

# Сетевые технологии

## Анализ трафика в Wireshark

---

Хамди Мохаммад

15 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цели и задачи работы

---

## Цель лабораторной работы

---

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

## Выполнение лабораторной работы

---

## Анализ кадров канального уровня

```
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. 1: Результат команды ipconfig

## Анализ кадров канального уровня

```
PS C:\work\hamdimohammad\vagrant>
PS C:\work\hamdimohammad\vagrant> 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

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 = 0 мсек, Среднее = 0 мсек
PS C:\work\hamdimohammad\vagrant> |
```

Рис. 2: Проверка доступности шлюза

# Анализ кадров канального уровня

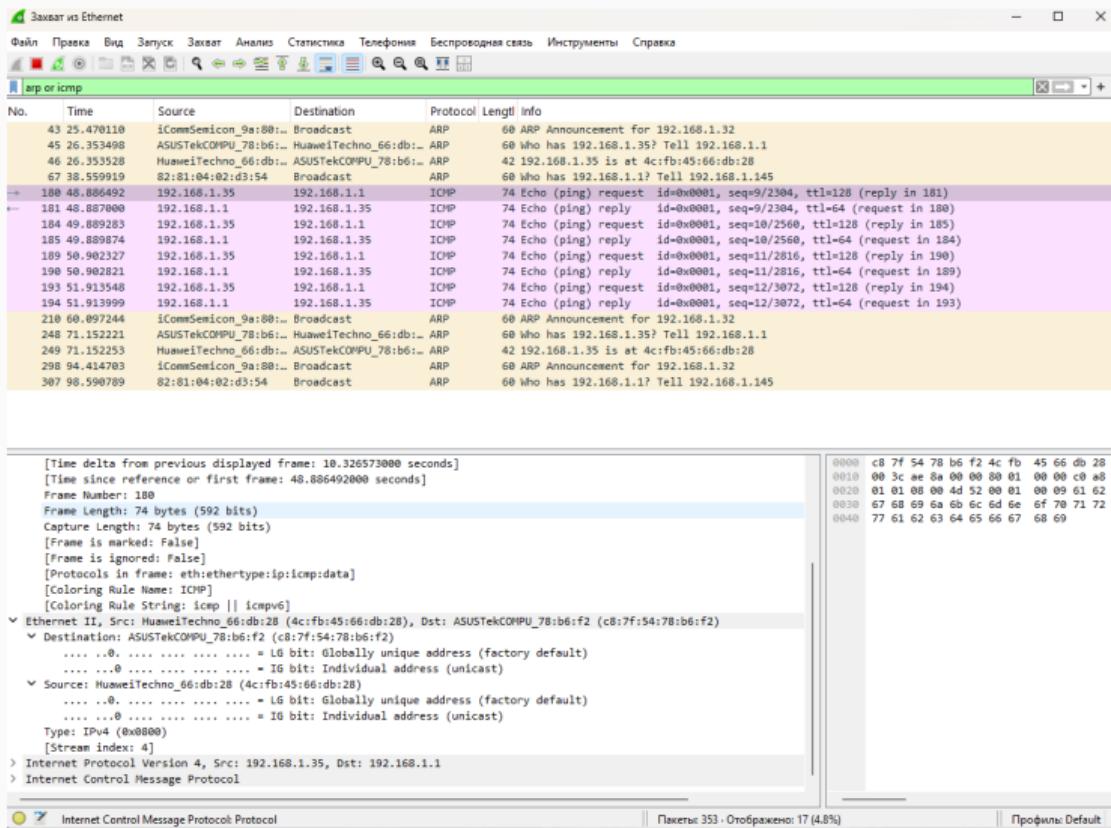


Рис. 2. ICMP-запрос и ответ в Wireshark.

## Анализ кадров канального уровня

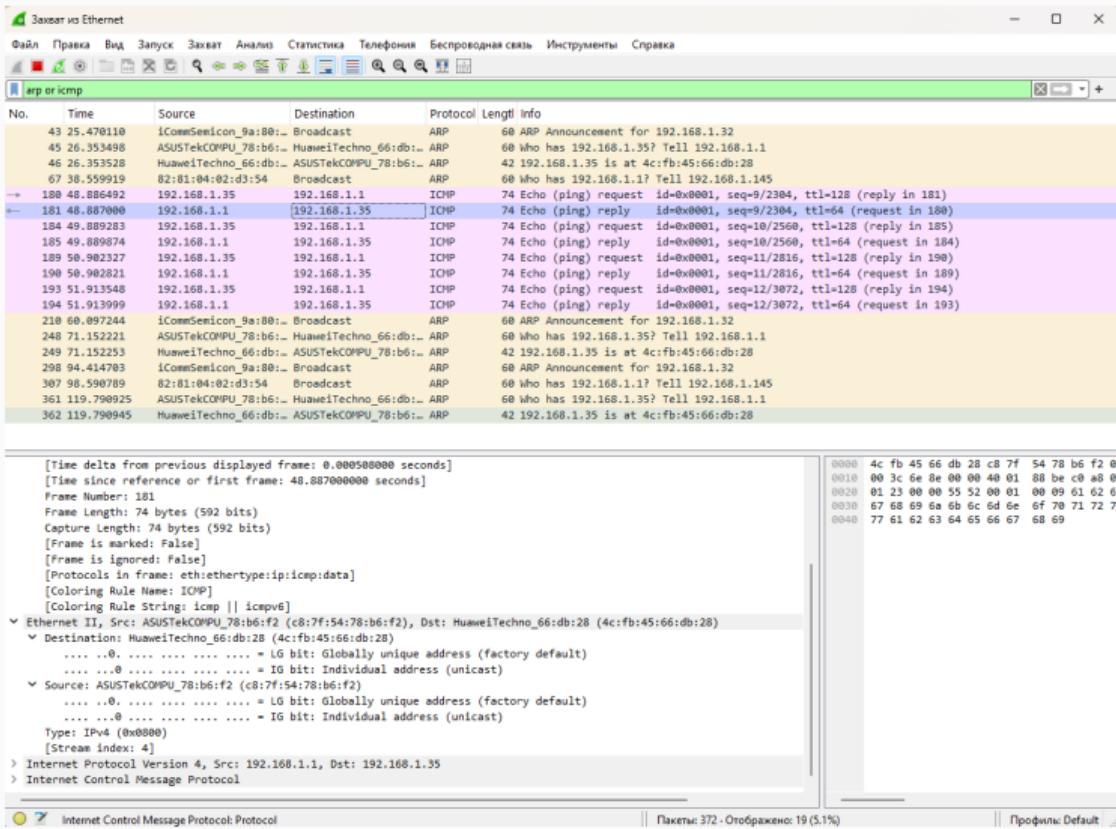


Рис. 4. Детализация ICMP запроса

## Анализ кадров канального уровня

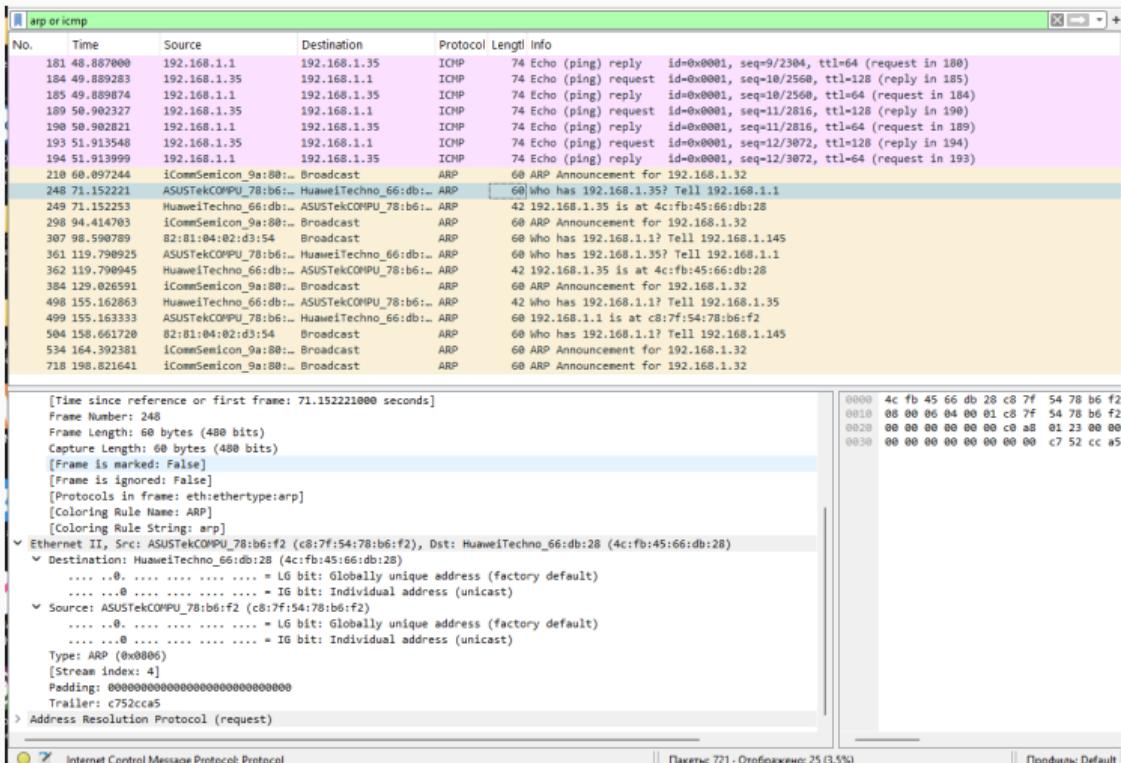


Рис. 5: Детализация ICMP-ответа

## Анализ ARP

```
PS C:\work\hamdimohammad\vagrant>
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

Статистика Ping для 209.85.233.138:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потеря)

Приблизительное время приема-передачи в мс:
    Минимальное = 18мсек, Максимальное = 18 мсек, Среднее = 18 мсек
PS C:\work\hamdimohammad\vagrant> |
```

Рис. 6: Анализ ARP-запроса

# Анализ ARP

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
42	7.023378	192.168.1.35	209.85.233.138	ICMP	74	[Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 43)]
43	7.042102	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=105 (request in 42)
46	8.035650	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 47)
47	8.054125	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=105 (request in 46)
49	9.051899	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 50)
50	9.070516	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=105 (request in 49)
51	10.065063	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 52)
52	10.083785	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=105 (request in 51)
60	13.317423	1ComSemIcon_9a:80.. Broadcast		ARP	60	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTekCOMPU_78:b6.. HuaweiTechno_66:db..		ARP	60	Ihlo has 192.168.1.357 Tell 192.168.1.1
79	24.423844	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: 0.000000000 seconds]  
[Time since reference or first frame: 7.023378000 seconds]  
Frame Number: 42  
Frame Length: 74 bytes (592 bits)  
Capture Length: 74 bytes (592 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ether:type: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)  
.... .0. .... .... .... = L6 bit: Globally unique address (factory default)  
.... .0. .... .... .... = L6 bit: Individual address (unicast)  
Source: HuaweiTechno\_66:db:28 (4c:fb:45:66:db:28)  
.... .0. .... .... .... = L6 bit: Globally unique address (factory default)  
.... .0. .... .... .... = L6 bit: Individual address (unicast)  
Type: IPv4 (0x0800)  
[Stream index: 0]  
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 209.85.233.138  
> Internet Control Message Protocol

Ethernet: <live capture in progress>

Пакеты 176 · Отображено: 11 (6.3%)

Профиль: Default

# Анализ ICMP и ARP при ping внешнего ресурса

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
→ 42	7.023378	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 43)
← 43	7.042102	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=105 (request in 42)
46	8.035650	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 47)
47	8.054125	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=105 (request in 46)
49	9.051899	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 50)
50	9.070316	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=105 (request in 49)
51	10.065063	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 52)
52	10.083705	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=105 (request in 51)
60	13.317423	iCommSemicon_9a:801.. Broadcast		ARP	68	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTekCOMP_78:b6.. HuaweiTechno_66:db..		ARP	68	Who has 192.168.1.35? Tell 192.168.1.32
79	24.423844	HuaweiTechno_66:db.. ASUSTekCOMP_78:b6:..		ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

[Time delta from previous displayed frame: 0.018724000 seconds]  
[Time since reference or first frame: 7.042102000 seconds]  
Frame Number: 43  
Frame Length: 94 bytes (592 bits)  
Capture Length: 74 bytes (592 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: ethertype:ip:icmp:payload]  
[Coloring Rule Name: ICMP]  
[Coloring Rule String: icmp || icmpv6]  
Ethernet II, Src: ASUSTekCOMP\_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)  
.....0. .... .... .... = LG bit: Globally unique address (factory default)  
.....0. .... .... .... = IG bit: Individual address (unicast)  
Source: ASUSTekCOMP\_78:b6:f2 (c8:7f:54:78:b6:f2)  
.....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: 209.85.233.138, Dst: 192.168.1.35  
> Internet Control Message Protocol

0000 4c fb 45 66 db 28 c8 7f 54 78 b6 f2 08  
0010 00 3c 00 00 00 00 69 01 d5 15 d1 55 e1  
0020 01 23 00 00 55 4e 00 01 00 0d 61 62 61  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 71  
0040 77 61 62 63 64 65 66 67 68 69

Пакеты: 190 · Отображено: 11 (5.8%) | Профиль: Default

# Анализ ICMP и ARP при ping внешнего ресурса

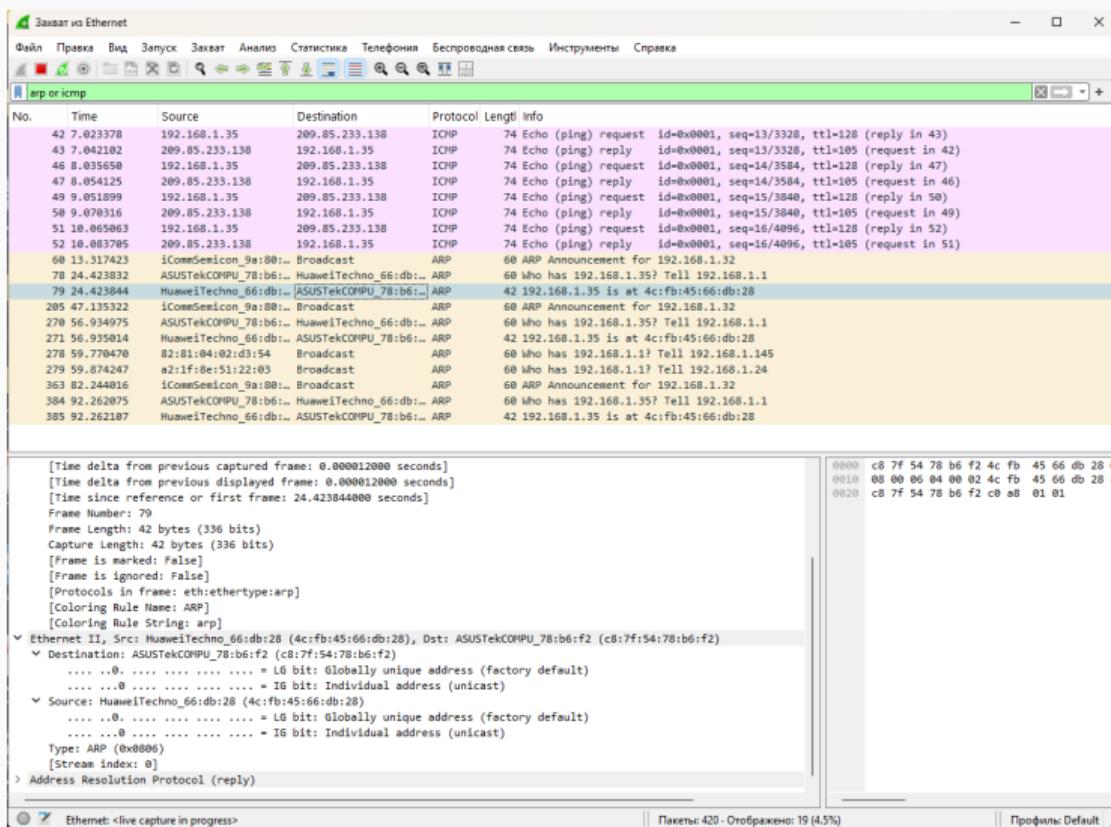


Рис. 6. Анализ ICMP для фильтра по имени ресурса

# Анализ транспортного уровня: HTTP

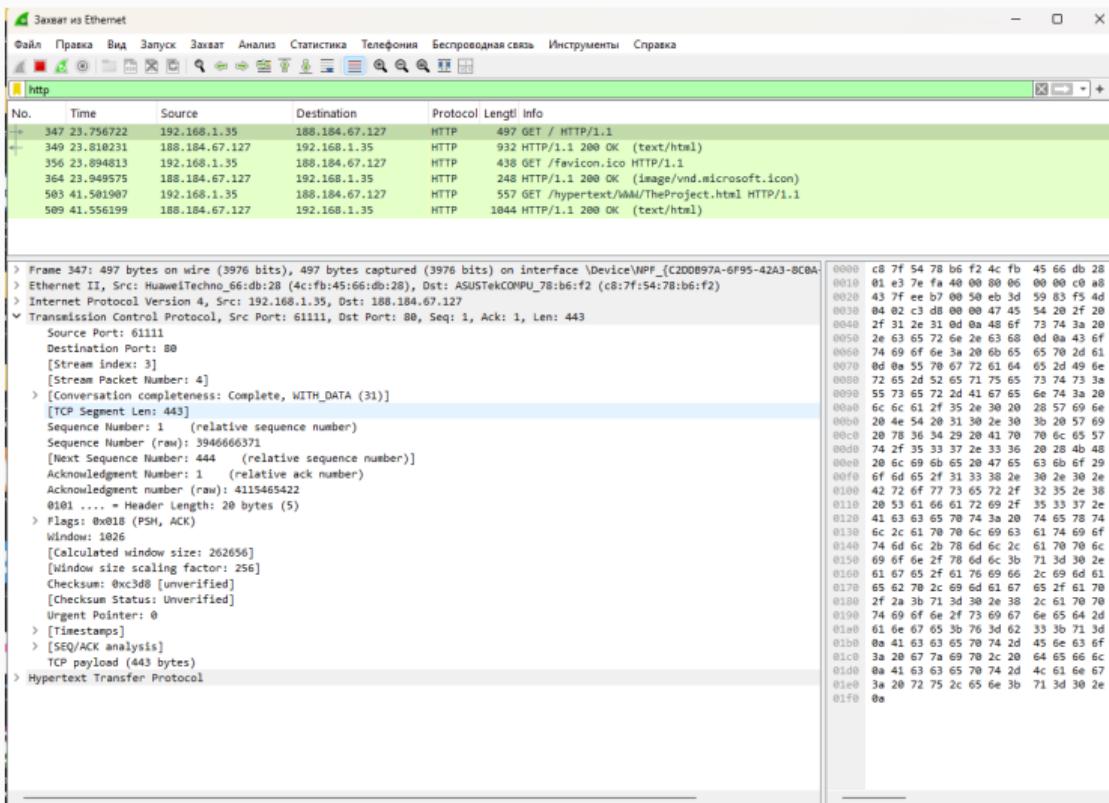


Рис. 10: HTTP-запрос в Wireshark

# Анализ транспортного уровня: HTTP

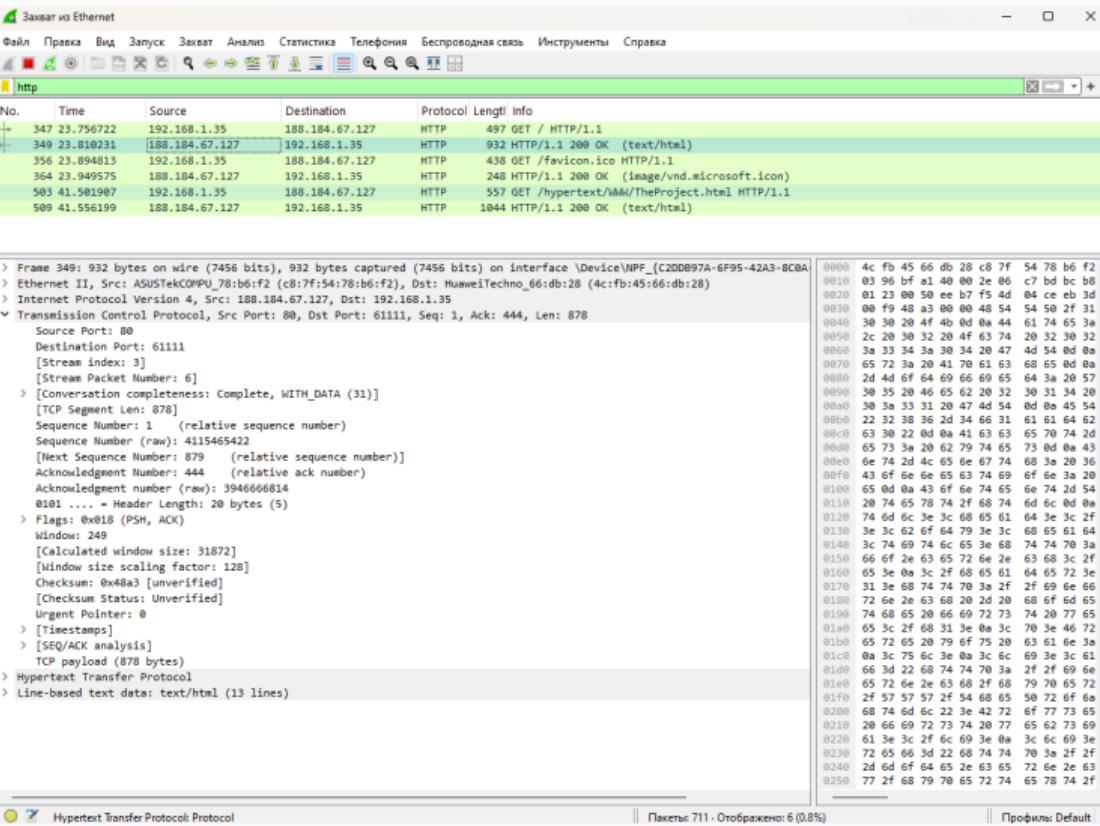


Рис. 11: HTTP-ответ в Wireshark

# Анализ транспортного уровня: DNS

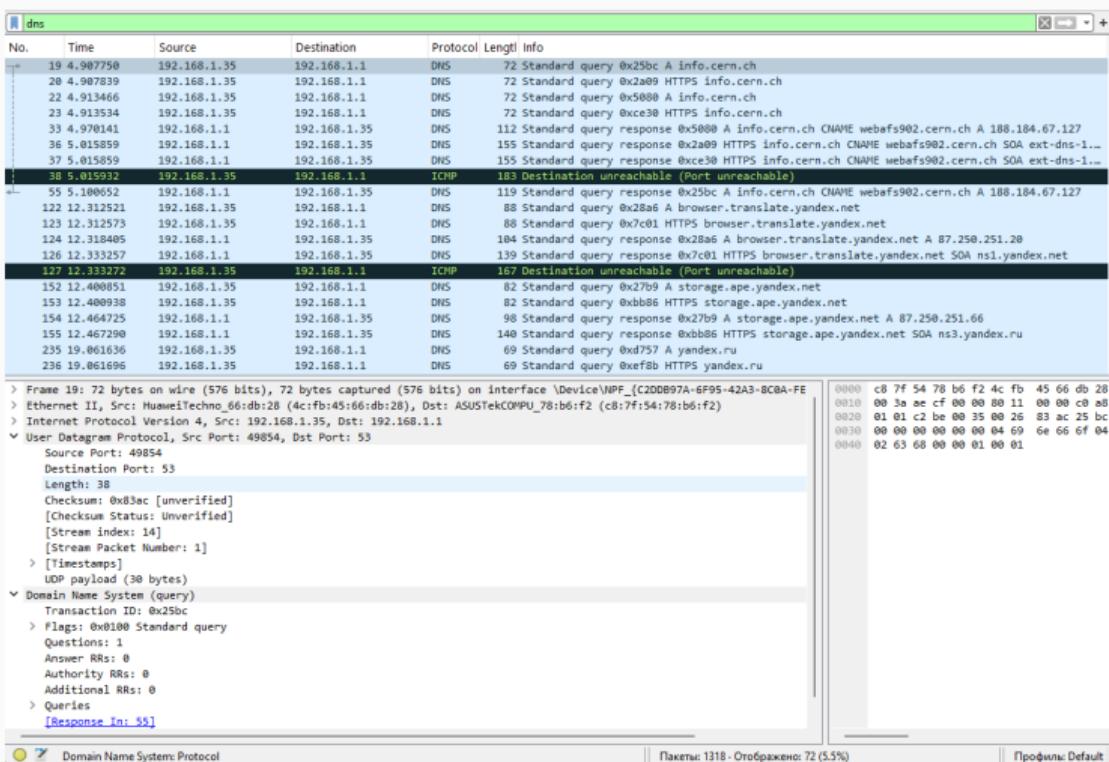


Рис. 12: DNS-запрос

# Анализ транспортного уровня: DNS

Захват из Ethernet

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

dns

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 0x2e09 HTTPS info.cern.ch
22	4.913466	192.168.1.35	192.168.1.1	DNS	72	Standard query 0x5080 A info.cern.ch
23	4.913534	192.168.1.35	192.168.1.1	DNS	72	Standard query 0xce30 HTTPS info.cern.ch
33	4.970141	192.168.1.1	192.168.1.35	DNS	112	Standard query response 0x5080 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 0xce30 HTTPS info.cern.ch CNAME webafs902.cern.ch SOA ext-dns-1...
38	5.015932	192.168.1.35	192.168.1.1	ICMP	183	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	88	Standard query 0x28a6 A browser.translate.yandex.net
123	12.312573	192.168.1.35	192.168.1.1	DNS	88	Standard query 0x7c01 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 0x7c01 HTTPS browser.translate.yandex.net SOA ns1.yandex.net
127	12.333272	192.168.1.35	192.168.1.1	ICMP	167	Destination unreachable (Port unreachable)
152	12.408051	192.168.1.35	192.168.1.1	DNS	82	Standard query 0x27b9 A storage.ape.yandex.net
153	12.408098	192.168.1.35	192.168.1.1	DNS	82	Standard query 0xbb86 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 0xbb86 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 0xebf0 HTTPS yandex.ru

> Frame 55: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on Interface \Device\NPF\_{C2DD897A-6F95-42A3-8C8A-...

> 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: 192.168.1.1, Dst: 192.168.1.35

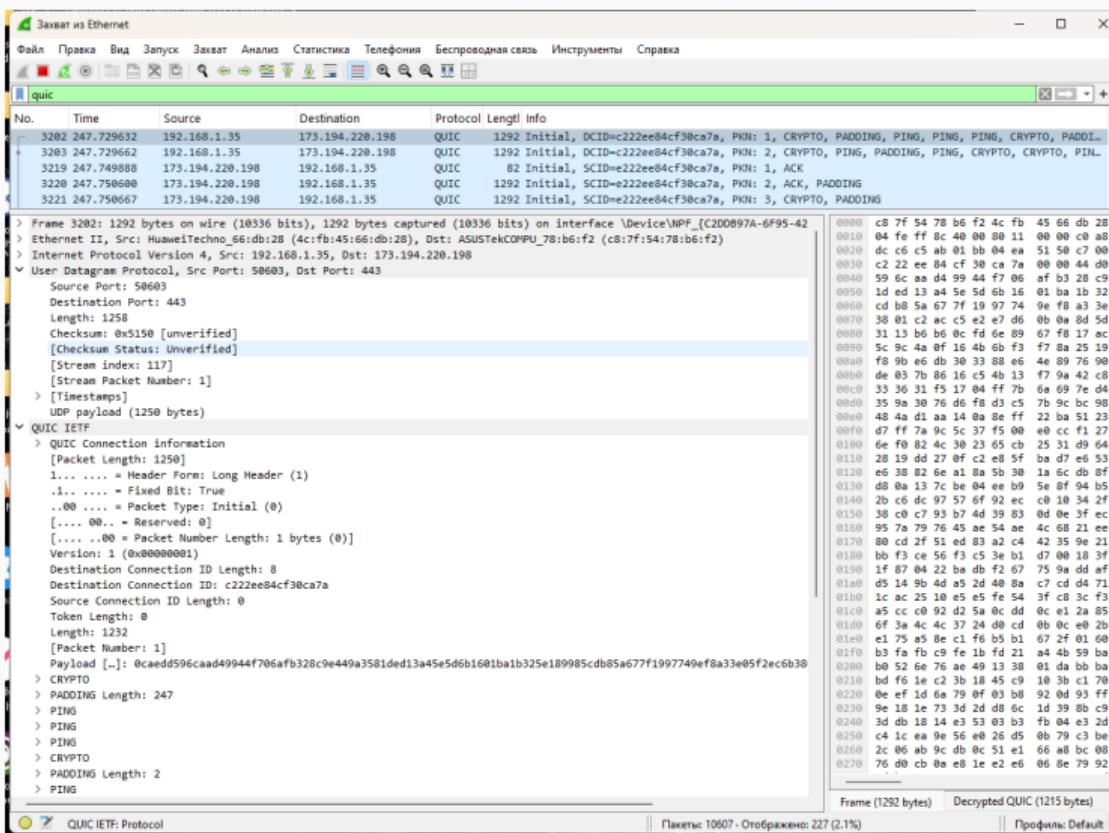
  User Datagram Protocol, Src Port: 53, Dst Port: 49854

    Source Port: 53  
    Destination Port: 49854  
    Length: 85  
    Checksum: 0x920b [unverified]  
    [Checksum Status: Unverified]  
    [Stream Index: 14]  
    [Stream Packet Number: 2]  
    > [Timestamps]  
    > Domain Name System (response)  
      Transaction ID: 0x25bc  
      > Flags: 0x8100 Standard query response, No error  
      Questions: 1  
      Answer RRs: 2  
      Authority RRs: 0  
      Additional RRs: 0  
      > Queries  
      > Answers

0000 4c fb 45 66 db 28 c8 7f 54 7b b6 f2 0  
0010 00 69 f5 f8 40 00 48 11 c1 16 c4 a8 0  
0020 01 23 00 35 c2 be 00 55 92 0b 25 bc 8  
0030 00 02 00 00 00 00 00 04 69 6e 66 6f 04 6  
0040 02 d3 68 00 00 01 00 01 c0 0c 00 05 0  
0050 01 ae 00 13 09 77 65 62 61 66 73 39 3  
0060 65 72 6e 02 63 68 00 c8 2a 00 01 00 0  
0070 84 00 04 bc b8 43 7f

Domain Name System: Protocol Пакеты: 1361 · Отображено: 72 (5.3%) Профиль: Default

## Аналіз транспортного рівня: QUIC



Page 16 - CHIC version

# Анализ транспортного уровня: QUIC

Захват из Ethernet

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

quic

No.	Time	Source	Destination	Protocol	Length	Info
3282	247.729632	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c222ee84cf30ca7a, PKN: 1, CRYPTO, PADDING, PING, PING, PING, CRYPTO, PADDI...
3203	247.729662	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c222ee84cf30ca7a, PKN: 2, CRYPTO, PING, PADDING, PING, CRYPTO, CRYPTO, PIN...
3219	247.749888	173.194.220.198	192.168.1.35	QUIC	82	Initial, SCID=e222ee84cf30ca7a, PKN: 1, ACK
3220	247.750608	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e222ee84cf30ca7a, PKN: 2, ACK, PADDING
3221	247.750667	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e222ee84cf30ca7a, PKN: 3, CRYPTO, PADDING

> Frame 3219: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{C2D0B97A-6F95-42A3-BC0A-FE:  
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: 173.194.220.198, Dst: 192.168.1.35  
> User Datagram Protocol, Src Port: 443, Dst Port: 50603  
    Source Port: 443  
    Destination Port: 50603  
    Length: 48  
    Checksum: 0xeb17 [unverified]  
    [Checksum Status: Unverified]  
    [Stream index: 117]  
    [Stream Packet Number: 3]  
    > [Timestamps]  
    UDP payload (40 bytes)  
        <QUIC IETF>  
        > QUIC Connection Information  
            [Packet Length: 40]  
            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: e222ee84cf30ca7a  
            Token Length: 0  
            Length: 22  
            [Packet Number: 1]  
            Payload: 6dc69378170595f7dd0ea54721fc9f1f2e16d5da44  
        > ACK

Frame (82 bytes) Decrypted QUIC (5 bytes)

Пакеты 10674 - Отображено 227 (2.1%) || Профиль: Default

QUIC IETF Protocol

# Анализ TCP handshake

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	689 GET / HTTP/1.1
20	3.635289	188.184.67.127	192.168.1.35	TCP	68 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	68 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 + 88 [ACK] Seq=556 Ack=198 Win=1025 Len=0
24	3.637253	192.168.1.35	188.184.67.127	TCP	54 61229 + 88 [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	68 443 + 61182 [ACK] Seq=1 Ack=196 Win=166 Len=0
28	3.655770	87.250.251.20	192.168.1.35	TCP	68 443 + 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	3.688828	87.250.251.20	192.168.1.35	TLSv1.2	633 Application Data
31	3.688828	188.184.67.127	192.168.1.35	TCP	68 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	3.738600	87.250.251.20	192.168.1.35	TCP	68 443 + 61182 [ACK] Seq=622 Ack=622 Win=166 Len=0

Рис. 16: Анализ TCP-сессии

# График потока TCP



Рис. 17: График потока TCP

## Выводы по проделанной работе

---

## Вывод

---

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.