МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра ИИТ

Отчёт
о лабораторной работе №6
по дисциплине «Компьютерные системы и сети»

Тема: «Анализ сетевого трафика и протоколов (на базе WireShark)»

Выполнил студент 2 курса
группы ПО-11 Сымоник И.А.
Номер зачетной книжки: 220220

Проверил: Савицкий Ю.В.

Брест 2024

Цель работы: приобретение навыков анализа сетевого трафика компьютерных сетей; изучение структуры сетевых протоколов различных уровней

Вариант 6

Ход работы

Вариант	**Адрес url**
6	https://ria.ru/

1. Остановить и сохранить захват. Для захваченных пакетов определить

статистические данные:

- процентное соотношение трафика разных протоколов в сети;

- среднюю скорость кадров/сек;

- среднюю скорость байт/сек;

- минимальный, максимальный и средний размеры пакета;

- степень использования полосы пропускания канала (загрузку сети)

Протокол	Процент пакетов	Пакеты	Процент байтов	Байты	Бит/с	Конечные пакеты	Конечные байты	Конечные бит/с	PDU
Frame	100.0	2409	100.0	1550655	1653 k	0	0	0	2409
Ethernet	100.0	2409	2.2	34038	36 k	0	0	0	2409
Internet Protocol Version 4	100.0	2409	3.1	48180	51 k	0	0	0	2409
User Datagram Protocol	24.7	595	0.3	4760	5077	0	0	0	595
QUIC IETF	20.0	481	21.7	337103	359 k	481	324189	345 k	500
Multicast Domain Name System	0.2	4	0.0	546	582	4	546	582	4
Domain Name System	4.6	110	0.4	6410	6836	110	6410	6836	110
Transmission Control Protocol	75.3	1814	72.5	1124586	1199 k	1378	854400	911 k	1814
Transport Layer Security	18.1	436	71.0	1100836	1174 k	436	932670	994 k	467

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	2409	643,69	54	1466	0,3212	100%	1,5200	2,790
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	944	59,71	54	79	0,1259	39,19%	0,5800	2,716
80-159	222	121,00	80	159	0,0296	9,22%	0,2000	5,160
160-319	86	241,65	161	317	0,0115	3,57%	0,1000	4,964
320-639	73	482,45	323	623	0,0097	3,03%	0,1000	3,060
640-1279	475	1185,63	640	1274	0,0633	19,72%	0,7400	3,211
1280-2559	609	1392,85	1288	1466	0,0812	25,28%	0,7200	2,711
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

2. Отфильтровать в захвате IP пакеты. Определить статистические данные:

- процентное соотношение трафика разных протоколов стека tcp/ip в сети;

- средний, минимальный, максимальный размеры пакета.

Протокол	Процент пакетов	Пакеты	Процент байтов	Байты	Бит/с	Конечные пакеты	Конечные байты	Конечные бит/с	PDU
Frame	100.0	117	100.0	79172	210 k	0	0	0	117
Ethernet	100.0	117	2.1	1656	4404	0	0	0	117
Internet Protocol Version 4	100.0	117	3.0	2340	6223	0	0	0	117
Transmission Control Protocol	100.0	117	95.0	75176	199 k	87	57788	153 k	117
Transport Layer Security	25.6	30	94.8	75048	199 k	30	66516	176 k	33

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	2409	643,69	54	1466	0,3212	100%	1,5200	2,790
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	944	59,71	54	79	0,1259	39,19%	0,5800	2,716
80-159	222	121,00	80	159	0,0296	9,22%	0,2000	5,160
160-319	86	241,65	161	317	0,0115	3,57%	0,1000	4,964
320-639	73	482,45	323	623	0,0097	3,03%	0,1000	3,060
640-1279	475	1185,63	640	1274	0,0633	19,72%	0,7400	3,211
1280-2559	609	1392,85	1288	1466	0,0812	25,28%	0,7200	2,711
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

3. На примере третьего захваченного IP-пакета указать структуры протокола канального уровня (протокола Ethernet 802.3, Wi-Fi 802.11, либо другого, используемого в вашей конфигурации) и протокола IPv4. Отметить поля заголовков и описать их и интерпретировать их значения.

Захваченный пакет:

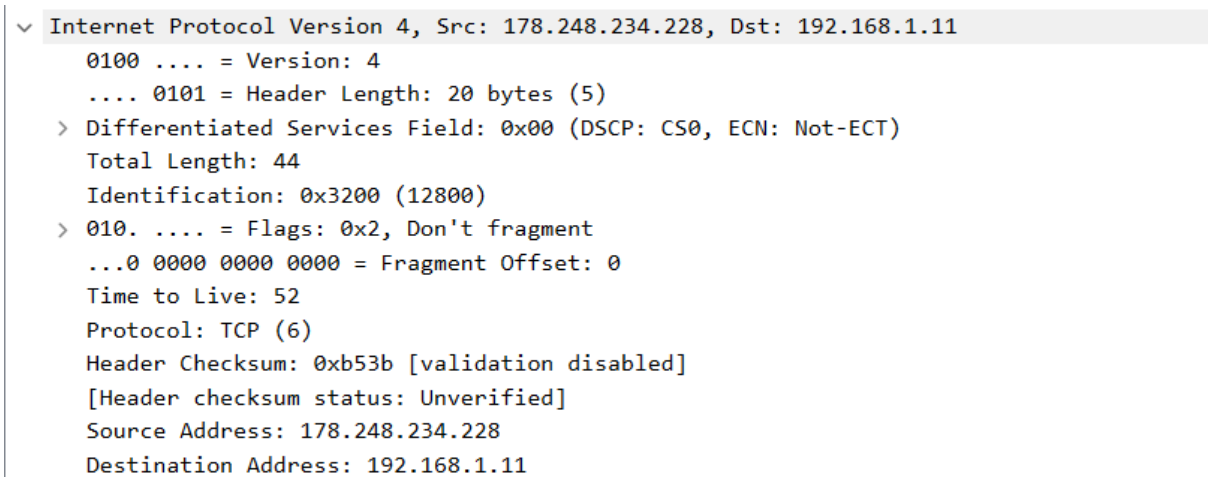
Протокол канального уровня(Ethernet 802.3):

MAC-адрес назначения (Destination MAC Address): 6 байт (30:03:c8:10:1a:57), адрес устройства-получателя.

MAC-адрес источника (Source MAC Address): 6 байт (80:7d:14:81:4a:77), адрес устройства-отправителя.

Тип или длина (Type/Length): 2 байта (0x0800), указывает на то, что это IPv4-пакет.

Протокол IPv4:



Версия (Version): 4, указывает на версию протокола IPv4.

Длина заголовка (Header Length): 4 бита, что соответствует 20 байтам (5 слов по 32 бита), так как это стандартный размер заголовка IPv4.

Тип сервиса (Type of Service): 8 бит, предназначен для определения приоритета обработки пакета.

Длина пакета (Total Length): 16 бит, указывает на общую длину пакета в байтах (включая заголовок и данные). Значение - 44

Идентификатор (Identification): 16 бит, идентифицирует фрагменты, связанные с одним и тем же исходным пакетом. Значение - 12800

Флаги (Flags): 3 бита, используются для управления фрагментацией. Значение – 010 (Установлен бит запрета фрагментирования)

Смещение фрагмента (Fragment Offset): 13 бит, указывает на смещение фрагмента в пакете. Значение – 0

Время жизни (Time to Live): 8 бит, определяет количество переходов, которое пакет может сделать через маршрутизаторы, прежде чем он будет отброшен. Значение – 52

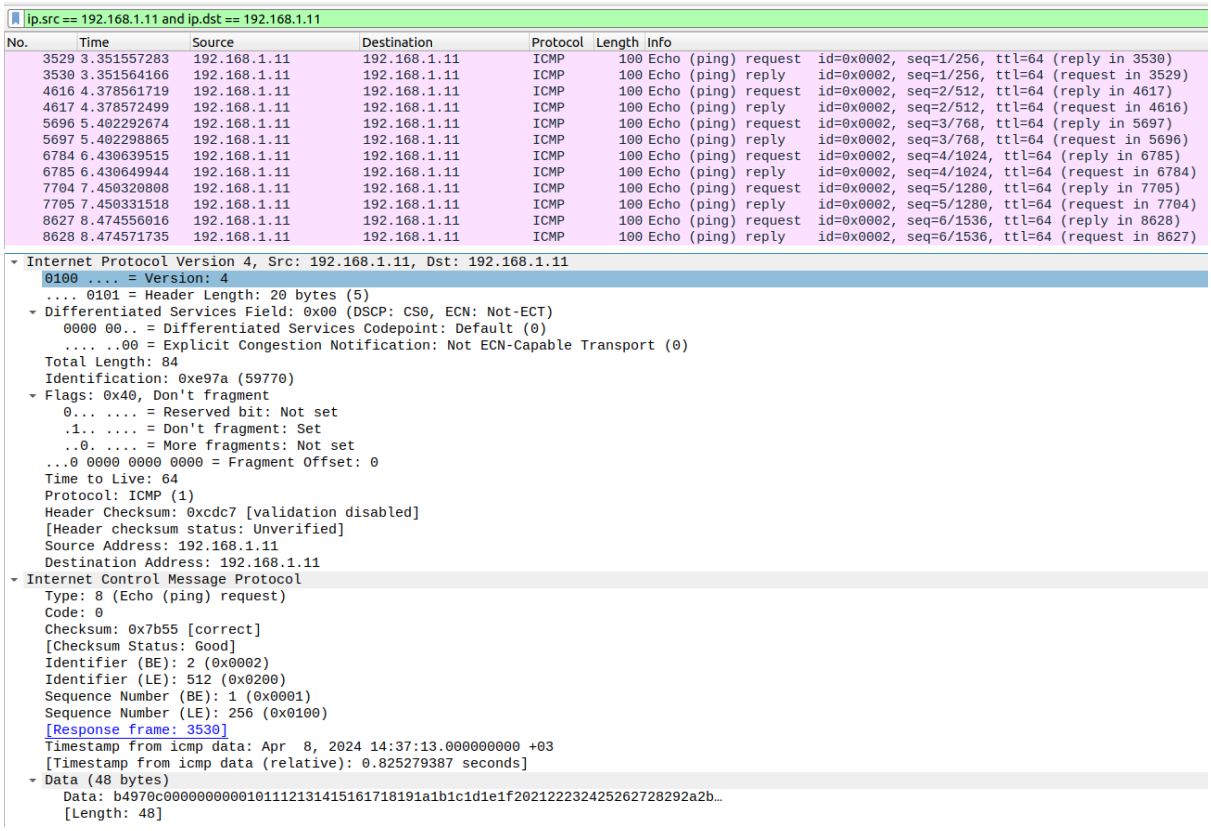
Протокол (Protocol): 8 бит, указывает на протокол верхнего уровня. Значение – TCP

Контрольная сумма заголовка (Header Checksum): 16 бит, используется для проверки целостности заголовка IPv4. Значение – 0xb53b

IP-адрес источника (Source IP Address): 32 бита (192.168.1.100), IP-адрес устройства-отправителя. Значение – 178.248.234.228

IP-адрес назначения (Destination IP Address): 32 бита (10.0.0.1), IP-адрес устройства-получателя. Значение – 192.168.1.11

4. Запустив Wireshark на захват, выполнить команду ping для IP адреса компьютера (предварительно определив его адрес с помощью ipconfig; пример команды: ping 172.17.20.246). 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.



В утилите ping используется протокол ICMP. В этом протоколе следующие поля:

Тип сообщения (Type): Определяет тип сообщения ICMP. Например, тип 8 соответствует эхо-запросу, а тип 0 - эхо-ответу. Значение – 8

Код (Code): Код, который обычно используется для более детальной классификации типа сообщения. Значение - 0

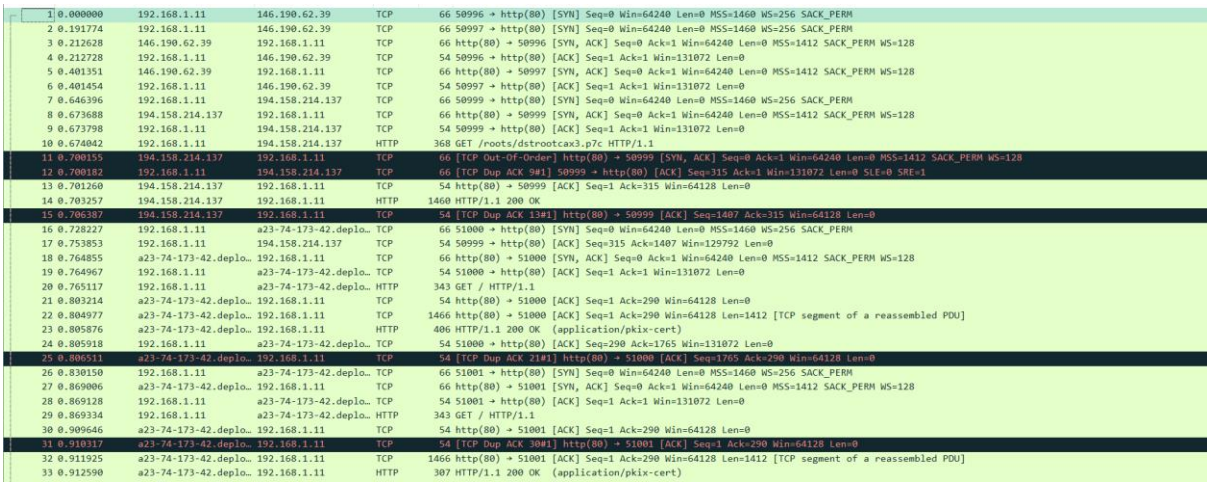
Контрольная сумма (Checksum): Проверка целостности пакета. Значение – 0x7b55

Идентификатор (Identifier) и последовательный номер (Sequence Number): Идентификатор и последовательный номер, которые помогают установить соответствие между эхо-запросами и эхо-ответами. Значения – 0x0002 и 0x0001 (порядок от старшего к младшему), . Значения – 0x0200 и 0x0100 (порядок от младшего к старшему).

Данные (Data): Сами данные, включая метку времени отправки и приема пакета.

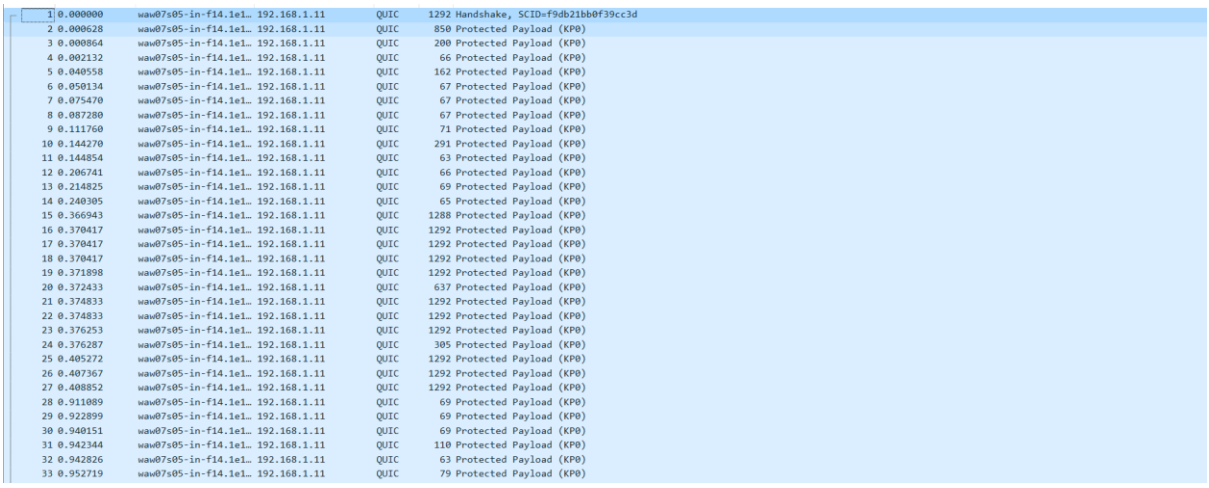
5. Сформировать не менее 3-х сложных фильтров захвата с использованием полей протоколов, операторов сравнения (таблицы 1 и 2 из файла теоретические_указания4) и логических операторов; каждый раз перезапуская захват, для каждого фильтра захватить соответствующие пакеты.

1) tcp port 80 and not arp



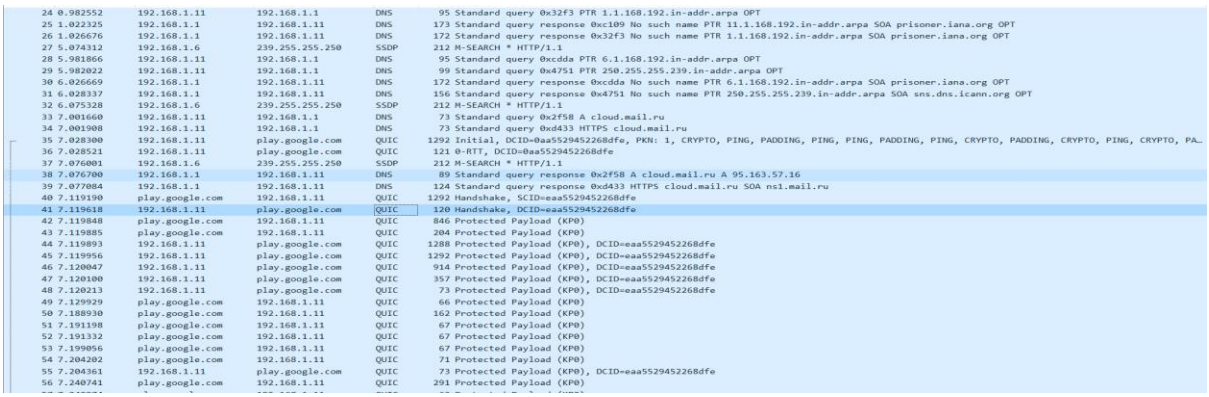
1	0.000000	192.168.1.11	146.190.62.39	TCP	66 50996 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.191774	192.168.1.11	146.190.62.39	TCP	66 50997 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3	0.212628	146.190.62.39	192.168.1.11	TCP	66 http(80) → 50996 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
4	0.212728	192.168.1.11	146.190.62.39	TCP	54 50996 → http(80) [ACK] Seq=1 Ack=1 Win=131072 Len=0
5	0.401351	146.190.62.39	192.168.1.11	TCP	66 http(80) → 50997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
6	0.401454	192.168.1.11	146.190.62.39	TCP	54 50997 → http(80) [ACK] Seq=1 Ack=1 Win=131072 Len=0
7	0.646396	192.168.1.11	194.158.214.137	TCP	66 50999 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
8	0.673688	194.158.214.137	192.168.1.11	TCP	66 http(80) → 50999 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
9	0.673798	192.168.1.11	194.158.214.137	TCP	54 50999 → http(80) [ACK] Seq=1 Ack=1 Win=131072 Len=0
10	0.674042	192.168.1.11	194.158.214.137	HTTP	368 GET /roots/dstrootcax3.p7c HTTP/1.1
11	0.700155	194.158.214.137	192.168.1.11	TCP	66 [TCP Out-Of-Order] http(80) → 50999 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
12	0.700182	192.168.1.11	194.158.214.137	TCP	66 [TCP Dup ACK 9#1] 50999 → http(80) [ACK] Seq=315 Ack=1 Win=131072 Len=0 SLE=0 SRE=1
13	0.701260	194.158.214.137	192.168.1.11	TCP	54 http(80) → 50999 [ACK] Seq=1 Ack=315 Win=64128 Len=0
14	0.703257	194.158.214.137	192.168.1.11	HTTP	1460 HTTP/1.1 200 OK
15	0.706387	194.158.214.137	192.168.1.11	TCP	54 [TCP Dup ACK 13#1] http(80) → 50999 [ACK] Seq=1407 Ack=315 Win=64128 Len=0
16	0.728227	192.168.1.11	a23-74-173-42.deplo…	TCP	66 51000 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17	0.753853	192.168.1.11	194.158.214.137	TCP	54 50999 → http(80) [ACK] Seq=315 Ack=1407 Win=129792 Len=0
18	0.764855	a23-74-173-42.deplo…	192.168.1.11	TCP	66 http(80) → 51000 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
19	0.764967	192.168.1.11	a23-74-173-42.deplo…	TCP	54 51000 → http(80) [ACK] Seq=1 Ack=1 Win=131072 Len=0
20	0.765117	192.168.1.11	a23-74-173-42.deplo…	HTTP	343 GET / HTTP/1.1
21	0.803214	a23-74-173-42.deplo…	192.168.1.11	TCP	54 http(80) → 51000 [ACK] Seq=1 Ack=290 Win=64128 Len=0
22	0.804977	a23-74-173-42.deplo…	192.168.1.11	TCP	1466 http(80) → 51000 [ACK] Seq=1 Ack=290 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
23	0.805876	a23-74-173-42.deplo…	192.168.1.11	HTTP	406 HTTP/1.1 200 OK (application/pkix-cert)
24	0.805918	192.168.1.11	a23-74-173-42.deplo…	TCP	54 51000 → http(80) [ACK] Seq=290 Ack=1765 Win=131072 Len=0
25	0.806511	a23-74-173-42.deplo…	192.168.1.11	TCP	54 [TCP Dup ACK 21#1] http(80) → 51000 [ACK] Seq=1765 Ack=290 Win=64128 Len=0
26	0.830150	192.168.1.11	a23-74-173-42.deplo…	TCP	66 51001 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
27	0.869006	a23-74-173-42.deplo…	192.168.1.11	TCP	66 http(80) → 51001 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
28	0.869128	192.168.1.11	a23-74-173-42.deplo…	TCP	54 51001 → http(80) [ACK] Seq=1 Ack=1 Win=131072 Len=0
29	0.869334	192.168.1.11	a23-74-173-42.deplo…	HTTP	343 GET / HTTP/1.1
30	0.909646	a23-74-173-42.deplo…	192.168.1.11	TCP	54 http(80) → 51001 [ACK] Seq=1 Ack=290 Win=64128 Len=0
31	0.910317	a23-74-173-42.deplo…	192.168.1.11	TCP	54 [TCP Dup ACK 30#1] http(80) → 51001 [ACK] Seq=1 Ack=290 Win=64128 Len=0
32	0.911925	a23-74-173-42.deplo…	192.168.1.11	TCP	1466 http(80) → 51001 [ACK] Seq=1 Ack=290 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
33	0.912590	a23-74-173-42.deplo…	192.168.1.11	HTTP	307 HTTP/1.1 200 OK (application/pkix-cert)

2) src port 443 and udp and not arp



1	0.000000	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Handshake, SCID=f9db21bb0f39cc3d
2	0.000628	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	850 Protected Payload (KP0)
3	0.000864	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	200 Protected Payload (KP0)
4	0.002132	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	66 Protected Payload (KP0)
5	0.040558	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	162 Protected Payload (KP0)
6	0.050134	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	67 Protected Payload (KP0)
7	0.075470	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	67 Protected Payload (KP0)
8	0.087280	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	67 Protected Payload (KP0)
9	0.111760	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	71 Protected Payload (KP0)
10	0.144270	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	291 Protected Payload (KP0)
11	0.144854	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	63 Protected Payload (KP0)
12	0.206741	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	66 Protected Payload (KP0)
13	0.214825	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	69 Protected Payload (KP0)
14	0.240305	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	65 Protected Payload (KP0)
15	0.366943	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1288 Protected Payload (KP0)
16	0.370417	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
17	0.370417	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
18	0.370417	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
19	0.371898	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
20	0.372433	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	637 Protected Payload (KP0)
21	0.374833	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
22	0.374833	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
23	0.376253	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
24	0.376287	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	305 Protected Payload (KP0)
25	0.405272	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
26	0.407367	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
27	0.408852	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	1292 Protected Payload (KP0)
28	0.911089	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	69 Protected Payload (KP0)
29	0.922899	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	69 Protected Payload (KP0)
30	0.940151	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	69 Protected Payload (KP0)
31	0.942344	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	110 Protected Payload (KP0)
32	0.942826	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	63 Protected Payload (KP0)
33	0.952719	waw07s05-in-f14.1e1…	192.168.1.11	QUIC	79 Protected Payload (KP0)

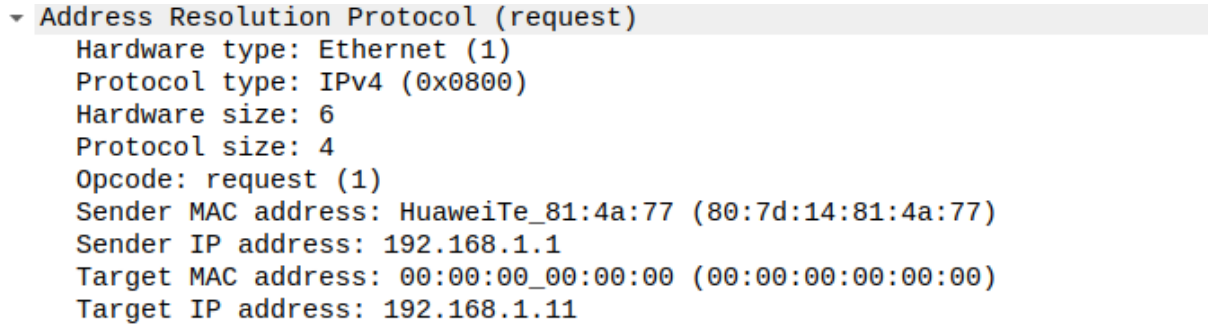
3) udp or icmp and not tcp



24	0.982552	192.168.1.11	192.168.1.1	DNS	95 Standard query 0x32f3 PTR 1.1.168.192.in-addr.arpa OPT
25	1.022325	192.168.1.1	192.168.1.11	DNS	173 Standard query response 0xc109 No such name PTR 11.1.168.192.in-addr.arpa SOA prisoner.iana.org OPT
26	1.026676	192.168.1.1	192.168.1.11	DNS	172 Standard query response 0x32f3 No such name PTR 1.1.168.192.in-addr.arpa SOA prisoner.iana.org OPT
27	5.074312	192.168.1.6	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
28	5.981866	192.168.1.11	192.168.1.1	DNS	95 Standard query 0xcdda PTR 6.1.168.192.in-addr.arpa OPT
29	5.982022	192.168.1.11	192.168.1.1	DNS	99 Standard query 0x4751 PTR 250.255.255.239.in-addr.arpa OPT
30	6.026669	192.168.1.1	192.168.1.11	DNS	172 Standard query response 0xcdda No such name PTR 6.1.168.192.in-addr.arpa SOA prisoner.iana.org OPT
31	6.028337	192.168.1.1	192.168.1.11	DNS	156 Standard query response 0x4751 No such name PTR 250.255.255.239.in-addr.arpa SOA sns.dns.icann.org OPT
32	6.075328	192.168.1.6	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
33	7.001660	192.168.1.11	192.168.1.1	DNS	73 Standard query 0x2f58 A cloud.mail.ru
34	7.001908	192.168.1.11	192.168.1.1	DNS	73 Standard query 0xd433 HTTPS cloud.mail.ru
35	7.028300	192.168.1.11	play.google.com	QUIC	1292 Initial, DCID=0aa5529452268dfe, PKN: 1, CRYPTO, PING, PADDING, PING, PING, PADDING, PING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PA…
36	7.028521	192.168.1.11	play.google.com	QUIC	121 0-RTT, DCID=0aa5529452268dfe
37	7.076001	192.168.1.6	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
38	7.076700	192.168.1.1	192.168.1.11	DNS	89 Standard query response 0x2f58 A cloud.mail.ru A 95.163.57.16
39	7.077084	192.168.1.1	192.168.1.11	DNS	124 Standard query response 0xd433 HTTPS cloud.mail.ru SOA ns1.mail.ru
40	7.119190	play.google.com	192.168.1.11	QUIC	1292 Handshake, SCID=eaa5529452268dfe
41	7.119618	192.168.1.11	play.google.com	QUIC	120 Handshake, DCID=eaa5529452268dfe
42	7.119848	play.google.com	192.168.1.11	QUIC	846 Protected Payload (KP0)
43	7.119885	play.google.com	192.168.1.11	QUIC	204 Protected Payload (KP0)
44	7.119893	192.168.1.11	play.google.com	QUIC	1288 Protected Payload (KP0), DCID=eaa5529452268dfe
45	7.119956	192.168.1.11	play.google.com	QUIC	1292 Protected Payload (KP0), DCID=eaa5529452268dfe
46	7.120047	192.168.1.11	play.google.com	QUIC	914 Protected Payload (KP0), DCID=eaa5529452268dfe
47	7.120100	192.168.1.11	play.google.com	QUIC	357 Protected Payload (KP0), DCID=eaa5529452268dfe
48	7.120213	192.168.1.11	play.google.com	QUIC	73 Protected Payload (KP0), DCID=eaa5529452268dfe
49	7.129929	play.google.com	192.168.1.11	QUIC	66 Protected Payload (KP0)
50	7.188930	play.google.com	192.168.1.11	QUIC	162 Protected Payload (KP0)
51	7.191198	play.google.com	192.168.1.11	QUIC	67 Protected Payload (KP0)
52	7.191332	play.google.com	192.168.1.11	QUIC	67 Protected Payload (KP0)
53	7.199056	play.google.com	192.168.1.11	QUIC	67 Protected Payload (KP0)
54	7.204202	play.google.com	192.168.1.11	QUIC	71 Protected Payload (KP0)
55	7.204361	192.168.1.11	play.google.com	QUIC	73 Protected Payload (KP0), DCID=eaa5529452268dfe
56	7.240741	play.google.com	192.168.1.11	QUIC	291 Protected Payload (KP0)

6. Выполнить анализ ARP-протокола по примеру из методических указаний.

3	0.024677001	HuaweiTe_81:4a:77		ARP	44 Who has 192.168.1.11? Tell 192.168.1.1
4	0.024696119	CloudNet_10:1a:57		ARP	44 192.168.1.11 is at 30:03:c8:10:1a:57
5	0.181237188	CloudNet_10:1a:57		ARP	44 Who has 192.168.1.1? Tell 192.168.1.11
6	0.200923530	HuaweiTe_81:4a:77		ARP	44 192.168.1.1 is at 80:7d:14:81:4a:77
49	10.036025073	HuaweiTe_81:4a:77		ARP	62 Who has 192.168.1.17? Tell 192.168.1.1
58	10.138375949	HuaweiTe_81:4a:77		ARP	62 Who has 192.168.1.17? Tell 192.168.1.1
71	13.749620094	CloudNet_10:1a:57		ARP	44 Who has 192.168.1.8? Tell 192.168.1.11
72	13.824839518	ASRockIn_5a:10:e2		ARP	62 192.168.1.8 is at a8:a1:59:5a:10:e2
93	16.384551679	ASRockIn_5a:10:e2		ARP	62 Who has 192.168.1.11? Tell 192.168.1.8
94	16.384570987	CloudNet_10:1a:57		ARP	44 192.168.1.11 is at 30:03:c8:10:1a:57



```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiTe_81:4a:77 (80:7d:14:81:4a:77)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.11
```

Hardware Type: Тип сетевого адаптера. Значение - Ethernet(1)

Protocol Type: Тип протокола, для которого выполняется разрешение адресов. Значение - IPv4(0x0800).

Hardware size: Длина аппаратного адреса. Значение - 6.

Protocol size: Длина сетевого адрес. Значение - 4

Opcode: Операция, выполняемая в ARP-запросе или ARP-ответе. Значение – request(запрос).

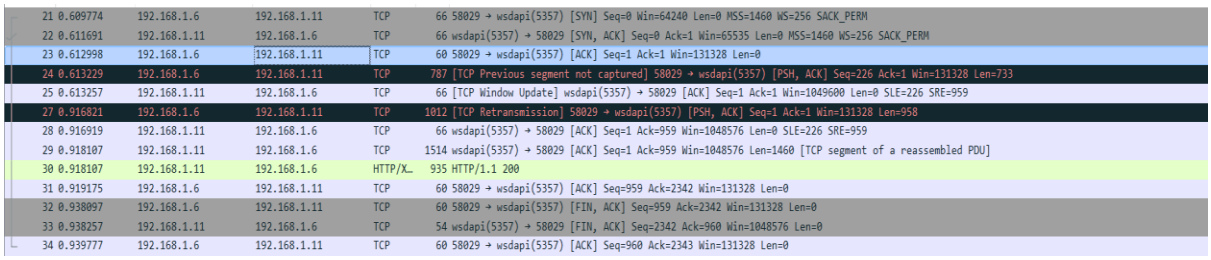
Sender MAC Address: MAC-адрес отправителя. Значение – 80:7d:14:81:4a:77

Sender IP Address: IP-адрес отправителя. Значение – 192.168.1.1

Target MAC Address: MAC-адрес целевого узла. Значение – отсутствует

Target IP Address: IP-адрес целевого узла. Значение – 192.168.1.11

7. Выполнить анализ TCP-сеансов по примеру из методических указаний



21	0.609774	192.168.1.6	192.168.1.11	TCP	66 58029 → wsdapi(5357) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22	0.611691	192.168.1.11	192.168.1.6	TCP	66 wsdapi(5357) → 58029 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
23	0.612998	192.168.1.6	192.168.1.11	TCP	60 58029 → wsdapi(5357) [ACK] Seq=1 Ack=1 Win=131328 Len=0
24	0.613229	192.168.1.6	192.168.1.11	TCP	787 [TCP Previous segment not captured] 58029 → wsdapi(5357) [PSH, ACK] Seq=226 Ack=1 Win=131328 Len=733
25	0.613257	192.168.1.11	192.168.1.6	TCP	66 [TCP Window Update] wsdapi(5357) → 58029 [ACK] Seq=1 Ack=1 Win=1049600 Len=0 SLE=226 SRE=959
27	0.916821	192.168.1.6	192.168.1.11	TCP	1012 [TCP Retransmission] 58029 → wsdapi(5357) [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=958
28	0.916919	192.168.1.11	192.168.1.6	TCP	66 wsdapi(5357) → 58029 [ACK] Seq=1 Ack=959 Win=1048576 Len=0 SLE=226 SRE=959
29	0.918107	192.168.1.11	192.168.1.6	TCP	1514 wsdapi(5357) → 58029 [ACK] Seq=1 Ack=959 Win=1048576 Len=1460 [TCP segment of a reassembled PDU]
30	0.918107	192.168.1.11	192.168.1.6	HTTP/X…	935 HTTP/1.1 200
31	0.919175	192.168.1.6	192.168.1.11	TCP	60 58029 → wsdapi(5357) [ACK] Seq=959 Ack=2342 Win=131328 Len=0
32	0.938097	192.168.1.6	192.168.1.11	TCP	60 58029 → wsdapi(5357) [FIN, ACK] Seq=959 Ack=2342 Win=131328 Len=0
33	0.938257	192.168.1.11	192.168.1.6	TCP	54 wsdapi(5357) → 58029 [FIN, ACK] Seq=2342 Ack=960 Win=1048576 Len=0
34	0.939777	192.168.1.6	192.168.1.11	TCP	60 58029 → wsdapi(5357) [ACK] Seq=960 Ack=2343 Win=131328 Len=0

Первые 3 пакета с флагами (SYN), (SYN,ACK),(ACK) создают TCP сессию. Следующие 7 пакетов отправляют данные. Последние 3 пакета с флагами (FIN,ACK), (FIN,ACK), (ACK) закрывают TCP сессию.

Вывод: приобрели навыки анализа сетевого трафика компьютерных сетей; изучили структуры сетевых протоколов различных уровней