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.

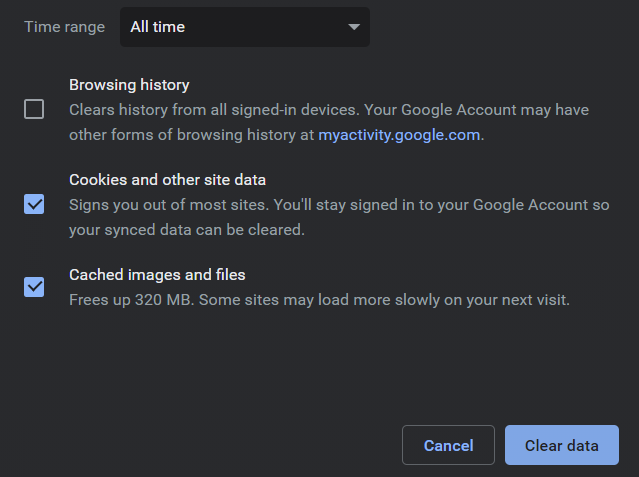
**Львів 2020**

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

**Порядок виконання роботи:**

*1 Перехоплення і аналіз кадрів Ethernet*

1.1 Очистив кеш браузера

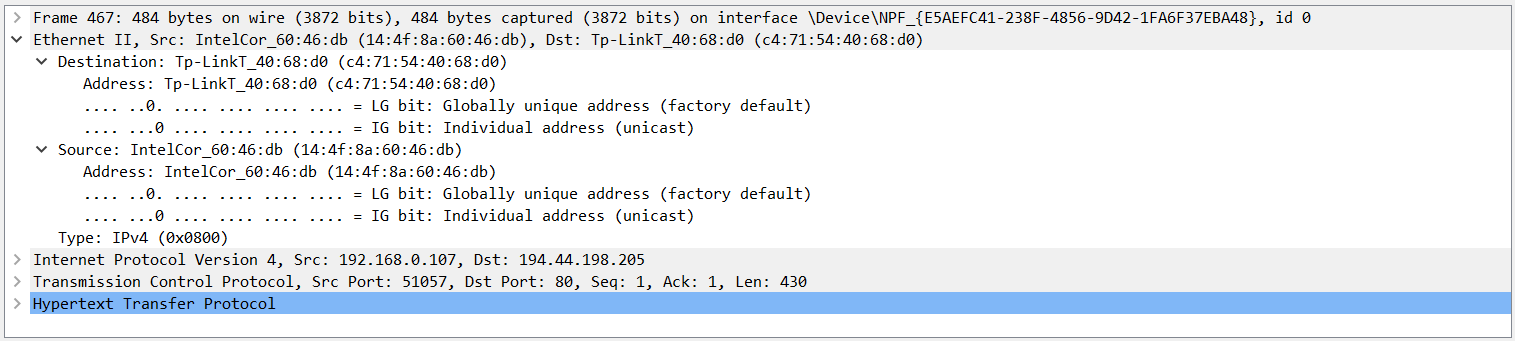


1.2 Запустив Wireshark і почав перехоплючати пакети, після цього перейшов на сайт <http://elct.lnu.edu.ua/> і зупинив перехоплення. Знайшов номери пакетів запитів HTTP GET (467) та пакет відповідь від сервера HTTP OK (690).





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 МАС-адреса Вашого комп’ютера?





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



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

3. Дайте шістнадцяткове представлення двохбайтового поля типу кадру Ethernet.

0x00000800

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

 55.

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

CRC — алгоритм обчислення контрольної суми, призначений для перевірки цілісності даних.

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



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?

MAC адреса роутера.

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

0x00000800

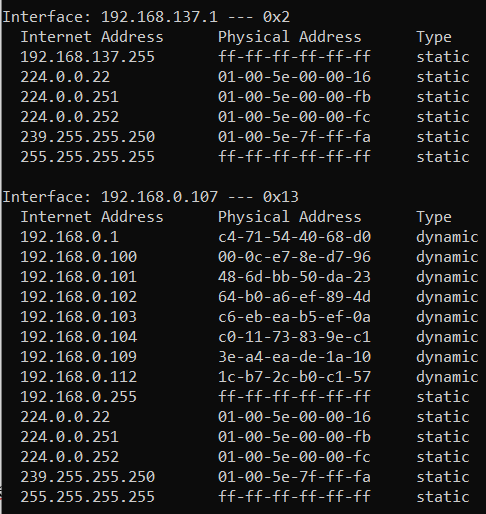
Біт що дорівнює 1 є частиною певної інформації що сам по собі не несе нічого. Його значення можна інтерпритувати як True

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

68

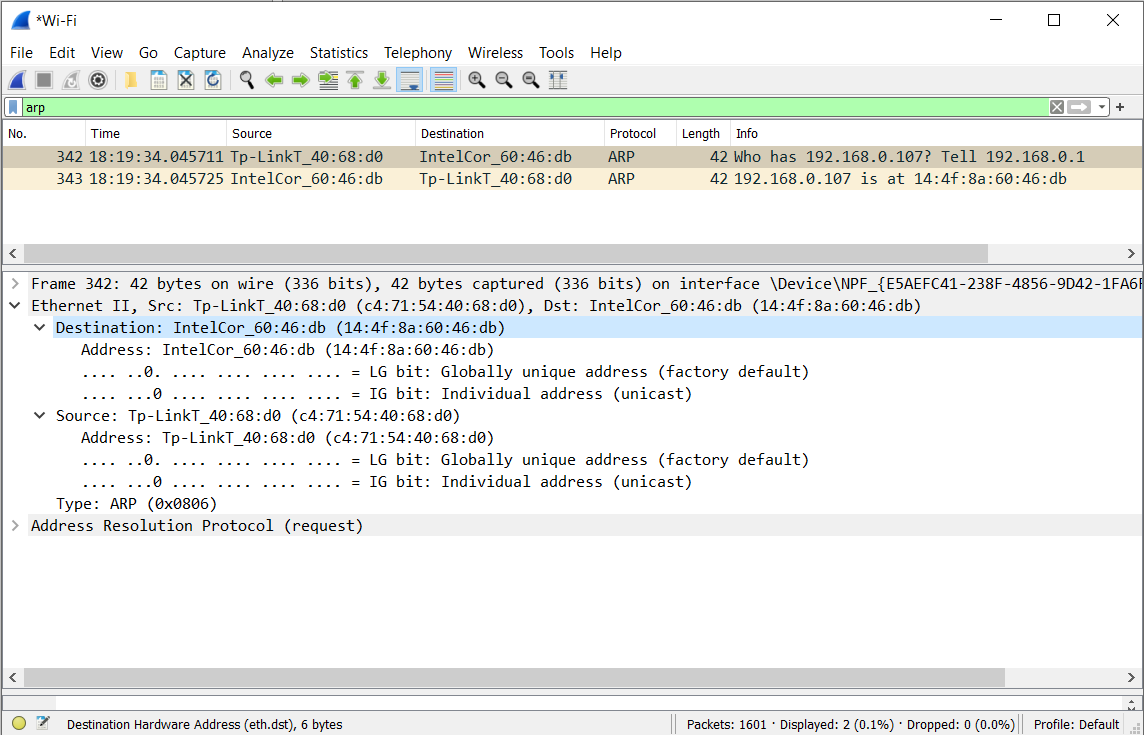
*2 Спостереження за ARP в дії*

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



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?

 – адреса відправника

– адреса отримувача

Вони мають інформацію про формат кадрів Ethernet

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.

**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.