МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

РУСЛАН СКУРАТОВСЬКИЙ

МЕТОДИЧНИЙ ПОСІБНИК

для виконання практики у лабораторії “Кіберполігон”

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ З ВИКОРИСТАННЯМ WIRESHARK

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНИЙ ПОСІБНИК
для виконання практики
у лабораторії "Кіберполігон"

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ З ВИКОРИСТАННЯМ WIRESHARK

Київ
2024

Підготовлено кандидатом фізико-математичних наук, завідуючим лабораторією Інституту безпеки, доцентом кафедри обчислювальної математики і комп'ютерного моделювання *Р. Скуратовським*

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (*протокол № 6 від 15.05.24*)

Методичний посібник для виконання практики у лабораторії "Кіберполігон" "Аналіз мережевого трафіку з використанням Wireshark" / уклад. Р. Скуратовський. Київ: МАУП, 2024. 48 с.

Методичний посібник містить доступно викладений матеріал як по застосуванню аналізатора мережевого трафіка Wireshark Network Analyzer, так і методи аналізу і знаходження патологічного трафіку. Схарактеризовано переваги Wireshark Network Analyzer. Згідно з вивченою в курсі дискретної математики теорією відносності створено і описано взаємозв'язок фільтрування мережевого трафіку, що реалізоване в Wireshark на рівні протоколів. Представлені всі команди на рівні фільтрів логічного типу і знакові системи, які реалізують такі відношення, як виключення, перетин, об'єднання. В роботі чудово представлено мережевий інтерфейс даної програми. Також описані фільтри для транспортних протоколів (наприклад, TCP, UDP).

Важливість зазначеної програми Wireshark в сучасному кіберсвіті є очевидною, оскільки вона дозволяє визначити можливі загрози для безпеки мережі, виявити паразитивний, вірусний і закільцьований трафіки, дамп трафіку і різного типу мережеві атаки.

Для студентів магістратури спеціальностей кібербезпека і комп'ютерні науки.

ВСТУП

Аналіз мережного трафіку є вкрай важливим для забезпечення стабільності, ефективності та безпеки мережі. Основні причини, чому аналіз мережного трафіку є важливим, включають:

1. Виявлення кіберзагроз та злочинної діяльності: аналіз мережевого трафіку дає змогу виявляти кіберзагрози та злочинну діяльність, такі як вторгнення, спам, фішинг та ін. Це допомагає запобігти можливим кібератакам і захистити мережу від стороннього втручання.
2. Підвищення ефективності мережі: аналіз мережевого трафіку уможливлює знаходити проблеми з пропускною спроможністю, визначати трафік, який споживає більше ресурсів мережі, та забезпечувати оптимальне використання ресурсів мережі, що підвищує ефективність її роботи.
3. Відновлення роботи мережі: аналіз мережевого трафіку може допомогти відновити роботу мережі після виникнення проблем, таких як відмова обладнання або програмного забезпечення.
4. Поліпшення безпеки мережі: аналіз мережевого трафіку може допомогти виявити вразливості мережі та допомогти виправити їх, щоб уникнути можливих кібератак.
5. Підтримка рішень: аналіз мережевого трафіку може допомогти приймати обґрунтовані рішення щодо конфігурації мережі, вибору обладнання та відповідності вимогам безпеки.

У цілому аналіз мережевого трафіку є важливим інструментом для забезпечення безпеки та ефективності мережі, а також для виявлення та усунення проблем.

Ми пропонуємо найбільш доступну і водночас просунуту програму мережевого аналізатора — Wireshark (сніфера). Безперечним залишається те, що є конкурентоздатним доповнення до існуючих Real-Time систем виявлення атак.

Її конкурент — Network Traffic Analyzer, NTA недоступна у вільному доступі.

Для успішного виконання лабораторної роботи необхідно знати стек протоколів TCP/IP, протокол UDP.

Завдання

Уявіть, що Ви є аналітиком комп'ютерної безпеки, який отримав відомість про підозрілий мережевий трафік на одному з серверів вашої організації. Ваше завдання — дослідити цей трафік з використанням програми Wireshark та визначити можливі загрози для безпеки мережі. Виявити паразитивний, вірусний і закільцьований трафіки, дамп трафіку.

Рекомендації для покрокового виконання:

1. Запустіть **Wireshark** та виберіть мережевий інтерфейс, через який ви хочете аналізувати трафік.
2. Надайте кілька скрінів, де є мережевий інтерфейс Wireshark. Опишіть їх вербально, зокрема їх переваги і недоліки.
3. Прокоментуйте, як Ви вибрали джерело трафіку і підкріпіть це скрінами.

Означення. **API** — applicated program interface.

На рис. 1. зображено API-інтерфейс версії 1.12.3 Wireshark Network Analyzer.

3.1. Почекайте деякий час, щоб зібрати достатню кількість пакетів.

3.2. Проаналізуйте заголовки пакетів, щоб виявити незвичайний або підозрілий трафік. Зверніть увагу на такі параметри, як джерело та призначення пакетів, тип протоколу тощо.

4. У командний рядок ввести команду *ssh* demo@test.rebex.net. та віддалено підключитися до тестового сервера.

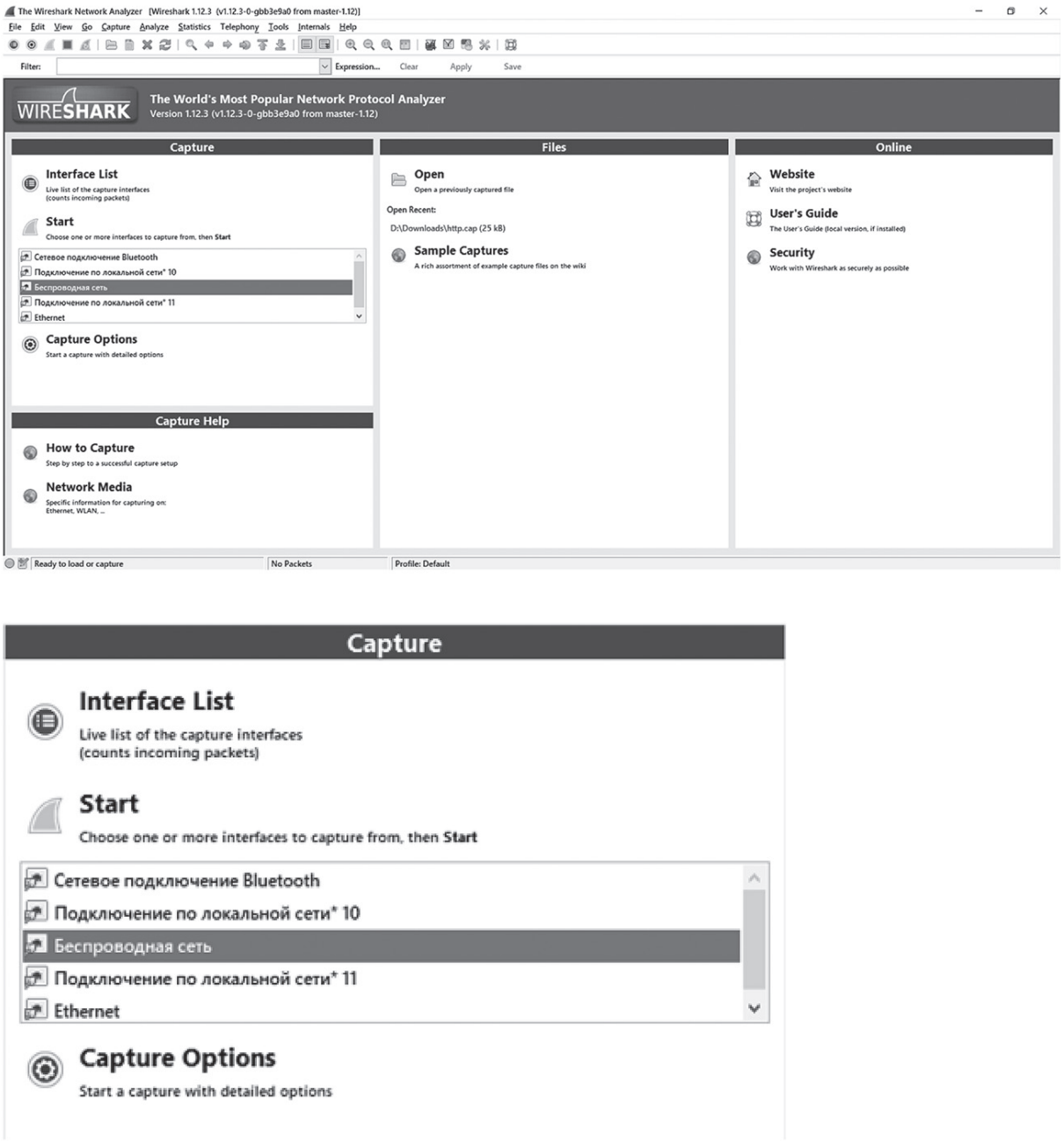

Рис. 1. **API-інтерфейс версії 1.12.3 Wireshark Network Analyzer**

Після відфільтрувати дані за протоколом SSH. #6 (див. рис. 2).

А тепер опишемо і застосуємо різні фільтри по IP та по типу протокола.

Відношення фільтрування

Створити фільтр можна вручну як у рядку запитів, так і за допомогою контекстно-залежного меню.

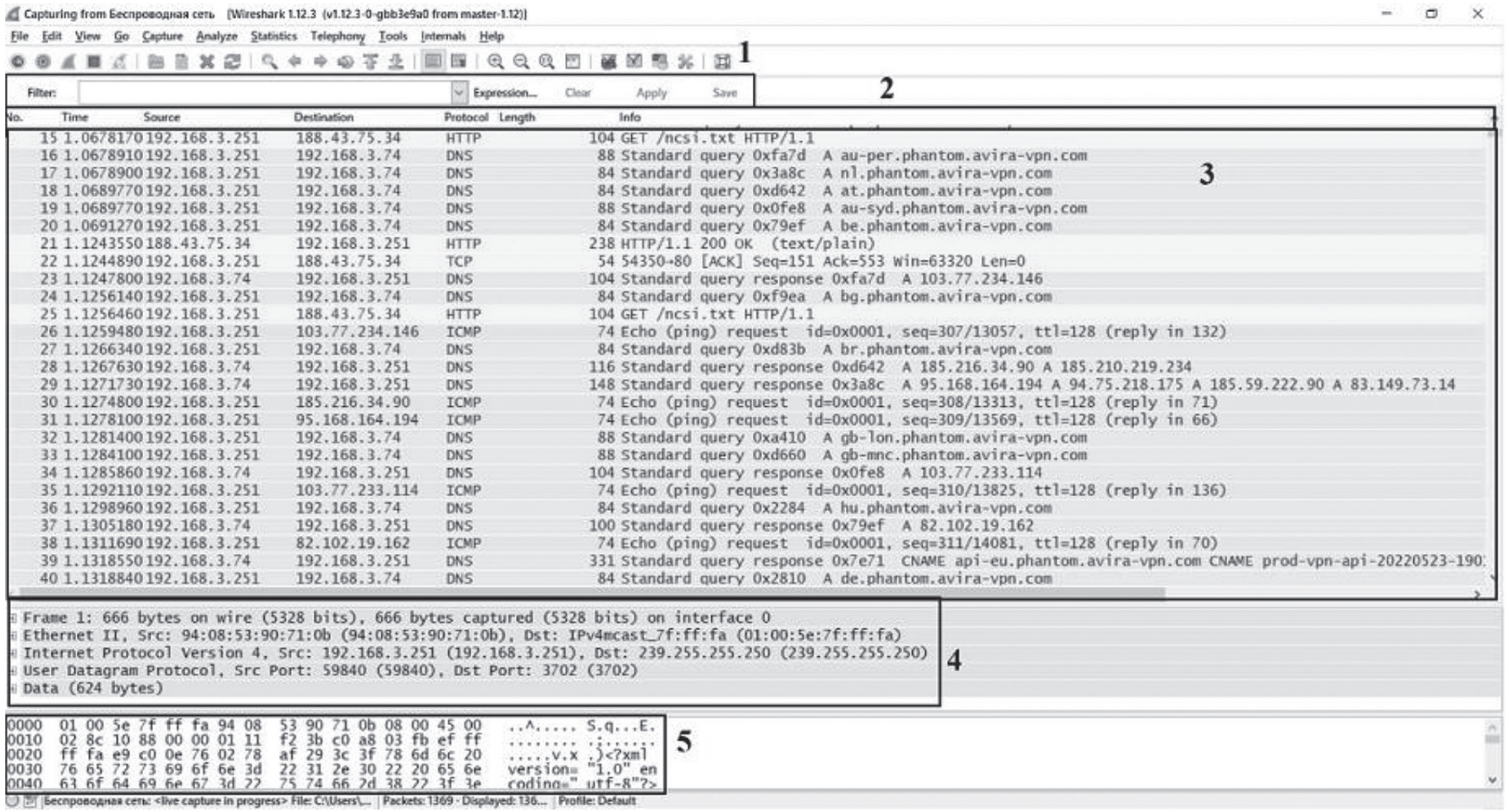

Рис. 2. **Занурення в бездротову мережу 1.12.3 Wireshark**

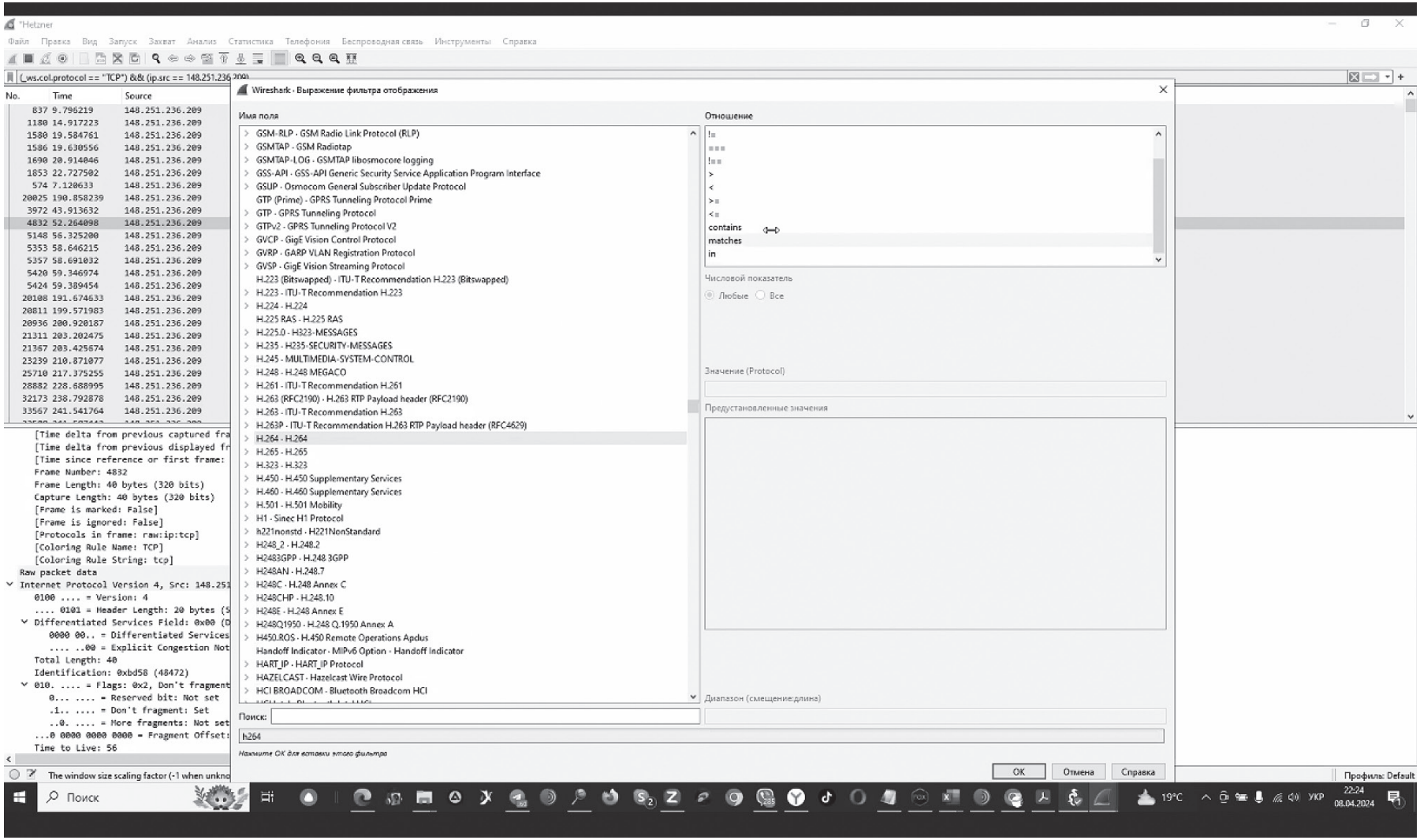

Рис. 3. **Вибравши поле, ми одразу зафіксуємо тип протоколу і IP, що відповідають цьому полю**

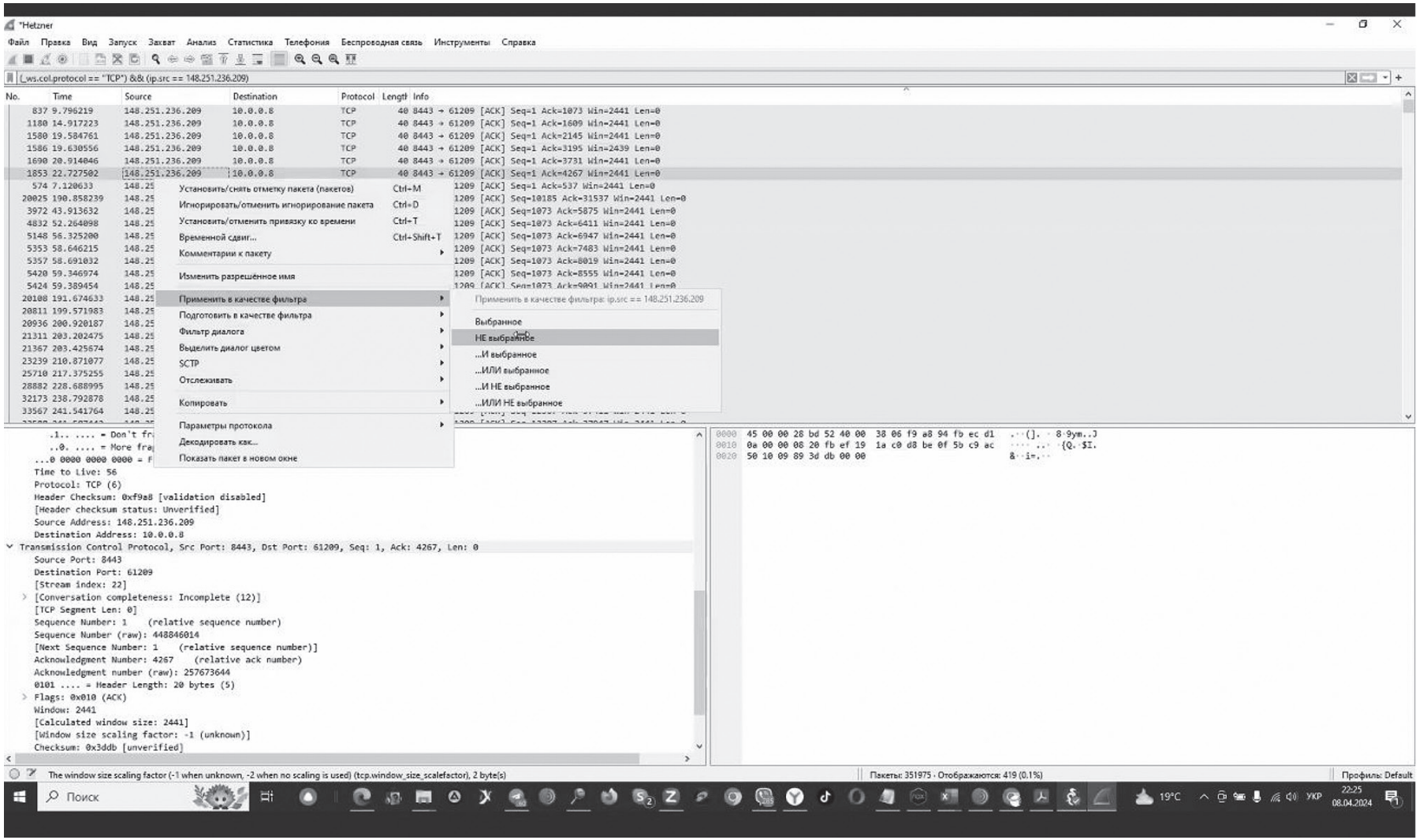

Рис. 4. **Не вибране.**

Створимо фільтр типу ВИКЛЮЧЕННЯ для конкретного IP. Це можна зробити прописавши у пошуковому рядку “!”

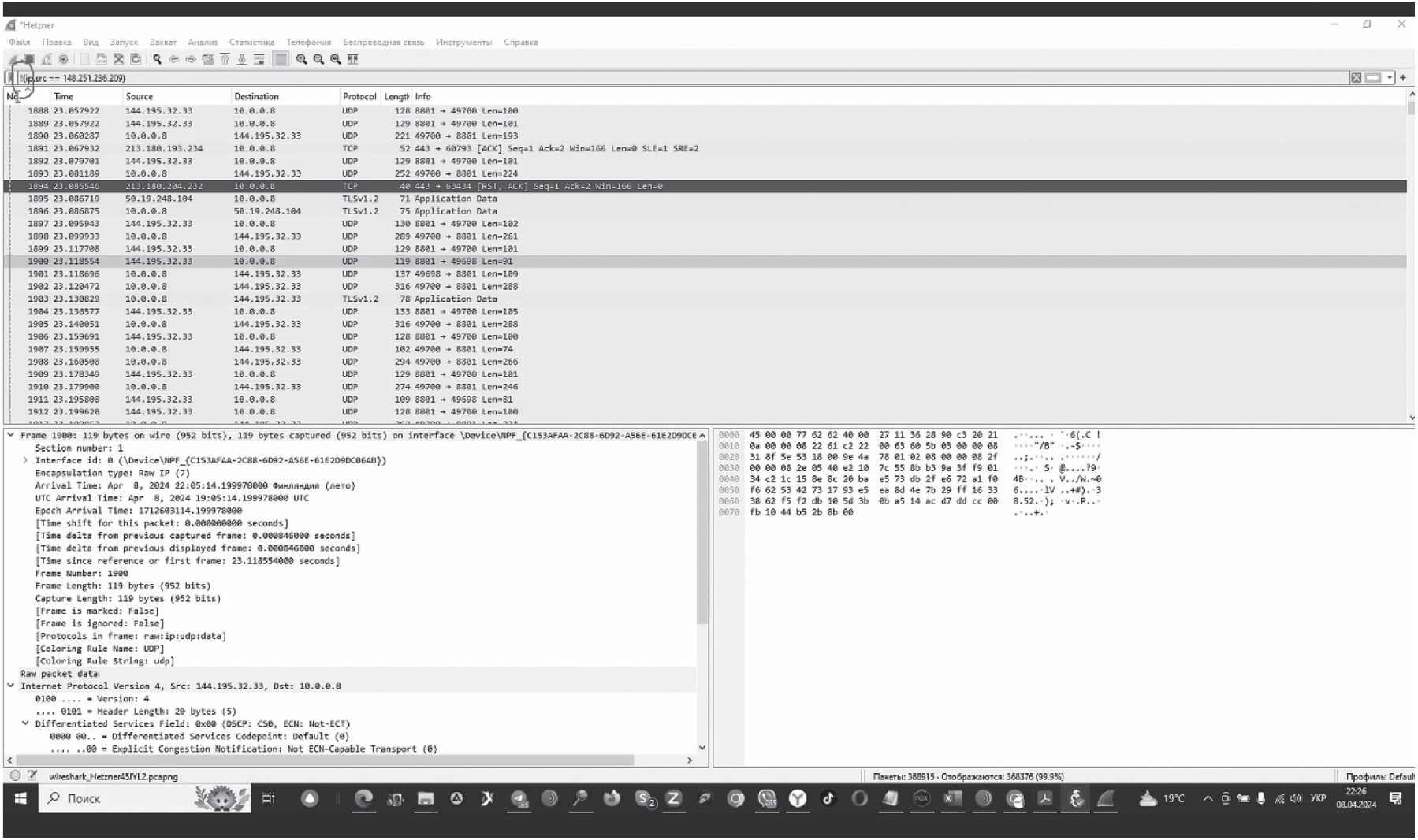

Рис. 5. **Виключення — це знак інверсії, який пишеться як “!” перед ip.src у командному рядку**

5. Використовуйте фільтри Wireshark для відсіювання непотрібної інформації та підкреслення потенційно небезпечного трафіку.

   Опишіть ці фільтри ось тут по назвах і по призначенню. Також давайте СКРІН, де використано фільтр.

6. Зверніть увагу на будь-які аномалії у звичайному шаблоні трафіку, такі як надмірна кількість запитів, незвичайний обсяг даних або неправильний тип запитів.
7. Якщо ви виявите підозрілий трафік, спробуйте встановити його джерело та призначення, а також тип даних, які передаються.
8. Після аналізу зробіть звіт з виявленими загрозами та рекомендаціями щодо подальших заходів з усунення можливих проблем безпеки.

Отримані навички

Це завдання допоможе учасникам практично застосувати навички аналізу мережевого трафіку з використанням програми Wireshark та виявлення можливих загроз для безпеки мережі.

Контрольні запитання

- Як за допомогою Wireshark виявити ознаки Ddos атаки у вашій мережі?
- По якому протоколу у вашій мережі отримано найбільше пакетів?
- Якою командою задається фільтр типу АБО?
- Якою командою задається фільтр типу І?
- Створіть фільтр типу ВИКЛЮЧЕННЯ для конкретного IP.

Примітка. Будьте обережні та дотримуйтесь внутрішніх політик безпеки вашої організації під час аналізу мережевого трафіку.