МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

Звіт до лабораторної роботи № 7

на тему “ Пошук інформації у відкритих джерелах за допомогою пошукових систем. Анонімний пошук та оператори пошуку. Частина 1”

Виконав студент(ка) Борщ Дмитро
Група КБ-01
Перевірила Лаврик Т.В.

Суми 2023

ЗВІТ

про виконану роботу

Частина 1. Анонімність в мережі Інтернет.

Надайте відповіді на питання:

1) Що означає анонімність користувача в мережі Інтернет і що це надає самому користувачу?

Анонімність користувача в мережі Інтернет це такий його стан, за якого неможливо визначити подробиці про його особистість, географічне розташування, чи інші дані, що можуть допомогти його ідентифікувати.

2) Які існують методи (технології) анонімізації в мережі Інтернет? Назвіть 2-3 методи і надайте їх коротку характеристику.

Використання проксі серверів — проксі сервер це такий собі “повторювач”, який пересилає увесь наш трафік до пункту призначення, але приховує його справннє походження

Використання VPN — використання мережі VPN схоже до простого використання проксі серверу, але в цьому методі в якості “повторювача” виступає gateway нашої VPN + до того з’єднання між нами й gateway додатково зшифроване протоколом VPN.

3) Якому з методів Ви би надали перевагу? У чому його перевага на Вашу думку?

Мабуть я б обрав проксі, бо якщо стоїть задача приховати джерело трафіку, а не сам трафік, то краще використовувати ланцюжки проксі серверів.

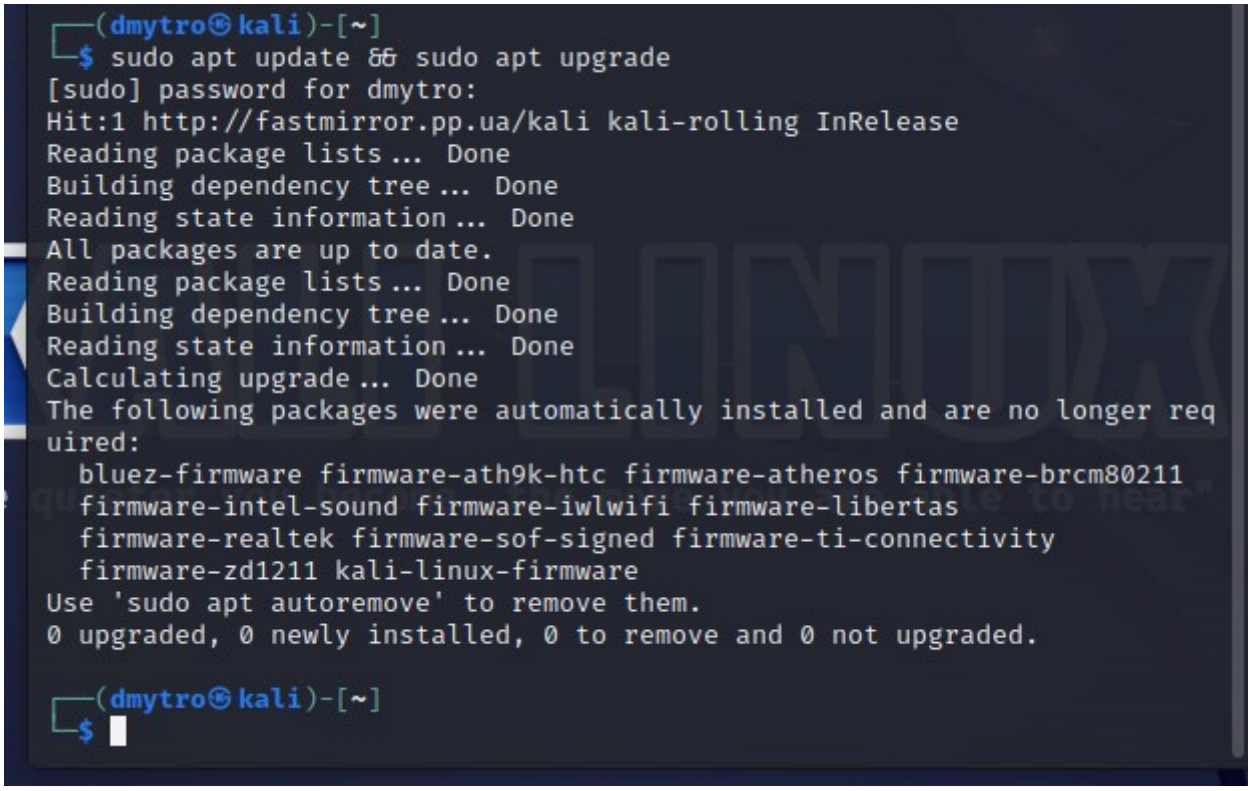
Частина 2. Анонімність в Kali Linux.

У цій частині лабораторної роботи налаштовуємо в Kali Linux анонімний режим роботи.

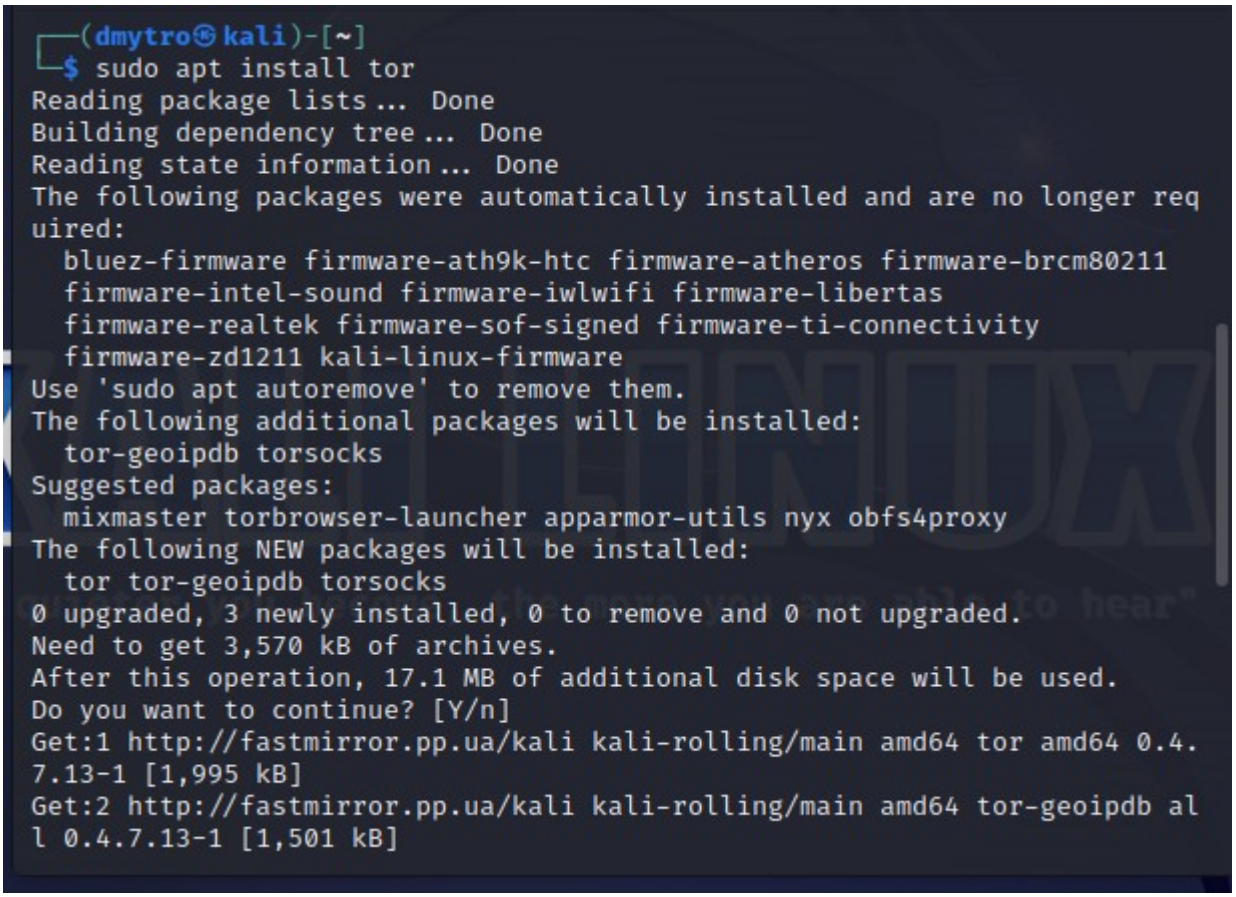
2.1 Запустіть Kali Linux.

2.2 Здійснити за інструкцією встановлення Tor.

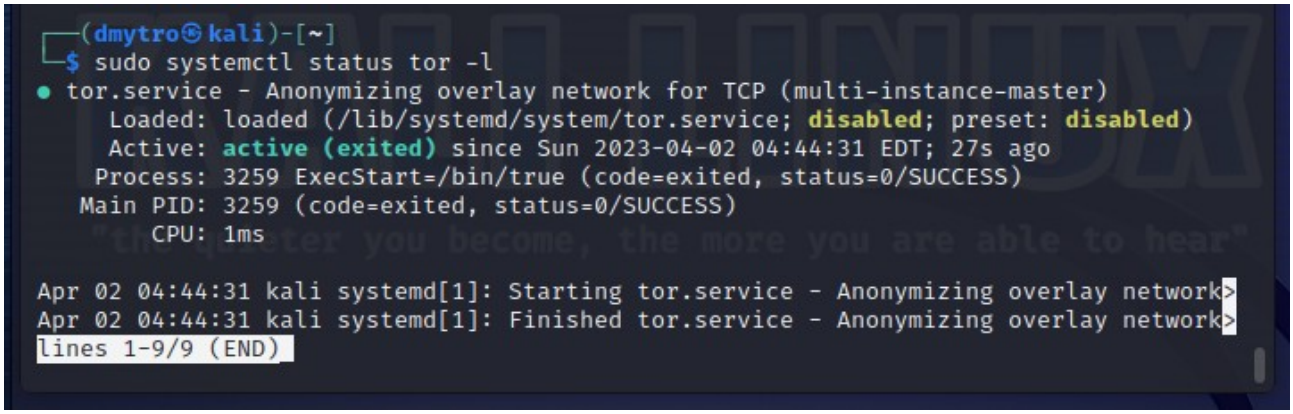
Оновлення списків пакетів та їх оновлення:



Встановлення tor:

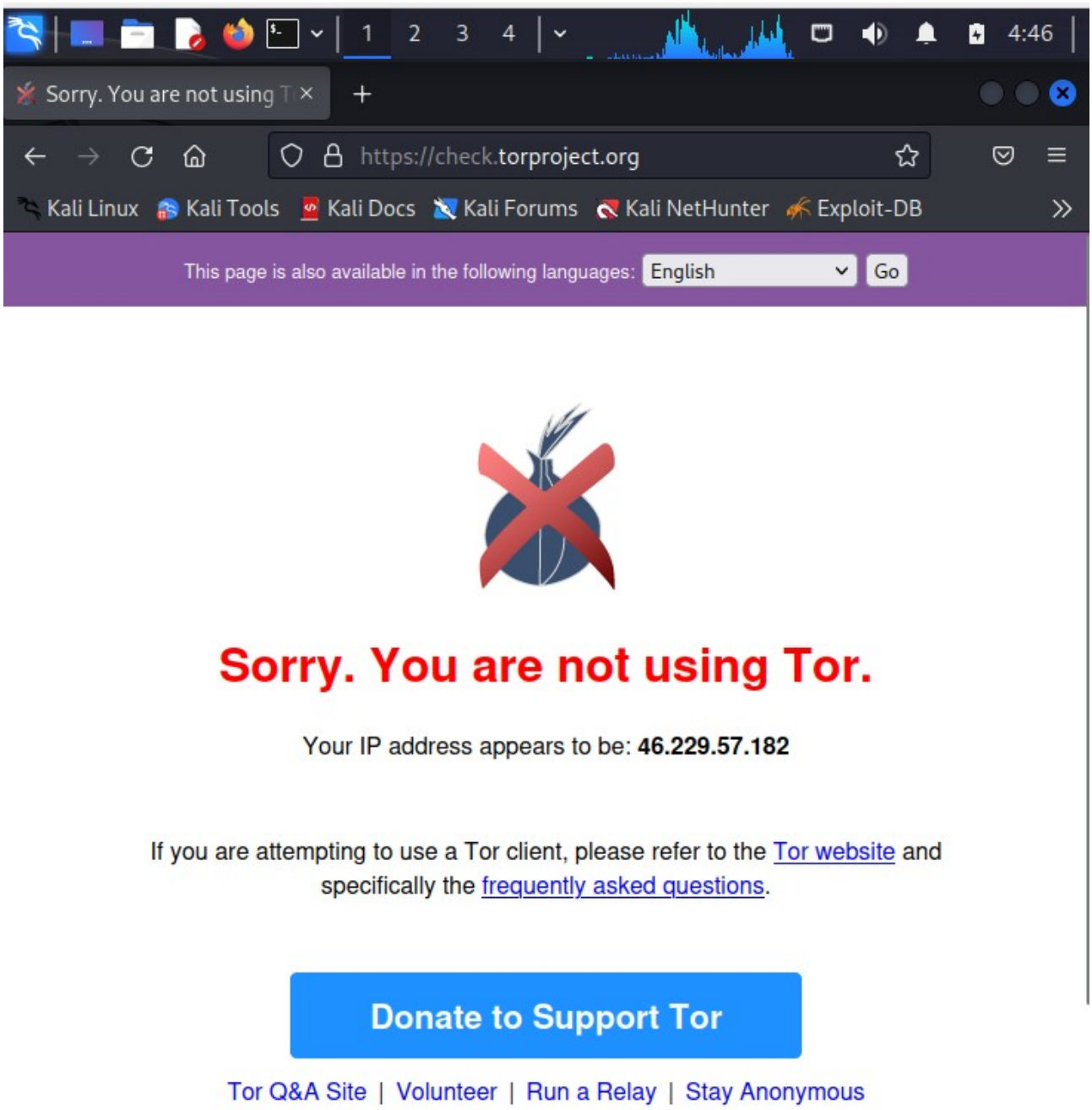


Перевірка статусу tor:



2.3 Запустити службу Tor. Відкрити у браузері (Firefox) ресурс TorCheck (https://check.torproject.org/).

Який результат отримано?



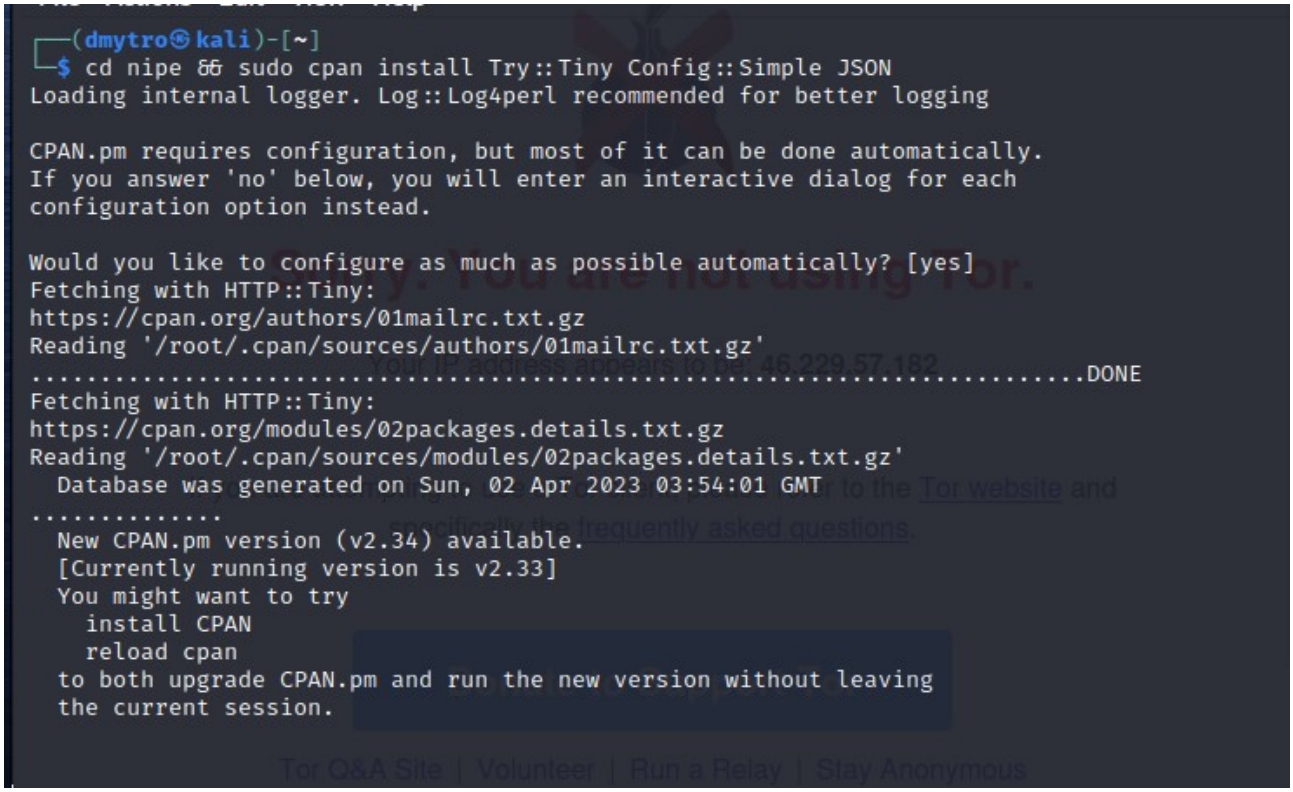
Чи вдалося приховати IP-адресу і визначити, що браузер працює не через Tor-мережу?

Ні, IP адреса не прихована й браузер не працює через мережу Tor

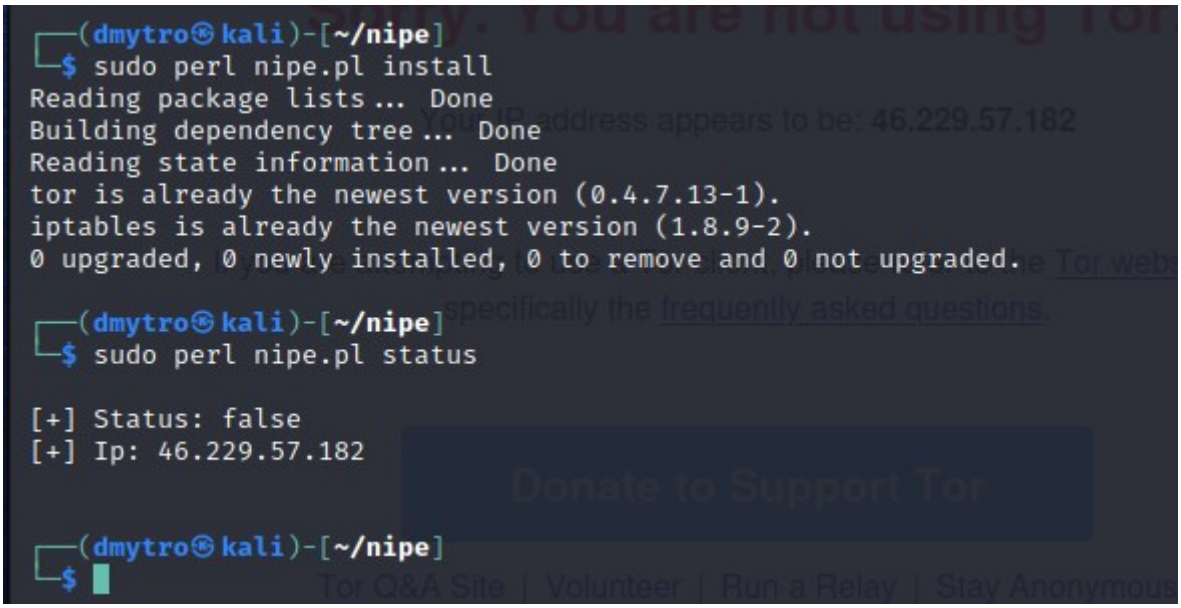
2.4 Здійснити за інструкцією встановлення NIPE.

Клонування репозиторію:

Встановлення Perl залежностей:



Встановлення та перевірка статусу nipe:

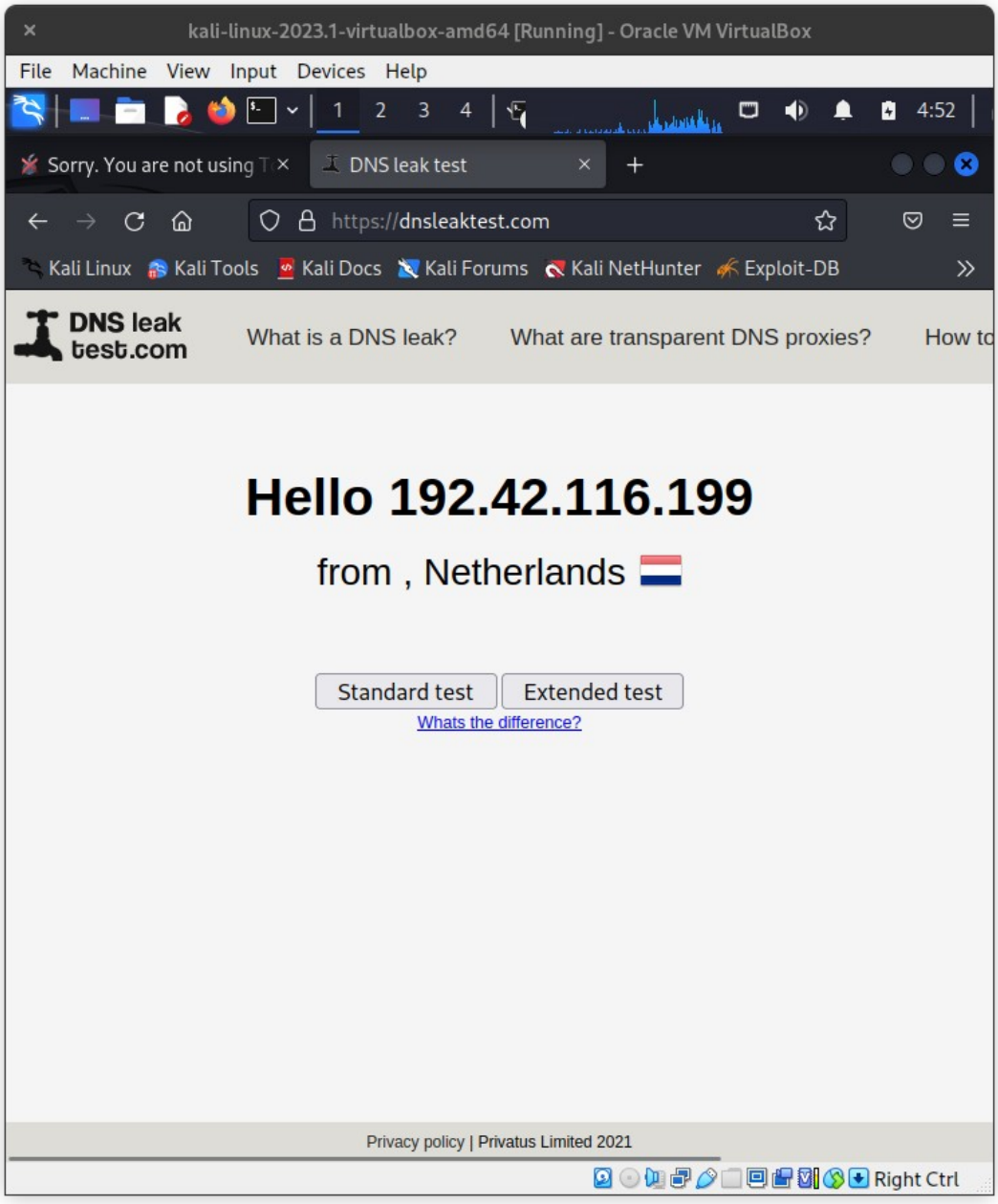


2.4 Запустити NIPE, перевірити статус.

Запуск та перевірка статусу nipe:

2.5 Перевірте поточну IP-адресу (наприклад, за допомогою ресурсу https://www.dnsleaktest.com/).

Який результат отримано?



Чи вдалося приховати IP-адресу?

Так, вдалося

2.6 Налаштувати Proxychains в Kali Linux і зберегти файл конфігурації.

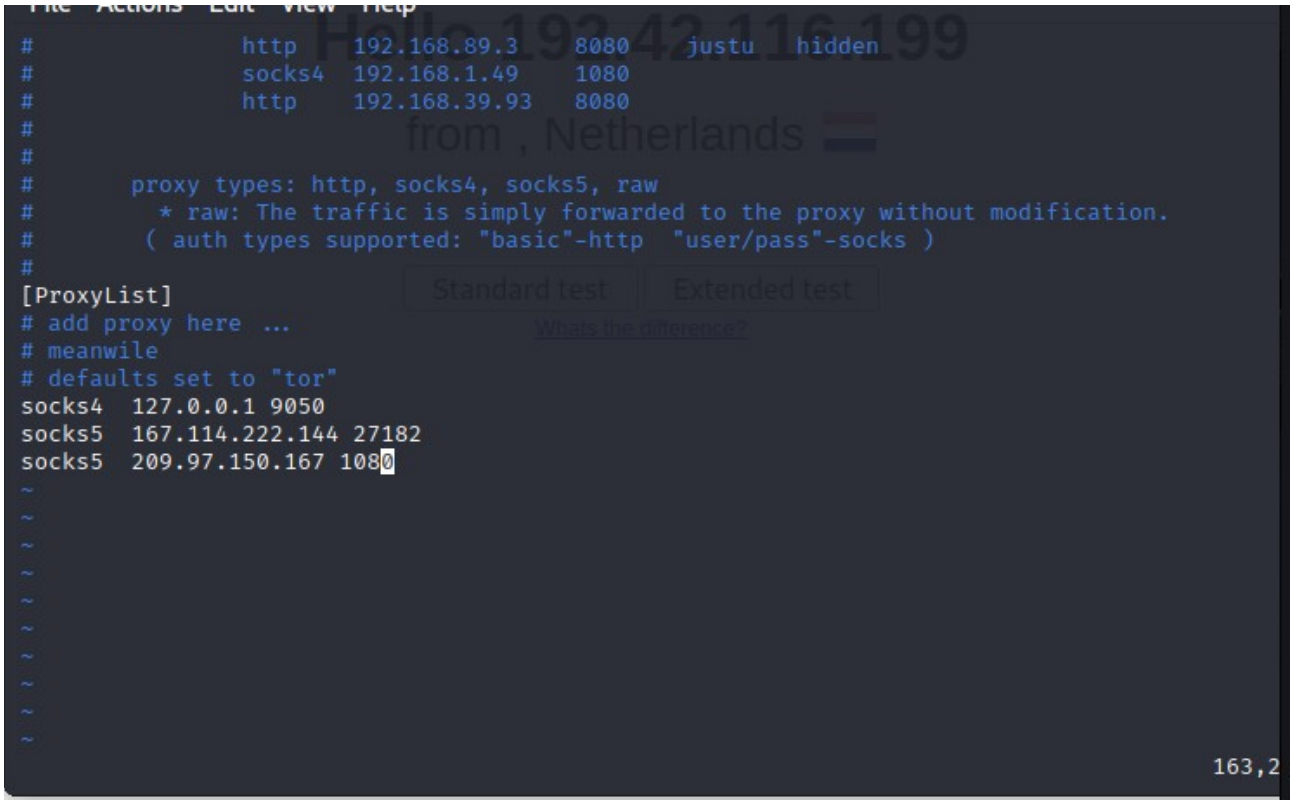
Перевірка наявності proxychains:

```
┌──(dmytro㉿kali)-[~]
└─$ proxychains

Usage:  proxychains -q -f config_file program_name [arguments]
        -q makes proxychains quiet - this overrides the config setting
        -f allows one to manually specify a configfile to use
        for example : proxychains telnet somehost.com
More help in README file


┌──(dmytro㉿kali)-[~]
└─$
```

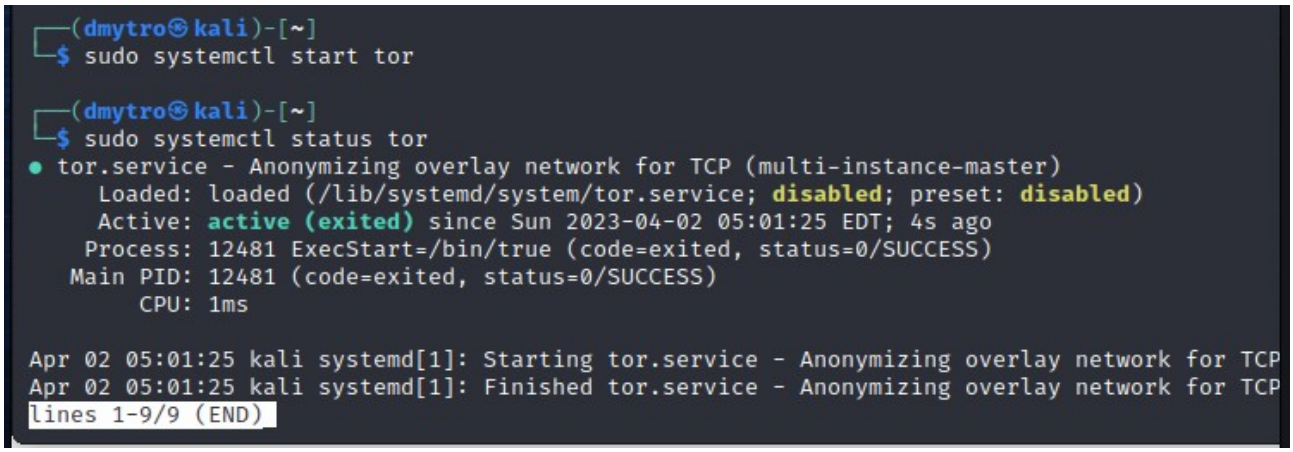
Зміна на dynamic_chain:

```
# proxychains.conf  VER 4.x
#
#        HTTP, SOCKS4a, SOCKS5 tunneling proxifier with DNS.


# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#round_robin_chain
#
                                                              21,27
```

Додам пару довлільних проксі:



2.7 Запустити службу Tor. Перевірити статус.

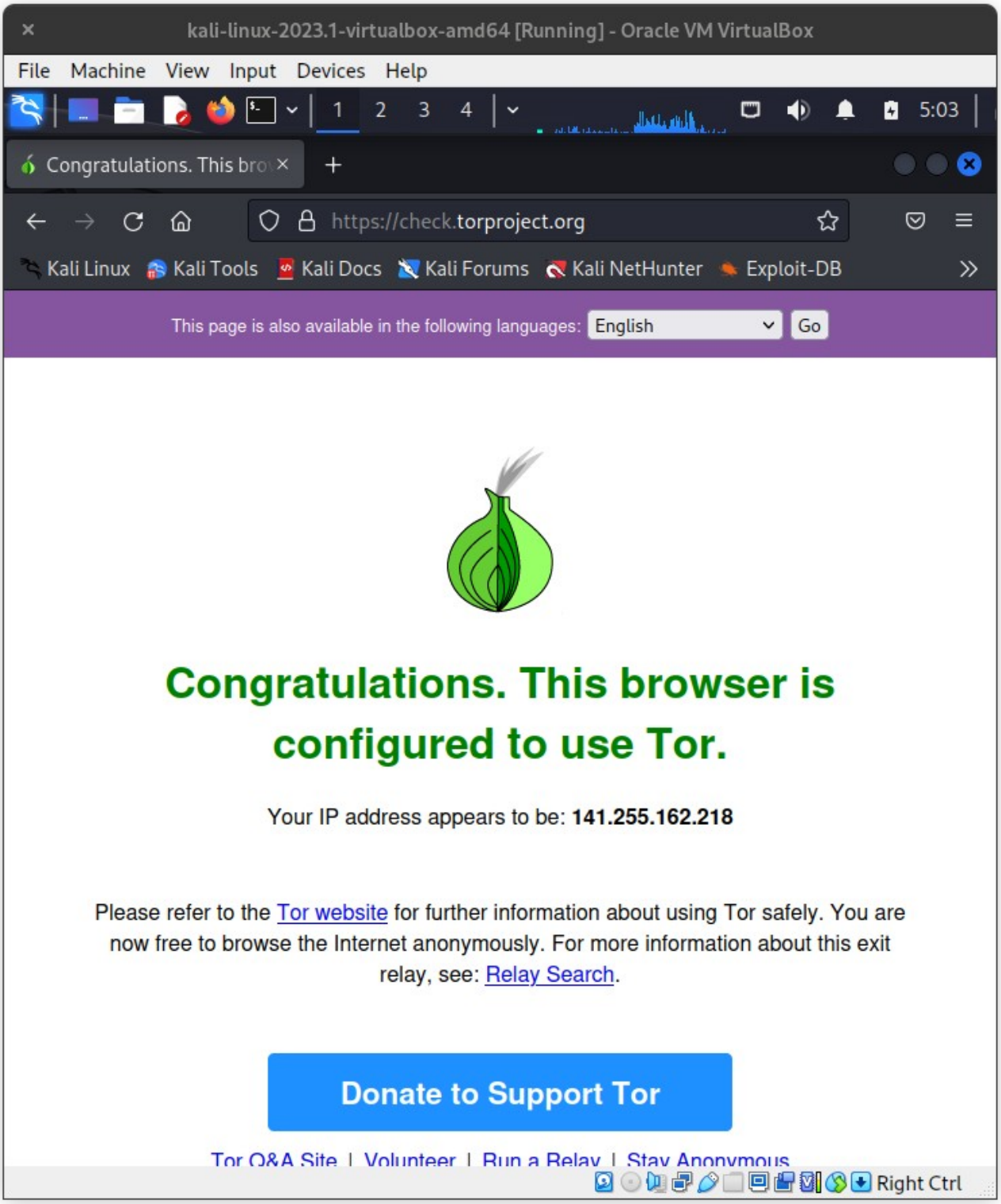


2.8 Запустити проксі-ланцюжки Proxychains, наприклад з браузером Firefox:

```
proxychains firefox
```

2.9 Відкрити у браузері (Firefox) ресурс TorCheck (https://check.torproject.org/).

Який результат отримано?



Чи вдалося приховати IP-адресу і визначити, що браузер працює не через Tor-мережу?

Так, тепер наш браузер використовує мережу Tor

Висновок:

Який із запропонованих способів анонімності Ви би обрали для подальшої роботи в Kali Linux?

Залежить від того, що нам необхідно зробити. Дуже часто нормальні системи знають які IP адреси належать до вихідних шлюзів Tor, тому запити з таких адрес часто блокуються. Нижче приклад такого детекту від Google. Тому якщо ми хочемо мімікрувати під звичайного користувача, то краще використовувати якісь звичайні публічні проксі. Але якщо нам потрібно максимально сховатися, то однозначно Tor.