МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**Тема № 2**. Електронна комунікаційна мережа об’єкта кіберзахисту як джерело ознак кіберінциденту.

**Заняття № 2/6.** Технологічні основи реєстрації подій в каналі електронної комунікації з використанням tcpdump.

**TCPDUMP, РОЗРОБЛЕННЯ ПРАВИЛ РЕЄСТРАЦІЇ ПОДІЙ**

**Виконав:** курсант 314 навчальної групи

мол. с-нт \_\_\_\_\_\_\_\_\_\_\_\_\_ МАРТИНЮК І.А.

15.04.2024

**Перевiрив:** викладач кафедри № 33

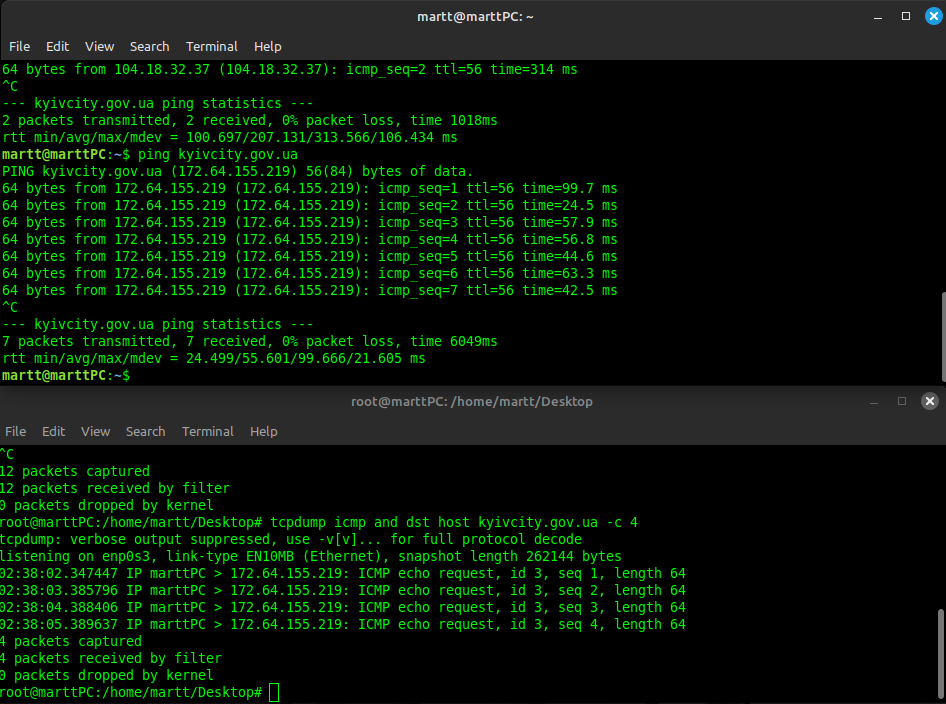
капітан\_\_\_\_\_\_\_\_\_\_\_ ПРИЙМА О.А.

Київ – 2024

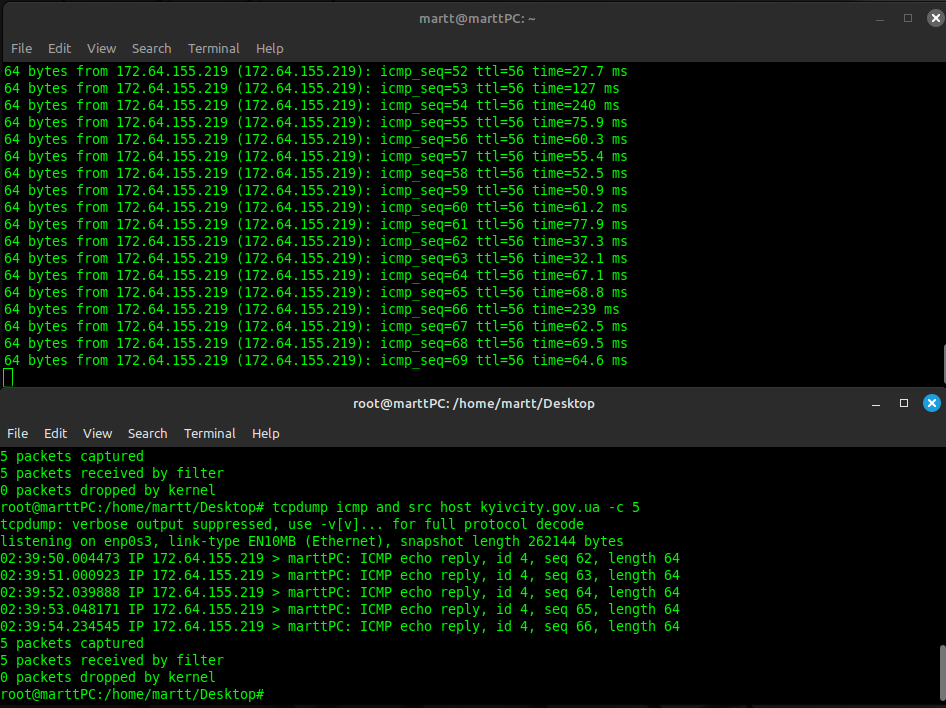
1. Обрана адреса – **kyivcity.gov.ua,**

її IP-адреса – *необхідно визначити в ході даного заняття*

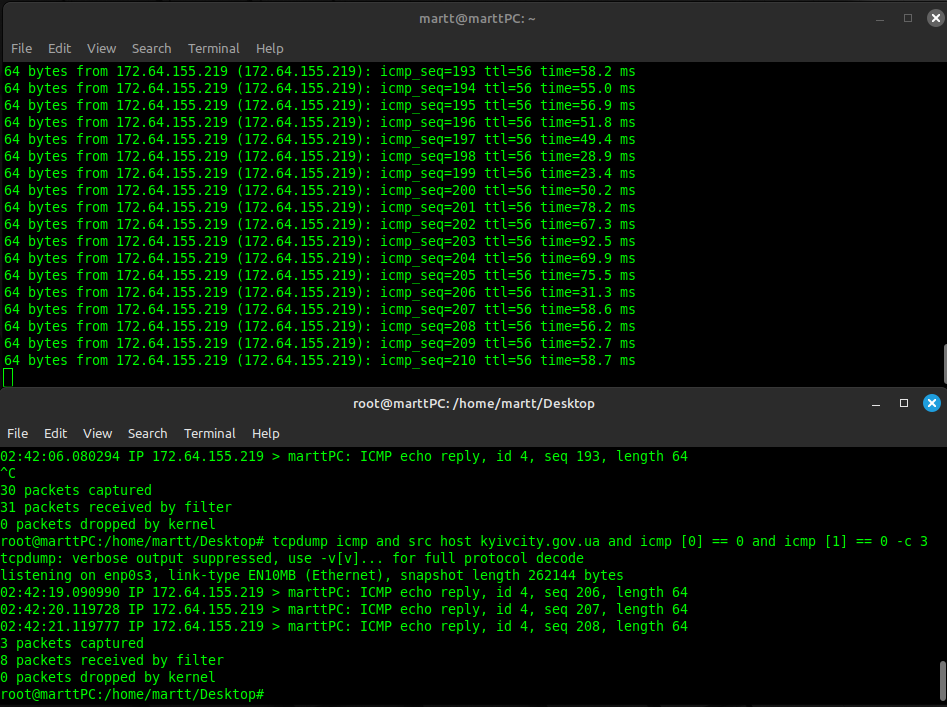
1. Застосування фільтру для перехоплення **всіх icmp пакетів** створених **чотирма** ехо-запитами до обраного сайту.



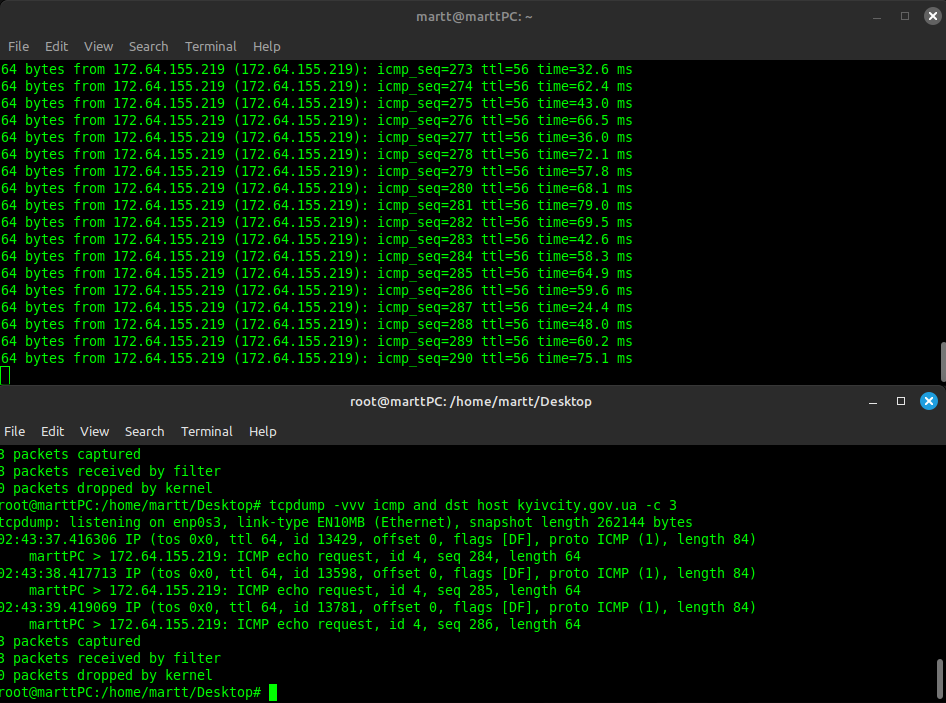
1. Застосування фільтру для перехоплення **icmp відповідей** створених **п’ятьма** запитами до обраного сайту.



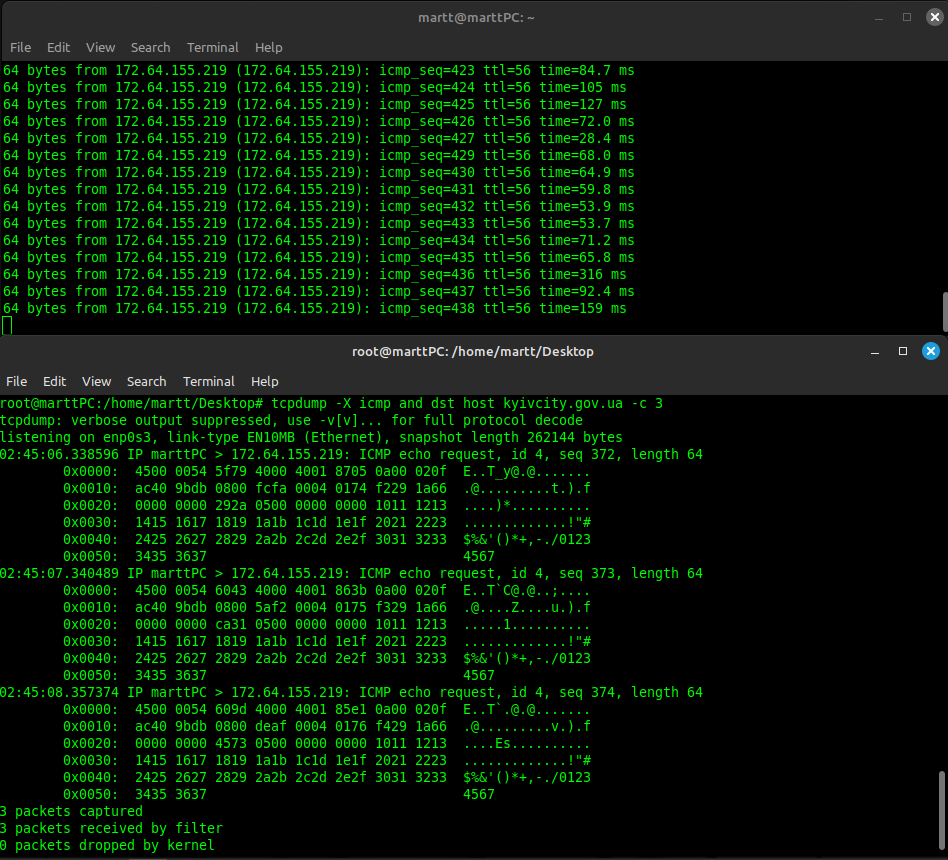
1. Застосування фільтру для перехоплення **лише перших трьох** **icmp відповідей без DNS перетворення** від обраного сайту.



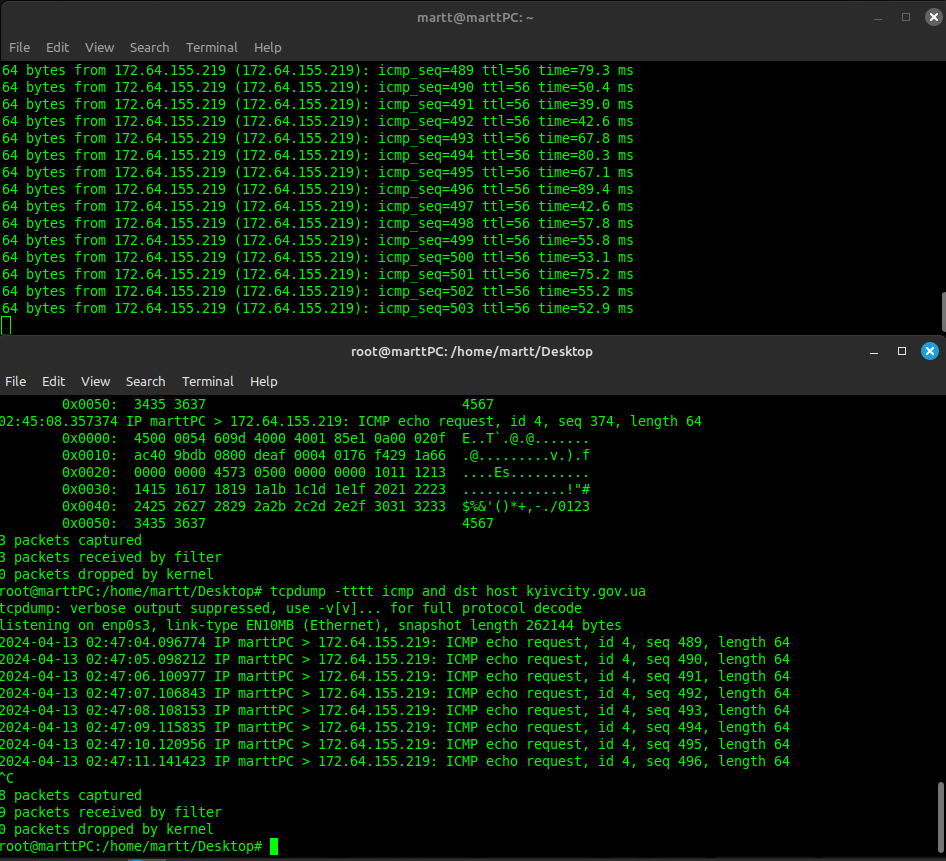
1. Застосування фільтру для максимально деталізованого виводу перехоплених **перших трьох** **icmp запитів** до обраного сайту.



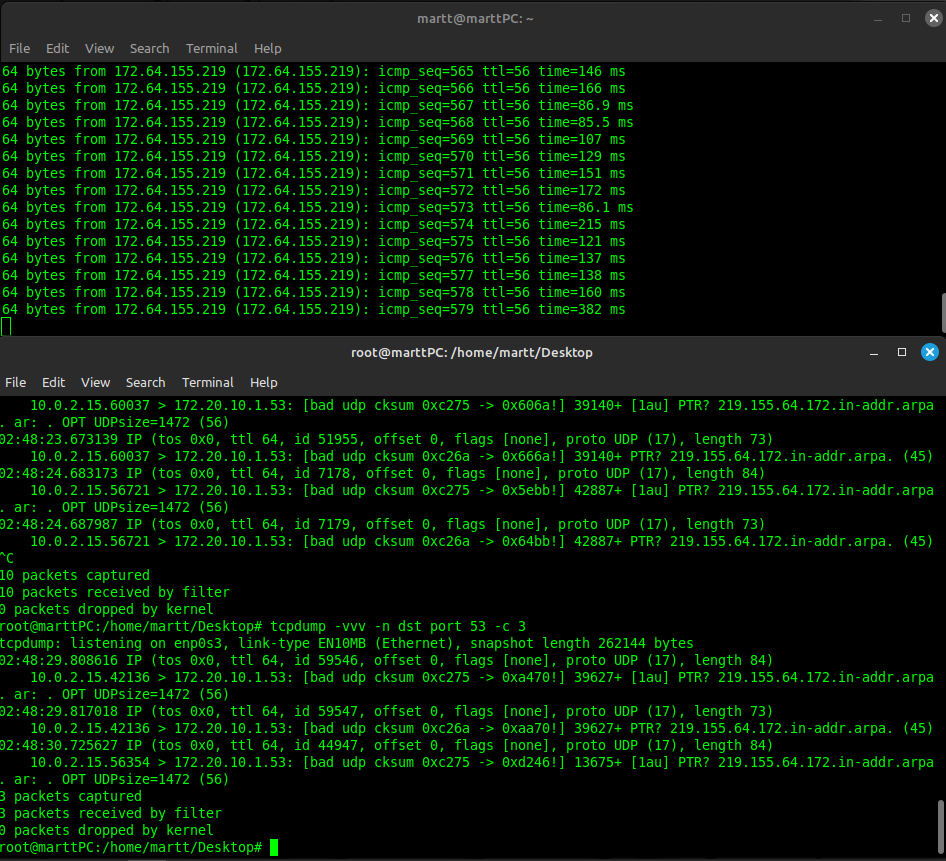
1. Застосування фільтру для виводу payload **в HEX форматі** перехоплених **перших трьох** **icmp запитів**. Зробіть скріншот обох вікон з відображенням даної інформації та скопіюйте у Звіт за дане ПЗ.



1. Для попереднього пункту змінено **формат часу** для виводу перехопленого трафіку, який починає відлік від першого перехопленого пакету.



1. Застосування фільтру для **перехоплення DNS трафіку** для визначення IP адреси обраного сайту.



1. Застосування фільтру для **перехоплення http** **трафіку**.
2. Результат застосування модифікованого фільтру з метою **відбору пакетів лише обраного сайту**.

