**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”**

**Інститут прикладного системного аналізу  
Кафедра системного проектування**

**ЗВІТ**

з виконання лабораторної роботи №1  
з дисципліни “Комп’ютерні мережі”

На тему “Організація обміну даних у моделі клієнт-сервер за допомогою протоколів UDP і TCP”

Виконав:

Студент групи ДА-82

Муравльов А.Д.

Варіант №18 (51)

Київ — 2021

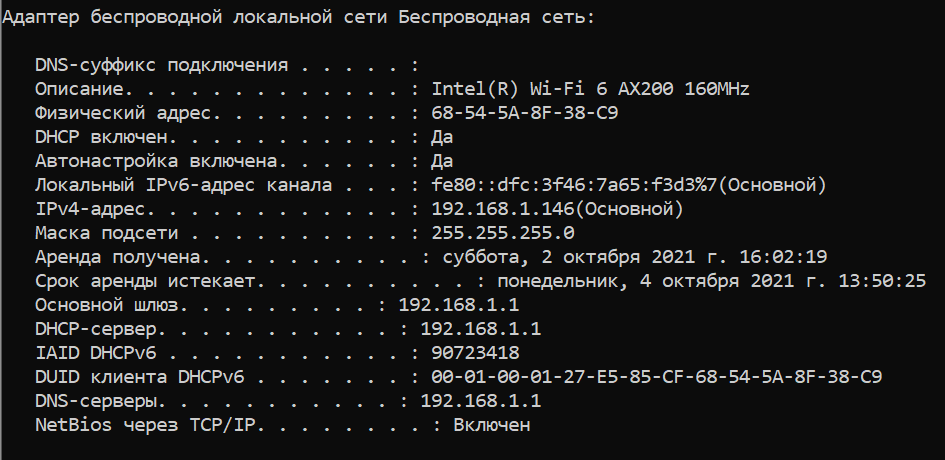
# **Мета роботи**

- Ознайомлення із засобами перехоплення, збереження і аналізу мережевого трафіку за допомогою відомих аналізаторів мережевого трафіку, як WireShark

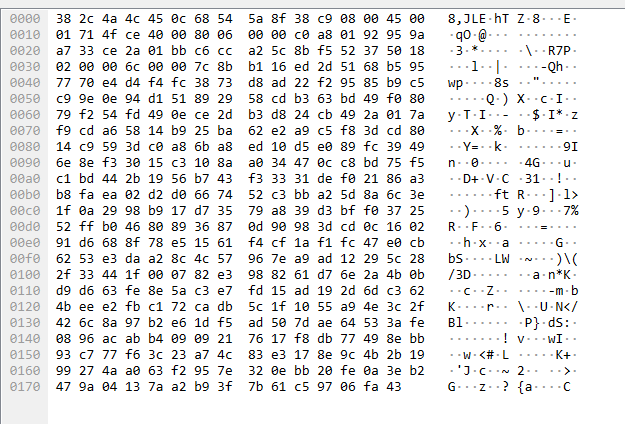
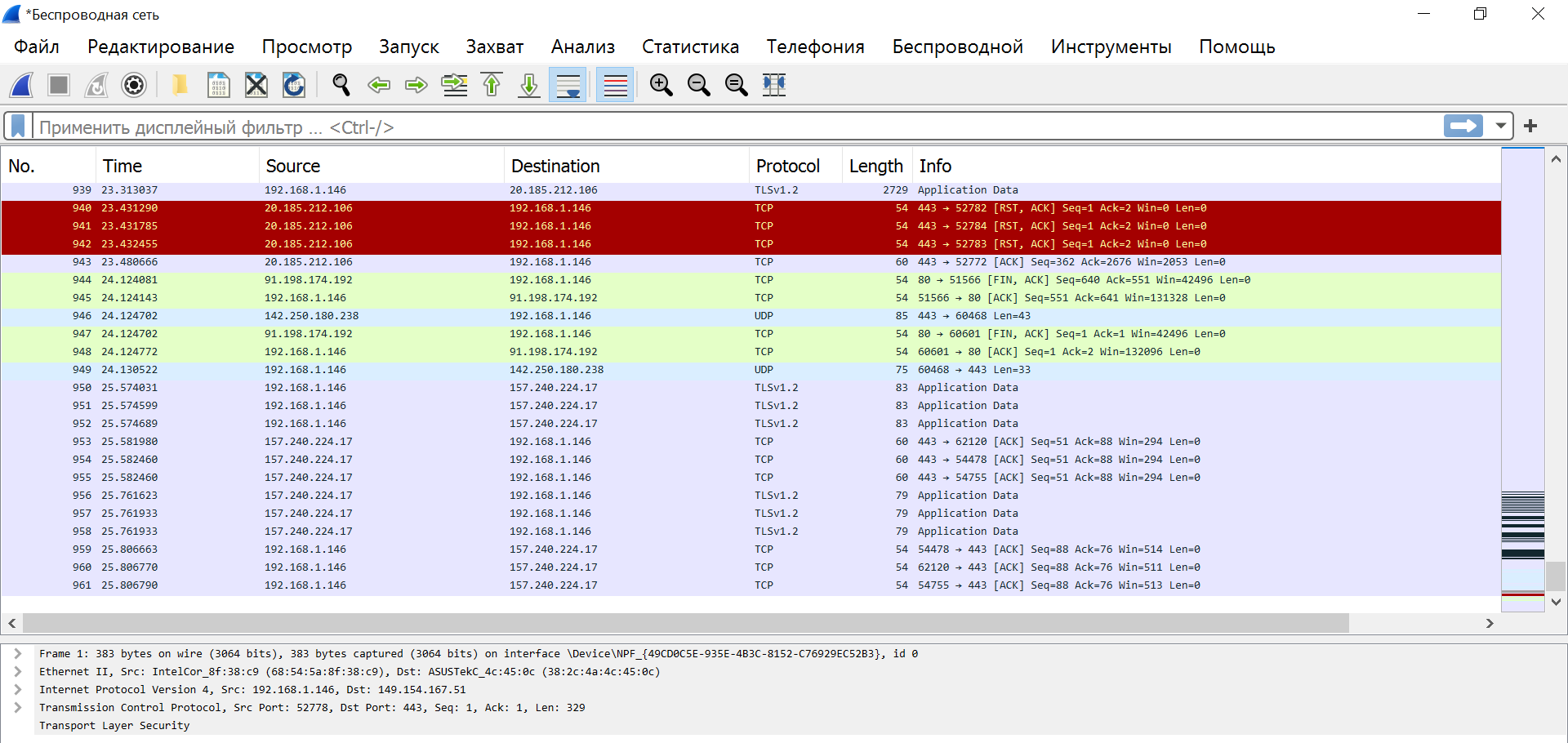
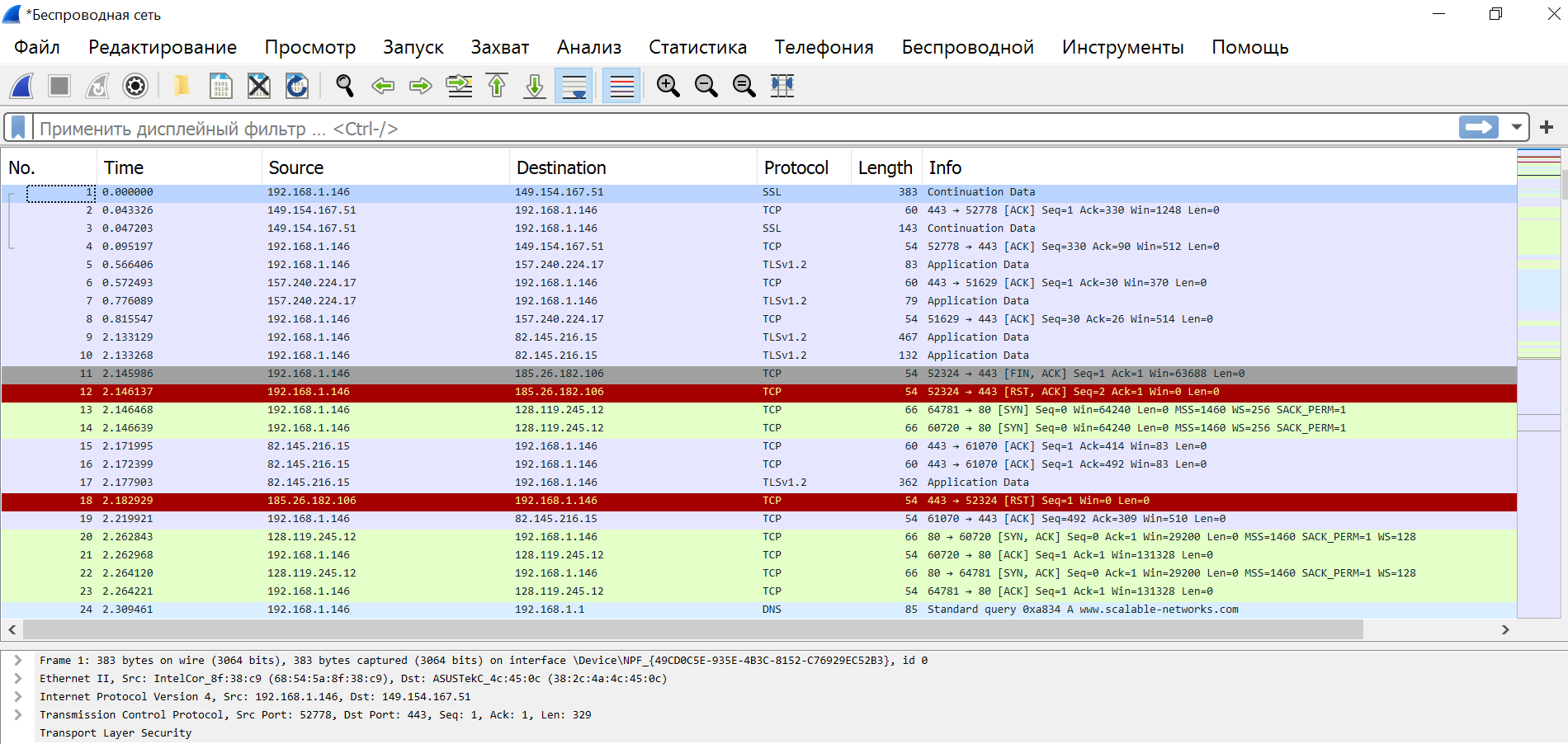
- Проведення аналізу мережевого сеансу транспортного протоколу TCP

# **Хід роботи**

1. Завантажте та установки Wireshark, якщо він ще не встановлений.
2. Запустіть браузер, і в ньому відкриється домашня сторінка.
3. Запустіть програму Wireshark.  
   Щоб точно дiзнатися IP-адресу i MAC-адресу бажаного iнтерфейсу (мережевого адаптера) на ПК, вiдкрийте вiкно командного рядка i введiть ipconfig/all. Запишiть IPадресу i MACадресу iнтерфейсу свого комп’ютера:

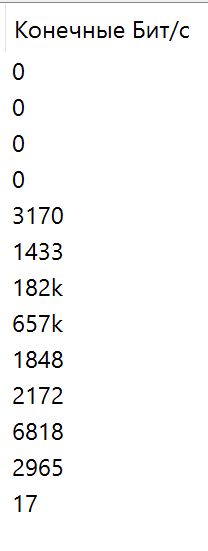
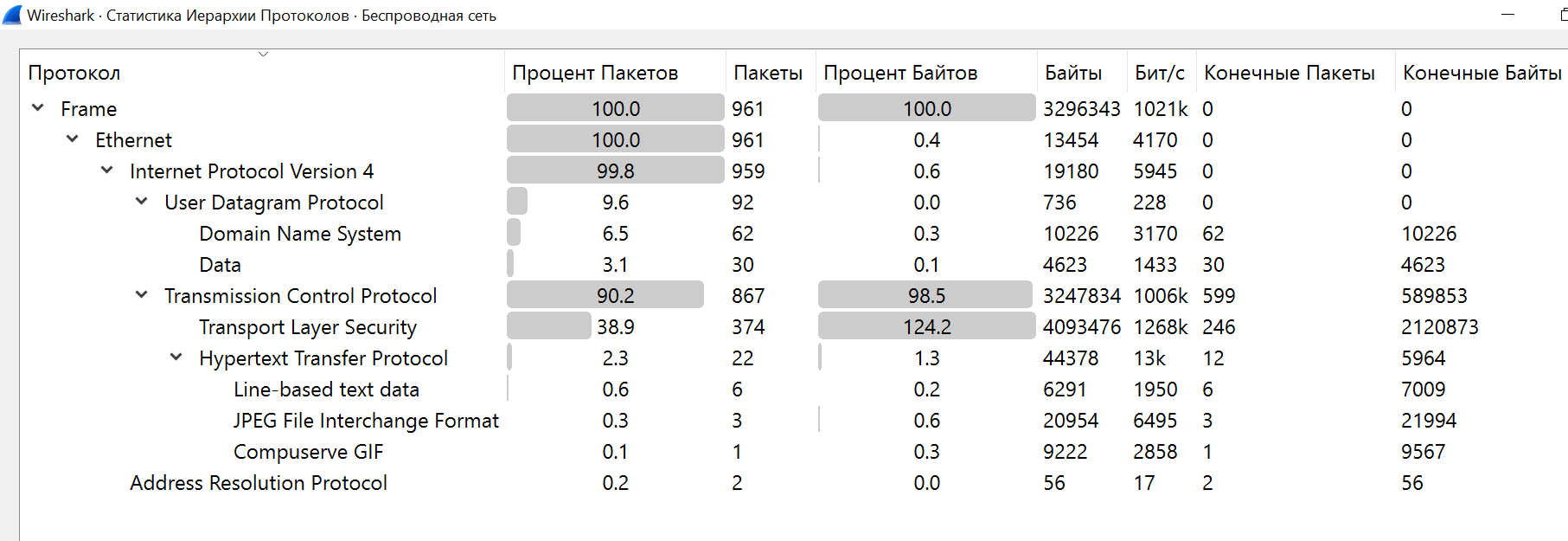


1. Почніть захоплення пакетів, вибравши в меню Capture команду Start.
2. Завантажте контент з веб-сайту браузером, адреса (http://gaia.cs.umass.edu/ або іншого віддаленого сайту з вітальною сторінкою без безлічі картинок).
3. Після того, як браузер відобразить сторінку, згорніть вікно сайту і поверніться в програму Wireshark.
4. Зупиніть захоплення пакетів, вибравши в меню Capture команду Stop.

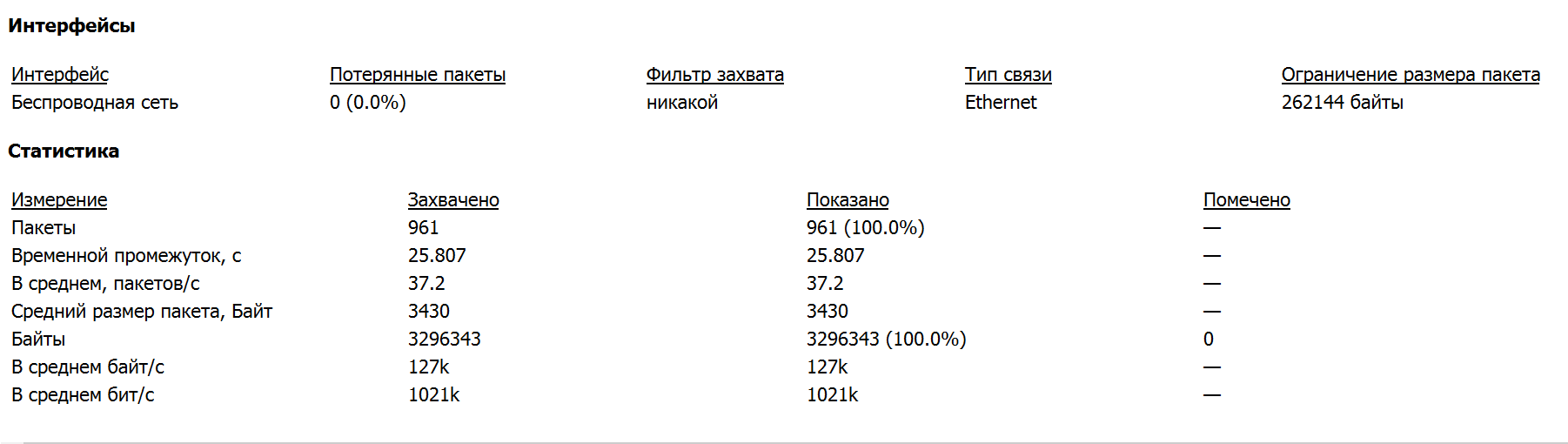


1. Використовуючи меню Statistics (Capture file properties, Protocol Hierarchy, Packet leanghs) визначте статистичні дані по захопленим пакетам:

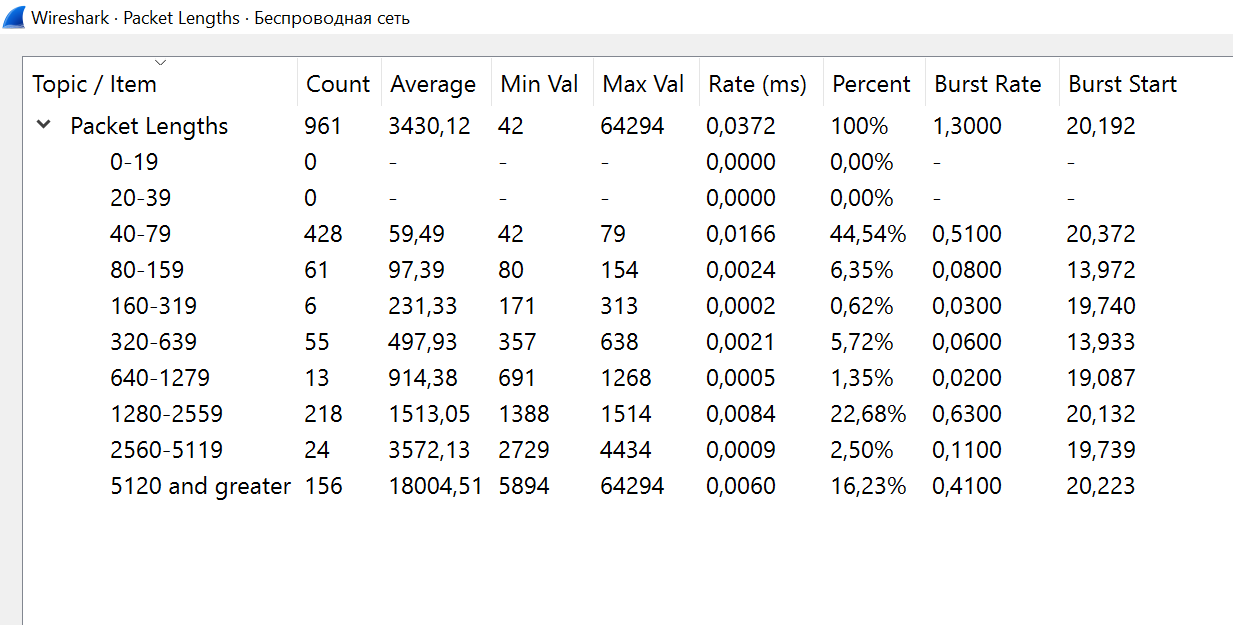
* процентне співвідношення трафіку різних протоколів в мережі;



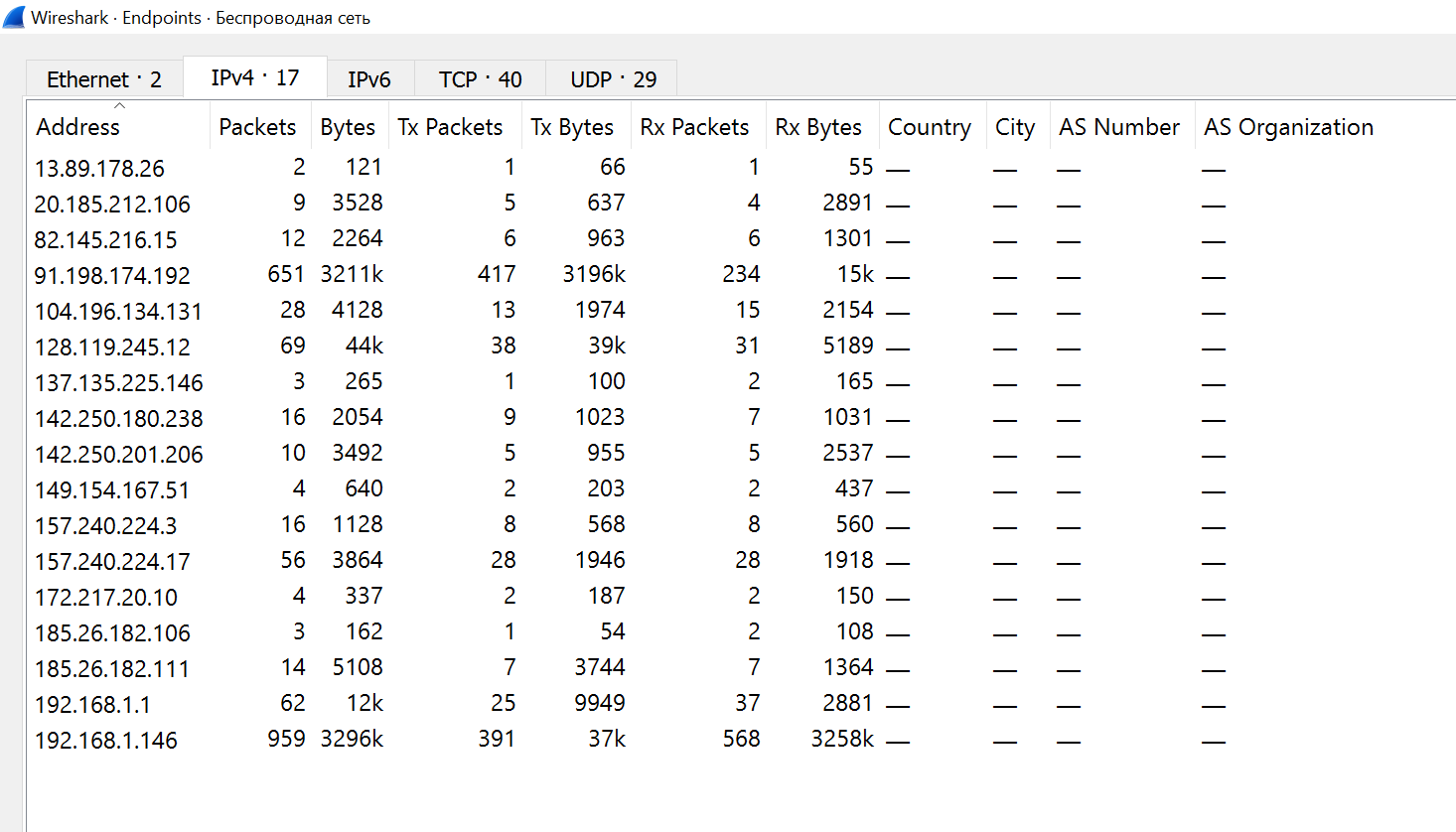
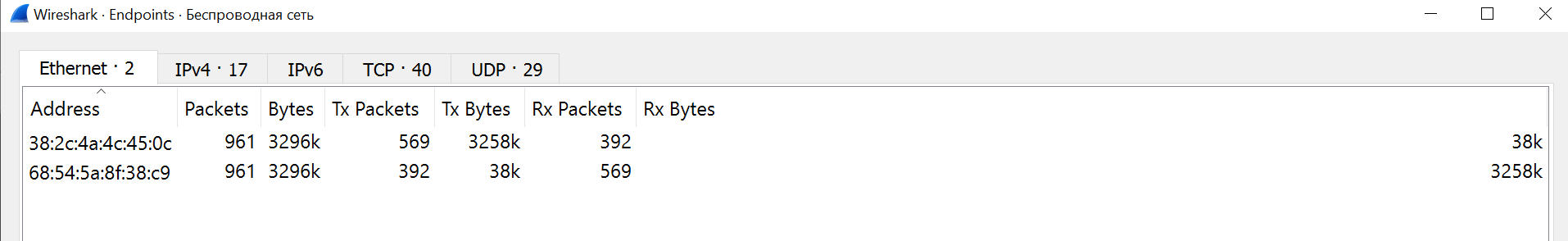
* середню швидкість біт/сек та байт/сек;



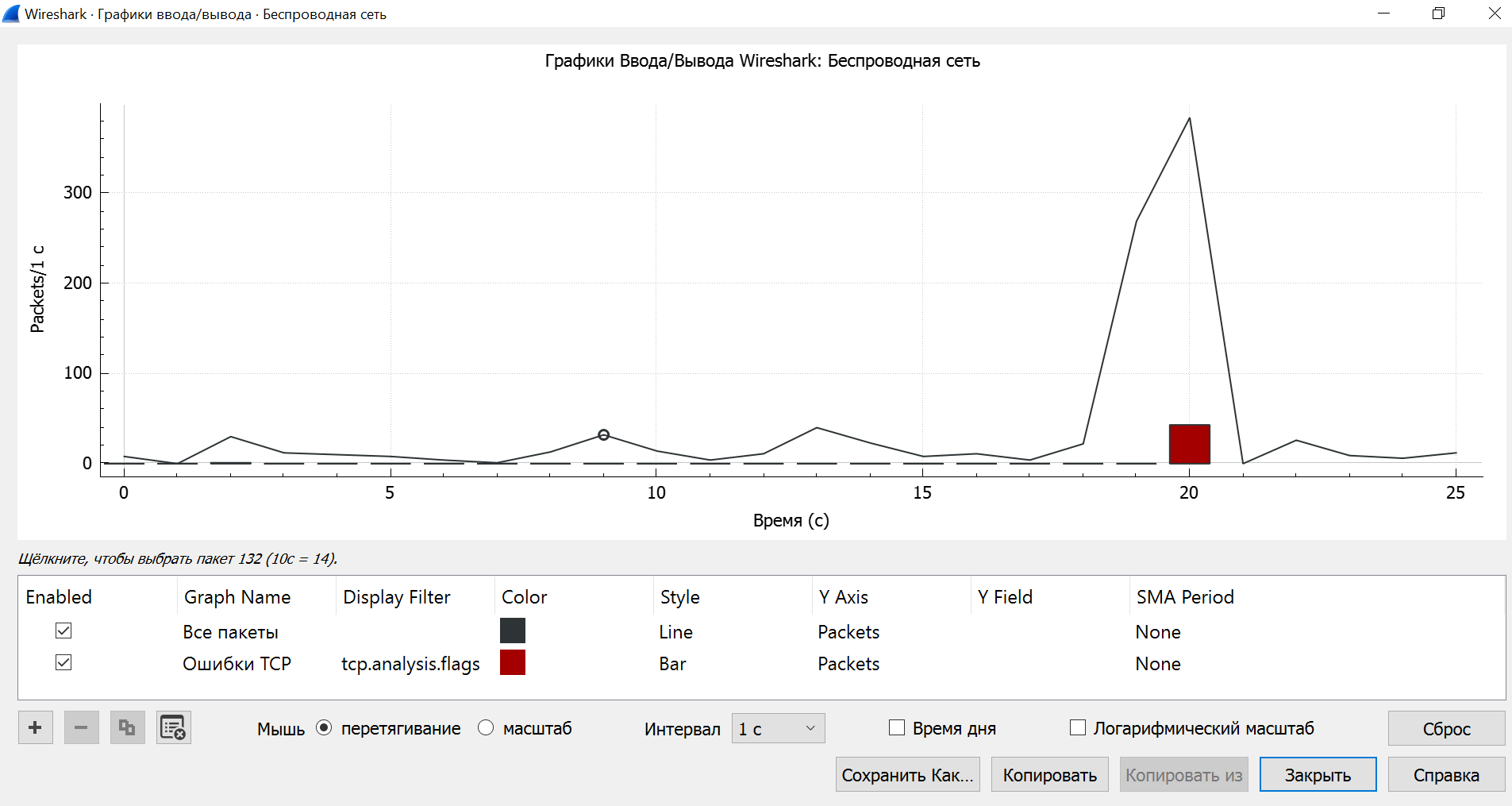
* мінімальний, максимальний та середній розміри пакету;



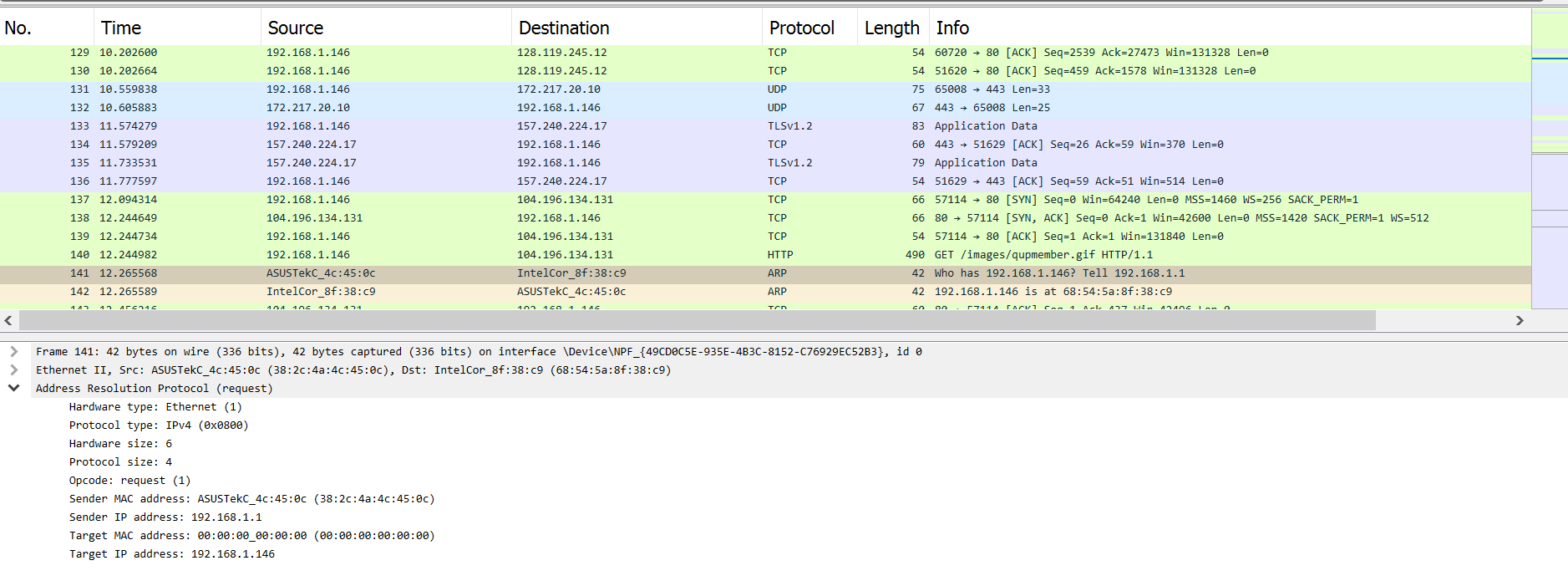
* подивіться по пункту End Points (Ethernet і IPv4), випишіть і поясніть;



* проаналізуйте по IO Gragh поведінку вашого мережевого інтерфейсу.

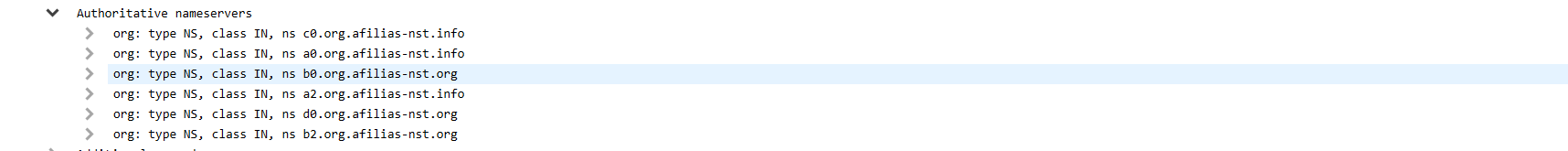
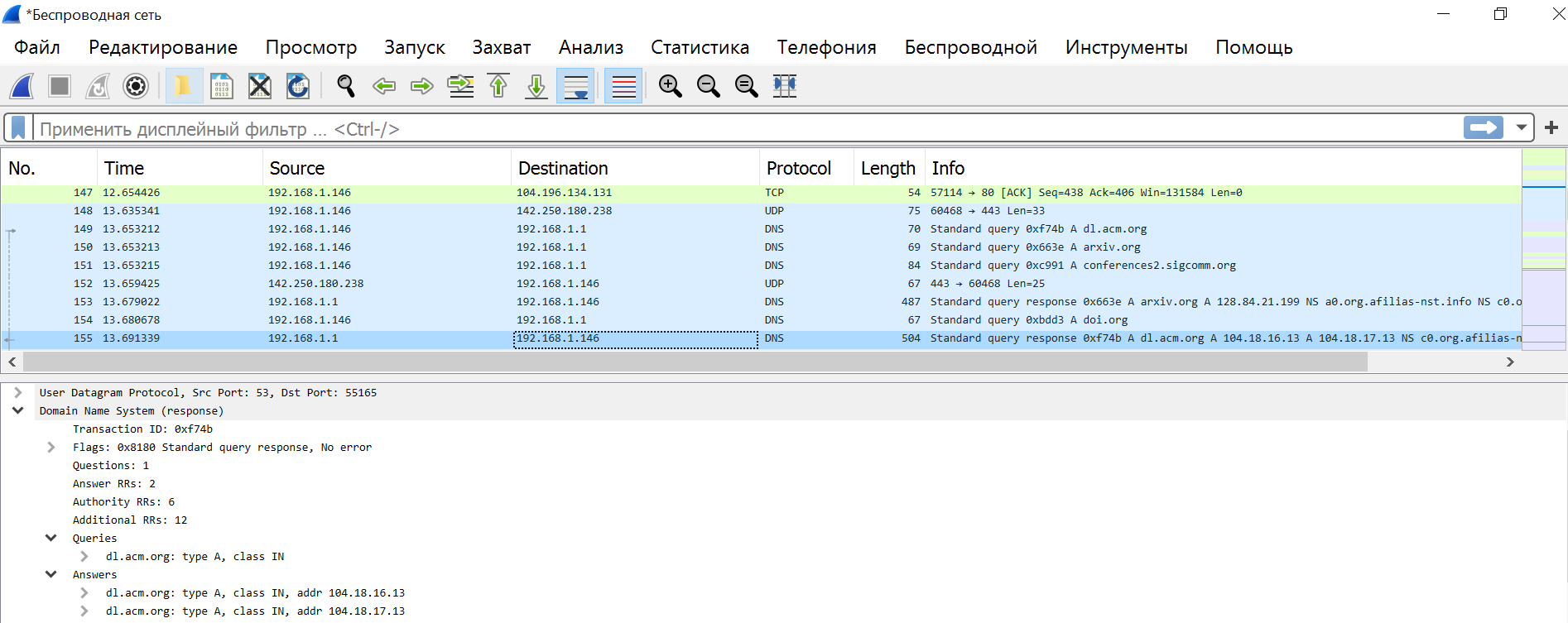


* 1. За даними ARP запиту і відповіді запишіть: IP-адреса і МАС адреса шлюзу вашого комп'ютера.

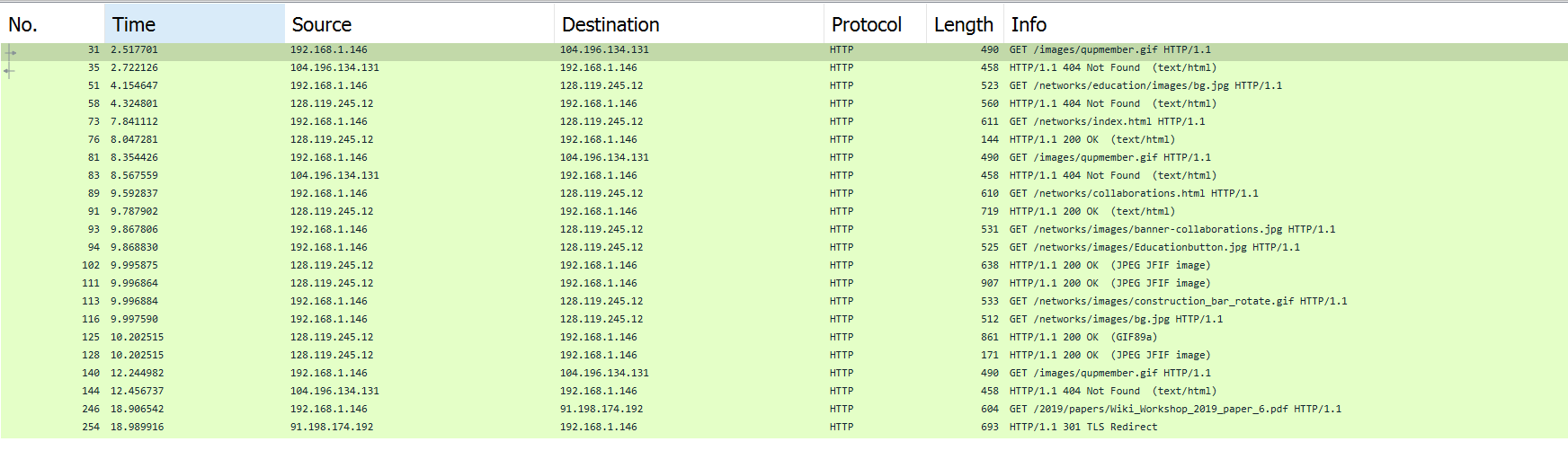


IP-адреса: 192.168.1.146, MAC-адреса шлюзу: 68:54:5a:8f:38:c9

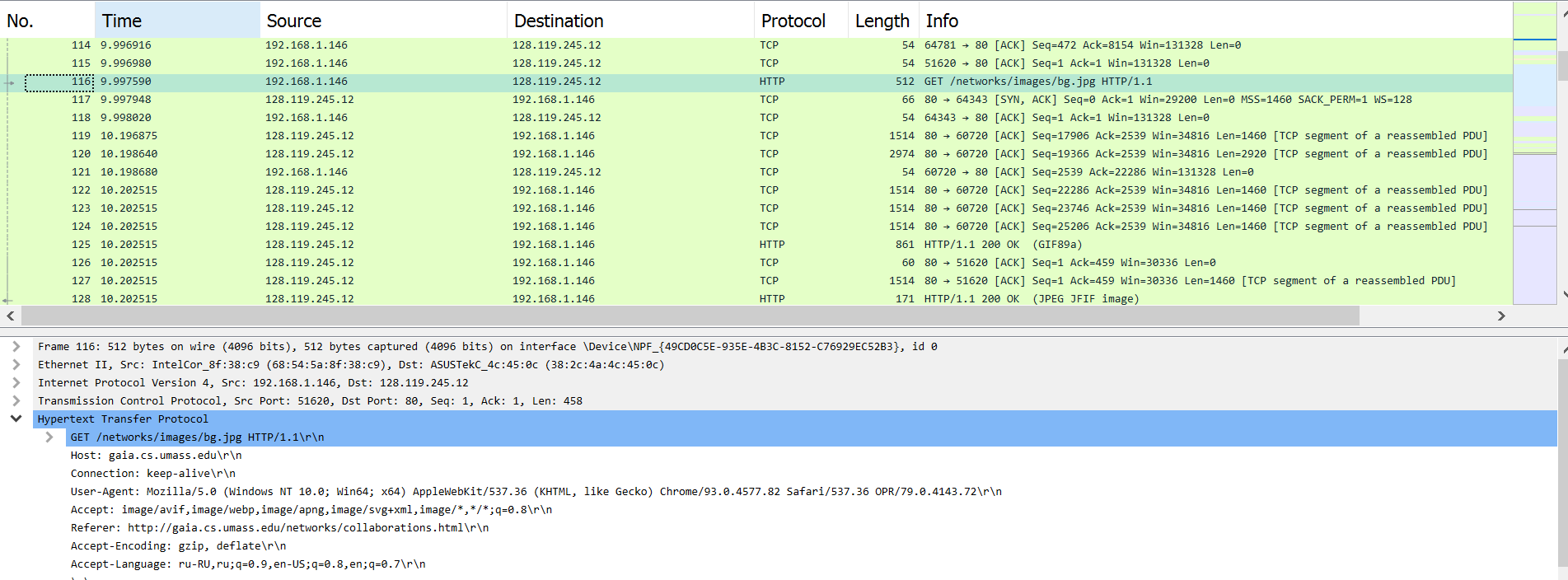
* 1. За даними DNS пакетів запишіть: IP-адреса DNS-сервера і IP-адреса веб-сервера сайту.



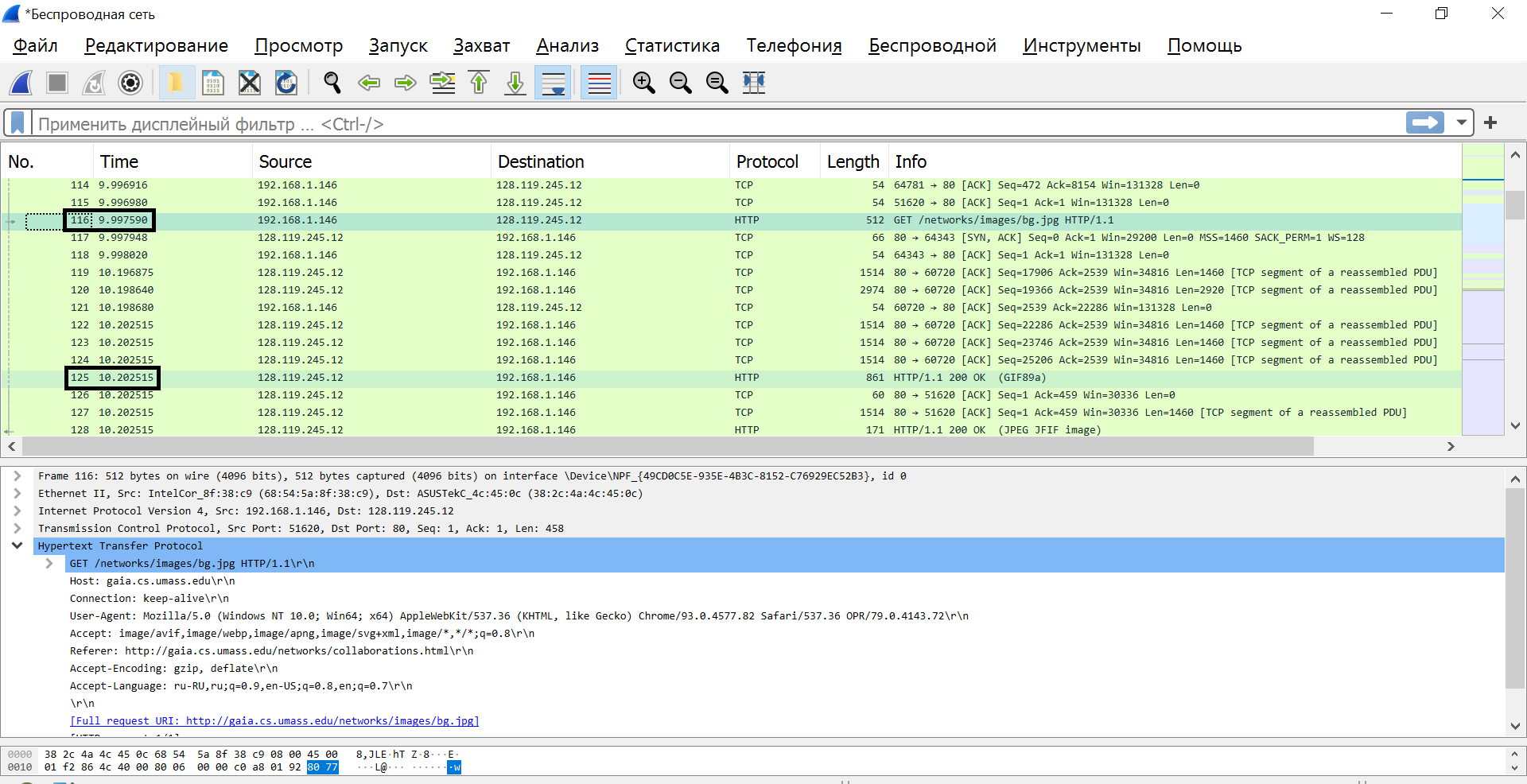
* 1. Для відображення тільки HTTP-повідомлень у вікні списку пакетів вкажіть значення http (всі імена протоколів в Wireshark пишуться в нижньому регістрі) в поле фільтра відображення. Якщо ви захопили не одну сесію HTTP, скористайтеся фільтрами відображення. В поле фільтра введіть http && ip.addr == x.x.x.x, де x.x.x.x - IP-адреса веб-сервера сайту, і натисніть клавішу Enter.



* 1. Знайдіть повідомлення GET протоколу HTTP, відправлене з вашого комп'ютера на HTTP-сервер (gaia.cs.umass.edu, www.google.com/ або інший), яке містить також введену вами адресу gaia.cs.umass.edu або інший. Виділіть знайдену рядок з повідомленням HTTP GET, у вікні деталей заголовків з'явиться інформація по заголовкам всіх нижчих протоколів, в які вкладено GET-повідомлення протоколу HTTP (міститься в сегменті TCP, який, в свою чергу, знаходиться (інкапсулюється) в IP-дейтаграми, яка інкапсулюється в кадр Ethernet).



* 1. Визначте, скільки часу пройшло від моменту відправки повідомлення GET протоколу HTTP до отримання відповідного повідомлення OK? (За замовчуванням, значення поля Time у вікні списку є час в секундах від початку трасування. Ви можете поміняти вид цього поля за вашим бажанням, вибравши в меню View пункт Time Display Format (Формат відображення часу) і потім вказавши відповідне подання часу).



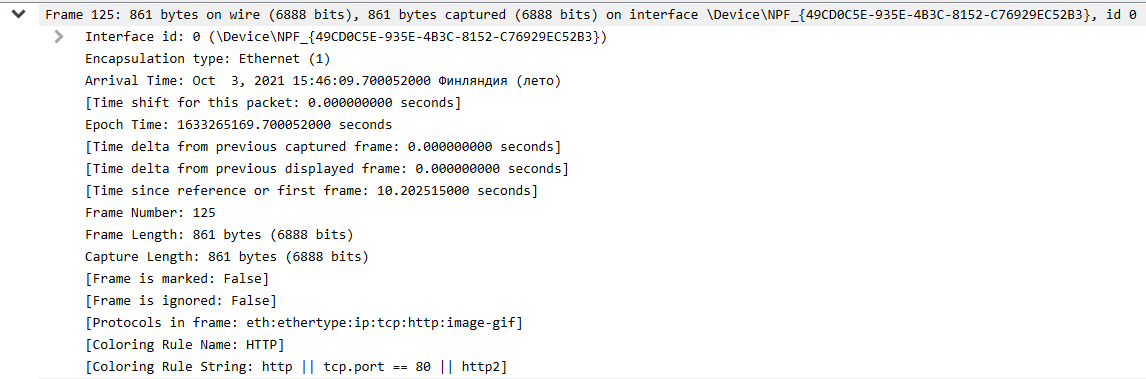
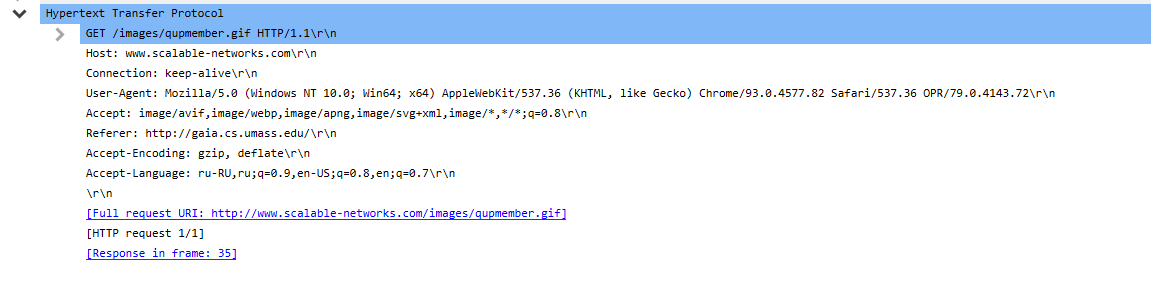
T = 10.202515 – 9.997590 = 0.204925 c

* 1. Користуючись кнопками + і - в лівій частині вікна деталей заголовків, по черзі відкривайте інформацію про кадри Ethernet, дейтаграми IP, сегменті TCP, повідомлення HTTP, скопіюйте в протокол і поясніть (коротко опишіть) призначення основних полів.

*http:*

Основні поля:   
Host – ім’я сайту

Далі йдуть т.зв. заголовки, які сервер може інтерпретувати як захоче. Так, браузер вказує у заголовку accept т.зв. media type, тобто тип, який повинен бути вказаний у заголовку Content-Type відповіді від сервера.



*TCP:*

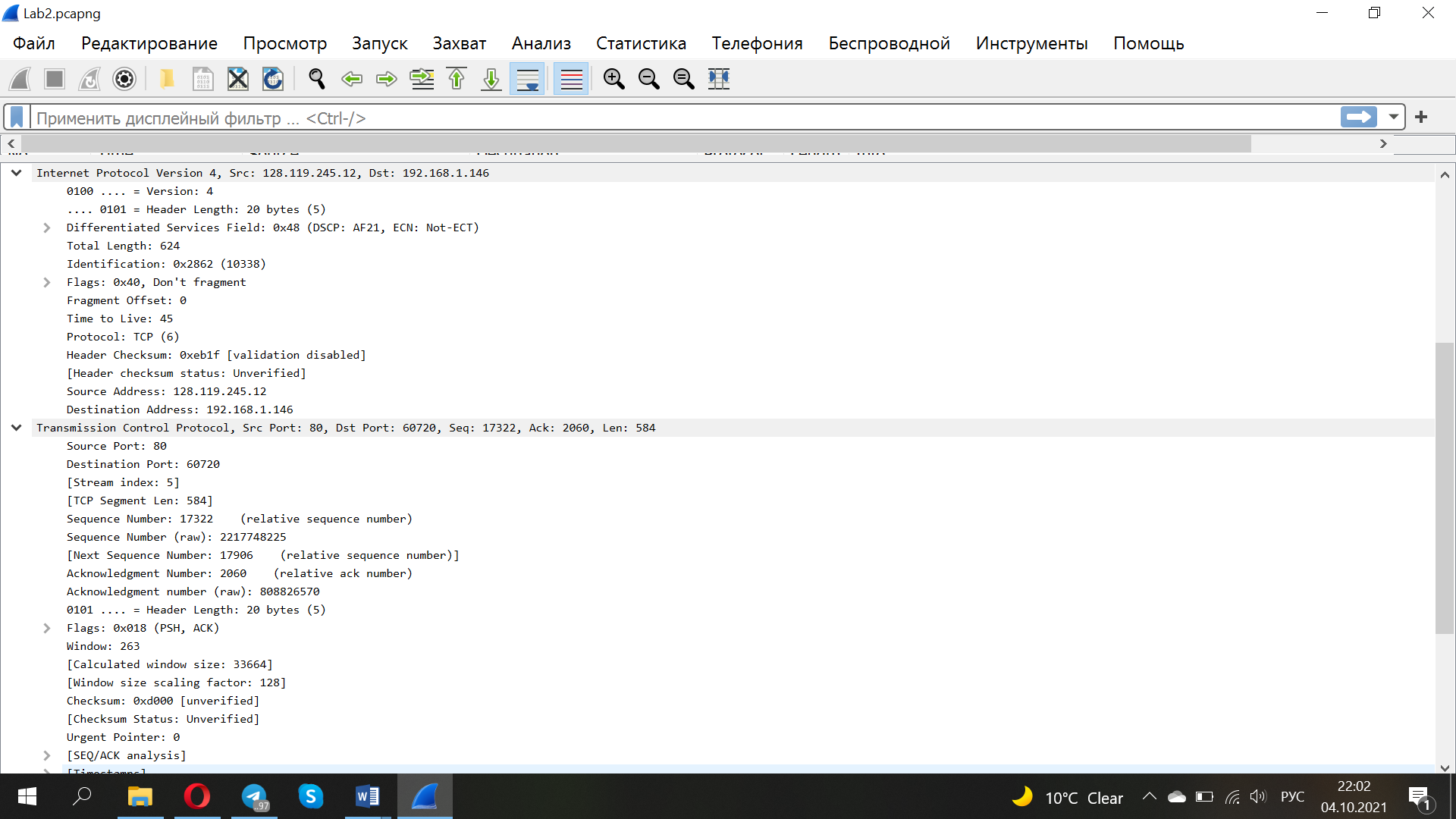
Основні поля:

Sequence Number - порядковий номер пакета

Source Port – номер порта на комп`ютері, з якого було надіслано дані.

Destination Port – порт серверу

Flags – TCP-флаги. PSH – пропустити буферизацію пакета. ACK – підтвердження отримання данних попереднього пакета.



• Source Port (16 біт). Він визначає порт джерела процесу додатки на відправляє пристрої.

• Destination Port (16 біт) - визначає порт призначення процесу додатки на приймаючому пристрої.

• Sequence Number (32 біта) - порядковий номер байтів даних сегмента в сеансі.

• Acknowledgement Number (32 біта). Коли встановлено прапор ACK, це число містить наступний порядковий номер очікуваного байта даних і працює як підтвердження попередніх отриманих даних.

• Data Offset (4 біта). У цьому полі маються на увазі як розмір заголовка TCP (32-розрядні слова), так і зміщення даних в поточному пакеті у всьому сегменті TCP.

• Reserved (3 біта) - зарезервовано для майбутнього використання, і все за замовчуванням встановлюються в нуль.

• Прапори (по 1 біт)

• Windows Size - це поле використовується для управління потоком між двома станціями і вказує обсяг буфера (в байтах), виділений одержувачем для сегмента, т. Е Скільки даних очікує приймач.

• Checksum - це поле містить контрольну суму заголовків, даних і псевдо-заголовків.

• Urgent Pointer. Він вказує на аварійний байт даних, якщо прапор URG встановлений в 1.

• Options - позначає додаткові опції, що не покриваються звичайним заголовком. Поле опцій завжди описується в 32-бітових словах. Якщо це поле містить дані розміром менше 32 біт, для заповнення решти бітів використовується додаток, щоб досягти 32-розрядної кордону.

*Ethernet:*

Містить інформацію про MAC-адресу роутера

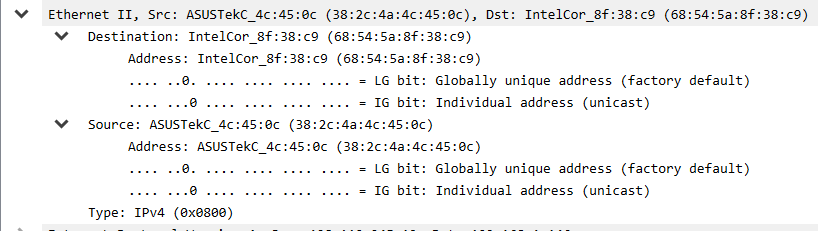
Із заголовка протоколу Ethernet деякого пакету даних:

*Ethernet II* – кадр протоколу Ethernet формату II.

*Src:* – ASUSTekC\_4c:45:0c(38:2с:4а:4с:45:0с) локальна адреса пристрою відправника, де (38:2с:4а:4с:45:0с) - виробник мережевої карти – компанія ASUSTecK.

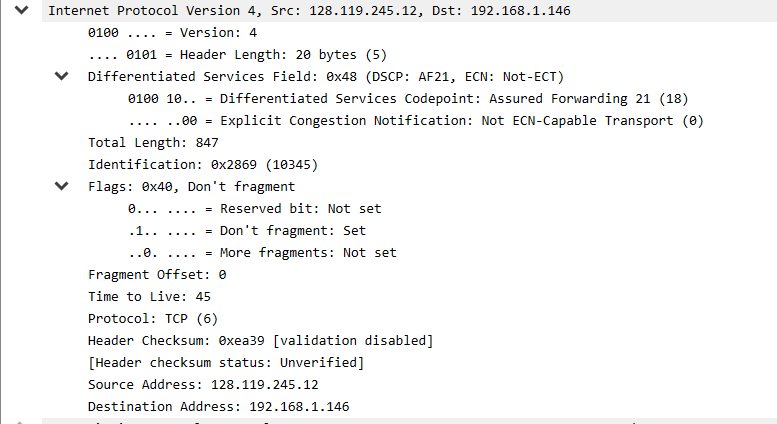
*Dst: IntelCpor\_8f:38:c9 (68:54:5a:8f:38:c9)* – локальна (фізична МАС-адреса) пристрою отримувача *(68:54:5a:8f:38:c9)*, виробник мережевої карти – компанія IntelCor.

*Type:* IP (0х0800) – на мережевому рівні використовується протокол IPv4. Значення цього поля дозволяє пристрою визначити, якому протоколу вищого рівня слід передати дані з поля PDU (призначення поля аналогічне номеру порта в ТСР). В даному випадку – це протокол IP v4. Інші найбільш часто зустрічаються значення поля Type: 0x0806 – ARP, 0x86DD – Ip v6.



*IPv4:*

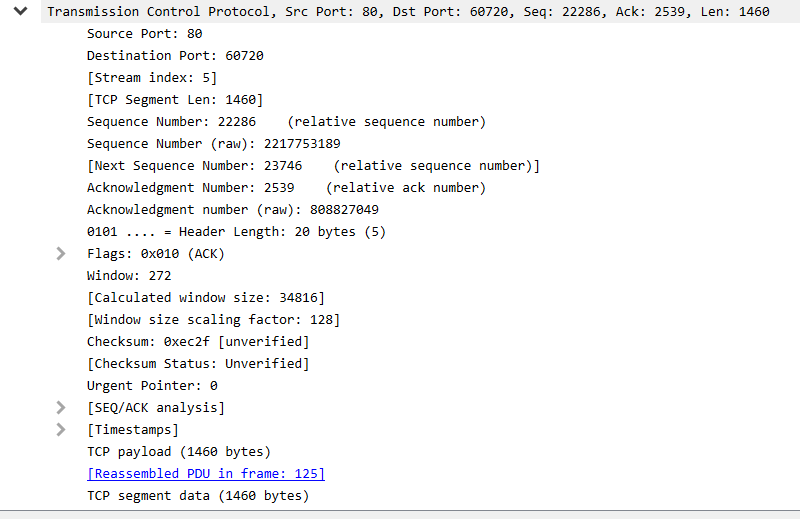
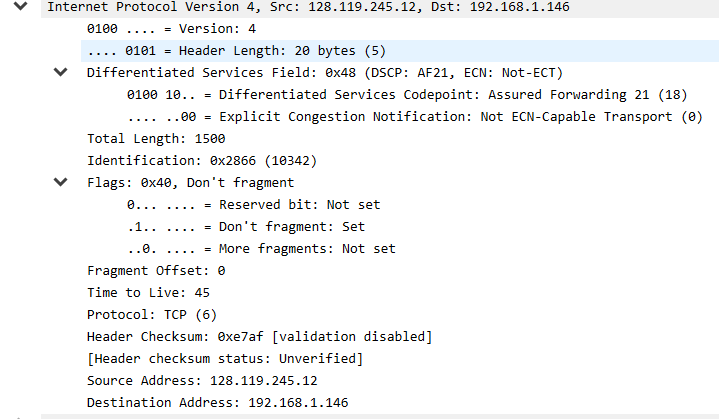
Містить IP-адреси отримувача та адресата у форматі IPv4



*Internet protocol версії 4*, – пакет протоколу IP,

*src: 128.119.245.12* – мережева адреса пристрою відправника *128.119.245.12*, перед адресою в дужках може бути вказано DNS ім’я пристрою відправника.

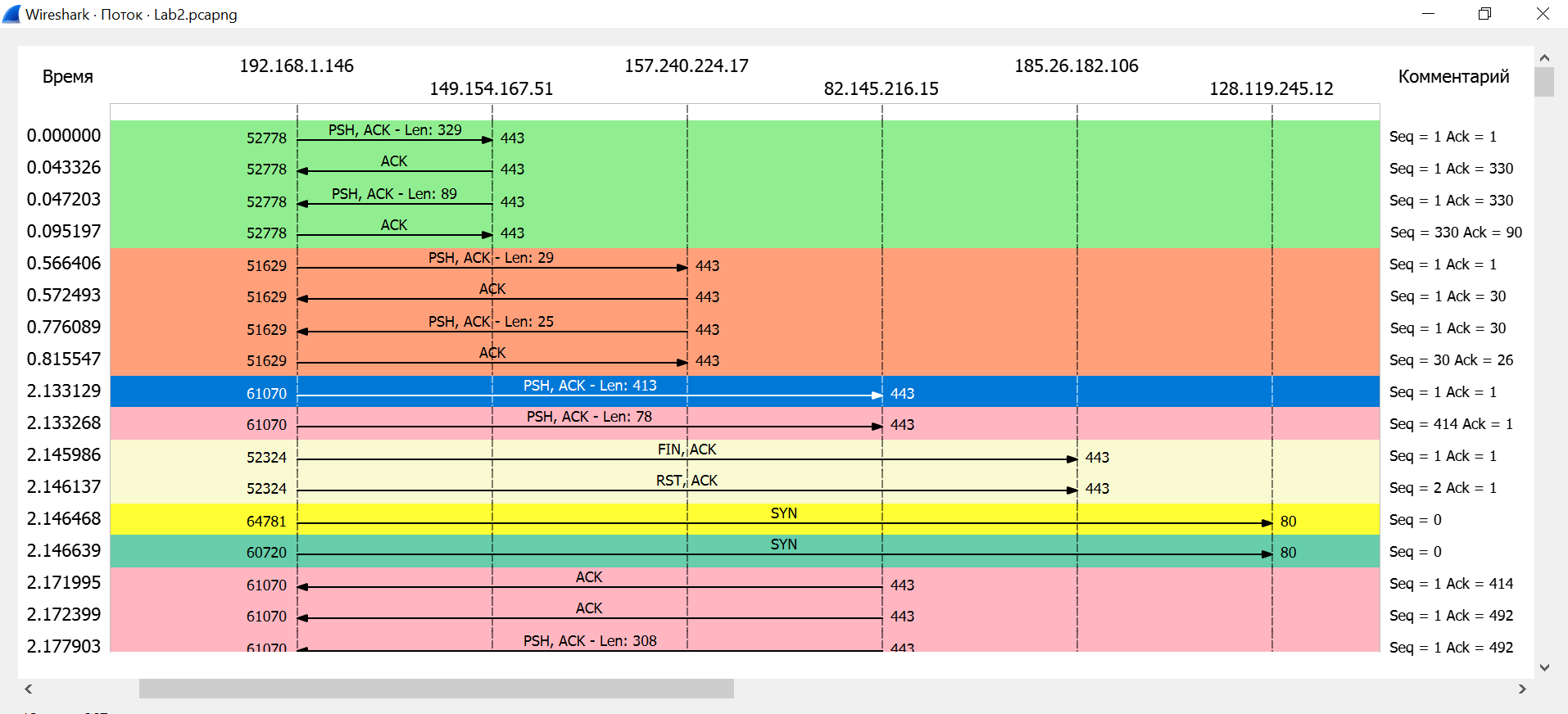
*Dst: 192.168.1.146* – мережева адреса пристрою отримувача *192.168.1.146*, перед адресою в дужках може бути вказано DNS ім’я пристрою отримувача.



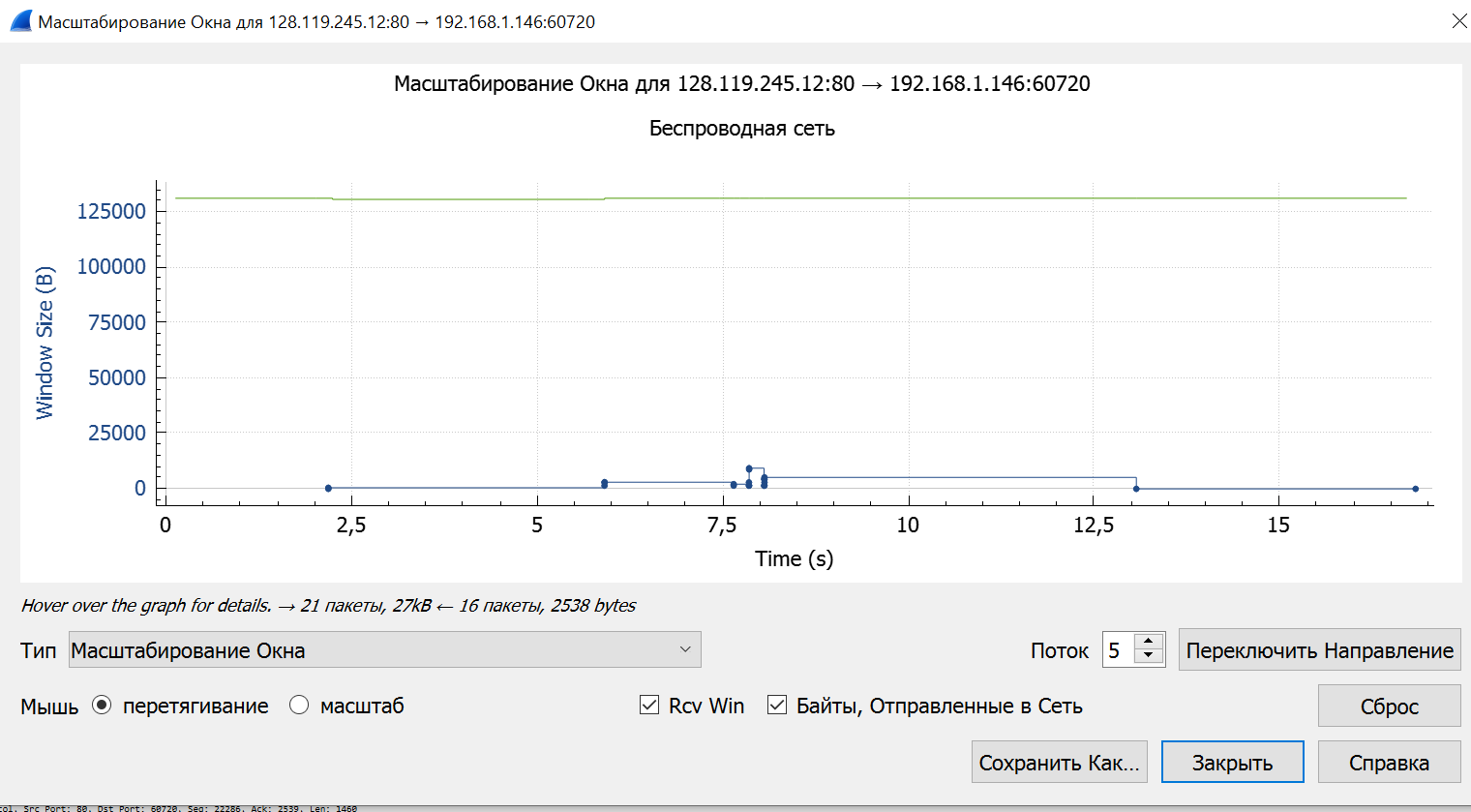
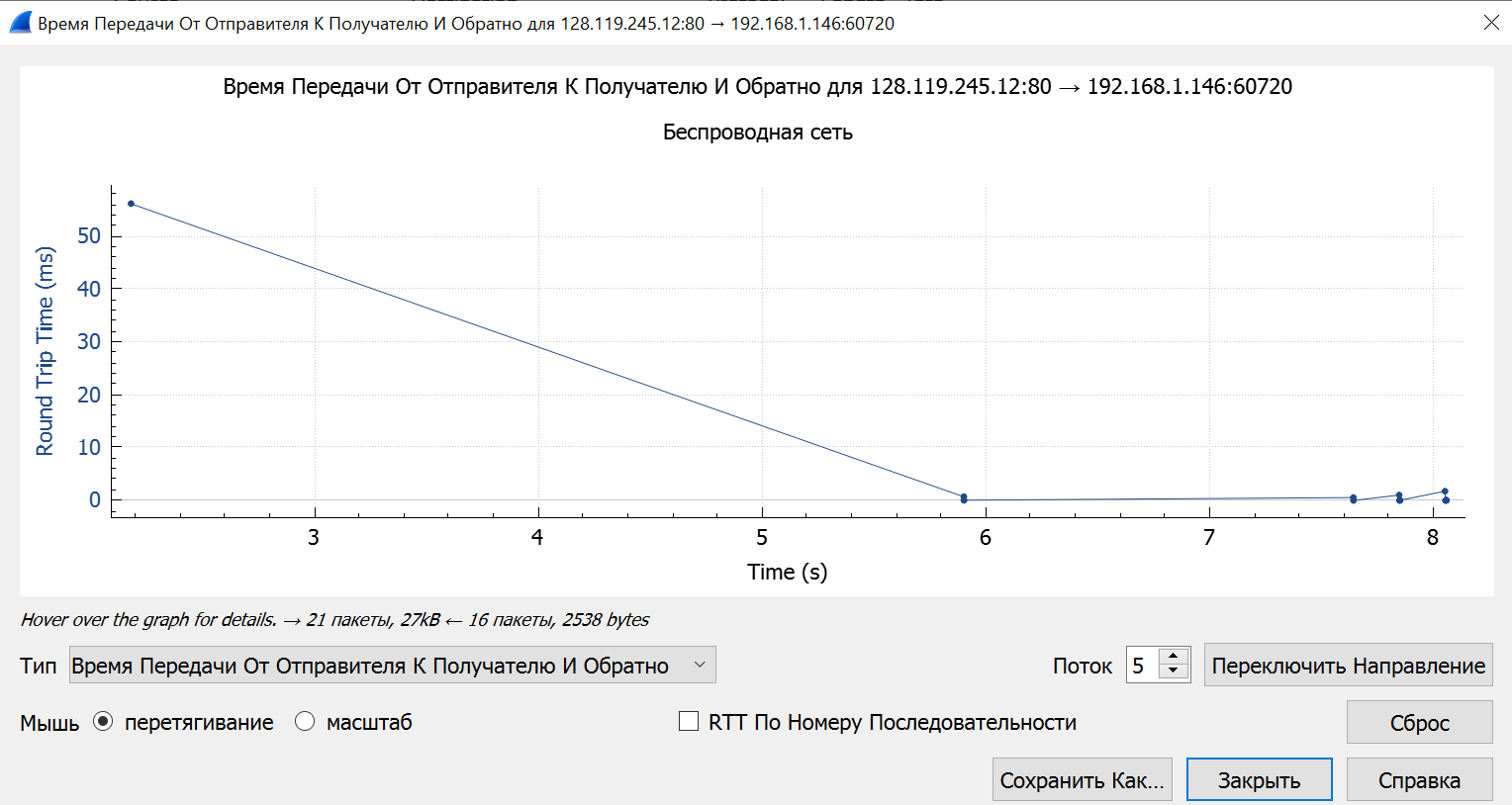
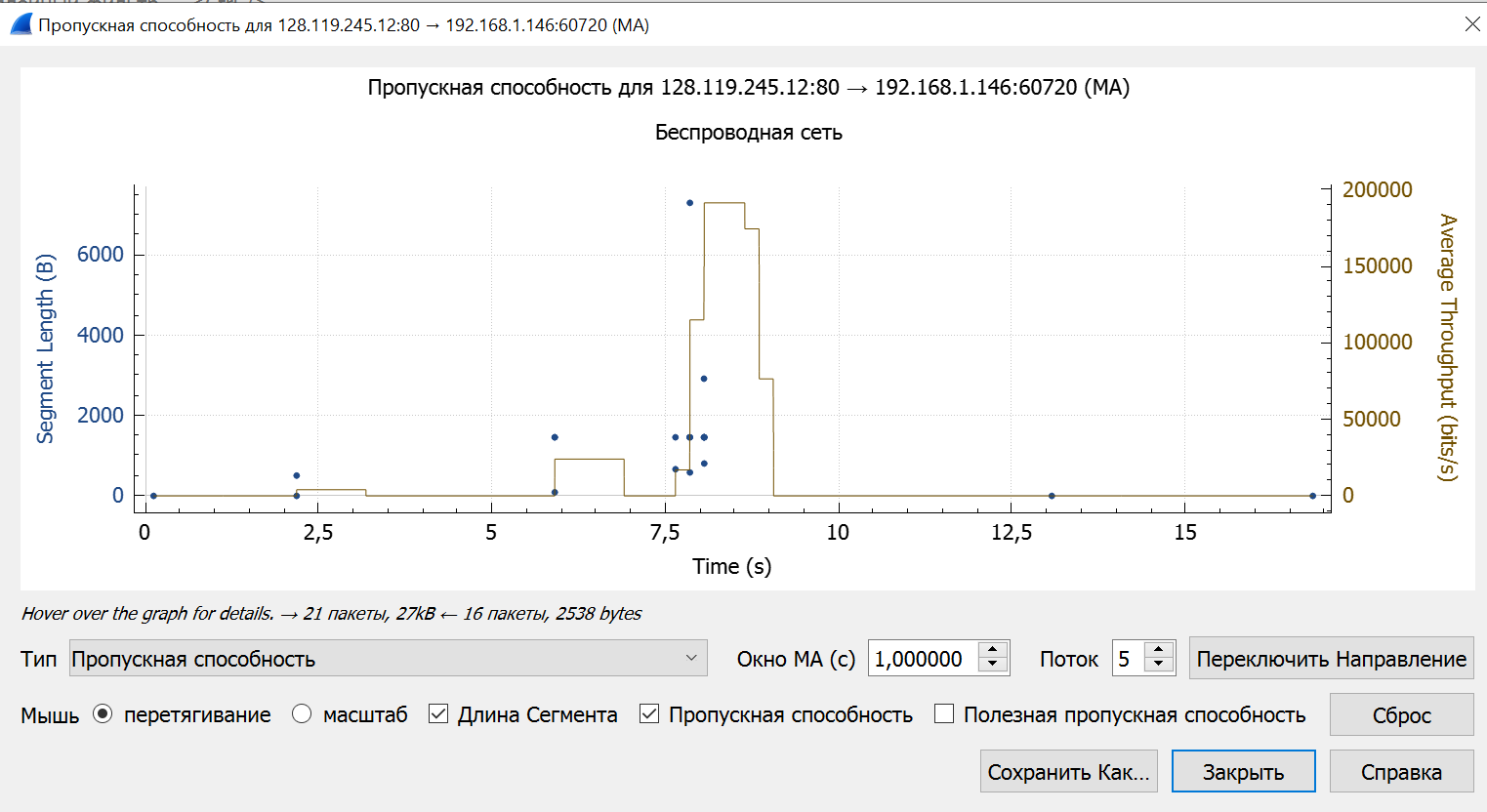
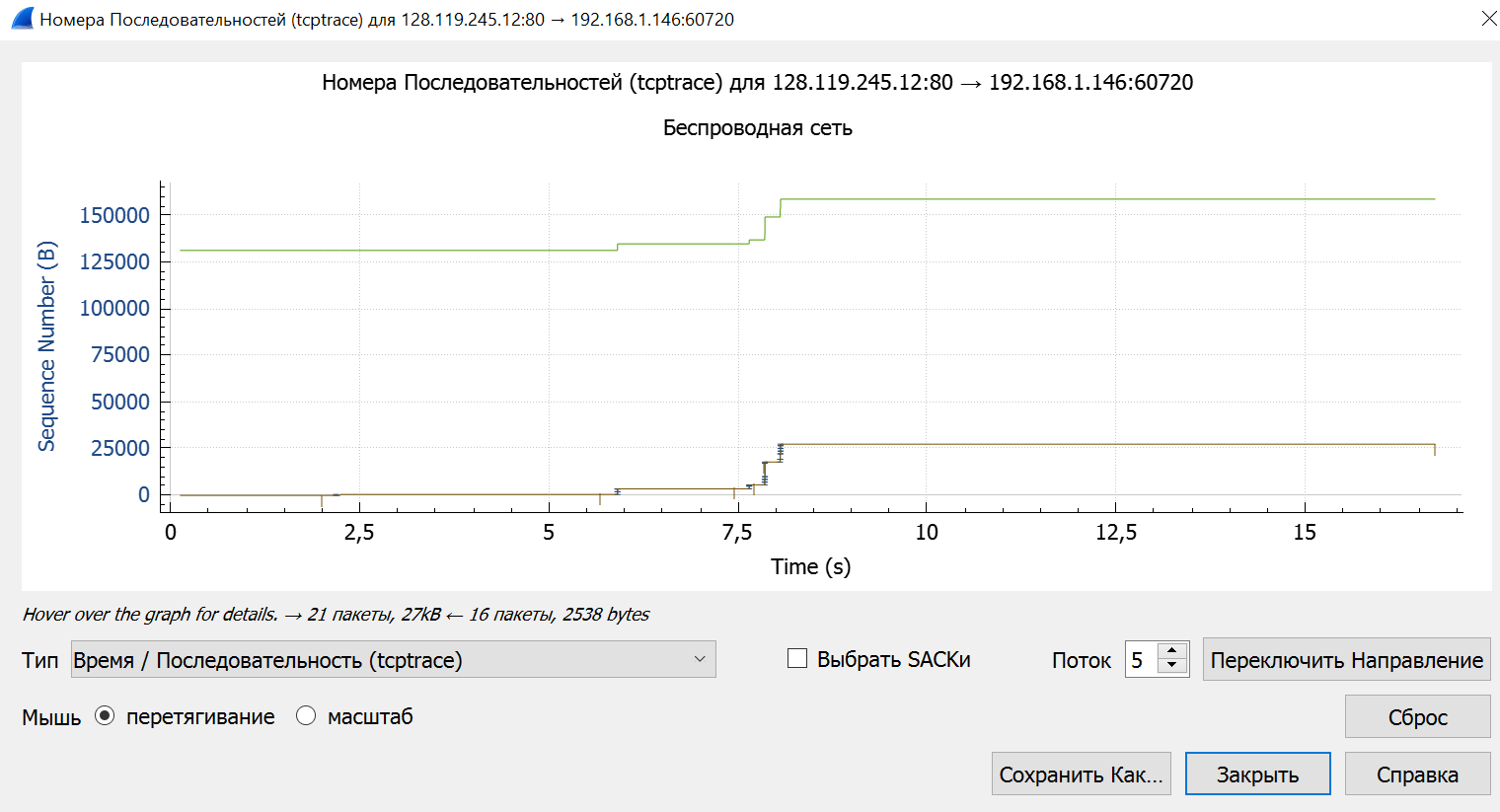
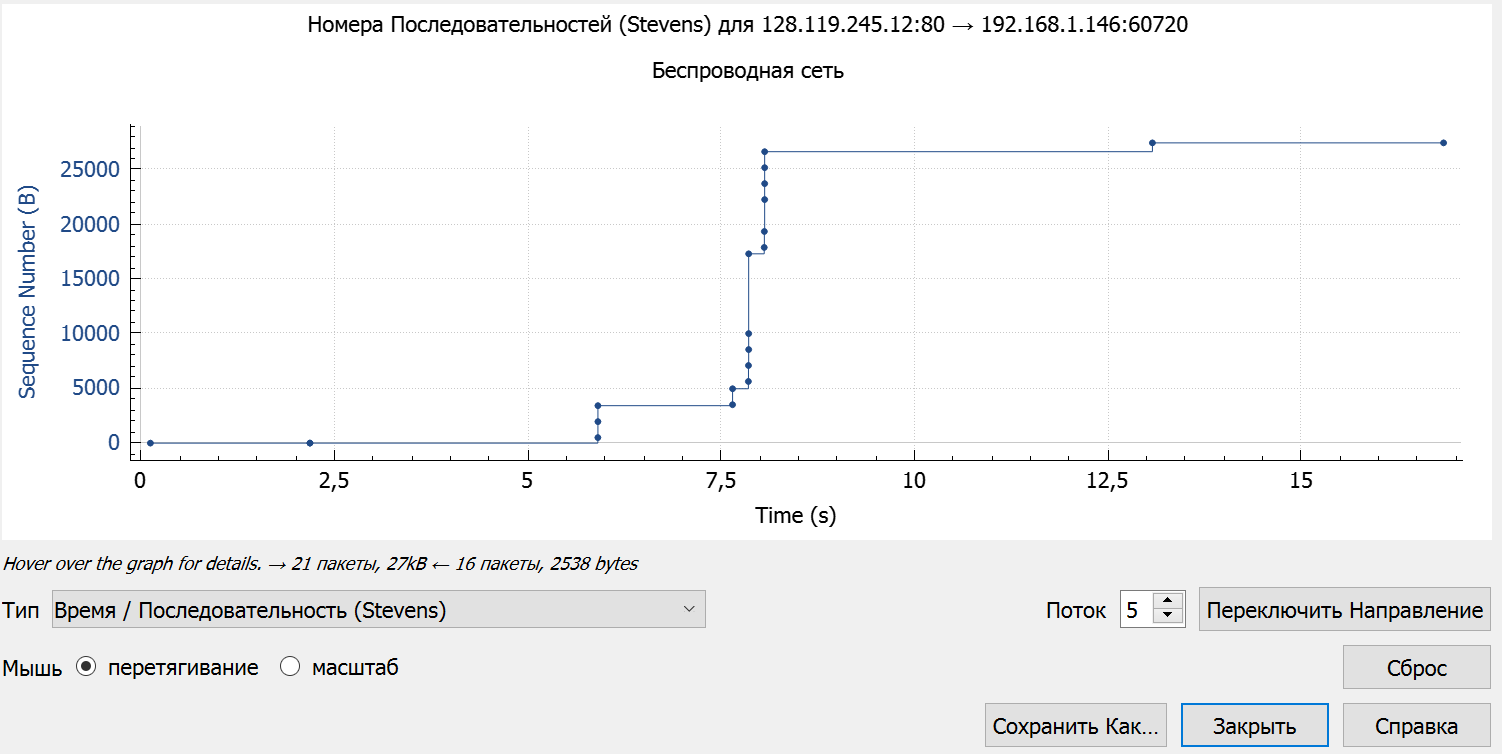
* 1. Проаналізуйте і опишіть повну сесію HTTP (без деталей кожного заголовка) і TCP (детально), використовуючи інформацію з поля списку пакетів і Flow Graph з меню Statistics. Внизу вікна Flow Graph є перемикач Flow Type для перемикання відображення загальної сесії HTTP і тільки TCP. Збережіть діаграму взаємодії машин.

Опис сесії TCP повинен включати:

* IP-адреси джерела і призначення;
* номера портів джерела і призначення;
* процедуру встановлення з'єднання, передачі даних і розриву з'єднання (номери пакетів і значення прапорців управління TCP);
* метод ковзного вікна (зміна значень відносних послідовних номерів і номерів підтвердження і розміру вікна). Це краще видно не на графі, а у  полі списку пакетів.



* 1. Дослідіть сесію інструментами з TCP Stream Graph з меню Statistics. Поясніть графіки, покажіть зміну довжини ковзаючого вікна у відправника і одержувача.



* 1. Результати збережено

Висновки:

Ми ознайомилися iз засобами перехоплення, збереження i аналiзу мережевого трафiку  
за допомогою вiдомого аналiзаторiв мережевого трафiку, а саме програми WireShark  
з встановленним драйвером для перехоплення локального трафiку – npcap.   
Програми – сніфери – це незамінний інструмент для вивчення того, що відбувається в мережі. Якщо знати, що насправді посилається або приймається по кабельній системі, то важкі, на перший погляд, помилки вдається легко знайти і виправити. Сніфер є також важливим інструментом для досліджень динаміки мережі та засобом навчання.

Був проведенний аналiз мережевого сеансу транспортного протоколу TCP. У стеці протоколів TCP / IP виконує функції транспортного рівня моделі OSI. Механізм TCP надає потік даних з попередньою установкою з'єднання, здійснює повторний запит даних в разі втрати даних і усуває дублювання при отриманні двох копій одного пакета, гарантуючи тим самим (на відміну від UDP) цілісність переданих даних і повідомлення відправника про результати передачі. Реалізації TCP зазвичай вбудовані в ядра ОС. Існують реалізації TCP, що працюють в просторі користувача. Коли здійснюється передача від комп'ютера до комп'ютера через Інтернет, TCP працює на верхньому рівні між двома кінцевими системами, наприклад, браузером і веб-сервером. TCP здійснює надійну передачу потоку байтів від одного процесу до іншого.