

25. Tor como herramienta de privacidad

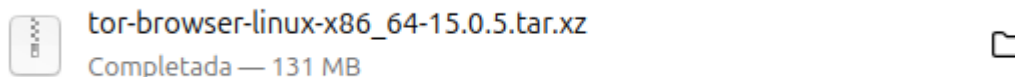
Instalación de Tor Browser

Paso 1 — Descargar Tor Browser (fuente oficial)

La web oficial:

- <https://www.torproject.org/download/>

Descarga Tor Browser para Linux (64-bit)



Paso 2 — Extraer el archivo

1. Ve a la carpeta de descargas:
 - `cd ~/Descargas`

```
ub@forense-ai:~$ cd ~/Descargas
```

2. Extrae el archivo:
 - `tar -xf tor-browser-linux-x86_64-*.tar.xz`

```
ub@forense-ai:~/Descargas$ tar -xf tor-browser-linux-x86_64-*.tar.xz
```

Paso 3 — Ejecutar Tor Browser

1. Entra en la carpeta:
 - `cd tor-browser`

```
ub@forense-ai:~/Descargas$ cd tor-browser
```

2. Lanza el navegador:
 - `./start-tor-browser.desktop`

```
ub@forense-ai:~/Descargas/tor-browser$ ./start-tor-browser.desktop
```

3. pulsa Conectar



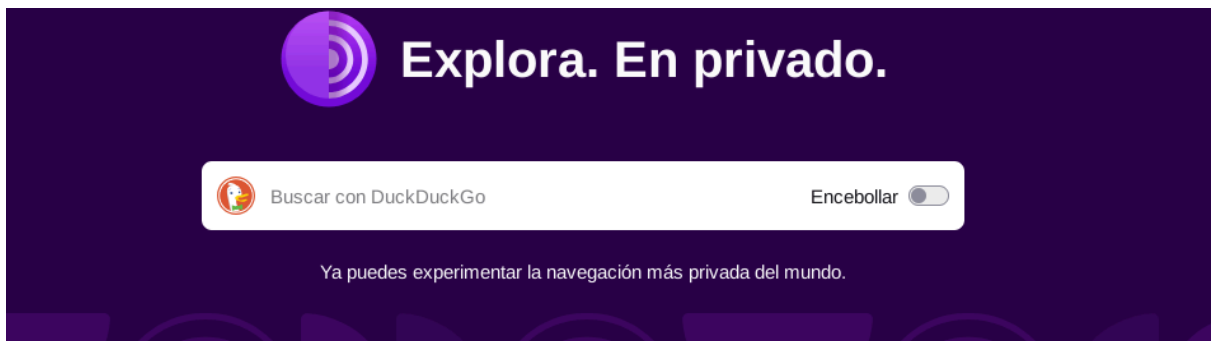
Conectar a Tor

El Navegador Tor enruta tu tráfico a través de la red Tor, mantenida por miles de voluntarios alrededor del mundo.

☐ Siempre conectar automáticamente

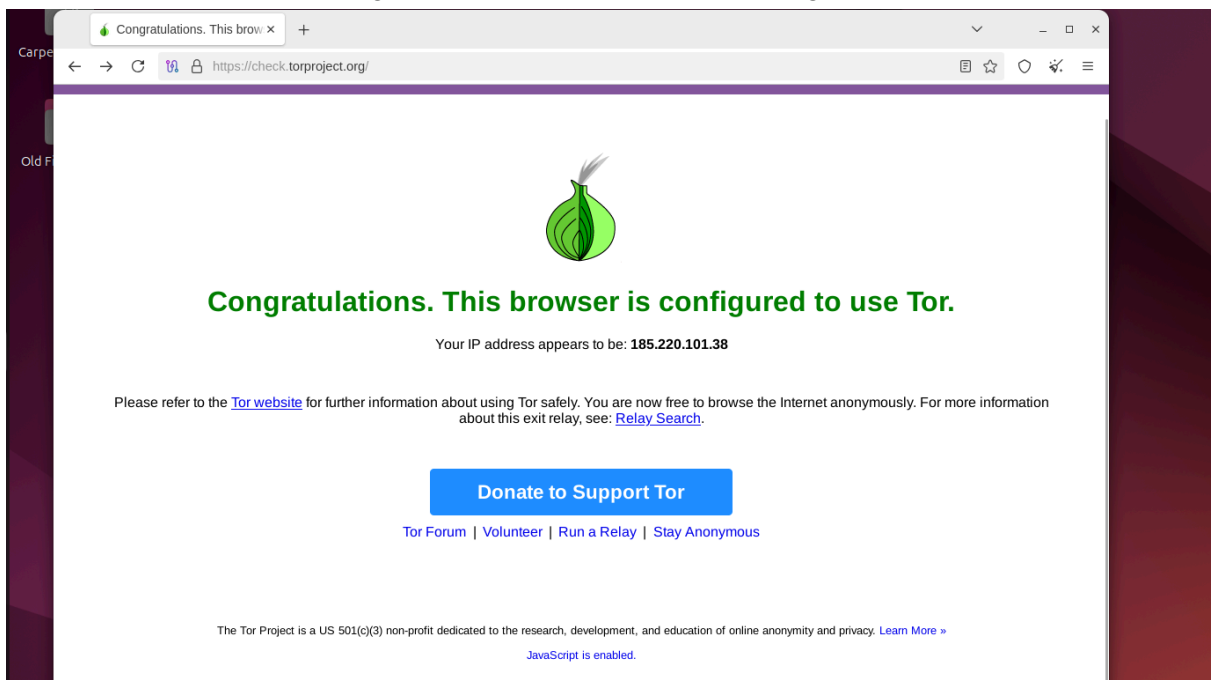
Configurar la conexión...

Conectar



Paso 4 — Verificar que funciona

1. Dentro de Tor Browser abre:
 - <https://check.torproject.org>
2. Tor Browser
 - Muestra: Congratulations. This browser is configured to use Tor.



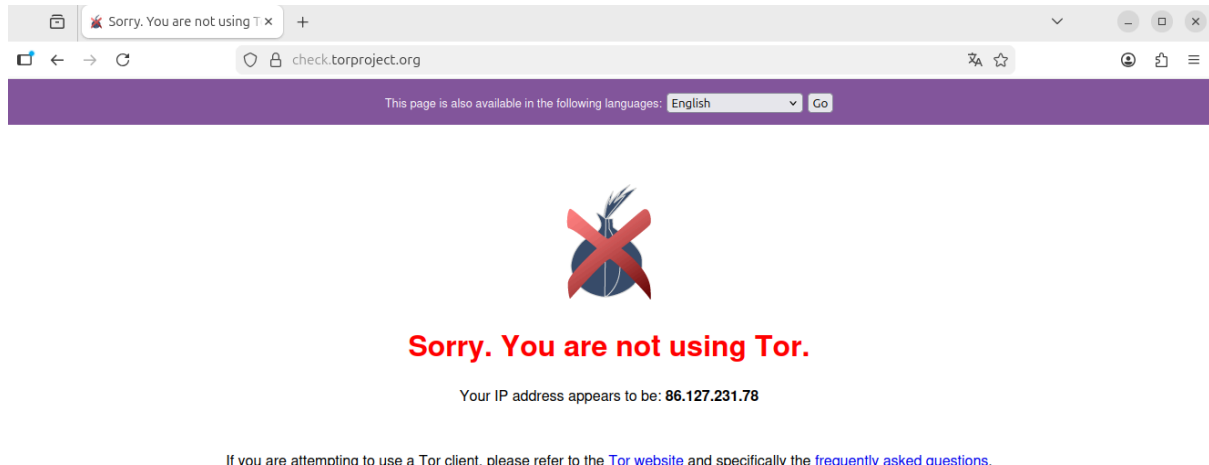
Actividad 1 — Comparativa (Normal vs Tor)

Comparar IP (Normal vs Tor)

Visita: <https://check.torproject.org/>

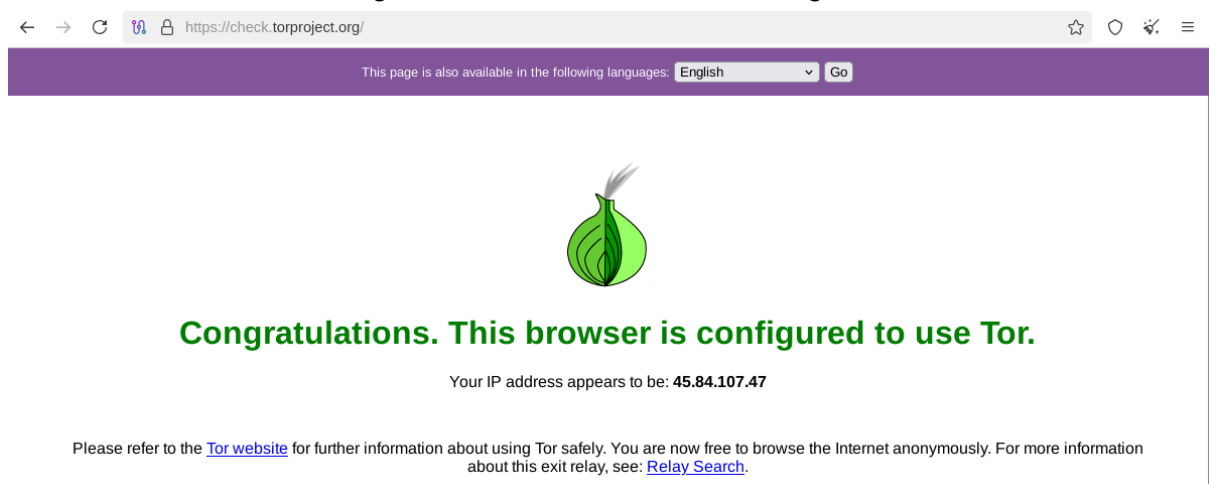
1. Normal Browser

- Muestra: Sorry. You are not using Tor.



2. Tor Browser

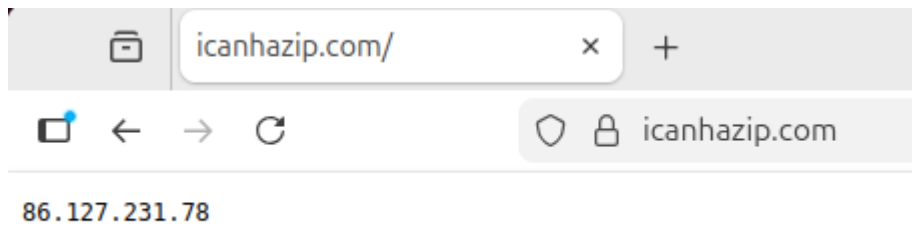
- Muestra: Congratulations. This browser is configured to use Tor.



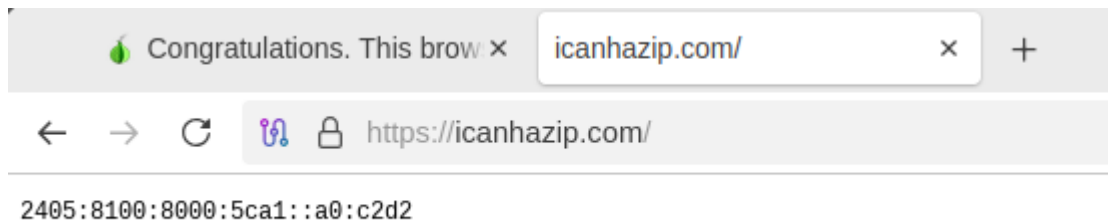
Las diferentes direcciones IP indican que Tor ha proporcionado con éxito el anonimato en el transporte, ocultando la verdadera fuente.

Visita: <https://icanhazip.com/>

- En navegador normal
IPv4: 86.127.231.78

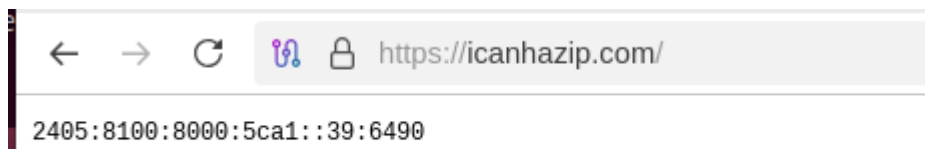


- En Tor Browser
IPv6: 2405:8100:8000:5ca1::a0:c2d2



Las direcciones IP de ambos son completamente diferentes, lo que indica que Tor oculta la verdadera dirección IP del usuario utilizando un nodo de salida. Además, Tor puede emplear IPv6 dependiendo del nodo de salida.

El nodo de salida puede cambiar cada vez que se renueva el circuito Tor.

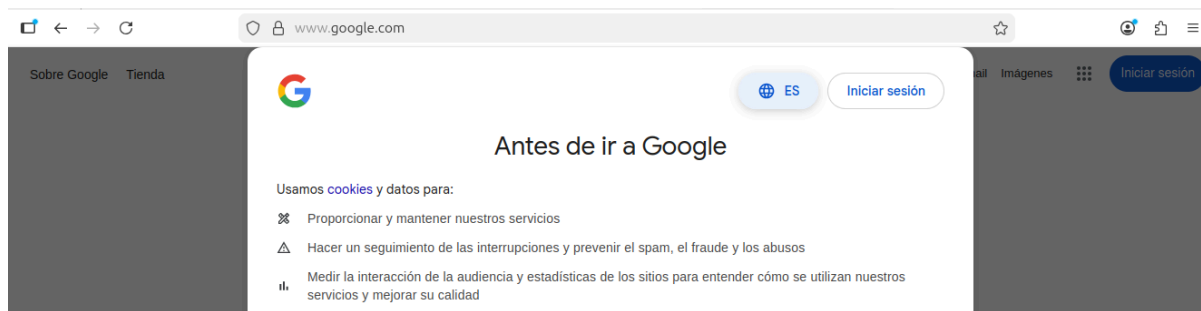


Comparar idioma detectado

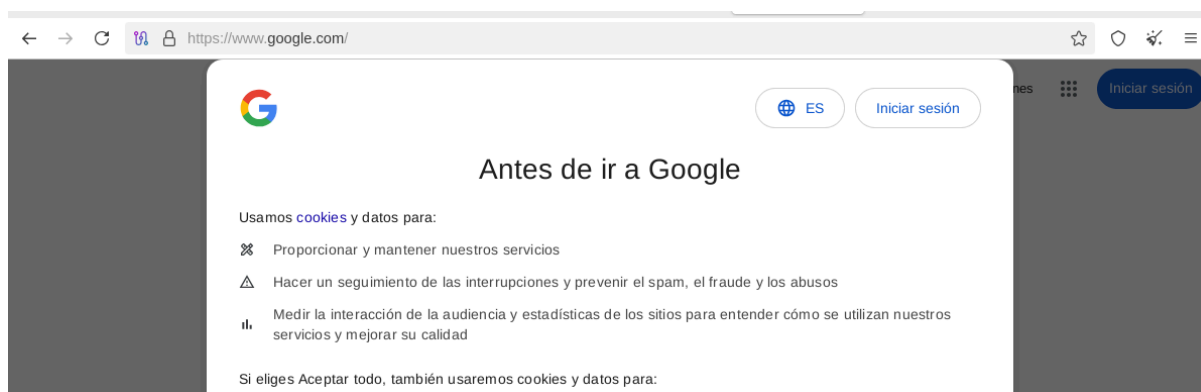
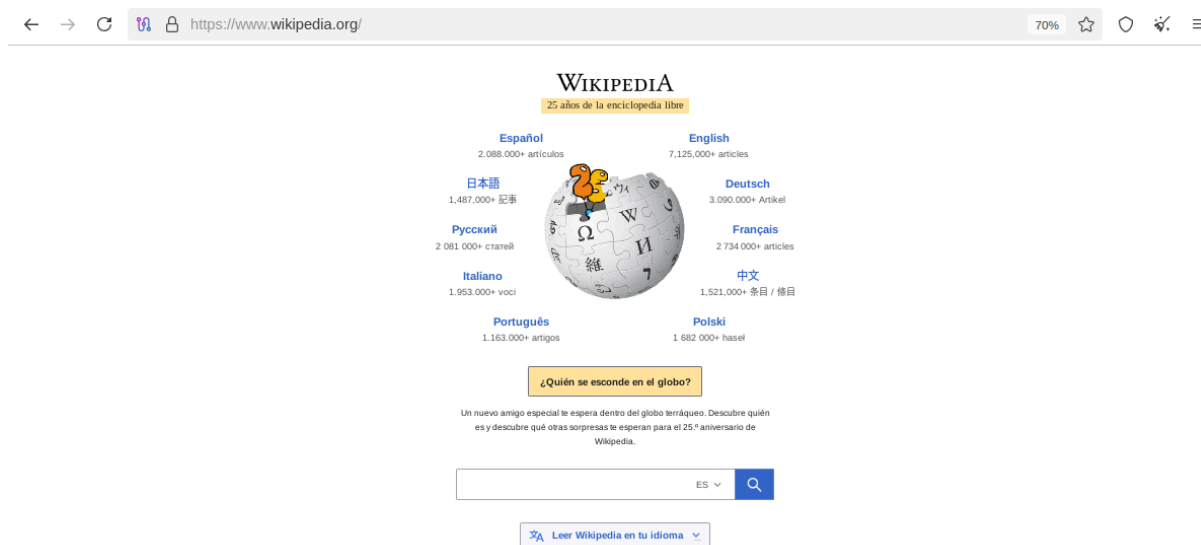
En navegador normal, visita:

- <https://www.wikipedia.org/> o (sin iniciar sesión) <https://www.google.com/>





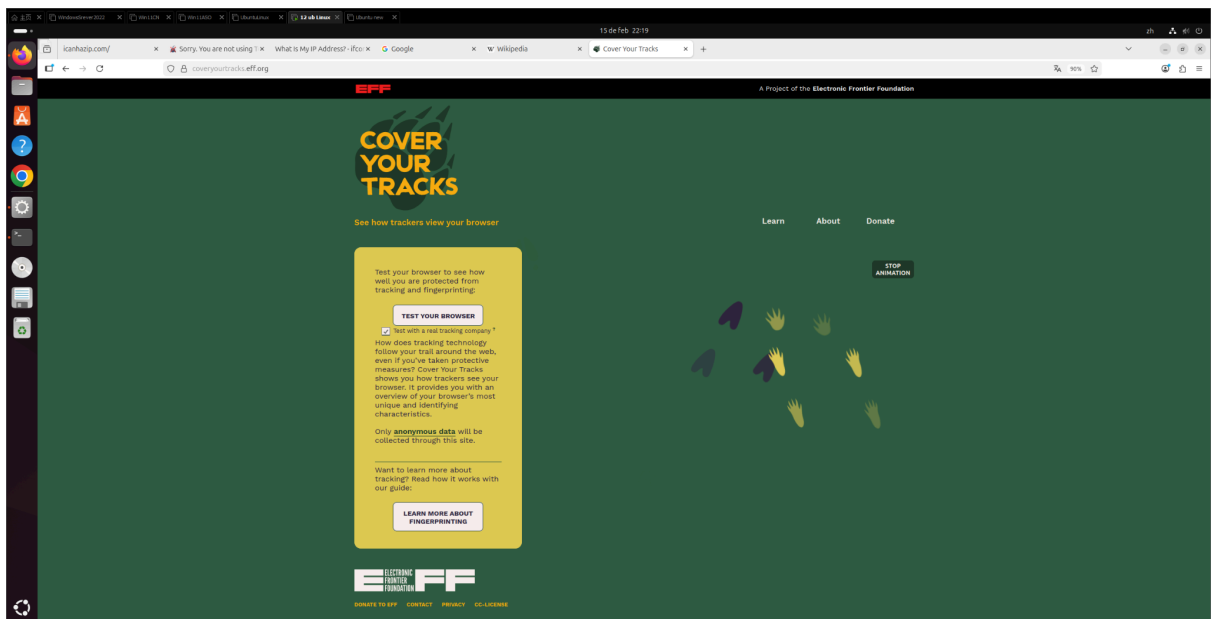
- En Tor Browser



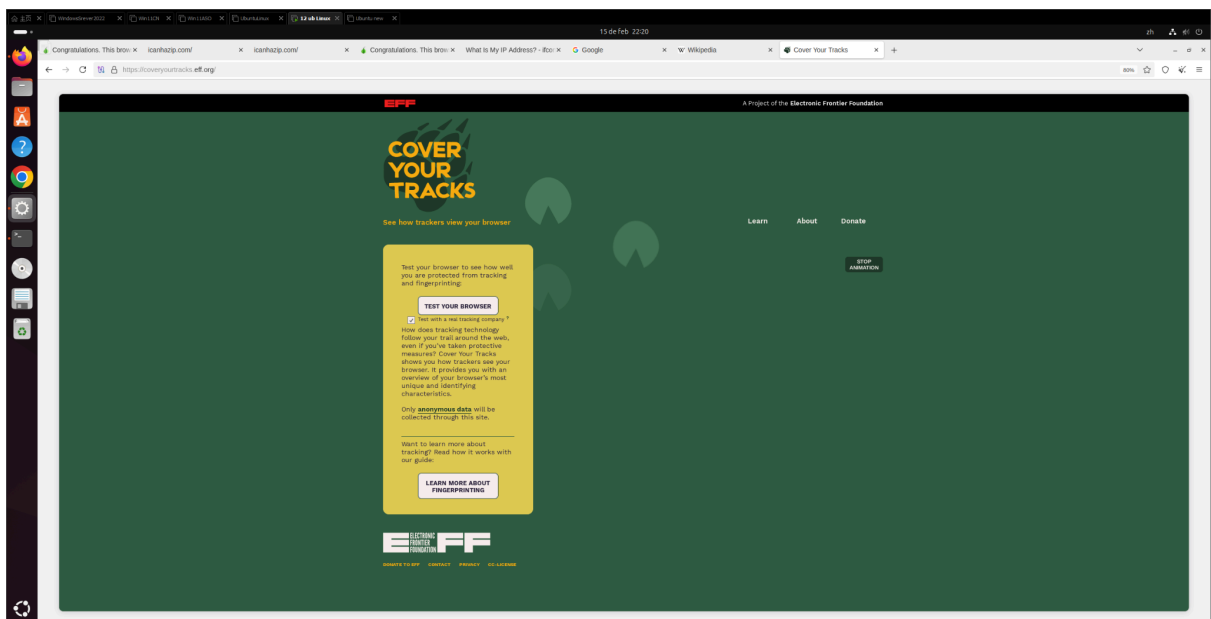
Ambos utilizan principalmente el idioma del sistema para traducir automáticamente las páginas web al español, detectando la región/idioma sin solicitarlo y sin exigir la selección del idioma/región. Sin embargo, los navegadores estándar ofrecen opciones para cambiar el idioma y la región, mientras que el navegador Tor no lo hace.

Fingerprint básico (huella del navegador)

- Navegador normal



- Tor Browser

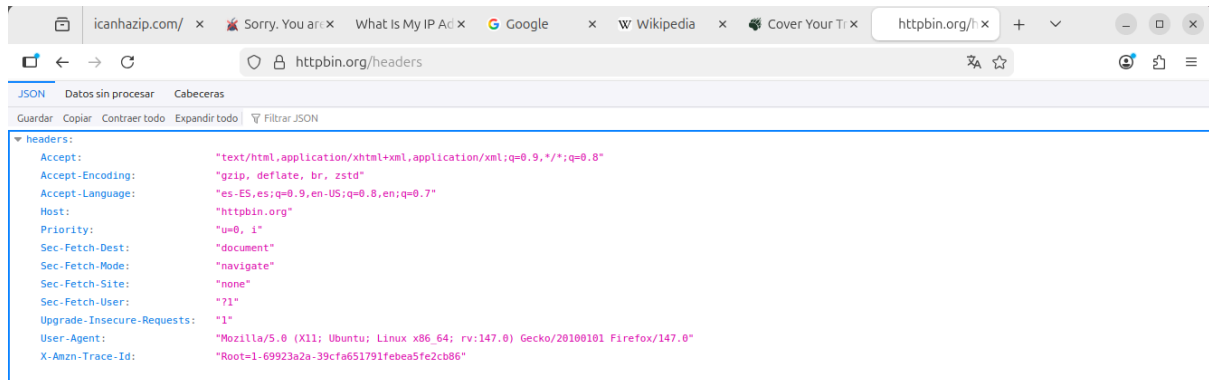


En el navegador normal, la huella digital es única y se recopilan muchos datos, lo que facilita el rastreo. En Tor Browser, la huella es menos única y más homogénea, ya que Tor unifica la configuración de todos los usuarios para reducir la identificación individual. Esto demuestra que Tor protege mejor contra el rastreo por huella del navegador.

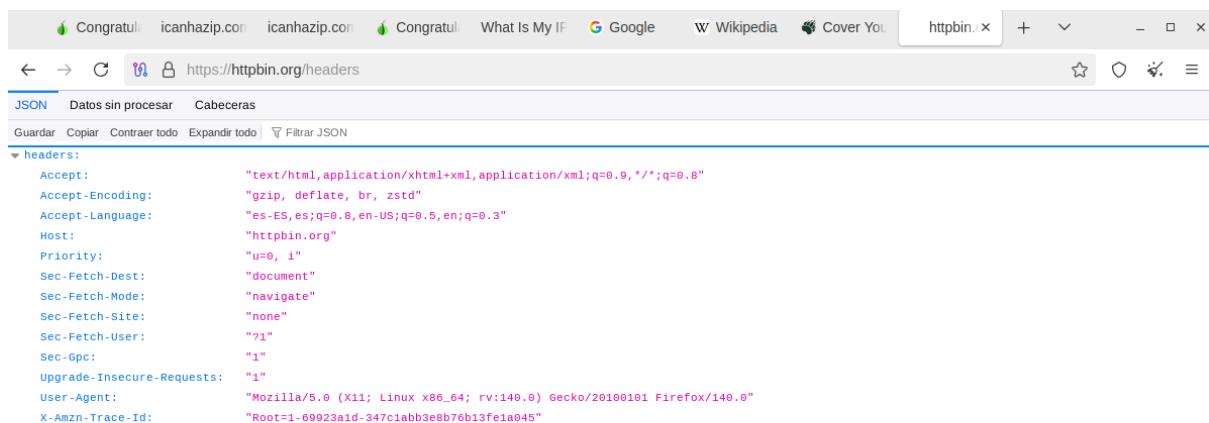
Actividad 2 — Análisis de cabeceras HTTP (Headers)

Ver headers desde una web (fácil y limpio)

- Navegador normal



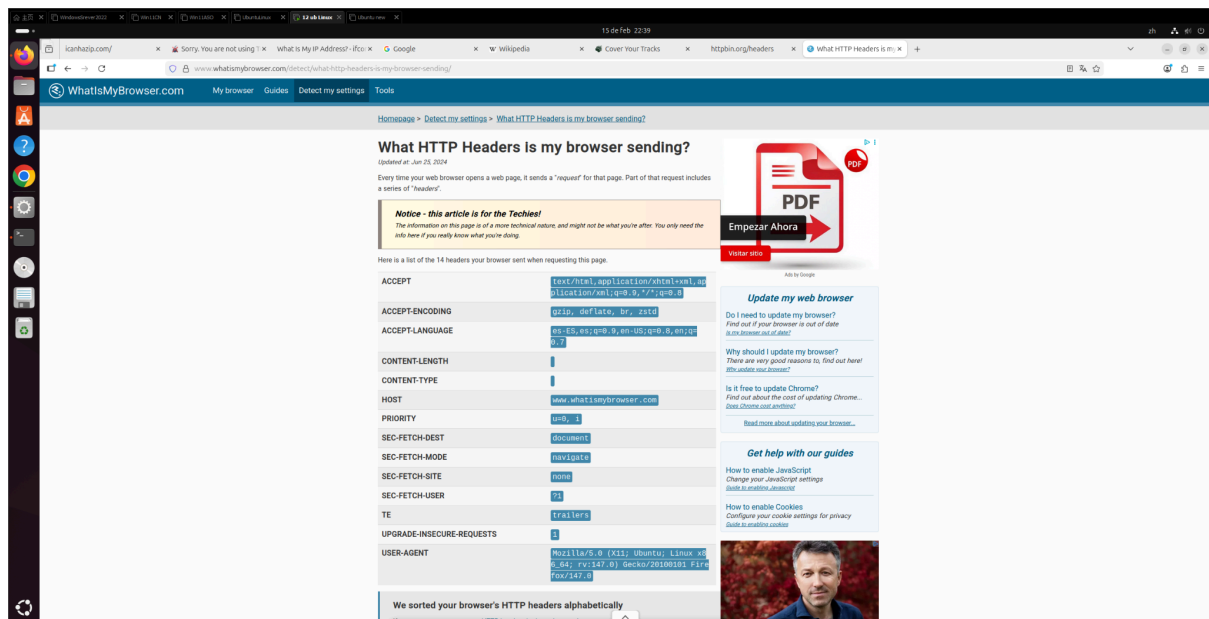
- Tor Browser



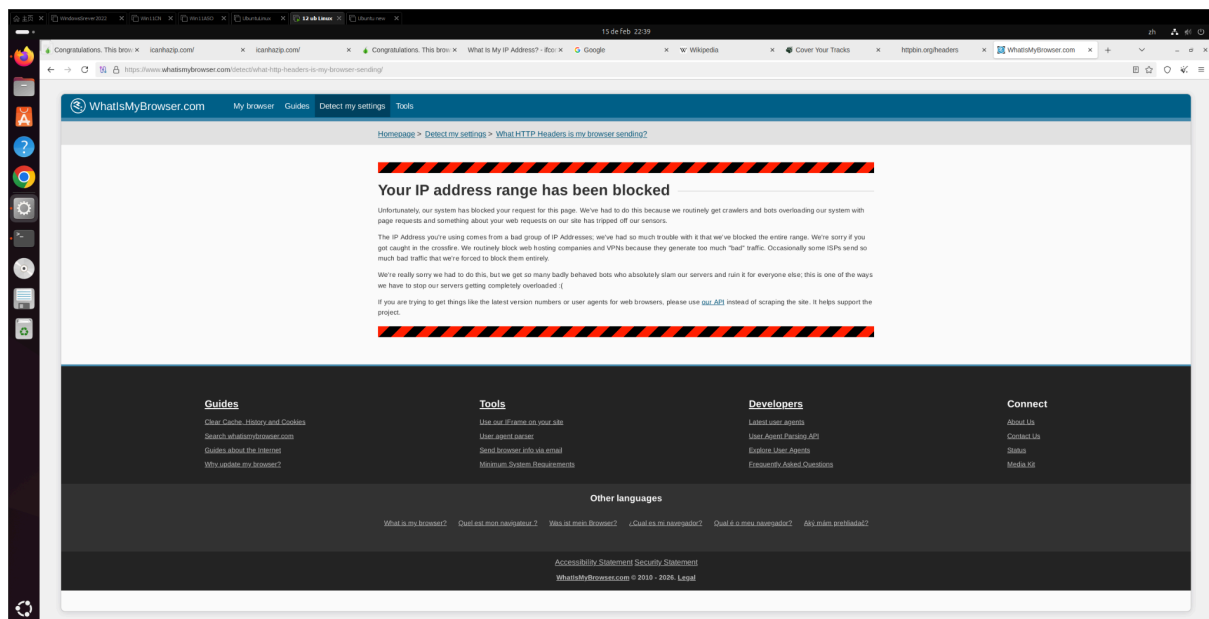
1. El agente de usuario es diferente: Tor emplea números de versión distintos para estandarizar las huellas digitales de los usuarios y mitigar los riesgos de identificación.
2. Idioma aceptado más neutral: Tor envía ponderaciones de preferencias lingüísticas más equilibradas, evitando el fuerte sesgo hacia el español que se observa en los navegadores estándar, lo que reduce la filtración de información regional.
3. Mayor estandarización: Tor envía menos campos de encabezado y más uniformes, lo que minimiza las diferencias entre los usuarios y dificulta que los sitios web los rastreen o identifiquen a través de los encabezados.

Bonus opcional (para alumnos más finos)

- Navegador normal



- Tor Browser



En el navegador normal, se transmite información detallada y exhaustiva en los encabezados, incluidas especificaciones precisas del agente de usuario y preferencias de idioma explícitas. Los sitios web pueden aprovechar estos datos para identificar y rastrear a los usuarios.

Por el contrario, en el navegador Tor, dado que utiliza la dirección IP de un nodo de salida de Tor, los sitios web bloquean activamente el acceso a la información de los encabezados. Esto confirma que el tráfico se enruta a través de la red Tor y se identifica como datos anónimos.