Санкт-Петербургский Национальный Исследовательский Университет Информационных Технологий, Механики и Оптики

Факультет Инфокоммуникационных Технологий

**Практическая работа №5**

**Изучение работы протоколов стека TCP/IP с помощью Wireshark.**

Выполнила:

Улитина М.С

Проверил:

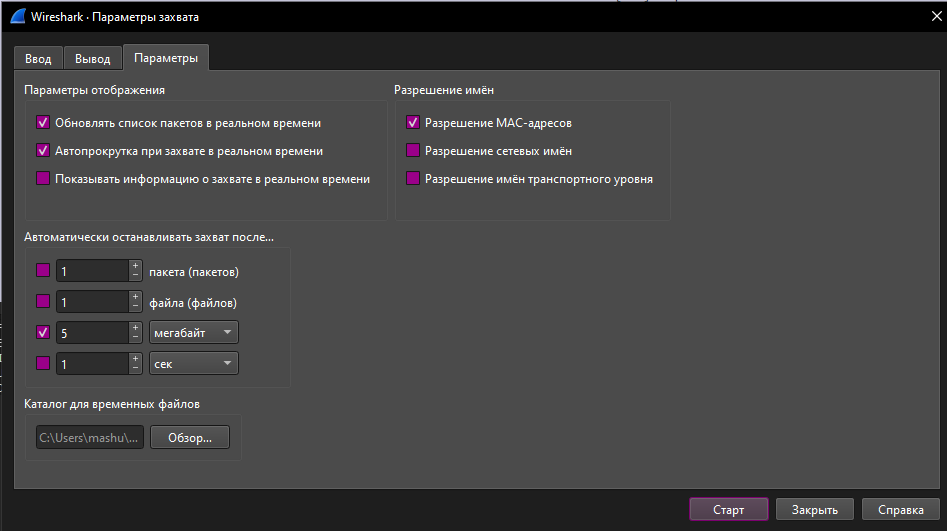
Харитонов А.Ю

Санкт-Петербург, 2024

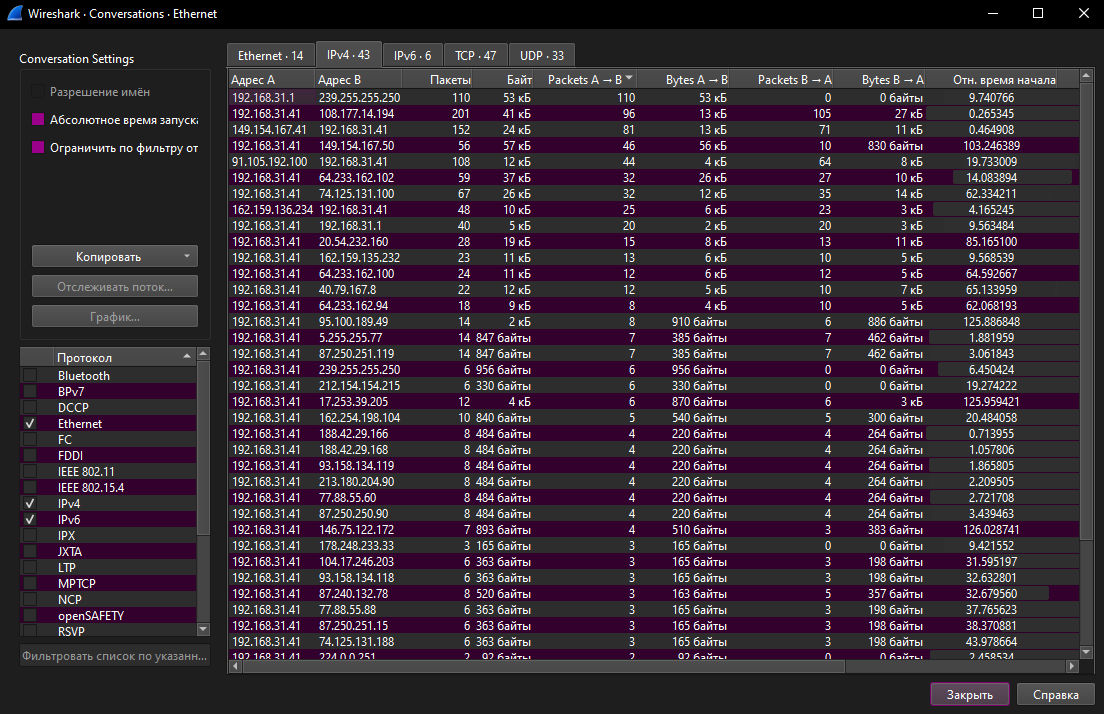
**Ход работы.**

## Начало работы с Wireshark.

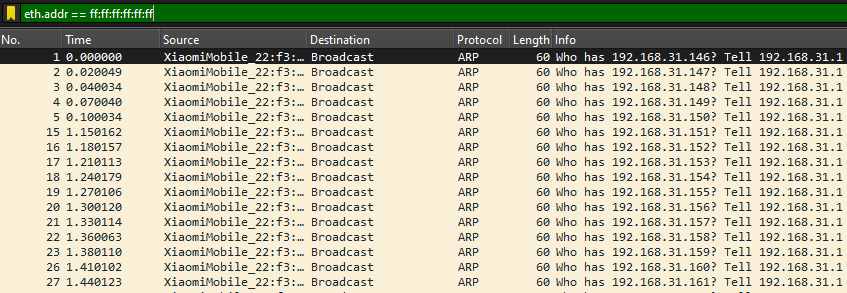
1. Настройте перехват трафика на интерфейсе, так чтобы он завершился после сбора 5 Мб

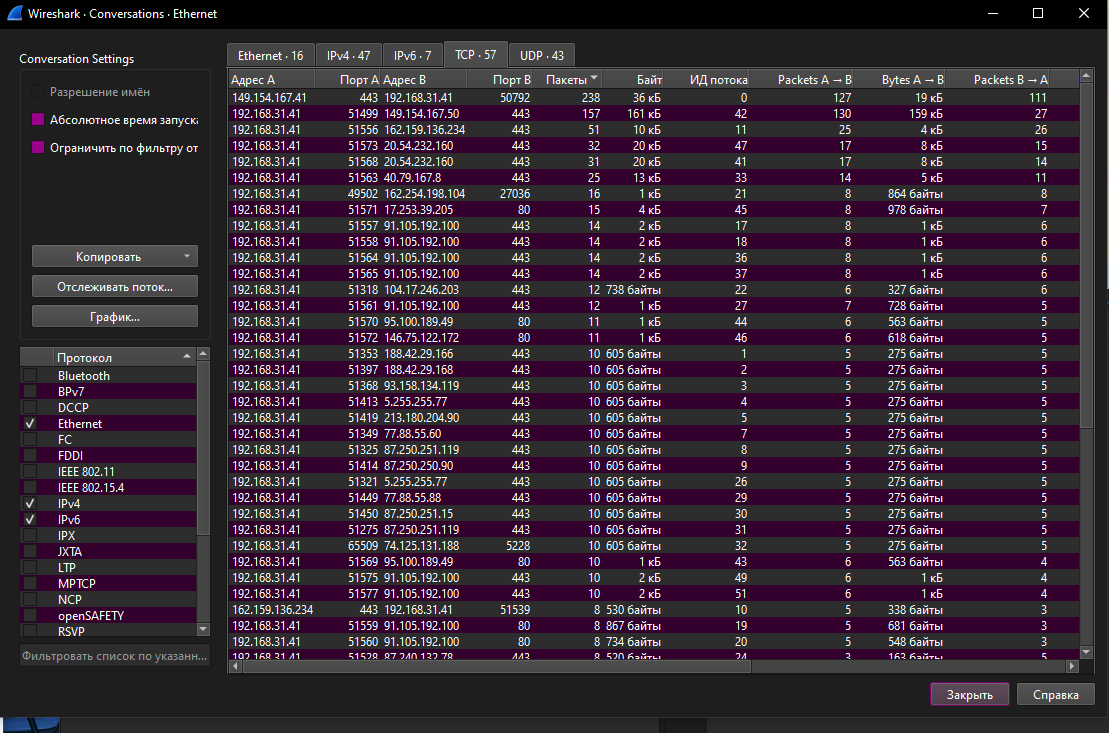


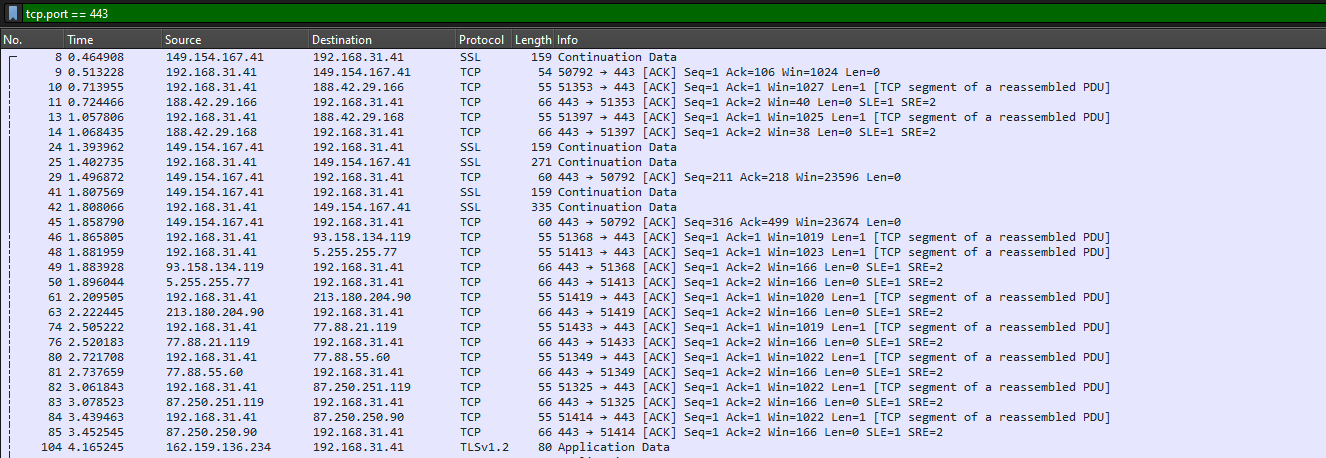
1. **Используя инструментарий статистики, определите:**
   1. Узел с максимальной активностью (по объему переданных данных),

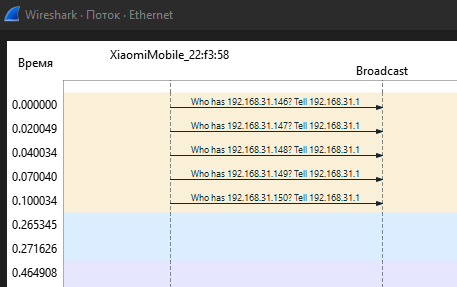


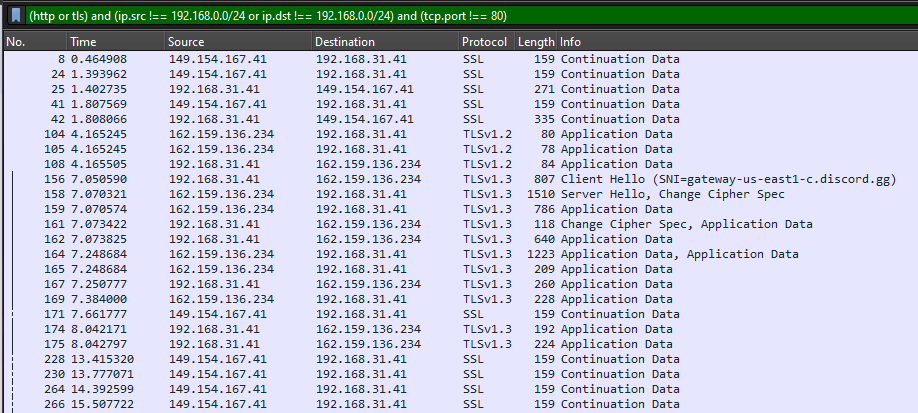
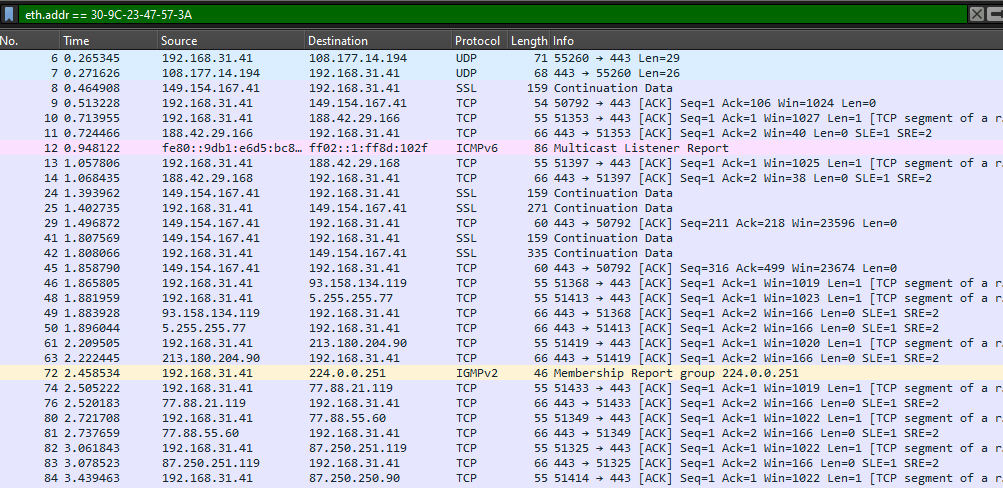
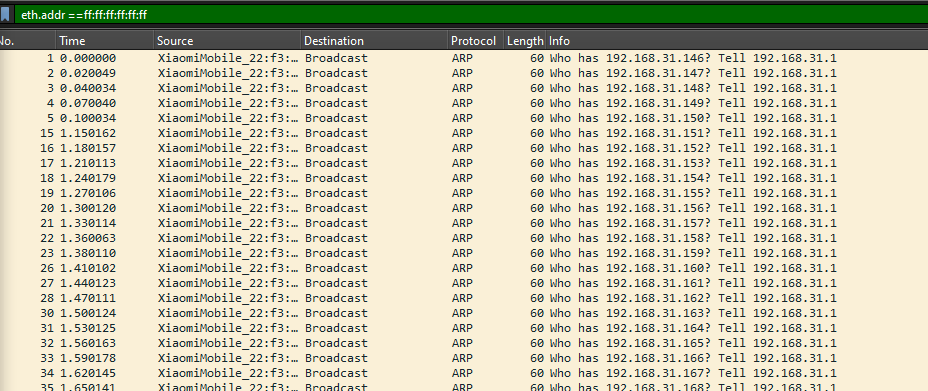
* 1. Узел, осуществивший наибольшее количество широковещательных рассылок,



* 1. Самый активный TCP-порт на хосте (по количеству переданных пакетов)  
     
  2. Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs).  
      и аналогично TCP  
     
  3. Постройте диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)

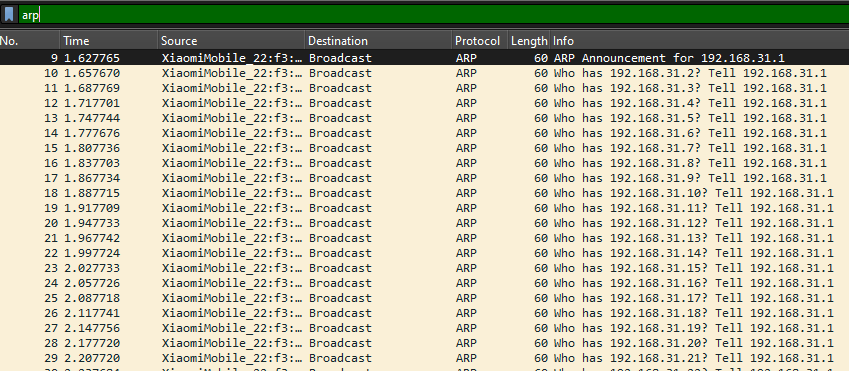




1. **Напишите фильтры, которые выделяют из общего числа пакеты:**
   1. Отбирающие сообщения протоколов HTTP, относящиеся **только** к взаимодействию локальных клиентов и внешнего сервера (но игнорировать трафик внутреннего сервера, если он есть). То есть в случае, если на вашем компьютере запущен и Web-броузер и Web-сервер, фильтр должен отбирать только трафик от и к локальным Web-браузерам, игнорируя трафик от и к локальному Web-серверу.  
      
   2. Все кадры Ethernet, отправленные с сетевого интерфейса хоста.  
      Выяснила mac-адрес  
      
   3. Напишите фильтр, отбирающий только широковещательные сообщения. Определите назначение 3-х широковещательных рассылок разных протоколов (или тех, которые удалось обнаружить).  
      Фильтр выбирает все сетевые пакеты с адресом назначения ff:ff:ff:ff:ff:ff, что представляет собой широковещательный адрес MAC  
      

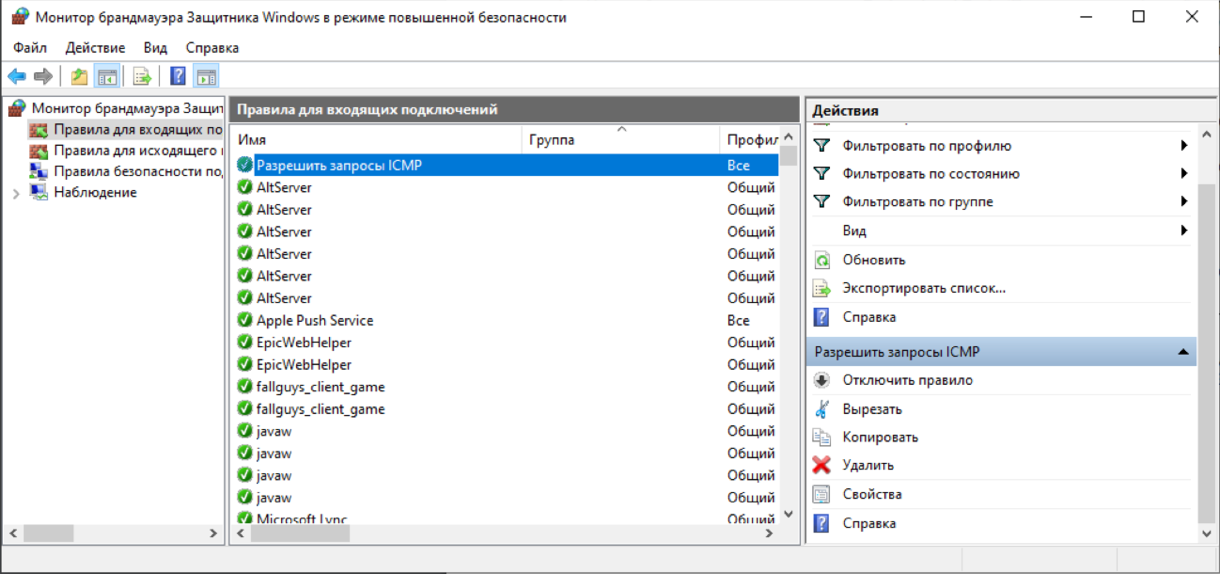
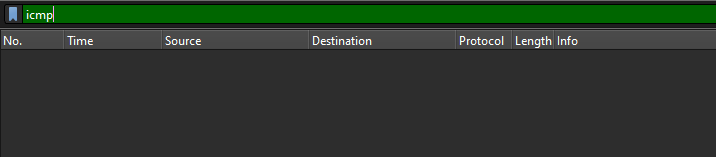
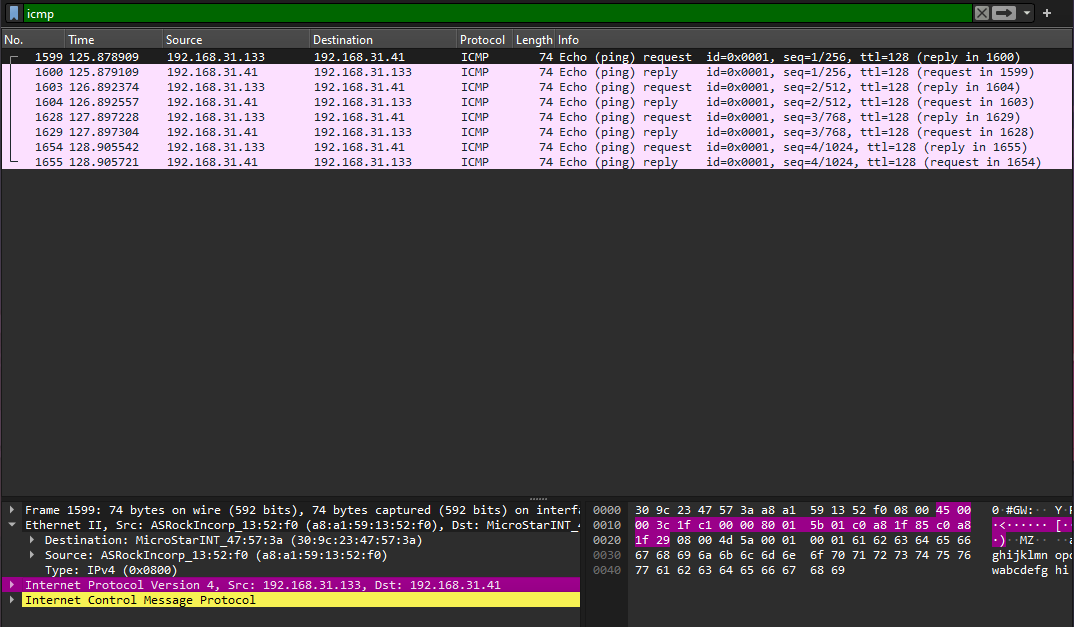
ARP (протокол разрешения адресов): используется для сопоставления IP-адресов с MAC-адресами

локальной сети. Устройство отправляет запросы ARP, чтобы найти MAC-адрес определенного IP-адресав локальной сети. Если устройству известен соответствующий MAC-адрес, оно ответит на запрос ARP своим MAC-адресом.

* 1. Определить адреса, на которые поступают данные кадры и пакеты для канального и сетевого уровня.  
     ARP(канальный) – широковещательный mac-адрес ff:ff:ff:ff:ff:ff
  2. Напишите фильтры для каждой из трех широковещательных рассылок, выбранных в пункте 3-с.  
     
  3. На основании собранной статистики и анализа адресов определить, к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор).   
     ?

## Сбор и углубленный анализ данных протокола ICMP

## Сбор и анализ данных протокола ICMP по локальным узлам.

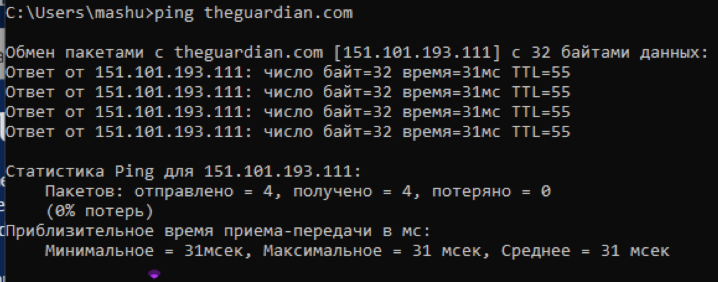
1. Узнайте IP адреса двух устройств в Вашей локальной сети (ноутбук и телефон, к примеру).  
   мой компьютер - 192.168.31.41  
   второй компьютер в сети -
2. Создайте новое правило межсетевого экрана, разрешающее прохождение ICMP-трафика через межсетевой экран Вашего устройства. Подробнее об этом в приложении А.  
   
3. Запустите Wireshark – захват на Вашем устройстве. В этой части нас интересуют только единицы данных протокола (PDU) ICMP (эхо-запрос с помощью команды ping). Для того чтобы вывести на экран только единицы данных протокола ICMP (ping-запрос), отфильтруйте их.  
   
4. Пошлите команду ping с другого устройства на Ваше устройство. +
5. Проверьте данные, сформированные ping-запросами.
   1. Выберите кадры PDU первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце **Source** (Источник) указывается IP-адрес вашего компьютера, а в столбце **Destination** (Назначение) — IP-адрес ПК другого участника, на который вы отправили ping-запрос.   
      
   2. Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Нажмите символ + слева от строки Ethernet II, чтобы просмотреть МАС-адреса источника и назначения. +
   3. Ответьте на вопросы:

Совпадает ли MAC-адрес источника с интерфейсом компьютера?   
Да, совпадает

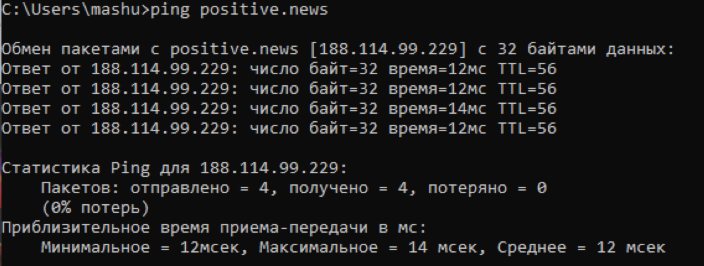
Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом источника?   
Да, совпадает

Как ваш ПК определил MAC-адрес другого устройства, с которого был отправлен эхо-запрос с помощью команды ping?  
При отправке эхо-запроса с помощью команды ping, компьютер использует ARP протокол для определения MAC-адреса устройства, соответствующего IP-адресу, на который он отправляет пакет. Когда компьютер отправляет ARP запрос, устройство с этим IP-адресом отвечает своим MAC-адресом, и ПК запоминает эту информацию для передачи данных.

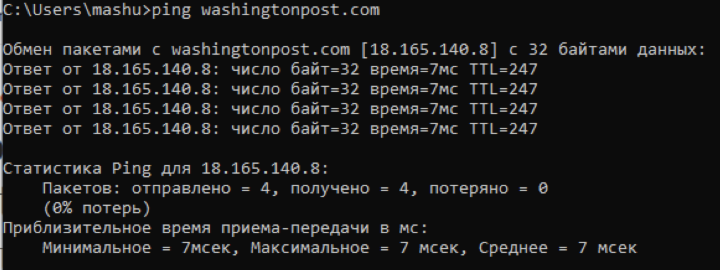
## Сбор и анализ данных протокола ICMP по удаленным узлам.

1. Отправьте эхо-запросы с помощью команды ping на 3 удаленных узла (расположенные за пределами локальной сети): сайты зарубежных СМИ. **Примечание.** При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует адрес URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.  
   

Ip-адрес theguardian.com: 151.101.193.111



Ip-адрес positive.news: 188.114.99.229

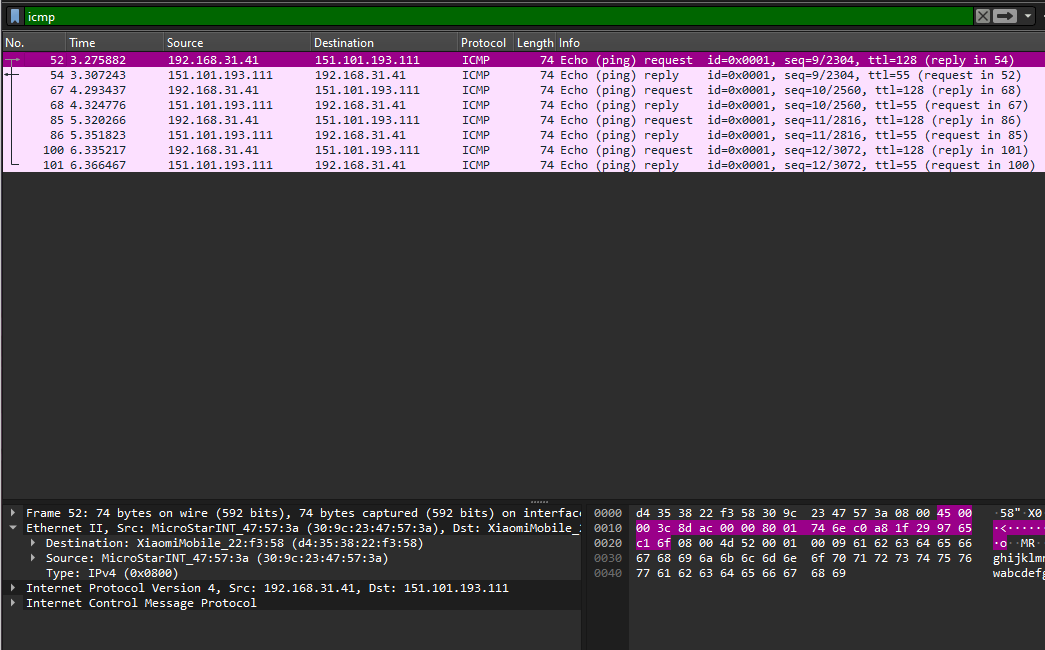


Ip-адрес washingtonpost.com: 18.165.140.8

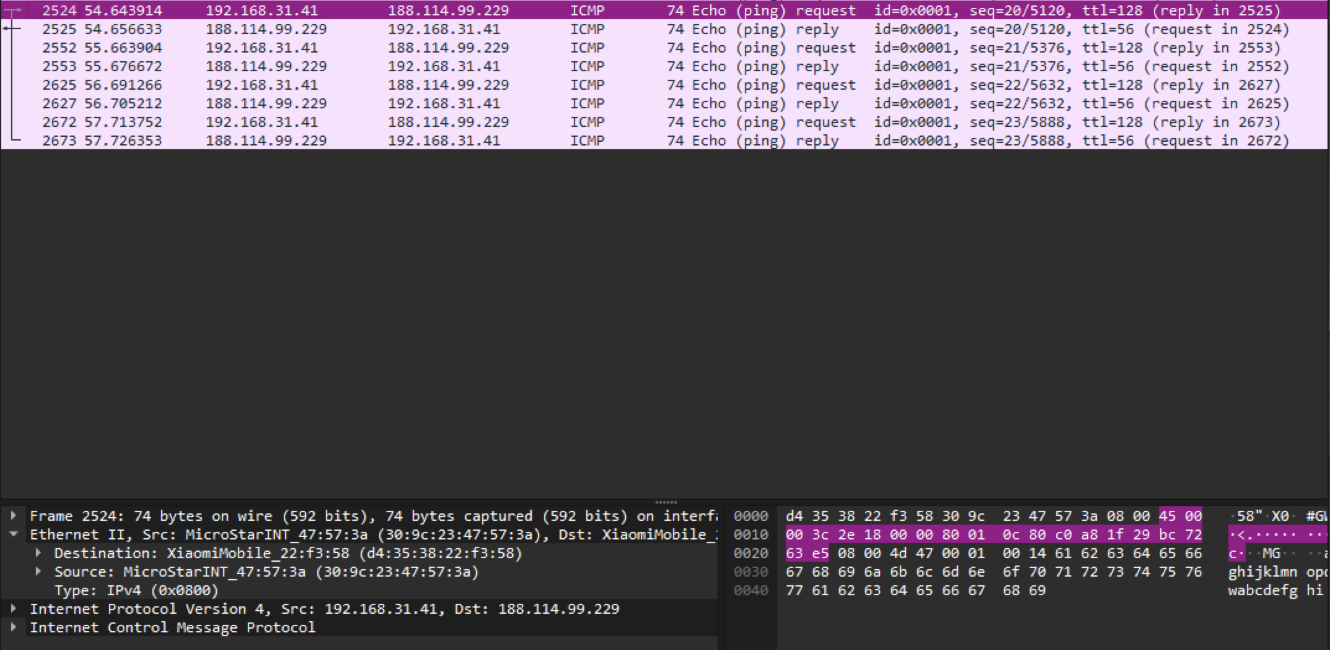
1. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили ping-запросы. Укажите IP- и MAC-адреса назначения для всех 3-х веб-сайтов.

Ip-адрес theguardian.com: 151.101.193.111

Mac-адрес: d4:35:38:22:f3:58

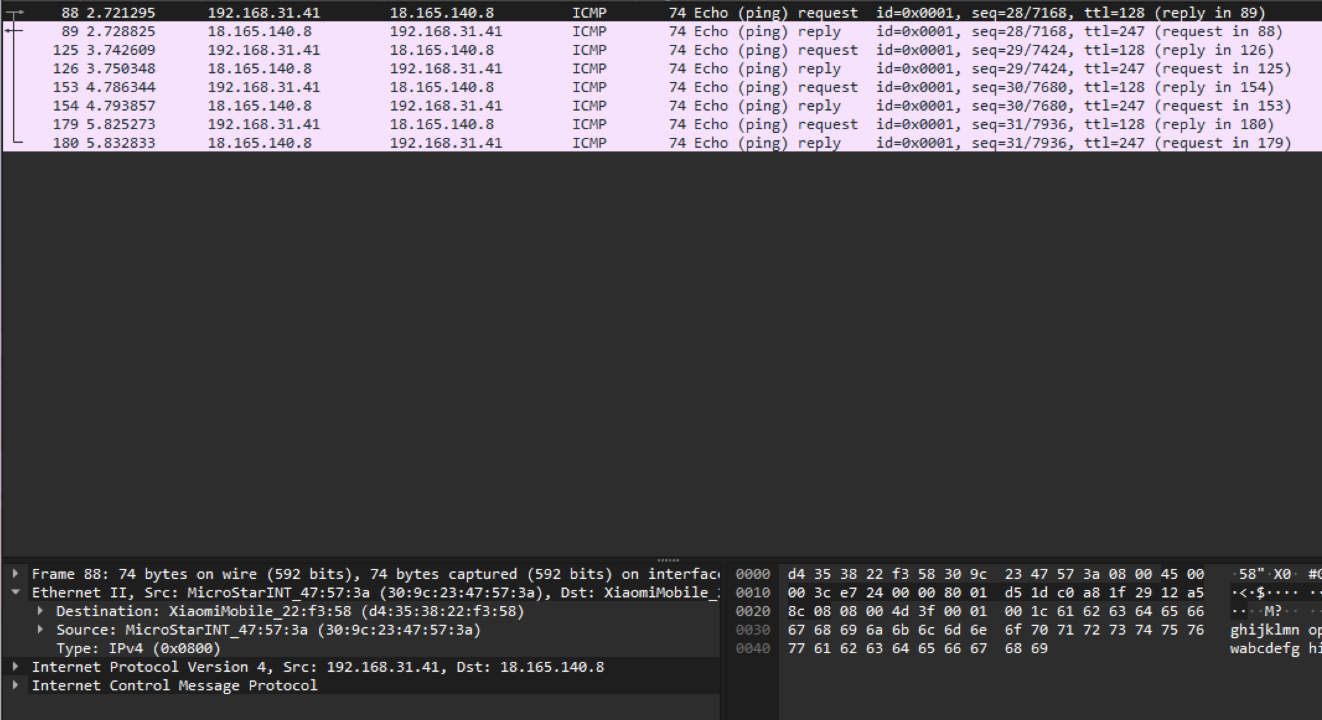
  
Ip-адрес positive.news: 188.114.99.229

Mac-адрес: d4:35:38:22:f3:58



Ip-адрес washingtonpost.com: 18.165.140.8

Mac-адрес: d4:35:38:22:f3:58



1. Ответьте на вопрос: почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?  
   В случае удаленных серверов Wireshark не может напрямую записывать их настоящие MAC-адреса, поскольку они не находятся в одной локальной сети. Вместо этого сохраняется MAC-адрес последнего маршрутизатора или шлюза перед тем, как пакет покинул локальную сеть. MAC-адрес удаленного сервера будет виден только в его локальной сети

## Анализ полей TCP

От ПК к серверу (SYN TCP):

|  |  |
| --- | --- |
| Название поля | Значение поля |
| IP-адрес источника | 192.168.31.41 |
| IP-адрес назначения | 198.246.121.209 |
| Номер порта источника | 53125 |
| Номер порта назначения | 443 |
| Порядковый номер | 0, 3242222356 |
| Номер подтверждения | 0, 0 |
| Длина заголовка | 32 b |
| Размер окна | 64240 |

Заполните приведенную ниже таблицу новыми данными с учетом сообщения SYN-ACK на основе своих данных от сервера.

|  |  |
| --- | --- |
| Название поля | Значение поля |
| IP-адрес источника | 198.246.121.209 |
| IP-адрес назначения | 192.168.31.41 |
| Номер порта источника | 443 |
| Номер порта назначения | 53125 |
| Порядковый номер | 0, 3286790501 |
| Номер подтверждения | 1, 3242222357 |
| Длина заголовка | 32b |
| Размер окна | 65535 |

Заполните приведенную ниже таблицу данными уже с учетом сообщения ACK.

|  |  |
| --- | --- |
| Название поля | Значение поля |
| IP-адрес источника | 192.168.31.41 |
| IP-адрес назначения | 198.246.121.209 |
| Номер порта источника | 53125 |
| Номер порта назначения | 443 |
| Порядковый номер | 1, 3242222357 |
| Номер подтверждения | 1, 3286790502 |
| Длина заголовка | 20 b |
| Размер окна | 1024(262144) |