Мережевий захист засобами синтаксичного аналізу трафіку

Студент: Мєдвєдєв Володимир Євгенович

Керівник: Медведєва Валентина Миколаївна

Мережевий захист засобами синтаксичного аналізу трафіку

Мета: розробка засобів підвищення ефективності мережевого захисту за допомогою застосування методу синтаксичного аналізу трафіку

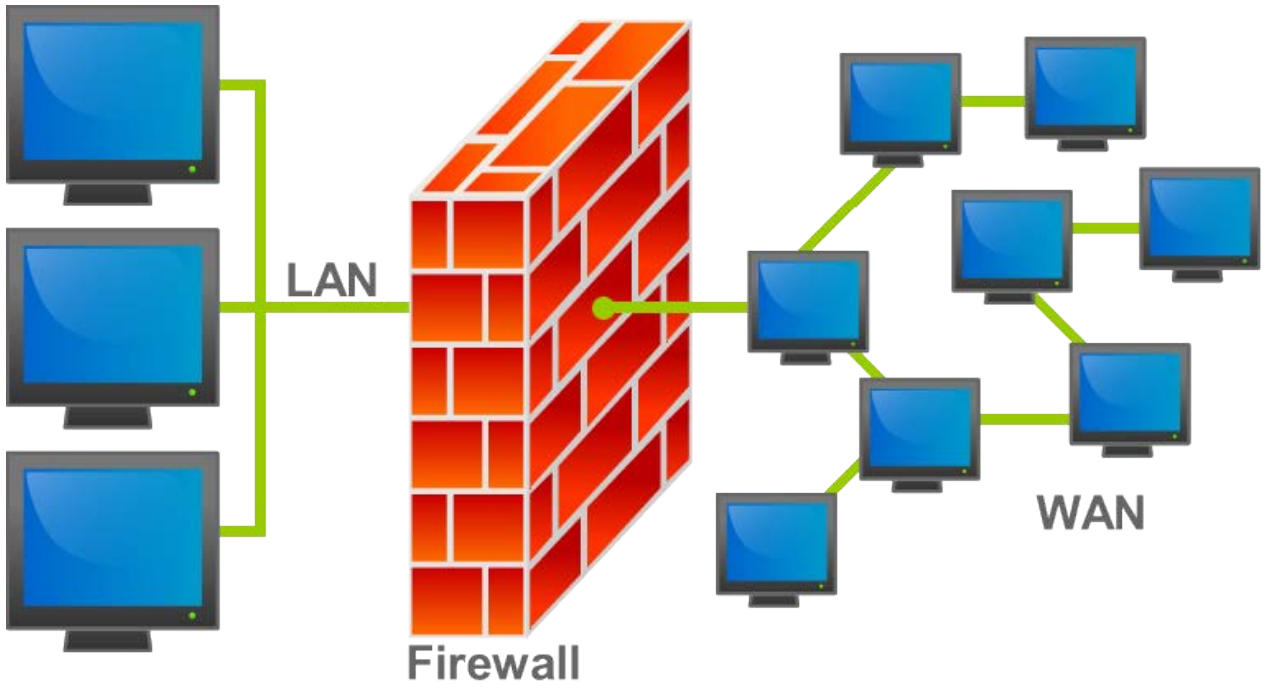
Задачі:

- дослідити засоби мережевого захисту;
- розробити алгоритм синтаксичного аналізу трафіку на основі опису взаємодії протоколів;
- розробити програмний засіб, що реалізує синтаксичний аналіз трафіку.

Об’єктом дослідження є програмне забезпечення мережевого захисту інформації.

Предметом дослідження є програмне забезпечення мережевого захисту засобами синтаксичного аналізу трафіку.

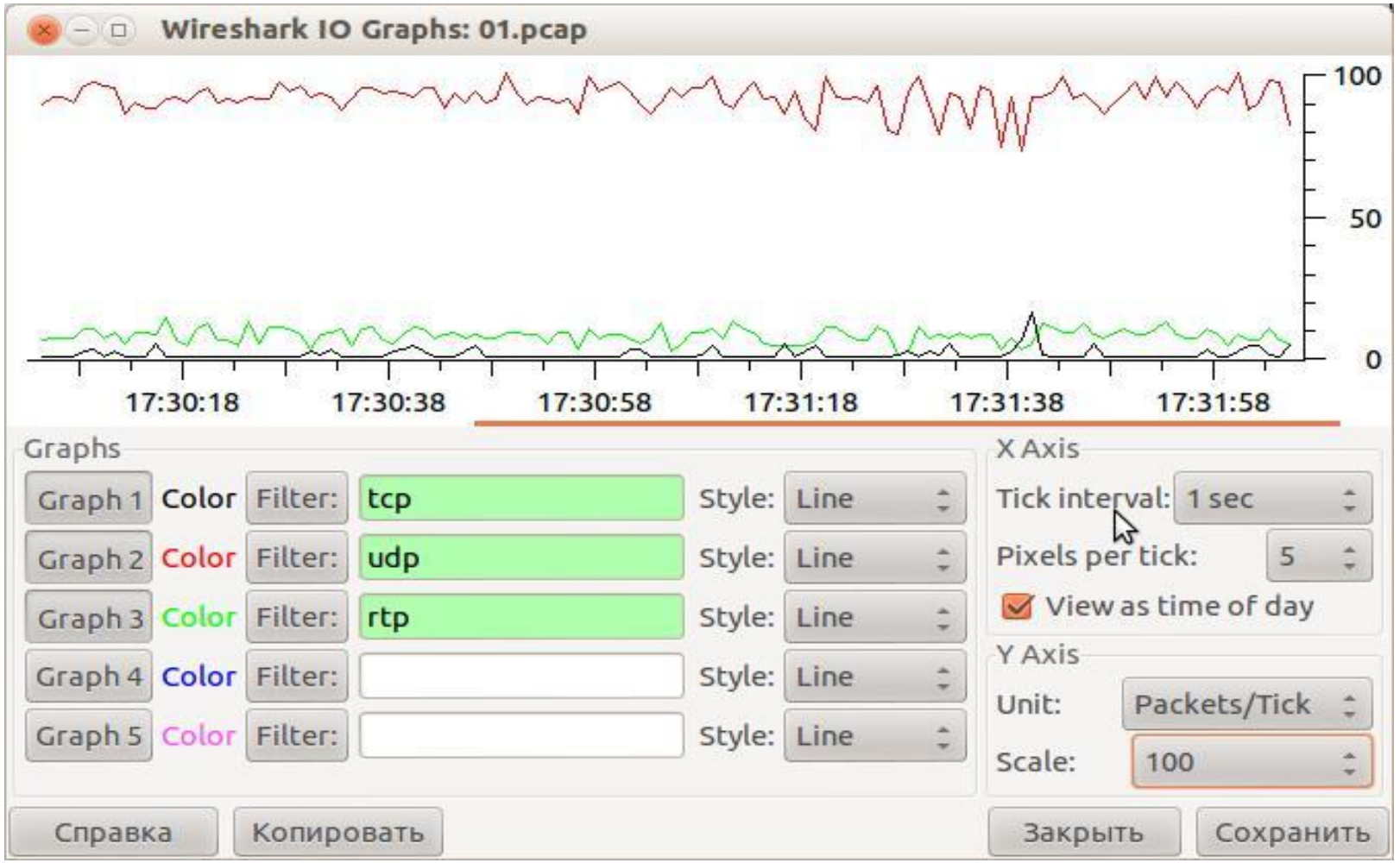
Мережевий екран



WAN (*Wide Area Network*) - глобальна мережа

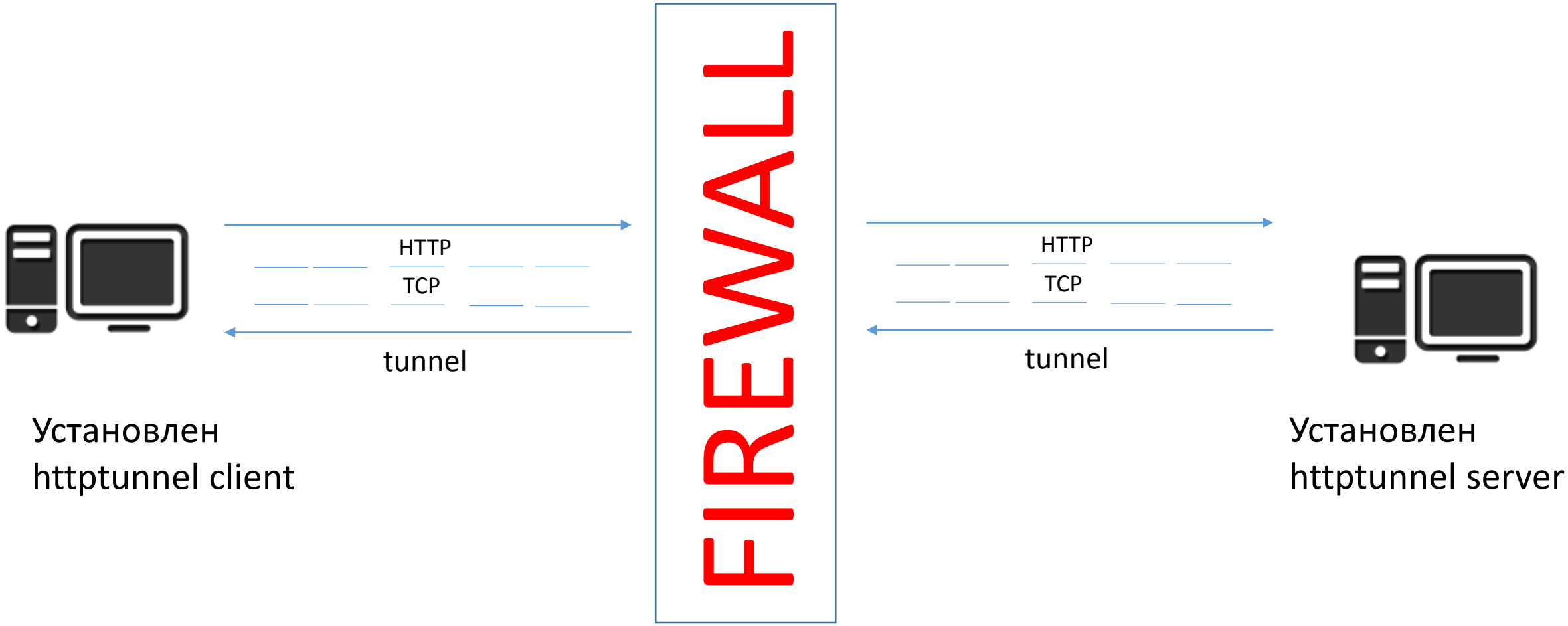
LAN (*Local Area Network*) - локальна комп‘ютерна мережа

Статистичні методи виявлення зовнішнього втручання



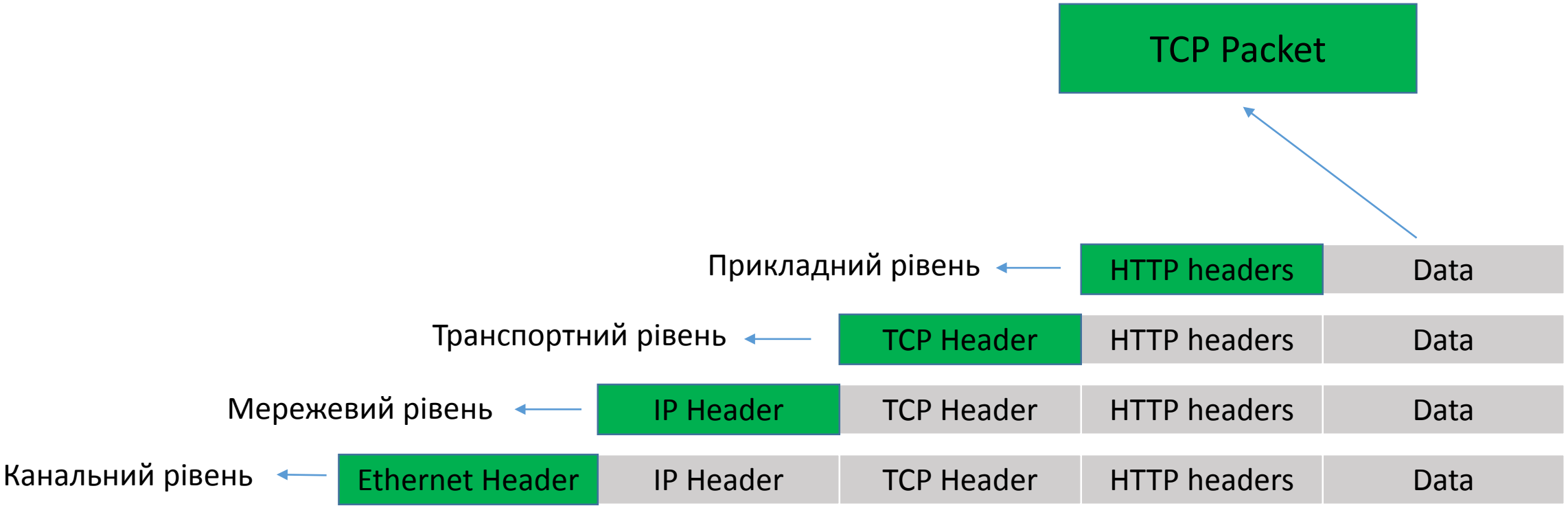
Wireshark, графік

Організація тунелів

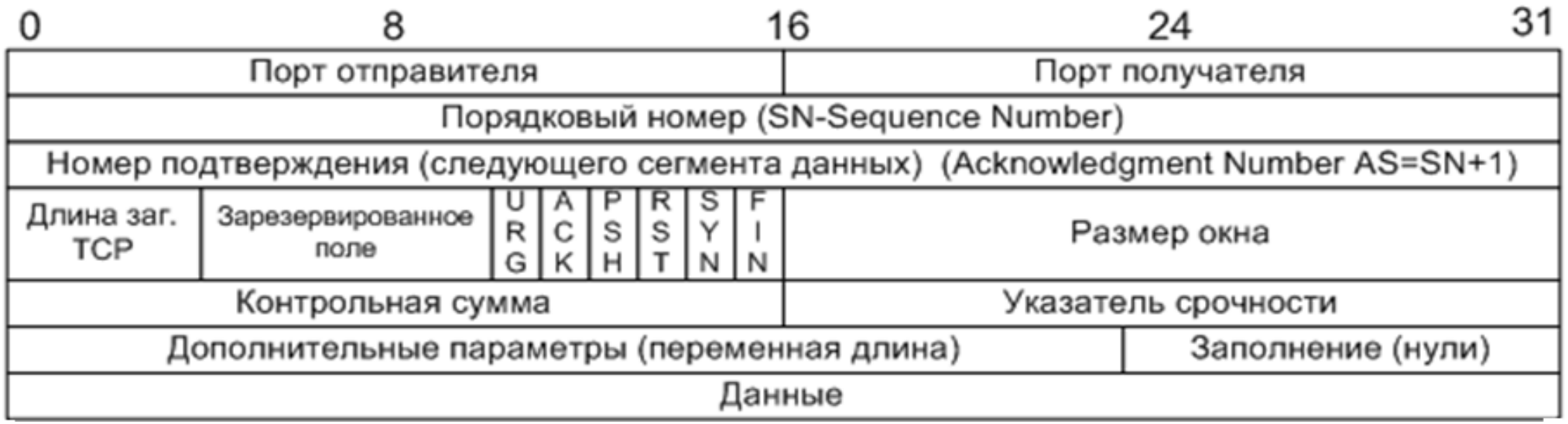


Інкапсуляція протоколів

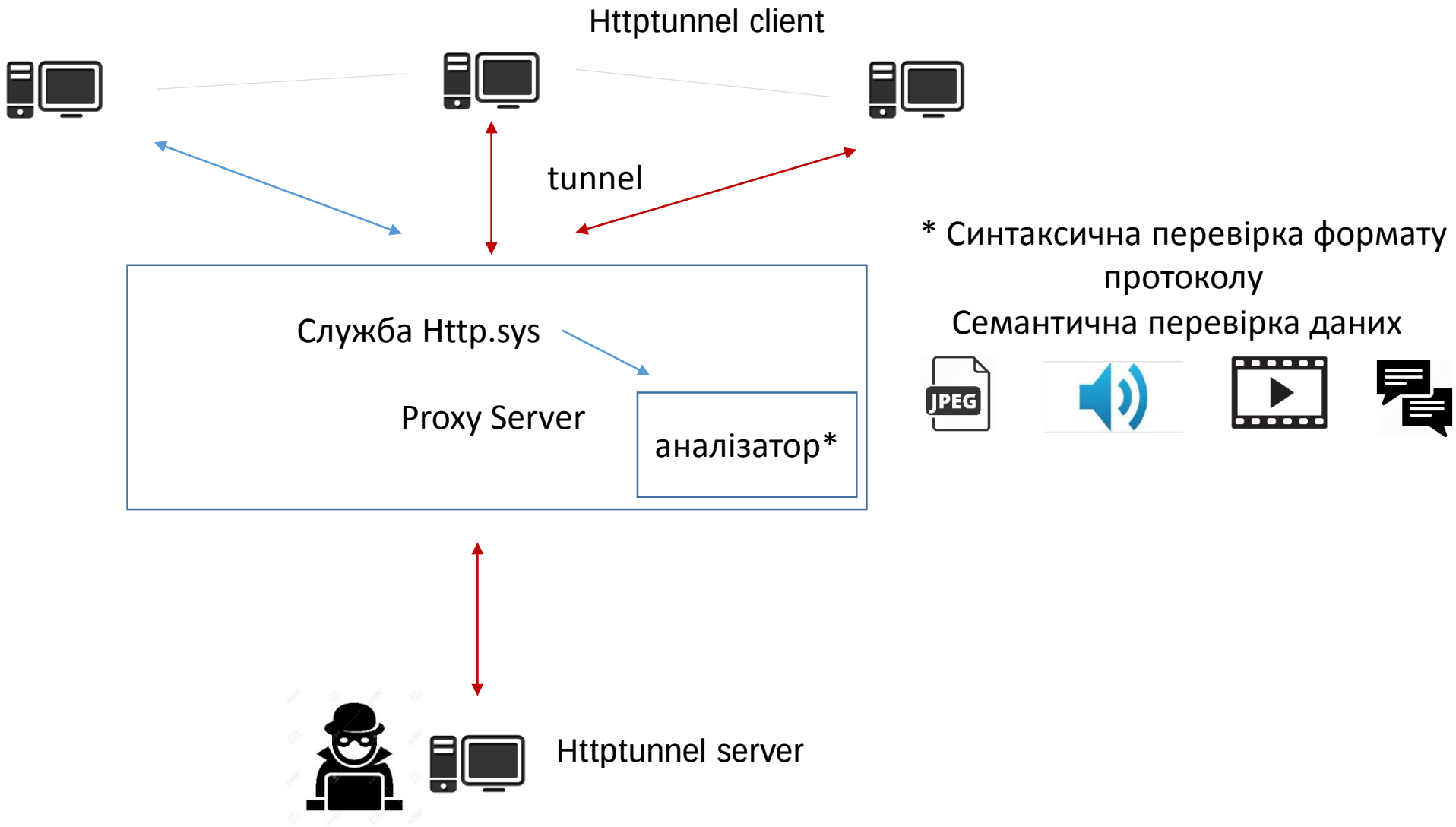
(тунелювання)



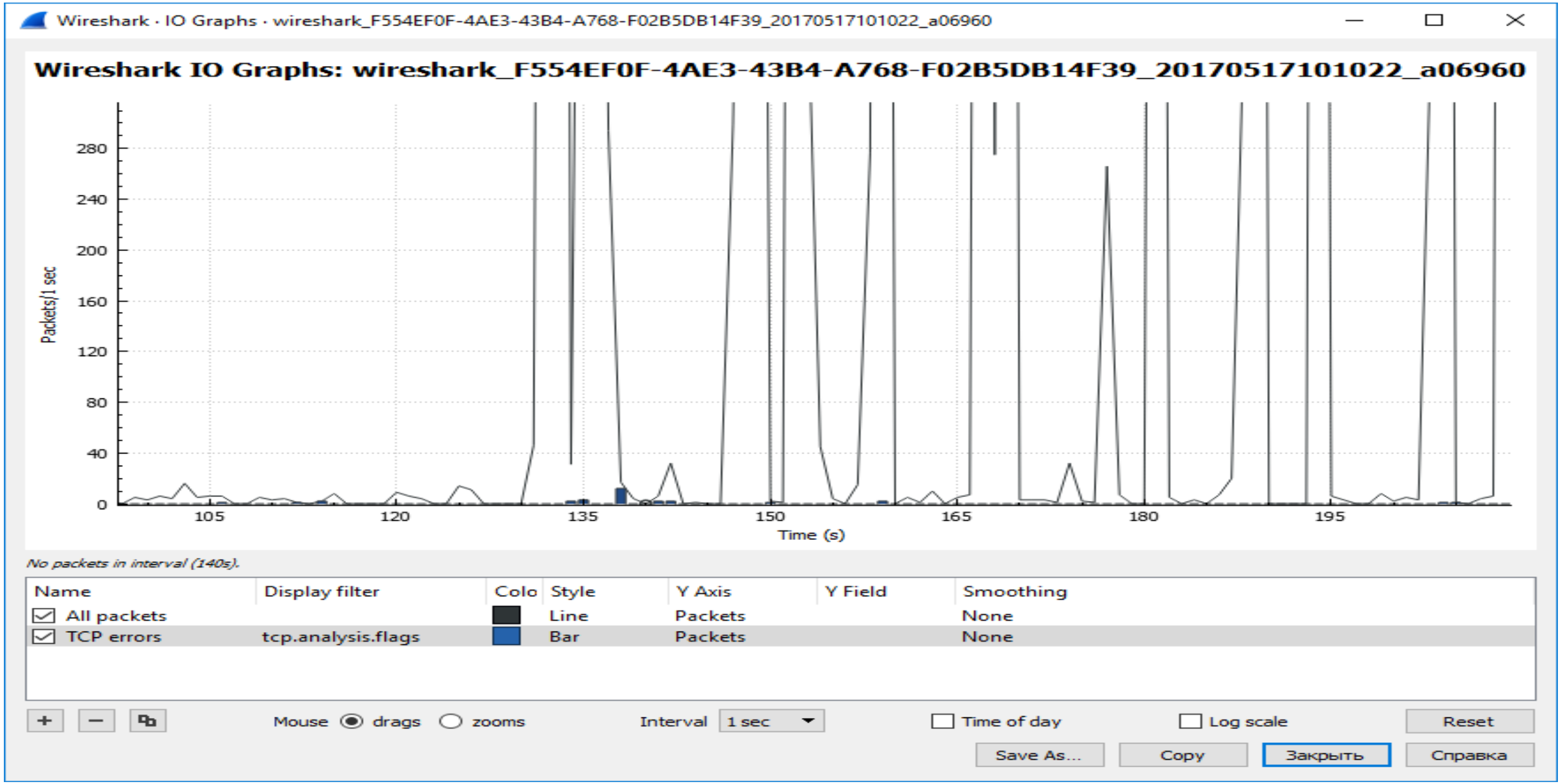
Фрагмент TCP



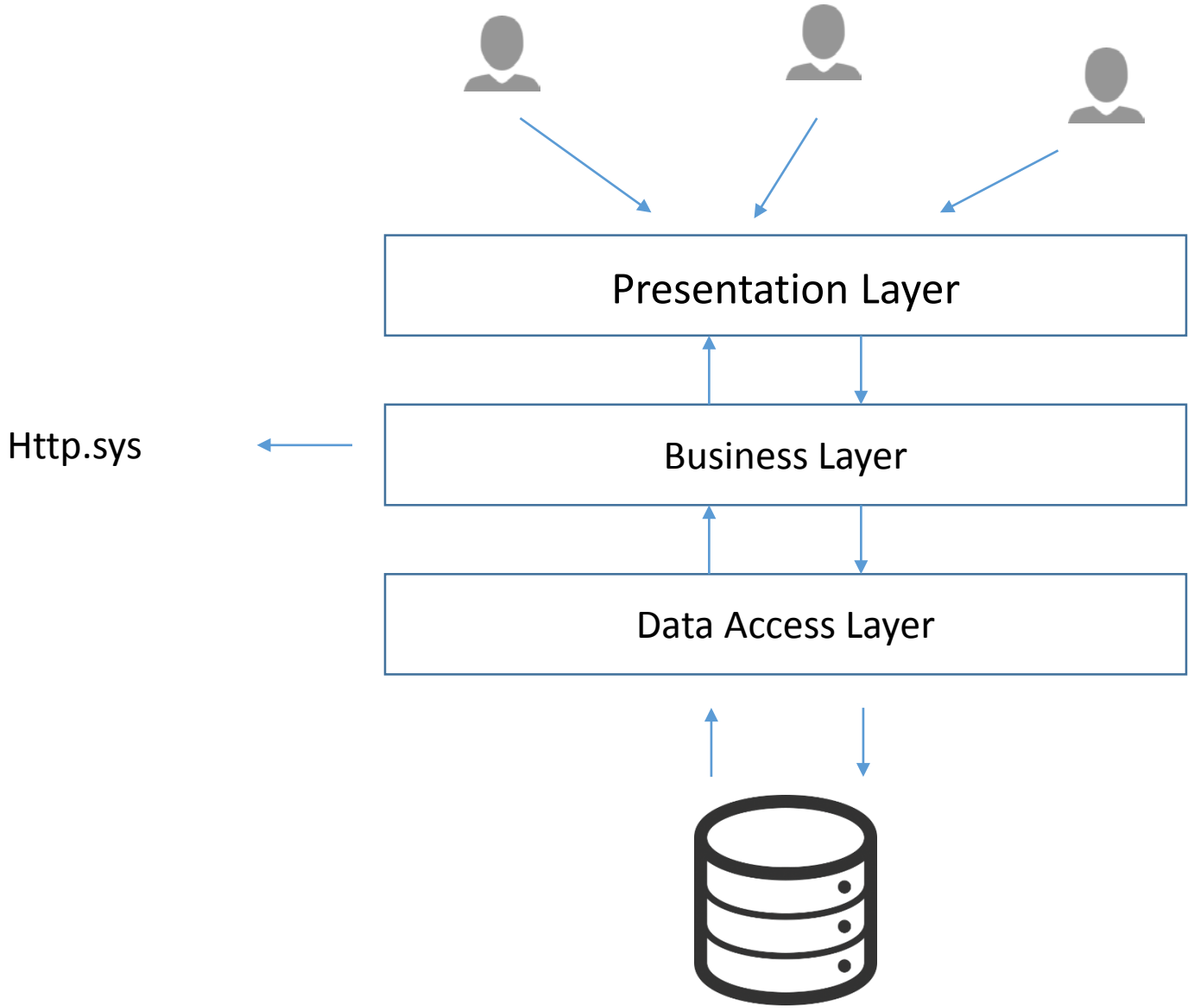
Синтаксичний аналізатор трафіку



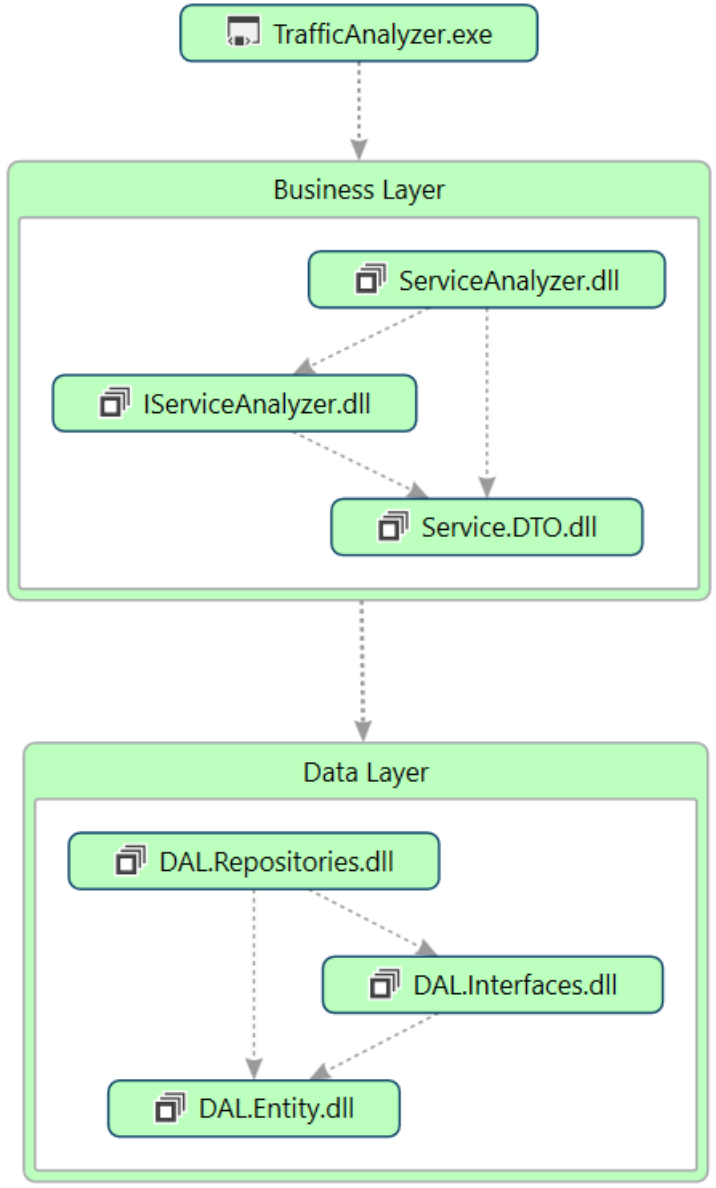
Статичний аналіз мережі при тунелюванні



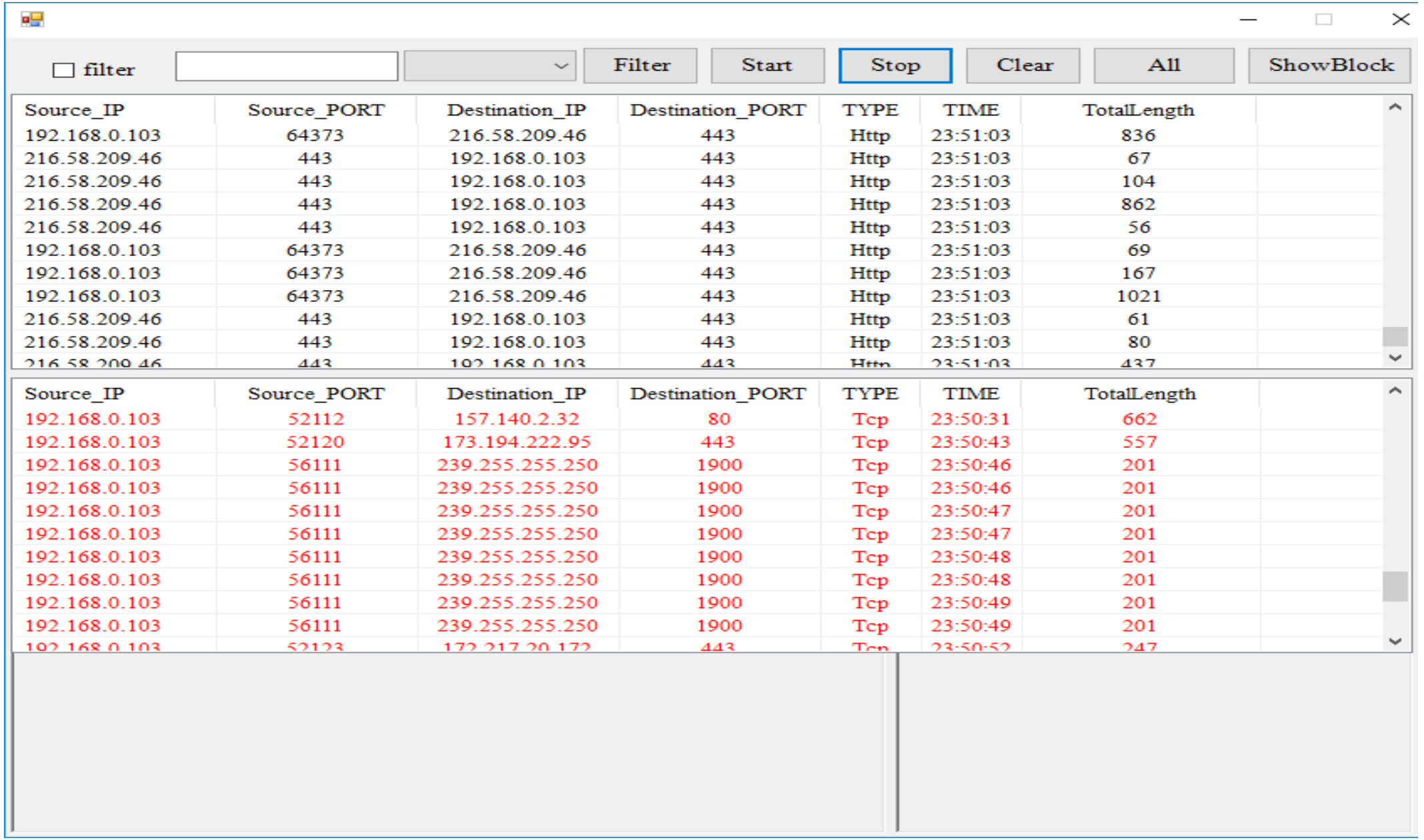
Архітектура системи



Компоненти системи



Результат виявлення тунелювання



Порівняння з існуючими рішеннями

Назва	Розпізнає тунелювання	Розпізнає тунелювання при високих навантаженнях	Легке впровадження	Висока вартість
Firewall	✗	✗	✓	✗
Stalker Traffic Analyst	✓	✗	✗	✓
Синтаксичний аналіз	✓	✓	✓	✗

Висновок

В процесі магістерської роботи були досліджені:

- засоби мережевого захисту;
- засоби обходу мережевого захисту.

та розроблені:

- алгоритм синтаксичного аналізу трафіку на основі опису протоколів;
- програмний засіб мережевого захисту за допомогую синтаксичного аналізу трафіку.

Дякую за увагу