



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 agr»

Варіант 24

Виконала
студентка групи ІА–13:
Сидорук Ольга Костянтинівна

Перевірив:
Куменко Ирина

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 утилітою 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

Теоретичні 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.

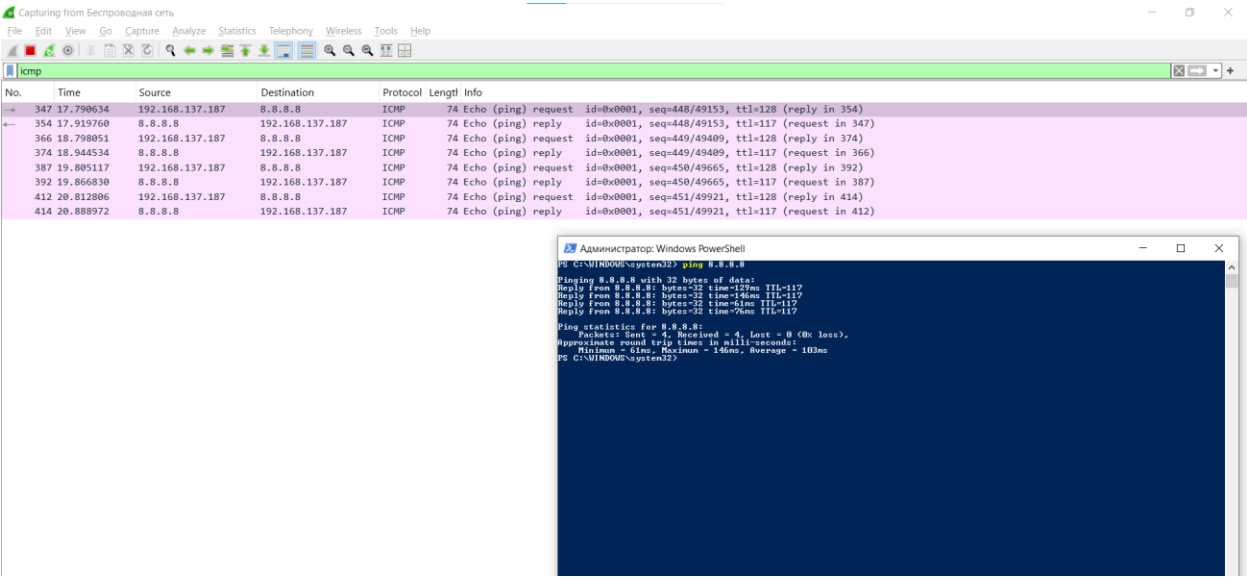
Протокол ARP (Address Resolution Protocol) – дозволяє дізнатися MAC-адресу по IP-адресі.

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

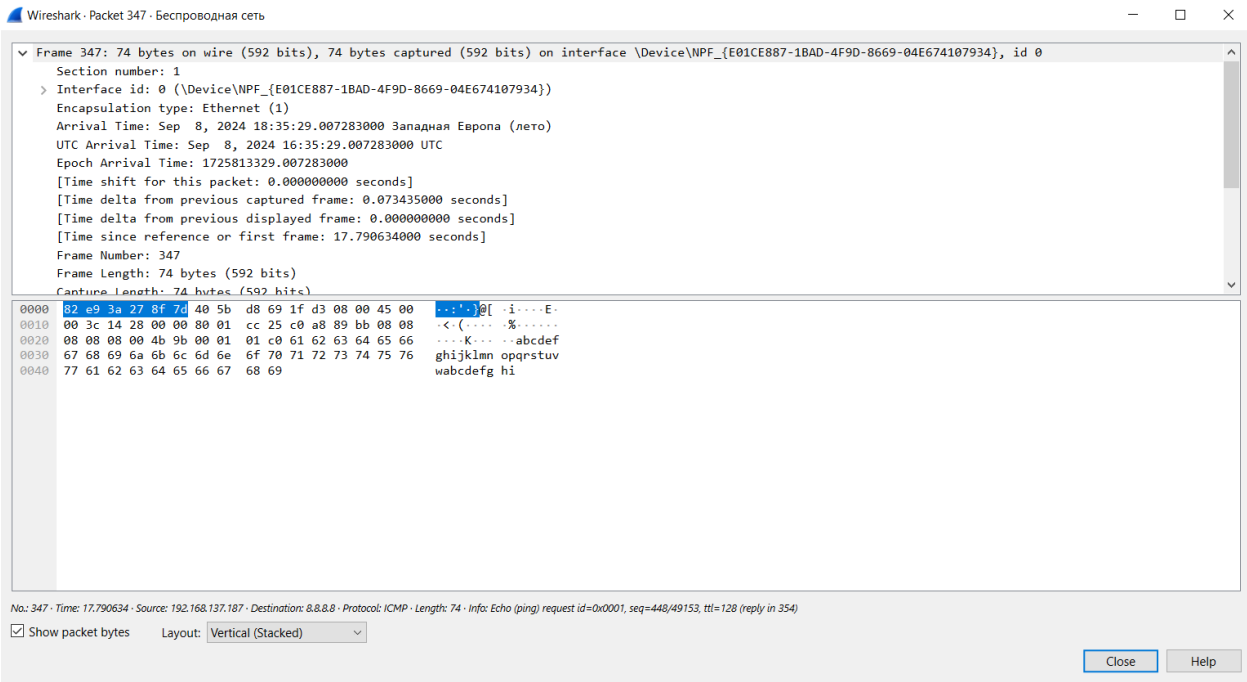
Частина 1

Хід роботи

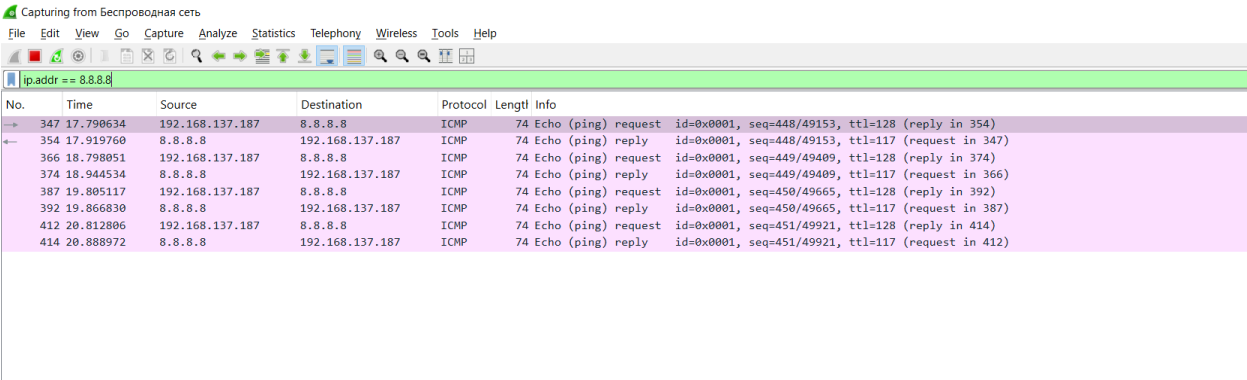
Перевіряємо роботу wireshark, пропінгуємо google



Тепер можна виділити будь-який пакет та переглянути детальну інформацію

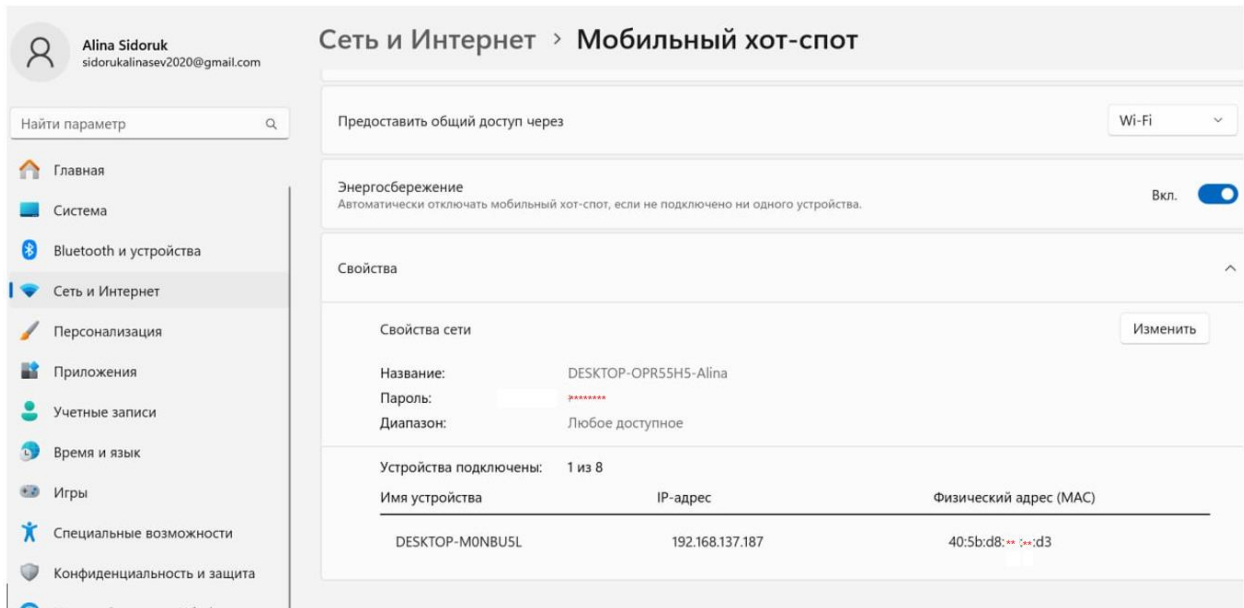


пофільтруємо по IP-адресі google:



Включаємо на Alina`s PC Мобільний хот-спот

PC: Alina



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

Настройка протокола IP для Windows

Адаптер Ethernet Radmin VPN:

    DNS-суффикс подключения . . . . . : 
    IPv6-адрес. . . . . : fdfd::1a5c:1fb7
    Локальный IPv6-адрес канала . . . : fe80::2a6a:674e:467f:9059%20
    IPv4-адрес. . . . . : 26.92.31.183
    Маска подсети . . . . . : 255.0.0.0
    Основной шлюз. . . . . : 26.0.0.1

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : 

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

    DNS-суффикс подключения . . . . . : 
    IPv4-адрес. . . . . : 192.168.137.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : home
    IPv4-адрес. . . . . : 192.168.1.102
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.1.1
```

Підключаємось з Olha`s PC до Alina`s PC

PC:Olha

Состояние

Состояние сети



DESKTOP-OPR55H5-Alina
Общественная сеть

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

Windows IP Configuration

Ethernet adapter Radmin UPN:

    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 OpenUPN 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 :

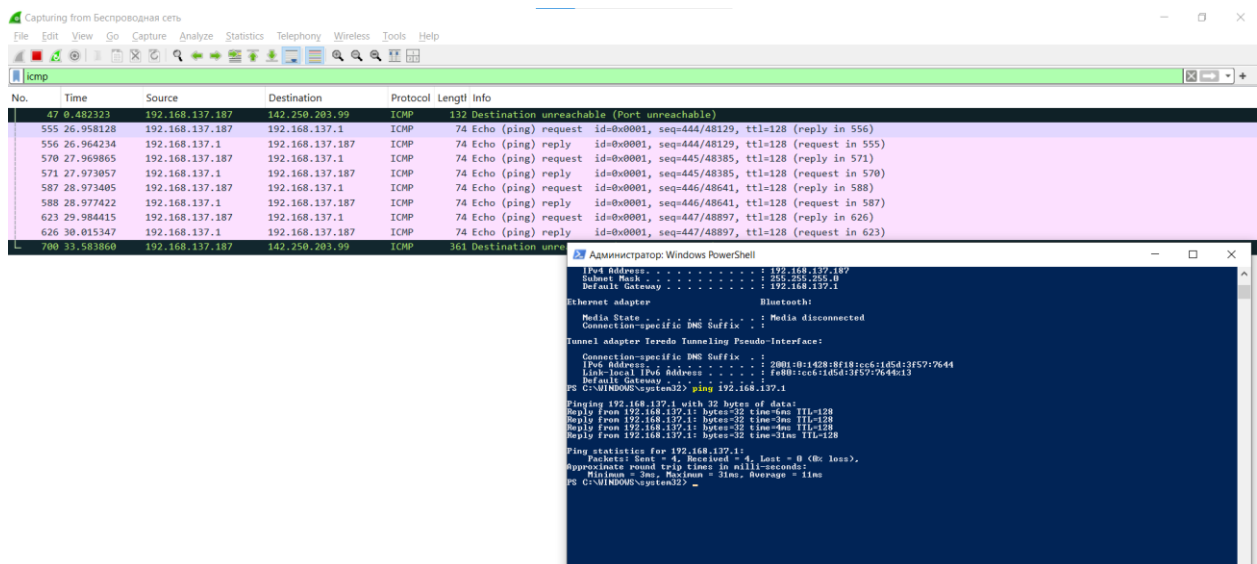
    Connection-specific DNS Suffix  . : mshome.net
    Link-local IPv6 Address . . . . . : fe80::d700:921c:cf2e:191e%20
    IPv4 Address. . . . . : 192.168.137.187
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.137.1

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

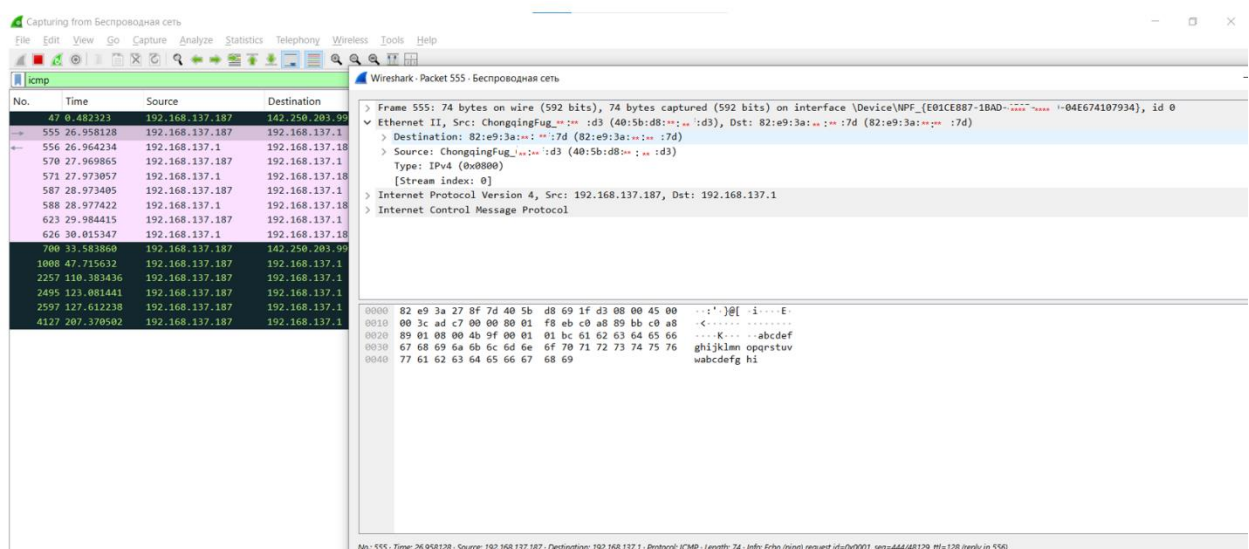
QA завдання:

Згідно з визначеними варіантами описати Test-case.

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

Хід роботи

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



Destination MAC address **82:e9:3a:00:00:01**

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

```
PS C:\WINDOWS\system32> arp -a

Interface: 26.145.175.35 --- 0xc
Internet Address      Physical Address      Type
26.0.0.1              02-00-00-*-*00       dynamic
26.255.255.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-*-*16       static
224.0.0.251           01-00-5e-*-*fb       static
224.0.0.252           01-00-5e-*-*fc       static
224.0.0.253           01-00-5e-*-*fd       static
239.192.152.143       01-00-5e-*-*8f       static
239.255.255.250       01-00-5e-*-*fa       static

Interface: 192.168.137.187 --- 0x14
Internet Address      Physical Address      Type
192.168.137.1         82-e9-3a-*-*7d       dynamic
192.168.137.255       ff-ff-ff-*-*ff       static
224.0.0.22            01-00-5e-*-*16       static
224.0.0.251           01-00-5e-*-*fb       static
224.0.0.252           01-00-5e-*-*fc       static
239.255.255.250       01-00-5e-*-*fa       static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

PS C:\WINDOWS\system32>
```

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 на канальному рівні моделі OSI. Поєднала два ноутбука за допомогою Wifi hot-spot