



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»  
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
Кафедра Інформаційної Безпеки

## Практикум з Основ комп'ютерних мереж

### Транспортні протоколи – TCP і UDP

Перевірив:

\_\_\_\_\_

Виконав:

студент I курсу

групи ФБ-01

Сахній Н.Р.

Київ 2021

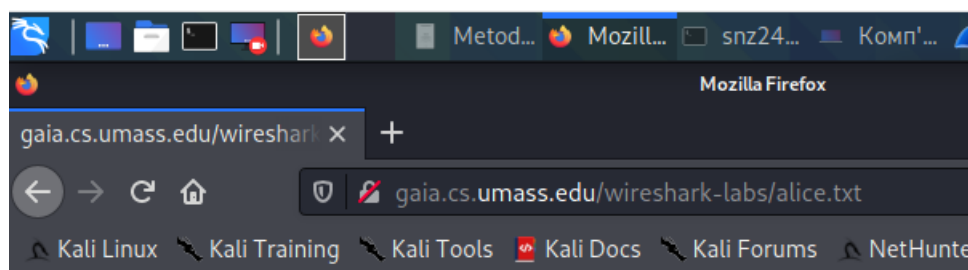
# Дослідження протоколу TCP

## 1. Перехоплення TCP пакетів, переданих від вашого комп'ютера на віддалений сервер

Перш ніж почати наше дослідження TCP, нам потрібно за допомогою Wireshark отримати TCP пакети, що пересилаються внаслідок передачі файлу з вашого комп'ютера на віддалений сервер. Це можна зробити, зайшовши на Web сторінку, що дозволить вам ввести ім'я локального файлу, а потім передати файл на Web сервер, використовуючи HTTP POST метод. В цьому випадку ми використовуємо POST метод, а не GET, через те, що нам потрібно передати велику кількість даних з локального комп'ютера на віддалений. Звичайно, ми будемо використовувати Wireshark під час передачі файлу для перехоплення TCP пакетів, що направлені до вашого хосту та від нього.

Зробіть наступне:

1. Запустіть web браузер. Зайдіть на <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> та завантажте файл «Alice in Wonderland» у ASCII кодуванні кудись на ваш комп'ютер.



ALICE'S ADVENTURES IN WONDERLAND

Lewis Carroll

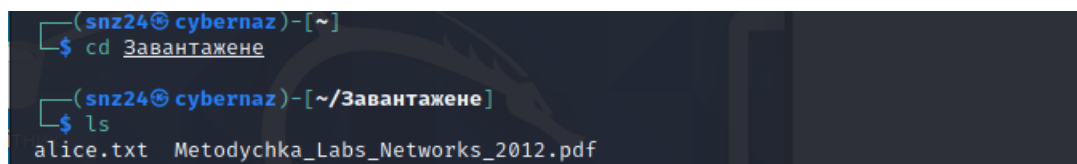
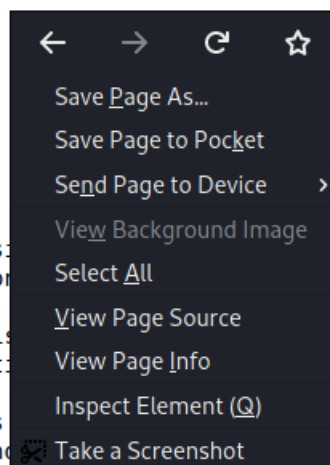
THE MILLENNIUM FULCRUM EDITION 3.0

CHAPTER I

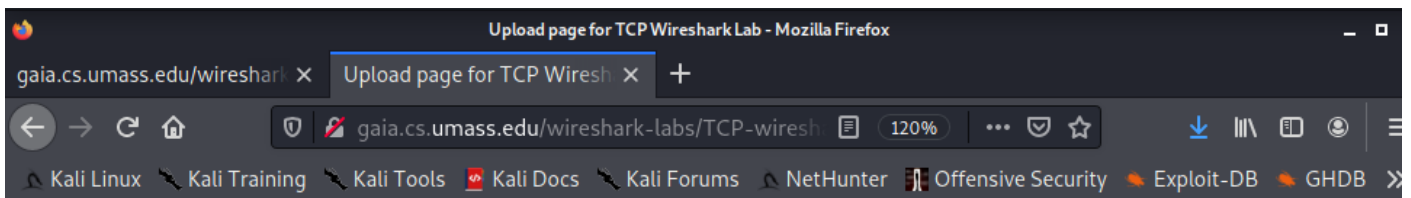
Down the Rabbit-Hole

Alice was beginning to get very tired of sitting on the bank, and of having nothing to do: so she took a peep into the book her sister was reading, and found pictures or conversations in it, 'and what is the thought Alice 'without pictures or conversations

So she was considering in her own mind (as well as the hot day made her feel very sleepy and stupid), whether the pleasure of making a daisy-chain would be worth the trouble of getting up and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.



2. Далі, зайдіть на <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.



## Upload page for TCP Wireshark Lab

Computer Networking: A Top Down Approach, 6th edition

Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of `alice.txt` that is stored on your computer.

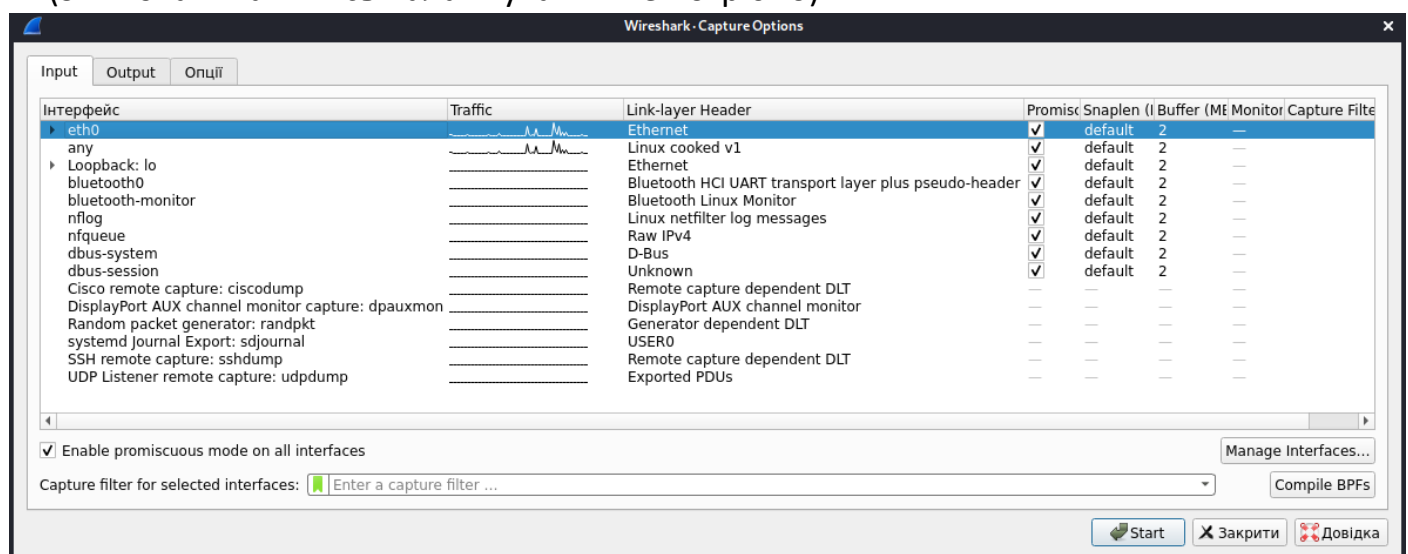
No file selected.

Once you have selected the file, click on the "Upload `alice.txt` file" button below. This will cause your browser to send a copy of `alice.txt` over an HTTP connection (using TCP) to the web server at `gaia.cs.umass.edu`. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of `alice.txt` from your computer to `gaia.cs.umass.edu`!!

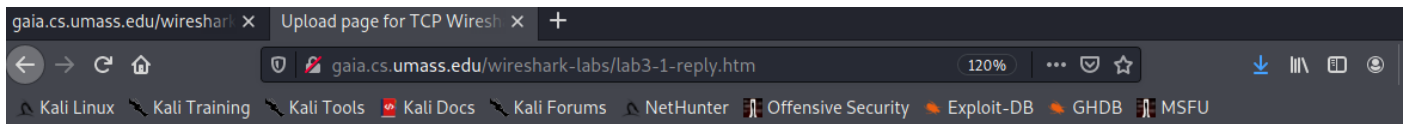
3. В полі вводу вкажіть повний шлях до щойно завантаженого локального файлу, але поки що не натискайте кнопку "Upload `alice.txt` file".

`alice.txt`

4. Тепер, запустіть Wireshark та розпочніть перехоплення пакетів (Capture->Options), та натисніть кнопку OK у вікні налаштувань Wireshark Packet Capture (змінювати там якісь налаштування не потрібно)



5. Поверніться до браузера та натисніть кнопку "Upload `alice.txt` file" для завантаження файлу на сервер `gaia.cs.umass.edu`. Тільки-но файл буде завантажено, невеличке привітальне повідомлення буде відображене у вашому браузері.



Congratulations!

You've now transferred a copy of alice.txt from your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

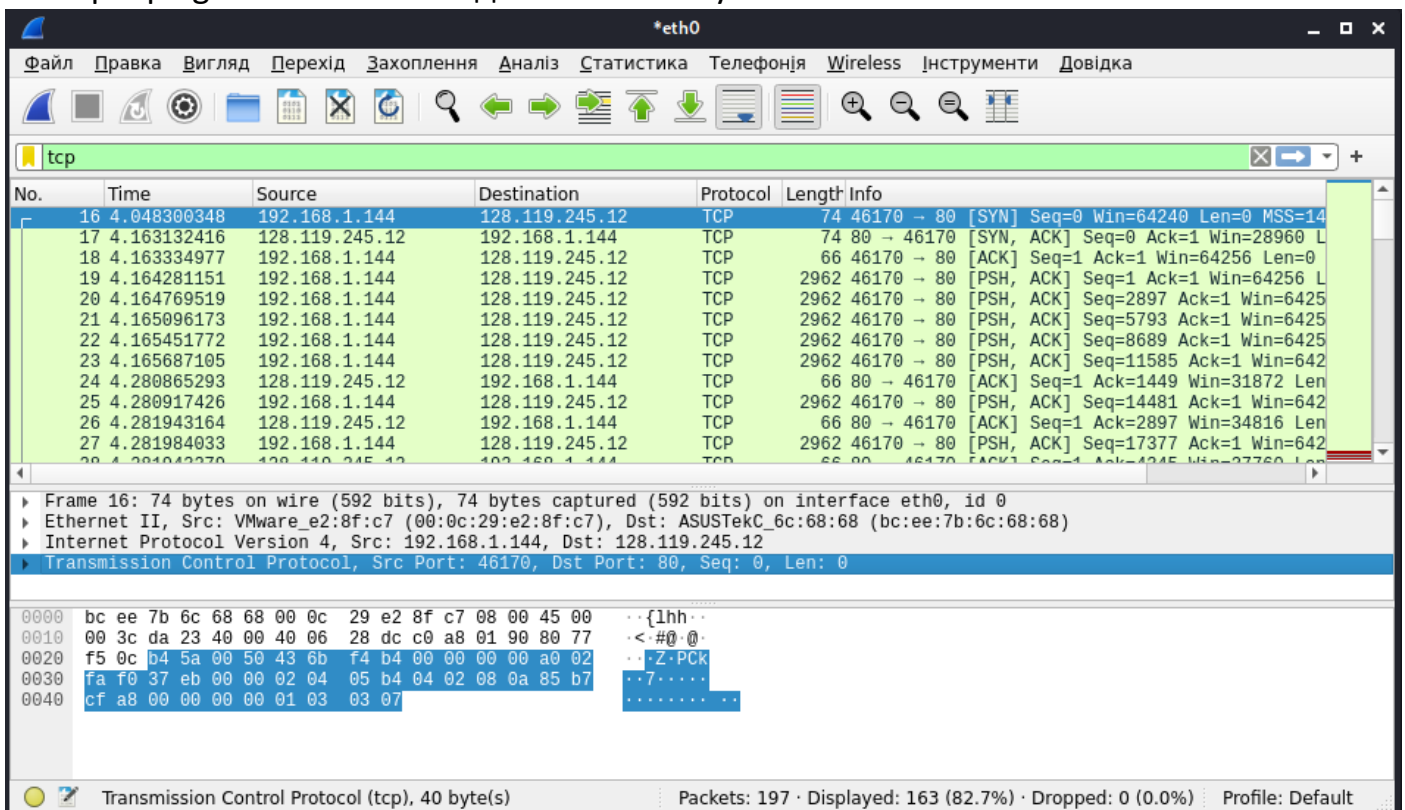
## 6. Зупиніть перехоплення пакетів.



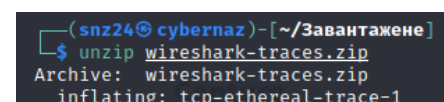
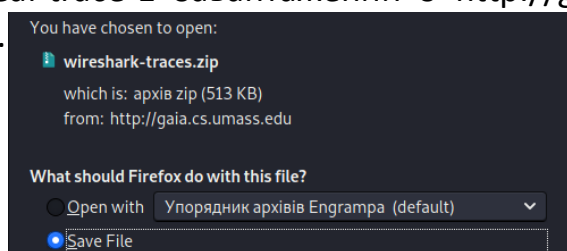
## 2. Перший погляд на перехоплені пакети

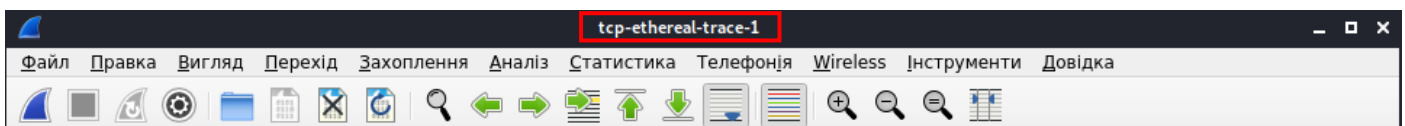
Перш ніж аналізувати поведінку TCP з'єднання в деталях, давайте глянемо на пакети загалом:

7. Спершу, відфільтруйте пакети, що відображаються у вікні Wireshark, набравши "tcp" у полі фільтру, що знаходиться на верхній панелі. Ви маєте побачити серії TCP та HTTP повідомлень, переданих між вашим комп'ютером та gaia.cs.umass.edu. Ви маєте побачити початкову процедуру рукоштовування – пакети, які містять SYN повідомлення. Далі - повідомлення HTTP POST та серію "HTTP Continuation" повідомлень, що відправлені від вашого комп'ютера до сервера. Нагадаємо, що насправді немає такого повідомлення, як HTTP Continuation. В такий спосіб Wireshark демонструє, що для передачі HTTP повідомлення використовувалося декілька TCP пакетів. Також, ви маєте побачити TCP ACK пакети, направлені від сервера gaia.cs.umass.edu до вашого хосту.

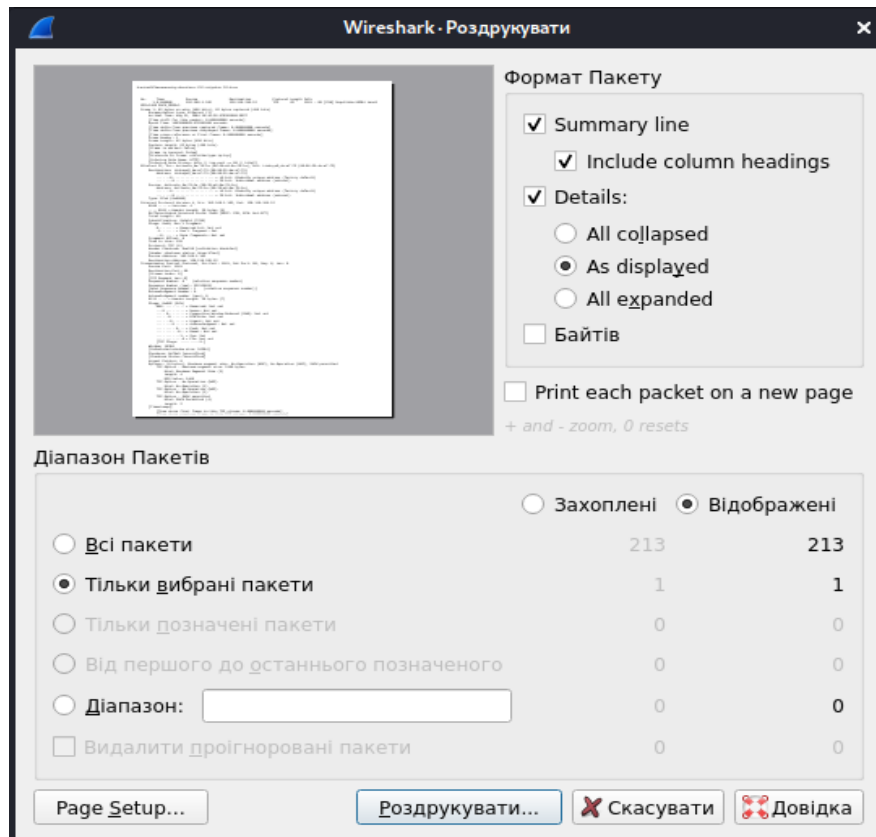


Перш ніж відповідати на питання, відкрийте у Wireshark файл перехоплених повідомлень tcp-ethereal-trace-1 завантажений з <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>.





Коли відповідаєте на наведені питання, бажано мати роздруківку перехоплених пакетів. Для друку пакетів натисніть File->Print в головному меню, виберіть пункти Selected packet only та Packet summary line, а також виберіть ту мінімальну кількість інформації для друку, що потрібна для відповідей на питання.



/home/snz24/Завантажене/tcp-ethereal-trace-1 213 total packets, 213 shown

```
No.      Time      Source      Destination  Protocol Length Info
1 0.000000 192.168.1.102 128.119.245.12 TCP 62 1161 -> 80 [SYN] Seq=0 Win=16384 Len=0
MSS=1460 SACK_PERM=1
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0
Encapsulation type: Ethernet (1)
Arrival Time: Aug 21, 2004 16:44:20.570381000 EEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1093095860.570381000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 62 bytes (496 bits)
Capture Length: 62 bytes (496 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)
... ..0. .... = LG bit: Globally unique address (factory default)
... ..0. .... = IG bit: Individual address (unicast)
Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
Address: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
... ..0. .... = LG bit: Globally unique address (factory default)
... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x1e1d (7709)
Flags: 0x40, Don't fragment
0... .... = Reserved bit: Not set
.1. .... = Don't fragment: Set
..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xa518 [validation failed]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.119.245.12
```

1. IP-адреса хоста: 198.168.1.102;  
TCP-порт, що використовується моїм комп'ютером: 1161.
2. IP-адреса gaia.cs.umass.edu: 128.119.245.12;  
Номер порта для прийому/відправлення TCP пакетів: 80.
3. TCP SYN пакет має порядковий номер 0;  
Флаг (SYN: Set) вказує на те, що даний TCP пакет є SYN пакетом



```

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...0 = Acknowledgment: Not set
.... ....0... = Push: Not set
.... .....0.. = Reset: Not set
.... .... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....S.]
Window: 16384
[Calculated window size: 16384]
Checksum: 0xf6e9 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
  TCP Option - Maximum segment size: 1460 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 1460
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - SACK permitted
    Kind: SACK Permitted (4)
    Length: 2
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

```

1. Яка IP адреса та номер TCP порту використовується вашим комп'ютером (джерелом) для відправки файлу на *gaia.cs.umass.edu*? Для відповіді на питання, мабуть, найлегше вибрати це HTTP повідомлення та дослідити детально TCP пакет, використовуючи вікно детального перегляду обраного пакету.
2. Яка IP адреса у *gaia.cs.umass.edu*? Який номер порту використовується для прийому/відправлення TCP пакетів?
3. Який порядковий номер (*sequence number*) TCP SYN пакета, який використовується для ініціювання TCP з'єднання між комп'ютером клієнта і *gaia.cs.umass.edu*? Що в цьому TCP пакеті вказує, що він є SYN пакетом?

### Відповіді на 1-3 питання виділені зверху на скріншоті↑

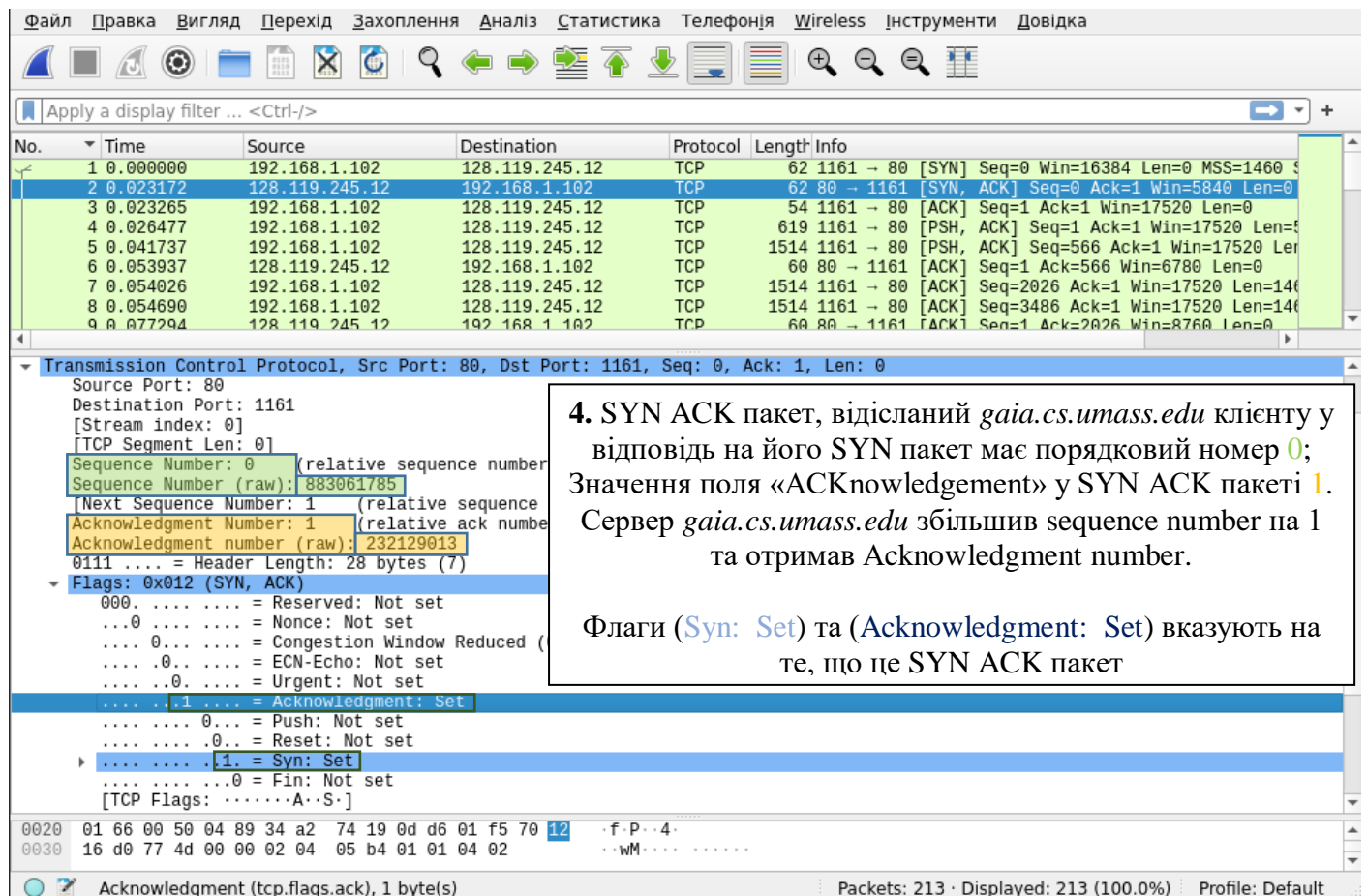
Оскільки цей Комп'ютерний практикум присвячена TCP, а не HTTP, давайте змінимо список відображених пакетів у Wireshark так, щоб він показував TCP сегменти, що використовуються для передачі HTTP повідомлень. Щоб зробити це, виберіть пункт меню **Analyze → Enabled Protocols**. Там у вікні зніміть галочку з HTTP та натисніть OK.

Це саме те, що нам потрібно – серія TCP пакетів пересланих між вашим комп'ютером та *gaia.cs.umass.edu* сервером. Ми будемо використовувати отриманий вами список перехоплених пакетів (або ж завантажений вами файл) для подальшого вивчення поведінки TCP пакетів.

### 3. Основи TCP

Дайте відповіді на наступні питання:

4. Який порядковий номер SYN ACK пакета, відісланого *gaia.cs.umass.edu* клієнту у відповідь на його SYN пакет? Яке значення поля «ACKnowledgment» у SYN ACK пакеті? Звідки сервер *gaia.cs.umass.edu* взяв це значення? Що в TCP пакеті вказує, що він є SYN ACK пакетом?



4. SYN ACK пакет, відісланий *gaia.cs.umass.edu* клієнту у відповідь на його SYN пакет має порядковий номер 0; Значення поля «ACKnowledgment» у SYN ACK пакеті 1. Сервер *gaia.cs.umass.edu* збільшив sequence number на 1 та отримав Acknowledgment number.

Флаги (Syn: Set) та (Acknowledgment: Set) вказують на те, що це SYN ACK пакет

5. Який порядковий номер TCP сегмента, що містить HTTP POST команду?

Для знаходження команди POST вам потрібно детальніше глянути на вміст пакету у вікні детального перегляду та знайти у полі даних фрагмент з командою "POST".

6. Розгляньте перший TCP пакет, що містить команду HTTP POST. Які порядкові номери перших шести TCP пакетів, що використовувалися для передачі файлу (починаючи з пакету, що містить HTTP POST команду)? Який час відправлення кожного такого пакету? Коли приходив пакет-підтвердження (ACK) для кожного відправленого пакету? Підрахувавши різницю між часом відправки TCP сегмента та часом отримання пакету підтвердження про доставку, вкажіть RTT час (Round-Trip Time – час обороту повідомлення) для кожного з шести сегментів.

7. Яка довжина кожного з шести TCP сегментів?

8. Який мінімальний розмір буферу був у сервера під час передавання файлу? Чи призупинялася передача даних через недостачу буферу на сервері?

## Відповіді на 5-8 питання виділені знизу на скріншоті↓

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassembled PDU]
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]
11	0.078157	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassembled PDU]

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits)

Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73)

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, **Len: 565**

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 565]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 232129013

[Next Sequence Number: 566 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 883061786

0001 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

000. .... = Reserved: Not set

...0 .... = Nonce: Not set

...0 .... = Congestion Window Reduced

...0 .... = ECN-Echo: Not set

...0 .... = Urgent: Not set

...1 .... = Acknowledgment: Set

...1 .... = Push: Set

...0 .... = Reset: Not set

...0 .... = Syn: Not set

...0 .... = Fin: Not set

[TCP Flags: .....AP...]

**Window: 17520**

[Calculated window size: 17520]

[Window size scaling factor: -2 (no window sca

Checksum: 0x1fbd [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[SEQ/ACK analysis]

[RTT: 0.023265000 seconds]

[Bytes in flight: 565]

[Bytes sent since last PSH flag: 565]

[Timestamps]

[Time since first frame in this TCP stream: 0.026477000 seconds]

[Time since previous frame in this TCP stream: 0.003212000 seconds]

TCP payload (565 bytes)

**Reassembled PDU in frame: 199**

TCP segment data (565 bytes)

0030 44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65 **DP...** **P0 S1** /

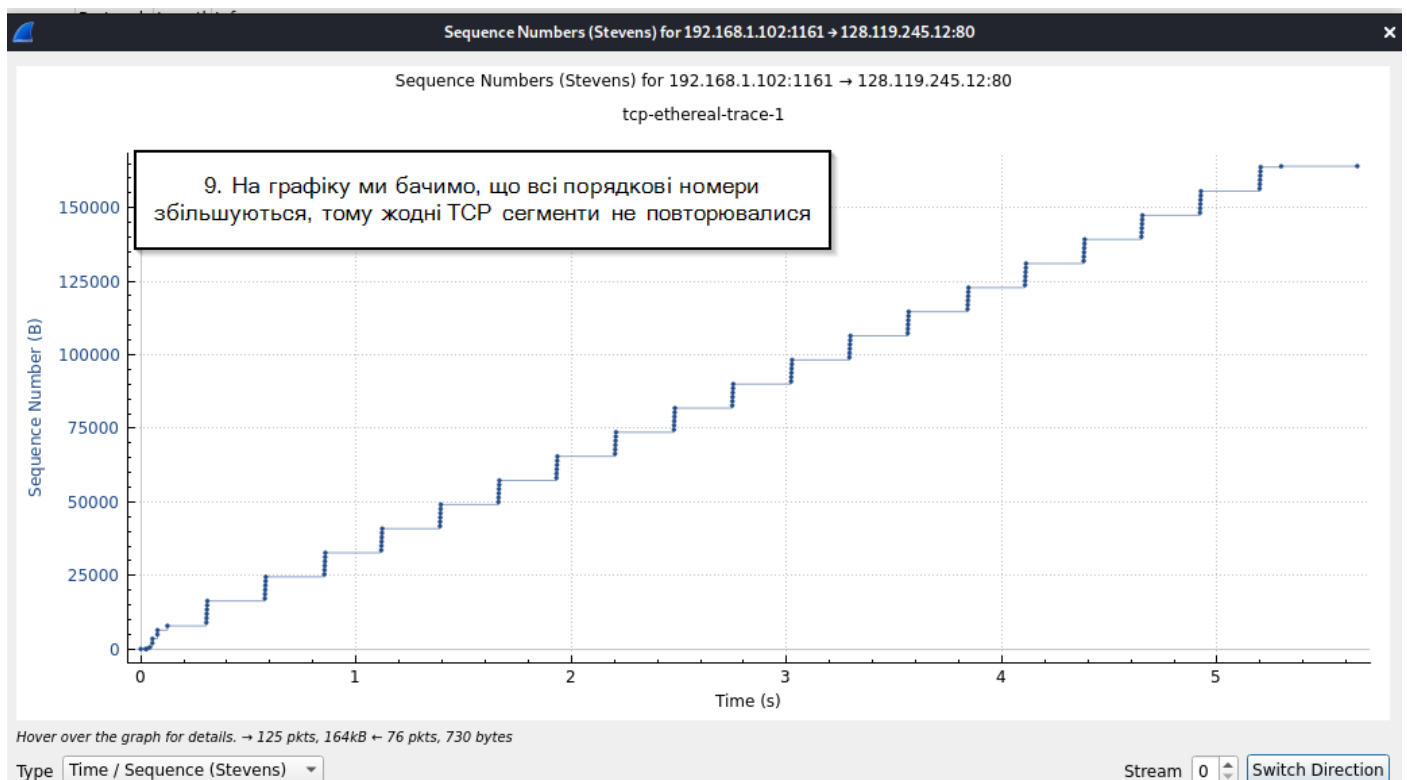
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 real-lab s/

0050 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f -reply.h tm

The window size value from the TCP header (tcp.window\_size\_value), 2 byte(s)

- Порядковий номер TCP сегмента, що містить HTTP POST команду – 1
- Для перших шести TCP пакетів, що використовувалися для передачі файлу
  - Seq = 1, час відправки 0.026477, АСК прийшов у 0.053937, Round-Trip Time 0.02746;
  - Seq = 566 (довжина + Seq попереднього), час відправки 0.041737, АСК прийшов у 0.077294, Round-Trip Time 0.035557;
  - Seq = 2026, час відправки 0.054026, АСК прийшов у 0.124085, Round-Trip Time 0.070059;
  - Seq = 3486, час відправки 0.054690, АСК прийшов у 0.169118, Round-Trip Time 0.114428;
  - Seq = 4946, час відправки 0.077405, АСК прийшов у 0.217299, Round-Trip Time 0.139894;
  - Seq = 3486, час відправки 0.078157, АСК прийшов у 0.267802, Round-Trip Time 0.189645;
- Довжина кожного пакету 1460 байт, крім першого (565 байт)
- Мінімальний розмір буферу у сервера під час передавання файлу був 17520. Передача даних не призупинялася через нестачу буферу на сервері

9. Чи були повторені якісь TCP сегменти? Що ви перевіряли (в перехоплених пакетах) для відповіді на це запитання?





10. Яка пропускна спроможність (кількість передавання байтів за одиницю часу) для TCP з'єднання? Поясніть, як ви підраховували цю величину.

No.	Time	Source	Destination	Pr	No.	Time	Source	Destination	Protoc
1	0.000000	192.168.1.102	128.119.245.12	TC	201	5.447887	128.119.245.12	192.168.1.102	TCP
2	0.023172	128.119.245.12	192.168.1.102	TC	202	5.455830	128.119.245.12	192.168.1.102	TCP
3	0.023265	192.168.1.102	128.119.245.12	TC	203	5.461175	128.119.245.12	192.168.1.102	HTTP
4	0.026477	192.168.1.102	128.119.245.12	TC	204	5.598090	192.168.1.100	192.168.1.1	SSDP
5	0.041737	192.168.1.102	128.119.245.12	TC	205	5.599082	192.168.1.100	192.168.1.1	SSDP

Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952) on interface 0  
Ethernet II, Src: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Dst: Linksys6\_da:af:73 (00:06:25:da:af:73), Length: 619  
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 232129013, Len: 565  
Source Port: 1161  
Destination Port: 80  
[Stream index: 0]  
[TCP Segment Len: 565]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 232129013  
[Next Sequence Number: 566 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment Number (raw): 883061786  
0101 .... = Header  
0000 .... = Data  
...0 ....  
...0 ....  
...0 ....  
...0 ....  
...0 ....  
...1 .... = Acknowledgment: Set  
...1... = Push: Set  
...0.. = Reset: Not set  
...0. = Syn: Not set  
...0 = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 17520  
[Calculated window size: 17520]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0x1fbd [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[SEQ/ACK analysis]  
[iRTT: 0.023265000 seconds]  
[Bytes in flight: 565]  
[Bytes sent since last PSH flag: 565]  
[Timestamps]  
[Time since first frame in this TCP stream: 0.026477000 seconds]  
[Time since previous frame in this TCP stream: 0.003212000 seconds]

10. Пропускна спроможність (кількість передавання байтів за одиницю часу) для TCP з'єднання дорівнює відношенню різниці між останнім АСК номером та першим порядковим номером (164091-1=164090) до різниці часу між АСК пакетом та першим TCP пакетом повідомлення (5.461175-0.026477=5.434698). Отже  $\frac{164090}{5.434698} = 30193$  Байт/с = 30.2 кБайт/с

Frame 203: 784 bytes on wire (6272 bits), 784 bytes captured (6272) on interface 0  
Ethernet II, Src: Linksys6\_da:af:73 (00:06:25:da:af:73), Dst: Actionte\_8a:70:1a (00:20:e0:8a:70:1a), Length: 784  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102  
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 883061786, Len: 730  
Source Port: 80  
Destination Port: 1161  
[Stream index: 0]  
[TCP Segment Len: 730]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 883061786  
[Next Sequence Number: 731 (relative sequence number)]  
Acknowledgment Number: 164091 (relative ack number)  
Acknowledgment Number (raw): 164091  
0101 .... = Header  
0000 .... = Data  
...0 ....  
...0 ....  
...0 ....  
...0 ....  
...1 .... = Acknowledgment: Set  
...1... = Push: Set  
...0.. = Reset: Not set  
...0. = Syn: Not set  
...0 = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 62780  
[Calculated window size: 62780]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0xa920 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[SEQ/ACK analysis]  
[iRTT: 0.023265000 seconds]  
[Bytes in flight: 730]  
[Bytes sent since last PSH flag: 730]  
[Timestamps]  
[Time since first frame in this TCP stream: 5.461175000 seconds]  
[Time since previous frame in this TCP stream: 0.005345000 seconds]

Not set

4. Керування перенавантаженням TCP

11. Використайте утиліту Time-Sequence- Graph(Stevens) для малювання графіку передачі TCP пакетів. Ви можете вказати, де починаються фази передавання TCP пакетів та де вони закінчуються і де працює механізм уникнення TCP заторів?

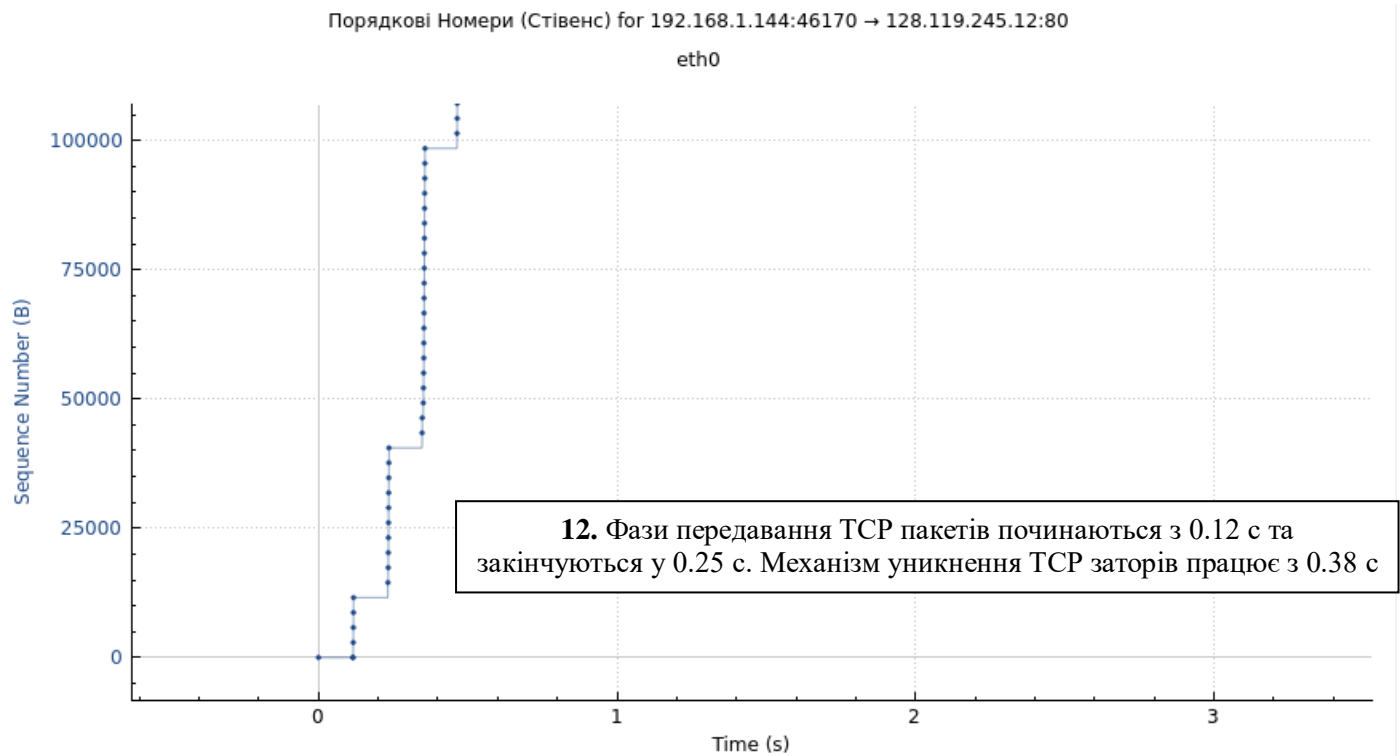
Порядкові Номери (Стівенс) for 192.168.1.102:1161 → 128.119.245.12:80

tcp-ethereal-trace-1

11. Фази передавання TCP пакетів починаються з 0 с та закінчуються у 0.04 с. Механізм уникнення TCP заторів працює з 0.14 с

Тут кожна точка представляє відправлений TCP сегмент, відображаючи порядковий номер пакету та час його відправлення. Зауважимо, що сукупність точок, розташованих одна над одною, вказує на пакети, які клієнт відправляв неперервно.

12. Дайте відповідь на попереднє питання, використовуючи результат вашого експерименту з передаванням файлу на сервер *gaia.cs.umass.edu*.



## Дослідження протоколу UDP

### Завдання

Розпочніть перехоплення пакетів за допомогою Wireshark, а потім зробіть що-небудь для того, щоб ваш хост почав приймати та передавати UDP пакети (один з можливих варіантів – це скористатися командою `nslookup`, яка розглядалася в лабораторній роботі по DNS). Після зупинки перехоплення пакетів налаштуйте фільтр відображення пакетів так, щоб Wireshark відображав лише UDP пакети. Виберіть один з UDP пакетів, та розгорніть його дані у вікні детального перегляду.

```
(snz24@cybernaz)-[~]  
$ nslookup gaia.cs.umass.edu  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
Name:   gaia.cs.umass.edu  
Address: 128.119.245.12
```

1. Виберіть один пакет. Визначте, скільки полів міститься в заголовку обраного UDP пакета. Перерахуйте ці поля.
2. Визначте довжину кожного поля в UDP заголовку.

3. Значення в полі Length (розмір) - це розмір чого? Покажіть це на прикладі перехопленого вами UDP пакету.
4. Яку максимальну кількість байтів може переносити UDP пакет?
5. Який максимальний номер порту джерела повідомлення?
6. Який номер протоколу відповідає UDP? Дайте відповідь у десятковому та шістнадцятиричному представленнях (для відповіді вам знадобиться заглянути в заголовки IP протоколу).

### Відповіді на 1-6 питання виділені знизу на скріншоті↓

/tmp/wireshark\_eth0BBXR40.pcapng 70 total packets, 48 shown

```

No.      Time      Source                Destination            Protocol Length Info
 38 35.600130427 192.168.1.144         192.168.1.1            DNS      77      Standard query 0x1a98 AAAA gaia.cs.umass.edu
Frame 38: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
Ethernet II, Src: VMware_e2:8f:c7 (00:0c:29:e2:8f:c7), Dst: ASUSTekC_6c:68:68 (bc:ee:7b:6c:68:68)
Internet Protocol Version 4, Src: 192.168.1.144, Dst: 192.168.1.1
 0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: No Diff. Serv. Type)
Total Length: 63
Identification: 0xfa0b (64011)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xfcc0 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.144
Destination Address: 192.168.1.1
User Datagram Protocol, Src Port: 40990, Dst Port: 53
Source Port: 40990
Destination Port: 53
Length: 43
Checksum: 0x841e [unverified]
[Checksum Status: Unverified]
[Stream index: 9]
[Timestamps]
UDP payload (35 bytes)
Domain Name System (query)
0000  bc ee 7b 6c 68 68 00 0c 29 e2 8f c7 08 00 45 00  ..{lhh..)....E.
0010  00 3f fa 0b 00 00 40 11 fc c0 c0 a8 01 90 c0 a8  .?....@.....
0020  01 01 a0 1e 00 35 00 2b 84 1e 1a 98 01 00 00 01  .....5.+.....
0030  00 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75  ....gaia.cs.u
0040  6d 61 73 73 03 65 64 75 00 00 1c 00 01          mass.edu....

```

1. У заголовку UDP пакета міститься 4 поля: Source Port, Destination Port, Length, Checksum;
2. Кожне поле заголовку UDP має довжину 2 байти;
3. Значення в полі Length (розмір) є сумою довжин 4 полів (ті, що по 2 байти) і 35 байт даних. У сумі маємо 43 байти;
4. Теоретично UDP пакет може максимально переносити 65 535 байт (8-байтний заголовок та 65 527 байт даних);
5. Максимальний номер порту джерела повідомлення 65 535;
6. Десятковим значенням значенням протоколу UDP є

7. Пошукайте “UDP” в пошуковій системі Google, та скажіть по яким полям UDP рахує контрольну суму (checksum).

Контрольна сума (Checksum) розраховується на основі усього TCP-сегменту включно із заголовком та важливих полів IP-пакета: IP-адрес хостів відправника та отримувача, номера протоколу (TCP має номер 6) та загального розміру IP-пакету. Контрольна сума забезпечує можливість перевірки цілісності надісланих даних.

8. Дослідіть пару UDP пакетів, з яких перший пакет був відправлений вашим комп'ютером, а другий – відповідь на нього. Опишіть взаємозв'язок між номерами портів в цих двох пакетах.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.144	192.168.1.1	DNS	77	Standard query 0x0e39 A gaia.cs.umass.edu
2	0.003553465	192.168.1.1	192.168.1.144	DNS	93	Standard query response 0x0e39 A gaia.cs.umass.edu A 128.119.245.12
3	0.003953880	192.168.1.144	192.168.1.1	DNS	77	Standard query 0xf140 AAAA gaia.cs.umass.edu
4	0.009441372	192.168.1.1	192.168.1.144	DNS	130	Standard query response 0xf140 AAAA gaia.cs.umass.edu SOA unix1.cs.u...
36	35.595883006	192.168.1.144	192.168.1.1	DNS	77	Standard query 0x1d13 A gaia.cs.umass.edu
37	35.599652315	192.168.1.1	192.168.1.144	DNS	93	Standard query response 0x1d13 A gaia.cs.umass.edu A 128.119.245.12

User Datagram Protocol, Src Port: 58796, Dst Port: 53  
 Source Port: 58796  
 Destination Port: 53  
 Length: 43  
 Checksum: 0x841e [unverified]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.144	192.168.1.1	DNS	77	Standard query 0x0e39 A gaia.cs.umass.edu
2	0.003553465	192.168.1.1	192.168.1.144	DNS	93	Standard query response 0x0e39 A gaia.cs.umass.edu A 128.119.245.12
3	0.003953880	192.168.1.144	192.168.1.1	DNS	77	Standard query 0xf140 AAAA gaia.cs.umass.edu
4	0.009441372	192.168.1.1	192.168.1.144	DNS	130	Standard query response 0xf140 AAAA gaia.cs.umass.edu SOA unix1.cs.u...
36	35.595883006	192.168.1.144	192.168.1.1	DNS	77	Standard query 0x1d13 A gaia.cs.umass.edu
37	35.599652315	192.168.1.1	192.168.1.144	DNS	93	Standard query response 0x1d13 A gaia.cs.umass.edu A 128.119.245.12

User Datagram Protocol, Src Port: 53, Dst Port: 58796  
 Source Port: 53  
 Destination Port: 58796  
 Length: 96  
 Checksum: 0x1a43 [unverified]

У випадку, коли UDP пакет був відправлений моїм комп'ютером, номер порта відправника 58796, номер порта отримувача 53, а у випадку, коли прийшла відповідь, то навпаки.