

Презентация по лабораторной работе №3

Анализ трафика в Wireshark

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

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

MAC-адресация

Выполнение лабораторной работы

```
C:\Users\ASUS\ngalacan>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet VirtualBox Host-Only Network:

    DNS-суффикс подключения . . . . . : 
    Локальный IPv6-адрес канала . . . . : fe80::1bd5:48ba:7abb:de7%14
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Адаптер беспроводной локальной сети Подключение по локальной сети* 10:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : 
    IPv6-адрес. . . . . : 2a00:1370:817c:636d:9a5f:987c:2bce:6cc8
    Временный IPv6-адрес. . . . . : 2a00:1370:817c:636d:b809:b59e:7667:c0ed
    Локальный IPv6-адрес канала . . . . : fe80::a9d7:906e:e66c:c49c%8
    IPv4-адрес. . . . . : 192.168.1.9
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : fe80::1%8
                           192.168.1.1

C:\Users\ASUS\ngalacan>
```

Рис. 1: Команда ipconfig

Адаптер беспроводной локальной сети Беспроводная сеть:

```
DNS-суффикс подключения . . . . . :  
Описание. . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card  
Физический адрес. . . . . : 90-E8-68-2A-62-33  
DHCP включен. . . . . : Да  
Автонастройка включена. . . . . : Да  
IPv6-адрес. . . . . : 2a00:1370:817c:636d:9a5f:987c:2bce:6cc8(Основной)  
Временный IPv6-адрес. . . . . : 2a00:1370:817c:636d:b809:b59e:7667:c0ed(Основной)  
Локальный IPv6-адрес канала . . . : fe80::a9d7:906e:e66c:c49c%8(Основной)  
IPv4-адрес. . . . . : 192.168.1.9(Основной)  
Маска подсети . . . . . : 255.255.255.0  
Аренда получена. . . . . : 9 октября 2024 г. 13:34:59  
Срок аренды истекает. . . . . : 10 октября 2024 г. 14:44:02  
Основной шлюз. . . . . : fe80::1%8  
                        192.168.1.1  
DHCP-сервер. . . . . : 192.168.1.1  
IAID DHCPv6 . . . . . : 428927080  
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2A-E8-2F-91-90-E8-68-2A-62-33  
DNS-серверы. . . . . : 192.168.1.1  
NetBios через TCP/IP. . . . . : Включен
```

C:\Users\ASUS\ngalacan>

Рис. 2: Команда `ipconfig /all`

Анализ кадров канального уровня в Wireshark

Выполнение лабораторной работы

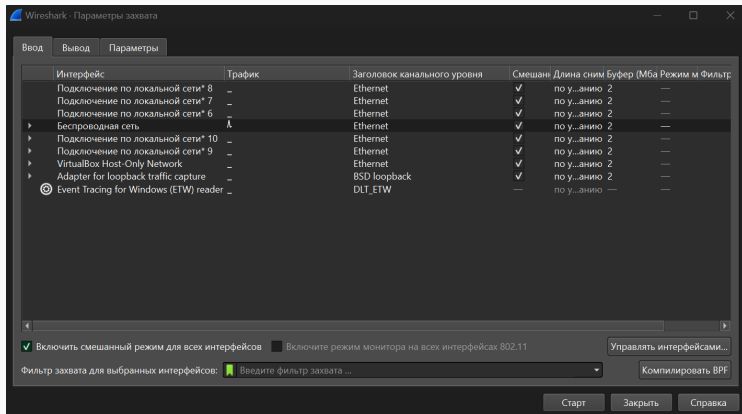


Рис. 3: Запуск захвата трафика


```
C:\Users\ASUS\ngalacan>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=2мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=2мс 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 = 2мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\Users\ASUS\ngalacan>
```

Рис. 4: Пинг шлюза по умолчанию

Выполнение лабораторной работы

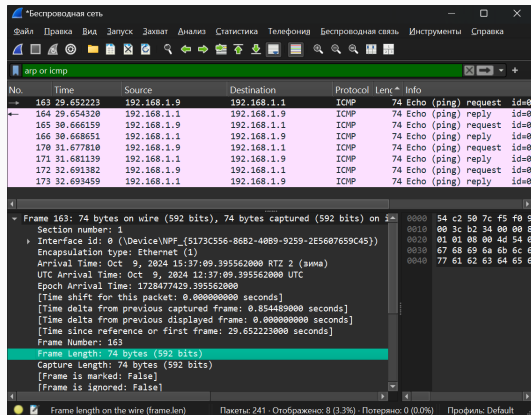


Рис. 5: Кадр ICMP - эхо-запрос: информация о длине кадра

Выполнение лабораторной работы

The screenshot shows the Wireshark interface with the title bar "*Беспроводная сеть". The menu bar includes: Файл, Правка, Вид, Запуск, Захват, Анализ, Статистика, Телефония, Беспроводная связь, Инструменты, Справка. The toolbar contains various icons for file operations, capture, analysis, and display. The filter bar shows "arp or icmp".

No.	Time	Source	Destination	Protocol	Length	Info
163	29.652223	192.168.1.9	192.168.1.1	ICMP	74	Echo (ping) request id=0
164	29.654320	192.168.1.1	192.168.1.9	ICMP	74	Echo (ping) reply id=0
165	30.666159	192.168.1.9	192.168.1.1	ICMP	74	Echo (ping) request id=0
166	30.668651	192.168.1.1	192.168.1.9	ICMP	74	Echo (ping) reply id=0
170	31.677810	192.168.1.9	192.168.1.1	ICMP	74	Echo (ping) request id=0
171	31.681139	192.168.1.1	192.168.1.9	ICMP	74	Echo (ping) reply id=0
172	32.691382	192.168.1.9	192.168.1.1	ICMP	74	Echo (ping) request id=0
173	32.693459	192.168.1.1	192.168.1.9	ICMP	74	Echo (ping) reply id=0

The packet details pane shows the following information for the selected packet (No. 163):

- [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: AzureWaveTec_2a:62:33 (90:e8:68:2a:62:33), Dst: Iskrat...
 - ▼ Destination: Iskrateldoo_7c:f5:f0 (54:c2:50:7c:f5:f0)
 - = LG bit: Globally unique address (fa
 - = IG bit: Individual address (unicast
 - ▼ Source: AzureWaveTec_2a:62:33 (90:e8:68:2a:62:33)
 - = LG bit: Globally unique address (fa
 - = IG bit: Individual address (unicast
 - Type: IPv4 (0x0800)
 - [Stream index: 0]
- Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.1
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 54 c2 50 7c f5 f0 9
0010 00 3c b2 34 00 00 8
0020 01 01 08 00 4d 54 0
0030 67 68 69 6a 6b 6c 6
0040 77 61 62 63 64 65 6
```

The status bar at the bottom indicates: Ethernet (eth), 14 байтов | Пакеты: 241 - Отображено: 8 (3.3%) - Потеряно: 0 (0.0%) | Профиль: Default

Рис. 6: Кадр ICMP - эхо-запрос: информация о типе Ethernet и MAC-адресах

Выполнение лабораторной работы

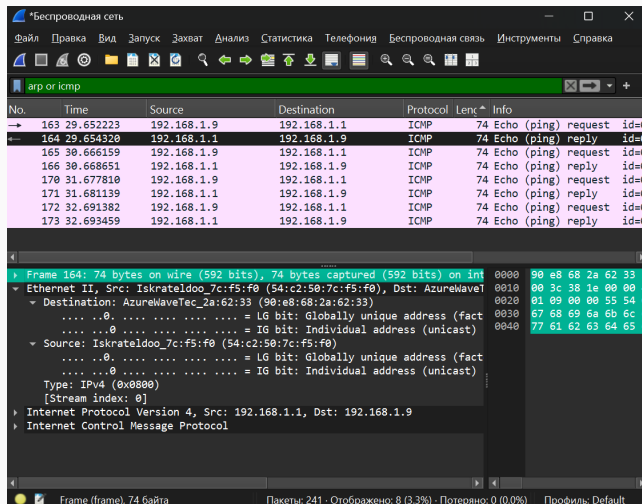


Рис. 7: Кадр ICMP - эхо-ответ: информация о длине кадра, типе Ethernet, MAC-адресах

Выполнение лабораторной работы

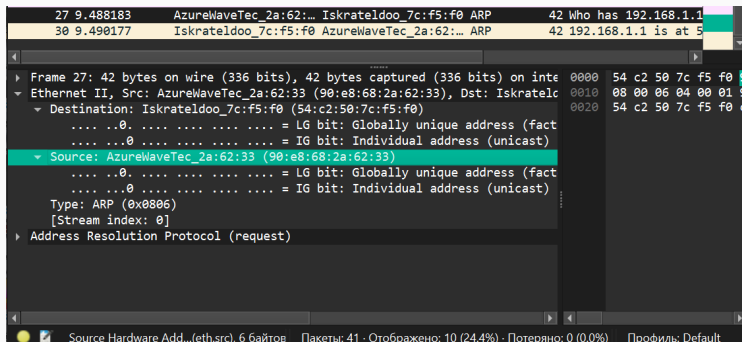


Рис. 8: Кадр ARP

Выполнение лабораторной работы

No.	Time	Source	Destination	Protocol	Length	Info
185	31.361579	192.168.1.9	185.178.208.57	ICMP	74	Echo (ping) request
252	36.011112	192.168.1.9	185.178.208.57	ICMP	74	Echo (ping) request
→ 468	60.857465	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
← 469	60.876378	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
472	61.867508	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
473	61.886630	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
474	62.889690	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
475	62.909891	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
480	63.910319	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
481	63.929275	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply

▶ Frame 468: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on int	0000	54 c2 50 7c f5 f0 9
▼ Ethernet II, Src: AzureWaveTec_2a:62:33 (90:e8:68:2a:62:33), Dst: Iskratelc	0010	00 3c 00 76 00 00 8
▼ Destination: Iskrateldoo_7c:f5:f0 (54:c2:50:7c:f5:f0)	0020	81 85 08 00 4d 43 0
.... ..0. = LG bit: Globally unique address (fact	0030	67 68 69 6a 6b 6c 6
.... ..0. = IG bit: Individual address (unicast)	0040	77 61 62 63 64 65 6
▼ Source: AzureWaveTec_2a:62:33 (90:e8:68:2a:62:33)		
.... ..0. = LG bit: Globally unique address (fact		
.... ..0. = IG bit: Individual address (unicast)		
Type: IPv4 (0x0800)		
[Stream index: 1]		
▶ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 87.240.129.133		
▶ Internet Control Message Protocol		

Destination Hardware... (eth.dst) 6 байто: Пакеты: 566 - Отображено: 14 (2.5%) - Потеряно: 0 (0.0%) Профиль: Default

Рис. 9: Пинг vk.com: запрос

Выполнение лабораторной работы

arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
185	31.361579	192.168.1.9	185.178.208.57	ICMP	74	Echo (ping) request
252	36.011112	192.168.1.9	185.178.208.57	ICMP	74	Echo (ping) request
→ 468	60.857465	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
← 469	60.876378	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
472	61.867508	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
473	61.886630	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
474	62.889690	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
475	62.909891	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply
480	63.910319	192.168.1.9	87.240.129.133	ICMP	74	Echo (ping) request
481	63.929275	87.240.129.133	192.168.1.9	ICMP	74	Echo (ping) reply

Frame 469: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Iskrateldoo_7c:f5:f0 (54:c2:50:7c:f5:f0), Dst: AzureWaveT_90:e8:68:2a:62:33 (90:e8:68:2a:62:33)

Destination: AzureWaveTec_2a:62:33 (90:e8:68:2a:62:33)

.... ..0. = LG bit: Globally unique address (fact)

.... ..0. = IG bit: Individual address (unicast)

Source: Iskrateldoo_7c:f5:f0 (54:c2:50:7c:f5:f0)

.... ..0. = LG bit: Globally unique address (fact)

.... ..0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 1]

Internet Protocol Version 4, Src: 87.240.129.133, Dst: 192.168.1.9

Internet Control Message Protocol

0000 90 e8 68 2a 62 33 5

0010 00 3c da 39 00 00 3

0020 01 09 00 00 55 43 0

0030 67 68 69 6a 6b 6c 6

0040 77 61 62 63 64 65 6

Ethernet (eth), 14 байтов Пакеты: 566 · Отображено: 14 (2.5%) · Потеряно: 0 (0.0%) Профиль: Default

Рис. 10: Пинг vk.com: ответ

Выполнение лабораторной работы

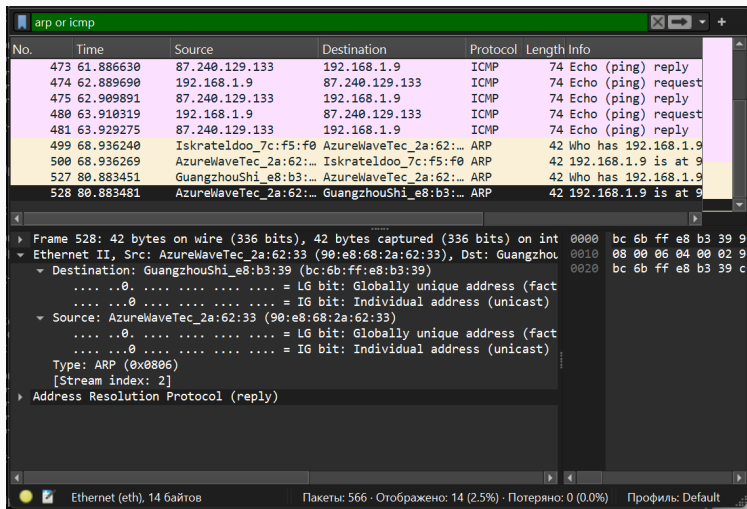


Рис. 11: Кадр ARP - эхо-ответ

Анализ протоколов транспортного уровня в Wireshark

Выполнение лабораторной работы

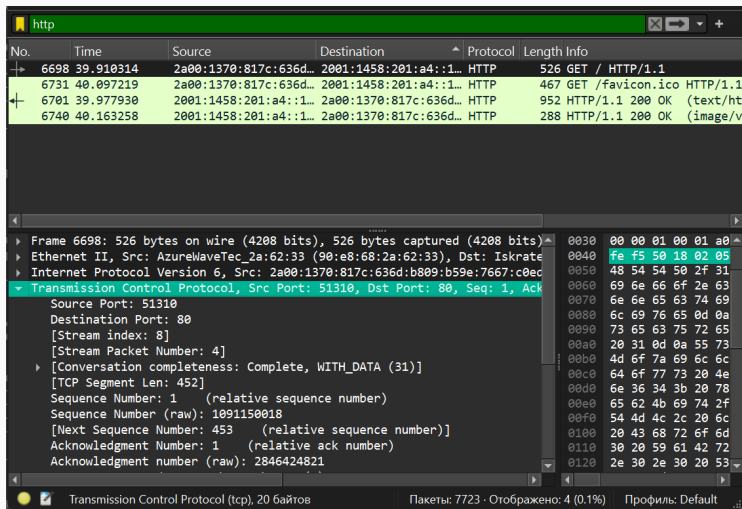


Рис. 12: Кадр http - запрос

Выполнение лабораторной работы

The image shows a Wireshark packet capture window titled 'http'. The packet list pane displays four packets. The selected packet is packet 6701, an HTTP 200 OK response. The packet details pane shows the Transmission Control Protocol (TCP) segment details, including source and destination ports, sequence and acknowledgment numbers, and flags (PSH, ACK). The packet bytes pane shows the raw data of the TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
6698	39.910314	2a00:1370:817c:636d...	2001:1458:201:a4::1...	HTTP	526	GET / HTTP/1.1
6731	40.097219	2a00:1370:817c:636d...	2001:1458:201:a4::1...	HTTP	467	GET /favicon.ico HTTP/1.1
6701	39.977930	2001:1458:201:a4::1...	2a00:1370:817c:636d...	HTTP	952	HTTP/1.1 200 OK (text/html)
6740	40.163258	2001:1458:201:a4::1...	2a00:1370:817c:636d...	HTTP	288	HTTP/1.1 200 OK (image/...)

Transmission Control Protocol, Src Port: 80, Dst Port: 51310, Seq: 1, Ack: 453

- Source Port: 80
- Destination Port: 51310
- [Stream index: 8]
- [Stream Packet Number: 6]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 878]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2846424821
- [Next Sequence Number: 879 (relative sequence number)]
- Acknowledgment Number: 453 (relative ack number)
- Acknowledgment number (raw): 1091150470
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 256

0030 b5 9e 76 67 c0 ed
0040 a2 86 50 18 01 00
0050 2e 31 20 32 30 30
0060 20 57 65 64 2c 20
0070 34 20 31 33 3a 30
0080 53 65 72 76 65 72
0090 4c 61 73 74 2d 4d
00a0 65 64 2c 20 30 35
00b0 31 36 3a 30 30 3a
00c0 61 67 3a 20 22 32
00d0 33 31 30 35 63 30
00e0 52 61 6e 67 65 73
00f0 6f 6e 74 65 6e 74
0100 34 36 0d 0a 43 6f
0110 63 6c 6f 73 65 0d
0120 79 70 65 3a 20 74

Transmission Control Protocol (tcp), 20 байтов Пакеты: 7886 · Отображено: 4 (0.1%) Профиль: Default

Рис. 13: Кадр http - ответ

Выполнение лабораторной работы

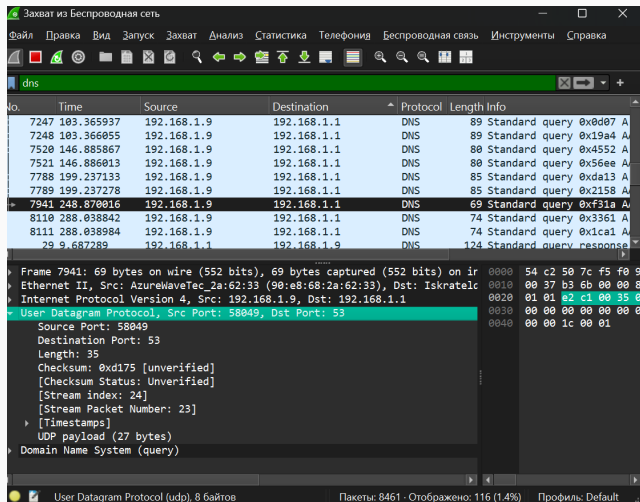


Рис. 14: Кадр dns - запрос

Выполнение лабораторной работы

The image shows a Wireshark packet capture window titled "dns". The packet list on the left shows several DNS packets. Packet 3179 is selected, showing a DNS response from 192.168.1.1 to 192.168.1.9. The packet details pane on the right shows the structure of the User Datagram Protocol (UDP) and Domain Name System (DNS) response.

No.	Time	Source	Destination	Protocol	Length	Info
2956	18.309324	192.168.1.1	192.168.1.9	DNS	157	Standard query response
3089	18.917390	192.168.1.1	192.168.1.9	DNS	122	Standard query response
3090	18.917390	192.168.1.1	192.168.1.9	DNS	134	Standard query response
3178	19.240086	192.168.1.1	192.168.1.9	DNS	97	Standard query response
3179	19.240086	192.168.1.1	192.168.1.9	DNS	109	Standard query response
3438	23.341062	192.168.1.1	192.168.1.9	DNS	161	Standard query response
3439	23.341062	192.168.1.1	192.168.1.9	DNS	173	Standard query response
3754	23.740732	192.168.1.1	192.168.1.9	DNS	105	Standard query response
3757	23.740732	192.168.1.1	192.168.1.9	DNS	93	Standard query response
5222	24.053724	192.168.1.1	192.168.1.9	DNS	321	Standard query response

Frame 3179: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on Ethernet II, Src: IskratelDoo_7c:f5:f2 (54:c2:50:7c:f5:f2), Dst: AzureWaveT Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.9

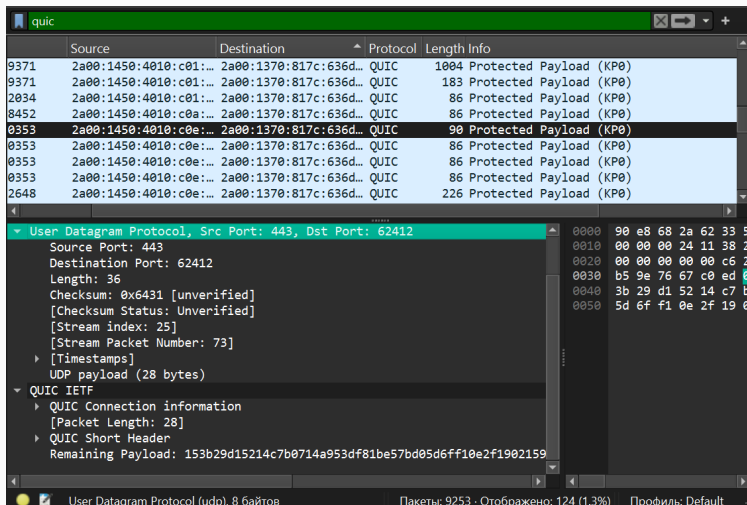
User Datagram Protocol, Src Port: 53, Dst Port: 58049

- Source Port: 53
- Destination Port: 58049
- Length: 75
- Checksum: 0xa8b1 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 24]
- [Stream Packet Number: 2]
- [Timestamps]
- UDP payload (67 bytes)
- Domain Name System (response)

User Datagram Protocol (udp), 8 байтов Пакеты: 8736 · Отображено: 124 (1.4%) Профиль: Default

Рис. 15: Кадр dns - ответ

Выполнение лабораторной работы



The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, with the following details visible:

No.	Source	Destination	Protocol	Length	Info
9371	2a00:1450:4010:c01::...	2a00:1370:817c:636d::...	QUIC	1004	Protected Payload (KP0)
9371	2a00:1450:4010:c01::...	2a00:1370:817c:636d::...	QUIC	183	Protected Payload (KP0)
2034	2a00:1450:4010:c01::...	2a00:1370:817c:636d::...	QUIC	86	Protected Payload (KP0)
8452	2a00:1450:4010:c0a::...	2a00:1370:817c:636d::...	QUIC	86	Protected Payload (KP0)
0353	2a00:1450:4010:c0e::...	2a00:1370:817c:636d::...	QUIC	90	Protected Payload (KP0)
0353	2a00:1450:4010:c0e::...	2a00:1370:817c:636d::...	QUIC	86	Protected Payload (KP0)
0353	2a00:1450:4010:c0e::...	2a00:1370:817c:636d::...	QUIC	86	Protected Payload (KP0)
2648	2a00:1450:4010:c0e::...	2a00:1370:817c:636d::...	QUIC	226	Protected Payload (KP0)

The bottom pane shows the details of the selected packet (0353), which is a User Datagram Protocol (UDP) packet. The details are as follows:

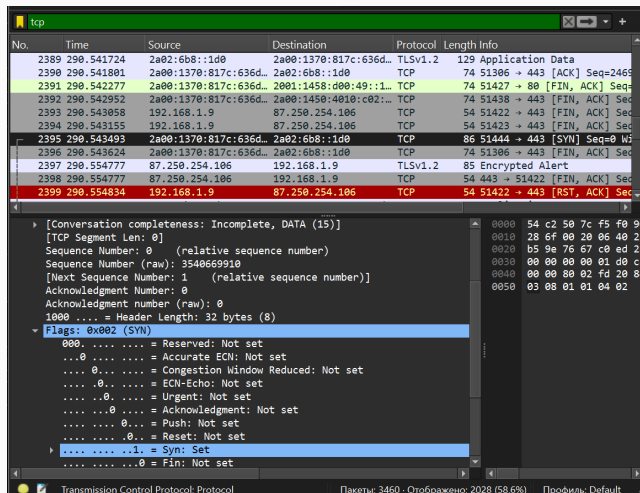
- User Datagram Protocol, Src Port: 443, Dst Port: 62412
 - Source Port: 443
 - Destination Port: 62412
 - Length: 36
 - Checksum: 0x6431 [unverified]
[Checksum Status: Unverified]
 - [Stream index: 25]
 - [Stream Packet Number: 73]
 - [Timestamps]
 - UDP payload (28 bytes)
- QUIC IETF
 - QUIC Connection information
[Packet Length: 28]
 - QUIC Short Header
Remaining Payload: 153b29d15214c7b0714a953df81be57bd05d6ff10e2f1902159

The bottom status bar indicates: User Datagram Protocol (udp), 8 байтов | Пакеты: 9253 · Отображено: 124 (1.3%) | Профиль: Default

Рис. 16: Кадр quic - ответ

Анализ handshake протокола TCP в Wireshark

Выполнение лабораторной работы



No.	Time	Source	Destination	Protocol	Length	Info
2389	290.541724	2a02:6b8::1d0	2a00:1370:817c:636d...	TLSv1.2	129	Application Data
2390	290.541801	2a00:1370:817c:636d...	2a02:6b8::1d0	TCP	74	51306 → 443 [ACK] Seq=2469
2391	290.542277	2a00:1370:817c:636d...	2001:1458:d00:49::1...	TCP	74	51427 → 80 [FIN, ACK] Seq=
2392	290.542952	2a00:1370:817c:636d...	2a00:1450:4010:c02:...	TCP	74	51438 → 443 [FIN, ACK] Seq=
2393	290.543058	192.168.1.9	87.250.254.106	TCP	54	51422 → 443 [FIN, ACK] Seq=
2394	290.543155	192.168.1.9	87.250.254.106	TCP	54	51423 → 443 [FIN, ACK] Seq=
2395	290.543493	2a00:1370:817c:636d...	2a02:6b8::1d0	TCP	86	51444 → 443 [SYN] Seq=0 Wi
2396	290.543624	2a00:1370:817c:636d...	2a02:6b8::1d0	TCP	74	51306 → 443 [FIN, ACK] Seq=
2397	290.554777	87.250.254.106	192.168.1.9	TLSv1.2	85	Encrypted Alert
2398	290.554777	87.250.254.106	192.168.1.9	TCP	54	443 → 51422 [FIN, ACK] Seq=
2399	290.554834	192.168.1.9	87.250.254.106	TCP	54	51422 → 443 [RST, ACK] Seq=

[Conversation completeness: Incomplete, DATA (15)]	
[TCP Segment Len: 0]	
Sequence Number: 0 (relative sequence number)	
Sequence Number (raw): 3540669910	
[Next Sequence Number: 1 (relative sequence number)]	
Acknowledgment Number: 0	
Acknowledgment number (raw): 0	
1000 = Header Length: 32 bytes (8)	
Flags: 0x002 (SYN)	
000.	Reserved: Not set
...0	Accurate ECN: Not set
.... 0...	Congestion Window Reduced: Not set
.... .0..	ECN-Echo: Not set
.... ..0.	Urgent: Not set
.... ...0	Acknowledgment: Not set
....0...	Push: Not set
....0..	Reset: Not set
....1.	Syn: Set
....0	Fin: Not set

Transmission Control Protocol: Protocol Пакеты: 3460 · Отображено: 2028 (58.6%) Профиль: Default

Рис. 17: Первая ступень handshake TCP

Выполнение лабораторной работы

The image shows a Wireshark packet capture window titled 'tcp'. The packet list on the left shows several packets, with packet 2399 selected. The packet details pane on the right shows the structure of the selected packet, which is a TCP segment. The packet is a RST (Reset) segment with the following details:

- Conversation completeness: Incomplete, DATA (15)
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2595859413
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 3506669911
- 1000 = Header Length: 32 bytes (8)
- Flags: 0x012 (SYN, ACK)
- 000. = Reserved: Not set
- ...0 = Accurate ECN: Not set
- 0... = Congestion Window Reduced: Not set
- 0... = ECN-Echo: Not set
-0. = Urgent: Not set
-1 = Acknowledgment: Set
- 0... = Push: Not set
-0.. = Reset: Not set
-1. = Syn: Set
-0 = Fin: Not set

The packet bytes pane on the right shows the raw data of the packet, with the first 16 bytes highlighted in green. The status bar at the bottom indicates 'Acknowledgment Number (tcp.ack), 4 байта' and 'Пакеты: 3615 · Отображено: 2136 (59.1%)'.

Рис. 18: Вторая ступень handshake TCP

Выполнение лабораторной работы

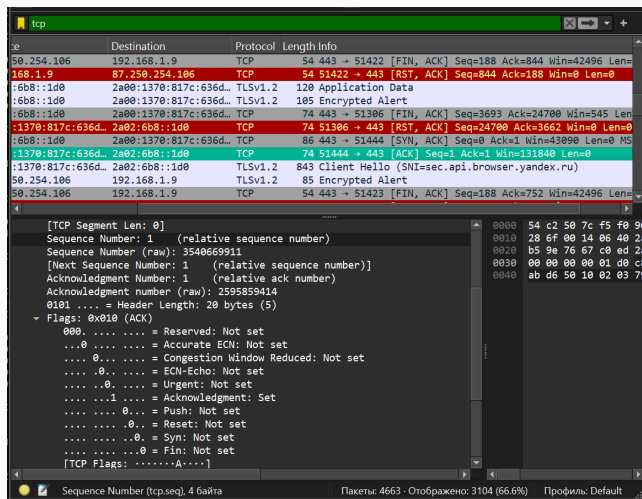


Рис. 19: Третья ступень handshake TCP

Выполнение лабораторной работы

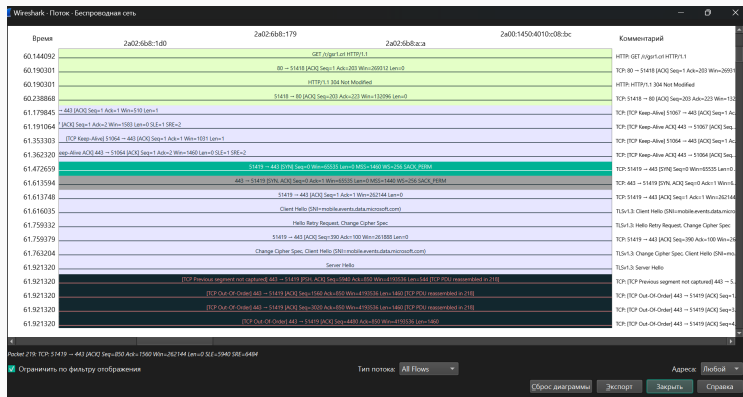


Рис. 20: График потока

В результате выполнения работы были изучены посредством Wireshark кадры Ethernet, произведен анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.