МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА
Факультет електроніки і комп’ютерних технологій

Звіт

про виконання лабораторної роботи № 4

«Налаштування і основні прийоми роботи з аналізатором мережевих пакетів Wireshark.»

Виконав:
студент групи ФеП-13
Карсанашвілі А.Р.
Викладач:
Продивус А.М.

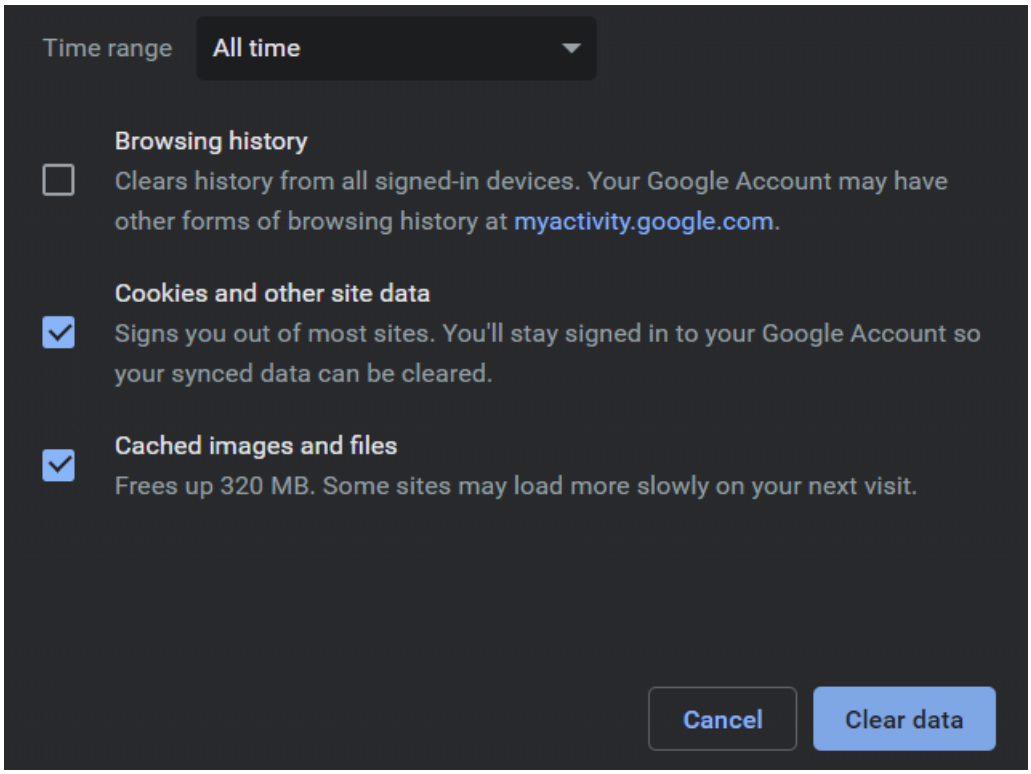
Львів 2020

Мета: дослідити протоколи Ethernet та ARP, використовуючи можливості програми Wireshark.

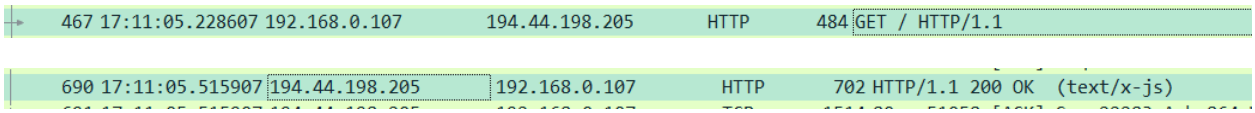
Порядок виконання роботи:

1 Перехоплення і аналіз кадрів Ethernet

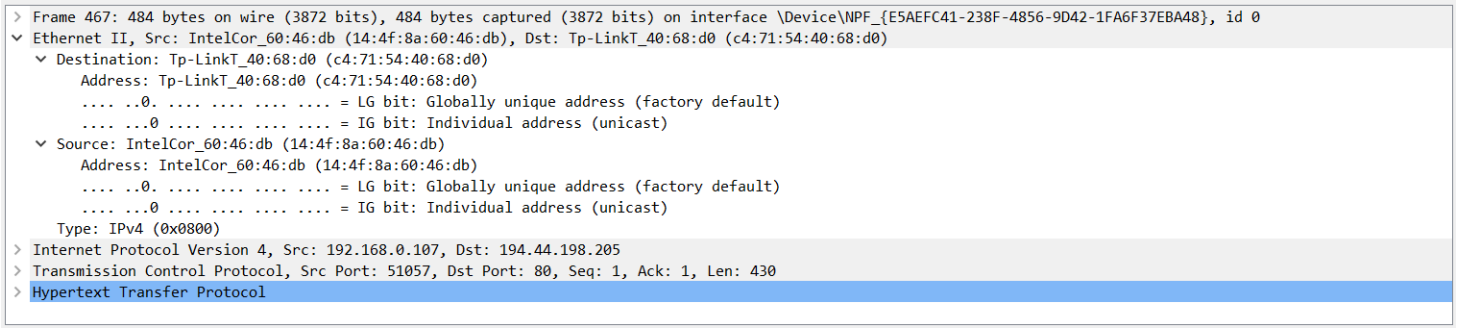
1.1 Очистив кеш браузера



1.2 Запустив Wireshark і почав перехоплючати пакети, після цього перейшов на сайт http://elct.lnu.edu.ua/ і зупинив перехоплення. Знайшов номери пакетів запитів HTTP GET (467) та пакет відповідь від сервера HTTP OK (690).



1.3 Змінюю фільтр перехоплених пакетів так, щоб він показував інформацію лише протоколів нижчих по відношенню до IP рівнів. Вибираю Ethernet кадр, що містить повідомлення HTTP GET. Розкриваю інформацію Ethernet в головному вікні.



1.4 Відповідь на контрольні питання:

1. Якою є 48-бітна MAC-адреса Вашого комп'ютера?

```
Src: IntelCor_60:46:db (14:4f:8a:60:46:db)
```

```
Physical Address. . . . . : 16-4F-8A-60-46-DB
```

2. Якою є 48-бітна MAC-адреса отримувача Ethernet кадру? Чи є ця адреса адресою сервера 10.25.0.1? Якщо ні, то який пристрій має цю Ethernet адресу?

```
Dst: Tp-LinkT_40:68:d0 (c4:71:54:40:68:d0)
```

На цю адресу ми відправили запит, так як она є адресою сервера.

3. Дайте шістнадцяткове представлення двохбайтового поля типу кадру Ethernet.

0x0800

4. Який відступ в кадрі Ethernet має літера "G" в "GET"?

```
0030  01 02 7a 8a 00 00 47 45  54 20 2f 20 48 54 54 50   ··z···GE T / HTTP
```

36.

5. Яке шістнадцяткове значення має поле CRC в цьому кадрі? Що це за поле?

CRC — алгоритм обчислення контрольної суми, призначений для перевірки цілісності даних. Шістнадцяткове представлення – 0x7dfcfa;

6. Якою є адреса відправника кадру? Чи є це адреса вашого комп'ютера або адреса 194.44.198.205.

```
0000  c4 71 54 40 68 d0 14 4f  8a 60 46 db 08 00 45 00   ·qT@h··O ·`F···E·
```

7. Якою є 48-бітна адреса отримувача Ethernet кадру? Чи є це адреса вашого комп’ютера? Якщо ні, то який пристрій має цю Ethernet адресу?

Так, це моя MAC адреса.

8. Дайте шістнадцяткове представлення двохбайтового поля типу кадру Ethernet. Що означає біт(и), які дорівнюють 1?

0x0800

9. Який відступ в кадрі Ethernet має літера“O” в “OK”?

43

2 Спостереження за ARP в дії

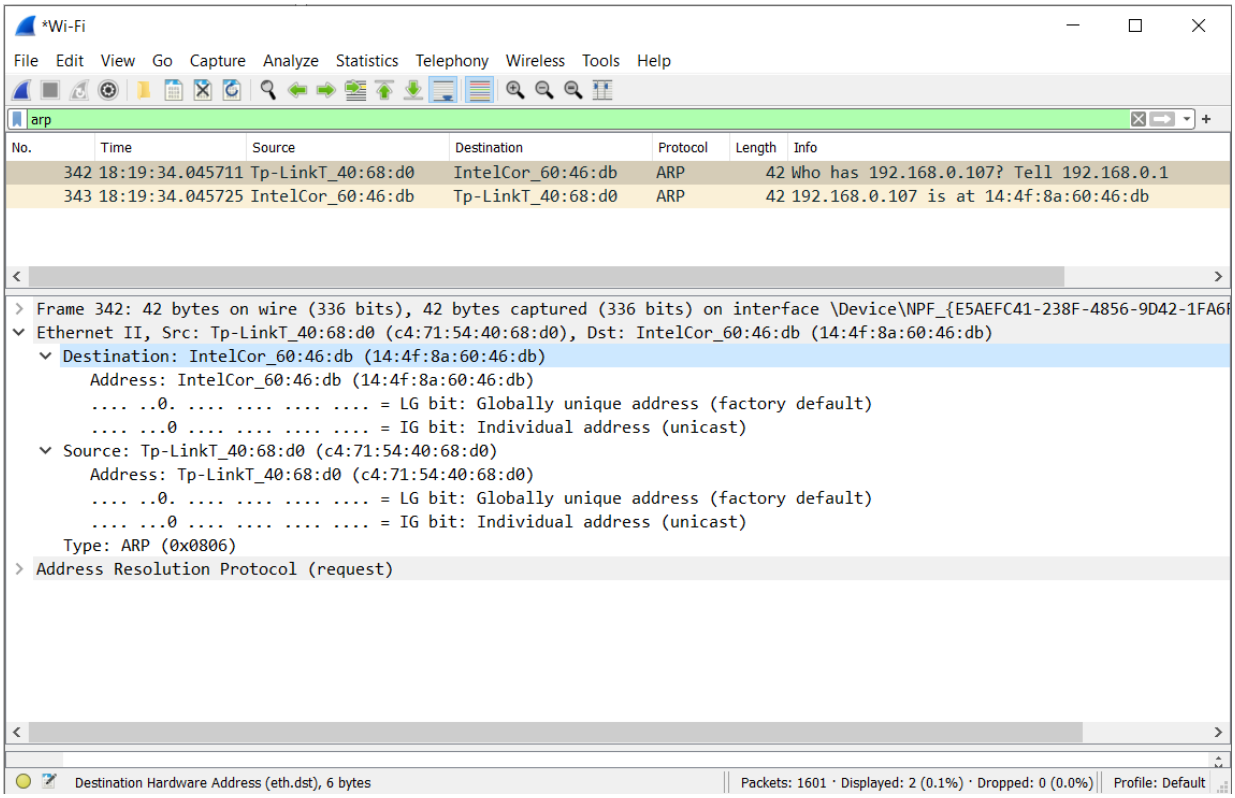
1.1 Виконуємо команду arp -a та переглядаємо вміст arp – кешу комп’ютера.

```
Interface: 192.168.137.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.137.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.107 --- 0x13
  Internet Address      Physical Address      Type
  192.168.0.1           c4-71-54-40-68-d0     dynamic
  192.168.0.100         00-0c-e7-8e-d7-96     dynamic
  192.168.0.101         48-6d-bb-50-da-23     dynamic
  192.168.0.102         64-b0-a6-ef-89-4d     dynamic
  192.168.0.103         c6-eb-ea-b5-ef-0a     dynamic
  192.168.0.104         c0-11-73-83-9e-c1     dynamic
  192.168.0.109         3e-a4-ea-de-1a-10     dynamic
  192.168.0.112         1c-b7-2c-b0-c1-57     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Значення перших двох стовбців — це відповідності ip-адрес їх фізичним адресам. Стовпець Тип визначає чи це динамічна адреса, чи статична.

2.2 Очищаємо arp – кеш а також кеш браузера. Після чого запускаємо сніфер Wireshark та переходимо по адресі https://translate.google.com.ua/.



2.3 Відповідь на контрольні питання:

11. Які шістнадцяткові значення мають адреса відправника і адреса одержувача в кадрах Ethernet, що містить повідомлення ARP?

14:4f:8a:60:46:db – адреса відправника

(c4:71:54:40:68:d0) – адреса отримувача

12. Дайте шістнадцяткове представлення поля типу кадру Ethernet. Що значать біти, значення яких дорівнюють 1?

Type: ARP (0x0806)

13. Чи містить ARP повідомлення IP адресу відправника?

Так

14. Знайдіть повідомлення ARP, що було надіслано у відповідь на запит ARP.

343 18:19:34.045725 IntelCor_60:46:db Tp-LinkT_40:68:d0 ARP 42 192.168.0.107 is at 14:4f:8a:60:46:db

Висновок: під час виконання даної лабораторної роботи я досліджував Ethernet та ARP протоколи. Також, використовуючи пакетний сніфер Wireshark, я проаналізував кадри типу ARP та Ethernet, знайшов необхідні дані та інформацію та дав відповідь на контрольні запитання.