Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №1

Аналіз кіберзагроз та класифікація атак

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** навчитися виявляти підозрілий мережевий трафік і класифікувати атаки за ознаками

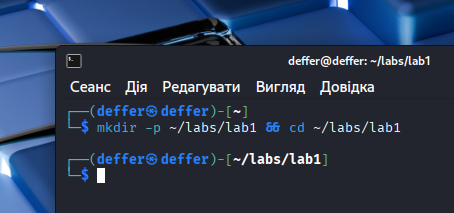
**Опис середовища:**

ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109

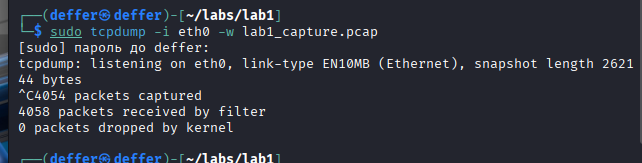
Wireshark 4.4.7., tcpdump version 4.99.5, libpcap version 1.10.5, OpenSSL 3.5.2 5 Aug 2025, 64-bit build, 64-bit time\_t, TShark (Wireshark) 4.4.7., Linux kali 6.12.38+kali-amd64, Local Kali ip: 192.168.135.128, Local Metasploitable ip: 192.168.135.129

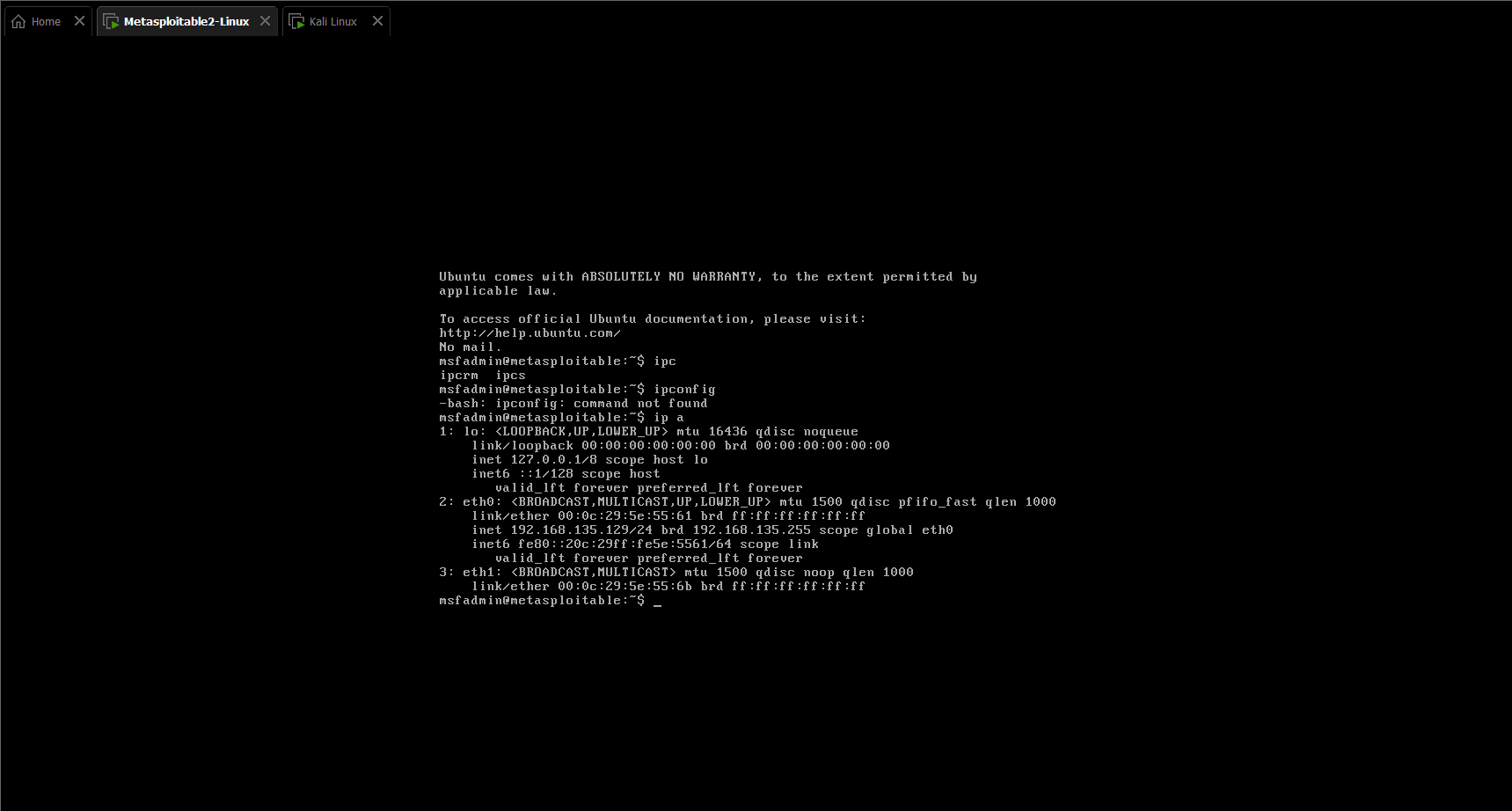
**Команди:**

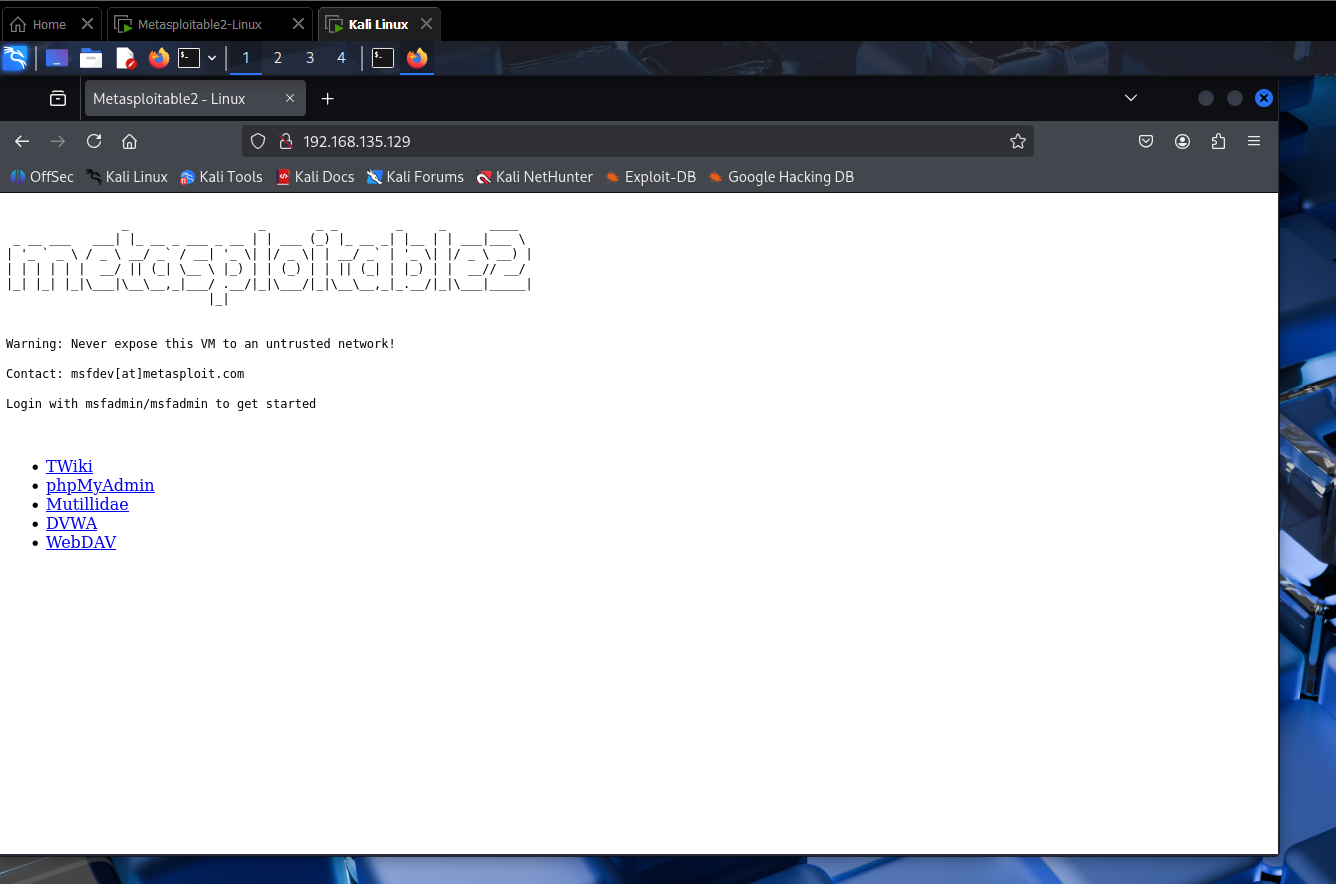
mkdir -p ~/labs/lab1 && cd ~/labs/lab1

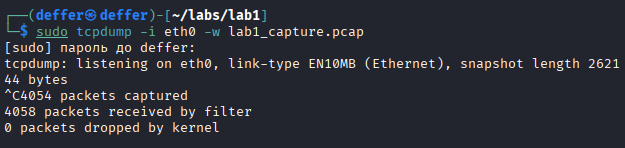


sudo tcpdump -i eth0 -w lab1\_capture.pcap

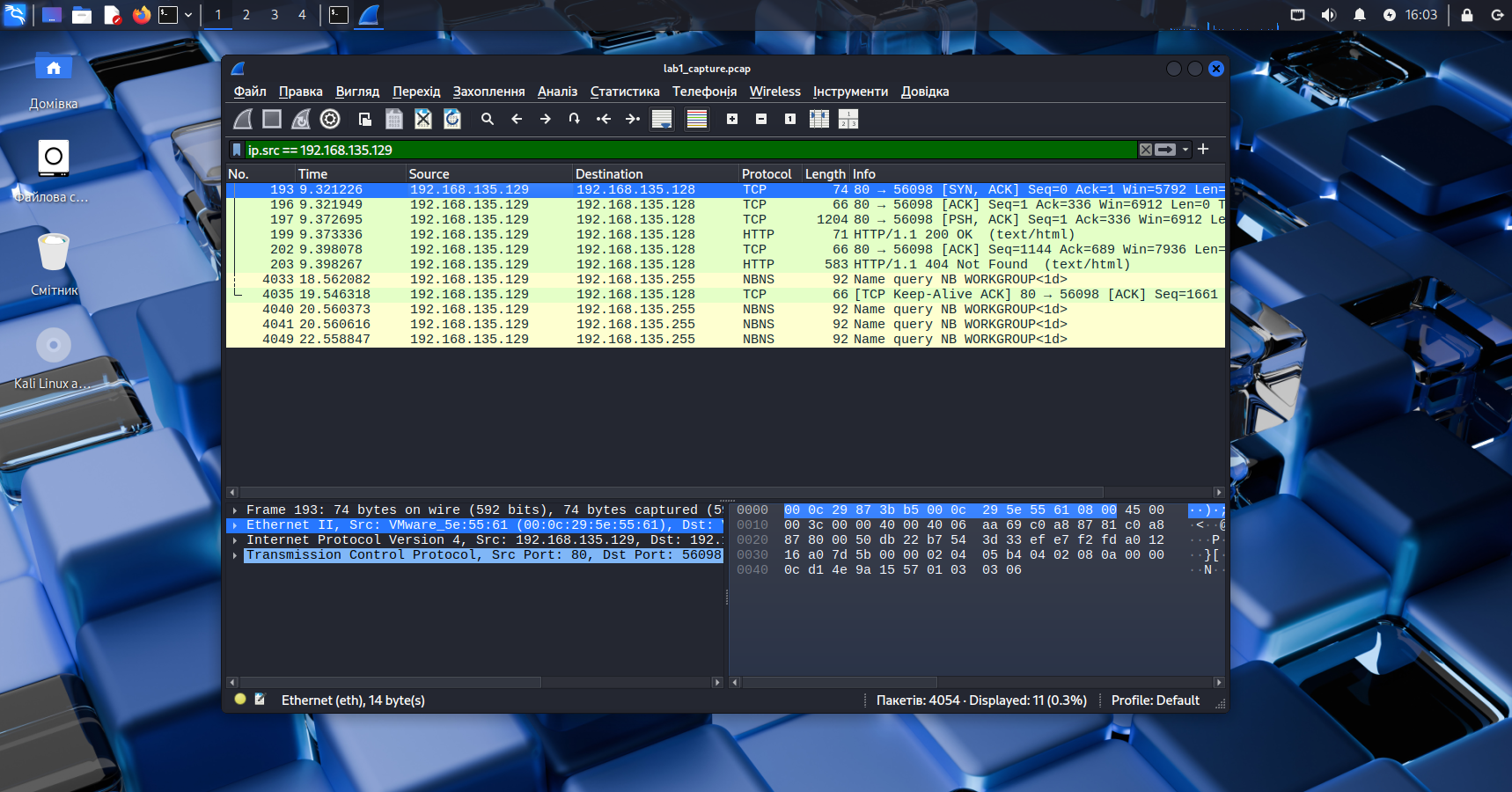


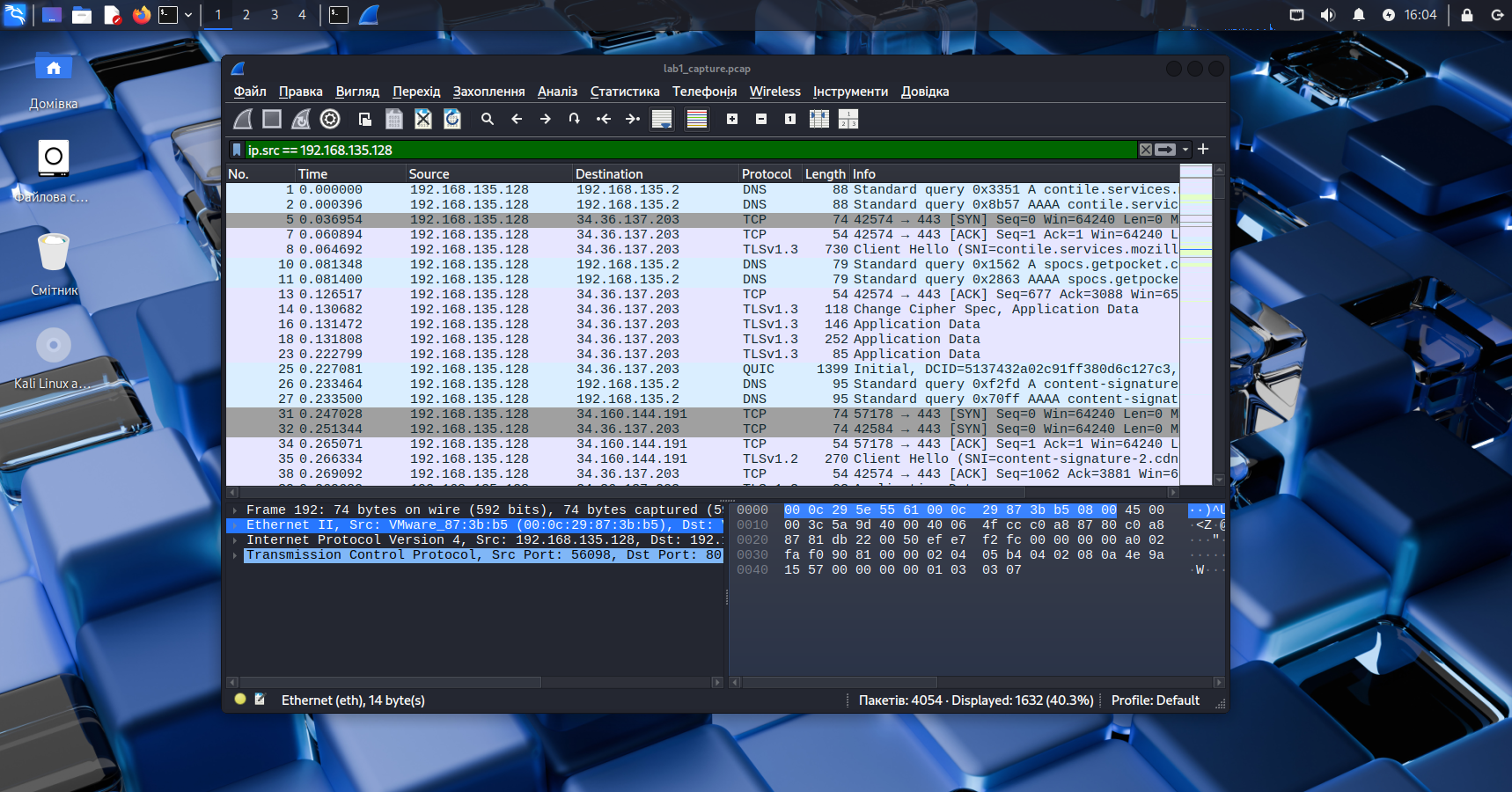


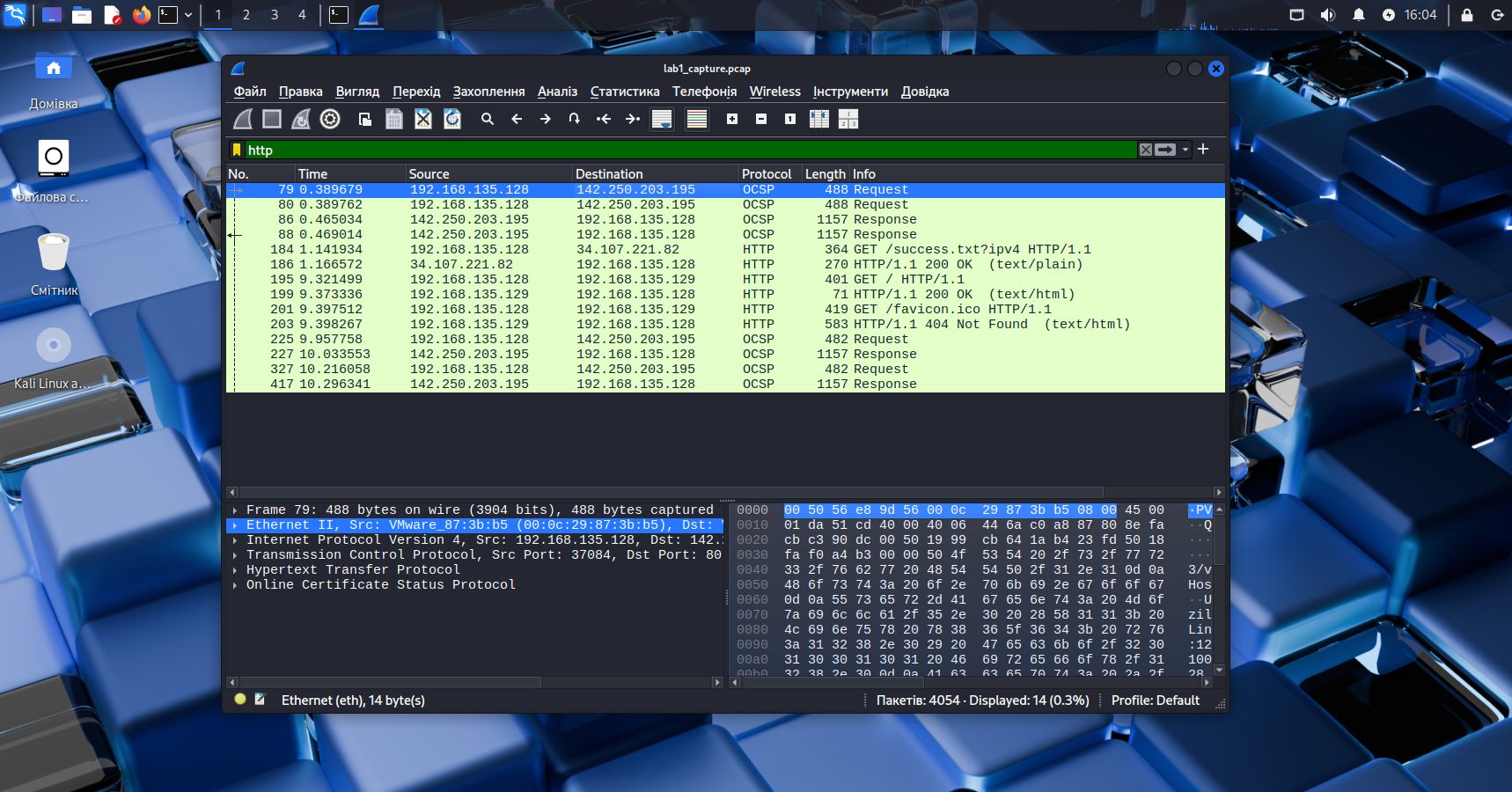




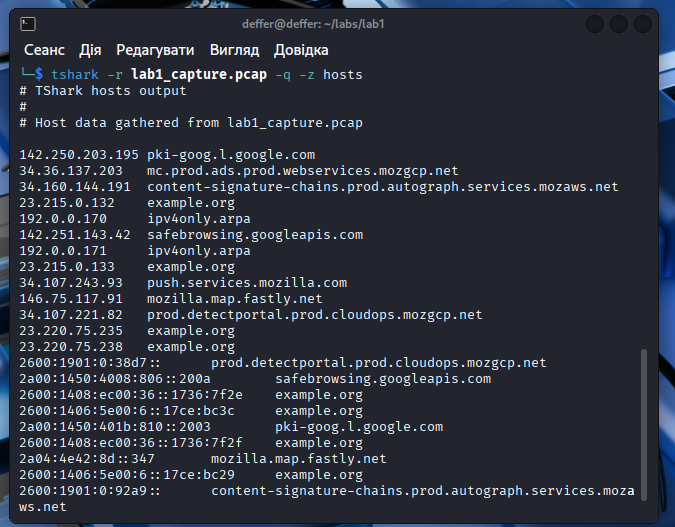
sudo wireshark lab1\_capture.pcap







tshark -r lab1\_capture.pcap -q -z hosts



**Класифікація атак за MITRE ATT&CK**

reconnaissance TA0043: Reconnaissance (Розвідка)

**Дія:** Використання браузера для доступу до вебсервера Metasploitable за його IP-адресою (192.168.135.129).

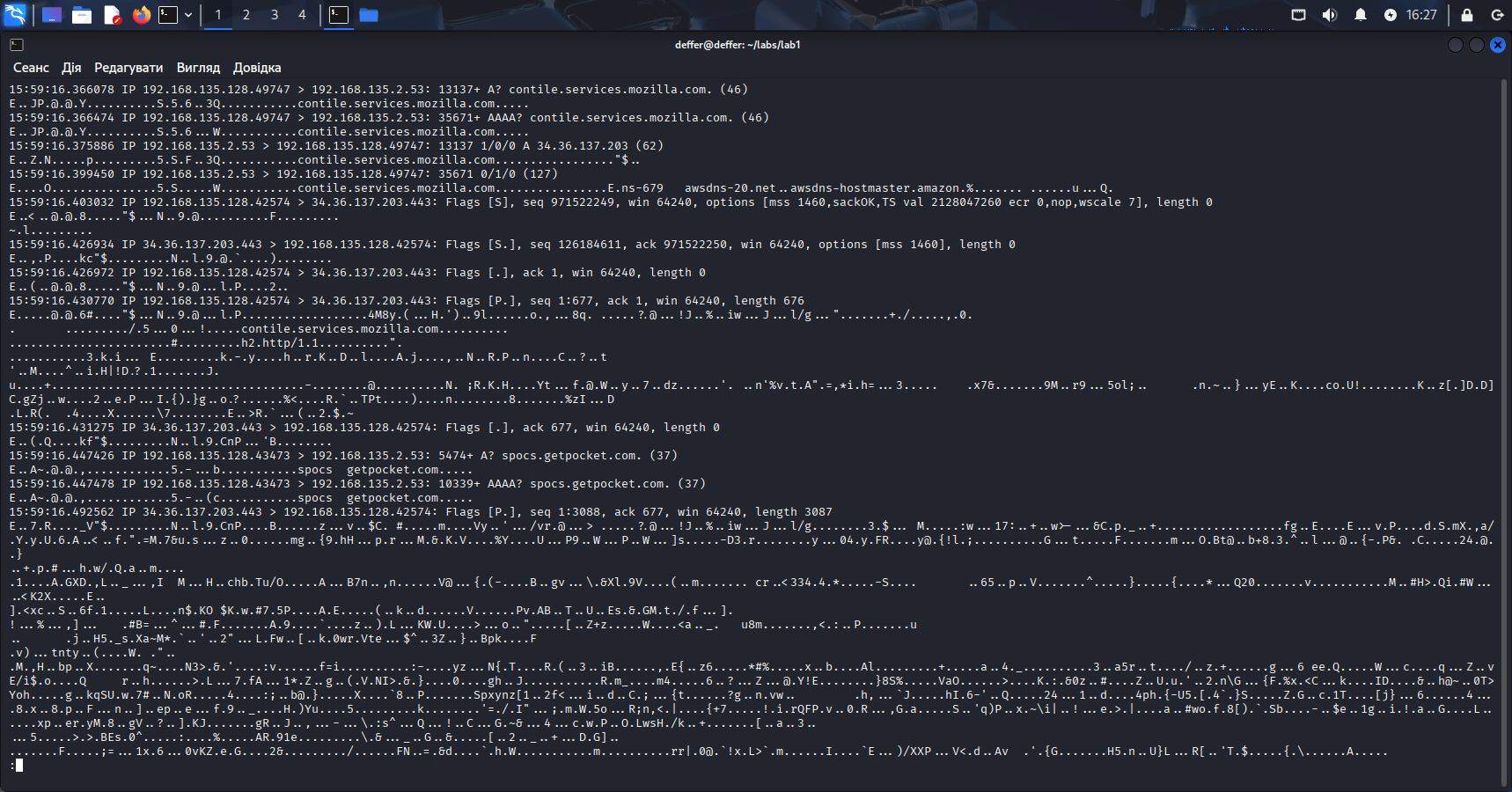
Цей крок є формою **активної розвідки**. Є підтвердження, що за цією IP-адресою існує активний хост і на ньому працює вебсервер. Зловмисник на цьому етапі перевіряє доступність сервісів, щоб знайти потенційні точки входу. Аналіз трафіку у Wireshark, особливо HTTP-запитів, показує саме цей процес.

discovery TA0007: Discovery (Виявлення)

**Дія:** Аналіз усього захопленого трафіку, зокрема запитів до зовнішніх ресурсів, таких як pki-goog.l.google.com або mozilla.map.fastly.net, що видно у виводі команди tshark.

У реальній атаці зловмисник, отримавши доступ до системи, намагатиметься зрозуміти, як вона взаємодіє з іншими внутрішніми та зовнішніми сервісами. Аналізуючи трафік, фактично виявляються мережеві з'єднання, які ініціював браузер під час сесії. Це імітує збір інформації про мережеву інфраструктуру та конфігурацію.

**Фрагмент файлу .pcap**



**Висновок:** На цій лабораторній роботі вдалось отримати pcap пакети, проаналізувати їх та встановити віртуальну машину VMWare з операційною системою Kali Linux