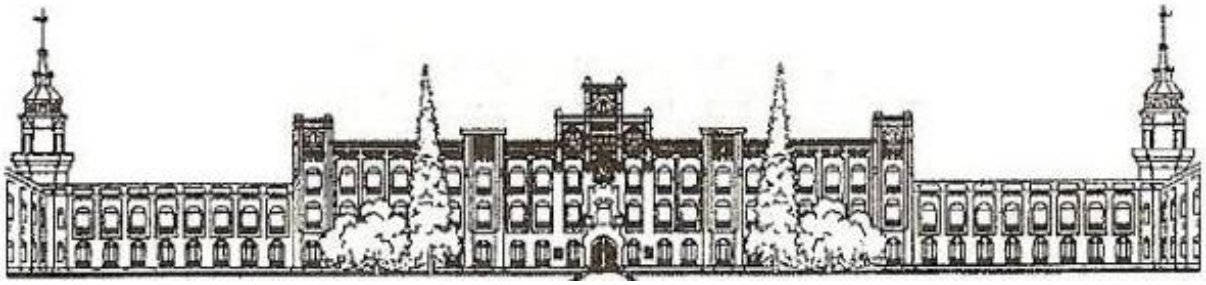


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 1 з дисципліни «Комп'ютерні мережі»

Виконала:

Студентка III курсу

Групи КА-74

Клименко І. О.

Перевірив: Кухарєв С. О.

Київ 2020

Тема: Основи захоплення та аналізу пакетів

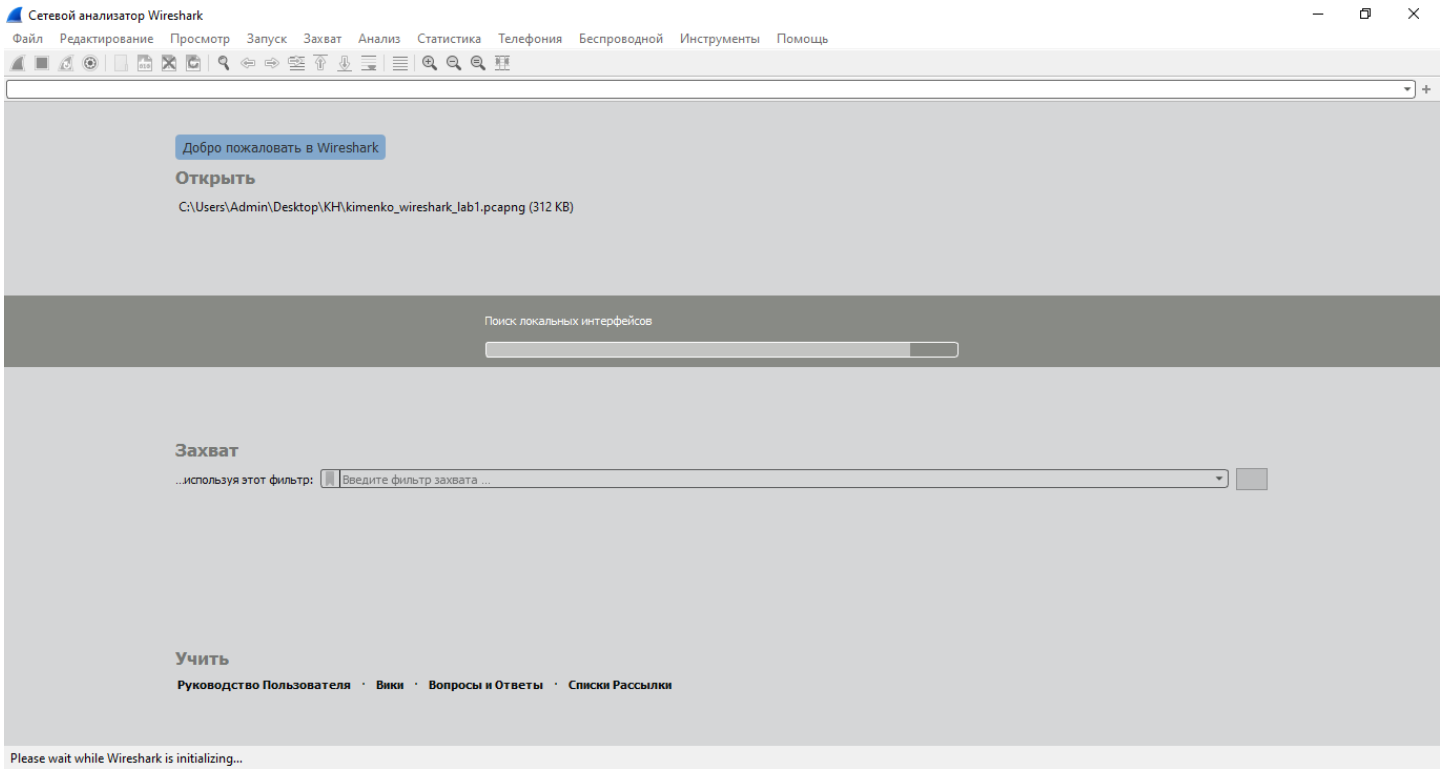
Мета роботи:

Оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

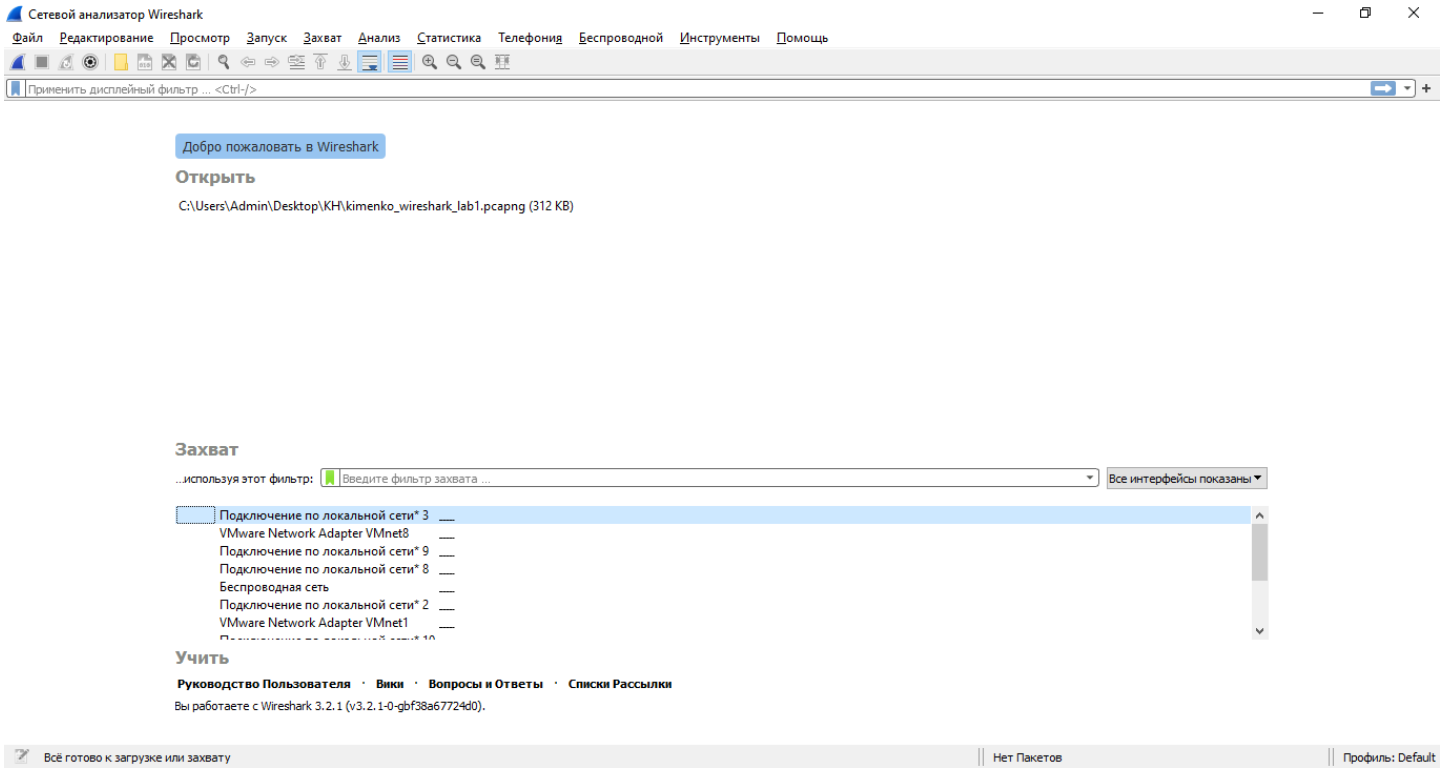
Хід роботи

Необхідно виконати наступні дії:

- ✓ Запустіть веб-браузер.
- ✓ Запустіть Wireshark.



- ✓ В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення:

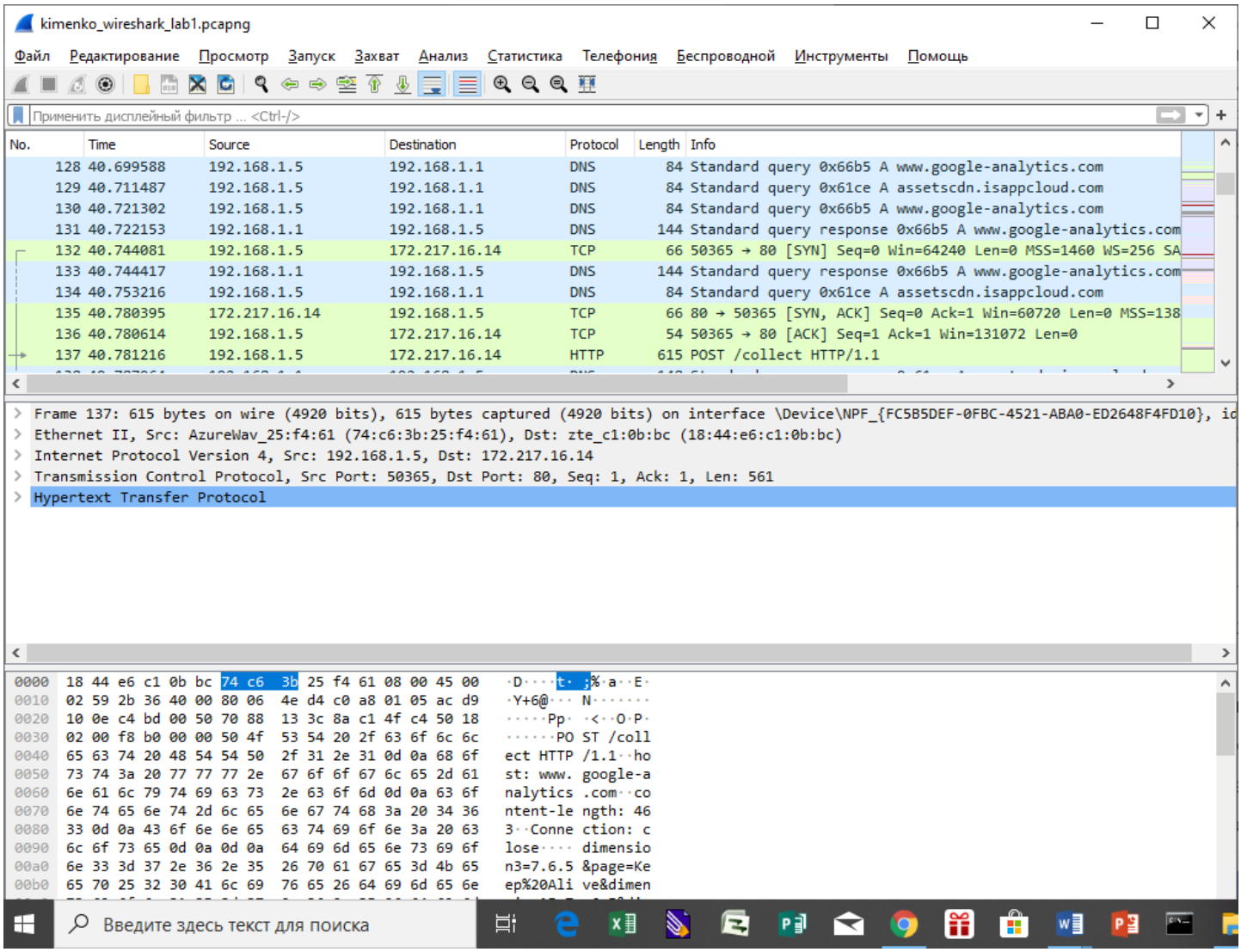


Capture >> Interfaces (або ж Ctrl + I)

✓ Далі виберіть той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натисніть кнопку Start навпроти нього

a. в випадку коли інтерфейс ще не ввімкнено можна вибрати any;

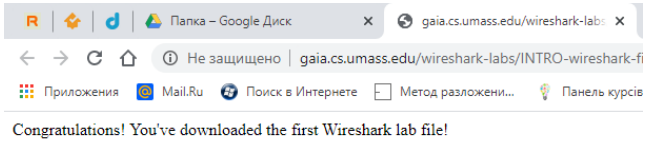
b. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;



✓ Поки Wireshark захоплює пакети, відкрийте в браузері сторінку за наступною адресою:

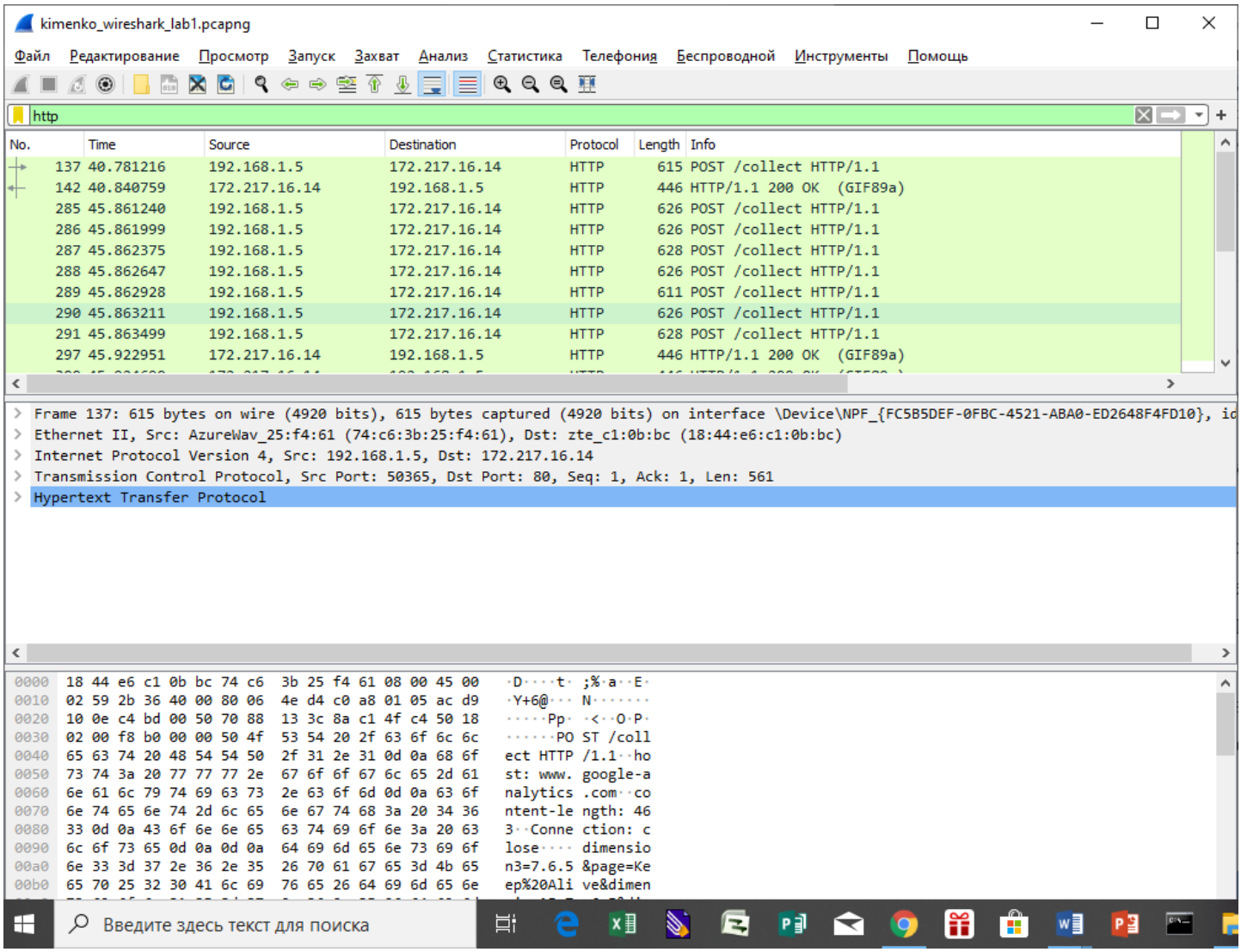
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.

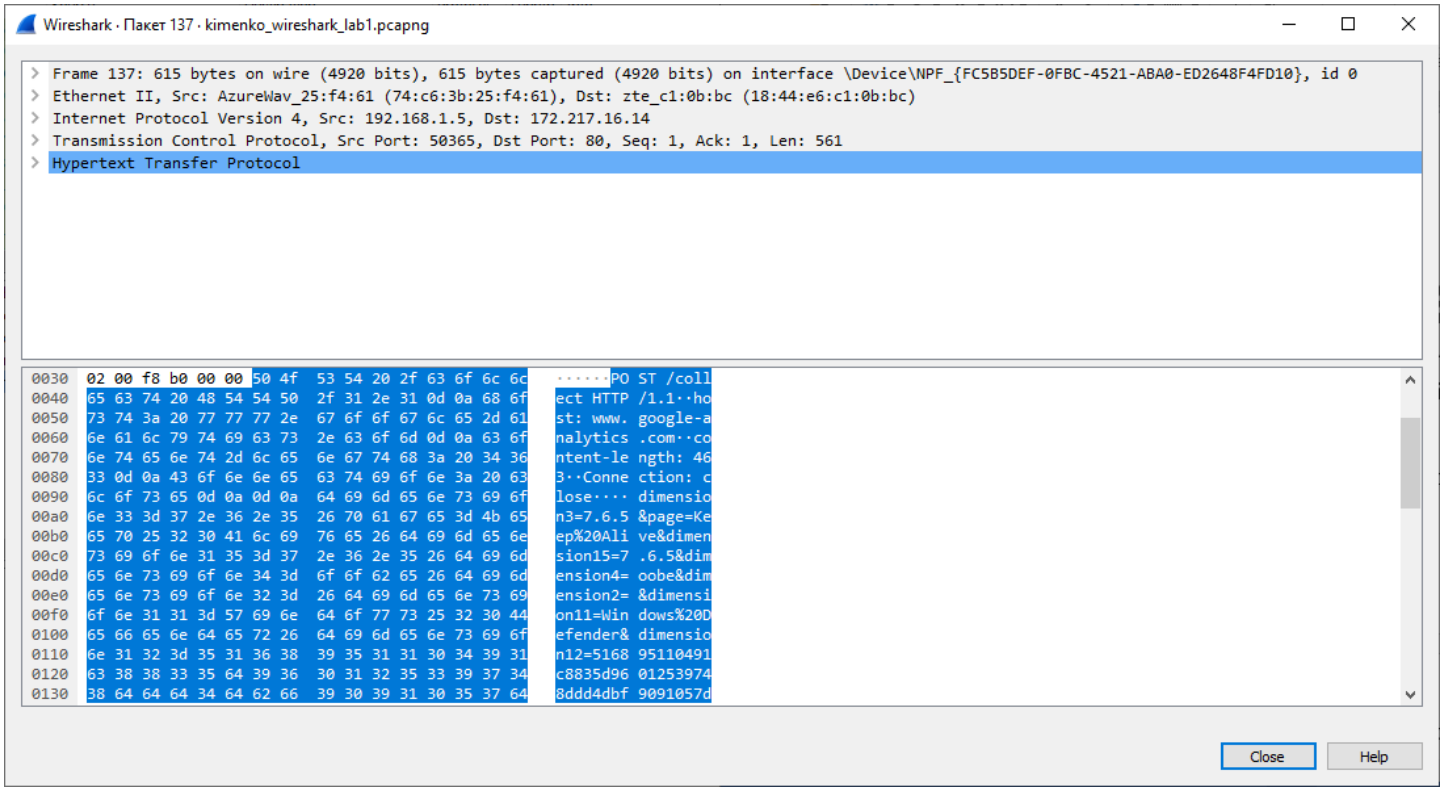


✓ Зупиніть захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl + E)

✓ Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів мають залишитися тільки пакети, які були створені протоколом HTTP.

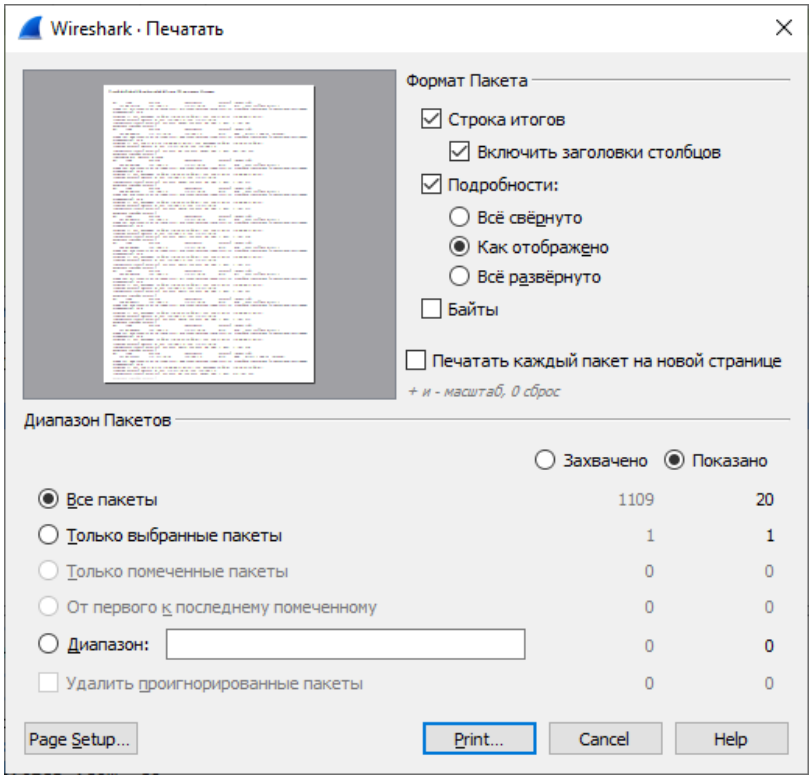


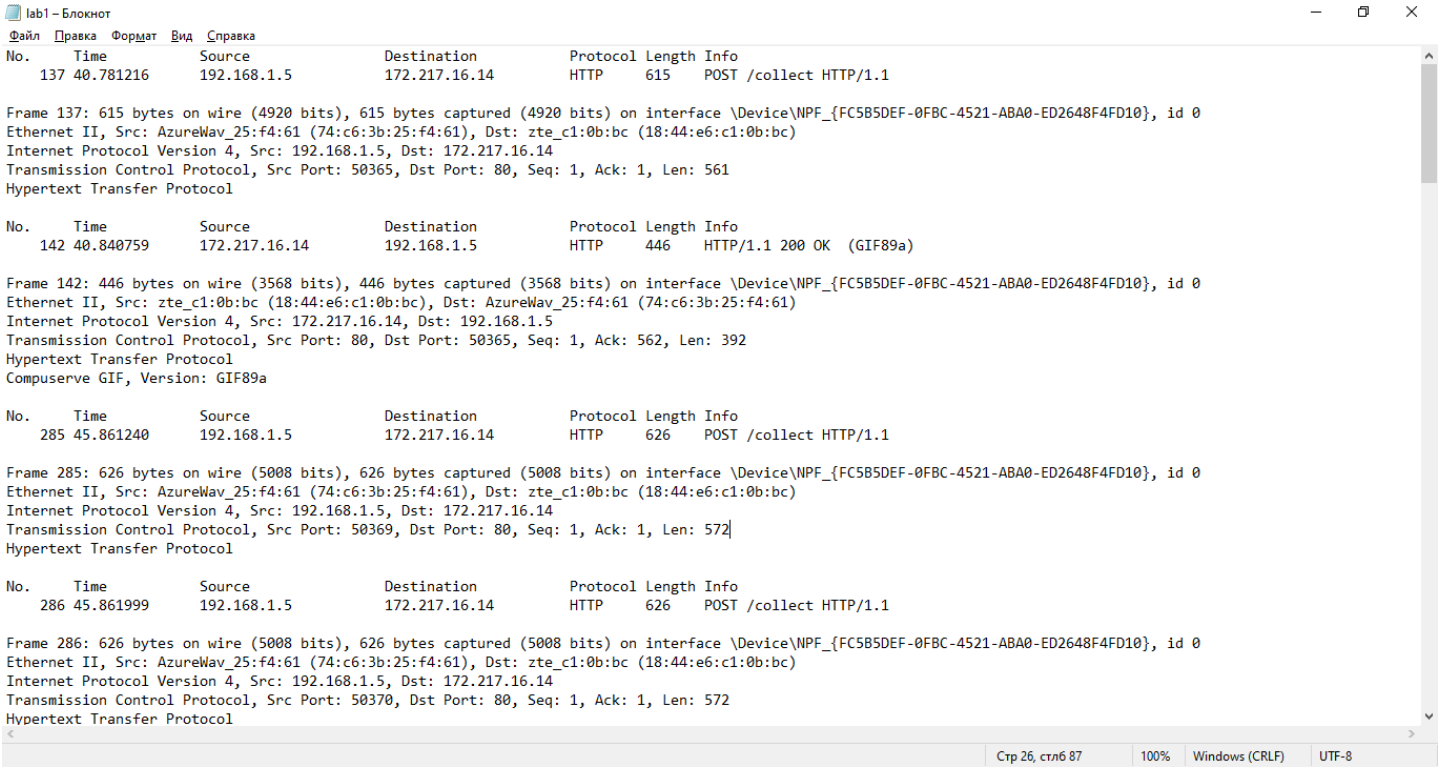
✓ Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.



✓ У вікні деталей заголовків розкрийте деталі, пов’язані з протоколом HTTP та скрийте детальну інформацію про інші протоколи.

✓ Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його так як показано на Малюнку 3 (ім’я файлу слід змінити на більш інформативне).





✓ Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.

✓ Закрийте Wireshark.

Контрольні запитання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
   DNS, TCP, HTTP, ICMPv6, IGMPv2, SSL, TLSv1.2, UDP, MDNS, LLMNR, NBNS
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
   Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, Hypertext Transfer Protocol.

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

   Пройшло 0.059543

3. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Запит:

Вихідний: 192.168.1.5

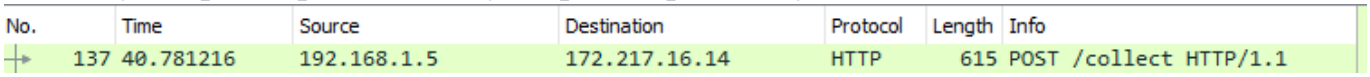
Цільовий: 172.217.16.14

Відповідь:

Вихідна:172.217.16.14

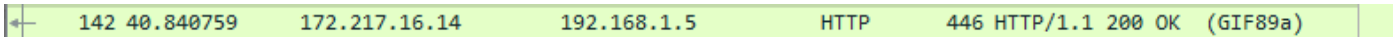
Цільова:192.168.1.5

4. Яким був перший рядок запиту на рівні протоколу HTTP?



No.	Time	Source	Destination	Protocol	Length	Info
137	40.781216	192.168.1.5	172.217.16.14	HTTP	615	POST /collect HTTP/1.1

5. Яким був перший рядок відповіді на рівні протоколу HTTP?



142	40.840759	172.217.16.14	192.168.1.5	HTTP	446	HTTP/1.1 200 OK (GIF89a)

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.