МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

Институт № 3 «Системы управления, информатика и электроэнергетика»

Кафедра 304 «Вычислительные машины, системы и сети»

Лабораторная работа № 3

по дисциплине «WEB технологии»

на тему «Модель OSI. Стек протоколов. Wireshark»

Выполнил

студент группы М3О-125БВ-24

Егоров А.В.

Приняли

ассистент каф. 304 Борисов А.И.

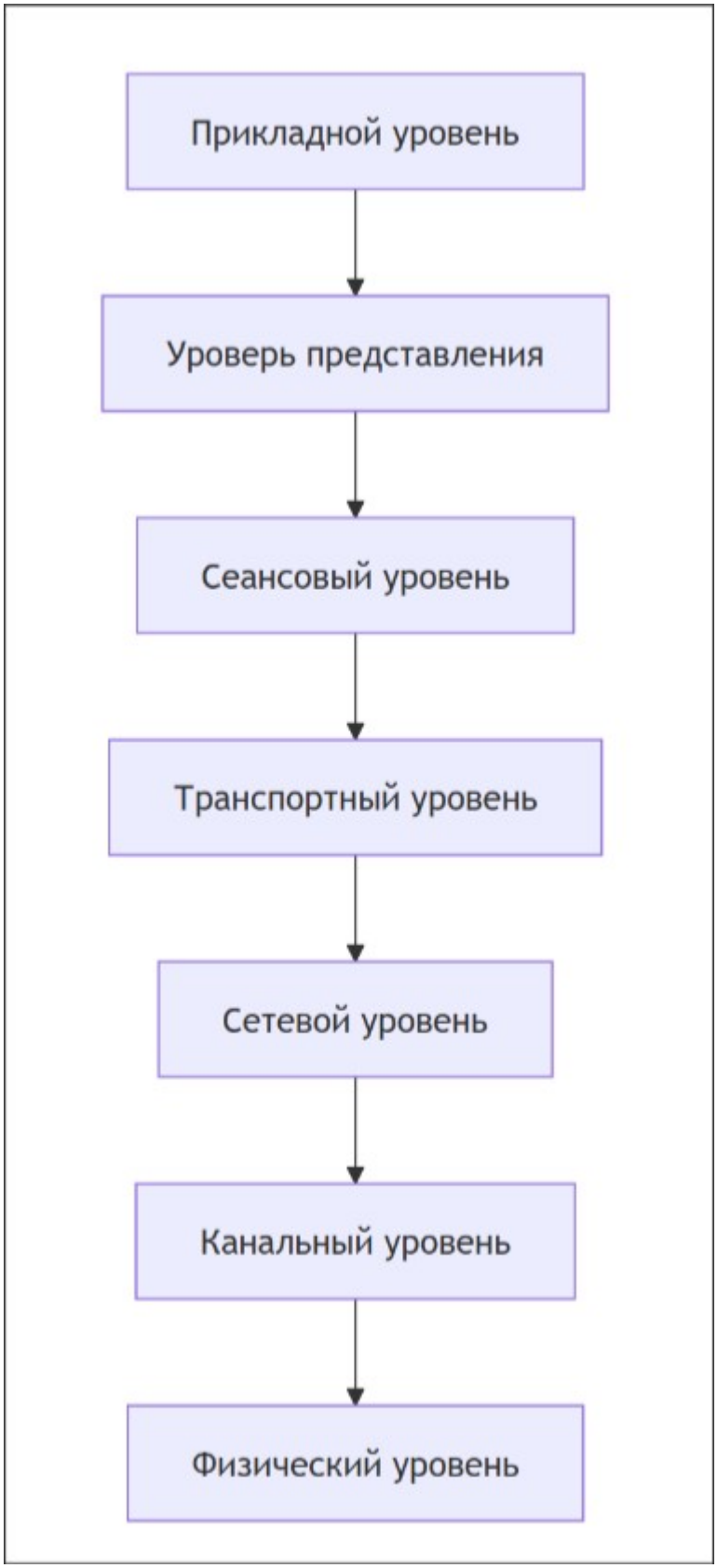
Москва
2025

Содержание:

Постановка задачи:

1. Рассмотреть классическую многоуровневую модель OSI. Определить, какие протоколы возможны на каждом уровне (привести по 2 примера на каждом уровне).
2. Запустить программу Wireshark. Настроить программу на активное интернет-соединение. Рассмотреть различные TCP и UDP соединения.
   - Привести в отчёте пример трехстороннего рукопожатия и трехстороннего завершения сеанса TCP (показать не только сам процесс, но и раскрыть флаги для каждого пакета).
   - Привести пример UDP-пакета.
3. Рассмотреть процесс установления TLS соединения.
   - В отчете привести заголовки стека протоколов основных сообщений при создании TLS соединения.
   - Раскрыть все параметры TLS соединения, отобразить все Chiper Suites, Extension, Certificate.
   - Показать данные протокола DH.
4. С помощью браузера отправить запрос для получения HTML-страницы по протоколу HTTP.
   - Найти соответствующий запрос и ответ в программе Wireshark.
   - В отчете полностью привести как HTTP запрос, так и HTTP ответ. Выделить содержимое тела запроса и тела ответа.
5. Проанализировать содержимое данных, отправленных в запросе и полученных в ответе. Расписать в отчете основные моменты соединения для каждого из протоколов.
6. Рассмотреть загрузку других ресурсов сайта (CSS/ PNG/ JPG и т.д.) как запрос на данный ресурс, так и ответ (привести только HTTP протокол).

Многоуровневая модель OSI.



1. Физический уровень:

Описание: происходит работа с сигналом и проводами, течёт ток или свет.
Единица информации: бит.
Протоколы: Wi-Fi, Bluetooth, Ethernet, USB.
Сетевые устройства: концентратор (хаб), репитор.

2. Канальный уровень:

Описание: происходит переача сообщений (фреймов - полезный данных с служебной информацией), исправление ошибок и физическая адресация.
Единица информации: фрейм.
Протоколы: Ethernet, PPP.
Сетевые устройства: коммутатор, мост.

3. Сетевой уровень:

Описание: происходит адресация по IP-адресам.
Протоколы: ARP, ICMP.
Единица информации: пакет.
Сетевые устройства: маршрутизатор (роутер).

4. Транспортный уровень:

Описание: обеспечивает передачу данных в сети.
Протоколы: TCP, UDP.

5. Сеансовый уровень:

Описание: управление соединениями.
Протоколы: L2TP, PPTP.

6. Уровень представления:

Описание: происходит преобразование сообщений (кодирование, сжатие), отвечает за корректную интерпретацию информации.
Протоколы: SSL/TLS, JPEG.

7. Прикладной уровень:

Описание: необходим для предоставления доступа к сети для приложений.
Протоколы: HTTP/HTTPS, FTP, SMTP.

TCP и UDP соединения.

Трёхстороннее рукопожатие TCP:

```
200 4.963025768   192.168.1.32        209.51.188.116       TCP
201 4.964789263   209.51.188.116      192.168.1.32         TCP
202 4.964813418   192.168.1.32        209.51.188.116       TCP
```

```
TCP      74 50780 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
TCP      74 443 → 50772 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
TCP      66 50772 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
```

192.168.3.32 – IP-адрес компьютера в локальной сети

209.51.188.116 – IP-адрес сайта (gnu.org)

Этапы (номер фрейма):

200 (установлен только флаг “SYN”):

```
▾ Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  ▾ .... .... ..1. = Syn: Set
    ▸ [Expert Info (Chat/Sequence): Connection establish request
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
```

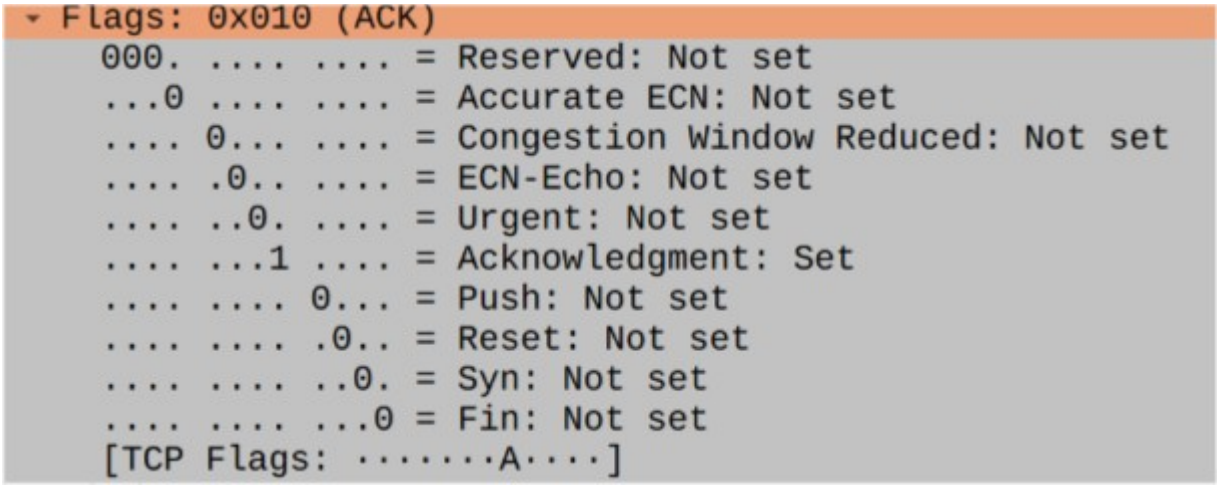
на данном этапе клиент отправляет запрос на синхронизацию начального номер последовательности (флаг “SYN) (с которого начнётся обмен данными).

201 (установлен флаг “SYN” и “ACK):

```
▾ Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  ▾ .... .... ..1. = Syn: Set
    ▸ [Expert Info (Chat/Sequence): Connection establish
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A··S·]
```

здесь сервер подтверждает получение запроса о синхронизации (флаг “ACK”) и отправляет свой начальный номер последовательности для синхронизации с клиентом (флаг “SYN”).

202 (установлен только флаг “ACK”):



на финальном этапе клиент отправляет ответ на сервер (флаг “ACK”) об успешной синхронизации. После данного ряда взаимодействий начинается обмен данными по TCP соединению.

Завершение TCP соединения:

```
1748 8.806092941   209.51.188.116   192.168.1.32
1749 8.806370271   192.168.1.32     209.51.188.116
1750 8.806413591   192.168.1.32     209.51.188.116
1751 9.012472926   209.51.188.116   192.168.1.32
```

```
TCP       66 443 → 33848 [FIN, ACK] Seq=16685 Ack=2443 Win=64128
TLSv1.3   90 Application Data
TCP       66 33848 → 443 [FIN, ACK] Seq=2467 Ack=16686 Win=48128
TCP       66 443 → 33848 [ACK] Seq=16686 Ack=2468 Win=64128 Len=0
```

Этапы (номер фрейма):

1748 (флаги “FIN” и “ACK”):

```
Flags: 0x011 (FIN, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced: Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
▾ .... .... ...1 = Fin: Set
```

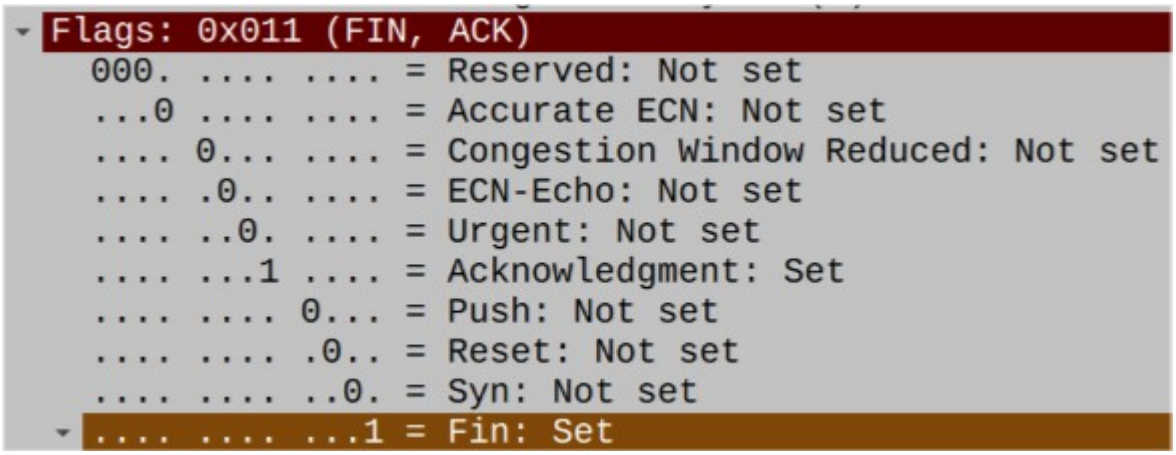
на данном этапе сервер отправляет запрос на разрыв TPC соединения. (флаг “ACK” в данном пакете означает, что сервер принял пердыдущий пакет с данными и к завершению соединение это не относится).

1749 (флаги “PSH” и “ACK”):

```
▾ Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
```

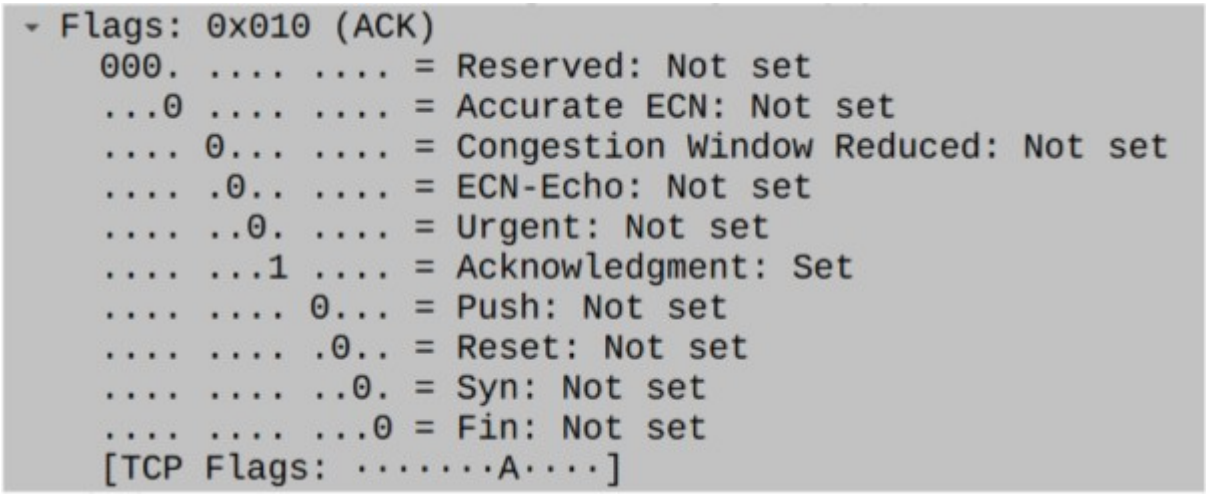
тут клиент подтверждает получение запроса на окончание соединение от сервера (флаг “ACK”) и пока что продолжает передавать данные на сервер (флаг “PSH”).

1750 (флаги “FIN” и “ACK”):



на этом этапе клиент отправляет запрос на завершение соединения (флаг “FIN) и ещё раз подтверждает запрос на завершение соединения со стороны сервера (флаг “ACK”).

1751 (флаг “ACK”):



это послдений пакет при завершении TCP соединения, в нём сервер отправляет подтверждение о закрытии соединения (флаг “ACK”) и после этого соединение считается полностью закрытым.

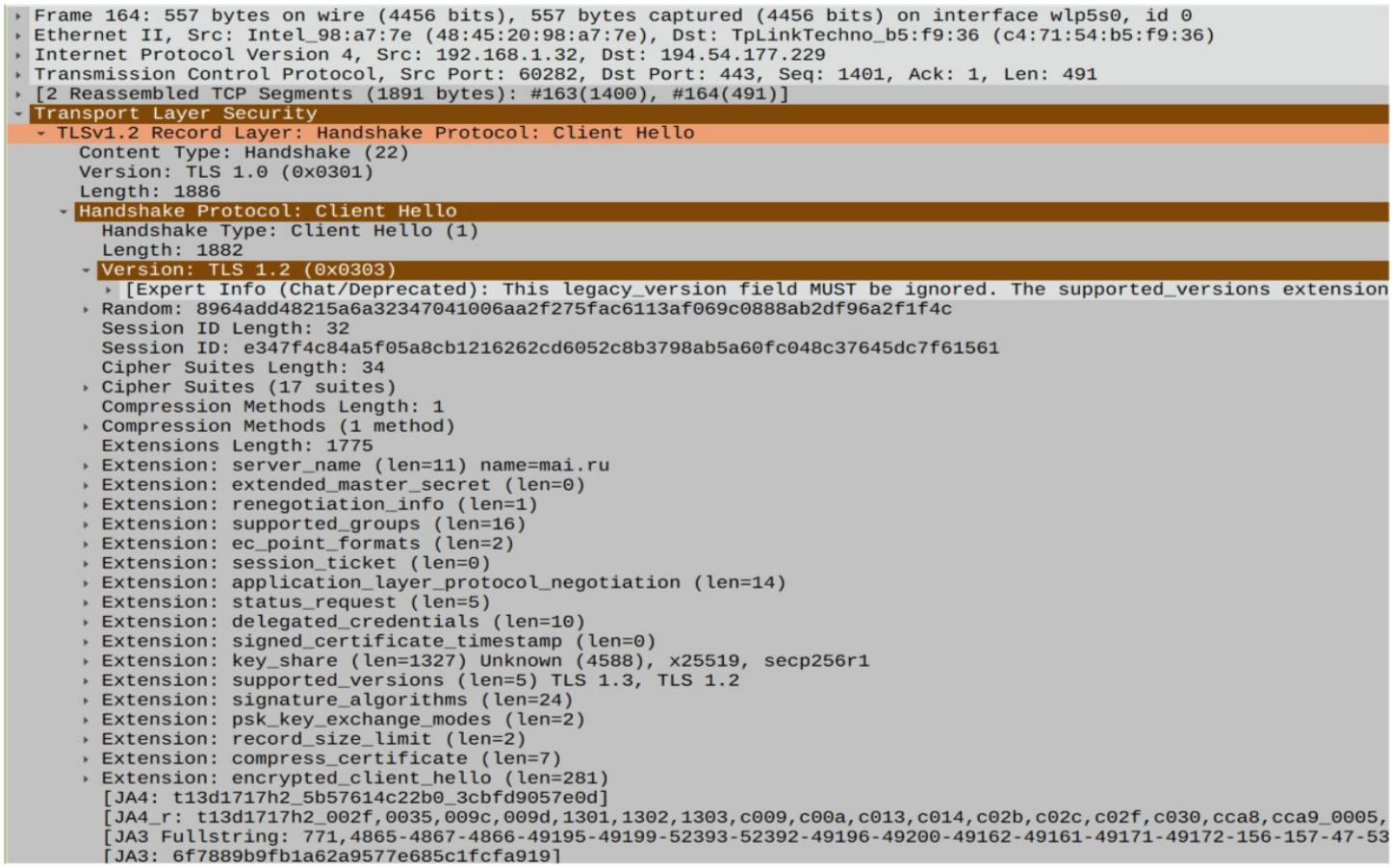
Пример UDP пакета:

```
▸ Frame 57: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: Intel_98:a7:7e (48:45:20:98:a7:7e), Dst: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36)
▸ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 192.168.1.1
▾ User Datagram Protocol, Src Port: 50673, Dst Port: 53
    Source Port: 50673
    Destination Port: 53
    Length: 33
    Checksum: 0x112b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (25 bytes)
▾ Domain Name System (query)
    Transaction ID: 0xba34
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 62]
```

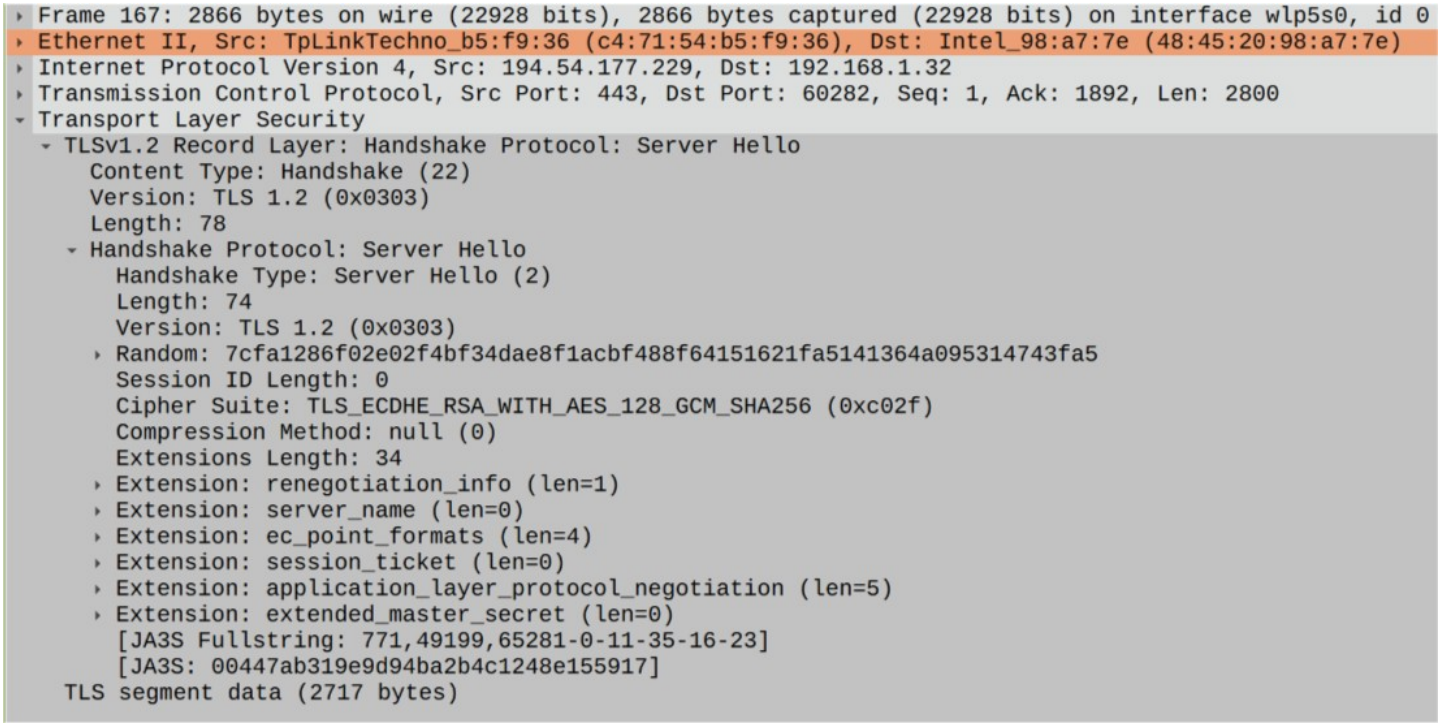
```
0000  c4 71 54 b5 f9 36 48 45  20 98 a7 7e 08 00 45 00   ·qT··6HE  ···~··E·
0010  00 35 b1 ca 00 00 40 11  45 7c c0 a8 01 20 c0 a8   ·5····@·  E|··· ··
0020  01 01 c5 f1 00 35 00 21  11 2b ba 34 01 00 00 01   ·····5·!  ·+·4····
0030  00 00 00 00 00 00 03 67  6e 75 03 6f 72 67 00 00   ·······g  nu·org··
0040  01 00 01                                          ···
```

Процесс установки TLS соединения.

Client Hello:



Server Hello:



Передача сертификата (сервером), Передача ключа шифрования сервером, Server Hello Done:

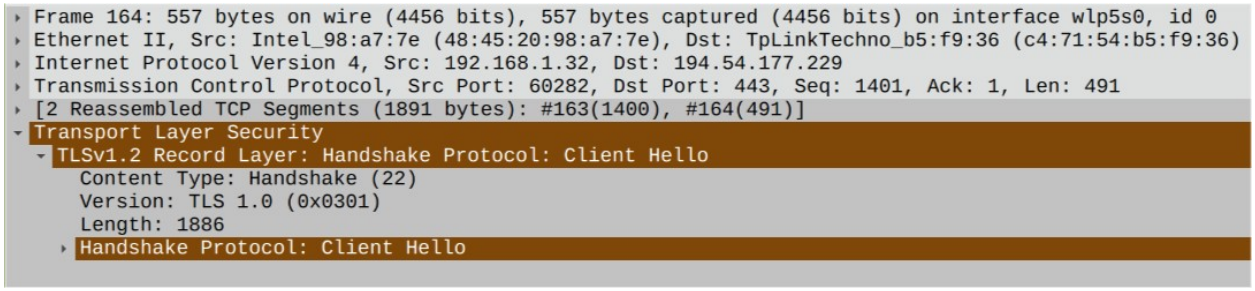
```
▸ Frame 168: 1357 bytes on wire (10856 bits), 1357 bytes captured (10856 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36), Dst: Intel_98:a7:7e (48:45:20:98:a7:7e)
▸ Internet Protocol Version 4, Src: 194.54.177.229, Dst: 192.168.1.32
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 60282, Seq: 2801, Ack: 1892, Len: 1291
▸ [2 Reassembled TCP Segments (3694 bytes): #167(2717), #168(977)]
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3689
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3685
        Certificates Length: 3682
      ▸ Certificates (3682 bytes)
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 300
    ▾ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 296
      ▸ EC Diffie-Hellman Server Params
  ▾ 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
```

Передача ключа шифрования клиентом, Переход на шифрованное соединение (change chiper spec), Окончание установки шифрованного соединения (Encrypted Handshake Message):

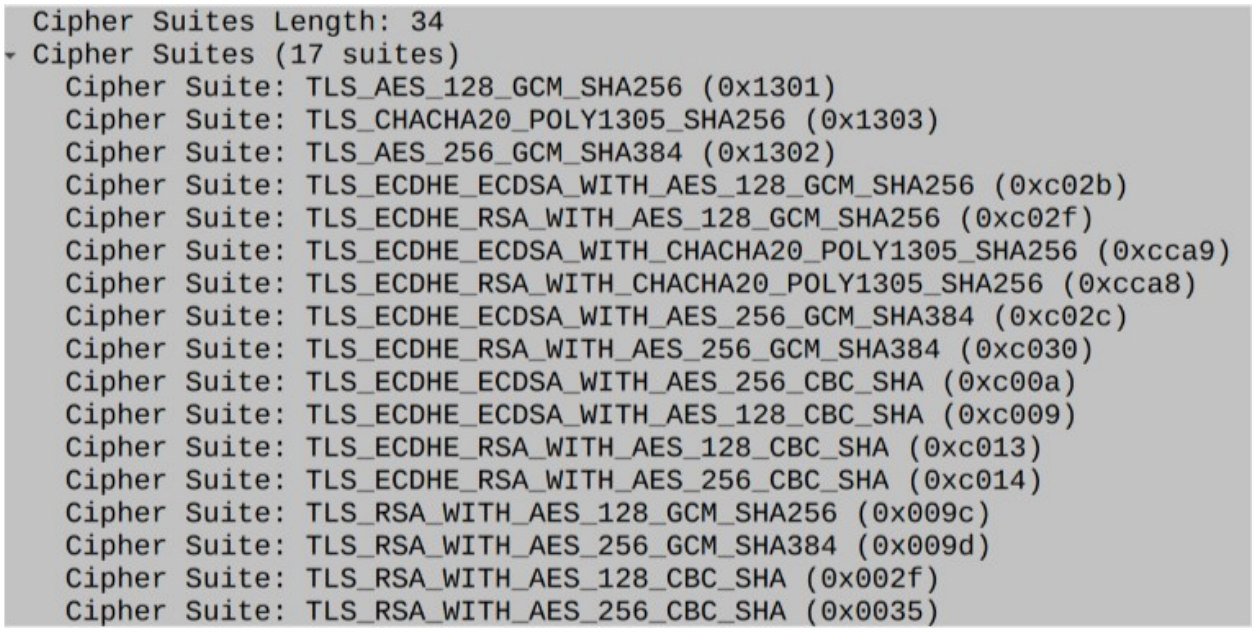
```
▸ Frame 171: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: Intel_98:a7:7e (48:45:20:98:a7:7e), Dst: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36)
▸ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 194.54.177.229
▸ Transmission Control Protocol, Src Port: 60282, Dst Port: 443, Seq: 1892, Ack: 4092, Len: 93
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 37
    ▾ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 33
      ▸ EC Diffie-Hellman Client Params
  ▾ 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
```

Параметры TLS соединения (Chiper Suites, Extension, Certificate).

Пакет (Client Hello):



Chiper Suites:



Extension:

```
  Extensions Length: 1775
▾ Extension: server_name (len=11) name=mai.ru
    Type: server_name (0)
    Length: 11
  ▸ Server Name Indication extension
▾ Extension: extended_master_secret (len=0)
    Type: extended_master_secret (23)
    Length: 0
▾ Extension: renegotiation_info (len=1)
    Type: renegotiation_info (65281)
    Length: 1
  ▸ Renegotiation Info extension
▾ Extension: supported_groups (len=16)
    Type: supported_groups (10)
    Length: 16
    Supported Groups List Length: 14
  ▸ Supported Groups (7 groups)
▾ Extension: ec_point_formats (len=2)
    Type: ec_point_formats (11)
    Length: 2
    EC point formats Length: 1
  ▸ Elliptic curves point formats (1)
▾ Extension: session_ticket (len=0)
    Type: session_ticket (35)
    Length: 0
    Session Ticket: <MISSING>
▾ Extension: application_layer_protocol_negotiation (len=14)
    Type: application_layer_protocol_negotiation (16)
    Length: 14
    ALPN Extension Length: 12
  ▸ ALPN Protocol
▾ Extension: status_request (len=5)
    Type: status_request (5)
    Length: 5
    Certificate Status Type: OCSP (1)
    Responder ID list Length: 0
    Request Extensions Length: 0
```

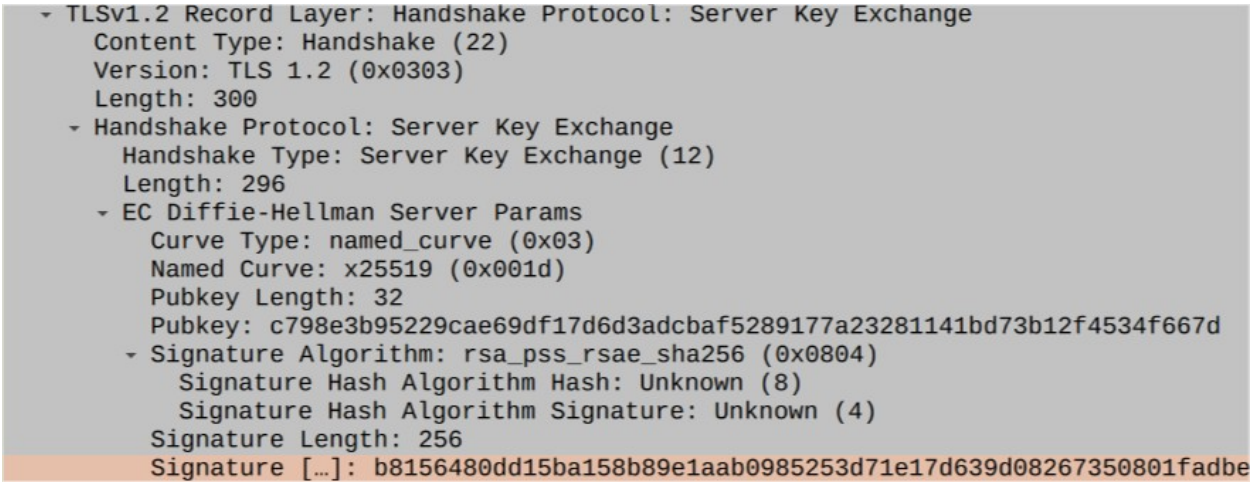
```
▾ Extension: delegated_credentials (len=10)
    Type: delegated_credentials (34)
    Length: 10
    Signature Hash Algorithms Length: 8
  ▸ Signature Hash Algorithms (4 algorithms)
▾ Extension: signed_certificate_timestamp (len=0)
    Type: signed_certificate_timestamp (18)
    Length: 0
▾ Extension: key_share (len=1327) Unknown (4588), x25519, secp256r1
    Type: key_share (51)
    Length: 1327
  ▸ Key Share extension
▾ Extension: supported_versions (len=5) TLS 1.3, TLS 1.2
    Type: supported_versions (43)
    Length: 5
    Supported Versions length: 4
    Supported Version: TLS 1.3 (0x0304)
    Supported Version: TLS 1.2 (0x0303)
▾ Extension: signature_algorithms (len=24)
    Type: signature_algorithms (13)
    Length: 24
    Signature Hash Algorithms Length: 22
  ▸ Signature Hash Algorithms (11 algorithms)
▾ Extension: psk_key_exchange_modes (len=2)
    Type: psk_key_exchange_modes (45)
    Length: 2
    PSK Key Exchange Modes Length: 1
    PSK Key Exchange Mode: PSK with (EC)DHE key establishment (psk_dhe_ke) (1)
▾ Extension: record_size_limit (len=2)
    Type: record_size_limit (28)
    Length: 2
    Record Size Limit: 16385
▾ Extension: compress_certificate (len=7)
    Type: compress_certificate (27)
    Length: 7
    Algorithms Length: 6
    Algorithm: zlib (1)
    Algorithm: brotli (2)
    Algorithm: zstd (3)
▾ Extension: encrypted_client_hello (len=281)
    Type: encrypted_client_hello (65037)
    Length: 281
    Client Hello type: Outer Client Hello (0)
  ▸ Cipher Suite: HKDF-SHA256/AES-128-GCM
    Config Id: 211
    Enc length: 32
    Enc: 3149f27ededd894ce9b3489ff1d37db877592515713ad70352ac6ccfd25afc1b
    Payload length: 239
    Payload […]: b4c3c7220a65d646892a2a76c45156a09c7602c870d4b9dc98ea706c49dddac
```

Certificate (второй пакет от сервера):

```
  Certificates Length: 3682
▾ Certificates (3682 bytes)
    Certificate Length: 1602
  ▾ Certificate […]: 3082063e30820526a003020102020c1be3f236e8afeb3cabe442
    ▾ signedCertificate
        version: v3 (2)
        serialNumber: 0x1be3f236e8afeb3cabe44246
      ▸ signature (sha256WithRSAEncryption)
      ▸ issuer: rdnSequence (0)
      ▸ validity
      ▸ subject: rdnSequence (0)
      ▸ subjectPublicKeyInfo
      ▸ extensions: 10 items
    ▾ algorithmIdentifier (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      Padding: 0
      encrypted […]: 7ec5bd4ecc81c71d9f9ec827ac9f525a902f825e298df8371f66
    Certificate Length: 867
  ▾ Certificate […]: 3082035f30820247a003020102020b040000000000121585308a2
    ▾ signedCertificate
        version: v3 (2)
        serialNumber: 0x040000000000121585308a2
      ▸ signature (sha256WithRSAEncryption)
      ▸ issuer: rdnSequence (0)
      ▸ validity
      ▸ subject: rdnSequence (0)
      ▸ subjectPublicKeyInfo
      ▸ extensions: 3 items
    ▾ algorithmIdentifier (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      Padding: 0
      encrypted […]: 4b40dbc050aafec80ceff796544549bb96000941acb313868628
```

```
  Certificate Length: 1204
▾ Certificate […]: 308204b030820398a003020102021077bd0e0742d5d9e9d04
  ▾ signedCertificate
      version: v3 (2)
      serialNumber: 0x77bd0e0742d5d9e9d049d774d02a6f9a
    ▸ signature (sha256WithRSAEncryption)
    ▸ issuer: rdnSequence (0)
    ▸ validity
    ▸ subject: rdnSequence (0)
    ▸ subjectPublicKeyInfo
    ▸ extensions: 8 items
  ▾ algorithmIdentifier (sha256WithRSAEncryption)
      Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
    Padding: 0
    encrypted […]: cbc8ff739e7479af3aa0291faf65bea6d4c261eea2573be8e
```

Данные протокола DH:



Получение HTML страницы путём отправки запроса по протоколу HTTP.

Запрос HTML страницы по протоколу HTTP:

```
291 2.248706857   192.168.1.32        195.181.172.2       HTTP      510 GET /http2/http1.html HTTP/1.1
```

```
▸ Frame 291: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: Intel_98:a7:7e (48:45:20:98:a7:7e), Dst: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36)
▸ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 195.181.172.2
▸ Transmission Control Protocol, Src Port: 36100, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
▾ Hypertext Transfer Protocol
  ▸ GET /http2/http1.html HTTP/1.1\r\n
    Host: 1153288396.rsc.cdn77.org\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: ru,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.http2demo.io/\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=4\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 354]
    [Full request URI: http://1153288396.rsc.cdn77.org/http2/http1.html]
```

Ответ на получение HTML страницы:

```
354 2.293497099   195.181.172.2       192.168.1.32        HTTP      2306 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 354: 2306 bytes on wire (18448 bits), 2306 bytes captured (18448 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36), Dst: Intel_98:a7:7e (48:45:20:98:a7:7e)
▸ Internet Protocol Version 4, Src: 195.181.172.2, Dst: 192.168.1.32
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 36100, Seq: 1, Ack: 445, Len: 2240
▾ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 09 May 2025 10:24:55 GMT\r\n
    Content-Type: text/html\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    ETag: W/"570b88dc-45c3"\r\n
    Cache-Control: no-cache\r\n
    Access-Control-Allow-Origin: *\r\n
    X-77-NZT: EwwBw7WsAQH3NBZjAQwBuUwKDAH3TJQMAAwB1GY4EQH3AwAAAA\r\n
    X-77-NZT-Ray: 4782413818190f8e1cd81d68f8556a06\r\n
    X-77-Cache: HIT\r\n
    X-77-Age: 3\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Server: CDN77-Turbo\r\n
    X-Cache: HIT\r\n
    X-Age: 23270964\r\n
    \r\n
    [Request in frame: 291]
    [Time since request: 0.044790242 seconds]
    [Request URI: /http2/http1.html]
    [Full request URI: http://1153288396.rsc.cdn77.org/http2/http1.html]
  ▸ HTTP chunked response
    Content-encoded entity body (gzip): 1774 bytes -> 17859 bytes
    File Data: 17859 bytes
```

HTML страница (часть), переданная в ответе:

```
Line-based text data: text/html (255 lines)
    <html>\n
        <head lang="en"></head>\n
        <body>\n
            <div class="iframe">\n
                <div align="center">\n
                    <h2 class="highlightType">\n
                        <strong>HTTP/1.1</strong>\n
                        <div id="IMGLoad">\n
                            <div class="highlightTime"><span id="timerCDN77">0</span>s</div>\n
                        </div>\n
                    </h2>\n
                </div>\n
                <div class="imgGroup">\n
                    <div class="imgInner">\n
    <div class="imgRow">\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_0.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_1.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_2.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_3.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_4.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_5.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_6.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_7.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_8.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_9.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_10.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_11.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_12.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_13.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_14.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_15.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_16.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_17.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_18.png'/>\n
    </div>\n
    <div class="imgRow">\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_19.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_20.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_21.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_22.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_23.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_24.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_25.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_26.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_27.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_28.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_29.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_30.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_31.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_32.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_33.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_34.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_35.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_36.png'/>\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_37.png'/>\n
    </div>\n
    <div class="imgRow">\n
    <img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_38.png'/>\n
```

```
<img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_166.png'/>\n
<img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_167.png'/>\n
<img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_168.png'/>\n
<img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_169.png'/>\n
<img height="48" width="32" onload='A5587LKJ()' src='/http2/tiles_final/tile_170.png'/>\n
</div>\n
                </div>\n
            </div>\n
        </div>\n
    </body>\n
</html>\n
\n
<style>\n
 […]    a{text-decoration:none}html{font-family:helvetica,arial,sans-serif}.imgGroup{height:0;padding-bot
    .cdn-features #IMGLoad,\n
    .cdn-features #IMGLoad .highlightTime {\n
        display: inline;\n
    }\n
    .cdn-features .highlightType {\n
        margin-left: 0;\n
\n
        text-align: left;\n
    }\n
\n
    .cdn-features .highlightType strong {\n
        color: #434343;\n
        font-size: 16px;\n
        font-weight: 400;\n
    }\n
\n
    .cdn-features .highlightTime {\n
        color: #434343;\n
        font-size: 24px;\n
        font-weight: 600;\n
    }\n
</style>\n
\n
<script>\n
 […]    var _0x3008=["\x6E\x6F\x77","\x70\x65\x72\x66\x6F\x72\x6D\x61\x6E\x63\x65","\x69\x6E\x6E\x65\x72\
\n
    var iframeVal = 0;\n
    var getVal = 0;\n
\n
    var myTimer = setInterval(function() {\n
        getVal = document.getElementById('timerCDN77').innerHTML;\n
\n
        if ((iframeVal === getVal) && (iframeVal != 0)) {\n
            parent.postMessage(iframeVal, '*');\n
            clearInterval(myTimer);\n
        }\n
\n
        iframeVal = getVal;\n
    }, 1000);\n
\n
    if(window.location.href.indexOf("cdn-features") > -1) {\n
        document.body.className = "cdn-features";\n
    }\n
</script>\n
```

HTTP запрос на получение CSS:

```
221 2.125562340   192.168.1.32          185.76.9.12           HTTP      428 GET /css/jssocials.css HTTP/1.1

▸ Frame 221: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: Intel_98:a7:7e (48:45:20:98:a7:7e), Dst: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36)
▸ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 185.76.9.12
▸ Transmission Control Protocol, Src Port: 55512, Dst Port: 80, Seq: 1, Ack: 1, Len: 362
▾ Hypertext Transfer Protocol
  ▸ GET /css/jssocials.css HTTP/1.1\r\n
    Host: www.http2demo.io\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: ru,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.http2demo.io/\r\n
    Priority: u=2\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 235]
    [Full request URI: http://www.http2demo.io/css/jssocials.css]
```

HTTP ответ:

```
235 2.170723887   185.76.9.12           192.168.1.32          HTTP      922 HTTP/1.1 200 OK  (text/css)

▸ Frame 235: 922 bytes on wire (7376 bits), 922 bytes captured (7376 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36), Dst: Intel_98:a7:7e (48:45:20:98:a7:7e)
▸ Internet Protocol Version 4, Src: 185.76.9.12, Dst: 192.168.1.32
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 55512, Seq: 1, Ack: 363, Len: 856
▾ Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 09 May 2025 10:24:54 GMT\r\n
    Content-Type: text/css\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    ETag: W/"55e03fc3-52f"\r\n
    Cache-Control: no-cache\r\n
    Access-Control-Allow-Origin: *\r\n
    X-77-NZT: EwwBuUwJCgHXrR/DAAwBuUwKCQH3J7VjAAwBJRPCLgH3i9P0AA\r\n
    X-77-NZT-Ray: e2f75420916ef8bcf6d71d6887700e3a\r\n
    X-77-Cache: HIT\r\n
    X-77-Age: 16044939\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
    Server: CDN77-Turbo\r\n
    X-Cache: HIT\r\n
    X-Age: 12787629\r\n
    \r\n
    [Request in frame: 221]
    [Time since request: 0.045161547 seconds]
    [Request URI: /css/jssocials.css]
    [Full request URI: http://www.http2demo.io/css/jssocials.css]
  ▸ HTTP chunked response
    Content-encoded entity body (gzip): 385 bytes -> 1327 bytes
    File Data: 1327 bytes
▸ Line-based text data: text/css (58 lines)
```

Часть полученных CSS стилей:

```
Line-based text data: text/css (58 lines)
  .jssocials-shares {\n
    margin: 0.2em 0; }\n
  \n
  .jssocials-shares * {\n
    box-sizing: border-box; }\n
  \n
  .jssocials-share {\n
    display: inline-block;\n
    vertical-align: top;\n
    margin: 0.3em; }\n
  \n
  .jssocials-share:first-child {\n
    margin-left: 0; }\n
  \n
  .jssocials-share:last-child {\n
    margin-right: 0; }\n
  \n
  .jssocials-share-logo {\n
    width: 1em;\n
    vertical-align: middle;\n
    font-size: 1.5em; }\n
  \n
  img.jssocials-share-logo {\n
    width: auto;\n
    height: 1em; }\n
  \n
  .jssocials-share-link {\n
    display: inline-block;\n
    text-align: center;\n
    text-decoration: none;\n
    line-height: 1; }\n
    .jssocials-share-link.jssocials-share-link-count {\n
      padding-top: .2em; }\n
      .jssocials-share-link.jssocials-share-link-count .jssocials-share-count {\
        display: block;\n
        font-size: .6em;\n
        margin: 0 -.5em -.8em -.5em; }\n
    .jssocials-share-link.jssocials-share-no-count {\n
      padding-top: .5em; }\n
      .jssocials-share-link.jssocials-share-no-count .jssocials-share-count {\n
        height: 1em; }\n
  \n
  .jssocials-share-label {\n
    padding-left: 0.3em;\n
    vertical-align: middle; }\n
  \n
  .jssocials-share-count-box {\n
    display: inline-block;\n
    height: 1.5em;\n
    padding: 0 0.3em;\n
    vertical-align: middle;\n
    cursor: default; }\n
    .jssocials-share-count-box.jssocials-share-no-count {\n
      display: none; }\n
  \n
```

HTTP запрос на получение PNG изображения:

```
249 2.197387922   192.168.1.32        185.76.9.12         HTTP      482 GET /img/cdn77logo.png HTTP/1.1
```

```
▸ Frame 249: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: Intel_98:a7:7e (48:45:20:98:a7:7e), Dst: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36)
▸ Internet Protocol Version 4, Src: 192.168.1.32, Dst: 185.76.9.12
▸ Transmission Control Protocol, Src Port: 55532, Dst Port: 80, Seq: 366, Ack: 6888, Len: 416
▾ Hypertext Transfer Protocol
  ▸ GET /img/cdn77logo.png HTTP/1.1\r\n
    Host: www.http2demo.io\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:138.0) Gecko/20100101 Firefox/138.0\r\n
    Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
    Accept-Language: ru,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://www.http2demo.io/\r\n
    Priority: u=5, i\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Response in frame: 292]
    [Full request URI: http://www.http2demo.io/img/cdn77logo.png]
```

HTTP ответ:

```
292 2.249841688   185.76.9.12         192.168.1.32        HTTP      1260 HTTP/1.1 200 OK  (PNG)
```

```
▸ Frame 292: 1260 bytes on wire (10080 bits), 1260 bytes captured (10080 bits) on interface wlp5s0, id 0
▸ Ethernet II, Src: TpLinkTechno_b5:f9:36 (c4:71:54:b5:f9:36), Dst: Intel_98:a7:7e (48:45:20:98:a7:7e)
▸ Internet Protocol Version 4, Src: 185.76.9.12, Dst: 192.168.1.32
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 55532, Seq: 18088, Ack: 782, Len: 1194
▸ [8 Reassembled TCP Segments (12394 bytes): #263(1400), #268(1400), #350(1400), #264(2800), #265(1400),
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Fri, 09 May 2025 10:24:55 GMT\r\n
    Content-Type: image/png\r\n
  ▸ Content-Length: 11965\r\n
    Connection: keep-alive\r\n
    ETag: "55d4978d-2ebd"\r\n
    Cache-Control: no-cache\r\n
    Access-Control-Allow-Origin: *\r\n
    X-77-NZT: EwwBuUwJCgHX2ObHAAwBuUwKDAH3wJ7+AAwBnJIhJwH3/a3IAA\r\n
    X-77-NZT-Ray: e2f75420eaaaecbdf7d71d687774bc02\r\n
    X-77-Cache: HIT\r\n
    X-77-Age: 13151741\r\n
    Server: CDN77-Turbo\r\n
    X-Cache: HIT\r\n
    X-Age: 13100760\r\n
    Accept-Ranges: bytes\r\n
    \r\n
    [Request in frame: 249]
    [Time since request: 0.052453766 seconds]
    [Request URI: /img/cdn77logo.png]
    [Full request URI: http://www.http2demo.io/img/cdn77logo.png]
    File Data: 11965 bytes
```

Информация о PNG изображении в HTPP ответе:

```
Portable Network Graphics
  PNG Signature: 89504e470d0a1a0a
  Image Header (IHDR)
    Len: 13
    Type: IHDR
    ..0. .... .... .... .... .... .... .... = Ancillary: This is a CRITICAL chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
    Width: 259
    Height: 66
    Bit Depth: 8
    Colour Type: Truecolour with alpha (6)
    Compression Method: Deflate (0)
    Filter Method: Adaptive (0)
    Interlace Method: No interlace (0)
    CRC: 0x53a2b3b6
  International textual data (iTXt)
    Len: 5184
    Type: iTXt
    ..1. .... .... .... .... .... .... .... = Ancillary: This is an ANCILLARY chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..1. .... = Safe To Copy: This chunk is SAFE TO COPY
    Data
    CRC: 0x144d80f7
  Embedded ICC profile (iCCP)
    Len: 389
    Type: iCCP
    ..1. .... .... .... .... .... .... .... = Ancillary: This is an ANCILLARY chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
    Data
    CRC: 0xd79caf69
  Physical pixel dimensions (pHYs)
    Len: 9
    Type: pHYs
    ..1. .... .... .... .... .... .... .... = Ancillary: This is an ANCILLARY chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..1. .... = Safe To Copy: This chunk is SAFE TO COPY
    Horizontal pixels per unit: 2835
    Vertical pixels per unit: 2835
    Unit: Unit is METRE (1)
    CRC: 0x009a9c18
  Image data chunk (IDAT)
    Len: 6290
    Type: IDAT
    ..0. .... .... .... .... .... .... .... = Ancillary: This is a CRITICAL chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
    Data
    CRC: 0x81151e57
  Image Trailer (IEND)
    Len: 0
    Type: IEND
    ..0. .... .... .... .... .... .... .... = Ancillary: This is a CRITICAL chunk
    .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
    .... .... .... .... .... .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
    CRC: 0xae426082
```

Основные моменты в соединении каждого протокола.

TCP (Transmission Control Protocol):

Протокол транспортного уровня модели OSI с установкой соединения при помощи 3-х стороннего рукопожатия. Обеспечивает надёжное соединение и гарантирует порядок и целостность доставки пакетов.

UDP (User Datagram Protocol):

Протокол транспортного уровня модели OSI без установки соединения. Отличается тем, что отправляет пакеты без подтверждения, в следствии чего нет гарантий порядка и целостности доставки пакетов. Отличается скоростью работы и низкими задержками.

HTTP (HyperText Transfer Protocol):

Протокол прикладного уровня модели OSI. Механизм работы основан на модели “запрос – ответ” (клиент – сервер). В качестве основы использует протокол TCP. Данные передаются без шифрования (TLS).

TLS (Transport Layer Security):

Протокол шифрования поверх TCP. Обычно используется в связке с HTTP, создавая HTTPS соединение. В его задачи входит установка защищённого соединения через handshake (рукопожатие), согласовывание алгоритмов шифрования, обмен ключами и передача сертификатов.

DH (Diffie–Hellman key exchange):

Криптографический алгоритм для обмена ключами. Обычно используется внутри TLS (DHE/ECDHE). Благодаря ему клиент и сервер обмениваются публичными ключами и независимо вычисляют общий секрет.

Вывод по работе:

Работа позволила на практике изучить, как протоколы взаимодействуют в модели OSI, как устанавливаются и завершаются соединения, и как данные передаются и защищаются в интернете. Использование Wireshark дало наглядное представление о сетевом трафике и структуре протоколов.

Ссылки:

Все файлы можно посмотреть на github:
https://github.com/swrneko/mai_shit/tree/main/1lvl_2sem/web/laba_3