УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Компьютерные сети»

Лабораторная работа №5

Студент

Кузнецов М. А.

P33131

Преподаватель

Тропченко А. А.

Санкт-Петербург, 2023 г.

Оглавление

Цель работы

Изучить структуру протокольных блоков данных, анализируя реальный трафик на компьютере студента с помощью бесплатно распространяемой утилиты Wireshark

Используемый веб-сайт: https://maxkuznetsov.space

Этап 1. Анализ трафика утилиты ping

`ping -l 1400 maxkuznetsov.space`

```
C:\Users\Max-PC>ping -l 1400 maxkuznetsov.space

Обмен пакетами с maxkuznetsov.space [94.228.122.208] с 1400 байтами данных:
Ответ от 94.228.122.208: число байт=1400 время=2543мс TTL=56
Ответ от 94.228.122.208: число байт=1400 время=2516мс TTL=56
Ответ от 94.228.122.208: число байт=1400 время=3687мс TTL=56
Ответ от 94.228.122.208: число байт=1400 время=2954мс TTL=56

Статистика Ping для 94.228.122.208:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2516мсек, Максимальное = 3687 мсек, Среднее = 2925 мсек
```

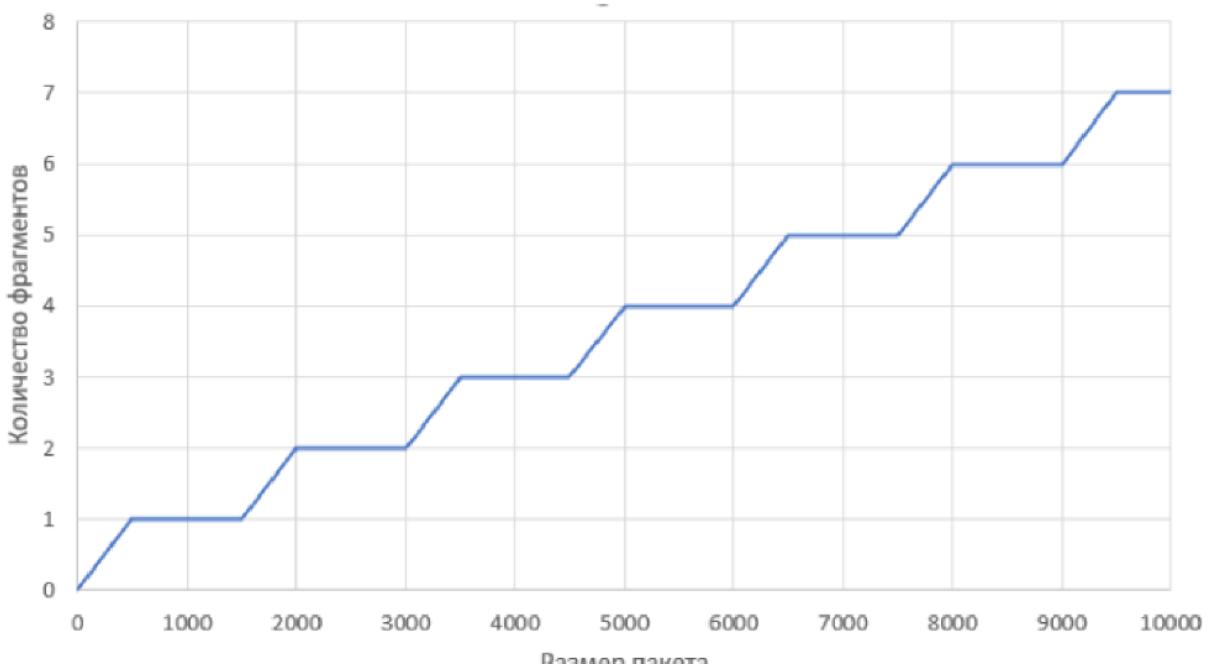
Анализ полученных пакетов

58202	356.146645	172.28.28.43	94.228.122.208	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3d32)
58203	356.146645	172.28.28.43	94.228.122.208	ICMP	562	Echo (ping) request id=0x0001, seq=25/6400, ttl=128
58716	360.771783	172.28.28.43	94.228.122.208	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3d33)
58717	360.771783	172.28.28.43	94.228.122.208	ICMP	562	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
59256	365.782768	172.28.28.43	94.228.122.208	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3d34)
59257	365.782768	172.28.28.43	94.228.122.208	ICMP	562	Echo (ping) request id=0x0001, seq=27/6912, ttl=128

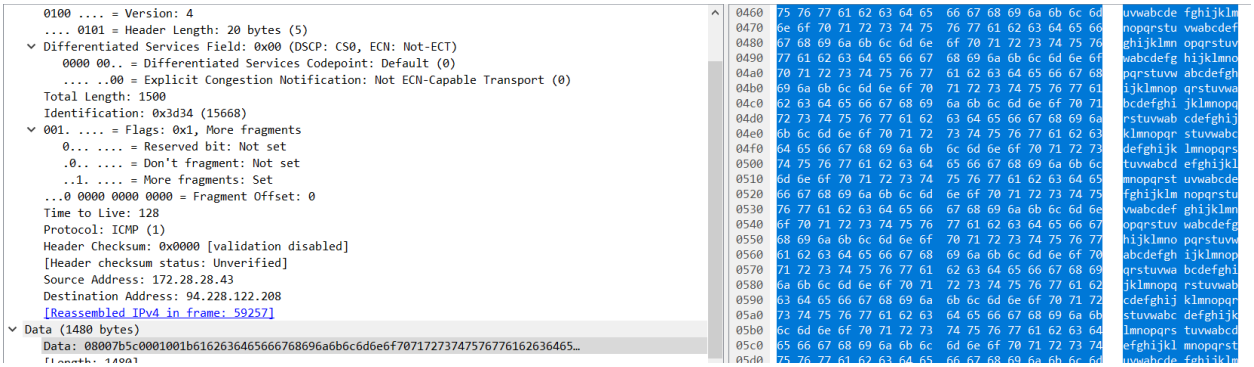
```
> Frame 58202: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\N
> Ethernet II, Src: IntelCor_da:5b:9c (50:76:af:da:5b:9c), Dst: Routerbo_21:4c:a6 (48:8f:5a:21:4c:a6)
v Internet Protocol Version 4, Src: 172.28.28.43, Dst: 94.228.122.208
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0x3d32 (15666)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.28.28.43
    Destination Address: 94.228.122.208
    [Reassembled IPv4 in frame: 58203]
```

1. ***Имеет ли место фрагментация исходного пакета? Какое поле на это указывает?*** *Да, имеет. Флаг More Fragments как раз указывает на наличие фрагментации исходного пакета.*
2. ***Какая информация указывает, является ли фрагмент пакета последним или промежуточным?*** *Для промежуточных пакетов поле MF=1, для последнего MF=0*
3. ***Чему равно количество фрагментов при передаче ping-пакетов?*** *Ping передает данные по 32 байта, так что фрагментации для них нет, т.е. 0 фрагментов*

График



4. ***Как изменить поле TTL с помощью утилиты ping?*** *Для изменения TTL нужно добавить ключ -i, его аргументом является срок жизни пакета в миллисекундах*
5. ***Что содержится в поле данных пакета ping?*** *Символы английского алфавита.*



Этап 2. Анализ трафика утилиты tracert

```
C:\WINDOWS\system32>tracert -d maxkuznetsov.space

Трассировка маршрута к maxkuznetsov.space [94.228.122.208]
с максимальным числом прыжков 30:

  1     1 ms     2 ms     2 ms  172.28.16.1
  2     2 ms     1 ms     1 ms  77.234.199.66
  3    12 ms     2 ms     2 ms  87.248.228.102
  4    34 ms   173 ms   102 ms  178.18.227.244
  5   107 ms   112 ms    57 ms  178.18.236.14
  6    99 ms   113 ms    59 ms  212.91.9.81
  7   106 ms   114 ms    60 ms  212.91.8.74
  8    99 ms   113 ms    60 ms  5.187.51.12
  9   109 ms   116 ms    58 ms  94.228.122.208

Трассировка завершена.
```

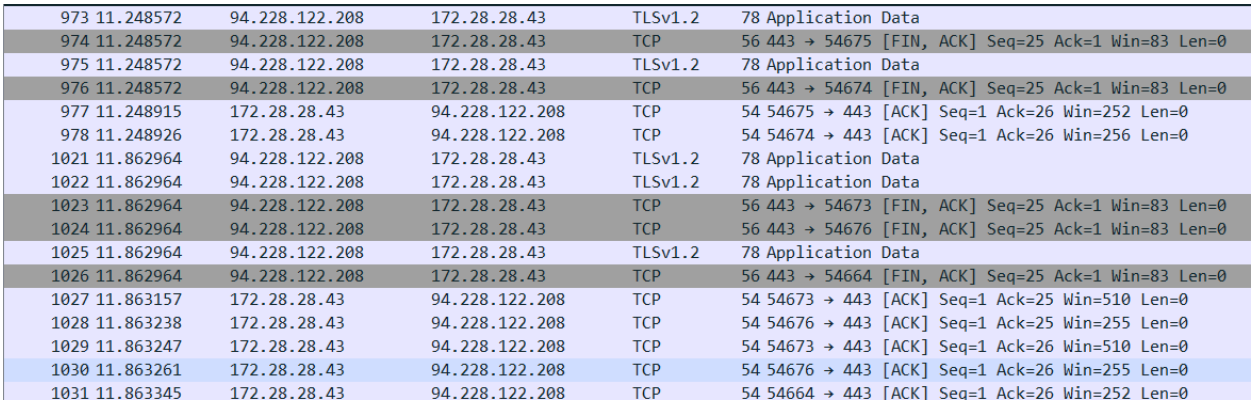
```
Internet Protocol Version 4, Src: 172.28.28.43, Dst: 94.228.122.208
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x3d58 (15704)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 8
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.28.28.43
    Destination Address: 94.228.122.208
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7bd [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 65 (0x0041)
    Sequence Number (LE): 16640 (0x4100)
  [No response seen]
    > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000000000000000…
      [Length: 64]
```

1. ***Сколько байт содержится в заголовке IP? Сколько байта содержится в поле данных?*** *Заголовок: 20 байт, данные: 64.*
2. ***Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracert?*** *Утилита отправляет первый пакет с TTL равным 1, и увеличивает значение на 1 для каждого последующего отправляемого пока назначение не ответит или пока не будет достигнуто максимальное значение.*
3. ***Чем отличаются ICMP пакеты, генерируемые утилитой tracert, от ICMP пакетов, генерируемых утилитой ping?*** *В поле данных у tracert содержатся нули.*

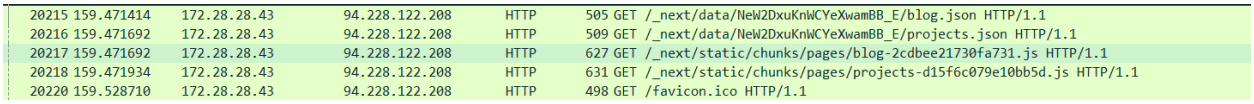
```
0020  7a d0 08 00 f7 bd 00 01  00 41 00 00 00 00 00 00   z·····A·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ····· ·····
0060  00 00 00 00 00 00 00 00  00 00                     ····· ··
```

4. ***Чем отличаются полученные пакеты ICMP reply от ICMP error и зачем нужны оба этих типа ответов?*** *Пакеты ICMP reply указывают на получение нового ответного сообщения. Пакеты ICMP error указывают на то, что произошла ошибка. Они используются, чтобы различать причину истечения TTL.*
5. ***Что изменится в работе tracert, если убрать ключ -d? Какой дополнительный трафик при этом будет генерироваться?*** *Будут также слаться DNS запросы, чтобы разрешить IP-адреса в доменные имена*

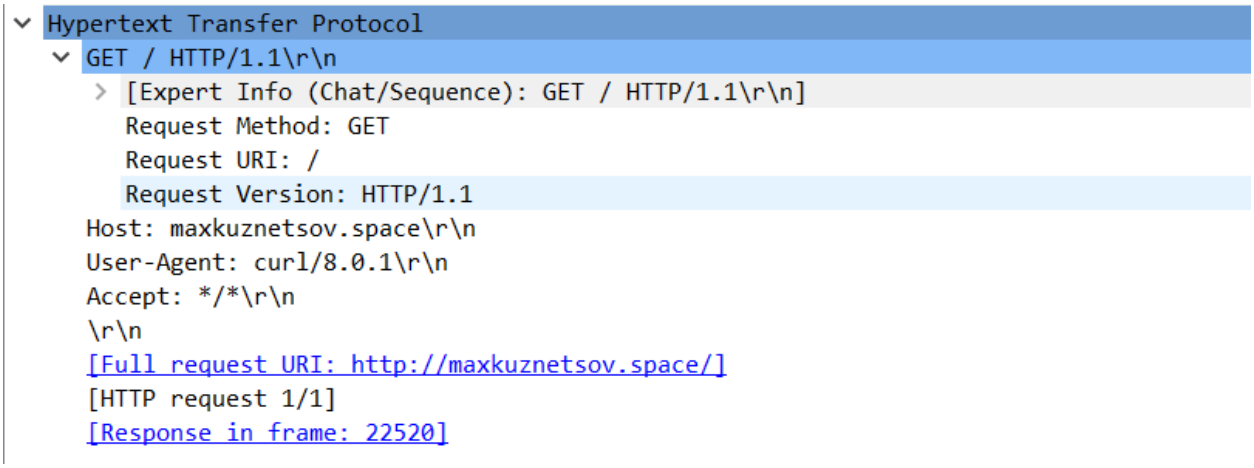
Этап 3. Анализ HTTP-трафика



973	11.248572	94.228.122.208	172.28.28.43	TLSv1.2	78 Application Data
974	11.248572	94.228.122.208	172.28.28.43	TCP	56 443 → 54675 [FIN, ACK] Seq=25 Ack=1 Win=83 Len=0
975	11.248572	94.228.122.208	172.28.28.43	TLSv1.2	78 Application Data
976	11.248572	94.228.122.208	172.28.28.43	TCP	56 443 → 54674 [FIN, ACK] Seq=25 Ack=1 Win=83 Len=0
977	11.248915	172.28.28.43	94.228.122.208	TCP	54 54675 → 443 [ACK] Seq=1 Ack=26 Win=252 Len=0
978	11.248926	172.28.28.43	94.228.122.208	TCP	54 54674 → 443 [ACK] Seq=1 Ack=26 Win=256 Len=0
1021	11.862964	94.228.122.208	172.28.28.43	TLSv1.2	78 Application Data
1022	11.862964	94.228.122.208	172.28.28.43	TLSv1.2	78 Application Data
1023	11.862964	94.228.122.208	172.28.28.43	TCP	56 443 → 54673 [FIN, ACK] Seq=25 Ack=1 Win=83 Len=0
1024	11.862964	94.228.122.208	172.28.28.43	TCP	56 443 → 54676 [FIN, ACK] Seq=25 Ack=1 Win=83 Len=0
1025	11.862964	94.228.122.208	172.28.28.43	TLSv1.2	78 Application Data
1026	11.862964	94.228.122.208	172.28.28.43	TCP	56 443 → 54664 [FIN, ACK] Seq=25 Ack=1 Win=83 Len=0
1027	11.863157	172.28.28.43	94.228.122.208	TCP	54 54673 → 443 [ACK] Seq=1 Ack=25 Win=510 Len=0
1028	11.863238	172.28.28.43	94.228.122.208	TCP	54 54676 → 443 [ACK] Seq=1 Ack=25 Win=255 Len=0
1029	11.863247	172.28.28.43	94.228.122.208	TCP	54 54673 → 443 [ACK] Seq=1 Ack=26 Win=510 Len=0
1030	11.863261	172.28.28.43	94.228.122.208	TCP	54 54676 → 443 [ACK] Seq=1 Ack=26 Win=255 Len=0
1031	11.863345	172.28.28.43	94.228.122.208	TCP	54 54664 → 443 [ACK] Seq=1 Ack=26 Win=252 Len=0



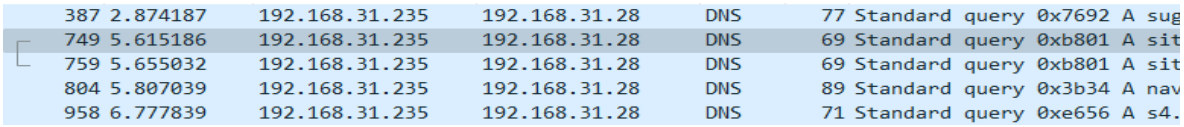
20215	159.471414	172.28.28.43	94.228.122.208	HTTP	505 GET /_next/data/NeW2DxuKnWCYeXwamBB_E/blog.json HTTP/1.1
20216	159.471692	172.28.28.43	94.228.122.208	HTTP	509 GET /_next/data/NeW2DxuKnWCYeXwamBB_E/projects.json HTTP/1.1
20217	159.471692	172.28.28.43	94.228.122.208	HTTP	627 GET /_next/static/chunks/pages/blog-2cdbee21730fa731.js HTTP/1.1
20218	159.471934	172.28.28.43	94.228.122.208	HTTP	631 GET /_next/static/chunks/pages/projects-d15f6c079e10bb5d.js HTTP/1.1
20220	159.528710	172.28.28.43	94.228.122.208	HTTP	498 GET /favicon.ico HTTP/1.1



```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
  Host: maxkuznetsov.space\r\n
  User-Agent: curl/8.0.1\r\n
  Accept: */*\r\n
  \r\n
  [Full request URI: http://maxkuznetsov.space/]
  [HTTP request 1/1]
  [Response in frame: 22520]
```

1. *Сначала получаем гипертекст на запрошенном сайте*
2. *Поочередно получаем необходимые в html тексте скрипты js*
3. *Поочередно получаем необходимые картинки для отображения содержимого сайта*
4. *При вторичном запросе-обновлении получаем код ответа 304 “Not modified”, т. к. содержимое страницы не менялось*

Этап 4. Анализ DNS трафика



387	2.874187	192.168.31.235	192.168.31.28	DNS	77 Standard query 0x7692 A sug
749	5.615186	192.168.31.235	192.168.31.28	DNS	69 Standard query 0xb801 A sit
759	5.655032	192.168.31.235	192.168.31.28	DNS	69 Standard query 0xb801 A sit
804	5.807039	192.168.31.235	192.168.31.28	DNS	89 Standard query 0x3b34 A nav
958	6.777839	192.168.31.235	192.168.31.28	DNS	71 Standard query 0xe656 A s4.

```
Internet Protocol Version 4, Src: 192.168.31.235, Dst: 192.168.31.28
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 55
   Identification: 0xd88d (55437)
 > Flags: 0x00
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 64
   Protocol: UDP (17)
   Header Checksum: 0xe1d0 [validation disabled]
   [Header checksum status: Unverified]
```

1. ***Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?*** *Так как кэш был очищен, то необходимо получить DNS запрашиваемого сайта у провайдеров.*
2. ***Какие бывают типы DNS-запросов****? Типы DNS-запросов:*
   - ***Итеративный (прямой).*** *Преобразование домена в IP адрес*
   - ***Рекурсивный.*** *Получает доменное имя и принимает IP-адрес, dns-сервер может обращаться к другим серверам*
   - ***Обратный.*** *Сервер получает IP, должен вернуть доменное имя.*
3. ***В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?***
   Выполнять дополнительные DNS запросы необходимо, когда картинки лежат на другом доменном имени, а не на том же хосте

Этап 4. Анализ ARP трафика

```
2917 87.853707164  PcsCompu_3a:9d:ff   Broadcast           ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
2918 87.854035630  RealtekU_12:35:02   PcsCompu_3a:9d:ff   ARP      60 10.0.2.2 is at 52:54:00:12:35:02
3202 130.315548685 PcsCompu_3a:9d:ff   Broadcast           ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
3203 130.315738767 RealtekU_12:35:02   PcsCompu_3a:9d:ff   ARP      60 10.0.2.2 is at 52:54:00:12:35:02
```

```
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: PcsCompu_3a:9d:ff (08:00:27:3a:9d:ff)
   Sender IP address: 10.0.2.15
   Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
   Target IP address: 10.0.2.2
```

1. ***Какие MAC-адреса присутствуют в захваченных пакетах ARP протокола? Что означают эти адреса? Какие устройства они идентифицируют?***
   - *08:00:27:3a:9d:ff- MAC-адрес нашего устройства*

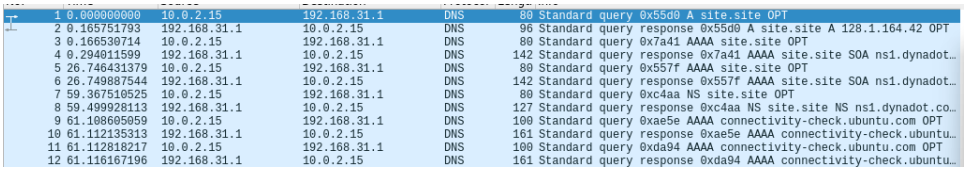
- *00:00:00:00:00:00 - MAC заполнитель, пока не будет получен реальный адрес*
- *52:54:00:12:35:02 - MAC-адрес маршрутизатора*

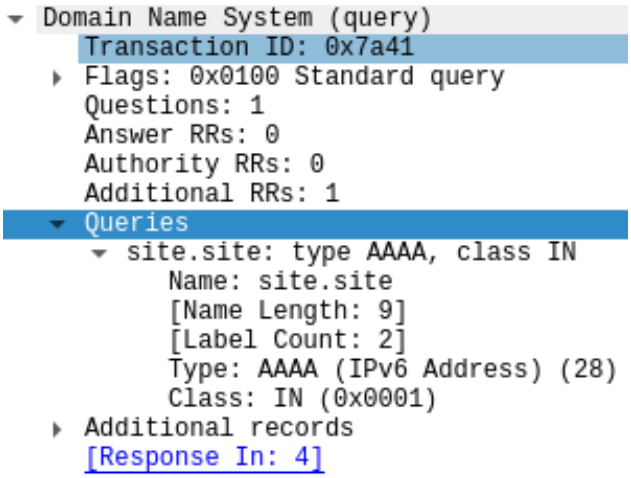
2. ***Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?*** *Те же самые, что и в первом пункте*
3. ***Для чего ARP-запрос содержит IP-адрес источника?*** *IP адрес содержится в запросе по следующим причинам:*

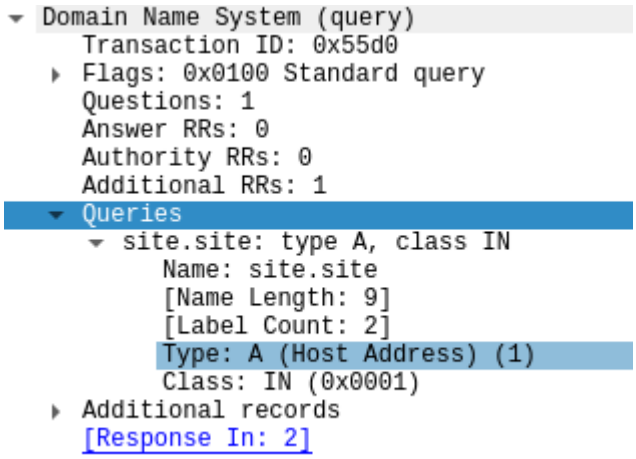
   Во-первых, этот адрес нужен для заполнения ARP-таблицы.

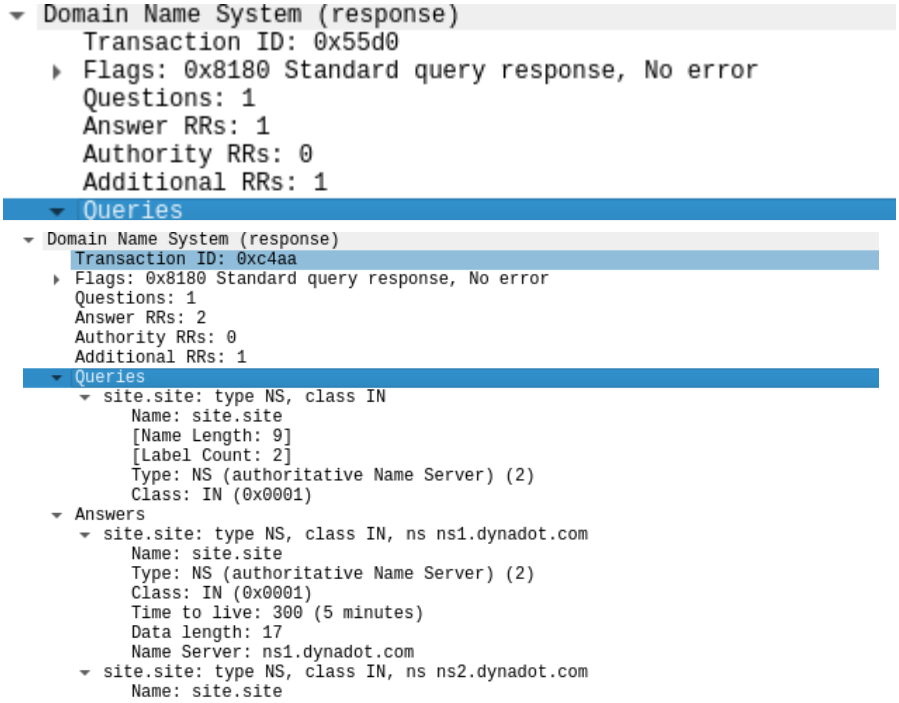
   Во-вторых, чтобы можно был сразу ответить на запрос, не отправляя ответный запрос

Этап 6. Анализ утилиты nslookup









1. ***Чем различается трасса трафика в п.2 и п.4, указанных выше?*** *Различия:*
   - *При запуске п.2 ищется IPv6 Address*
   - *При запуске п.4 ищется Name Server*
2. ***Что содержится в поле «Answers» DNS-ответа?*** *В зависимости от типа запроса поле может содержать:*
   - *IPv4 адрес (для типа A)*
   - *IPv6 адрес (для типа AAAA)*
   - *Доменное имя сервера (для типа NS)*
   - *MX (для почты)*
3. ***Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?*** *Серверов, возвращающих авторитативный отклик, нет. Авторитативный отклик возвращают серверы, которые являются ответственными за зону, в которой описана информация, необходимая DNS клиенту.*

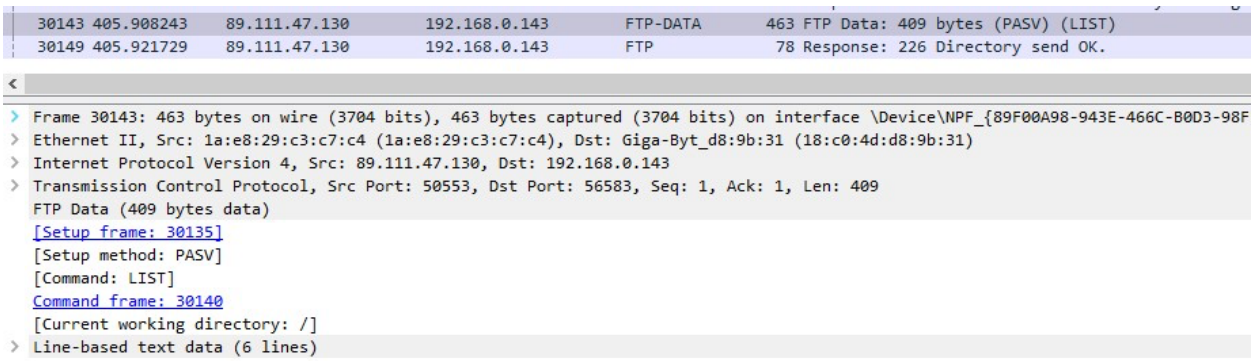
```
C:\WINDOWS\system32>nslookup -type=NS maxkuznetsov.space
╤xËтxË:  UnKnown
Address:  172.28.16.1

Не заслуживающий доверия ответ:
maxkuznetsov.space      nameserver = ns2.timeweb.ru
maxkuznetsov.space      nameserver = ns4.timeweb.org
maxkuznetsov.space      nameserver = ns3.timeweb.org
maxkuznetsov.space      nameserver = ns1.timeweb.ru

maxkuznetsov.space      nameserver = ns4.timeweb.org
maxkuznetsov.space      nameserver = ns3.timeweb.org
maxkuznetsov.space      nameserver = ns1.timeweb.ru
maxkuznetsov.space      nameserver = ns2.timeweb.ru
ns2.timeweb.ru  internet address = 92.53.98.100
ns4.timeweb.org internet address = 139.45.249.139
ns3.timeweb.org internet address = 139.45.232.67
ns1.timeweb.ru  internet address = 92.53.116.200
ns4.timeweb.org internet address = 139.45.249.139
ns3.timeweb.org internet address = 139.45.232.67
ns1.timeweb.ru  internet address = 92.53.116.200
ns2.timeweb.ru  internet address = 92.53.98.100
```

Этап 7. Анализ FTP трафика

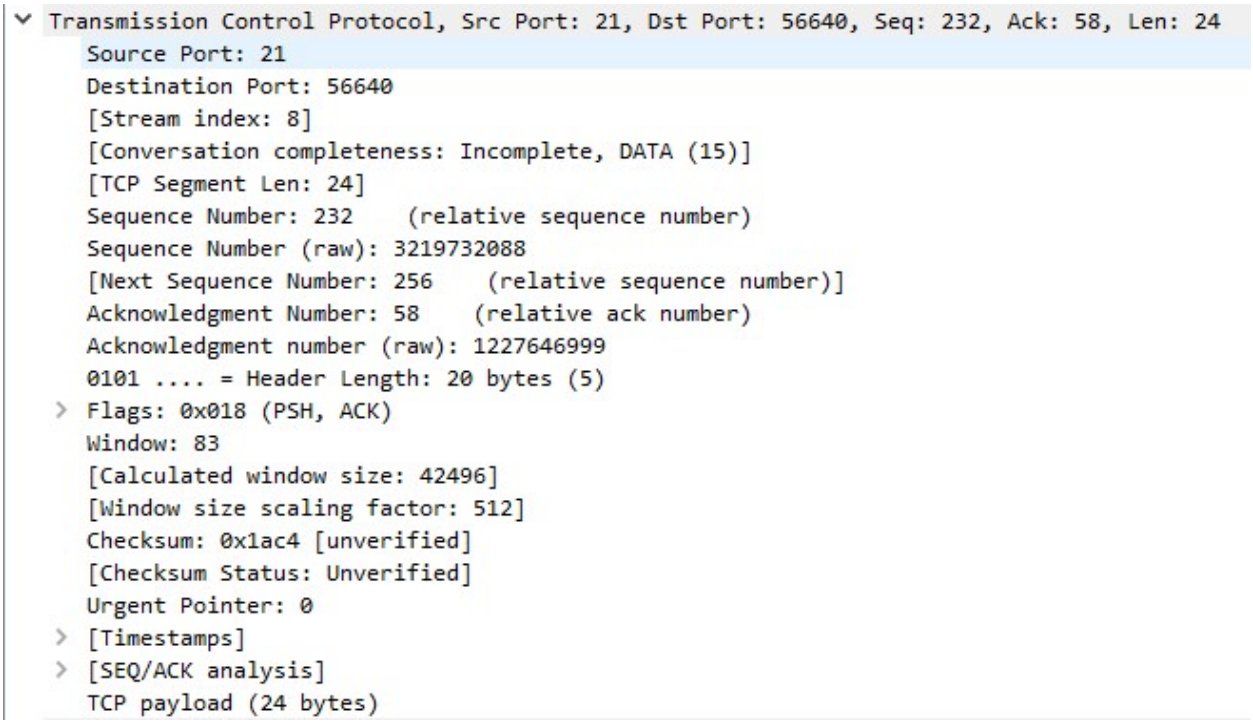
1. **Сколько байт данных содержится в пакете FTP-DATA?**
   Размер может быть любым, но не больше MTU. В данном случае 409 байт.



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

   Для потока управления на сервере используется порт 21. Для передачи данных используется порт 20, если передача идет в

активном режиме, либо с любого порта клиента к любому порту сервера в пассивном режиме.



3. **Чем отличаются пакеты FTP от FTP-DATA?**

FTP используется для выполнения команд (request/response), а FTP-DATA работает с файлами.

Вывод по лабораторной работе

Во время выполнения лабораторной работы мы познакомились с работой различных протоколов передачи данных, проанализировали переданные пакеты с помощью программы Wireshark и протестировали соединения через разные утилиты.