HOW THE INTERNET WORKS

+ Secure Browsing, Circumvention and Anonymous Browsing

(Simplified)

Disusun oleh: dhyta caturani – PurpleCode Collective

Webmail

Komputer Siti

Wifi

Router

ISP Siti

ISP Joko

Penyedia Layanan Email

National Gateway

Server Farm

Komputer Joko

Wifi

Router

Routing Server

National Gateway

Browsing

Komputer Siti

Wifi

Router

ISP Siti

National Gateway

ISP Website

National Gateway

Trackers

www.news.com

Routing Server

Browsing VIA VPN

Komputer Siti

Wifi

Router

ISP Siti

VPN Provider

VPN

ISP Website

National Gateway

National Gateway

www.news.com

Routing Server

Hal Dasar Yang Perlu Diketahui

- Kita membutuhan Internet Service Provider (ISP) atau Penyedia Layanan Internet untuk terkoneksi ke internet. ISP ini kebanyakan dimiliki oleh perusahaan telekomunikasi besar atau kecil. Contoh ISP di Indonesia adalah Telkomsel, Indosat, XL. Firstmedia, Gig, Centrin, dll.
- Ketika kita terkoneksi ke Internet, ISP memberikan kita IP (Internet Protocol) Address yang berupa sederet angka. IP Address inilah yang memungkinan kita mengirim dan menerima komunikasi internet dalam rupa email, chat, web browsing, dll..
- IP Address dialokasikan secara geografis, yang artinya setiap negara memiliki IP address yang berbeda-beda.
- Setiap koneksi akan diberikan IP address tersendiri, sehingga ini menjadi identitas unik masing-masing orang yang terkoneksi ke internet.

Protocol/Jalur Komunikasi di Internet

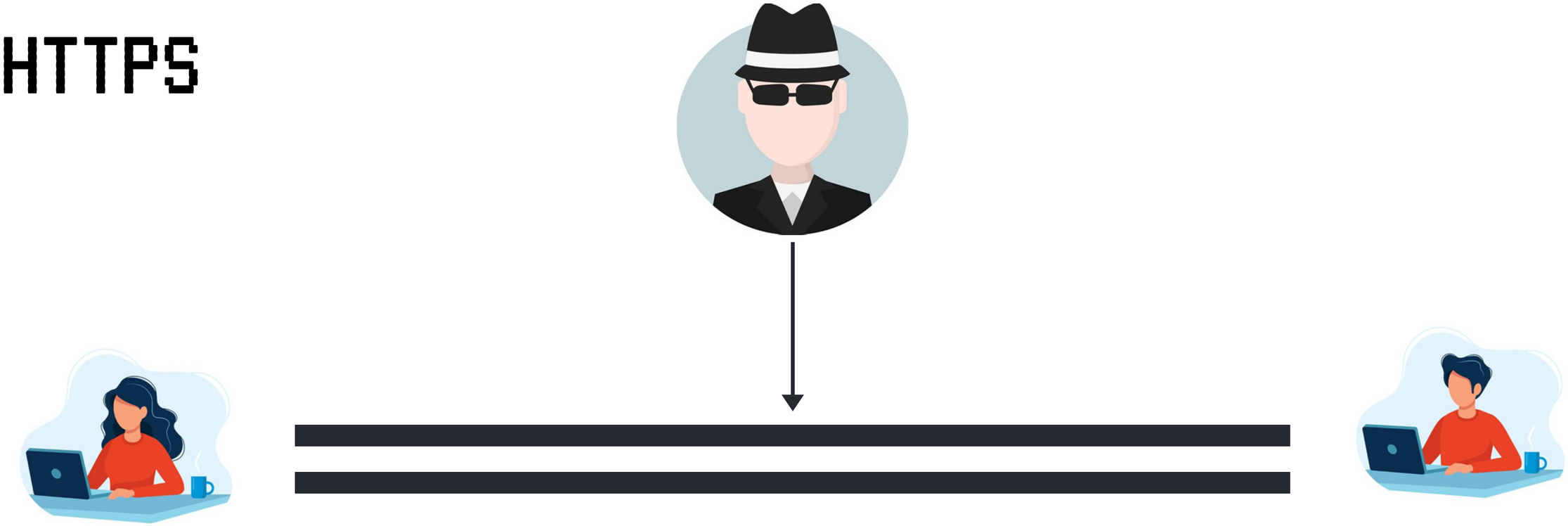
- HTTP/HTTPS: Hyper Text Transfer Protocol/Secure: adalah jalur atau protokol yang membuat kita bisa berkomunikasi dengan server penyedia layanan, baik website, email, chat, media sosial, dll

HTTP

Ketika kita menggunakan HTTP, maka kita seperti menggunakan jalur yang terbuka, dimana semua data/informasi digital kita bisa diketahui oleh pihak-pihak yang kita lewati. Data yang terbuka termasuk: Dari dan tujuan (dari komputer kita menuju website tertentu), Tanggal + jam dan metadata lainnya, laman yang kita kunjungi, login dan password, broswer fingerprints.

Apabila kita mengirimkan email, maka isi emailpun bisa diketahui.

HTTPS



Ketika kita menggunakan HTTPS, maka kita seperti menggunakan jalur yang tertutup. Protokol ini dienkripsi oleh penyedia layanan yang kita gunakan (email, website, chat, media sosial, dll). Data yang bisa diketahui oleh pihak-pihak lain hanyalah: Dari dan tujuan (dari komputer kita menuju website tertentu), tanggal + jam dan metadata lainnya. Namun penyedia layanan bisa melihat data dan informasi lengkap seperti jika kita menggunakan HTTP.

Circumvention

HTTPS + VPN

Encrypted

IP Address asli

VPN

Unencrypted

IP Address baru

Ketika kita meramban (browsing) dengan menggunakan VPN (Virtual Private Network), maka traffic internet kita akan melalui VPN provider dimana kita diberikan sebuah IP address baru untuk melalui semua jalur selanjutnya. Dengan menggunakan VPN ini maka orang yang memiliki kemampuan mengawasi traffic internet hanya bisa mengetahui bahwa kita mengakses VPN namun tidak bisa mengetahui tujuan kita atau data yang kita kirimkan setelah VPN. VPN ini menjadi alat yang efektif untuk menerabas pemblokiran dan menutup informasi kita. Namun penyedia layanan website bisa melihat data dan informasi lengkap kita seperti jika kita menggunakan HTTP. Karena VPN yang mengarahkan traffic kita 1 kali saja, maka identitas kita bisa ditelusuri ke belakang. Itu sebabnya memilih VPN yang bisa dipercaya akan membantu meningkatkan keamanan kita.

Secure Browsing Tips

- Pilihlah mesin peramban (browser) yang lebih menjaga privacy seperti Firefox
- Gunakan mesin pencari (search engine) yang lebih menjaga privacy seperty Duckduckgo
- Gunakan beberapa Ad-ons yang melindunggi keamanan dan privacy saat merambah (browsing seperti HTTPS Everywhere, Privacy Badger, dan Ghostery (Ad Blocker)
- Gunakan VPN

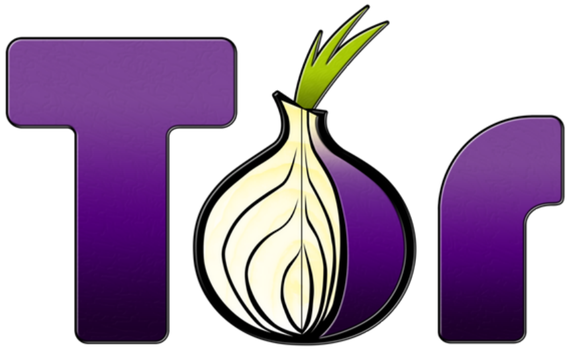

DuckDuckGo


HTTPS Everywhere


Privacy Badger


GHOSTERY

Anonymous Browsing



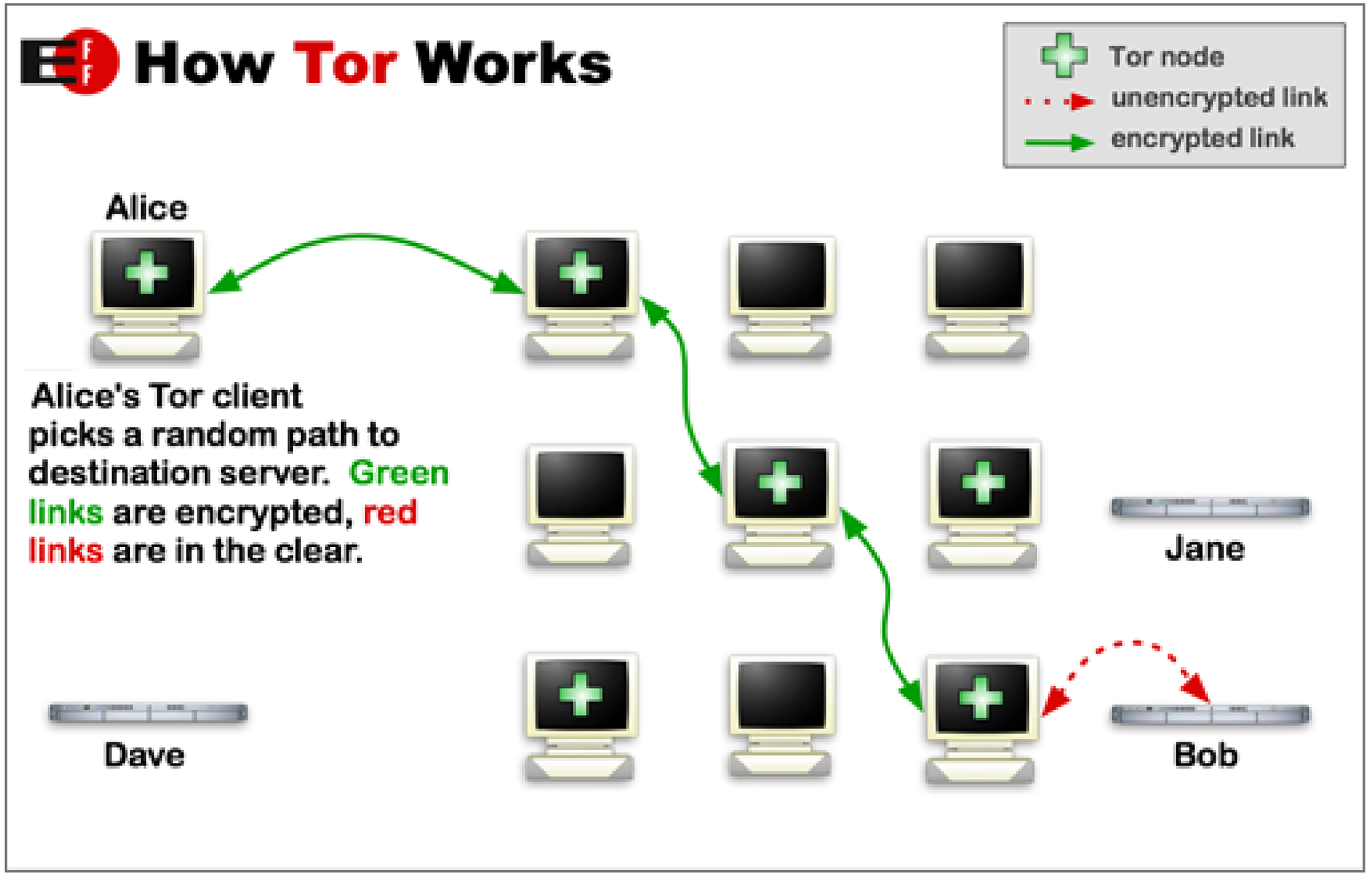
TOR Browser adalah sebuah peramban (browser) gratis dan bersumber terbuka (open source) yang memungkinkan kita untuk melakukan komunikasi secara anonim di internet.

Tor bekerja dengan cara mengarahkan lalu-lintas internet yang terenkripsi melalui 3 relay acak dalam jaringan Tor yang dijalankan oleh relawan di seluruh dunia.

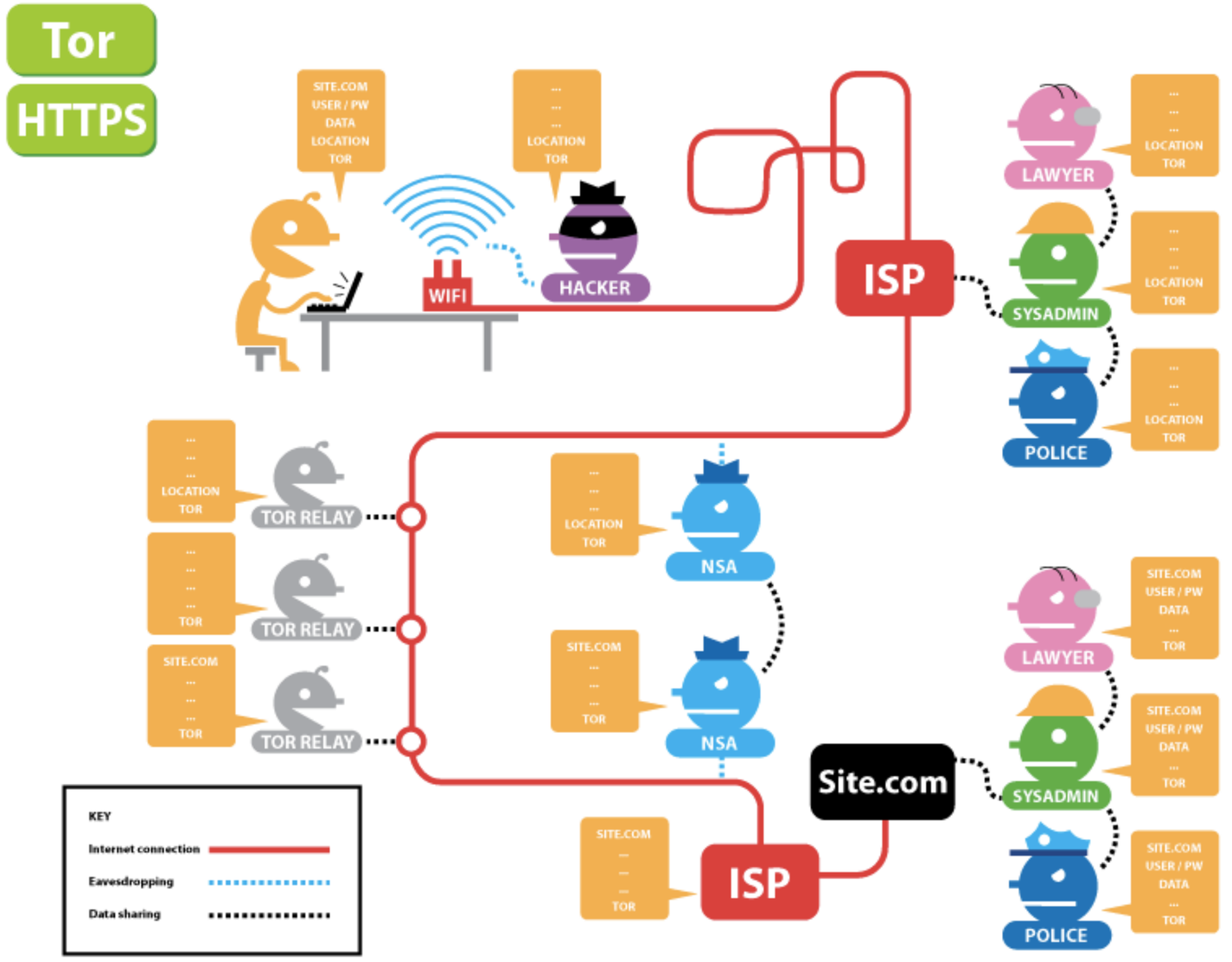
Mengapa Menggunakan Tor?

- Tor Browser melindungi kita dari pengawasan (surveillance) orang lain baik perusahan-perusahaan tech dan telco, negara, maupun individu-induvidu. Satu-satunya yang mereka ketahui adalah bahwa kita menggunakan Tor Network.
- Tor Browser mengisolasi website yang kita kunjungi sehingga trackers dan ads pihak ketiga (third party) tidak bisa mengintai dan mengamati aktivitas berselancar kita. Tor Browser secara otomatis membersihkan cookies ketika kita selesai berselancar dan tidak mencatat history perambanan kita.
- Mencegah Fingerprinting berbasikan informasi mesin peramban dan devicemu dengan cara membuat semua orang yang menggunakan Tor nampak sama (tidak mencatat informasi tersebut)
- Lalu lintas (traffic) internet kita diarahkan (relayed) dan dienkripsi sebanyak 3 kali selama melewati Tor Network. Tor Network terdiri dari ribuan server yang dijalankan oleh relawan di seluruh dunia yang biasa juga disebut sebagai Tor Relays.
- Tor Browser memungkinkan kita kita mengakses website yang diblokir.

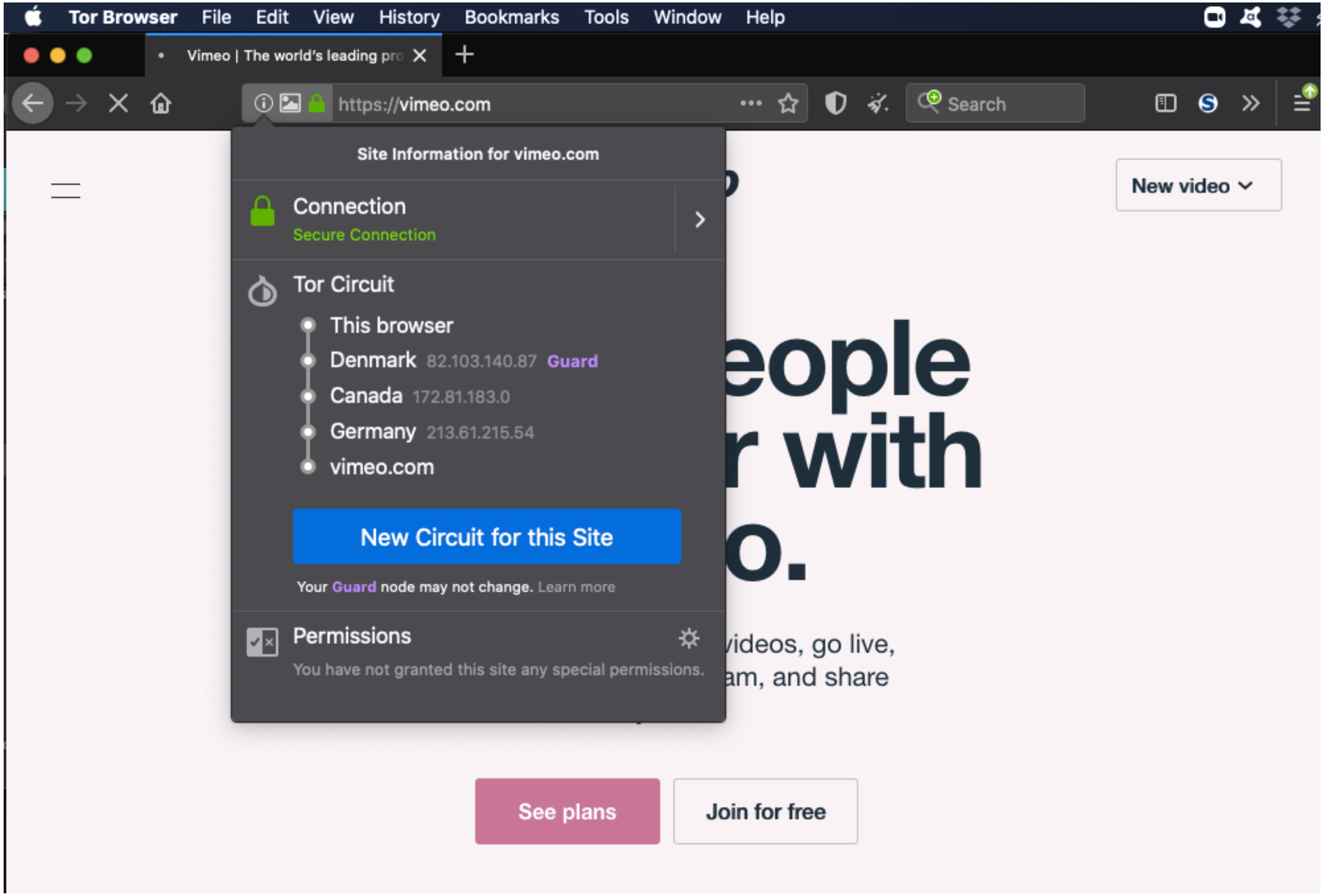
Bagaimana Tor Bekerja



Siapa yang bisa mengawasi kita saat menggunakan Tor dan HTTPS?



Contoh 3 Relay Dalam Circuit Tor



Glossaries

- Wifi: (Wireless Fidelity) : adalah perangkat teknologi yang menyediakan protokol untuk menghubungkan gawai (komputer, smartphone) ke jaringan komputer lokal (local network) untuk bertukar data dan untuk mengakses internet secara nirkabel..

- Router:a dalah perangkat teknologi jaringan komputer yand berfungsi untuk menghubungkan jaringan yang sama atau berbeda. Router juga berfungsi untuk mengirimkan paket data melalui jaringan internet.

- ISP (Internet Service Provider): adalah institusi/lembaga yang menyediakan layanan untuk mengakses, menggunakan atau berpartisipasi di Internet. ISP bisa berupa komersial, nirlaba, berbasis dan dimiliki komunitas, dimliki sektor privat (contoh korporasi)

- Server: adalah sistem atau perangkat komputer yang menyediakan fungsi atau layanan (service) tertentu untuk perangkat komputer lain (biasa disebut sebagai client) dalam jaringan komputer. Arsitektur ini biasa disebut client-server model yang cara kerjanya disebut dengan request-response model.

- Server Farm:: adalah kumpulan server dalam jumlah besar/banyak

Glossaries

- Routing Server: adalah server yang berfungsi untuk mencari dan mengarahkan jalur request – response antar server. Routing server terletak di Network Access Points.

- National Gateway: adalah perangkat komputer yang mengatur lalu lintas internet di dalam negeri dan dari dalam ke luar negeri (dan sebaliknya)

- IP address Internet Protocol Address): adalah identitas numerikal yang diperuntukkan/diberikan pada setiap gawai yang terhubung ke jaringan Internet. IP Address menjadi identitas online kita.

- HTTP (Hyper Text Transfer Protocol): adalah protokol yang membuat kita berkomunikasi dengan server dalam Wordl Wide Web

- HTTPS (Hyper Text Transfer Protocol Secure) adalah ekstensi dari HTTP yang membuat komunikasi kita lebih aman di internet. Komunikasi menggunakan HTTPS yang terenkripsi dengan menggunakan Transport Layer Security (TSL) atau yang dulu dikenal dengan Secure Sockets Layer.

Glossaries

- Circumvention: adalah bermacam metode atau cara untuk menerabas sensor atau pemblokiran di internet.

- VPN (Virtual Private Network): adalah perangkat komputer yang mengarahkan/mengubah IP address kita agar nampak dari lokasi yang berbeda. VPN juga untuk tunneling (menutup) data kita dengan sistem enkripsi.

- Browser Ad-ons: adalah program komputer yang menambahkan fitur pada browser

- Tor Relay: juga merujuk sebagai "routers" atau "nodes yang berfungsi untuk menerima lalu lintas di dalam jaringan Tor dan mengarahkannya ke tujuan.

- Node: (lihat Tor Relay)

- Encryption: adalah proses pengkodean informasi dengan menggunakan sistem chryptography. Proses ini mengubah informasi asli dalam bentuk plain text ke dalam bentuk cyphertext.

Glossaries

- Cookies (juga dikenal sebagai HTTP Cookies): adalah file program kecil yang terintegrasi ke dalam website dan terkirim dan kemudian tersimpan ke dalam komputer users (pengguna).. Cookies didisain sebagai mekanisme agar website-website tersebut bisa mengingat informasi yang diakses oleh penggunanya atau merekam aktivitas berselancar (contoh: mencatat/mengingat laman terakhir yang dikunjungi, logging in, klik tombol tertentu di tampilan website)

- Browsing history adalah pencatatan atau rekaman laman-laman yang kita kunjungi melalui browser.