LAPORAN KEAMANAN JARINGAN KOMPUTER

Oleh:

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

LABORATORIUM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

A. Webite dalam negeri (attahalilintarhabit.com)
Informasi domain :

Domain Information

Domain:	attahalilintarhabit.com
Registrar:	PDR Ltd. d/b/a PublicDomainRegistry.com
Registered On:	2017-10-03
Expires On:	2019-10-03
Updated On:	2018-07-20
Status:	clientTransferProhibited
Name Servers:	yukbisnis.earth.orderbox-dns.com yukbisnis.mars.orderbox-dns.com yukbisnis.mercury.orderbox-dns.com yukbisnis.venus.orderbox-dns.com

Registrant Contact

Name:	Domain Admin
Organization:	Privacy Protect, LLC (PrivacyProtect.org)
Street:	10 Corporate Drive
City:	Burlington
State:	MA
Postal Code:	01803
Country:	US
Phone:	+1.8022274003
Email:	contact@privacyprotect.org

Administrative Contact

Name:	Domain Admin
Organization:	Privacy Protect, LLC (PrivacyProtect.org)
Street:	10 Corporate Drive
City:	Burlington
State:	MA
Postal Code:	01803
Country:	US
Phone:	+1.8022274003
Email:	contact@privacyprotect.org

Technical Contact

Name:	Domain Admin
Organization:	Privacy Protect, LLC (PrivacyProtect.org)
Street:	10 Corporate Drive
City:	Burlington
State:	MA
Postal Code:	01803
Country:	US
Phone:	+1.8022274003

Netcraft site report :

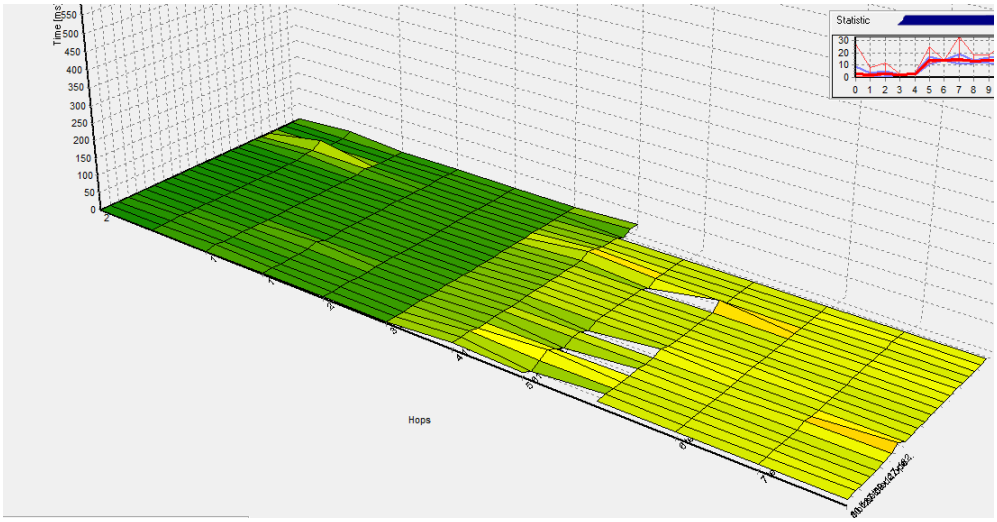
Network

Site	http://attahalilintarhabit.com	**Netblock Owner**	PT Biznet Data Center
Domain	attahalilintarhabit.com	**Nameserver**	yukbisnis.mars.orderbox-dns.com
IP address	116.206.197.105 (VirusTotal)	**DNS admin**	attahalilintarhabit@gmail.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	PublicDomainRegistry.com	**Nameserver organisation**	whois.PublicDomainRegistry.com
Organisation	Privacy Protect, LLC (PrivacyProtect.org), 10 Corporate Drive, Burlington, 01803, US	**Hosting company**	Biznet Networks
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Biznet Data Center Corporate / Direct Member IDNIC Midplaza 2, 8th Floor Jl. Jend Sudirman Kav 10-11 Jakarta, Indonesia	116.206.197.105	Linux	unknown	4-Feb-2019

Berikut hasil dari 3d traceroute :



Hop	IP	Hostname	last [ms]	min [ms]	max [ms]	ava. [ms]
1	192.168.238.1	1.238.168.192.in-addr.arpa	1	1	27	3
2	192.168.100.1	1.100.168.192.in-addr.arpa	1	1	8	1
3	110.137.112.1	1.subnet110-137-112.speedy.telkom.net.id	3	2	12	3
4	125.160.14.161	161.subnet125-160-14.speedy.telkom.net.id	2	2	28	3
5	61.94.115.209	61.94.115.209	3	2	26	4
6	218.100.36.56	telkom.openixp.net	12	12	31	13
7	218.100.36.2	tengiga-0-1.openixp.net	12	12	23	13
8	218.100.36.118	biznetcloud.openixp.net	13	12	33	14
9	137.59.127.154	137-59-127-154.biznetgiocloud.com	13	12	19	13
10	137.59.127.182	137-59-127-182.biznetgiocloud.com	18	13	18	14
11	116.206.197.105	attahalilintarhabit.com	13	13	28	14

Setelah didapatkan alamat ip website tersebut dari software 3dtracerroute, masukkan ip tersebut website robtex dan didapat hasil berikut ini.

ANALYSIS

This section shows a quick analyis of the given host name or ip number.

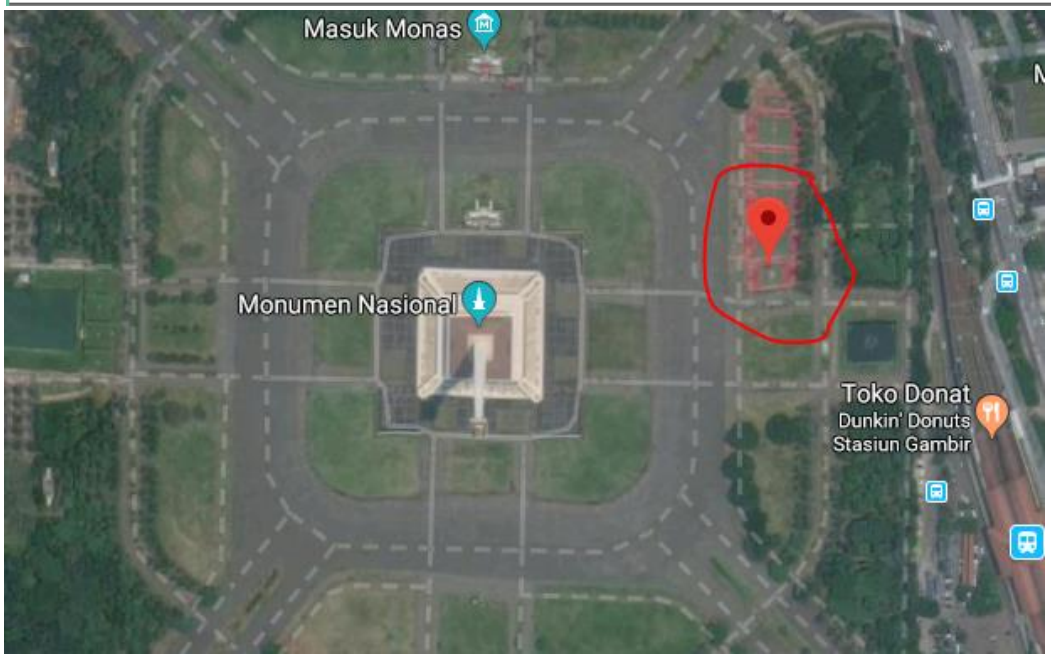
The IP number is in Indonesia. It is hosted by Routes announced to Level 3 by BIZNET..

We investigated 100 host names that point to 116.206.197.105. Example: **sporfista-sarangoriginal**.com, **dermanefskin**.com, www.**printerkomputer**.com and **gamainterstudi**.com. We estimate that it is used as ip number by 2,910 host names.

We have a premium report available for 116.206.197.105.

IPINFO.IO

Hostname	undefined
City	, ID
Latitude/Longitude	-6.1750,106.8290
Postal Code	undefined

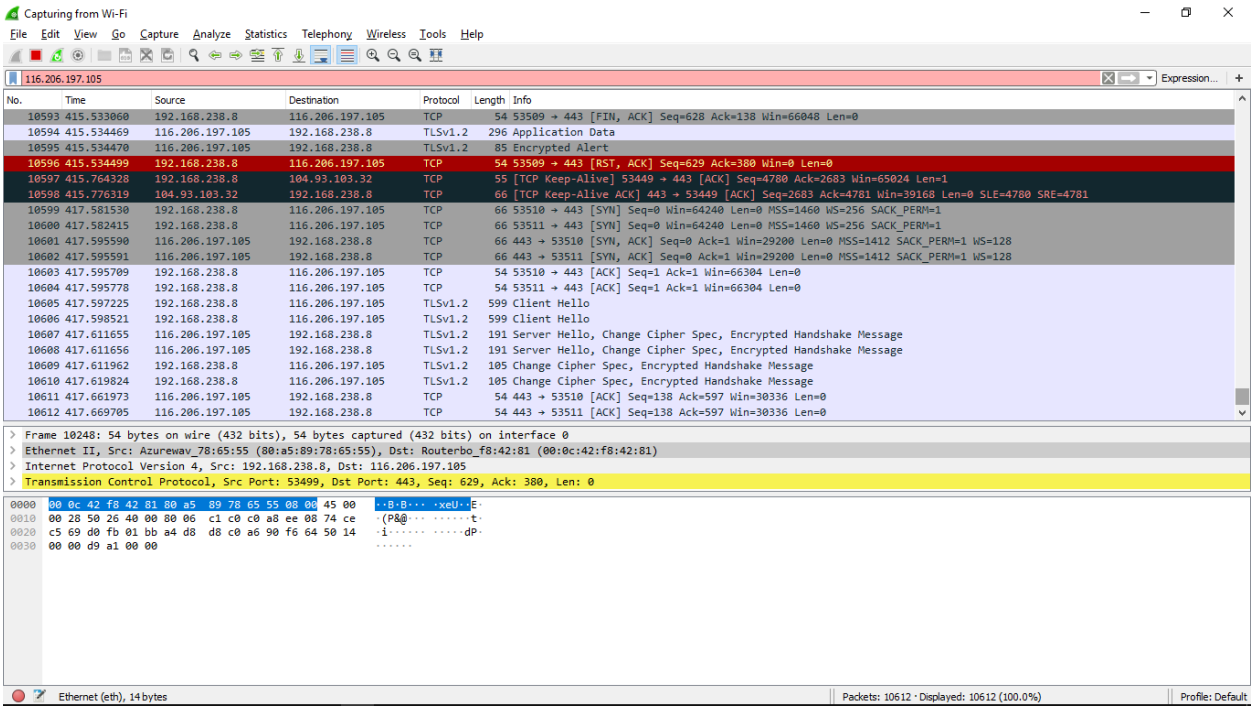


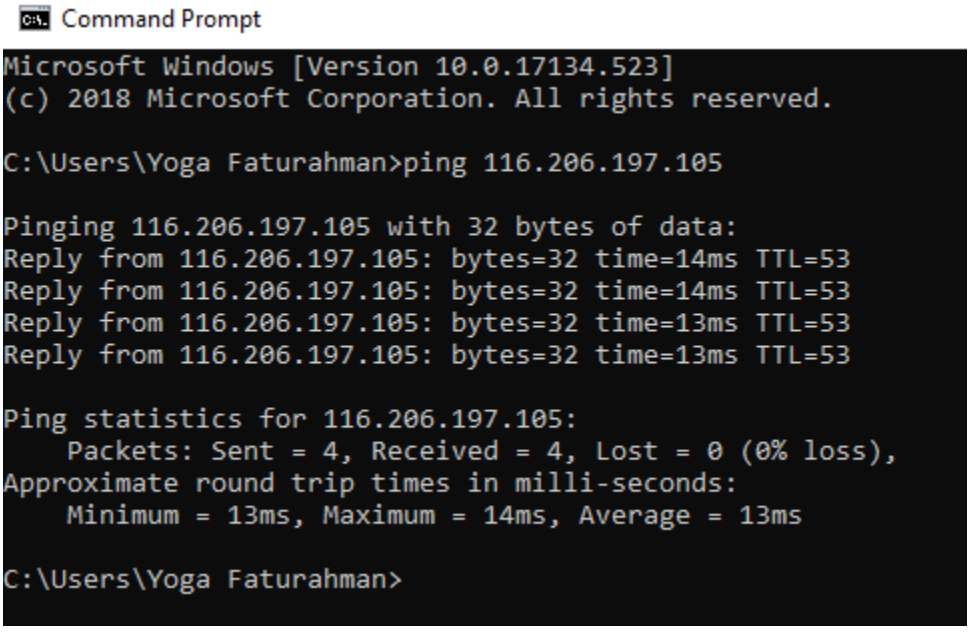
Dari 10 IP yang didapat dari 3dtraceroute kita ambil sample 1 IP yaitu 116.206.197.105

Jika dianalisis menggunakan wireshark maka :

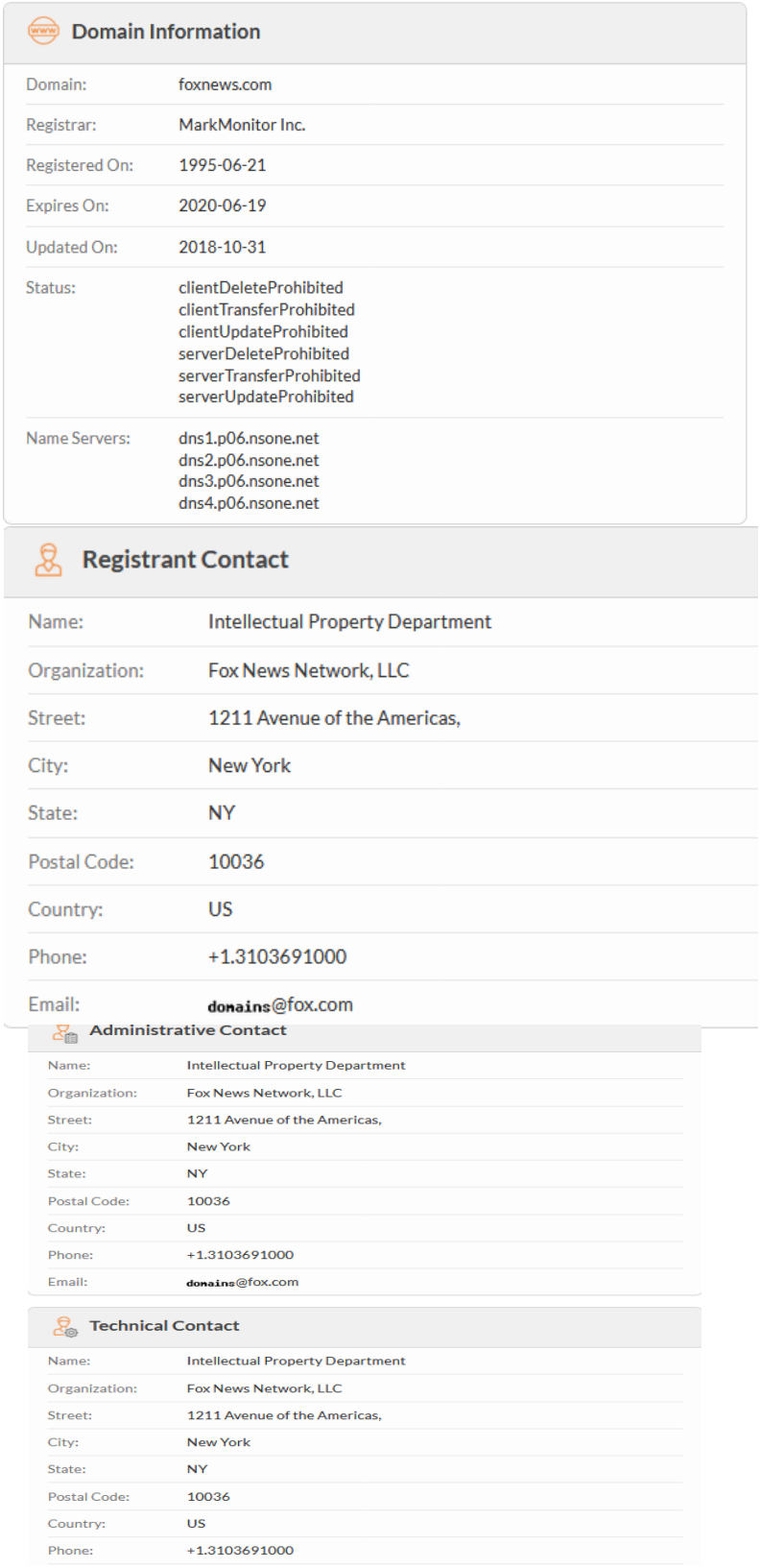
Source : 192.168.238.8

Destination : 116.206.197.105





B. Website luar negeri (https://www.foxnews.com)
Infomasi domain



Domain Information

Domain:	foxnews.com
Registrar:	MarkMonitor Inc.
Registered On:	1995-06-21
Expires On:	2020-06-19
Updated On:	2018-10-31
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	dns1.p06.nsone.net dns2.p06.nsone.net dns3.p06.nsone.net dns4.p06.nsone.net

Registrant Contact

Name:	Intellectual Property Department
Organization:	Fox News Network, LLC
Street:	1211 Avenue of the Americas,
City:	New York
State:	NY
Postal Code:	10036
Country:	US
Phone:	+1.3103691000
Email:	domains@fox.com

Administrative Contact

Name:	Intellectual Property Department
Organization:	Fox News Network, LLC
Street:	1211 Avenue of the Americas,
City:	New York
State:	NY
Postal Code:	10036
Country:	US
Phone:	+1.3103691000
Email:	domains@fox.com

Technical Contact

Name:	Intellectual Property Department
Organization:	Fox News Network, LLC
Street:	1211 Avenue of the Americas,
City:	New York
State:	NY
Postal Code:	10036
Country:	US
Phone:	+1.3103691000

Netcraft site report :

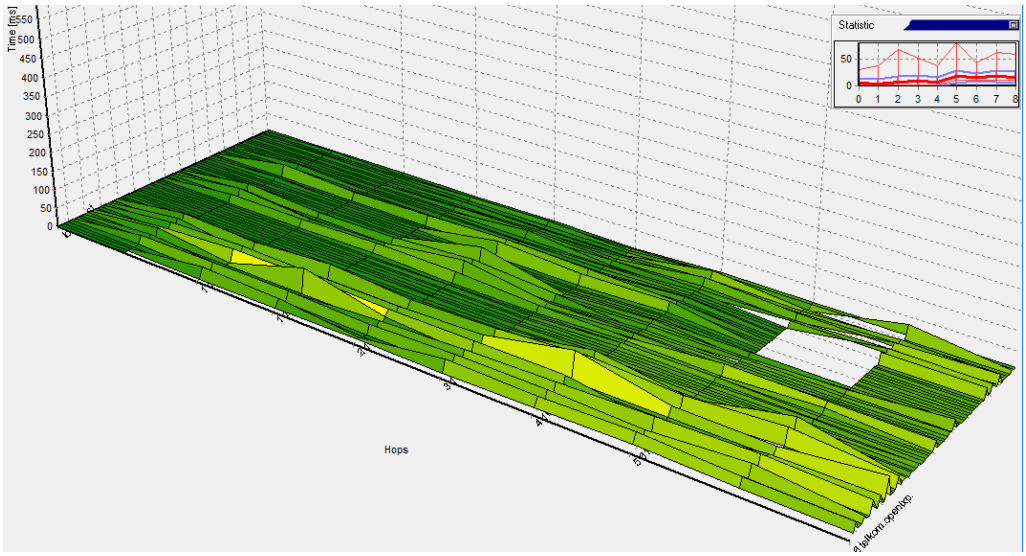
Network

Site	http://www.foxnews.com	**Netblock Owner**	Akamai International, BV
Domain	foxnews.com	**Nameserver**	dns1.p06.nsone.net
IP address	23.200.107.80 (VirusTotal)	**DNS admin**	hostmaster@nsone.net
IPv6 address	2a02:26f0:71:288:0:0:0:1324	**Reverse DNS**	a23-200-107-80.deploy.static.akamaitechnologies.com
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.name.com
Organisation	*unknown*	**Hosting company**	Akamai Technologies
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	Enabled
Hosting country	NL		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.183	Linux	AkamaiGHost	5-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.197.255.146	Linux	AkamaiGHost	5-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.183	Linux	AkamaiGHost	2-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.197.255.146	Linux	AkamaiGHost	2-Feb-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.43.77.140	Linux	AkamaiGHost	28-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.197.255.146	Linux	AkamaiGHost	27-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.183	Linux	AkamaiGHost	20-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.197.255.146	Linux	AkamaiGHost	20-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.232.183	Linux	AkamaiGHost	17-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.197.255.146	Linux	AkamaiGHost	16-Jan-2019

Berikut hasil dari 3dtraceroute:



Hop	IP	Hostname	last [ms]	min [ms]	max [ms]	ava. [ms]	var. [ms]	total Loss	perc. Loss	Latitude	Longitude	RTTL	ASN
1	192.168.238.1	1.238.168.192.in-addr.arpa	1	1	31	5	8					64	
2	192.168.100.1	1.100.168.192.in-addr.arpa	1	1	37	4	8					63	AS7632
3	110.137.112.1	1.subnet110-137-112.speedy.telkom.net.id	3	2	67	7	11					253	AS17974
4	125.160.14.161	161.subnet125-160-14.speedy.telkom.net.id	2	2	52	8	11					61	AS17974
5	61.94.115.209	61.94.115.209	2	2	37	7	9					60	AS17974
6	218.100.36.56	telkom.openixp.net	12	11	80	16	11	2				59	
7	218.100.36.2	tengiga-0-1.openixp.net	12	11	42	15	8	25				248	
8	218.100.36.86	akamai.openixp.net	16	11	63	18	11					248	
9	23.0.180.187	www.foxnews.com	12	11	59	16	9					56	

Setelah didapatkan alamat ip website tersebut dari software 3dtracerroute, masukkan ip tersebut website robtex dan didapat hasil berikut ini:

ANALYSIS

This section shows a quick analysis of the given host name or ip number.

23.0.180.187 has one PTR.

Akamaitechnologies PTR

The PTR is a23-0-180-187.deploy.**akamaitechnologies**.com. The IP number is in Cambridge, United States. It is hosted by Akamai Technologies.

IPINFO.IO

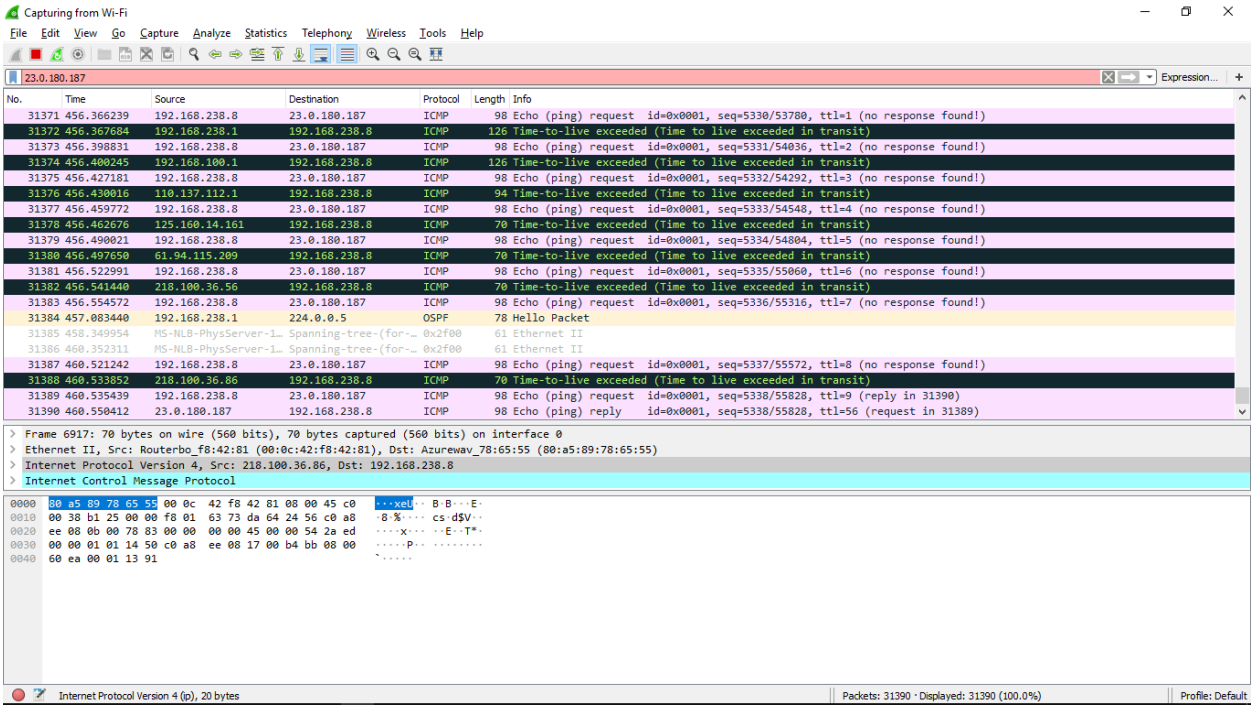
Hostname	a23-0-180-187.deploy.static.akamaitechnologies.com
City	, US
Latitude/Longitude	37.7510,-97.8220
Postal Code	undefined

Dari 9 IP yang didapat dari 3dtraceroute kita ambil sample 1 IP yaitu 23.0.180.187

Jika dianalisis menggunakan wireshark maka :

Source : 192.168.238.8

Destination : 23.0.180.187




```
C:\Users\Yoga Faturahman>ping 23.0.180.187

Pinging 23.0.180.187 with 32 bytes of data:
Reply from 23.0.180.187: bytes=32 time=12ms TTL=56
Reply from 23.0.180.187: bytes=32 time=12ms TTL=56
Reply from 23.0.180.187: bytes=32 time=12ms TTL=56
Reply from 23.0.180.187: bytes=32 time=11ms TTL=56

Ping statistics for 23.0.180.187:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

C. Website pemerintahan(http://disdukcapil.palembang.go.id)
Nah untuk website yang pemerintahan, tidak ditemukan domain information, jika dilihat dari netcraft site report maka data yang di dapatkan sebagai berikut.

Site title	Dinas Kependudukan dan Catatan Sipil Kota Palembang	**Date first seen**	July 2014
Site rank		**Primary language**	Indonesian
Description	Dinas Kependudukan dan Catatan Sipil Kota Palembang		
Keywords	Dinas Kependudukan dan Catatan Sipil Kota Palembang, pemkot, kota, palembang, e-government, e-gov, sumsel, sumatera selatan, sriwijaya, wong kito galo, indonesia, jeramba, jerambacms, muhammad riyadi, m.riyadi, plado, riri thamrin, riyadi thamrin, muhammad riyadi thamrin		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://disdukcapil.palembang.go.id	**Netblock Owner**	PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA
Domain	palembang.go.id	**Nameserver**	ns1.palembang.go.id
IP address	36.67.66.179 (VirusTotal)	**DNS admin**	root@palembang.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA	36.67.66.179	Linux	Apache/2	6-Feb-2019

Hop	IP	Hostname	last [ms]	min [ms]	max [ms]	ava. [ms]	var. [ms]	total Loss	perc. Loss	Latitude	Longitude	RTTL	ASN
1	192.168.238.1	1.238.168.192.in-addr.arpa	8	1	8	2	2					64	
2	192.168.100.1	1.100.168.192.in-addr.arpa	1	1	6	1	1					63	AS7632
3	110.137.112.1	1.subnet110-137-112.speedy.telkom.net.id	3	2	9	3	2					253	AS17974
4	125.160.14.161	161.subnet125-160-14.speedy.telkom.net.id	3	2	23	4	5					61	AS17974
5	61.94.115.209	61.94.115.209	3	2	21	6	5					60	AS17974
6	61.94.4.182	182.4.94.61.in-addr.arpa	3	3	13	4	2					250	AS17974
7	172.16.34.2	2.34.16.172.in-addr.arpa	3	2	21	4	4						
8	36.67.66.179	disdukcapil.palembang.go.id	3	2	20	4	3					57	

Setelah didapatkan alamat ip website tersebut dari software 3dtracerroute, masukkan ip tersebut website robtex dan didapat hasil berikut ini:

ANALYSIS

This section shows a quick analyis of the given host name or ip number.

The IP number is in Indonesia. It is hosted by PT. Telekomunikasi Indonesia.

We investigated seven host names that point to 36.67.66.179. Example: disperindagkop.**palembang**.go.id, bakesbangpolinmas.**palembang**.go.id, dinkes.**palembang**.go.id and disdukcapil.**palembang**.go.id.

IPINFO.IO

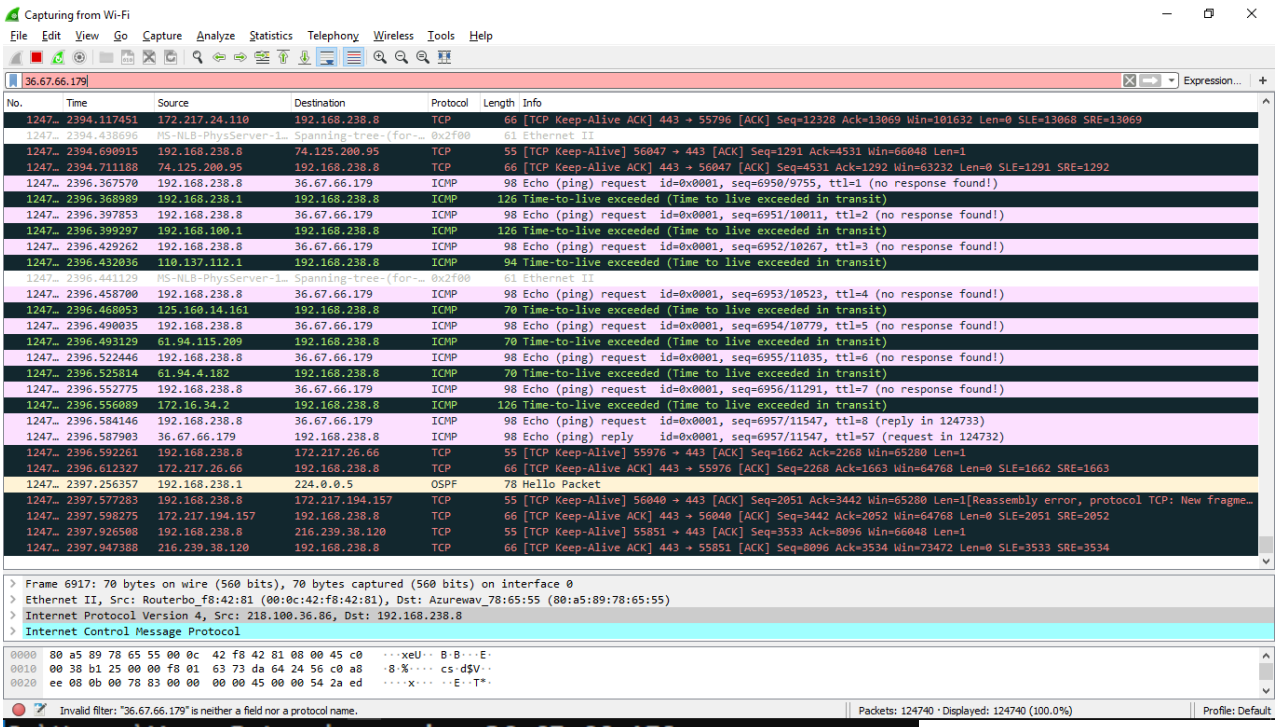
Hostname	undefined
City	Depok, West Java ID
Latitude/Longitude	-6.3433,106.4990
Postal Code	undefined

Dari 9 IP yang didapat dari 3dtraceroute kita ambil sample 1 IP yaitu 36.67.66.179

Jika dianalisis menggunakan wireshark maka :

Source : 192.168.238.8

Destination : 36.67.66.179




```
C:\Users\Yoga Faturahman>ping 36.67.66.179

Pinging 36.67.66.179 with 32 bytes of data:
Reply from 36.67.66.179: bytes=32 time=4ms TTL=57
Reply from 36.67.66.179: bytes=32 time=4ms TTL=57
Reply from 36.67.66.179: bytes=32 time=3ms TTL=57
Reply from 36.67.66.179: bytes=32 time=4ms TTL=57

Ping statistics for 36.67.66.179:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```