

Отчёт по лабораторной работе 3

Анализ трафика в Wireshark

Элсаиед Адел

Содержание

1 Цель работы	5
2 Выполнение работы	6
2.1 Анализ сетевого соединения	6
2.2 Анализ кадров канального уровня в Wireshark	8
2.3 Анализ протоколов транспортного уровня в Wireshark (HTTP, DNS, QUIC)	15
2.4 Анализ handshake протокола TCP в Wireshark	23
3 Заключение	27

Список иллюстраций

2.1 Вывод параметров сетевого соединения командой ipconfig /all	7
2.2 Проверка доступности шлюза по умолчанию	8
2.3 ICMP Echo request	10
2.4 ICMP Echo reply	11
2.5 ARP request	12
2.6 Ping по доменному имени	12
2.7 ARP reply	13
2.8 ICMP request к внешнему узлу	14
2.9 ICMP reply от внешнего узла	15
2.10 HTTP GET запрос и параметры TCP-сегмента	17
2.11 HTTP ответ 200 OK и сборка TCP-сегментов	18
2.12 DNS запрос по протоколу UDP	19
2.13 DNS ответ с результатом разрешения имени	20
2.14 QUIC Initial пакет и параметры соединения	21
2.15 QUIC Handshake пакет	22
2.16 Последовательность TCP handshake в списке пакетов Wireshark . .	24
2.17 График потока TCP-соединения в Wireshark	25

Список таблиц

1 Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

2 Выполнение работы

2.1 Анализ сетевого соединения

1. На рабочей станции под управлением ОС Windows в консоли выполнен вывод параметров текущего сетевого соединения командой `ipconfig` с расширенной опцией `/all`, позволяющей получить полную информацию о сетевом адаптере (MAC-адрес, параметры DHCP и DNS, сведения об аренде адреса).

В ходе анализа установлено, что активным интерфейсом является беспроводной адаптер **Intel(R) Wi-Fi 6E AX211 160MHz**. В выводе команды отражены:

- Physical Address – аппаратный MAC-адрес сетевого интерфейса;
- DHCP enabled – автоматическое получение сетевых параметров;
- IPv6 link-local – локальный IPv6-адрес канального уровня;
- IPv4 address – адрес узла в локальной сети;
- Subnet Mask – маска подсети;
- Default Gateway – адрес маршрутизатора;
- DHCP Server и DNS Server – сетевые службы, обслуживающие подключение;
- Lease Obtained / Lease Expires – сроки действия DHCP-аренды.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : 
Описание . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Физический адрес . . . . . : F8-FE-5E-6F-7B-EC
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::da3b:4057:9ef4:1e28%7(Основной)
IPv4-адрес . . . . . : 192.168.1.69(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 19 января 2026 г. 11:23:48
Срок аренды истекает . . . . . : 20 января 2026 г. 11:23:46
Основной шлюз . . . . . : 192.168.1.1
DHCP-сервер . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 133758558
DUID клиента DHCPv6 . . . . . : 00-01-00-01-30-47-94-1A-10-FF-E0-21-D6-B4
DNS-серверы . . . . . : 192.168.1.1
NetBIOS через TCP/IP . . . . . : Включен
```

Рис. 2.1: Вывод параметров сетевого соединения командой ipconfig /all

2. По результатам выполнения команды `ipconfig /all` определены основные параметры сетевого подключения:

- IPv4-адрес: 192.168.1.69;
- Маска подсети: 255.255.255.0;
- Шлюз по умолчанию: 192.168.1.1;
- DHCP-сервер: 192.168.1.1;
- DNS-сервер: 192.168.1.1;
- MAC-адрес интерфейса Wi-Fi: F8-FE-5E-6F-7B-EC.

3. Для проверки доступности шлюза по умолчанию выполнена команда `ping 192.168.1.1`. В результате получены ответы на все отправленные ICMP-запросы без потерь пакетов, а время отклика составило менее 1 мс, что свидетельствует о корректной работе локального сетевого сегмента.

```
PS C:\Users\Adel\Documents> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
PS C:\Users\Adel\Documents>
```

Рис. 2.2: Проверка доступности шлюза по умолчанию

4. MAC-адреса сетевых интерфейсов определены:

- из вывода ipconfig /all: F8-FE-5E-6F-7B-EC;
- из захваченных кадров Ethernet II в Wireshark (поле Source): f8:fe:5e:6f:7b:ec.

Также определён MAC-адрес шлюза по умолчанию: c8:7f:54:78:b6:f2.

5. Структура MAC-адреса рассмотрена на примере F8-FE-5E-6F-7B-EC:

- первые 24 бита (F8-FE-5E) – идентификатор производителя (OUI);
- последние 24 бита (6F-7B-EC) – уникальный идентификатор сетевого интерфейса.

Первый октет F8 в двоичном виде равен 11111000.

- младший бит равен 0 – адрес индивидуальный (unicast);
- второй младший бит равен 0 – адрес глобально администрируемый (назначен производителем).

2.2 Анализ кадров канального уровня в Wireshark

6. На рабочем устройстве установлен и запущен анализатор сетевого трафика Wireshark. В качестве интерфейса захвата выбран активный беспроводной

сетевой адаптер.

7. В консоли определены IP-адрес устройства и шлюз по умолчанию с использованием команды `ipconfig`.
8. Для генерации трафика выполнена команда `ping 192.168.1.1`. После этого захват трафика в Wireshark был остановлен и применён фильтр отображения `arp or icmp`.
9. Проанализирован кадр ICMP Echo Request:
 - длина кадра – 74 байта;
 - тип канального кадра – Ethernet II;
 - MAC-адрес источника – `f8:fe:5e:6f:7b:ec`;
 - MAC-адрес назначения – `c8:7f:54:78:b6:f2`;
 - оба MAC-адреса являются индивидуальными и глобально администрируемыми.

No.	Time	Source	Destination	Protocol	Length Info
26	6.485226	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.1
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
→	239 24.146270	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=
←	240 24.147153	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec

Frame 239: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3A 0000 c...
Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) 0010 0...
 Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
 0. = LG bit: Globally unique address (factory default) 0020 0...
 0. = IG bit: Individual address (unicast) 0030 6...
 Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec) 0040 7...
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 192.168.1.1
Internet Control Message Protocol

Рис. 2.3: ICMP Echo request

10. Проанализирован кадр ICMP Echo Reply:

- длина кадра – 78 байт;
- тип кадра – Ethernet II с тегом 802.1Q VLAN;
- MAC-адрес источника – c8:7f:54:78:b6:f2;
- MAC-адрес назначения – f8:fe:5e:6f:7b:ec.

No.	Time	Source	Destination	Protocol	Length Info
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168...
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
→	239 24.146270	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=1
←	240 24.147153	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=2
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=2
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=3
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=3
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request id=0x0001, seq=4
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=4
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168...
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1...
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168...
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
993	126.700352	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1...

```

Frame 240: Packet, 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{3A
Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
  Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Source: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Type: 802.1Q Virtual LAN (0x8100)
    [Stream index: 0]
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 0
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.69
> Internet Control Message Protocol

```

Рис. 2.4: ICMP Echo reply

11. Изучены кадры протокола ARP. Рассмотрен ARP-запрос, в котором шлюз определяет MAC-адрес узла по его IP-адресу. В кадре зафиксированы поля Ethernet II и заголовок ARP.

ZO	0.403220	d2.11.0e.31.22.03	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00
40	11.743931	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69?	Tell 192.168.					
41	11.743962	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69	is at f8:fe:5e:6f:7b:ec					
239	24.146270	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=1					
240	24.147153	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply	id=0x0001, seq=2					
247	25.157390	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=3					
248	25.158336	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply	id=0x0001, seq=4					
251	26.170340	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=5					
252	26.171444	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply	id=0x0001, seq=6					
260	27.184725	192.168.1.69	192.168.1.1	ICMP	74 Echo (ping) request	id=0x0001, seq=7					
261	27.185433	192.168.1.1	192.168.1.69	ICMP	78 Echo (ping) reply	id=0x0001, seq=8					
558	58.078856	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69?	Tell 192.168.					
559	58.078888	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69	is at f8:fe:5e:6f:7b:ec					
597	66.592141	a2:1f:8e:51:22:03	Broadcast	ARP	42 Who has 192.168.1.1?	Tell 192.168.1.					
906	105.949471	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69?	Tell 192.168.					
907	105.949501	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42 192.168.1.69	is at f8:fe:5e:6f:7b:ec					

Рис. 2.5: ARP request

12. Выполнён новый захват трафика и отправлен ICMP-запрос по доменному имени `www.yandex.ru`. Имя было успешно разрешено в IP-адрес `77.88.55.88`, и получены ответы без потерь пакетов.

```
PS C:\Users\Adel\Documents> ping www.yandex.ru

Обмен пакетами с www.yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=53
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=53

Статистика Ping для 77.88.55.88:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 10 мсек, Среднее = 9 мсек
```

Рис. 2.6: Ping по доменному имени

13. Проанализирован ARP-ответ, содержащий сопоставление IP-адреса 192.168.1.69 с MAC-адресом f8:fe:5e:6f:7b:ec.

No.	Time	Source	Destination	Protocol	Length Info
37	7.660993	ASUSTekCOMPU_78:b6:f2	Intel_6f:7b:ec	ARP	46 Who has 192.168.1.69? Tell 192.168.1.69
38	7.661021	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:f2	ARP	42 192.168.1.69 is at f8:fe:5e:6f:7b:ec
60	13.586320	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
61	13.596571	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
62	14.591521	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
63	14.602207	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
69	15.604749	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
70	15.614817	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1
86	16.617226	192.168.1.69	77.88.55.88	ICMP	74 Echo (ping) request id=0x0001, seq=1
87	16.627143	77.88.55.88	192.168.1.69	ICMP	78 Echo (ping) reply id=0x0001, seq=1

Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)	0000
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)	0010
.... .0. = LG bit: Globally unique address (factory default)	0020
.... .0. = IG bit: Individual address (unicast)	
Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)	
.... .0. = LG bit: Globally unique address (factory default)	
.... .0. = IG bit: Individual address (unicast)	
Type: ARP (0x0806)	
[Stream index: 0]	
Address Resolution Protocol (reply)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: reply (2)	
Sender MAC address: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)	
Sender IP address: 192.168.1.69	
Target MAC address: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)	
Target IP address: 192.168.1.1	

Рис. 2.7: ARP reply

14. Изучен ICMP Echo Request к внешнему узлу 77.88.55.88. На канальном уровне кадр направляется на MAC-адрес шлюза, так как целевой IP-адрес находится за пределами локальной подсети.

No.	Time	Source	Destination	Protocol	Length	Info
37	7.660993	ASUSTekCOMPU_78:b6:...	Intel_6f:7b:ec	ARP	46	Who has 192.168.1.69? Tell 192.168...
38	7.661021	Intel_6f:7b:ec	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.69 is at f8:fe:5e:6f:7b:e...
→	60 13.586320	192.168.1.69	77.88.55.88	ICMP	74	Echo (ping) request id=0x0001, seq=0
←	61 13.596571	77.88.55.88	192.168.1.69	ICMP	78	Echo (ping) reply id=0x0001, seq=1
62	14.591521	192.168.1.69	77.88.55.88	ICMP	74	Echo (ping) request id=0x0001, seq=2

...0.... = IG bit: Individual address (unicast)
 Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
 ...0.... = LG bit: Globally unique address (factory default)
 ...0.... = IG bit: Individual address (unicast)
 Type: IPv4 (0x0800)
 [Stream index: 0]
 Internet Protocol Version 4, Src: 192.168.1.69, Dst: 77.88.55.88
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x3edd (16093)
 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: ICMP (1)
 Header Checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.69
 Destination Address: 77.88.55.88
 [Stream index: 12]
 Internet Control Message Protocol
 Type: Echo (ping) request (8)
 Code: 0
 Checksum: 0x4d56 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 5 (0x0005)
 Sequence Number (LE): 1280 (0x0500)
 [Response frame: 61]
 Data (32 bytes)

Рис. 2.8: ICMP request к внешнему узлу

15. Изучен ICMP Echo Reply от внешнего узла. На канальном уровне источник кадра — MAC-адрес шлюза, что подтверждает корректную работу маршрутизации и повторную инкапсуляцию пакетов при передаче в локальную сеть.

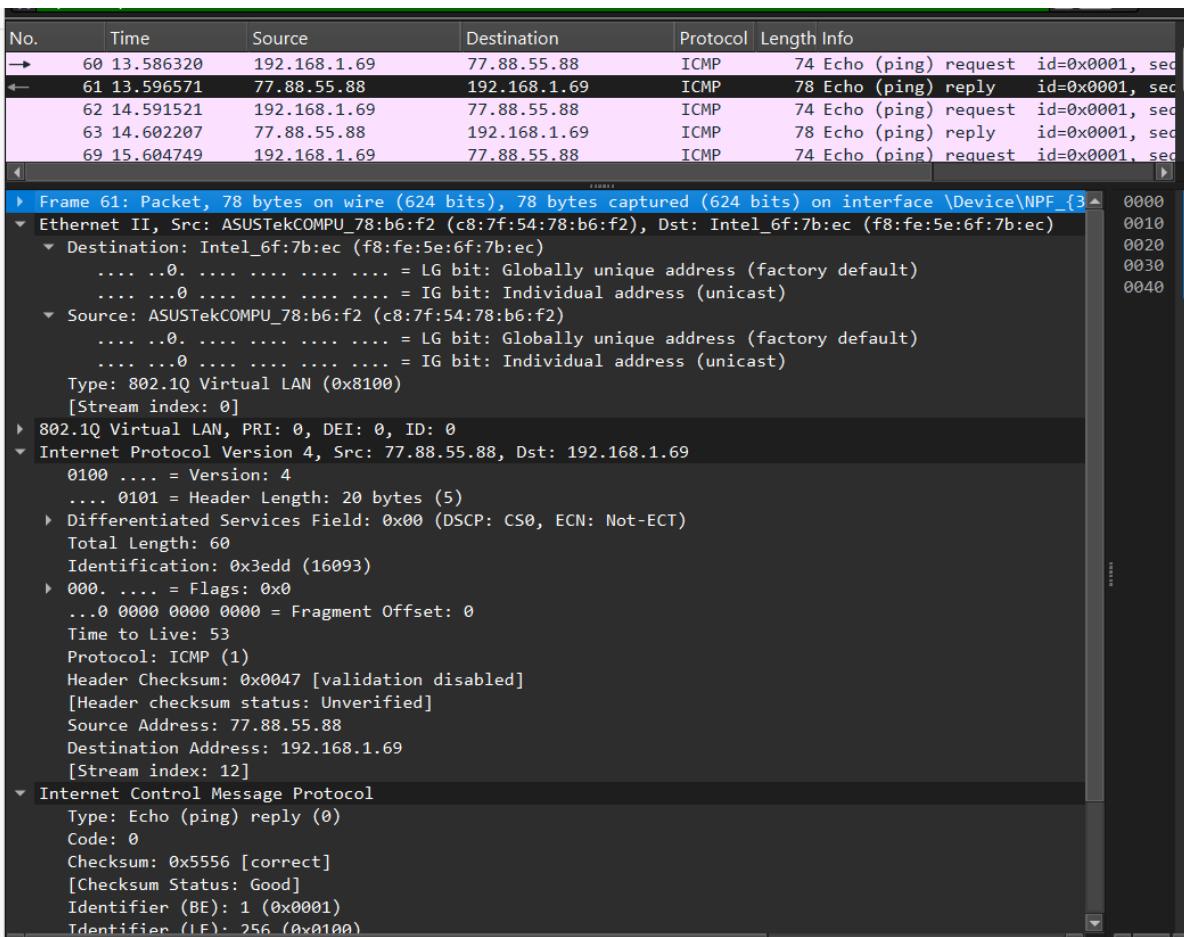


Рис. 2.9: ICMP reply от внешнего узла

2.3 Анализ протоколов транспортного уровня в Wireshark (HTTP, DNS, QUIC)

- На рабочем устройстве запущен анализатор сетевого трафика Wireshark. В качестве интерфейса захвата выбран активный беспроводной сетевой адаптер. Убедившись в начале захвата пакетов, выполнены действия для генерации сетевого трафика.
- В браузере выполнен переход на сайт, работающий по протоколу HTTP. В процессе загрузки страницы и перехода по ссылкам был сгенерирован HTTP-трафик, который зафиксирован в Wireshark.

3. Для анализа HTTP-трафика в строке фильтра Wireshark указан фильтр `http`. В результате отображены HTTP-запросы и ответы, инкапсулированные в сегменты TCP.

Проанализирован HTTP-запрос **GET**:

- IP-адрес источника: `192.168.1.69`;
- IP-адрес назначения: `188.184.67.127`;
- Протокол транспортного уровня: TCP;
- Порт источника: `54457` (динамический клиентский порт);
- Порт назначения: `80` (HTTP);
- Флаги TCP: PSH, ACK, указывают на передачу прикладных данных и подтверждение ранее полученных сегментов;
- Длина полезной нагрузки TCP: 473 байта;
- На прикладном уровне зафиксирован HTTP-запрос GET ресурса `/hypertext/www/TheProject.html`.

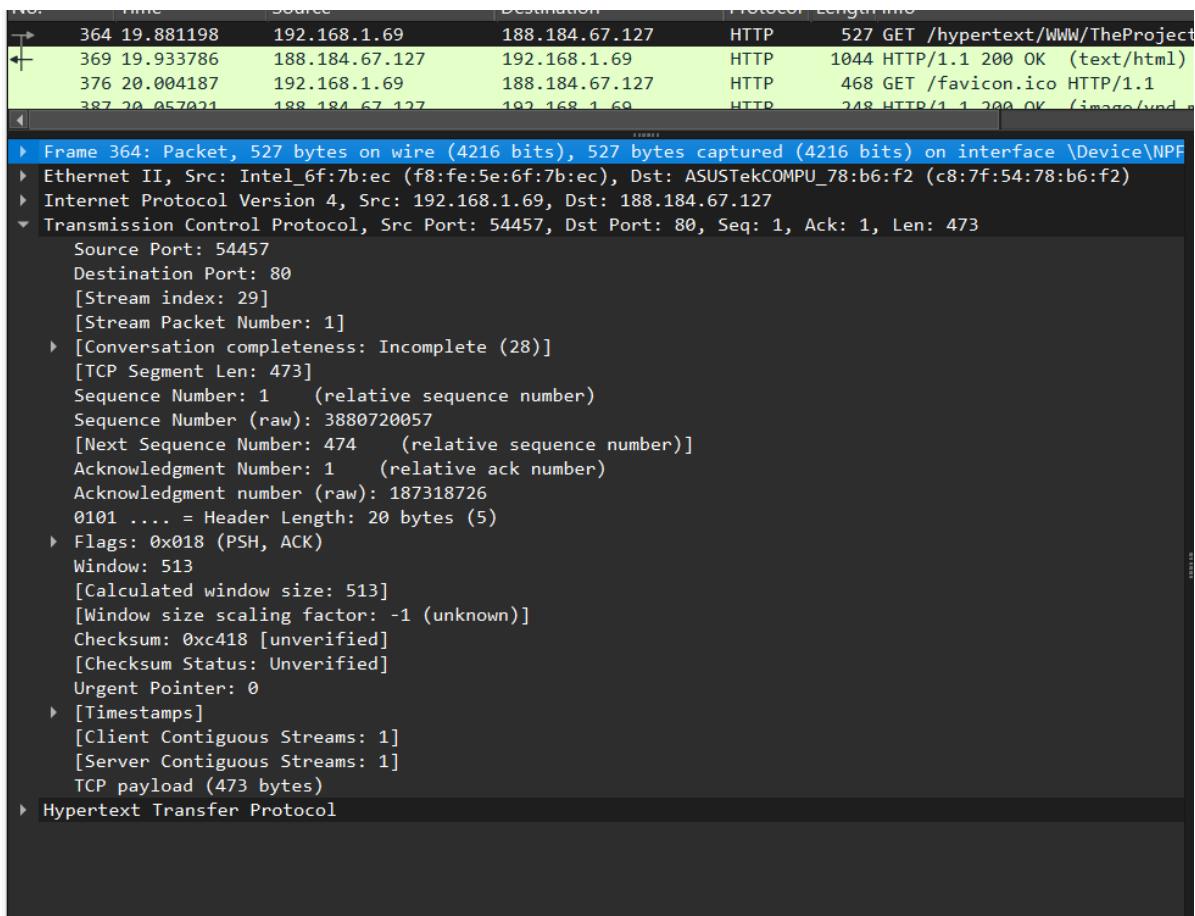


Рис. 2.10: HTTP GET запрос и параметры TCP-сегмента

4. Проанализирован HTTP-ответ сервера:

- IP-адрес источника: 188.184.67.127;
- IP-адрес назначения: 192.168.1.69;
- Порт источника: 80;
- Порт назначения: 54457;
- Длина TCP-сегмента: 990 байт;
- Зафиксирован статус ответа **HTTP/1.1 200 OK**;
- Тип содержимого: **text/html**;
- Данные передаются в нескольких TCP-сегментах с последующей сборкой (TCP reassembly).

No.	Time	Source	Destination	Protocol	Length	Info
364	19.881198	192.168.1.69	188.184.67.127	HTTP	527	GET /hypertext/WWW/TheProject.htm
369	19.933786	188.184.67.127	192.168.1.69	HTTP	1044	HTTP/1.1 200 OK (text/html)
376	20.004187	192.168.1.69	188.184.67.127	HTTP	468	GET /favicon.ico HTTP/1.1
387	20.057021	188.184.67.127	192.168.1.69	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
Frame 369: Packet, 1044 bytes on wire (8352 bits), 1044 bytes captured (8352 bits) on interface \Device\N						
Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)						
Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.1.69						
Transmission Control Protocol, Src Port: 80, Dst Port: 54457, Seq: 1461, Ack: 474, Len: 990						
Source Port: 80						
Destination Port: 54457						
[Stream index: 29]						
[Stream Packet Number: 4]						
[Conversation completeness: Incomplete (28)]						
[TCP Segment Len: 990]						
Sequence Number: 1461 (relative sequence number)						
Sequence Number (raw): 187320186						
[Next Sequence Number: 2451 (relative sequence number)]						
Acknowledgment Number: 474 (relative ack number)						
Acknowledgment number (raw): 3880720530						
0101 = Header Length: 20 bytes (5)						
Flags: 0x018 (PSH, ACK)						
Window: 501						
[Calculated window size: 501]						
[Window size scaling factor: -1 (unknown)]						
Checksum: 0x3d23 [unverified]						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
[Timestamps]						
[SEQ/ACK analysis]						
[Client Contiguous Streams: 1]						
[Server Contiguous Streams: 1]						
TCP payload (990 bytes)						
TCP segment data (990 bytes)						
[2 Reassembled TCP Segments (2450 bytes): #368(1460), #369(990)]						
Hypertext Transfer Protocol						
Line-based text data: text/html (73 lines)						

Рис. 2.11: HTTP ответ 200 OK и сборка TCP-сегментов

5. Для анализа доменных запросов в строке фильтра Wireshark указан фильтр dns. В результате отображены DNS-запросы и ответы, передаваемые по протоколу UDP.

Проанализирован DNS-запрос:

- IP-адрес источника: 192.168.1.69;
- IP-адрес назначения: 192.168.1.1 (DNS-сервер);
- Протокол транспортного уровня: UDP;
- Порт источника: 55855 (динамический);
- Порт назначения: 53 (DNS);
- Тип сообщения: Standard query;

- Тип запроса: A / HTTPS;
- Длина UDP-пакета: 48 байт.

No.	Time	Source	Destination	Protocol	Length	Info
48	4.826737	192.168.1.69	192.168.1.1	DNS	88	Standard query 0x822f HTTPS brows
49	4.826824	192.168.1.69	192.168.1.1	DNS	88	Standard query 0x2b0c A browser.t
52	4.848430	192.168.1.1	192.168.1.69	DNS	139	Standard query response 0x822f HT
53	4.848681	192.168.1.1	192.168.1.69	DNS	104	Standard query response 0x2b0c A
78	4.897774	192.168.1.69	192.168.1.1	DNS	82	Standard query 0x06b4 HTTPS stora
79	4.897869	192.168.1.69	192.168.1.1	DNS	82	Standard query 0x7cd0 A storage.a
80	4.930811	192.168.1.1	192.168.1.69	DNS	140	Standard query response 0x06b4 HT
81	4.930811	192.168.1.1	192.168.1.69	DNS	98	Standard query response 0x7cd0 A

Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.69, Dst: 192.168.1.1
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 68
Identification: 0x81bd (33213)
000. = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.69
Destination Address: 192.168.1.1
[Stream index: 8]
User Datagram Protocol, Src Port: 55855, Dst Port: 53
Source Port: 55855
Destination Port: 53
Length: 48
Checksum: 0x83d8 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (40 bytes)
Domain Name System (query)

Рис. 2.12: DNS запрос по протоколу UDP

6. Проанализирован DNS-ответ сервера:

- IP-адрес источника: 192.168.1.1;
- IP-адрес назначения: 192.168.1.69;
- Протокол транспортного уровня: UDP;
- Порт источника: 53;
- Порт назначения: 55855;
- Тип сообщения: Standard query response;
- В ответе содержится сопоставление доменного имени с IP-адресом;

- Установлен флаг **Don't fragment**, значение TTL равно 64.

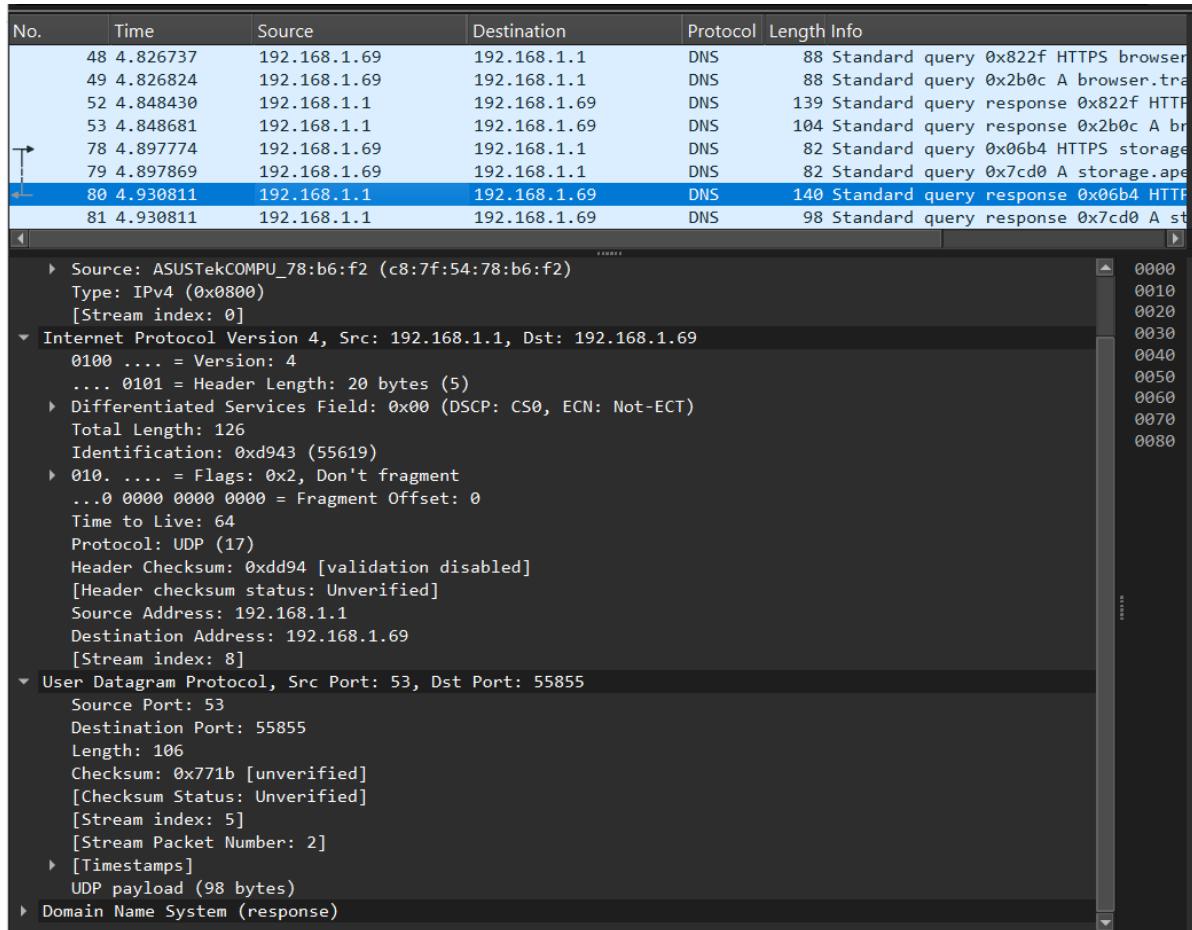


Рис. 2.13: DNS ответ с результатом разрешения имени

7. Для анализа современного транспортного протокола в строке фильтра Wireshark указан фильтр `quic`. Зафиксирован обмен данными между клиентом и внешним сервером по протоколу QUIC, использующему UDP.

Проанализирован пакет QUIC Initial:

- IP-адрес источника: 173.194.220.94;
- IP-адрес назначения: 192.168.1.69;
- Протокол транспортного уровня: UDP;
- Порт источника: 443;
- Порт назначения: 50215;

- Тип заголовка QUIC: Long Header;
- Тип пакета: Initial;
- Версия QUIC: 1;
- Используются идентификаторы соединения (Connection ID);
- Передаётся криптографическая информация для установки защищённого соединения.

No.	Time	Source	Destination	Protocol	Length	Info
3570	486.615374	192.168.1.69	173.194.220.94	QUIC	121	0-RTT, DCID=ec4db1023fe2ebc3
3694	486.638934	173.194.220.94	192.168.1.69	QUIC	82	Initial, SCID=ec4db1023fe2ebc3
3712	486.639045	173.194.220.94	192.168.1.69	QUIC	1292	Initial, SCID=ec4db1023fe2ebc3
3725	486.644577	173.194.220.94	192.168.1.69	QUIC	1292	Initial, SCID=ec4db1023fe2ebc3
3726	486.644577	173.194.220.94	192.168.1.69	QUIC	341	Protected Payload (KP0)
3727	486.644577	173.194.220.94	192.168.1.69	QUIC	990	Protected Payload (KP0)
3786	486.644869	192.168.1.69	173.194.220.94	QUIC	120	Handshake, DCID=ec4db1023fe2ebc3
3787	486.644908	192.168.1.69	173.194.220.94	QUIC	73	Protected Payload (KP0), DCID=ec4db1023fe2ebc3

Internet Protocol Version 4, Src: 173.194.220.94, Dst: 192.168.1.69

User Datagram Protocol, Src Port: 443, Dst Port: 50215

Source Port: 443
Destination Port: 50215
Length: 1258
Checksum: 0x3c61 [unverified]
[Checksum Status: Unverified]
[Stream index: 70]
[Stream Packet Number: 6]
[Timestamps]
UDP payload (1250 bytes)

QUIC IETF

QUIC Connection information
[Packet Length: 1250]
1.... = Header Form: Long Header (1)
.1... = Fixed Bit: True
.00 = Packet Type: Initial (0)
[.... 00.. = Reserved: 0]
[.... ..00 = Packet Number Length: 1 bytes (0)]
Version: 1 (0x00000001)
Destination Connection ID Length: 0
Source Connection ID Length: 8
Source Connection ID: ec4db1023fe2ebc3
Token Length: 0
Length: 1232
[Packet Number: 3]
Payload [...]: 5fc8414638cb551c65eb5bac46f67931a41cebc85d2176654955e613c94724b6d5e183647c2a46f601e0a8

CRYPTO
PADDING Length: 27

Рис. 2.14: QUIC Initial пакет и параметры соединения

8. Проанализирован пакет QUIC Handshake:

- Тип пакета: Handshake;
- Длина пакета: 78 байт;
- Передача осуществляется поверх UDP;

- Часть полезной нагрузки зашифрована, что подтверждается невозможностью расшифровки без ключей;
- Протокол QUIC обеспечивает встроенное шифрование и установку защищённого канала без использования TCP.

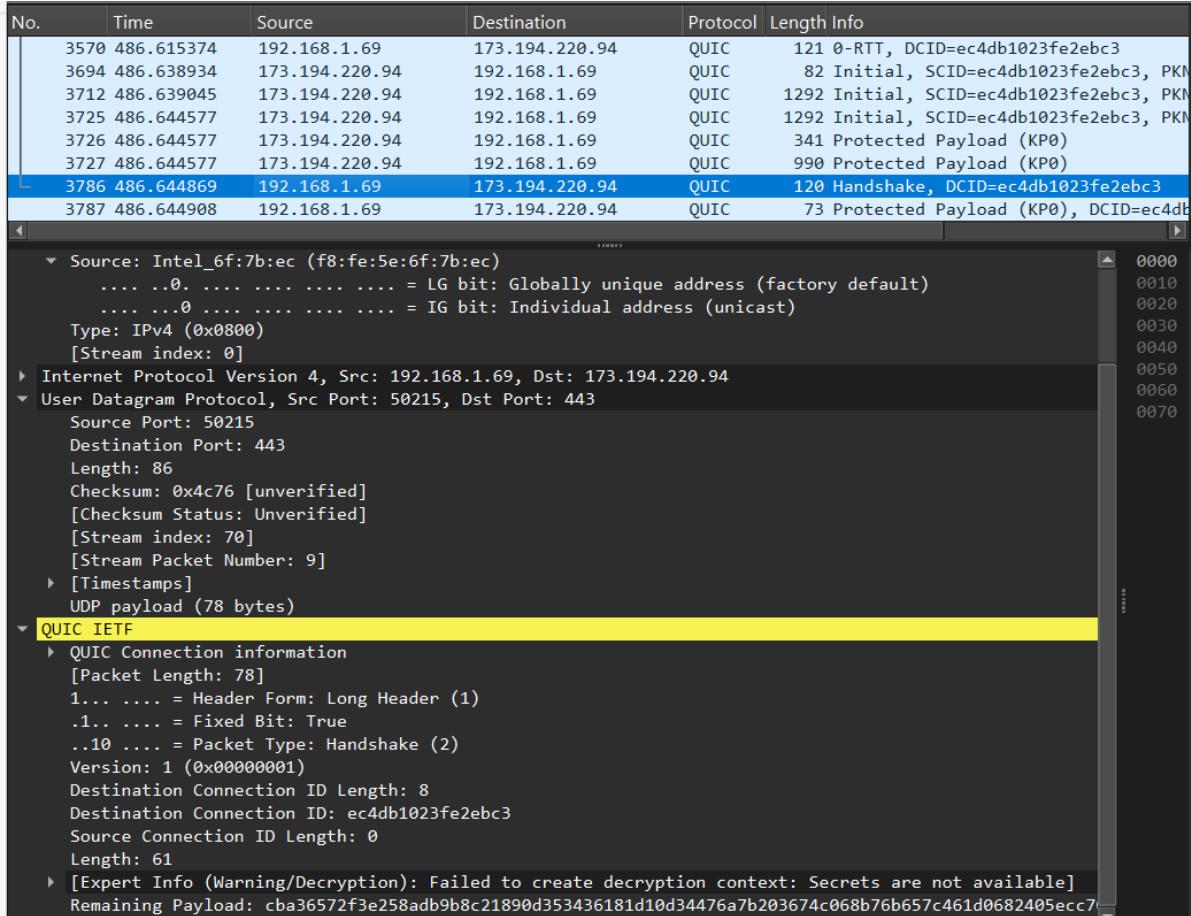


Рис. 2.15: QUIC Handshake пакет

9. По завершении анализа захвата трафика в Wireshark был остановлен. Полученные данные подтверждают особенности работы транспортных протоколов:

- HTTP использует TCP с установлением соединения и подтверждением доставки;
- DNS преимущественно использует UDP для быстрого обмена запросами и ответами;

- QUIC работает поверх UDP, объединяя функции транспортного уровня и криптографической защиты, обеспечивая низкие задержки и защищённую передачу данных.

2.4 Анализ handshake протокола TCP в Wireshark

1. На рабочем устройстве запущен Wireshark. В качестве источника захвата выбран активный беспроводной сетевой интерфейс. После выбора интерфейса подтверждено начало процесса захвата сетевого трафика.
2. Для генерации TCP-трафика выполнено подключение к удалённому веб-серверу по протоколу HTTP. В результате инициировано установление TCP-соединения между локальным узлом с IP-адресом 192.168.1.69 и удалённым сервером 188.184.67.127 по порту 80.
3. В процессе анализа списка пакетов Wireshark рассмотрен пример установки TCP-соединения (three-way handshake):

Этап 1 – SYN

Клиент инициирует соединение, отправляя TCP-сегмент:

- Источник: 192.168.1.69, порт 58579;
- Назначение: 188.184.67.127, порт 80;
- Установлен флаг SYN;
- Номер последовательности (Sequence Number): 0.

Этап 2 – SYN, ACK

Сервер подтверждает получение запроса и предлагает собственный номер последовательности:

- Источник: 188.184.67.127, порт 80;
- Назначение: 192.168.1.69, порт 58579;
- Установлены флаги SYN, ACK;

- Sequence Number: 0;
- Acknowledgment Number: 1, что подтверждает получение SYN от клиента.

Этап 3 – ACK

Клиент завершает установление соединения:

- Источник: 192.168.1.69, порт 58579;
- Назначение: 188.184.67.127, порт 80;
- Установлен флаг ACK;
- Sequence Number: 1;
- Acknowledgment Number: 1.

После выполнения этих трёх шагов TCP-соединение считается установленным, и стороны переходят к обмену данными прикладного уровня (HTTP).

22 1.751454	192.168.1.69	5.255.255.77	TCP	54 61516 → 443 [RST] Seq=2 Win=0
32 1.869600	192.168.1.69	188.184.67.127	TCP	66 58579 → 80 [SYN] Seq=0 Win=642
33 1.869939	192.168.1.69	188.184.67.127	TCP	66 63356 → 80 [SYN] Seq=0 Win=642
34 1.917396	188.184.67.127	192.168.1.69	TCP	66 80 → 58579 [SYN, ACK] Seq=0 Ack=1 Win=642
35 1.917491	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [ACK] Seq=1 Ack=1 Win=642
36 1.917776	192.168.1.69	188.184.67.127	HTTP	639 GET /hypertext/WWW/TheProject.html
37 1.918821	188.184.67.127	192.168.1.69	TCP	66 80 → 63356 [SYN, ACK] Seq=0 Ack=1 Win=642
38 1.918886	192.168.1.69	188.184.67.127	TCP	54 63356 → 80 [ACK] Seq=1 Ack=1 Win=642
39 1.966544	188.184.67.127	192.168.1.69	TCP	54 80 → 58579 [ACK] Seq=1 Ack=586
40 1.967158	188.184.67.127	192.168.1.69	HTTP	250 HTTP/1.1 304 Not Modified
41 1.967158	188.184.67.127	192.168.1.69	TCP	54 80 → 58579 [FIN, ACK] Seq=197 Ack=198
42 1.967188	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [ACK] Seq=586 Ack=199
43 1.967343	192.168.1.69	188.184.67.127	TCP	54 58579 → 80 [FIN, ACK] Seq=586 Ack=200
48 1.988930	192.168.1.69	87.250.251.20	TCP	66 63242 → 443 [SYN] Seq=0 Win=642
49 2.010326	87.250.251.20	192.168.1.69	TCP	66 443 → 63242 [SYN, ACK] Seq=0 Ack=1
50 2.010376	192.168.1.69	87.250.251.20	TCP	54 63242 → 443 [ACK] Seq=1 Ack=1 Win=642
51 2.010705	192.168.1.69	87.250.251.20	TLSv1.2	1984 Client Hello (SNI=browser.tra...
52 2.013386	192.168.1.69	149.154.167.99	TLSv1.2	203 Application Data

Рис. 2.16: Последовательность TCP handshake в списке пакетов Wireshark

4. После установления соединения зафиксирована передача данных:

- HTTP GET-запрос передаётся с флагами PSH, ACK;
- Сервер отправляет подтверждения (ACK) и ответ HTTP;
- В завершении соединения стороны обмениваются сегментами с флагами FIN, ACK, после чего соединение корректно закрывается.

Также зафиксированы TCP-сегменты с флагом RST, что указывает на принудительное завершение соединения для отдельных попыток подключения (например, при обращении к закрытому порту).

5. Для наглядного анализа последовательности обмена TCP-сегментами в Wireshark использован инструмент «Статистика → График потока». На графике отчётливо отображается:

- направление передачи сегментов между клиентом и сервером;
- этапы SYN → SYN, ACK → ACK;
- дальнейшая передача данных с флагами PSH, ACK;
- корректное завершение соединения с использованием FIN, ACK.

Изменение значений Seq и Ack на графике подтверждает корректную работу механизма нумерации байтов и подтверждения доставки данных в TCP.

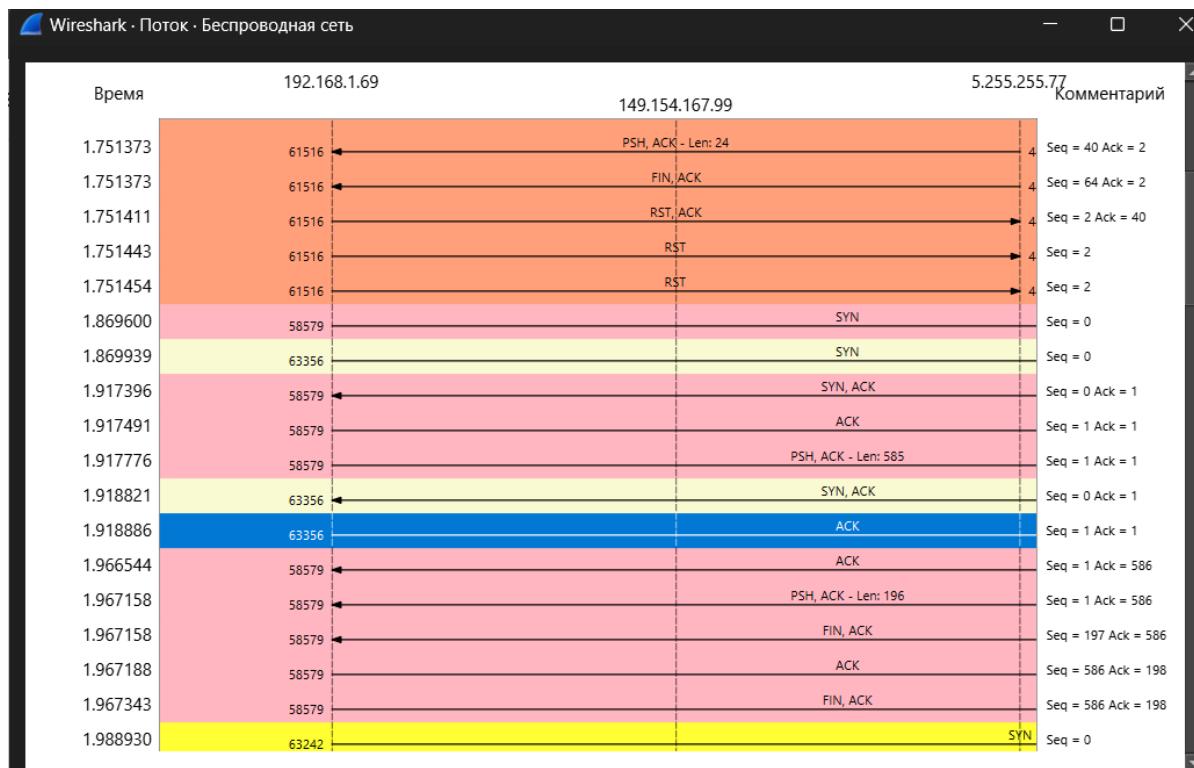


Рис. 2.17: График потока TCP-соединения в Wireshark

6. По завершении анализа захват трафика в Wireshark был остановлен. Получ-

ченные результаты подтверждают стандартный механизм установки TCP-соединения, состоящий из трёх этапов, а также демонстрируют процесс передачи данных и корректного завершения сеанса связи.

3 Заключение

В ходе выполнения лабораторной работы был выполнен захват и анализ сетевого трафика с использованием программы Wireshark. Изучены параметры сетевого подключения рабочей станции, определены IP- и MAC-адреса, а также принципы их использования на канальном и сетевом уровнях модели OSI.

Проведён анализ кадров протоколов ARP и ICMP, что позволило проследить процесс разрешения IP-адресов в MAC-адреса и подтвердить корректную работу механизма проверки доступности узлов в локальной и внешней сетях. Установлено, что при взаимодействии с внешними ресурсами на канальном уровне кадры адресуются MAC-адресу шлюза по умолчанию.

Дополнительно изучены протоколы транспортного и прикладного уровней HTTP, DNS и QUIC. Показаны различия в использовании протоколов TCP и UDP, а также особенности протокола QUIC, совмещающего функции транспортного уровня и криптографической защиты.

Отдельное внимание удалено анализу процесса установления TCP-соединения. На практике подтверждена работа трёхстороннего рукопожатия TCP, а также корректная передача и завершение соединения с использованием соответствующих флагов.

В результате выполненной работы закреплены практические навыки анализа сетевого трафика, интерпретации заголовков пакетов и понимания принципов взаимодействия протоколов различных уровней сетевой модели.