

Міністерство освіти і науки України Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського” Факультет інформатики та обчислювальної техніки Кафедра інформаційних систем та технологій

Лабораторна робота №2

**Тестування та контроль якості (QA) вбудованих систем**

«*Дослідження засобів канального рівня моделі OSI. Протокол ARP»*

Варіант 17

|  |  |
| --- | --- |
| Виконав: | Перевірила: |
| студент групи ІА-13 |  |
| Окаянченко Д.О. | Міщенко Л.Д. |

Київ 2024

**Тема:** налаштування мережного оточення та тестування протоколу ARP.

**Мета:** навчитися налаштовувати мережне оточення для тестування вбудованих систем та пристроїв IoT. Навчитися використовувати утиліту wireshark для аналізу трафіка в комп’ютерній мережі. Протестувати мережне оточення на канальному рівні моделі OSI.

# Завдання

▪ налаштувати оточення для експериментального дослідження основних

процесів та артефактів канального рівня моделі ОSI, зокрема форматів

фреймів Ethernet, формату MAC адрес, протоколу ARP;

▪ експериментально ознайомитися з протоколом передавання службових

повідомлень ІCMP;

▪ навчитися користуватися мережною утілітою ping;

▪ з використанням програми wireshark дослідити основні етапи отримання

MAC адрес протоколом ARP на канальному рівні моделі OSI.

**QA завдання:**

Згідно з визначеними варіантами описати **Test-case**.

**Визначення варіанту:** Останні дві цифри номеру залікової книжки розділити на три. Остача від ділення і буде номером варіанту.

1. Переконатися в отриманні МАС-адреси по відомій IP-адресі.
2. Переконатися в тому, що arp-таблиця оновлюється при отриманні arp-reply.
3. Додати статичний запис у arp-таблицю та після цього пропінгувати інший пристрій, при цьому відстежувати трафік у wireshark.

## Визначення варіанту

Розрахунок варіанту: 71 mod 3 = 2

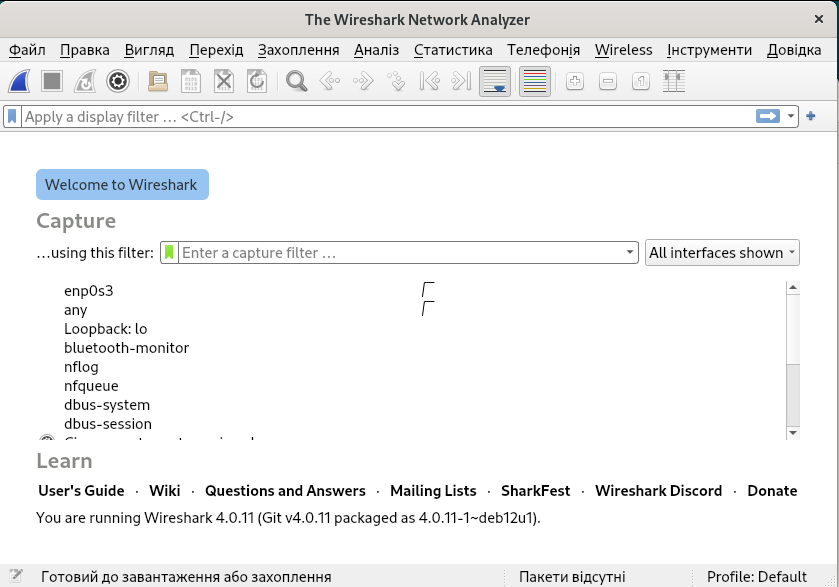
*2) Додати статичний запис у arp-таблицю та після цього пропінгувати інший пристрій, при цьому відстежувати трафік у wireshark.*

# Хід роботи

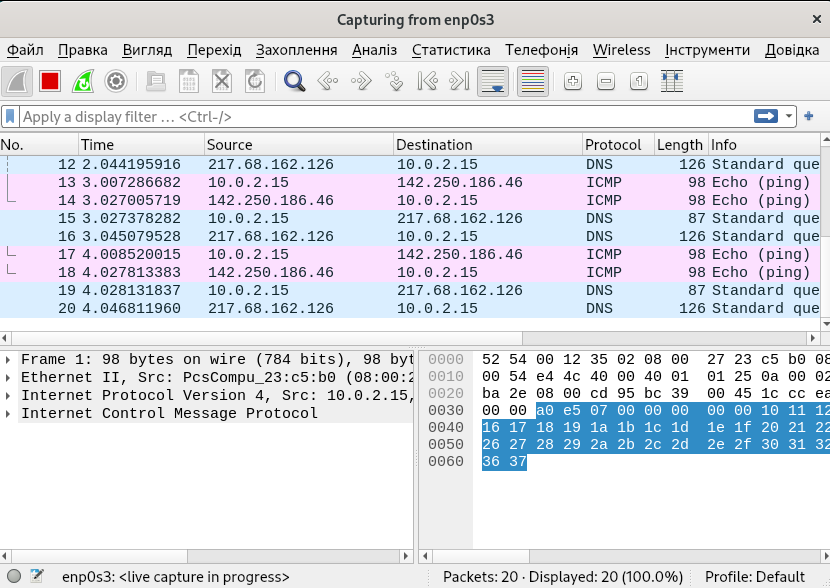
**Посилання на репозиторій:** [**https://github.com/mrEkso/QA\_Testing**](https://github.com/mrEkso/QA_Testing)**.**

1. Налаштовуємо мережеве оточення 1.1.Встановлюємо Wireshark

Так як я буду використовувати дві віртуальні машини Debian + lubuntu.

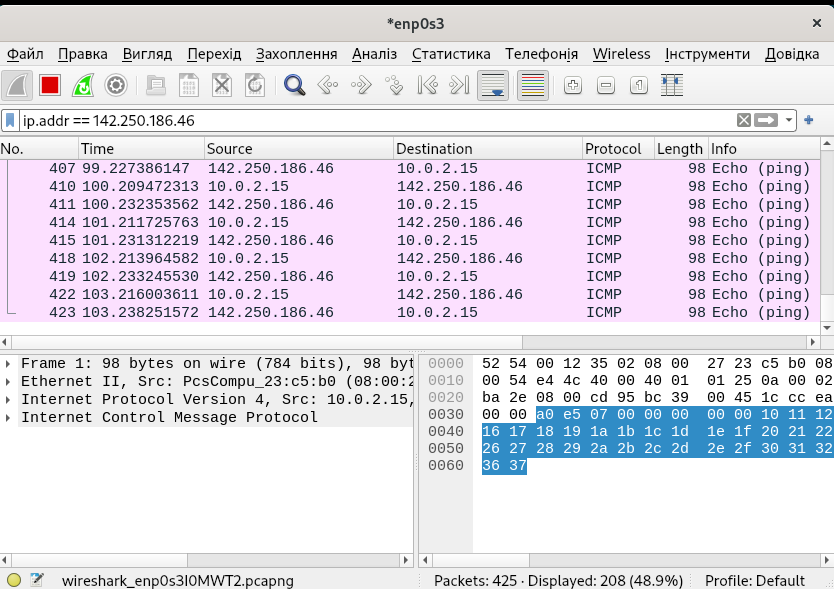


* 1. Захоплюємо пакети у Wireshark.

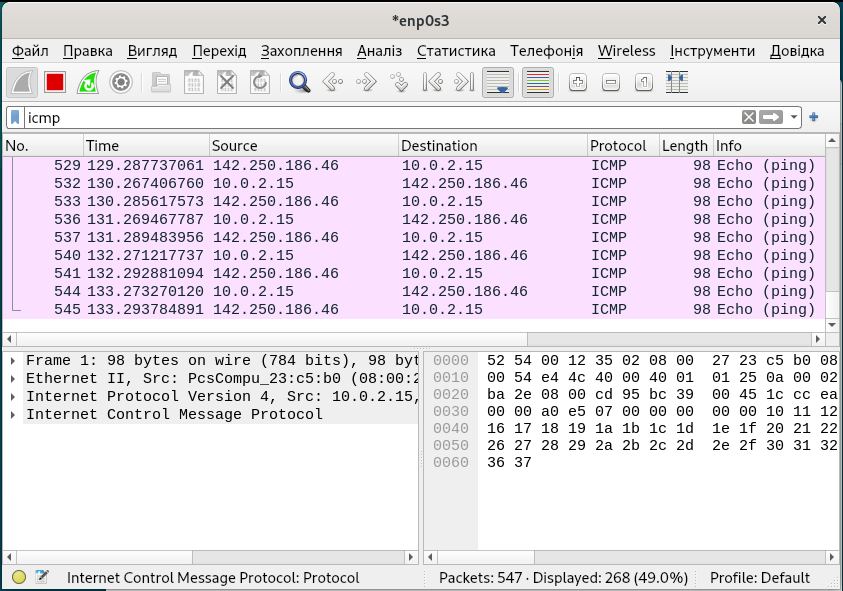


* 1. Налаштування фільтрів у Wireshark.

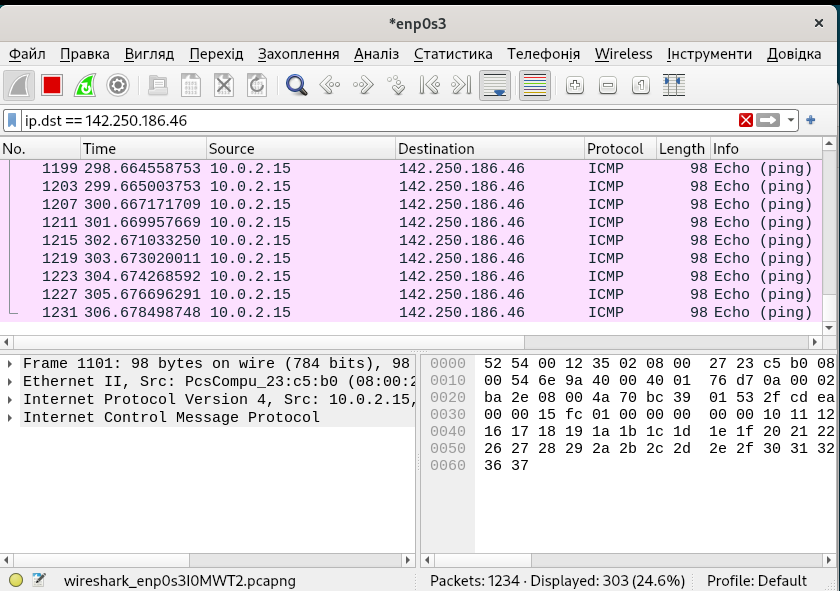
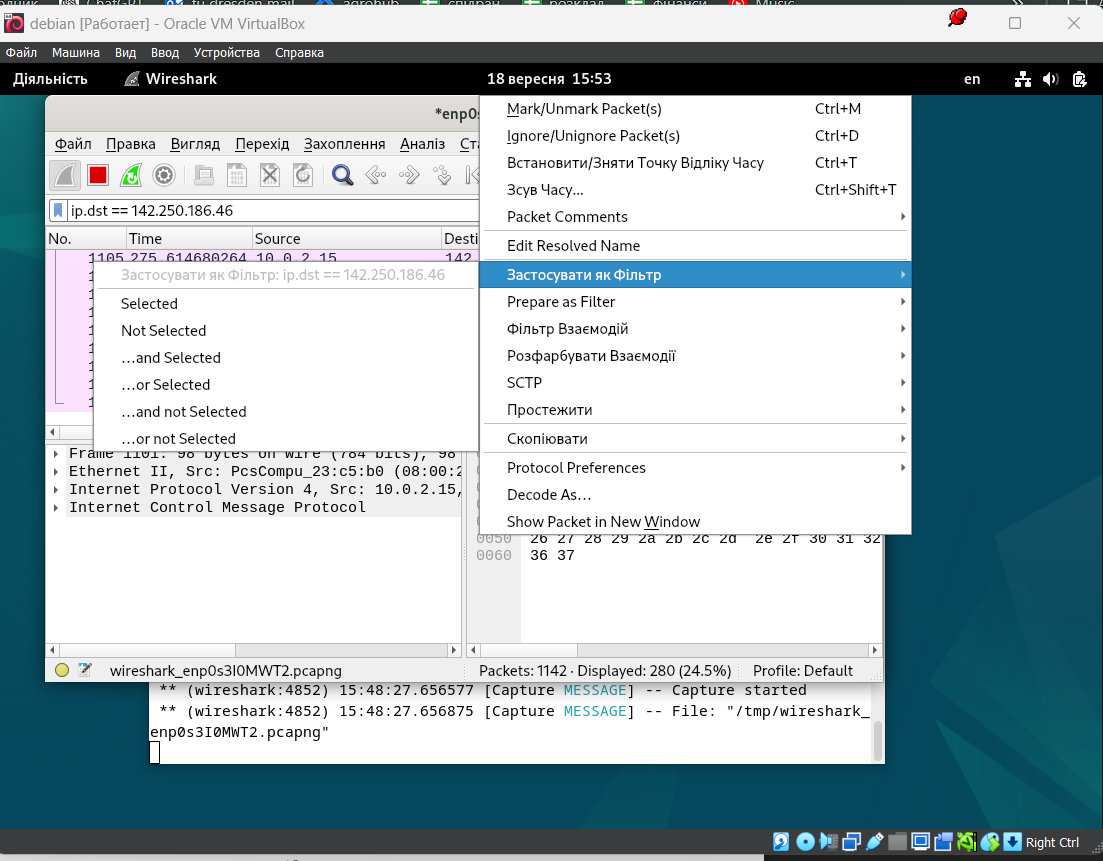
*фільтр по ІР-адресі*

**

*фільтр по протоколу*

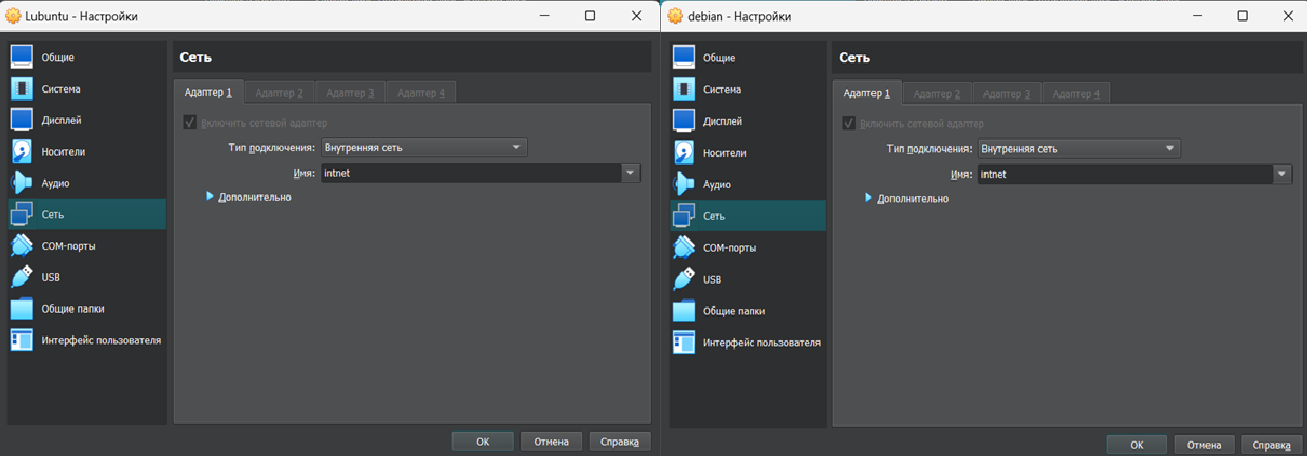
**

*Apply as Filter*

**

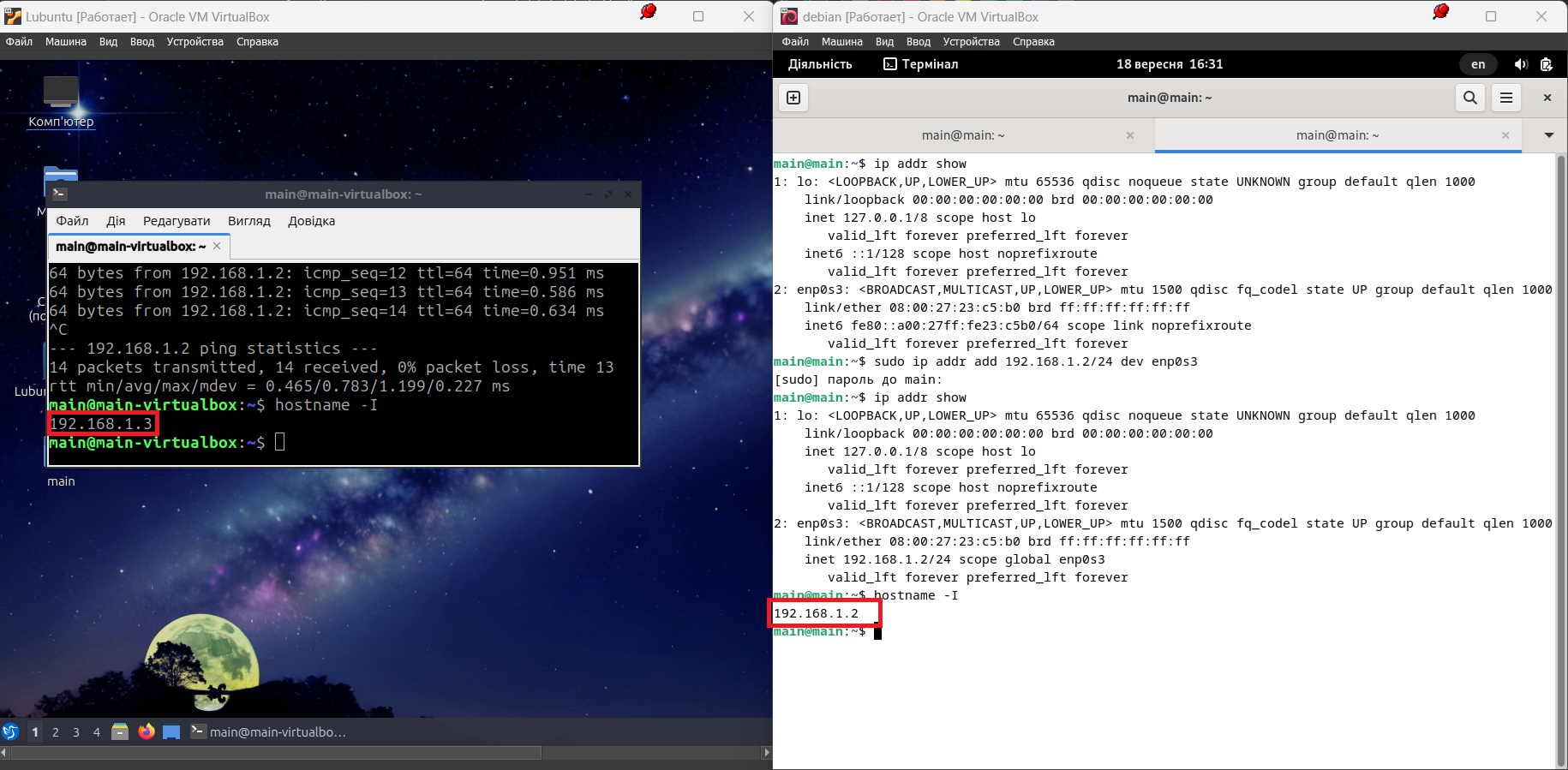
1. Для коректного виконання завдання налаштуємо внутрішню мережу

на обох віртуальних машинах.



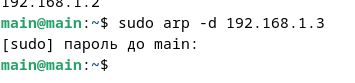
Lubuntu (ВМ2) буде використовуватися як основний приймаючий пристрій, на який буде здійснюватися надсилання ICMP-запитів.

Попередньо дізнаємся IP-адресу ВМ1 та ВМ2.

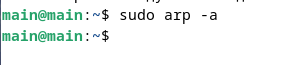


Тепер працюємо на Debian (ВМ1).

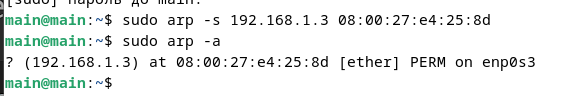
1. Очищуємо arp таблицю від IP-адреси ВМ1:



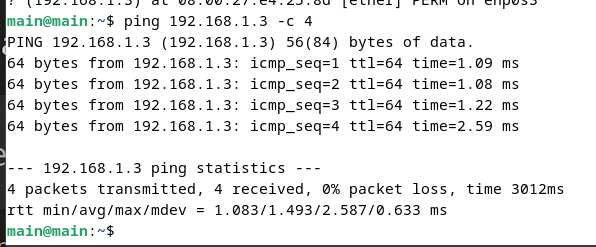
1. Переконуємось, що arp таблиця порожня:



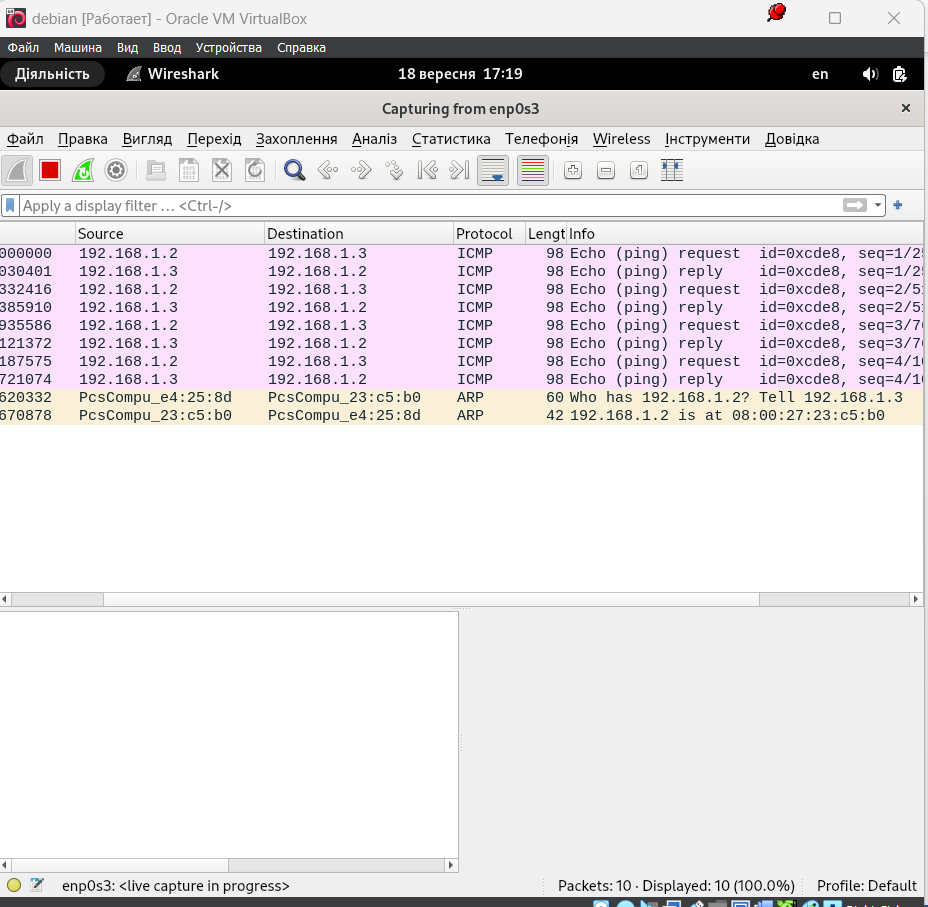
1. Додаємо статичний запис до ARP таблиці за IP-адресою та фізичної MAC-адресою.



1. Виконаємо пінг до цільової машини.



1. Аналізуємо отриманий трафік у Wireshark:



З наведеного зображення видно, що ICMP-повідомлення відправляються попередньо без ARP-запита, адже ми вже маємо його в таблиці.

QA Test-case #2

Test objective: Add a static entry to the arp table and then ping another device, while monitoring traffic in wireshark.

Description:

* + Two virtual machines with Linux (VM1 & VM2)
  + VMs connected with each other by Internal Network
  + Wireshark is available on the VM1

|  |  |  |
| --- | --- | --- |
|  | Steps | Expected result |
| 1 | Clear arp-table | Arp-table is empty |
| 2 | Start capturing process in Wireshark | Capturing process is started |
| 2 | Run ping traffic from VM1 to VM2 by ping | Ping is running |
| 4 | Wait up to about 5 seconds and stop  capturing | Capturing process is  Stopped |
| 5 | Analyze arp-table | Verify that no ARP-request was sent beforehand |

**Висновок:** У ході виконання цієї лабораторної роботи я навчився налаштовувати мережне оточення для тестування вбудованих систем та пристроїв IoT, а також використовувати утиліту wireshark для аналізу трафіка в комп’ютерній мережі, протестувавши протокол ARP.