Pemilu Indonesia 2024 - investigasi DNS

Cyberity - 2024 - v1.0

Abstrak

Metode dalam mengetahui darimana asal DNS aplikasi web. Target:

1. Pemilu2024.kpu.go.id

2. Sirekap-web.kpu.go.id

Pertanyaan:

1. Apakah data pemilu warga disimpan di dalam atau di luar negeri?

Apa yang dibutuhkan?

- IP address
- Informasi lebih jauh mengenai IP address
- NS1 dan NS2 untuk melihat server ada di mana.
- MX Records untuk melihat transaksi data dan email ada di mana.

Cara mencari IP address

Target

- ➔ Pemilu2024.kpu.go.id
- ➔ Sirekap-web.kpu.go.id

Metode:

1. Buka Terminal
2. Gunakan NSLOOKUP

Untuk target 1, hasil —>

```
% nslookup pemilu2024.kpu.go.id
Server:         1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
pemilu2024.kpu.go.id
canonical name =
pemilu2024.kpu.go.id.w.cdngslb.com.
Name:
pemilu2024.kpu.go.id.w.cdngslb.com

Address: 47.246.50.79
```

Metode:

1. Buka Terminal
2. Gunakan NSLOOKUP

Untuk target 2, hasil —>

```
% nslookup sirekap-web.kpu.go.id
Server:		1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
sirekap-web.kpu.go.id  canonical name = 4w4kpyk1tqp8s14z.aliyunddos0010.com.
Name: 4w4kpyk1tqp8s14z.aliyunddos0010.com
Address: 170.33.97.36
```

Hasil awal

IP Address

- ➔ Pemilu2024.kpu.go.id

  47.246.50.79

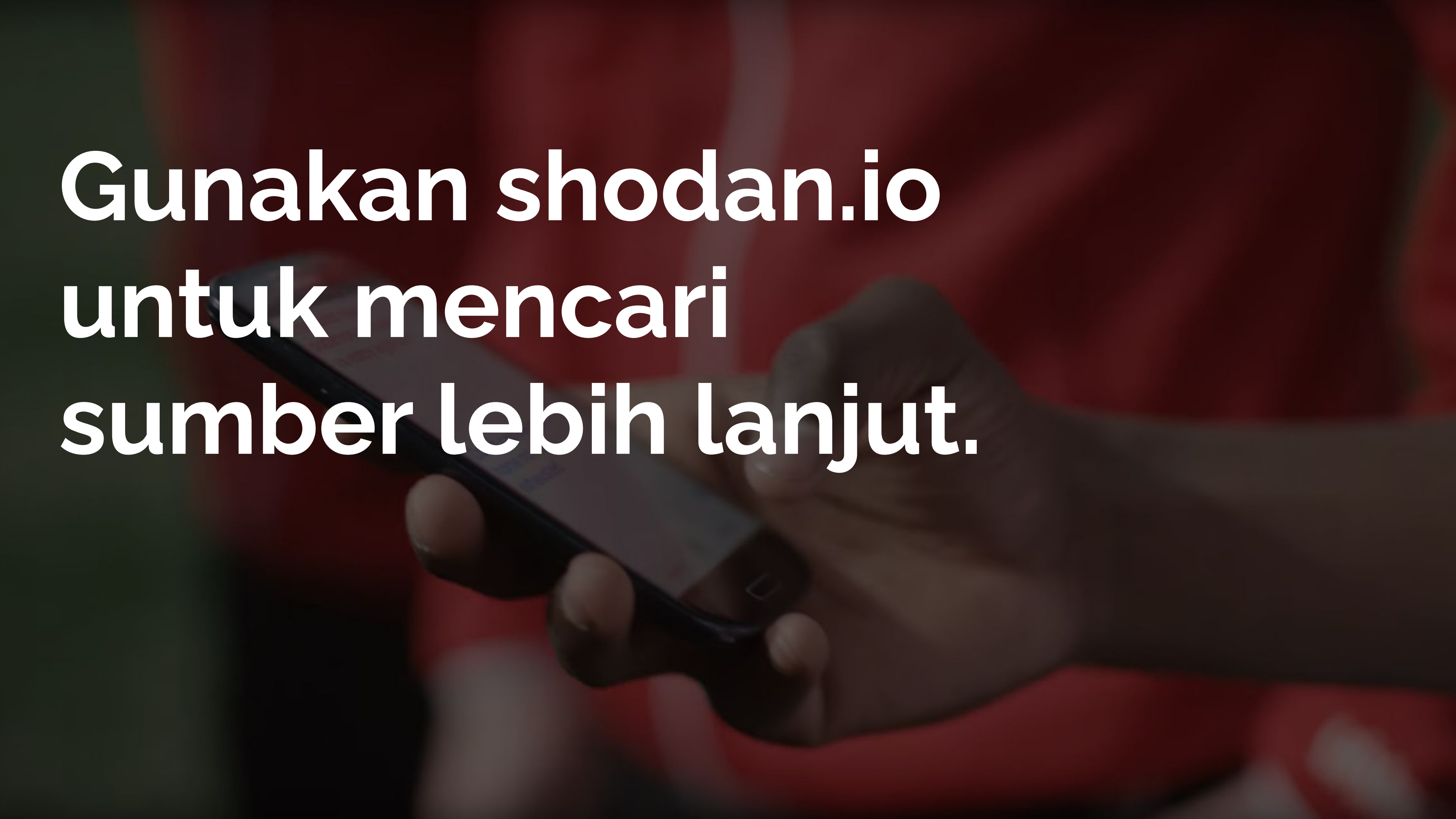
- ➔ Sirekap-web.kpu.go.id

  170.33.97.36

Cara mencari informasi lebih jauh mengenai IP address

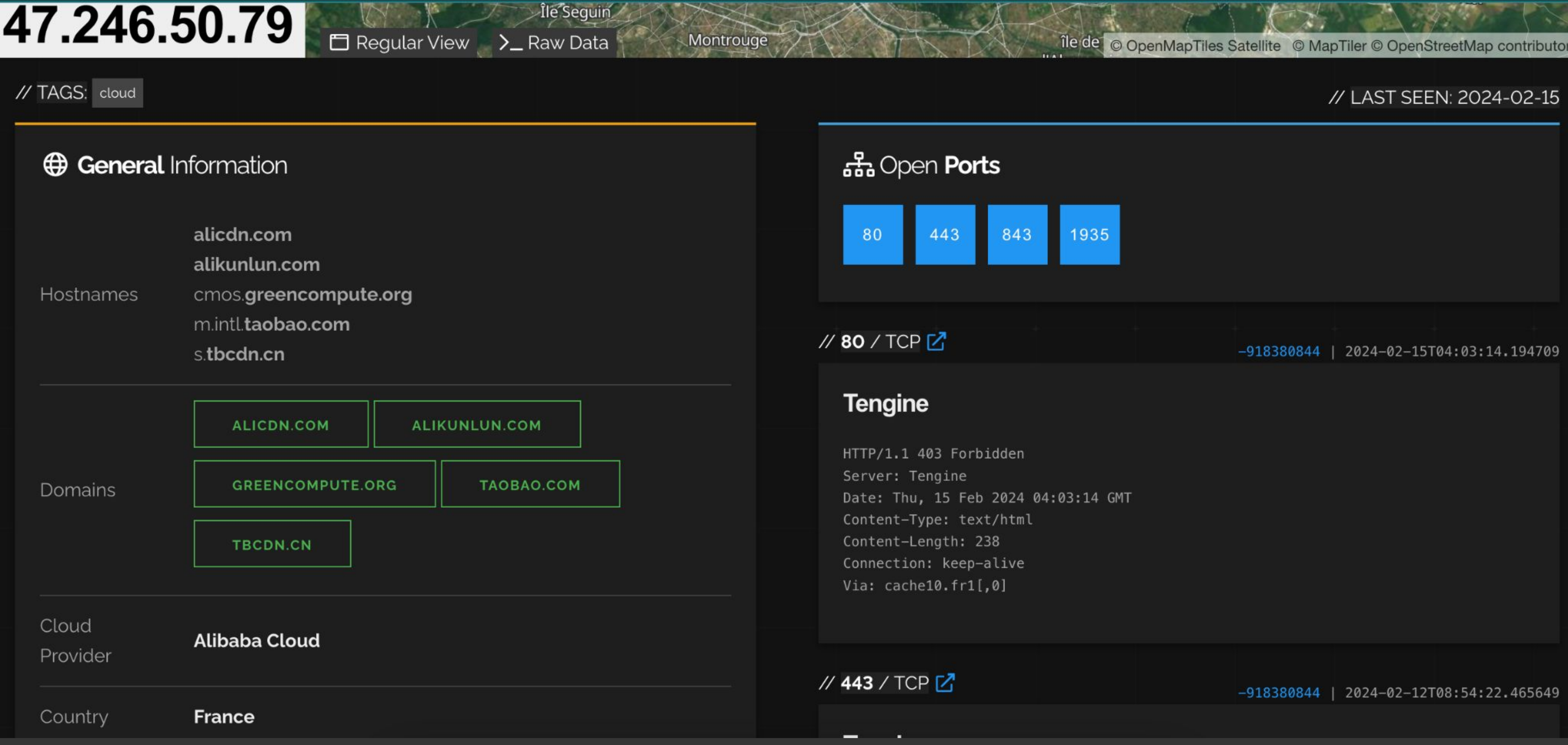
Menggunakan Shodan Tools

- ➔ 47.246.50.79
- ➔ 170.33.97.36



Gunakan shodan.io untuk mencari sumber lebih lanjut.

Hasil Pemilu2024.kpu.go.id - 47.246.50.79 dari shodan.io


Île Seguin
Montrouge
île de
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributo
Regular View
>_ Raw Data

47.246.50.79

// TAGS: cloud

// LAST SEEN: 2024-02-15

General Information

Hostnames	alicdn.com alikunlun.com cmos.greencompute.org m.intl.taobao.com s.tbcdn.cn
Domains	ALICDN.COM ALIKUNLUN.COM GREENCOMPUTE.ORG TAOBAO.COM TBCDN.CN
Cloud Provider	Alibaba Cloud
Country	France

Open Ports

80 443 843 1935

// 80 / TCP

-918380844 | 2024-02-15T04:03:14.194709

Tengine

```
HTTP/1.1 403 Forbidden
Server: Tengine
Date: Thu, 15 Feb 2024 04:03:14 GMT
Content-Type: text/html
Content-Length: 238
Connection: keep-alive
Via: cache10.fr1[,0]
```

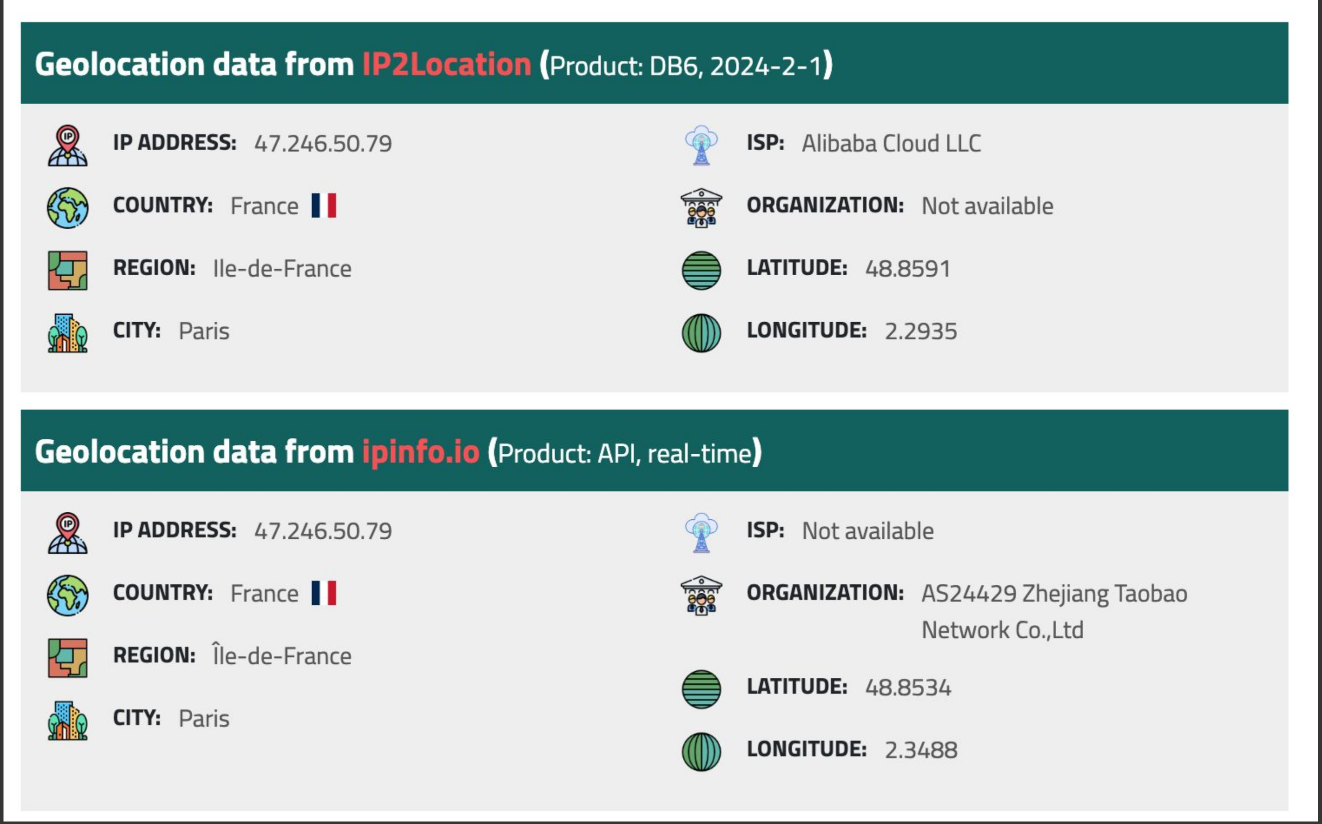
// 443 / TCP

-918380844 | 2024-02-12T08:54:22.465649

Hasil Pemilu2024.kpu.go.id - 47.246.50.79 dari shodan.io

Domain	pemilu2024.kpu.go.id	**IP address**	47.246.50.79
canonical name	pemilu2024.kpu.go.id.w.cdngslb.com.	**Open ports**	80 - 443- 843 - 1935
Hostnames:	alicdn.com	**Cloud Provider**	Alibaba Cloud
	alikunlun.com	**Country**	France
	cmos.greencompute.org	**City**	Paris
	m.intl.taobao.com	**Organization**	Alibaba Cloud LLC
	s.tbcdn.cn	**ISP**	Zhejiang Taobao Network Co.,Ltd
Domains	ALICDN.COM	**ASN**	AS24429
	ALIKUNLUN.COM		
	GREENCOMPUTE.ORG		
	TAOBAO.COM		
	TBCDN.CN		

Hasil Pemilu2024.kpu.go.id - 47.246.50.79 dari IP2Location dan Ipinfo.io Server ada di Paris, Perancis.



Geolocation data from IP2Location (Product: DB6, 2024-2-1)

IP ADDRESS: 47.246.50.79

COUNTRY: France

REGION: Ile-de-France

CITY: Paris

ISP: Alibaba Cloud LLC

ORGANIZATION: Not available

LATITUDE: 48.8591

LONGITUDE: 2.2935

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 47.246.50.79

COUNTRY: France

REGION: Île-de-France

CITY: Paris

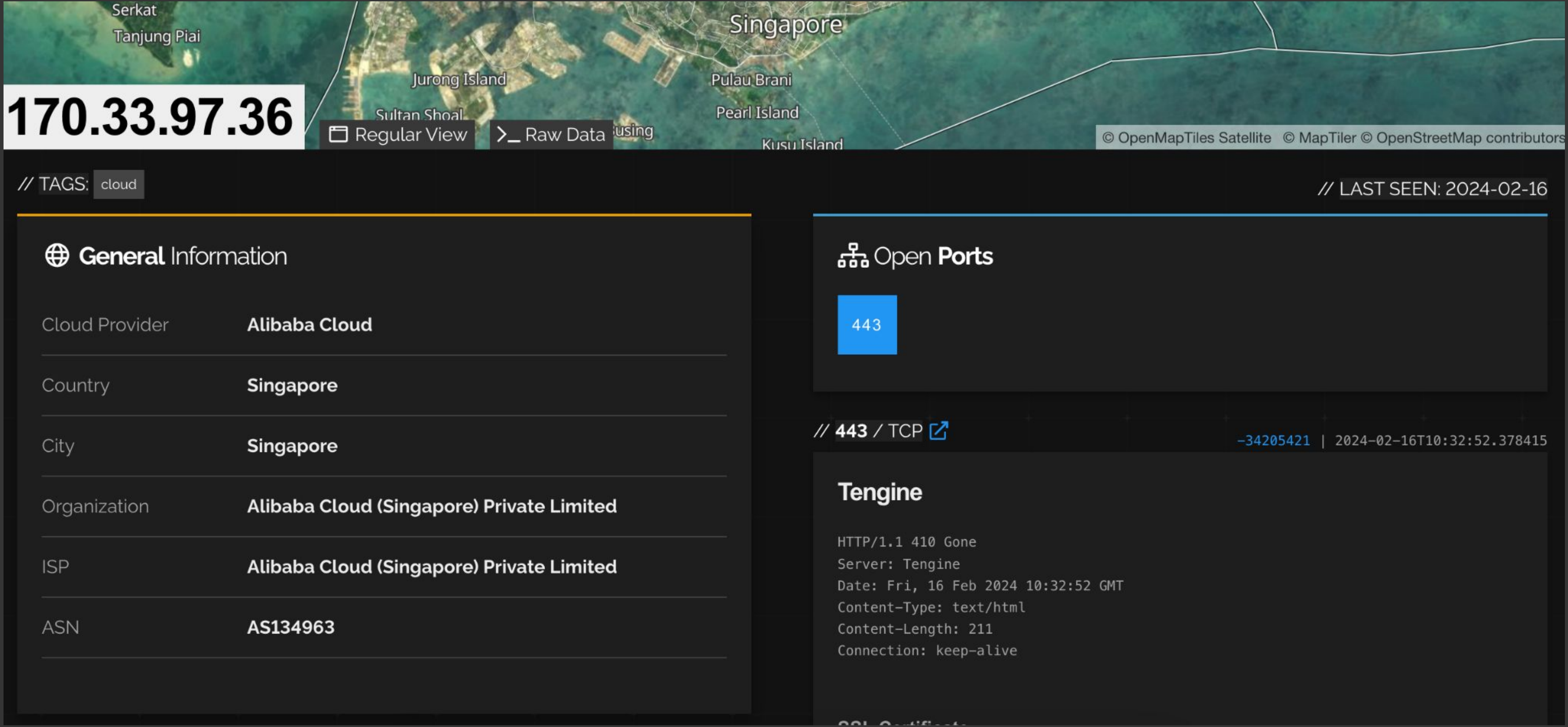
ISP: Not available

ORGANIZATION: AS24429 Zhejiang Taobao Network Co.,Ltd

LATITUDE: 48.8534

LONGITUDE: 2.3488

Hasil sirekap-web.kpu.go.id - 170.33.97.36 dari shodan.io
Server ada di Singapore



170.33.97.36

// TAGS: cloud

// LAST SEEN: 2024-02-16

General Information

Cloud Provider	Alibaba Cloud
Country	Singapore
City	Singapore
Organization	Alibaba Cloud (Singapore) Private Limited
ISP	Alibaba Cloud (Singapore) Private Limited
ASN	AS134963

Open Ports

443

// 443 / TCP

-34205421 | 2024-02-16T10:32:52.378415

Tengine

```
HTTP/1.1 410 Gone
Server: Tengine
Date: Fri, 16 Feb 2024 10:32:52 GMT
Content-Type: text/html
Content-Length: 211
Connection: keep-alive
```

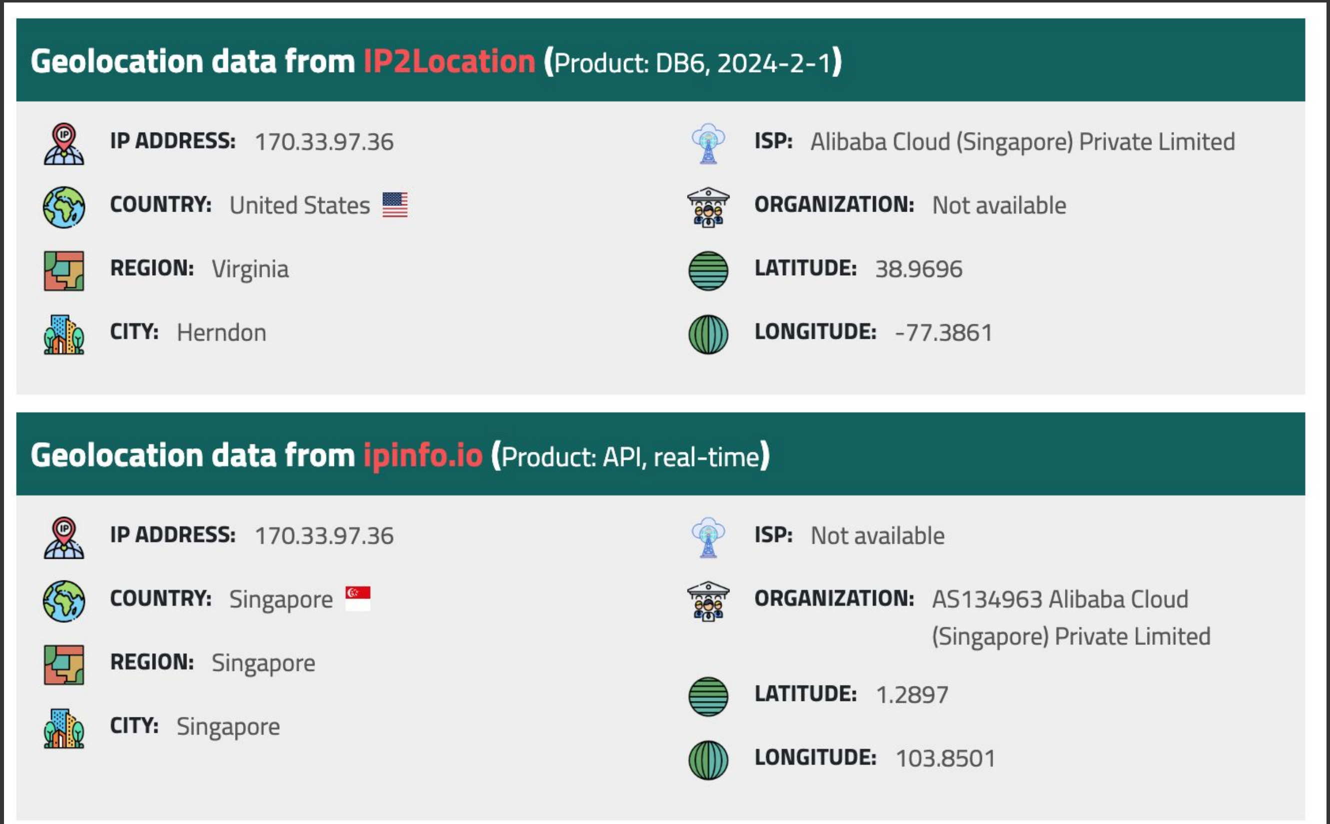
SSL Certificate

Hasil sirekap-web.kpu.go.id - 170.33.97.36 dari shodan.io

Domain	sirekap-web.kpu.go.id
canonical name	4w4kpyk1tqp8s14z.aliyunddos0010.com
Hostnames:	

IP address	47.246.50.79
Open ports	80 - 443
Cloud Provider	Alibaba Cloud
Country	Singapore
City	Singapore
Organization	Alibaba Cloud (Singapore) Private Limited
ISP	Alibaba Cloud (Singapore) Private Limited
ASN	AS134963
SSL Cert Serial Number	c6:f7:01:03:eb:c3:eb:64

Hasil sirekap-web.kpu.go.id - 170.33.97.36 dari IP2Location dan Ipinfo.io Server mirror di US dan Singapore.



Geolocation data from IP2Location (Product: DB6, 2024-2-1)

IP ADDRESS: 170.33.97.36

COUNTRY: United States

REGION: Virginia

CITY: Herndon

ISP: Alibaba Cloud (Singapore) Private Limited

ORGANIZATION: Not available

LATITUDE: 38.9696

LONGITUDE: -77.3861

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 170.33.97.36

COUNTRY: Singapore

REGION: Singapore

CITY: Singapore

ISP: Not available

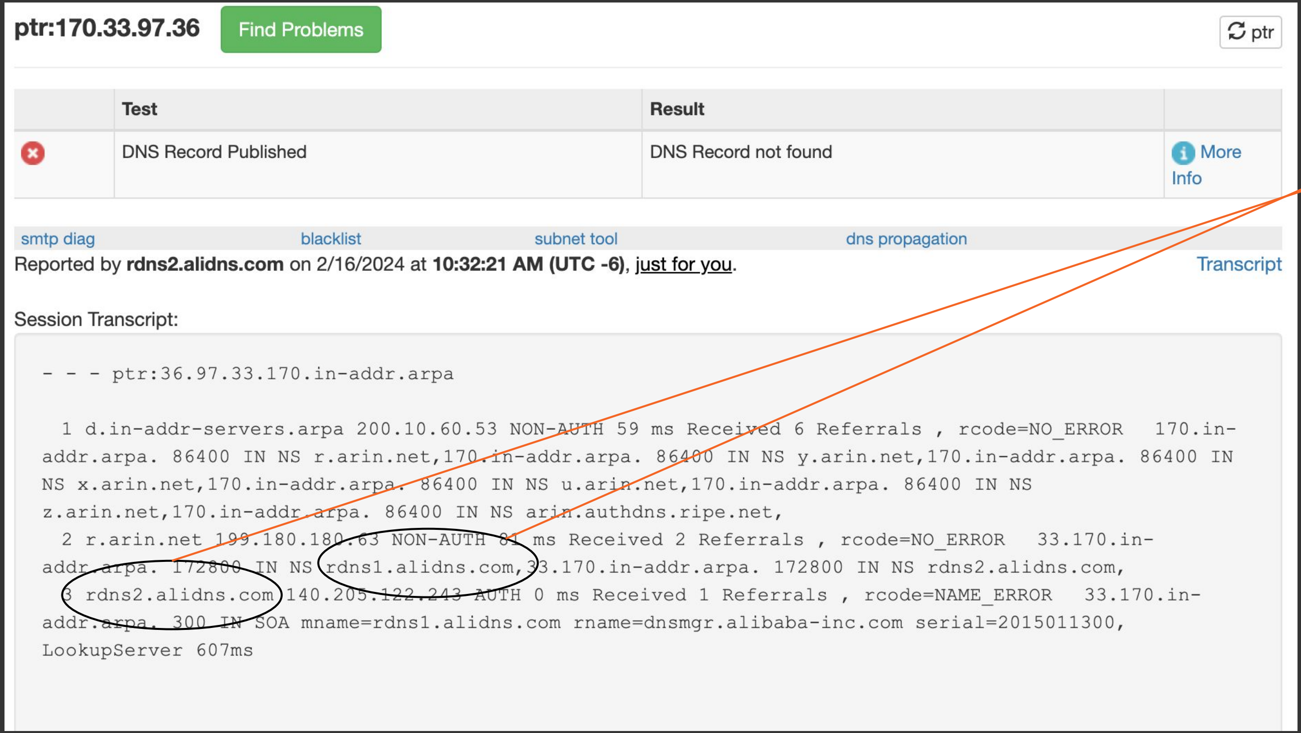
ORGANIZATION: AS134963 Alibaba Cloud (Singapore) Private Limited

LATITUDE: 1.2897

LONGITUDE: 103.8501

Hasil sirekap-web.kpu.go.id - 170.33.97.36 - MX Reverse Name Server milik Perusahaan Alibaba di RRC.

Cara; buka di browser perintah untuk melihat Domain Name Server:
https://mxtoolbox.com/SuperTool.aspx?action=ptr%3a170.33.97.36&run=toolpage



	Test	Result	
☒	DNS Record Published	DNS Record not found	More Info

Reported by **rdns2.alidns.com** on 2/16/2024 at **10:32:21 AM (UTC -6)**, just for you.

Session Transcript:

```
- - - ptr:36.97.33.170.in-addr.arpa

 1 d.in-addr-servers.arpa 200.10.60.53 NON-AUTH 59 ms Received 6 Referrals , rcode=NO_ERROR   170.in-
addr.arpa. 86400 IN NS r.arin.net,170.in-addr.arpa. 86400 IN NS y.arin.net,170.in-addr.arpa. 86400 IN
NS x.arin.net,170.in-addr.arpa. 86400 IN NS u.arin.net,170.in-addr.arpa. 86400 IN NS
z.arin.net,170.in-addr.arpa. 86400 IN NS arin.authdns.ripe.net,
 2 r.arin.net 199.180.180.63 NON-AUTH 81 ms Received 2 Referrals , rcode=NO_ERROR   33.170.in-
addr.arpa. 172800 IN NS rdns1.alidns.com,33.170.in-addr.arpa. 172800 IN NS rdns2.alidns.com,
 3 rdns2.alidns.com 140.205.122.243 AUTH 0 ms Received 1 Referrals , rcode=NAME_ERROR   33.170.in-
addr.arpa. 300 IN SOA mname=rdns1.alidns.com rname=dnsmgr.alibaba-inc.com serial=2015011300,
LookupServer 607ms
```

NS1 dan NS2 menuju DNS milik Alibaba

Penggunaan Gobuster

```
gobuster dir -u https://pemilu2024.kpu.go.id -w /Users/wordlist/big.txt  -t 4 --delay 1s -o results.txt
```

```
gobuster dns -d http://170.33.97.36 -w /Users/wordlist/shubs-subdomains.txt
```

/Users/wordlist/big.txt => https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/big.txt

/Users/wordlist/shubs-subdomains.txt => https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/shubs-subdomains.txt

Kesimpulan sementara:

Baik pada domain maupun data pemilu2024.kpu.go.id maupun sirekap-web.kpu.go.id, nama domain serta transaksi data ada di luar Indonesia.

Tapi:

Apakah data juga disimpan di luar Indonesia?

Mencari informasi mengenai data melalui IP address

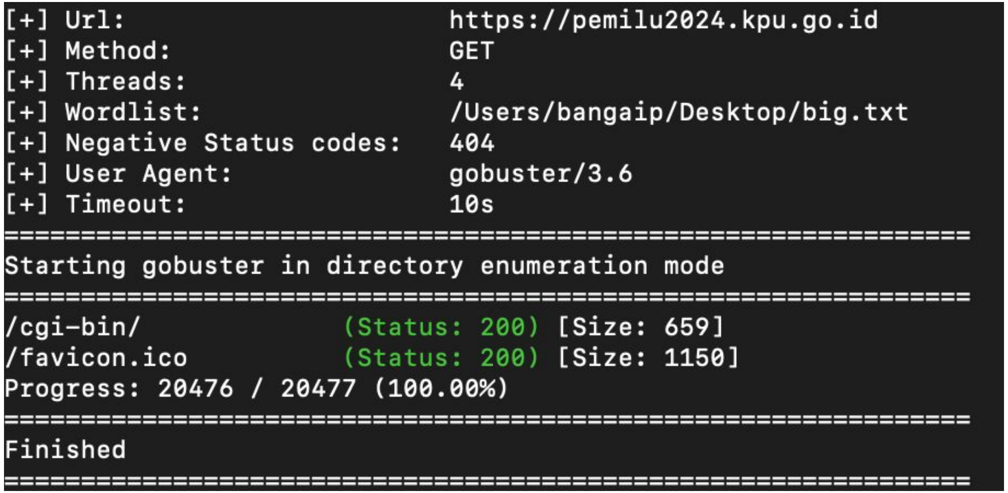
Menggunakan gobuster, nslookup dan dig Tools. Target:

- ➔ 47.246.50.79
- ➔ 170.33.97.36

Penggunaan Gobuster

gobuster dir -u https://pemilu2024.kpu.go.id -w /Users/wordlist/big.txt -t 4 --delay 1s -o results.txt

Hasil tidak begitu banyak. Hanya ada dua status OK 200

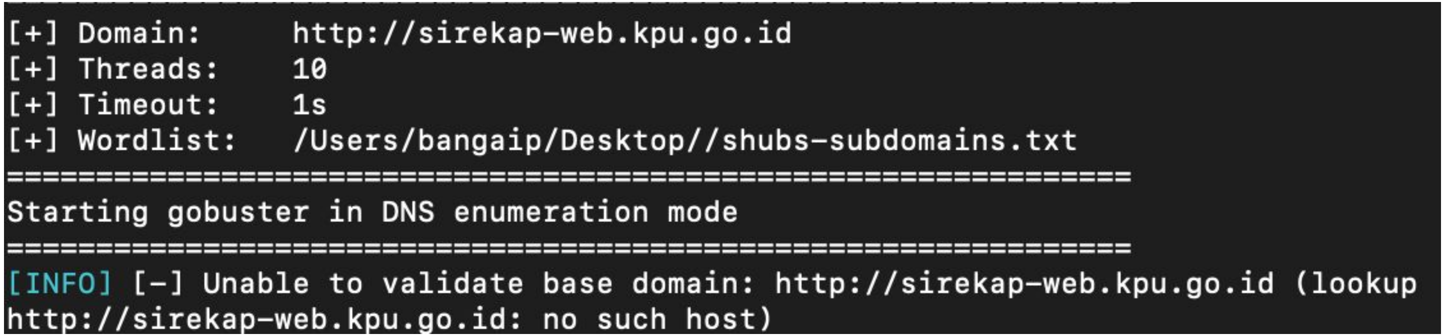


```
[+] Url:                     https://pemilu2024.kpu.go.id
[+] Method:                  GET
[+] Threads:                 4
[+] Wordlist:                /Users/bangaip/Desktop/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/cgi-bin/             (Status: 200) [Size: 659]
/favicon.ico          (Status: 200) [Size: 1150]
Progress: 20476 / 20477 (100.00%)
===============================================================
Finished
===============================================================
```

Penggunaan Gobuster

gobuster dir -u https://pemilu2024.kpu.go.id -w /Users/wordlist/big.txt -t 4 --delay 1s -o results.txt

Tidak bisa saat ini karena aplikasi SiRekap down (16 Februari 2024 23:57 WIB)



```
[+] Domain:     http://sirekap-web.kpu.go.id
[+] Threads:    10
[+] Timeout:    1s
[+] Wordlist:   /Users/bangaip/Desktop//shubs-subdomains.txt
===============================================================
Starting gobuster in DNS enumeration mode
===============================================================
[INFO] [-] Unable to validate base domain: http://sirekap-web.kpu.go.id (lookup
http://sirekap-web.kpu.go.id: no such host)
```

Metode:

1. Buka Terminal
2. Gunakan NSLOOKUP

Untuk target 1 (**pemilu2024.kpu.go.id**), hasil —>

Didapat informasi email melalui alamat **root.cdngslb.com**

```
% nslookup -type=mx
pemilu2024.kpu.go.id
Server:                 192.168.1.204
Address:        192.168.1.204#53

Non-authoritative answer:
pemilu2024.kpu.go.id        canonical name =
pemilu2024.kpu.go.id.w.cdngslb.com.

Authoritative answers can be found from:
w.cdngslb.com
        origin = ns1.vip.cdngslb.com
        mail addr = root.cdngslb.com
        serial = 181010
        refresh = 3600
        retry = 3600
        expire = 360000
        minimum = 300
```

Hasil pencarian server email Pemilu2024.kpu.go.id - melalui jalur root.cdngslb.com

Menggunakan

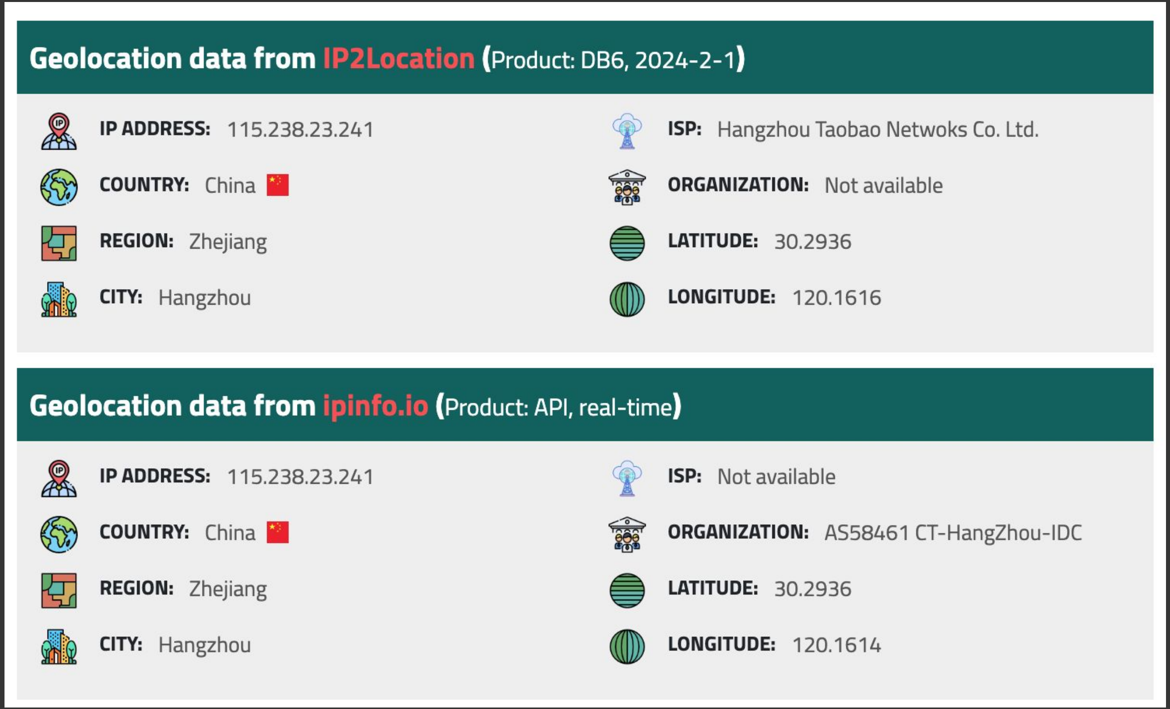
nslookup cdngslb.com

Hasil adalah: IP Address 115.238.23.241

Dig cdngslb.com

Hasil adalah: A Records 115.238.23.241

Hasil pencarian server email Pemilu2024.kpu.go.id - **melalui jalur root.cdngslb.com - 115.238.23.241 **Server dan data email ada di RRC



Geolocation data from IP2Location (Product: DB6, 2024-2-1)

IP ADDRESS:	115.238.23.241	**ISP:**	Hangzhou Taobao Netwoks Co. Ltd.
COUNTRY:	China 🇨🇳	**ORGANIZATION:**	Not available
REGION:	Zhejiang	**LATITUDE:**	30.2936
CITY:	Hangzhou	**LONGITUDE:**	120.1616

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS:	115.238.23.241	**ISP:**	Not available
COUNTRY:	China 🇨🇳	**ORGANIZATION:**	AS58461 CT-HangZhou-IDC
REGION:	Zhejiang	**LATITUDE:**	30.2936
CITY:	Hangzhou	**LONGITUDE:**	120.1614

Metode:

1. Buka Terminal
2. Gunakan NSLOOKUP

Untuk target 1 **(sirekap-web.kpu.go.id)**, hasil —>

Didapat informasi email melalui alamat **hostmaster.hichina.com**

```
% nslookup -type=mx
sirekap-web.kpu.go.id
Server:                 192.168.1.204
Address:        192.168.1.204#53

Non-authoritative answer:
sirekap-web.kpu.go.id       canonical name =
4w4kpyk1tqp8s14z.aliyunddos0010.com.

Authoritative answers can be found from:
aliyunddos0010.com
        origin = vip5.alidns.com
        mail addr = hostmaster.hichina.com
        serial = 2024010807
        refresh = 3600
        retry = 1200
        expire = 86400
        minimum = 600
```

Hasil pencarian server email sirekap-web.kpu.go.id - melalui jalur hostmaster.hichina.com

Menggunakan

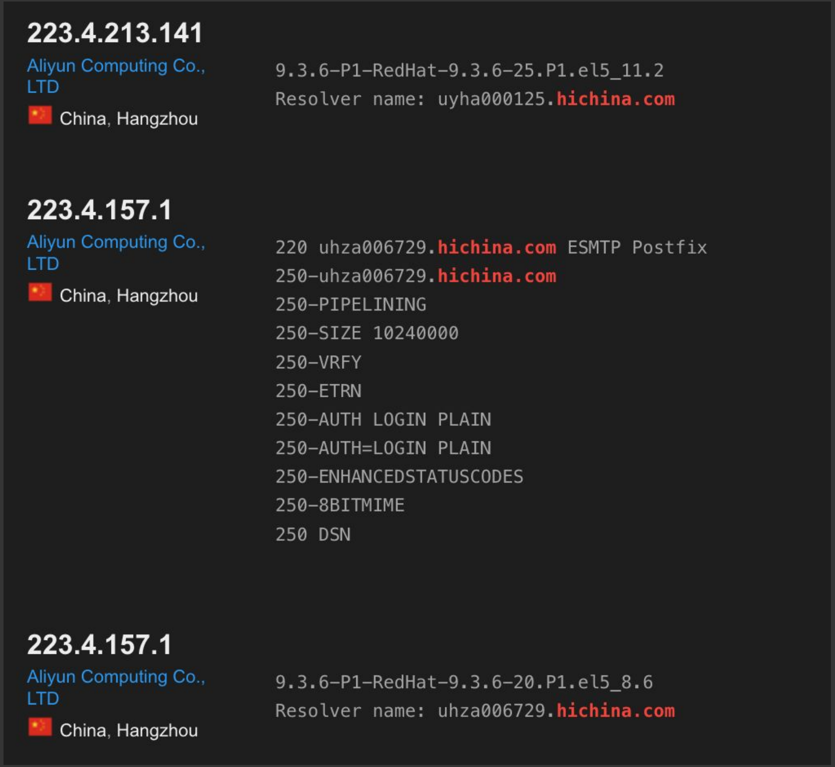
Nslookup hostmaster.hichina.com

Hasil adalah: IP Address (*** Can't find hichina.com: No answer)

Dig hostmaster.hichina.com

Hasil adalah: A Records (Tidak ada)

Hasil pencarian server email sirekap-web.kpu.go.id - melalui jalur hostmaster.hichina.com



223.4.213.141

Aliyun Computing Co., LTD

China, Hangzhou

```
9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.2
Resolver name: uyha000125.hichina.com
```

223.4.157.1

Aliyun Computing Co., LTD

China, Hangzhou

```
220 uhza006729.hichina.com ESMTP Postfix
250-uhza006729.hichina.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

223.4.157.1

Aliyun Computing Co., LTD

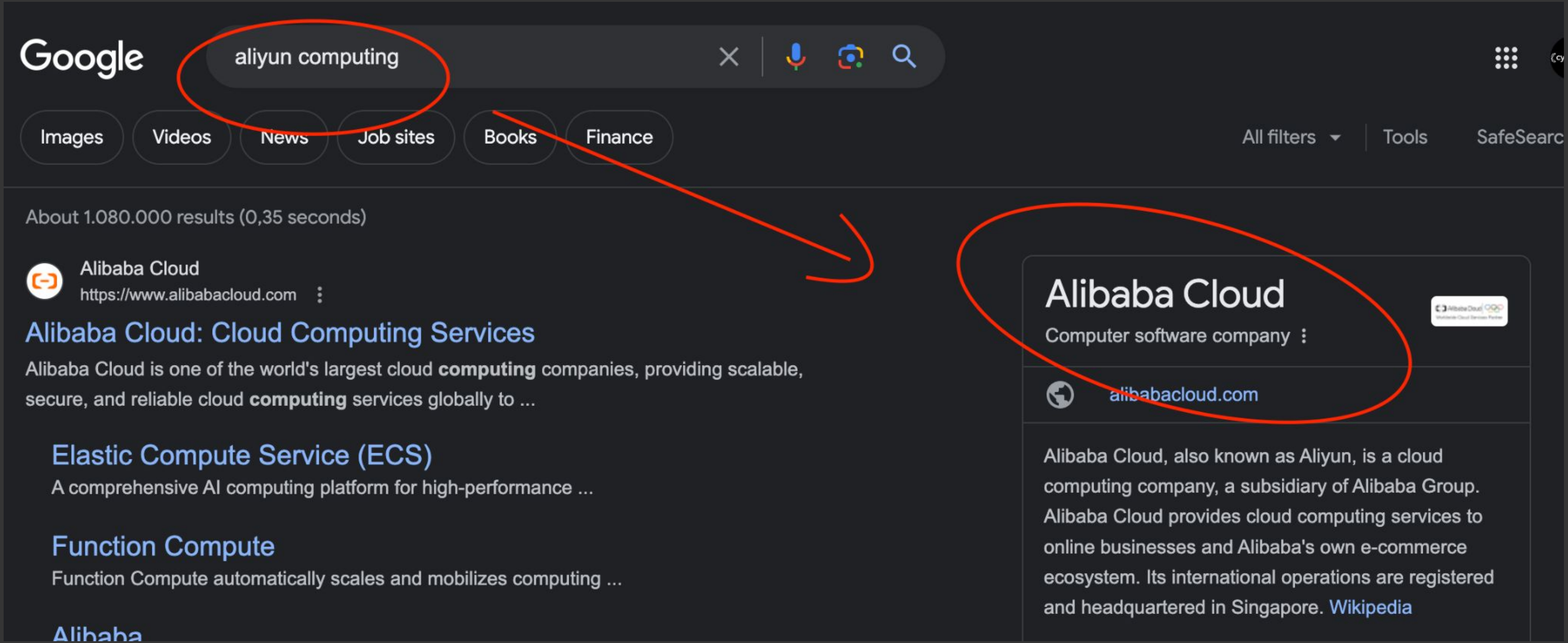
China, Hangzhou

```
9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6
Resolver name: uhza006729.hichina.com
```

Ditemukan bahwa hichina adalah milik Aliyun Computing Co., LTD di Hangzhou, China.

— **Hasil pencarian server email sirekap-web.kpu.go.id** - melalui jalur hostmaster.hichina.com

Aliyun Computing ternyata adalah Alibaba Cloud



About 1.080.000 results (0,35 seconds)

Alibaba Cloud
https://www.alibabacloud.com

Alibaba Cloud: Cloud Computing Services

Alibaba Cloud is one of the world's largest cloud **computing** companies, providing scalable, secure, and reliable cloud **computing** services globally to ...

Elastic Compute Service (ECS)

A comprehensive AI computing platform for high-performance ...

Function Compute

Function Compute automatically scales and mobilizes computing ...

Alibaba

Alibaba Cloud

Computer software company

alibabacloud.com

Alibaba Cloud, also known as Aliyun, is a cloud computing company, a subsidiary of Alibaba Group. Alibaba Cloud provides cloud computing services to online businesses and Alibaba's own e-commerce ecosystem. Its international operations are registered and headquartered in Singapore. Wikipedia

Kesimpulan sementara:

Dengan menggunakan metode dan tools sederhana, dapat dilihat bahwa data email pemilu2024.kpu.go.id maupun sirekap-web.kpu.go.id, diatur dan ada di luar Indonesia.

Terimakasih!

Cyberity researcher:

1. Bangaip
2. Harry Sufehmi