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 навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_ ПЕТРЕНКО К.В.

05.04.2024

**Перевiрив:** викладач кафедри № 33

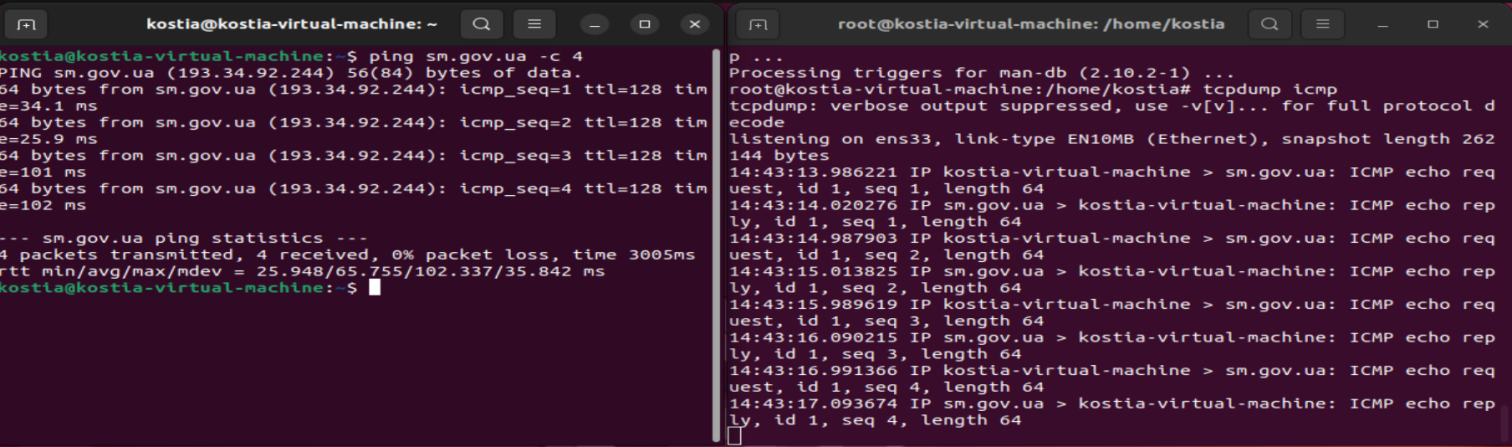
капітан\_\_\_\_\_\_\_ Прийма О.О.

Київ – 2024

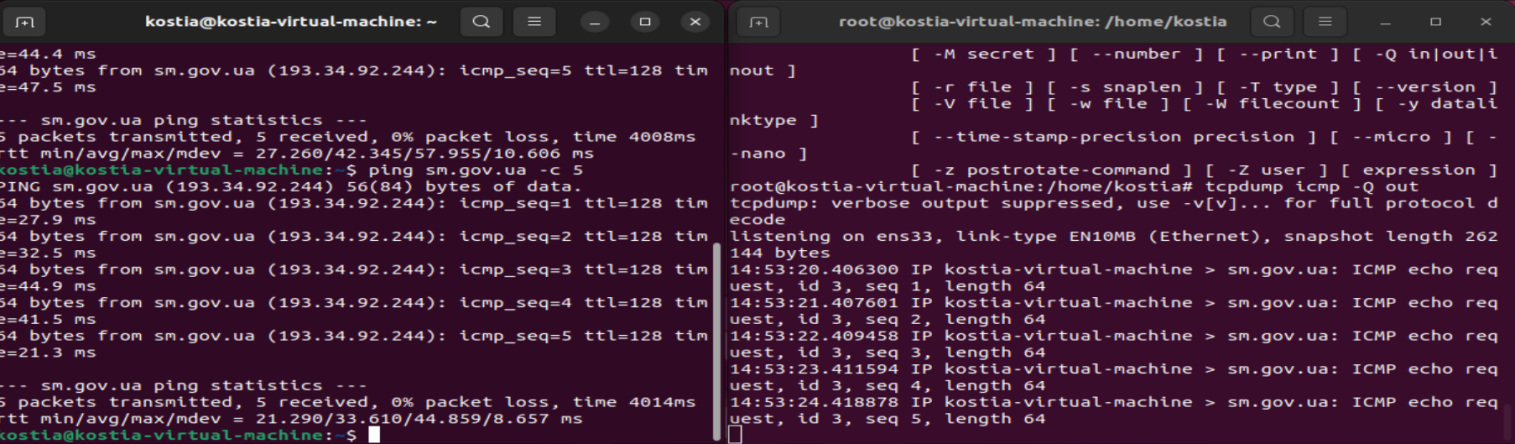
1. Обрана адреса – **sm**.**gov.ua,**

її IP-адреса – *193.34.92.244*

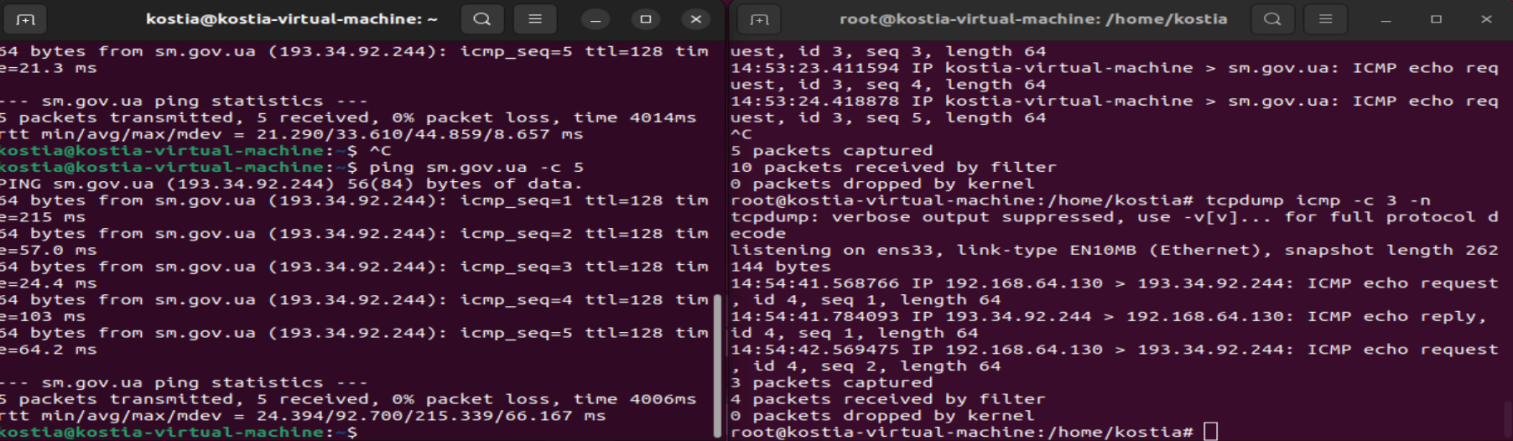
1. Застосування фільтру для перехоплення **всіх icmp пакетів** створених **чотирма** ехо-запитами до обраного сайту.



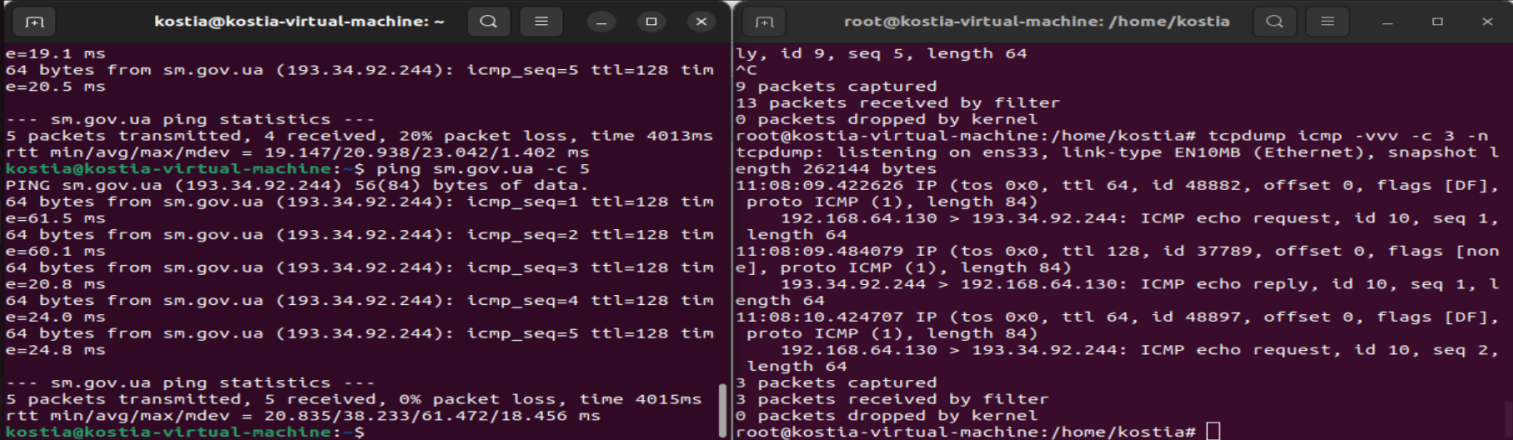
1. Застосування фільтру для перехоплення **icmp відповідей** створених **п’ятьма** запитами до обраного сайту.



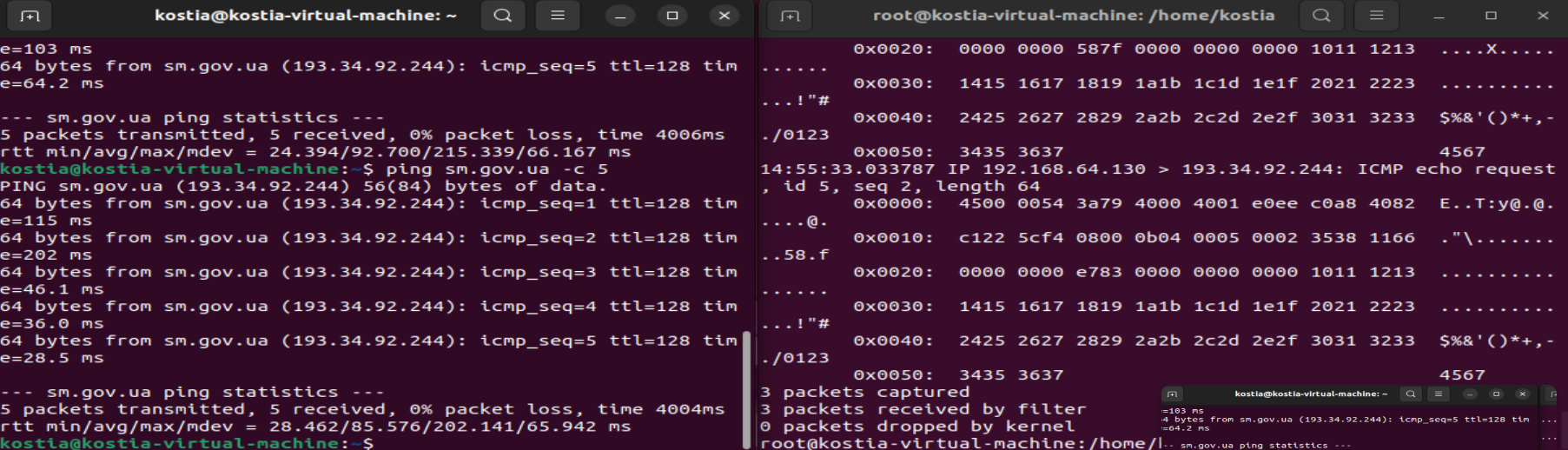
1. Застосування фільтру для перехоплення **лише перших трьох** **icmp відповідей без DNS перетворення** від обраного сайту.



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.



tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes

13:49:59.579891 IP (tos 0x0, ttl 64, id 20303, offset 0, flags [DF], proto ICMP (1), length 84)

kostia-virtual-machine > sm.gov.ua: ICMP echo request, id 69, seq 1, length 64

0x0000: 4500 0054 4f4f 4000 4001 cc18 c0a8 4082 E..TOO@.@.....@.

0x0010: c122 5cf4 0800 a9d0 0045 0001 57d7 0f66 ."\......E..W..f

0x0020: 0000 0000 1fd9 0800 0000 0000 1011 1213 ................

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

0x0050: 3435 3637 4567

13:50:00.581441 IP (tos 0x0, ttl 64, id 20443, offset 0, flags [DF], proto ICMP (1), length 84)

kostia-virtual-machine > sm.gov.ua: ICMP echo request, id 69, seq 2, length 64

0x0000: 4500 0054 4fdb 4000 4001 cb8c c0a8 4082 E..TO.@.@.....@.

0x0010: c122 5cf4 0800 a4c9 0045 0002 58d7 0f66 ."\......E..X..f

0x0020: 0000 0000 23df 0800 0000 0000 1011 1213 ....#...........

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

0x0050: 3435 3637 4567

13:50:01.583435 IP (tos 0x0, ttl 64, id 20594, offset 0, flags [DF], proto ICMP (1), length 84)

kostia-virtual-machine > sm.gov.ua: ICMP echo request, id 69, seq 3, length 64

0x0000: 4500 0054 5072 4000 4001 caf5 c0a8 4082 E..TPr@.@.....@.

0x0010: c122 5cf4 0800 dac0 0045 0003 59d7 0f66 ."\......E..Y..f

0x0020: 0000 0000 ece6 0800 0000 0000 1011 1213 ................

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

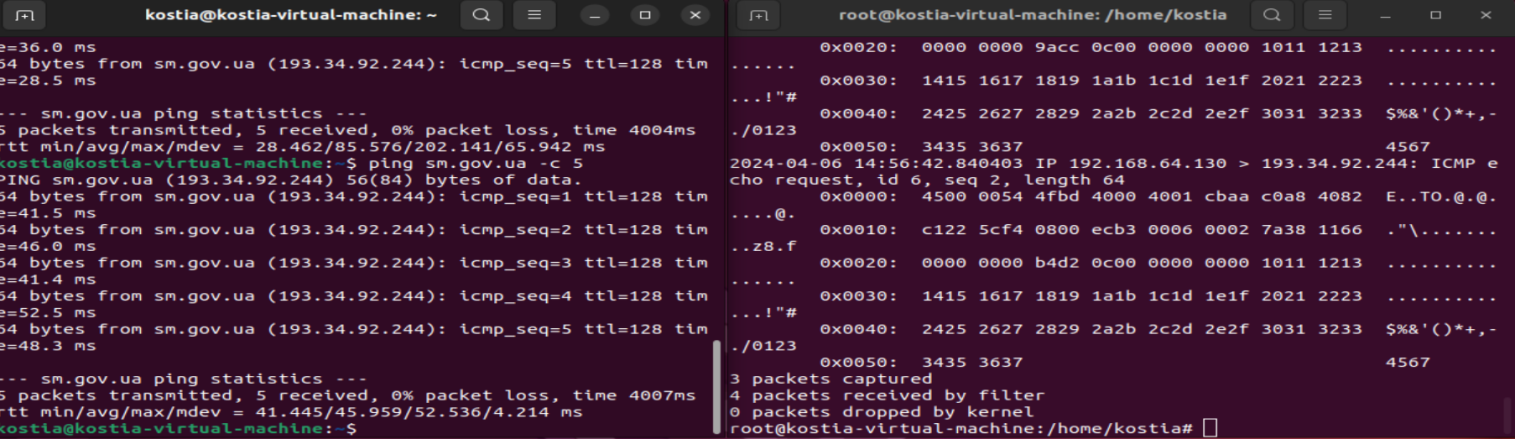
0x0050: 3435 3637 4567

3 packets captured

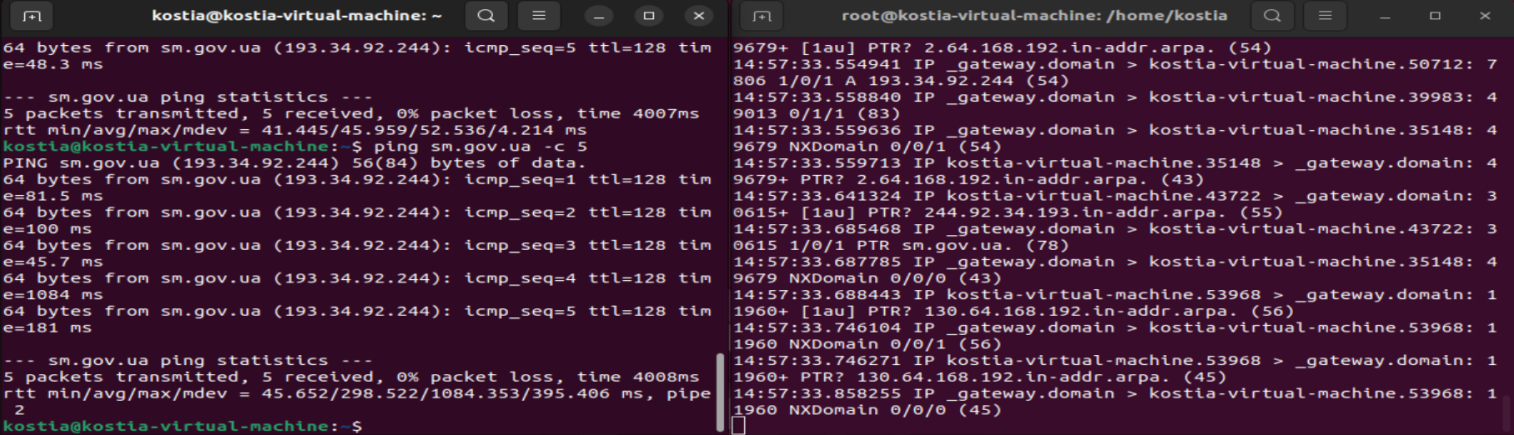
4 packets received by filter

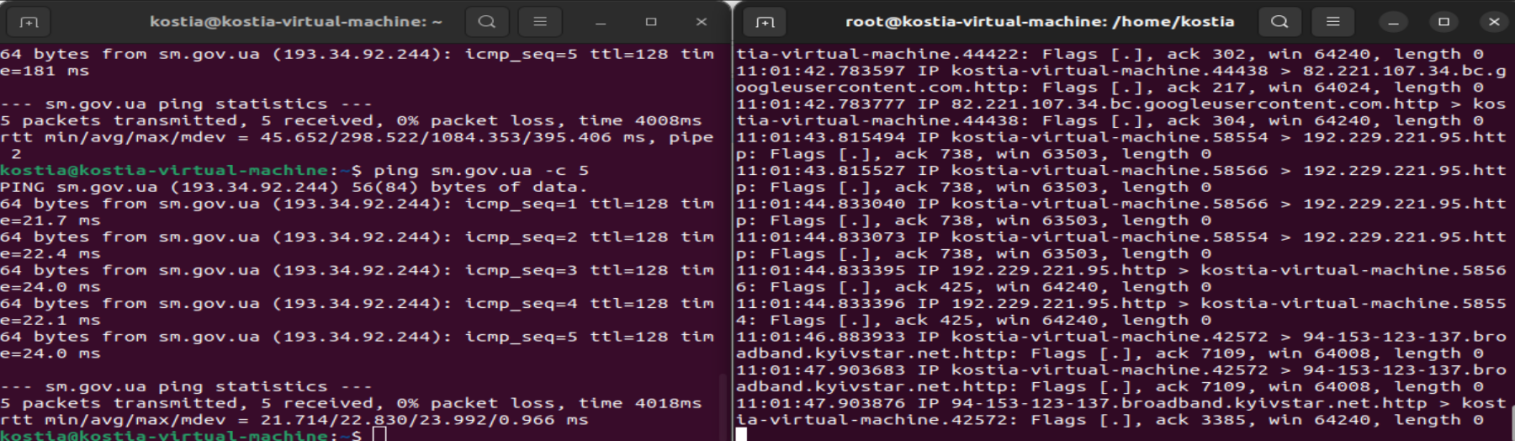
0 packets dropped by kernel

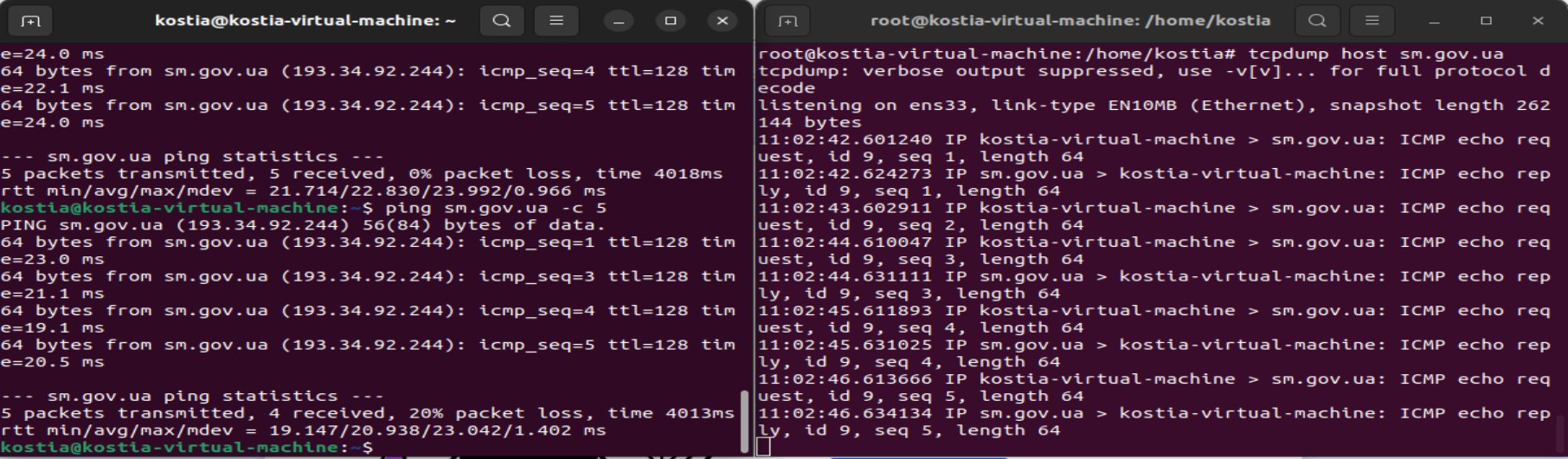
1. Для попереднього пункту змінено **формат часу** для виводу перехопленого трафіку, який починає відлік від першого перехопленого пакету.



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**.



**Висновок:** утиліта tcpdump дозволила відстежити мережевий трафік, пов'язаний з зверненням до веб-сайту sm.gov.ua. Шляхом аналізу отриманих пакетів було встановлено IP-адресу сервера, з якого надходили відповіді на запити до sm.gov.ua та час відповіді. Такий підхід до моніторингу мережевого трафіку є корисним для виявлення можливих проблем з доступністю веб-сайту або швидкістю його завантаження.

Отже, використання утиліти tcpdump дозволило здійснити докладний аналіз мережевого трафіку, пов'язаного з веб-сайтом sm.gov.ua шляхом його пінгування і захоплення трафіку з практичним відпрацюванням функціоналу утиліти у різних режимах.