

KEAMANAN JARINGAN KOMPUTER



Oleh:

(TIARA NUR AZMI PUSPA DAMAYANTI)

(09040581721003)

(Kelas TKJ4)

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

A. Website dalam negeri (video.com)

Informasi Domain

Domain Name: VIDIO.COM
Registrar: GANDI SAS
Sponsoring Registrar IANA ID: 81
Whois Server: whois.gandi.net
Referral URL: <http://www.gandi.net>
Name Server: NS-1062.AWSDNS-04.ORG
Name Server: NS-2043.AWSDNS-63.CO.UK
Name Server: NS-226.AWSDNS-28.COM
Name Server: NS-848.AWSDNS-42.NET
Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Updated Date: 13-aug-2014
Creation Date: 28-nov-1997
Expiration Date: 13-aug-2024

>>> Last update of whois database: Wed, 29 Mar 2017 11:31:38 GMT <<<

Netcraft site report

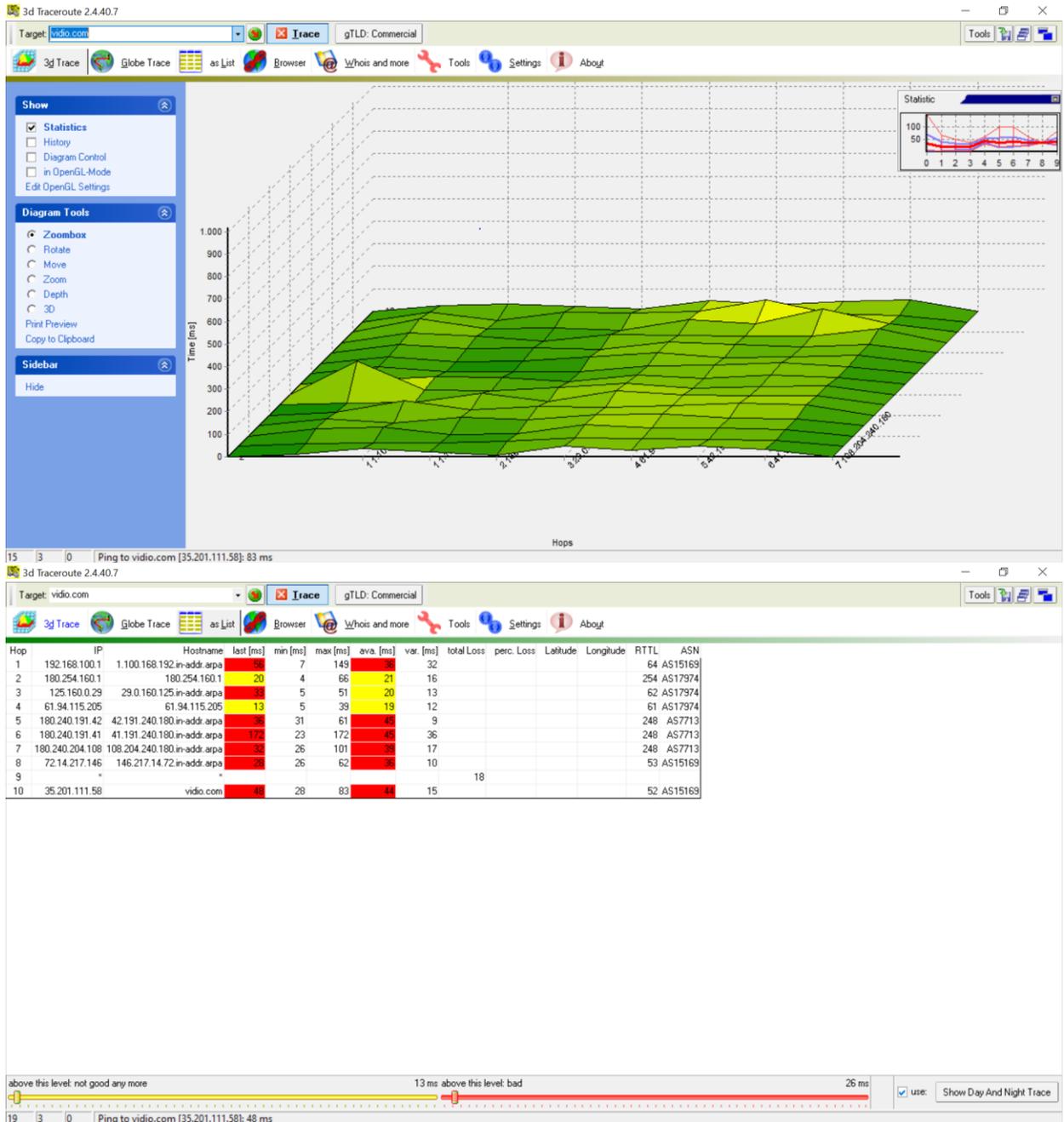
Network

Site	http://vidio.com	Netblock Owner	Google LLC
Domain	vidio.com	Nameserver	ns-848.awsdns-42.net
IP address	35.201.111.58 (VirusTotal)	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	<i>Not Present</i>	Reverse DNS	58.111.201.35.bc.googleusercontent.com
Domain registrar	gandi.net	Nameserver organisation	whois.markmonitor.com
Organisation	Obfuscated whois Gandi-Paris, 75013, France	Hosting company	Amazon - Asia Pacific (Singapore) datacenter
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	<i>unknown</i>
Hosting country	 sg		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Amazon Data Services Singapore Bedok Central Post Office PO Box 482 Singapore SG 049481	13.229.29.212	Linux	Varnish	6-Mar-2018
Amazon Data Services Singapore Bedok Central Post Office PO Box 482 Singapore SG 049481	52.221.25.55	Linux	Varnish	1-Mar-2017
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	52.76.4.215	Linux	Varnish	21-Feb-2017
Amazon Data Services Singapore Bedok Central Post Office PO Box 482 Singapore SG 049481	52.220.12.214	Linux	Varnish	4-Jan-2017
Amazon Data Services Singapore Bedok Central Post Office PO Box 482 Singapore SG 049481	52.220.207.44	Linux	Varnish	1-Jan-2017
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	52.77.147.134	Linux	Varnish	20-Jun-2016
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	54.169.54.187	Linux	Varnish	17-Jun-2016

Berikut hasil dari 3d traceroute



Setelah didapatkan alamat ip website tersebut dari 3dtracroute, masukan ip tersebut website robtex dan didapat hasil berikut ini.

ANALYSIS ↑ ↓

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

Vidio.com has four name servers, five mail servers and one IP number.

Name servers

The name servers are ns-226.awsdns-28.com, ns-848.awsdns-42.net, ns-1062.awsdns-04.org and ns-2043.awsdns-63.co.uk.

Google mail servers

The mail servers are aspmx.l.google.com, alt1.aspmx.l.google.com, alt2.aspmx.l.google.com, alt3.aspmx.l.google.com and alt4.aspmx.l.google.com.

This domain uses google to handle it's email.

IP number

The IP number is 35.201.111.58. The PTR of the IP number is 58.111.201.35.bc.googleusercontent.com. The IP number is in Ann Arbor, United States. It is hosted by Google.

Results found

Vidio.at, vidio.be, vidio.bid, vidio.biz, vidio.bz, vidio.ca, vidio.cam, vidio.chat, vidio.co, vidio.company, vidio.cz and vidio.de.

Dari 10 IP yang didapat dari 3dtracert kita ambil sample 1 Ip yaitu 118.97.159.33 jika dianalisis menggunakan wireshark maka:

Source : 192.168.100.17

Destination : 118.97.159.33

The image shows a Wireshark network traffic capture and a Windows Command Prompt window. The Wireshark window displays a list of network packets with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
290	37.330246	HuaweiTe_f3:d8:0f	Broadcast	ARP	42	Who has 192.168.100.20? Tell 192.168.100.1
291	38.456864	HuaweiTe_f3:d8:0f	Broadcast	ARP	42	Who has 192.168.100.20? Tell 192.168.100.1
292	39.378416	HuaweiTe_f3:d8:0f	Broadcast	ARP	42	Who has 192.168.100.20? Tell 192.168.100.1
293	40.239710	fe80::d8f4:f616:f3...	ff02::1:2	DHCPv6	84	Information-request XID: 0x6de12f
294	40.334678	fe80::1	fe80::d8f4:f616:f3...	DHCPv6	84	Reply XID: 0x6de12f
295	40.404541	HuaweiTe_f3:d8:0f	Broadcast	ARP	42	Who has 192.168.100.20? Tell 192.168.100.1
296	40.989522	192.168.100.17	118.97.159.33	TCP	55	[TCP Keep-Alive] 52421 → 80 [ACK] Seq=1 Ack=1 Win=63856 Len=1
297	40.994840	118.97.159.33	192.168.100.17	TCP	54	[TCP Keep-Alive ACK] 80 → 52421 [ACK] Seq=1 Ack=2 Win=4534 Len=0
298	41.426254	HuaweiTe_f3:d8:0f	Broadcast	ARP	42	Who has 192.168.100.20? Tell 192.168.100.1

The selected packet (No. 297) details are:

- Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
- Ethernet II, Src: HuaweiTe_f3:d8:0f (f8:75:88:f3:d8:0f), Dst: ca:ff:3c:5d:92:80 (ca:ff:3c:5d:92:80)
- Internet Protocol Version 4, Src: 161.69.45.107, Dst: 192.168.100.17
- Transmission Control Protocol, Src Port: 443, Dst Port: 52432, Seq: 0, Ack: 1, Len: 0

The packet bytes are displayed in hexadecimal and ASCII:

```
0000 ca ff 3c 5d 92 80 f8 75 88 f3 d8 0f 00 00 45 00 ...<]...u .....E
0010 00 30 ca 31 40 00 f3 06 ca 2b a1 45 2d 6b c0 a8 0-1@...+E-k..
0020 64 11 01 bb cc d0 8f f0 11 a2 fd 08 56 54 70 12 d.....VTP:
0030 10 8c bc ce 00 00 02 04 05 84 04 02 00 00 .....
```

The Windows Command Prompt window shows the following output:

```
C:\Users\Lenovo>ping 118.97.159.33

Pinging 118.97.159.33 with 32 bytes of data:
Reply from 118.97.159.33: bytes=32 time=31ms TTL=59
Reply from 118.97.159.33: bytes=32 time=20ms TTL=59
Reply from 118.97.159.33: bytes=32 time=28ms TTL=59
Reply from 118.97.159.33: bytes=32 time=58ms TTL=59

Ping statistics for 118.97.159.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 58ms, Average = 34ms

C:\Users\Lenovo>
```