LAPORAN KEAMANAN JARINGAN KOMPUTER

"Tor Browser"

Oleh:

NAMA	: Yoga Faturahman
NIM	: 09040581721006
Kelas	: TKJ4
Mata Kuliah	: Keamanan Jaringan Komputer

LABORATORIUM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

Pendahuluan Tor Browser

Tor Browser adalah versi Mozilla Firefox yang termutakhir dan dioptimalkan untuk privasi. Ia merupakan peramban gratis dengan perangkat lunak sumber terbuka yang memampukan anonimitas penembusan sensor daring. Tidak seperti peramban lainnya, Tor Browser:

- menyediakan anonimitas daring dengan menyembunyikan alamat IP pengguna
- menembus sensor daring dengan memampukan pengguna untuk mengakses situs web dan/atau halaman web yang diblokir.
- tidak memiliki fitur pelacakan daring baku
- tidak menghasilkan uang dari data pengguna
- didukung dan direkomendasikan oleh para pakar keamanan terkemuka di dunia

Jaringan Tor terdiri dari ribuan server yang dijalankan oleh relawan di seluruh dunia. Setiap kali ToR Browser membuat koneksi baru, ia memilih tiga **relay Tor** dan terhubung ke Internet melaluinya. Ia mengenkripsi setiap langkah perjalanan ini dengan cara tertentu sehingga relay sendiri tidak mengetahui seluruh lintasan yang dilaluinya ketika ia mengirimkan dan menerima data.

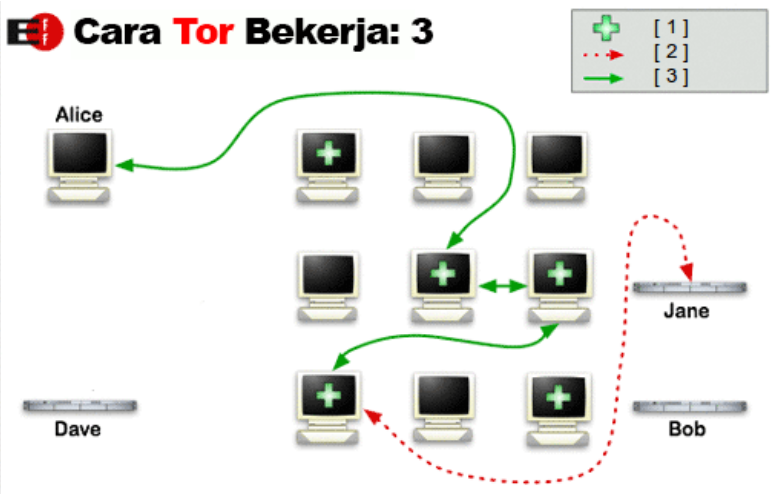
Ketika anda menggunakan Tor Browser, lalu lintas internet anda akan terlihat seolah berasal dari *alamat IP* yang berbeda, umumnya di negara yang berbeda. Alhasil, Tor Browser menyamarkan alamat IP anda dari situs web yang anda masuki sekaligus menyamarkan situs yang anda kunjungi dari pihak ketiga yang mungkin mencoba mengawasi lalu lintas anda. Ia juga memastikan bahwa satu Tor relay sendiri tidak dapat mengetahui *baik* lokasi anda di internet *maupun* situs yang anda kunjungi (walaupun sebagian dari mereka akan mengetahui salah satu di antara keduanya).

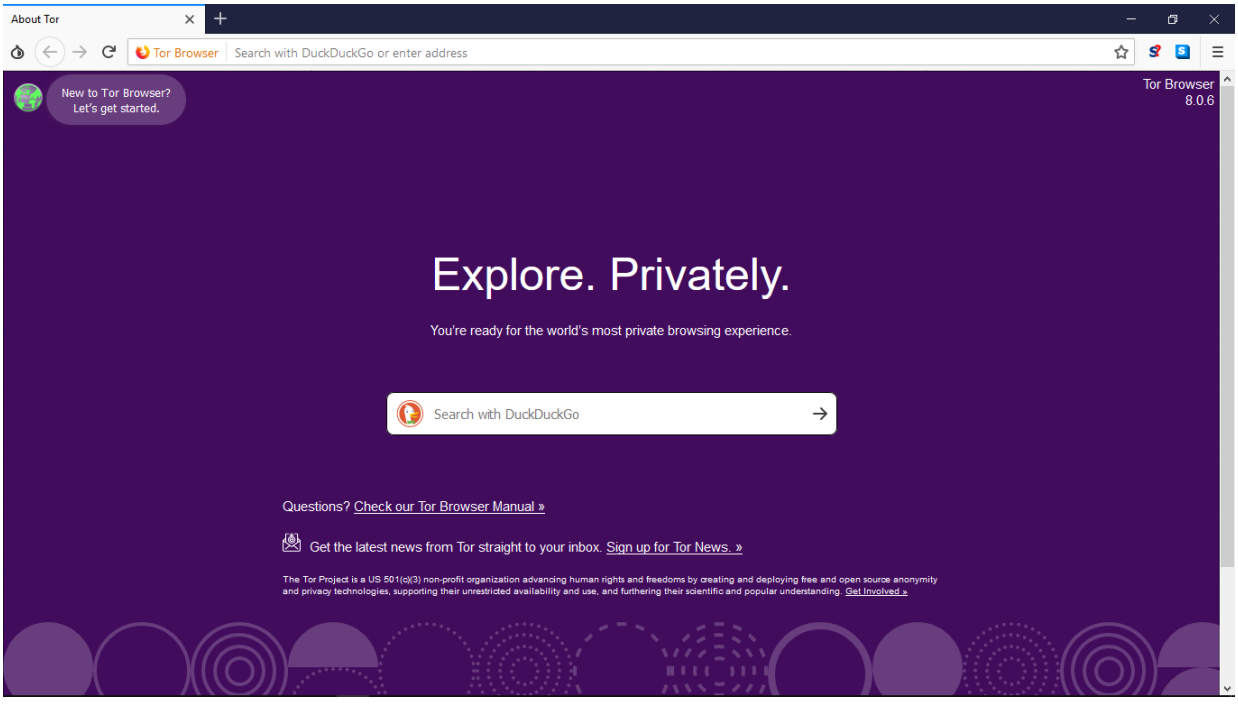
Tor juga mengambil langkah untuk mengenkripsi komunikasi yang masuk ke dalam dan yang melalui jaringannya. Namun, perlindungan ini tidak menjangkau sampai situs web yang dapat diakses melalui saluran tidak terenkripsi (yaitu situs web yang tidak mendukung HTTPS).

Karena Tor Browser menyembunyikan koneksi antara anda dengan situs web yang anda kunjungi, ia memampukan anda untuk menjelajah Web secara anonim dan menghindari pelacakan daring. Ia juga dapat melewati penyaringan daring, sehingga anda dapat mengakses konten dari (atau memuatkan konten ke) situs web yang, dalam keadaan lain, akan dibatasi.

bagaimana jaringan Tor bekerja ?

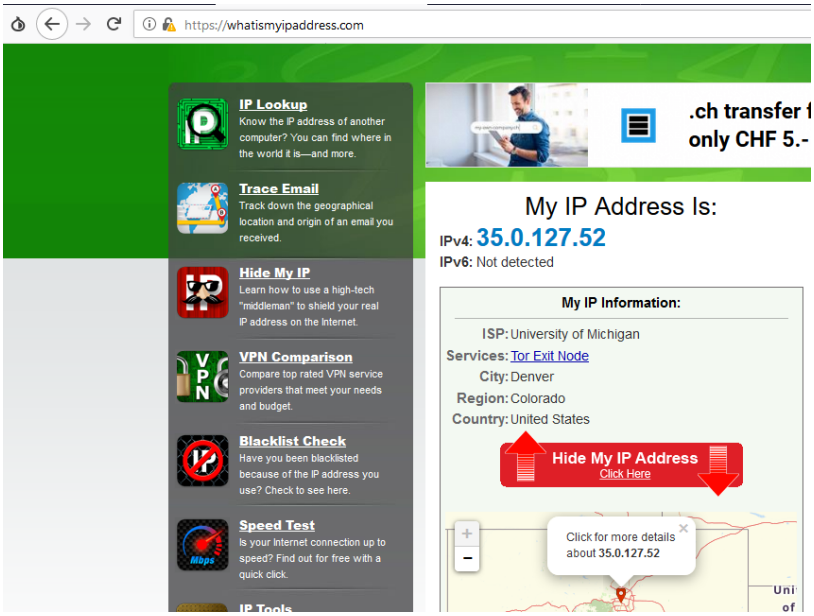

Cara Tor Bekerja: 2
[1]
[2]
[3]
Alice
Jane
Dave
Bob


Cara Tor Bekerja: 3
[1]
[2]
[3]
Alice
Jane
Dave
Bob

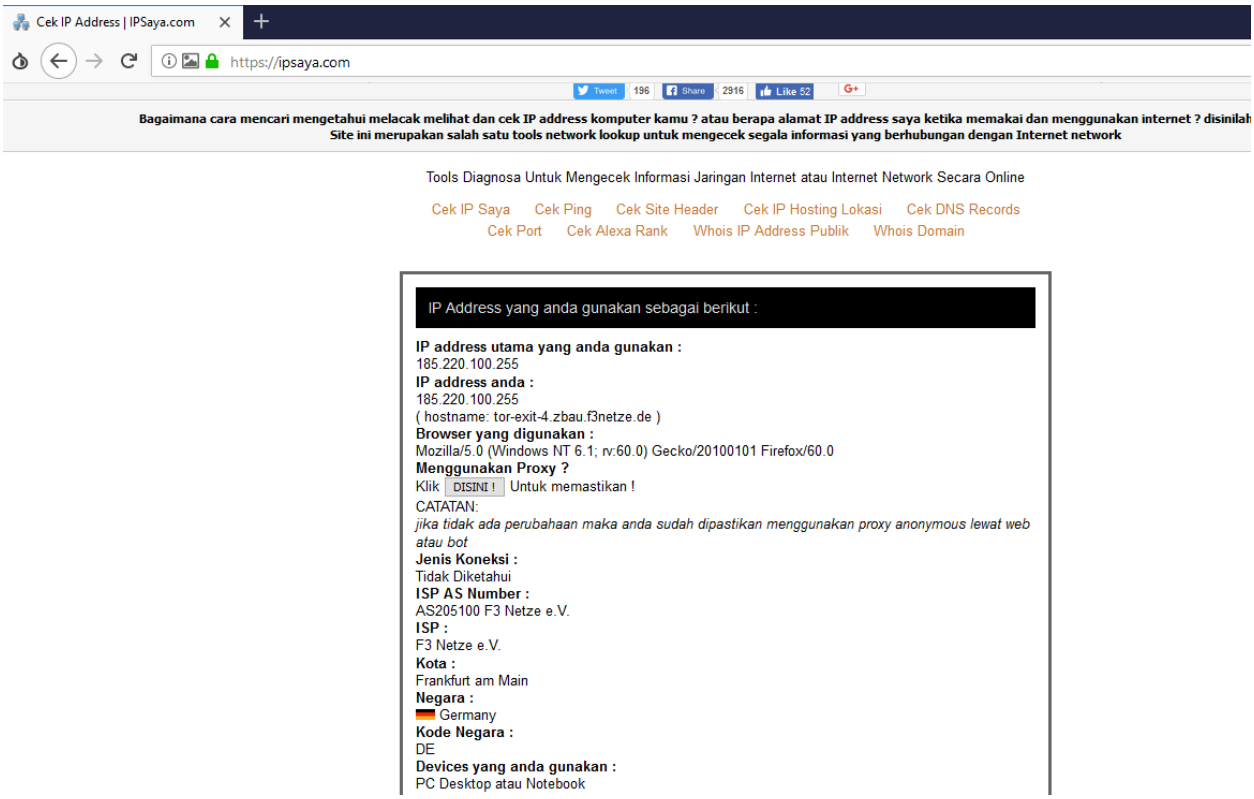

About Tor
Tor Browser
Search with DuckDuckGo or enter address
New to Tor Browser? Let's get started.
Tor Browser 8.0.6
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

Sedikit catatan, jika ada pesan Tor Failed to establish a Tor Network Connection maka perhatikan date & time pada PC.

Sesuai dengan cara kerja TOR browser, ketika kita cek ip kita melalui website “whatsmyip” maka yang timbul bukanlah alamat ip kita yang sebenarnya.



Ketika kita cek di website yang lain maka akan beda lagi, contohnya seperti berikut, cek menggunakan “ipsaya”



Ketika kita cek ip melalui cmd maka hasil yang kita dapat adalah seperti berikut:

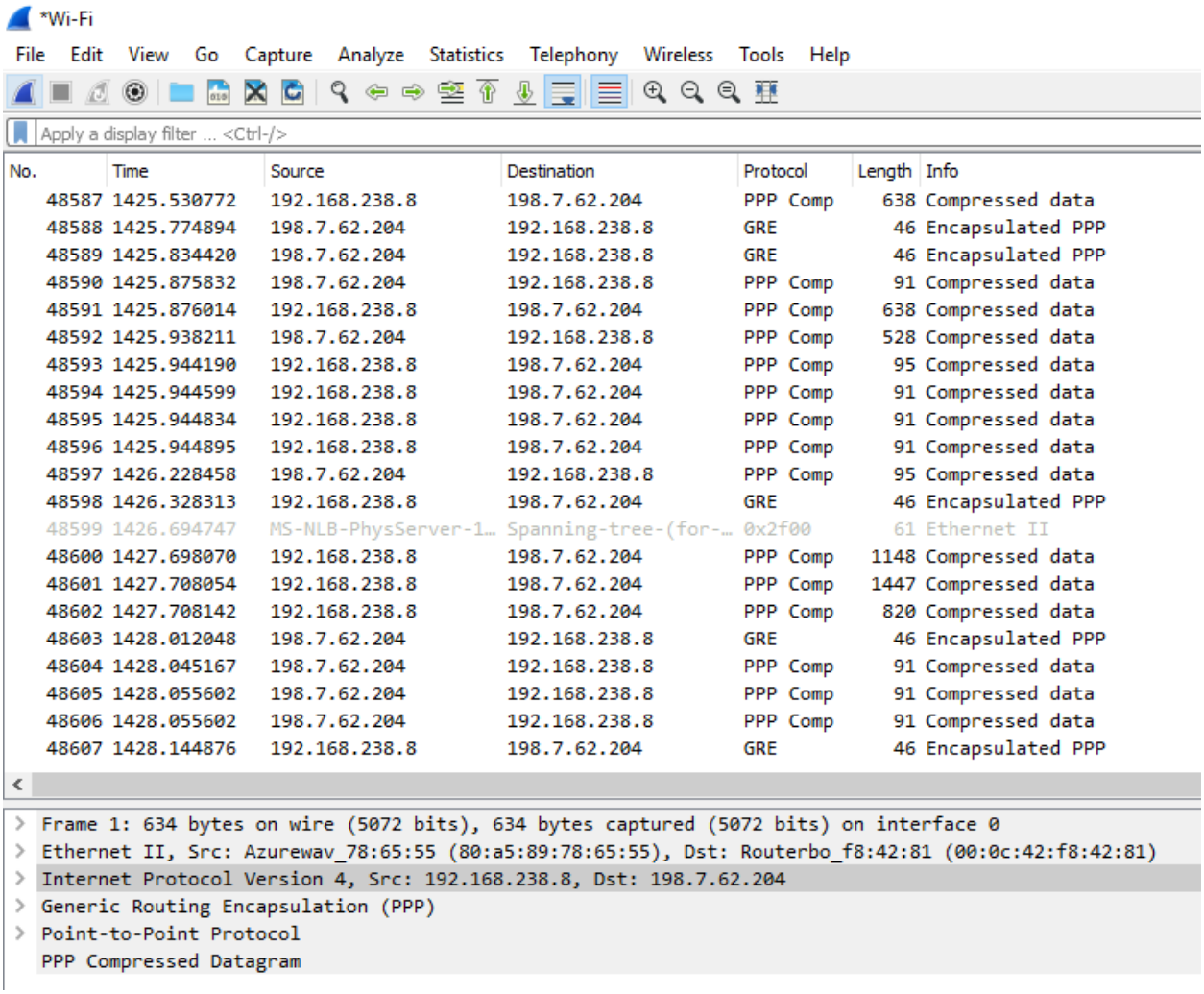
```
PPP adapter tis:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.36.186
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
```

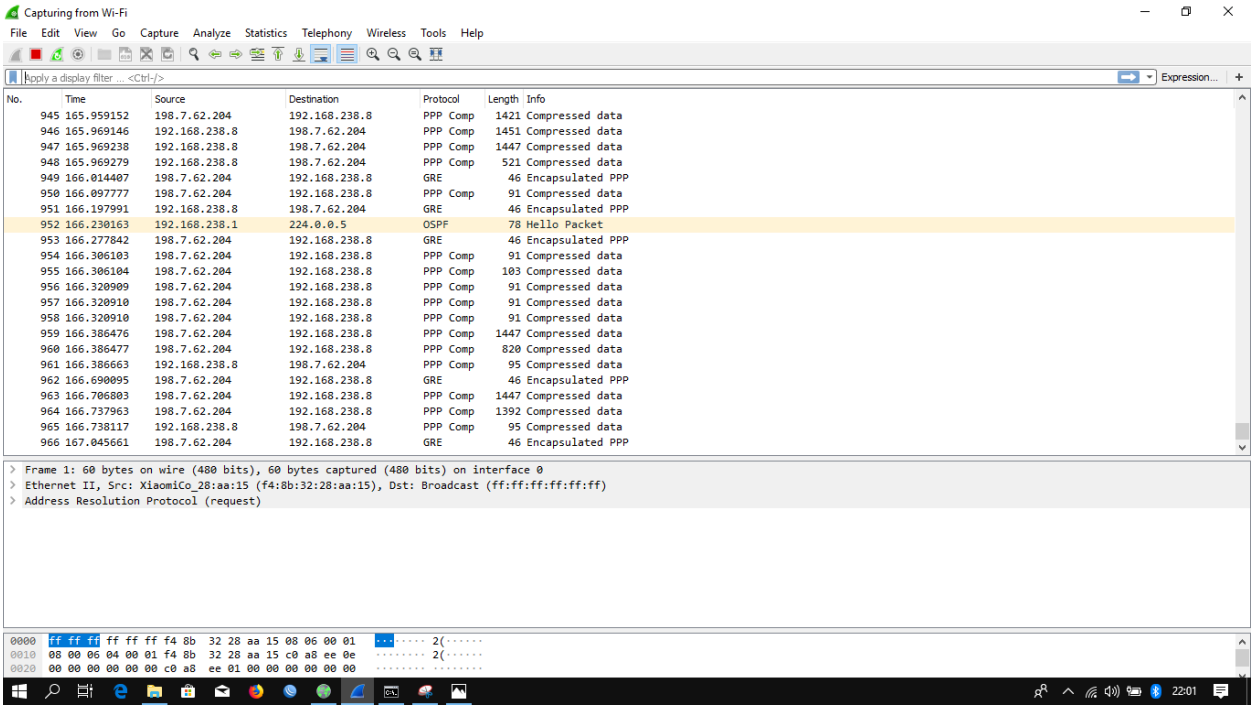
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::50df:7591:25d9:a0ae%8
   IPv4 Address. . . . . . . . . . . : 192.168.238.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.238.1
```

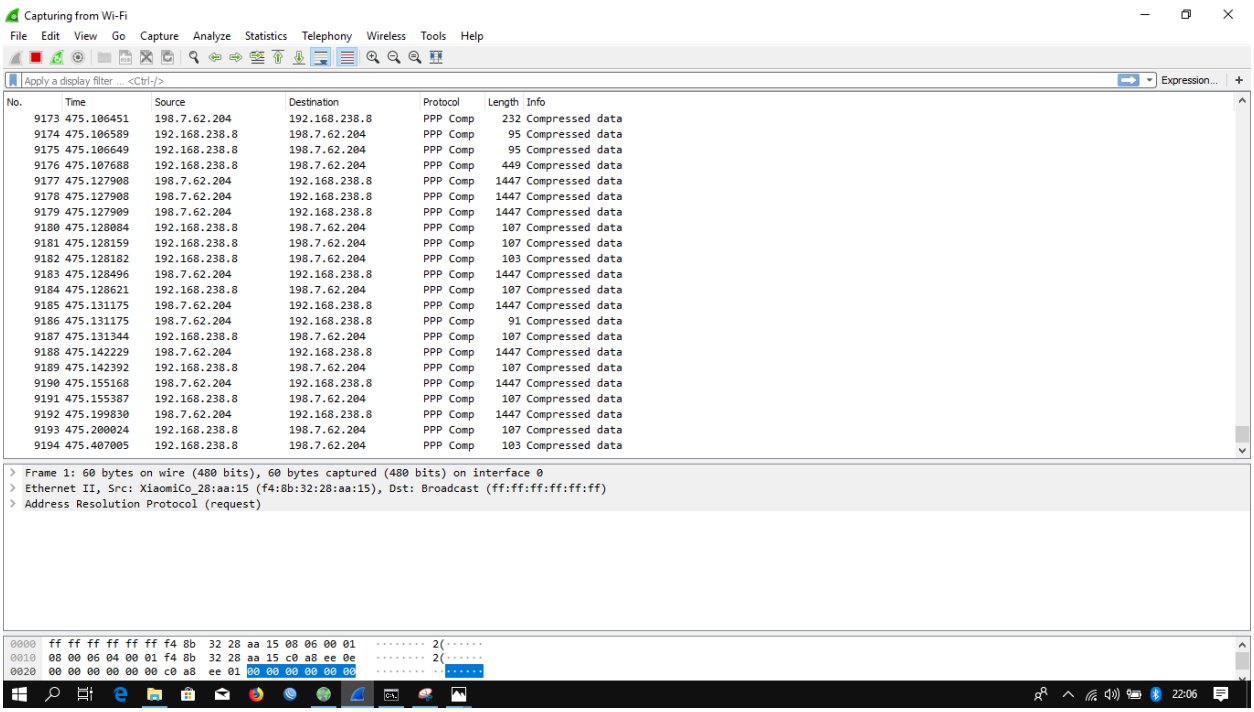
Jika dilihat melalui wireshark, kita ambil contoh membuka tiga website yang berbeda secara bergantian, website pertama adalah www.attahalilintarhabit.com



Website yang kedua adalah http://disdukcapil.palembang.go.id



Dan website yang terakhir adalah www.foxnews.com



Jika kita perhatikan, ketika kita membuka tiga website tersebut maka three way handshake yang terjadi adalah 192.168.238.8 sebagai Destination dan 198.7.62.204 sebagai source atau sebaliknya, 2 alamat ip itu tetap sama meskipun berbeda website yang dibuka. Protocol yang terdeteksi adalah PPP.