Reconnaissance

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

Reconnaissance

Adalah sebuah fase persiapan sebelum (attacker) melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Teknik ini akan menyertakan network scanning baik melalui jaringan internal atau external yang tentu saja tanpa mengantongi ijin.

Pada Kasus ini saya menggunakan 4 website dan 2 aplikasi untuk mengidentifikasi(Reconnaissance) destination yang diinginkan.

Website :
1. whois.com
2. internet archive wayback machine
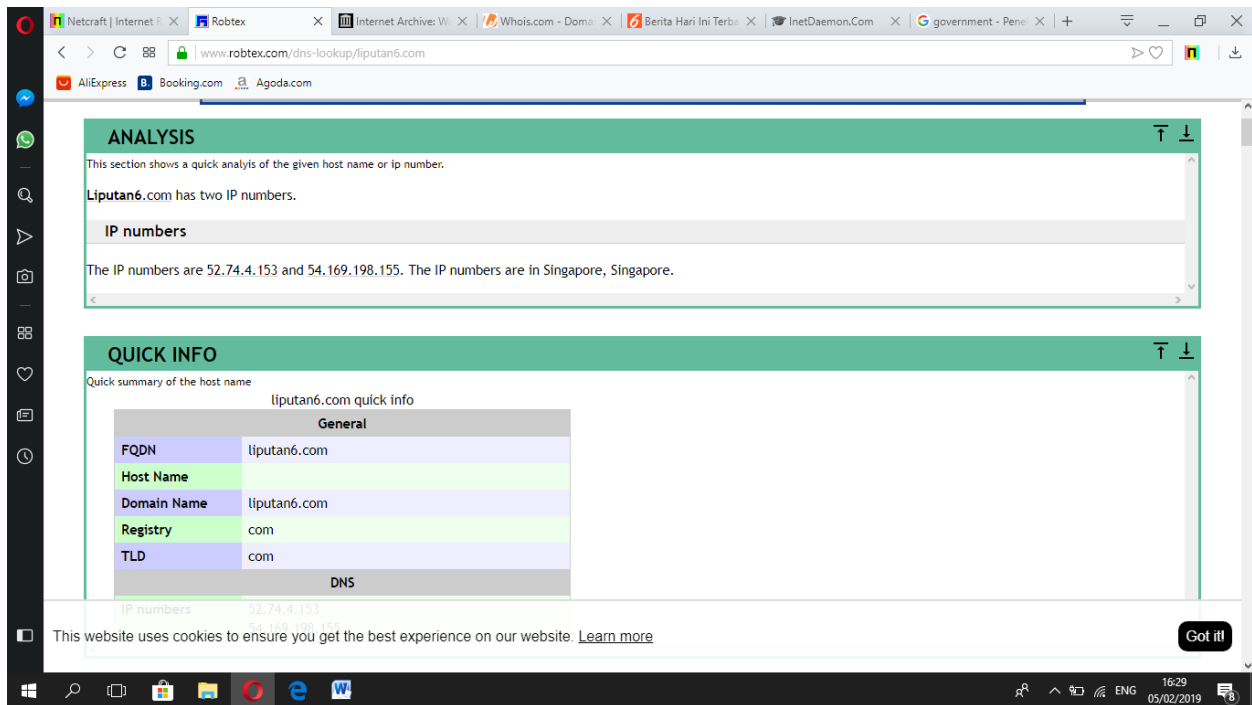3. netcraft
4. Robtex

Aplikasi :
1. VisualRoute
2. Wireshark

Website yang dituju yaitu :
1. liputan6.com (Dalam Negeri)
2. kotaprabumulih.go.id (Government)
3. https://www.inetdaemon.com (Luar Negeri)
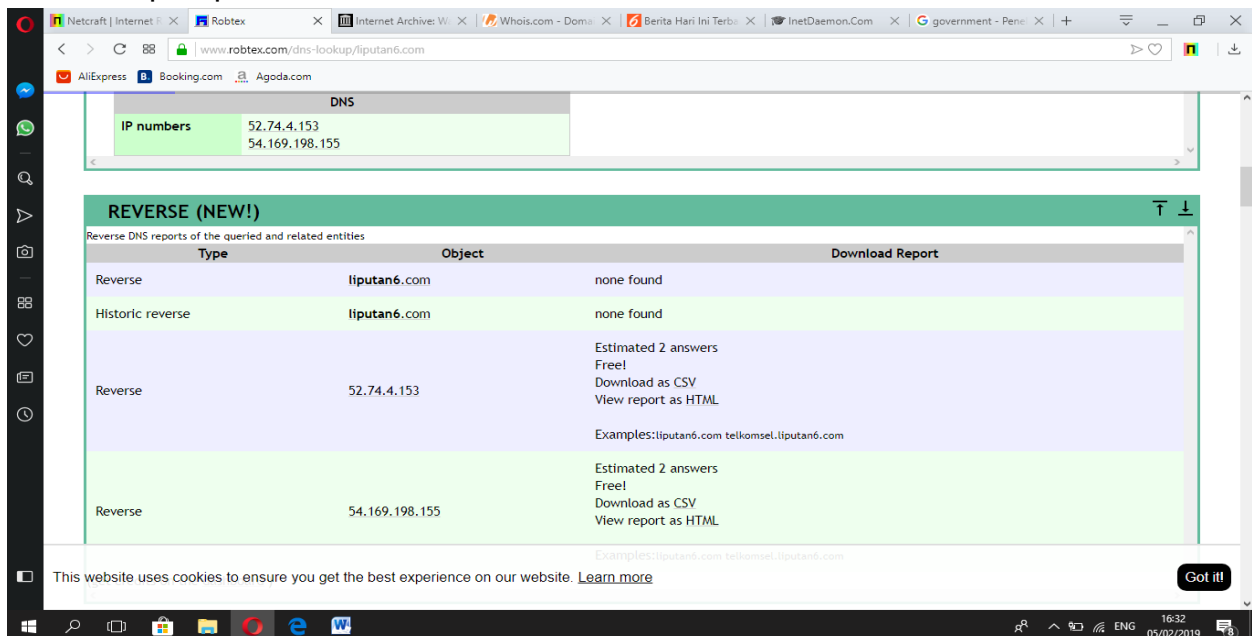
I.   Liputan6.com

Melalui Website Robtex

- Disini bisa dilihat bahwa liputan6.com memiliki dua ip =
- 52.74.4.153
- 54.169.198.155

Lalu terdapat quick info,dan reserve

Ada records

Dan juga terdapat info-info tentang liputan6.com dengan nama WHOIS

Dan juga terdapat GRAPH

Melalui website netcraft :

Disini terdapat backround, Network, Hosting History, dll..

Melalui whois :

Sama seperti website-website sebelumnya, disini juga terdapat informasi-informasi yang kita butuhkan.

www.whois.com/whois/liputan6.com

AliExpress | Booking.com | Agoda.com

Administrative Contact

Name:	On behalf of liputan6.com administrative contact
Organization:	Whois Privacy Service
Street:	P.O. Box 81226
City:	Seattle
State:	WA
Postal Code:	98108-1226
Country:	US
Phone:	+1.2065771368
Email:	admin-6714371@liputan6.com.whoisprivacyservice.org

Technical Contact

Name:	On behalf of liputan6.com technical contact
Organization:	Whois Privacy Service
Street:	P.O. Box 81226
City:	Seattle

---

www.whois.com/whois/liputan6.com

AliExpress | Booking.com | Agoda.com

Technical Contact

Name:	On behalf of liputan6.com technical contact
Organization:	Whois Privacy Service
Street:	P.O. Box 81226
City:	Seattle
State:	WA
Postal Code:	98108-1226
Country:	US
Phone:	+1.2065771368
Email:	tech-6714371@liputan6.com.whoisprivacyservice.org

Raw Whois Data

```
Domain Name: liputan6.com
Registry Domain ID: 15927627_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2018-11-18T23:44:33.293Z
Creation Date: 1999-12-23T11:02:59Z
Registrar Registration Expiration Date: 2019-12-23T11:02:59Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
```

Melalui internet archive wayback machine :

Disini kita bias melihat perubahan-perubahan yang dilakukan oleh si destination, terutama tampilan dan isi website.
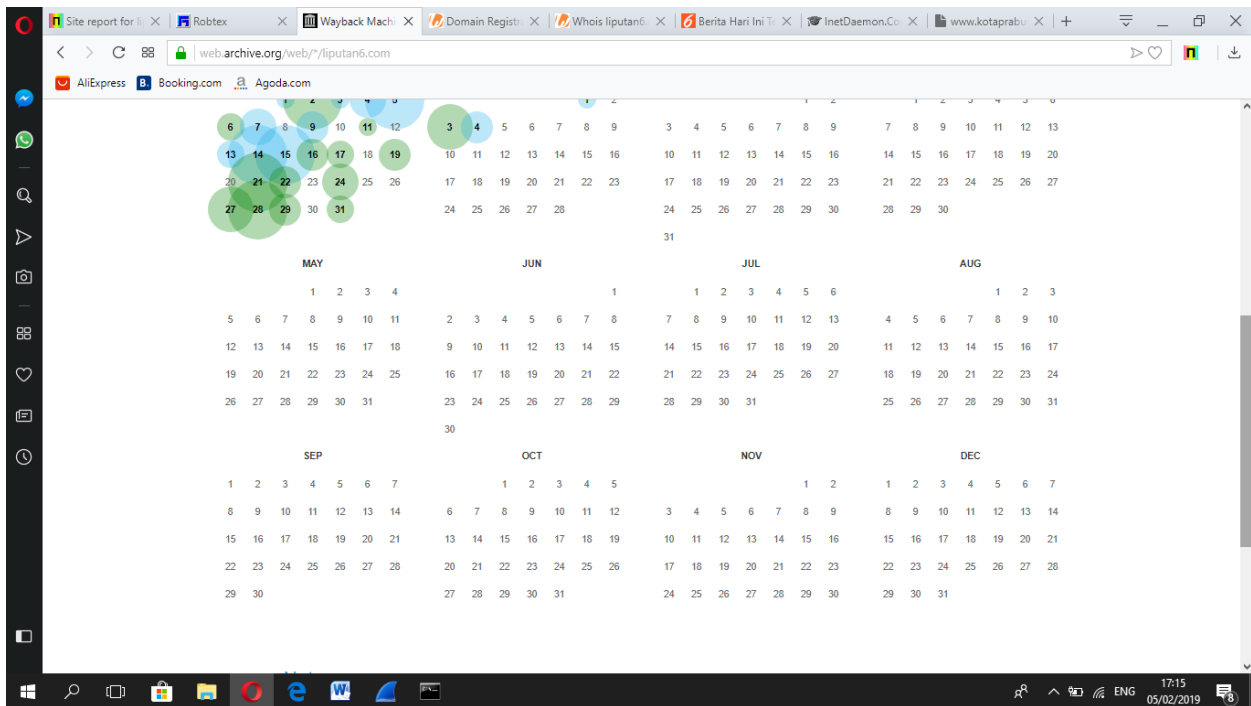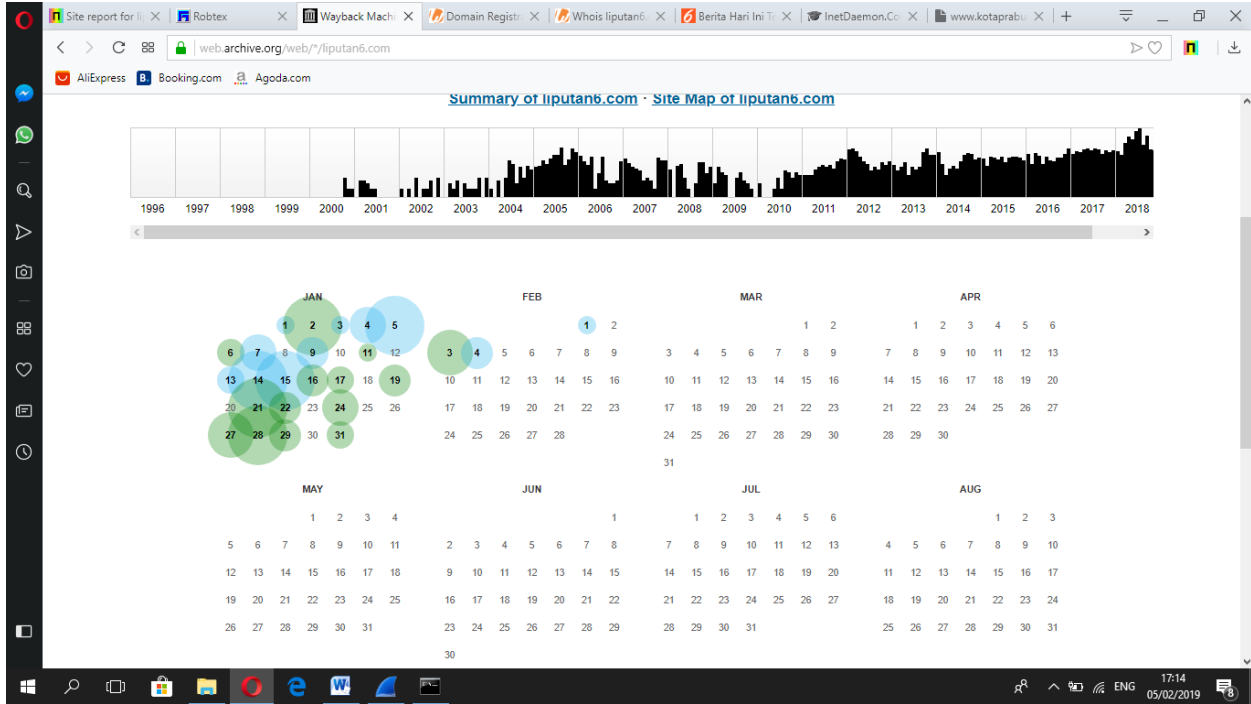
Ini merupakan contoh website liputan6.com pada 06 januari 2010
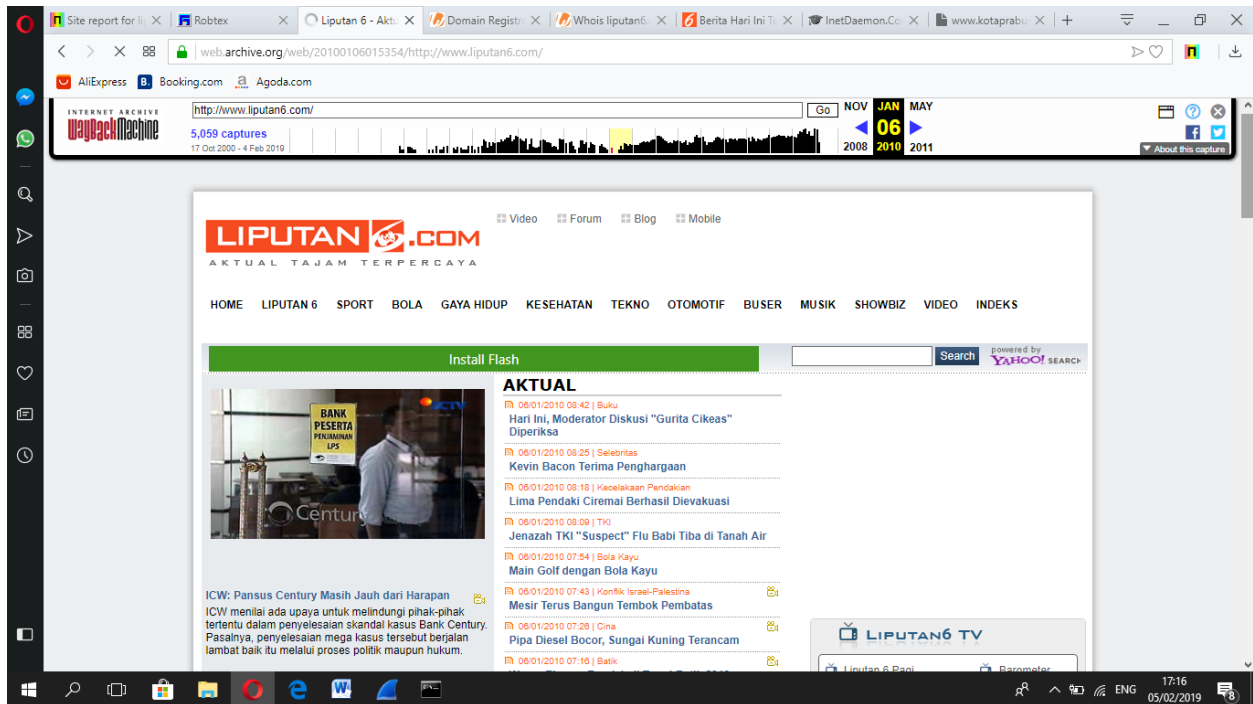
Pengecekan informasi melalui IP address yang kita dapatkan dari pencarian sebelumnya untuk website liputan6.com dengan menggunakan robtex :

1. <u>52.74.4.153</u>
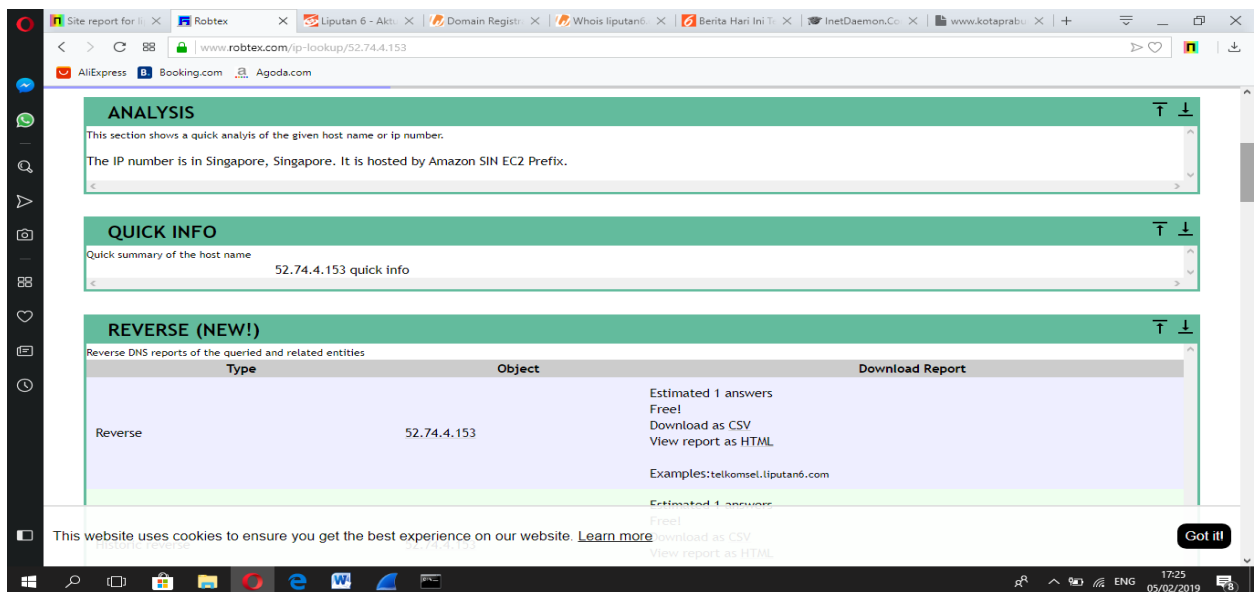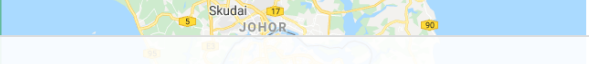
REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Type	Object	Download Report
Reverse	52.74.4.153	Estimated 1 answers Free! Download as CSV View report as HTML Examples: telkomsel.liputan6.com
Historic reverse	52.74.4.153	Estimated 1 answers Free! Download as CSV View report as HTML Examples: liputan6.com

(get credits on the dashboard)

IPINFO.IO

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

IPINFO.IO

Hostname	ec2-52-74-4-153.ap-southeast-1.compute.amazonaws.com
City	Singapore, SINGAPORE SG
Latitude/Longitude	1.2931,103.8560
Postal Code	undefined

Courtesy of ipinfo.io

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

Screenshot 1

Postal Code   undefined

Courtesy of ipinfo.io

RECORDS

Hierarchical analysis of the entity

52.74.4.153

whois	Amazon Technologies Inc. (AT-88-Z)
route	52.74.0.0/16
bgp	AS38895
asname	AMAZON-AS-AP Amazon.com Tech Telecom
descr	Amazon SIN EC2 Prefix
location	Singapore, Singapore

THREATMINER

Threat information such as virus etc

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

Screenshot 2

WHOIS

Description: Amazon Technologies Inc. (AT-88-Z)

Netname: AT-88-Z

NetRange: 52.64.0.0 - 52.79.255.255

CIDR: 52.64.0.0/12

NetName: AT-88-Z

NetHandle: NET-52-64-0-0-1

Parent: NET52 (NET-52-0-0-0-0)

NetType: Direct Allocation

OriginAS:

Organization: Amazon Technologies Inc. (AT-88-Z)

RegDate: 1991-12-19

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

127.0.0.1

whois-contacts.abusix.org
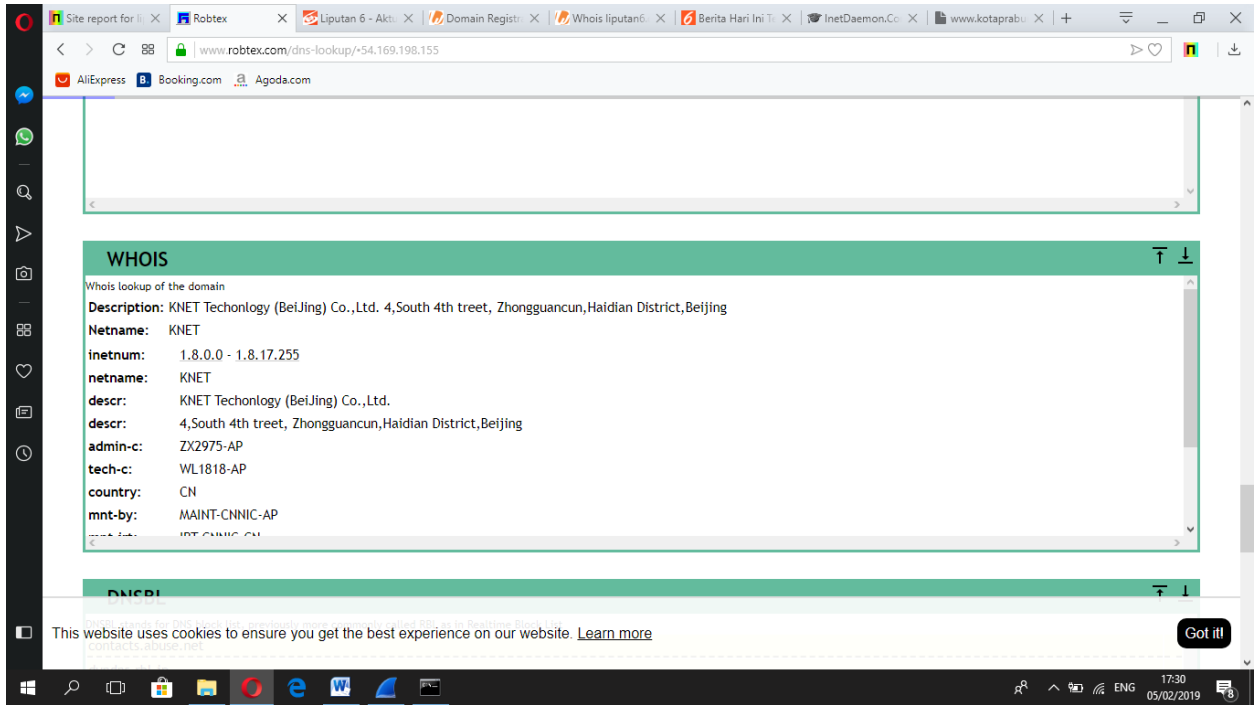
127.0.0.88

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

2. 54.169.198.155

Sama seperti IP address yang pertama tapi disini saya langsung berikan tampilan ke WHOIS Karena pada gambar diatas WHOIS tidak ada informasi yang tertera

Melalui VisualRoute :

Disini berisi informasi liputan6.com tentang analysis,Map,Route Graph, dll.

II.   3 way handshake menggunakan wireshark dan melakukan ping ke tujuan/ website destination

Pertama kita harus mengecek IP address laptop/komputermu :

Kemudian melakukan ping ke liputan6.com

II. kotaprabumulih.go.id (Government)

Melalui Website Robtex ;

Sama seperti sebelumnya disini terdapat informasi-informasi yang kita butuhkan.

Screenshot 1 (top):

Browser tabs: Whois kotaprabumulih.go | Wayback Machine | Site report for www.kotap | Robtex | +

URL: www.robtex.com/dns-lookup/www.kotaprabumulih.go.id

AliExpress | Booking.com | Agoda.com

HISTORY

Historical changes to the DNS data

Tue Feb 5 09:56:46 2019

CNAME kotaprabumulih.go.id

Mon May 22 13:54:48 2017

CNAME kotaprabumulih.go.id

Sat Sep 24 09:20:14 2016

NS   ns1.domosquare.com

WHOIS

Whois lookup of the domain

Domain ID: PANDI-DO53545

Domain Name: KOTAPRABUMULIH.GO.ID

Last Updated On: 21-Jan-2018 09:27:19 UTC

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

18:31 05/02/2019

Screenshot 2 (bottom):

Browser tabs: Whois kotaprabumulih.go | Wayback Machine | Site report for www.kotap | Robtex | +

URL: www.robtex.com/dns-lookup/www.kotaprabumulih.go.id

AliExpress | Booking.com | Agoda.com

NS   ns1.domosquare.com

WHOIS

Whois lookup of the domain

Domain ID: PANDI-DO53545
Domain Name: KOTAPRABUMULIH.GO.ID
Created On: 10-May-2000 13:23:33 UTC
Last Updated On: 21-Jan-2018 09:27:19 UTC
Expiration Date: 31-Jan-2020 23:59:59 UTC
Status: ok

    ==

Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar Street1:   Jl. Medan Merdeka Barat No. 9

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

postmaster.rfc-clueless.org   127.0.0.3

contacts.abuse.net

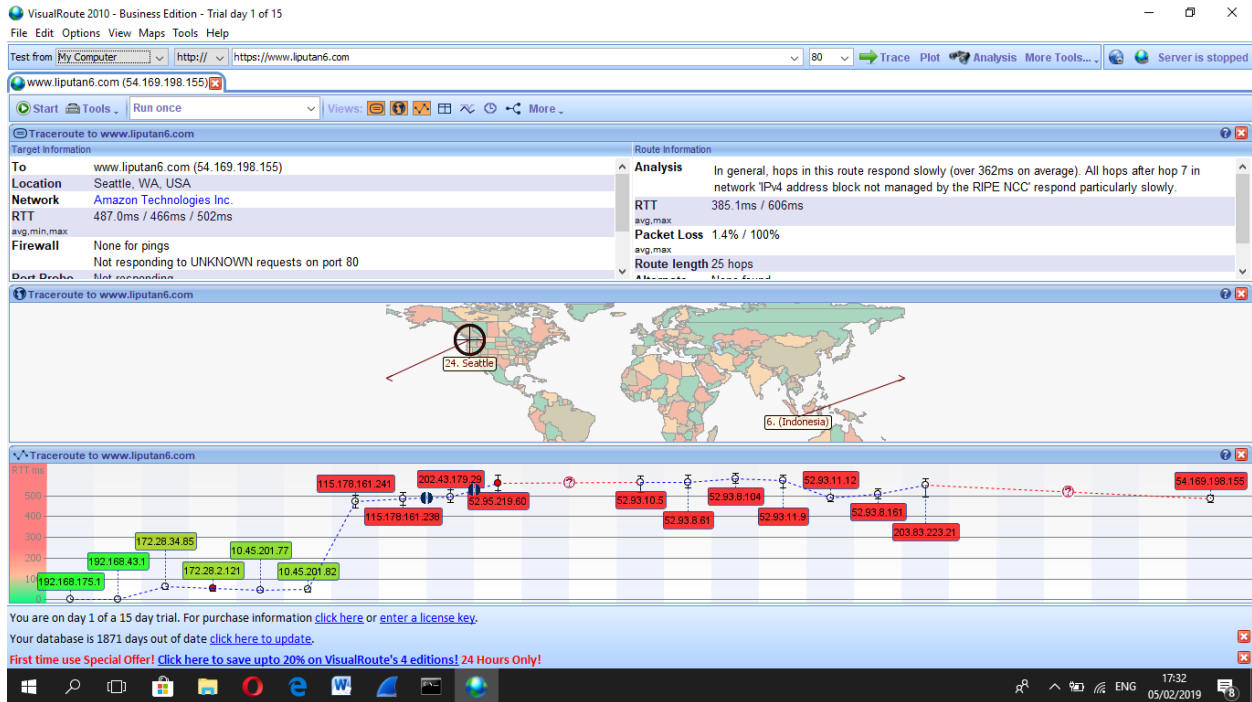This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

ex.dnsbl.org

18:31 05/02/2019

Melalui website netraft :
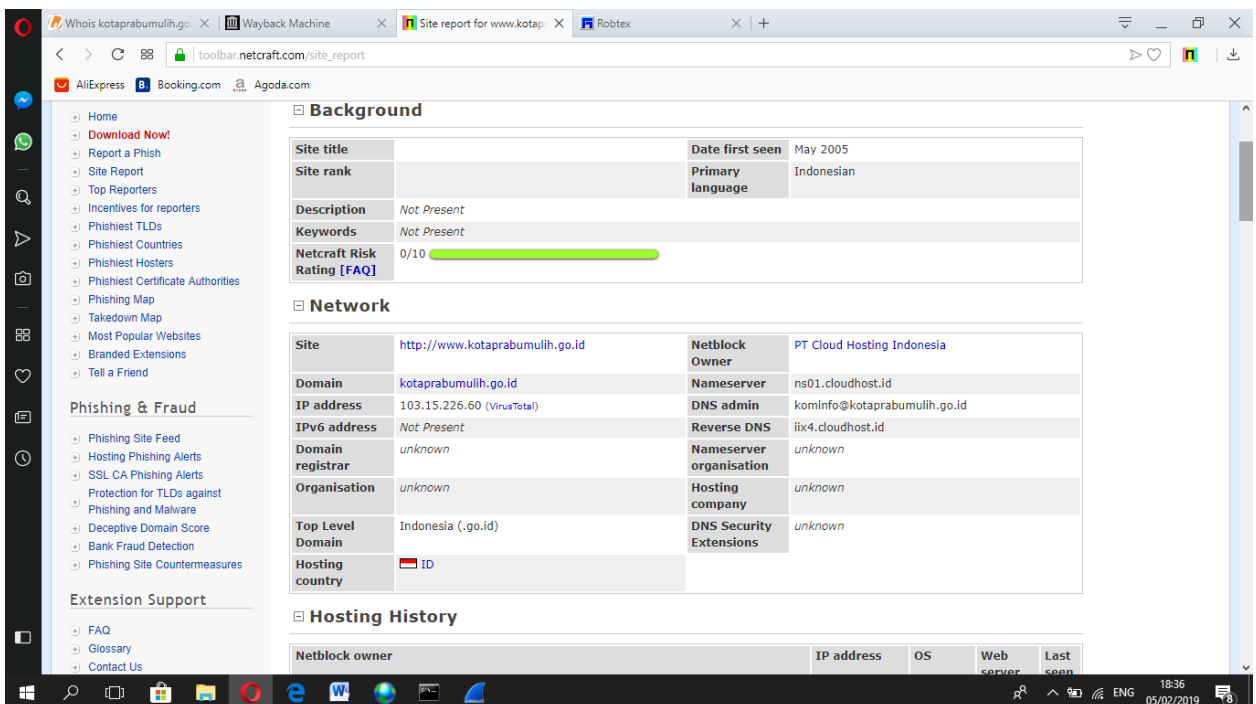
Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

- Netcraft Home
- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Cloud Hosting Indonesia Corporate / Direct Member IDNIC Pinus Raya Reni Jaya AG-1 No.01 Pamulang Barat, Pamulang Tangerang Selatan, Banten	103.15.226.60	Linux	LiteSpeed	5-Nov-2018
Ronny Isdhianto Lebak Indah Jaya I No. 15 Surabaya OT ID 60134	67.228.98.196	Linux	LiteSpeed	29-Mar-2016
Internet Service Provider Jl. Jakarta No.5 Ulak Karang Padang Sumatra Barat 2513	119.2.71.99	Linux	Apache	27-Jun-2012
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	203.130.196.40	Windows Server 2003	Microsoft-IIS/6.0	28-Nov-2011
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	-	Microsoft-IIS/5.0	7-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	5-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	Microsoft-IIS/5.0	2-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	1-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows	Microsoft-	28-

---

PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	5-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	Microsoft-IIS/5.0	2-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	1-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	Microsoft-IIS/5.0	28-Mar-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	26-Mar-2005

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Qualifier	Mechanism	Argument
+ (Pass)	a	
+ (Pass)	mx	
+ (Pass)	ip4	103.15.226.60
~ (SoftFail)	all	

Modifiers extend the functionality of SPF records. The most common one is the redirect which indicates another host contains the SPF record being searched for.

Modifier	Argument

Melalui website whois :

5. Melalui website internet archive wayback machine

Kita juga bisa mengakses isi website pada tahun-tahun
sebelumnya seperti pada gambar pada 03 maret 2011
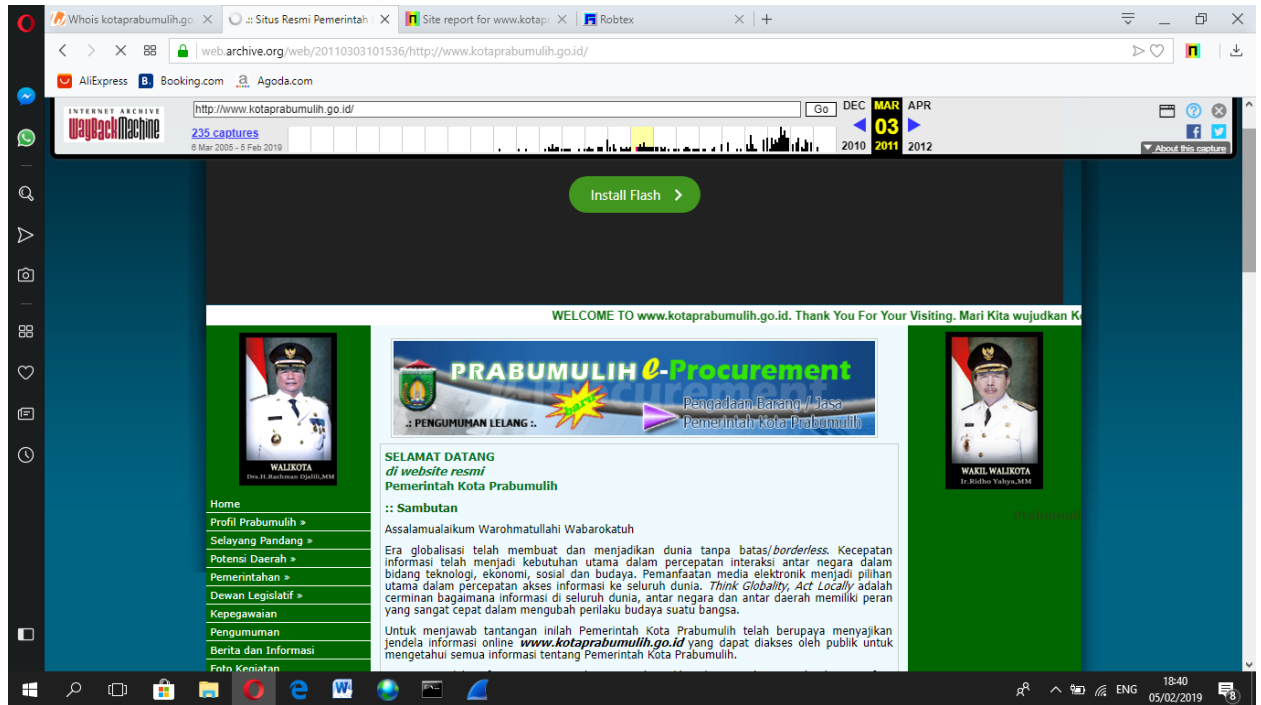
Pengecekan informasi melalui IP address yang kita dapatkan dari pencarian
sebelumnya untuk website kotaprabumulih.go.id dengan menggunakan robtex :
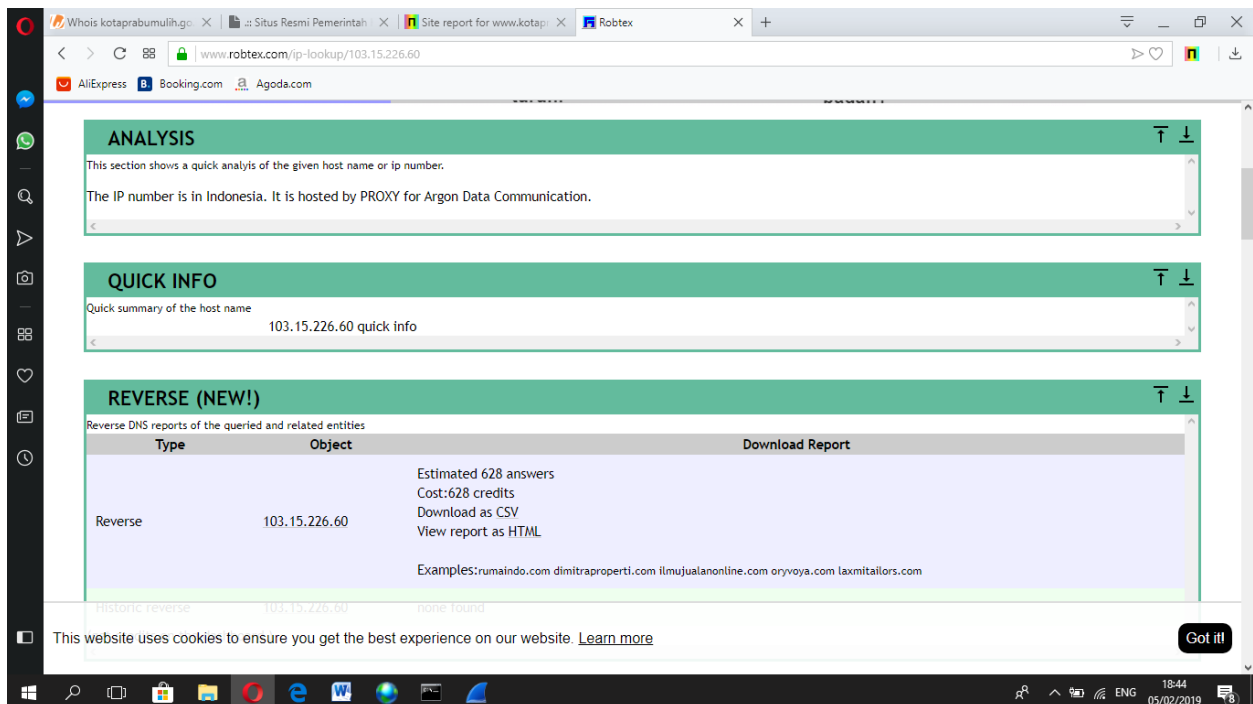
Window 1 (top)

IPINFO.IO

Hostname	iix4.cloudhost.id
City	, ID
Latitude/Longitude	-6.1750,106.8290
Postal Code	undefined

Courtesy of ipinfo.io

RECORDS

103.15.226.60

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

Window 2 (bottom)

RECORDS

Hierarchical analysis of the entity

103.15.226.60

whois	PT Cloud Hosting Indonesia Corporate / Direct Member IDNIC Pinus Raya Reni Jaya AG-1 No.01 Pamulang Barat, Pamulang Tangerang Selatan, Banten
route	103.15.226.0/24
bgp	AS136052
asname	IDNIC-IDCLOUDHOST-AS-ID PT Cloud Hosting
descr	PROXY for Argon Data Communication
location	Indonesia

THREATMINER

Threat information such as virus etc
Source: Threatminer

SHARED

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

HISTORY

Historical changes to the DNS data

Tue Feb 5 11:42:58 2019

PTR iix4.cloudhost.id

Mon Jul 30 08:10:08 2018

PTR iix4.cloudhost.id

WHOIS

Whois lookup of the domain

Description: PT Cloud Hosting Indonesia Corporate / Direct Member IDNIC Pinus Raya Reni Jaya AG-1 No.01 Pamulang Barat, Pamulang Tangerang Selatan, Banten

Netname: IDNIC-IDCLOUDHOST-ID

netname: IDNIC-IDCLOUDHOST-ID

WHOIS

Whois lookup of the domain

Description: PT Cloud Hosting Indonesia Corporate / Direct Member IDNIC Pinus Raya Reni Jaya AG-1 No.01 Pamulang Barat, Pamulang Tangerang Selatan, Banten

Netname:	IDNIC-IDCLOUDHOST-ID
inetnum:	103.15.226.0 - 103.15.226.255
netname:	IDNIC-IDCLOUDHOST-ID
descr:	PT Cloud Hosting Indonesia
descr:	Corporate / Direct Member IDNIC
descr:	Pinus Raya Reni Jaya AG-1 No.01
descr:	Pamulang Barat, Pamulang
descr:	Tangerang Selatan, Banten
admin-c:	APS20-AP

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

abuse-contacts.abusix.org   127.0.0.1
admin\@idcloudhost.com

all.ascc.dnsbl.bit.nl   127.0.0.78
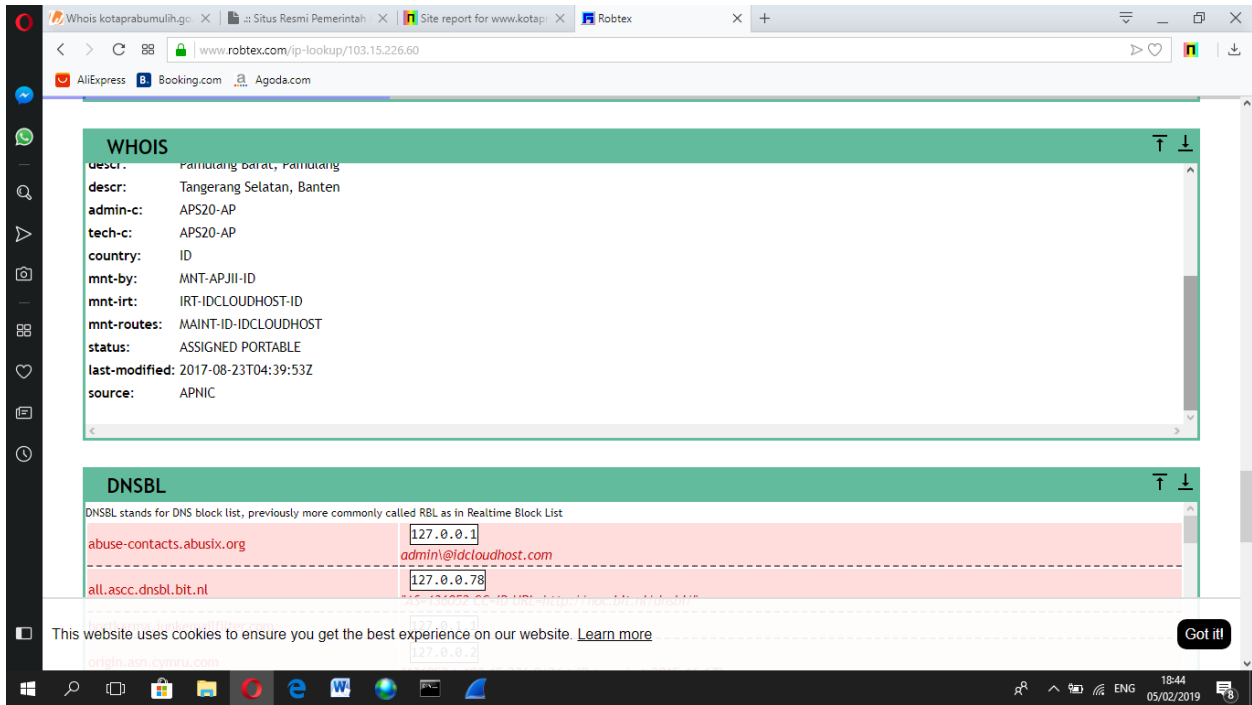
Melalui VisualRoute :

Disini berisi informasi kotaprabumulih.go.id tentang analysis,Map,Route Graph, dll.
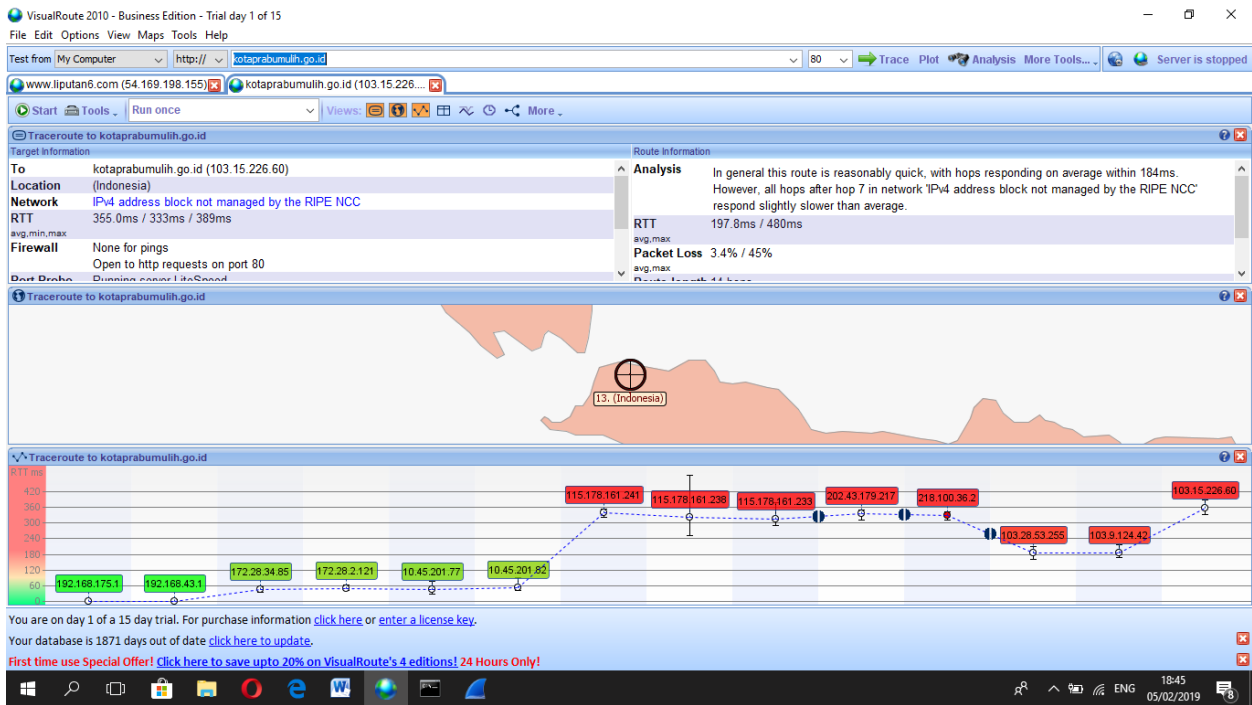
I.   3 way handshake menggunakan wireshark dan melakukan ping ke tujuan/ website destination

Pertama kita harus mengecek IP address laptop/komputermu :
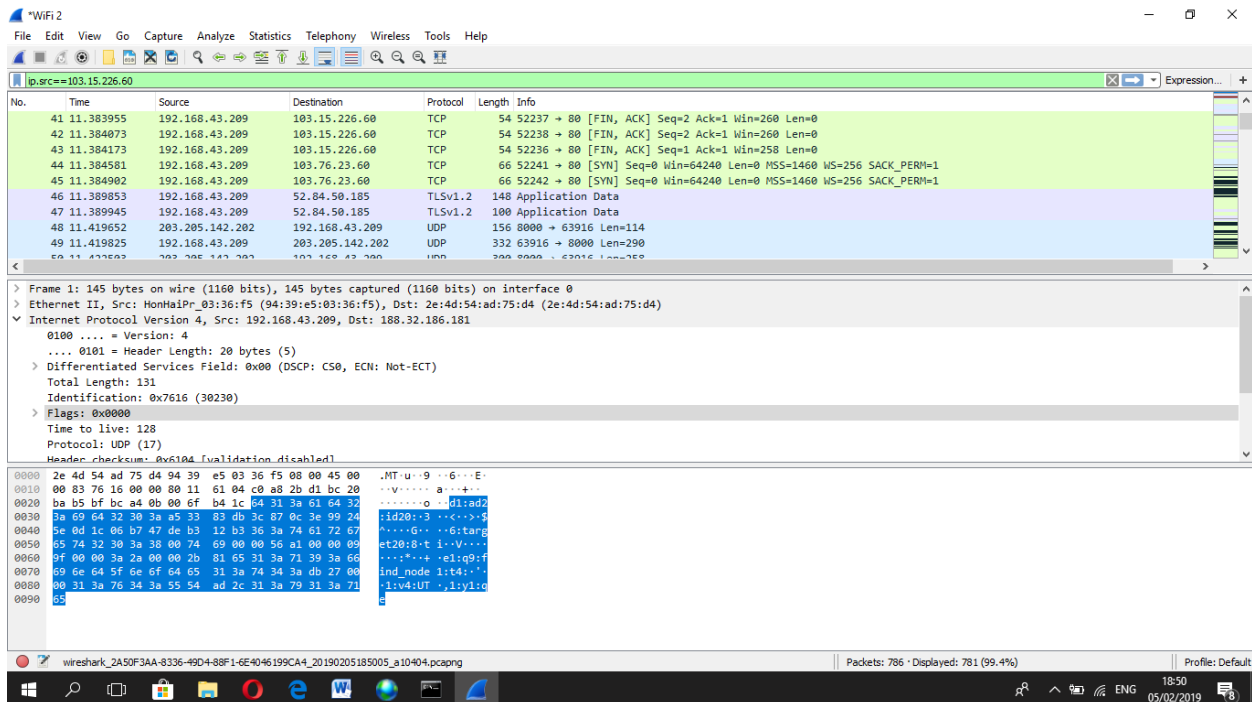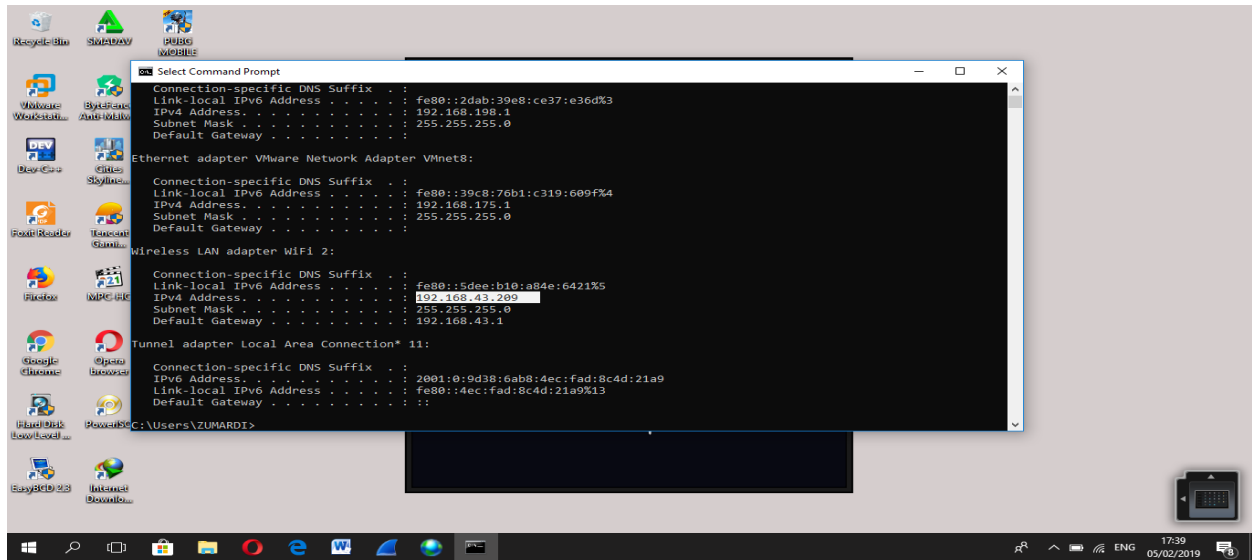
Kemudian melakukan ping ke kotaprabumulih.go.id
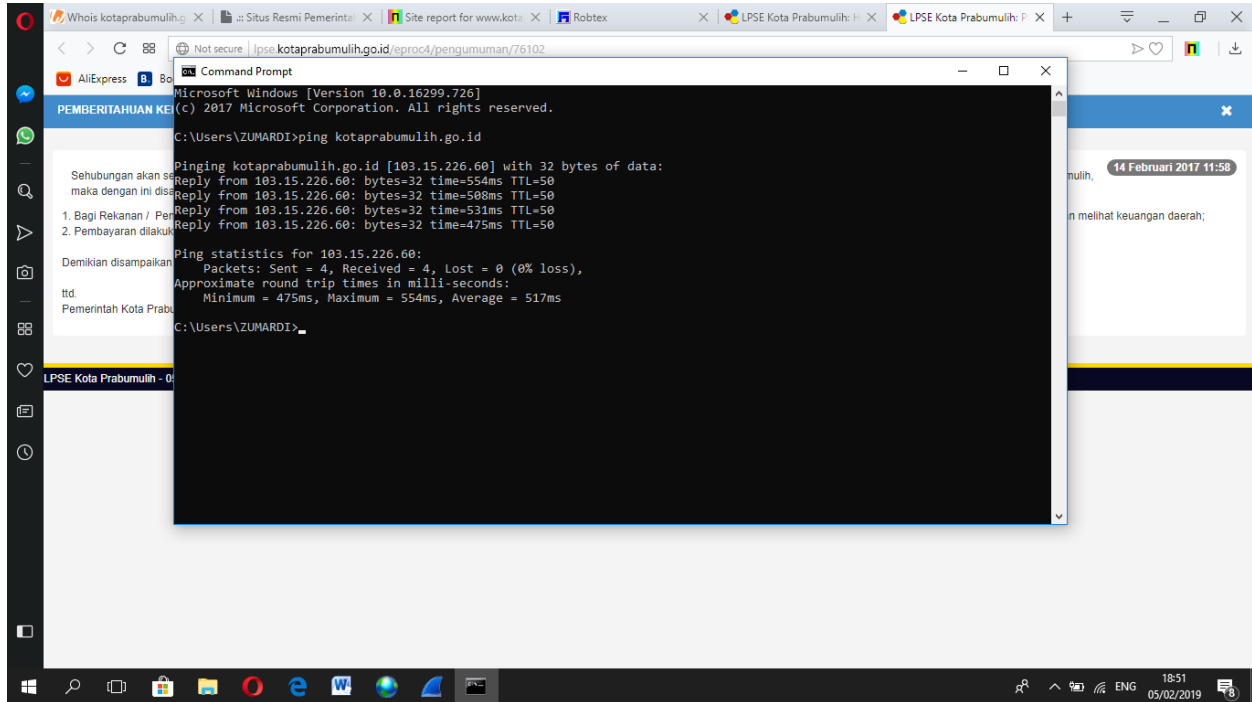
III.   https://www.inetdaemon.com (Luar Negeri)

Melalui Website Robtex
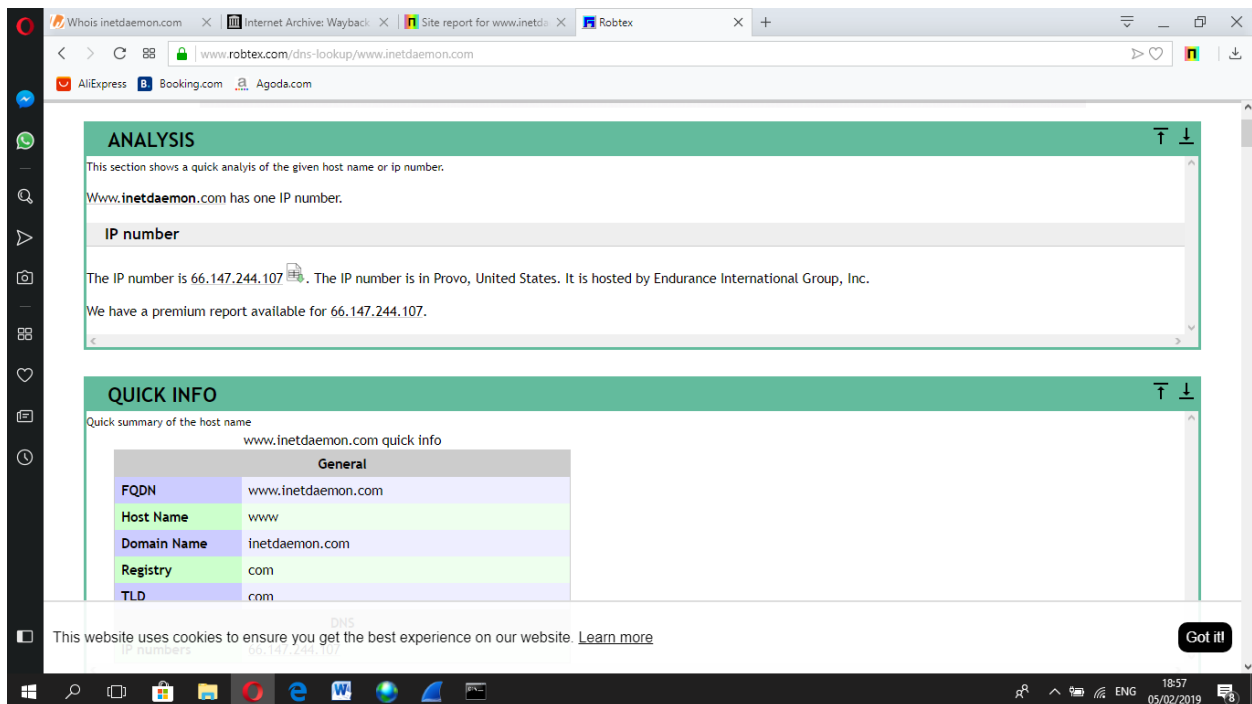
QUICK INFO

Quick summary of the host name

www.inetdaemon.com quick info

General	
FQDN	www.inetdaemon.com
Host Name	www
Domain Name	inetdaemon.com
Registry	com
TLD	com
DNS	
IP numbers	66.147.244.107

REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Type	Object		Download Report
Reverse	www.inetdaemon.com	none found	
Historic reverse	www.inetdaemon.com	none found	

Estimated 5398 answers

Got it!

This website uses cookies to ensure you get the best experience on our website. Learn more

---

REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Type	Object		Download Report
Reverse	www.inetdaemon.com	none found	
Historic reverse	www.inetdaemon.com	none found	
Reverse	66.147.244.107	Estimated 5398 answers Cost:5398 credits Download as CSV View report as HTML Examples:kabbalatorah.com mail.missnailsdecatur.com mail.detskjerioslo.ru berkeleycrossroads.com flyledlighting.com	

(get credits on the dashboard)

RECORDS

Hierarchical analysis of the entity

www.inetdaemon.com

a 66.147.244.107

whois Unified Layer (BLUEH-2)

route 66.147.240.0/20

AS46606

Got it!

This website uses cookies to ensure you get the best experience on our website. Learn more

www.robtex.com/dns-lookup/www.inetdaemon.com

AliExpress B. Booking.com a. Agoda.com

Examples: kabbalatorah.com mail.missnailsdecatur.com mail.detskjerioslo.ru berkeleycrossroads.com flyledlighting.com

(get credits on the dashboard)

RECORDS

Hierarchical analysis of the entity

www.**inetdaemon**.com

a 66.147.244.107

whois Unified Layer (BLUEH-2)

route 66.147.240.0/20

bgp AS46606

asname EIGI Endurance International Group, Inc

descr Endurance International Group, Inc

location Provo, United States

UD **inetdaemon** com

SEO

Search Engine Optimization information

inetdaemon.com SEO data

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

Ranked as #954375 according to Cisco Umbrella

---

www.robtex.com/dns-lookup/www.inetdaemon.com

AliExpress B. Booking.com a. Agoda.com

HISTORY

Historical changes to the DNS data

Tue Feb 5 05:08:44 2019

A 66.147.244.107

Wed May 27 23:42:40 2015

A 66.147.244.107

WHOIS

Whois lookup of the domain

Domain Name:	INETDAEMON.COM
Registry Domain ID:	6594336_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.fastdomain.com
Registrar URL:	http://www.fastdomain.com
Updated Date:	2017-04-01T07:31:48Z
Creation Date:	1999-05-18T23:05:51Z
Registrar:	FastDomain Inc.

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

WHOIS

Whois lookup of the domain

Domain Name:	INETDAEMON.COM
Registry Domain ID:	6594336_DOMAIN_COM-VRSN
Registrar WHOIS Server:	whois.fastdomain.com
Registrar URL:	http://www.fastdomain.com
Updated Date:	2017-04-01T07:31:48Z
Creation Date:	1999-05-18T23:05:51Z
Registry Expiry Date:	2019-05-18T23:06:27Z
Registrar:	FastDomain Inc.
Registrar IANA ID:	1154
Registrar Abuse Contact Email:	
Registrar Abuse Contact Phone:	

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

dyndns.rbl.jp

WHOIS

Registrar IANA ID:	1154
Registrar Abuse Contact Email:	
Registrar Abuse Contact Phone:	
Domain Status:	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server:	NS1.BLUEHOST.COM
Name Server:	NS2.BLUEHOST.COM
DNSSEC:	unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2019-02-05T05:11:20Z <<<

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

This website uses cookies to ensure you get the best experience on our website. Learn more   Got it!

dyndns.rbl.jp

Melalui netcraft :

Heartbleed revocation

All certificates affected by the Heartbleed vulnerability have been revoked.

Serial	Common Name(s)	Normally Expires	CRL revocation status	Chrome CRLSet revocation status
0x19bb4ed1d33830ab915565ce1d3aead2	*.bluehost.com	2020-02-18	revoked on 2017-08-17 11:08:29	not revoked

Revocation information last updated 2019-02-04 18:00 GMT.

Assurance	Domain validation			
Organisation	Not Present		Common name	inetdaemon.com
State	Not Present		Country	Not Present
Organisational unit	Not Present		Subject Alternative Name	inetdaemon.com, inetdaemon.net, inetdaemon.org, mail.inetdaemon.net, mail.inetdaemon.org, www.inetdaemon.com, www.inetdaemon.net, www.inetdaemon.org
Validity period	From Dec 15 2018 to Mar 15 2019 (3 months)		Matches hostname	Yes
Server	nginx/1.14.1		Public key algorithm	rsaEncryption
Protocol version	TLSv1.2		Public key length	2048
Certificate check	ok		Signature algorithm	sha256WithRSAEncryption
Serial number	0x03ee40e3c87df48929d4556a174081d395f8		Cipher	ECDHE-RSA-AES128-GCM-SHA256
Version number	0x02		Perfect Forward Secrecy	Yes
Next Protocol Negotiation	h2,http/1.1		Supported TLS Extensions	RFC5746 renegotiation info, RFC4366 server name, RFC4492 EC point formats, RFC5077 session ticket, Next Protocol Negotiation, unknown

---

Certificate check	ok		Signature algorithm	sha256WithRSAEncryption
Serial number	0x03ee40e3c87df48929d4556a174081d395f8		Cipher	ECDHE-RSA-AES128-GCM-SHA256
Version number	0x02		Perfect Forward Secrecy	Yes
Next Protocol Negotiation	h2,http/1.1		Supported TLS Extensions	RFC5746 renegotiation info, RFC4366 server name, RFC4492 EC point formats, RFC5077 session ticket, Next Protocol Negotiation, unknown
Issuing organisation	Let's Encrypt		Issuer common name	Let's Encrypt Authority X3
Issuer unit	Not Present		Issuer location	Not Present
Issuer country	US		Issuer state	Not Present
Certificate Revocation Lists	Not Present		Certificate Hash	Nh0e0Q2fh9UOLM7j60p9zNBz5Qo
Public Key Hash	82754d2fd4d54c7e2d6a057a293946d415defd76aa2cbeed88f5aab506a715cf			
OCSP servers	http://ocsp.int-x3.letsencrypt.org - 100% uptime in the past 24 hours			
OCSP stapling response	No response received			

Certificate transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Cloudflare Nimbus 2019 dH7ag2GtMxCRIZzdU9CcMK//V5CIAjGNzV55hB7zFY=	2018-12-15 13:10:12	Success
Certificate	Google Argon 2019 Y/Lbzeg7zCzPC3KE31drMGSNYXePvXWmOLHHWfRL2I0=	2018-12-15 13:10:12	Success

⊞ SSL Certificate Chain

Melalui whois :

Registrant Contact

Name:	DOMAIN PRIVACY SERVICE FBO REGISTRANT
Organization:	THE ENDURANCE INTERNATIONAL GROUP, INC.
Street:	10 CORPORATE DR, STE 300
City:	BURLINGTON
State:	MASSACHUSETTS
Postal Code:	01803
Country:	US
Phone:	+1.8017659400
Email:	WHOIS@BLUEHOST.COM

Administrative Contact

Name:	DOMAIN PRIVACY SERVICE FBO REGISTRANT
Organization:	THE ENDURANCE INTERNATIONAL GROUP, INC.
Street:	10 CORPORATE DR, STE 300
City:	BURLINGTON

Administrative Contact

Name:	DOMAIN PRIVACY SERVICE FBO REGISTRANT
Organization:	THE ENDURANCE INTERNATIONAL GROUP, INC.
Street:	10 CORPORATE DR, STE 300
City:	BURLINGTON
State:	MASSACHUSETTS
Postal Code:	01803
Country:	US
Phone:	+1.8017659400
Email:	WHOIS@BLUEHOST.COM

Technical Contact

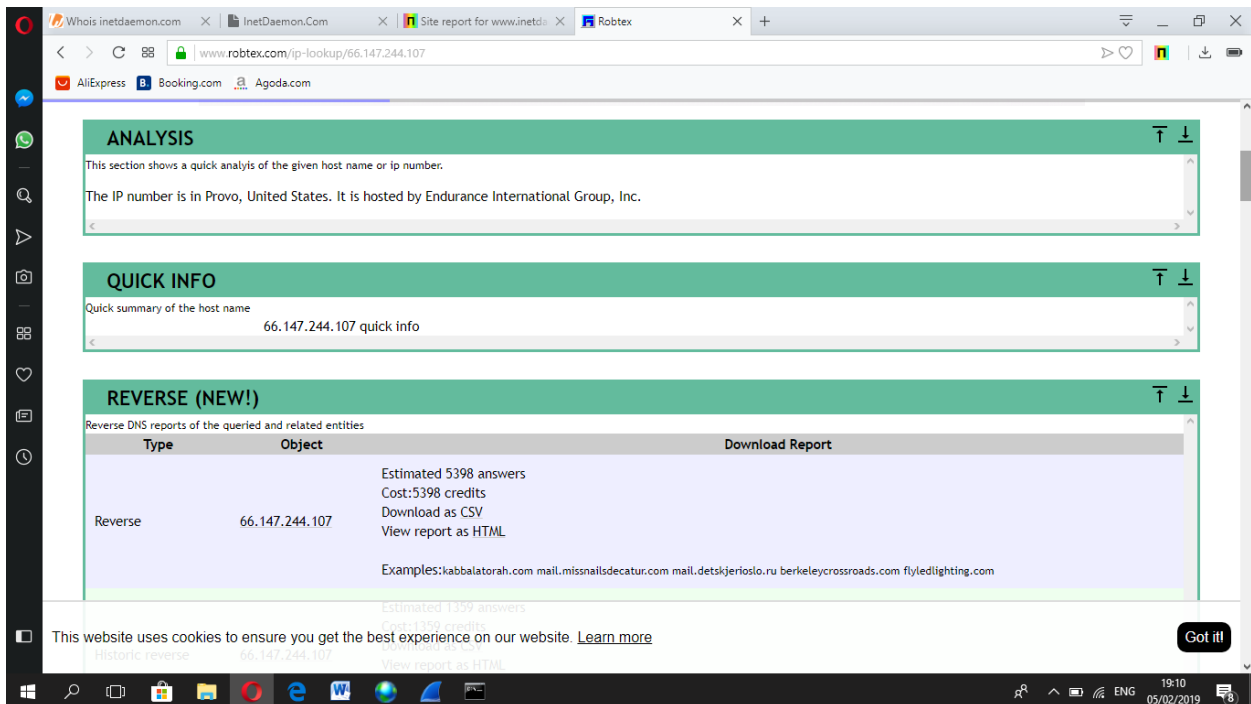|	
Name:	DOMAIN PRIVACY SERVICE FBO REGISTRANT
Organization:	THE ENDURANCE INTERNATIONAL GROUP, INC.
Street:	10 CORPORATE DR, STE 300
City:	BURLINGTON
State:	MASSACHUSETTS

Melalui internet archive wayback machine

Akses pada website di tanggal 02 maret 2008

Pengecekan informasi melalui IP address yang kita dapatkan dari pencarian sebelumnya untuk website https://www.inetdaemon.com dengan menggunakan robtex :

REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Type	Object	Download Report
Reverse	66.147.244.107	Estimated 5398 answers Cost:5398 credits Download as CSV View report as HTML Examples:kabbalatorah.com mail.missnailsdecatur.com mail.detskjerioslo.ru berkeleycrossroads.com flyledlighting.com
Historic reverse	66.147.244.107	Estimated 1359 answers Cost:1359 credits Download as CSV View report as HTML Examples:mail.pic-world.com mail.luvthisone.com trueoyoufood.com mail.aetherchem.com mail.astonlowery.com

(get credits on the dashboard)

IPINFO.IO

IPINFO.IO

Hostname	box807.bluehost.com
City	Provo, Utah US
Latitude/Longitude	40.2347,-111.6450
Postal Code	84606

Courtesy of ipinfo.io

RECORDS

Hierarchical analysis of the entity

66.147.244.107

whois	Unified Layer (BLUEH-2)
route	66.147.240.0/20
bgp	AS46606
asname	EIGI Endurance International Group, Inc
descr	Endurance International Group, Inc
location	Provo, United States

THREATMINER

Threat information such as virus etc

URI

Last Seen	URL
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in

---

THREATMINER

Threat information such as virus etc

URI

Last Seen	URL
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/e5389720b2d85fda1f932dd26d9da71e/
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/mgen/f1e968935737a006b9b31a2787bf4b515/
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/MGen/F1e968935737a006b9b31a2787bf4b515
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/MGen/F96080ab407aff8af16651b53eaf17817/
2016-07-29 13:36:54	http://thepainpros.com/include/database/pgsql/service/home/sign-in/MGen/F96080ab407aff8af16651b53eaf17817? dispatch=fv2RXf9W5AMZwbMBLMvAgrqw6Taa.JLfZblQey0bDBYD89pJVbI

HISTORY

Historical changes to the DNS data

Tue Feb 5 12:10:02 2019

PTR box807.bluehost.com

Thu Aug 13 15:46:34 2015

PTR box807.bluehost.com

WHOIS

Whois lookup of the domain

Description:

Netname: UL-66.147.244.107/32

network: Class-Name:network

WHOIS

Whois lookup of the domain

Description:

Netname: UL-66.147.244.107/32

%rwhois V-1.5: 000080:00 rwhois.unifiedlayer.com (by Unified Layer, V-1.0.0)

network: Class-Name:network

network: ID: NETBLK-UL.66.147.244.107/32

network: Auth-Area: 66.147.244.107/32

network: Network-Name: UL-66.147.244.107/32

network: IP-Network: 66.147.244.107/32

network: Organization: publicschoolsfirstnc.org

network: Tech-Contact: ybrannon@gmail.com

DNSBL

DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

abuse-contacts.abusix.org

127.0.0.1

abuse\@bluehost.com

127.0.0.3

Melalui VisualRoute :

Disini berisi informasi https://www.inetdaemon.com tentang analysis,Map,Route Graph, dll.

3 way handshake menggunakan wireshark dan melakukan ping ke tujuan/ website destination

Pertama kita harus mengecek IP address laptop/komputermu :

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

Kesimpulan :

Dengan menggunakan beberapa website yang telah disebutkan sebelumnya, maka bisa dikatakan kita telah mengumpulkan informasi mengenai website yang akan kita jadikan destination.