ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Компьютерные сети
Лабораторная №3

Выполнил:
Беляков Дмитрий
Группа:
P33122
Преподаватель:
Маркина Т. А.

Санкт-Петербург
2021

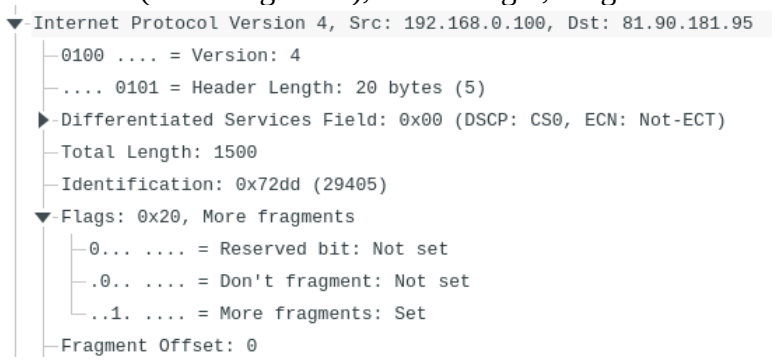
Цель работы: изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark.

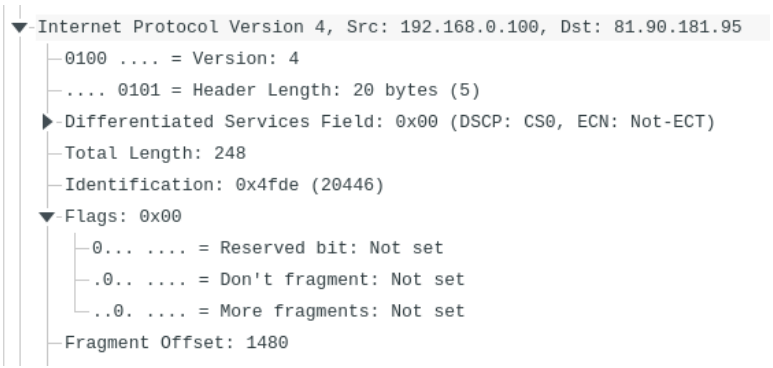
Вариант: www.доктор-беляков.рф (IP: 81.90.181.95)

1. Анализ трафика утилиты ping

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

Да, фрагментация происходит на уровне сетевом уровне (IP), заметить это можно по следующим флагам:
Флаг MF (more fragments), Total Length, Fragment Offset





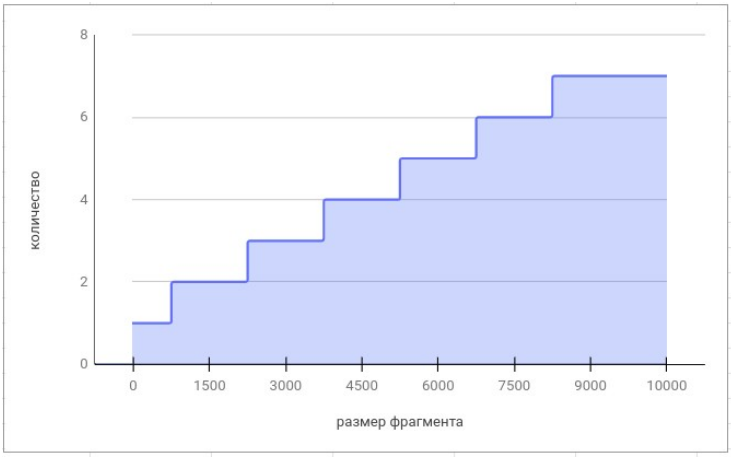
2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

Как можем видеть из предыдущих картинок, где указаны 2 последовательных кадра (при размере пакета = 1700 байт) — первый и последний, флаг, который указывает на промежуточный пакет — MF = 1, если это промежуточный, MF = 0, если фрагмент является последним.

3. Чему равно количество фрагментов при передаче ping-пакетов?

Примерно размер_пакета/размер_фрагмента, для сетей ethernet = 1500 (надо ещё учитывать заголовки протоколов)

4. Построить график, в котором на оси абсцисс находится размер_пакета, а по оси ординат - количество фрагментов, на которое был разделён каждый ping-пакет.



5. Как изменить поле TTL с помощью утилиты ping?

Установить флаг «i»

6. Что содержится в поле данных ping-пакета?

Повторяющиеся комбинации в виде:

```
00 00 ed ce 05 00 00 00  00 00 10 11 12 13 14 15  ........ ........
16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25  ........ .. !"#$%
26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
36 37 38 39 3a 3b 3c 3d  3e 3f 40 41 42 43 44 45  6789:;<= >?@ABCDE
46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
56 57 58 59 5a 5b 5c 5d  5e 5f 60 61 62 63 64 65  VWXYZ[\] ^_`abcde
66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
76 77 78 79 7a 7b 7c 7d  7e 7f 80 81 82 83 84 85  vwxyz{|} ~·······
86 87 88 89 8a 8b 8c 8d  8e 8f 90 91 92 93 94 95  ........ ........
```

2. Анализ трафика утилиты tracert (traceroute)

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?

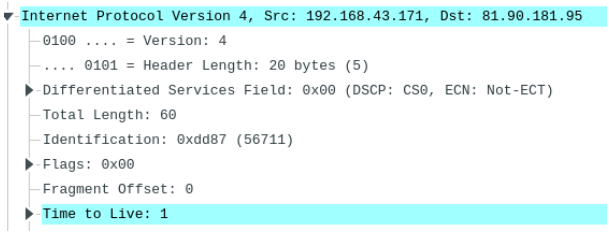
В заголовке IP - 20 байт. В поле данных содержится 32 байта

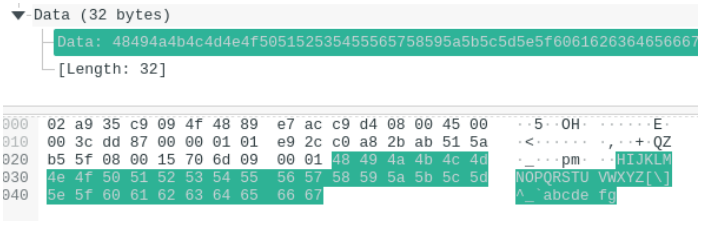
2. Как и почему изменяется поле TTL в следующих друг за другом ICMP-пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

Если сообщение не дошло до адреса назначения, промежуточный узел отправит ICMP-сообщение об окончании жизни пакета, в таком случае traceroute увеличит TTL на 1.

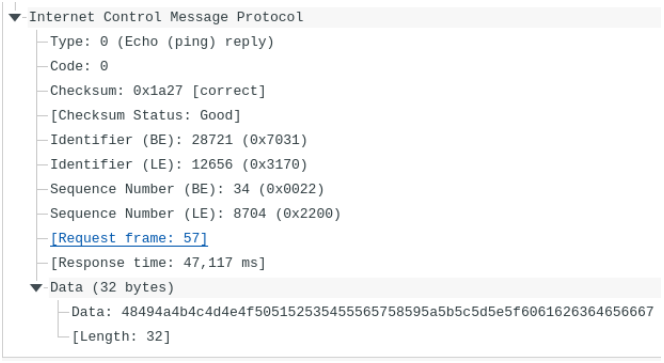
3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP-пакетов, генерируемых утилитой ping (см. предыдущее задание).

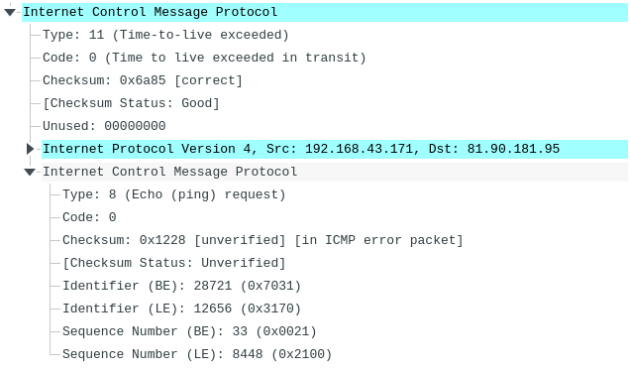
Данными (их размер), а так же значением TTL.





4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?





Когда TTL в ходе определения пути уменьшается и достигает значение 0, узел, получивший такое сообщение отправляет «ICMP error», что означает, что сообщение не дошло. В случае, когда сообщение достигает адреса назначения, узел генерирует сообщение «ICMP reply».

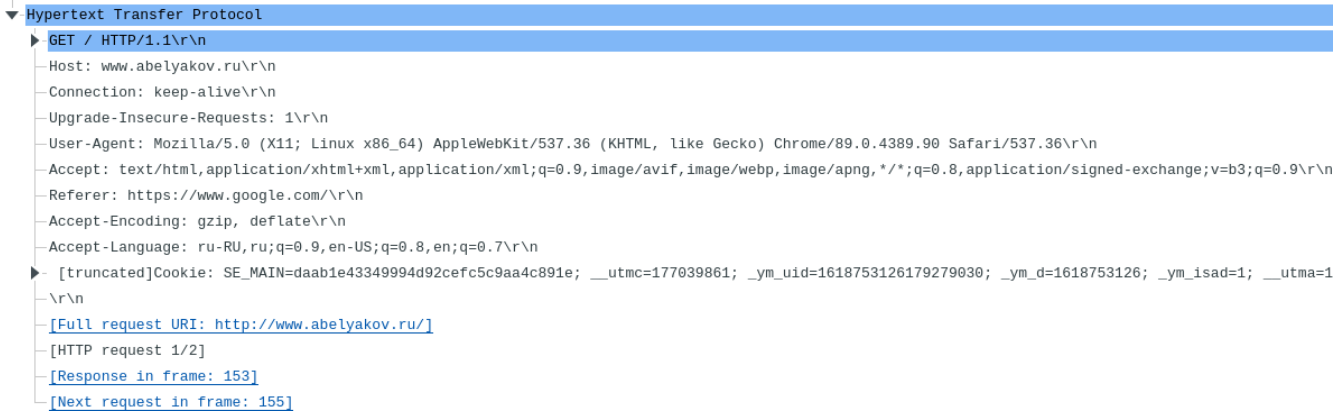
5. Что изменится в работе tracert, если убрать ключ “-d”? Какой дополнительный трафик при этом будет генерироваться?

'-d' - Останавливает попытки разрешения IP-адресов промежуточных маршрутизаторов в имена, что может ускорить возврат результатов.

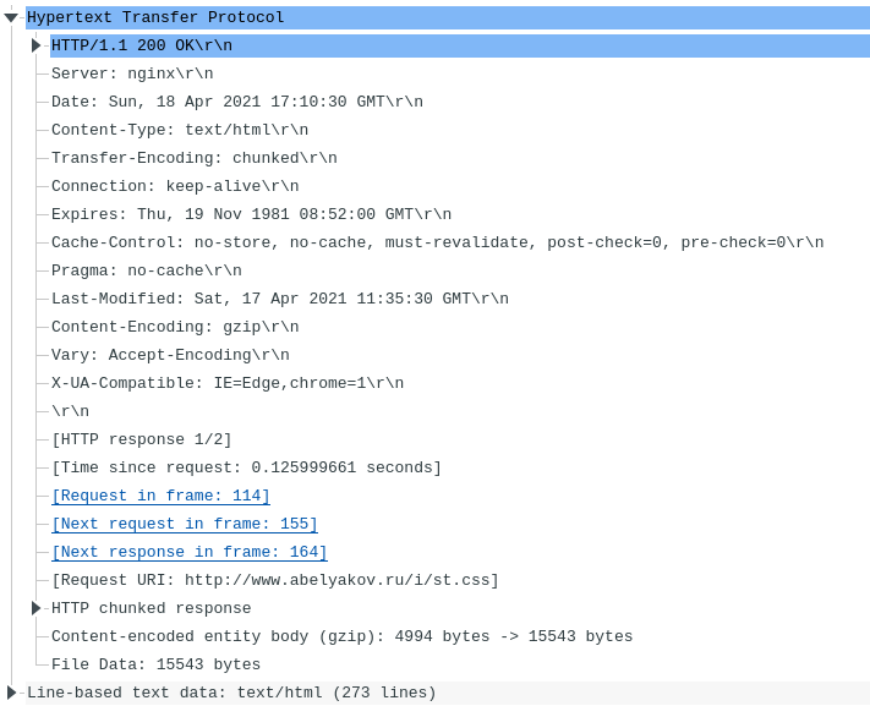
3. Анализ HTTP-трафика

По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т.е. при различных видах GET-запросов).

Первый HTTP-запрос

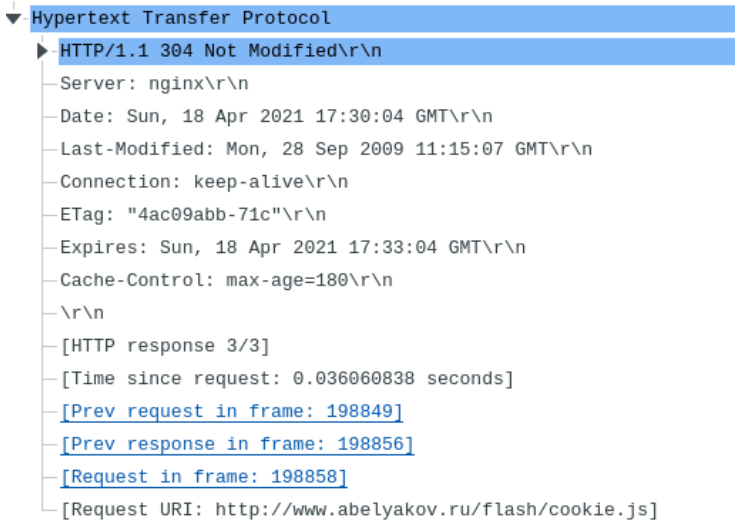


HTTP-ответ



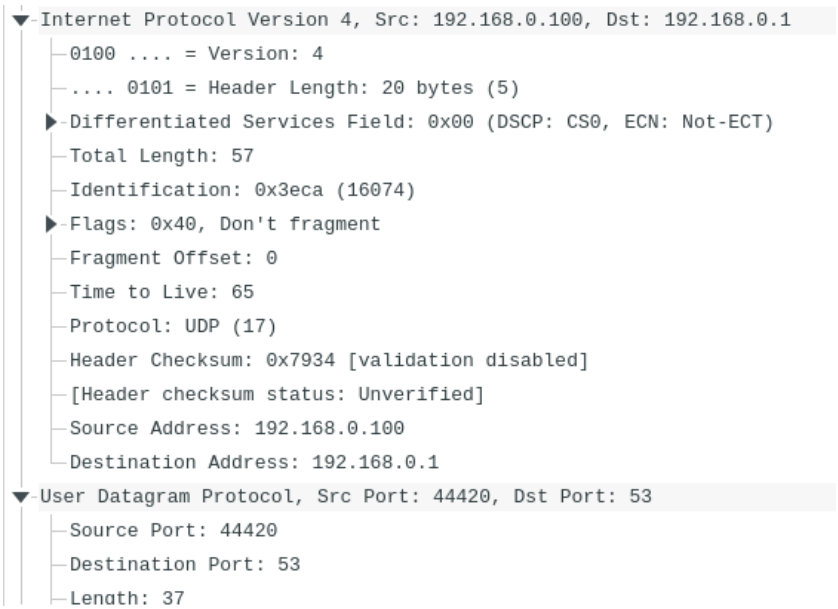
Повтороный HTTP-запрос

HTTP-ответ



4. Анализ DNS-трафика

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?



Потому что запрос отправляется на DNS сервер

2. Какие бывают типы DNS-запросов?

- Итеративные: посылается запрос к DNS-серверу и запрашивается либо IP-адрес домена, либо имя DNS-сервера, ответственного за этот домен.
- Рекурсивный: посылается запрос к DNS-серверу и запрашивается IP-адрес домена, DNS-сервер может обращаться к другим DNS-серверам
- Обратный запрос: посылается запрос к DNS-серверу и запрашивается IP-адрес домена

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Если в источнике изображения указан сторонний домен

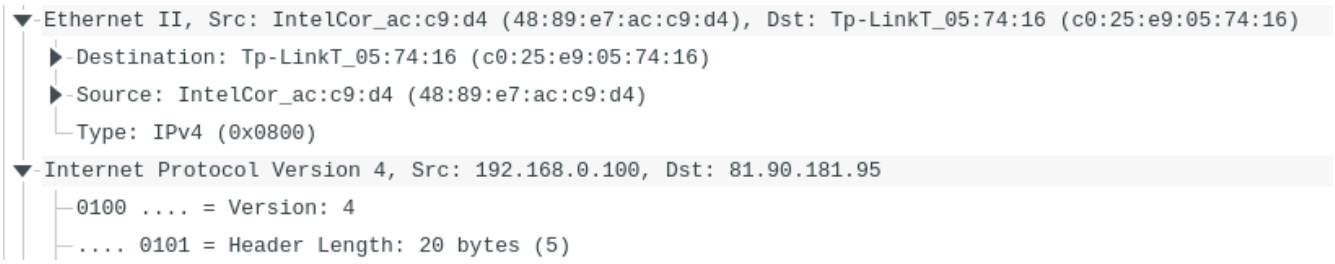
5. Анализ ARP-трафика

1. Какие MAC-адреса присутствуют в захваченных пакетах ARP-протокола? Что означают эти адреса? Какие устройства они идентифицируют?

В запросе:
MAC-адрес ноутбука — отправителя (IntelCor), а так же широковещательный адрес- адрес получателя, так как после очистки кэша нам известен только IP, а не MAC-адрес.

В ответе:
MAC-адрес ноутбука в получателях и MAC-адрес роутера в отправителях

2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?



48:89:e7:ac:c9:d4 – MAC-адрес сетевой карты ноутбука
c0:25:e9:05:74:16 – MAC-адрес роутера

3. Для чего ARP-запрос содержит IP-адрес источника?

Чтобы знать, куда куда отправлять ответ.

6. Анализ трафика утилиты nslookup

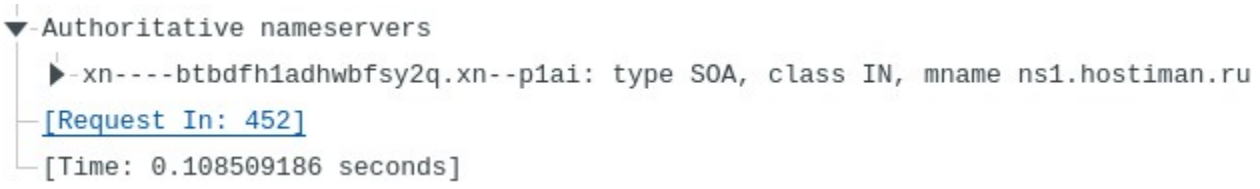
1. Чем различается трасса трафика в п.2 и п.4, указанных выше?

В п.2 возвращаются имена авторитативных серверов, а во 4 — IP-адрес домена.

2. Что содержится в поле «Answers» DNS-ответа?

Имя хоста, тип записи, класс записи, время жизни записи, размер данных и запрашиваемый адрес хоста/имя авторитарного сервера.

3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?
ns1.hostiman.ru



7. Анализ FTP-трафика

ftp://iso.netbsd.org

1. Сколько байт данных содержится в пакете FTP-DATA?

1388

2. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?

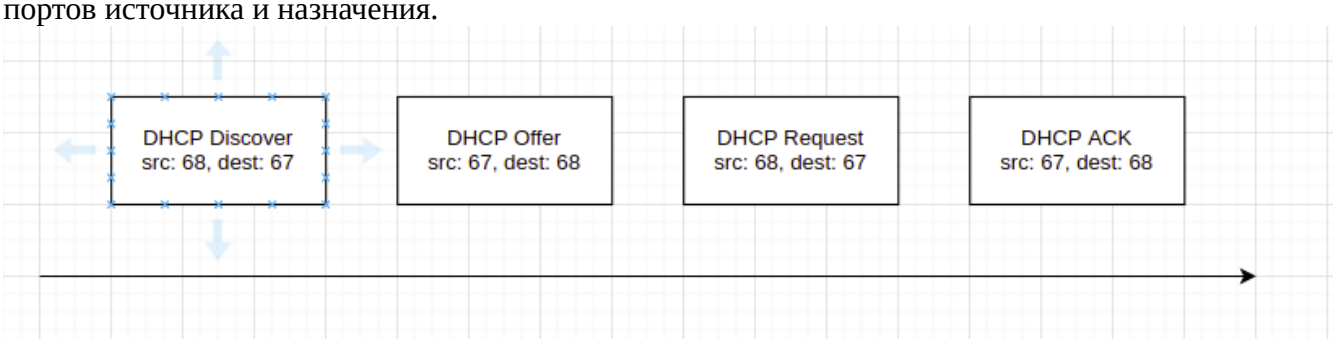
Клиент обычно динамически выбирает порт для передачи данных. Для стороны сервера — 21 — управляющий порт, 20 — порт передачи данных.

3. Чем отличаются пакеты FTP от FTP-DATA?

FTP — передача команд, FTP-DATA — передача данных.

8. Анализ DHCP-трафика

Нарисуйте временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя DHCP-пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номера портов источника и назначения.

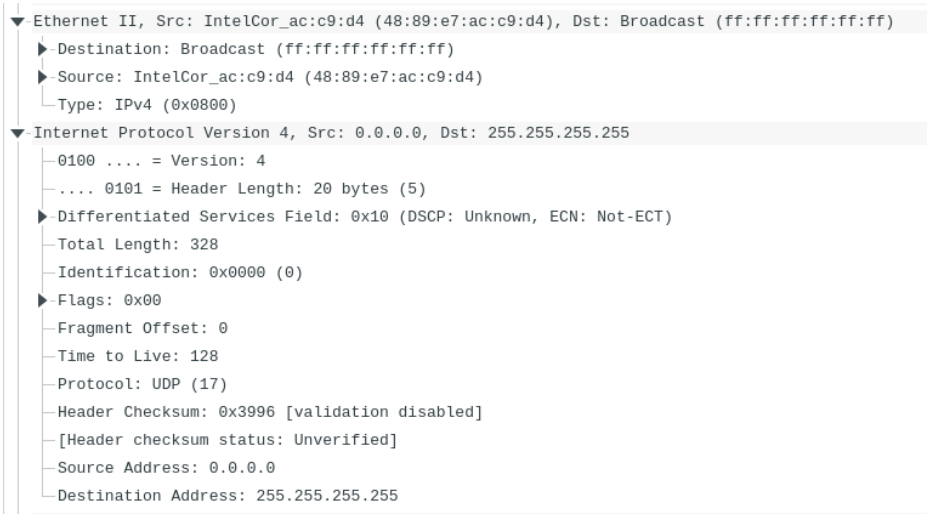


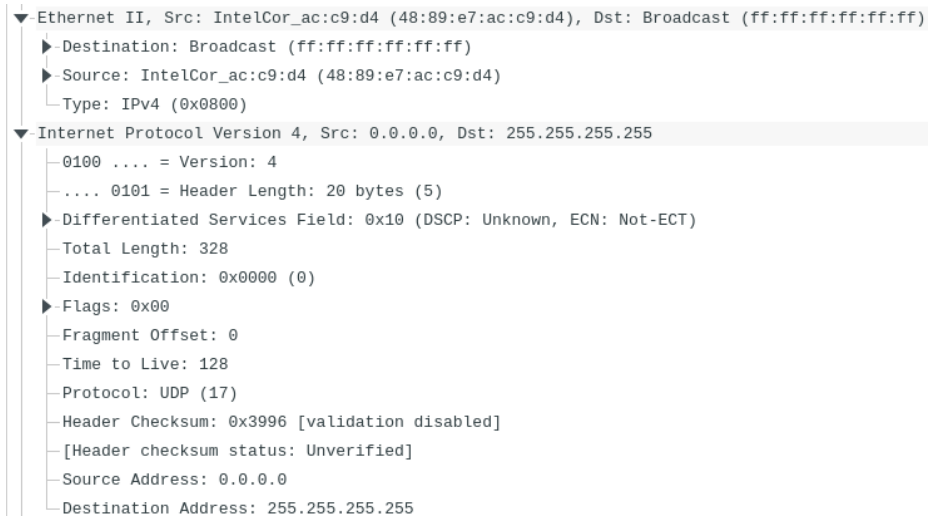
1. Чем различаются пакеты «DHCP Discover» и «DHCP Request»?

Изначально клиент, не имея собственного IP-адреса, посылает широковещательный запрос с целью обнаружить DHCP-серверы и получить от них IP-адрес (Discover). Когда клиент подтверждает предложенный DHCP-сервером адрес — он отправляет Request с идентификатором сервера.

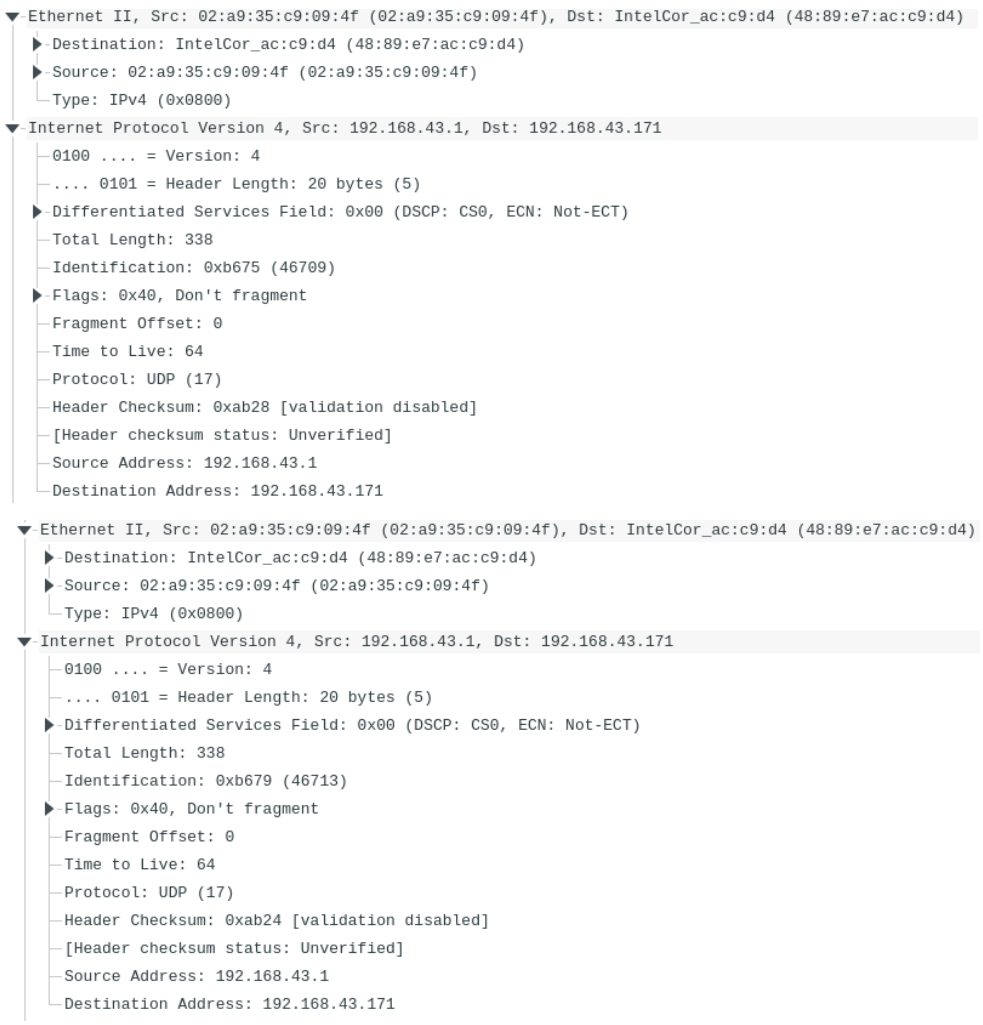
2. Как и почему менялись MAC- и IP-адреса источника и назначения в переданных DHCP-пакетах.

При отправке Discover и Request адрес источника «0.0.0.0» так как клиенту ещё не присвоен IP-адрес, MAC-адрес источника — адрес сетевой платы ноутбука. IP-адрес назначения и MAC-адрес — широковещательные, так как адрес DHCP-сервера неизвестны.





При отправке Offer, ACK — IP и MAC-адреса — DHCP-сервера, IP-адрес назначения — предполагаемый/подтверждённый адрес, MAC-адрес — адрес сетевой платы ноутбука.



3. Каков IP-адрес DHCP-сервера?

192.168.43.1

4. Что произойдёт, если очистить использованный фильтр “bootp”?

Фильтров не будет → мы увидим все захваченные пакеты.

9. Анализ трафика приложения Discord

Текстовые сообщения:

1	0.000000000	192.168.43.171	162.159.128.233	TLSv1.2	151	Application Data
2	0.000197408	192.168.43.171	162.159.128.233	TLSv1.2	185	Application Data, Application Data
3	0.085349407	162.159.128.233	192.168.43.171	TCP	54	443 → 58570 [ACK] Seq=1 Ack=98 Win=121 Len=0
4	0.085420653	162.159.128.233	192.168.43.171	TCP	54	443 → 58570 [ACK] Seq=1 Ack=229 Win=123 Len=0
5	0.086961520	162.159.128.233	192.168.43.171	TLSv1.2	93	Application Data
6	0.086996901	192.168.43.171	162.159.128.233	TCP	54	58570 → 443 [ACK] Seq=229 Ack=40 Win=3858 Len=0
7	0.372112460	162.159.134.234	192.168.43.171	TLSv1.2	134	Application Data
8	0.372161078	192.168.43.171	162.159.134.234	TCP	54	40896 → 443 [ACK] Seq=1 Ack=81 Win=501 Len=0
9	0.372234764	162.159.128.233	192.168.43.171	TLSv1.2	717	Application Data
10	0.372255912	192.168.43.171	162.159.128.233	TCP	54	58570 → 443 [ACK] Seq=229 Ack=703 Win=3880 Len=0
11	0.375948538	162.159.128.233	192.168.43.171	TLSv1.2	85	Application Data
12	0.376000288	192.168.43.171	162.159.128.233	TCP	54	58570 → 443 [ACK] Seq=229 Ack=734 Win=3880 Len=0

Как мы видим сообщения передаются по протоколу TLS, который является транспортным защищенным протоколом, поэтому содержимое не сможем посмотреть.

Аудио-сеанс

519	10.170646241	188.122.65.159	192.168.43.171	UDP	175 50004 → 34979 Len=133
520	10.177835068	192.168.43.171	188.122.65.159	UDP	200 34979 → 50004 Len=158
521	10.187463072	188.122.65.159	192.168.43.171	UDP	183 50004 → 34979 Len=141
522	10.198880384	192.168.43.171	188.122.65.159	UDP	169 34979 → 50004 Len=127
523	10.200612786	192.168.43.171	188.122.65.159	RTCP	94 Receiver Report
524	10.214554969	192.168.43.171	188.122.65.159	UDP	160 34979 → 50004 Len=118
525	10.220150344	188.122.65.159	192.168.43.171	UDP	174 50004 → 34979 Len=132
526	10.240687889	192.168.43.171	188.122.65.159	UDP	85 34979 → 50004 Len=43
527	10.253058542	188.122.65.159	192.168.43.171	UDP	180 50004 → 34979 Len=138
528	10.253588569	188.122.65.159	192.168.43.171	UDP	171 50004 → 34979 Len=129
529	10.256271117	192.168.43.171	188.122.65.159	UDP	85 34979 → 50004 Len=43
530	10.258647633	192.168.43.171	162.159.130.235	TLSv1.2	140 Application Data
531	10.278583320	192.168.43.171	188.122.65.159	UDP	85 34979 → 50004 Len=43
532	10.298492415	162.159.130.235	192.168.43.171	TCP	54 443 → 51434 [ACK] Seq=4865 Ack=2724 Win=71680 Len=0
533	10.299435666	192.168.43.171	188.122.65.159	UDP	85 34979 → 50004 Len=43
534	10.299748370	188.122.65.159	192.168.43.171	UDP	176 50004 → 34979 Len=134
535	10.299855849	188.122.65.159	192.168.43.171	UDP	178 50004 → 34979 Len=136
536	10.313346485	188.122.65.159	192.168.43.171	UDP	172 50004 → 34979 Len=130
537	10.320408165	192.168.43.171	188.122.65.159	UDP	85 34979 → 50004 Len=43

Аудио-сеанс осуществлялся с помощью UDP -данных, TLS — служебные данные, RTCP — протокол, который используется для передачи информации о потерях медиа-пакетов, уровне звукого сигнала и пр.

Видео-сеанс

3132	17.593522694	192.168.43.171	188.122.65.156	UDP	1205 48315 → 50004 Len=1163
3133	17.593608228	192.168.43.171	188.122.65.156	UDP	1205 48315 → 50004 Len=1163
3134	17.593642597	192.168.43.171	188.122.65.156	UDP	1205 48315 → 50004 Len=1163
3135	17.604131237	192.168.43.171	188.122.65.156	UDP	177 48315 → 50004 Len=135
3136	17.617447505	192.168.43.171	188.122.65.156	RTCP	102 Sender Report
3137	17.619080340	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3138	17.619244942	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3139	17.619292728	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3140	17.619323100	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3141	17.619348835	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3142	17.619371969	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3143	17.619393988	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3144	17.623529233	192.168.43.171	188.122.65.156	UDP	85 48315 → 50004 Len=43
3145	17.623733150	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3146	17.623817348	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3147	17.623884750	192.168.43.171	188.122.65.156	UDP	1170 48315 → 50004 Len=1128
3148	17.625916337	188.122.65.156	192.168.43.171	UDP	189 50004 → 48315 Len=147
3149	17.633719935	188.122.65.156	192.168.43.171	UDP	192 50004 → 48315 Len=150
3150	17.644764454	192.168.43.171	188.122.65.156	UDP	85 48315 → 50004 Len=43
3151	17.646490529	192.168.43.171	162.159.138.234	TLSv1.2	140 Application Data
3152	17.647893379	188.122.65.156	192.168.43.171	UDP	189 50004 → 48315 Len=147
3153	17.650429147	192.168.43.171	188.122.65.156	UDP	1148 48315 → 50004 Len=1106

Аналогично адио-сеансу

1. Чем различаются пакета разных видов discord-трафика (текст, аудио, видео)?

Текст передаётся только через TLS, аудио и видео данные через RTCP, TLS + UDP.

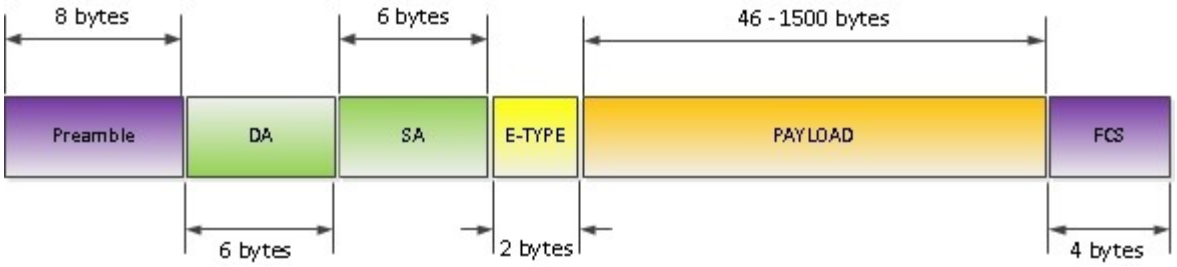
2. Какой Wireshark-фильтр следует использовать для независимой идентификации discord-трафика разных видов (текст, аудио, видео)?

Для идентификации аудио и видео можно использовать RTCP || TLS || UDP, однако это всё равно требует информацию о том аудио это или видео.

Структуры наблюдаемых пакетов

Ethernet II

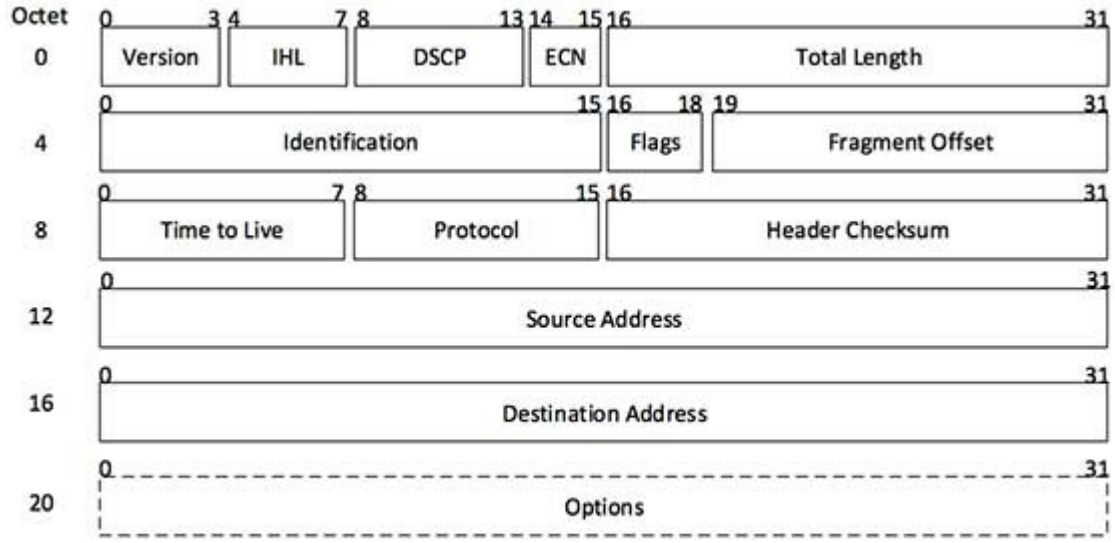
Данный протокол отвечает за физическую адресацию. Содержит MAC-адреса источника и назначения.



Preamble – последовательность бит, определяющая начало Ethernet фрейма.
DA — destination MAC-адрес
SA — source MAC-адрес
E-TYPE это двухбайтовое поле в заголовке ethernet кадра, которое содержит информацию о типе протокола инкапсулированных в данный кадр данных.
Payload – L3 пакет размером от 46 до 1500 байт
FCS (Frame Check Sequences) – 4 байтное значение CRC используемое для выявления ошибок передачи.

Internet Protocol Version 4

Данный протокол отвечает за определение маршрута и логическую адресацию. Содержит IP адреса источника и приемника.



[Image: IP Header]

Version — версия протокола
IHL - Internet Header Length — так как Options не является обязательным, используется данное поле для указания длины
DSCP (Differentiated Services Code Point), это поле используется для разделения трафика на классы обслуживания.
ECN (Explicit Congestion Notification) или указатель перегрузки, используется, когда пропускная способность канала связи меньше, чем трафик, который в текущий момент передается по каналу.
Total Length — размер заголовока + данные
Identification — используется при фрагментации, чтобы понимать, в каком порядке собирать пакеты
Flags:

- нулевой бит зарезервирован и должен быть всегда равен нулю;
- если значение первого бита ноль, то допускается фрагментация пакетов, если единица (бит DF или Do not Fragment), то устройства компьютерной сети не будут выполнять фрагментацию;
- второй бит служит для того, чтобы конечные узлы понимали, где начинается последовательность фрагментированных пакетов, а где она заканчивается, если значение этого бита равно единице (MF More Fragments), то узел понимает, что этот пакет не последний и нужно ждать еще пакеты, чтобы собрать изначально разделенный пакет.

Fragment Offset — используется при фрагментации, чтобы определять смещение относительно первого фрагмента.
Time to Live, TTL — максимальное кол-во пройденных узлов, уменьшается на 1 при прохождении узла (ещё операторы любят им ограничивать раздачу трафика)
Protocol — так как IP используется протоколами транспортного уровня, при получении такого пакета надо понимать, какому обрабочику отдавать эти пакеты, указывает на протоколы транспортного уровня.
Header Checksum — контрольная сумма.
Addresses — IP — адреса назначения и источника
Options — необязательное поле

TCP

Протокол транспортного уровня, обеспечивает надежную доставку с установлением соединения.

Бит	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт источника, **Source Port**			Порт назначения, **Destination Port**
32	Порядковый номер, **Sequence Number (SN)**			
64	Номер подтверждения, **Acknowledgment Number (ACK SN)**			
96	Длина заголовка	Зарезервировано	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции (необязательное, но используется практически всегда)			
160/192+	Данные			

Порт источника, порт приёмника.
Номер в последовательности - положение данных TCP-пакета внутри исходящего потока данных, существующего в рамках текущего логического соединения.

Acknowledgment Number (ACK SN) (32 бита) - если установлен бит ACK, то это поле содержит порядковый номер октета, который отправитель данного сегмента желает получить. Это означает, что все предыдущие октеты (с номерами от ISN+1 (Initial Sequence Number) до ACK-1 включительно) были успешно получены.
Длина заголовка (смещение данных) - определяет размер заголовка пакета TCP в 4-байтных словах. Минимальный размер составляет 5 слов, а максимальный — 15, что составляет 20 и 60 байт соответственно. Смещение считается от начала заголовка TCP.
Зарезервировано (6 бит) для будущего использования и должно устанавливаться в ноль. Из них два (5-й и 6-й) уже определены:

- CWR (Congestion Window Reduced) — Поле «Окно перегрузки уменьшено» — флаг установлен отправителем, чтобы указать, что получен пакет с установленным флагом ECE (RFC 3168)
- ECE (ECN-Echo) — Поле «Эхо ECN» — указывает, что данный узел способен на ECN (явное уведомление перегрузки) и для указания отправителю о перегрузках в сети (RFC 3168)

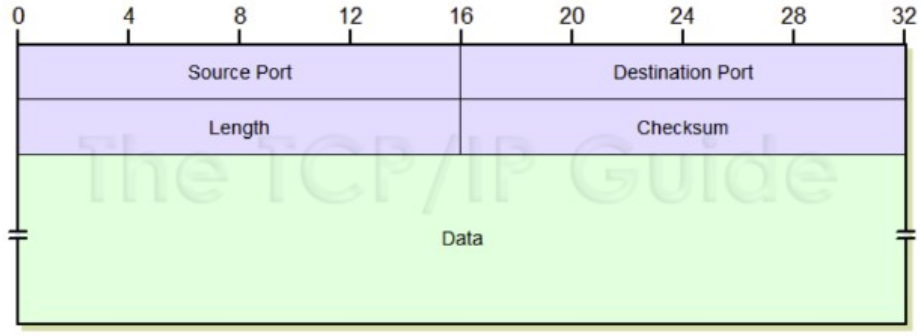
Флаги (управляющие биты):

- URG — поле «Указатель важности» задействовано
- ACK — поле «Номер подтверждения» задействовано
- PSH — инструктирует получателя протолкнуть данные, накопившиеся в приёмном буфере, в приложение пользователя
- RST — оборвать соединения, сбросить буфер
- SYN — синхронизация номеров последовательности
- FIN — флаг, будучи установлен, указывает на завершение соединения

Размер окна
Количество байт данных начиная с последнего номера подтверждения, которые может принять отправитель данного пакета. Иначе говоря, отправитель пакета располагает для приема данных буфером длинной "размер окна" байт.
Контрольная сумма
Опции — расширяют протокол

UDP

Протокол транспортного уровня, не гарантирует доставку, однако данные передаются быстрее, чем при использовании tcp.



ICMP

Протокол межсетевых управляющих сообщений, предназначен для выявления и передачи информации об ошибках приложению.

тип (1 байт) — числовой идентификатор типа сообщения;
код (1 байт) — числовой идентификатор, более тонко дифференцирующий тип ошибки;
контрольная сумма (2 байта) — подсчитывается для всего ICMP-сообщения.
Содержимое оставшихся четырех байтов в заголовке и поле данных зависит от значений полей типа и кода.

ARP

Данный протокол предназначен для определения MAC адреса узла по его IP адресу.

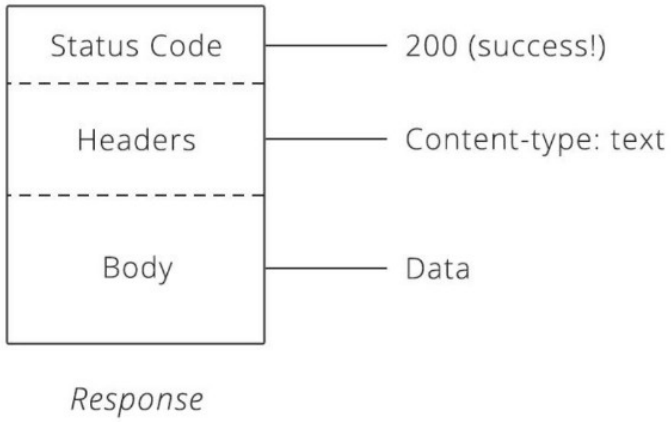
Октет	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	
0	Hardware Type (HTYPE)	Protocol Type (PTYPE)
4	Hardware length (HLEN) | Protocol length (PLEN)	Operation (OPER)
	Sender hardware address (SHA)	
	Sender protocol address (SPA)	
	Target hardware address (THA)	
	Target protocol address (TPA)	

Hardware type (HTYPE) Каждый канальный протокол передачи данных имеет свой номер, который хранится в этом поле. Например, Ethernet имеет номер 0x0001
Protocol type (PTYPE) Код сетевого протокола. Например, для IPv4 будет записано 0x0800
Hardware length (HLEN) Длина физического адреса в байтах. Адреса Ethernet имеют длину 6 байт.
Protocol length (PLEN) Длина логического адреса в байтах. IPv4 адреса имеют длину 4 байта.
Operation Код операции отправителя: 1 в случае запроса и 2 в случае ответа.
Sender hardware address (SHA) Физический адрес отправителя.
Sender protocol address (SPA) Логический адрес отправителя.
Targethardwareaddress (THA) Физический адрес получателя. Поле пусто при запросе.

Target protocol address (TPA) Логический адрес получателя.
HTTP

Запрос

Ответ



DNS

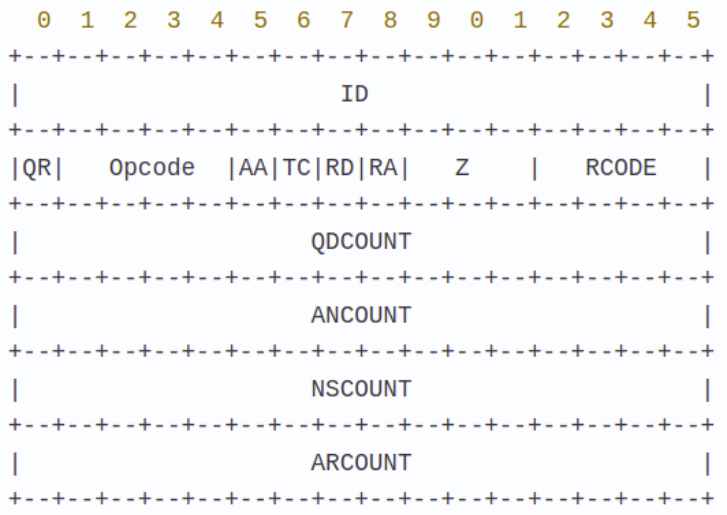
Структура пакета:

```
+---------------------+
|        Header       | Заголовок
+---------------------+
|       Question      | Секция запросов
+---------------------+
|        Answer       | Секция ответа
+---------------------+
|      Authority      | Секция ответа об уполномоченных серверах
+---------------------+
|      Additional     | Секция ответа дополнительных записей
+---------------------+
```

Header — Заголовок DNS пакета, состоящий из 12 октет.
Question section — в этой секции DNS-клиент передает запросы DNS-серверу сообщая о том, для какого имени необходимо разрешить запись DNS, а также какого типа (NS, A, TXT и т.д.). Сервер при ответе, копирует эту информацию и отдает клиенту обратно в этой же секции.

Answer section — сервер сообщает клиенту ответ или несколько ответов на запрос, в котором сообщает вышеуказанные данные.
Authoritative Section — содержит сведения о том, с помощью каких авторитетных серверов было получена информация включенная в секцию DNS-ответа.
Additional Record Section — дополнительные записи, которые относятся к запросу, но не являются строго ответами на вопрос.

Структура заголовка:



ID (16 бит) — данное поле используется как уникальный идентификатор транзакции. Указывает на то, что пакет принадлежит одной и той же сессии “запросов-ответов” и занимает 16 бит.
QR (1 бит) — данный бит служит для индентификации того, является ли пакет запросом (QR = 0) или ответом (QR = 1).
Opcode (4 бита) — с помощью данного кода клиент может указать тип запроса, где обычное значение:
0 — стандартный запрос,
1 — инверсный запрос,
2 — запрос статуса сервера.
3-15 – зарезервированы на будущее.
AA (1 бит) — данное поле имеет смысл только в DNS-ответах от сервера и сообщает о том, является ли ответ авторитетным либо нет.
TC (1 бит) — данный флаг устанавливается в пакете ответе в том случае если сервер не смог поместить всю необходимую информацию в пакет из-за существующих ограничений.
RD (1 бит) — этот однобитовый флаг устанавливается в запросе и копируется в ответ. Если он флаг устанавливается в запросе — это значит, что клиент просит сервер не сообщать ему промежуточных ответов, а вернуть только IP-адрес.
RA (1 бит) — отправляется только в ответах, и сообщает о том, что сервер поддерживает рекурсию
Z (3 бита) — являются зарезервированными и всегда равны нулю.
RCODE (4 бита) — это поле служит для уведомления клиентов о том, успешно ли выполнен запрос или с ошибкой.
0 — значит запрос прошел без ошибок;
1 — ошибка связана с тем, что сервер не смог понять форму запроса;
2 — эта ошибка с некорректной работой сервера имен;

3 — имя, которое разрешает клиент не существует в данном домене;
4 — сервер не может выполнить запрос данного типа;
5 — этот код означает, что сервер не может удовлетворить запроса клиента в силу административных ограничений безопасности.

QDCOUNT(16 бит) – количество записей в секции запросов
ANCOUNT(16 бит) – количество записей в секции ответы
NSCOUNT(16 бит) – количество записей в Authority Section
ARCOUNT(16 бит) – количество записей в Additional Record Section

FTP

Взаимодействие по этому протоколу представляет собой отправку команд от клиента к серверу и передачу пакетов FTP-DATA.

Команды:
- AUTH протокол – аутентификация по защищенному протоколу
- USER пользователь – указание имени пользователя
- PASS пароль – указание пароля пользователя
- CLNT клиент – указание клиента, используемого пользователем
- CWD путь – изменение текущей рабочей директории
- TYPE тип – тип передаваемых данных
- STOR имя файла – загрузить файл на сервер
- RETR имя файла – запрос на скачивание файла
- QUIT – отключение от сервера

DHCP

Протокол, предназначенный для динамической выдачи IP-адресов узлам в сети.

Dynamic Host Configuration Protocol				
Bit Offset	0–15		16–31	
0	OpCode	Hardware Type	Hardware Length	Hops
32	Transaction ID			
64	Seconds Elapsed		Flags	
96	Client IP Address			
128	Your IP Address			
160	Server IP Address			
196	Gateway IP Address			
228+	Client Hardware Address (16 bytes)			
	Server Host Name (64 bytes)			
	Boot File (128 bytes)			
	Options			

opcode (op) - указывает нам на тип DHCP-сообщения. Если в этом поле вы видите значение 0×01, то это говорит нам о том, что сообщение является запросом от клиента к серверу. Такое сообщение еще иногда называется BOOTREQUEST. Если же в поле opCode записано значение 0×02, то это означает, что оно являет ответом DHCP-сервера или BOOTREPLY.
Hardware Type (htype) - тип адреса на канальном уровне. DHCP может работать поверх различных протоколов на канальном уровне
Hardware Length (hlen) - длина аппаратного адреса в байтах. Для протокола Ethernet и, соответственно, мак-адресов, указывается значение 0×06
Hops - количество промежуточных маршрутизаторов, которые находятся на пути между клиентом и сервером
Transaction ID (xid) - сервер генерирует значение этого поля, чтобы не перепутать с запросами другого пользователя
Seconds Elapsed (secs) - время в секундах с момента начала процесса получения IP-адреса
Flags - поле для флагов или специальных параметров протокола DHCP
Client IP Address (ciaddr) - поле, в котором указывается IP-адрес клиента. Клиент заполняет его только в том случае, если у него уже есть IP-адрес и он может ответить на ARP-запрос. Такая ситуация возможно в том случае, если клиент хочет продлить время аренды IP-адреса
Your ID Address (yiaddr) — предлагаемый сервером IP-адрес
Server IP Address (siaddr) — IP -адрес сервера
Gateway IP Address (giaddress) - если используется схема с DHCP Relay Agent, то в этом поле передается его IP-адрес
Client Hardware Address (chaddr) - если на канальном уровне используется протокол Ethernet, то в это поле записывается MAC-адрес клиента
Server Host Name (sname) - если у сервера есть доменное имя/имя хоста, то он может сообщить его в этом поле, поле не является обязательным
Boot File (file) - поле не является обязательным и служит указателем для бездисковых рабочих станций о том, как называется файл на сервере, которые следует использовать для загрузки
Options — различная дополнительная информация

Вывод: в данной лабораторной работе я на практике ознакомился с основными сетевыми протоколами, их структурой, для этого я использовал утилиту захвата и анализа сетевого трафика — WireShark.