

PRACTICA 3

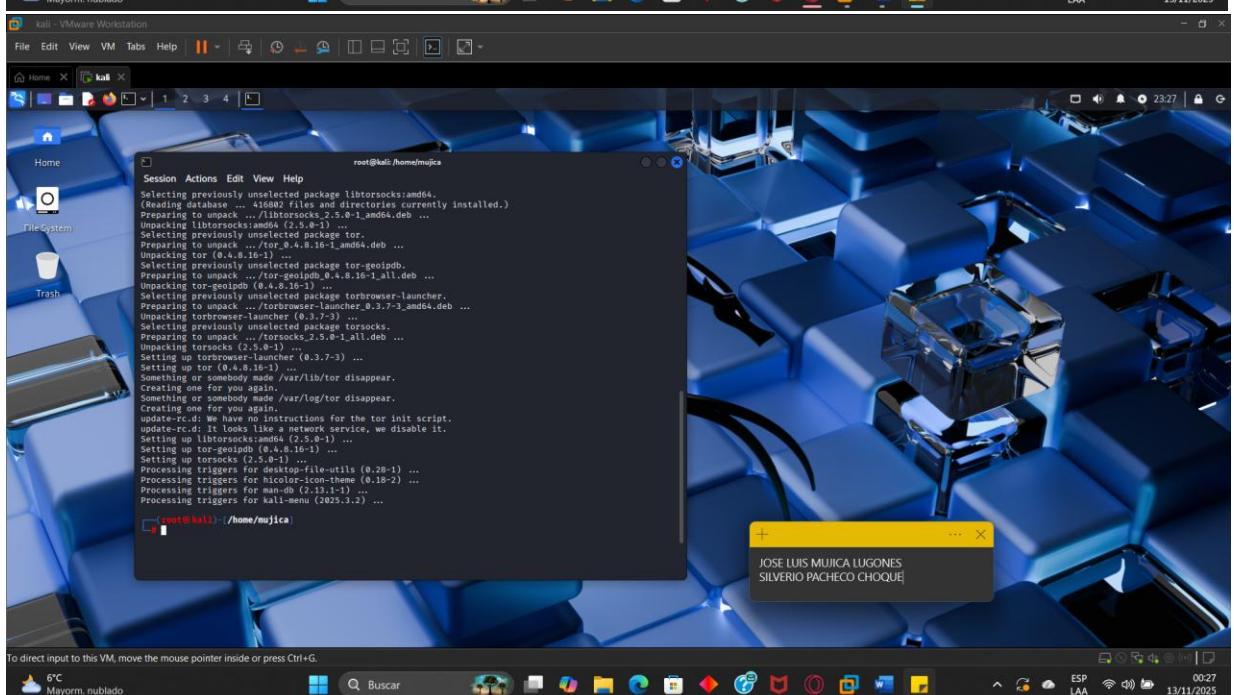
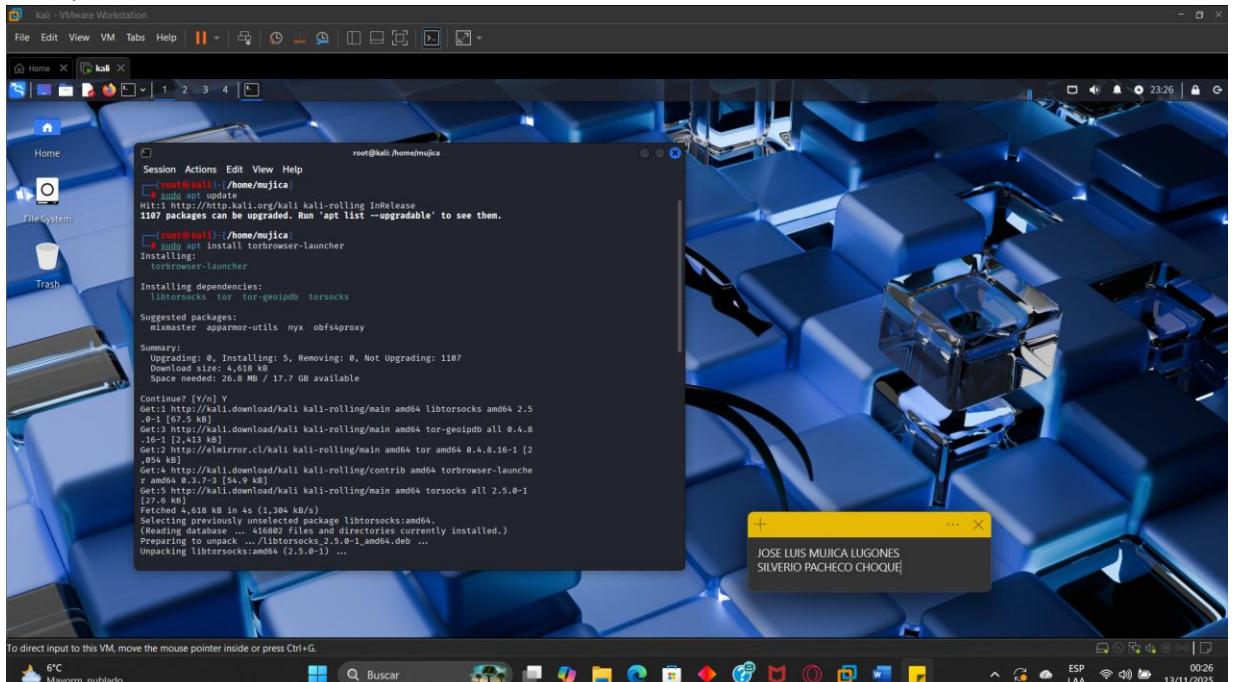
NOMBRE: JOSE LUIS MUJICA LUGONES
SILVERIO PACHECO CHOQUE

MATERIA: SEGURIDAD DE SISTEMAS

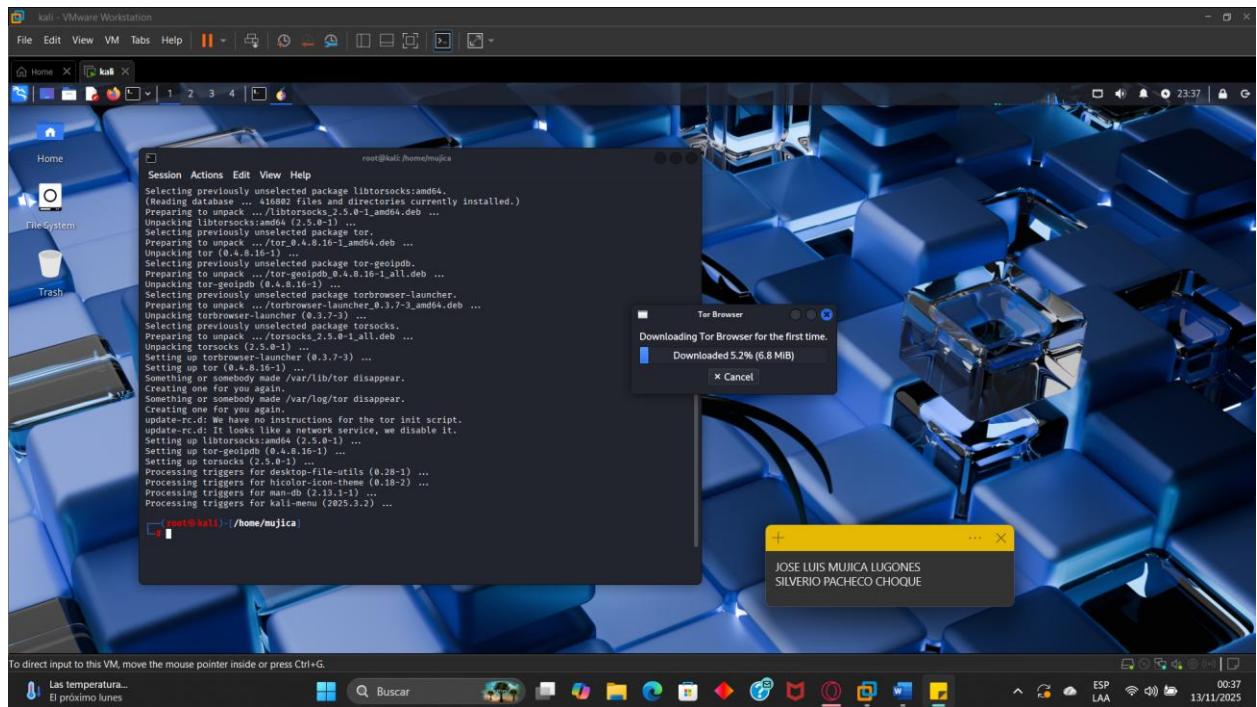
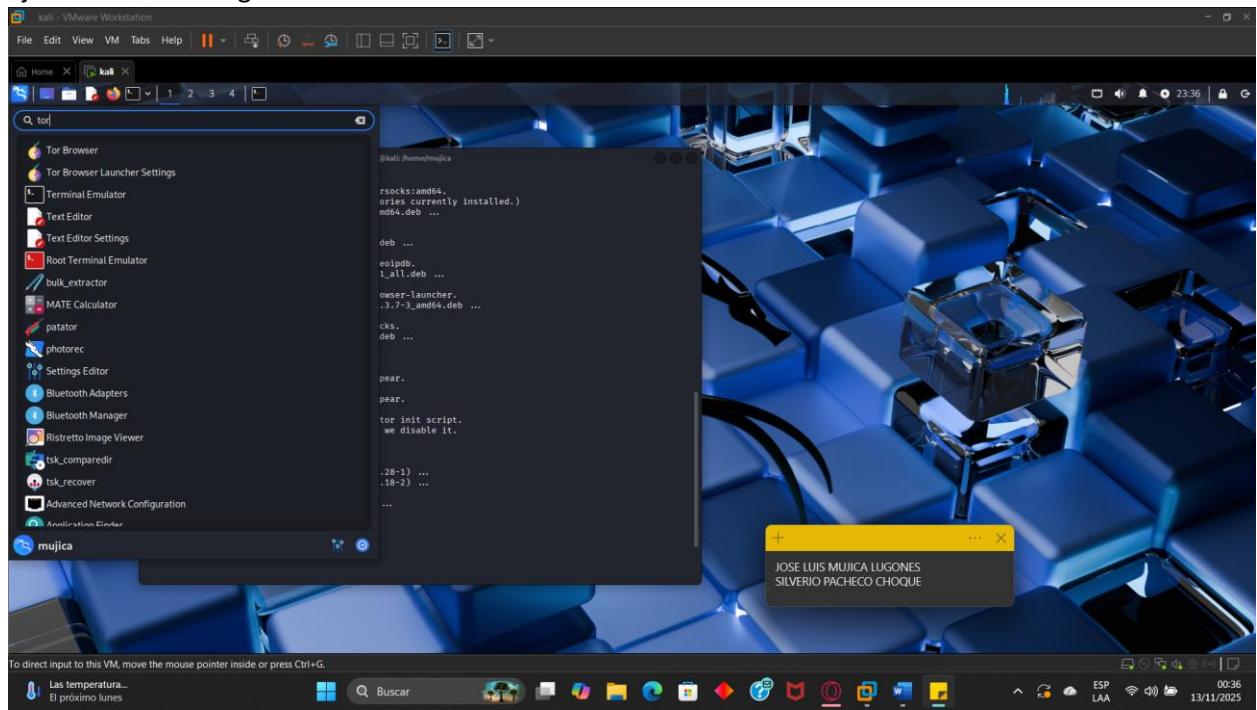
1. Instalación de Tor Browser en Kali.

Sudo apt update

Sud apt install torbrowser-launcher

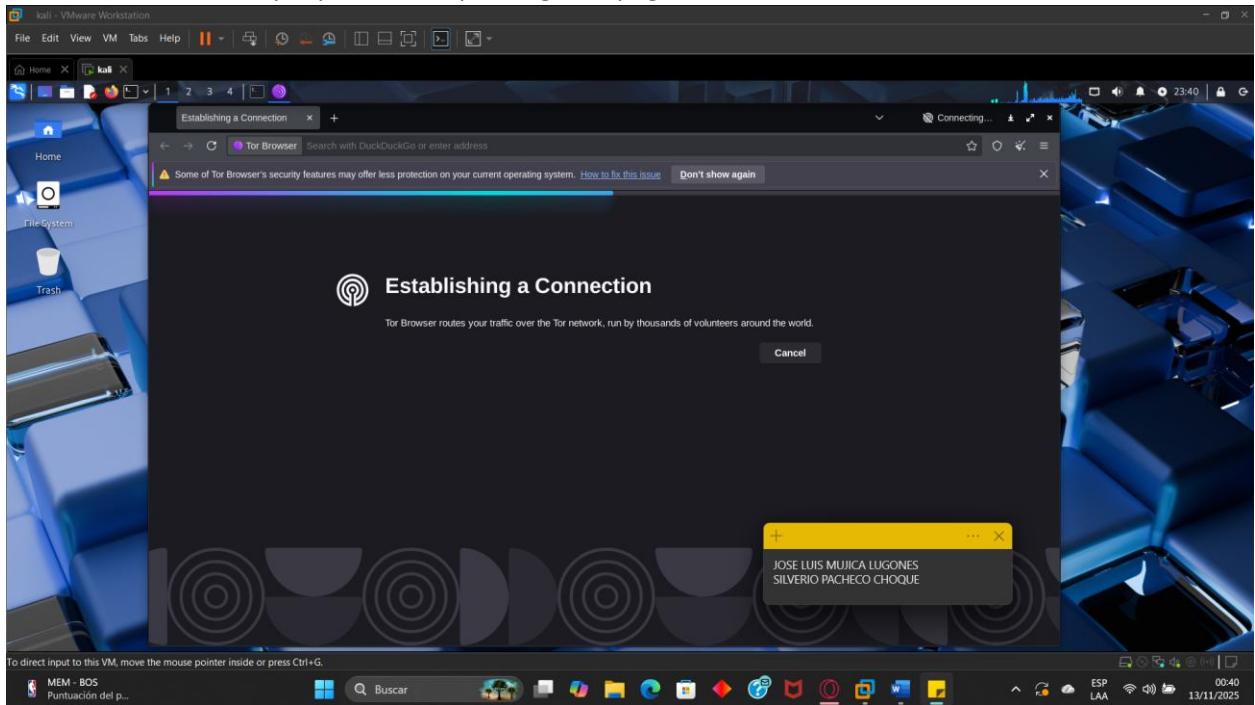


2. Ejecutamos el navegador Tor:

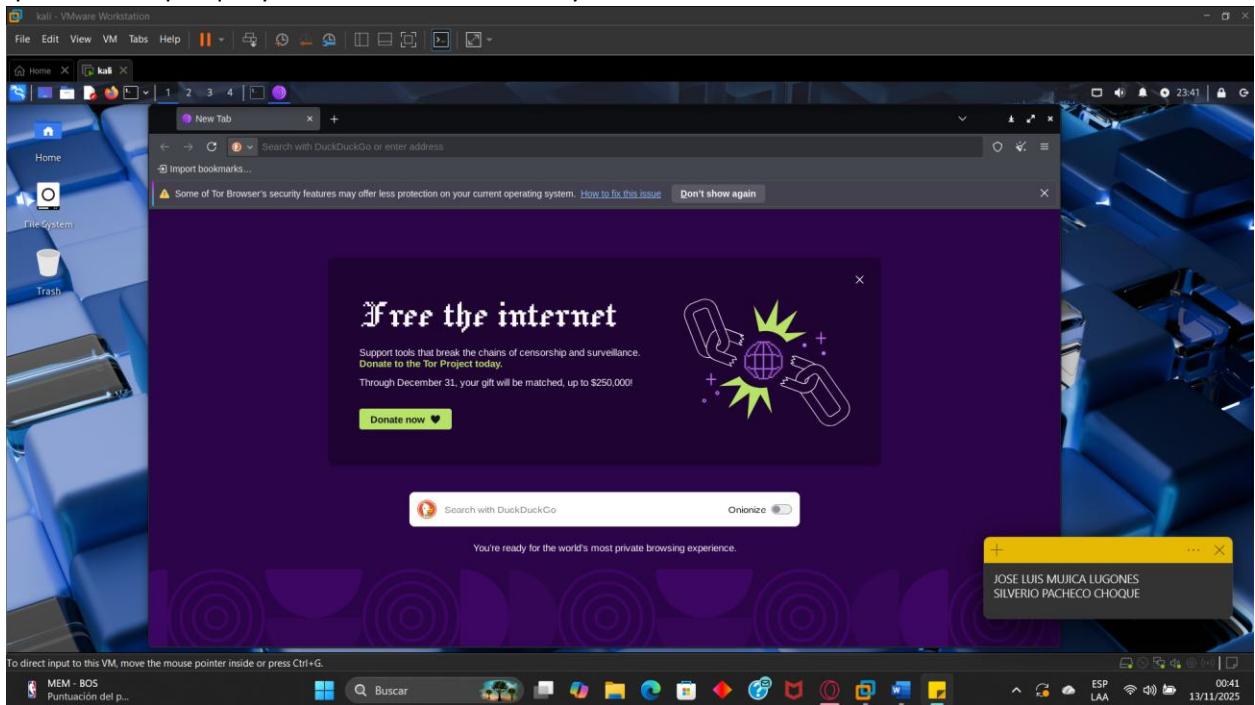


3. Seguiremos los siguientes pasos.

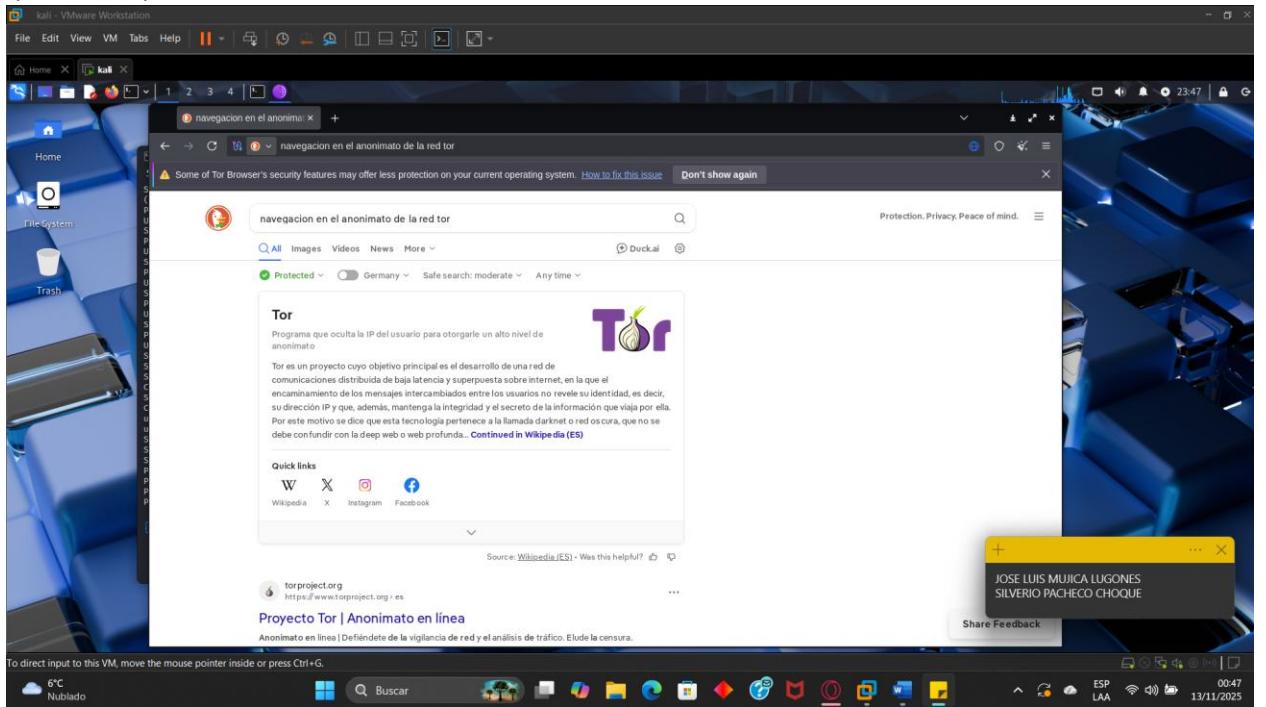
Ponemos en conectar y esperemos a que cargue la página.



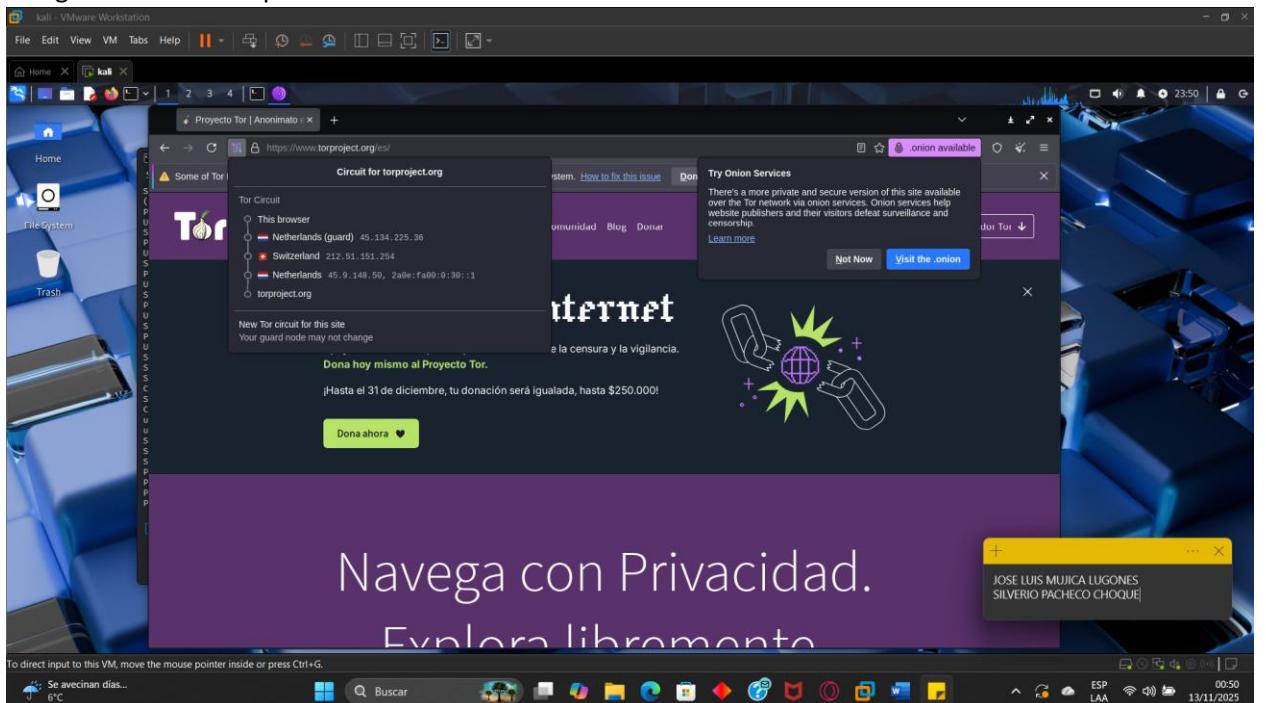
Una vez que cargo la pagina podemos observar que nos dice que estamos conectados, eso quiere decir que ya tenemos VPN activado y estamos en la red TOR.



Ahora lo que se hará es entrar dentro de una pagina normal primeramente y veremos como es que se comporta.

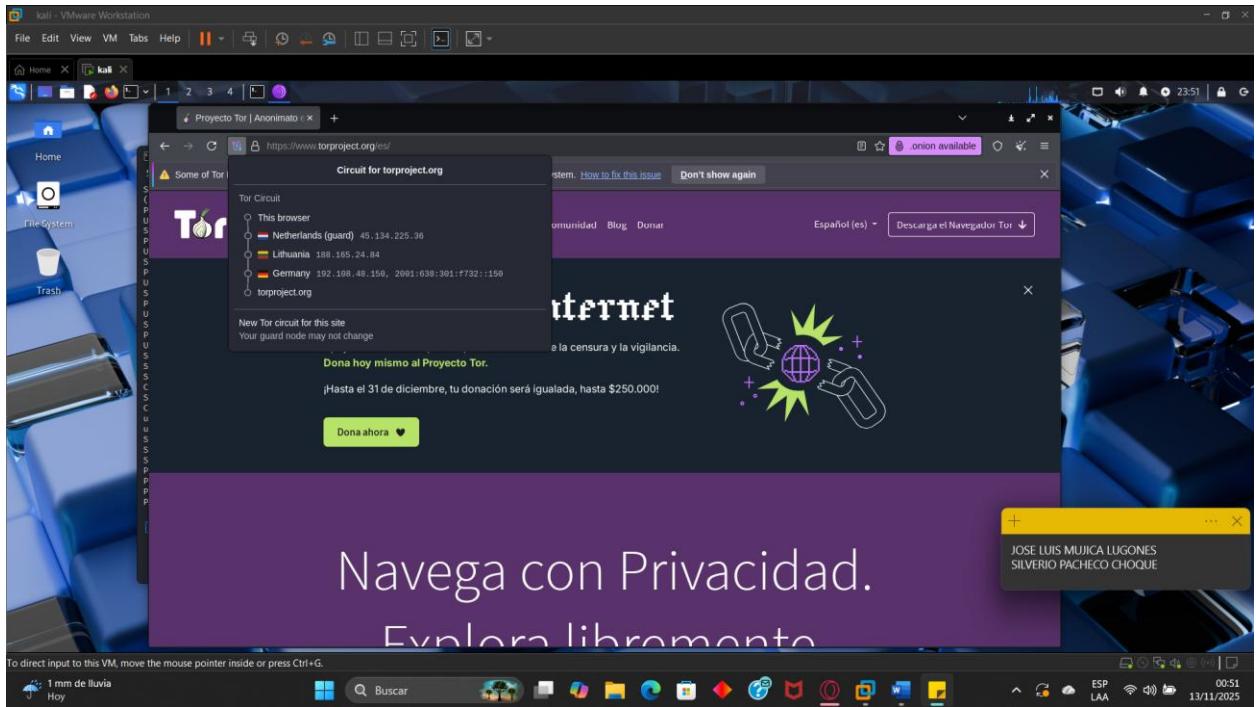


Luego hacemos click para ver los los circuitos.

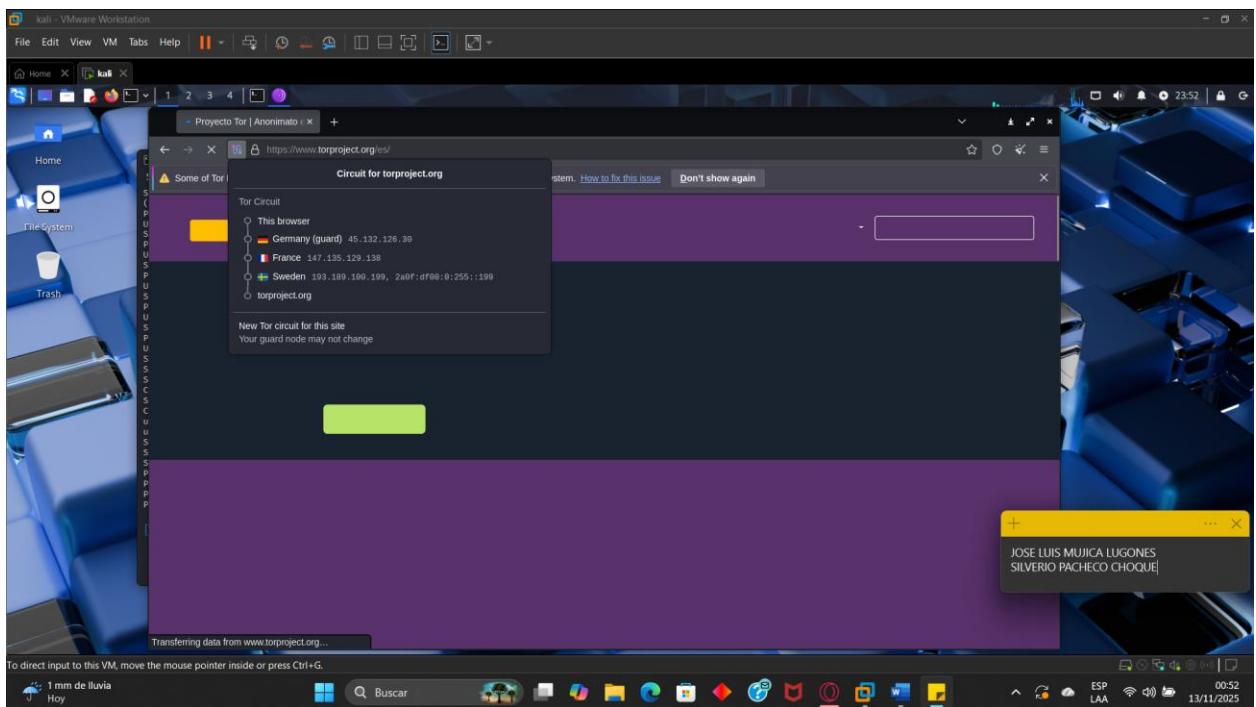


Cambiar el circuito de Tor manualmente de 3 a 5 veces.

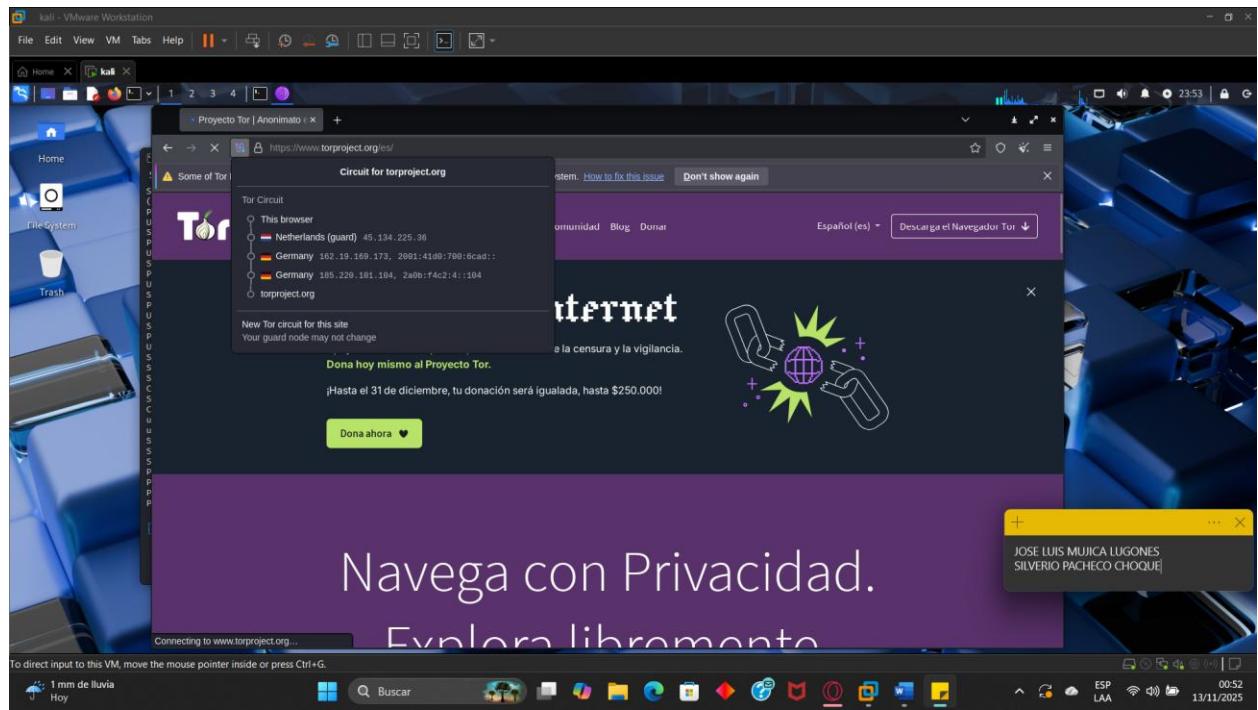
1



2

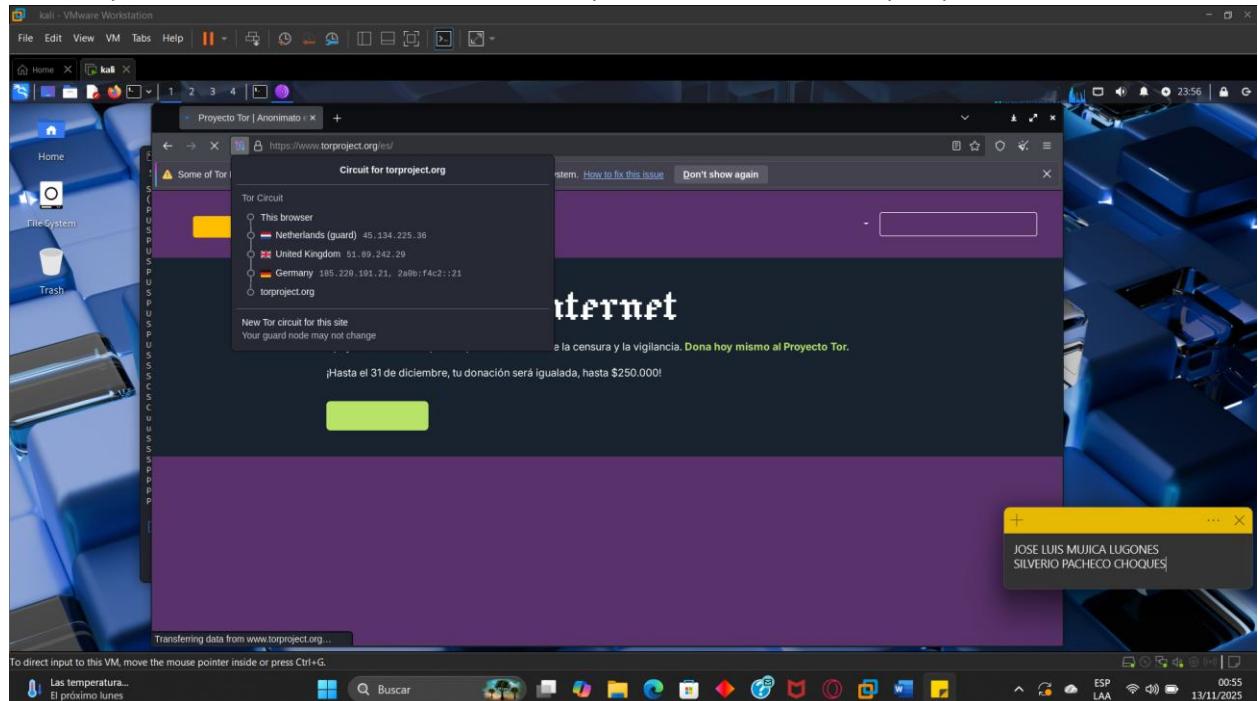


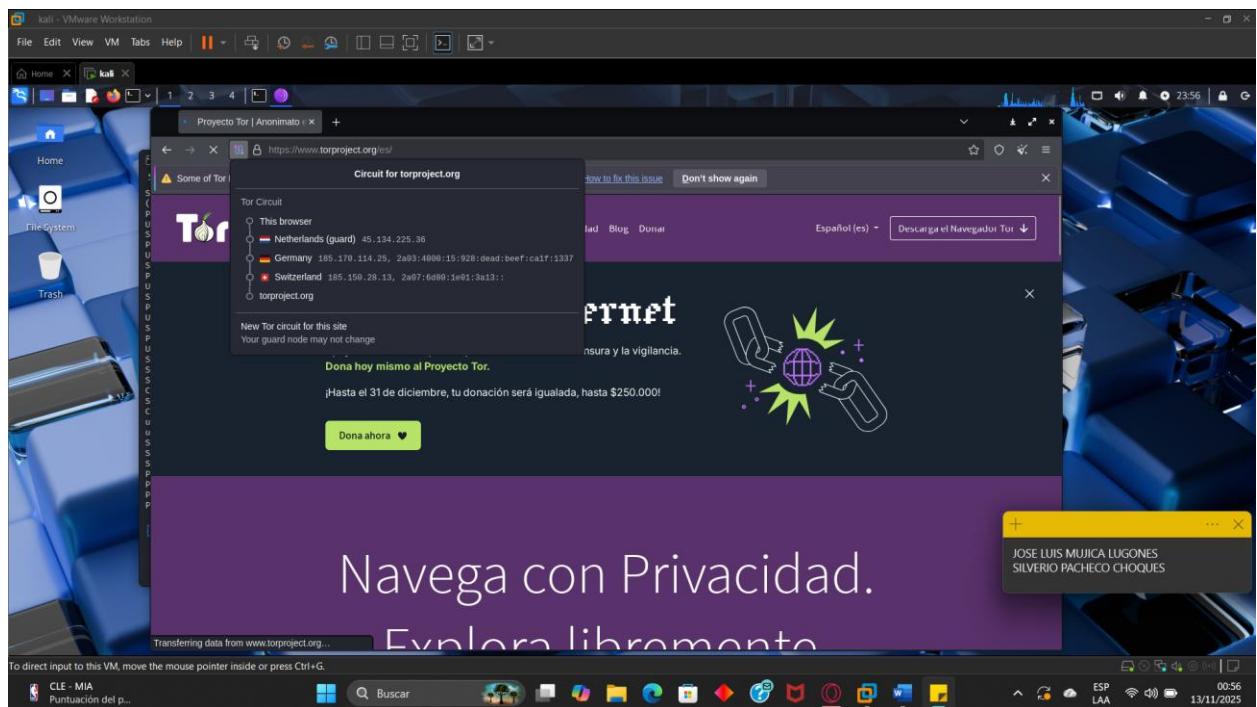
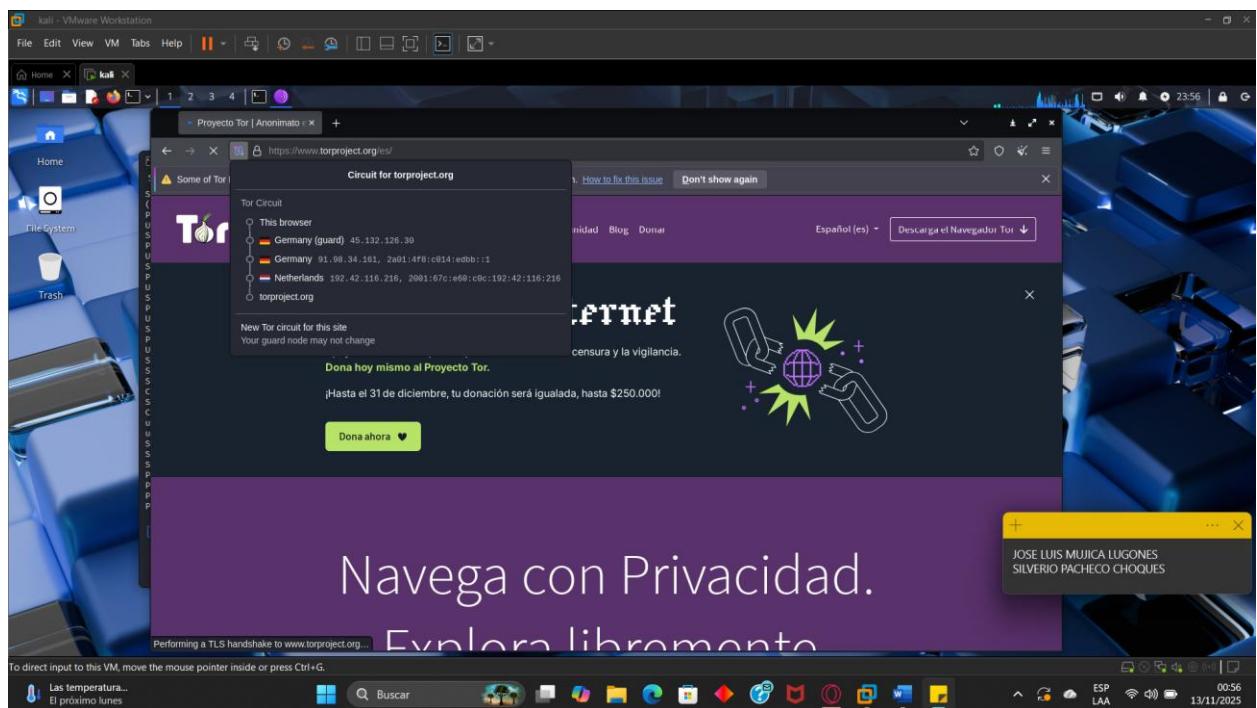
3

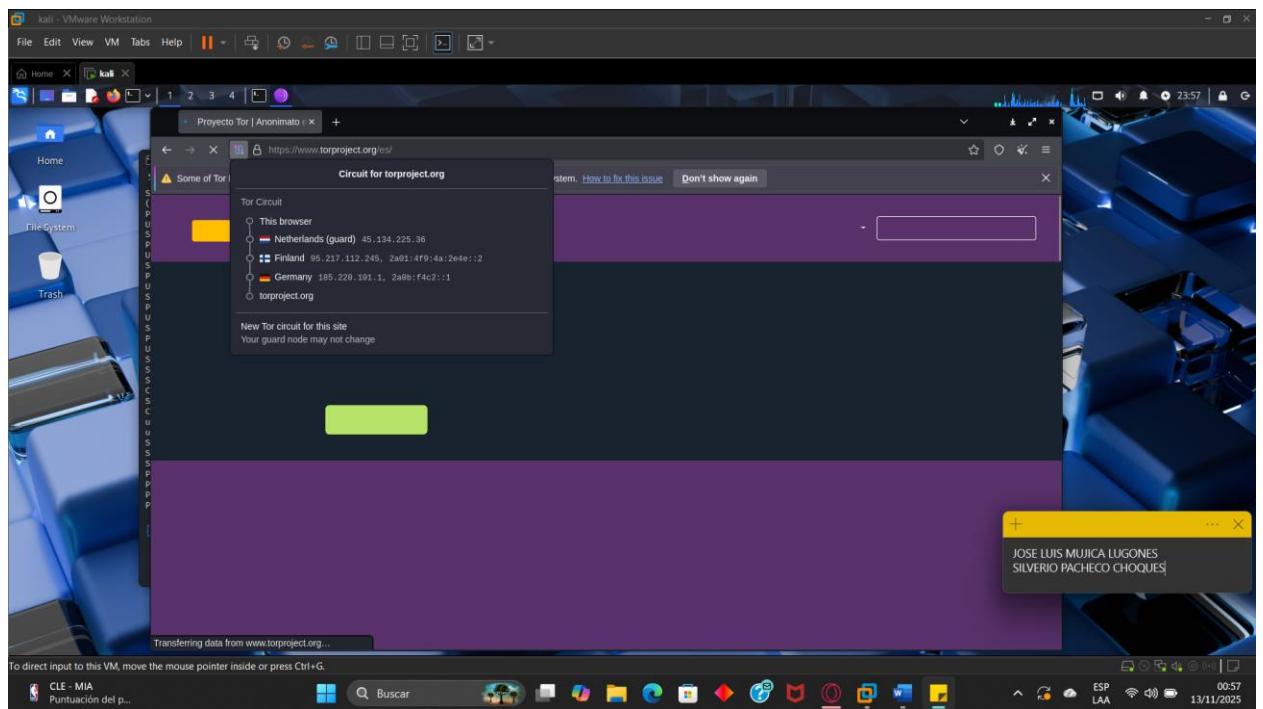
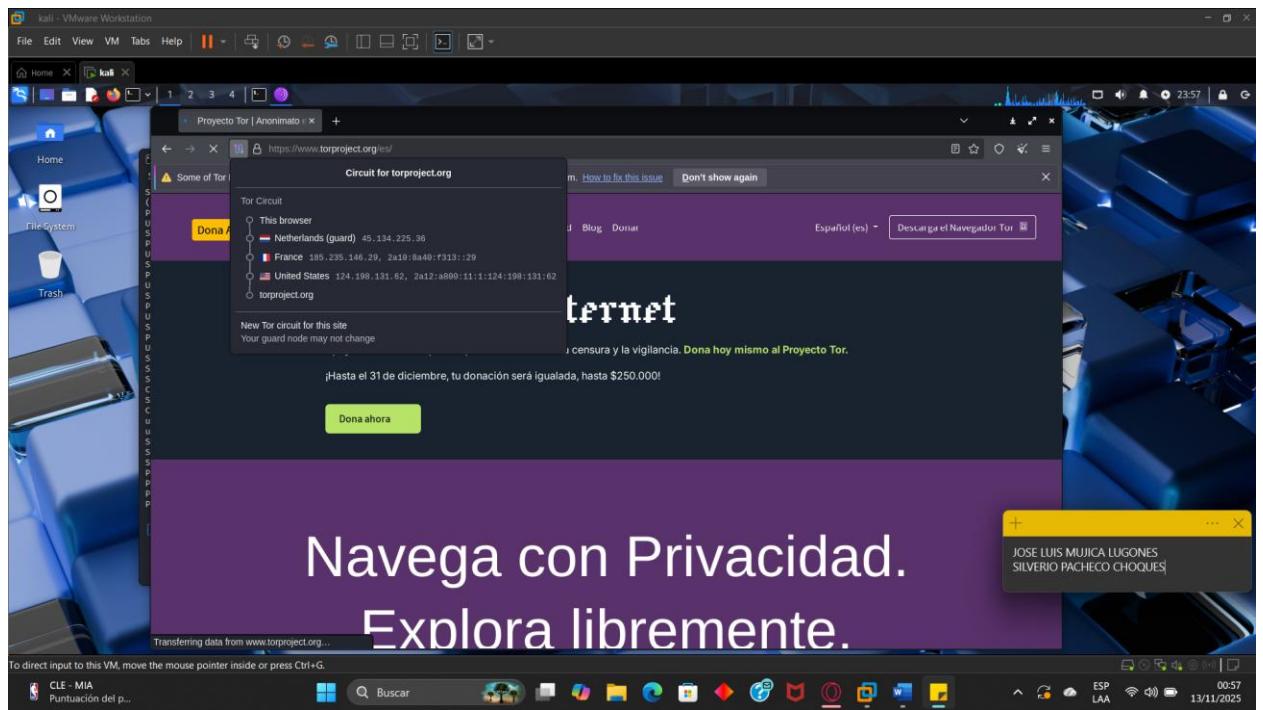


EVALUACION 1

Toma capturas de cada nuevo circuito, anota los países/IPS involucrados, y responda.







EVALUACION 1

1) ¿Por qué aparecen ciertos países más seguido?

R: Aparecen más seguido porque la red Tor es mantenida por **voluntarios**. Los países que tienen **más relés** o nodos Tor disponibles (como Estados Unidos o Alemania) tienen más posibilidades de ser elegidos. Además, Tor intenta usar los relés que son más **rápidos y estables**, y muchos de estos están concentrados en países con mejor infraestructura de internet.

2) ¿Hay algún patrón?

R: Sí, hay dos patrones principales:

- **Patrón de Diversidad:** El circuito de Tor (Guarda, Intermedio, Salida) casi siempre usa **tres países diferentes** para evitar que una sola entidad pueda vigilar todo el camino.
- **Patrón de Estabilidad (Guarda):** El **primer país (Nodo de Guardia)** no cambia cada vez que pides un "Nuevo circuito Tor". Solo cambian los nodos intermedio y de salida, ya que el nodo de guardia se mantiene fijo por semanas para aumentar la seguridad contra ciertos ataques.

3) Investigar si existe más navegadores que permitan estas funciones...

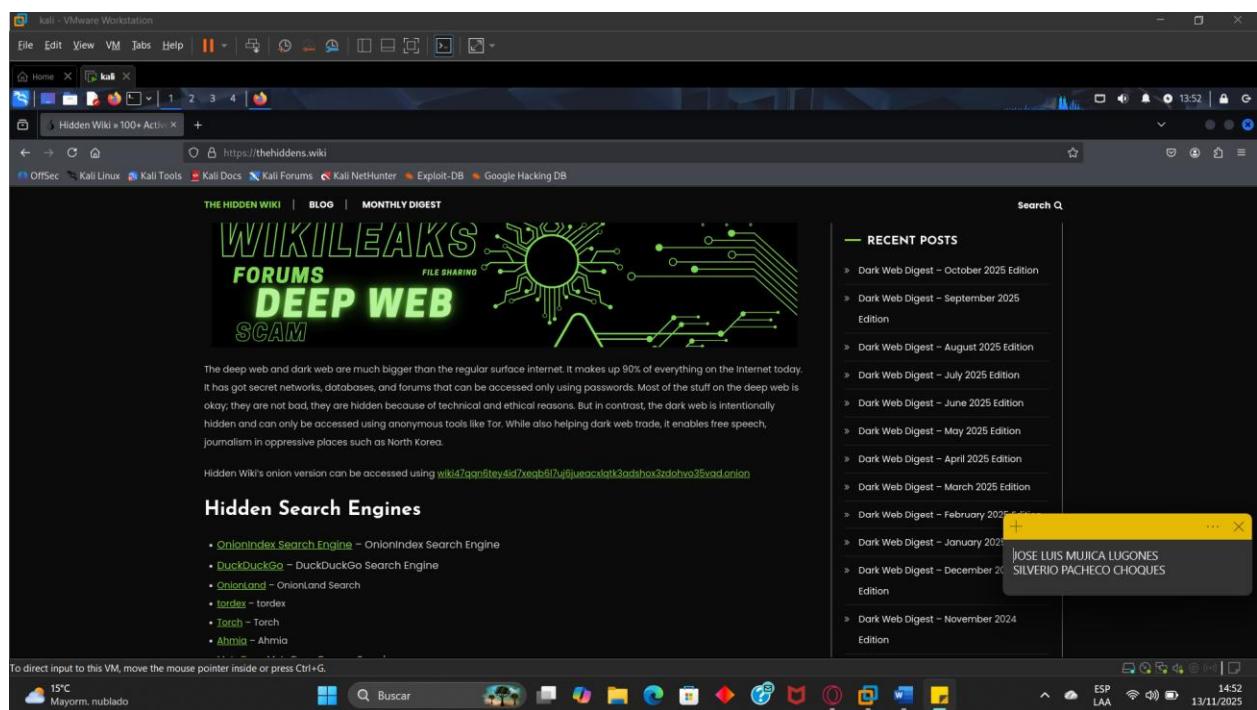
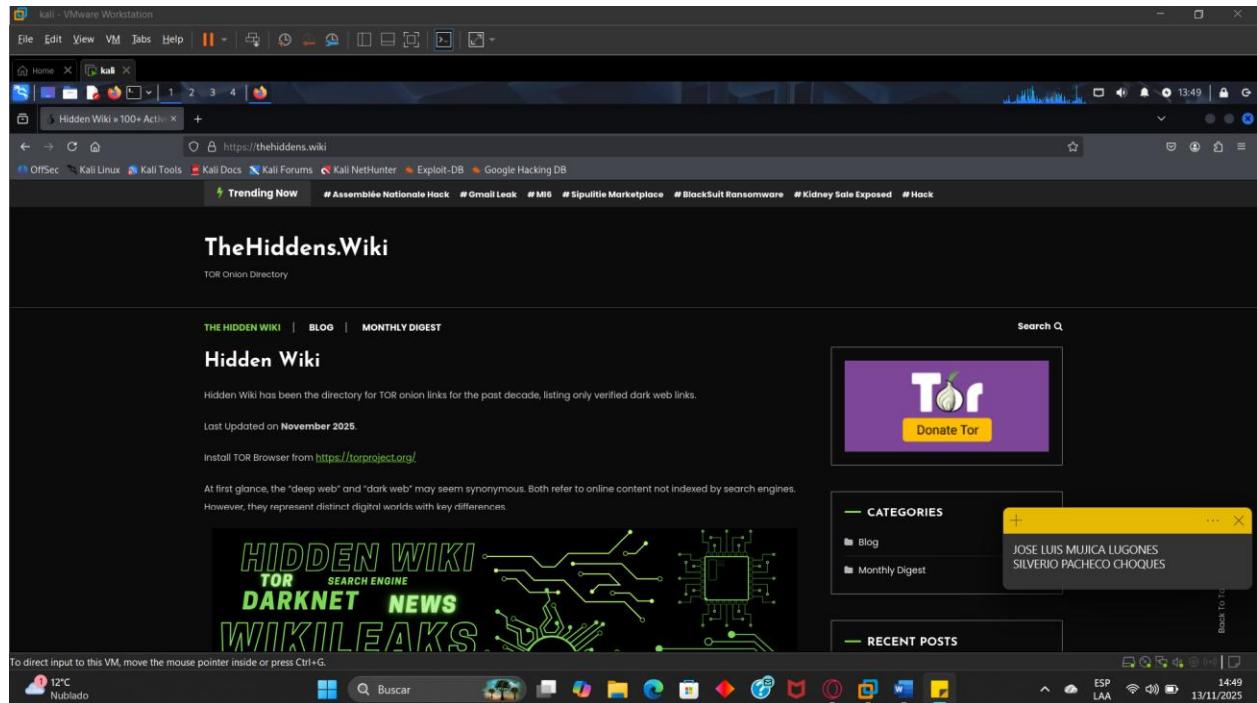
R: Sí, hay otros navegadores que ofrecen funciones similares de privacidad, aunque la red Tor es única.

- **Brave Browser:** Tiene una función integrada llamada "**Ventana Privada con Tor**" que usa la red Tor para ocultar la IP y la ubicación.
- **Epic Privacy Browser:** Usa un **proxy cifrado (como un VPN)** integrado para ocultar la IP.
- **VPNs:** Aunque no son navegadores, son el principal método para ocultar la IP al enrutar todo el tráfico por un servidor en otro país.

PARTE 2

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

Primeramente, lo que se hará es acceder desde un navegador normal su máquina física a esta página.



Si vamos buscando dentro de este sitio nos vamos a dar cuenta que justamente ahí se encuentra el enlace al

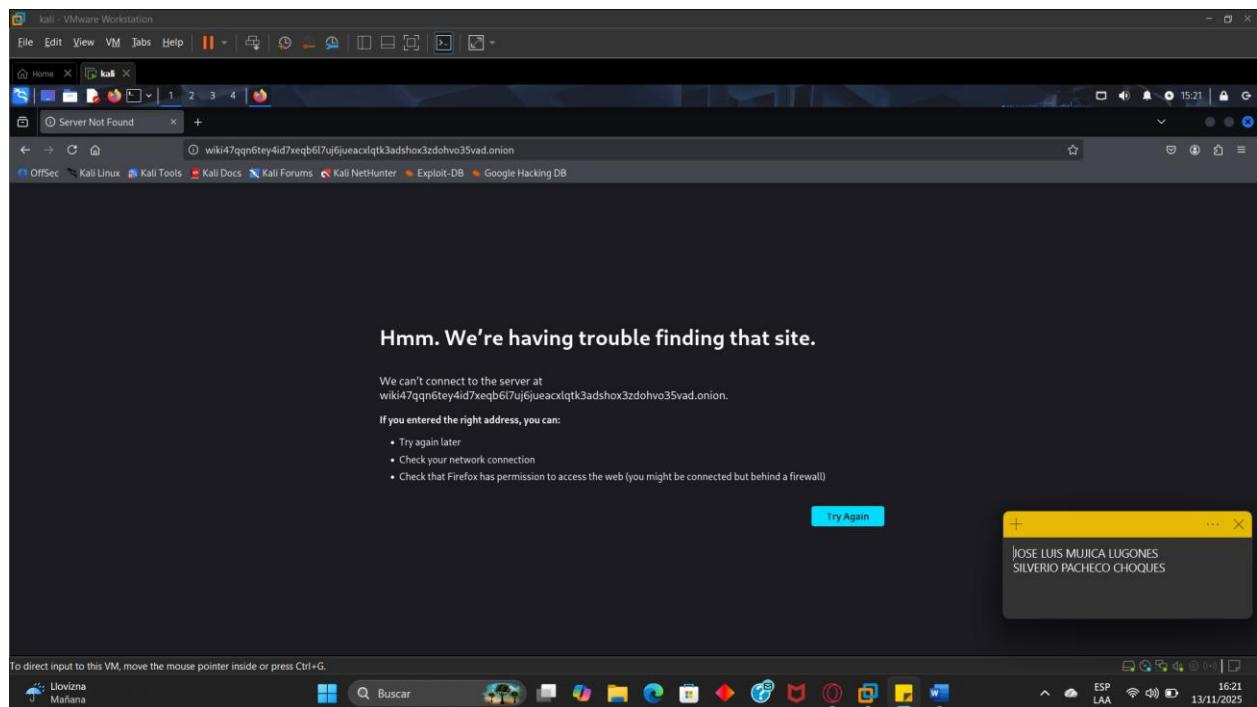
sitio web anteriormente mencionado el cual es el enlace .onion original:

<http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>

EVALUCION 2

1. Ahora lo que se debe hacer es intentar acceder a ese enlace desde un navegador normal (Firefox,

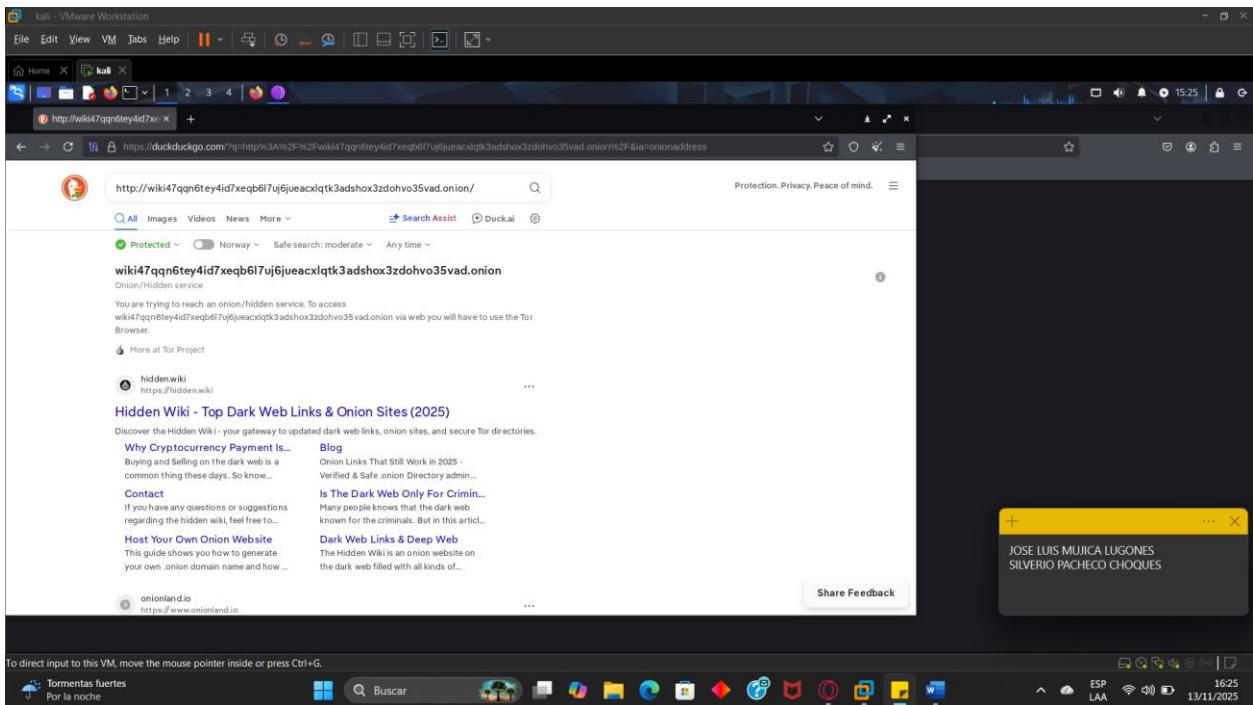
Chrome, etc.). y mostrar que resultado es el que aparece y explique él porque



El acceso falla porque los navegadores normales utilizan el Sistema de Nombres de Dominio (DNS) estándar. Los dominios .onion no están registrados en el DNS público y solo pueden ser resueltos y enrutados por el Navegador Tor, que está configurado para la red Tor

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 tardó al acceder al sitio.



Explicación del Tiempo: El tiempo de carga es significativamente más lento que un sitio web normal. Esto se debe a que el navegador Tor tiene que construir un circuito cifrado de 6 nodos (en lugar de los 3 nodos para sitios normales) a través de la red de voluntarios para establecer la conexión con el servicio oculto, lo cual añade una latencia considerable.

3. Responda a las siguientes preguntas

1) ¿Qué sucede en cada caso?

R: La respuesta ya está arriba.

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

R: El navegador normal **NO accede**.

Justification:

1. **Protocolo Exclusivo:** Los dominios. onion son un protocolo de **servicios ocultos** que solo la red Tor puede entender y utilizar.
2. **Fallo de DNS:** Un navegador normal le pregunta a un servidor DNS cómo llegar a la dirección. onion, y el servidor no tiene información, ya que no es un dominio público. Esto resulta en un error de conexión.

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

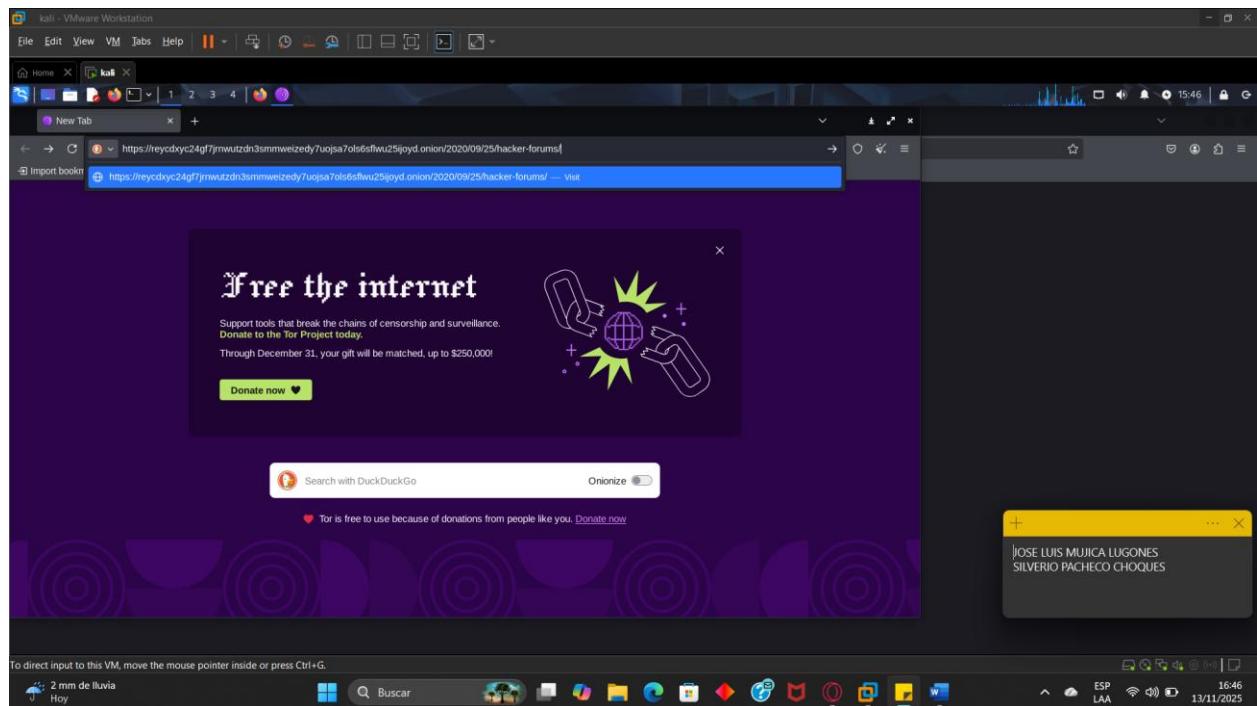
TOR

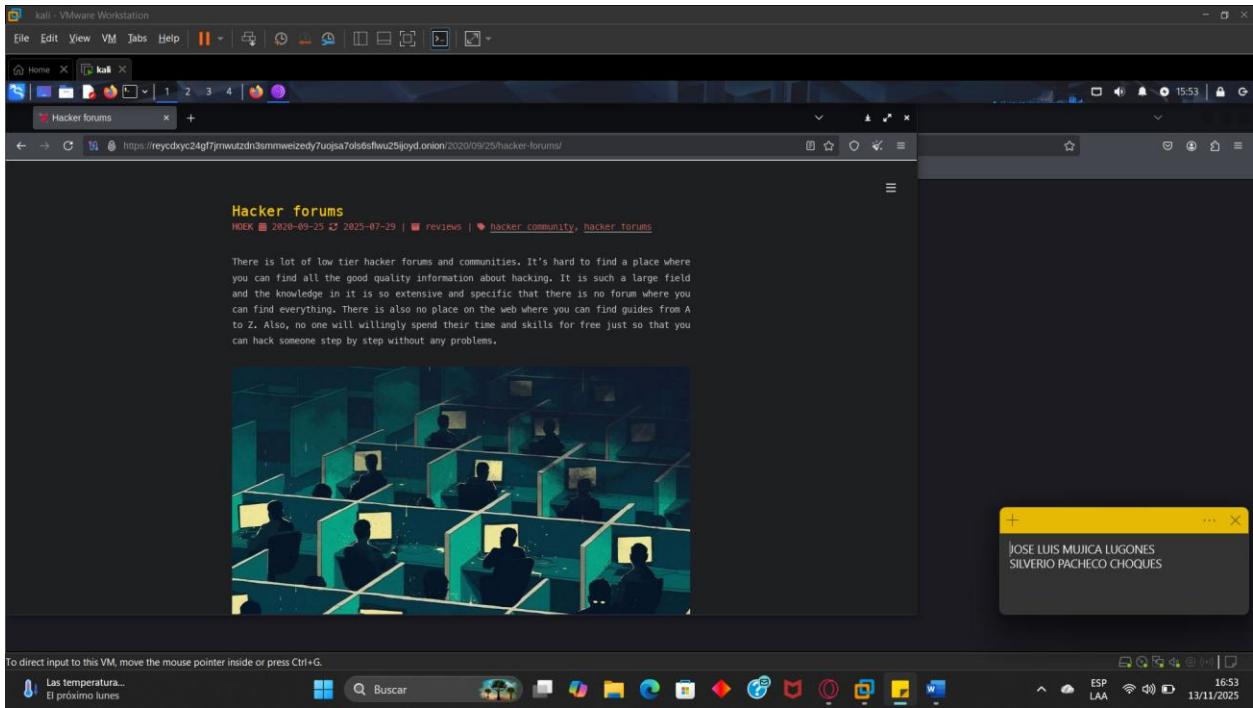
R: Tor cifra el tráfico en múltiples capas y lo enruta a través de nodos aleatorios, ocultando la IP real y permitiendo acceder a servicios ocultos (.onion) Sin Tor, estos sitios son inaccesibles.

PARTE 3

1. Accede desde Tor a este blog .onion:

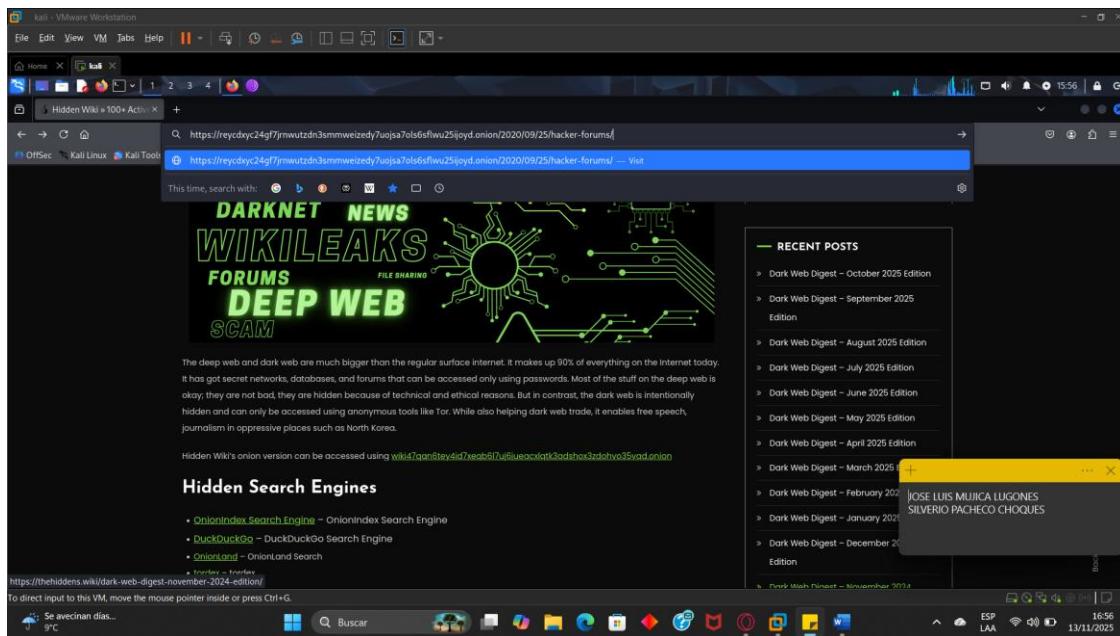
<https://reycdxyc24gf7jrnwutzdn3smmweizedy7uojsa7ols6sfwu25ijoyd.onion/2020/09/25/hacker-forums/>

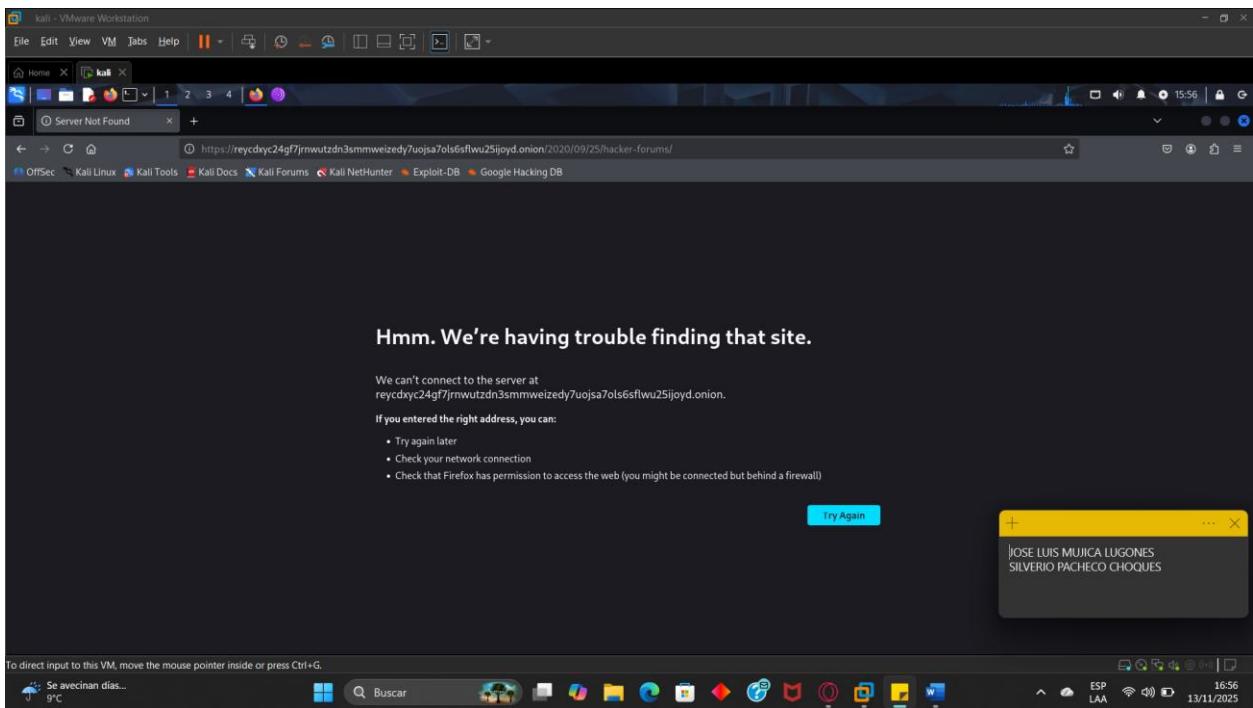




El concepto principal es que el verdadero conocimiento de hacking se obtiene mediante el estudio profundo (libros, cursos) y la práctica constante, y no a través de foros o guías fáciles que, además de ser a menudo de baja calidad, no preparan al individuo para resolver los problemas reales que surgen en la práctica.

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





Los enlaces con el dominio de nivel superior ficticio **.onion** son utilizados exclusivamente por el servicio de anonimato Tor (The Onion Router). Estos no son dominios tradicionales de Internet (como .com o .org) y no están registrados en el sistema de nombres de dominio (DNS) convencional.

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?)

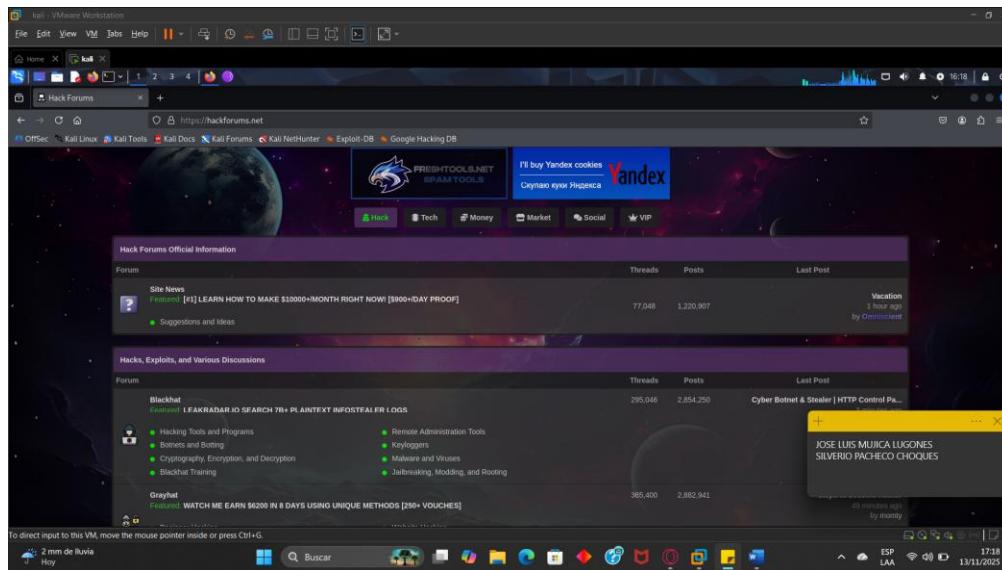
R: La red Tor (The Onion Router) es fundamental para garantizar el anonimato y la privacidad en línea. Su mecanismo principal consiste en encriptar las conexiones a Internet y enrutar el tráfico a través de una cadena de múltiples nodos distribuidos geográficamente. Este proceso de cifrado por capas hace que sea sumamente difícil rastrear la verdadera ubicación o la identidad del usuario, protegiendo así su actividad en la red.

El uso de Tor resulta esencial para acceder a numerosos sitios de la web profunda, especialmente aquellos identificados con la extensión **.onion**. Estos sitios suelen estar vinculados a actividades que requieren un alto grado de confidencialidad y anonimato, como la investigación de seguridad, el *hacking* ético o la interacción con información sensible. Al utilizar Tor para visitar estos foros y sitios específicos, se asegura que el usuario no pueda ser rastreado o identificado fácilmente por terceros o actores externos maliciosos, salvaguardando su 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

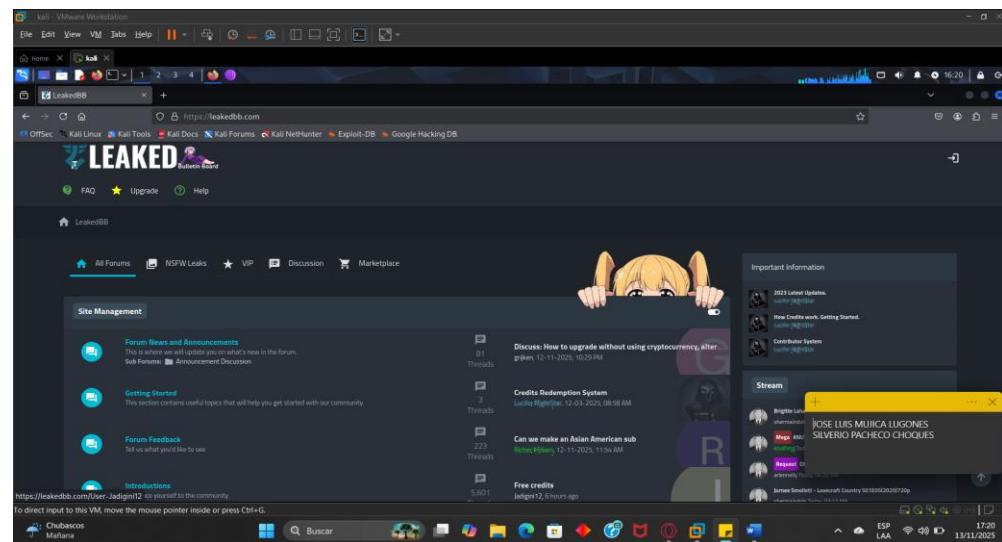
R: Hack forums (<https://hackforums.net/>)

Este es uno de los foros de hacking mas conocidos y, aunque su contenido es variado y cubre tanto temas legales como ilegales, sigue siendo una buena fuente para aprender sobre distintas técnicas y herramientas.



LeakedBB (<https://leakedbb.com/>)

Esta foto esta enfocado en la publicación y discusión de base de datos filtradas. La posibilidad de acceder a estas bases de datos puede ser útil para quienes trabajan en análisis de seguridad o investigación forense digital.



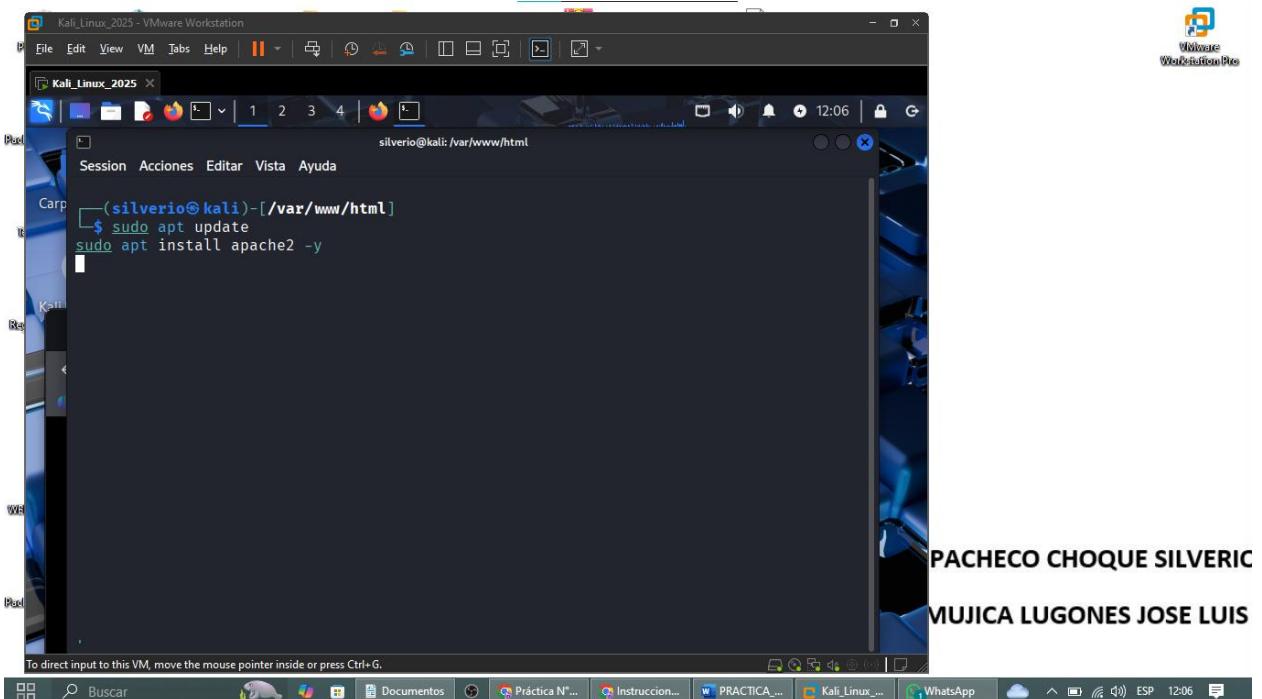
PARTE 4

EVALUACION

Instalar Apache:

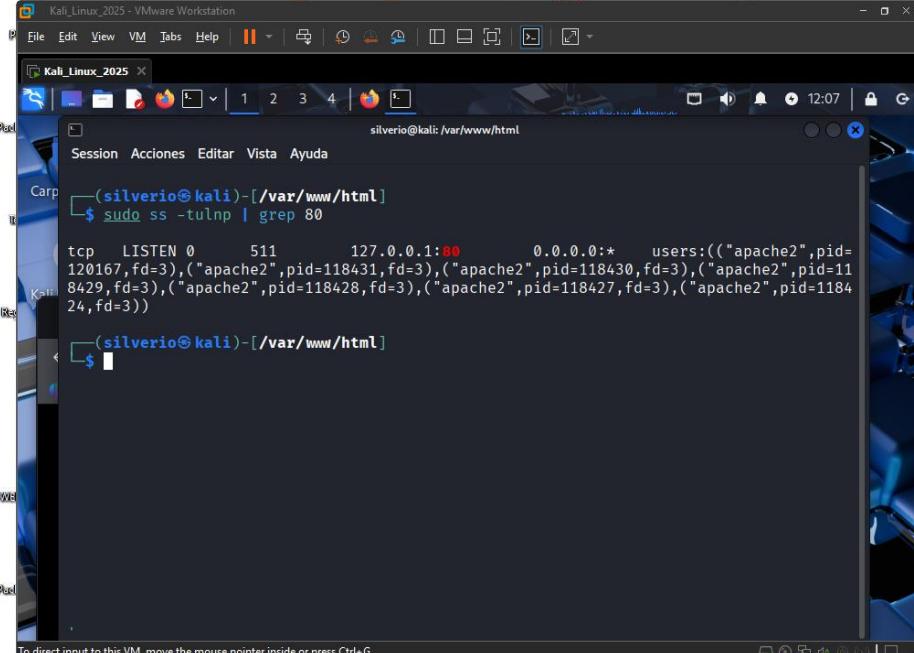
```
sudo apt update
```

```
sudo apt install apache2 -y
```



Verificar que Apache está escuchando en el puerto 80:

```
sudo ss -tulnp | grep 80
```



```
silverio@kali: /var/www/html
$ sudo ss -tulnp | grep 80
tcp  LISTEN  0      511          127.0.0.1:80          0.0.0.0:*      users:(("apache2",pid=120167,fd=3),("apache2",pid=118431,fd=3),("apache2",pid=118430,fd=3),("apache2",pid=118429,fd=3),("apache2",pid=118428,fd=3),("apache2",pid=118427,fd=3),("apache2",pid=118424,fd=3))
```

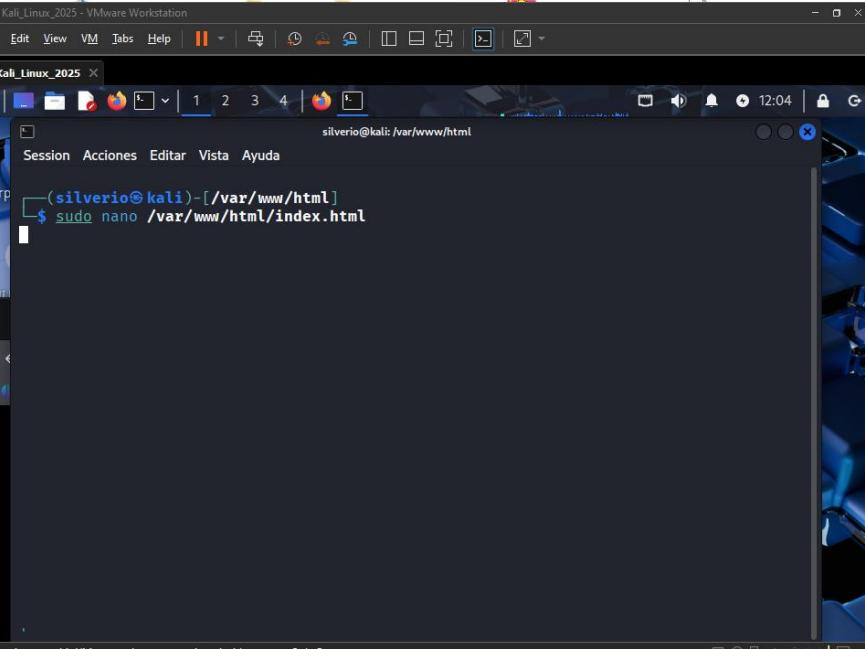
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Crear la página web (index.html)

En Kali:

```
cd /var/www/html/index.html
```

```
sudo nano /var/www/html/index.html
```



```
silverio@kali: /var/www/html
$ sudo nano /var/www/html/index.html
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
silverio@kali: /var/www/html
```

```
GNU nano 8.6           /var/www/html/index.html
<html>
<body style="background:black; color:lime; font-family:Courier;">
<center>
<h1>Hacking Today</h1>
<p>Servidor oculto en la red TOR</p>
</center>
</body>
</html>
```

```
[ 8 líneas leidas ]
```

```
^G Ayuda      ^O Guardar     ^F Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación
^X Salir      ^R Leer fich.  ^W Reemplazar  ^U Pegar       ^J Justificar   ^/ Ir a linea
```

INSTALAR TOR EN KALI

```
sudo apt install tor -y
```

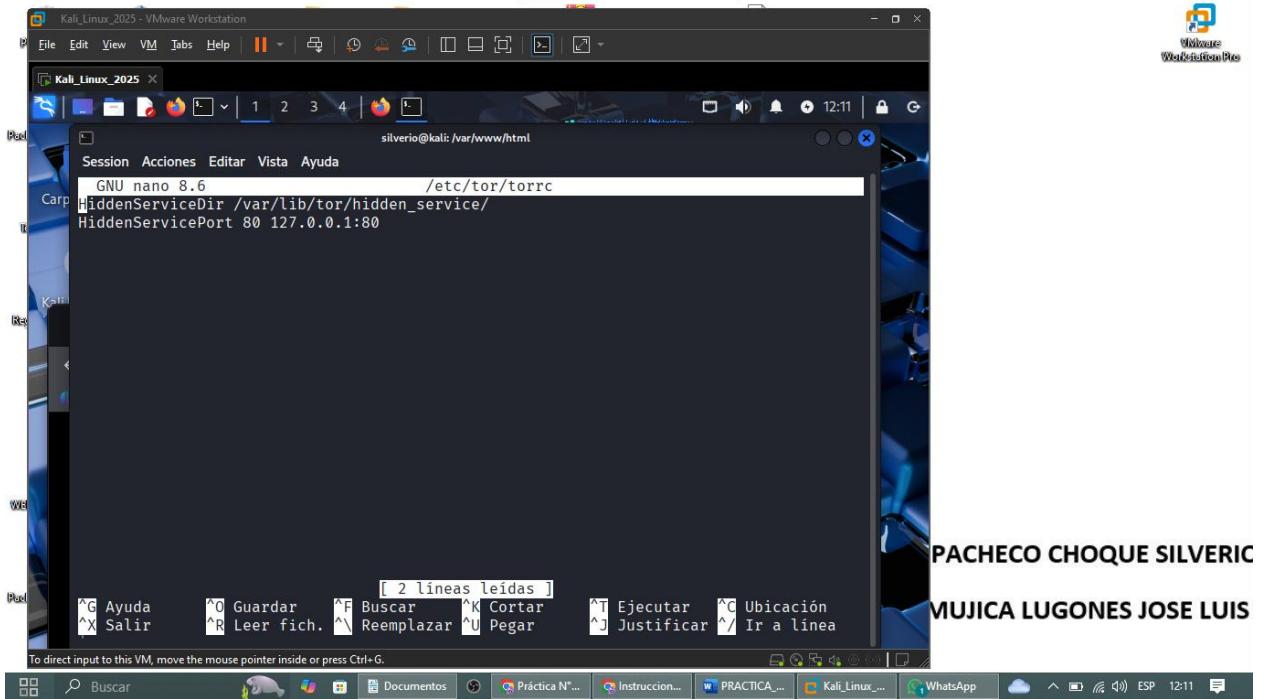
CONFIGURAR TOR PARA CREAR EL SERVICIO OCULTO

```
sudo nano /etc/tor/torrc
```

```
silverio@kali: /var/www/html
```

```
(silverio@kali)-[~/var/www/html]
```

```
$ sudo nano /etc/tor/torrc
```



INICIAR EL SERVICIO TOR CORRECTO

Iniciar Tor:

```
sudo systemctl start tor@default.service
```

Activar para que se inicie siempre:

```
sudo systemctl enable tor@default.service
```

Comprobar:

```
sudo systemctl status tor@default.service
```

```
silverio@kali: /var/www/html
$ sudo systemctl start tor@default.service

silverio@kali: /var/www/html
$ sudo systemctl enable tor@default.service

The unit files have no installation config (WantedBy=, RequiredBy=, UpheldBy=,
Also=, or Alias= settings in the [Install] section, and DefaultInstance= for
template units). This means they are not meant to be enabled or disabled using systemctl.

Possible reasons for having these kinds of units are:
• A unit may be statically enabled by being symlinked from another unit's
.wants/, .requires/, or .upholds/ directory.
• A unit's purpose may be to act as a helper for some other unit which has
a requirement dependency on it.
• A unit may be started when needed via activation (socket, path, timer,
D-Bus, udev, scripted systemctl call, ...).
• In case of template units, the unit is meant to be enabled with some
instance name specified.

silverio@kali: /var/www/html
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

PACHECO CHOQUE SILVERIC
MUJICA LUGONES JOSE LUIS

```
silverio@kali: /var/www/html
$ sudo systemctl status tor@default.service

● tor@default.service - Anonymizing overlay network for TCP
   Loaded: loaded (/usr/lib/systemd/system/tor@default.service; enabled-runtime; pr
   Active: active (running) since Fri 2025-11-14 11:55:57 -04; 17min ago
     Invocation: 9144489ee41468aa5483d594e300aa6
      Main PID: 118630 (tor)
        Tasks: 3 (limit: 4412)
       Memory: 47.7M (peak: 49.5M)
         CPU: 1.985s
        CGroup: /system.slice/system-tor.slice/tor@default.service
                └─118630 /usr/bin/tor --defaults-torrc /usr/share/tor/tor-service-defaults.torrc

nov 14 11:55:58 kali Tor[118630]: Opened Socks listener connection (ready) on /run/tor/control
nov 14 11:55:58 kali Tor[118630]: Opening Control listener on /run/tor/control
nov 14 11:55:58 kali Tor[118630]: Opened Control listener connection (ready) on /run/tor/control
nov 14 11:55:59 kali Tor[118630]: Bootstrapped 10% (conn_done): Connected to a relay
nov 14 11:55:59 kali Tor[118630]: Bootstrapped 14% (handshake): Handshaking with a relay
nov 14 11:56:00 kali Tor[118630]: Bootstrapped 15% (handshake_done): Handshake with a relay
nov 14 11:56:00 kali Tor[118630]: Bootstrapped 75% (enough_dirinfo): Loaded enough directory information
nov 14 11:56:00 kali Tor[118630]: Bootstrapped 90% (ap_handshake_done): Handshake finished
nov 14 11:56:00 kali Tor[118630]: Bootstrapped 95% (circuit_create): Establishing a circuit
nov 14 11:56:01 kali Tor[118630]: Bootstrapped 100% (done): Done
lines 1-21/21 (END)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

PACHECO CHOQUE SILVERIC
MUJICA LUGONES JOSE LUIS

OBTENER TU DIRECCIÓN .ONION

```
sudo cat /var/lib/tor/hidden_service/hostname
```

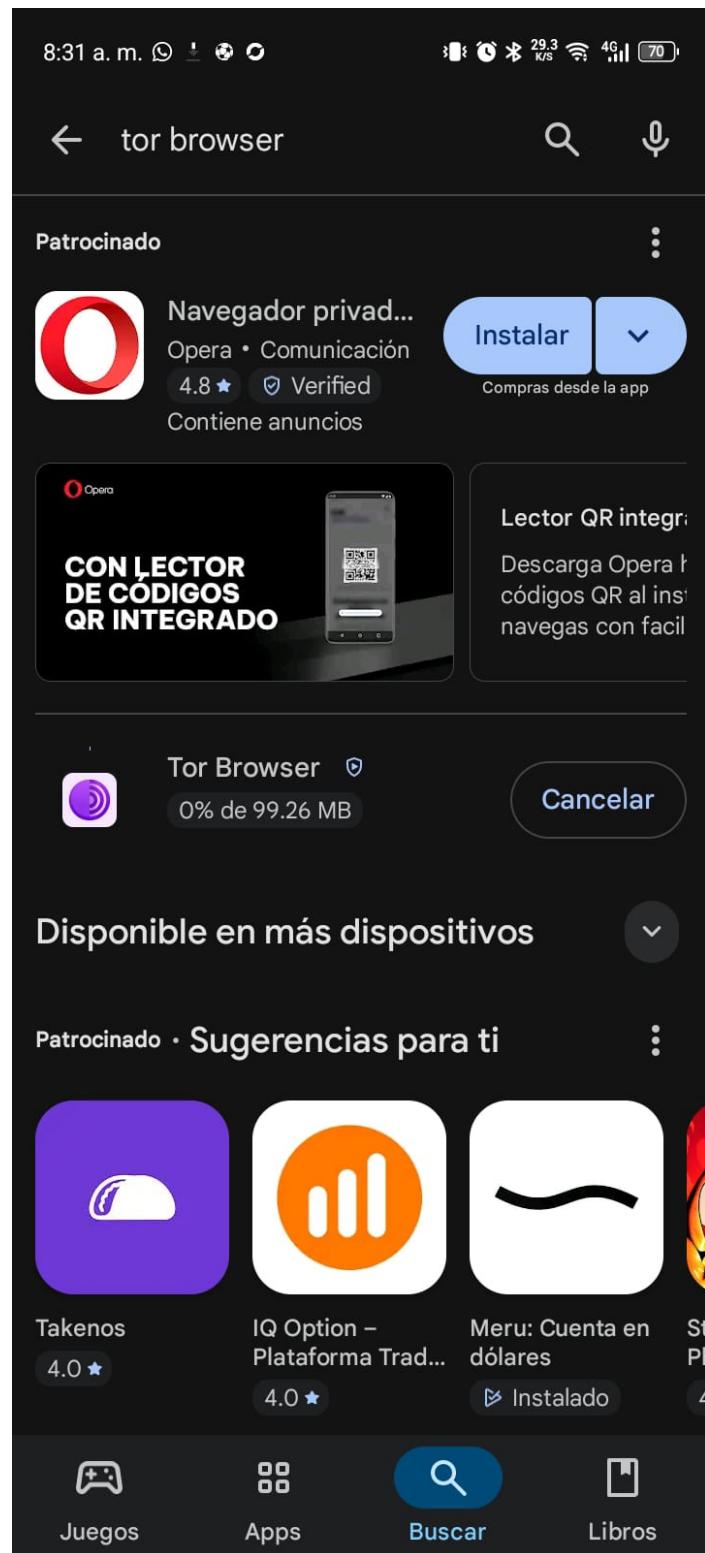
The screenshot shows a terminal window titled "Kali_Linux_2025" running in VMware Workstation Pro. The terminal session is on the root user of Kali Linux, with the command \$ sudo cat /var/lib/tor/hidden_service/hostname being run. The output is a long string of characters: 4pwlrjjxgqz4fp3dg74xzhfxvaxetubhmm5ce35mjsnkikgmij666qd.onion. The desktop environment includes a taskbar with various icons like Documentos, Práctica N°..., Instrucción..., WhatsApp, and Kali_Linux_2025.

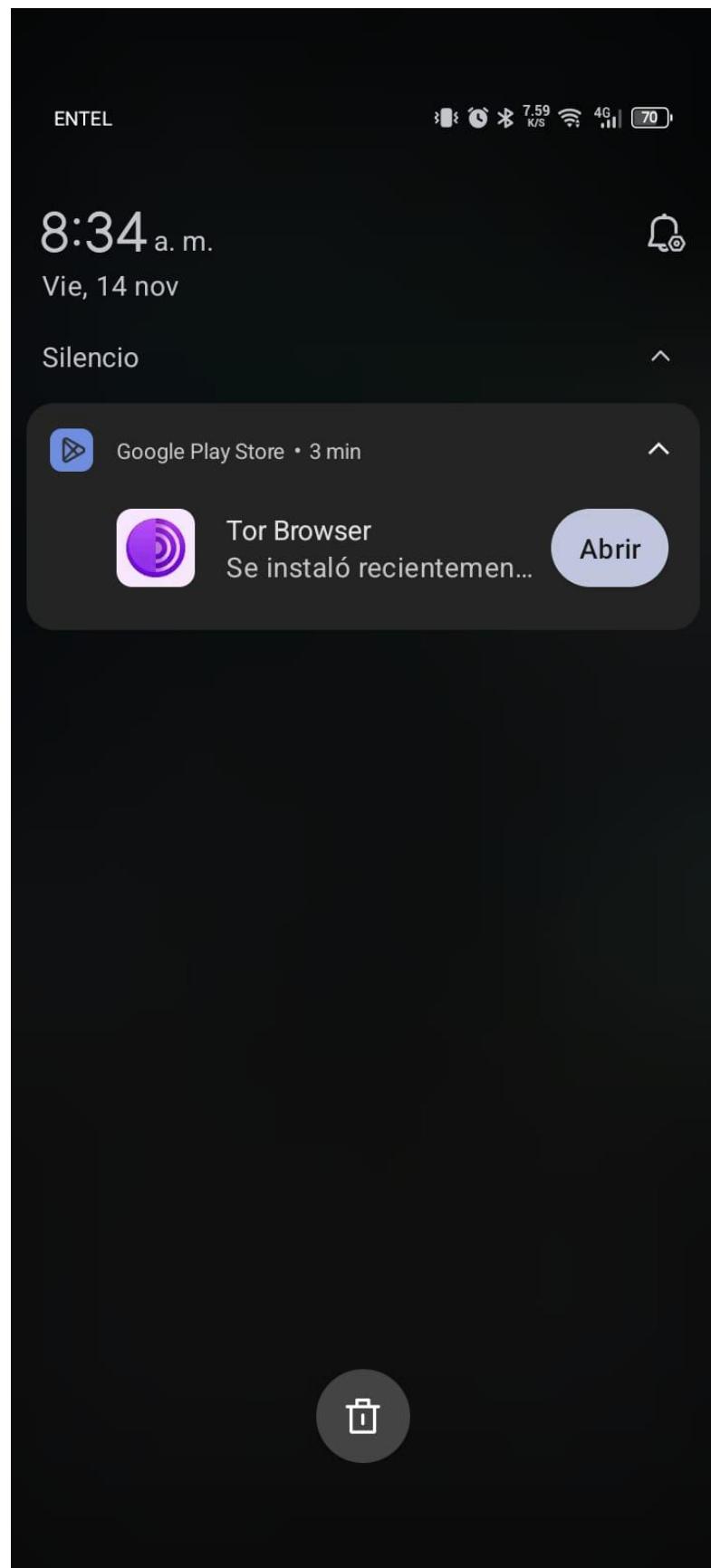
```
silverio@kali: /var/www/html
$ sudo cat /var/lib/tor/hidden_service/hostname
4pwlrjjxgqz4fp3dg74xzhfxvaxetubhmm5ce35mjsnkikgmij666qd.onion
```

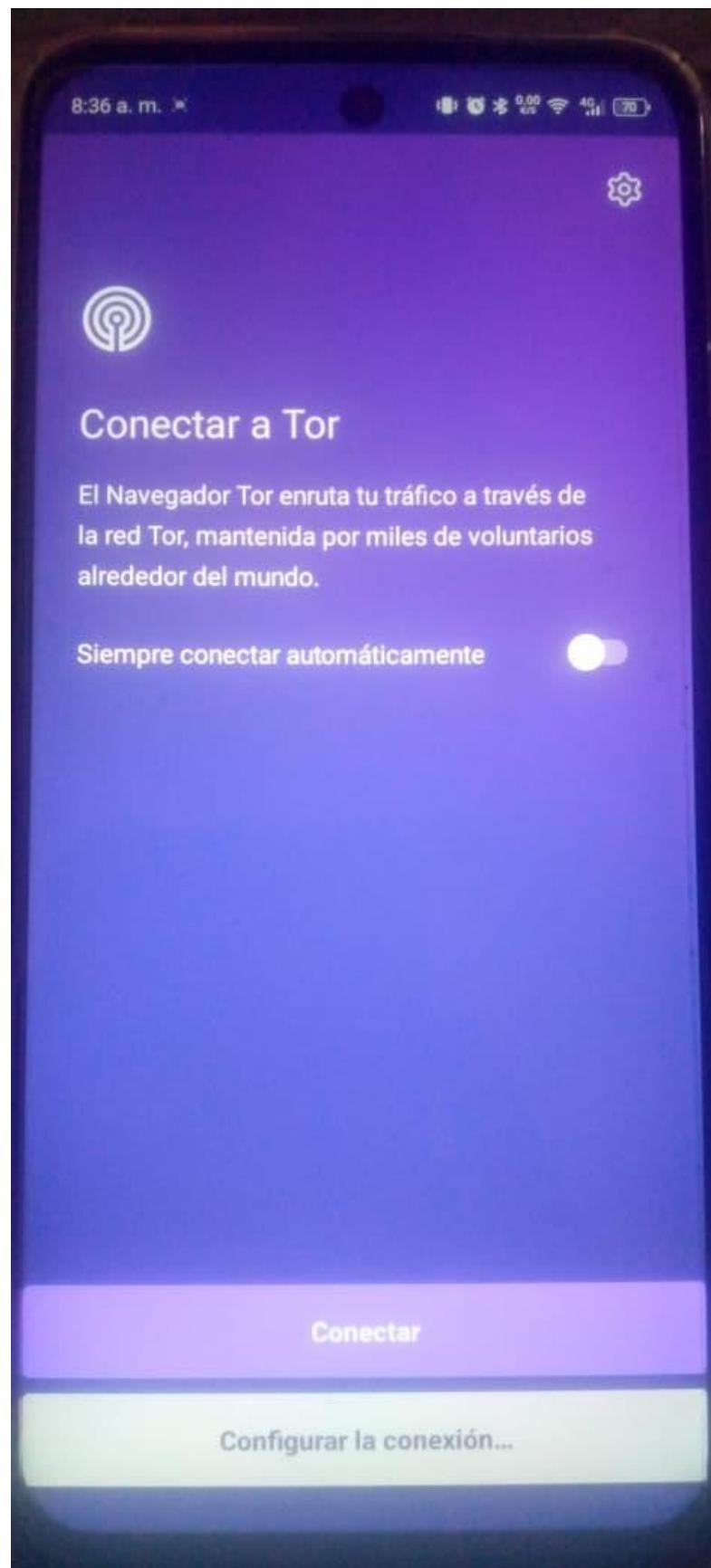
PROBAR EL SERVICIO DESDE UN CELULAR O PC

ACCESO DESDE NAVEGADOR TOR

En nuestro celular: Descargar Browser

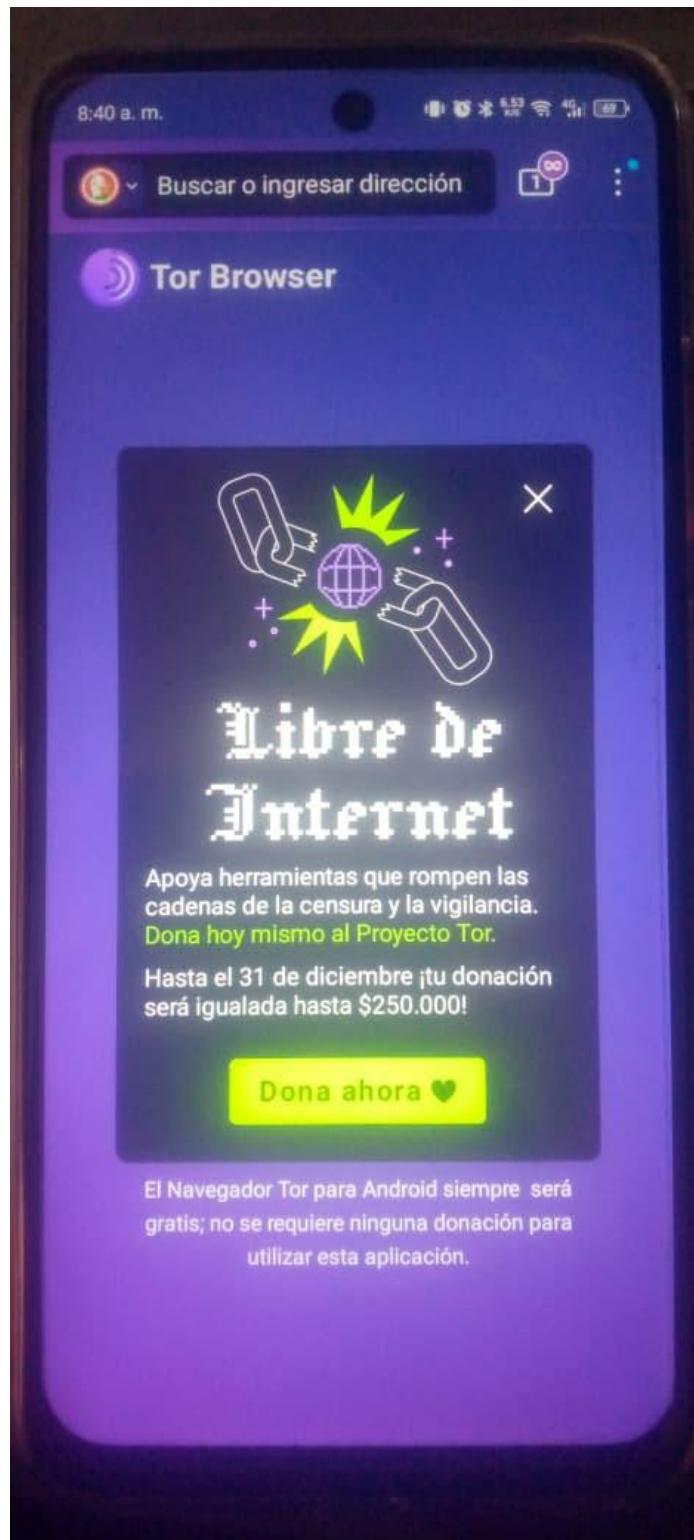


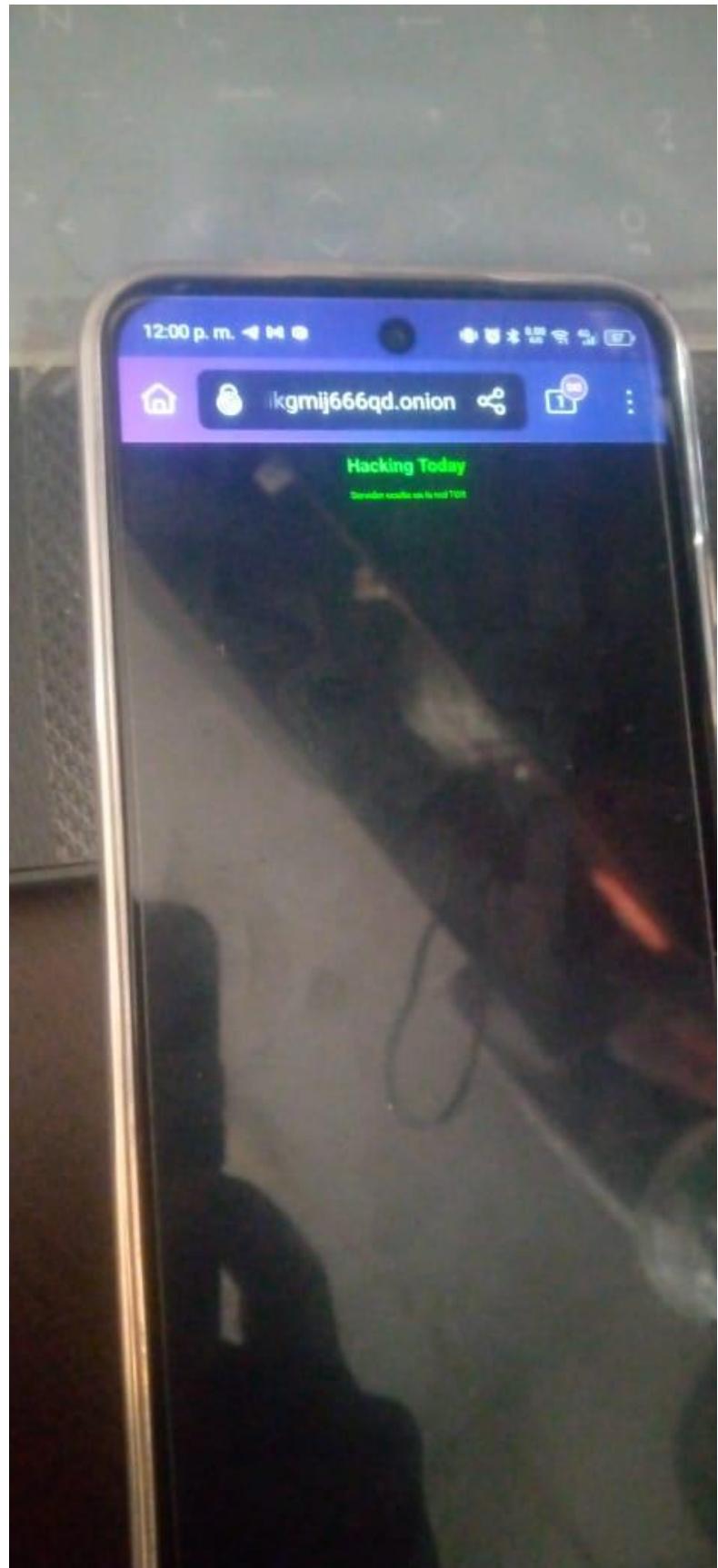




Pega tu URL:

ugc74omy33hnaufxnyvx34h2c3pfguhwxyvo4jc2szq5dcrfdswndgid.onion

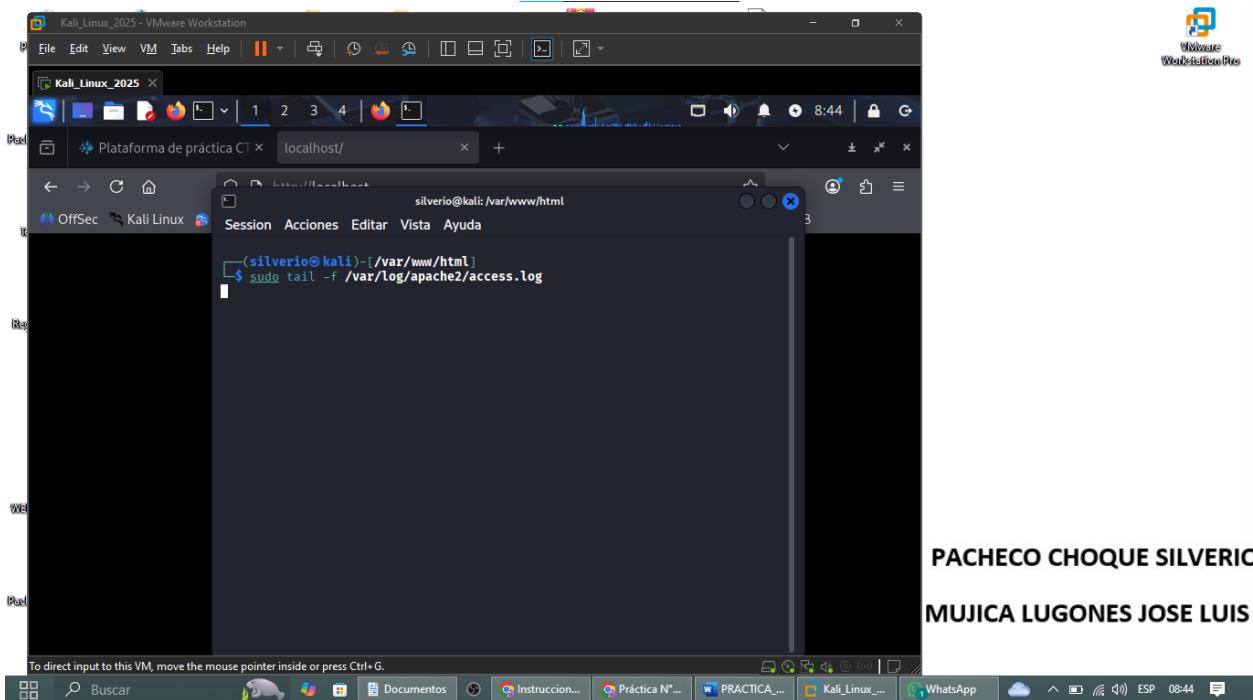




ACTIVAR LOS LOGS EN KALI (lado del servidor)

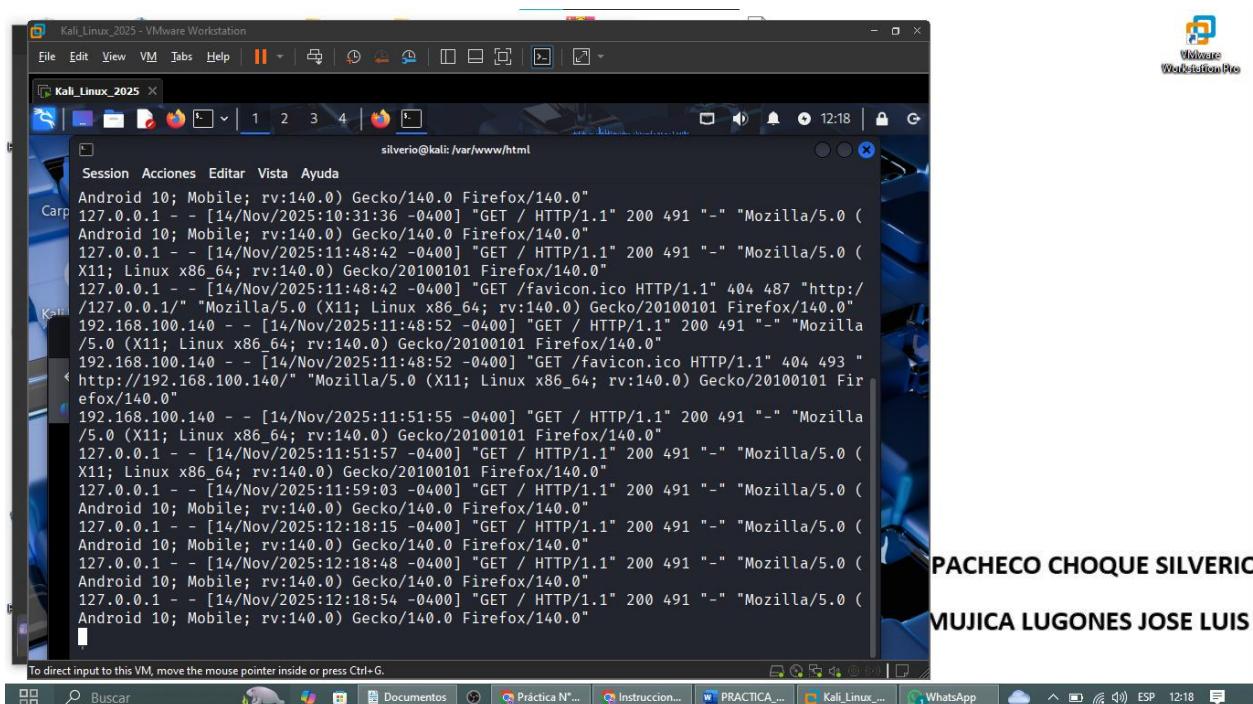
Ejecuta:

```
sudo tail -f /var/log/apache2/access.log
```



```
(silverio㉿kali)-[~/var/www/html]
└─$ sudo tail -f /var/log/apache2/access.log
```

PACHECO CHOQUE SILVERIC
MUJICA LUGONES JOSE LUIS



```
silverio㉿kali:~/var/www/html
Session Acciones Editar Vista Ayuda
Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:10:31:36 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:11:48:42 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:11:48:42 -0400] "GET /favicon.ico HTTP/1.1" 404 487 "http://127.0.0.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
192.168.100.140 - - [14/Nov/2025:11:48:52 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
192.168.100.140 - - [14/Nov/2025:11:48:52 -0400] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.140/" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
192.168.100.140 - - [14/Nov/2025:11:51:55 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:11:51:57 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:11:59:03 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:12:18:15 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:12:18:48 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
127.0.0.1 - - [14/Nov/2025:12:18:54 -0400] "GET / HTTP/1.1" 200 491 "-" "Mozilla/5.0 (Android 10; Mobile; rv:140.0) Gecko/140.0 Firefox/140.0"
```

PACHECO CHOQUE SILVERIC
MUJICA LUGONES JOSE LUIS

