

LAPORAN KEAMANAN JARINGAN KOMPUTER

“Perbandingan Tor Browser dengan Browser biasa”



Oleh:

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

**LABORATORIUM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

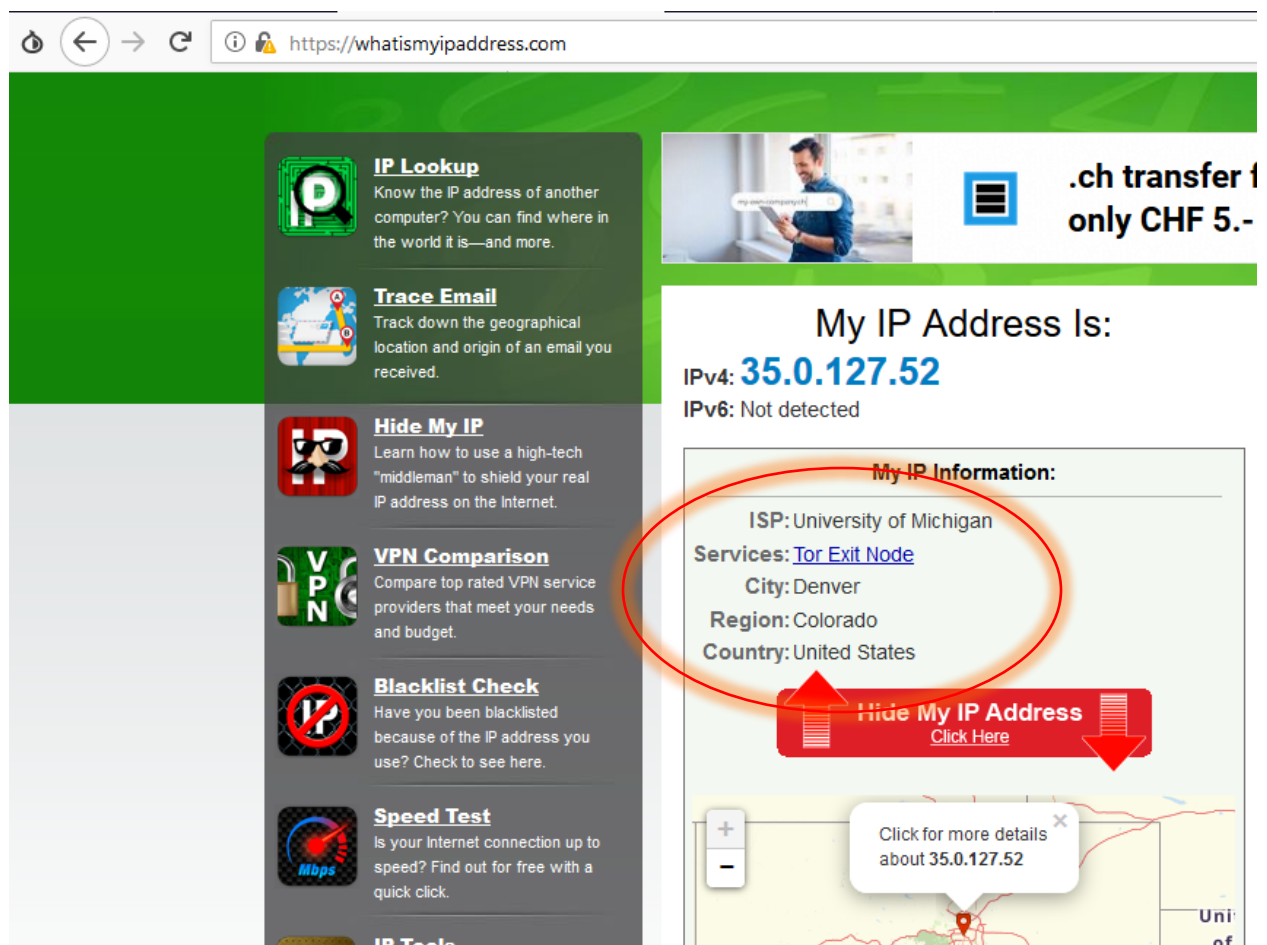
Pendahuluan Tor Browser

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

- menyediakan anonimitas daring dengan menyembunyikan alamat IP pengguna
- menembus sensor daring dengan memungkinkan 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.

Jika kita menggunakan browser biasa maka IP yang terdeteksi adalah IP yang tetap dan sesuai dengan keadaan yang sebenarnya atau paling tidak mendekati. Contohnya jika menggunakan TOR browser dan kita pergi ke website www.whatismyipaddress.com maka IP yang akan tertampil adalah



The screenshot shows a web browser window with the address bar displaying <https://www.whatismyipaddress.com>. The website has a green header and a sidebar with various tools like IP Lookup, Trace Email, Hide My IP, VPN Comparison, Blacklist Check, and Speed Test. The main content area displays the user's IP address information:

My IP Address Is:
IPv4: **35.0.127.52**
IPv6: Not detected

My IP Information:
ISP: University of Michigan
Services: [Tor Exit Node](#)
City: Denver
Region: Colorado
Country: United States

A red circle highlights the "My IP Information" section. Below it is a red button labeled "Hide My IP Address" with a "Click Here" link. At the bottom, there is a map showing the location of the IP address with a tooltip that says "Click for more details about 35.0.127.52".

Pada bagian “My IP Information” ISP,service,city, region, dan country tidak ada yang benar. Ketika tidak menggunakan TOR browser dan membuka website www.whatismyipaddress.com maka akan tertampil data yang benar atau paling tidak mendekati.

My IP Address Is:

IPv4: 36.76.198.50

IPv6: Not detected

My IP Information:

ISP: PT Telkom Indonesia

City: Bandar Lampung

Region: Lampung

Country: Indonesia

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

The screenshot shows a web browser window with the address bar displaying <https://ipsaya.com>. The page content includes a navigation menu with links like 'Cek IP Saya', 'Cek Ping', 'Cek Site Header', etc. The main content area displays the following information:

IP Address yang anda gunakan sebagai berikut :

IP address utama yang anda gunakan :
185.220.100.255

IP address anda :
185.220.100.255
(hostname: tor-exit-4.zbau.f3netze.de)

Browser yang digunakan :
Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0

Menggunakan Proxy ?
Klik Untuk memastikan !

CATATAN:
jika tidak ada perubahan maka anda sudah dipastikan menggunakan proxy anonymous lewat web atau bot

Jenis Koneksi :
Tidak Diketahui

ISP AS Number :
AS205100 F3 Netze e.V.

ISP :
F3 Netze e.V.

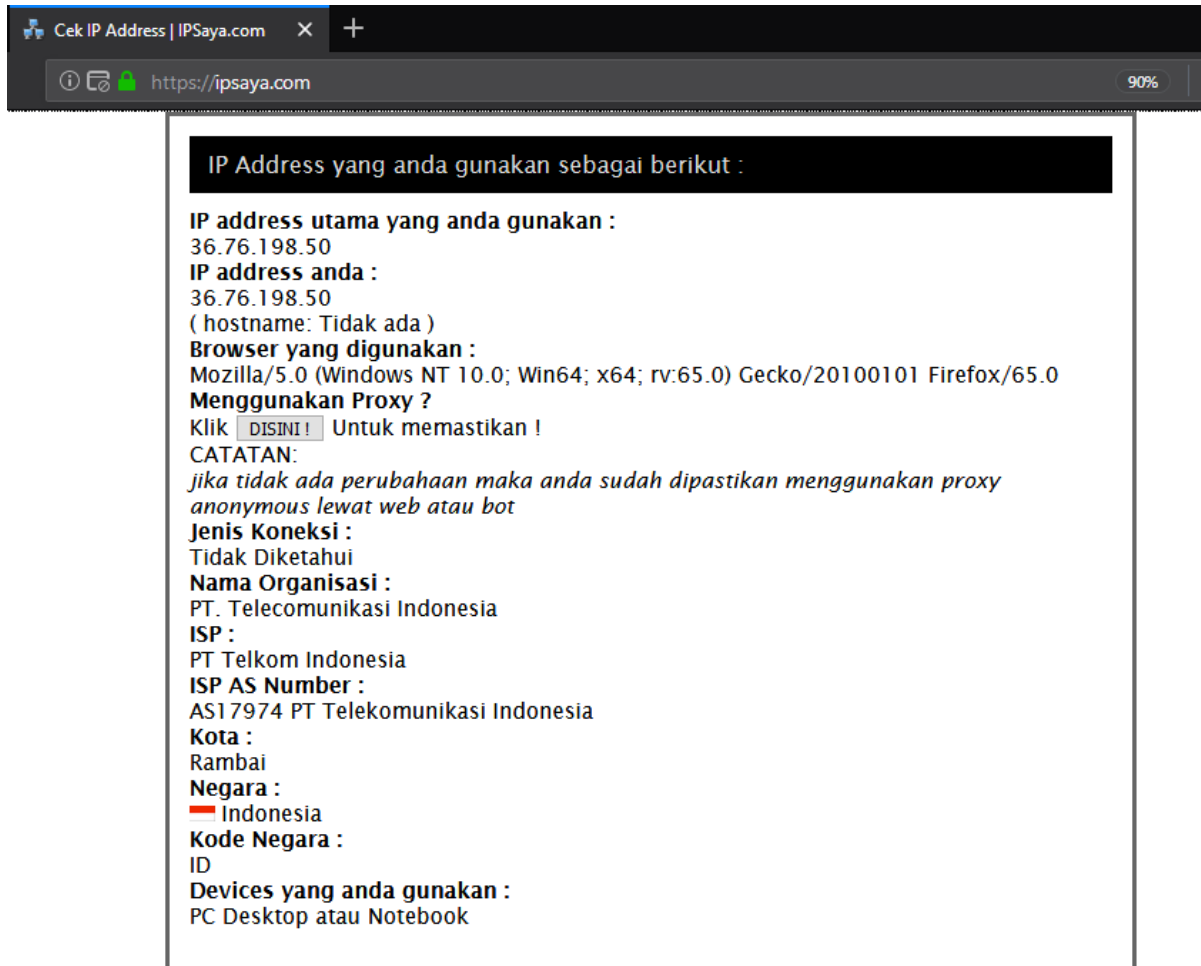
Kota :
Frankfurt am Main

Negara :
 Germany

Kode Negara :
DE

Devices yang anda gunakan :
PC Desktop atau Notebook

Ketika tidak menggunakan TOR browser dan membuka website [www. https://ipsaya.com/](https://ipsaya.com/) maka akan tertampil data yang benar atau paling tidak mendekati.



Ketika kita cek ip melalui cmd dan menggunakan TOR browser 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:

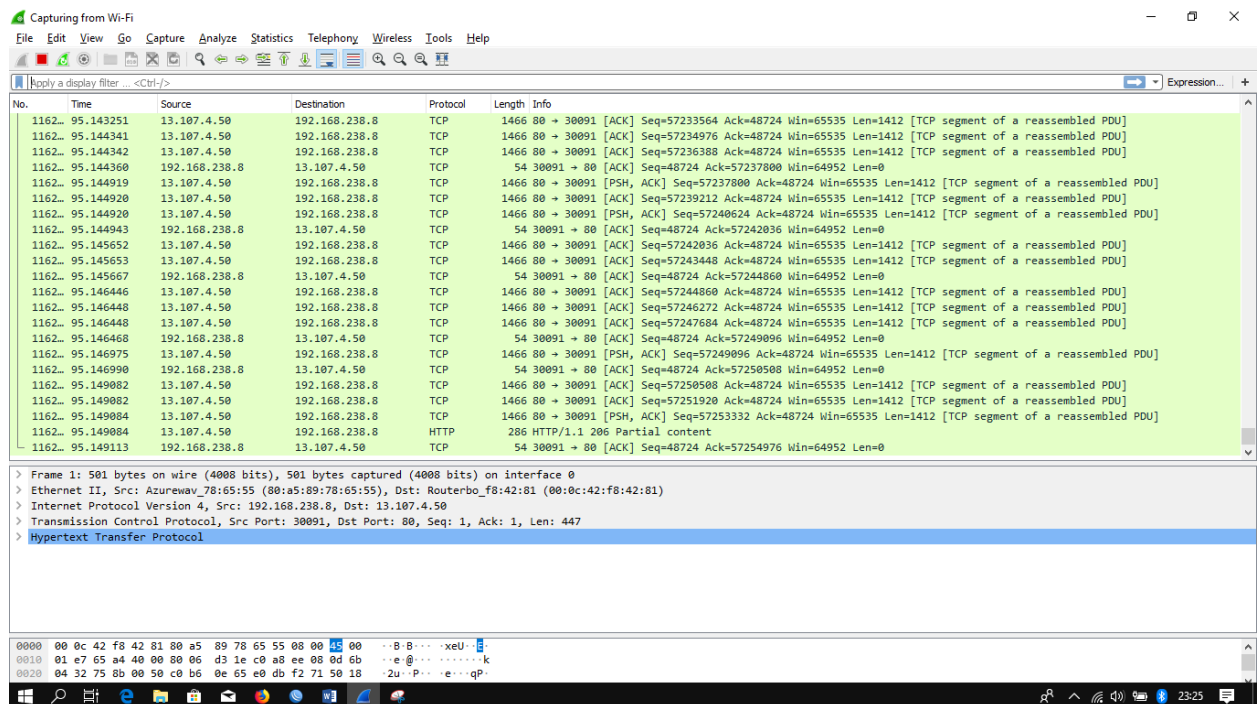
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::50df:7591:25d9:a0ae%8
IPv4 Address. . . . . : 192.168.238.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.238.1
```

Jika tidak menggunakan TOR browser maka akan tampil seperti berikut ini

```
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 kedua adalah www.foxnews.com

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
3292	305.072044	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.072114	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=55231 Win=66048 Len=0
3292	305.072736	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.072762	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=56643 Win=66048 Len=0
3292	305.073251	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075611	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075613	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075613	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075614	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075614	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075615	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075649	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=66527 Win=66048 Len=0
3292	305.075658	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data, Application Data [TCP segment of a reassembled PDU]
3292	305.075659	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.076607	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=69351 Win=66048 Len=0
3292	305.077454	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.077481	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=70763 Win=66048 Len=0
3292	305.079877	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079878	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079878	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079879	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079927	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=76411 Win=66048 Len=0

> Frame 1: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0

> Ethernet II, Src: Azurewav_78:65:55 (80:a5:09:78:65:55), Dst: Routerbo_f8:42:81 (00:0c:42:f8:42:81)

> Internet Protocol Version 4, Src: 192.168.238.8, Dst: 13.107.4.50

> Transmission Control Protocol, Src Port: 30091, Dst Port: 80, Seq: 1, Ack: 1, Len: 447

> Hypertext Transfer Protocol

0000 00 0c 42 f8 42 81 80 a5 89 78 65 55 00 00 45 00 ..8.B....xeU...E

0010 01 e7 65 a4 40 00 06 d3 1e c0 a8 ee 00 0d 6b ...e.@.....k

0020 04 32 75 8b 00 50 c0 b6 0e 65 e0 db f2 71 50 16 2u..P...e...qP

Wi-Fi: <live capture in progress> Packets: 329230 • Displayed: 329230 (100.0%) Profile: Default

Dan website yang terakhir adalah <http://disdukcapil.palembang.go.id>

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
3292	305.072044	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.072114	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=55231 Win=66048 Len=0
3292	305.072736	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.072762	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=56643 Win=66048 Len=0
3292	305.073251	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075611	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075613	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075613	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075614	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075614	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075615	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.075649	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=66527 Win=66048 Len=0
3292	305.075658	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data, Application Data [TCP segment of a reassembled PDU]
3292	305.075659	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.076607	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=69351 Win=66048 Len=0
3292	305.077454	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.077481	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=70763 Win=66048 Len=0
3292	305.079877	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079878	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079878	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079879	74.125.68.132	192.168.238.8	TLSv1.2	1466	Application Data [TCP segment of a reassembled PDU]
3292	305.079927	192.168.238.8	74.125.68.132	TCP	54	30706 → 443 [ACK] Seq=1105 Ack=76411 Win=66048 Len=0

> Frame 1: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0

> Ethernet II, Src: Azurewav_78:65:55 (80:a5:09:78:65:55), Dst: Routerbo_f8:42:81 (00:0c:42:f8:42:81)

> Internet Protocol Version 4, Src: 192.168.238.8, Dst: 13.107.4.50

> Transmission Control Protocol, Src Port: 30091, Dst Port: 80, Seq: 1, Ack: 1, Len: 447

> Hypertext Transfer Protocol

0000 00 0c 42 f8 42 81 80 a5 89 78 65 55 00 00 45 00 ..8.B....xeU...E

0010 01 e7 65 a4 40 00 06 d3 1e c0 a8 ee 00 0d 6b ...e.@.....k

0020 04 32 75 8b 00 50 c0 b6 0e 65 e0 db f2 71 50 16 2u..P...e...qP

Wi-Fi: <live capture in progress> Packets: 329230 • Displayed: 329230 (100.0%) Profile: Default

Jika kita perhatikan, ketika kita membuka tiga website tersebut maka three way handshake yang terjadi adalah 192.168.238.8 sebagai source dan berbagai macam alamat IP dari setiap website yang kita kunjungi sebagai destination, berbeda dengan menggunakan TOR Browser maka akan tertampil alamat IP 192.168.238.8 sebagai source atau dan satu alamat IP yang tetap meskipun kita mengunjungi website yang berbeda.

