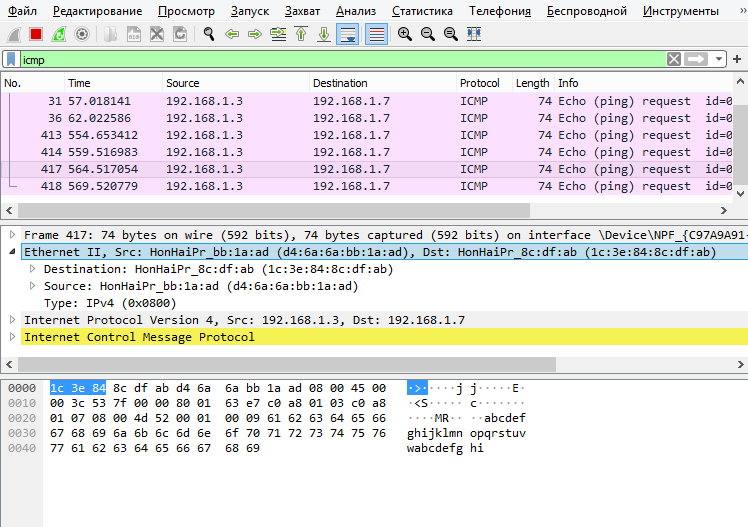
**Часть 1. Просмотр сетевого трафика.**



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера?

Совпадает

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?

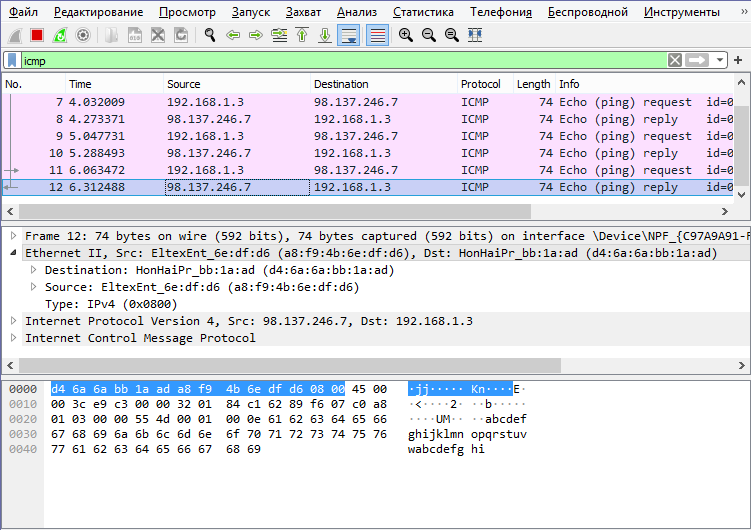
Совпадает

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

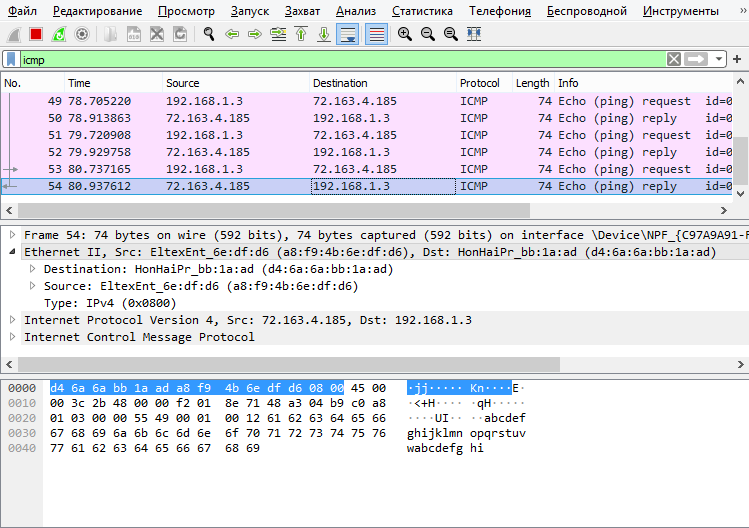
(???)Для этого существуют таблицы маршрутизации, по которым компьютер видит окружающие устройства. Если в этой таблице нет нужного адресата – запрос уходит на шлюз по умолчанию и уже вышестоящее в иерархии устройство ищет этого адресата.

Часть с удаленными узлами.

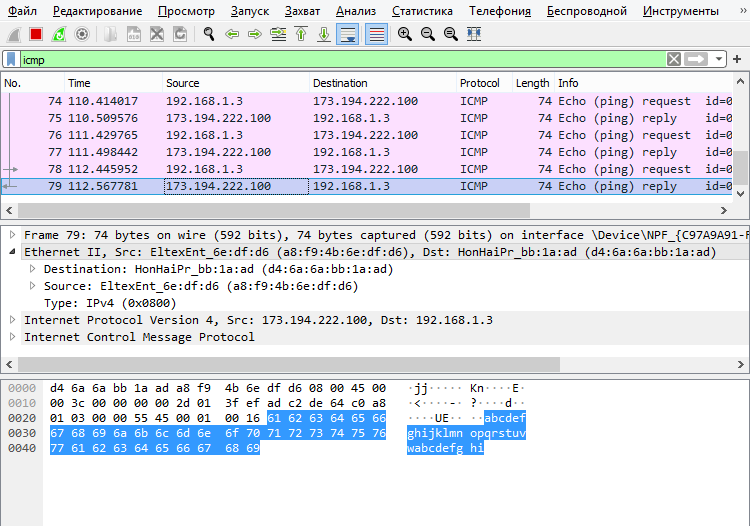
Запрос на yahoo.com



Запрос на cisco.com



Запрос на google.com



1-й адрес:IP: 98.137.246.7 MAC: a8:f9:4b:6e:df:d6

2-й адрес:IP: 72.163.4.185 MAC: a8:f9:4b:6e:df:d6

3-й адрес:IP: 173.194.222.100 MAC: a8:f9:4b:6e:df:d6

Какова существенная особенность этих данных?

Во всех случаях содержатся MAC адреса шлюза.

Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

В части 1 были получены mac адреса устройств, находящихся в локальной сети. Во части 2 во всех запросах был получен MAC адрес шлюза.

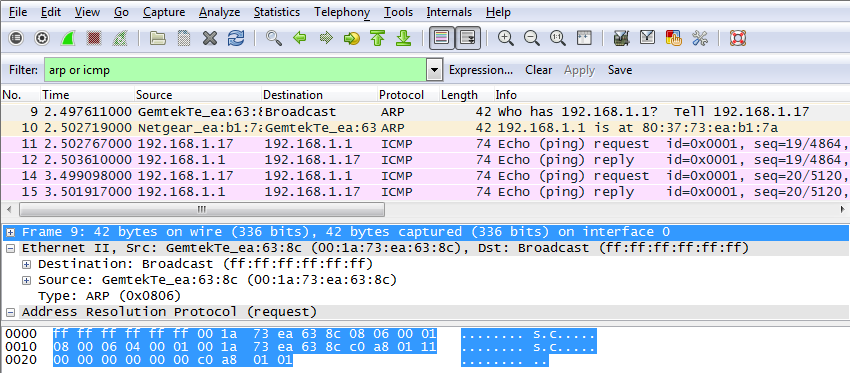
Вопросы для повторения

Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

MAC адрес используется только для идентификации узлов внутри локальной сети. Если мы связываемся с устройством в локальной сети, то будем получать его MAC адрес, если связываемся с удаленными узлами – получим MAC адрес устройства, которое нам передало информацию, то есть MAC адрес шлюза.

**Часть 2. Анализ кадров Ethernet.**

Часть 1

****

Какова особенность содержания поля адреса назначения?

Адрес может быть как широковещательным, так и индивидуальным

Почему перед первым эхо-запросом ПК отправляет широковещательную рассылку ARP?

Потому что широковещательныя рассылка используется при условии, что в ARP таблице нет искомого IP и MAC адреса. Перед первым эхо-запросом таблица пуста, поэтому требуется заполнить таблицу первичными данными. Среди них – адреса шлюза.

Назовите MAC-адрес источника в первом кадре.

MAC-адрес источника – физический адрес устройства, с которого выполнялся запрос.

В примере выше MAC адрес следующий: 00:1a:73:ea:63:8c

Назовите идентификатор производителя (OUI) сетевой платы источника.

00:1a:73

Какая часть МАС-адреса соответствует OUI?

Первые шесть цифр

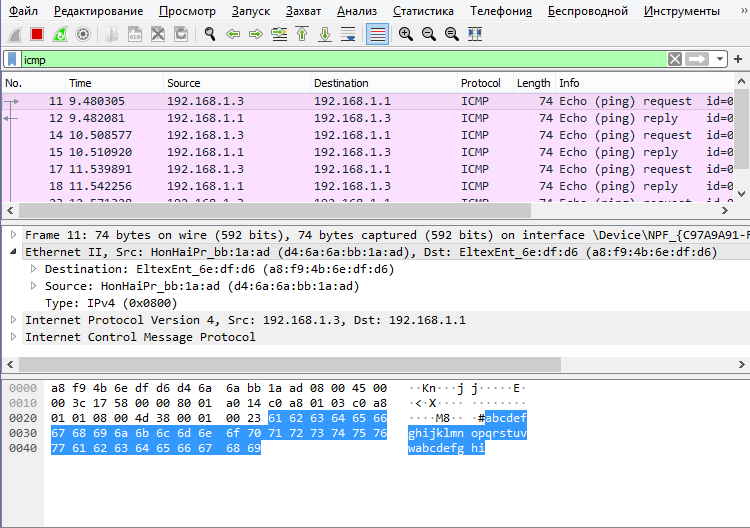
Назовите серийный номер сетевой платы источника.

ea:63:8c

Часть 2

Назовите IP-адрес шлюза ПК по умолчанию.

192.168.1.1



Назовите MAC-адрес сетевой платы этого ПК.

d4:6a:6a:bb:1a:ad

Назовите MAC-адрес шлюза по умолчанию.

a8:f9:4b:6e:df:d6

Назовите отображающийся тип кадра.

IPv4

Назовите IP-адрес источника.

192.168.1.3

Назовите IP-адрес назначения.

192.168.1.1

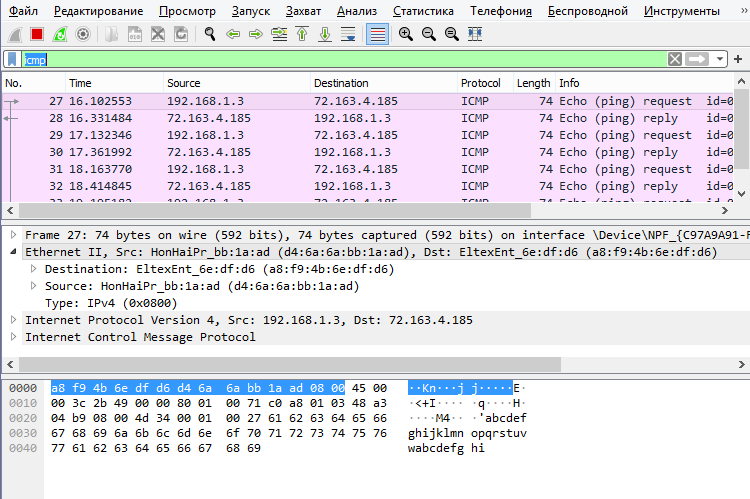
Какое слово образуют последние два выделенных октета?

abcdefghijklmnopqrstuvwabcdefghi

Какое устройство и MAC-адрес отображаются в качестве адреса назначения?

Отображается шлюз, адрес a8:f9:4b:6e:df:d6

Совершен эхо-запрос по адресу [www.cisco.com](http://www.cisco.com)



Назовите МАС-адреса источника и назначения в первом кадре эхо-запроса.

**Источник**: d4:6a:6a:bb:1a:ad

**Назначение**: a8:f9:4b:6e:df:d6

Назовите IP-адреса источника и назначения в поле данных кадра.

**Источник**: 192.168.1.3

**Назначение**: 72.163.4.185

Сравните эти адреса с адресами, полученными в шаге 6. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а MAC-адрес назначения остался прежним?

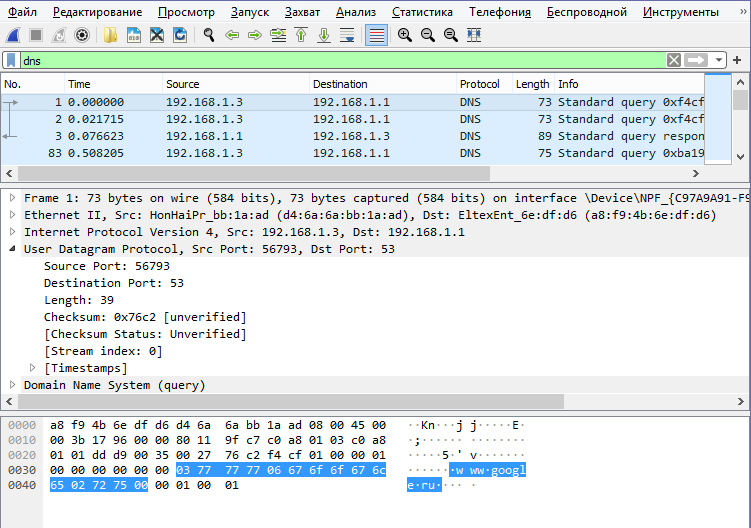
MAC адрес используется только для идентификации узлов внутри локальной сети. Если мы связываемся с устройством в локальной сети, то будем получать его MAC адрес, если связываемся с удаленными узлами – получим MAC адрес устройства, которое нам передало информацию, то есть MAC адрес шлюза. IP адреса используются для адресации удаленных узлов, поэтому он должен быть изменен при запросе на другой удаленный узел.

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

Преамбула является передовой частью пакета (кадра). Поле преамбулы занимает 8 байт и состоит из 1-байтной последовательности 10101011, которая указывает на начало кадра (пакета), и семи байтов, в которых чередуются 1 и 0 (каждый байт — последовательность вида: 10101010) Они служат для синхронизации приёмного терминала. Преамбула обеспечивает синхронизацию приёмника и услуги по разграничению кадров.

**Часть 3. Изучение захваченных пакетов DNS и UDP**

|  |  |
| --- | --- |
| IP-адрес | 192.168.1.3 |
| MAC-адрес | d4:6a:6a:bb:1a:ad |
| IP-адрес шлюза по умолчанию | 192.168.1.1 |
| IP-адрес DNS-сервера | 192.168.1.1 |



Совпадает ли MAC-адрес источника с адресом, записанным в части 1 для локального ПК?

Совпадает

|  |  |  |
| --- | --- | --- |
| Устройство | IP-адрес | MAC-адрес |
| Локальный ПК | 192.168.1.3 | d4:6a:6a:bb:1a:ad |
| Шлюз по умолчанию | 192.168.1.1 | a8:f9:4b:6e:df:d6 |

|  |  |
| --- | --- |
| Размер кадра | 73 |
| MAC-адрес источника | d4:6a:6a:bb:1a:ad |
| MAC-адрес назначения | a8:f9:4b:6e:df:d6 |
| IP-адрес источника | 192.168.1.3 |
| IP-адрес назначения | 192.168.1.1 |
| Порт источника | 56793 |
| Порт назначения | 53 |

Совпадает ли IP-адрес источника с IP-адресом локального ПК, записанным в части 1?

Да

Совпадает ли IP-адрес назначения со шлюзом по умолчанию, записанным в части 1?

Да

Если судить по кадру Ethernet II для DNS-ответа, какому устройству соответствует MAC-адрес источника и какое устройство соответствует MAC-адресу назначения?

Источник – устройство, посылавшее запрос, назначение – шлюз по умолчанию.

Обратите внимание на IP-адреса источника и назначения в IP-пакете. Назовите IP-адрес назначения. Назовите IP-адрес источника.

IP-адрес назначения: 192.168.1.1

IP-адрес источника: 192.168.1.3

В чем преимущества использования протокола UDP вместо протокола TCP в качестве транспортного протокола для DNS?

UDP быстрее, т. к не устанавливает соединение и не контролирует доставку данных

**Часть 4. Изучение пакетов TCP и UDP.**