**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Московский приборостроительный техникум**

**Лабораторная работа №4**

по учебной практике

УП.01.02 Средства мониторинга и анализа в локальных сетях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование практики*

Профессионального модуля ПМ.01«Выполнение работ по проектированию

сетевой инфраструктуры»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование профессионального модуля*

Специальность 09.02.06 Сетевое и системное администрирование

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*код и наименование специальности*

Студент Карпов Артем Владимирович

*(фамилия, имя, отчество)*

Группа СА50-1-22

Руководитель по практической подготовке от техникума

Кульчинская Нелли Андреевна

*(фамилия, имя, отчество)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 года

**ARP**

1. Выполнил команду arp -a в виртуальной машине linux. Я увидел ip адреса сопоставленные с их физическим адресом, это ARP таблица.

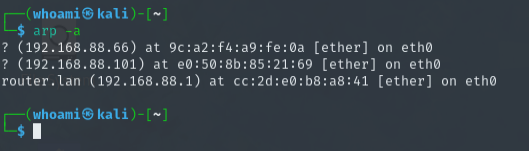
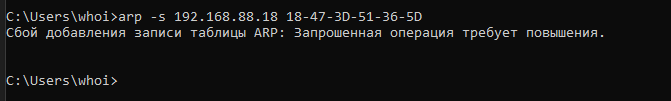


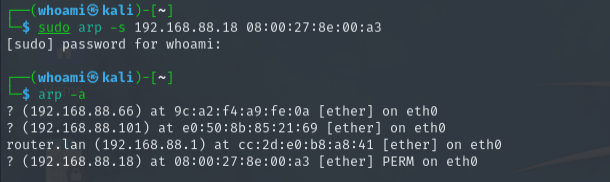
Рис. 1 – arp -a

1. Чтобы сделать статическую запись в ARP таблицу на разных ОС надо:

Windows



Linux



IOS

sudo arp -s 192.168.1.5 00:1c:b3:09:85:15

Cisco

arp <ip-address> <hardware-address> [arpa | probe | sap]

Где:

<ip-address> — IP-адрес устройства, для которого вы хотите добавить статическую ARP-запись.

<hardware-address> — MAC-адрес устройства.

[arpa | probe | sap] — необязательные параметры, указывающие тип ARP-записи. Обычно используется arpa для Ethernet сетей.

1. Просканировал свою сеть и отфильтровал по arp запросам

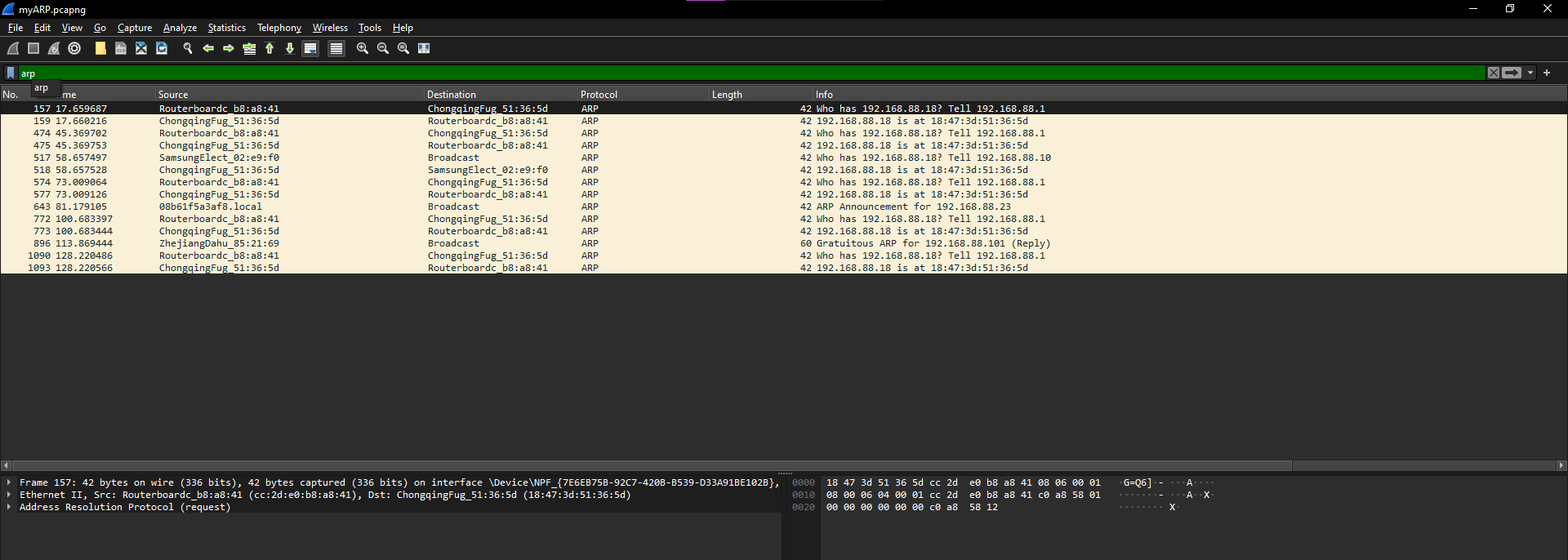


Рис. 3 – скан сети по arp

1. Таблица Ethernet

|  |  |  |
| --- | --- | --- |
| **Тип сообщения** | **MAC Адрес отправителя** | **MAC адрес получателя** |
| ARP запрос | cc:2d:e0:b8:a8:41 | 18:47:3d:51:36:5d |
| ARP ответ | 18:47:3d:51:36:5d | cc:2d:e0:b8:a8:41 |

1. Таблица ARP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Тип сообщения** | **MAC отправителя** | **IP адрес отправителя** | **Target MAC** | **Target IP** |
| Arp запрос | cc:2d:e0:b8:a8:41 | 192.168.88.1 | 00:00:00:00:00:00 | 192.168.88.18 |
| Arp ответ | 18:47:3d:51:36:5d | 192.168.88.18 | cc:2d:e0:b8:a8:41 | 192.168.88.1 |

1. Провел ARP разведку в своей локальной сети

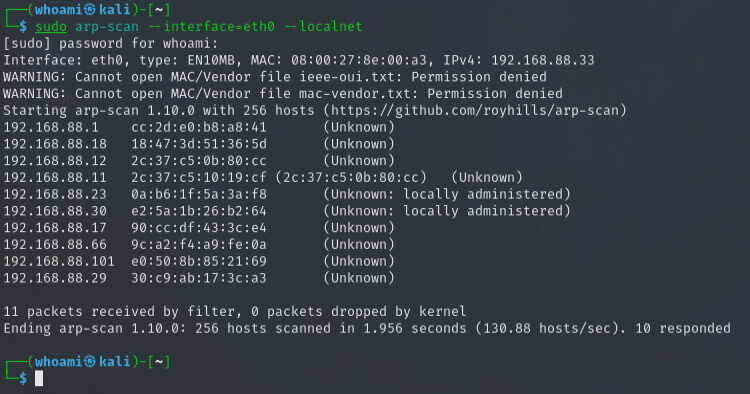


Рис. 4 – ARP разведка

Контрольные вопросы:

1. \*\*Протокол ARP в сети:\*\*

- \*\*Назначение:\*\* ARP (Address Resolution Protocol) используется для сопоставления IP-адресов сетевых узлов с их физическими (MAC) адресами. Когда устройство в сети знает IP-адрес, но не знает соответствующего ему MAC-адреса, оно использует ARP для определения MAC-адреса устройства.

- \*\*Уровень модели TCP/IP:\*\* Протокол ARP находится на канальном уровне (втором уровне) модели OSI и стека протоколов TCP/IP. Он работает с физическими адресами, обеспечивая связь между сетевым и канальным уровнями.

2. \*\*ARP Таблица:\*\*

- \*\*Назначение:\*\* ARP таблица содержит соответствия между IP-адресами и соответствующими им MAC-адресами в локальной сети. Она используется для ускорения процесса поиска физических адресов устройств в сети и избегания постоянных ARP-запросов для одних и тех же узлов.

3. \*\*Два адреса в сети IP и MAC:\*\*

- \*\*IP-адрес:\*\* Используется на сетевом уровне для идентификации узла в глобальной сети и обеспечивает маршрутизацию.

- \*\*MAC-адрес:\*\* Используется на канальном уровне для уникальной идентификации устройства в локальной сети. MAC-адресы несут информацию о производителе оборудования.

4. \*\*Широковещательный домен:\*\*

- \*\*Определение:\*\* Широковещательный домен - это сегмент сети, в котором широковещательные пакеты могут достигнуть всех устройств. В сетях Ethernet широковещательные пакеты обычно используются с MAC-адресом, в котором все биты установлены в 1 (например, FF:FF:FF:FF:FF:FF).

- \*\*Применение:\*\* ARP-запросы, DHCP-запросы и другие сетевые службы используют широковещательные пакеты для обнаружения устройств в пределах локальной сети. Широковещательные пакеты не покидают границы широковещательного домена.

**IP, ICMP**

1. Запустил Wireshark и начал захват трафика на активном сетевом интерфейсе.

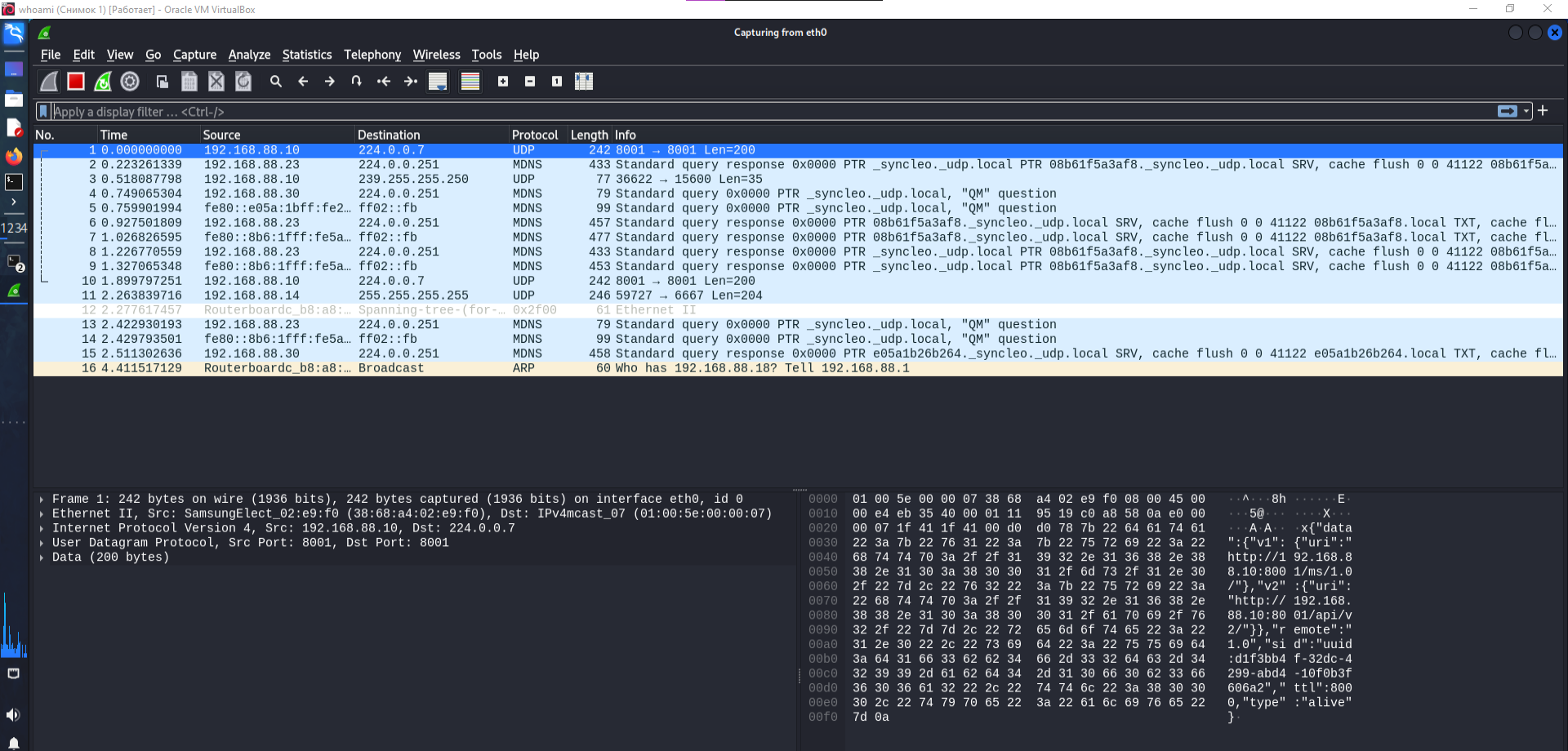


Рис. 1 – захват трафика

1. Открыл консоль и выполнил команду ping 8.8.8.8

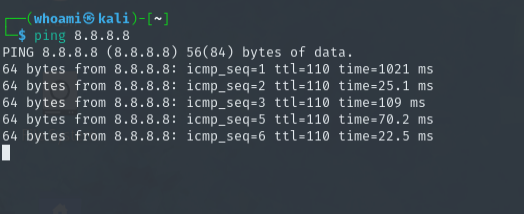


Рис. 2 – ping

1. Таблица ICMP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Тип пакета** | **IP адрес отправителя** | **IP адрес получателя** | **TTL** | **следующий протокол** |
| PC, linux | 192.168.88.33 | 8.8.8.8 | 64 |  |
| Unix, server | 8.8.8.8 | 192.168.88.33 | 84 |  |

1. Время ответа от 8.8.8.8 составило 1020.691 ms

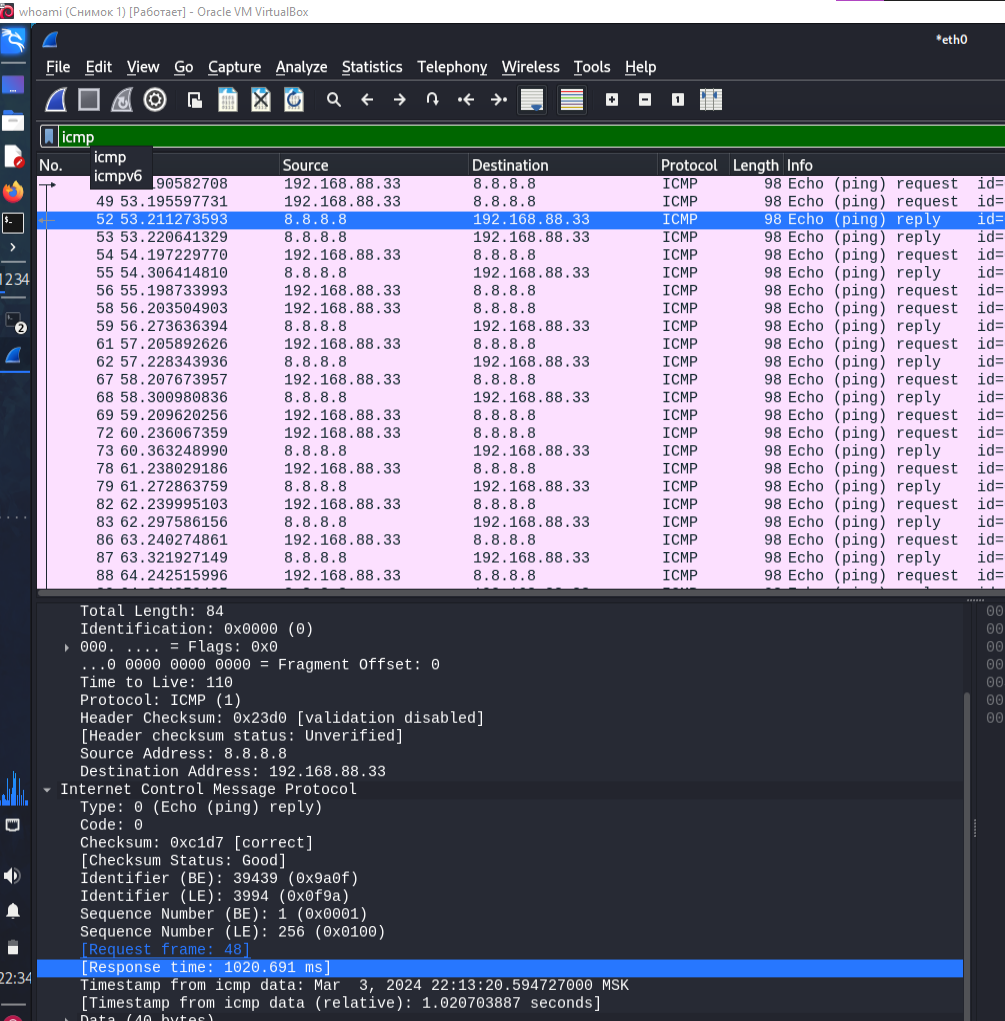


Рис. 3 – время ответа 8.8.8.8

1. Скачал и открыл файл в wireshark

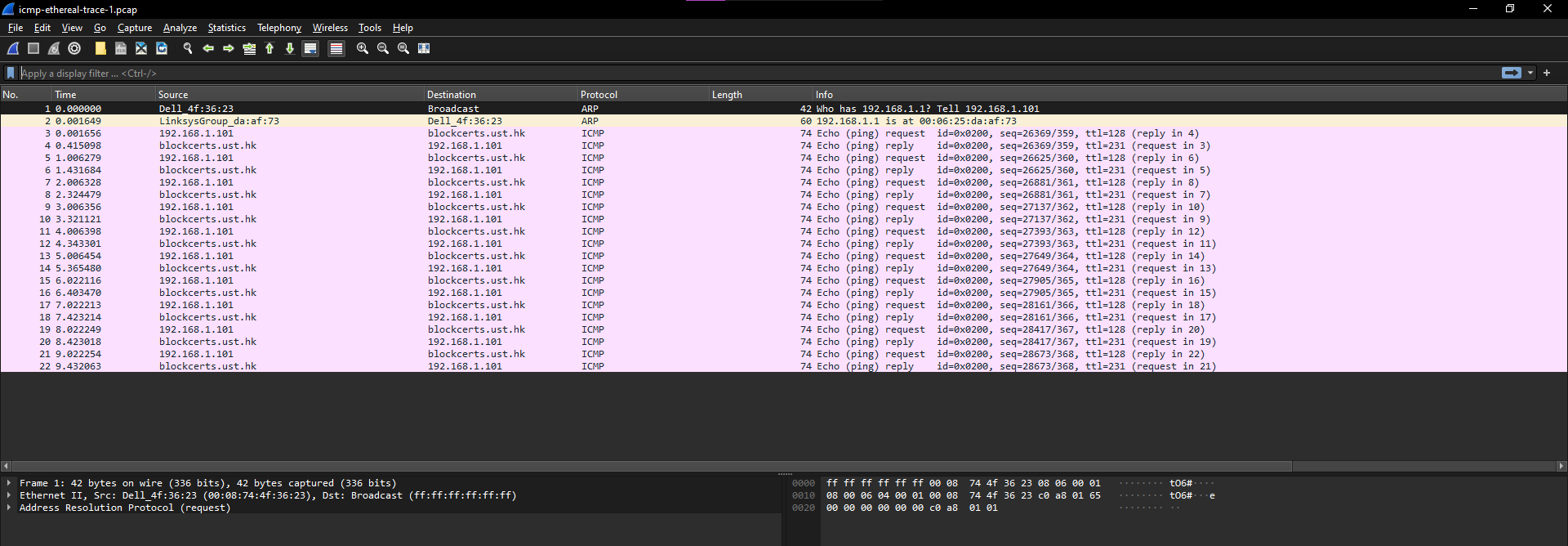


Рис. 4 – скаченный dump

|  |  |
| --- | --- |
| **Тип и номер пакета** | **Время ответа** |
| 1) ICMP ответ | 413.442 ms |
| 2) ICMP ответ | 425.405 ms |
| 3) ICMP ответ | 318.151 ms |
| 4) ICMP ответ | 314.765 ms |
| 5) ICMP ответ | 336.903 ms |
| 6) ICMP ответ | 359.026 ms |
| 7) ICMP ответ | 381.354 ms |
| 8) ICMP ответ | 401.001 ms |
| 9) ICMP ответ | 400.769 ms |
| 10) ICMP ответ | 409.809 ms |

Среднее время ответа: 376,0625 ms

1. Выполнил команду traceroute 8.8.8.8. Наибольшая задержка была 36,921 ms

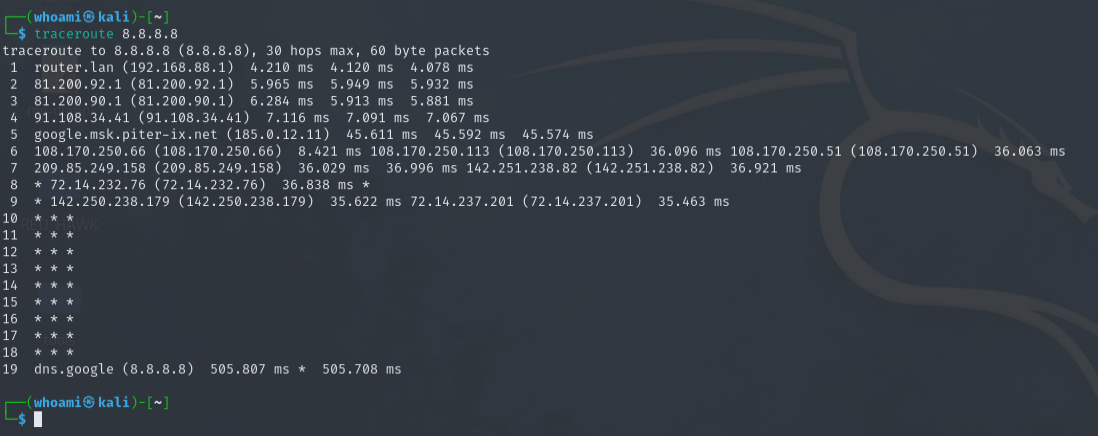


Рис. 5 – traceroute

Контрольные вопросы:

1. \*\*Протокол IP:\*\*

- \*\*Представление:\*\* Протокол IP (Internet Protocol) представляет собой сетевой протокол, отвечающий за маршрутизацию и доставку пакетов данных между узлами в сети.

- \*\*Область применения:\*\* Используется для маршрутизации и передачи данных в глобальных сетях, таких как Интернет.

- \*\*Уровень модели TCP/IP:\*\* IP находится на сетевом уровне (третьем уровне) модели OSI и стека протоколов TCP/IP.

2. \*\*Поля пакета IP:\*\*

- \*\*Source IP Address (Адрес отправителя) \*\*

- \*\*Destination IP Address (Адрес получателя) \*\*

- \*\*Version (Версия)\*\*

- \*\*Header Length (Длина заголовка)\*\*

- \*\*Type of Service (Тип обслуживания)\*\*

- \*\*Total Length (Общая длина)\*\*

- \*\*Identification (Идентификатор)\*\*

- \*\*Flags (Флаги)\*\*

- \*\*Fragment Offset (Смещение фрагмента)\*\*

- \*\*Time to Live (Время жизни)\*\*

- \*\*Protocol (Протокол)\*\*

- \*\*Header Checksum (Контрольная сумма заголовка)\*\*

- \*\*Options (Опции)\*\*

- \*\*Padding (Дополнение)\*\*

- \*\*Data (Данные)\*\*

3. \*\*TTL (Time to Live):\*\*

- \*\*Определение:\*\* TTL представляет собой поле в заголовке IP-пакета, которое указывает максимальное количество переходов (хопов) пакета по сети, прежде чем он будет отброшен.

- \*\*Назначение:\*\* Используется для предотвращения бесконечного цикла в сети и ограничения времени жизни пакета.

4. \*\*Протокол ICMP:\*\*

- \*\*Представление:\*\* Протокол ICMP (Internet Control Message Protocol) - это протокол для передачи сообщений об ошибках и контроля состояния сети.

- \*\*Область применения:\*\* Используется для отправки сообщений об ошибках, тестирования сетевой связности (например, с помощью утилиты Ping).

- \*\*Уровень модели TCP/IP:\*\* ICMP находится на сетевом уровне (третьем уровне) модели OSI и стека протоколов TCP/IP.

5. \*\*Утилиты, использующие ICMP:\*\*

- \*\*Ping:\*\* Проверяет доступность узла в сети и измеряет время, необходимое для передачи пакета к узлу и обратно.

- \*\*Traceroute (traceroute в UNIX/Linux, tracert в Windows):\*\* Отслеживает маршрут пакета к указанному узлу, указывая IP-адреса промежуточных узлов.

- \*\*PathPing:\*\* Комбинирует функциональность утилиты Ping с отслеживанием маршрута, анализом производительности и обнаружением проблем в сети.

6. \*\*Wireshark и анализ протокола ICMP:\*\*

- Wireshark позволяет отслеживать и анализировать сетевой трафик, включая пакеты ICMP. Можно просматривать содержимое пакетов, IP- и MAC-адреса, время жизни (TTL) и другую информацию.

7. \*\*Расчет Response Time в ICMP:\*\*

- Response Time в ICMP измеряется с использованием утилиты Ping и представляет собой время, затраченное на отправку пакета к узлу и получение ответа. Время измеряется в миллисекундах и предоставляет информацию о задержке в сети.