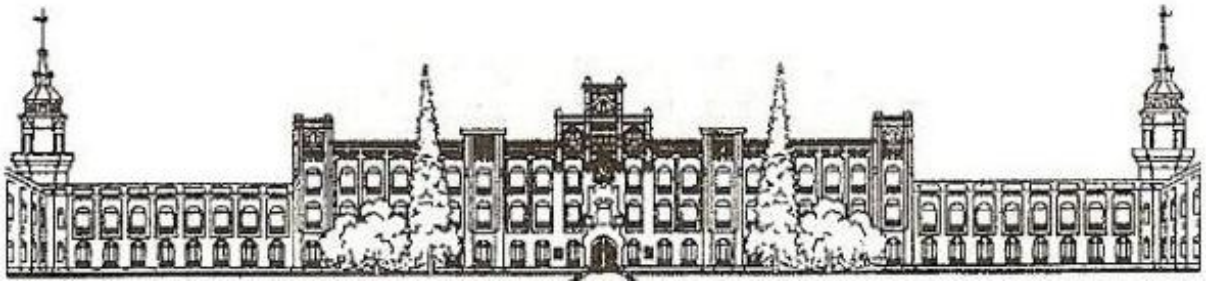


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

КАФЕДРА ММСА

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

Виконав:

Студент III курсу

Групи КА-74

Микитенко О.В.

Перевірив: Кухарєв С. О.

Київ 2020

Тема: Основи захоплення та аналізу пакетів

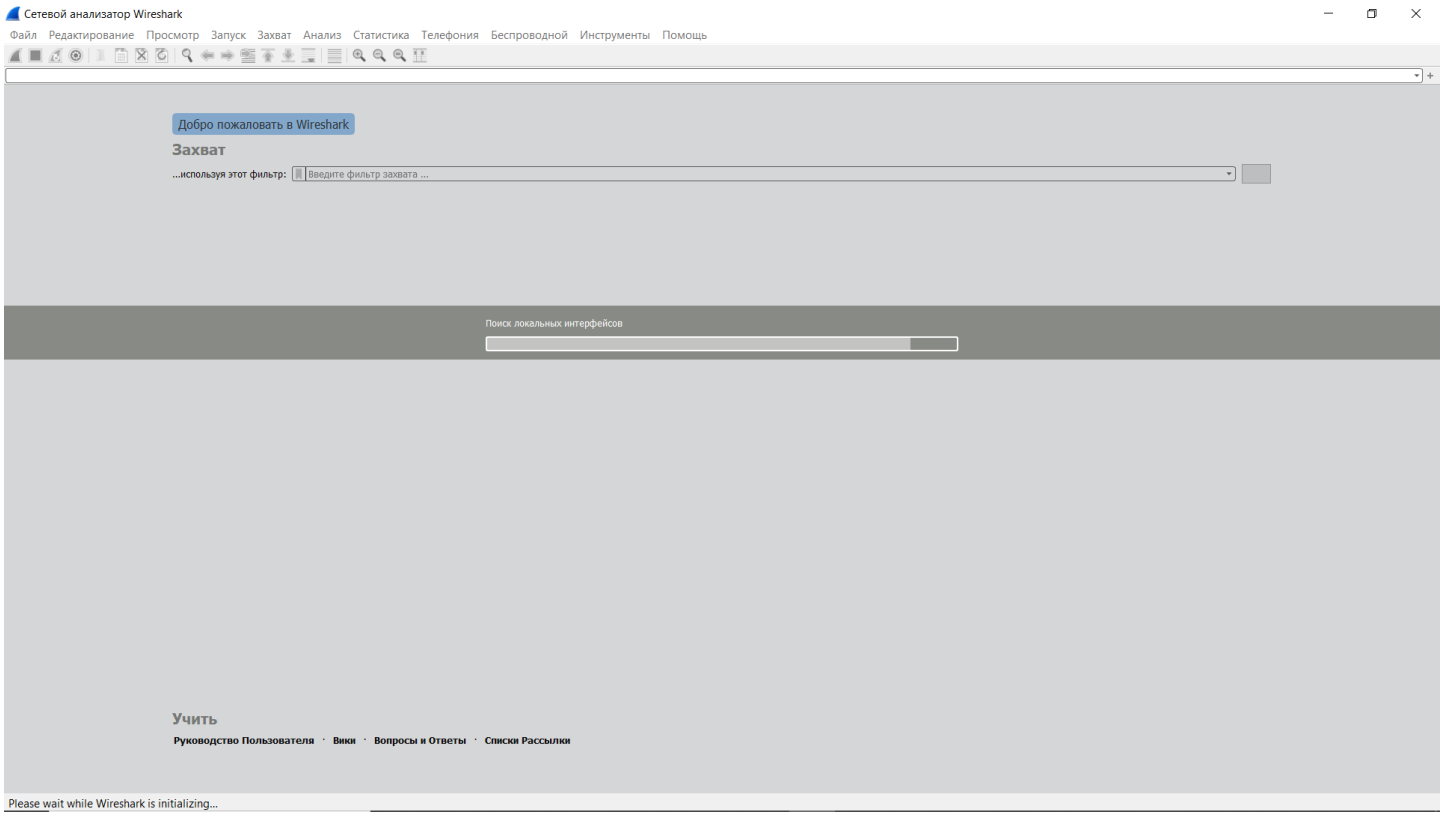
Мета роботи:

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

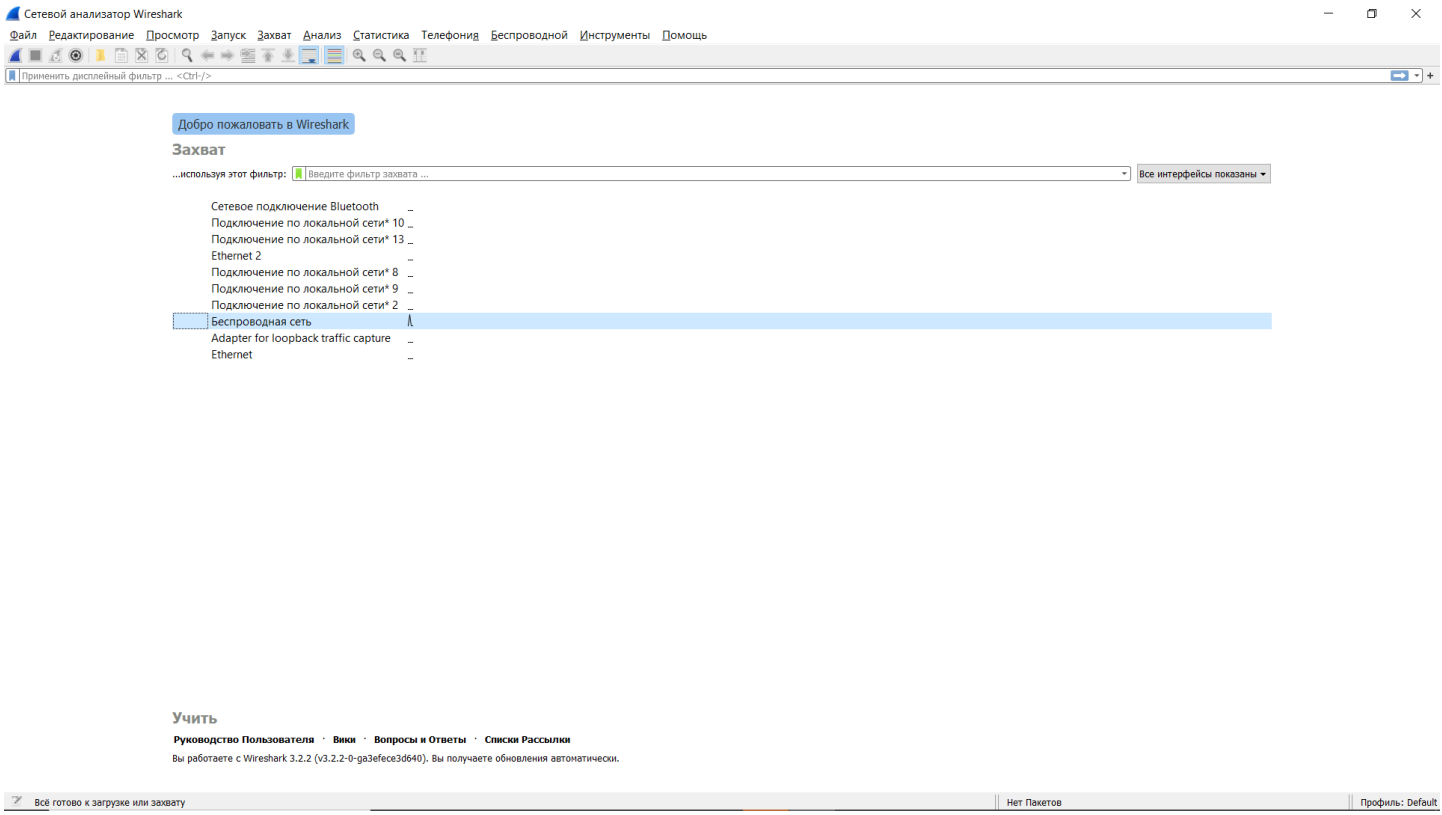
Хід роботи

Необхідно виконати наступні дії:

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



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

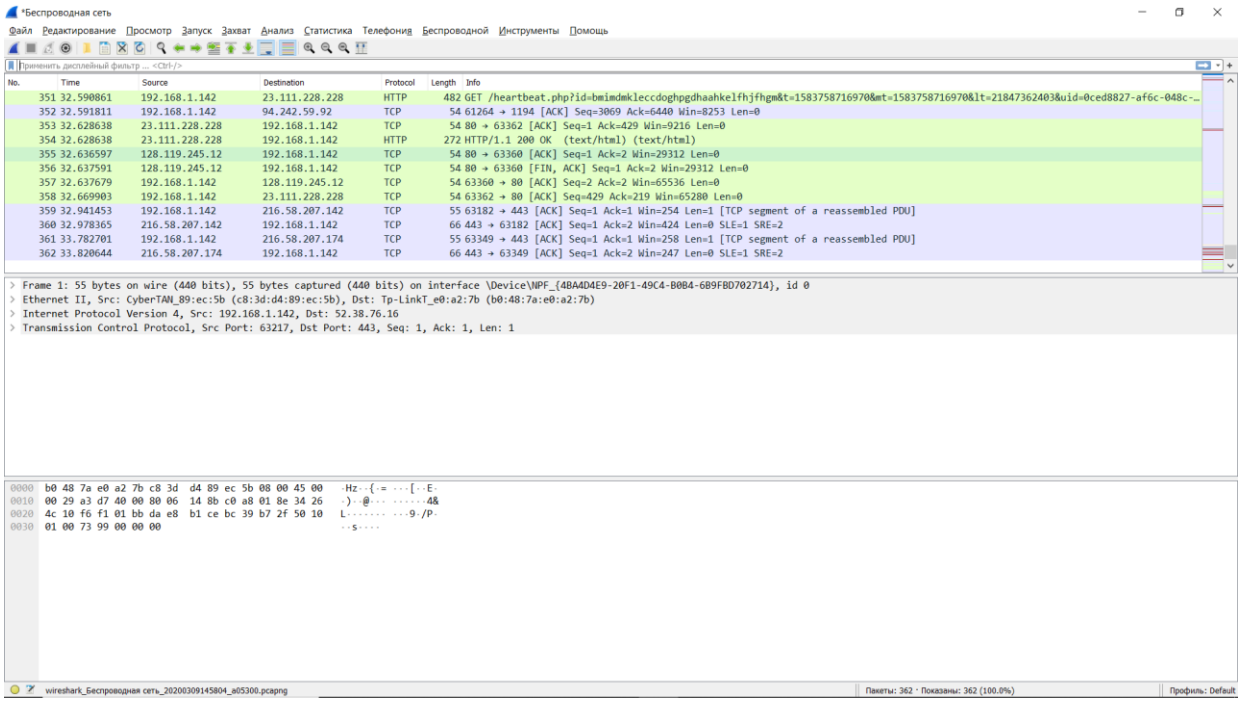


Capture >> Interfaces (або ж Ctrl + I)

✓ 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;

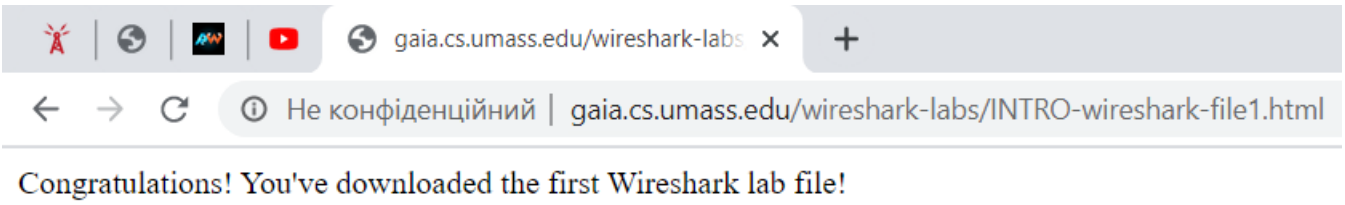
b. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;



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

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

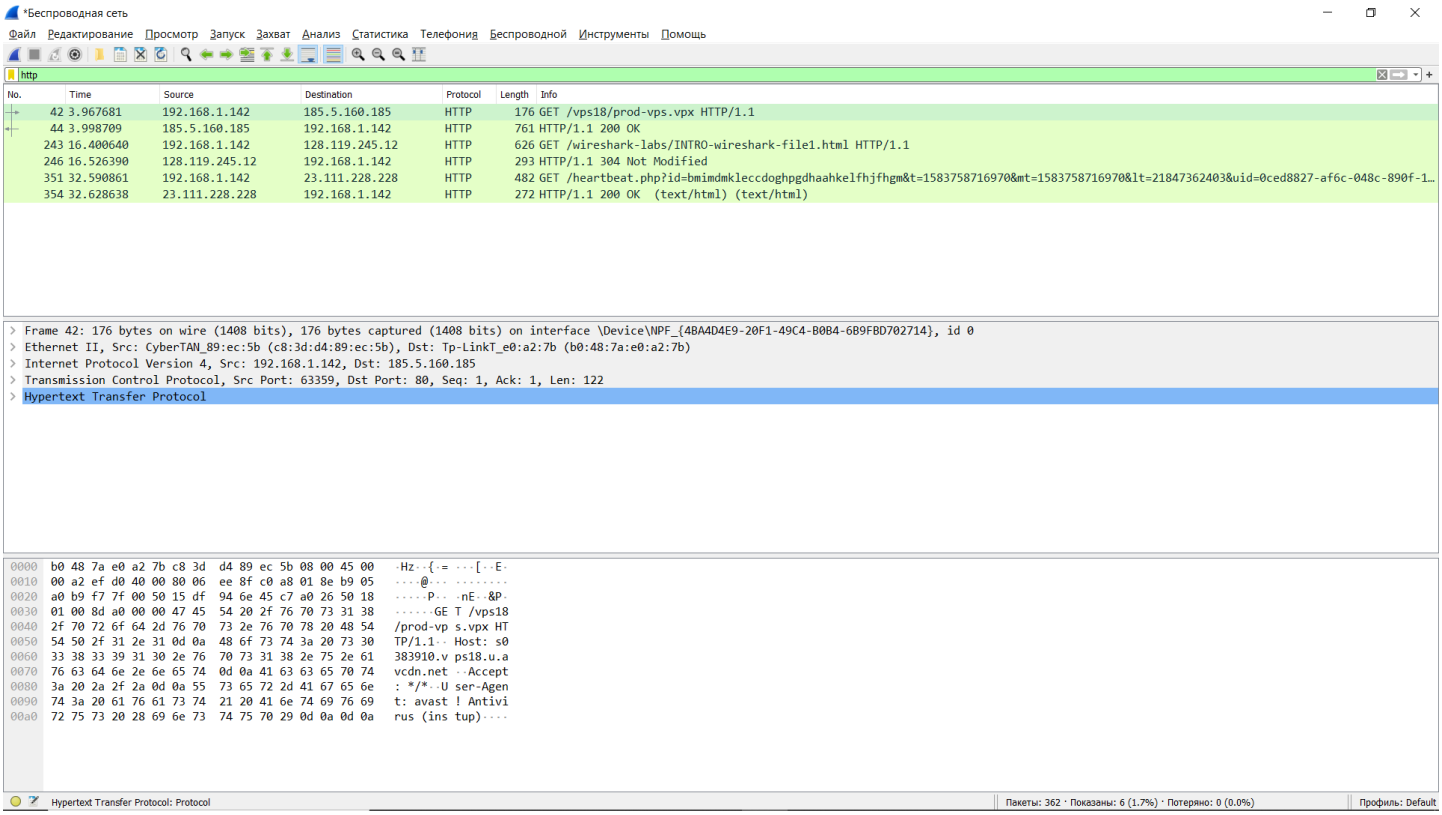
Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.



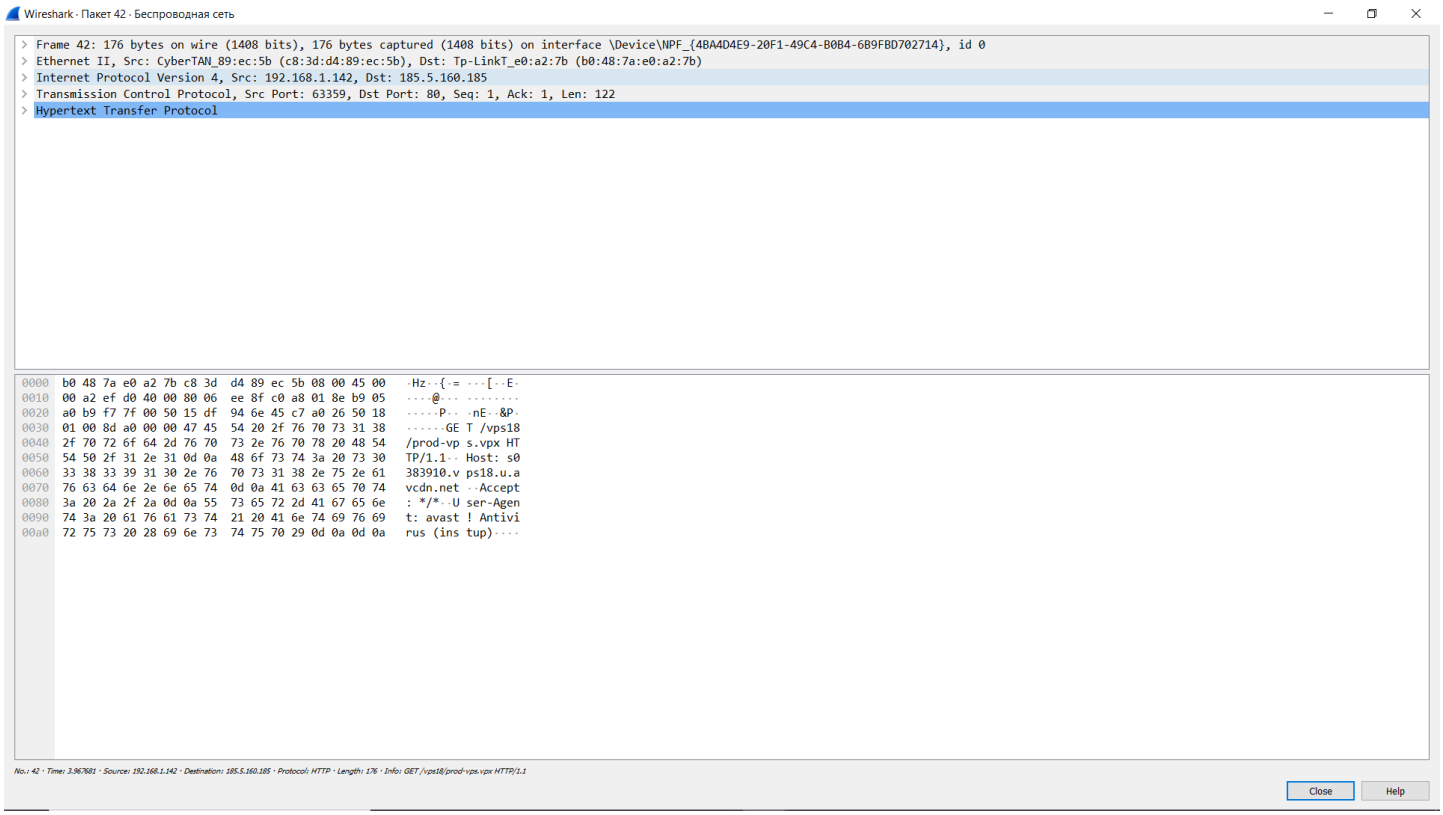
✓ Зупиніть захоплення пакетів за допомогою команди

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).

Wireshark · Печатать

Формат Пакета

- [x] Строка итогов
  - [x] Включить заголовки столбцов
- [x] Подробности:
  - ( ) Всё свёрнуто
  - (•) Как отображено
  - ( ) Всё развёрнуто
- [ ] Байты

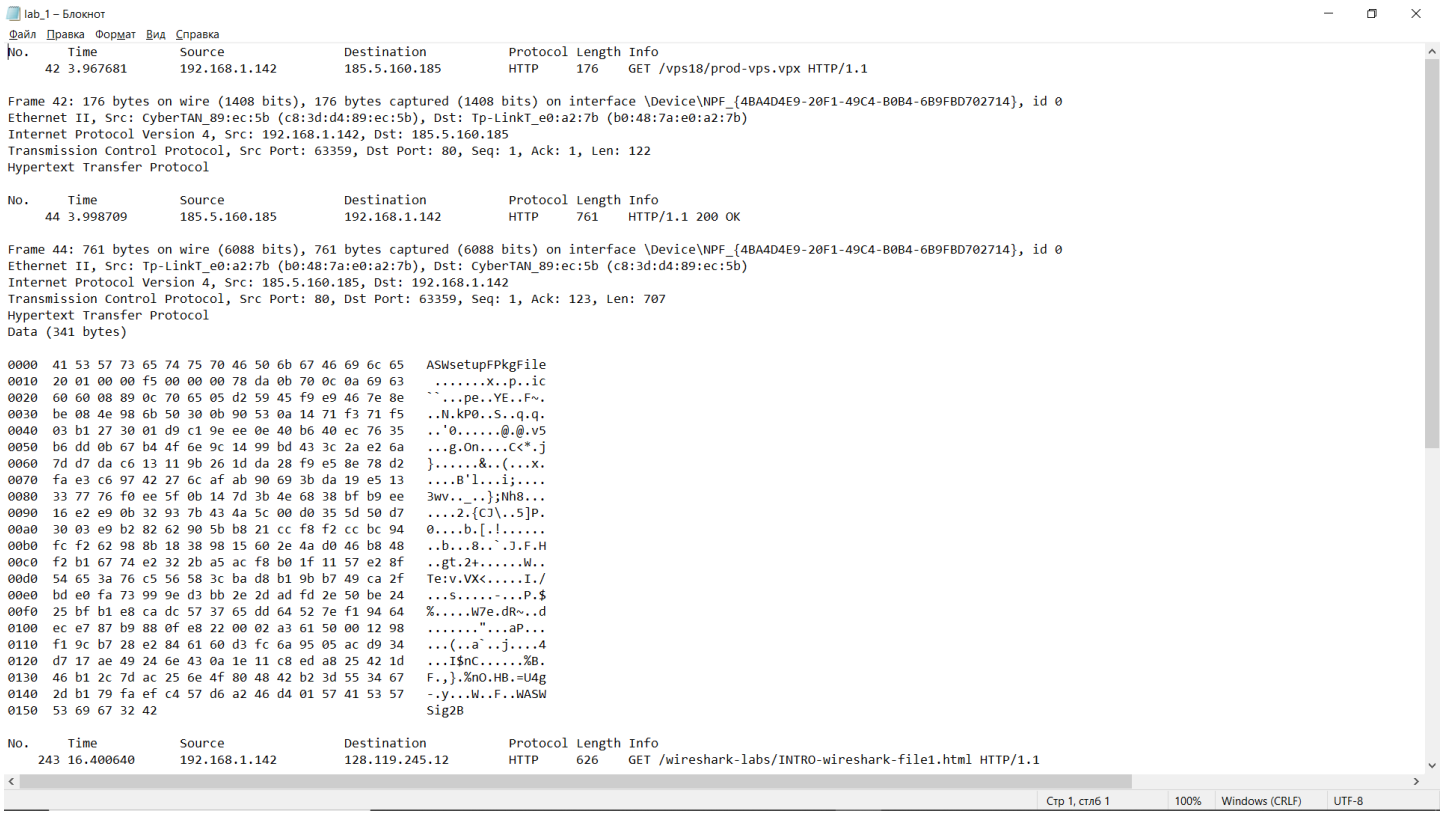
- [ ] Печатать каждый пакет на новой странице

+ и - масштаб, 0 сброс

Диапазон Пакетов

		Захвачено	Показано
(•)	Все пакеты	362	6
( )	Только выбранные пакеты	1	1
( )	Только помеченные пакеты	0	0
( )	От первого к последнему помеченному	0	0
( )	Диапазон:	0	0
[ ]	Удалить проигнорированные пакеты	0	0

Page Setup... | Print... | Cancel | Help



lab_1 – Блокнот

Файл Правка Формат Вид Справка

```
No.     Time           Source                Destination           Protocol Length Info
     42 3.967681       192.168.1.142         185.5.160.185         HTTP     176    GET /vps18/prod-vps.vpx HTTP/1.1

Frame 42: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface \Device\NPF_{4BA4D4E9-20F1-49C4-B0B4-6B9FBD702714}, id 0
Ethernet II, Src: CyberTAN_89:ec:5b (c8:3d:d4:89:ec:5b), Dst: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b)
Internet Protocol Version 4, Src: 192.168.1.142, Dst: 185.5.160.185
Transmission Control Protocol, Src Port: 63359, Dst Port: 80, Seq: 1, Ack: 1, Len: 122
Hypertext Transfer Protocol

No.     Time           Source                Destination           Protocol Length Info
     44 3.998709       185.5.160.185         192.168.1.142         HTTP     761    HTTP/1.1 200 OK

Frame 44: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits) on interface \Device\NPF_{4BA4D4E9-20F1-49C4-B0B4-6B9FBD702714}, id 0
Ethernet II, Src: Tp-LinkT_e0:a2:7b (b0:48:7a:e0:a2:7b), Dst: CyberTAN_89:ec:5b (c8:3d:d4:89:ec:5b)
Internet Protocol Version 4, Src: 185.5.160.185, Dst: 192.168.1.142
Transmission Control Protocol, Src Port: 80, Dst Port: 63359, Seq: 1, Ack: 123, Len: 707
Hypertext Transfer Protocol
Data (341 bytes)

0000  41 53 57 73 65 74 75 70 46 50 6b 67 46 69 6c 65   ASWsetupFPkgFile
0010  20 01 00 00 f5 00 00 00 78 da 0b 70 0c 0a 69 63    .......x..p..ic
0020  60 60 08 89 0c 70 65 05 d2 59 45 f9 e9 46 7e 8e  ``...pe..YE..F~.
0030  be 08 4e 98 6b 50 30 0b 90 53 0a 14 71 f3 71 f5  ..N.kP0..S..q.q.
0040  03 b1 27 30 01 d9 c1 9e ee 0e 40 b6 40 ec 76 35  ..'0......@.@.v5
0050  b6 dd 0b 67 b4 4f 6e 9c 14 99 bd 43 3c 2a e2 6a  ...g.On....C<*.j
0060  7d d7 da c6 13 11 9b 26 1d da 28 f9 e5 8e 78 d2  }......&..(...x.
0070  fa e3 c6 97 42 27 6c af ab 90 69 3b da 19 e5 13  ....B'l...i;....
0080  33 77 76 f0 ee 5f 0b 14 7d 3b 4e 68 38 bf b9 ee  3wv.._..};Nh8...
0090  16 e2 e9 0b 32 93 7b 43 4a 5c 00 d0 35 5d 50 d7  ....2.{CJ\..5]P.
00a0  30 03 e9 b2 82 62 90 5b b8 21 cc f8 f2 cc bc 94  0....b.[.!......
00b0  fc f2 62 98 8b 18 38 98 15 60 2e 4a d0 46 b8 48  ..b...8..`.J.F.H
00c0  f2 b1 67 74 e2 32 2b a5 ac f8 b0 1f 11 57 e2 8f  ..gt.2+......W..
00d0  54 65 3a 76 c5 56 58 3c ba d8 b1 9b b7 49 ca 2f  Te:v.VX<.....I./
00e0  bd e0 fa 73 99 9e d3 bb 2e 2d ad fd 2e 50 be 24  ...s.....-...P.$
00f0  25 bf b1 e8 ca dc 57 37 65 dd 64 52 7e f1 94 64  %.....W7e.dR~..d
0100  ec e7 87 b9 88 0f e8 22 00 02 a3 61 50 00 12 98  .......".."...aP...
0110  f1 9c b7 28 e2 84 61 60 d3 fc 6a 95 05 ac d9 34  ...(..a`..j....4
0120  d7 17 ae 49 24 6e 43 0a 1e 11 c8 ed a8 25 42 1d  ...I$nC......%B.
0130  46 b1 2c 7d ac 25 6e 4f 80 48 42 b2 3d 55 34 67  F.,}.%nO.HB.=U4g
0140  2d b1 79 fa ef c4 57 d6 a2 46 d4 01 57 41 53 57  -.y...W..F..WASW
0150  53 69 67 32 42                                   Sig2B

No.     Time           Source                Destination           Protocol Length Info
    243 16.400640      192.168.1.142         128.119.245.12        HTTP     626    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
```

Стр 1, стлб 1 | 100% | 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?
   ARP, HTTP, MDNS, OpenVPN, SSDP, SSL, TCP, TLSv1.2
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 0.031028

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

Запит:

Вихідний: 192.168.1.142

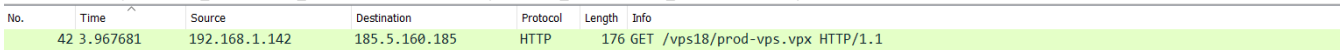
Цільовий: 185.5.160.185

Відповідь:

Вихідна: 185.5.160.185

Цільова: 192.168.1.142

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



No.	Time	Source	Destination	Protocol	Length	Info
42	3.967681	192.168.1.142	185.5.160.185	HTTP	176	GET /vps18/prod-vps.vpx HTTP/1.1

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

44	3.998709	185.5.160.185	192.168.1.142	HTTP	761	HTTP/1.1 200 OK

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.