

# 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 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.

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 memungkinkan 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.

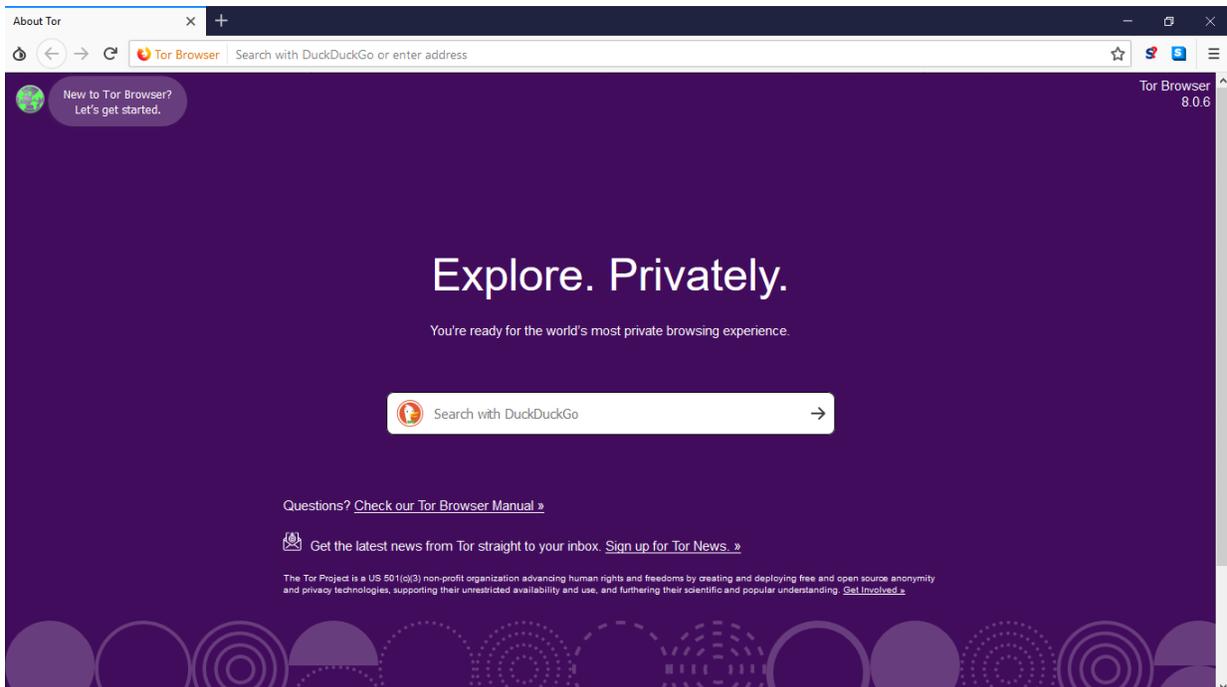
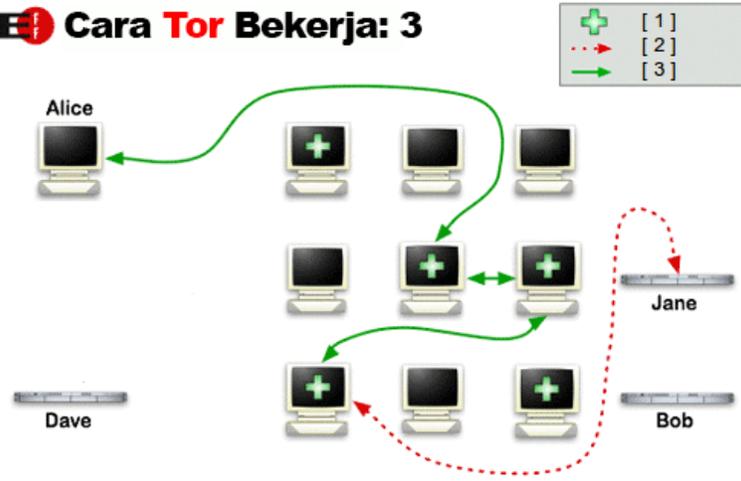
bagaimana jaringan Tor bekerja ?



## 1 Cara Tor Bekerja: 2



## 1 Cara Tor Bekerja: 3

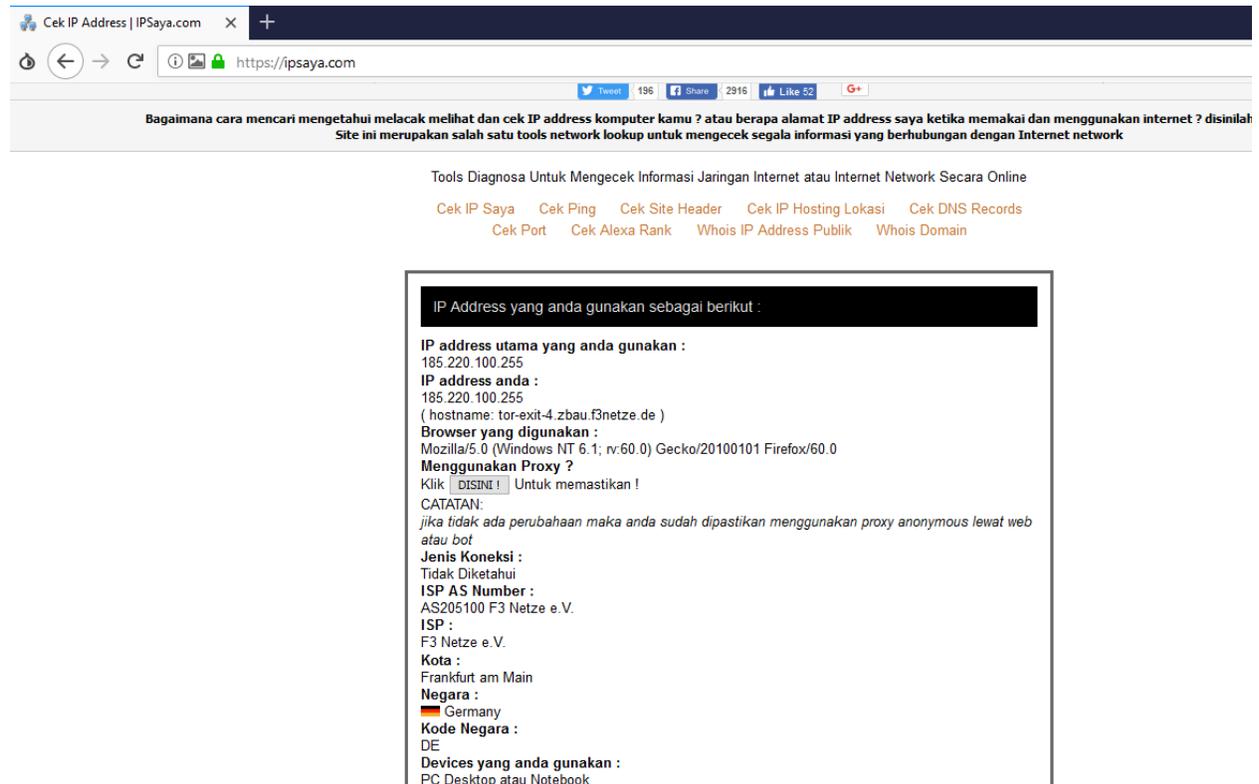


Sedikit catatan, jika ada pesan Tor Failed to establish a Tor Network Connection maka perhatikan date & time pada PC.

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.attahaliintarhabit.com](http://www.attahaliintarhabit.com)

The screenshot shows the Wireshark interface with the following components:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard network analysis icons for capture, display, and analysis.
- Filter Bar:** "Apply a display filter ... <Ctrl-/>"
- Packets List:** A table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** A detailed view of a selected packet (Frame 1) showing its structure: Ethernet II, Internet Protocol Version 4, Generic Routing Encapsulation (PPP), Point-to-Point Protocol, and PPP Compressed Datagram.

No.	Time	Source	Destination	Protocol	Length	Info
48587	1425.530772	192.168.238.8	198.7.62.204	PPP Comp	638	Compressed data
48588	1425.774894	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
48589	1425.834420	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
48590	1425.875832	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
48591	1425.876014	192.168.238.8	198.7.62.204	PPP Comp	638	Compressed data
48592	1425.938211	198.7.62.204	192.168.238.8	PPP Comp	528	Compressed data
48593	1425.944190	192.168.238.8	198.7.62.204	PPP Comp	95	Compressed data
48594	1425.944599	192.168.238.8	198.7.62.204	PPP Comp	91	Compressed data
48595	1425.944834	192.168.238.8	198.7.62.204	PPP Comp	91	Compressed data
48596	1425.944895	192.168.238.8	198.7.62.204	PPP Comp	91	Compressed data
48597	1426.228458	198.7.62.204	192.168.238.8	PPP Comp	95	Compressed data
48598	1426.328313	192.168.238.8	198.7.62.204	GRE	46	Encapsulated PPP
48599	1426.694747	MS-NLB-PhysServer-1...	Spanning-tree-(for-...	0x2f00	61	Ethernet II
48600	1427.698070	192.168.238.8	198.7.62.204	PPP Comp	1148	Compressed data
48601	1427.708054	192.168.238.8	198.7.62.204	PPP Comp	1447	Compressed data
48602	1427.708142	192.168.238.8	198.7.62.204	PPP Comp	820	Compressed data
48603	1428.012048	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
48604	1428.045167	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
48605	1428.055602	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
48606	1428.055602	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
48607	1428.144876	192.168.238.8	198.7.62.204	GRE	46	Encapsulated PPP

Packet Details for Frame 1:

- > Frame 1: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface 0
- > Ethernet II, Src: Azurewav\_78:65:55 (80:a5:89:78:65:55), Dst: Routerbo\_f8:42:81 (00:0c:42:f8:42:81)
- > Internet Protocol Version 4, Src: 192.168.238.8, Dst: 198.7.62.204
- > Generic Routing Encapsulation (PPP)
- > Point-to-Point Protocol
- PPP Compressed Datagram

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

The screenshot shows a Wireshark interface with a list of captured packets. The selected packet is an ARP request. The detailed view shows the Ethernet II header and the ARP request payload.

No.	Time	Source	Destination	Protocol	Length	Info
945	165.959152	198.7.62.204	192.168.238.8	PPP Comp	1421	Compressed data
946	165.969146	192.168.238.8	198.7.62.204	PPP Comp	1451	Compressed data
947	165.969238	192.168.238.8	198.7.62.204	PPP Comp	1447	Compressed data
948	165.969279	192.168.238.8	198.7.62.204	PPP Comp	521	Compressed data
949	166.014407	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
950	166.097777	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
951	166.197991	192.168.238.8	198.7.62.204	GRE	46	Encapsulated PPP
952	166.230163	192.168.238.1	224.0.0.5	OSPF	78	Hello Packet
953	166.277842	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
954	166.306103	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
955	166.306104	198.7.62.204	192.168.238.8	PPP Comp	103	Compressed data
956	166.320909	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
957	166.320910	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
958	166.320910	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
959	166.386476	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
960	166.386477	198.7.62.204	192.168.238.8	PPP Comp	820	Compressed data
961	166.386663	192.168.238.8	198.7.62.204	PPP Comp	95	Compressed data
962	166.690095	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP
963	166.706803	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
964	166.737963	198.7.62.204	192.168.238.8	PPP Comp	1392	Compressed data
965	166.738117	192.168.238.8	198.7.62.204	PPP Comp	95	Compressed data
966	167.045661	198.7.62.204	192.168.238.8	GRE	46	Encapsulated PPP

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
> Ethernet II, Src: XiaoMiCo\_28:aa:15 (f4:8b:32:28:aa:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff f4 8b 32 28 aa 15 08 06 00 01 ..... 2(.....
0010 08 00 06 04 00 01 f4 8b 32 28 aa 15 c0 a8 ee 0e ..... 2(.....
0020 00 00 00 00 00 c0 a8 ee 01 00 00 00 00 00 00 ..... .....
```

Dan website yang terakhir adalah [www.foxnews.com](http://www.foxnews.com)

The screenshot shows a Wireshark interface with a list of captured packets. The selected packet is an ARP request. The detailed view shows the Ethernet II header and the ARP request payload.

No.	Time	Source	Destination	Protocol	Length	Info
9173	475.106451	198.7.62.204	192.168.238.8	PPP Comp	232	Compressed data
9174	475.106589	192.168.238.8	198.7.62.204	PPP Comp	95	Compressed data
9175	475.106649	192.168.238.8	198.7.62.204	PPP Comp	95	Compressed data
9176	475.107688	192.168.238.8	198.7.62.204	PPP Comp	449	Compressed data
9177	475.127908	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9178	475.127908	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9179	475.127909	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9180	475.128084	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9181	475.128159	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9182	475.128182	192.168.238.8	198.7.62.204	PPP Comp	103	Compressed data
9183	475.128496	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9184	475.128621	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9185	475.131175	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9186	475.131175	198.7.62.204	192.168.238.8	PPP Comp	91	Compressed data
9187	475.131344	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9188	475.142229	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9189	475.142392	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9190	475.155168	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9191	475.155387	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9192	475.199830	198.7.62.204	192.168.238.8	PPP Comp	1447	Compressed data
9193	475.200024	192.168.238.8	198.7.62.204	PPP Comp	107	Compressed data
9194	475.407005	192.168.238.8	198.7.62.204	PPP Comp	103	Compressed data

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
> Ethernet II, Src: XiaoMiCo\_28:aa:15 (f4:8b:32:28:aa:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

```
0000 ff ff ff ff ff ff f4 8b 32 28 aa 15 08 06 00 01 ..... 2(.....
0010 08 00 06 04 00 01 f4 8b 32 28 aa 15 c0 a8 ee 0e ..... 2(.....
0020 00 00 00 00 00 c0 a8 ee 01 00 00 00 00 00 00 ..... .....
```

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.