

**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 справне 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 зашифроване 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:

```
(dmytro@kali)-[~]  
$ sudo apt update && sudo apt upgrade  
[sudo] password for dmytro:  
Hit:1 http://fastmirror.pp.ua/kali kali-rolling InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
All packages are up to date.  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Calculating upgrade... Done  
The following packages were automatically installed and are no longer required:  
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211  
  firmware-intel-sound firmware-iwlwifi firmware-libertas  
  firmware-realtek firmware-sof-signed firmware-ti-connectivity  
  firmware-zd1211 kali-linux-firmware  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
  
(dmytro@kali)-[~]  
$
```

## Встановлення tor:

```
(dmytro@kali)-[~]
$ sudo apt install tor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211
  firmware-intel-sound firmware-iwlwifi firmware-libertas
  firmware-realtek firmware-sof-signed firmware-ti-connectivity
  firmware-zd1211 kali-linux-firmware
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher apparmor-utils nyx obfs4proxy
The following NEW packages will be installed:
  tor tor-geoipdb torsocks
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,570 kB of archives.
After this operation, 17.1 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://fastmirror.pp.ua/kali kali-rolling/main amd64 tor amd64 0.4.
7.13-1 [1,995 kB]
Get:2 http://fastmirror.pp.ua/kali kali-rolling/main amd64 tor-geoipdb al
l 0.4.7.13-1 [1,501 kB]
```

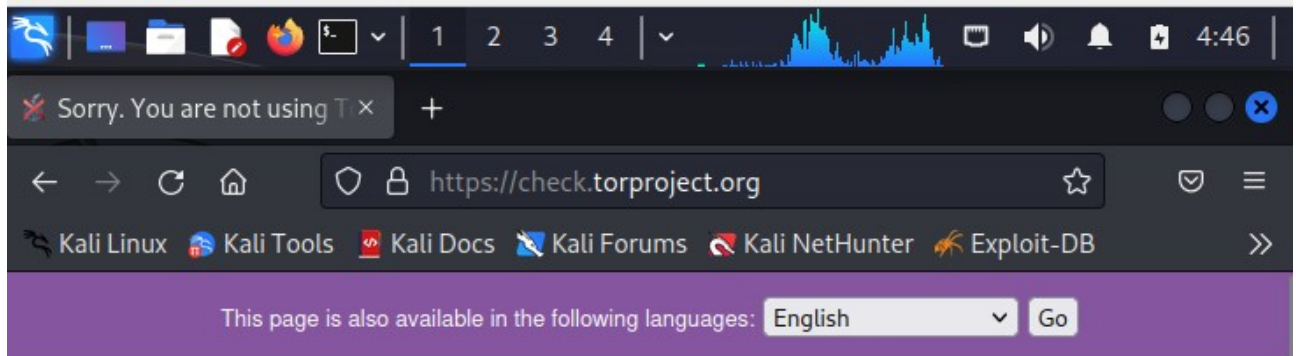
## Перевірка статусу tor:

```
(dmytro@kali)-[~]
$ sudo systemctl status tor -l
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; preset: disabled)
   Active: active (exited) since Sun 2023-04-02 04:44:31 EDT; 27s ago
     Process: 3259 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 3259 (code=exited, status=0/SUCCESS)
      CPU: 1ms

Apr 02 04:44:31 kali systemd[1]: Starting tor.service - Anonymizing overlay network>
Apr 02 04:44:31 kali systemd[1]: Finished tor.service - Anonymizing overlay network>
lines 1-9/9 (END)
```

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

Який результат отримано?



**Sorry. You are not using Tor.**

Your IP address appears to be: **46.229.57.182**

If you are attempting to use a Tor client, please refer to the [Tor website](#) and specifically the [frequently asked questions](#).

**Donate to Support Tor**

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)



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

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

## 2.4 Здійснити за інструкцією встановлення NIPE.

Клонування репозиторію:

```
(dmytro@kali)-[~]
$ git clone https://github.com/htrgouvea/nipe
Cloning into 'nipe' ...
remote: Enumerating objects: 1714, done.
remote: Counting objects: 100% (185/185), done.
remote: Compressing objects: 100% (108/108), done.
remote: Total 1714 (delta 73), reused 145 (delta 57), pack-reused 1529
Receiving objects: 100% (1714/1714), 262.90 KiB | 1.80 MiB/s, done.
Resolving deltas: 100% (886/886), done.
```

Встановлення Perl залежностей:

```
(dmytro@kali)-[~]
$ cd nipe && sudo cpan install Try::Tiny Config::Simple JSON
Loading internal logger. Log::Log4perl recommended for better logging

CPAN.pm requires configuration, but most of it can be done automatically.
If you answer 'no' below, you will enter an interactive dialog for each
configuration option instead.

Would you like to configure as much as possible automatically? [yes]
Fetching with HTTP::Tiny:
https://cpan.org/authors/01mailrc.txt.gz
Reading '/root/.cpan/sources/authors/01mailrc.txt.gz'
.....DONE
Fetching with HTTP::Tiny:
https://cpan.org/modules/02packages.details.txt.gz
Reading '/root/.cpan/sources/modules/02packages.details.txt.gz'
Database was generated on Sun, 02 Apr 2023 03:54:01 GMT
.....
New CPAN.pm version (v2.34) available.
[Currently running version is v2.33]
You might want to try
  install CPAN
  reload cpan
to both upgrade CPAN.pm and run the new version without leaving
the current session.
```

Встановлення та перевірка статусу nipe:

```
(dmytro@kali)-[~/nipe]
$ sudo perl nipe.pl install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tor is already the newest version (0.4.7.13-1).
iptables is already the newest version (1.8.9-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(dmytro@kali)-[~/nipe]
$ sudo perl nipe.pl status

[+] Status: false
[+] Ip: 46.229.57.182

(dmytro@kali)-[~/nipe]
$
```

2.4 Запустити NIPE, перевірити статус.

Запуск та перевірка статусу nipe:

```
(dmytro@kali)-[~/nipe]
$ sudo perl nipe.pl start
starting to use a Tor client, please refer to the Tor website
specifically the frequently asked questions.

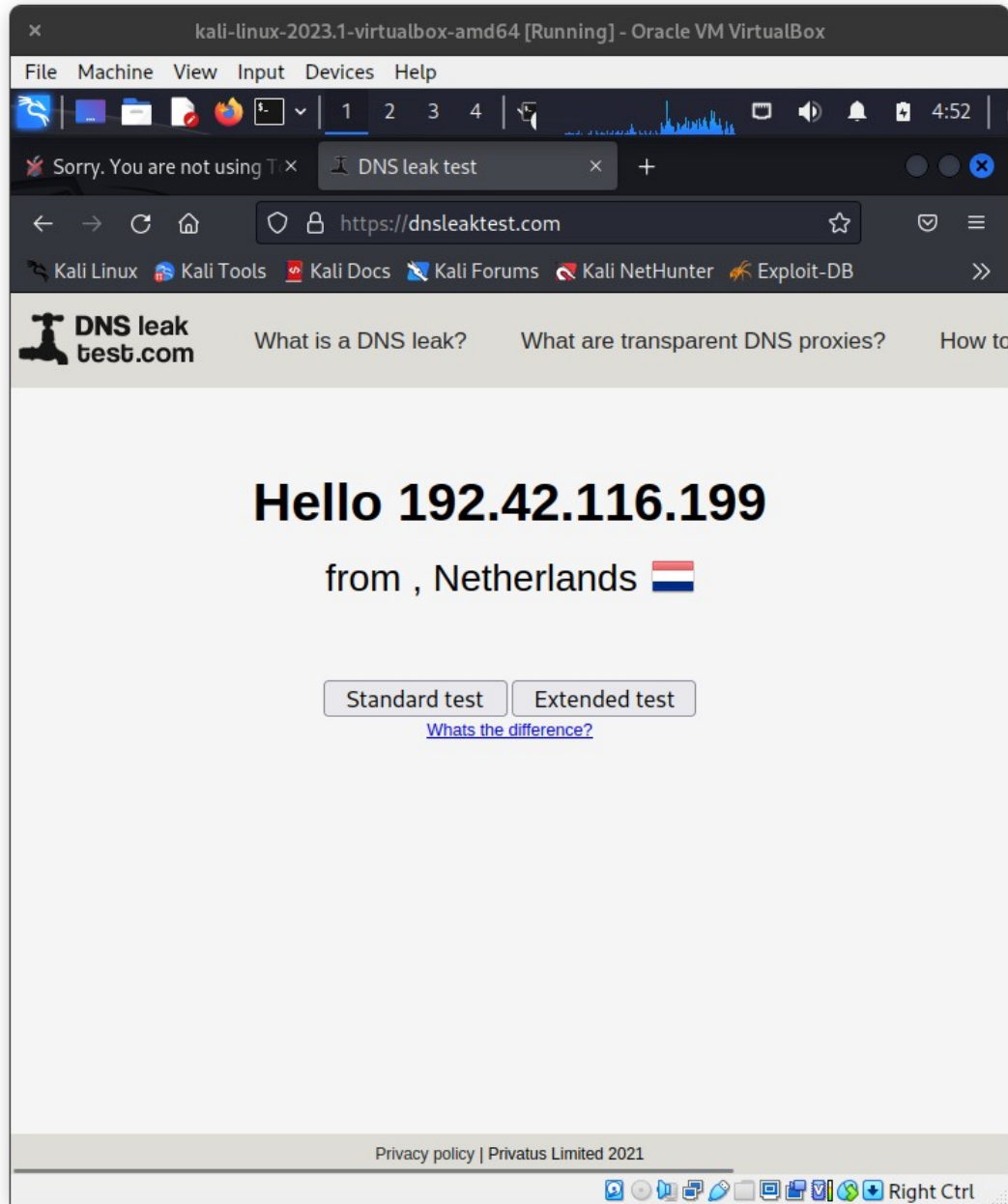
(dmytro@kali)-[~/nipe]
$ sudo perl nipe.pl status

[+] Status: true
[+] Ip: 192.42.116.199

(dmytro@kali)-[~/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:

```
File Actions Edit View Help
# 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      Standard test  Extended test
#
# 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
#
```

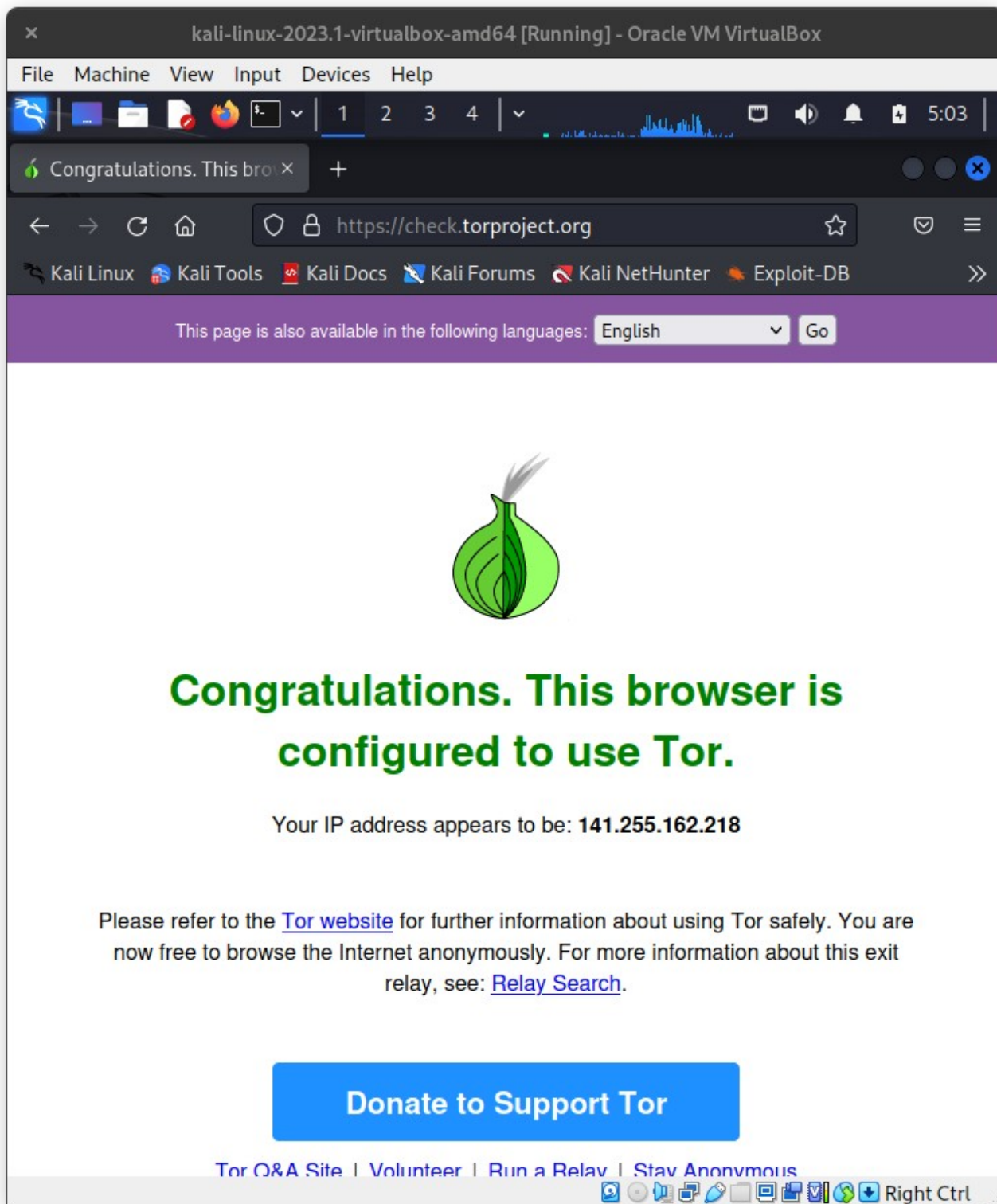


2.8 Запустити проксі-ланцюжки Proxuchains, наприклад з браузером Firefox:

proxuchains 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 Тор-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 Тор, тому запити з таких адрес часто блокуються. Нижче приклад такого детекту від Google. Тому якщо ми хочемо мімікувати під звичайного користувача, то краще використовувати якісь звичайні публічні проксі. Але якщо нам потрібно максимально сховатися, то однозначно Тор.

