 22085]
22083 601.016852    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=17214 Ack=2881 Win=31872 Len=1440 [TCP PDU reassembled in 22085]
22084 601.016852    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [PSH, ACK] Seq=18654 Ack=2881 Win=31872 Len=1440 [TCP PDU reassembled in 22085]
22085 601.016852    195.209.112.86    192.168.31.36     TLSv1.3   289 Application Data
22086 601.016852    195.209.112.86    192.168.31.36     TLSv1.3   896 Application Data
22087 601.016951    192.168.31.36     195.209.112.86    TCP        54 64896 → 443 [ACK] Seq=3104 Ack=21171 Win=132352 Len=0
22088 601.017526    195.209.112.86    192.168.31.36     TCP        54 443 → 64896 [ACK] Seq=21171 Ack=3104 Win=31872 Len=0
22089 601.017526    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=21171 Ack=3104 Win=31872 Len=1440 [TCP PDU reassembled in 22090]
22090 601.017526    195.209.112.86    192.168.31.36     TLSv1.3   907 Application Data
22091 601.017608    192.168.31.36     195.209.112.86    TCP        54 64896 → 443 [ACK] Seq=3104 Ack=23464 Win=132352 Len=0
22092 601.018859    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=23464 Ack=3104 Win=31872 Len=1440 [TCP PDU reassembled in 22109]
22093 601.018859    195.209.112.86    192.168.31.36     TCP      1494 443 → 64896 [ACK] Seq=24904 Ack=3104 Win=31872 Len=1440 [TCP PDU reassembled in 22109]
```

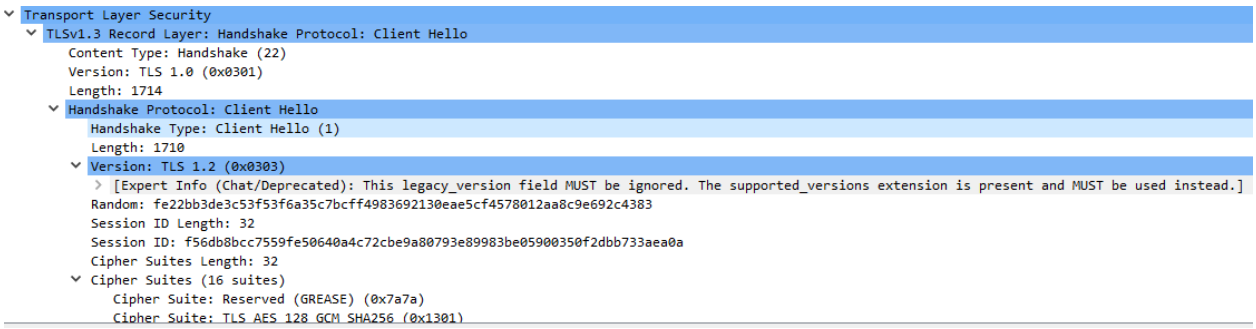
7. *Анализ TLS рукопожатия*

```
22034 600.959901    192.168.31.36     195.209.112.86    TLSv1.3   429 Client Hello (SNI=npi-tu.ru)
22037 600.965390    195.209.112.86    192.168.31.36     TCP        54 443 → 64896 [ACK] Seq=1 Ack=1441 Win=31872 Len=0
22038 600.965390    195.209.112.86    192.168.31.36     TCP        54 443 → 64896 [ACK] Seq=1 Ack=1816 Win=31872 Len=0
22042 600.966665    195.209.112.86    192.168.31.36     TLSv1.3  1494 Server Hello, Change Cipher Spec, Application Data
```

Client Hello:

- SNI: schedule.npi-tu.ru (в расширении server_name)
- Версия TLS: 1.2 (с поддержкой 1.3 через расширение)
- Cipher Suites: 16 алгоритмов

3 алгоритма TLS 1.38 современных ECDHE алгоритмов
5 устаревших для совместимости



Server Hello:

ФАЗА 1: CLIENT HELLO
- Поддерживаемые версии: TLS 1.3, TLS 1.2
- Cipher Suites: 16 алгоритмов
- Supported Groups: (ожидается secp256r1, secp384r1)
ФАЗА 2: SERVER HELLO
- Выбранная версия: TLS 1.3 (повышение с TLS 1.2)
- Выбранный cipher: TLS_AES_128_GCM_SHA256
- Key Share: параметры для обмена ключами
ФАЗА 3: ЗАВЕРШЕНИЕ
- Encrypted handshake messages
- Установлено зашифрованное соединение

Вывод

В ходе работы был проведен сравнительный анализ сетевого трафика с использованием Wireshark. Для сайта government.ru, использующего HTTP-протокол, был успешно перехвачен и проанализирован сетевой трафик. Определен IP-адрес 95.173.136.168 через утилиту nslookup. Анализ HTTP Stream показал, что все данные передаются в открытом виде - видны HTTP-заголовки, параметры запросов и HTML-контент, что подтверждает отсутствие шифрования и уязвимость протокола.

Для сайта npi-tu.ru с HTTPS-протоколом определен IP-адрес 195.209.112.86. Анализ показал, что весь трафик зашифрован - пакеты отображаются как Application Data TLSv1.2, а содержимое недоступно для чтения. Проведен анализ TLS handshake: клиент в Client Hello предложил 16 алгоритмов шифрования и поддержку TLS 1.3/1.2, а сервер в Server Hello выбрал современный TLS 1.3 с алгоритмом TLS_AES_128_GCM_SHA256, что демонстрирует повышение версии протокола

безопасности. Работа наглядно показала критическое различие между незащищенным HTTP и безопасным HTTPS соединениями.