

Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Кафедра математичних методів системного аналізу

## ЗВІТ

Про виконання лабораторних робіт

З дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-ЗП93

Шаповалова О.І.

Прийняв: Кухарєв С.О.

Київ - 2020

## Лабораторна робота №1

### Основи захоплення та аналізу пакетів

**Мета роботи:** оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

#### *Хід роботи*

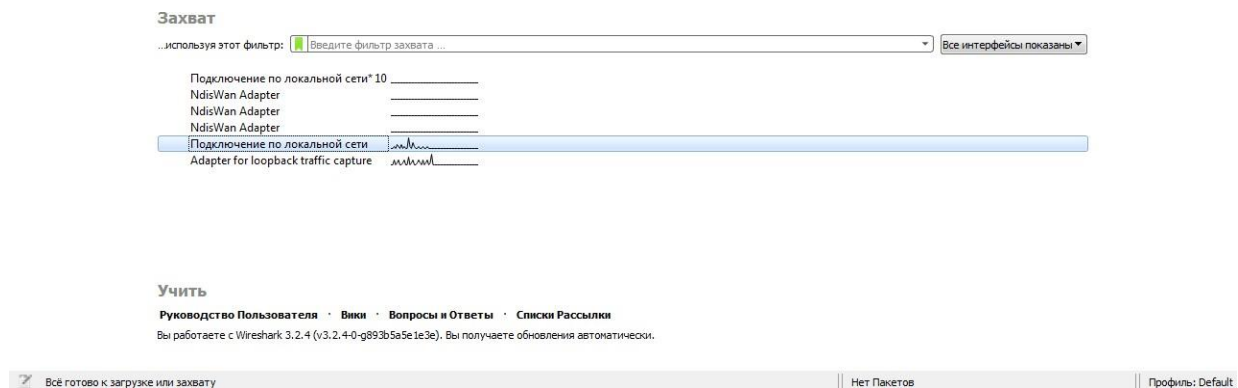
Необхідно виконати наступні дії:

1. Запустіть веб-браузер.
2. Запустіть Wireshark.
3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення:

Capture >> Interfaces (або ж Ctrl + I)

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

- у випадку коли інтерфейс ще не ввімкнено можна вибрати any;
- у випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;



Для виконання лабораторної роботи була обрана локальна мережа. Мережа “adapter for loopback traffic capture” не була обрана, оскільки в такому випадку захоплення пакетів HTTP не відбувалось.

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

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

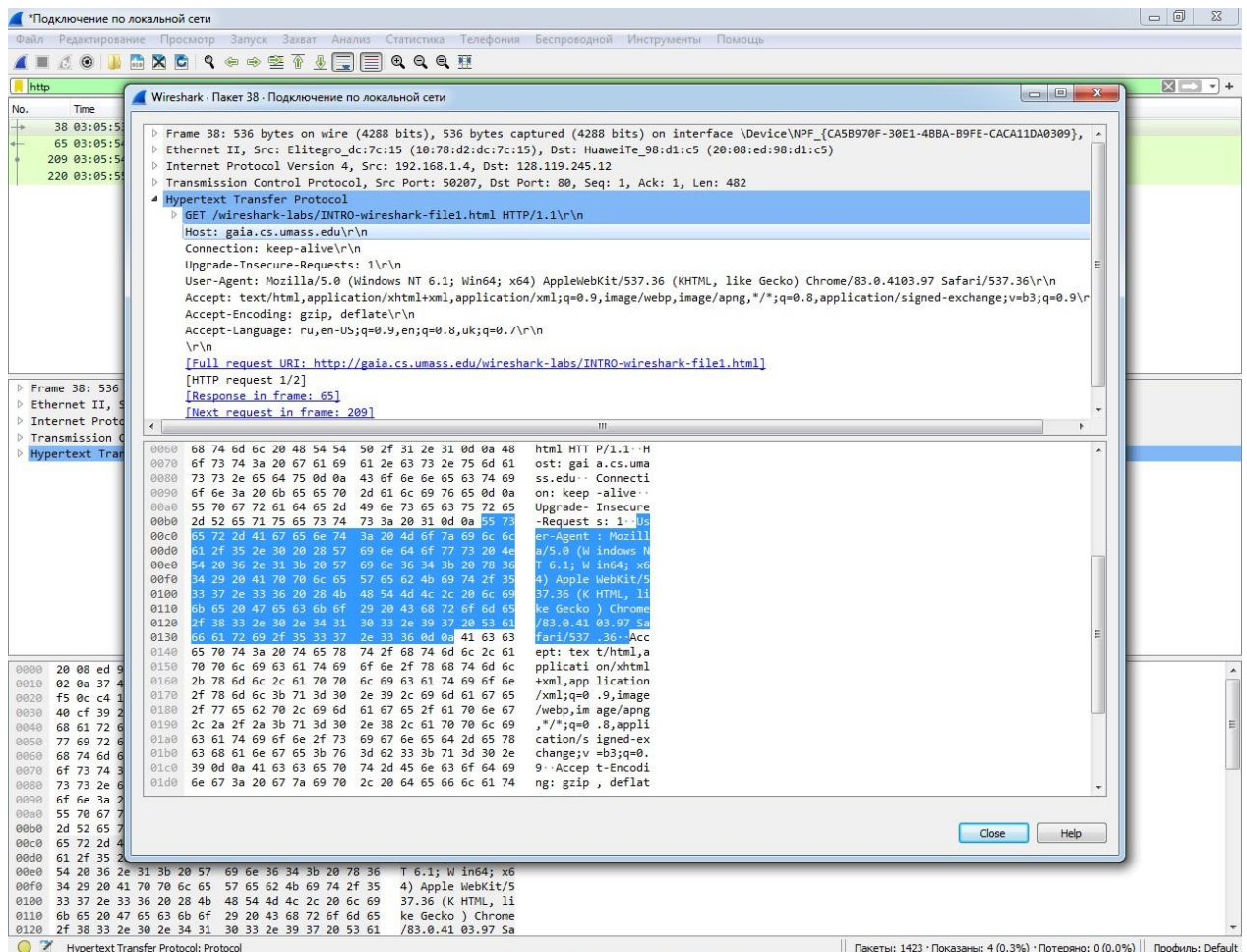
Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.

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

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

8. 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.

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



10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його

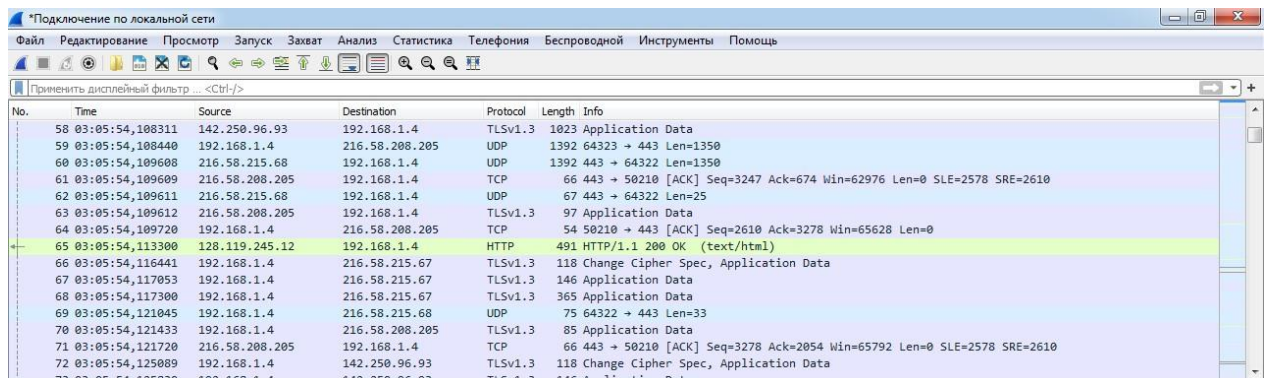
11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.

12. Закрийте Wireshark.

### Контрольні запитання

1. Які протоколи відображались в вікні лістингу протоколів до включення фільтрації?

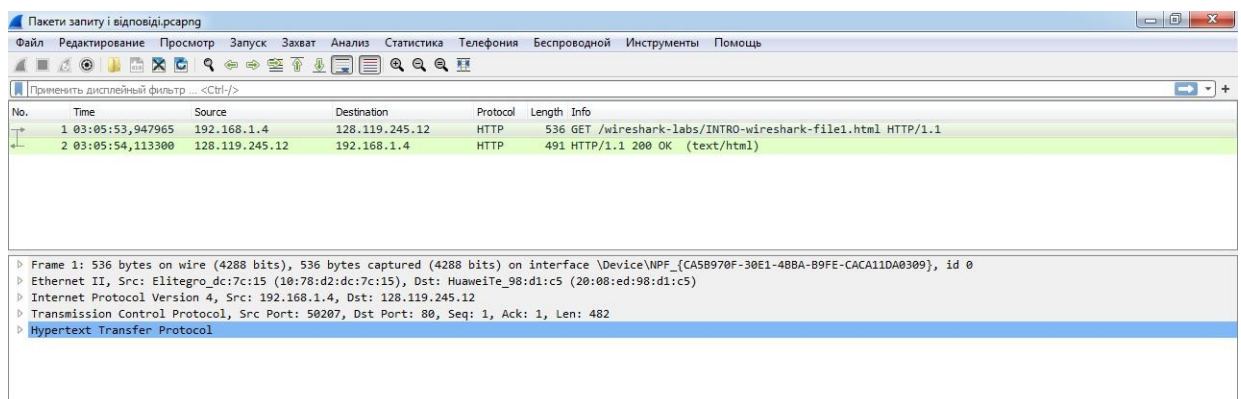
До включення фільтру відображались різноманітні протоколи типу UDP, TCP, HTTP, TLSv1.3.



No.	Time	Source	Destination	Protocol	Length	Info
58	03:05:54,108311	142.250.96.93	192.168.1.4	TLSv1.3	1023	Application Data
59	03:05:54,108440	192.168.1.4	216.58.208.205	UDP	1392	64323 → 443 Len=1350
60	03:05:54,109608	216.58.215.68	192.168.1.4	UDP	1392	443 → 64322 Len=1350
61	03:05:54,109609	216.58.208.205	192.168.1.4	TCP	66	443 → 50210 [ACK] Seq=3247 Ack=674 Win=62976 Len=0 SLE=2578 SRE=2610
62	03:05:54,109611	216.58.215.68	192.168.1.4	UDP	67	443 → 64322 Len=25
63	03:05:54,109612	216.58.208.205	192.168.1.4	TLSv1.3	97	Application Data
64	03:05:54,109720	192.168.1.4	216.58.208.205	TCP	54	50210 → 443 [ACK] Seq=2610 Ack=3278 Win=65628 Len=0
65	03:05:54,113300	128.119.245.12	192.168.1.4	HTTP	491	HTTP/1.1 200 OK (text/html)
66	03:05:54,116441	192.168.1.4	216.58.215.67	TLSv1.3	118	Change Cipher Spec, Application Data
67	03:05:54,117053	192.168.1.4	216.58.215.67	TLSv1.3	146	Application Data
68	03:05:54,117300	192.168.1.4	216.58.215.67	TLSv1.3	365	Application Data
69	03:05:54,121045	192.168.1.4	216.58.215.68	UDP	75	64322 → 443 Len=33
70	03:05:54,121433	192.168.1.4	216.58.208.205	TLSv1.3	85	Application Data
71	03:05:54,121720	216.58.208.205	192.168.1.4	TCP	66	443 → 50210 [ACK] Seq=3278 Ack=2054 Win=65792 Len=0 SLE=2578 SRE=2610
72	03:05:54,125089	192.168.1.4	142.250.96.93	TLSv1.3	118	Change Cipher Spec, Application Data
73	03:05:54,125090	192.168.1.4	142.250.96.93	TLSv1.3	146	Application Data

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

В збережених пакетах запиту та відповіді використовуються протоколи HTTP

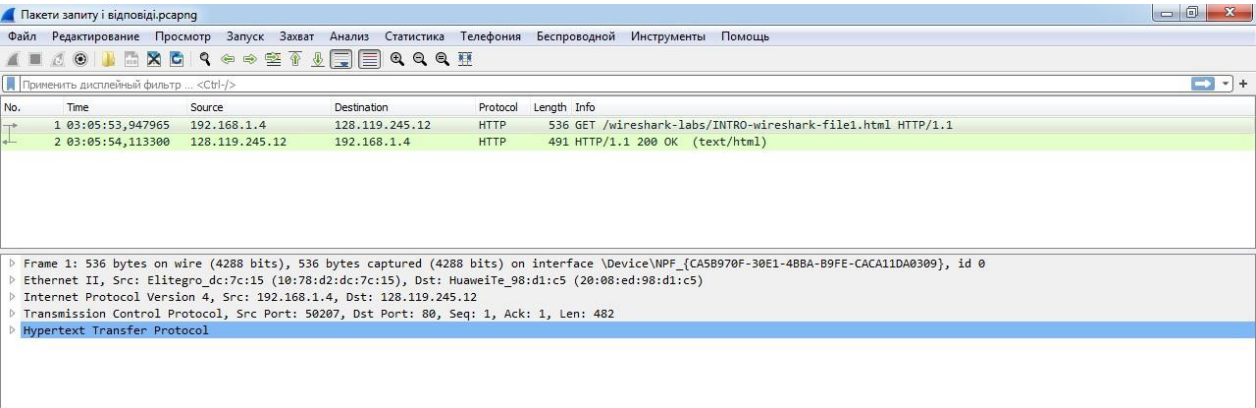


No.	Time	Source	Destination	Protocol	Length	Info
1	03:05:53,947965	192.168.1.4	128.119.245.12	HTTP	536	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2	03:05:54,113300	128.119.245.12	192.168.1.4	HTTP	491	HTTP/1.1 200 OK (text/html)

Frame 1: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF\_{C45B970F-30E1-48BA-B9FE-CACA11DA0309}, id 0  
Ethernet II, Src: Elitegro\_dc7c:15 (10:78:d2:dc:7c:15), Dst: HuaweiTe\_98:d1:c5 (20:08:ed:98:d1:c5)  
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 50207, Dst Port: 80, Seq: 1, Ack: 1, Len: 482  
Hypertext Transfer Protocol

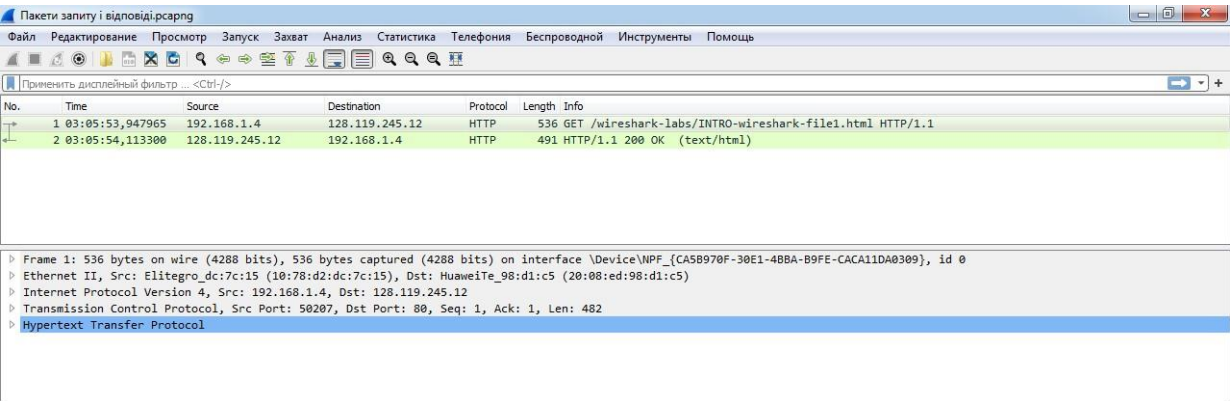
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

Тривалість періоду часу, що пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера, складає 165335 мікросекунд (1000000-947965+113300=165335 мікросекунд)



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

	Вихідна адреса	Цільова адреса
Пакет із запитом	192.168.1.4	128.119.245.12
Пакет із відповіддю	128.119.245.12	192.168.1.4



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

	Перший рядок
Пакет запиту	Запит GET /wireshark-labs/INTRO-wireshark-file1.html
Пакет відповіді	Відповідь сервера із статус кодом 200 (Ok)

