**Лабораторна робота №6.**

**Вивчення мережевого протоколу UDP і протоколу рівня додатків DNS**

**Мета роботи:** вивчити мережевий протокол UDP і протокол рівня додатків DNS. Визначити основні етапи і особливості використання протоколів.

**Короткі теоретичні відомості**

Протокол UDP є найпростішим транспортним протоколом без гарантії доставки даних і без встановлення з'єднання. Даний протокол забезпечує мультиплексування даних між додатками за допомогою поля port а так само контроль правильності даних за допомогою поля checksum. Даний протокол використовується для обміну короткими структурованими даними в режимі "запит-відповідь" а так само для посилки широкомовних повідомлень. У порівнянні з протоколом TCP цей протокол забезпечує більшу швидкодію, оскільки не має витрат на установку і призвести до втрати з'єднання. Зручно так само застосування протоколу UDP для випадків спеціального транспорту, коли транспорт TCP з яких-небудь міркувань не влаштовує розробника. Однак слід зазначити, що механізми підтвердження і збірки потоку в цьому випадку повинні забезпечуватися додатком.

Служба доменних імен DNS є основною системною службою в мережах TCP / IP, оскільки ця служба забезпечує дозвіл символьних імен в IP адреси і навпаки. Кожна програма, що використовує мережеві функції, звертається до базової системної бібліотеці libc, частиною якої є так званий резольвер (resolver). Резольвер має свій файл конфігурації /etc/resolv.conf, в якому описані найближчі сервера імен та порядок підстановки суфіксів.

Основою DNS є уявлення про ієрархічну структуру доменного ім’я і зонах. Кожен сервер, що відповідає за ім'я, може делегувати відповідальність за подальшу частину домена іншому серверу (з адміністративної точки зору — іншій організації або людині), що дозволяє покласти відповідальність за актуальність інформації на сервери різних організацій (людей), що відповідають лише за «свою» частину доменного імені.

У мережі повинно бути як мінімум два сервера імен для забезпечення безперебійного дозволу імен. Звернення резольвера відбувається спочатку до першого сервера, і якщо відповідь не отримана протягом короткого часу, до другого. Якщо сервер не може самостійно відпрацювати запит, він звертається до серверів домену кореневого домена "." і здійснює пошук сервера, здатного обробити запит. Отримана відповідь перенаправляється клієнту і кешується на сервері для прискорення наступних відповідей.

**Хід роботи**

1. Для визначення адреси DNS, була використана команда ipconfig /all, DNS сервер що використовується на ПК зображено на рисунку 1.

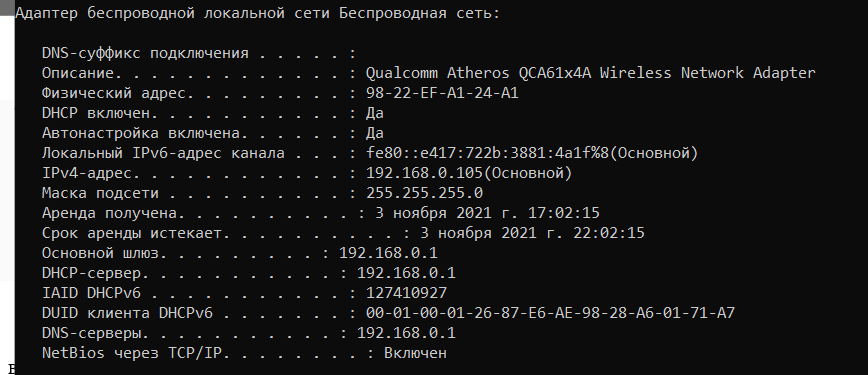


Рисунок 1 - Адреса DNS серверу

Як адресу хоста www використано адресу домену www.ukr.net, для визначення ip адреси серверу була використана утиліта nslookup. Результат виконання зображено на рисунку 2.

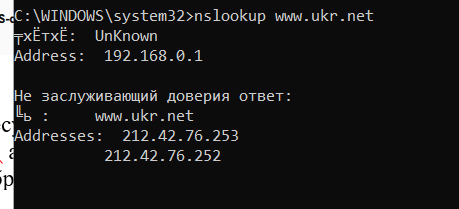


Рисунок 2 – Результат виконання команди nslookup

Фільтр буде мати вигляд (ip.src == 192.168.0.105 && (ip.dst == 192.168.0.1 )) || (ip.src == 192.168.0.105 && ip.dst == 212.42.76.253) || (ip.src == 192.168.0.1 && ip.dst == 192.168.0.105)

2. Результат захвату пакетів під час виконання команди ping до DNS серверу та серверу ukr.net зображено на рисунку 3.

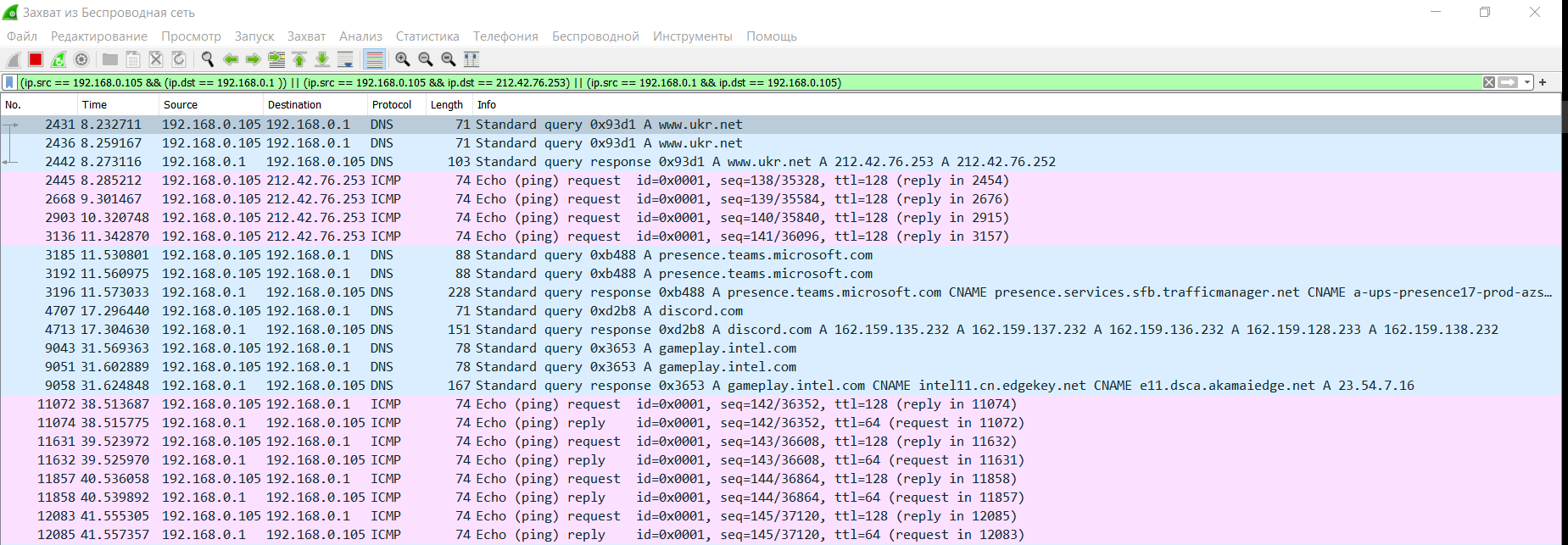


Рисунок 3 - Результат захвату пакетів під час виконання команди ping

4. Результат захвату пакетів під час перегляду Web сервісу зображено на рисунку 4.

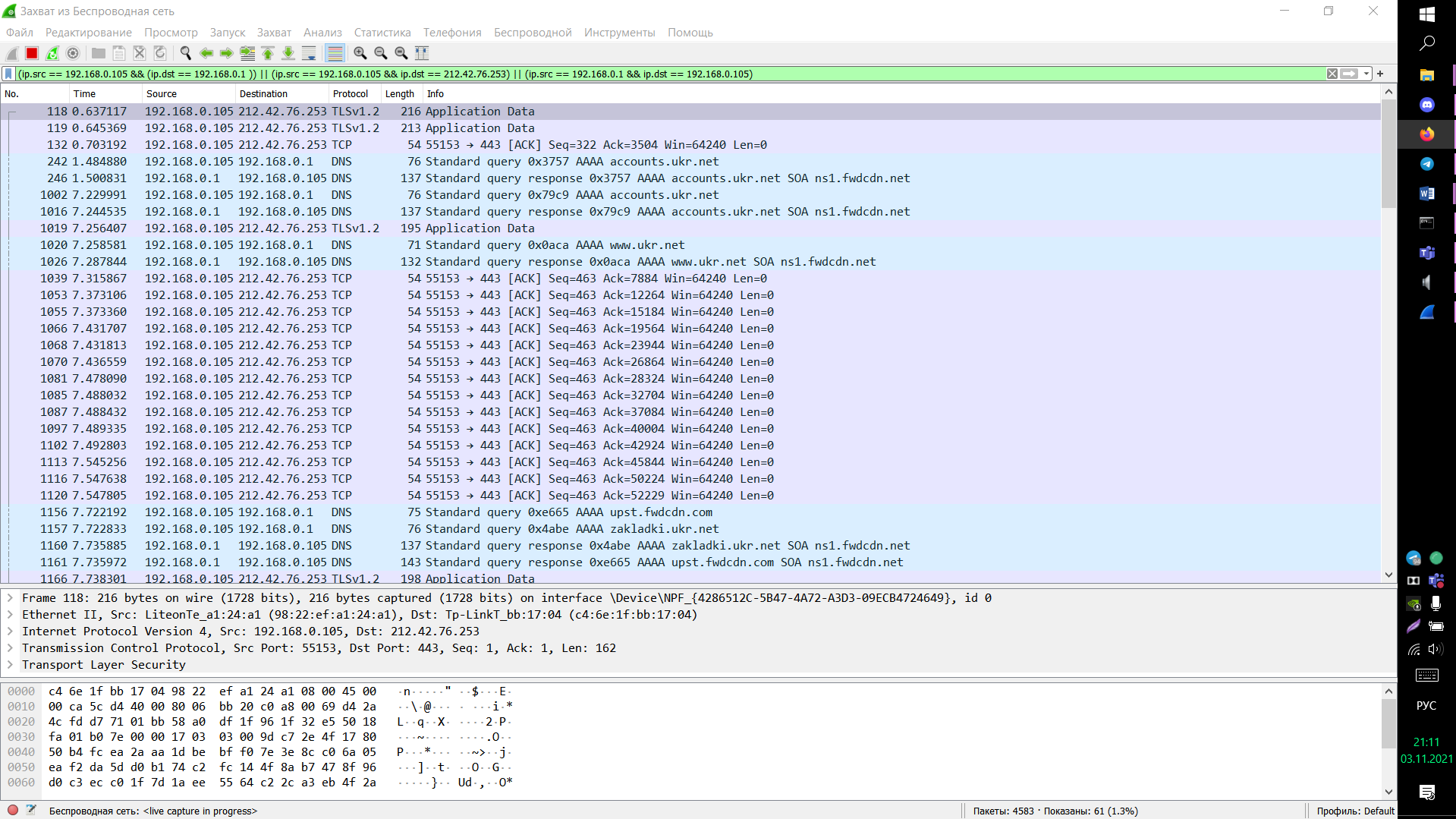


Рисунок 4 - Результат захвату пакетів під час перегляду web

Вміст файлу розбору команди tcpdump зображено на рисунку 5.

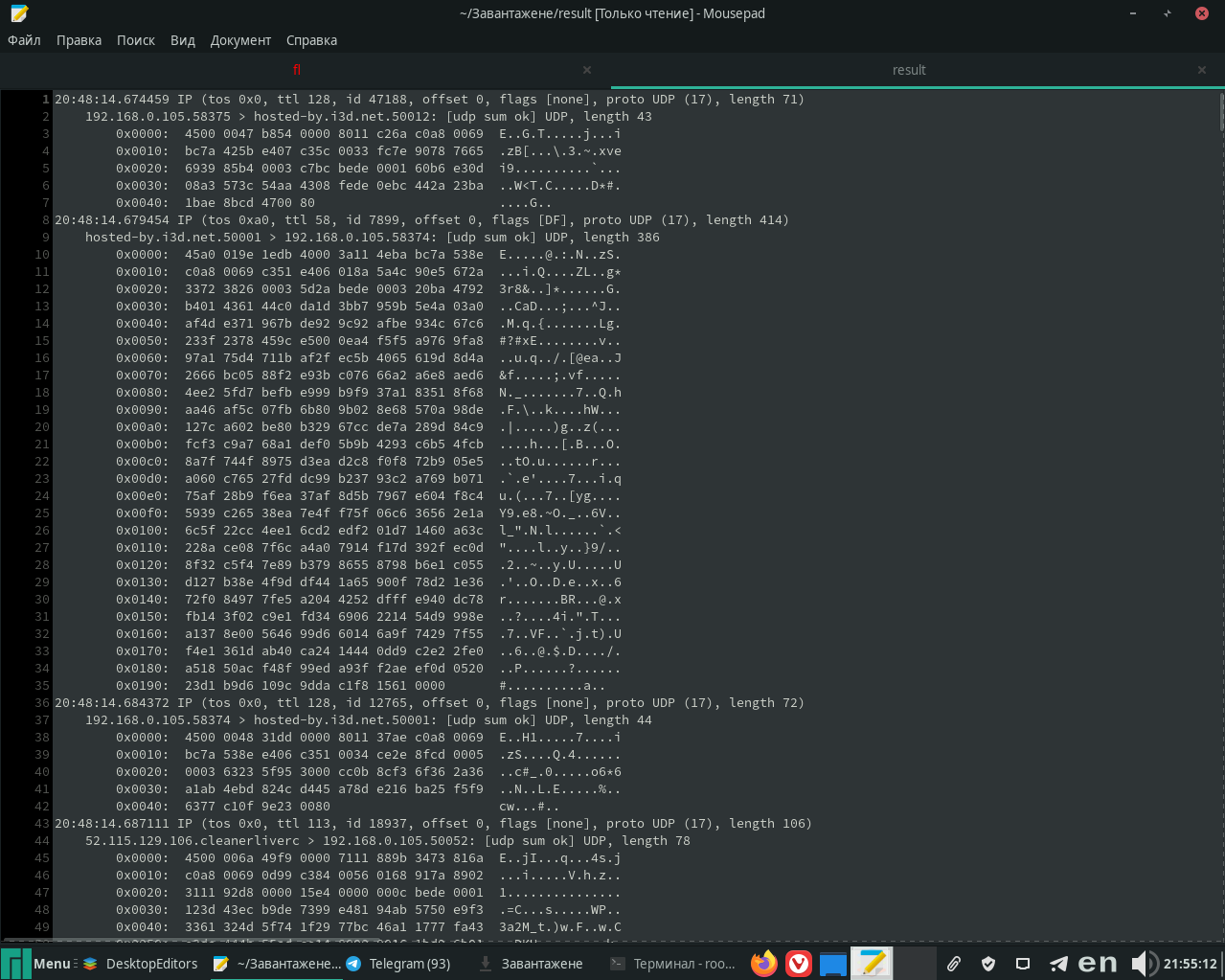


Рисунок 5 - Вміст файлу розбору команди tcpdump

На початку виконується DNS звертання до сайту? запит до DNS серверу, в данному прикладі це маршрутизатор з адресою 192.168.0.1, маршрутизатор виконує запит на DNS сервер провайдера та повертає адресу сервера, потім за допомогою протокола TCP виконується з’єднання з сервером додатку ukr.net.

9. www.yahoo.com має декілька ip адрес серверів, тому фільтр буде мати вигляд - (ip.src == 192.168.0.105 && ip.dst == 192.168.0.1) || (ip.src == 192.168.0.105 && (ip.dst == 87.248.100.216 || ip.dst == 87.248.100.215)) || (ip.src == 192.168.0.1 && ip.dst ==192.168.0.105. Результат захвату аналізатором Wireshark зображено на рисунку 6. Вміст файлу розбору команди tcpdump зображено на рисунку 7.

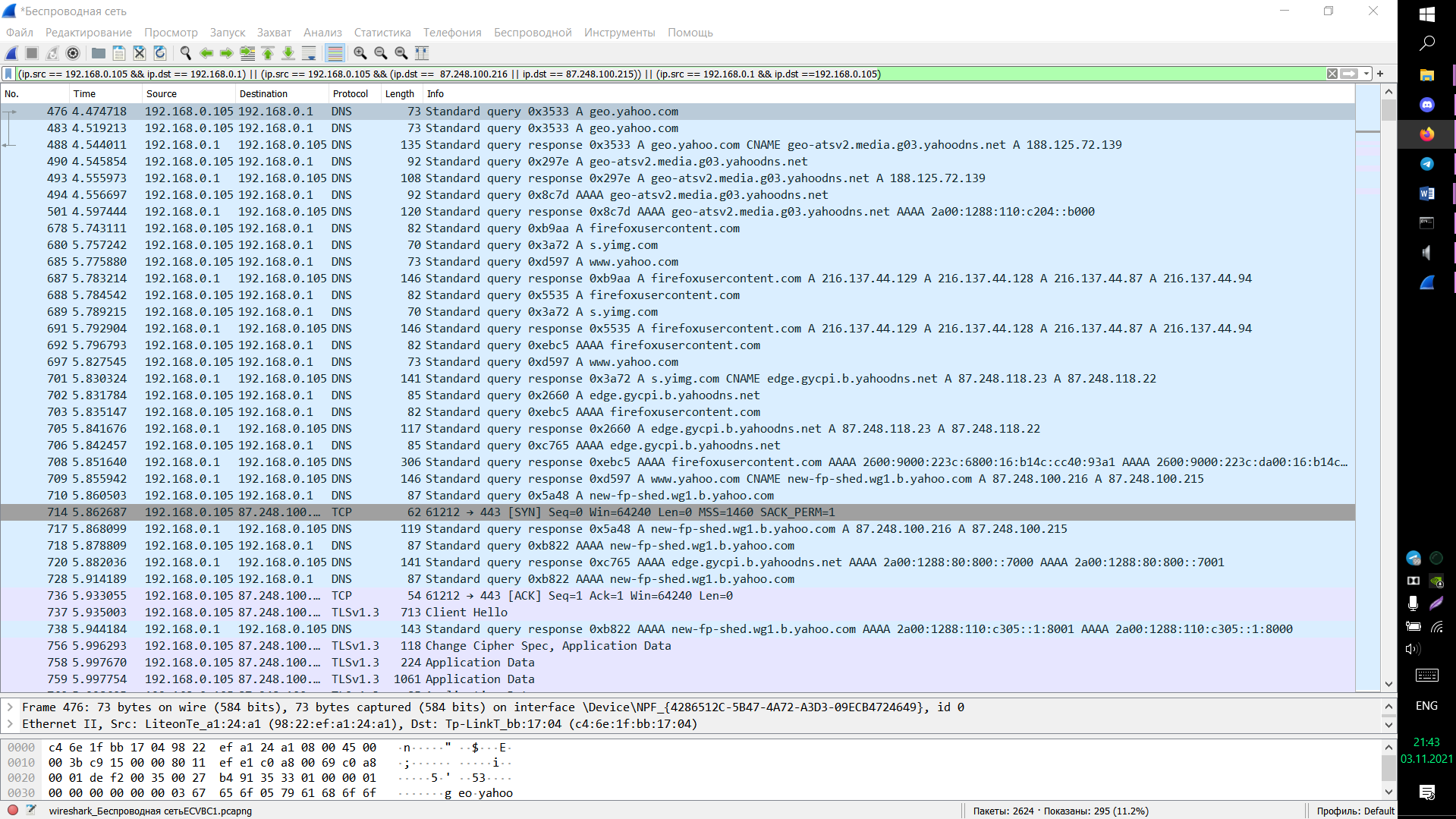


Рисунок 6 - Результат захвату аналізатором Wireshark

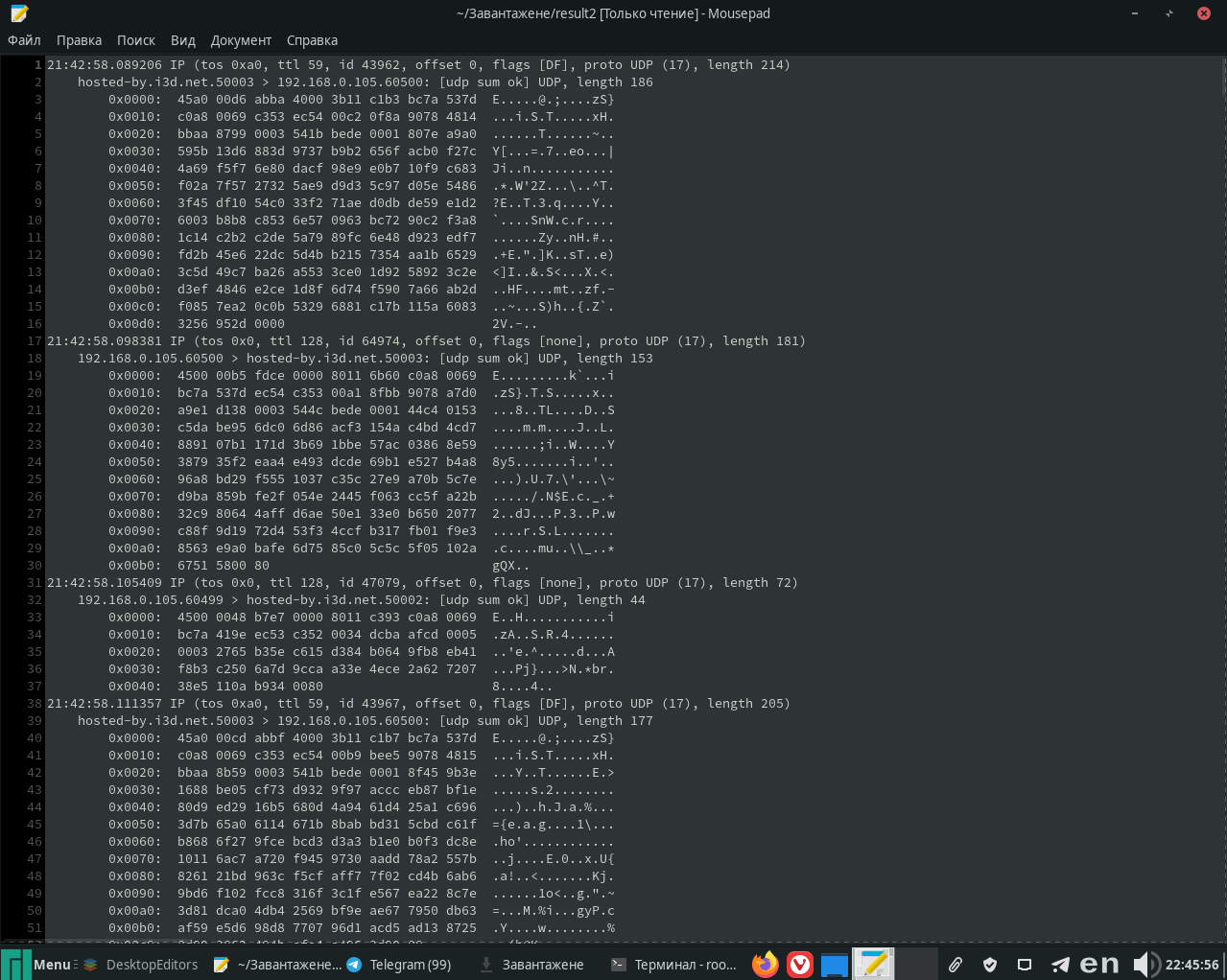


Рисунок 7 - Вміст файлу розбору команди tcpdump

Для визначення доменного імені адреси 193.193.193.100 використана команда nslookup, домен - ns.lucky.net. Оскільки веб ресурс недоступний, то використана команда ping. Результат захвату аналізатором Wireshark зображено на рисунку 8. Вміст файлу розбору команди tcpdump зображено на рисунку 9.

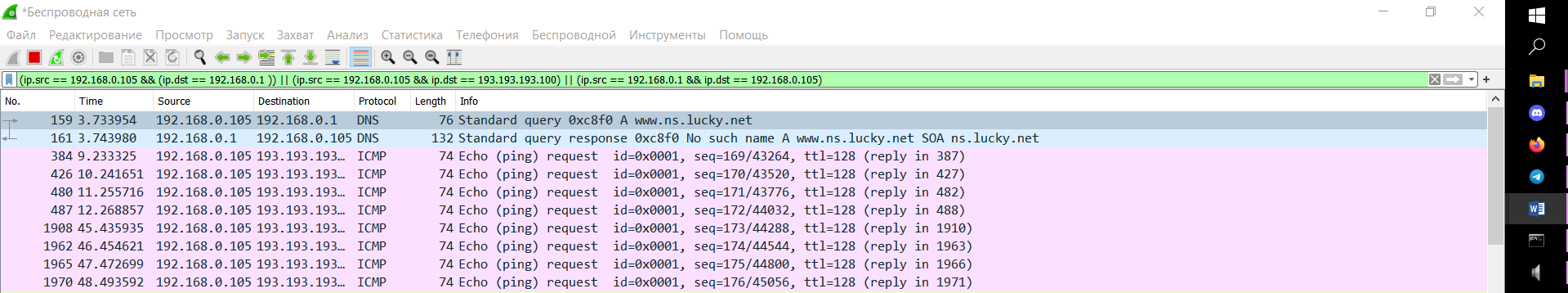


Рисунок 8 - Результат захвату аналізатором Wireshark адреси 193.193.193.100

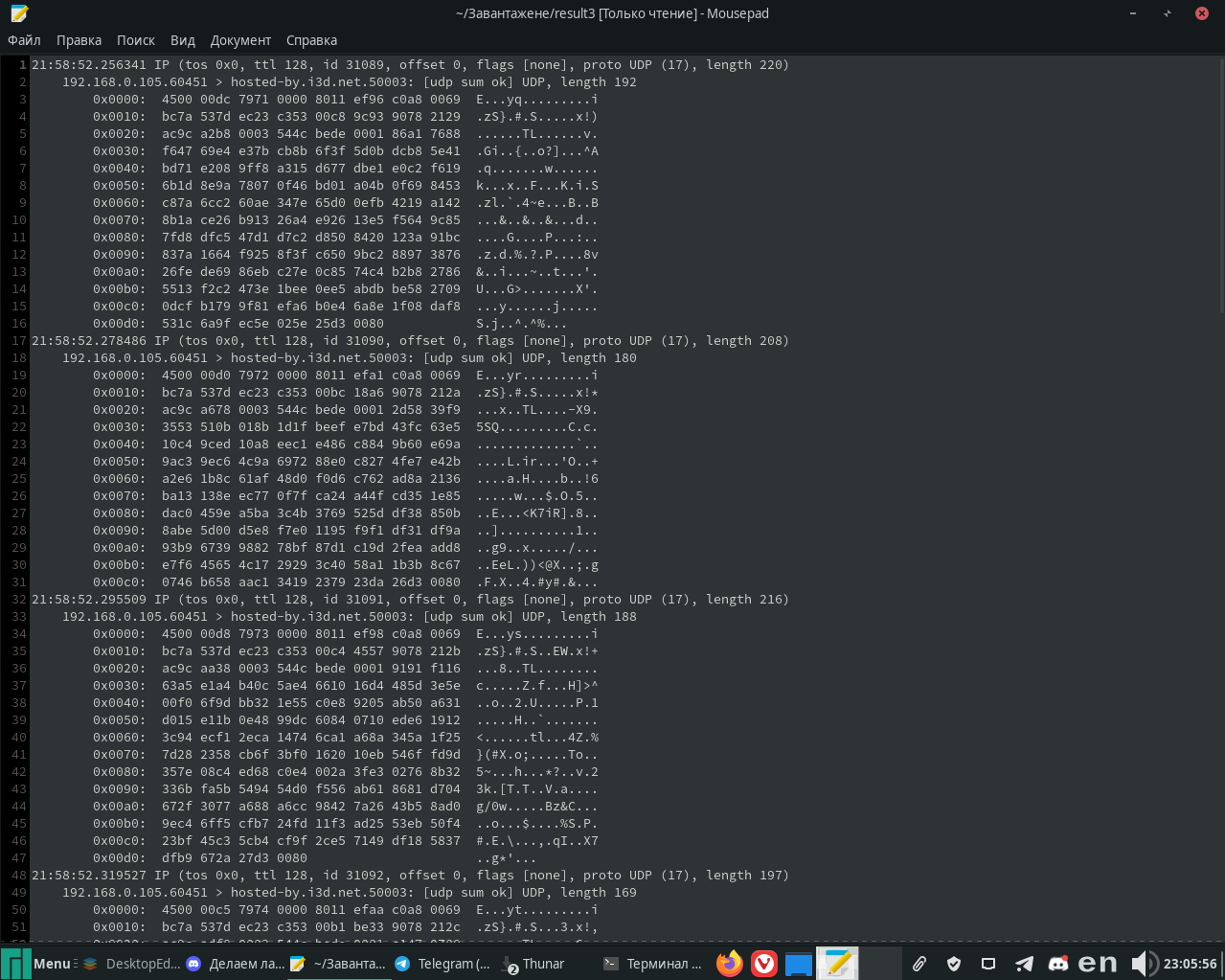


Рисунок 9 - Вміст файлу розбору команди tcpdump

**Висновок**: на даній лабораторній роботі я вивчив мережевий протокол UDP і протокол рівня додатків DNS. Визначив основні етапи і особливості використання протоколів. Виконав захоплення пакетів за допомогою Wireshark.