

Tapping Menggunakan TOR



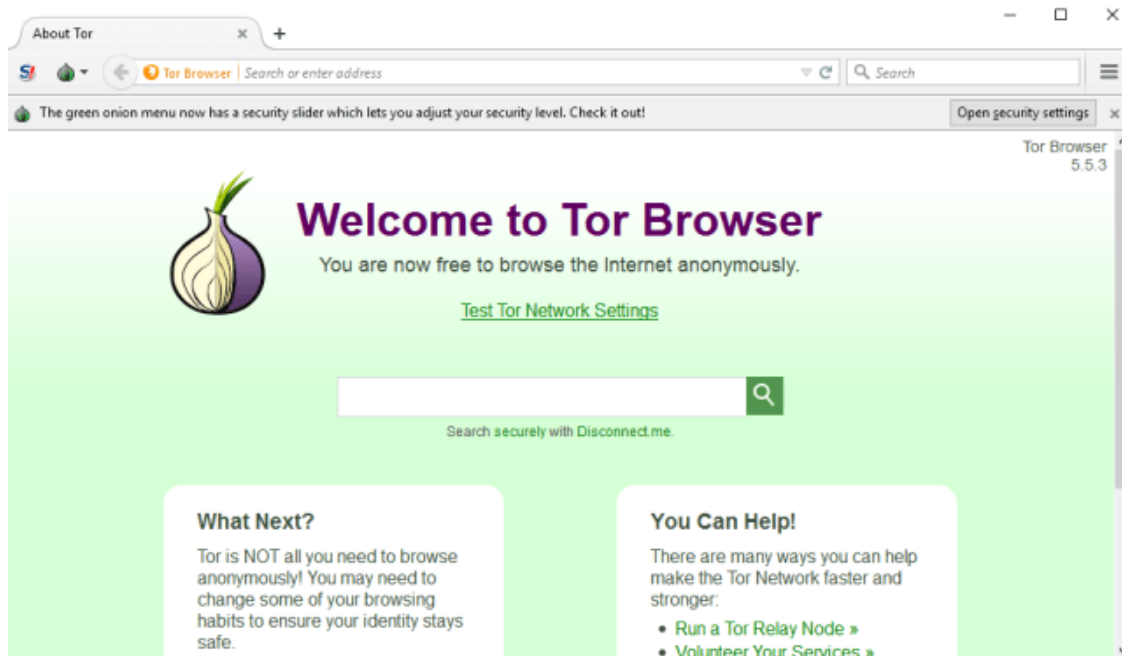
Oleh:

Nama : Zumardi Irfan
NIM : 09040581721014
Prodi : TKJ4
Mata Kuliah : Keamanan Jaringan Komputer
Dosen Pengampu : Deris Stiawan, M.T., Ph.D.

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

Apa itu Tor?

Dalam definisi yang paling sederhana, Tor merupakan perangkat lunak web browser yang menyembunyikan identitas anda ketika sedang online. Hal ini dapat dilakukan dalam beberapa cara yang berbeda. Pertama, menggunakan enkripsi untuk mengacak data yang sedang dikomunikasikan dalam jaringan. Yang kedua, rute data antara server diatur secara acak dalam jaringan Tor untuk menyembunyikan identitas online Anda, termasuk data terkait dengan alamat IP pribadi.



Website yang dituju yaitu :

1. liputan6.com (Dalam Negeri)
2. kotaprabumulih.go.id (Government)
3. <https://www.inetdaemon.com> (Luar Negeri)

Disini saya menggunakan VPN

-Pertama cek ip kita

```
Wireless LAN adapter WiFi 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5dee:b10:a84e:6421%7
IPv4 Address. . . . . : 192.168.43.209
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1
```

- Disini saya sudah membuka TOR Browser, dan mengecek ip dari laptop, didapatkan dari dua sumber semua ip yang terdeteksi berbeda-beda.

Your IP Address: 185.72.244.24

Find your current IP address and additional information including maps and location info.

Your Public IPv6 is: 2001:920:198c:83c:6368:537d:f8b4:5555

Your IPv4 is: 213.61.215.54

Location: Dusseldorf, NW DE ?

ISP: Colt Telecom

-lakukan browsing dengan web yang kita tuju, disini web yang saya pilih yaitu liputan6.com, terlihat saya mencoba ping melalui CMD, semuanya mereply dan terhubung dengan baik, dengan ip yang ditampilkan berbeda.



```

C:\Users\ZUMARDI>ping 51.68.180.4

Pinging 51.68.180.4 with 32 bytes of data:
Reply from 51.68.180.4: bytes=32 time=372ms TTL=44
Reply from 51.68.180.4: bytes=32 time=390ms TTL=44
Reply from 51.68.180.4: bytes=32 time=380ms TTL=44
Reply from 51.68.180.4: bytes=32 time=374ms TTL=44

Ping statistics for 51.68.180.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 372ms, Maximum = 390ms, Average = 379ms

C:\Users\ZUMARDI>ping www.liputan6.com

Pinging www.liputan6.com [13.251.186.151] with 32 bytes of data:
Reply from 13.251.186.151: bytes=32 time=748ms TTL=229
Reply from 13.251.186.151: bytes=32 time=740ms TTL=229
Reply from 13.251.186.151: bytes=32 time=749ms TTL=229
Reply from 13.251.186.151: bytes=32 time=738ms TTL=229

Ping statistics for 13.251.186.151:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 738ms, Maximum = 749ms, Average = 743ms

```

-ini merupakan tampilan tapping dari capturean wireshark, didapat 107bytes packet data atau 856 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, point-to-point protocol (PPP)

```

> Frame 27858: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
> Ethernet II, Src: HonHaiPr_03:36:f5 (94:39:e5:03:36:f5), Dst: 2e:4d:54:ad:75:d4 (2e:4d:54:ad:75:d4)
> Internet Protocol Version 4, Src: 192.168.43.209, Dst: 51.68.180.4
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
  PPP Compressed Datagram

```

11593	128.770978	192.168.43.209	51.68.180.4	PPP Co...	131 Compressed data
11594	128.779862	51.68.180.4	192.168.43.209	PPP Co...	1447 Compressed data
11595	128.780140	192.168.43.209	51.68.180.4	PPP Co...	131 Compressed data
11596	128.839998	51.68.180.4	192.168.43.209	PPP Co...	1451 Compressed data
11597	128.840213	192.168.43.209	51.68.180.4	PPP Co...	131 Compressed data
11598	128.840454	51.68.180.4	192.168.43.209	PPP Co...	1451 Compressed data
11599	128.840456	51.68.180.4	192.168.43.209	PPP Co...	91 Compressed data
11600	128.840627	192.168.43.209	51.68.180.4	PPP Co...	131 Compressed data
11601	128.859346	51.68.180.4	192.168.43.209	PPP Co...	1451 Compressed data
11602	128.859501	192.168.43.209	51.68.180.4	PPP Co...	131 Compressed data

-selanjutnya website pemerintahan, disini saya pilih kotaprabumulih.go.id (Government),



-Disini saya melakukan ping ke website kotaprabumulih.go.id (Government, didapatkan pingan ke website berhasil. Dengan ip yang didapat 103.15.226.60

```
C:\Users\ZUMARDI>ping kotaprabumulih.go.id

Pinging kotaprabumulih.go.id [103.15.226.60] with 32 bytes of data:
Reply from 103.15.226.60: bytes=32 time=693ms TTL=51
Reply from 103.15.226.60: bytes=32 time=639ms TTL=51
Reply from 103.15.226.60: bytes=32 time=667ms TTL=51
Reply from 103.15.226.60: bytes=32 time=710ms TTL=51

Ping statistics for 103.15.226.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 639ms, Maximum = 710ms, Average = 677ms
```

- ini merupakan tampilan tapping dari capturean wireshark, didapat 1447bytes packet data atau 11576 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, point-to-point protocol (PPP), coba kita perhatikan IP yang destination, kita mendapatkan IP yang sama seperti liputan 6.com

```
> Frame 120: 1447 bytes on wire (11576 bits), 1447 bytes captured (11576 bits) on interface 0
> Ethernet II, Src: 2e:4d:54:ad:75:d4 (2e:4d:54:ad:75:d4), Dst: HonHaiPr_03:36:f5 (94:39:e5:03:36:f5)
> Internet Protocol Version 4, Src: 51.68.180.4, Dst: 192.168.43.209
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
  PPP Compressed Datagram
```

No.	Time	Source	Destination	Protocol	Length	Info
115	25.471343	51.68.180.4	192.168.43.209	PPP Co...	1447	Compressed data
116	25.471663	192.168.43.209	51.68.180.4	PPP Co...	95	Compressed data
117	25.517300	51.68.180.4	192.168.43.209	PPP Co...	1447	Compressed data
118	25.517754	192.168.43.209	51.68.180.4	PPP Co...	95	Compressed data
119	25.573190	51.68.180.4	192.168.43.209	PPP Co...	193	Compressed data
120	25.582320	51.68.180.4	192.168.43.209	PPP Co...	1447	Compressed data
121	25.582849	192.168.43.209	51.68.180.4	PPP Co...	638	Compressed data
122	25.890364	51.68.180.4	192.168.43.209	PPP Co...	107	Compressed data
123	25.896927	51.68.180.4	192.168.43.209	GRE	46	Encapsulated PPP
124	25.896928	51.68.180.4	192.168.43.209	GRE	46	Encapsulated PPP

-dan yang terakhir yaitu <https://www.inetdaemon.com> (Luar Negeri),

<https://www.inetdaemon.com/technology/autonomous-system-number-tutorial-updated/>

INETDAEMON.COM
Training the Next Generation of IT Engineers

FREE ONLINE IT TUTORIALS | BLOG | ABOUT | DONATIONS

< [DIY VMWare Whitebox](#) [Member signup disabled \(temporarily\)](#) >

AUTONOMOUS SYSTEM NUMBER TUTORIAL UPDATED

Published February 3, 2014 | By InetDaemon

In 1999 I wrote a series of [Border Gateway Protocol tutorials](#) including a tutorial on [autonomous system](#) numbers. Since then AS numbers have been changed from 16-bit to 32-bit numbers to avoid running out of identifiers for [BGP](#) sessions. I have updated the [BGP AS numbers tutorial](#) with a table that outlines what each range of autonomous system numbers are used for.

SHARE:

[Tweet](#) [Share](#) [G+](#) [Save](#) [Print](#)

LIKE THIS:

[★ Like](#)

Be the first to like this.

- Disini saya melakukan ping ke website <https://www.inetdaemon.com>, didapatkan pingan ke website berhasil. Dengan ip yang didapat 66.147.244.107.

```
C:\Users\ZUMARDI>ping www.inetdaemon.com

Pinging www.inetdaemon.com [66.147.244.107] with 32 bytes of data:
Reply from 66.147.244.107: bytes=32 time=558ms TTL=40
Reply from 66.147.244.107: bytes=32 time=521ms TTL=40
Reply from 66.147.244.107: bytes=32 time=529ms TTL=40
Reply from 66.147.244.107: bytes=32 time=525ms TTL=40

Ping statistics for 66.147.244.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 521ms, Maximum = 558ms, Average = 533ms
```

- ini merupakan tampilan tapping dari capturean wireshark, didapat 556bytes packet data atau 4448 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, point-to-point protocol (PPP), coba kita perhatikan IP yang destination, kita mendapatkan IP yang sama seperti liputan 6.com dan www.inetdaemon.com. Jadi ketika kita tapping menggunakan TOR browser akan didapatkan IP yang akan selalu sama untuk destination walaupun web yang diakses berbeda.

```
> Frame 21: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
> Ethernet II, Src: HonHaiPr_03:36:f5 (94:39:e5:03:36:f5), Dst: 2e:4d:54:ad:75:d4 (2e:4d:54:ad:75:d4)
> Internet Protocol Version 4, Src: 192.168.43.209, Dst: 51.68.180.4
> Generic Routing Encapsulation (PPP)
> Point-to-Point Protocol
  PPP Compressed Datagram
```

16	2.260319	192.168.43.209	51.68.180.4	PPP Co...	1447 Compressed data
17	2.260434	192.168.43.209	51.68.180.4	PPP Co...	1447 Compressed data
18	2.260580	192.168.43.209	51.68.180.4	PPP Co...	100 Compressed data
19	2.260722	192.168.43.209	51.68.180.4	PPP Co...	1447 Compressed data
20	2.260874	192.168.43.209	51.68.180.4	PPP Co...	1447 Compressed data
21	2.261023	192.168.43.209	51.68.180.4	PPP Co...	556 Compressed data
22	2.547944	51.68.180.4	192.168.43.209	PPP Co...	107 Compressed data
23	2.647647	192.168.43.209	51.68.180.4	GRE	46 Encapsulated PPP
24	2.661028	51.68.180.4	192.168.43.209	PPP Co...	91 Compressed data