Perbandingan Trafic Tapping Menggunakan TOR Dan Tools Lain

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

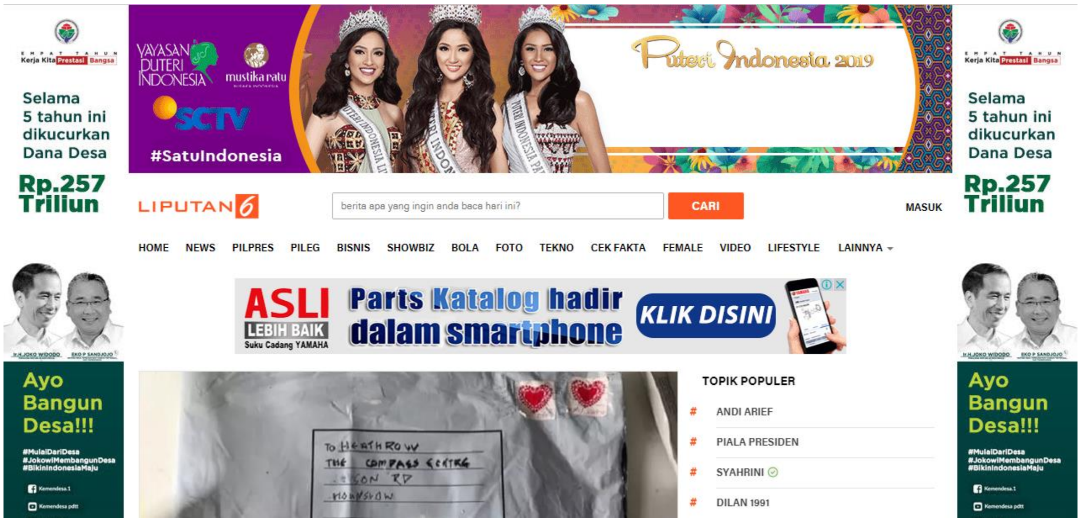
2019

Website yang dituju yaitu :

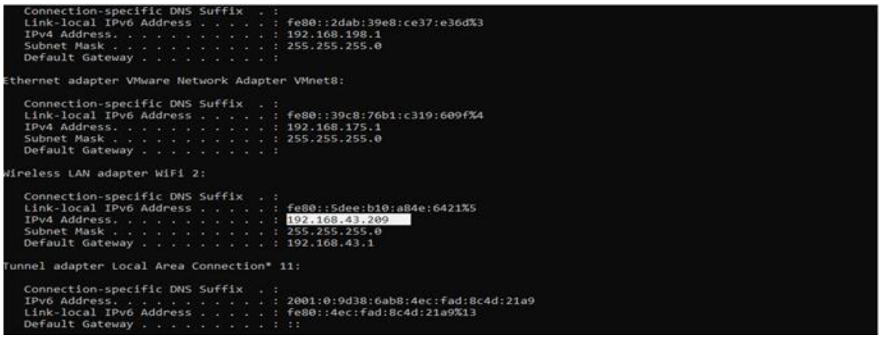
1. liputan6.com (Dalam Negeri)
2. kotaprabumulih.go.id (Government)
3. https://www.inetdaemon.com (Luar Negeri)

1. liputan6.com (Dalam Negeri)

   Pada gambar dibawah saya tidak menggunakan TOR browser dan TIDAK menggunakan VPN

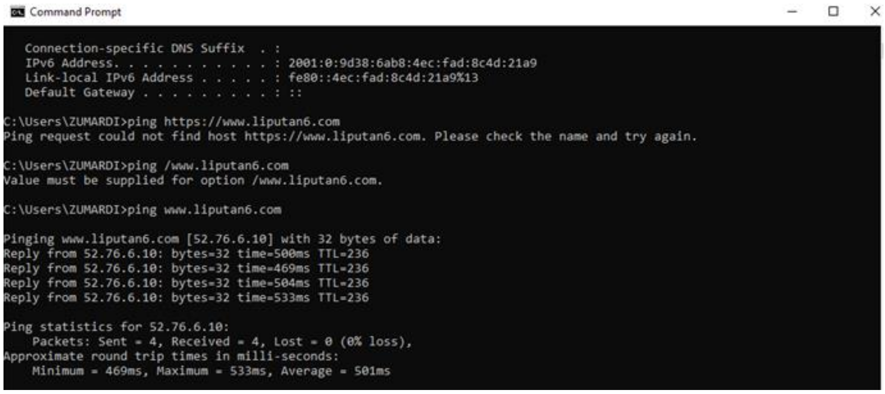


-ini merupakan perintah ipconfig untuk melihat ip kita,



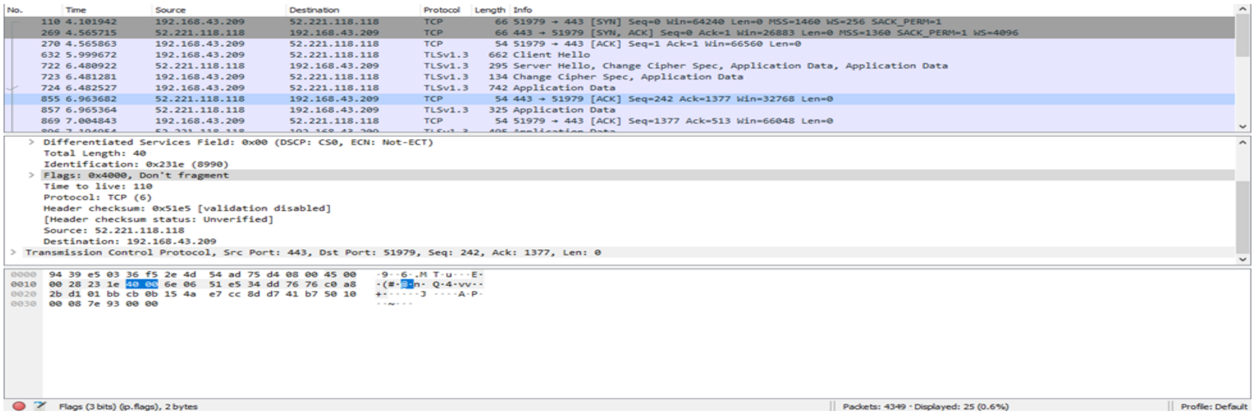
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2dab:39e8:ce37:e36d%3
   IPv4 Address. . . . . . . . . . . : 192.168.198.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::39c8:76b1:c319:609f%4
   IPv4 Address. . . . . . . . . . . : 192.168.175.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter WiFi 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5dee:b10:a84e:6421%5
   IPv4 Address. . . . . . . . . . . : 192.168.43.209
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:4ec:fad:8c4d:21a9
   Link-local IPv6 Address . . . . . : fe80::4ec:fad:8c4d:21a9%13
   Default Gateway . . . . . . . . . : ::
```

-Disini lakukan ping ke liputan6.com dengan ip yang didapat 52.76.6.10



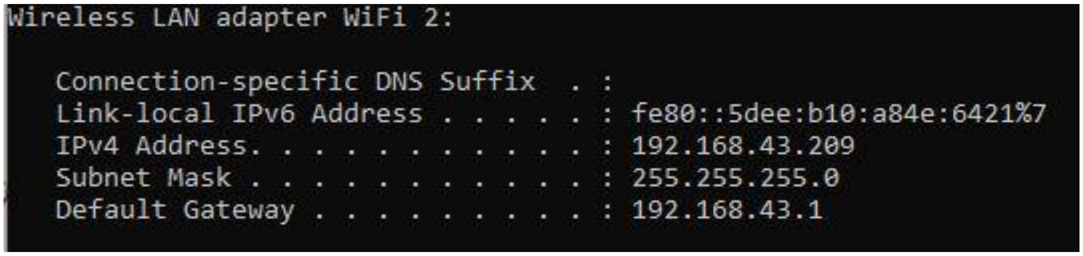
```
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:4ec:fad:8c4d:21a9
   Link-local IPv6 Address . . . . . : fe80::4ec:fad:8c4d:21a9%13
   Default Gateway . . . . . . . . . : ::

C:\Users\ZUMARDI>ping https://www.liputan6.com
Ping request could not find host https://www.liputan6.com. Please check the name and try again.

C:\Users\ZUMARDI>ping /www.liputan6.com
Value must be supplied for option /www.liputan6.com.

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

Pinging www.liputan6.com [52.76.6.10] with 32 bytes of data:
Reply from 52.76.6.10: bytes=32 time=500ms TTL=236
Reply from 52.76.6.10: bytes=32 time=469ms TTL=236
Reply from 52.76.6.10: bytes=32 time=504ms TTL=236
Reply from 52.76.6.10: bytes=32 time=533ms TTL=236

Ping statistics for 52.76.6.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 469ms, Maximum = 533ms, Average = 501ms
```

-ini merupakan tampilan tapping dari capturean wireshark, didapat 54bytes packet data, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, Transmission Control Protocol(TCP)



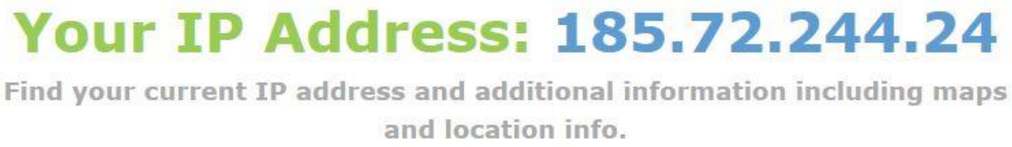
```
No.   Time       Source           Destination      Protocol  Length Info
  110 4.101942   192.168.43.209   52.221.118.118   TCP          66 51979 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  269 4.565715   52.221.118.118   192.168.43.209   TCP          66 443 → 51979 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1360 SACK_PERM=1 WS=4096
  270 4.565863   192.168.43.209   52.221.118.118   TCP          54 51979 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
  632 5.999672   192.168.43.209   52.221.118.118   TLSv1.3     662 Client Hello
  722 6.480922   52.221.118.118   192.168.43.209   TLSv1.3     295 Server Hello, Change Cipher Spec, Application Data, Application Data
  723 6.481281   192.168.43.209   52.221.118.118   TLSv1.3     134 Change Cipher Spec, Application Data
  724 6.482527   192.168.43.209   52.221.118.118   TLSv1.3     742 Application Data
  855 6.963682   52.221.118.118   192.168.43.209   TCP          54 443 → 51979 [ACK] Seq=242 Ack=1377 Win=32768 Len=0
  857 6.965364   52.221.118.118   192.168.43.209   TLSv1.3     325 Application Data
  869 7.004843   192.168.43.209   52.221.118.118   TCP          54 51979 → 443 [ACK] Seq=1377 Ack=513 Win=66048 Len=0
  896 7.104954   52.221.118.118   192.168.43.209   TLSv1.3     405 Application Data

    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 40
      Identification: 0x231e (8990)
    > Flags: 0x4000, Don't fragment
      Time to live: 110
      Protocol: TCP (6)
      Header checksum: 0x51e5 [validation disabled]
      [Header checksum status: Unverified]
      Source: 52.221.118.118
      Destination: 192.168.43.209
  > Transmission Control Protocol, Src Port: 443, Dst Port: 51979, Seq: 242, Ack: 1377, Len: 0

0000  94 39 e5 03 36 f5 2e 4d  54 ad 75 d4 08 00 45 00   ·9··6·.M T·u···E·
0010  00 28 23 1e 40 00 6e 06  51 e5 34 dd 76 76 c0 a8   ·(#·@·n· Q·4·vv··
0020  2b d1 01 bb cb 0b 15 4a  e7 cc 8d d7 41 b7 50 10   +······J ····A·P·
0030  00 08 7e 93 00 00                                  ··~···

Flags (3 bits) (ip.flags), 2 bytes          Packets: 4349 · Displayed: 25 (0.6%)          Profile: Default
```

Pada gambar dibawah ini menggunakan TOR browser dan menggunakan VPN
-Pertama cek ip kita



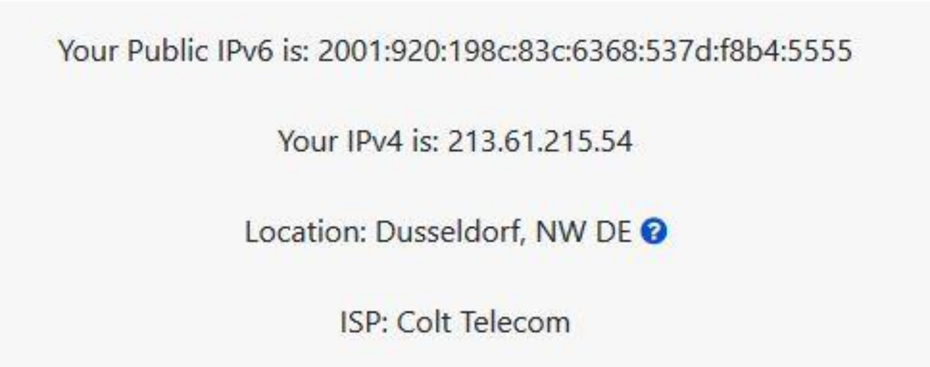
```
Wireless LAN adapter WiFi 2:

   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.



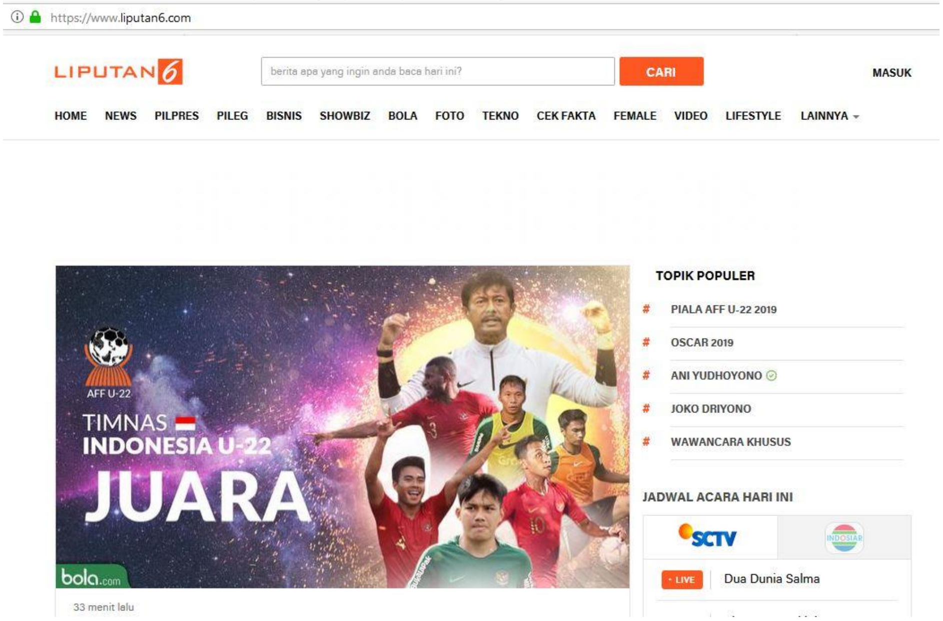
Your Public IPv6 is: 2001:920:198c:83c:6368:537d:f8b4:5555

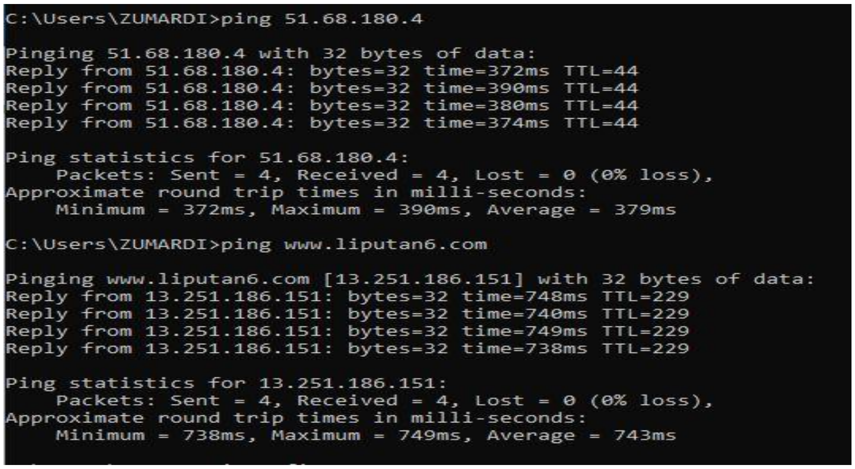
Your IPv4 is: 213.61.215.54

Location: Dusseldorf, NW DE

ISP: Colt Telecom

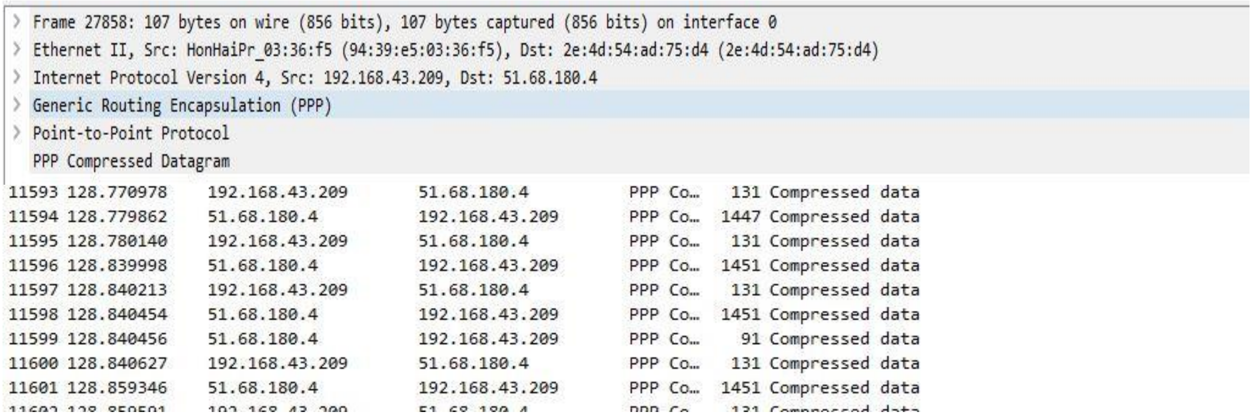
-lakukan browsing dengan web yang kita tuju, disini web yang saya pilih yaitu liputan6.com, terlihat saya mencoba ping melalui CMD, semuanya mereply dan terhubung dengan baik, dengan ip yang ditampilkan berbeda.





```
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
```

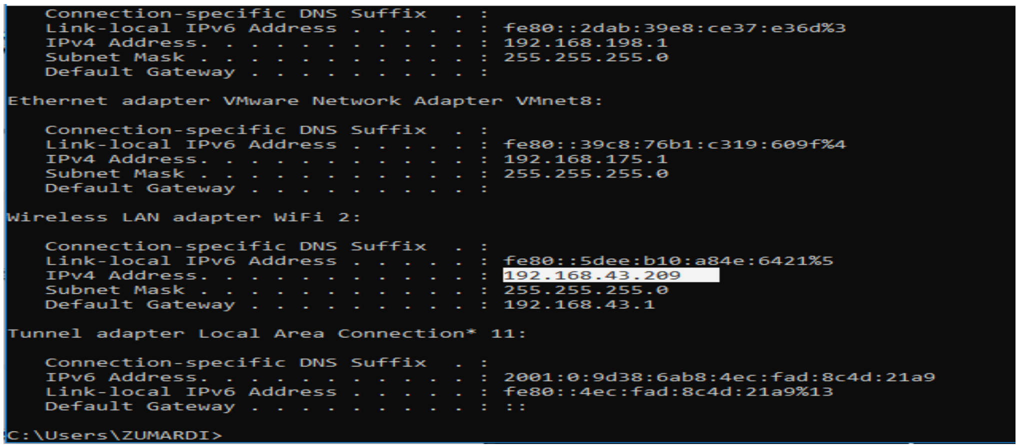
-ini merupakan tampilan tapping dari capturean wireshark, didapat 107bytes packet data atau 856 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, point-to-point protocol (PPP)



```
> 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 128.859591    192.168.43.209      51.68.180.4         PPP Co…   131 Compressed data
```

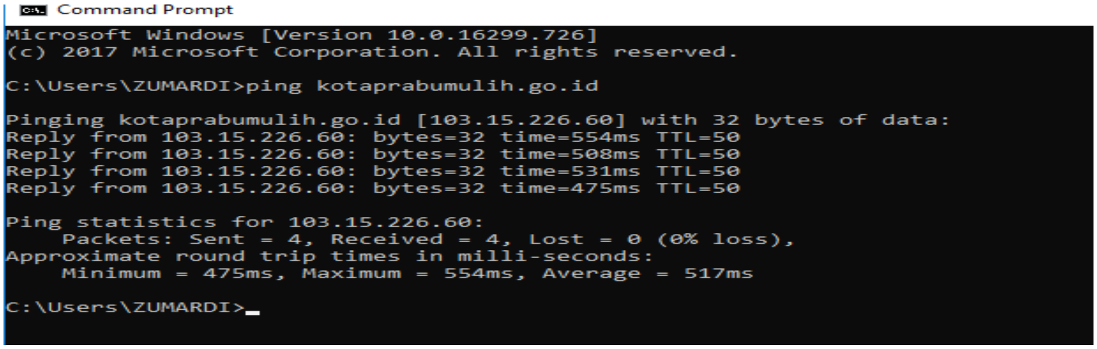
2. kotaprabumulih.go.id (Government)

-Pertama kita harus mengecek IP address laptop/komputermu



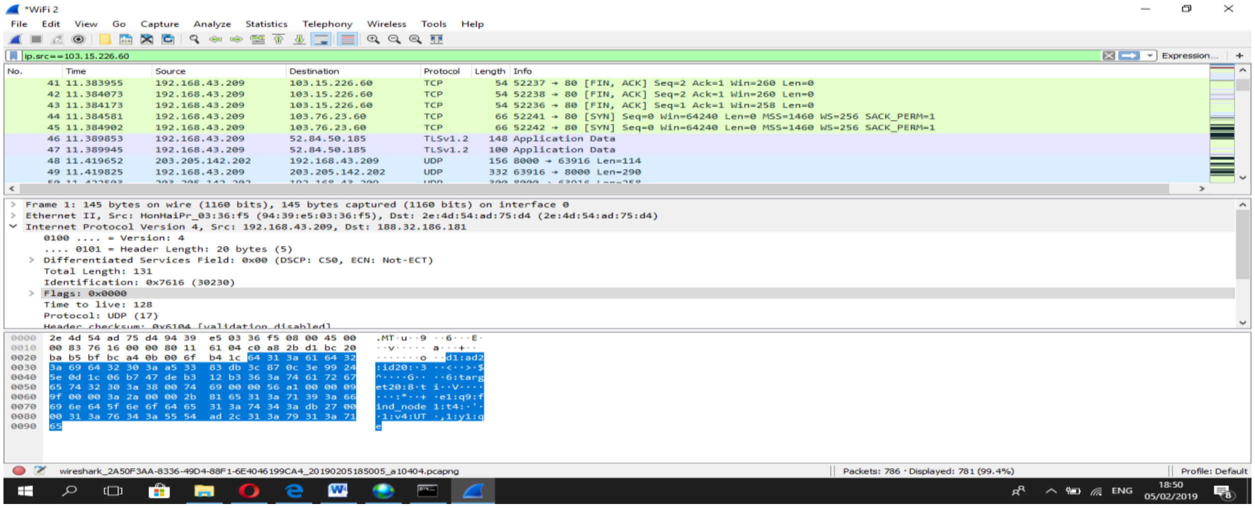
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2dab:39e8:ce37:e36d%3
   IPv4 Address. . . . . . . . . . . : 192.168.198.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::39c8:76b1:c319:609f%4
   IPv4 Address. . . . . . . . . . . : 192.168.175.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter WiFi 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5dee:b10:a84e:6421%5
   IPv4 Address. . . . . . . . . . . : 192.168.43.209
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:4ec:fad:8c4d:21a9
   Link-local IPv6 Address . . . . . : fe80::4ec:fad:8c4d:21a9%13
   Default Gateway . . . . . . . . . : ::

C:\Users\ZUMARDI>
```

-Kemudian melakukan ping ke kotaprabumulih.go.id dimana ip yang didapat yaitu 103.15.226.60



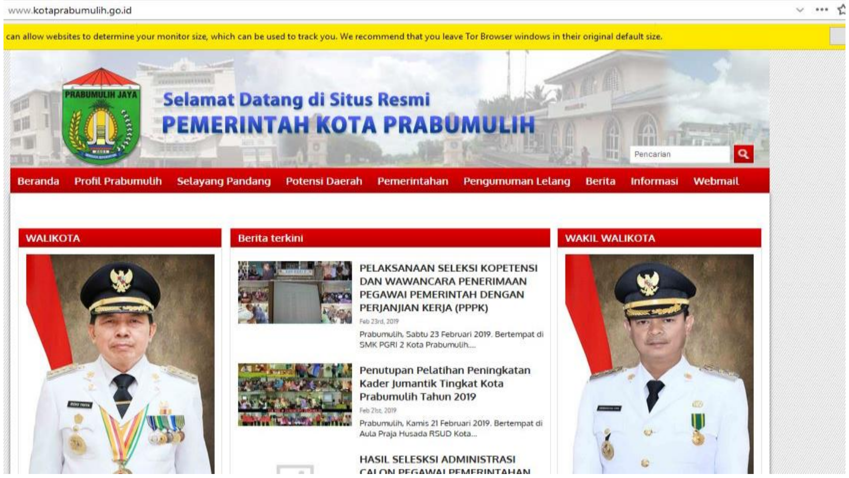
```
Microsoft Windows [Version 10.0.16299.726]
(c) 2017 Microsoft Corporation. All rights reserved.

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=554ms TTL=50
Reply from 103.15.226.60: bytes=32 time=508ms TTL=50
Reply from 103.15.226.60: bytes=32 time=531ms TTL=50
Reply from 103.15.226.60: bytes=32 time=475ms TTL=50

Ping statistics for 103.15.226.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 475ms, Maximum = 554ms, Average = 517ms

C:\Users\ZUMARDI>_
```

- ini merupakan tampilan tapping dari capturean wireshark, didapat 145bytes packet data atau 1160 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan, dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, Transmission Control Protocol(TCP).


*WiFi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
ip.src==103.15.226.60

No.  Time          Source            Destination       Protocol  Length Info
  41 11.383955     192.168.43.209    103.15.226.60     TCP        54 52237 → 80 [FIN, ACK] Seq=2 Ack=1 Win=260 Len=0
  42 11.384073     192.168.43.209    103.15.226.60     TCP        54 52238 → 80 [FIN, ACK] Seq=2 Ack=1 Win=260 Len=0
  43 11.384173     192.168.43.209    103.15.226.60     TCP        54 52236 → 80 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
  44 11.384581     192.168.43.209    103.76.23.60      TCP        66 52241 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  45 11.384902     192.168.43.209    103.76.23.60      TCP        66 52242 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  46 11.389853     192.168.43.209    52.84.50.185      TLSv1.2   148 Application Data
  47 11.389945     192.168.43.209    52.84.50.185      TLSv1.2   100 Application Data
  48 11.419652     203.205.142.202   192.168.43.209    UDP       156 8000 → 63916 Len=114
  49 11.419825     192.168.43.209    203.205.142.202   UDP       332 63916 → 8000 Len=290

> Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 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)
v Internet Protocol Version 4, Src: 192.168.43.209, Dst: 188.32.186.181
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 131
    Identification: 0x7616 (30230)
  > Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x6104 [validation disabled]

0000  2e 4d 54 ad 75 d4 94 39  e5 03 36 f5 08 00 45 00   .MT·u··9 ··6···E·
0010  00 83 76 16 00 00 80 11  61 04 c0 a8 2b d1 bc 20   ··v····· a···+··
0020  ba b5 bf bc a4 0b 00 6f  b4 1c 64 31 3a 61 64 32   ·······o ··d1:ad2
0030  3a 69 64 32 30 3a a5 33  83 db 3c 87 0c 3e 99 24   :id20:·3 ··<··>·$
0040  5e 0d 1c 06 b7 47 de b3  12 b3 36 3a 74 61 72 67   ^····G·· ··6:targ
0050  65 74 32 30 3a 38 00 74  69 00 00 56 a1 00 00 09   et20:8·t i··V····
0060  9f 00 00 3a 2a 00 00 2b  81 65 31 3a 71 39 3a 66   ···:*··+ ·e1:q9:f
0070  69 6e 64 5f 6e 6f 64 65  31 3a 74 34 3a db 27 00   ind_node 1:t4:·'·
0080  00 31 3a 76 34 3a 55 54  ad 2c 31 3a 79 31 3a 71   ·1:v4:UT ·,1:y1:q
0090  65                                                 e

wireshark_2A50F3AA-8336-49D4-88F1-6E4046199CA4_20190205185005_a10404.pcapng
Packets: 786 · Displayed: 781 (99.4%)    Profile: Default
```

selanjutnya website pemerintahan, disini saya pilih kotaprabumulih.go.id (Government),
-Pada gambar dibawah ini menggunakan TOR browser dan menggunakan VPN



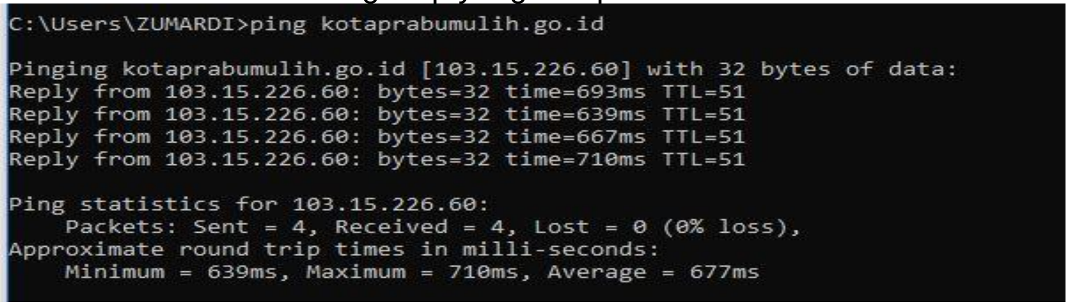
can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.

PELAKSANAAN SELEKSI KOPETENSI DAN WAWANCARA PENERIMAAN PEGAWAI PEMERINTAH DENGAN PERJANJIAN KERJA (PPPK)
Feb 23rd, 2019
Prabumulih, Sabtu 23 Februari 2019. Bertempat di SMK PGRI 2 Kota Prabumulih....

Penutupan Pelatihan Peningkatan Kader Jumantik Tingkat Kota Prabumulih Tahun 2019
Feb 21st, 2019
Prabumulih, Kamis 21 Februari 2019. Bertempat di Aula Praja Husada RSUD Kota...

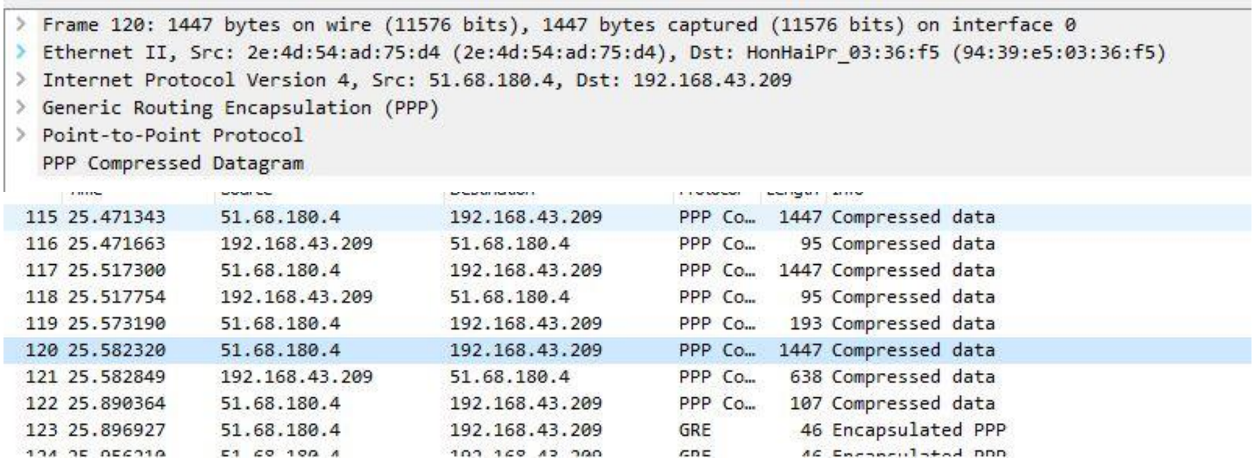
HASIL SELESKSI ADMINISTRASI CALON PEGAWAI PEMERINTAHAN

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



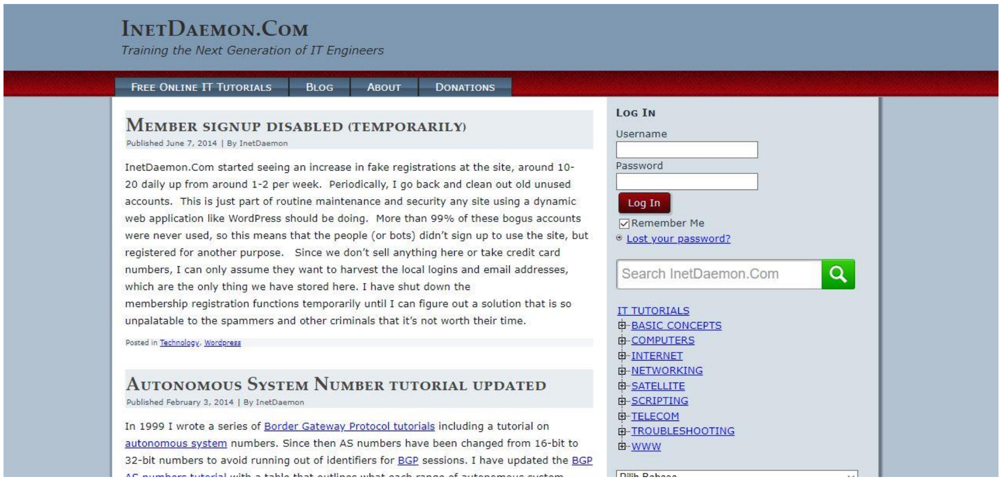
```
C:\Users\ZUMARDI>ping kotaprabumulih.go.id

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 dengan menggunakan TOR Browser tapi berbeda dengan tidak menggunakan TOR browser.



```
> 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

 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
```

3.https://www.inetdaemon.com (Luar Negeri)



MEMBER SIGNUP DISABLED (TEMPORARILY)

Published June 7, 2014 | By InetDaemon

InetDaemon.Com started seeing an increase in fake registrations at the site, around 10-20 daily up from around 1-2 per week. Periodically, I go back and clean out old unused accounts. This is just part of routine maintenance and security any site using a dynamic web application like WordPress should be doing. More than 99% of these bogus accounts were never used, so this means that the people (or bots) didn't sign up to use the site, but registered for another purpose. Since we don't sell anything here or take credit card numbers, I can only assume they want to harvest the local logins and email addresses, which are the only thing we have stored here. I have shut down the membership registration functions temporarily until I can figure out a solution that is so unpalatable to the spammers and other criminals that it's not worth their time.

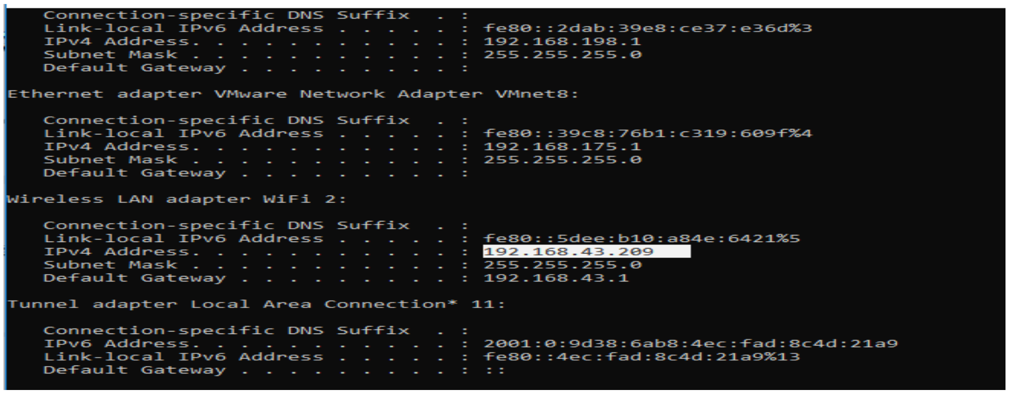
Posted in Technology, Wordpress

AUTONOMOUS SYSTEM NUMBER TUTORIAL UPDATED

Published February 3, 2014 | By InetDaemon

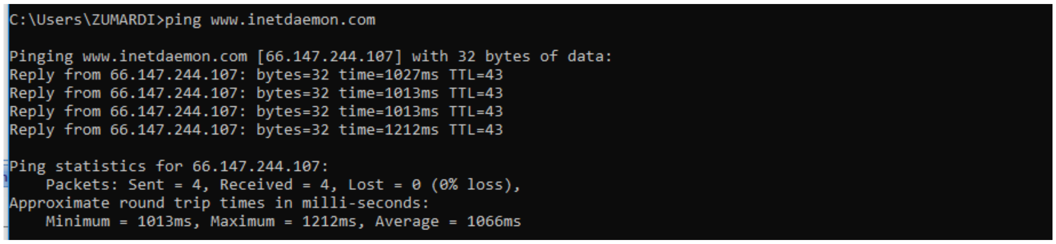
In 1999 I wrote a series of Border Gateway Protocol tutorials including a tutorial on autonomous system numbers. Since then AS numbers have been changed from 16-bit to 32-bit numbers to avoid running out of identifiers for BGP sessions. I have updated the BGP

Pertama kita harus mengecek IP address laptop/komputermu



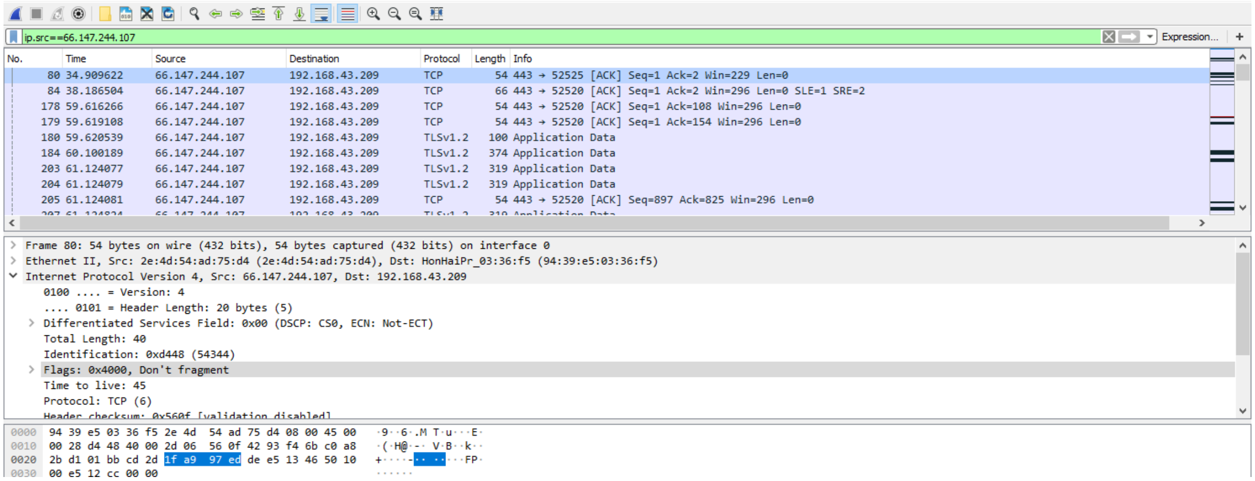
```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2dab:39e8:ce37:e36d%3
   IPv4 Address. . . . . . . . . . . : 192.168.198.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::39c8:76b1:c319:609f%4
   IPv4 Address. . . . . . . . . . . : 192.168.175.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter WiFi 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5dee:b10:a84e:6421%5
   IPv4 Address. . . . . . . . . . . : 192.168.43.209
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6ab8:4ec:fad:8c4d:21a9
   Link-local IPv6 Address . . . . . : fe80::4ec:fad:8c4d:21a9%13
   Default Gateway . . . . . . . . . : ::
```

Kemudian melakukan ping ke https://www.inetdaemon.com



```
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=1027ms TTL=43
Reply from 66.147.244.107: bytes=32 time=1013ms TTL=43
Reply from 66.147.244.107: bytes=32 time=1013ms TTL=43
Reply from 66.147.244.107: bytes=32 time=1212ms TTL=43

Ping statistics for 66.147.244.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1013ms, Maximum = 1212ms, Average = 1066ms
```

- ini merupakan tampilan tapping dari capturean wireshark, didapat 54bytes packet data atau 432 bits, lalu didapat mac address dari laptop source dan destination, Tipe ip yang digunakan,port yang digunakan dan protocol yang digunakan, disini didapat protocol yang digunakan yaitu, Transmission Control Protocol(TCP).

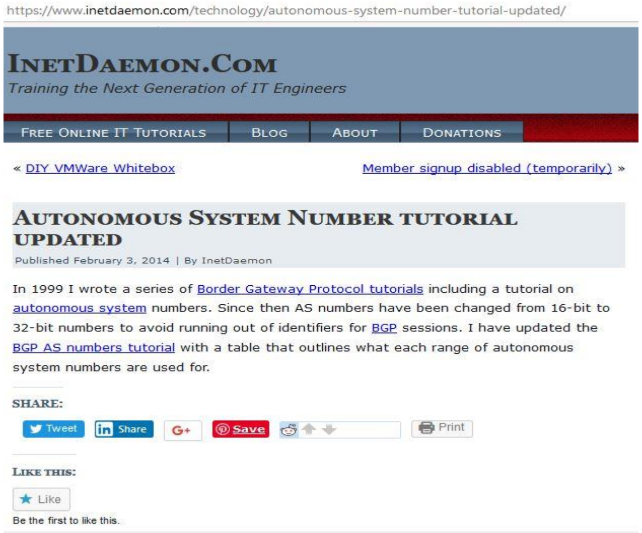


No.	Time	Source	Destination	Protocol	Length	Info
80	34.909622	66.147.244.107	192.168.43.209	TCP	54	443 → 52525 [ACK] Seq=1 Ack=2 Win=229 Len=0
84	38.186504	66.147.244.107	192.168.43.209	TCP	66	443 → 52520 [ACK] Seq=1 Ack=2 Win=296 Len=0 SLE=1 SRE=2
178	59.616266	66.147.244.107	192.168.43.209	TCP	54	443 → 52520 [ACK] Seq=1 Ack=108 Win=296 Len=0
179	59.619108	66.147.244.107	192.168.43.209	TCP	54	443 → 52520 [ACK] Seq=1 Ack=154 Win=296 Len=0
180	59.620539	66.147.244.107	192.168.43.209	TLSv1.2	100	Application Data
184	60.100189	66.147.244.107	192.168.43.209	TLSv1.2	374	Application Data
203	61.124077	66.147.244.107	192.168.43.209	TLSv1.2	319	Application Data
204	61.124079	66.147.244.107	192.168.43.209	TLSv1.2	319	Application Data
205	61.124081	66.147.244.107	192.168.43.209	TCP	54	443 → 52520 [ACK] Seq=897 Ack=825 Win=296 Len=0
207	61.124824	66.147.244.107	192.168.43.209	TLSv1.2	319	Application Data

```
> Frame 80: 54 bytes on wire (432 bits), 54 bytes captured (432 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)
v Internet Protocol Version 4, Src: 66.147.244.107, Dst: 192.168.43.209
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xd448 (54344)
  > Flags: 0x4000, Don't fragment
    Time to live: 45
    Protocol: TCP (6)
    Header checksum: 0x560f [validation disabled]
```

```
0000  94 39 e5 03 36 f5 2e 4d  54 ad 75 d4 08 00 45 00   ·9··6·.M T·u···E·
0010  00 28 d4 48 40 00 2d 06  56 0f 42 93 f4 6b c0 a8   ·(·H@·-· V·B··k··
0020  2b d1 01 bb cd 2d 1f a9  97 ed de e5 13 46 50 10   +····-·· ·····FP·
0030  00 e5 12 cc 00 00                                  ······
```

Pada gambar dibawah ini menggunakan TOR browser dan menggunakan VPN



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

INETDAEMON.COM
Training the Next Generation of IT Engineers

« DIY VMWare Whitebox   Member signup disabled (temporarily) »

AUTONOMOUS SYSTEM NUMBER TUTORIAL UPDATED

Published February 3, 2014 | By InetDaemon

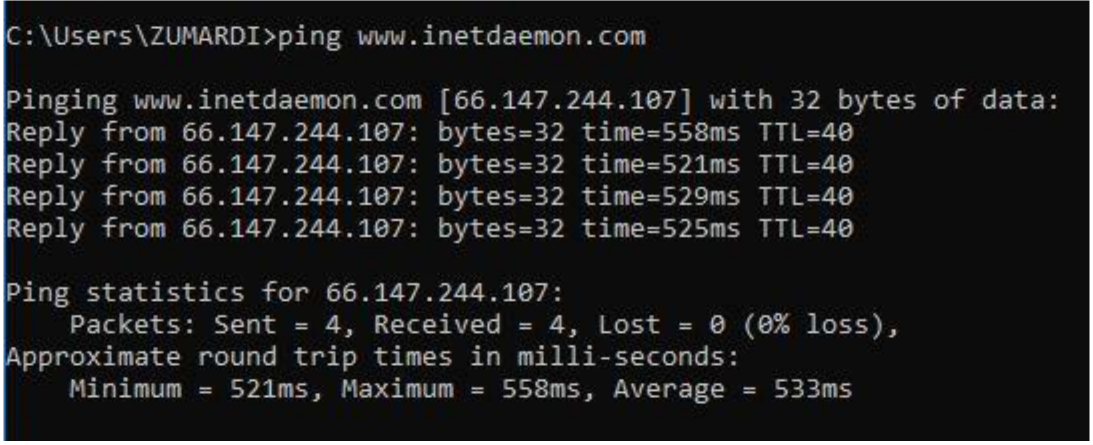
In 1999 I wrote a series of Border Gateway Protocol tutorials including a tutorial on autonomous system numbers. Since then AS numbers have been changed from 16-bit to 32-bit numbers to avoid running out of identifiers for BGP sessions. I have updated the BGP AS numbers tutorial with a table that outlines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

SHARE:

LIKE THIS:

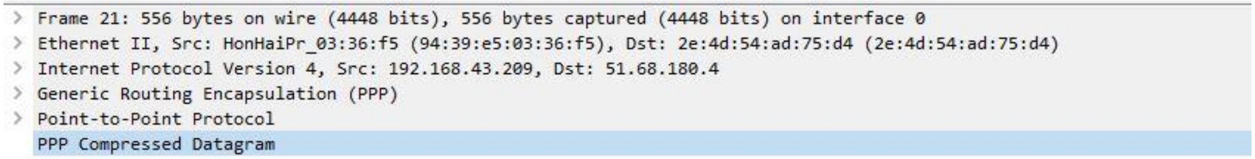
Be the first to like this.

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

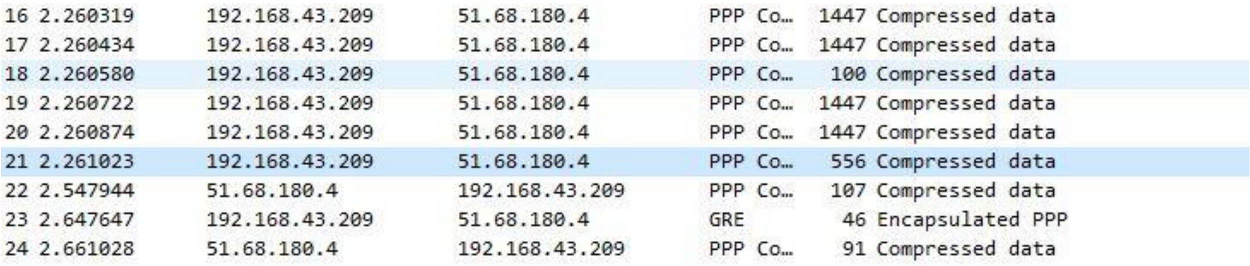


```
C:\Users\ZUMARDI>ping www.inetdaemon.com

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
```

Kesimpulan :

Perbandingan terdapat pada perbedaan IP destination yang didapatkan dan juga pada Protokol jaringan. Dimana ketika menggunakan TOR kita akan mendapati IP Destination dan protocol yang sama setiap kali mengakses website.