

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**  
**КАФЕДРА ММСА**

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

**Виконала:**  
**Студентка ІІІ курсу**  
**Групи КА-74**  
**Клименко І. О.**  
**Перевірів: Кухарєв С. О.**

**Київ 2020**

## **Тема: Основи захоплення та аналізу пакетів**

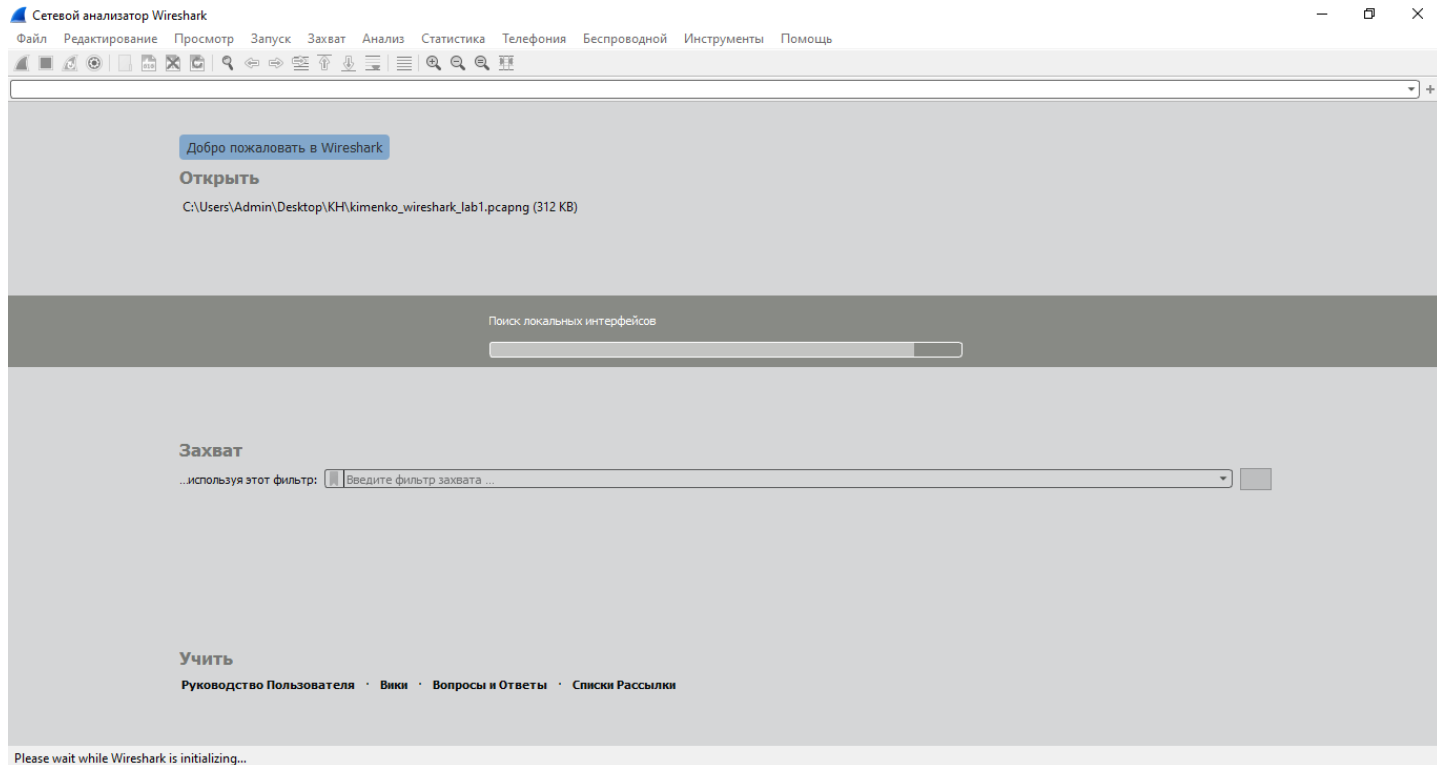
### **Мета роботи:**

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

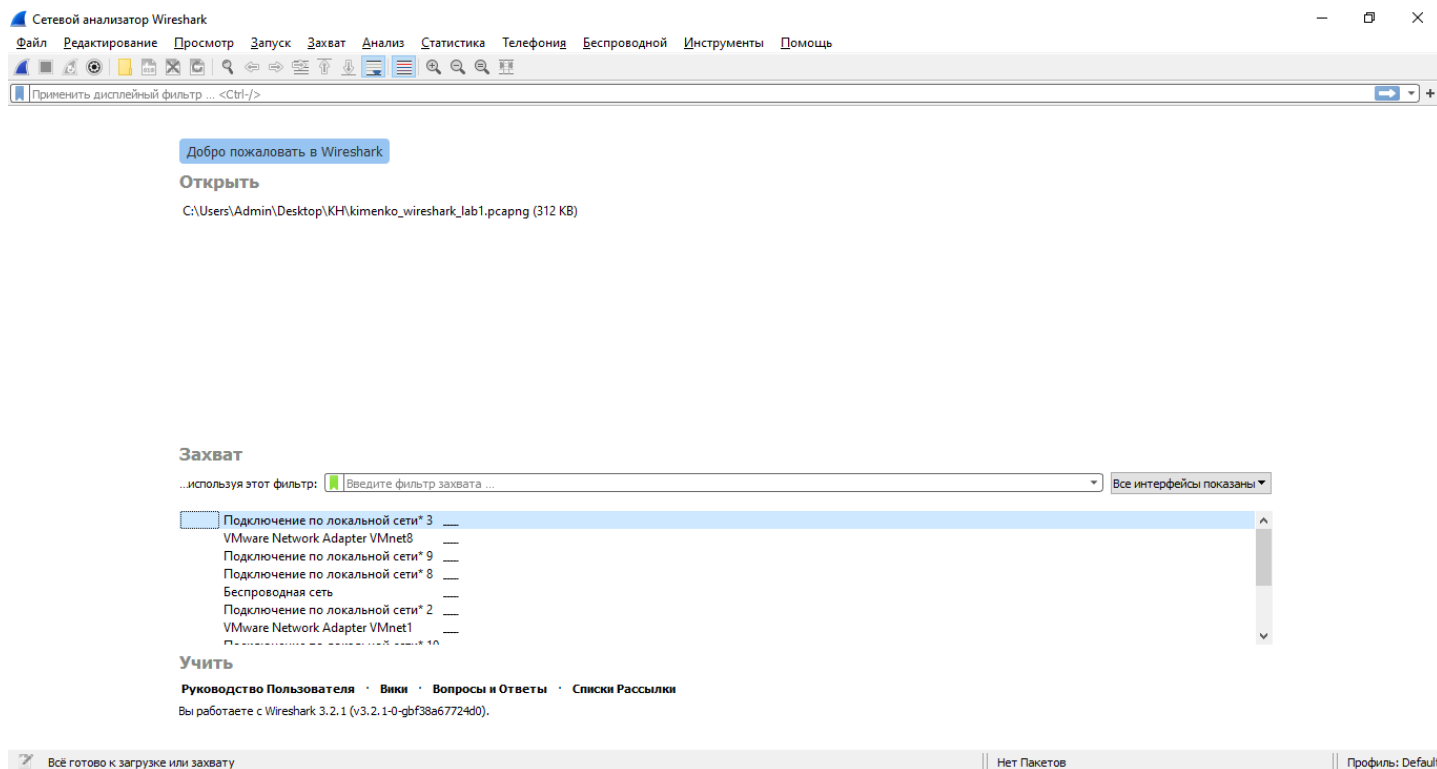
## Хід роботи

Необхідно виконати наступні дії:

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



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

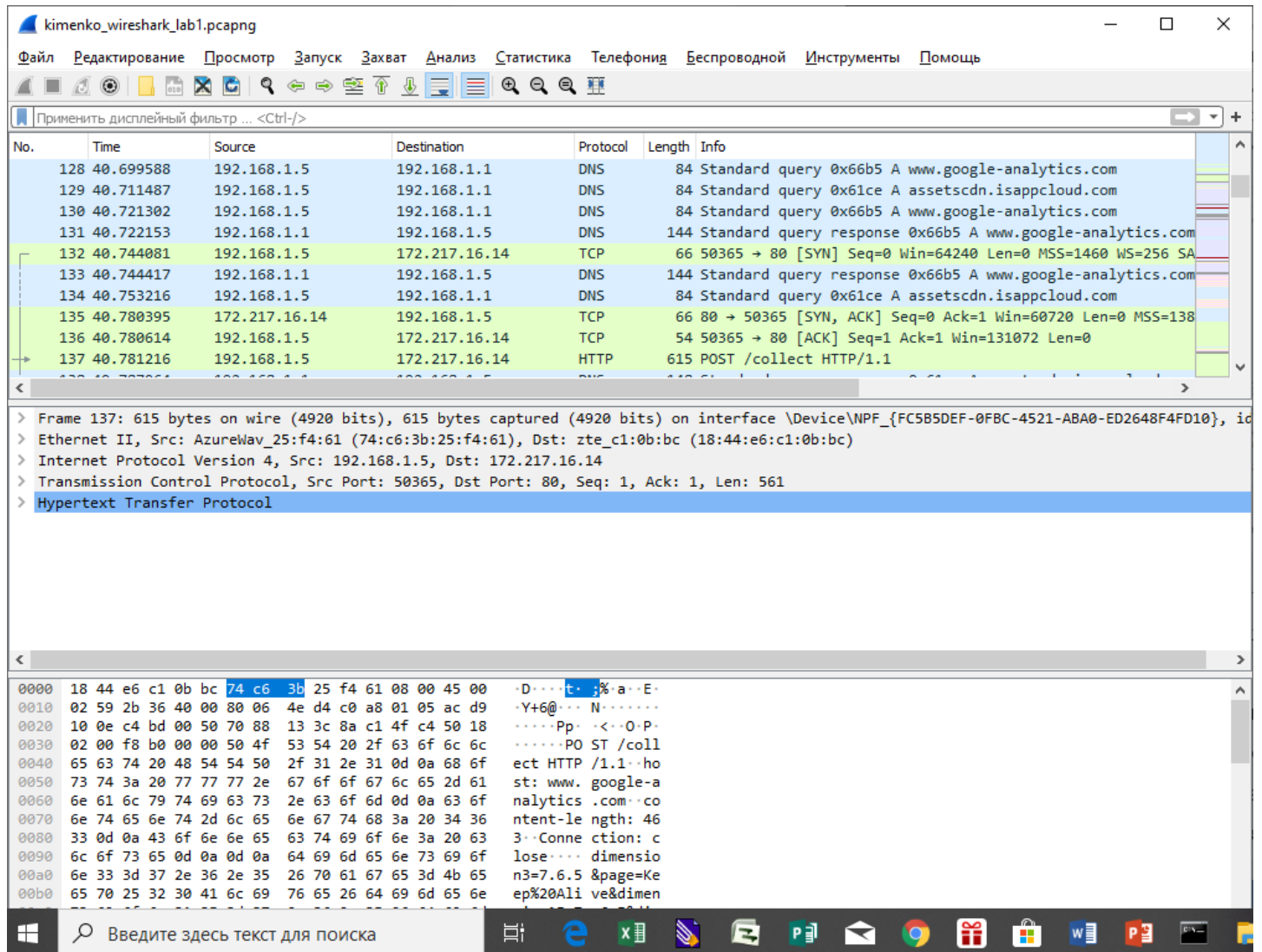


Capture >> Interfaces (або ж Ctrl + I)

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

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

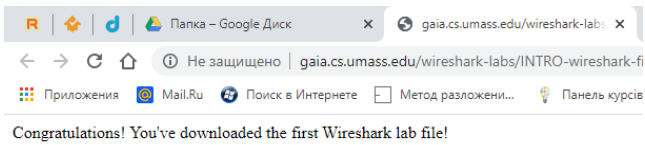
б. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;



✓ 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.

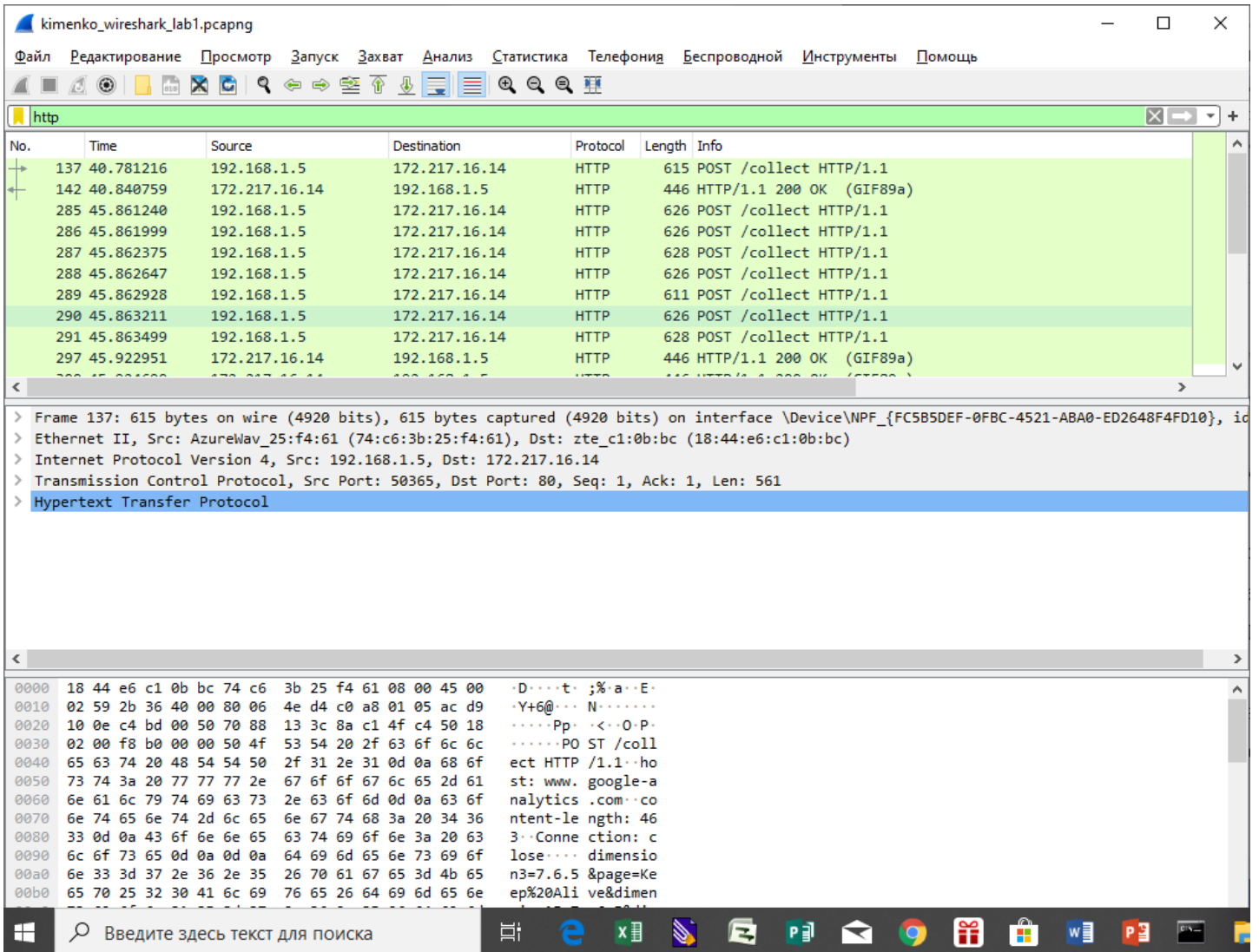


- ✓ Зупиніть захоплення пакетів за допомогою команди

Capture >> Stop (або Ctrl + E)

- ✓ Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів

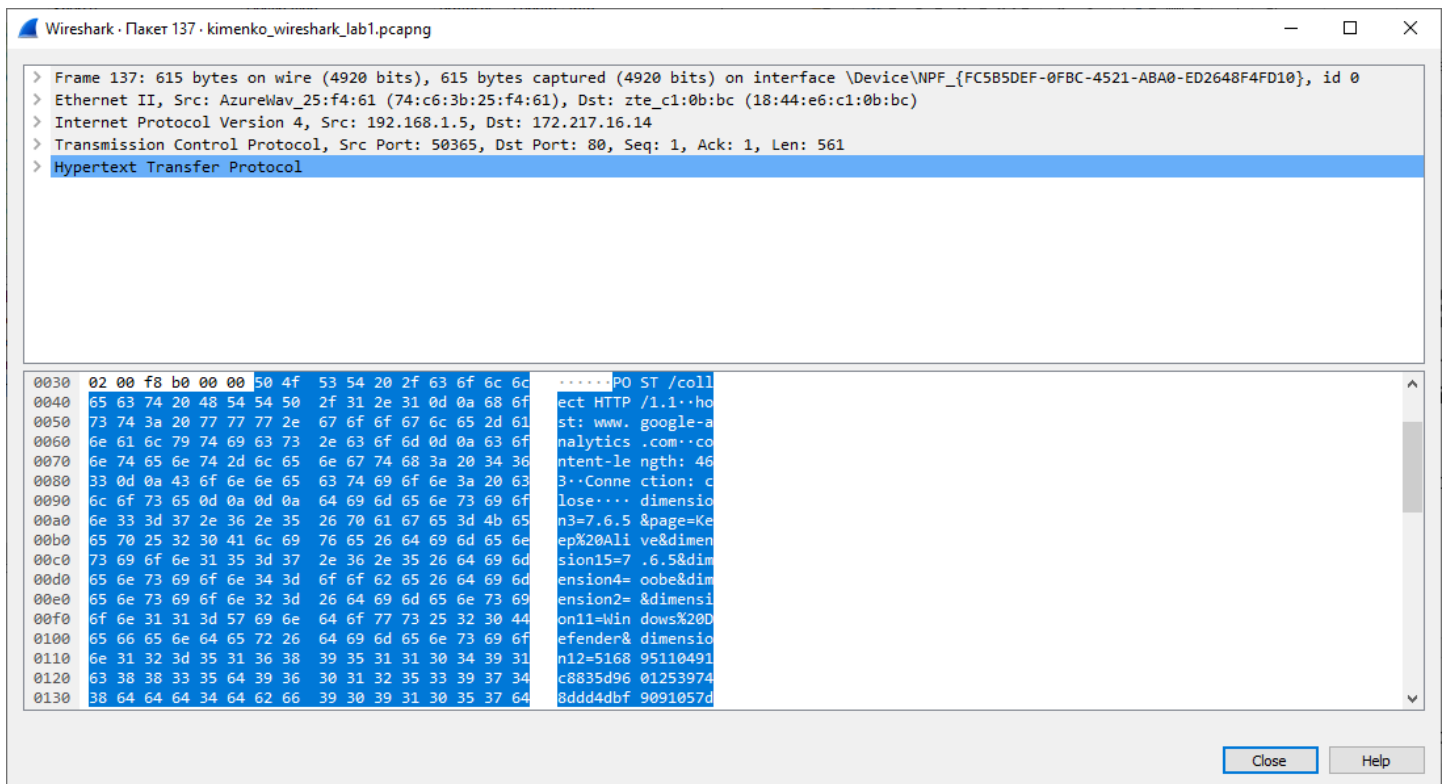
мають залишитися тільки пакети, які були створені протоколом HTTP.



- ✓ Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути

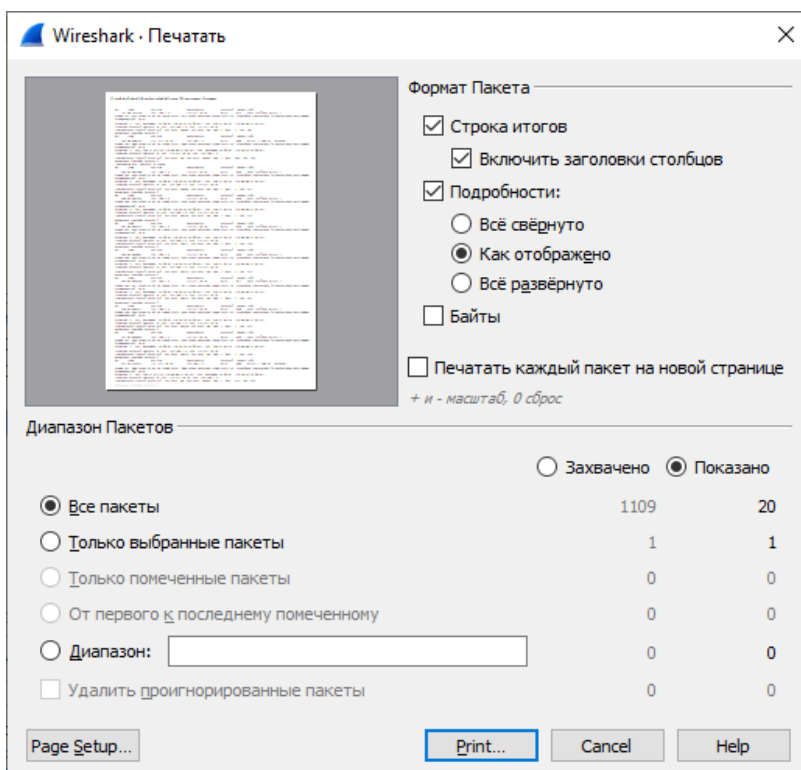
повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації

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).



lab1 - Блокнот

Файл	Правка	Формат	Вид	Справка		
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
Frame 137: 615 bytes on wire (4920 bits), 615 bytes captured (4920 bits) on interface \Device\NPF_{FC5B5DEF-0FBC-4521-ABA0-ED2648F4FD10}, id 0 Ethernet II, Src: AzureWav_25:f4:61 (74:c6:3b:25:f4:61), Dst: zte_c1:0b:bc (18:44:e6:c1:0b:bc) Internet Protocol Version 4, Src: 192.168.1.5, Dst: 172.217.16.14 Transmission Control Protocol, Src Port: 50365, Dst Port: 80, Seq: 1, Ack: 1, Len: 561 Hypertext Transfer Protocol						
No.	Time	Source	Destination	Protocol	Length	Info
142	40.840759	172.217.16.14	192.168.1.5	HTTP	446	HTTP/1.1 200 OK (GIF89a)
Frame 142: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface \Device\NPF_{FC5B5DEF-0FBC-4521-ABA0-ED2648F4FD10}, id 0 Ethernet II, Src: zte_c1:0b:bc (18:44:e6:c1:0b:bc), Dst: AzureWav_25:f4:61 (74:c6:3b:25:f4:61) Internet Protocol Version 4, Src: 172.217.16.14, Dst: 192.168.1.5 Transmission Control Protocol, Src Port: 80, Dst Port: 50365, Seq: 1, Ack: 562, Len: 392 Hypertext Transfer Protocol CompuServe GIF, Version: GIF89a						
No.	Time	Source	Destination	Protocol	Length	Info
285	45.861240	192.168.1.5	172.217.16.14	HTTP	626	POST /collect HTTP/1.1
Frame 285: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{FC5B5DEF-0FBC-4521-ABA0-ED2648F4FD10}, id 0 Ethernet II, Src: AzureWav_25:f4:61 (74:c6:3b:25:f4:61), Dst: zte_c1:0b:bc (18:44:e6:c1:0b:bc) Internet Protocol Version 4, Src: 192.168.1.5, Dst: 172.217.16.14 Transmission Control Protocol, Src Port: 50369, Dst Port: 80, Seq: 1, Ack: 1, Len: 572 Hypertext Transfer Protocol						
No.	Time	Source	Destination	Protocol	Length	Info
286	45.861999	192.168.1.5	172.217.16.14	HTTP	626	POST /collect HTTP/1.1
Frame 286: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{FC5B5DEF-0FBC-4521-ABA0-ED2648F4FD10}, id 0 Ethernet II, Src: AzureWav_25:f4:61 (74:c6:3b:25:f4:61), Dst: zte_c1:0b:bc (18:44:e6:c1:0b:bc) Internet Protocol Version 4, Src: 192.168.1.5, Dst: 172.217.16.14 Transmission Control Protocol, Src Port: 50370, Dst Port: 80, Seq: 1, Ack: 1, Len: 572 Hypertext Transfer Protocol						

Стр 26, стр 6 87100%Windows (CRLF)UTF-8

✓ 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.