

Отчёт по лабораторной работе 3

Анализ трафика в Wireshark

Хамди Мохаммад

Содержание

1	Цель работы	5
2	Ход выполнения	6
2.1	Анализ кадров канального уровня в Wireshark	6
2.2	Анализ протоколов транспортного уровня в Wireshark	12
2.3	Анализ handshake протокола TCP в Wireshark	17
3	Заключение	19

Список иллюстраций

2.1	Результат команды <code>ipconfig</code>	7
2.2	Проверка доступности шлюза	7
2.3	Проверка доступности внешнего ресурса	11
2.4	Анализ ICMP-трафика при <code>ping google.com</code>	12
2.5	Анализ TCP-сессии	17
2.6	График потока TCP	18

Список таблиц

1 Цель работы

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

2 Ход выполнения

2.1 Анализ кадров канального уровня в Wireshark

1. На устройство была установлена программа **Wireshark** и запущен захват трафика на активном сетевом интерфейсе.
2. С помощью команды **ipconfig** были определены параметры сетевого подключения:
 - IP-адрес устройства — **192.168.1.35**
 - Маска подсети — **255.255.255.0**
 - Шлюз по умолчанию — **192.168.1.1**

```

PS C:\work\hamdimohammad\vagrant> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::52ff:33b6:449a:870f%18
    IPv4-адрес. . . . . : 192.168.1.35
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.1.1

Адаптер Ethernet Ethernet 2:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::d3f2:8384:1a21:d660%21
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

```

Рис. 2.1: Результат команды ipconfig

3. Для проверки доступности шлюза по умолчанию выполнена команда **ping 192.168.1.1**.

Ответы получены успешно, потерь пакетов нет.

```

PS C:\work\hamdimohammad\vagrant>
PS C:\work\hamdimohammad\vagrant> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 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% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\work\hamdimohammad\vagrant> |

```

Рис. 2.2: Проверка доступности шлюза

4. В **Wireshark** был применён фильтр `arp or icmp`, после чего зафиксированы ICMP-запросы и ответы между устройством и шлюзом.

Захват из Ethernet

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
43	25.470110	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
45	26.353498	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
46	26.353528	HuaweiTechno_66:db:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
67	38.559919	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145
180	48.886492	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
181	48.887000	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184	49.889283	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185	49.889674	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189	50.902327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190	50.902821	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193	51.913548	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194	51.913999	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
210	60.097244	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
248	71.152221	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
249	71.152253	HuaweiTechno_66:db:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
298	94.414703	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
307	98.590789	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145

[Time delta from previous displayed frame: 10.326573000 seconds]
[Time since reference or first frame: 48.886492000 seconds]
Frame Number: 180
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)
Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream Index: 4]
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
Internet Control Message Protocol

Internet Control Message Protocol: Protocol Пакеты: 353 · Отображено: 17 (4.8%) Профиль: Default

Захват из Ethernet

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
43	25.470110	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
45	26.353498	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
46	26.353528	HuaweiTechno_66:db:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
67	38.559919	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145
180	48.886492	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
181	48.887000	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184	49.889283	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185	49.889674	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189	50.902327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190	50.902821	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193	51.913548	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194	51.913999	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
210	60.097244	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
248	71.152221	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
249	71.152253	HuaweiTechno_66:db:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
298	94.414703	iCommSemicon_9a:80:...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
307	98.590789	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145
361	119.790925	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
362	119.790945	HuaweiTechno_66:db:...	ASUSTekCOMPU_78:b6:...	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

[Time delta from previous displayed frame: 0.000505000 seconds]
[Time since reference or first frame: 48.887000000 seconds]
Frame Number: 181
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
Destination: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)
Source: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream Index: 4]
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35
Internet Control Message Protocol

Internet Control Message Protocol: Protocol Пакеты: 372 · Отображено: 19 (5.1%) Профиль: Default

No.	Time	Source	Destination	Protocol	Length	Info
181	48.887000	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
184	49.889283	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
185	49.889874	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
189	50.902327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
190	50.902821	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
193	51.913548	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
194	51.913999	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
210	58.497244	IComSemicon_9a:80:: Broadcast	ARP	60	ARP Announcement for 192.168.1.32	
248	71.152221	ASUSTechno_78:b6:f2:: Broadcast	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1	
249	71.152253	HuaweiTechno_66:db:28:: ASUSTechno_78:b6:f2:: Broadcast	ARP	42	192.168.1.35 is at Ac:f0:45:66:db:28	
298	94.417403	IComSemicon_9a:80:: Broadcast	ARP	60	ARP Announcement for 192.168.1.32	
307	98.590789	82:81:04:82:d3:54 Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145	
361	119.790925	ASUSTechno_78:b6:f2:: Broadcast	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1	
362	119.790945	HuaweiTechno_66:db:28:: ASUSTechno_78:b6:f2:: Broadcast	ARP	42	192.168.1.35 is at Ac:f0:45:66:db:28	
394	129.825991	IComSemicon_9a:80:: Broadcast	ARP	60	ARP Announcement for 192.168.1.32	
498	155.162863	ASUSTechno_78:b6:f2:: Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.35	
499	155.163333	ASUSTechno_78:b6:f2:: Broadcast	ARP	42	192.168.1.1 is at c8:7f:54:78:b6:f2	
594	158.661720	82:81:04:82:d3:54 Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145	
534	164.392381	IComSemicon_9a:80:: Broadcast	ARP	60	ARP Announcement for 192.168.1.32	
718	198.821641	IComSemicon_9a:80:: Broadcast	ARP	60	ARP Announcement for 192.168.1.32	

[Time since reference or first frame: 71.152221000 seconds]

Frame Number: 248

Frame Length: 60 bytes (480 bits)

Capture Length: 60 bytes (480 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: ethernetII:arp]

[Coloring Rule Name: ARP]

[Coloring Rule String: arp]

▼ Ethernet II, Src: ASUSTechno_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno_66:db:28 (Ac:f0:45:66:db:28)

 Destination: HuaweiTechno_66:db:28 (Ac:f0:45:66:db:28)

 0. LG bit: Globally unique address (factory default)

 0. TG bit: Individual address (unicast)

 Source: ASUSTechno_78:b6:f2 (c8:7f:54:78:b6:f2)

 0. LG bit: Globally unique address (factory default)

 0. TG bit: Individual address (unicast)

 Type: ARP (0x0806)

 [Stream Index: 4]

 Packing: 00000000000000000000000000000000

 Trailer: c752ca5

▼ Address Resolution Protocol (request)

```
0000  Ac f0 45 66 db 28 c8 7f 54 78 b6 f2
0010  00 00 00 04 00 01 c8 7f 54 78 b6 f2
0020  00 00 00 00 00 00 c0 85 01 23 00 00
0030  00 00 00 00 00 00 00 00 c7 52 cc a5
```

Internet Control Message Protocol: Protocol

Пакеți: 721 - Обработано: 25 (3.5%)

Профиль: Default

Анализ ISMP-запроса:

- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника: **4c:fb:45:66:db:28** (устройство)
- MAC-адрес получателя (шлюз): **c8:7f:54:78:b6:f2**
- Тип MAC-адресов: **уникальные (unicast)**

Анализ ISMP-ответа:

- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника (шлюз): **c8:7f:54:78:b6:f2**

- MAC-адрес получателя (устройство): **4c:fb:45:66:db:28**

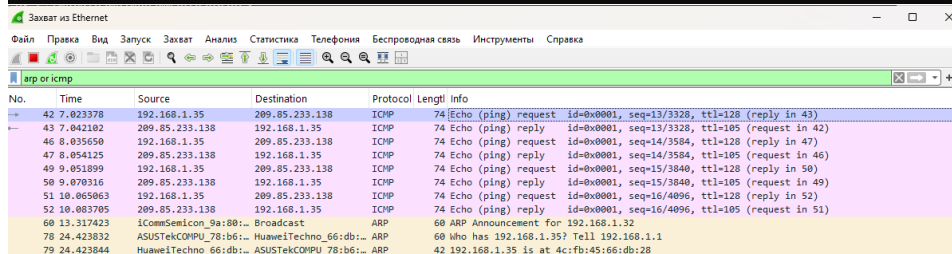
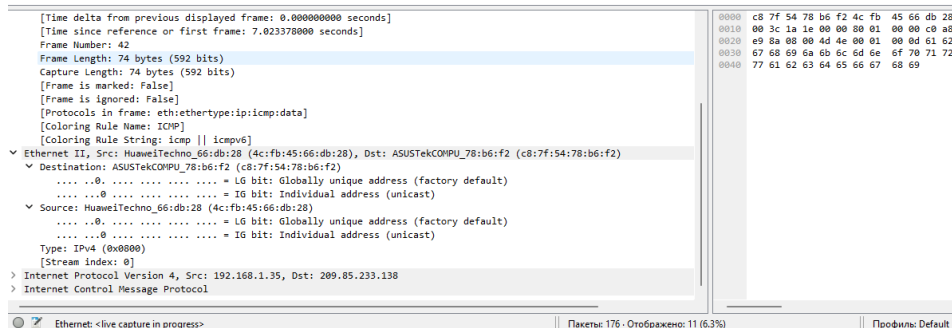
- Тип MAC-адресов: **уникальные (unicast)**

- Далее изучены кадры протокола **ARP**, фиксирующие обмен информацией об IP- и MAC-адресах в сети.

```
PS C:\work\hamdimohammad\vagrant> ping google.com

Обмен пакетами с google.com [209.85.233.138] с 32 байтами данных:
Ответ от 209.85.233.138: число байт=32 время=18мс TTL=105
Ответ от 209.85.233.138: число байт=32 время=18мс TTL=105
Ответ от 209.85.233.138: число байт=32 время=18мс TTL=105
Ответ от 209.85.233.138: число байт=32 время=18мс TTL=105

Статистика Ping для 209.85.233.138:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 18мсек, Максимальное = 18 мсек, Среднее = 18 мсек
PS C:\work\hamdimohammad\vagrant> |
```

ARP-запрос:

- “Кто имеет IP **192.168.1.35?**”

- Источник: **c8:7f:54:78:b6:f2**

- Адрес назначения: **ff:ff:ff:ff:ff:ff** (широковещательный, broadcast)

ARP-ответ:

- “IP **192.168.1.35** принадлежит MAC **4c:fb:45:66:db:28**”
- Источник: **4c:fb:45:66:db:28**
- Адрес назначения: **c8:7f:54:78:b6:f2**

6. Для анализа взаимодействия с внешними ресурсами был выполнен **ping google.com**.

Устройство получило ответы от IP-адреса **209.85.233.138**, время отклика составило в среднем **18 мс**.

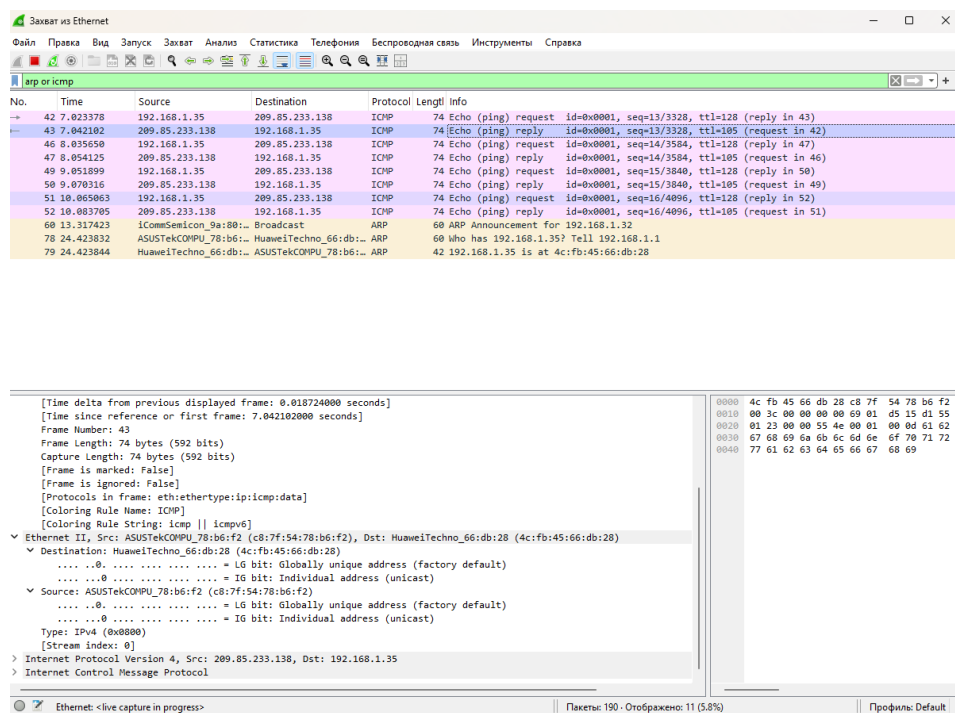


Рис. 2.3: Проверка доступности внешнего ресурса

В Wireshark были зафиксированы соответствующие ICMP-запросы и ответы, а также ARP-обмен для определения адреса шлюза.

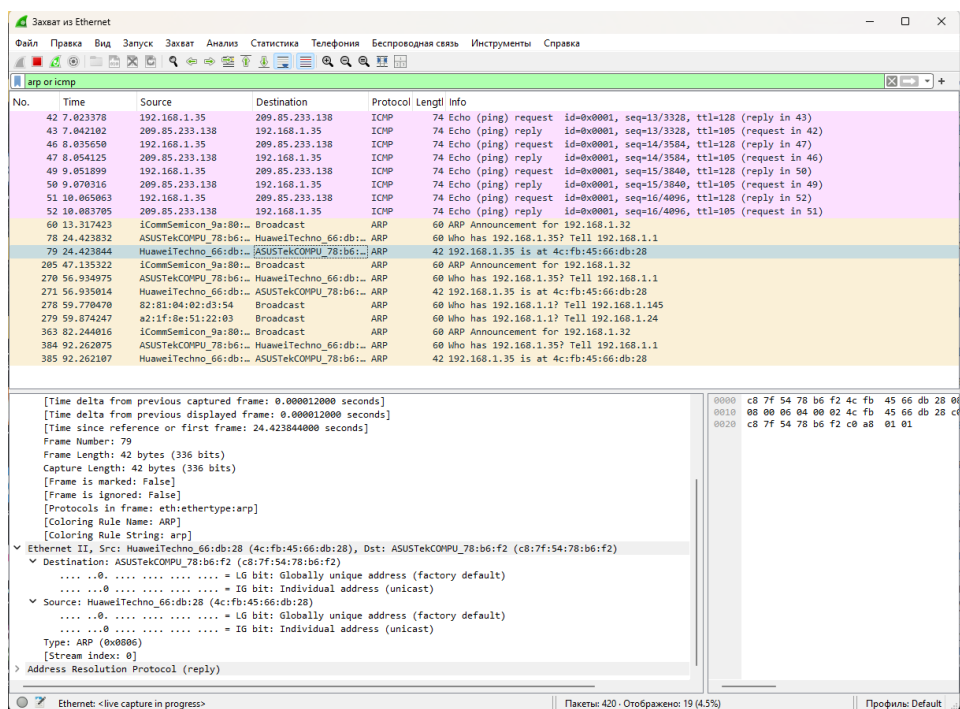


Рис. 2.4: Анализ ICMP-трафика при ping google.com

2.2 Анализ протоколов транспортного уровня в Wireshark

1. В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.
2. В браузере произведён переход на сайт <http://info.cern.ch/>, работающий по протоколу **HTTP**.
3. В Wireshark применён фильтр **http**. Зафиксирован обмен HTTP-запросами и ответами поверх протокола **TCP**.

Захват из Ethernet

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

http

No.	Time	Source	Destination	Protocol	Length	Info
347	23.756722	192.168.1.35	188.184.67.127	HTTP	497	GET / HTTP/1.1
349	23.810231	188.184.67.127	192.168.1.35	HTTP	932	HTTP/1.1 200 OK (text/html)
356	23.894813	192.168.1.35	188.184.67.127	HTTP	438	GET /favicon.ico HTTP/1.1
364	23.949575	188.184.67.127	192.168.1.35	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
503	41.501907	192.168.1.35	188.184.67.127	HTTP	557	GET /hypertext/WWW/TheProject.html HTTP/1.1
509	41.556199	188.184.67.127	192.168.1.35	HTTP	1044	HTTP/1.1 200 OK (text/html)

> Frame 347: 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interface \Device\NPF_{C2D0897A-6F95-42A3-8C8A-000000000000} (08:00:00:00:00:00) on interface \Device\NPF_{C2D0897A-6F95-42A3-8C8A-000000000000} (08:00:00:00:00:00)

> Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) (c8:7f:54:78:b6:f2)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 188.184.67.127

> Transmission Control Protocol, Src Port: 61111, Dst Port: 80, Seq: 1, Ack: 1, Len: 443

Source Port: 61111

Destination Port: 80

[Stream index: 3]

[Stream Packet Number: 4]

> [Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 443]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3946666371

[Next Sequence Number: 444 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 4115465422

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 1026

[calculated window size: 262656]

[Window size scaling factor: 256]

Checksum: 0xc3d8 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (443 bytes)

> Hypertext Transfer Protocol

Захват из Ethernet

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

http

No.	Time	Source	Destination	Protocol	Length	Info
347	23.756722	192.168.1.35	188.184.67.127	HTTP	497	GET / HTTP/1.1
349	23.810231	188.184.67.127	192.168.1.35	HTTP	932	HTTP/1.1 200 OK (text/html)
356	23.894813	192.168.1.35	188.184.67.127	HTTP	438	GET /favicon.ico HTTP/1.1
364	23.949575	188.184.67.127	192.168.1.35	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
503	41.501907	192.168.1.35	188.184.67.127	HTTP	557	GET /hypertext/WWW/TheProject.html HTTP/1.1
509	41.556199	188.184.67.127	192.168.1.35	HTTP	1044	HTTP/1.1 200 OK (text/html)

> Frame 349: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF_{C2D0897A-6F95-42A3-8C8A-000000000000} (08:00:00:00:00:00) on interface \Device\NPF_{C2D0897A-6F95-42A3-8C8A-000000000000} (08:00:00:00:00:00)

> Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)

> Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.1.35

> Transmission Control Protocol, Src Port: 80, Dst Port: 61111, Seq: 1, Ack: 444, Len: 878

Source Port: 80

Destination Port: 61111

[Stream index: 3]

[Stream Packet Number: 6]

> [Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 878]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 4115465422

[Next Sequence Number: 879 (relative sequence number)]

Acknowledgment Number: 444 (relative ack number)

Acknowledgment number (raw): 3946666814

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window: 249

[calculated window size: 31872]

[Window size scaling factor: 128]

Checksum: 0x0da3 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

> [SEQ/ACK analysis]

TCP payload (878 bytes)

> Hypertext Transfer Protocol

> Line-based text data: text/html (13 lines)

Пакеты: 711 - Отображено: 6 (0.8%)

Профиль: Default

Пояснение:

- Запрос отправляется с порта **61111** клиента (192.168.1.35) на порт **80** сервера (188.184.67.127).

- Используется протокол **Ethernet II** → **IPv4** → **TCP** → **HTTP**.

- В TCP-сегменте указывается **Sequence Number** и **Acknowledgment Number**, обеспечивающие надёжную доставку данных.

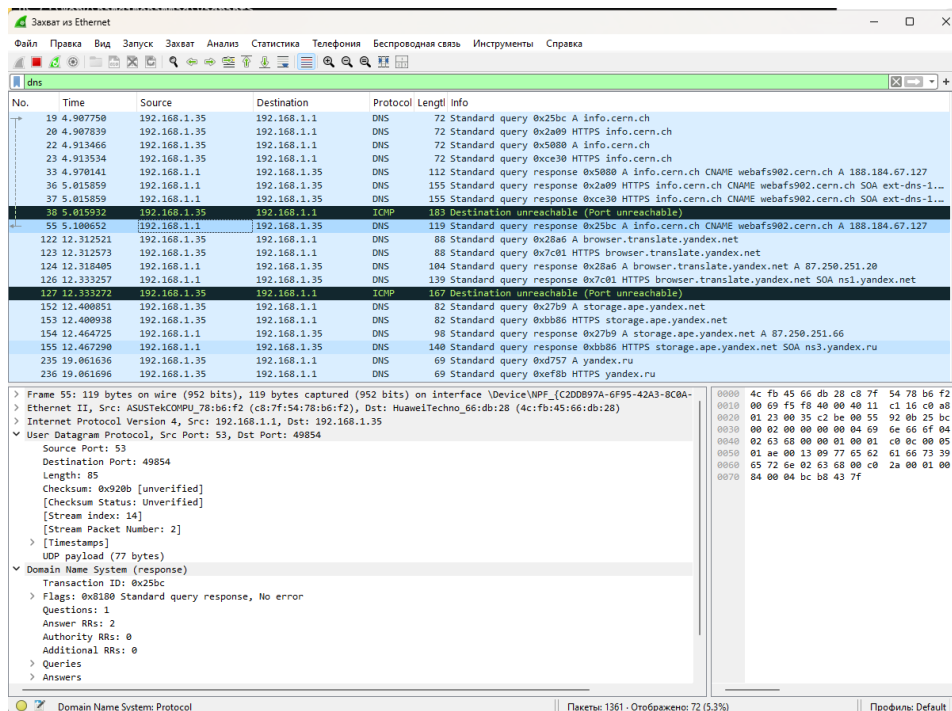
- В кадре видно передачу **HTTP GET-запроса** и ответ **HTTP/1.1 200 OK** с HTML-страницей.

4. В Wireshark применён фильтр dns. Зафиксированы запросы и ответы по протоколу **DNS**, работающему поверх **UDP**.

No.	Time	Source	Destination	Protocol	Length	Info
19	4.907750	192.168.1.35	192.168.1.1	DNS	72	Standard query 0x25bc A info.cern.ch
20	4.907839	192.168.1.35	192.168.1.1	DNS	72	Standard query 0x2a09 HTTPS info.cern.ch
22	4.913466	192.168.1.35	192.168.1.1	DNS	72	Standard query 0x5000 A info.cern.ch
23	4.913534	192.168.1.35	192.168.1.1	DNS	72	Standard query 0xc30 HTTPS info.cern.ch
33	4.970141	192.168.1.1	192.168.1.35	DNS	112	Standard query response 0x5000 A info.cern.ch CNAME webafs902.cern.ch A 188.184.67.127
36	5.015859	192.168.1.1	192.168.1.35	DNS	155	Standard query response 0x2a09 HTTPS info.cern.ch CNAME webafs902.cern.ch SOA ext-dns-1...
37	5.015859	192.168.1.1	192.168.1.35	DNS	155	Standard query response 0xc30 HTTPS info.cern.ch CNAME webafs902.cern.ch SOA ext-dns-1...
38	5.015932	192.168.1.35	192.168.1.1	TCP	163	Destination unreachable (Port unreachable)
55	5.100652	192.168.1.1	192.168.1.35	DNS	119	Standard query response 0x25bc A info.cern.ch CNAME webafs902.cern.ch A 188.184.67.127
122	12.312521	192.168.1.35	192.168.1.1	DNS	80	Standard query 0x28a6 A browser.translate.yandex.net
123	12.312573	192.168.1.35	192.168.1.1	DNS	80	Standard query 0x7c81 HTTPS browser.translate.yandex.net
124	12.318405	192.168.1.1	192.168.1.35	DNS	104	Standard query response 0x28a6 A browser.translate.yandex.net A 87.250.251.20
126	12.333257	192.168.1.1	192.168.1.35	DNS	139	Standard query response 0x7c81 HTTPS browser.translate.yandex.net SOA ns1.yandex.net
127	12.333272	192.168.1.35	192.168.1.1	TCP	167	Destination unreachable (Port unreachable)
152	12.400851	192.168.1.35	192.168.1.1	DNS	82	Standard query 0x27b9 A storage.ape.yandex.net
153	12.400930	192.168.1.35	192.168.1.1	DNS	82	Standard query 0xb0b6 HTTPS storage.ape.yandex.net
154	12.464725	192.168.1.1	192.168.1.35	DNS	98	Standard query response 0x27b9 A storage.ape.yandex.net A 87.250.251.66
155	12.467290	192.168.1.1	192.168.1.35	DNS	140	Standard query response 0xb0b6 HTTPS storage.ape.yandex.net SOA ns3.yandex.ru
235	19.061636	192.168.1.35	192.168.1.1	DNS	69	Standard query 0xd757 A yandex.ru
236	19.061696	192.168.1.35	192.168.1.1	DNS	69	Standard query 0xef8b HTTPS yandex.ru

Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on Interface \Device\NPF_{C2D0897A-6F95-42A3-8C0A-FE...} (c8:7f:54:78:b6:f2)
 Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
 Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 49854, Dst Port: 53
 Source Port: 49854
 Destination Port: 53
 Length: 38
 Checksum: 0x83ac [unverified]
 [Checksum Status: Unverified]
 [Stream index: 14]
 [Stream Packet Number: 1]
 [Timestamps]
 UDP payload (30 bytes)
 Domain Name System (query)
 Transaction ID: 0x25bc
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 [Response In: 55]

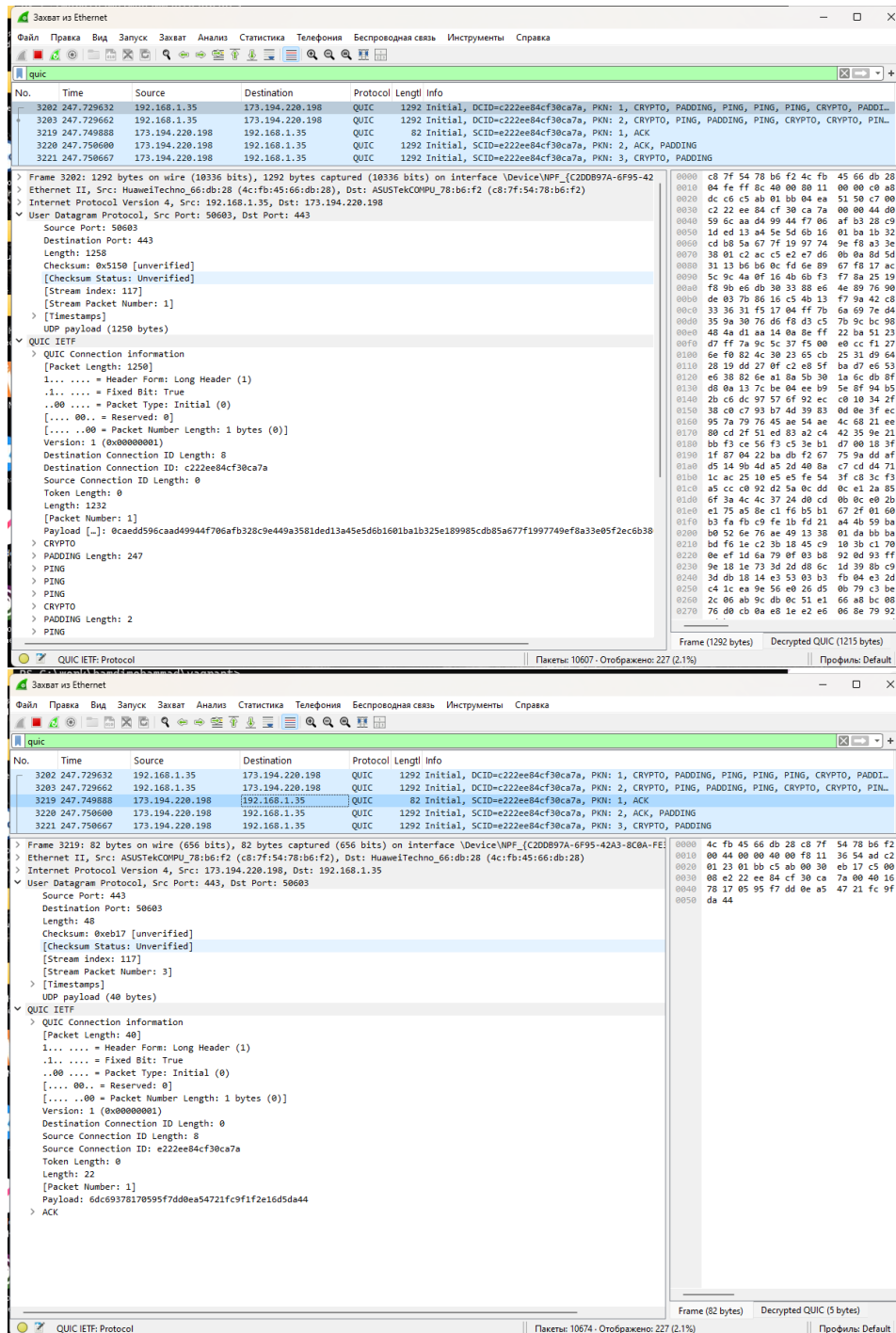
Domain Name System: Protocol Пакеты: 1318 · Отображено: 72 (5.5%) Профиль: Default



Пояснение:

- Запрос отправляется с порта **49854** клиента (192.168.1.35) на порт **53** сервера (192.168.1.1).
- Пример: запрос имени `info.cern.ch` с типом записи **A**.
- В ответ сервер возвращает IP-адрес **188.184.67.127**, что подтверждает успешное разрешение имени.
- Используется структура: **Ethernet II** → **IPv4** → **UDP** → **DNS**.

5. В Wireshark применён фильтр `quic`. Зафиксирован обмен трафиком по протоколу **QUIC**, работающему поверх **UDP**.



Пояснение:

- Источник: клиент **192.168.1.35**, назначение: сервер **173.194.220.198**, порт **443**.

- Используется протокол: **Ethernet II → IPv4 → UDP → QUIC**.

2.3 Анализ handshake протокола TCP в Wireshark

1. В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.
2. Для генерации TCP-трафика было выполнено соединение с веб-сервером по протоколу **HTTP**.
3. В Wireshark зафиксирован процесс установления TCP-сессии (трёхстороннее рукопожатие).

18	3.580515	192.168.1.35	192.168.1.1	DNS	72 Standard query 0xba41 HTTPS info.cern.ch
19	3.581124	192.168.1.35	188.184.67.127	HTTP	609 GET / HTTP/1.1
20	3.635289	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=1 Ack=556 Win=249 Len=0
21	3.636939	188.184.67.127	192.168.1.35	HTTP	250 HTTP/1.1 304 Not Modified
22	3.636973	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [FIN, ACK] Seq=197 Ack=556 Win=249 Len=0
23	3.636994	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [ACK] Seq=556 Ack=198 Win=1025 Len=0
24	3.637253	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [FIN, ACK] Seq=556 Ack=198 Win=1025 Len=0
25	3.647228	192.168.1.35	87.250.251.20	TLSv1.2	249 Application Data
26	3.647254	192.168.1.35	87.250.251.20	TLSv1.2	358 Application Data
27	3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=196 Win=166 Len=0
28	3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=500 Win=165 Len=0
29	3.656358	87.250.251.20	192.168.1.35	TLSv1.2	96 Application Data
30	3.688028	87.250.251.20	192.168.1.35	TLSv1.2	633 Application Data
31	3.688028	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=198 Ack=557 Win=249 Len=0
32	3.688107	192.168.1.35	87.250.251.20	TCP	54 61182 → 443 [ACK] Seq=500 Ack=622 Win=1019 Len=0
33	3.688797	192.168.1.35	87.250.251.20	TLSv1.2	96 Application Data
34	3.721314	192.168.1.1	192.168.1.35	DNS	155 Standard query response 0xba41 HTTPS info.cern.ch CNAME webafs902.cern.ch SOA ex
35	3.738500	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=500 Ack=622 Win=1019 Len=0

Рис. 2.5: Анализ TCP-сессии

Этапы установления соединения:

- **SYN**: клиент (192.168.1.35) отправляет на сервер (188.184.67.127) запрос на установление соединения с флагом SYN и начальным номером последовательности (**Seq = 1**).
- **SYN + ACK**: сервер отвечает подтверждением с флагами SYN и ACK, устанавливая свой номер последовательности (**Seq = 1**) и подтверждая получение данных клиента (**Ack = 2**).
- **ACK**: клиент подтверждает получение пакета от сервера, устанавливая **Ack = 2**.

После этого соединение считается установленным, и возможна передача данных (HTTP-запрос/ответ).

4. Для анализа был построен **график потока** (Flow Graph) в Wireshark.

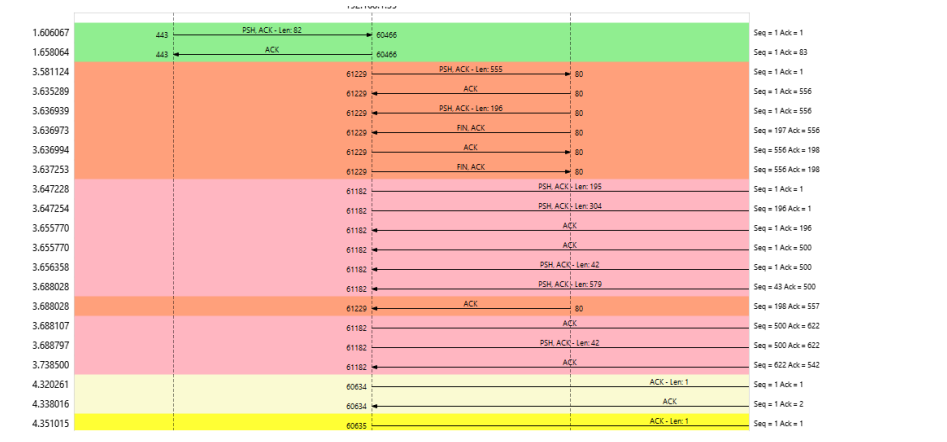


Рис. 2.6: График потока TCP

Пояснение к графику:

- На графике наглядно отображены все этапы TCP-взаимодействия.
- Видно трёхстороннее рукопожатие (SYN → SYN+ACK → ACK).
- После установления соединения фиксируется передача данных (HTTP GET, ответы сервера, обмен ACK).
- Завершение соединения происходит с помощью пакетов **FIN**, **ACK**, что также отражено на графике.

5. После анализа захват трафика в Wireshark был остановлен.

3 Заключение

В ходе работы был проведён анализ установления соединения по протоколу **TCP** с использованием программы **Wireshark**.

Было зафиксировано трёхстороннее рукопожатие ($\text{SYN} \rightarrow \text{SYN+ACK} \rightarrow \text{ACK}$), подтверждающее успешное начало TCP-сессии.

С помощью графика потока были проанализированы этапы установления и завершения соединения, а также последующая передача данных.