****

Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет інформатики та обчислювальної техніки

Кафедра автоматики та управління в технічних системах

# Лабораторна робота №1 Дослідження засобів канального рівня моделі OSI. Протокол ARP

|  |  |  |
| --- | --- | --- |
| Виконав  студент групи ІА-92: |  | Перевірила: |
|  |  |  |
|  |  |  |
| Мешко І.С. |  | Гайдай |

Київ 2022

**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.

**Тестова документація:**

### Перед початком перевірки треба втановити **Wireshark** для аналізу мережевих протоколів на 1 комп’ютері (PC1).Він дозволяє бачити, що відбувається у мережі, на мікроскопічному рівні **Встановимо та запустимо wireshark:**

1. Додайте офіційний, PPA щоб завантажити останню стабільну версію

$ sudo add-apt-repository ppa:wireshark-dev/stable

1. Оновіть списки пакетів з репозиторіїв для оновлення пакетів

$ sudo apt-get update

1. Завантажте ***wireshark***

$ sudo apt-get install wireshark

1. Запустіть ***wireshark***

$ sudo wireshark

Якщо ви отримали таку помилку, що зображена на рис. 1.1, слід ввести

наступну команду, виконання якої відкриє вікно для конфігурації (рис. 1.2):

$ sudo dpkg-reconfigure wireshark-common

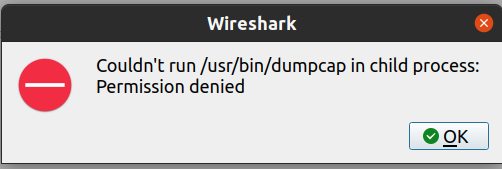


Рис.1.1. Повідомлення про помилку

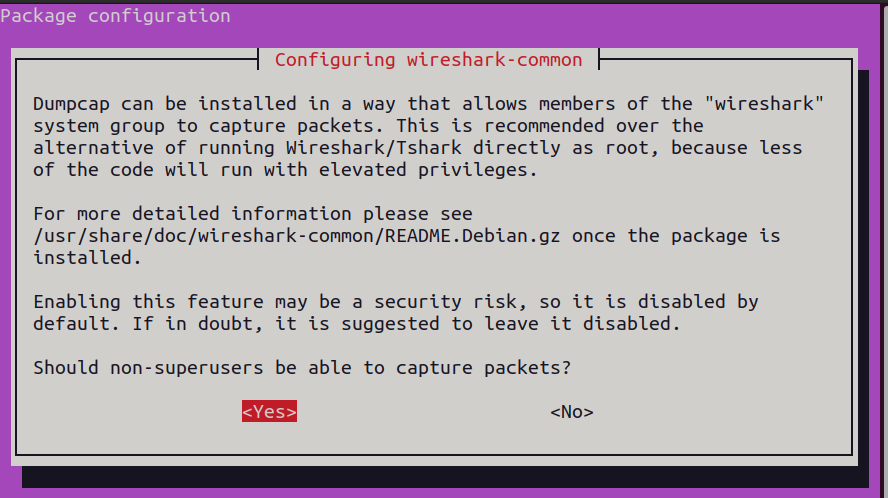


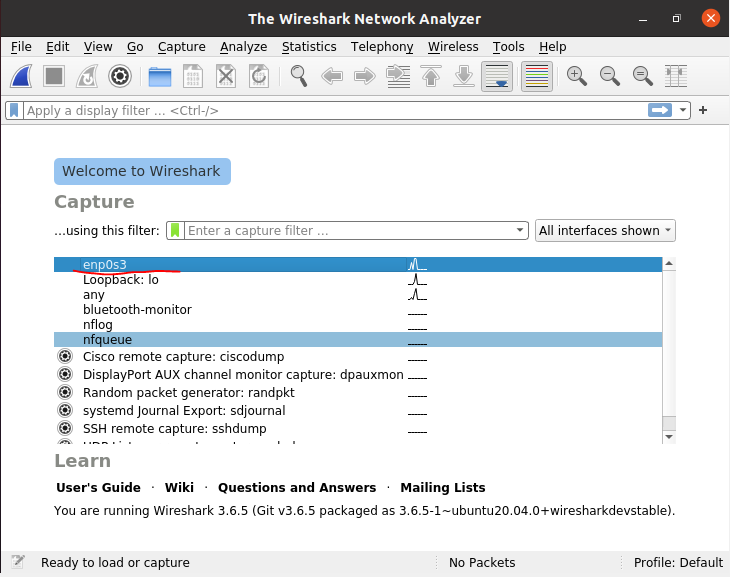
Рис. 1.2. Вікно для конфігурації

Оберіть опцію «Yes». Оскільки ви дозволили не-суперкористувачу (***non- superuser***) перехоплювати пакети, то необхідно додати користувача в групу ***wireshark*** наступною командою:

$ sudo adduser $USER wireshark

**Захоплення пакетів у Wireshark:**

Після запуску ***Wireshark***, ви побачите список доступних інтерфейсів, які ви можете використати для захоплення пакетів (рис. 1.3).

  
Рис. 1.3. Перелік інтерфейсів для аналізу трафіка  
  
  
  
  
Спробуйте в іншому терміналі ввести $ ping google.com та відстежити трафік, який передається через обраний інтерфейс – *захоплення пакетів* програмою ***Wireshark*** (рис. 1.4).

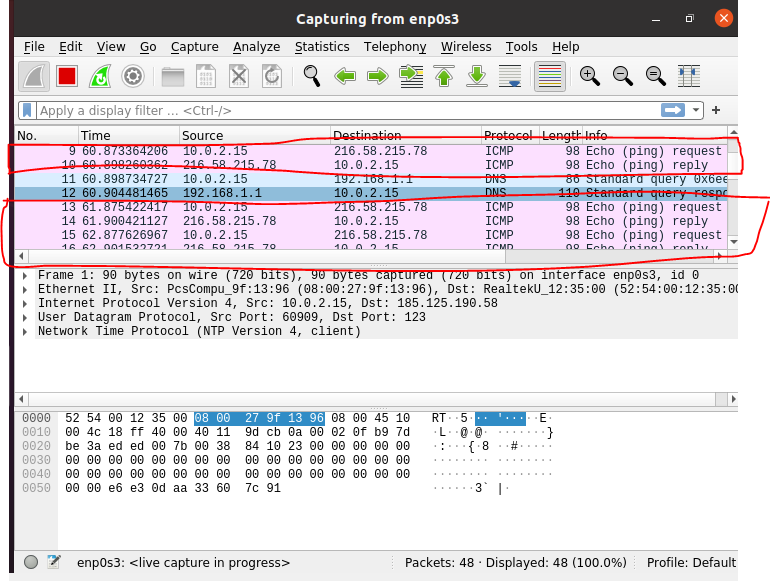


Рис. 1.4. Перегляд інформації про захоплення пакетів

Щоб припинити захоплення пакетів, необхідно натиснути на червону піктограму (рис. 1.5).

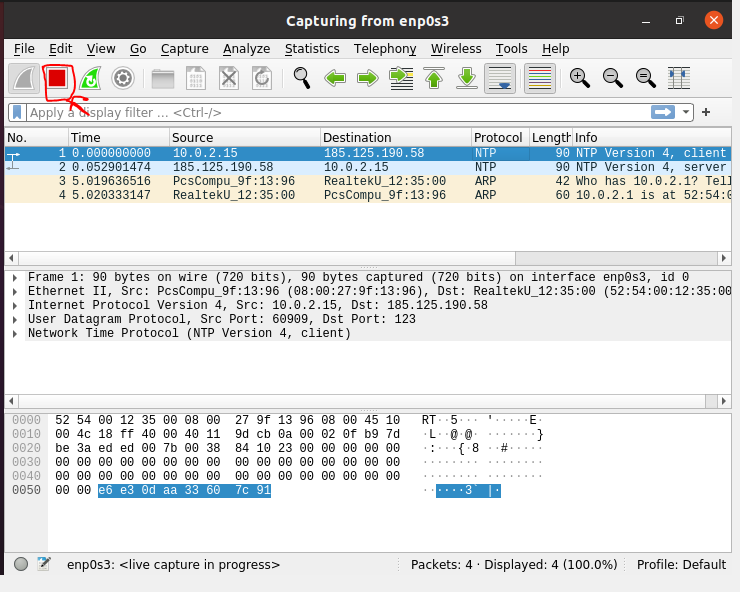
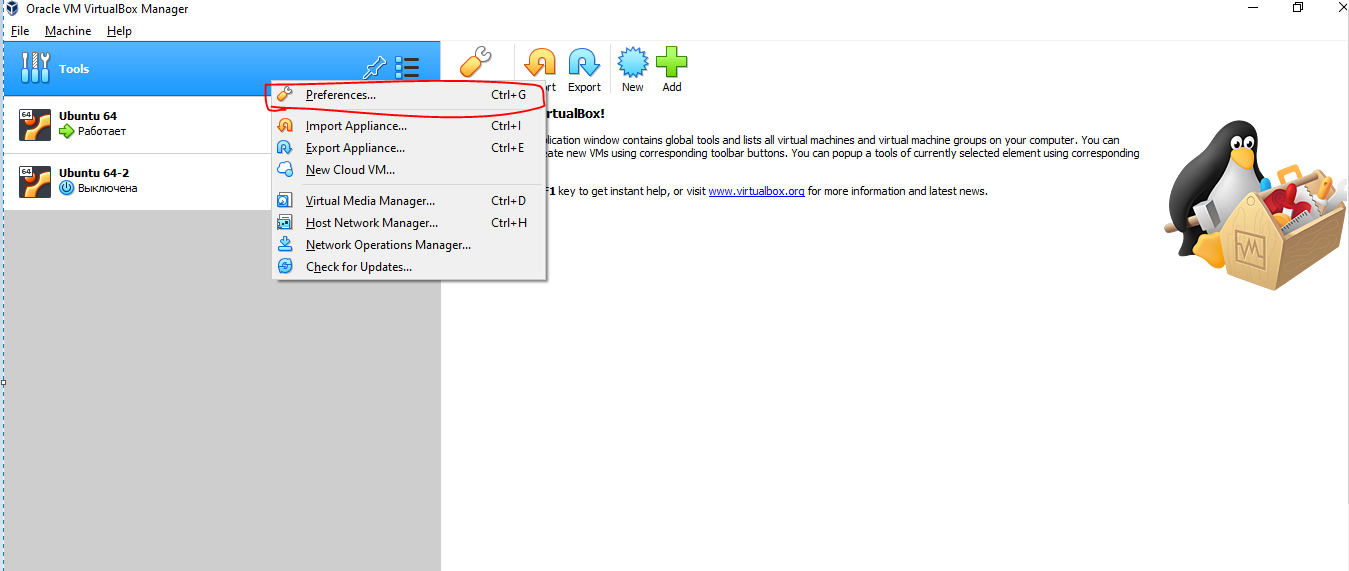
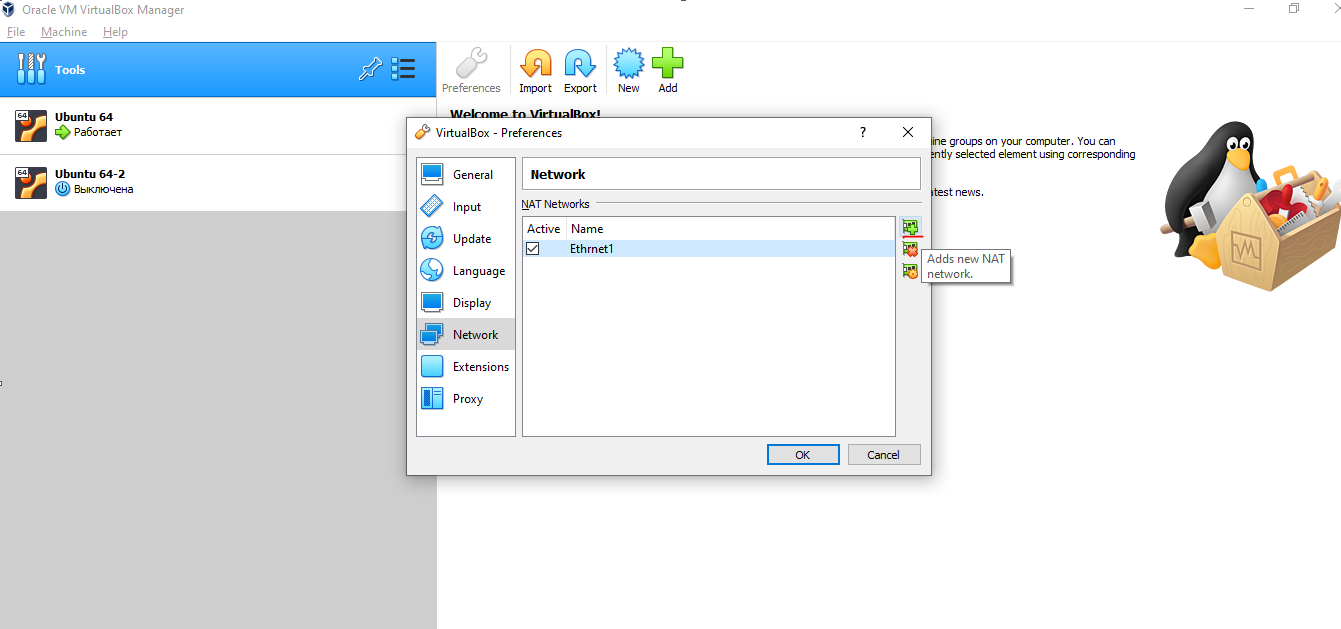
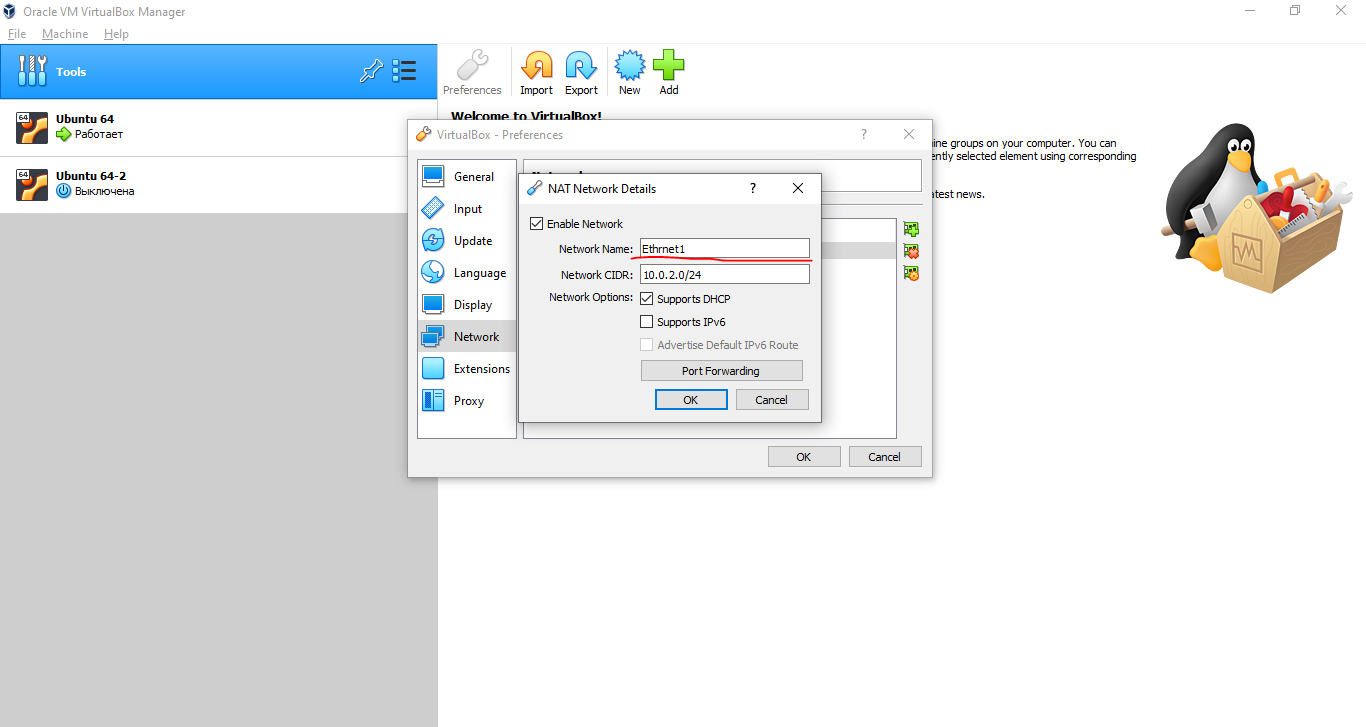


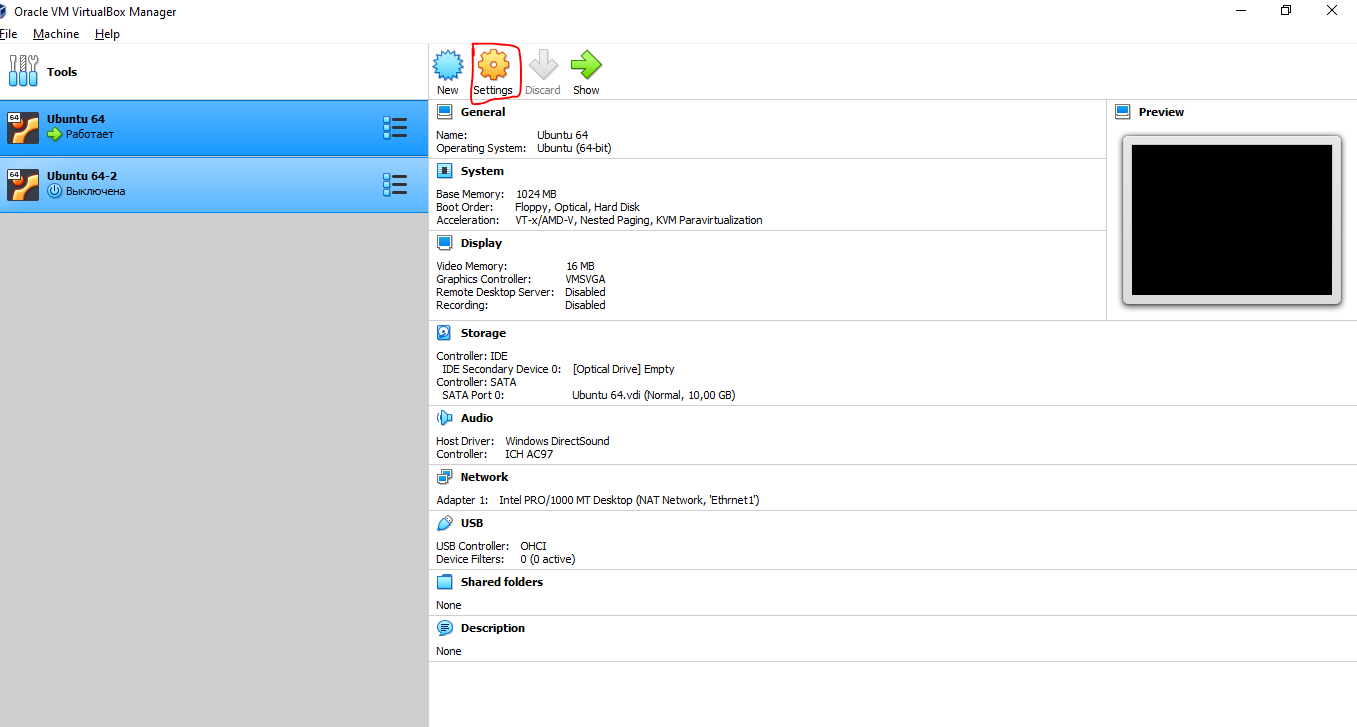
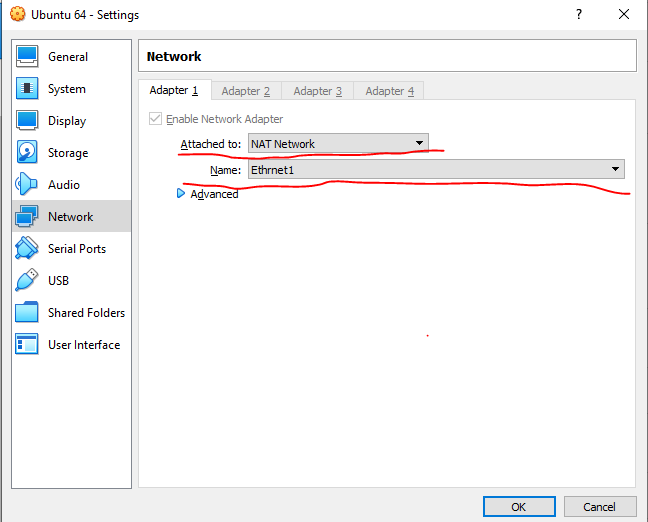
Рис. 1.5. Припинення захоплення пакетів

**Налаштування мережі**Для виконання завдання лабораторної роботи, нам пострібно з’єднанайте два PC один з

одним через інтерфейс NAT Network.  
Step:

1. У VirtualBox натисніть у верхній частині Tools правою кнопкою мищі та виберіть Preferences   
   
2. Далі, вам виведе вікно, після якого потрібно натисніть Nework та натиснути “Adds new NAT network”   
   
3. Після натискання у “Списку мереж” з’явиться нова мережа, у випадках перейменування, потрібно натиснути на неї двічі, і після редагування натисніть “OK”



1. Далі виберіть любу віртуальну машину, та натисніть Setting  
   
2. Після натискання перейдіть до вкладки Network, та у “Attached to”  
   Виберіть NAT Network   
   
3. Далі натисніть “OK”

### **Завдання на лабораторну роботу**

QA завдання:

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

Визначення варіанту: 0) Переконатися в отриманні МАС-адреси по відомій IP-адресі.

**Результати виконання практичного завдання**

Title: ARP функціонал. Розпізнавання MAC за IP-адресою

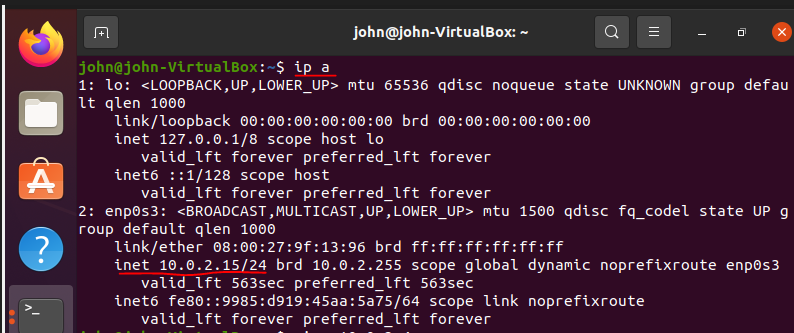
Description: переконайтеся, що протокол ARP розпізнає MAC та оновіть таблицю arp

Version: ARP v1

Setup Description:  
PC1 ----etherne1 ---- PC2

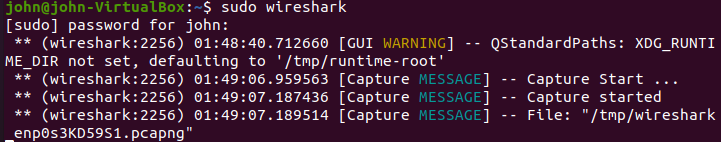
PC1: 10.0.2.15

PC2: 10.0.2.4

Prerequisites: Щоб дізнатися який IP у віртуальні машині потрібно в терміналі самій віртуальці ввести “ip -a”, та виберіть IP в залежності від мережі  


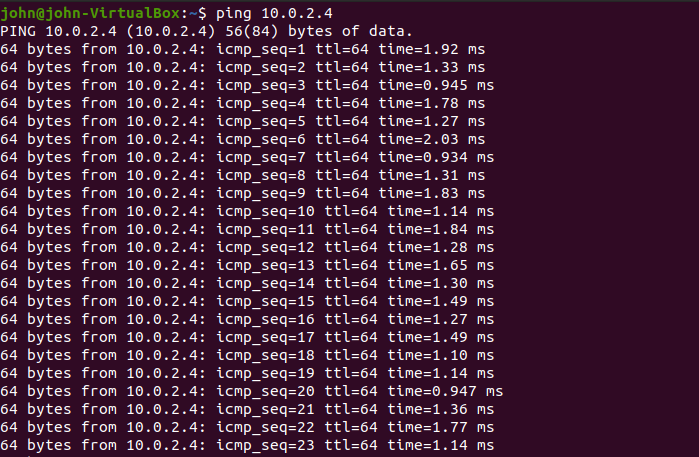
Steps:

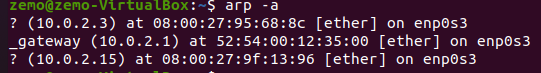
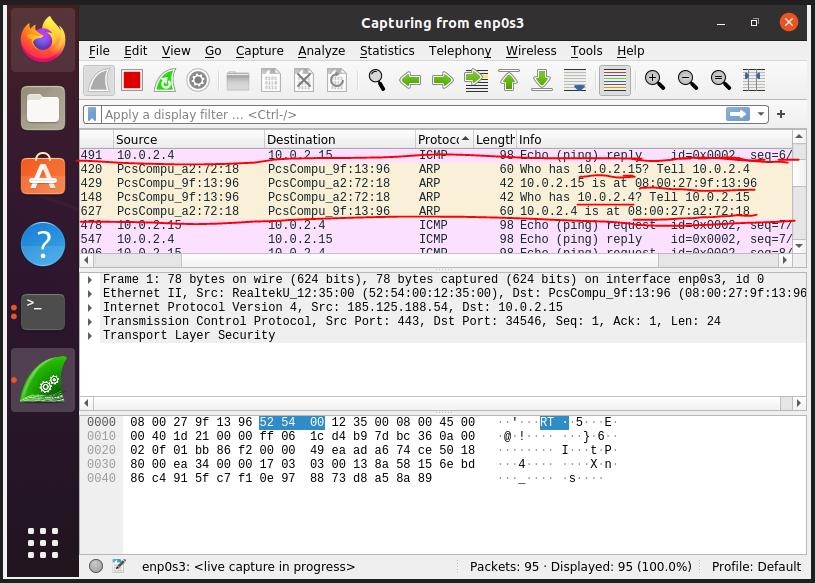
1. Почистіть arp таблиці через команду:  
   sudo arp -d <для IP PC2>
2. Далі запустіть на Wireshark на PC1:

sudo wireshark  


1. Далі запустіть новий термінал та пінганіть з PC1 на PC2:

ping PC2



1. Звіряємося з ARP таблицею з команди arp – a  
   
2. Звіряємося з Wireshark ARP протоколом  
   

Посилання на репозиторій:

<https://github.com/Jou2323/QA-Lab1.git>

Висновок: У даній лабораторній роботі я зрозумів як робити зробити перший Test Case з ARP запитами, та аналізувати мережевий трафік за допомогою програми WireShark