TUGAS KEAMANAN JARINGAN KOMPUTER

“ ANALISA RECONNAISSANCE PADA LAZADA ”

NAMA : DESY MARITA

NIM : 09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

Untuk mengambil contoh situs yang mengusung sistem belanja online atau E-commerce, saya mengambil contoh situs belanja online yang sudah cukup terkenal di Indonesia, yaitu Lazada. Lazada.co.id adalah salah satu toko online terbaik tanah air yang hadir dengan konsep produk yang lengkap dan kemudahan belanja online pesan antar. Adalah sebuah perjalanan yang menabjubkan bagi Lazada.co.id dan orang-orang dibelakanganya yang membuat Lazada menjadi besar seperti sekarang. Lazada.co.id dapat juga disebut dengan toko online adalah sistem penjualan dengan menggunakan jasa internet, berbasis web dan dapat bertransaksi dengan online tanpa adanya tatap muka antara pembeli dan penjual. Ini tentu saja memudahkan para pembeli yang berasal dari daerah yang jauh untuk melakukan transaksi dengan harga yang normal. Tentu saja daerah si pembeli yang jauh akan mempengaruhi lama tidaknya barang yang dibeli sampai ke pembeli tersebut.

Promosi yang dilakukan lazada, tidak hanya melalui situs lazada.co.id, tetapi juga lazada melakukan kegiatan publikasi melalui media seperti :

> Facebook (dengan nama ID Lazada.co.id)

> Twitter (dengan nama ID @LazadaID)

> Linkedln (dengan nama ID Lazada Indonesia)

> Google+ (dengan nama ID Lazada Indonesia)

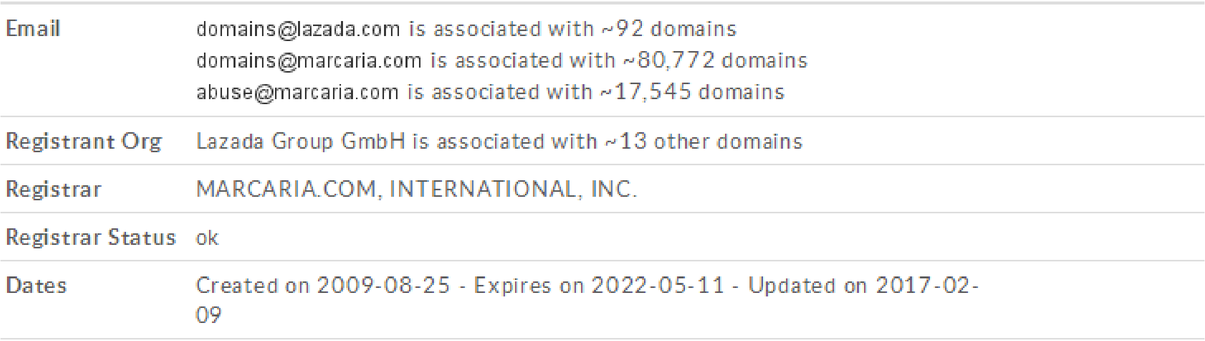
> Youtube (dengan nama ID LazadaID)

> Pinterest (dengan nama ID LazadaID)

> Blog (dengan alamat www.blog.lazada.co.id)

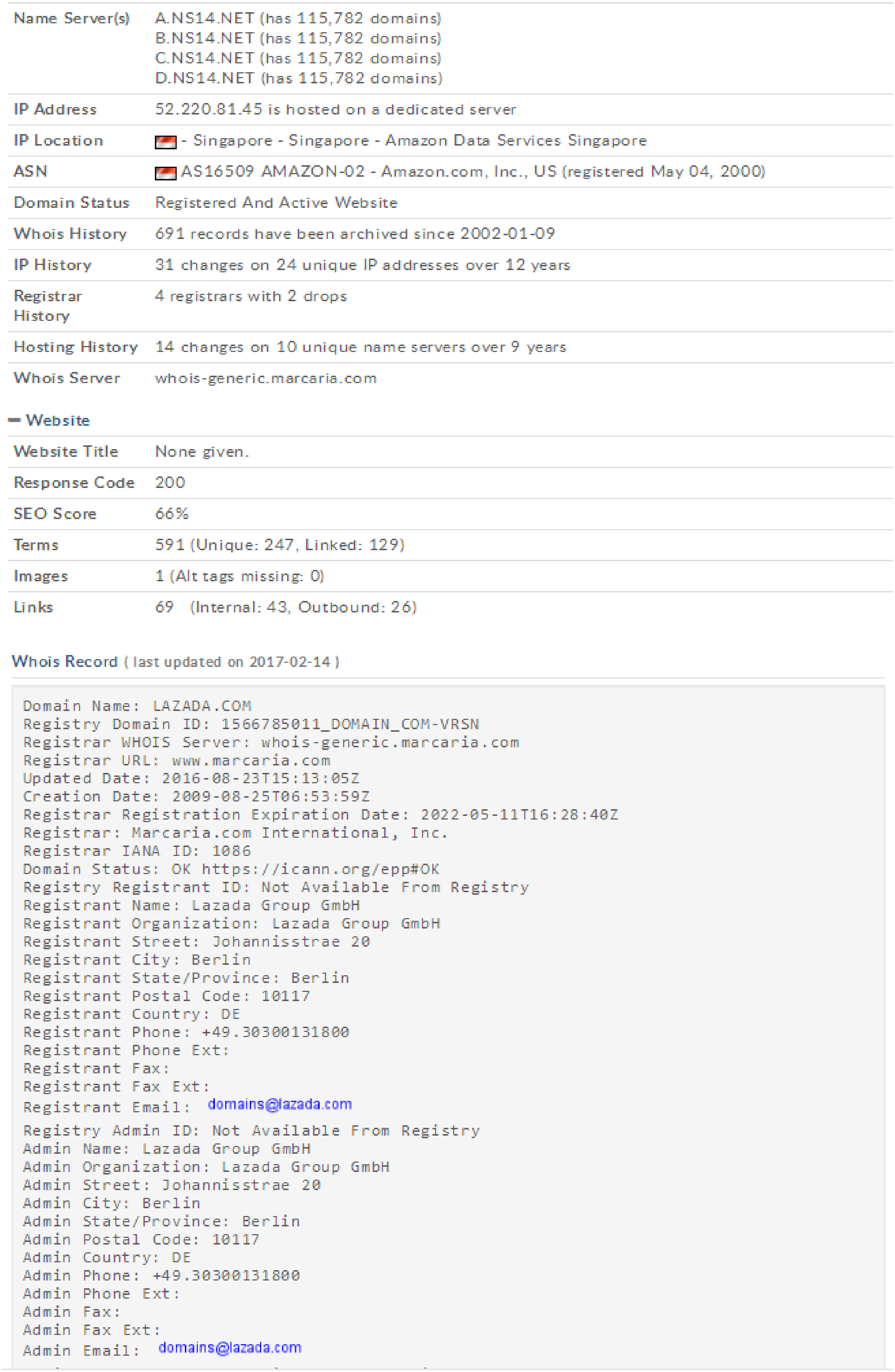
Lazada.co.id menjamin keamanan pelanggan dalam melakukan transaksi melalui website yang digunakan pada halaman checkout dan setelah login. Enskripsi yang digunakan adalah High-Grade encryption (TLS_ECDHE_RSA_WITH_RC4_128_SHA, 128 bit keys), dengan begitu semua data informasi pelanggan akan dienkripsi dan terjamin keamananya.

Berikut adalah capture reconnaissance yang dilakukan pada Lazada.co.id :



Email	domains@lazada.com is associated with ~92 domains domains@marcaria.com is associated with ~80,772 domains abuse@marcaria.com is associated with ~17,545 domains
Registrant Org	Lazada Group GmbH is associated with ~13 other domains
Registrar	MARCARIA.COM, INTERNATIONAL, INC.
Registrar Status	ok
Dates	Created on 2009-08-25 - Expires on 2022-05-11 - Updated on 2017-02-09

Dapat dilihat pada gambar diatas terdapat 3 domain pada Lazada.



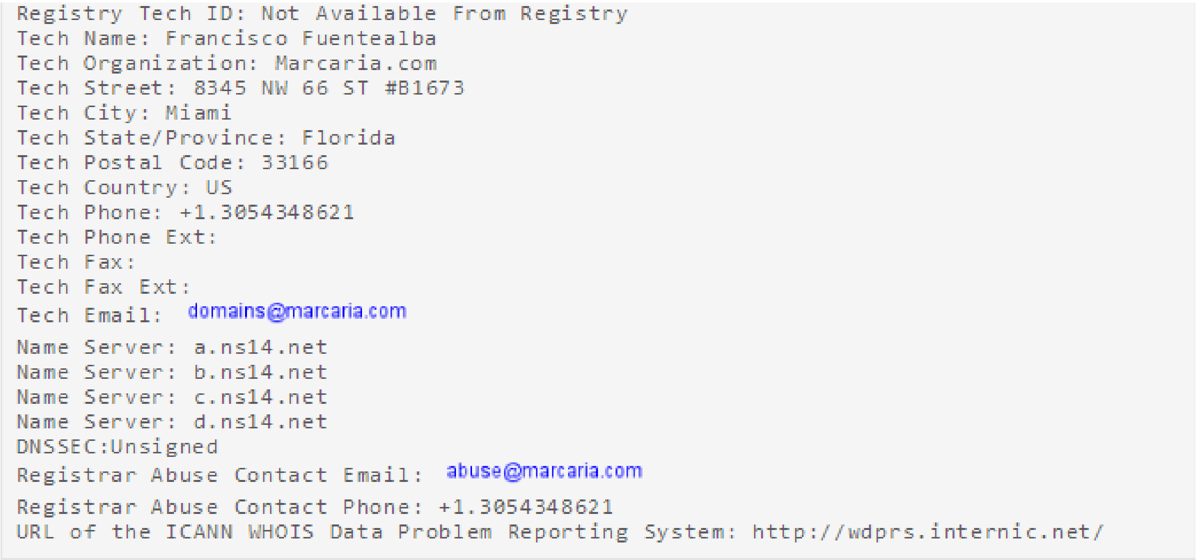
Name Server(s)	A.NS14.NET (has 115,782 domains) B.NS14.NET (has 115,782 domains) C.NS14.NET (has 115,782 domains) D.NS14.NET (has 115,782 domains)
IP Address	52.220.81.45 is hosted on a dedicated server
IP Location	- Singapore - Singapore - Amazon Data Services Singapore
ASN	AS16509 AMAZON-02 - Amazon.com, Inc., US (registered May 04, 2000)
Domain Status	Registered And Active Website
Whois History	691 records have been archived since 2002-01-09
IP History	31 changes on 24 unique IP addresses over 12 years
Registrar History	4 registrars with 2 drops
Hosting History	14 changes on 10 unique name servers over 9 years
Whois Server	whois-generic.marcaria.com

− Website

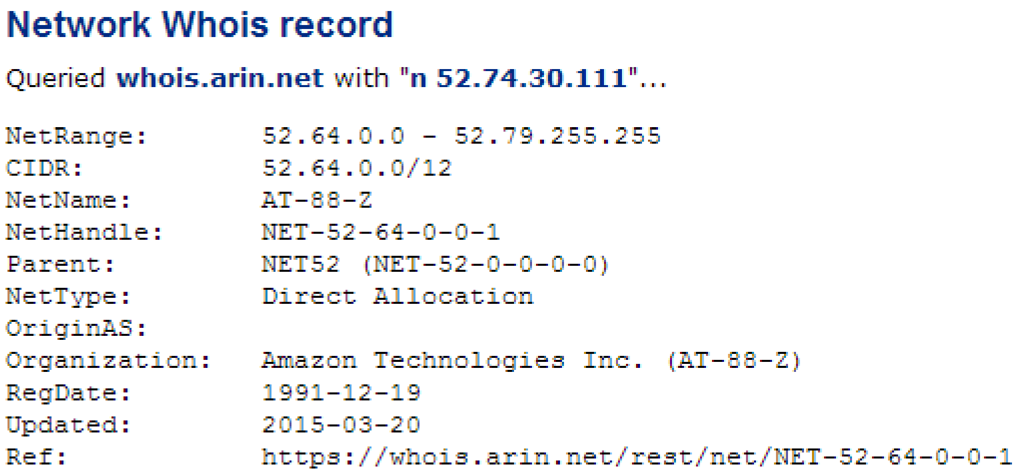
Website Title	None given.
Response Code	200
SEO Score	66%
Terms	591 (Unique: 247, Linked: 129)
Images	1 (Alt tags missing: 0)
Links	69 (Internal: 43, Outbound: 26)

Whois Record (last updated on 2017-02-14)

```
Domain Name: LAZADA.COM
Registry Domain ID: 1566785011_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois-generic.marcaria.com
Registrar URL: www.marcaria.com
Updated Date: 2016-08-23T15:13:05Z
Creation Date: 2009-08-25T06:53:59Z
Registrar Registration Expiration Date: 2022-05-11T16:28:40Z
Registrar: Marcaria.com International, Inc.
Registrar IANA ID: 1086
Domain Status: OK https://icann.org/epp#OK
Registry Registrant ID: Not Available From Registry
Registrant Name: Lazada Group GmbH
Registrant Organization: Lazada Group GmbH
Registrant Street: Johannisstrae 20
Registrant City: Berlin
Registrant State/Province: Berlin
Registrant Postal Code: 10117
Registrant Country: DE
Registrant Phone: +49.30300131800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domains@lazada.com
Registry Admin ID: Not Available From Registry
Admin Name: Lazada Group GmbH
Admin Organization: Lazada Group GmbH
Admin Street: Johannisstrae 20
Admin City: Berlin
Admin State/Province: Berlin
Admin Postal Code: 10117
Admin Country: DE
Admin Phone: +49.30300131800
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domains@lazada.com
```



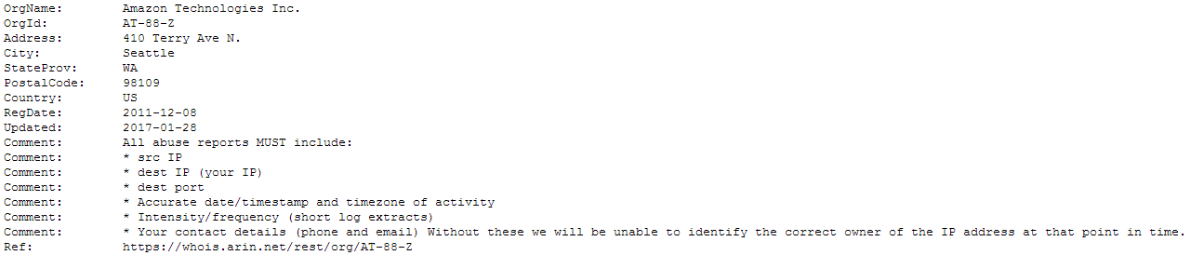
```
Registry Tech ID: Not Available From Registry
Tech Name: Francisco Fuentealba
Tech Organization: Marcaria.com
Tech Street: 8345 NW 66 ST #B1673
Tech City: Miami
Tech State/Province: Florida
Tech Postal Code: 33166
Tech Country: US
Tech Phone: +1.3054348621
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:  domains@marcaria.com
Name Server: a.ns14.net
Name Server: b.ns14.net
Name Server: c.ns14.net
Name Server: d.ns14.net
DNSSEC:Unsigned
Registrar Abuse Contact Email:  abuse@marcaria.com
Registrar Abuse Contact Phone: +1.3054348621
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```



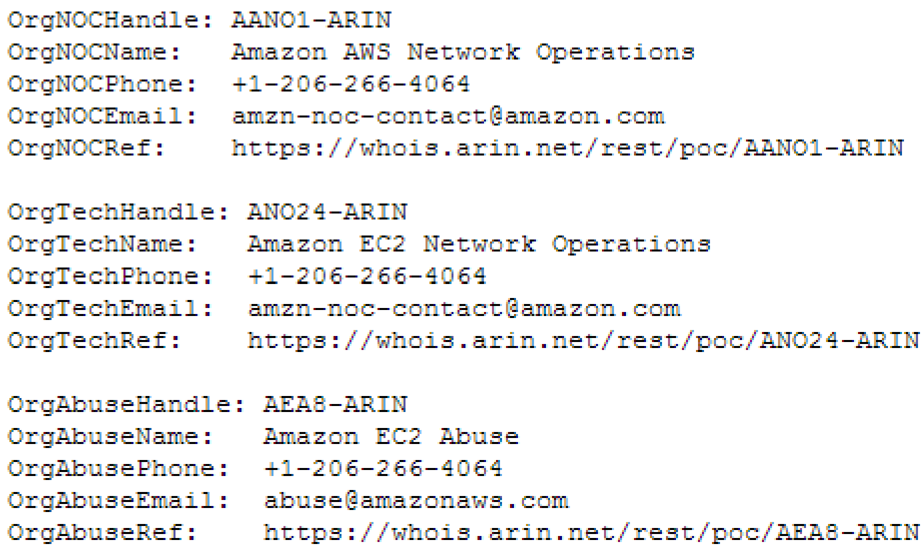
Network Whois record

Queried **whois.arin.net** with "**n 52.74.30.111**"...

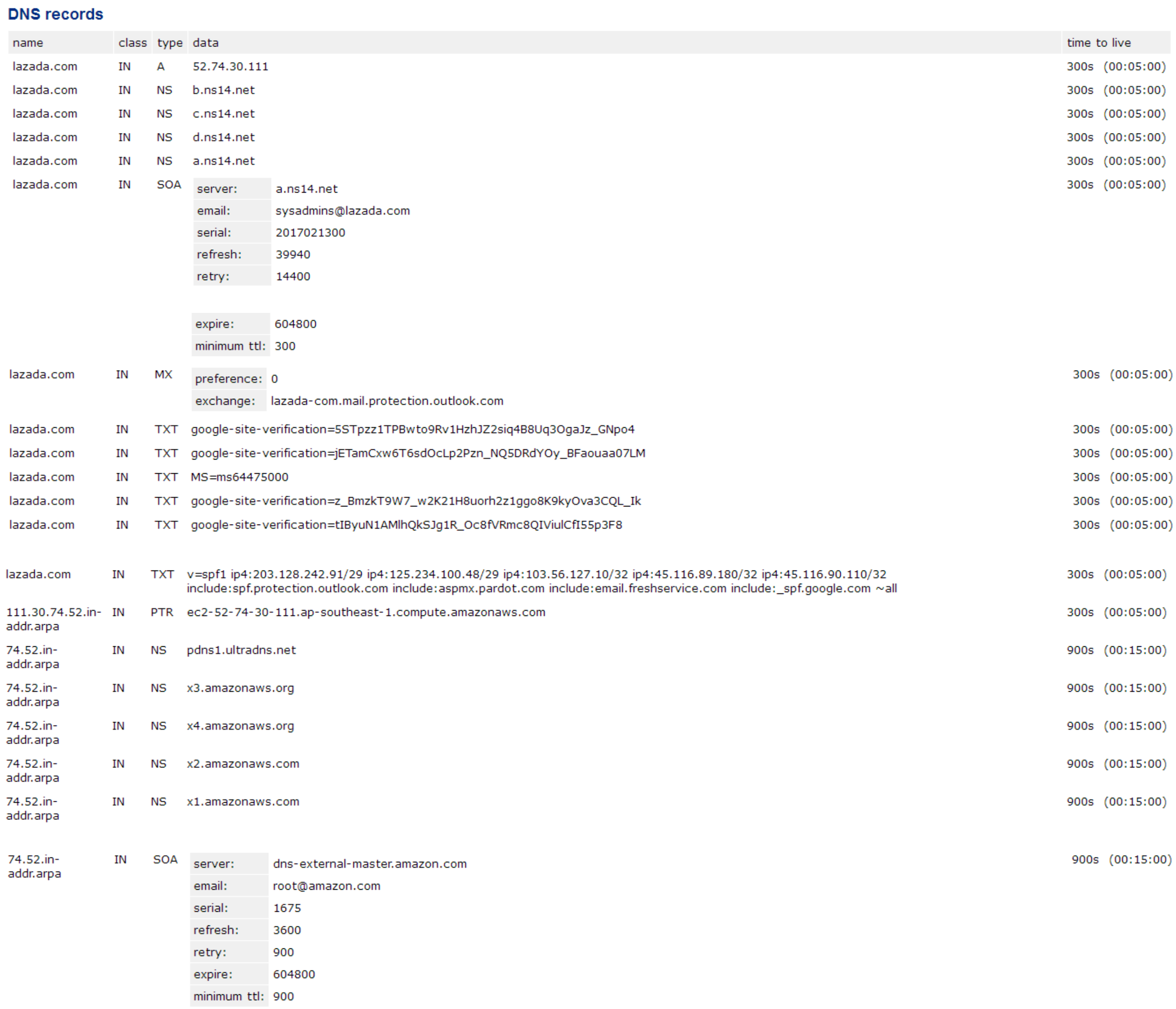
```
NetRange:       52.64.0.0 - 52.79.255.255
CIDR:           52.64.0.0/12
NetName:        AT-88-Z
NetHandle:      NET-52-64-0-0-1
Parent:         NET52 (NET-52-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon Technologies Inc. (AT-88-Z)
RegDate:        1991-12-19
Updated:        2015-03-20
Ref:            https://whois.arin.net/rest/net/NET-52-64-0-0-1
```



```
OrgName:        Amazon Technologies Inc.
OrgId:          AT-88-Z
Address:        410 Terry Ave N.
City:           Seattle
StateProv:      WA
PostalCode:     98109
Country:        US
RegDate:        2011-12-08
Updated:        2017-01-28
Comment:        All abuse reports MUST include:
Comment:        * src IP
Comment:        * dest IP (your IP)
Comment:        * dest port
Comment:        * Accurate date/timestamp and timezone of activity
Comment:        * Intensity/frequency (short log extracts)
Comment:        * Your contact details (phone and email) Without these we will be unable to identify the correct owner of the IP address at that point in time.
Ref:            https://whois.arin.net/rest/org/AT-88-Z
```

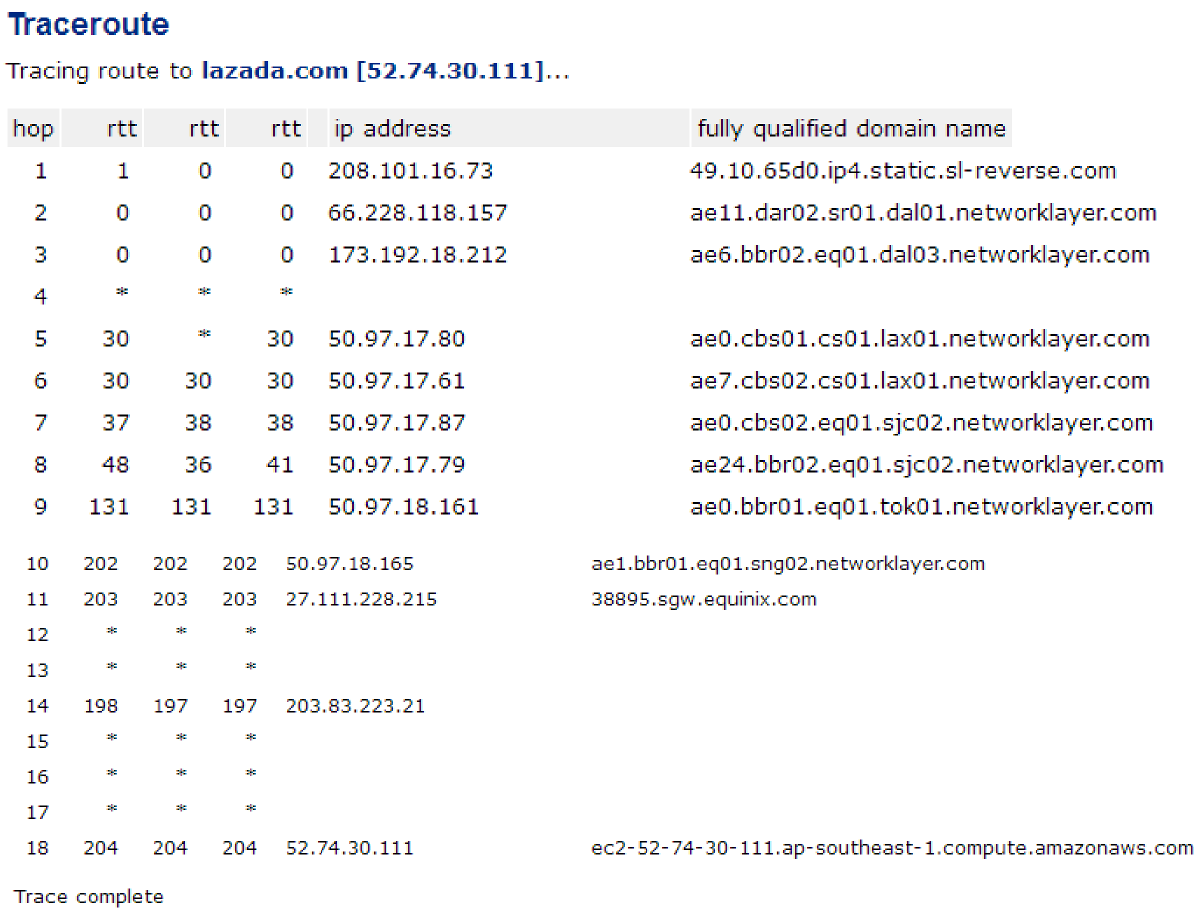


```
OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-266-4064
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://whois.arin.net/rest/poc/AANO1-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName:   Amazon EC2 Network Operations
OrgTechPhone:  +1-206-266-4064
OrgTechEmail:  amzn-noc-contact@amazon.com
OrgTechRef:    https://whois.arin.net/rest/poc/ANO24-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName:   Amazon EC2 Abuse
OrgAbusePhone:  +1-206-266-4064
OrgAbuseEmail:  abuse@amazonaws.com
OrgAbuseRef:    https://whois.arin.net/rest/poc/AEA8-ARIN
```



DNS records

name	class	type	data	time to live
lazada.com	IN	A	52.74.30.111	300s (00:05:00)
lazada.com	IN	NS	b.ns14.net	300s (00:05:00)
lazada.com	IN	NS	c.ns14.net	300s (00:05:00)
lazada.com	IN	NS	d.ns14.net	300s (00:05:00)
lazada.com	IN	NS	a.ns14.net	300s (00:05:00)
lazada.com	IN	SOA	server: a.ns14.net email: sysadmins@lazada.com serial: 2017021300 refresh: 39940 retry: 14400 expire: 604800 minimum ttl: 300	300s (00:05:00)
lazada.com	IN	MX	preference: 0 exchange: lazada-com.mail.protection.outlook.com	300s (00:05:00)
lazada.com	IN	TXT	google-site-verification=5STpzz1TPBwto9Rv1HzhJZ2siq4B8Uq3OgaJz_GNpo4	300s (00:05:00)
lazada.com	IN	TXT	google-site-verification=jETamCxw6T6sdOcLp2Pzn_NQ5DRdYOy_BFaouaa07LM	300s (00:05:00)
lazada.com	IN	TXT	MS=ms64475000	300s (00:05:00)
lazada.com	IN	TXT	google-site-verification=z_BmzkT9W7_w2K21H8uorh2z1ggo8K9kyOva3CQL_Ik	300s (00:05:00)
lazada.com	IN	TXT	google-site-verification=tIByuN1AMlhQkSJg1R_Oc8fVRmc8QIViulCfI55p3F8	300s (00:05:00)
lazada.com	IN	TXT	v=spf1 ip4:203.128.242.91/29 ip4:125.234.100.48/29 ip4:103.56.127.10/32 ip4:45.116.89.180/32 ip4:45.116.90.110/32 include:spf.protection.outlook.com include:aspmx.pardot.com include:email.freshservice.com include:_spf.google.com ~all	300s (00:05:00)
111.30.74.52.in-addr.arpa	IN	PTR	ec2-52-74-30-111.ap-southeast-1.compute.amazonaws.com	300s (00:05:00)
74.52.in-addr.arpa	IN	NS	pdns1.ultradns.net	900s (00:15:00)
74.52.in-addr.arpa	IN	NS	x3.amazonaws.org	900s (00:15:00)
74.52.in-addr.arpa	IN	NS	x4.amazonaws.org	900s (00:15:00)
74.52.in-addr.arpa	IN	NS	x2.amazonaws.com	900s (00:15:00)
74.52.in-addr.arpa	IN	NS	x1.amazonaws.com	900s (00:15:00)
74.52.in-addr.arpa	IN	SOA	server: dns-external-master.amazon.com email: root@amazon.com serial: 1675 refresh: 3600 retry: 900 expire: 604800 minimum ttl: 900	900s (00:15:00)



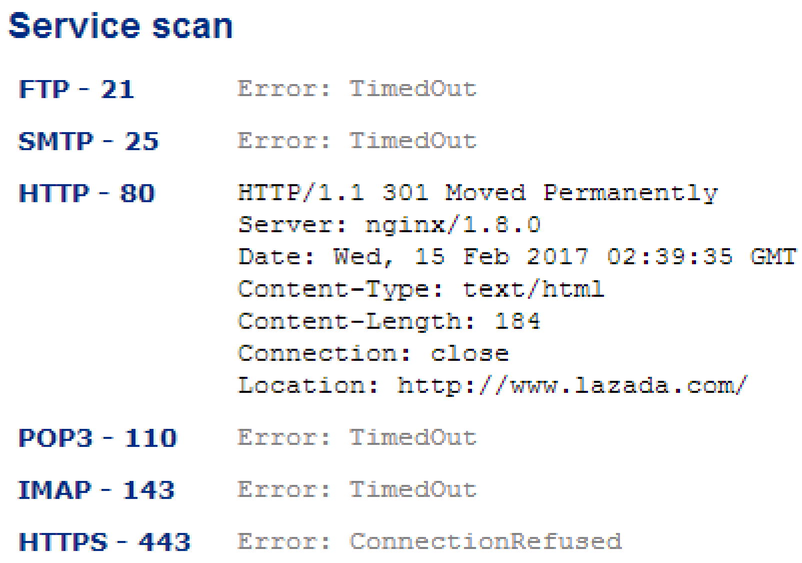
Traceroute

Tracing route to **lazada.com [52.74.30.111]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	0	0	208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com
2	0	0	0	66.228.118.157	ae11.dar02.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.212	ae6.bbr02.eq01.dal03.networklayer.com
4	*	*	*		
5	30	*	30	50.97.17.80	ae0.cbs01.cs01.lax01.networklayer.com
6	30	30	30	50.97.17.61	ae7.cbs02.cs01.lax01.networklayer.com
7	37	38	38	50.97.17.87	ae0.cbs02.eq01.sjc02.networklayer.com
8	48	36	41	50.97.17.79	ae24.bbr02.eq01.sjc02.networklayer.com
9	131	131	131	50.97.18.161	ae0.bbr01.eq01.tok01.networklayer.com
10	202	202	202	50.97.18.165	ae1.bbr01.eq01.sng02.networklayer.com
11	203	203	203	27.111.228.215	38895.sgw.equinix.com
12	*	*	*		
13	*	*	*		
14	198	197	197	203.83.223.21	
15	*	*	*		
16	*	*	*		
17	*	*	*		
18	204	204	204	52.74.30.111	ec2-52-74-30-111.ap-southeast-1.compute.amazonaws.com

Trace complete

Dapat dilihat pada gambar di atas ip addres untuk Tracing route ke lazada.com disana terdapat 12 ip address.



Service scan

FTP - 21 Error: TimedOut

SMTP - 25 Error: TimedOut

HTTP - 80

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.8.0
Date: Wed, 15 Feb 2017 02:39:35 GMT
Content-Type: text/html
Content-Length: 184
Connection: close
Location: http://www.lazada.com/
```

POP3 - 110 Error: TimedOut

IMAP - 143 Error: TimedOut

HTTPS - 443 Error: ConnectionRefused