

Сетевые технологии

Анализ трафика в Wireshark

Хамди Мохаммад

15 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

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

Выполнение лабораторной работы

```
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

```
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
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: Проверка доступности шлюза

Анализ кадров канального уровня

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	49.889874	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: eth: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)
 0... .. = LG bit: Globally unique address (factory default)
 0... .. = IG bit: Individual address (unicast)
 ▼ Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
 0... .. = LG bit: Globally unique address (factory default)
 0... .. = 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

0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28 08
0010 00 3c ae 8a 00 00 80 01 00 00 c8 a8 01
0020 01 01 08 0d 52 00 01 00 09 61 62 63
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
0040 77 61 62 63 64 65 66 67 68 69

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

Анализ кадров канального уровня

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	68	ARP Announcement for 192.168.1.32
45	26.353496	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	68	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	68	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	49.889874	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	68	ARP Announcement for 192.168.1.32
248	71.152221	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	68	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	68	ARP Announcement for 192.168.1.32
307	98.590789	82:81:04:02:d3:54	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.145
361	119.790925	ASUSTekCOMPU_78:b6:...	HuaweiTechno_66:db:...	ARP	68	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: 0.000500000 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: eth: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)

... ..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: IPv4 (0x0800)
[Stream index: 4]

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35
> Internet Control Message Protocol

0000 4c fb 45 66 db 28 c8 7f 54 78 b6 f2 00
0010 00 3c 6e 8e 00 00 40 01 88 be c0 a8 0
0020 01 23 00 00 55 52 00 01 00 09 61 62 6
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 7
0040 77 61 62 63 64 65 66 67 68 69

Internet Control Message Protocol: Protocol

Пакеты: 372 · Отображено: 19 (5.1%)

Профили: Default

Анализ кадров канального уровня

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 248), which is an ICMP Echo (ping) request. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
181	48.887800	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	49.889874	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:f2::	HuaweiTechno_66:db:28::	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
249	71.152253	HuaweiTechno_66:db:28::	ASUSTekCOMPU_78:b6:f2::	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:f2::	HuaweiTechno_66:db:28::	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
362	119.790945	HuaweiTechno_66:db:28::	ASUSTekCOMPU_78:b6:f2::	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
384	129.026591	iCommSemicon_9a:80::	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
498	155.162863	HuaweiTechno_66:db:28::	ASUSTekCOMPU_78:b6:f2::	ARP	42	Who has 192.168.1.1? Tell 192.168.1.35
499	155.163333	ASUSTekCOMPU_78:b6:f2::	HuaweiTechno_66:db:28::	ARP	60	192.168.1.1 is at c8:7f:54:78:b6:f2
504	158.661720	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145
534	164.392381	iCommSemicon_9a:80::	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
718	198.821641	iCommSemicon_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: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]

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)
 -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: ARP (0x0806)
- [Stream index: 4]
- Padding: 00000000000000000000000000000000
- Trailer: c752cca5

Address Resolution Protocol (request)

Internet Control Message Protocol: Protocol | Пакеты: 721 - Отображено: 25 (3.5%) | Профиль: Default

0000 4c fb 45 66 db 28 c8 7f 54 78 b6 f2
0010 08 00 06 04 00 01 c8 7f 54 78 b6 f2
0020 00 00 00 00 00 c0 a8 01 23 00 00
0030 00 00 00 00 00 00 00 c7 52 cc a5

Рис. 5: Детализация ICMP-ответа

```
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
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> |
```

Рис. 6: Анализ ARP-запроса

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=120 (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=120 (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=120 (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=120 (reply in 52)
52	10.083795	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	iComSemicon_9a:80:.. Broadcast		ARP	60	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTekCOMPU_78:b6:.. HuaweiTechno_66:db:..		ARP	60	Who has 192.168.1.35? 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: 0.00000000 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: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)
 ...0... = LG bit: Globally unique address (factory default)
 ...0... = IG bit: Individual address (unicast)
 Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
 ...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: 192.168.1.35, Dst: 209.85.233.138
 > Internet Control Message Protocol

0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28 f
 0010 00 3c 1a 1e 00 00 00 01 00 00 c0 a8 f
 0020 e9 8a 08 00 4d 4e 00 01 00 0d 61 62 f
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 f
 0040 77 61 62 63 64 65 66 67 68 69

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:00:1...	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTekCOMPU_78:b6:1...	HuaweiTechno_66:db:1...	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
79	24.423844	HuaweiTechno_66:db:1...	ASUSTekCOMPU_78:b6:1...	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: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth: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)
 - 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: 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 00
0010 00 3c 00 00 00 00 69 01 d5 15 d1 55 ef
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 73
0040 77 61 62 63 64 65 66 67 68 69

Ethernet <live capture in progress> | Пакеты: 190 · Отображено: 11 (5.8%) | Профиль: Default

Анализ ICMP и ARP при ping внешнего ресурса

The screenshot displays the Wireshark interface with a packet capture named 'Захват из Ethernet'. The filter bar shows 'arp or icmp'. The packet list on the left shows a series of ICMP Echo (ping) requests and replies, followed by ARP announcements and requests. The selected packet (packet 79) is an ARP request from HuaweiTechno_66:db:13 to ASUSTekCOMPU_78:b6:f2. The packet details pane on the right shows the Ethernet II header, the destination and source MAC addresses, and the ARP request structure. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

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	10.083795	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:80:13	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTekCOMPU_78:b6:f2	HuaweiTechno_66:db:13	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
79	24.423844	HuaweiTechno_66:db:13	ASUSTekCOMPU_78:b6:f2	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
205	47.135322	iCommSemicon_9a:80:13	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
270	56.934975	ASUSTekCOMPU_78:b6:f2	HuaweiTechno_66:db:13	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
271	56.935014	HuaweiTechno_66:db:13	ASUSTekCOMPU_78:b6:f2	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
278	59.770470	82:81:04:02:d3:54	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.145
279	59.874247	a2:1f:8e:51:22:03	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.24
363	82.244016	iCommSemicon_9a:80:13	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
384	92.262075	ASUSTekCOMPU_78:b6:f2	HuaweiTechno_66:db:13	ARP	60	Who has 192.168.1.35? Tell 192.168.1.1
385	92.262107	HuaweiTechno_66:db:13	ASUSTekCOMPU_78:b6:f2	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

[Time delta from previous captured frame: 0.000012000 seconds]
[Time delta from previous displayed frame: 0.000012000 seconds]
[Time since reference or first frame: 24.423844000 seconds]
Frame Number: 79
Frame Length: 42 bytes (336 bits)
Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: HuaweiTechno_66:db:13 (4c:fb:45:66:db:13), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Source: HuaweiTechno_66:db:13 (4c:fb:45:66:db:13)
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 0]
Address Resolution Protocol (reply)

Ethernet -> live capture in progress | Пакеты: 420 - Отображено: 19 (4.5%) | Профили: Default

Анализ транспортного уровня: HTTP

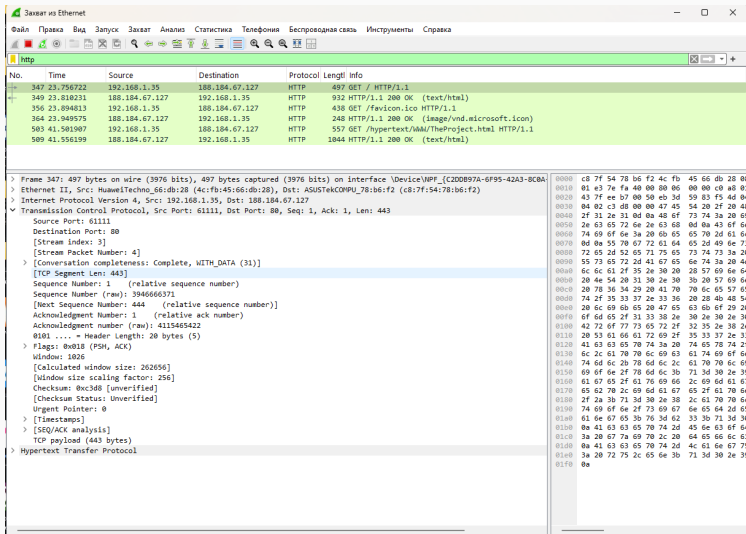


Рис. 10: HTTP-запрос в Wireshark

Анализ транспортного уровня: HTTP

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, with packet 349 selected. The middle pane shows the details of this packet, which is an HTTP GET request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

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)

Packet 349 Details:

- Frame 349: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF_{C20DB97A-6F95-42A3-8CBA-...}
- 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): 394666814
 - 0101 - Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window: 249
 - [Calculated window size: 31872]
 - [Window size scaling factor: 128]
 - Checksum: 0x48a3 [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)

Raw Data (Hex):

```
0000 4c fb 45 66 db 28 c 7f 54 78 b6 f2
0010 03 96 bf e1 40 00 2e 86 c7 bd bc b8
0020 01 23 00 50 ee b7 f5 4d 04 ce eb 3d
0030 00 f9 48 a3 00 00 48 54 54 50 2f 31
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a
0050 2c 20 30 32 20 4f 63 74 20 32 30 32
0060 3a 33 34 3a 30 34 20 47 4d 54 0d 0a
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a
0080 2d 4d 6f 64 69 66 69 65 64 3a 20 57
0090 30 35 20 46 65 62 20 32 30 31 34 20
00a0 30 3a 33 11 20 47 4d 54 0d 0a 45 54
00b0 22 32 38 36 2d 34 66 31 61 61 64 62
00c0 63 30 22 0d 0a 41 63 63 65 70 74 2d
00d0 65 73 3a 20 62 79 74 65 73 0d 0a 43
00e0 6e 74 2d 4c 65 6e 67 74 68 3a 20 36
00f0 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
0100 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54
0110 20 74 65 78 74 2f 68 74 6d 6c 0d 0a
0120 74 6d 6c 3e 3c 68 65 61 64 3e 3c 2f
0130 3e 3c 62 6f 64 79 3e 3c 68 65 61 64
0140 3c 74 69 74 6c 65 3e 68 74 74 70 3a
0150 66 6f 2e 63 65 72 6e 2e 63 68 3c 2f
0160 65 3e 0a 3c 2f 68 65 61 64 65 72 3e
0170 31 3e 68 74 74 70 3a 2f 2f 69 6e 6e
0180 72 6e 2e 63 68 20 2d 30 68 6f 6d 65
0190 74 68 65 20 66 69 72 73 74 20 77 65
01a0 65 3c 2f 68 31 3e 0a 3c 70 3e 46 72
01b0 65 72 65 20 79 6f 75 20 63 61 6e 3a
01c0 0a 3c 75 6c 3e 0a 3c 6c 69 3e 3c 61
01d0 66 3d 22 68 74 74 70 3a 2f 2f 69 6e
01e0 65 72 6e 2e 63 68 2f 68 79 70 65 72
01f0 2f 57 57 2f 54 68 65 50 72 6f 6e
0200 68 74 6d 6c 22 3e 42 72 6f 77 73 65
0210 20 66 69 72 73 74 20 77 65 62 73 69
0220 61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 3e
0230 72 65 66 3d 22 68 74 70 3a 2f 2f
0240 2d 6d 6f 64 65 2e 63 65 72 6e 2e 63
0250 77 2f 68 79 70 65 72 74 65 78 74 2f
```

Status Bar: Пакеты: 711 · Отображено: 6 (0.8%) | Профили: Default

Рис. 11: HTTP-отклик в Wireshark

Анализ транспортного уровня: DNS

The screenshot displays a network capture in Wireshark, specifically focusing on a DNS transaction. The packet list on the left shows a standard query from 192.168.1.35 to 192.168.1.1. The packet details on the right show the query for 'info.cern.ch'. The packet bytes on the right show the raw data.

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 0xce30 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 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	12.400851	192.168.1.35	192.168.1.1	DNS	82	Standard query 0x27b9 A storage.ape.yandex.net
153	12.400938	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	148	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 0xef8b HTTPS yandex.ru

Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{C2D0B97A-6F95-42A3-8CBA-FE} (0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28 0)

Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2) (0010 00 3a ae cf 00 00 00 11 00 00 c8 a8 0)

Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1 (0020 01 01 c2 be 00 35 00 26 83 ac 25 bc 0)

User Datagram Protocol, Src Port: 49854, Dst Port: 53 (0030 00 00 00 00 00 04 69 6e 66 6f 04 6)

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]
0040 02 63 68 00 00 01 00 01

Domain Name System: Protocol | Пакеты: 1318 · Отображено: 72 (5,5%) | Профили: Default

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 0x2a09 HTTPS info.cern.ch
22	4.913466	192.168.1.35	192.168.1.1	DNS	72	Standard query 0x5800 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 0x5800 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	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	12.318495	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	12.332557	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	162	Destination unreachable (Port unreachable)
152	12.400851	192.168.1.35	192.168.1.1	DNS	82	Standard query 0x27b9 A storage.apc.yandex.net
153	12.400938	192.168.1.35	192.168.1.1	DNS	82	Standard query 0xbb86 HTTPS storage.apc.yandex.net
154	12.464725	192.168.1.1	192.168.1.35	DNS	98	Standard query response 0x27b9 A storage.apc.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.apc.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 0xf8b0 HTTPS yandex.ru

> Frame 55: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface \Device\NPF_{C2D0B97A-6F95-42A3-8C0A-...}

> Ethernet II, Src: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno_66:d6:28 (4c:fb:45:66:d6:28)

> 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]
UDP payload (77 bytes)

▼ Domain Name System (response)

Transaction ID: 0x25bc

> Flags: 0x0100 Standard query response, No error

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0

> Queries

> Answers

0000 4c fb 45 66 d6 28 c8 7f 54 78 b6 f2 0
0010 00 69 f5 f8 40 00 00 11 c1 16 c0 a0 0
0020 01 23 00 35 c2 be 00 55 92 0b 25 bc 8
0030 00 02 00 00 00 00 04 69 6e 66 6f 04 6
0040 02 63 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 c0 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

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
3202	247.729632	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c22ee84cf30ca7a, PKN: 1, CRYPTO, PADDING, PING, PING, PING, CRYPTO, PADDI...
3203	247.729662	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c22ee84cf30ca7a, PKN: 2, CRYPTO, PING, PADDING, PING, CRYPTO, CRYPTO, PING...
3219	247.749888	173.194.220.198	192.168.1.35	QUIC	82	Initial, SCID=e22ee84cf30ca7a, PKN: 1, ACK
3220	247.750600	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e22ee84cf30ca7a, PKN: 2, ACK, PADDING
3221	247.750607	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e22ee84cf30ca7a, PKN: 3, CRYPTO, PADDING

> Frame 3202: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{C2D0B97A-6F95-42...}

> Ethernet II, Src: HuaweiTechno_66:db:28 (4c:f6:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)

> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 173.194.220.198

> User Datagram Protocol, Src Port: 50603, Dst Port: 443

Source Port: 50603

Destination Port: 443

Length: 1258

Checksum: 0x3150 [unverified]

[Checksum Status: Unverified]

[Stream index: 117]

[Stream Packet Number: 1]

> [Timestamps]

UDP payload (1250 bytes)

> QUIC IETF

> QUIC Connection information

[Packet Length: 1250]

1... .. = Header Form: Long Header (1)

1... .. = Fixed Bit: True

1... .. = Packet Type: Initial (0)

..00 .. = Reserved: 0

[... ..00 = Packet Number Length: 1 bytes (0)]

Version: 1 (0x00000001)

Destination Connection ID Length: 8

Destination Connection ID: c22ee84cf30ca7a

Source Connection ID Length: 0

Token Length: 0

Length: 1232

[Packet Number: 1]

Payload [-]: 0caedd596caad49944f706afb328c9e449a3581ded13a45e5d6b1601ba1b325e1899085cd8b5a677f1997749ef8a33e05f2ec6b30

> CRYPTO

> PADDING Length: 247

> PING

> PING

> PING

> CRYPTO

> PADDING Length: 2

> PING

0000 c8 7f 54 78 b6 f2 4c fb 45 66 db 28

0010 04 fe ff 8c 40 00 80 11 00 00 c0 a8

0020 dc c5 c5 ab 01 bb 04 ea 51 50 c7 00

0030 c2 22 ee 84 cf 30 ca 7a 00 00 44 d0

0040 59 6c aa d4 99 44 f7 06 af b3 28 c9

0050 1d ed 13 a4 5e 5d 6b 16 01 ba 1b 32

0060 cd b0 5a 67 7f 19 97 74 9e f8 a3 3e

0070 38 01 c2 ac c5 e2 e7 d6 0b 0a 8d 5d

0080 31 13 b6 b6 0c fd 6e 89 67 f8 17 ac

0090 5c 9c 4a 8f 16 4b 6b f3 f7 8a 25 15

00a0 f8 9b e6 db 30 33 88 e6 4e 89 76 90

00b0 de 03 7b 86 16 c5 4b 13 f7 9a 42 c8

00c0 33 36 31 f5 17 04 ff 7b 6a 69 7e d4

00d0 35 9a 30 76 d6 f8 d3 c5 7b 9c bc 98

00e0 48 4a d1 aa 14 0a 8e ff 22 ba 51 23

00f0 d7 ff 7a 9c 5c 37 f5 00 0e cc f1 27

0100 6e f0 82 4c 30 23 65 cb 25 31 d9 64

0110 28 19 dd 27 0f c2 e8 5f ba d7 e8 53

0120 e6 38 82 6e a1 9a 5b 30 1a 6c db 8f

0130 d8 0a 13 7c be 0a ee b9 5e 8f 94 b5

0140 2b c6 dc 97 57 6f 92 ec c0 10 34 2f

0150 38 c0 c7 93 b7 4d 39 83 00 0e 3f ec

0160 95 7a 79 76 45 ae 54 ae 4c 68 21 ee

0170 80 cd 2f 51 ed 83 a2 c4 42 35 9e 21

0180 bb f3 ce 56 f3 c5 3a b1 d7 00 18 3f

0190 1f 87 04 22 ba db f2 67 75 9a dd af

01a0 d5 14 9b ad a5 2d 40 8a c7 cd d4 71

01b0 1c ac 25 10 e5 e5 fe 54 3f c8 3c f3

01c0 a5 cc c0 92 d2 5a 0c dd 0c e1 2a 85

01d0 6f 3a 4c 4c 37 24 d0 cd 0b 0c e0 2b

01e0 e1 75 a5 8e c1 f6 b5 b1 67 2f 01 60

01f0 b3 fa fb c9 fe 1b fd 21 a4 40 59 ba

0200 b0 52 6e 76 ae 49 13 38 01 da bb ba

0210 bd f6 1e c2 3b 18 45 c9 10 3b c1 70

0220 0e ef 1d 6a 79 0f 03 b8 92 0d 93 ff

0230 9e 18 1e 73 3d 2d d8 6c 1d 39 8b c9

0240 3d db 18 a4 e3 53 03 b3 fb 04 e3 2d

0250 c4 1c ea 9e 56 e0 26 d5 0b 79 c3 be

0260 2c 06 ab 9c db 0c 51 e1 66 a8 bc 00

0270 76 d0 cb 0a e8 1e e2 e6 0e 8e 79 92

Frame (1292 bytes) Decrypted QUIC (1215 bytes)

QUIC IETF: Protocol

Пакеты: 10607 - Отображено: 227 (2.1%)

Профиль: Default

Анализ транспортного уровня: QUIC

Wireshark packet capture analysis of a QUIC connection. The interface shows a list of packets, with packet 3219 selected. The packet details pane shows the QUIC connection information, including source and destination connection IDs. The packet bytes pane shows the raw frame and the decrypted QUIC data.

No.	Time	Source	Destination	Protocol	Length	Info
3202	247.729632	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c222ee84cf38ca7a, PKN: 1, CRYPTO, PADDING, PING, PING, PING, CRYPTO, PADDI...
3203	247.729662	192.168.1.35	173.194.220.198	QUIC	1292	Initial, DCID=c222ee84cf38ca7a, PKN: 2, CRYPTO, PING, PADDING, PING, CRYPTO, PING...
3219	247.749808	173.194.220.198	192.168.1.35	QUIC	82	Initial, SCID=e222ee84cf38ca7a, PKN: 1, ACK
3220	247.750600	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e222ee84cf38ca7a, PKN: 2, ACK, PADDING
3221	247.750667	173.194.220.198	192.168.1.35	QUIC	1292	Initial, SCID=e222ee84cf38ca7a, PKN: 3, CRYPTO, PADDING

Frame 3219: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{C2D0B97A-6F95-42A3-8C8A-FE1...}

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: e222ee84cf38ca7a
Token Length: 0
Length: 22
[Packet Number: 1]
Payload: 6dc69378170595f7d08ea54721fc9f1f2e16d5da44

ACK

Frame (82 bytes) Decrypted QUIC (5 bytes)

QUIC IETF: Protocol Пакеты: 10674 - Отображено: 227 (2.1%) Профили: Default

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	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	3.738000	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=633 Ack=543 Win=166 Len=0

Рис. 16: Анализ TCP-сессии

График потока TCP

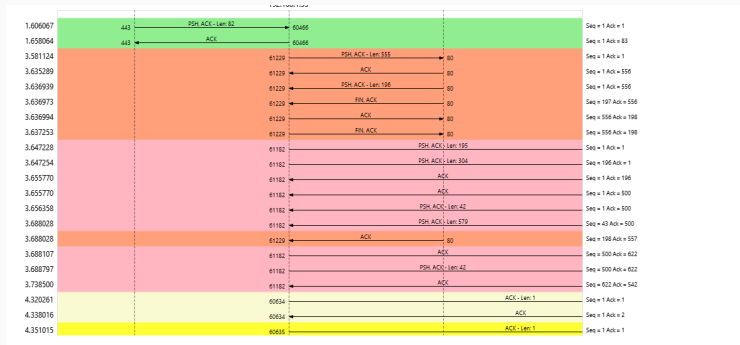


Рис. 17: График потока TCP

Выводы по проделанной работе

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

Было зафиксировано трёхстороннее рукопожатие (SYN → SYN+ACK → ACK), подтверждающее успешное начало TCP-сессии.

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