Лабораторна робота №1

“Налаштування оточення та тестування протоколу ARP”

**Мета**: Ознайомитися з ARP та ICMP протоколами. Навчитися аналізувати трафік за допомогою утиліти wireshark.

**Засоби**: утиліта ping, wireshark

**Теоретичні відомості та встановлення додаткових програм**

Утиліта ping — дозволяє переконатися у доступності віддаленого хоста. Для цього ping перевіряє, чи відповідає хост на мережеві запити, використовуючи протокол ICMP. Утиліта передає невеликий пакет з даними ICMP і очікує відповідь. Якщо відповідь отримана, то вважається, що віддалений хост доступний.

Протокол ICMP (Internet Control Message Protocol) — мережевий протокол, який використовується для передачі службових повідомлень та повідомлень про помилку.

Протокол ARP (Address Resolution Protocol) — дозволяє дізнатися МАС-адресу по ІР-адресі.

**Wireshark**

Wireshark - це передовий та широко використовуваний аналізатор мережевих протоколів. Він дозволяє бачити, що відбувається у мережі, на мікроскопічному рівні. Працює з переважною більшістю протоколів і надає повну інформацію про протокол, дозволяючи дізнатися значення кожного поля протоколу. Аналізатори мережевих протоколів потрібні для того, щоб досліджувати мережеві програми та протоколи, а також, щоб знаходити проблеми в роботі мережі та виявляти причини цих проблем.

Wireshark своїм функціоналом схожа на tcpdump, проте на відміну від tcpdump, має графічний інтерфейс, який дуже зручний та зрозумілий.

Також, Wireshark має дуже потужну систему фільтрів.

Встановимо та запустимо wireshark:

1) Додайте офіційний PPA, щоб завантажити останню стабільну версію

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

2) Оновіть списки пакетів з репозиторіїв для оновлення пакетів

sudo apt-get update

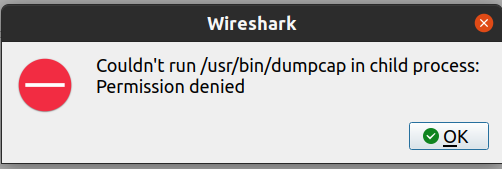
3) Завантажте wireshark

sudo apt-get install wireshark

4) Запустіть wireshark

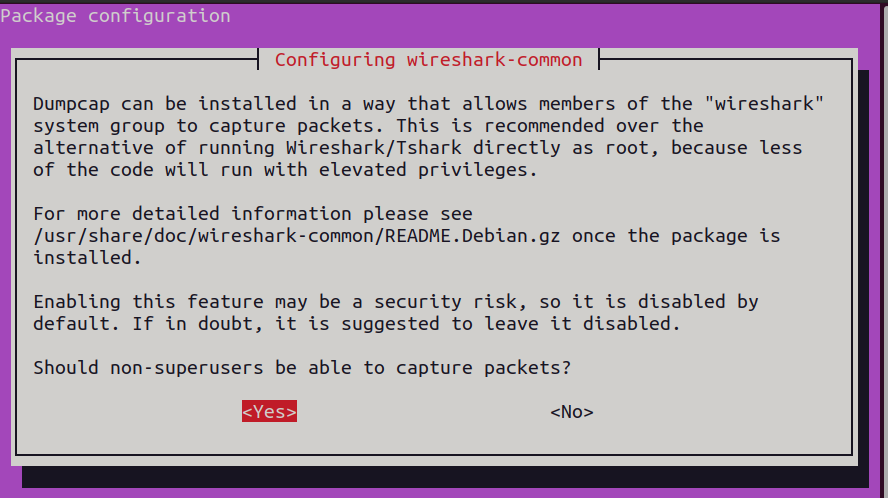
$ sudo wireshark

Якщо ви отримали таку помилку



то введіть наступну команду:

$ sudo dpkg-reconfigure wireshark-common



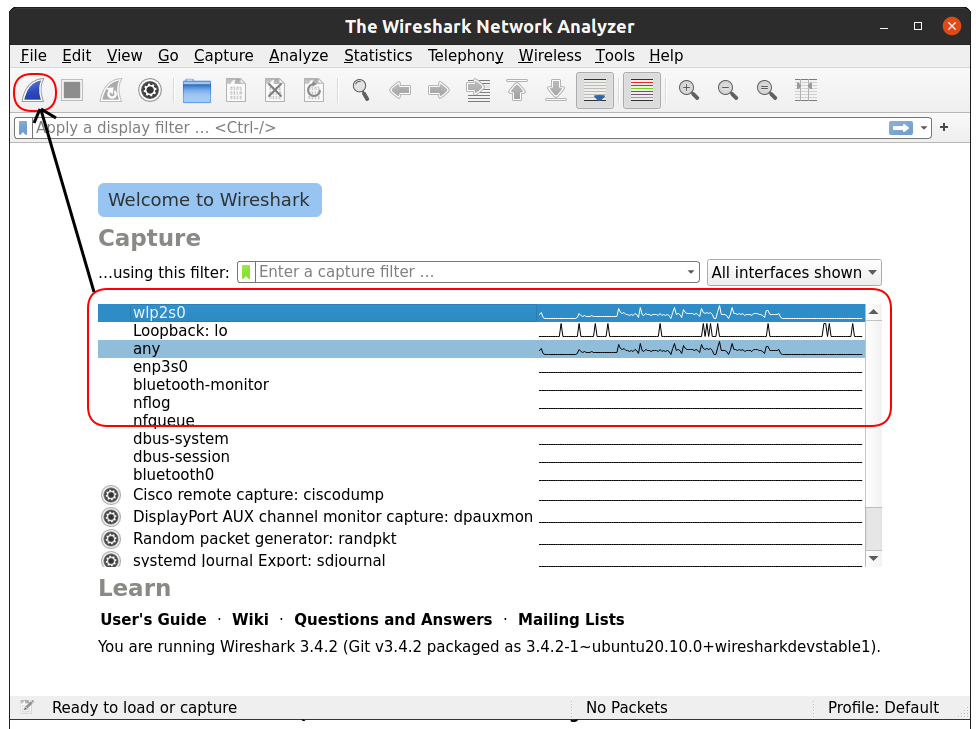
Оберіть “Yes”. Оскільки ви дозволили не-суперкористувачу перехоплювати пакети, то необхідно додати користувача в групу wireshark командою:

$ sudo adduser $USER wireshark

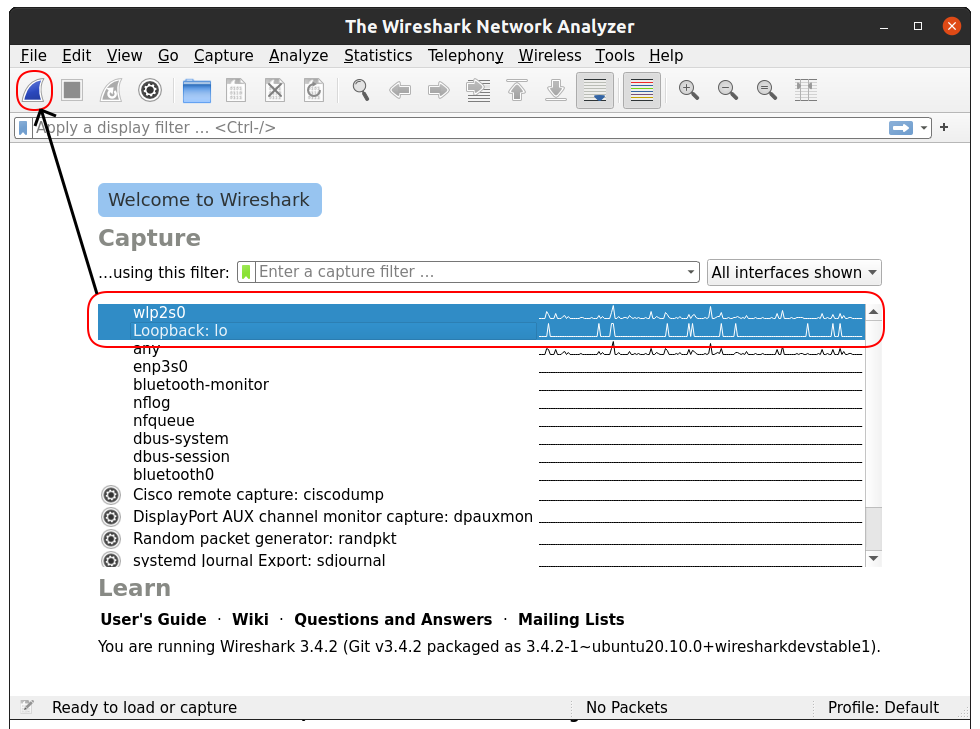
**Захоплення пакетів у Wireshark**

Після запуску wireshark, ви побачите список доступних інтерфейсів, які ви можете використати для захоплення пакетів.

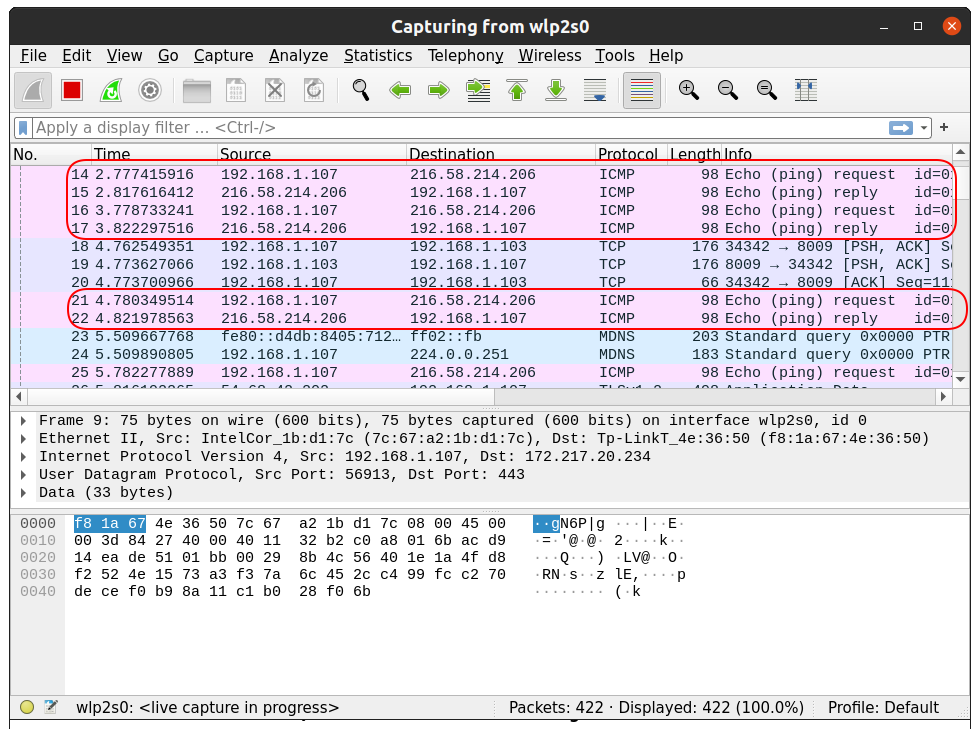
Для захоплення пакетів, оберіть бажаний інтерфейс та натисніть на значок “Почати захоплення пакетів”.



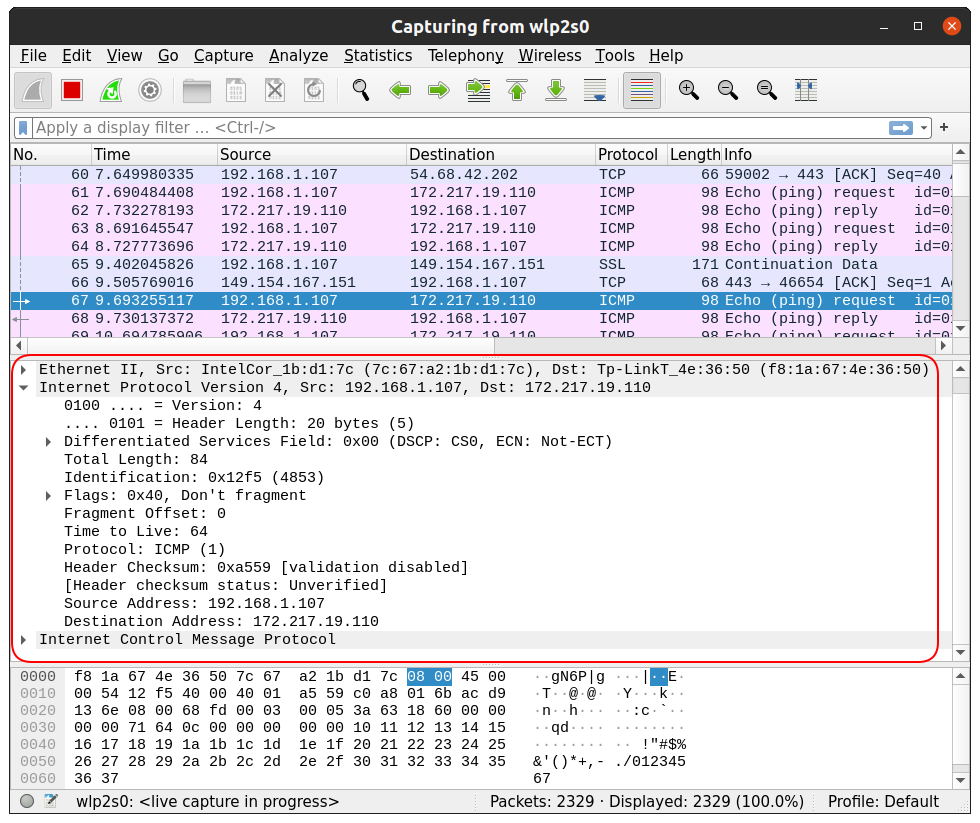
Також можна захоплювати пакети з двох та більше інтерфейсів одночасно. Для цього натисніть та утримуйте кнопку “Ctrl”, натискаючи на бажані інтерфейси, а потім натисніть на значок “Почати захоплення пакетів”.



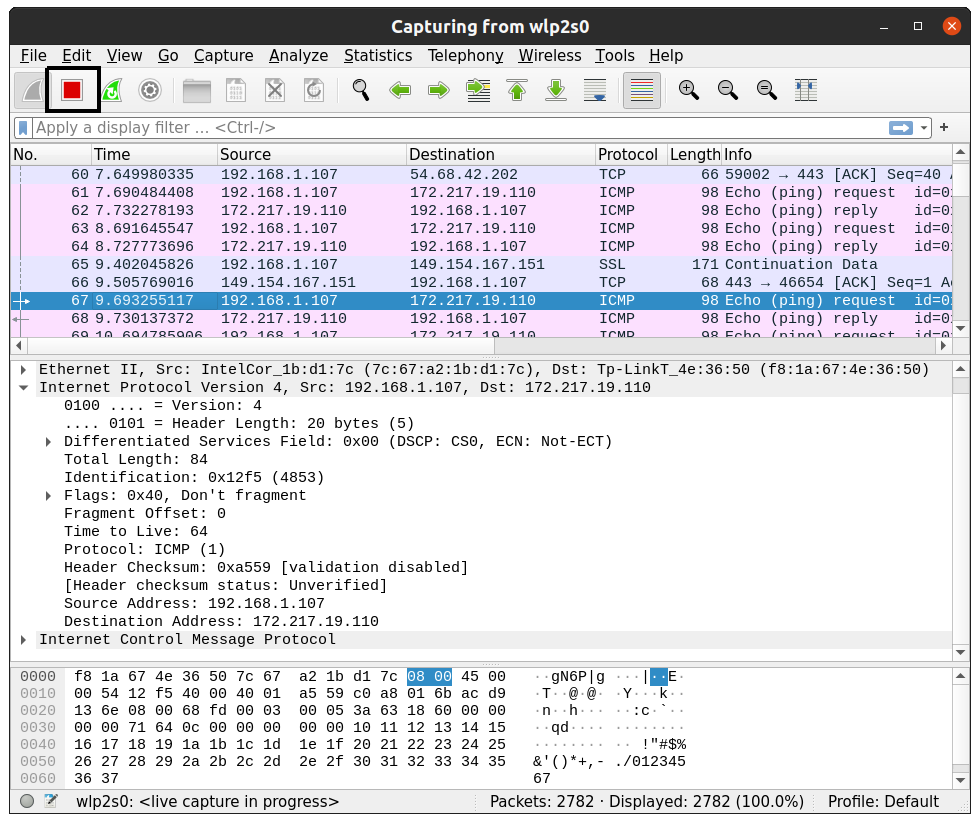
Спробуйте в іншому терміналі ввести $ ping google.com та відстежити захоплення пакетів



Тепер можна натиснути на будь-який пакет та переглянути детальну інформацію.



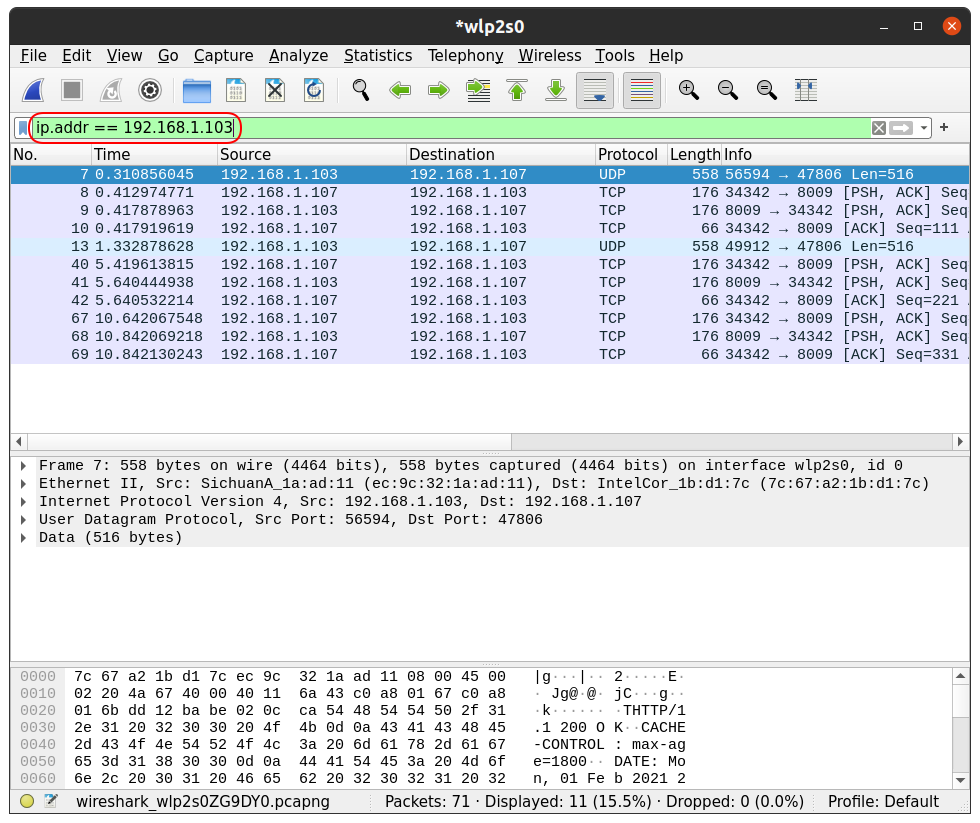
Щоб припинити захоплення пакетів, необхідно натиснути на червоний значок



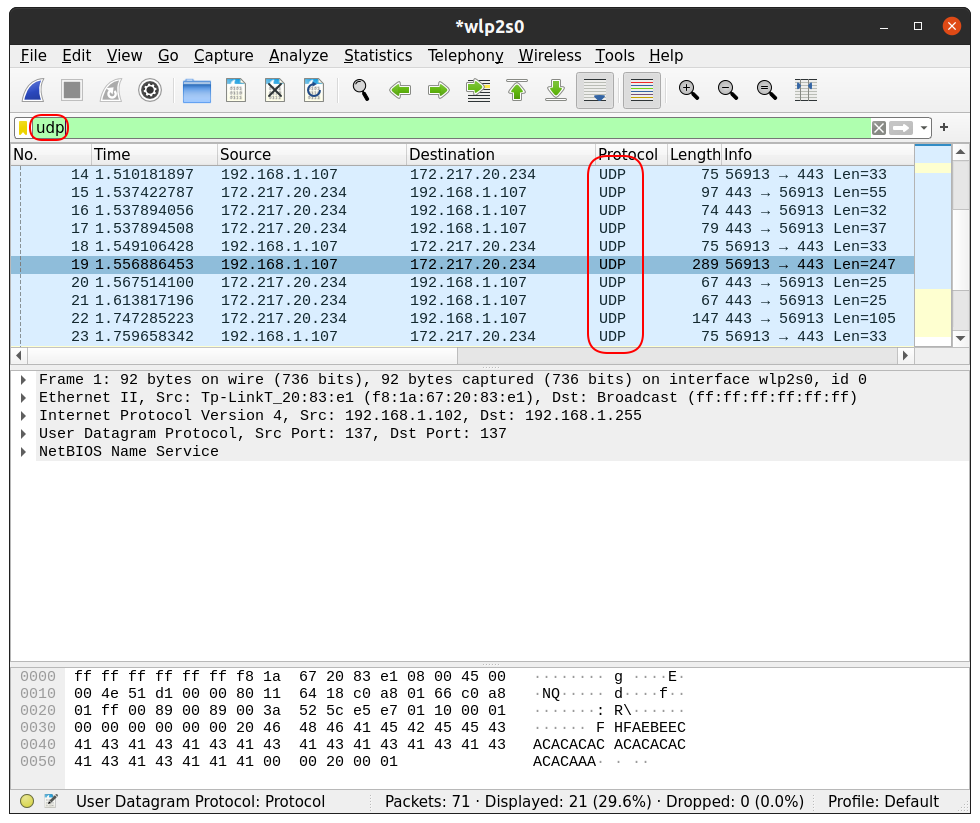
**Використання фільтрів у Wireshark**

Це дуже потужна можливість. За допомогою фільтрів можна прибрати трафік, який нас не цікавить, та залишити тільки потрібний. Трафік можна фільтрувати по МАС-адресі, ІР-адресі, підмережі або протоколу.

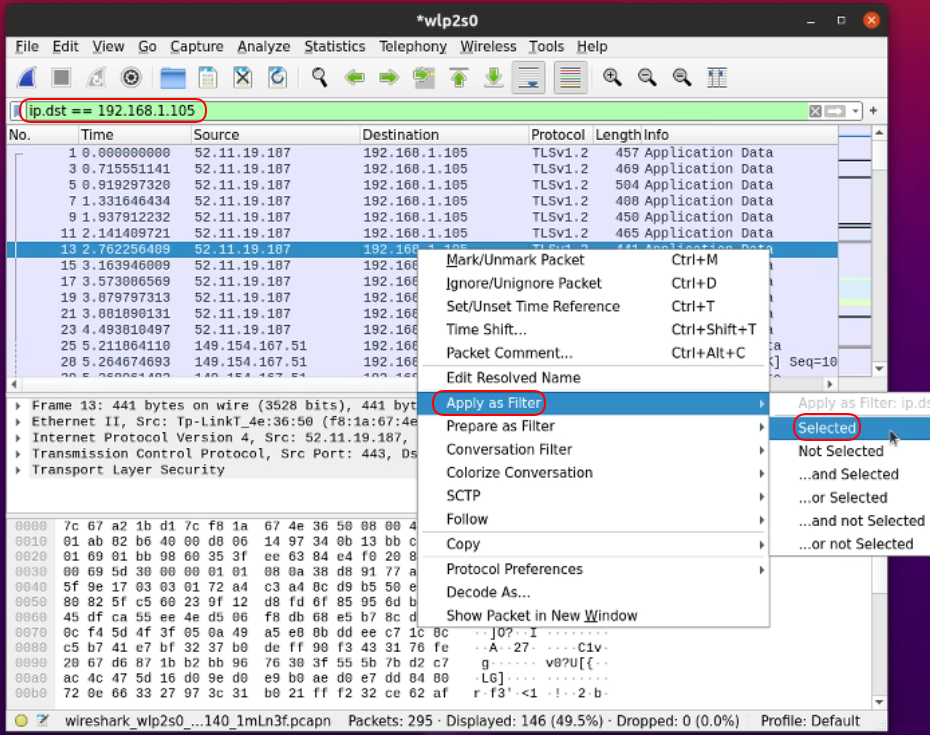
**Приклад фільтрів по ІР-адресі**



**Приклад фільтрів по протоколу**



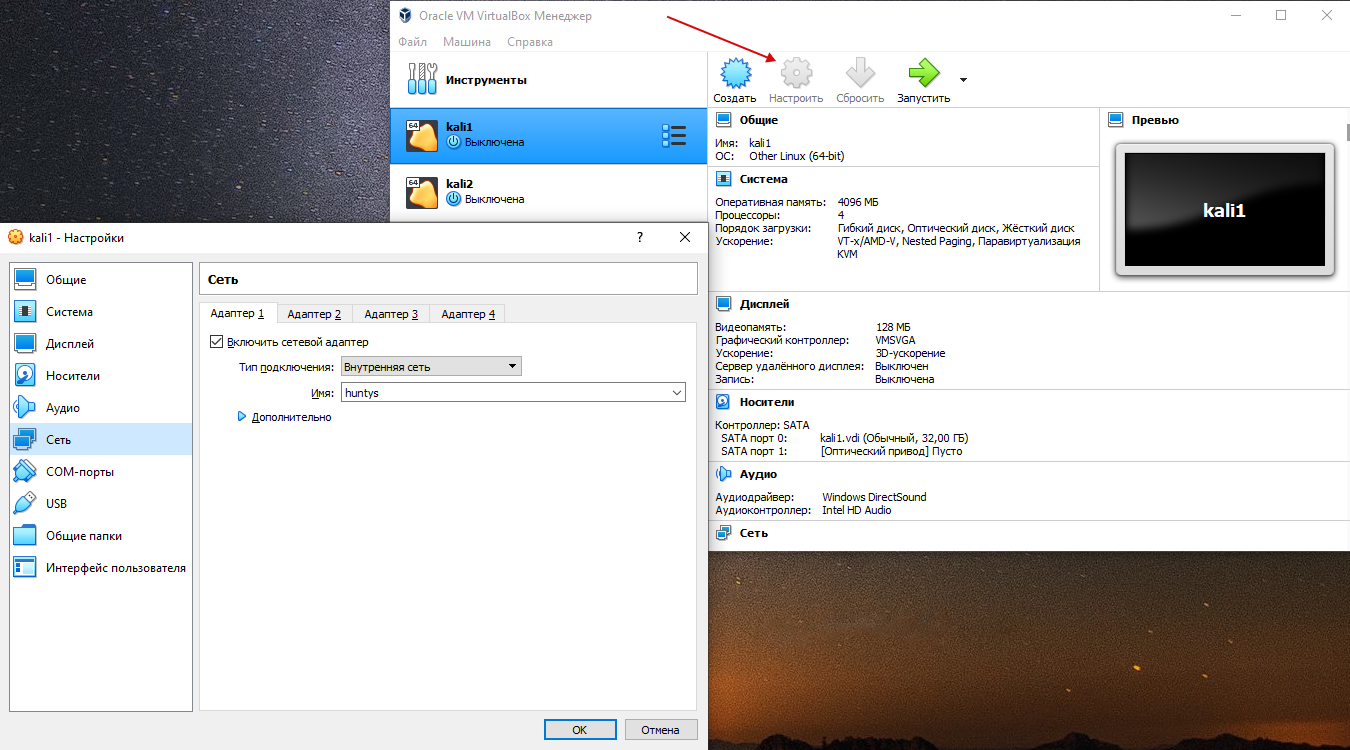
**Примітка**: Також, можна відфільтрувати за допомогою функції “Apply as Filter”. Для цього натисніть, наприклад, на бажану IP-адресу правою кнопкою миші -> Apply as Filter -> Selected. Це допоможе фільтрувати трафік без запам’ятовування усіх фільтрів.



**Виконання лабораторної роботи**

Приклад буде виконаний на двох ноутбуках, під’єднаних через Ethernet. Якщо у вас немає можливості виконати роботу на двох комп’ютерах, то нижче буде наведено приклад для одного комп’ютера. Також, якщо у вас немає Ethernet, то можете виконувати лабораторну роботу через Wi-Fi, проте в такому випадку складно аналізувати трафік через Wireshark, бо буде багато трафіку з браузера та інших програм.

У випадку неможливості всіх вище описаних варіантів, рекомендується використовувати дві віртуальні машини зі встановленим Linux. Якщо для запуску віртуальних машин використовується VirtualBox, на наступному скріншоті показано налаштування мережі.



А саме, для корректного виконання роботи, необхідно на обох машинах вказати налаштувати загальну внутрішню мережу.

Спочатку, очистіть arp таблицю за допомогою команди:

$ sudo arp -d IP-адреса

Переконайтесь, що arp таблиця порожня:

$ arp -a

Введіть в терміналі

$ sudo wireshark

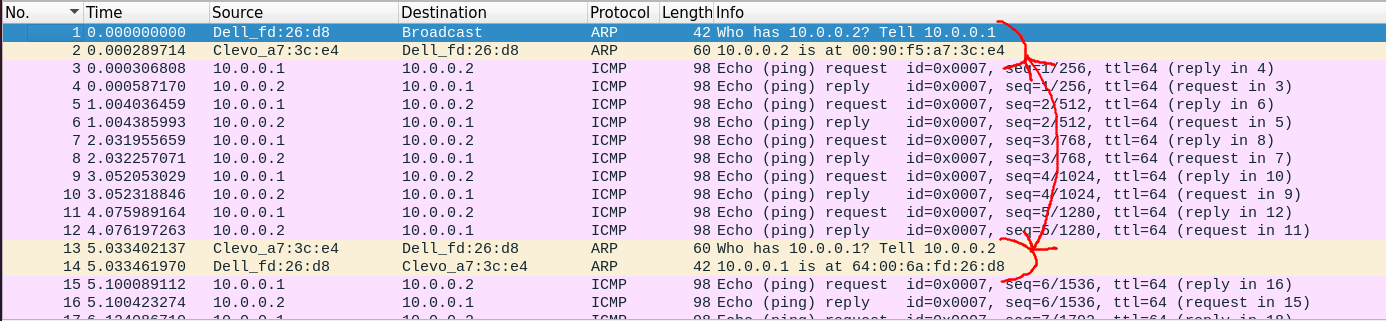
Відкрийте для аналізу трафіку відповідний інтерфейс (у мене це - enp3s0)



Після цього відкрийте другий термінал та пропінгуйте другий пристрій:

$ ping ipPC2

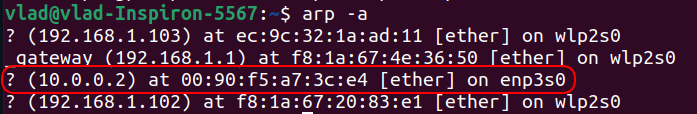
Проаналізуйте отриманий трафік у Wireshark.



У 1 рядку ми бачимо, що 1 комп’ютер надсилає запит, щоб дізнатися МАС-адресу 2 комп’ютера. У 2 рядку 1 комп’ютер отримує відповідь. У 13 та 14 рядку відбувається те саме, але вже 2 комп’ютер дізнається МАС-адресу 1 комп’ютера.

Тепер перевірте arp таблицю командою:

$ arp -a



Як бачимо, з’явився рядок з ІР-адресою та МАС-адресою 2 комп’ютера.

**Варіант для одного комп’ютера**

1) Запустіть Wireshark.

2) Пропінгуйте з комп’ютера свій смартфон через Wi-Fi.

3) У Wireshark приберіть трафік, який нас не цікавить, та виділіть рядки з arp-протоколом, використовуючи фільтри.

**Варіанти на лабораторну роботу**

Згідно за варіантом описати тест-кейс.

Визначення варіанту: Останні дві цифри номеру залікової книжки розділити на 3. Остача від ділення і буде варіантом.

0) Переконатися в отриманні МАС-адреси по IP-адресі

1) Переконатися в тому, що при отриманні arp-reply arp-таблиця оновлюється

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

**Також, можна вигадати свій тест-кейс та описати його.**