**Лабораторна робота №4.**

**Вивчення мережевих аналізаторів tcpdump і Wireshark**

**Мета роботи:** Вивчити мережеві аналізатори tcpdump і Wireshark. Провести дослідження мережевого трафіку і виявити його особливості.

**Короткі теоретичні відомості**

Аналізатор трафіку, або сніфер (від англ. to sniff – нюхати) – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Під час роботи сніфера мережевий інтерфейс перемикається в т.з. «режим прослуховування» (Promiscuous mode), що і дозволяє йому одержувати пакети, адресовані іншим інтерфейсам в мережі.

Утиліта tcpdump призначена для аналізу мережевого трафіку і входить до складу всіх POSIX систем. Ця утиліта виводить заголовки пакетів, які відповідають заданим критеріям, на мережевому інтерфейсі, перекладеному попередньо в режим прийому всіх пакетів (promiscous mode). Критерії задаються в формі логічного виразу.

Логічні вирази для критеріїв необхідні для того, що б із загального мережевого трафіку виділити тільки ті, котрі цікавлять нас пакети. Синтаксис логічних виразів включає наступні ключові слова: host - IP адреса або DNS ім’я хоста, net - адреса мережі, наприклад – net 192.168.7, net 192.168.7.0 mask 255.255.255.224, port – номер порту (має сенс для протоколів TCP та UDP), proto – тип протокола. Можливі типи: ether, fddi, tr, ip, ip6, arp, rarp, decnet, lat, sca, moprc, mopdl, iso, esis, isis, icmp, icmp6, tcp and udp. Наприклад, tcpdump tcp port 80, dir – напрямок, можливі значення – src або dst . Наприклад – tcpdump src host cs.stu.cn.ua.

Крім того, можна використовувати адреси несучої мережі Ethernet: tcpdump ether dst 00:02:44:5b:ee:9b або IP мережа – tcpdump net src 192.168.7.0/27

Більш повну інформацію про можливості утиліти tcpdunp можна отримати зі стандартної сторінки допомоги, задавши команду man tcpdump.

Мережевий аналізатор Wireshark побудований на тій же бібліотеці (libpacap), що і утиліта tcpdump, але має зручний графічний користувальницький інтерфейс.

Головне вікно програми наведено на рисунку 1.

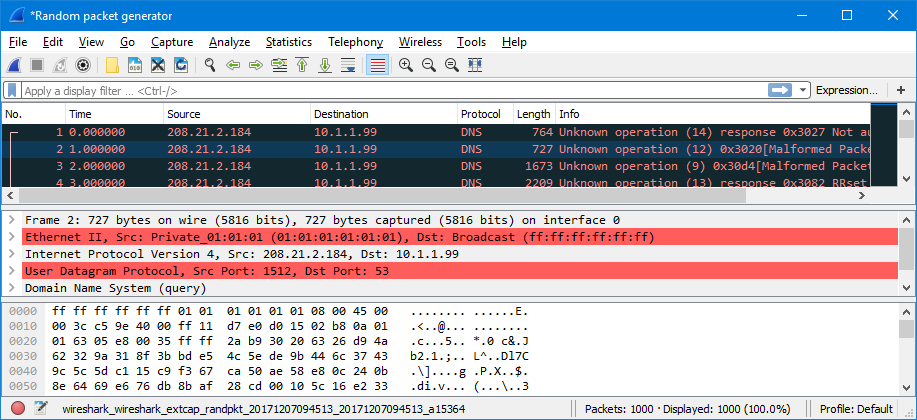


Рисунок 1 – Головне вікно Wireshark підчас захоплення мережевих пакетів

У верхній частині вікна міститься перелік пакетів, захоплених з мережі. При натисканні правої кнопки миші на тому чи іншому пакеті з’являється контекстне меню. Список можна відсортувати за будь-яким полем.

Середнє вікно містить інформацію щодо протоколів, що інкапсулюються відповідно загальним принципам моделі OSI для обраного у верхньому вікні пакета.

Нижнє вікно містить шістнадцяткове подання обраного пакета. При обиранні того або іншого поля в середньому вікні автоматично буде підсвічуватися відповідна ділянка шістнадцяткового подання.

Для захоплення або відображення тільки тих пакетів, які цікавлять, використовуються два види фільтрації: під час захоплення і під час відображення.

**Хід роботи**

1. Захоплення пакетів утилітою Wireshark без фільтра зображено на рисунку 1.

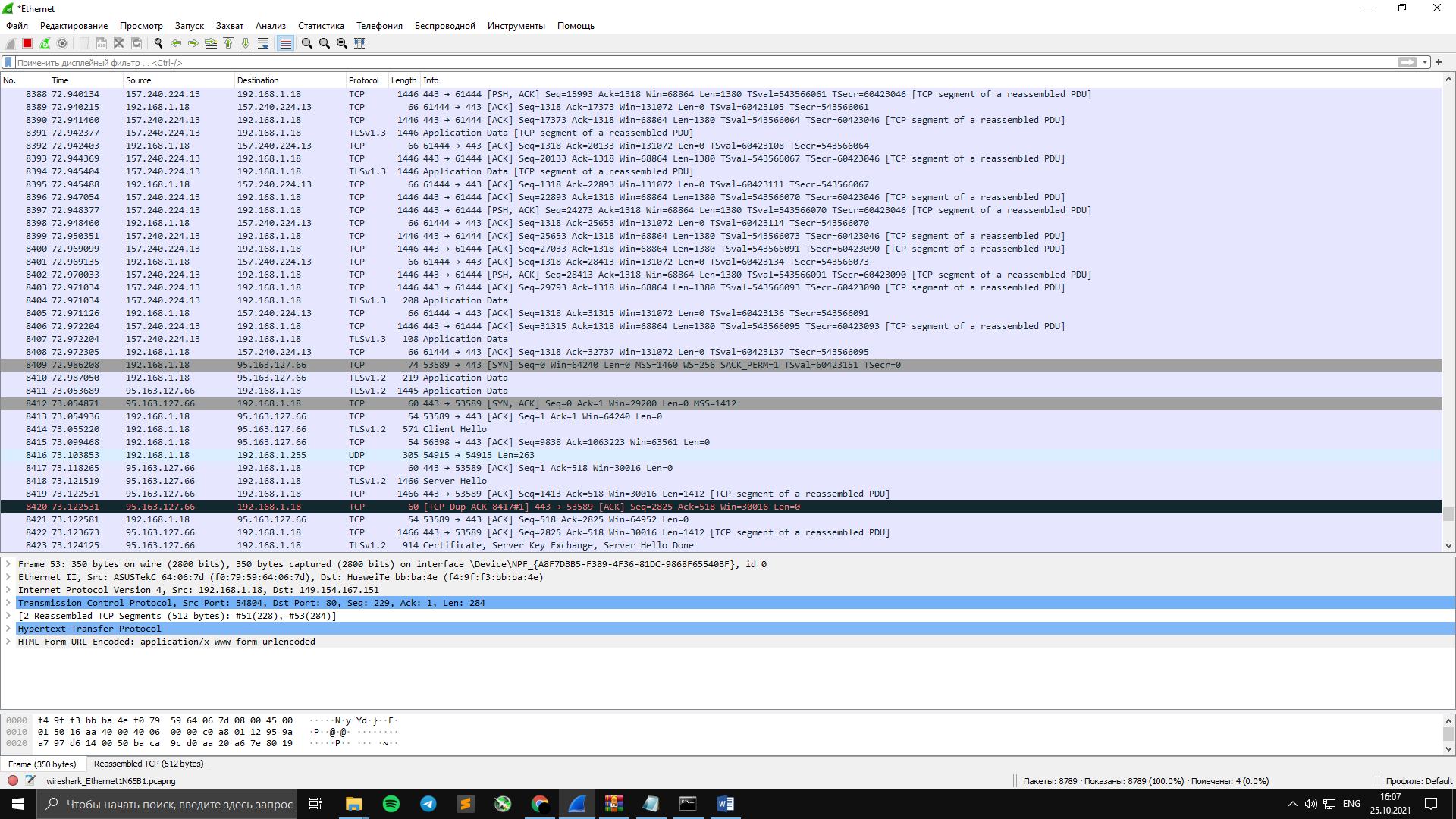


Рисунок 1 – Захоплення пакетів без фільтра

2. Захоплення тільки широкомовних пакетів зображено на рисунку 2, захоплення виконується командою eth.dst == ff:ff:ff:ff:ff:ff.

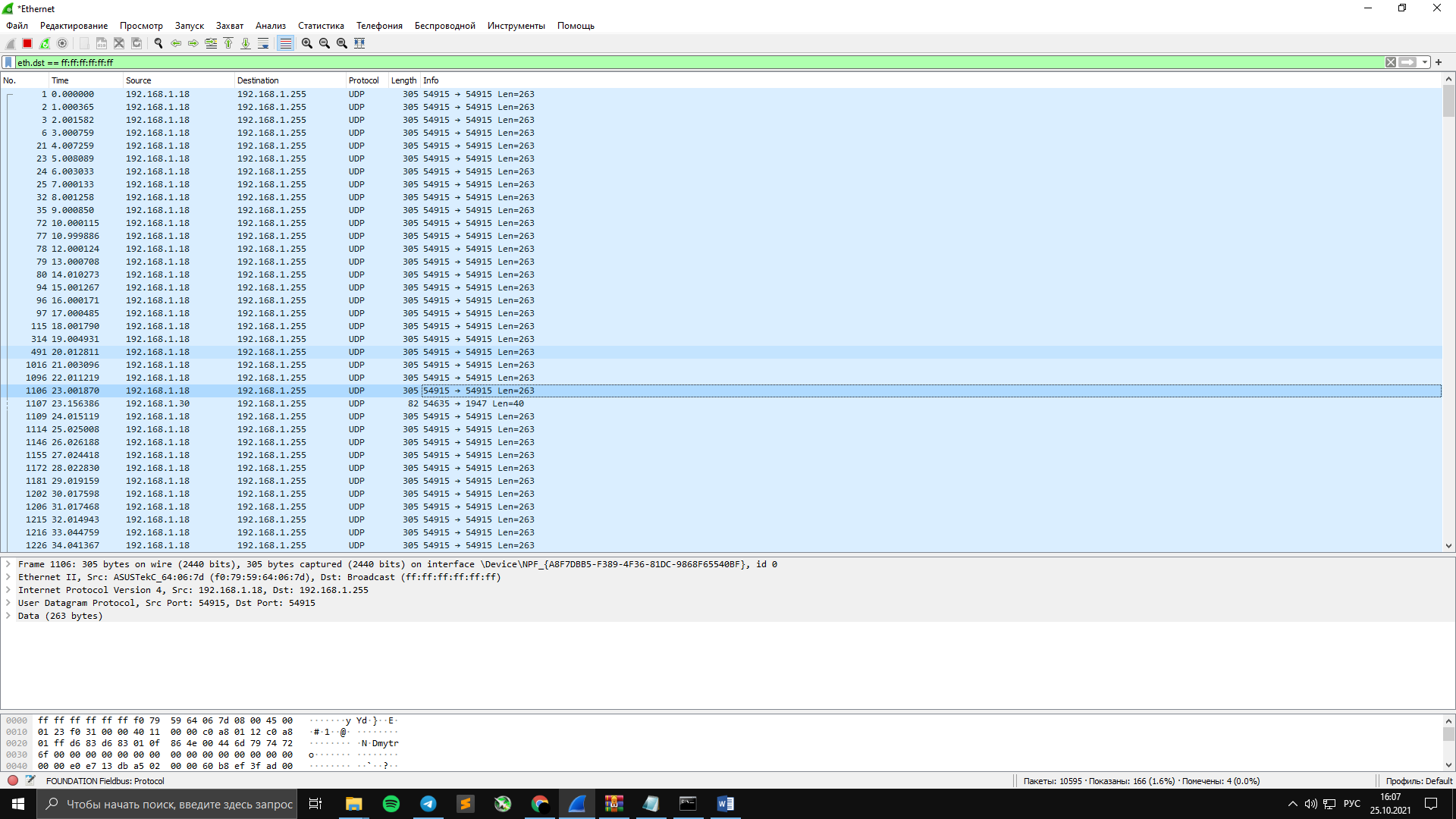


Рисунок 2 – Захоплення широкомовних пакетів

3. Захоплення пакетів ICMP зображено на рисунку 3.

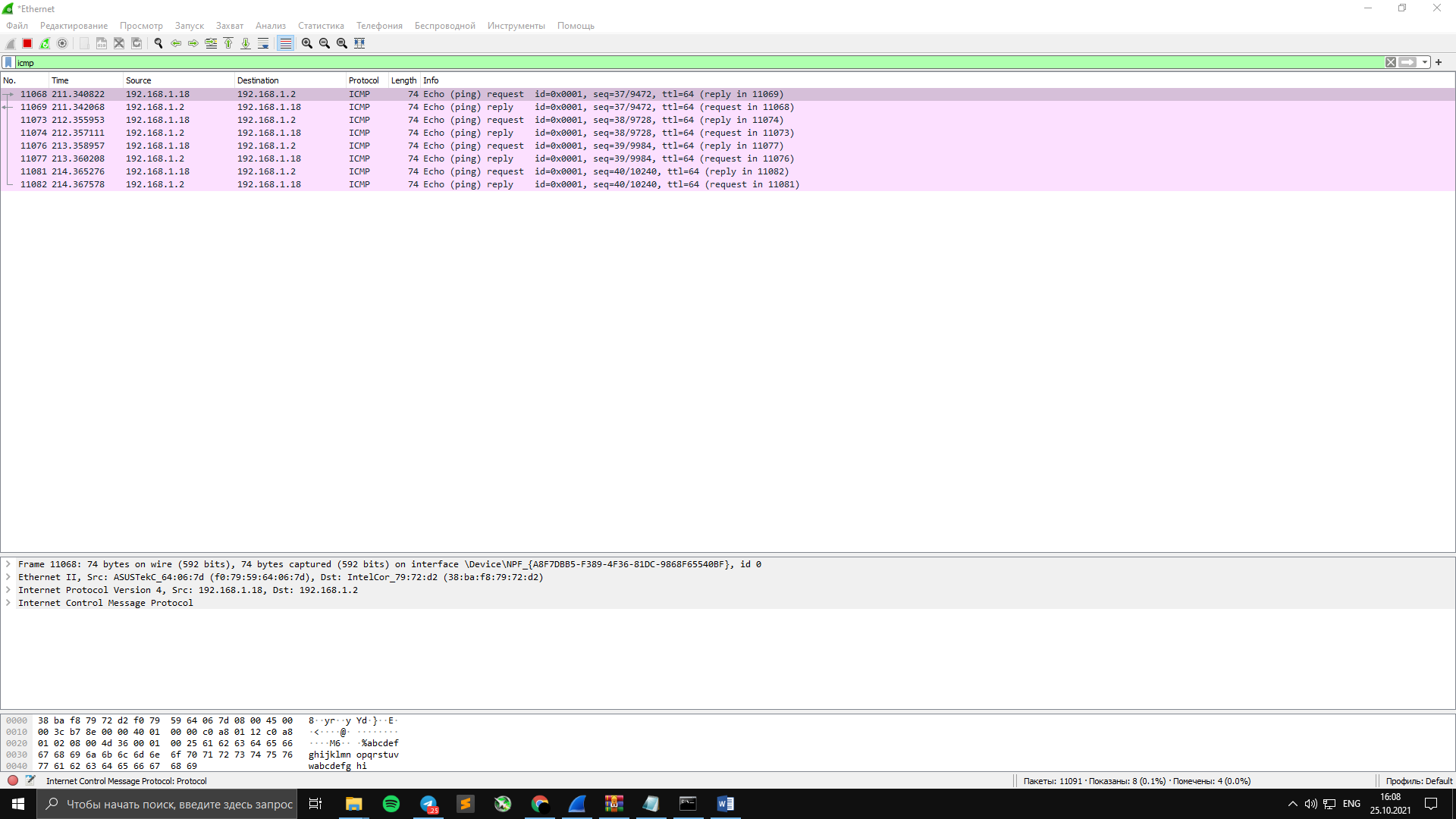


Рисунок 3 – Захоплення ICMP

4. Після запуску команди ping на другому хості до третього, пакети не були захоплені, для захоплення потрібно ще використовувати утиліту ретранслятор, як наприклад - CAIN & ABEL. Утиліта виконає підміну шлюза для потрібного хоста, і всі пакети будуть приходити через нашу систему.

5. Результат захоплення пакетів утилітою tcpdump зображено на рисунку 4.

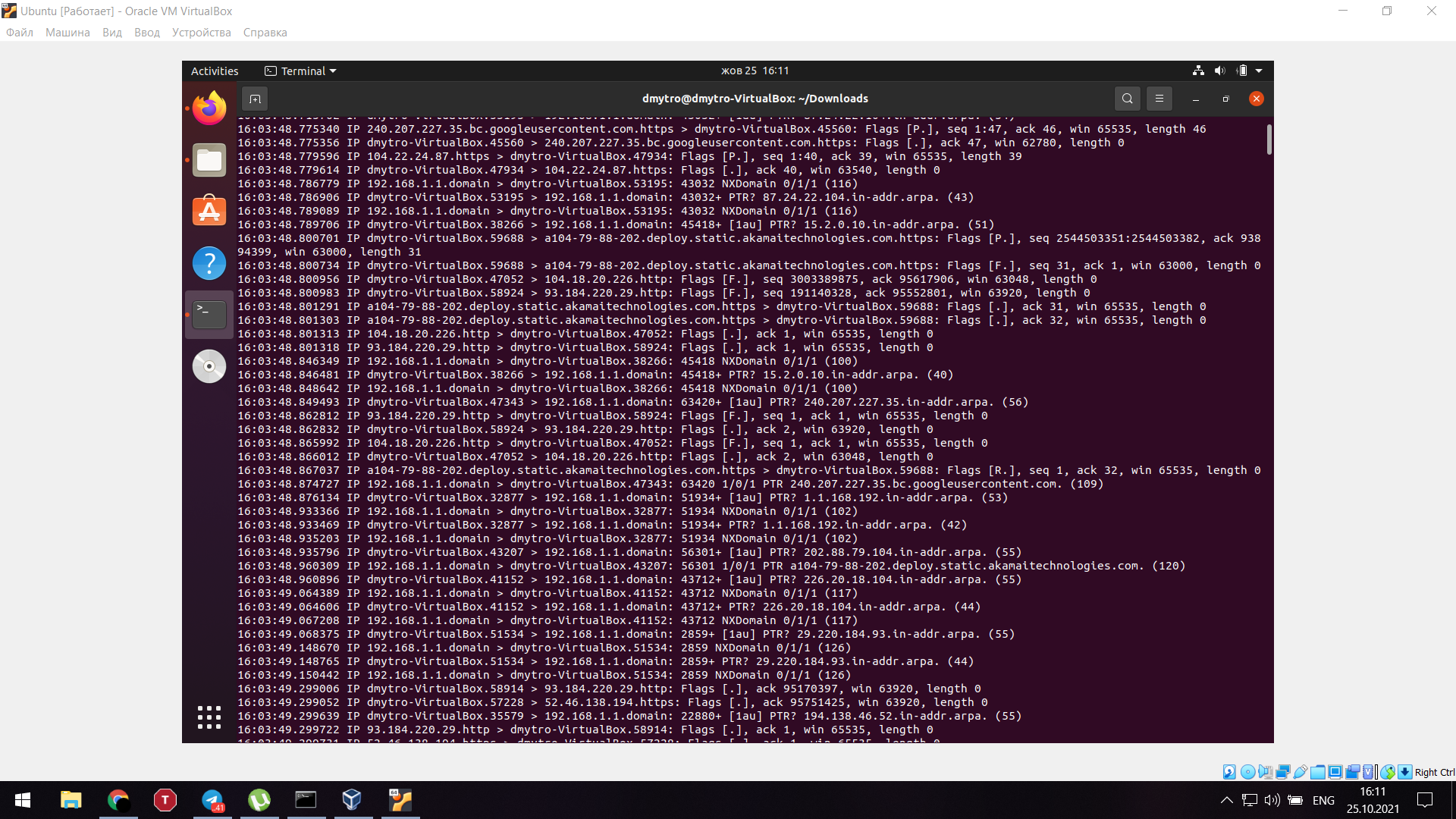


Рисунок 4 – Захоплення пакетів утилітою tcpdump

Висновок: на даній лабораторній роботі я вивчив мережеві аналізатори tcpdump і Wireshark. Провів дослідження мережевого трафіку та навчивсь використовувати команди фільтрації Wireshark.