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 якості QA вбудованих систем

«Налаштування мережного оточення та

Тестування протоколу arp»

Варіант 24

Виконала
студентка групи ІА–13:
Сидорук Ольга Костянтинівна

Перевірив:
Куменко Ирина

Київ 2024

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 OSI, зокрема форматів фреймів Ethernet, формату MAC адрес, протоколу ARP;

▪ експериментально ознайомитися з протоколом передавання службових повідомлень ICMP;

▪ навчитися користуватися мережною утілітою ping;

▪ з використанням програми wireshark дослідити основні етапи отримання MAC адрес протоколом ARP на канальному рівні моделі OSI.

QA завдання: QA Embedded Testing на прикладі протоколу ARP

Теорітичні віомості:

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.

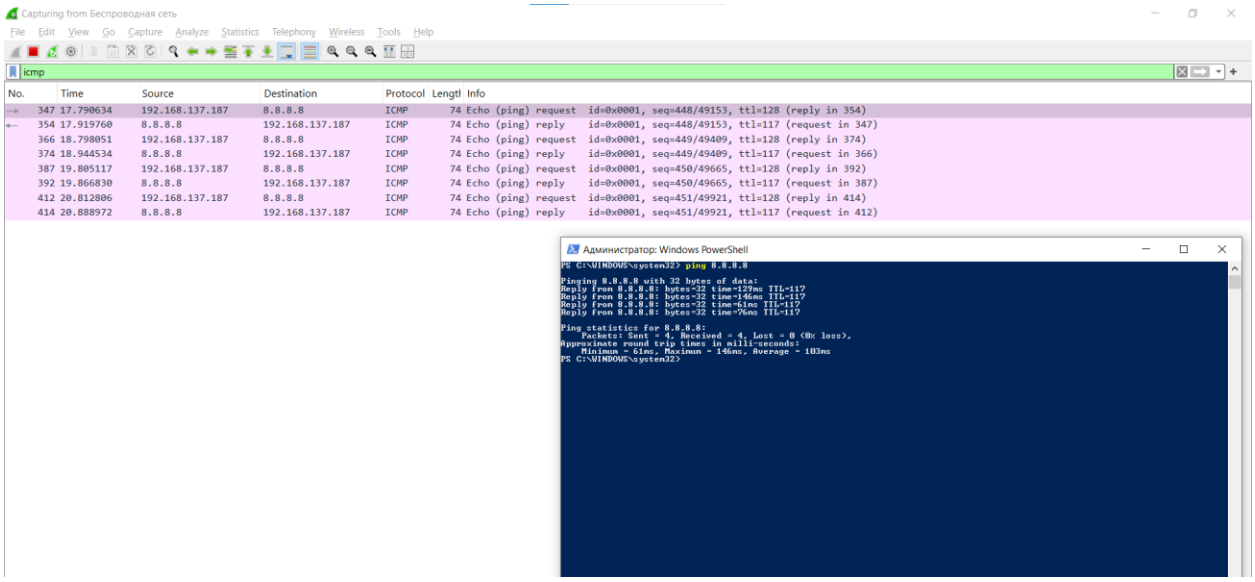
Протокол ARP (Address Resolution Protocol) – дозволяє дізнатися MAC-адресу по IP-адресі.

Wireshark – це передовий та широко використовуваний аналізатор мережевих протоколів. Він дозволяє бачити, що відбувається у мережі, на мікроскопічному рівні.

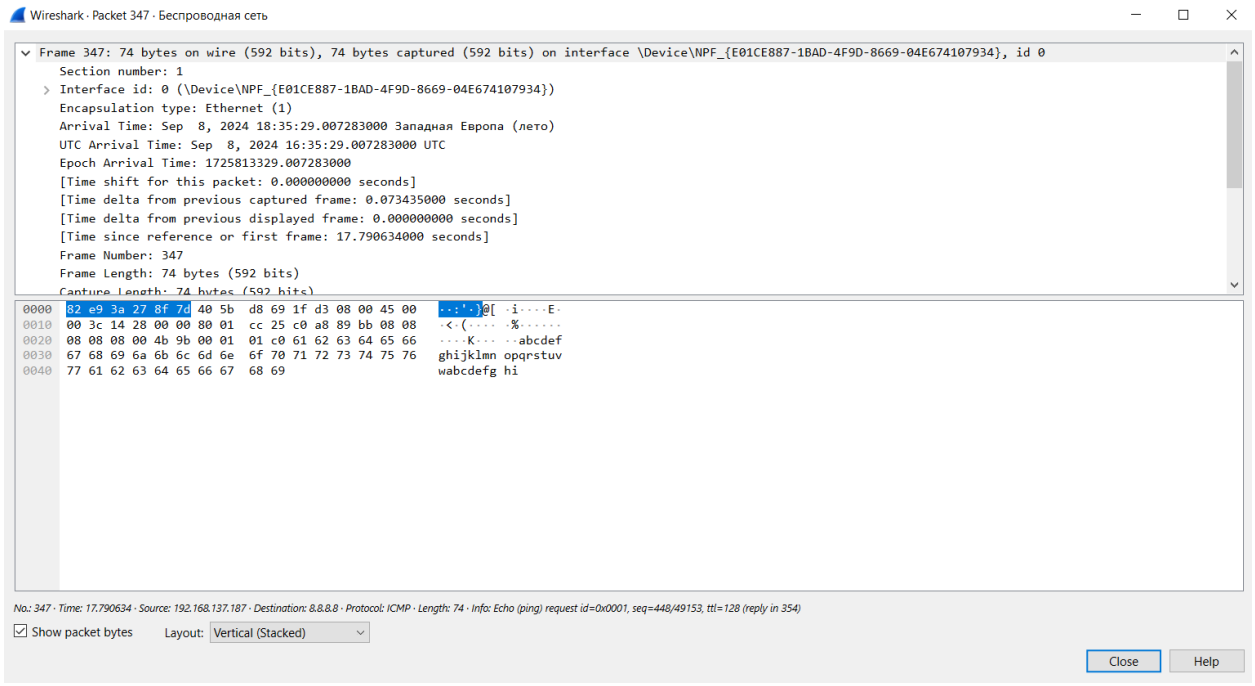
Частина 1

Хід роботи

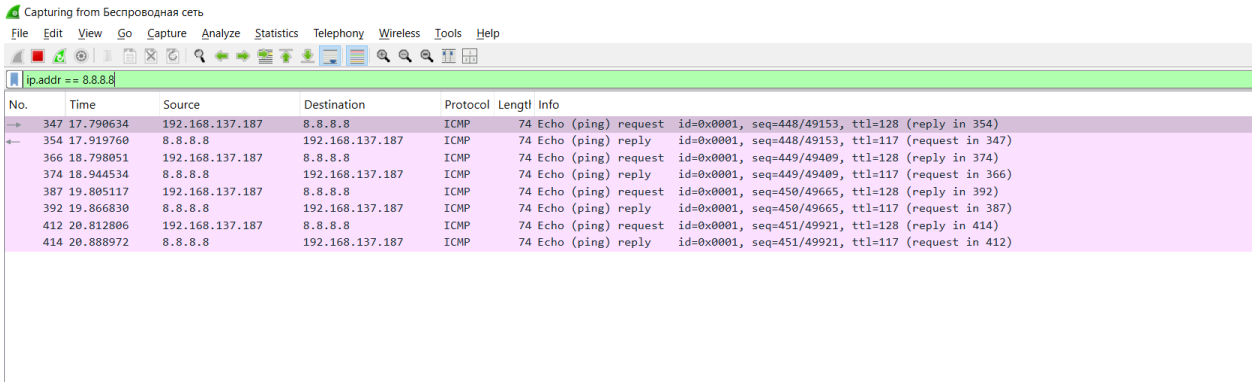
Перевіряємо роботу wireshark, пропінгуємо google



Тепер можна виділити будь-який пакет та переглянути детальну інформацію

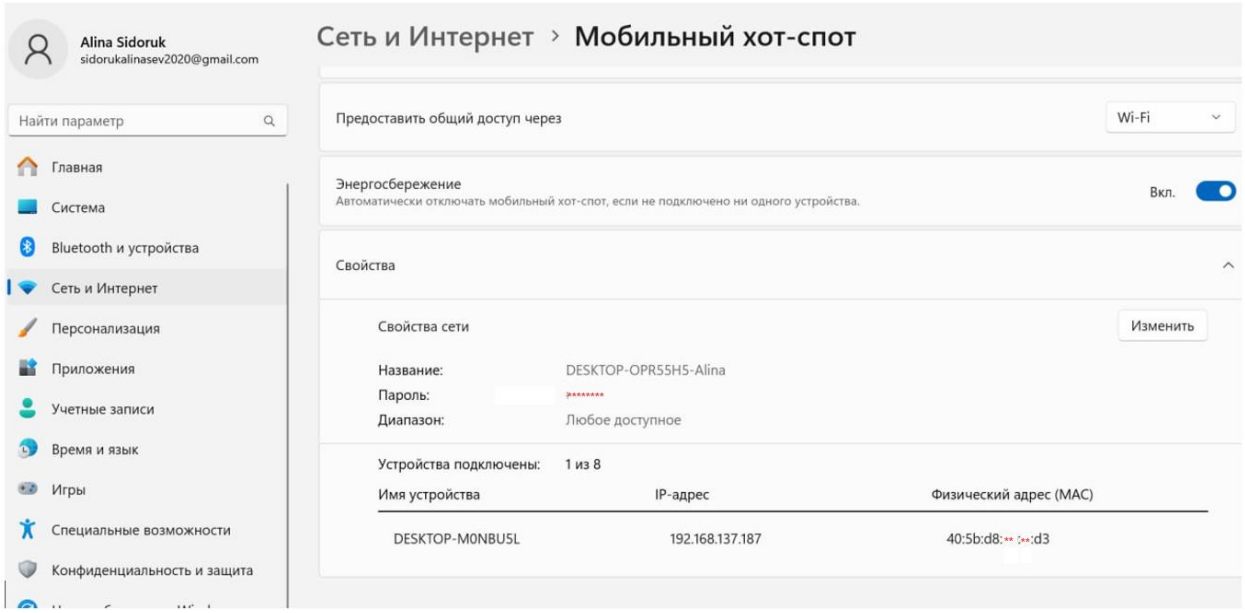


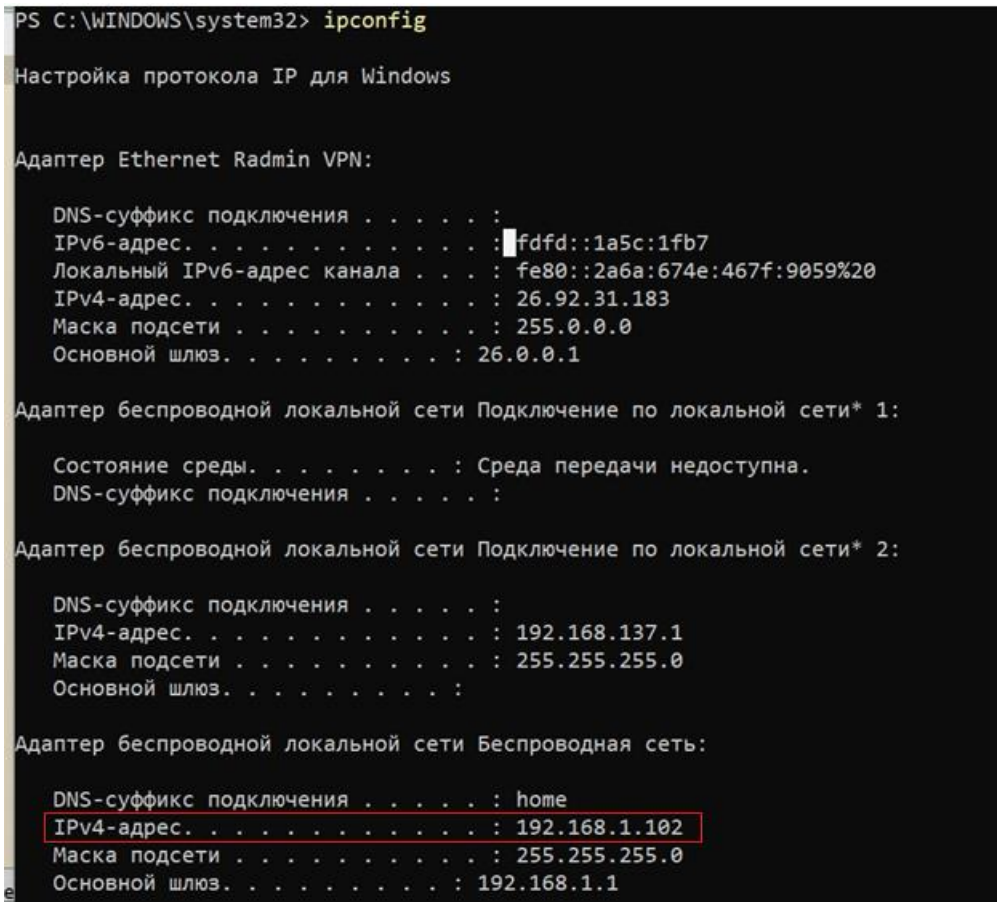
пофільтруємо по IP-адресі google:



Включаємо на Alina`s PC Мобільний хот-спот

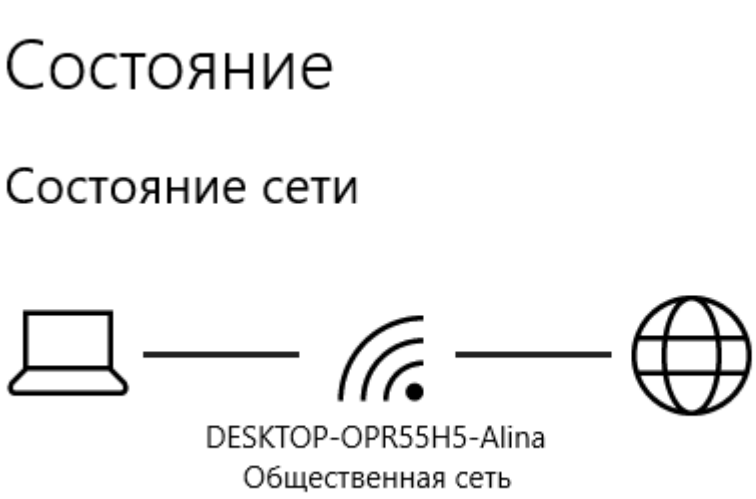
PC: Alina





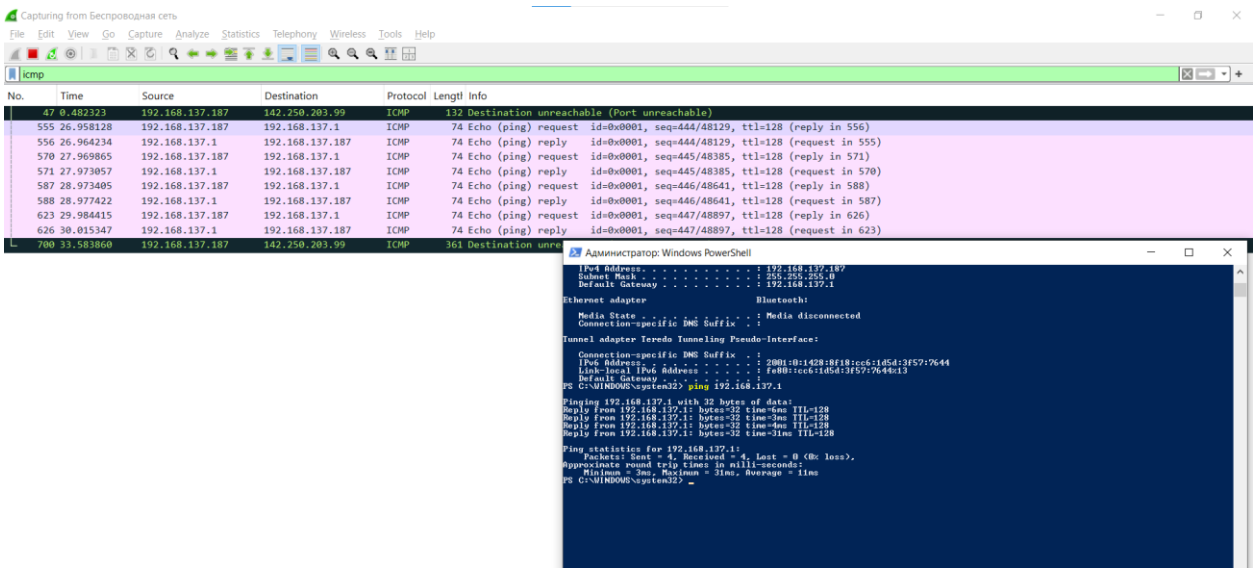
Підключаємось з Olha`s PC до Alina`s PC

PC:Olha




```
PS C:\WINDOWS\system32> ipconfig

Windows IP Configuration


Ethernet adapter Radmin VPN:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fdfd::1a91:af23
   Link-local IPv6 Address . . . . . : fe80::b5de:fc1a:a7ca:31f9%12
   IPv4 Address. . . . . . . . . . . : 26.145.175.35
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 26.0.0.1

Unknown adapter                               :

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter OpenVPN Connect DCO Adapter:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter                                * 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter                                * 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter                    :

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::d700:921c:cf2e:191e%20
   IPv4 Address. . . . . . . . . . . : 192.168.137.187
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.137.1

Ethernet adapter                        Bluetooth:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:
```

Протестуємо з’єднання, пропінгував з Olha`s PC до Alina`s PC:



Супер, все працює і ми можемо бачити результат у wireshark

Частина 2

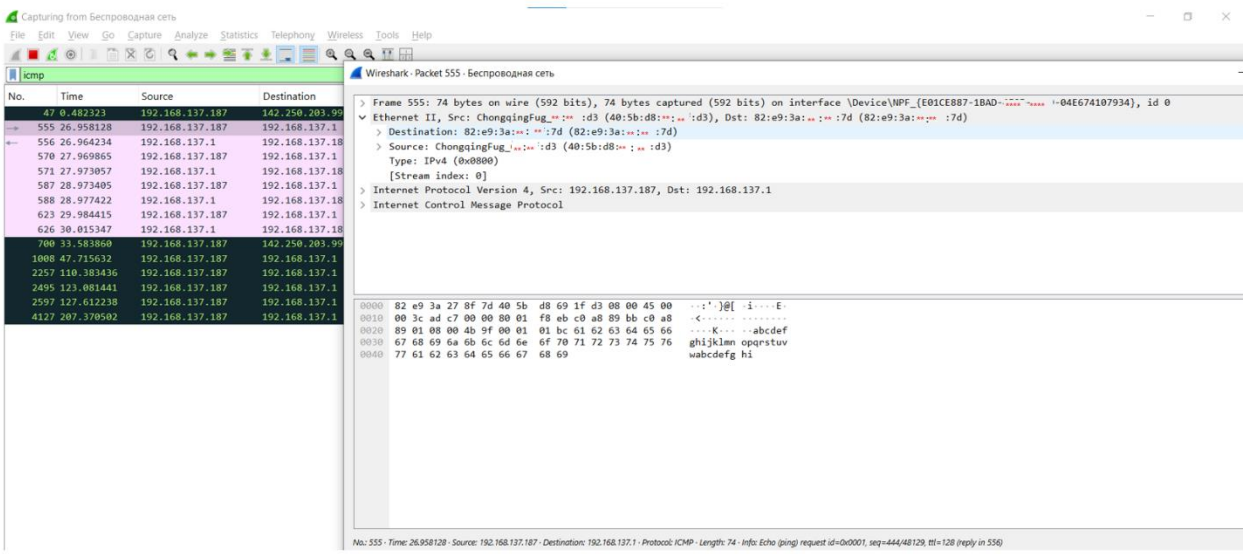
QA завдання:

Згідно з визначеними варіантами описати Test-case.

0) Переконатися в отриманні MAC-адреси по відомій IP-адресі.

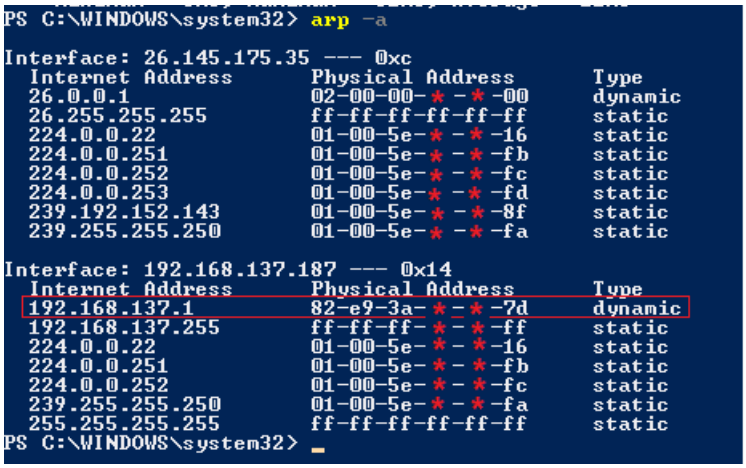
Хід роботи

В пакеті ICMP можемо відкрити розділEthernet 2 і подивитися Destination MAC address:



Destination MAC address 82:e9:3a:**:**:7d

Або вводимо MAC таблицю в терміналі за допомогою команди arp -a



Бачимо такий самий MAC адрес: 82:e9:3a:**:**:7d

Посилання на репозиторій: ***https://github.com/OlhaSydoruk/QA_KPI***

Висновок*:* В ході лабораторної роботи, я навчилась налаштовувати мережне оточення для тестування вбудованих систем та пристроїв IoT. Навчилась використовувати утиліту wireshark для аналізу трафіка в комп'ютерній мережі. Протестувала мережне оточення наканальному рівні моделі OSI. Поєднала два ноутбука за допомогою Wifi hot-spot