Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Лабораторная работа №6
по дисциплине: **КСиС**
Тема: Анализ сетевого трафика и протоколов на базе WIRESHARK

Выполнил
студент 2 курса
Корнасевич И. Д.

Проверил
Савицкий Ю. В.

Брест 2021

Цель работы: Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark (файл netWS.pdf), изучить типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.

Запустив Wireshark на захват, выполнить загрузку доступной в лабораторных условиях страницы (bstu.by, iit.bstu.by или др.). Остановить и сохранить захват. Для захваченных пакетов определить статистические данные:

1. процентное соотношение трафика разных протоколов в сети
2. среднюю скорость кадров/сек
3. среднюю скорость байт/сек
4. минимальный, максимальный и средний размеры пакета
5. степень использования полосы пропускания канала (загрузку сети)

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	6332	100.0	5347260	1,053 k	0	0	0
Ethernet	100.0	6332	1.7	88648	17 k	0	0	0
Slow Protocols	0.1	8	0.0	8	1	0	0	0
OSSP	0.1	8	0.0	440	86	8	440	86
Internet Protocol Version 6	0.7	46	0.0	1840	362	0	0	0
User Datagram Protocol	0.7	42	0.0	336	66	0	0	0
Domain Name System	0.7	42	0.0	2591	510	42	2591	510
Internet Control Message Protocol v6	0.1	4	0.0	112	22	4	112	22
Internet Protocol Version 4	98.8	6254	2.3	125080	24 k	0	0	0
User Datagram Protocol	88.9	5631	0.8	45048	8,877	0	0	0
QUIC IETF	74.1	4692	77.4	4141134	816 k	4669	4137749	815 k
Data	15.2	962	10.3	548453	108 k	962	548453	108 k
Transmission Control Protocol	9.8	623	7.4	394069	77 k	326	93752	18 k
Transport Layer Security	4.9	313	7.2	385653	75 k	297	356678	70 k
Address Resolution Protocol	0.4	24	0.0	1068	210	24	1068	210

File

Name:	/tmp/wireshark_enp8s0_20210506160158_CTuBlh.pcapng
Length:	5,554 kB
Hash (SHA256):	78d0c1b8c6bb7a4f050d8ab43cdc97200899ae6319131ebe1bcd3bed99e189d2
Hash (RIPEMD160):	b464ecc0cb49671db7dd6742d2128a56440ea566
Hash (SHA1):	8a3bebe8a673d0e703c4299d841af5ecee992032
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2021-05-06 16:01:59
Last packet:	2021-05-06 16:02:39
Elapsed:	00:00:40

Capture

Hardware:	AMD Ryzen 5 2600 Six-Core Processor (with SSE4.2)
OS:	Linux 5.8.0-50-generic
Application:	Dumpcap (Wireshark) 3.2.3 (Git v3.2.3 packaged as 3.2.3-1)

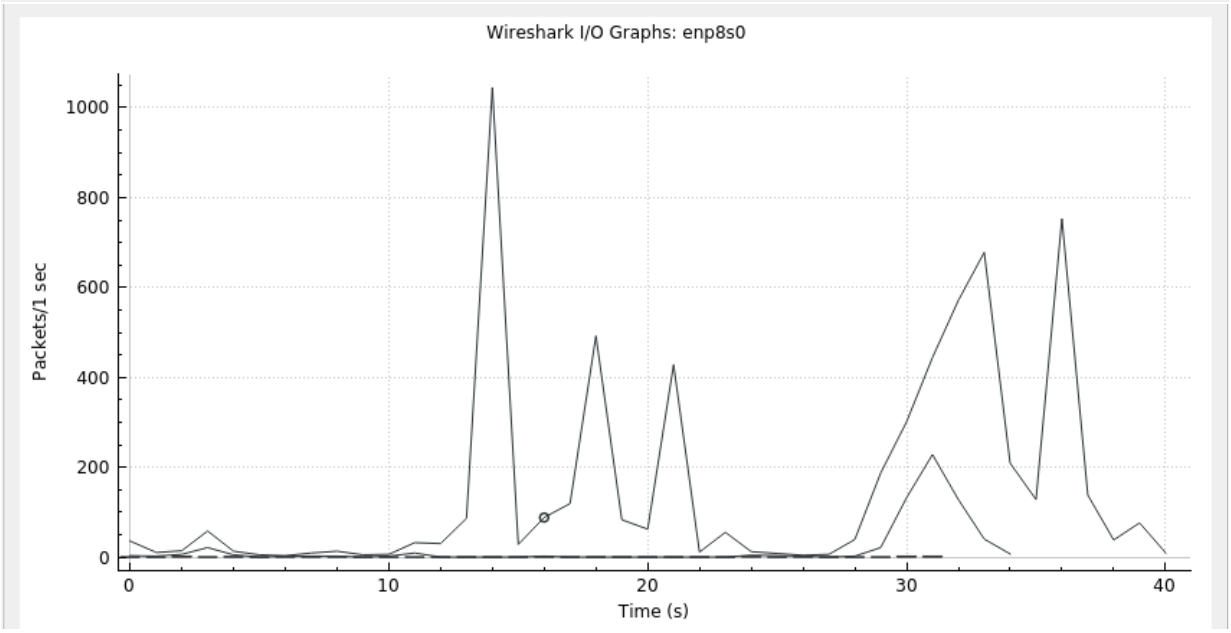
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
enp8s0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	6332	623 (9.8%)	—
Time span, s	40.595	33.898	—
Average pps	156.0	18.4	—
Average packet size, B	844	667	—
Bytes	5347260	415275 (7.8%)	0
Average bytes/s	131 k	12 k	—
Average bits/s	1,053 k	98 k	—

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	6332	844.48	42	7186	0.1560	100%	7.2300	36.094
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	1942	71.99	42	79	0.0478	30.67%	0.8400	36.095
80-159	302	112.69	80	159	0.0074	4.77%	0.1500	30.760
160-319	284	227.16	161	318	0.0070	4.49%	0.1700	14.649
320-639	191	471.39	320	638	0.0047	3.02%	0.1000	14.857
640-1279	229	893.58	642	1279	0.0056	3.62%	0.1300	36.089
1280-2559	3330	1395.34	1288	2279	0.0820	52.59%	6.1400	36.094
2560-5119	52	2969.69	2850	4338	0.0013	0.82%	0.1600	31.413
5120 and greater	2	6679.50	6173	7186	0.0000	0.03%	0.0200	32.634



Wireshark · Packet Lengths · enp8s0

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	6332	844.48	42	7186	0.1560	100%	7.2300	36.094
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	1942	71.99	42	79	0.0478	30.67%	0.8400	36.095
80-159	302	112.69	80	159	0.0074	4.77%	0.1500	30.760
160-319	284	227.16	161	318	0.0070	4.49%	0.1700	14.649
320-639	191	471.39	320	638	0.0047	3.02%	0.1000	14.857
640-1279	229	893.58	642	1279	0.0056	3.62%	0.1300	36.089
1280-2559	3330	1395.34	1288	2279	0.0820	52.59%	6.1400	36.094
2560-5119	52	2969.69	2850	4338	0.0013	0.82%	0.1600	31.413
5120 and greater	2	6679.50	6173	7186	0.0000	0.03%	0.0200	32.634

Display filter: tcp

Apply

Copy Save as... Close

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	6254	853.82	54	7186	0.1541	100%	7.2300	36.094
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	1908	72.16	54	79	0.0470	30.51%	0.8400	36.095
80-159	264	113.01	80	159	0.0065	4.22%	0.1400	30.787
160-319	278	227.86	161	318	0.0068	4.45%	0.1700	14.649
320-639	191	471.39	320	638	0.0047	3.05%	0.1000	14.857
640-1279	229	893.58	642	1279	0.0056	3.66%	0.1300	36.089
1280-2559	3330	1395.34	1288	2279	0.0820	53.25%	6.1400	36.094
2560-5119	52	2969.69	2850	4338	0.0013	0.83%	0.1600	31.413
5120 and greater	2	6679.50	6173	7186	0.0000	0.03%	0.0200	32.634

Display filter: ip Apply

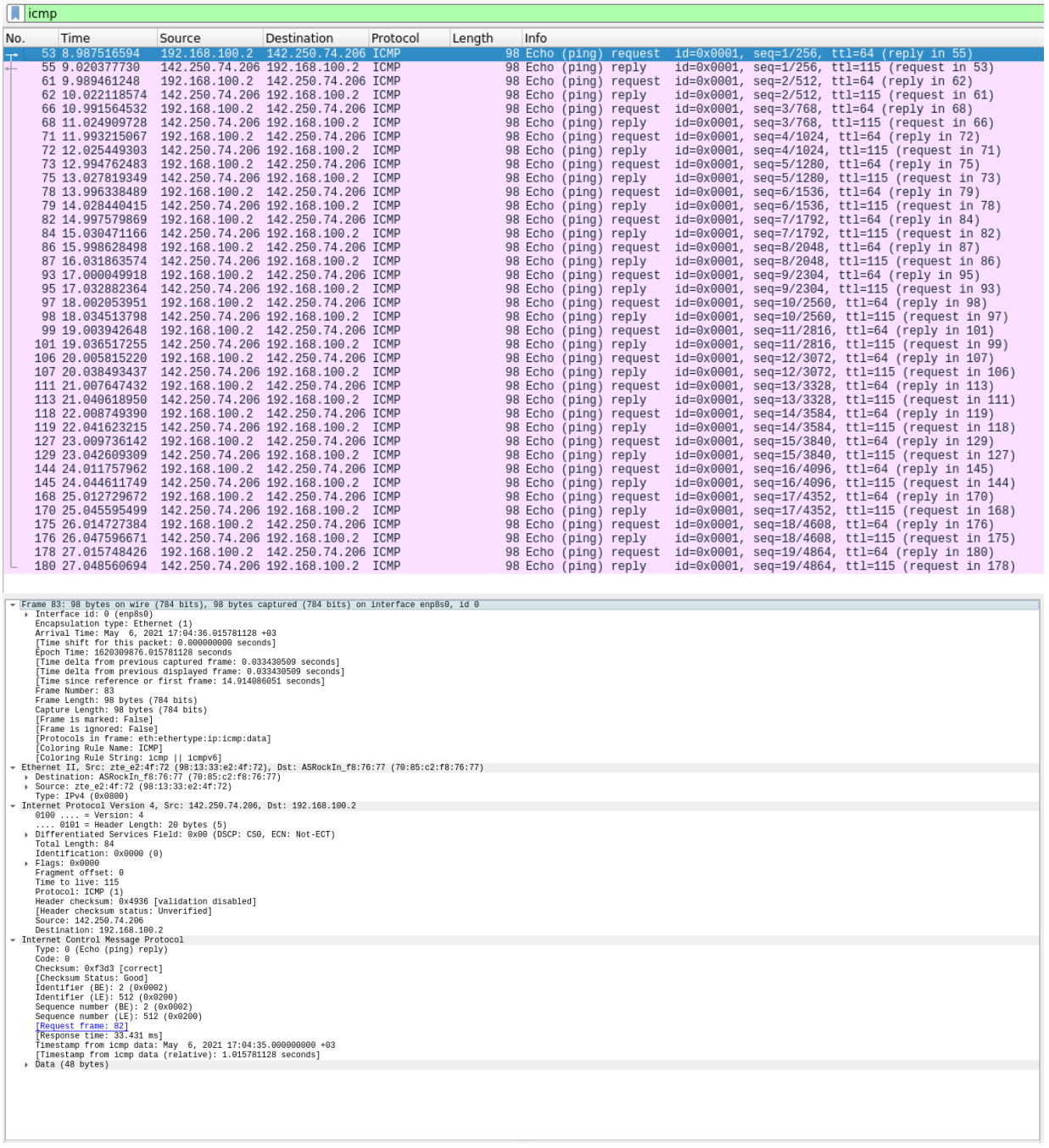
На примере любого IP-пакета указать структуры протоколов Ethernet и IP. Отметить поля заголовков и описать их и интерпретировать их значения.

```
Frame 74: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp8s0, id 0
    Interface id: 0 (enp8s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: May  6, 2021 16:02:02.421337089 +03
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1620306122.421337089 seconds
    [Time delta from previous captured frame: 0.016730365 seconds]
    [Time delta from previous displayed frame: 0.021167968 seconds]
    [Time since reference or first frame: 3.018283887 seconds]
    Frame Number: 74
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: zte_e2:4f:72 (98:13:33:e2:4f:72), Dst: ASRockIn_f8:76:77 (70:85:c2:f8:76:77)
    Destination: ASRockIn_f8:76:77 (70:85:c2:f8:76:77)
    Source: zte_e2:4f:72 (98:13:33:e2:4f:72)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 87.240.129.131, Dst: 192.168.100.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xb9bf (47551)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 55
    Protocol: TCP (6)
    Header checksum: 0x8be6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 87.240.129.131
    Destination: 192.168.100.2
Transmission Control Protocol, Src Port: 443, Dst Port: 32924, Seq: 303, Ack: 302, Len: 0
    Source Port: 443
    Destination Port: 32924
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence number: 303    (relative sequence number)
    Sequence number (raw): 4138743265
    [Next sequence number: 303    (relative sequence number)]
    Acknowledgment number: 302    (relative ack number)
    Acknowledgment number (raw): 1713378593
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x010 (ACK)
    Window size value: 202
    [Calculated window size: 202]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x3761 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [SEQ/ACK analysis]
    [Timestamps]
```

- Source — физический адрес устройства отправителя.
- Destination — физический адрес устройства получателя.
- Type — тип протокола.
  - Internet Protocol Version 4 - пакет протокола IPv4.
  - Time to live: 64 – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети, равняется 64.
  - Protocol: TCP (6) – На транспортном уровне используется протокол TCP. Значение данного поля позволяет устройству определить, какому протоколу транспортного уровня следует передать полученное PDU. В данном случае это протокол TCP.

Запустив Wireshark на захват, выполнить команду ping для IP адреса соседней рабочей станции в лаборатории (предварительно определив ее адрес с помощью ipconfig). Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping. На базе полученных пакетов и значений их полей интерпретировать результат работы утилиты ping. Описать все

протоколы, используемые утилитой. Составить диаграмму взаимодействия машин при работе утилиты ping. Примечание. Данная утилита использует протокол ICMP (RFC 792 и RFC 960).



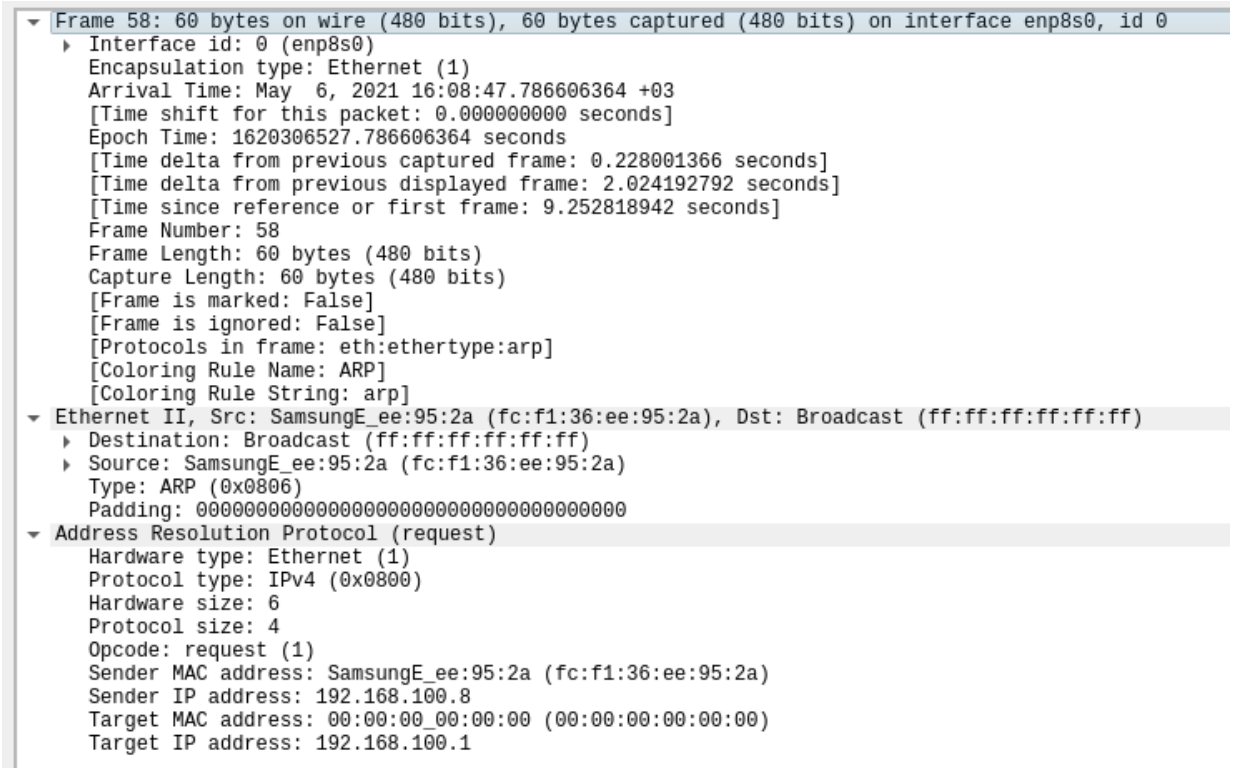
icmp

No.	Time	Source	Destination	Protocol	Length	Info
53	8.987516594	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 55)
55	9.020377730	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=1/256, ttl=115 (request in 53)
61	9.989461248	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 62)
62	10.022118574	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=2/512, ttl=115 (request in 61)
66	10.991564532	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 68)
68	11.024909728	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=3/768, ttl=115 (request in 66)
71	11.993215067	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 72)
72	12.025449303	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=4/1024, ttl=115 (request in 71)
73	12.994762483	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 75)
75	13.027819349	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=5/1280, ttl=115 (request in 73)
78	13.996338489	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 79)
79	14.028440415	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=6/1536, ttl=115 (request in 78)
82	14.997579869	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 84)
84	15.030471166	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=7/1792, ttl=115 (request in 82)
86	15.998628498	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 87)
87	16.031863574	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=8/2048, ttl=115 (request in 86)
93	17.000049918	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 95)
95	17.032882364	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=9/2304, ttl=115 (request in 93)
97	18.002053951	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 98)
98	18.034513798	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=10/2560, ttl=115 (request in 97)
99	19.003942648	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=11/2816, ttl=64 (reply in 101)
101	19.036517255	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=11/2816, ttl=115 (request in 99)
106	20.005815220	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=12/3072, ttl=64 (reply in 107)
107	20.038493437	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=12/3072, ttl=115 (request in 106)
111	21.007647432	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (reply in 113)
113	21.040618950	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=13/3328, ttl=115 (request in 111)
118	22.008749390	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=14/3584, ttl=64 (reply in 119)
119	22.041623215	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=14/3584, ttl=115 (request in 118)
127	23.009736142	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 129)
129	23.042609309	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=15/3840, ttl=115 (request in 127)
144	24.011757962	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 145)
145	24.044611749	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=16/4096, ttl=115 (request in 144)
168	25.012729672	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 170)
170	25.045595499	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=17/4352, ttl=115 (request in 168)
175	26.014727384	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 176)
176	26.047596671	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=18/4608, ttl=115 (request in 175)
178	27.015748426	192.168.100.2	142.250.74.206	ICMP	98	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 180)
180	27.048560694	142.250.74.206	192.168.100.2	ICMP	98	Echo (ping) reply id=0x0001, seq=19/4864, ttl=115 (request in 178)

```
Frame 83: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp8s0, id 0
    Interface id: 0 (enp8s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: May  6, 2021 17:04:36.015781128 +03
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1620309876.015781128 seconds
    [Time delta from previous captured frame: 0.033430509 seconds]
    [Time delta from previous displayed frame: 0.033430509 seconds]
    [Time since reference or first frame: 14.914086051 seconds]
    Frame Number: 83
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 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: zte_e2:4f:72 (98:13:33:e2:4f:72), Dst: ASRockIn_f8:76:77 (70:85:c2:f8:76:77)
    Destination: ASRockIn_f8:76:77 (70:85:c2:f8:76:77)
    Source: zte_e2:4f:72 (98:13:33:e2:4f:72)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 142.250.74.206, Dst: 192.168.100.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x0000
    Fragment offset: 0
    Time to live: 115
    Protocol: ICMP (1)
    Header checksum: 0x4936 [validation disabled]
    [Header checksum status: Unverified]
    Source: 142.250.74.206
    Destination: 192.168.100.2
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xf3d3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
    [Request frame: 82]
    [Response time: 33.431 ms]
    Timestamp from icmp data: May  6, 2021 17:04:35.000000000 +03
    [Timestamp from icmp data (relative): 1.015781128 seconds]
    Data (48 bytes)
```

- Type: 0 (Echo (ping) reply) - тип сообщения ICMP.
- 0 - эхо-ответ (Echo Replay).
- Checksum: 0xf3d3 [correct] - контрольная сумма, вычисляется из части ICMP пакета.
- Data (48 bytes) – поле данных

Выполнить анализ ARP-протокола по примеру из методических указаний. ARP — сетевой протокол, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP.



- Sender MAC address — MAC-адрес отправителя.
- Sender IP address — IP-адрес отправителя.
- Target IP address — IP-адрес получателя.

Вывод: В ходе данной лабораторной работы мы изучили типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.