

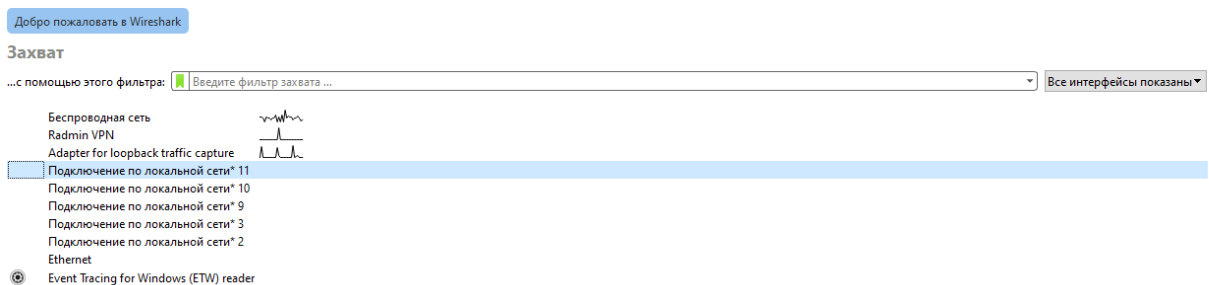
Практическое задание №1

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). Отобразить 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:

No.	Time	Source	Destination	Protocol	Length	Info
42	3.563161	149.154.167.99	192.168.31.36	TLSv1.2	167	Application Data
43	3.614102	192.168.31.36	149.154.167.99	TCP	54	64895 → 443 [ACK] Seq=434 Ack=981 Win=512 Len=0
44	3.614102	192.168.31.36	149.154.167.99	TCP	54	64854 → 443 [ACK] Seq=299 Ack=227 Win=512 Len=0
45	3.644772	92.223.127.134	192.168.31.36	TLSv1.2	70	Application Data
46	3.644945	192.168.31.36	92.223.127.134	TLSv1.2	82	Application Data
47	3.699248	92.223.127.134	192.168.31.36	TCP	54	443 → 62218 [ACK] Seq=25 Ack=29 Win=83 Len=0
48	4.395805	XiaomiMobile_9d:22:30:1e	LiteonTechno_2a:30:e1	ARP	42	Who has 192.168.31.36? Tell 192.168.31.1
49	4.395828	LiteonTechno_2a:30:e1	XiaomiMobile_9d:22:30:1e	ARP	42	192.168.31.36 is at ac:e8:10:2a:30:e1
50	4.755468	192.168.31.36	213.180.193.234	TCP	55	64568 → 443 [ACK] Seq=1 Ack=1 Win=588 Len=1
51	4.757695	213.180.193.234	192.168.31.36	TCP	66	443 → 64568 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
52	4.952943	192.168.31.36	95.173.136.168	TCP	66	[TCP Retransmission] 64634 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
53	5.186136	84.16.251.41	192.168.31.36	TLSv1.2	182	Application Data
54	5.232883	192.168.31.36	84.16.251.41	TCP	54	62215 → 443 [ACK] Seq=34 Ack=475 Win=514 Len=0
55	5.582349	192.168.31.36	149.154.167.99	TLSv1.2	203	Application Data
56	5.582578	192.168.31.36	149.154.167.99	TLSv1.2	187	Application Data
57	5.572383	149.154.167.99	192.168.31.36	TLSv1.2	393	Application Data
58	5.574991	149.154.167.99	192.168.31.36	TLSv1.2	167	Application Data
59	5.576571	192.168.31.36	149.154.167.99	TLSv1.2	253	Application Data
60	5.625929	192.168.31.36	149.154.167.99	TCP	54	64854 → 443 [ACK] Seq=448 Ack=340 Win=511 Len=0
61	5.680940	149.154.167.99	192.168.31.36	TCP	54	443 → 64855 [ACK] Seq=840 Ack=766 Win=1491 Len=0

Frame 52: 66 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0), 54 bytes from 192.168.31.36 to 95.173.136.168 on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0)

Ethernet II, Src: LiteonTechno_2a:30:e1 (ac:e8:10:2a:30:e1), Dst: XiaomiMobile_9d:22:30:1e (ac:e8:10:2a:30:e1)

Internet Protocol Version 4, Src: 192.168.31.36, Dst: 95.173.136.168

Transmission Control Protocol, Src Port: 443, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

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

No.	Time	Source	Destination	Protocol	Length	Info
14036	407.581886	95.173.136.168	192.168.31.36	TCP	1434	80 → 64825 [ACK] Seq=1488 Ack=755 Win=64128 Len=1380 [TCP PDU reassembled in 14400]
14040	407.581886	95.173.136.168	192.168.31.36	TCP	1434	80 → 64825 [PSH, ACK] Seq=42868 Ack=755 Win=64128 Len=1380 [TCP PDU reassembled in 14400]
14042	407.582026	192.168.31.36	95.173.136.168	TCP	54	64825 → 80 [ACK] Seq=755 Ack=44248 Win=131072 Len=0
14074	407.517278	95.173.136.168	192.168.31.36	TCP	1434	80 → 64826 [ACK] Seq=8607 Ack=1097 Win=64128 Len=1380 [TCP PDU reassembled in 14079]
14075	407.517278	95.173.136.168	192.168.31.36	TCP	1434	80 → 64826 [PSH, ACK] Seq=9987 Ack=1097 Win=64128 Len=1380 [TCP PDU reassembled in 14079]
14077	407.517494	192.168.31.36	95.173.136.168	TCP	54	64826 → 80 [ACK] Seq=1097 Ack=11367 Win=131072 Len=0
14078	407.520639	95.173.136.168	192.168.31.36	TCP	1434	80 → 64826 [ACK] Seq=11367 Ack=1097 Win=64128 Len=1380 [TCP PDU reassembled in 14079]
14079	407.520639	95.173.136.168	192.168.31.36	HTTP	630	HTTP/1.1. 200 OK (text/css)
14091	407.520791	192.168.31.36	95.173.136.168	TCP	54	64826 → 80 [ACK] Seq=1097 Ack=13323 Win=131072 Len=0
14102	407.525491	192.168.31.36	95.173.136.168	HTTP	478	GET /static/main/images/GOV/GOV-Logo-B-NoText.svg HTTP/1.1
14130	407.512433	95.173.136.168	192.168.31.36	TCP	1434	80 → 64823 [ACK] Seq=13533 Ack=1086 Win=64128 Len=1380 [TCP PDU reassembled in 14134]
14131	407.532433	95.173.136.168	192.168.31.36	TCP	1434	80 → 64823 [PSH, ACK] Seq=14913 Ack=1086 Win=64128 Len=1380 [TCP PDU reassembled in 14134]
14132	407.532433	95.173.136.168	192.168.31.36	TCP	1434	80 → 64823 [ACK] Seq=16293 Ack=1086 Win=64128 Len=1380 [TCP PDU reassembled in 14134]
14133	407.532433	95.173.136.168	192.168.31.36	TCP	1434	80 → 64823 [PSH, ACK] Seq=17673 Ack=1086 Win=64128 Len=1380 [TCP PDU reassembled in 14134]
14134	407.532433	95.173.136.168	192.168.31.36	HTTP	1206	HTTP/1.1. 200 OK (text/css)
14135	407.532433	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=142242 Ack=1559 Win=64128 Len=1380 [TCP PDU reassembled in 14136]
14136	407.532433	95.173.136.168	192.168.31.36	HTTP	952	HTTP/1.1. 200 OK (text/css)
14137	407.532433	95.173.136.168	192.168.31.36	HTTP	999	HTTP/1.1. 200 OK (text/css)
14141	407.532599	192.168.31.36	95.173.136.168	TCP	54	64823 → 80 [ACK] Seq=1886 Ack=20259 Win=131072 Len=0
14143	407.532713	192.168.31.36	95.173.136.168	TCP	54	64818 → 80 [ACK] Seq=1559 Ack=144520 Win=131072 Len=0

Frame 6519: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0), 66 bytes from 192.168.31.36 to 95.173.136.168 on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0)

Ethernet II, Src: LiteonTechno_2a:30:e1 (ac:e8:10:2a:30:e1), Dst: XiaomiMobile_9d:22:30:1e (ac:e8:10:2a:30:e1)

Internet Protocol Version 4, Src: 192.168.31.36, Dst: 95.173.136.168

Transmission Control Protocol, Src Port: 64764, Dst Port: 443, Seq: 0, Len: 0

4. Выбираю пакет 'GET / HTTP/1.1'

No.	Time	Source	Destination	Protocol	Length	Info
13395	404.254567	192.168.31.36	95.173.136.168	TCP	66	64819 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13401	404.277581	95.173.136.168	192.168.31.36	TCP	66	80 → 64819 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128
13405	404.277696	192.168.31.36	95.173.136.168	TCP	54	64819 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
13451	405.167030	95.173.136.168	192.168.31.36	TCP	66	[TCP Retransmission] 80 → 64818 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128
13452	405.167091	192.168.31.36	95.173.136.168	TCP	66	[TCP Dup ACK 1337241] 64818 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0 SLE=0 SRE=1
13456	405.208703	95.173.136.168	192.168.31.36	TCP	66	[TCP Retransmission] 80 → 64819 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128
13457	405.208744	192.168.31.36	95.173.136.168	TCP	66	[TCP Dup ACK 1340541] 64819 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0 SLE=0 SRE=1
13504	407.257877	192.168.31.36	95.173.136.168	HTTP	537	GET / HTTP/1.1
13505	407.280973	95.173.136.168	192.168.31.36	TCP	54	80 → 64818 [ACK] Seq=1 Ack=484 Win=64128 Len=0
13506	407.280973	95.173.136.168	192.168.31.36	TCP	501	80 → 64818 [PSH, ACK] Seq=1 Ack=484 Win=64128 Len=447 [TCP PDU reassembled in 13566]
13507	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=448 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13508	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=1828 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13509	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=1208 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13510	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=4588 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13511	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [PSH, ACK] Seq=5968 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13512	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=7348 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13513	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=7728 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13514	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [ACK] Seq=10188 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13515	407.280973	95.173.136.168	192.168.31.36	TCP	1434	80 → 64818 [PSH, ACK] Seq=11488 Ack=484 Win=64128 Len=1380 [TCP PDU reassembled in 13566]
13516	407.281857	192.168.31.36	95.173.136.168	TCP	54	64818 → 80 [ACK] Seq=484 Ack=12868 Win=131072 Len=0

Frame 13504: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0), 537 bytes from 192.168.31.36 to 95.173.136.168 on interface \Device\NPF_{1A628896-340E-4133-B000-000000000000} (en0)

Ethernet II, Src: LiteonTechno_2a:30:e1 (ac:e8:10:2a:30:e1), Dst: XiaomiMobile_9d:22:30:1e (ac:e8:10:2a:30:e1)

Internet Protocol Version 4, Src: 192.168.31.36, Dst: 95.173.136.168

Transmission Control Protocol, Src Port: 64818, Dst Port: 80, Seq: 1, Ack: 1, Len: 483

Hypertext Transfer Protocol

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 передаваемые 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

```
Transport Layer Security
  TLv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1714
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 1710
  Version: TLS 1.2 (0x0303)
    > [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
    Random: fe22bb3de3c53f53f6a35c7bcff4983692130eae5cf4578012aa8c9e692c4383
    Session ID Length: 32
    Session ID: f56db8bcc7559fe50640a4c72cbe9a80793e89983be05900350f2dbb733aea0a
    Cipher Suites Length: 32
  Cipher Suites (16 suites)
    Cipher Suite: Reserved (GREASE) (0x7a7a)
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
```

Server Hello:

```
Transport Layer Security
  TLv1.3 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)
    > [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
    Random: cb05611dfc179dff66ece1902e9e41683f052fd289b1c998289ed532f49e47
    Session ID Length: 32
    Session ID: f56db8bcc7559fe50640a4c72cbe9a80793e89983be05900350f2dbb733aea0a
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
    Compression Method: null (0)
    Extensions Length: 46
  Extension: supported_versions (len=2) TLS 1.3
    Type: supported_versions (43)
```

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 pri-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.