C1.

INTRODUCCIÓN A LA DEEPWEB Y LA DARK WEB

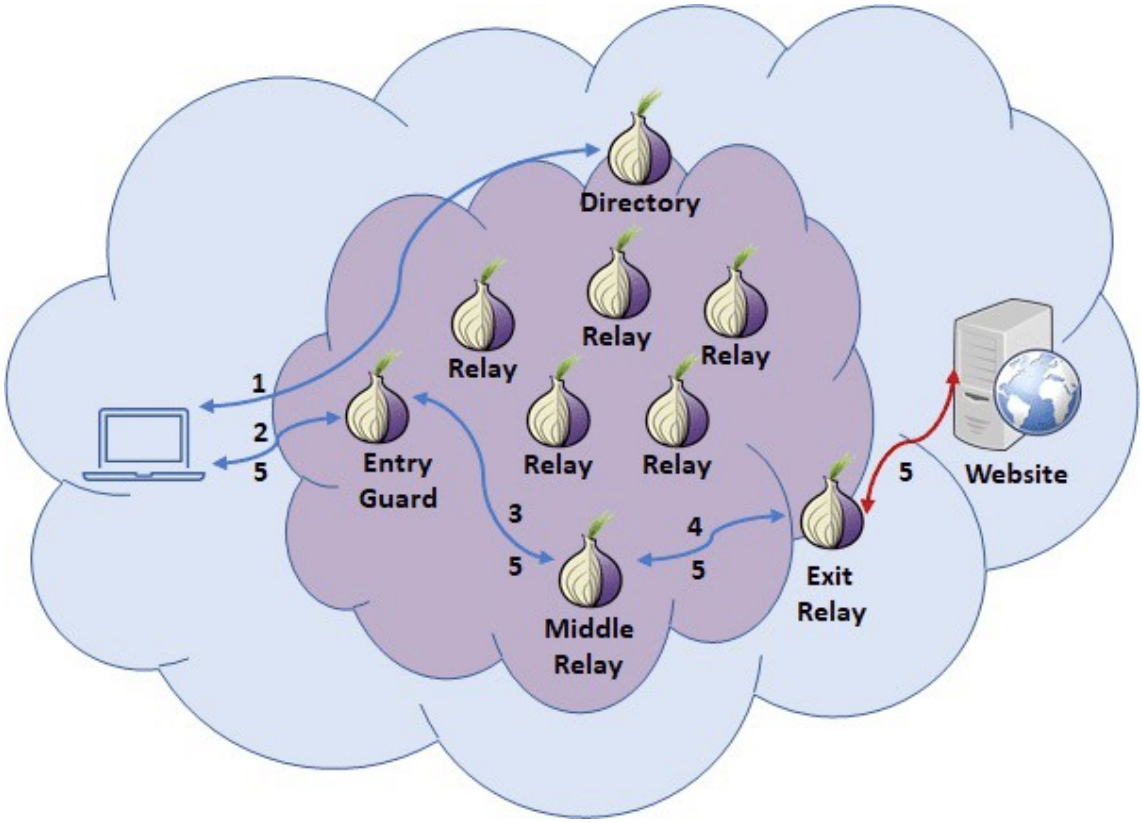
C1.2. Acceso a Darknets

ÍNDICE

1 LA RED TOR

Tor originariamente era (y es, actualmente) un sistemas de enrutamiento del tráfico de Internet que aplica un protocolo conocido como el protocolo cebolla, debido a que utiliza varias capas por las que los paquetes pasan encriptando las IPs de origen. El nombre **Tor** es, precisamente, acrónimo de ***The Onion Router***.

El objetivo fundamental es, como ya se ha dicho, asegurar la navegación anónima. Para ello, la red dispone de un elevado número de nodos o *relays*. Cuando un usuario inicia una sesión en **Tor**, se establece un circuito de varios de estos *relays* por el cual viajarán los paquetes de esa sesión. En cada nodo de ese circuito (relay) los paquetes son "oscurecidos". Cuando el paquete sale, finalmente, de esa red a través de un nodo de salida y se encamina a su verdadero destino, no hay forma de saber cuál era su **IP** real de origen. Dicho de otra forma, dentro de la red de *relays* (la cebolla), la **IP** original de los paquetes se hace opaca de unas capas a otras. Los puntos de destino final, fuera de la cebolla, sólo conocen la **IP** del *relay* de salida del circuito interno de **Tor**.



Básicamente, **Tor** tiene dos componentes: el navegador y los llamados servicios **Tor**.

2 EL NAVEGADOR TOR

Se trata de un navegador web aparentemente normal, como cualquiera de los habituales (*Chrome, Firefox, Edge, Safari* ….). De hecho, clona muchas de las funcionalidades de *Firefox*, incluso su aspecto visual y operacional; los complementos y plugins *Firefox* funcionarán también en el navegador **Tor**.
Tor permite navegar en el *Web de Superficie*, con URLs normales, y también, indistintamente, en los sitios ocultos **Tor**, que tienen direcciones diferentes. Los sitios ocultos **Tor** consisten en una secuencia de 56 caracteres, seguida del sufijo de dominio ***.onion***
Por ejemplo:

http://search7tdrcvri22rieiwgi5g46qnwsesvnubqav2xakhezv4hjzkkad.onion
http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/onions.php

Hay que tener en cuenta que **Tor** está actualmente en la versión 3 y que, en versiones anteriores, la secuencia de caracteres que va antes de ***.onion*** era de sólo 32 caracteres. Estas direcciones antiguas de 32 caracteres no funcionarán y no podrá accederse a ellas.

INSTALACIÓN

Hay versiones del navegador **Tor** para Windows, Linux, Mac y Android, que pueden descargarse del sitio web de **Tor**:

https://torproject.org/en/

El proceso de instalación es tan simple como descargar y descomprimir; naturalmente, pueden añadirse enlaces al escritorio, entradas en los menús del sistema, atajos, etc. si se desea y según cada sistema operativo.

Tor puede configurarse casi de la misma forma que configuramos *Firefox*; naturalmente, algunas de las funcionalidades de éste carecen de sentido en **Tor**, como la instalación y administración de certificados digitales. Difícilmente querremos firmar digitalmente cosas cuando hacemos navegación anónima.

USO DEL NAVEGADOR TOR

Cuando iniciamos **Tor** éste debe conectarse a un circuito de *relays* de la propia red **Tor**; esto puede tardar unos segundos, dependiendo del estado de las redes. A partir de ahí, la navegación es básicamente como con cualquier otro navegador: escribiendo la dirección o URL

deseado en la barra de direcciones, utilizando nuestros propios marcadores o favoritos, o a través de algún buscador.

Como se ha comentado anteriormente, el navegador **Tor** nos permite acceder y utilizar sitios y páginas de la Web de Superficie, pero de forma totalmente anónima. Cualquier sitio web funcionará perfectamente en el navegador **Tor**; sus resultados serán exactamente los mismos que si lo usáramos en el Web de Superficie, pero sin queese sitio web conozca nuestra **IP** y pueda, en consecuencia, rastrearnos.

NAVEGACIÓN ANÓNIMA

Entendemos por navegación anónima aquélla en la que nuestra **IP** no llega a conocerse por los servidores a los que nos conectamos. Existen otros medios para que los servidores nos identifiquen, como las conocidas *cookies*, pero éstas pueden gestionarse e incluso borrarse desde cualquier navegador "normal". El navegador **Tor** también permite gestionar *cookies* (exactamente igual que *Firefox*) pero además ocultará nuestra **IP**, que es la clave del anonimato.

Los servidores web registran todas las peticiones o *requests* que reciben; lo hacen cuando nos conectamos a una página o cuando pinchamos con el ratón en un enlace o actividades similares. Dependiendo del software de servidor web que tenga cada sistema, ese registro se guarda con un formato u otro (aunque hay formatos más o menos estandarizados para esto).

Una gran mayoría de servidores web utilizan un software de servidor llamado *Apache*; un ejemplo de una entrada en el *log* del servidor disponible en la máquina *abubilla.usal.es*:

```
4.250.24.75 - - [15/Jun/2023:02:05:26 +0200] "GET /
HTTP/1.1" 200 3453 "-" "Mozilla/5.0 (Windows NT 6.1;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/61.0.3163.100 Safari/537.36"
```

La línea está dividida en varios campos, que dependen de la configuración impuesta por el administrador del servidor, pero que al menos recogerá:

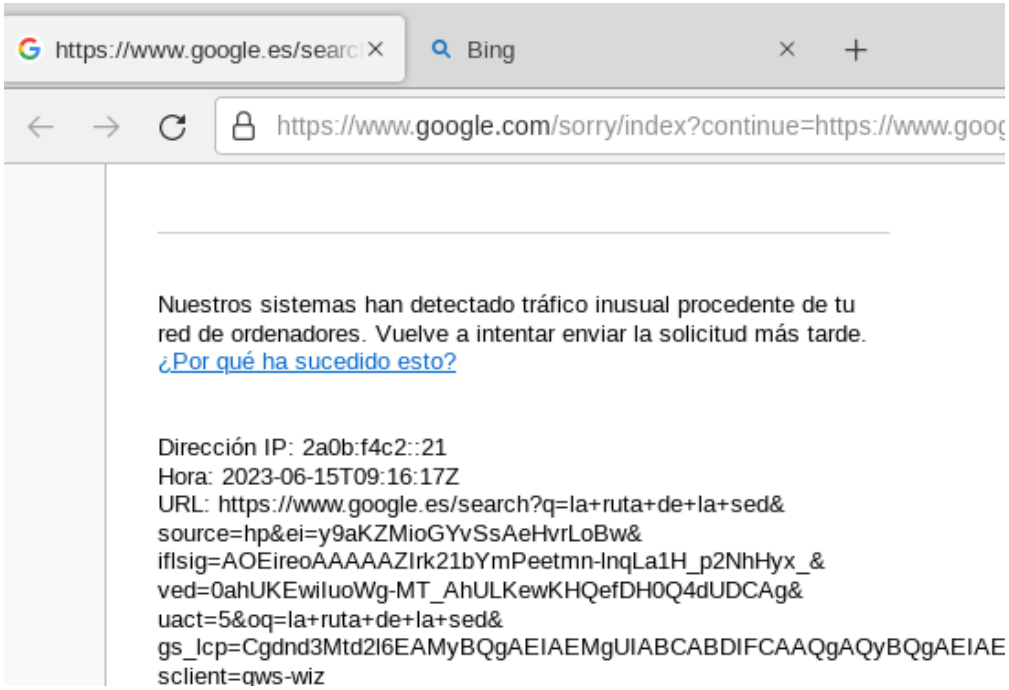
- la **IP** de quien se conecta al servidor (campo 1: 4.250.24.75 en este ejemplo)
- fecha y hora de esa conexión
- la petición concreta que se hace al servidor (GET / HTTP/1.1)
- el código de estado del servidor (200)

- y otras informaciones.

Normalmente, cuando nos conectamos a esa página, el *log* del servidor web recogerá nuestra verdadera **IP**.

Sin embargo, cuando lo hacemos desde el navegador **Tor**, aunque nuestra **IP** sigue siendo la misma, el *log* recoge otra completamente distinta: la **IP** del nodo o *relay* de salida del circuito que nuestro navegador haya establecido dentro de la red **Tor**.

Aunque la red **Tor** consta de miles de puntos de salida (el portal del propio **Tor** proporciona métricas y estadísticas sobre esto), existen listas de las **IP**s de esos puntos de salida. Estas listas son utilizadas como listas negras por algunos sitios web de Superficie, que nos denegarán el acceso cuando intentamos acceder con el navegador **Tor**.



Un caso típico es el del buscador *Google,* que detecta (no siempre) si estamos usando **Tor** y nos denegará el acceso. *Bing* también lo hace, aunque parece que sus listas no son (todavía) tan precisas y detecta **Tor** con más dificultad.

SERVICIOS TOR

Los servicios **Tor** son, en su mayor parte, sitios y páginas web a los cuales se accede a través de **Tor**. Tienen una dirección **Tor** y, en consecuencia, sólo puede accederse a ellos con el navegador **Tor**.

A excepción de la dirección, las páginas de los servicios **Tor** son páginas en código HTML normal y corriente. Ciertamente, muchos de los que crean esas páginas procuran evitar llamadas a elementos externos, código JavaScript y similares a fin de evitar posibles agujeros de seguridad. Pero, por lo demás, son servicios web técnicamente 'normales'.

Para acceder, podemos utilizar la barra de direcciones del navegador **Tor** y escribir allí la dirección .onion del servicio en cuestión. Aunque, dada la naturaleza de estas direcciones, es una opción poco cómoda, hay que tener en cuenta que podemos encontrar direcciones de servicios **Tor** en páginas del web de superficie. La posibilidad de copiar y pegar puede ser una opción.

Además de ello, tenemos dos posibilidades: el uso de buscadores específicos para la red **Tor** y la consulta de directorios y repertorios de listas de direcciones **Tor**.