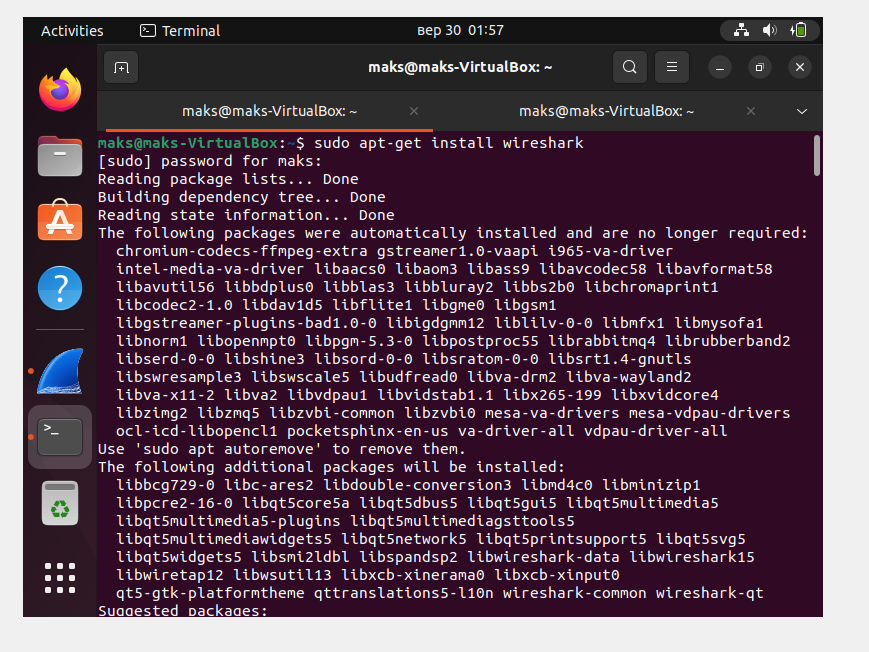
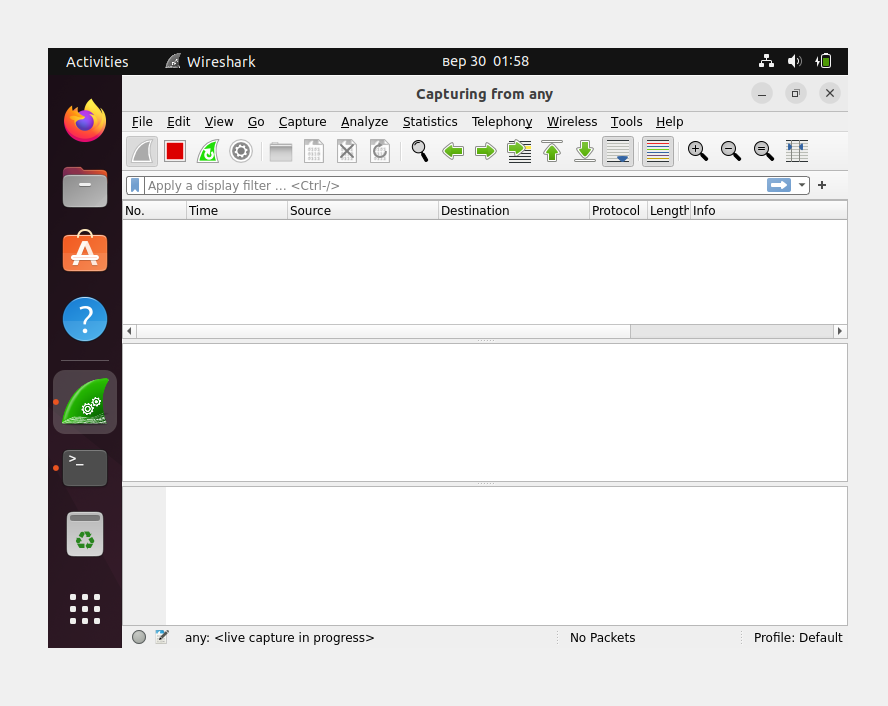
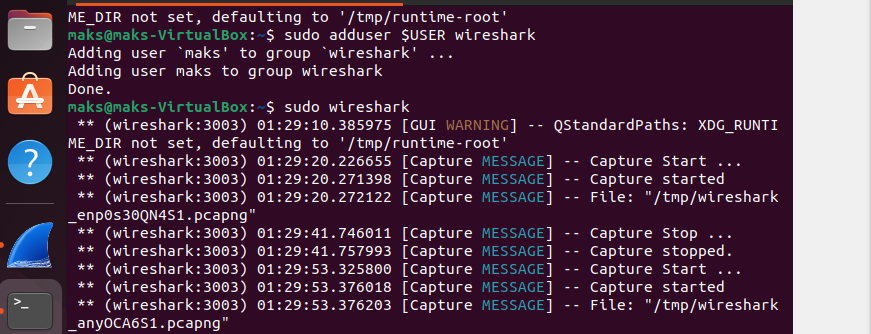
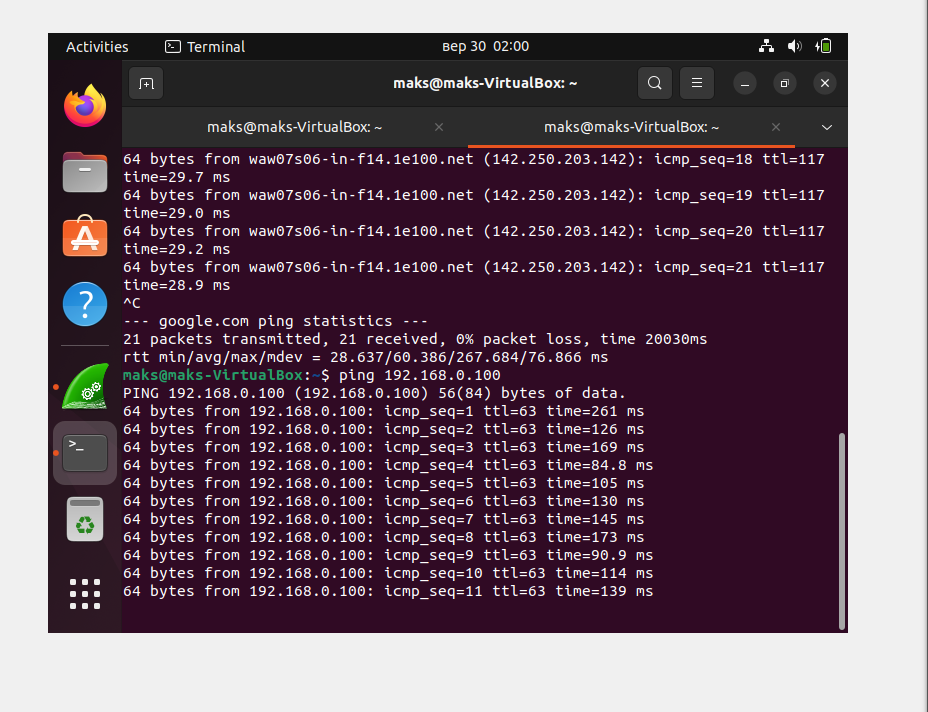
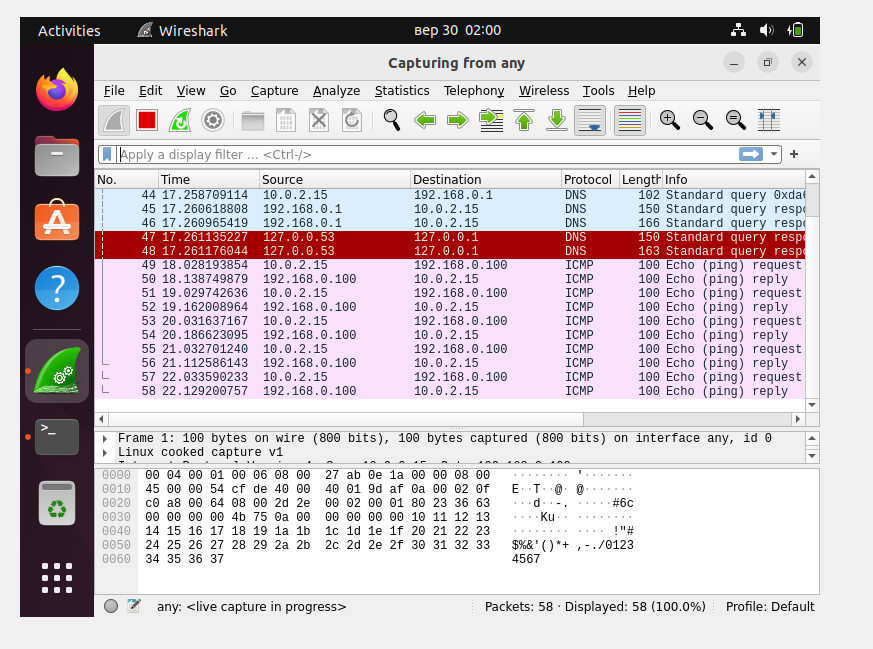
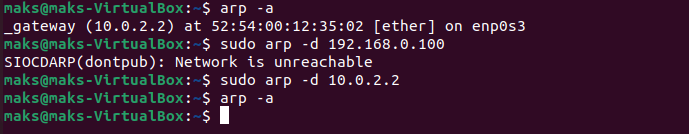
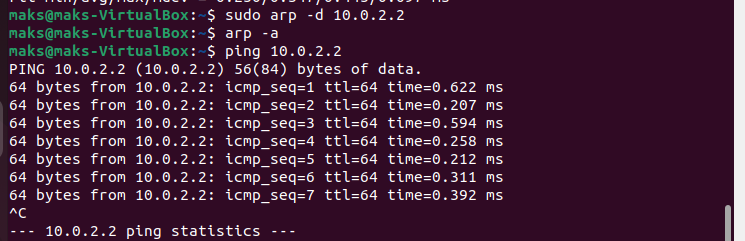
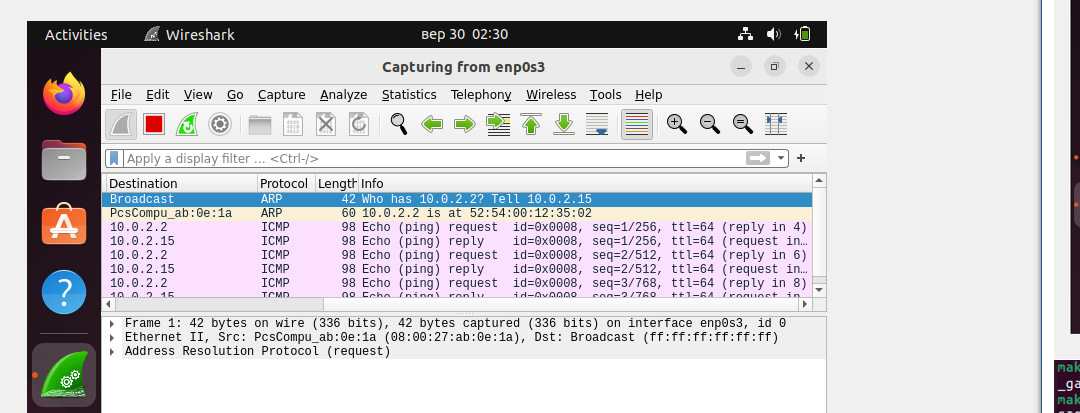
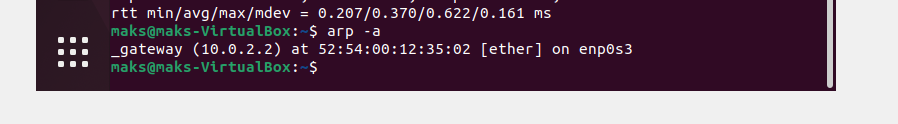
Терехов Максим, ІК-93, ФІОТ  
Лабораторна робота №1  
НАЛАШТУВАННЯ МЕРЕЖНОГО ОТОЧЕННЯ ТА ТЕСТУВАННЯ ПРОТОКОЛУ ARP

Варіант завдання – 0 (Переконатися в отриманні МАС-адреси по відомій IP-адресі.)

Теоретичні відомості:

1. Встановлення утиліти для сніффінгу трафіка Wireshark
2. Запуск утиліти
3. Тестовий пінг
4. Зібранний трафік
5. Перевірка таблиці apr та видалення записів з неї  
   
6. Пінг ip-адреси всередині мережі
7. Зібрані пакети з запитом mac-адреси
8. Відповідний запис в apr-таблиці

TEST-CASE

**Topic** – Wireshark functionality. Virtual machine gateway IP and MAC address resolving

**Description** - Make sure to get a vm machine gateway IP and MAC address

**Attachments** – ARP\_Tests.pcapng

**Version**:

net-tools 2.10-alpha

wireshark 3.6.2

**Setup**:

1. Virtual machine with Ubuntu OS
2. PC1-adapter-gateway-internet

PC1 IP – 192.168.0.1

**Preparation:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Description** | **Action** | **ER** |
| **1** | Check net-tools and wireshark installed | *dpkg -s wireshark*  *dpkg -s net-tools* | installed - ok |
| **2** | Clean arp table | *sudo arp -d* | *arp – a* doesn’t print anything |
| **3** | Launch wireshark | Sudowireshark | Wireshark window is opened |

Steps:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Description** | **Action** | **ER** |
| 1 | Pick Wireshark interface (any or enp0s3) |  | Capture menu is opened |
| 2 | Open additional terminal |  |  |
| 3 | Ping some external addresses from new terminal | *ping google.com* | 64 bytes from <host> (<ip-adress>): icmp\_seq=2 ttl=118 time=16.6 ms  Will be printed repetatly |
| 4 | Check new packets captured | *Open wireshark window* | New rows will appear in capturing table |
| 4 | Stop packets capturing | *Click “Stop packets capturing” button* | New rows will stop appearing |
| 5 | Filter ARP protocol | *Write arp in filter input field* | There have to be 2 packets with ARP protocol |
| 6 | Check packets info | *Search “info” column* | First packet info has been “Who has <IP>” and second info is “<IP> is at <MAC>” |
| 7 | Close or minimize the wireshark window | *You can save capturing file if you want to work with it lately* |  |
| 8 | Check arp table | *arp -a in terminal* | \_gateway <IP> at <MAC>[ether] on enp0s3 |
| 9 | Compare results |  | IP and MAC from Wireshark and ARP must be identical |

Висновки:

В ході лабораторної роботи ми написали тест-кейс для тестування роботи ARP протоколу та вивчили основні принципи його роботи, та принцип сніффінгу трафіку за допомогою утиліти Wireshark