

Сетевые технологии

Анализ трафика в Wireshark (Лабораторная работа №3)

Заур Мустафаев

3 октября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

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

Выполнение лабораторной работы

Получение информации о сетевых интерфейсах

```
Ада п т е р Ethernet Ethernet 2:  
DNS-суф ф и кс по дключе ния . . . . . :  
Ло ка льн ы й IPвб-а др е с с ка на ла . . . : fe80::bae0:cc2e:9d1e:b2d4%19  
IPv4-а др е с . . . . . : 192.168.56.1  
Маска по дсе ти . . . . . : 255.255.255.0  
Осн овн ой шлюз . . . . . :  
  
Ада п т е р бе сп ров одн ой ло ка льн ой се ти По дключе ние по ло ка льн ой се ти * 1:  
Со ст оя ние ср еды . . . . . : Ср еда п ере да чи н е до ступ на .  
DNS-суф ф и кс по дключе ния . . . . . :  
  
Ада п т е р бе сп ров одн ой ло ка льн ой се ти По дключе ние по ло ка льн ой се ти * 2:  
Со ст оя ние ср еды . . . . . : Ср еда п ере да чи н е до ступ на .  
DNS-суф ф и кс по дключе ния . . . . . :  
  
Ада п т е р бе сп ров одн ой ло ка льн ой се ти Бе сп ров одн ая се ть:  
DNS-суф ф и кс по дключе ния . . . . . :  
Ло ка льн ы й IPвб-а др е с с ка на ла . . . : fe80::da3b:4057:9ef4:1e28%7  
IPv4-а др е с . . . . . : 192.168.101.83  
Маска по дсе ти . . . . . : 255.255.255.0  
Осн овн ой шлюз . . . . . : 192.168.101.1  
  
C:\Users\zmustafaev>
```

Рис. 1: Вывод команды ipconfig

Определение MAC-адресов

- MAC-адрес состоит из 48 бит (6 байт).
- Первые 3 байта — OUI производителя.
- Последние 3 байта — уникальный идентификатор интерфейса.

Анализ кадров канального уровня

```
C:\Users\zmustafaev>ping 192.168.101.1

Обмен пакетами с 192.168.101.1 по с 32 байтами данных:
Превышение интервала задержки для запроса.

Статистика Ping для 192.168.101.1:
Пакетов: отправлено = 4, получено = 0, потеряно = 4
(100% потеря)

C:\Users\zmustafaev>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
Превышение интервала задержки для запроса.

Статистика Ping для 192.168.1.1:
Пакетов: отправлено = 4, получено = 0, потеряно = 4
(100% потеря)

C:\Users\zmustafaev>ping ya.ru
```

Рис. 2: Ping шлюза

Фильтрация ARP и ICMP пакетов

*Беспроводная сеть

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

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
396	86.119549	192.168.101.83	192.168.101.1	ICMP	168	Destination unreachable (Port unreachable)
438	86.456178	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=21
439	86.460885	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=21
442	87.469211	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=22
443	87.476664	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=22
444	88.484575	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=23
445	88.490151	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=23
452	89.499469	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=24
453	89.504309	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=24
458	97.806980	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	Who has 192.168.101.1? Tell 192.168.101.1
459	97.814040	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	192.168.101.1 is at ca:7f:54:58:b6:f2
465	106.777916	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	Who has 192.168.101.83? Tell 192.168.101.83
466	106.777940	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	192.168.101.83 is at f8:fe:5e:6f:7b:ec

> Frame 439: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{3ABB42...}

▼ Ethernet II, Src: ca:7f:54:58:b6:f2 (ca:7f:54:58:b6:f2), Dst: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)

 > Destination: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)

 ▼ Source: ca:7f:54:58:b6:f2 (ca:7f:54:58:b6:f2)

 1. = LG bit: Locally administered address (this is NOT the factory default)

 0. = IG bit: Individual address (unicast)

 Type: IPv4 (0x0800)

 [Stream index: 0]

▼ Internet Protocol Version 4, Src: 5.255.255.242, Dst: 192.168.101.83

 0100 = Version: 4

 0101 = Header Length: 20 bytes (5)

 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

 Total Length: 60

 Identification: 0x40aa (16554)

 > 000. = Flags: 0x0

0000 f8 fe 5e
0010 00 3c 41
0020 65 53 01
0030 67 68 61
0040 77 61 61

Internet Control Message Protocol: Protocol

Пакеты: 466 · Отображено: 28 (6.0%) · Потеряно: 0 (0.0%)

Профиль: Default

6/12

ICMP Echo Request

*Беспроводная сеть

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

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
396	86.119549	192.168.101.83	192.168.101.1	ICMP	168	Destination unreachable (Port unreachable)
→ 438	86.456178	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=21,
← 439	86.460885	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=21,
442	87.469211	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=22,
443	87.476664	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=22,
444	88.484575	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=23,
445	88.490151	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=23,
452	89.499469	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=24,
453	89.504309	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=24,
458	97.806980	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	Who has 192.168.101.1? Tell 192.168.101.1
459	97.814040	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	192.168.101.1 is at ca:7f:54:58:b6:f2
465	106.777916	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	Who has 192.168.101.83? Tell 192.168.101.83
466	106.777940	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	192.168.101.83 is at f8:fe:5e:6f:7b:ec

[Header checksum status: Unverified]
Source Address: 192.168.101.83
Destination Address: 5.255.255.242
[Stream index: 18]

Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d46 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 21 (0x0015)
Sequence Number (LE): 5376 (0x1500)
[Response frame: 439]

Data (32 bytes)

0000	ca	7f	5
0010	00	3c	4
0020	ff	f2	0
0030	67	68	6
0040	77	61	6

Internet Control Message Protocol: Protocol
Пакеты: 466 · Отображено: 28 (6.0%) · Потрачено: 0 (0.0%)
Профиль: Default

ARP-запрос

*Беспроводная сеть

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

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
396	86.119549	192.168.101.83	192.168.101.1	ICMP	168	Destination unreachable (Port unreachable)
438	86.456178	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=21
439	86.460885	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=21
442	87.469211	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=22
443	87.476664	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=22
444	88.484575	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=23
445	88.490151	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=23
452	89.499469	192.168.101.83	5.255.255.242	ICMP	74	Echo (ping) request id=0x0001, seq=24
453	89.504309	5.255.255.242	192.168.101.83	ICMP	74	Echo (ping) reply id=0x0001, seq=24
458	97.806980	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	Who has 192.168.101.1? Tell 192.168.101.1
459	97.814040	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	192.168.101.1 is at ca:7f:54:58:b6:f2
465	106.777916	ca:7f:54:58:b6:f2	Intel_6f:7b:ec	ARP	42	Who has 192.168.101.83? Tell 192.168.101.83
466	106.777940	Intel_6f:7b:ec	ca:7f:54:58:b6:f2	ARP	42	192.168.101.83 is at f8:fe:5e:6f:7b:ec

▼ Ethernet II, Src: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec), Dst: ca:7f:54:58:b6:f2 (ca:7f:54:58:b6:f2)
 > Destination: ca:7f:54:58:b6:f2 (ca:7f:54:58:b6:f2)
 > Source: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
 Type: ARP (0x0806)
 [Stream index: 0]

▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: Intel_6f:7b:ec (f8:fe:5e:6f:7b:ec)
 Sender IP address: 192.168.101.83
 Target MAC address: ca:7f:54:58:b6:f2 (ca:7f:54:58:b6:f2)
 Target IP address: 192.168.101.1

0000 ca 7f 5
0010 08 00 0
0020 ca 7f 5

Internet Control Message Protocol
Пакеты: 465. Отображены: 28 (6.0%). Потерянные: 0 (0.0%). Порядок: Default

8/12

Анализ протоколов транспортного уровня

HTTP (TCP)

Захват из Беспроводная сеть

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

http

No.	Time	Source	Destination	Protocol	Length	Info
211	32.320098	192.168.101.83	188.184.67.127	HTTP	502	GET / HTTP/1.1
216	32.372883	188.184.67.127	192.168.101.83	HTTP	932	HTTP/1.1 200 OK (text/html)
222	32.394296	192.168.101.83	188.184.67.127	HTTP	443	GET /favicon.ico HTTP/1.1
231	32.451183	188.184.67.127	192.168.101.83	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
253	37.098234	192.168.101.83	188.184.67.127	HTTP	562	GET /hypertext/www/TheProject.html HTTP/1.1
262	37.153440	188.184.67.127	192.168.101.83	HTTP	1044	HTTP/1.1 200 OK (text/html)
299	39.926291	192.168.101.83	188.184.67.127	HTTP	588	GET /hypertext/www/History.html HTTP/1.1
306	39.979676	188.184.67.127	192.168.101.83	HTTP	871	HTTP/1.1 200 OK (text/html)

Transmission Control Protocol, Src Port: 80, Dst Port: 51748, Seq: 1, Ack: 449, Len: 878

Source Port: 80
Destination Port: 51748
[Stream index: 6]
[Stream Packet Number: 6]

> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 878]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3543265741
[Next Sequence Number: 879 (relative sequence number)]
Acknowledgment Number: 449 (relative ack number)
Acknowledgment number (raw): 2504905904
0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH ACK)

0020 65 53
0030 00 f9
0040 30 30
0050 2e 20
0060 3a 30
0070 65 72
0080 2d 4d
0090 30 35
00a0 30 3a
00b0 22 32
00c0 63 30
00d0 65 73
00e0 6e 74
00f0 43 6f
0100 65 0d
0110 20 74
0120 5c 5d

Анализ TCP Handshake

Захват из Беспроводная сеть

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

tcp

No.	Time	Source	Destination	Protocol	Length	Info
210	31.235536	192.168.101.83	213.180.204.63	TCP	54	56211 → 443 [ACK] Seq=6810 Ack=5711 Win=128
211	32.320098	192.168.101.83	188.184.67.127	HTTP	502	GET / HTTP/1.1
212	32.320523	192.168.101.83	188.184.67.127	TCP	66	59570 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS
213	32.371053	188.184.67.127	192.168.101.83	TCP	54	80 → 51748 [ACK] Seq=1 Ack=449 Win=31872 Len=0
214	32.372555	188.184.67.127	192.168.101.83	TCP	66	443 → 59570 [SYN, ACK] Seq=1 Ack=1 Win=3216
215	32.372628	192.168.101.83	188.184.67.127	TCP	54	59570 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
216	32.372883	188.184.67.127	192.168.101.83	HTTP	932	HTTP/1.1 200 OK (text/html)
217	32.372883	188.184.67.127	192.168.101.83	TCP	54	80 → 51748 [FIN, ACK] Seq=879 Ack=449 Win=0
218	32.372911	192.168.101.83	188.184.67.127	TCP	54	51748 → 80 [ACK] Seq=449 Ack=880 Win=130304
219	32.373003	192.168.101.83	188.184.67.127	TLSv1.3	2127	Client Hello (SNI=info.cern.ch)
220	32.373421	192.168.101.83	188.184.67.127	TCP	54	51748 → 80 [FIN, ACK] Seq=449 Ack=880 Win=0
221	32.389189	192.168.101.83	213.180.193.234	TCP	55	53877 → 443 [ACK] Seq=1 Ack=1 Win=507 Len=1
222	32.394296	192.168.101.83	188.184.67.127	HTTP	443	GET /favicon.ico HTTP/1.1
223	32.396238	213.180.193.234	192.168.101.83	TCP	66	443 → 53877 [ACK] Seq=1 Ack=2 Win=166 Len=0

Destination Port: 80
[Stream index: 6]
[Stream Packet Number: 8]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 449 (relative sequence number)
Sequence Number (raw): 2504905904
[Next Sequence Number: 449 (relative sequence number)]
Acknowledgment Number: 880 (relative ack number)
Acknowledgment number (raw): 3543266620
0101 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 509
[Calculated window size: 130304]
[Window size scaling factor: 256]

0000 ca 7f 54 t
0010 00 28 b7 t
0020 43 7f ca z
0030 01 fd 26 z

Transmission Control Protocol: Protocol
Пакеты: 181351 · Отображено: 181034 (99.8%)
Профиль: Default

10/12

Визуализация TCP Handshake

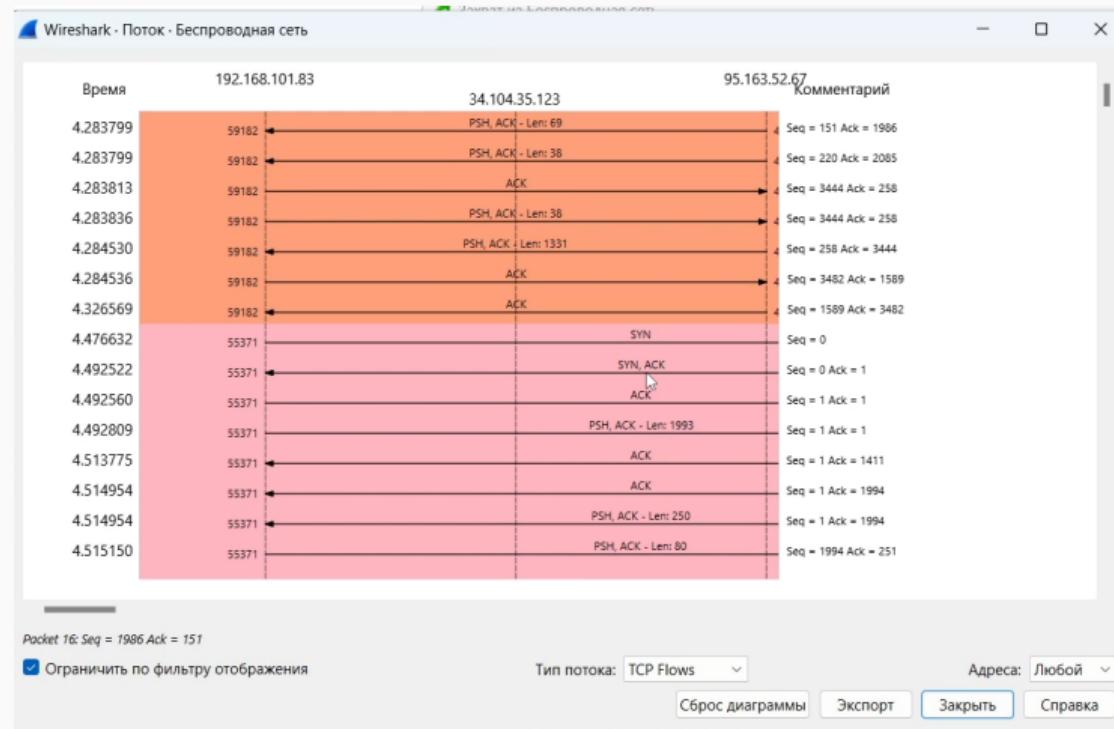


Рис. 10: График TCP потока

Выводы по работе

Вывод

В ходе работы с помощью Wireshark были проанализированы пакеты Ethernet, ICMP, ARP, HTTP, DNS и QUIC. Подробно изучен процесс установления TCP-соединения (трёхстороннее рукопожатие). Получены практические навыки фильтрации и анализа сетевого трафика.