UNIVERSIDADE DA CORUÑA

Ocultación

LSI - 2019/2020

José Manuel Vázquez Naya
jose@udc.es

Contenido

- Objetivos de la ocultación
- Proxies
- VPN
- Redes de anonimato
  - La red Tor
  - Otras redes de anonimato
- Navegación anónima

Objetivos de la ocultación

- Derecho a la privacidad y al anonimato
- Prevenir que se conozca nuestra IP y/o hábitos de navegación
- Acceder a contenido sin censura
- …
- "Otros" objetivos…

https://t.co/ICLfoWwZtT

PROXIES

Uso de proxies

- Una IP proporciona mucha información

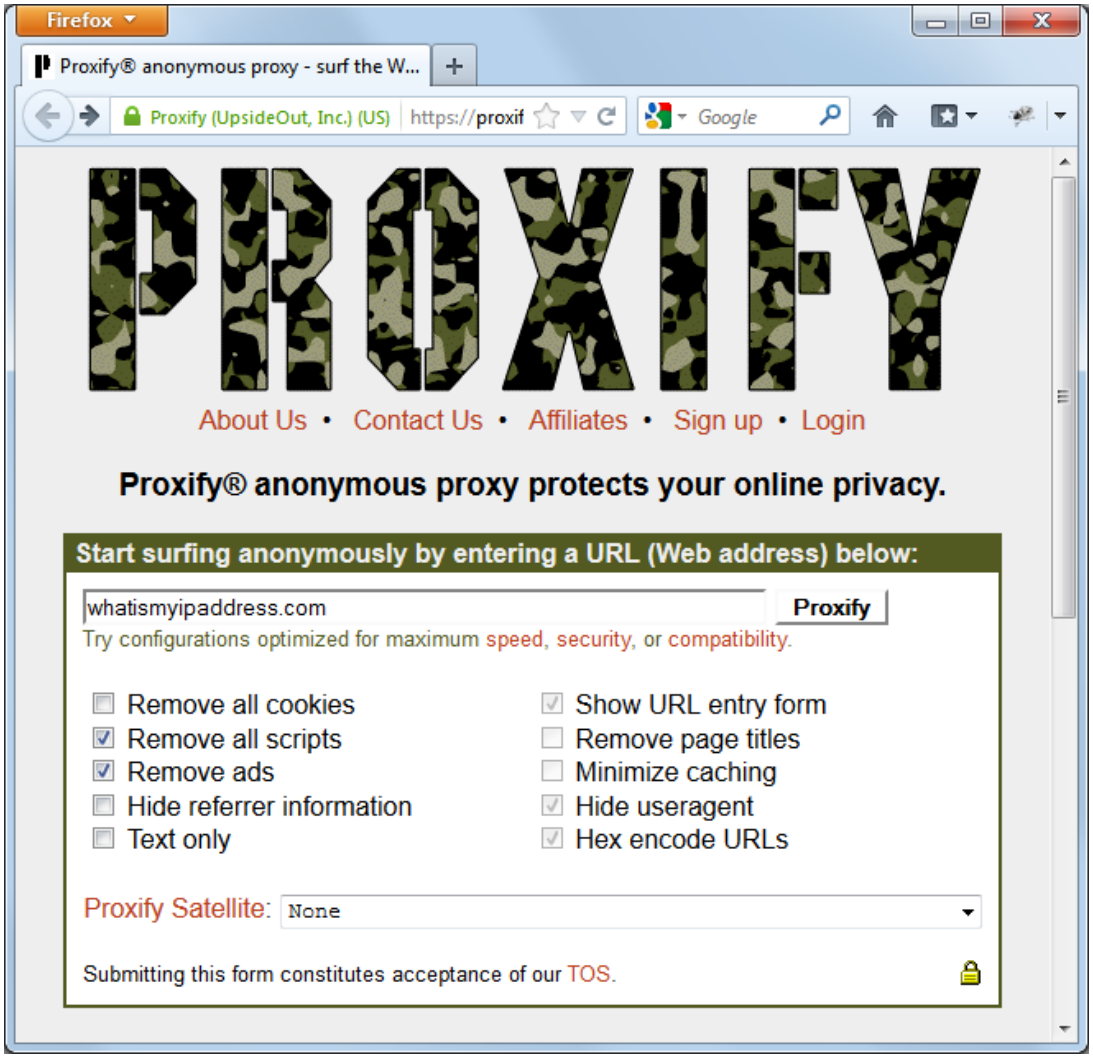
- Se puede ocultar la dirección IP usando un proxy
  - El proxy actúa como un intermediario
  - El destinatario ve la IP del proxy

- Tipos
  - Web-based Proxies
  - Open Proxies

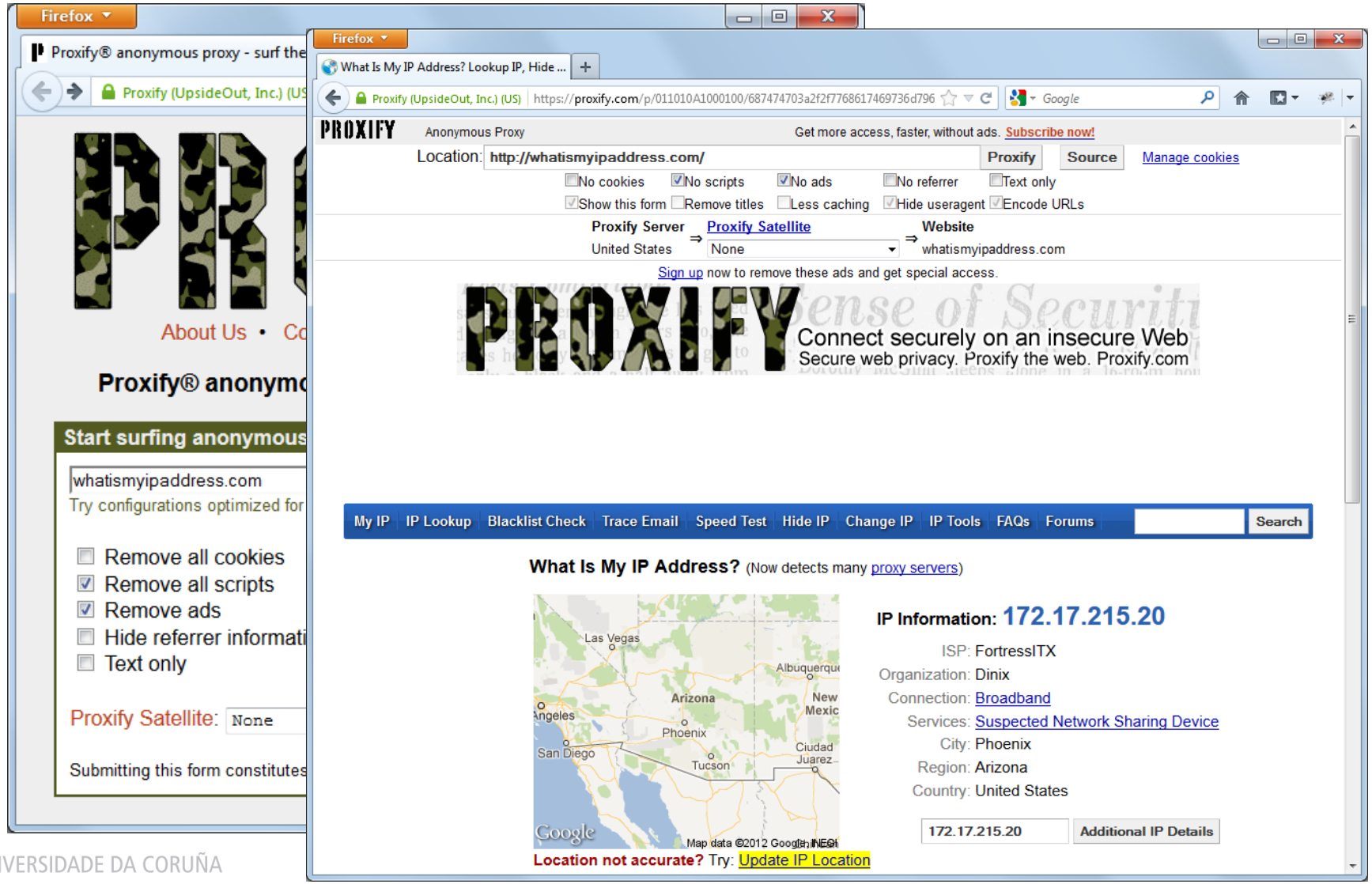
Tipos de Proxies

- ***Web-based Proxies***
  - Sitios Web que permiten acceder al contenido de terceros
  - No requieren configuración en cliente (se accede a través del navegador)
  - Ocultan dirección IP del usuario -> **privacidad**
  - Además, la mayoría de los proxies cifra el tráfico entre el usuario y el proxy -> **confidencialidad**
  - Algunas páginas pueden no mostrarse correctamente
  - Publicidad o pago
  - Lista en: http://proxy.org/cgi_proxies.shtml

Tipos de Proxies



Tipos de Proxies



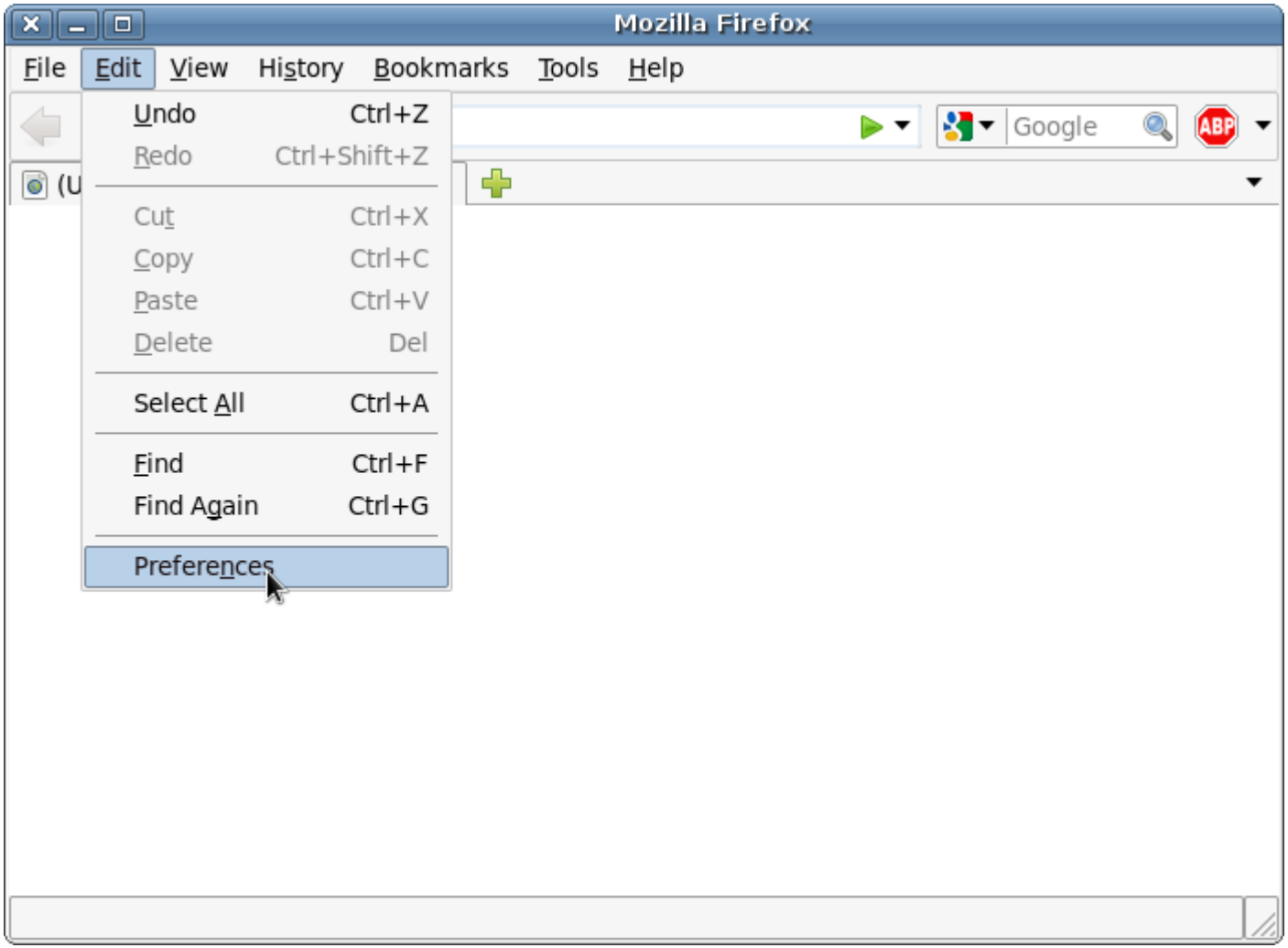
Tipos de Proxies

- ***Open Proxies***
  - El cliente debe configurar los datos del proxy. Después de eso, la navegación es "transparente" para el usuario
  - Dos tipos:
    - HTTP
    - SOCKS
  - No alteran la página original
  - Ejemplos:
    - http://proxyhttp.net/
    - http://sockslist.net/

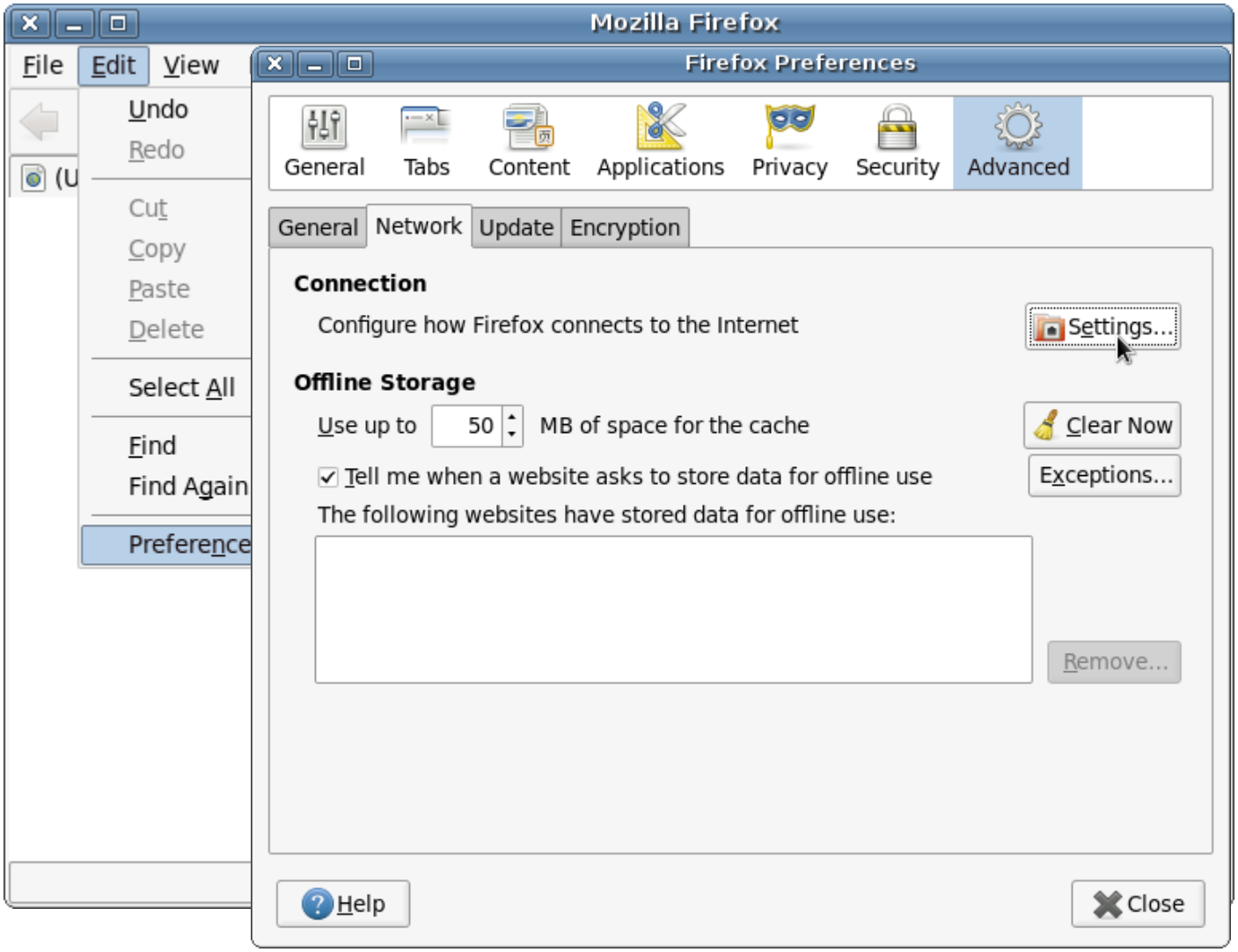
Open proxies

- En los datos de los proxies, aparece una columna "Anonymity", cuyos valores pueden ser:
  - Transparent: sin anonimato
  - Anonymous:
    - no HTTP_X_FORWARDED_FOR header
    - Cuando accedermos a un servidor a través de un proxy, el servidor puede leer esa variable para obtener la IP del cliente
  - High anonymous/Elite proxy:
    - no HTTP_X_FORWARDED_FOR, HTTP_VIA, HTTP_FORWARDED, HTTP_X_CLUSTER_CLIENT_IP, HTTP_CLIENT_IP, HTTP_PROXY_CONNECTION headers
    - Se eliminan otras variables que pudieran revelar la IP real del cliente

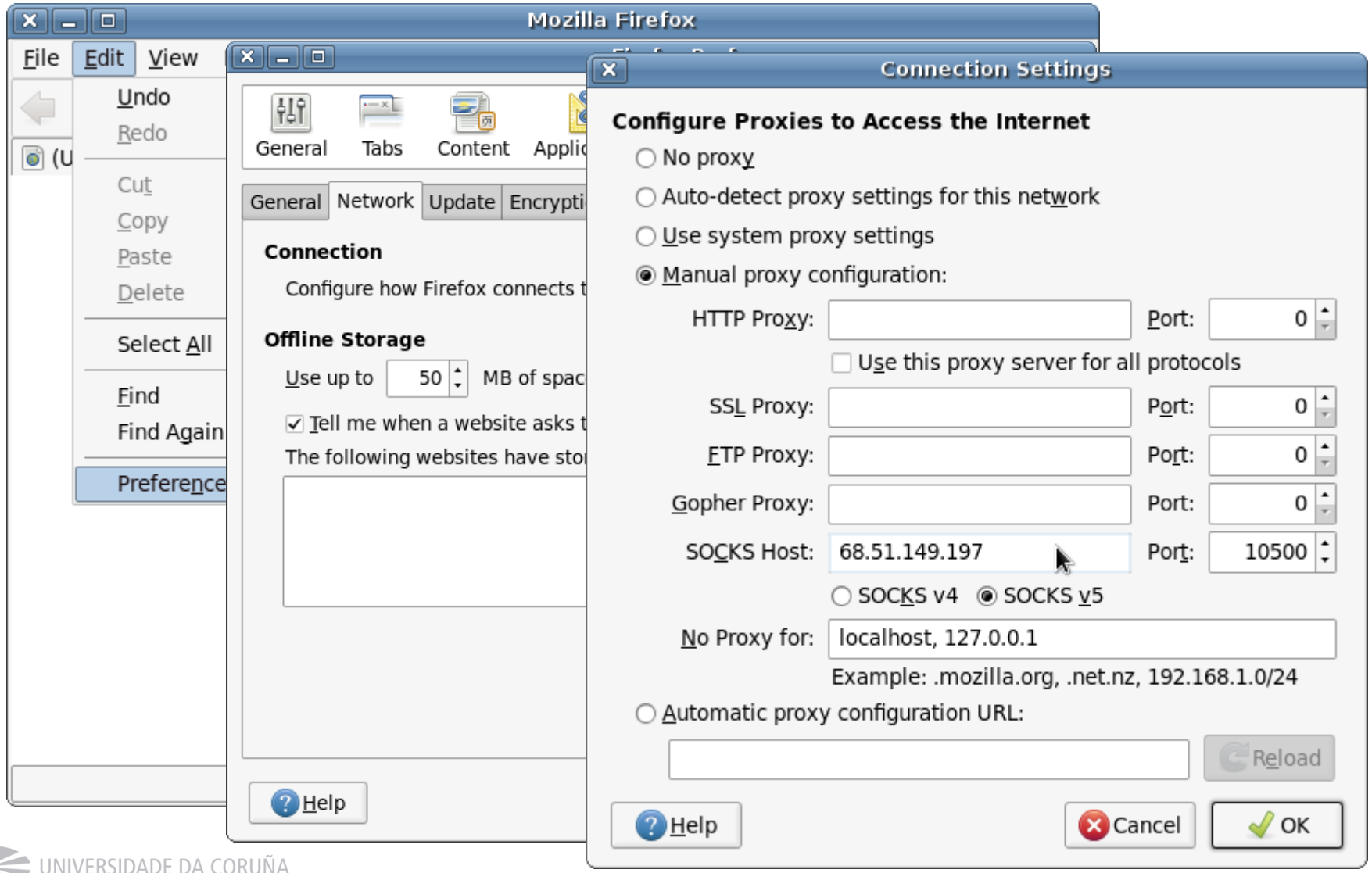
Tipos de Proxies



Tipos de Proxies



Tipos de Proxies



Uso de Proxies

- Pero… ¿quién gestiona el proxy?

- Si la conexión es en claro (no cifrada, p.ej. http) el proxy puede leer todo el tráfico

VPN

- Hay servicios comerciales que ofrecen aplicaciones para establecer una conexión a través de VPN.
  - Mediante un software cliente, se crea un túnel entre el equipo cliente y un servidor de la organización proveedora del servicio.
  - Depositamos nuestra confianza en la organización.
  - P.ej.: Anonymizer, Hotspot Shield, Tunnelbear, …
  - La calidad, fiabilidad y eficacia de estos servicios varía mucho de unos a otros.

REDES DE ANONIMATO

Redes de anonimato

- Permiten a sus usuarios comunicarse de forma anónima.
- Usan cifrado por capas (*onion routing*).
- Los usuarios comparten sus recursos con la red (ancho de banda,…).
- Ralentizan la comunicación.
- Ejemplos: Freenet, I2P, JAP, y TOR.

La red Tor

- Qué es?
- Cómo funciona?
- Tor project

La red Tor. Qué es?

- Tor o TOR es una abreviatura de “**The Onion Routing**”.

- Evolución del proyecto "*onion routing*" del Naval Research Laboratory de los EE.UU.
  - Objetivo original: proteger las comunicaciones del gobierno.

La red Tor. Qué es?

- Es una herramienta gratuita cuyo objetivo es que la gente pueda usar Internet de forma anónima (anonimato de origen).

- Tor protege al usuario haciendo rebotar sus comunicaciones sobre una red distribuida de ***relays*** (también llamados ***Onion Routers***) ejecutados por **voluntarios** de todo el mundo:
  - Evita que alguien que escucha la conexión a Internet sepa qué sitios visita el usuario (cifrado).
  - Evita que los sitios que visita conozcan su **dirección IP real**.
  - Permite acceder a sitios bloqueados para el usuario.

- Tiene puntos débiles (no puede considerarse infalible).

Componentes

- Dos tipos de entidades:
  - **Onion Router (OR)**
    - Encaminadores, **nodos** (AKA ***relays***) de la red Tor.
    - Cualquier usuario puede actuar como nodo.
    - Los nodos se comunican entre sí mediante TLS.
    - Algunos, además, funcionan como **servicio de directorio.**
      - Proporcionan lista de ORs, con información de cada uno.
  - **Onion Proxy (OP)**
    - Son los usuarios finales.
    - Software que permite:
      - Consultar servicio de directorio.
      - Establecer circuitos aleatorios a través de la red.
      - Gestionar conexiones de aplicaciones del usuario.

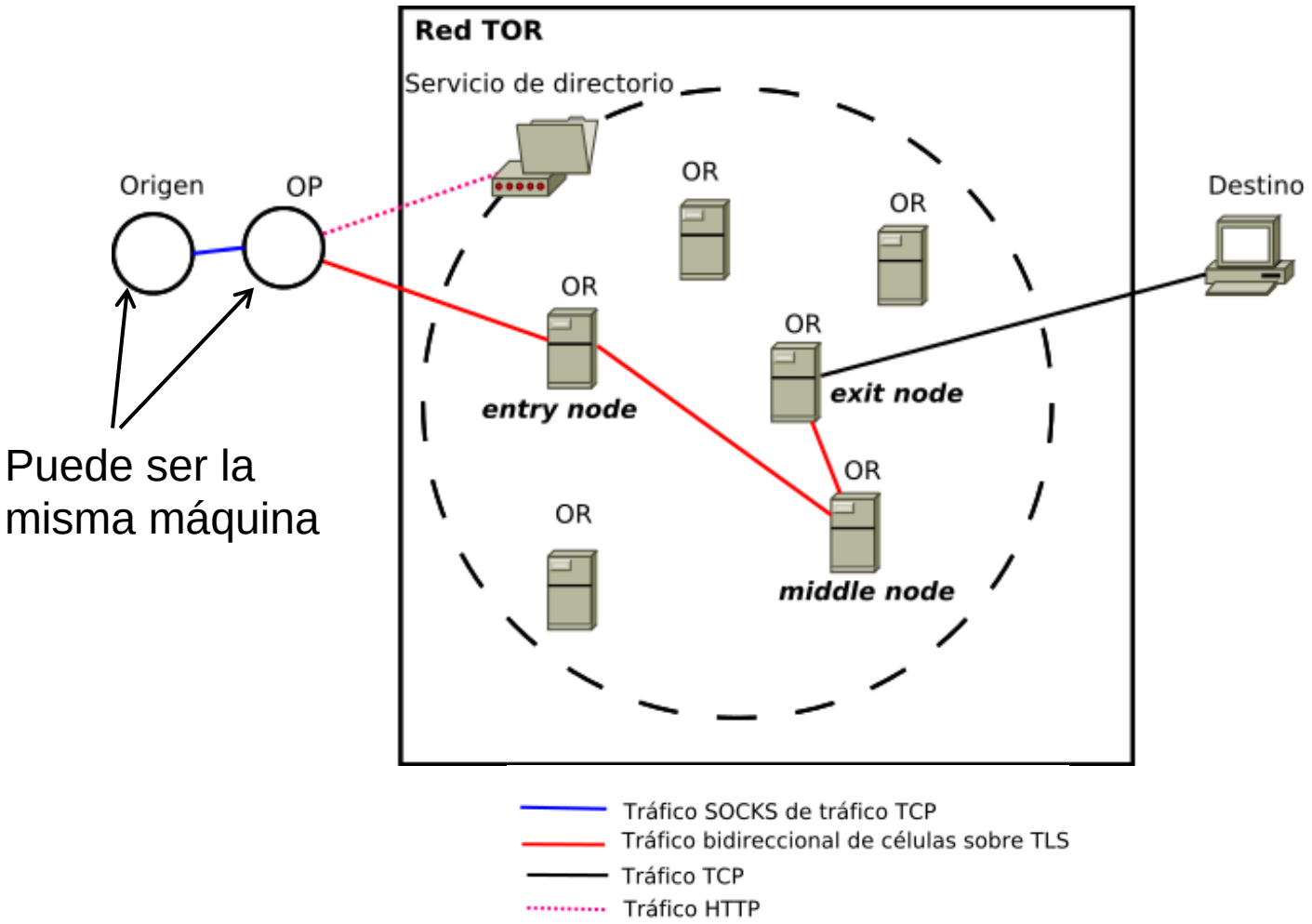
Lista de nodos Tor

- ¿Pero quién tiene nodos en la red Tor?
  - Compañías como Amazon, Universidades como el Massachusetts Institute Of Technology, …
  - Se puede consultar el listado en https://torstatus.blutmagie.de/
  - En https://metrics.torproject.org/rs.html se pueden realizar consultas. Por ejemplo:
    - Ver los principales *relays*:
      - https://metrics.torproject.org/rs.html#toprelays
    - Ver *relays* en España:
      - https://metrics.torproject.org/rs.html#search/country:es

Patrocinadores del proyecto Tor

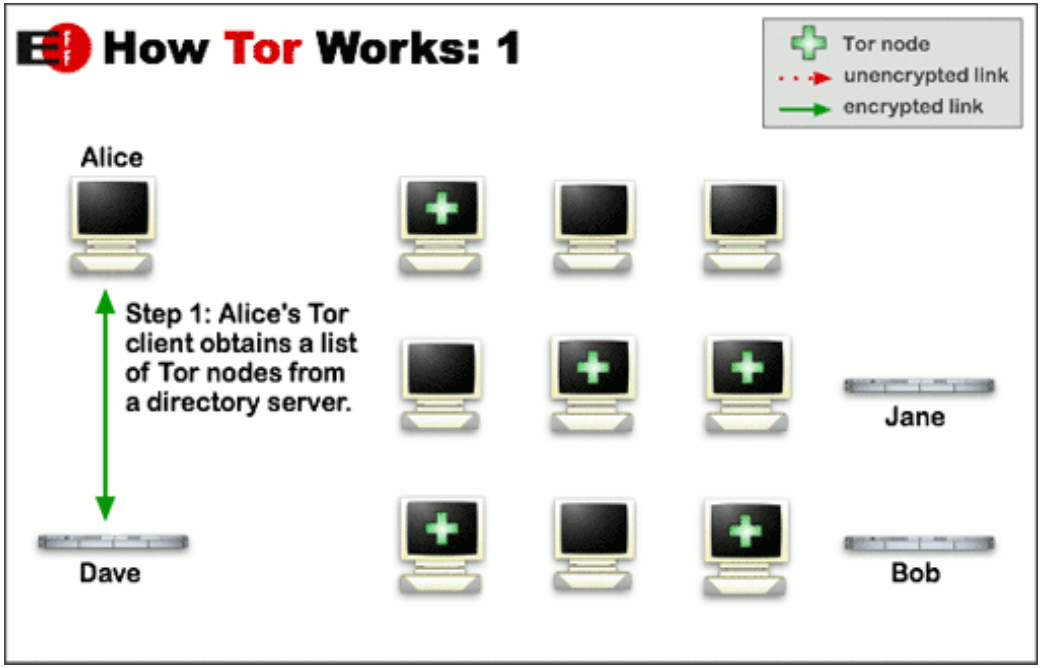
- ¿Y quién lo financia?
  - https://www.torproject.org/about/sponsors/

Funcionamiento de la red Tor



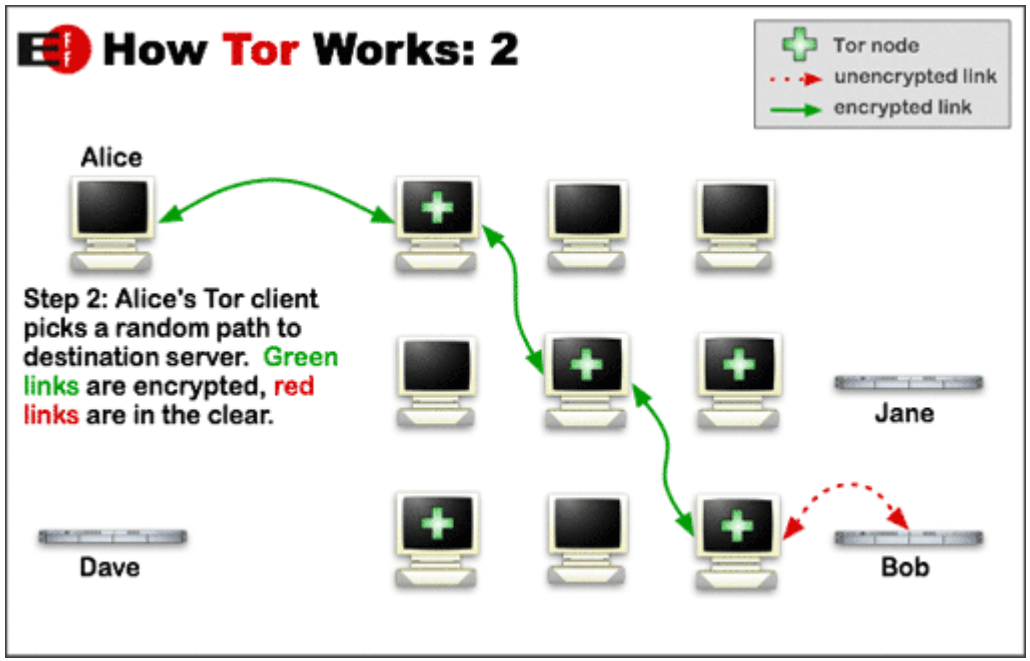
Funcionamiento de la red Tor

- Paso 1: Obtener un listado de nodos
  - Alice quiere establecer una conexión con Bob a través de la red Tor
  - Utilizando un software cliente (p.ej. Tor Browser Bundle) se conecta a un servidor de directorio y recupera una lista de nodos de la red Tor



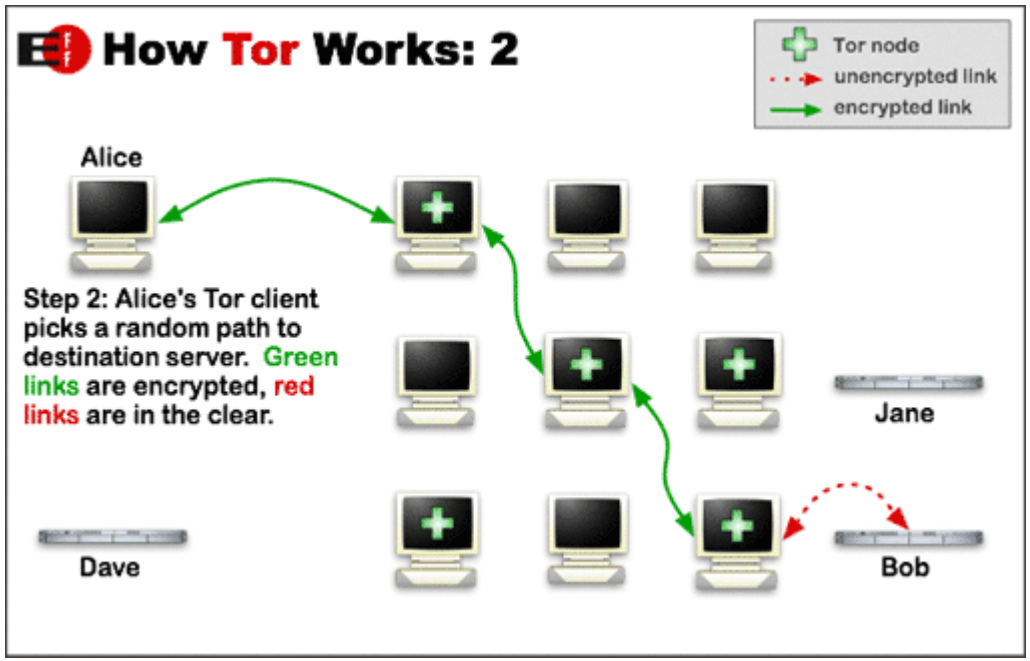
Funcionamiento de la red Tor

- Paso 2: Crear un circuito
  - El software cliente selecciona un conjunto de nodos (OR) al azar (defecto, 3)
  - El cliente negocia un conjunto de claves separadas para cada nodo del circuito para asegurar que ningún nodo puede trazar las conexiones



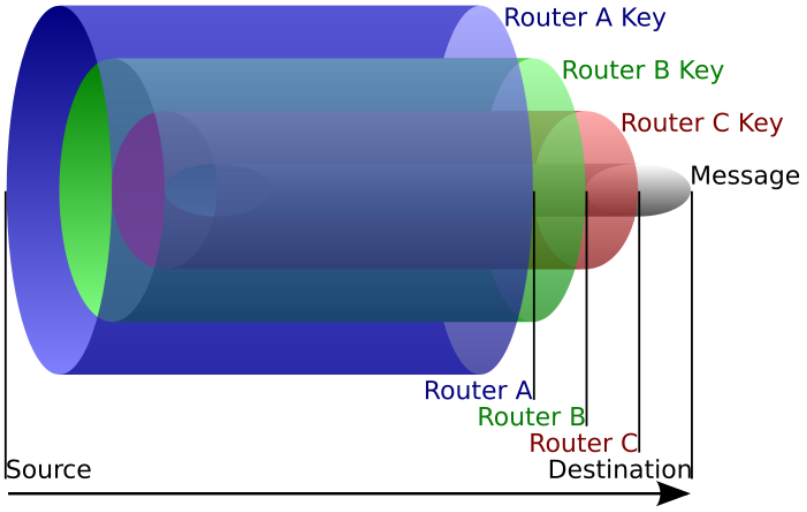
Funcionamiento de la red Tor

- Paso 2: Crear un circuito (cont.)
  - Cada OR de la ruta conoce sólo al OR del que recibe datos y al OR al que le envía datos
  - Ningún OR conoce en ningún momento la ruta completa



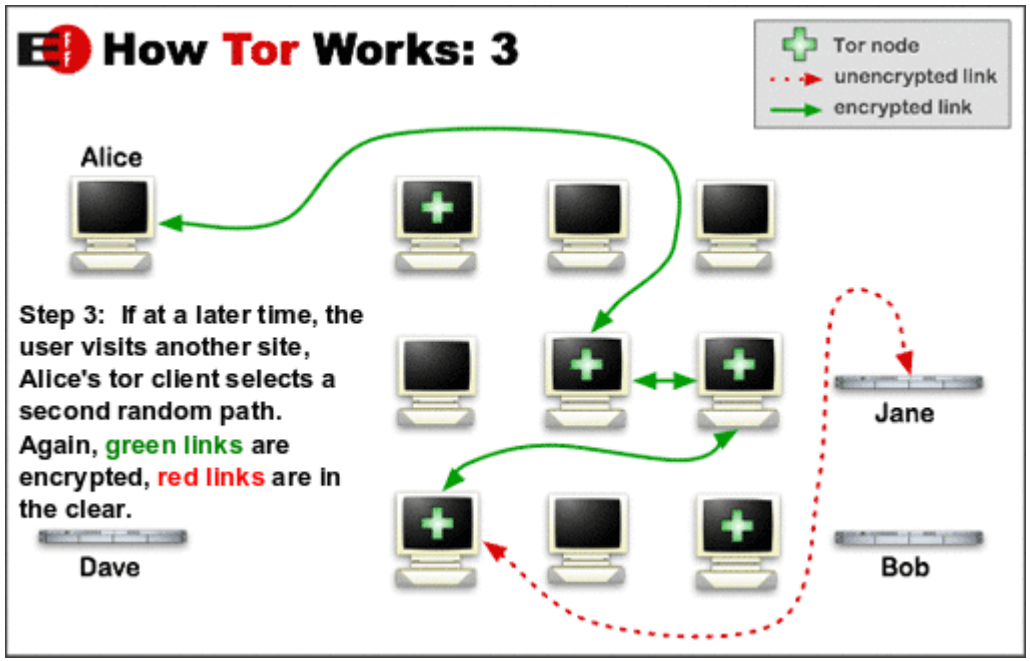
Funcionamiento de la red Tor

- Los mensajes se cifran repetidamente y se envían a través de los ORs seleccionados
- Cada OR elimina una capa de cifrado para descubrir **instrucciones de enrutado** y envía el mensaje al siguiente router, donde se repite el proceso. Esto evita que los nodos intermediarios sepan el origen y el destino y los contenidos del mensaje



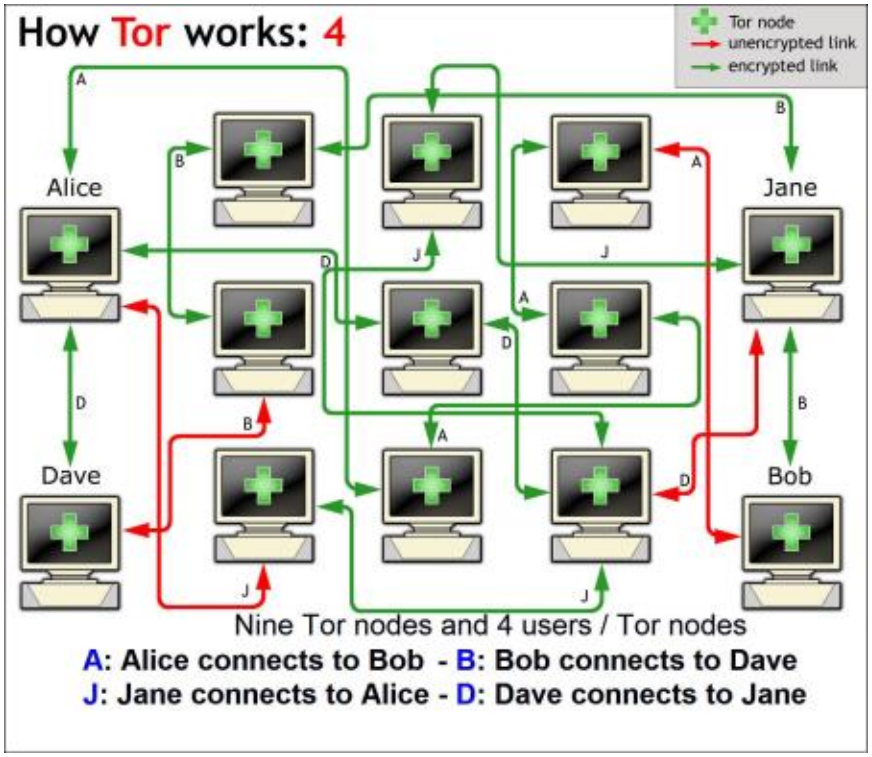
Funcionamiento de la red Tor

- Paso 3: Cambiar el circuito
  - Por razones de eficiencia, Tor usa el mismo circuito para las conexiones que se realicen durante un intervalo de 10 min aprox.
  - Pasado este tiempo, se selecciona un nuevo circuito (para evitar que se puedan asociar las nuevas acciones con las anteriores)



Funcionamiento de la red Tor

- Paso 4 (opcional): Alice como un nodo de Tor
  - Para incrementar su anonimidad, Alice podría funcionar como un nodo de Tor
    - Pero… ¿no es pública la identidad de los nodos?
    - Más conexiones a la red Tor ¿Cuál como usuario y cuál como nodo?

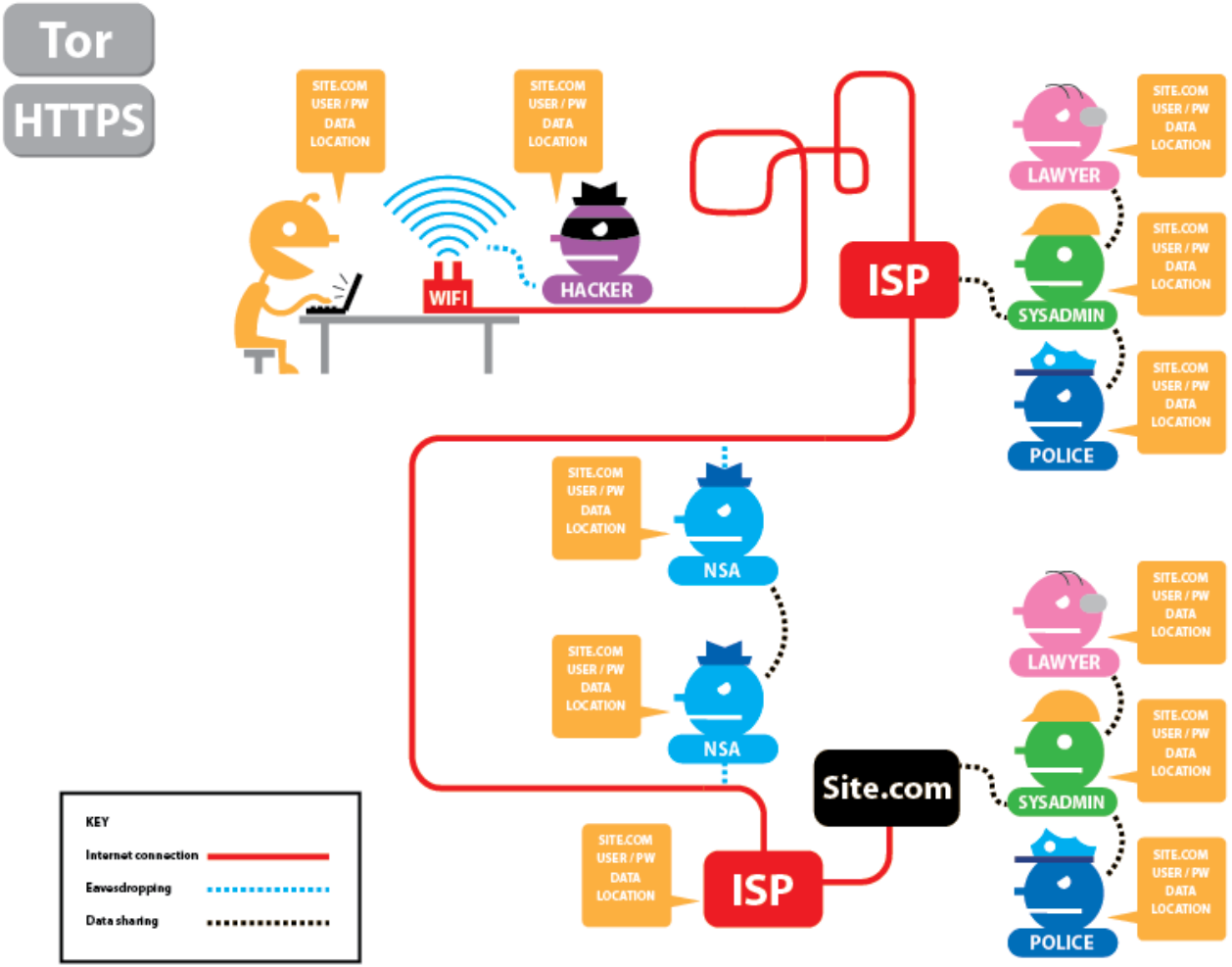


Funcionamiento de la red Tor

- El enrutado anónimo no asegura el que la **entidad** origen sea desconocida para la entidad destino
  - Esto es debido a que los protocolos de nivel superior pueden transmitir información sobre la identidad. Por ejemplo un servicio web puede usar cookies, o simplemente pedir que nos identifiquemos
  - Por esta razón es recomendable usar Tor Browser Bundle (bloquea Javascript, no acepta cookies, no almacena contraseñas, ...)

- La red Tor cifra la información a su entrada y la descifra a la salida
  - El propietario de un nodo de salida puede ver toda la información cuando es descifrada antes de llegar a Internet, por lo que aunque no pueda conocer el emisor sí que puede acceder a la información

Funcionamiento de la red Tor



https://www.eff.org/pages/tor-and-https

La red Tor. Tor project

- Tor project
  - Navegador Web, Mensajería Instantánea, Login remoto, …
  - Free y Open Source para Windows, Linux/Unix, Mac y Android
  - **https**://www.torproject.org/

La red Tor. Tor project

Tor Browser
Tor Browser contains everything you need to safely browse the Internet.

Orbot
Tor for Google Android devices.

Tails
Live CD/USB operating system preconfigured to use Tor safely.

Nyx
Terminal (command line) application for monitoring and configuring Tor.

Relay Search
Site providing an overview of the Tor network.

Pluggable Transports
Pluggable transports help you circumvent censorship.

Stem
Library for writing scripts and applications that interact with Tor.

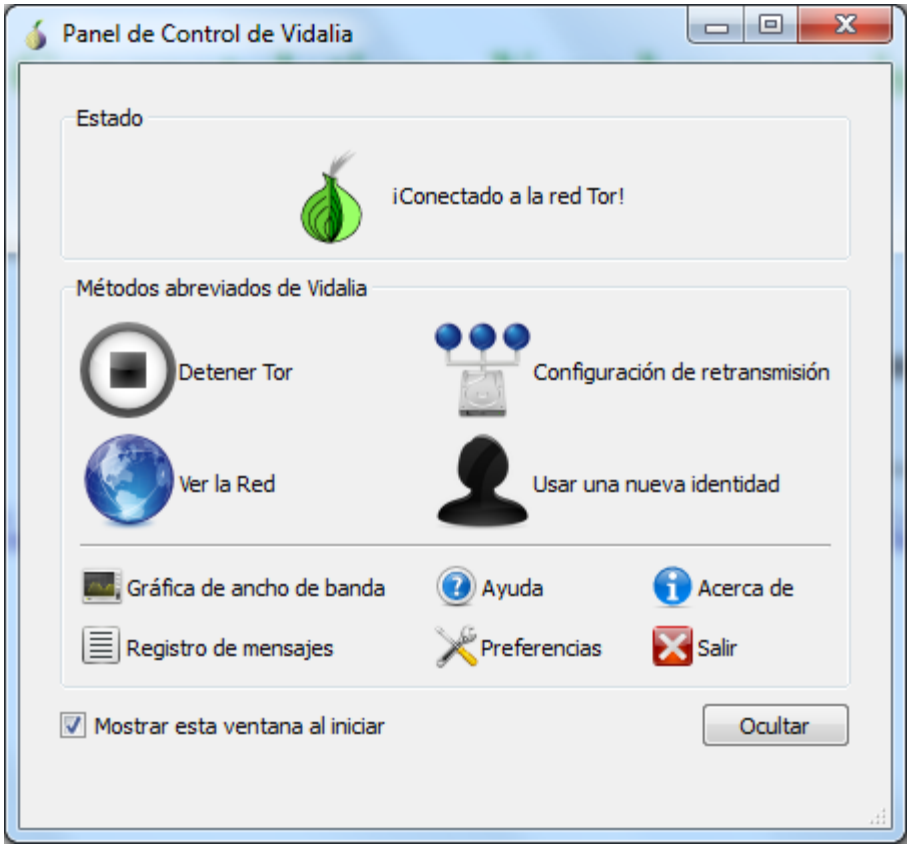
OONI
Global observatory monitoring for network censorship.

https://2019.www.torproject.org/index.html.en

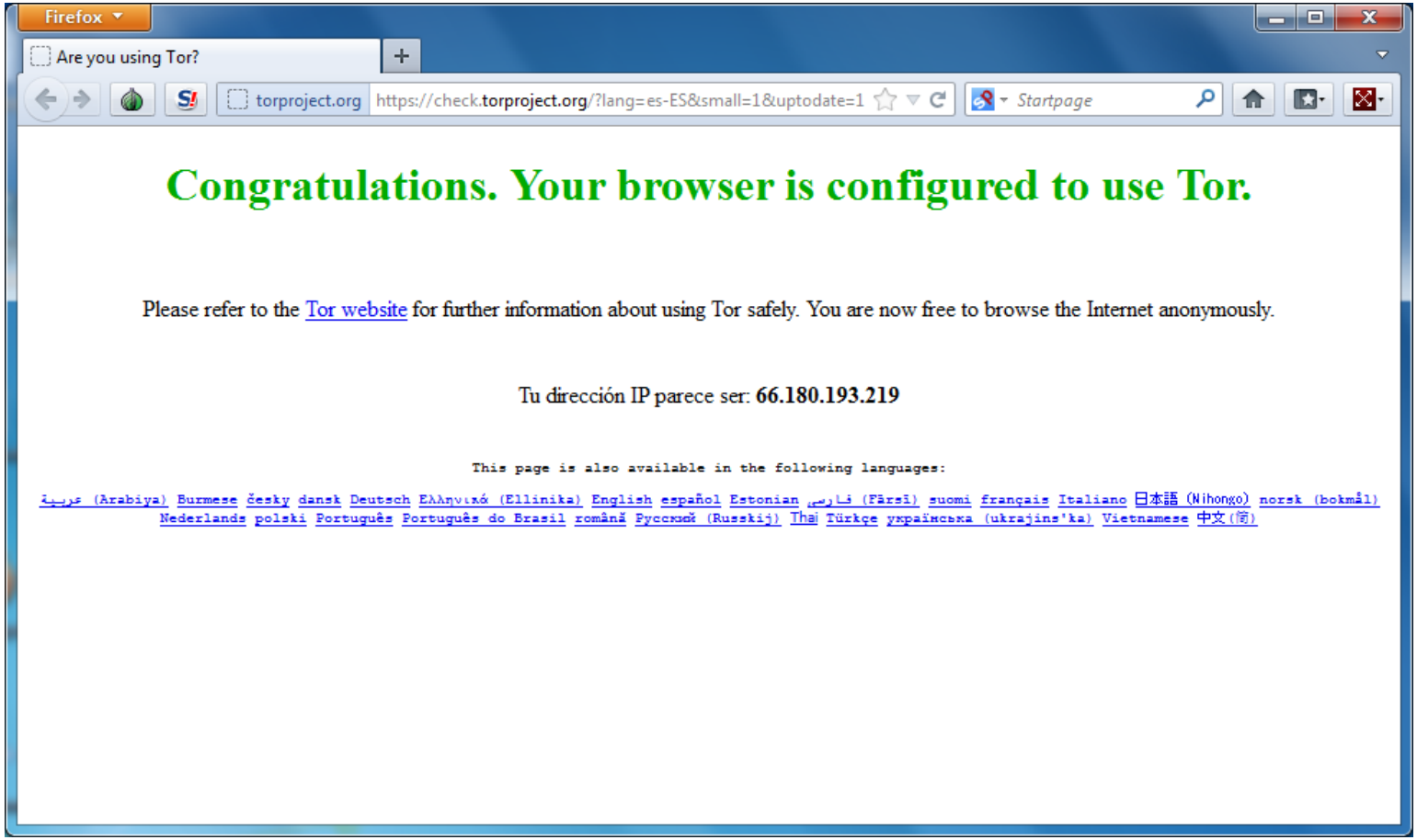
La red Tor. Tor Browser Bundle

- Es una versión portable de Firefox, securizada y pre-configurada para navegar de forma anónima usando la red Tor
- Es una opción más segura que configurar nuestro navegador
- Es necesario permanecer alerta: la ejecución de código fuera de Tor Browser puede revelar nuestra identidad

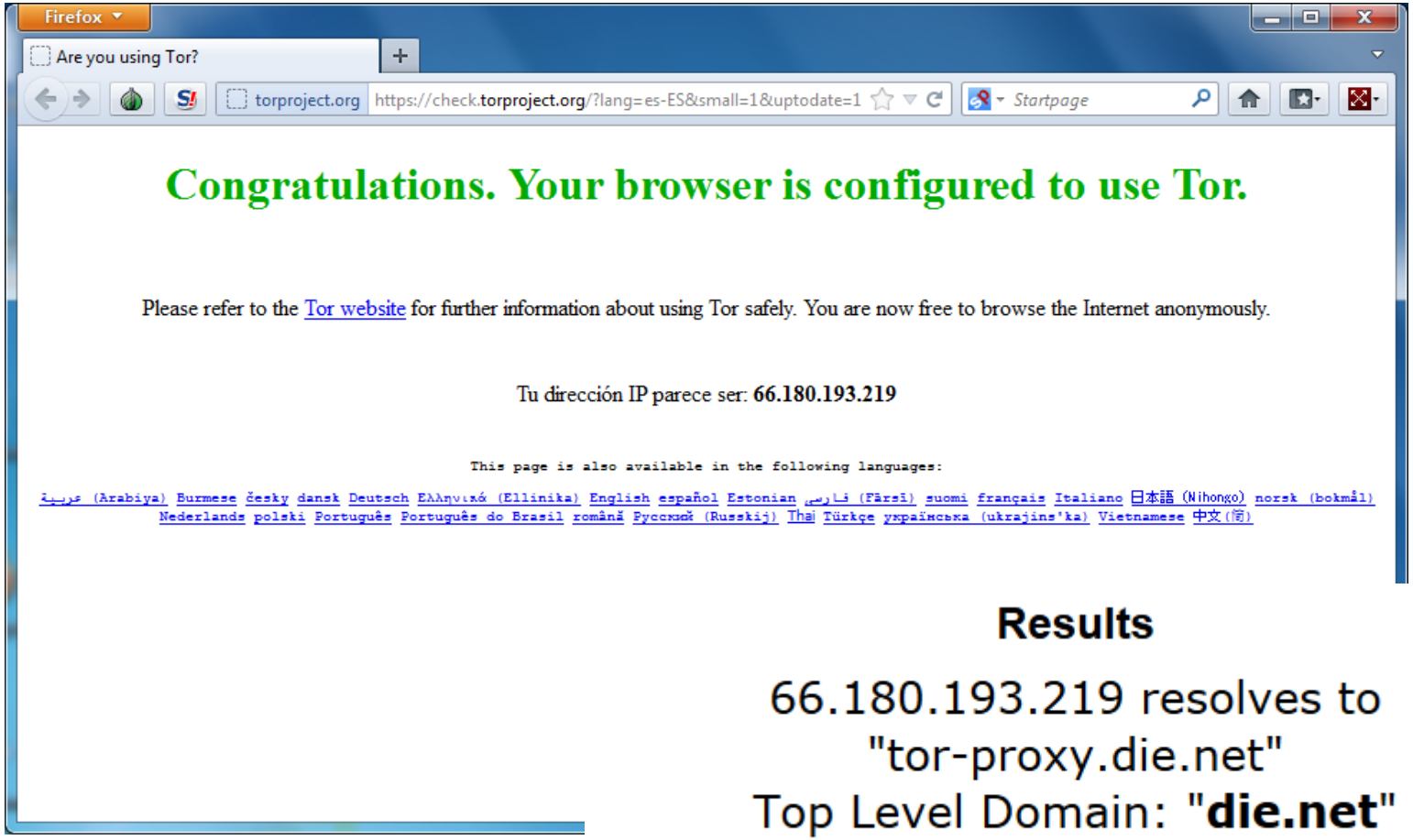
La red Tor. Tor Browser Bundle



La red Tor. Tor Browser Bundle



La red Tor. Tor Browser Bundle



Results

66.180.193.219 resolves to
"tor-proxy.die.net"
Top Level Domain: "**die.net**"
Country IP Address: **UNITED STATES**

Ataques a la red Tor

- TorMoil
  - Noviembre 2017
  - CVE-2017-16541
  - Afecta a usuarios de TOR Browser de Mac y Linux
  - Vulnerabilidad de Firefox y que se traslada a Tor Browser
    - Si un usuario pincha sobre un enlace tipo “file://”, el navegador establece conexión directa con el destino, fuera de la red Tor, revelando así la IP real del usuario
  - Corregido en la versión 7.0.9 de Tor Browser

Hidden service

- Tor permite a los usuarios ofrecer varios tipos de servicios (publicación web, mensajería instantánea, etc.) ocultando su ubicación

- Usando "rendezvous points" (puntos de encuentro), otros usuarios de Tor se pueden conectar a estos servicios ocultos, sin que ninguno de los dos conozca la identidad del otro

Tor y la Deep Web

- Deep Web: información que no puede ser indexada por los buscadores
  - Páginas protegidas por contraseña
  - Datos sólo accesibles tras consulta a BD
  - …

- Tor, además de permitir navegación anónima, da acceso a la **Deep Web Onion**
  - Dominios virtuales .onion
  - Core.onion: http://eqt5g4fuenphqinx.onion/
  - Hidden wiki

Surface Web, Deep Web y Dark Web

https://en.wikipedia.org/wiki/Deep_web#/media/File:Deepweb_graphical_representation.svg

Otras redes de anonimato

- I2P (Invisible Internet Project)
  - http://www.i2p2.de/
- Freenet
  - https://freenetproject.org/
- J.A.P.
  - http://anon.inf.tu-dresden.de/index_en.html

Navegación anónima

- Las técnicas vistas proporcionan cierto grado de anonimato y privacidad, pero hay ciertos aspectos que es necesario tener en cuenta

- Consejos:
  - Desactivar cookies
  - Bloquear JavaScript
  - …

- Los navegadores modernos incorporan modo de navegación privada

- Además, hay multitud de plug-ins para los principales navegadores, que nos facilitan esta tarea

Adblock Plus

- Plug-in para el navegador (incluye los principales)
- Código abierto
- https://adblockplus.org
- Recomendado por la EFF
- Funcionalidades:

NoScript

- Extensión para Mozilla, Firefox, SeaMonkey y otros navegadores basados en Mozilla
- Gratuito
- Código abierto
- Bloquea código JavaScript, Java, Flash, Silverlight, …
  - El usuario puede permitir la ejecución de código de ciertos sitios de confianza, añadiéndolos a una lista (*whitelist*)
- Proporciona protección frente a ataques como XSS, CSRF, clickjacking, man-in-the-middle y DNS rebinding
- http://noscript.net/

HTTPS Everywhere

- Extensión para Firefox, Chrome y Ópera
- Colaboración entre “Tor Project” y la “Electronic Frontier Foundation”
- Fuerza a usar SSL siempre que sea posible
- https://www.eff.org/https-everywhere

Documentos y Sitios de Interés

- How Tor Works. Video. Disponible en: http://www.excivity.com/ComputeCycle/howtorworks/
- Onion Routing. http://www.onion-router.net/
- Proxy.org. http://proxy.org.
  - Información sobre privacidad online y navegación anónima
- Tor project. https://www.torproject.org/
- ¿Qué es la #DeepWeb? Ciberdebate Palabra de hacker. https://www.youtube.com/watch?v=6lr5khBoSik
- La Deep Web | Documental. http://www.deepwebthemovie.com