**Лабораторна робота №5.**

**Вивчення мережевого протоколу TCP і протоколу рівня додатків telnet**

**Мета роботи:** Вивчити мережевий протокол ТСР і протокол додатків telnet. Визначити основні етапи і особливості використання протоколів.

**Короткі теоретичні відомості**

Протокол TCP є транспортним протоколом з гарантованою доставкою даних, з встановленням з'єднання і повторною втрачених сегментів.

Встановлення з'єднання відбувається за допомогою механізму т.зв. триразового рукостискання (three way handshake).

Хост А, ініціатор з'єднання, посилає сегмент без даних з встановленим прапором SYN. Ініціює з'єднання програма - клієнт. Порт призначення визначається жорстко або як добре відомий сервіс (Well Known Serviсe), наприклад web-сервіс зазвичай має порт 80, або задається користувачем. Порт джерела зазвичай виділяється системою з пулу вільних НЕ привілейованих портів (> 1023).

У відповідь хост В посилає сегмент без даних з встановленими прапорами SYN, ACK. При цьому, в залежності від режиму роботи серверного сокета, можлива заміна фіксованого порту на динамічний в якості вихідного.

Хост А, прийнявши описаний вище пакет, сигналізує про готовність до обміну даними, посилаючи сегмент без даних з встановленим прапором ACK. Після цього сокети готові до двонаправленого обміну даними.

Розрив з'єднання відбувається аналогічно з використанням прапора FIN.

Протокол TELNET є протоколом рівня додатків, призначеним для віддаленого доступу по мережі до текстового терміналу. При ініціалізації з'єднання надсилаються команди і клієнтом, і сервером, що забезпечують узгодження можливостей для користувача терміналу і установку необхідних змінних оточення на сервері.

**Хід роботи**

1. Для встановлення сервісу телнет на обох машинах було увімкнено програмний компонент windows Telnet, на другій машині була встановлена утиліта hk-telnet-server для запуску сервера Telnet, також було створено профіль користувача з логіном та паролем - admin. Результат запуску сервера зображено на рисунку 1.

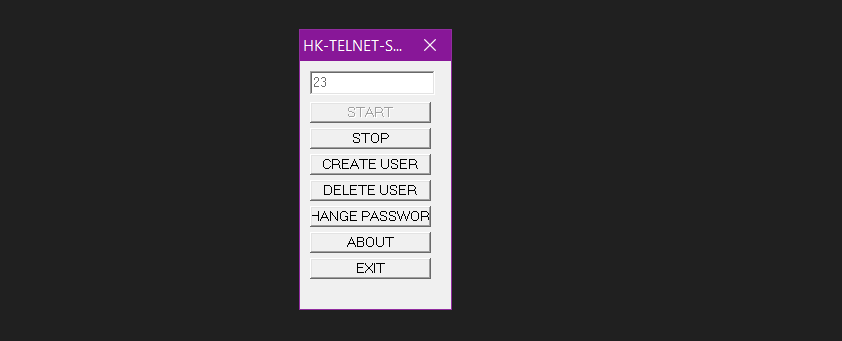


Рисунок 1 - Результат запуску сервера

2. Термінальний доступ до хосту зображено на рисунку 2. Як приклад виконана команда dir диску D.

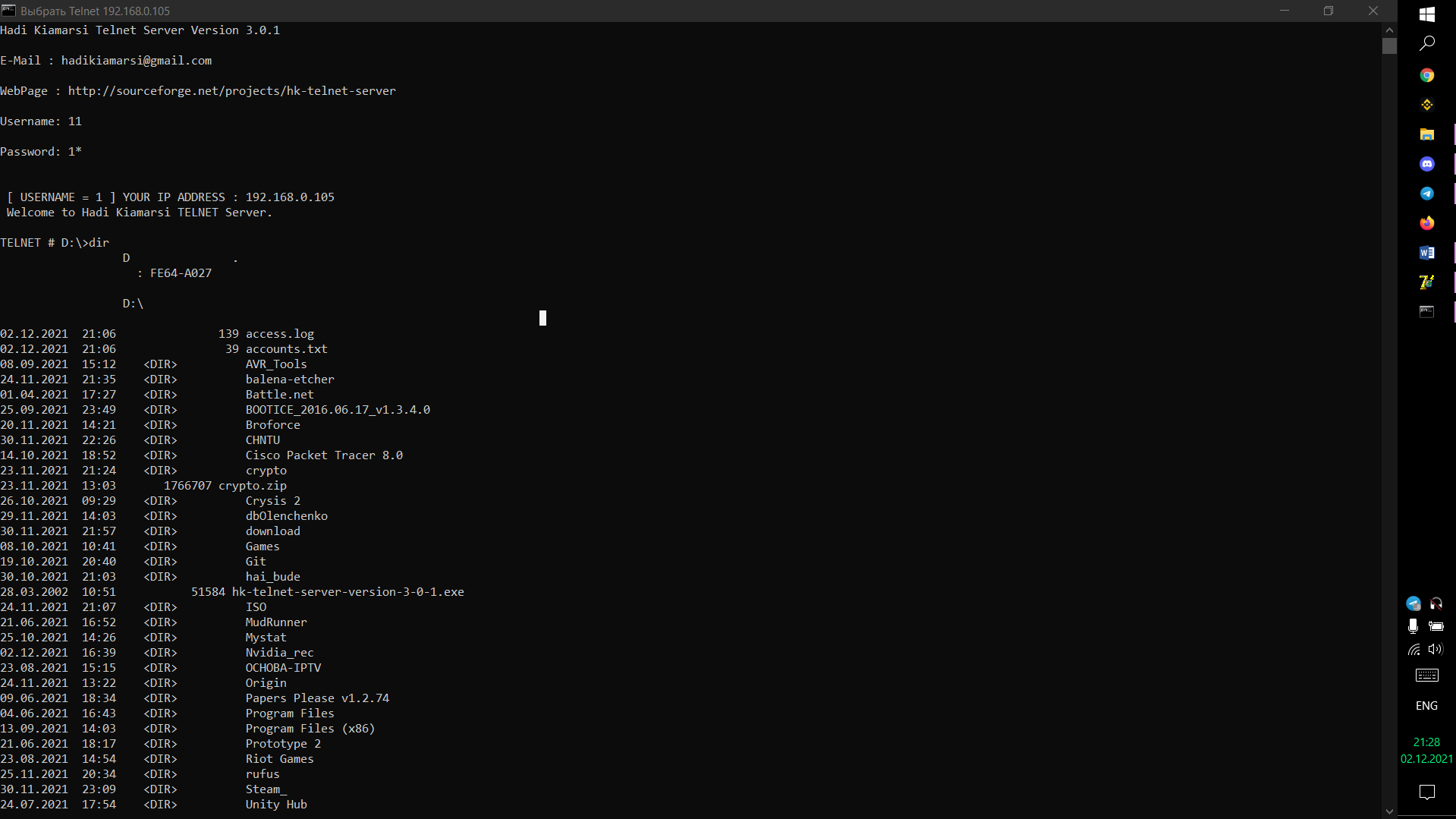


Рисунок 2 - Термінальний доступ до хосту

3. Команда WireShark буде мати вигляд (ip.src == 192.168.0.105 && ip.dst == 192.168.0.106) || (ip.src == 192.168.0.106 && ip.dst == 192.168.0.105)

4. Результат захвату пакетів сесії зображено на рисунку 3.

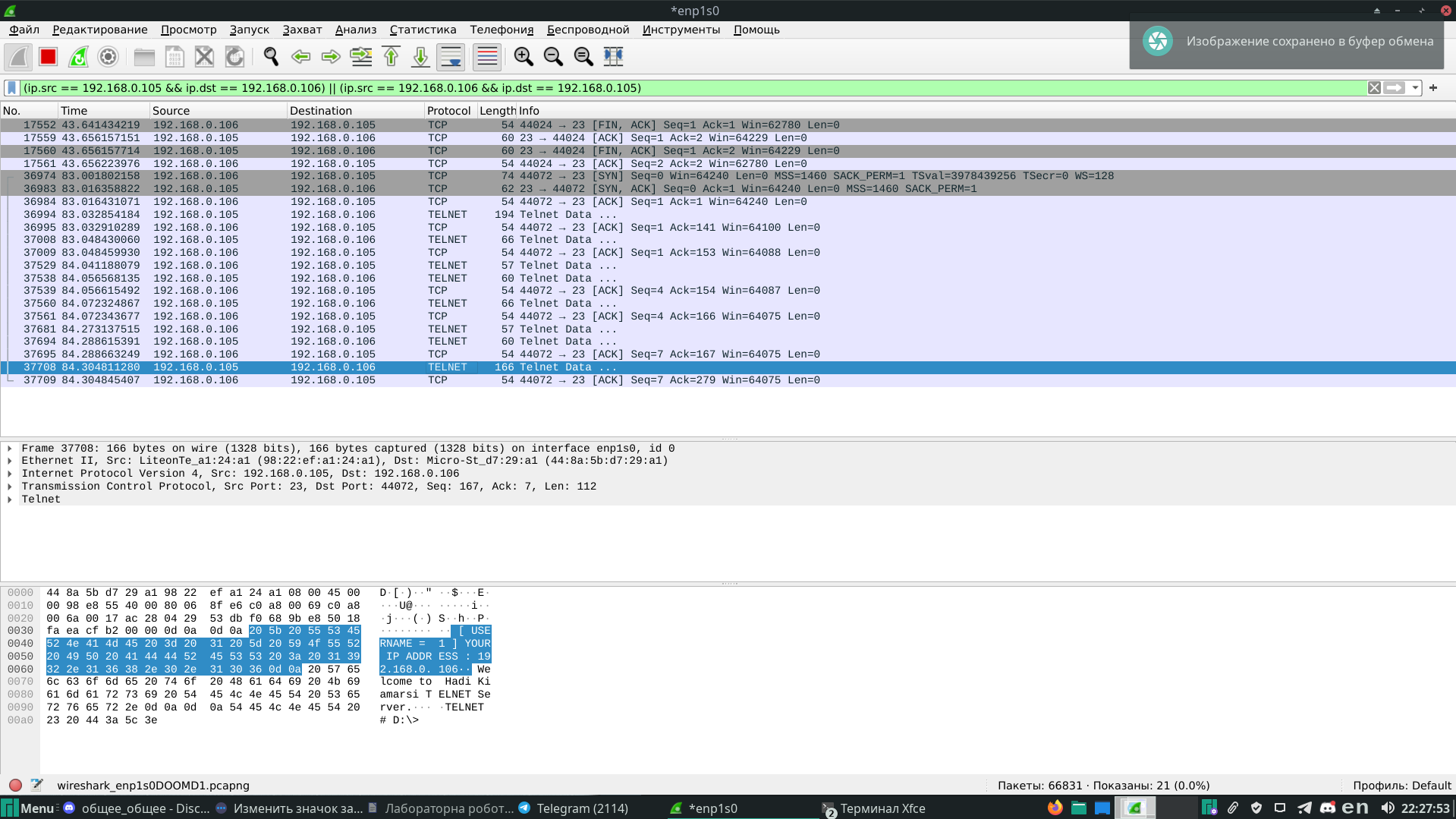


Рисунок 3 - Результат захвату пакетів

5. Результат розбору файлу утилітою tcpdump зображено на рисунку 4.

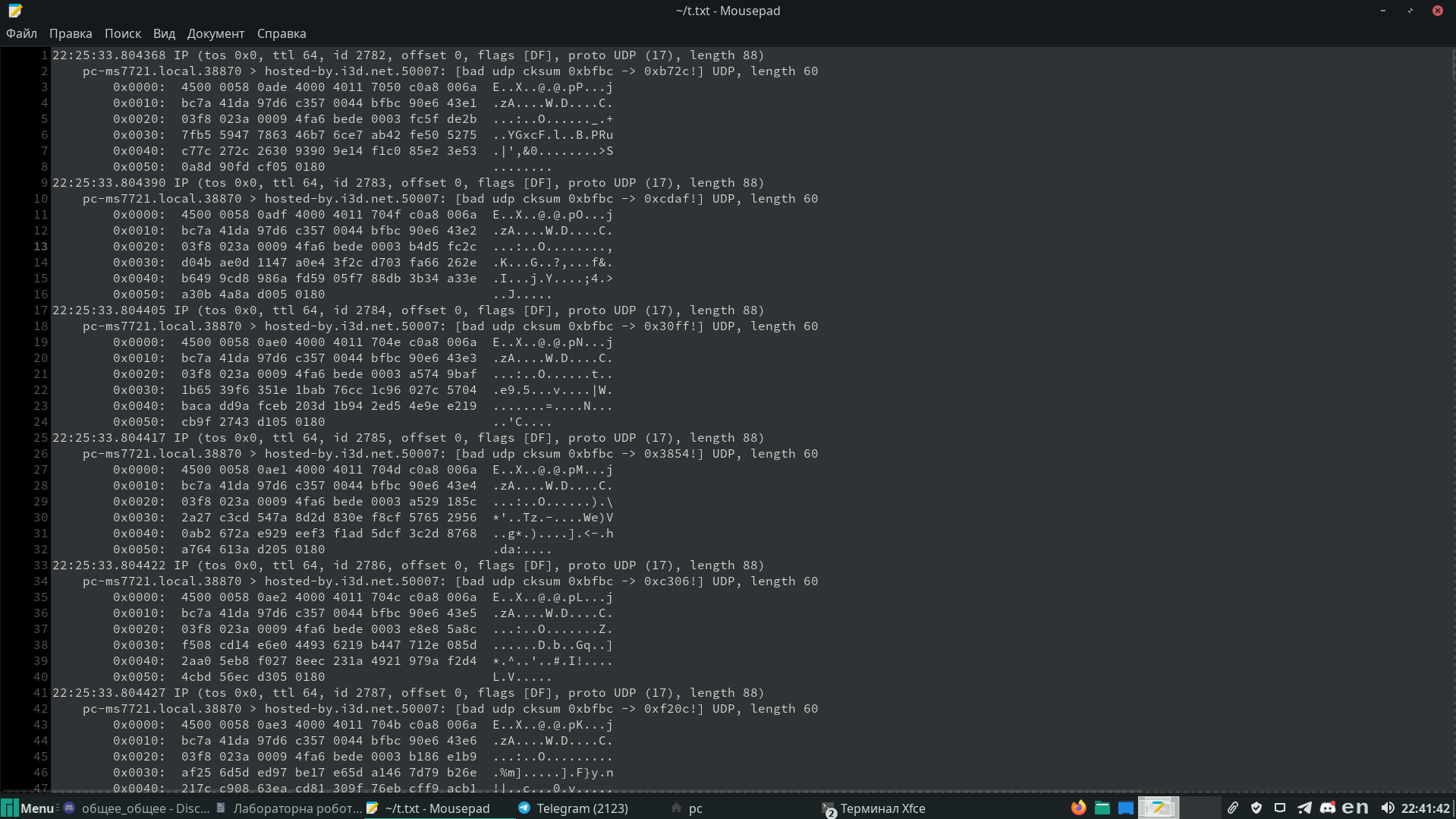


Рисунок 4 - Результат розбору файлу утилітою tcpdump

6. Початок з’єднання з сервером телнет зображено на рисунку 5. На початку запиту клієнт відправляє сегмент з встановленим прапором SYN та вказуючи найперше значення номера послідовності, яке використовується для відслідковування потоку даних від клієнта до сервера. Сегмент з встановленим прапором SYN зображено на рисунку 6.

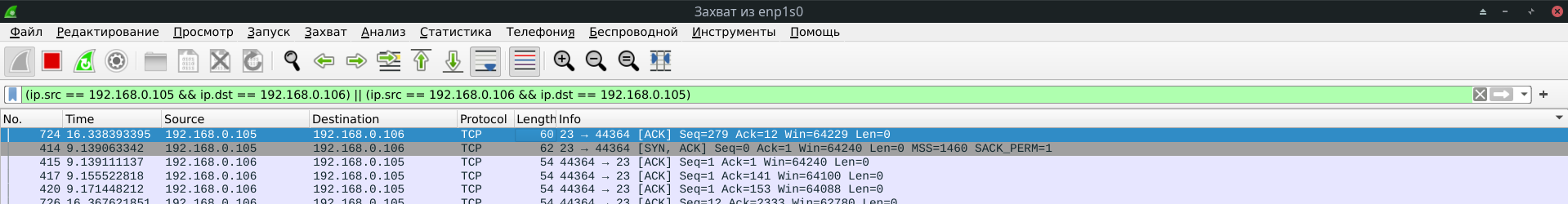


Рисунок 5 - З’єднання з сервером телнет

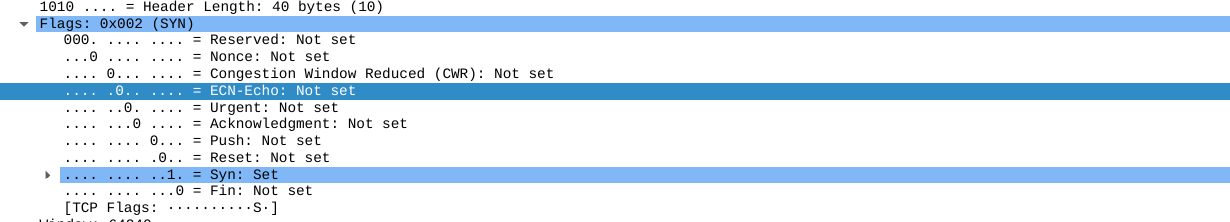


Рисунок 6 - Сегмент з встановленим прапором SYN

Після отримання сегмента від клієнта сервер повертає сегмент клієнту з встановленим прапором ACK, що вказує що поле номеру підтвердження задіяно. Сегмент з встановленими прапорами SYN та ACK зображено на рисунку 7. Після цього клієнт відповідає серверу сегментом з встановленим прапором ACK і після цього фактично з’єднання установлено.



Рисунок 7 - Сегмент з встановленими прапорами SYN та ACK

При завершенні сеансу зв’язку клієнт надсилає серверу сегмент з встановленим прапорами FIN та ACK, сервер повертає сегмент з прапорами FIN та ACK, прапор FIN повідомляє що всі пакети були відправлені і з’єднання можна завершити. Сегмент з встановленими прапорами FIN та ACK зображено на рисунку 8.

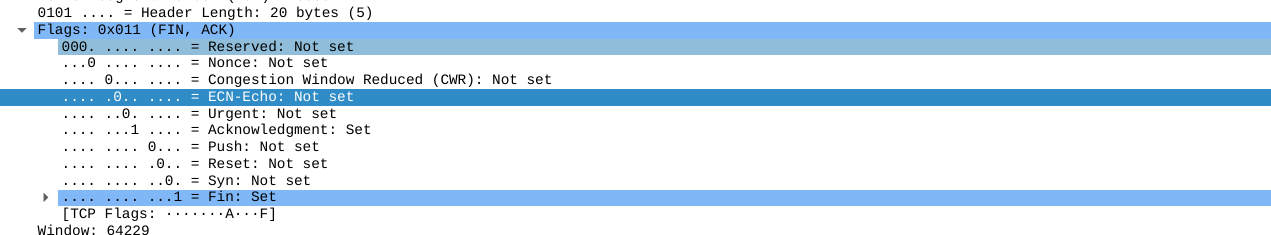


Рисунок 8 - Сегмент з встановленими прапорами FIN та ACK

Оскільки протокол Telnet не використовує шифрування пакетів, аналізатором можна побачити дані логіну та паролю. Логін та пароль зображені на рисунку 9, вони виділені червоним.

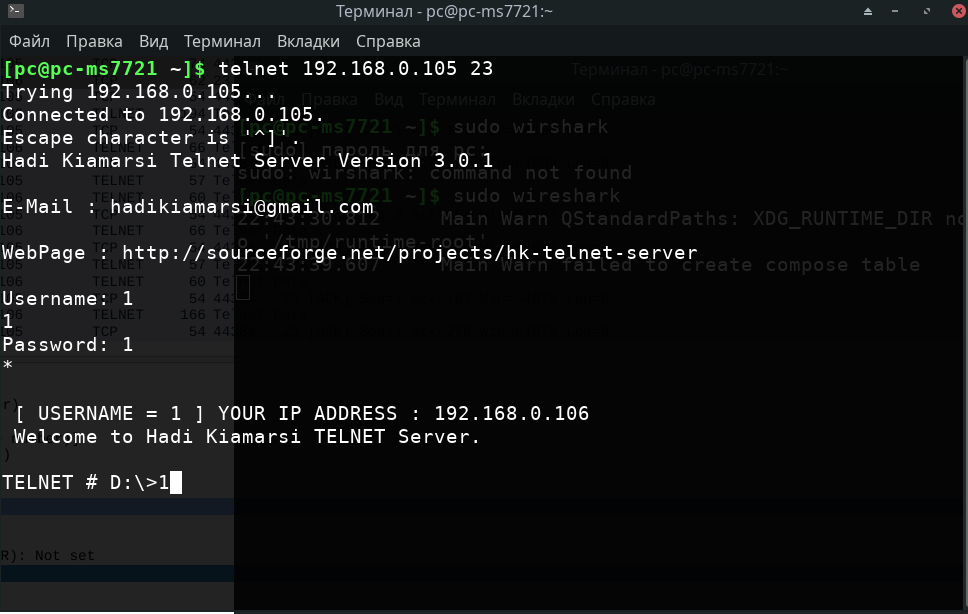


Рисунок 9 – Дані логіну та паролю для входу

7. На початку пакета даних йде заголовок протоколу Ethernet, заголовок зображений на рисунку 10.

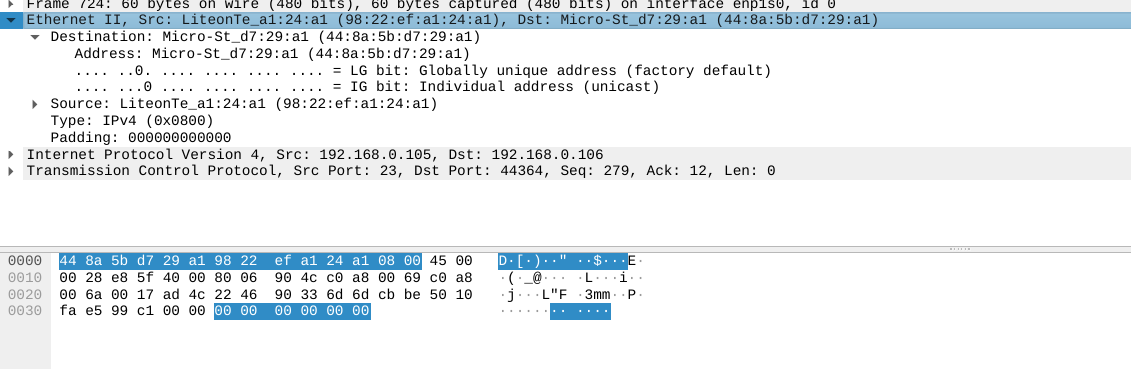


Рисунок 10 - Заголовок протоколу Ethernet

Потім йде заголовок протоколу IPv4, заголовок зображений на рисунку 11.

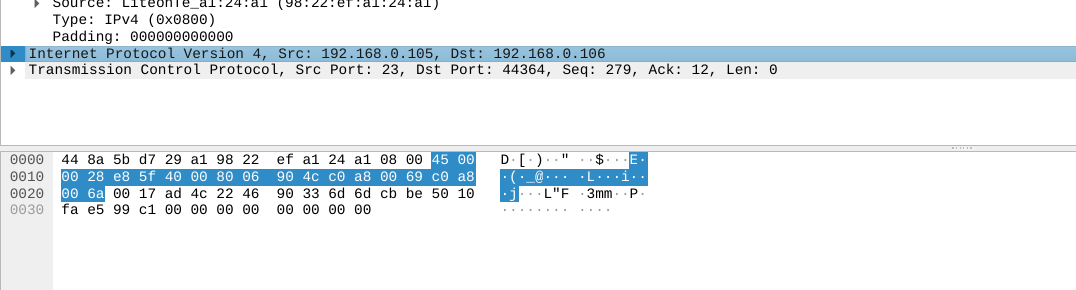


Рисунок 11 - Заголовок протоколу IPv4

Заголовок транспортного рівня зображений на рисунку 12

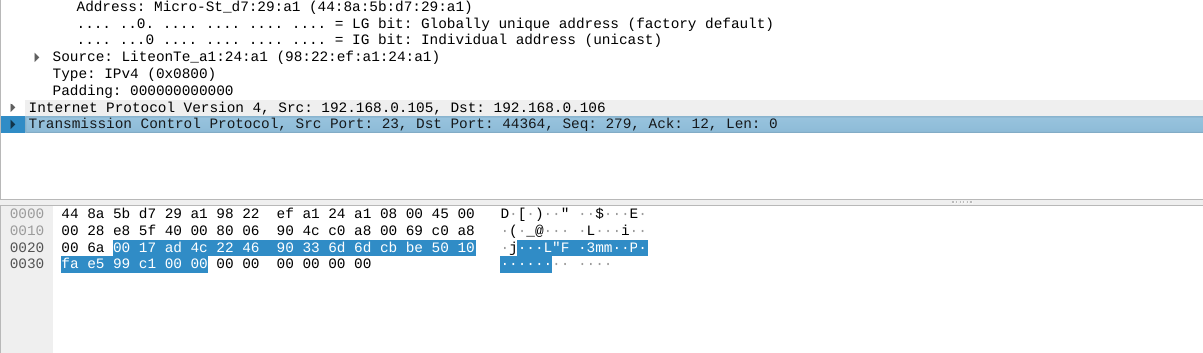


Рисунок 12- Заголовок протоколу TCP

В кінці, йдуть дані прикладного протоколу Telnet, що зображені на рисунку 13.

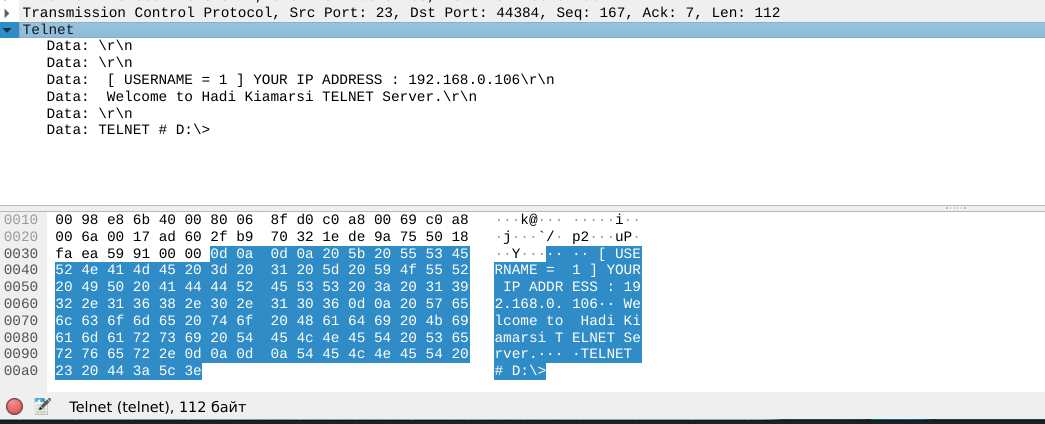


Рисунок 13 - Дані протоколу Telnet

Висновок: на даній лабораторній роботі я вивчив принцип роботи мережевого протоколу ТСР та протоколу додатків telnet. Визначив основні етапи і особливості використання протоколів.