

TUGAS KEAMANAN JARINGAN KOMPUTER

“SCANNING”



Disusun Oleh:

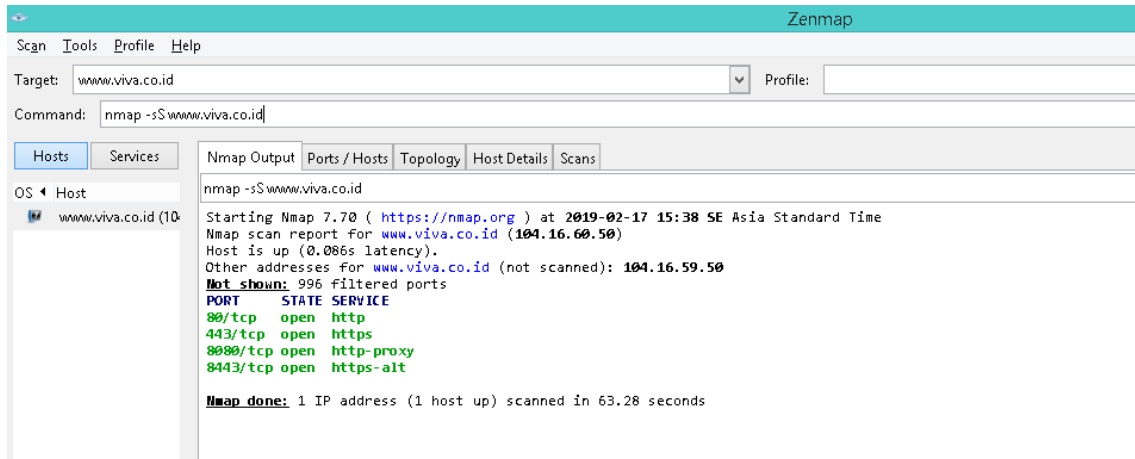
Nama : MUHAMMAD FAJAR PUTRA
NIM : 09011181520009
Kelas : SK8

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019**

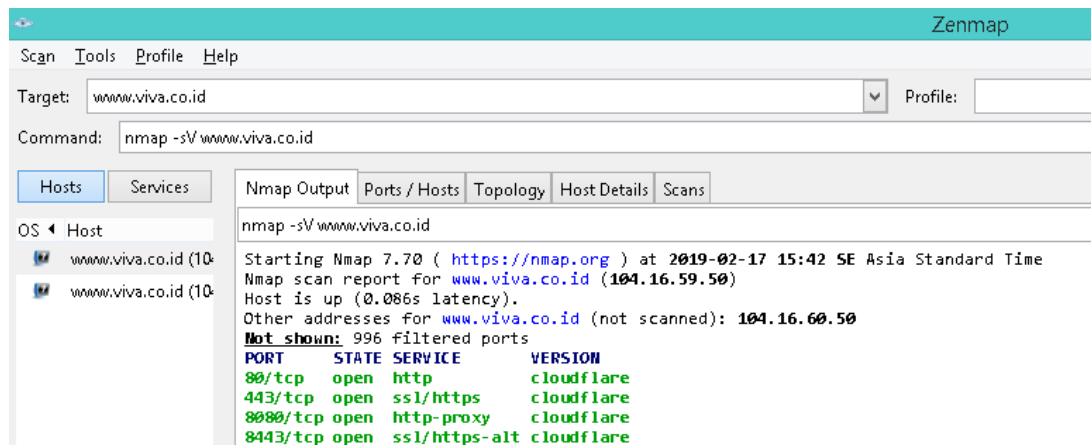
1.Scanning Menggunakan NMAP

www.viva.co.id

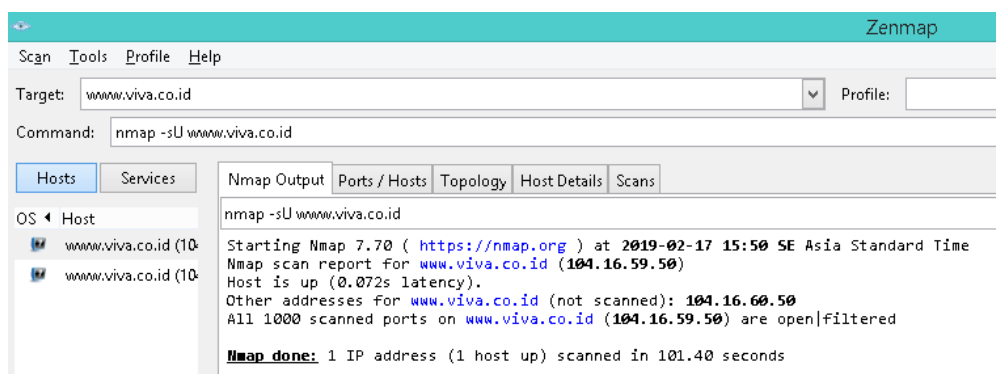
Menggunakan command *nmap -sS*



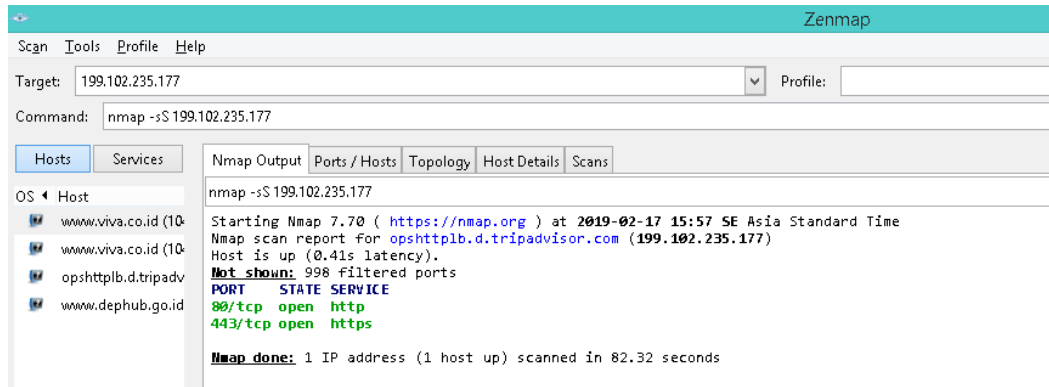
Menggunakan command *nmap -sV*



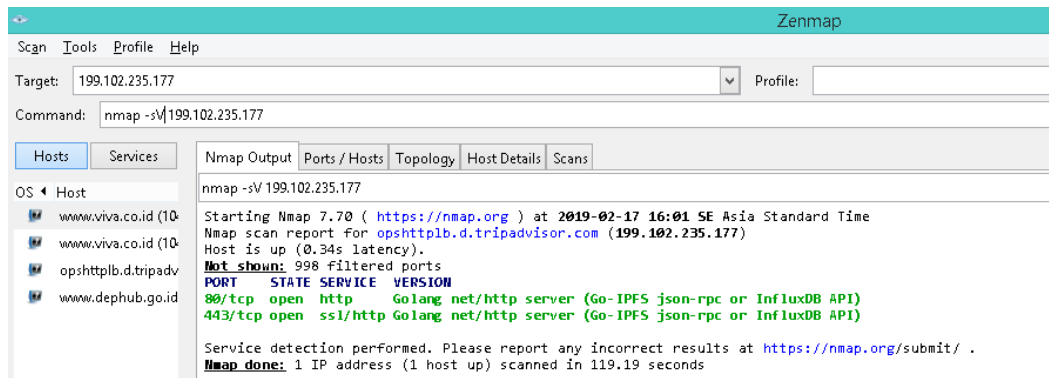
Menggunakan command *nmap -sU*



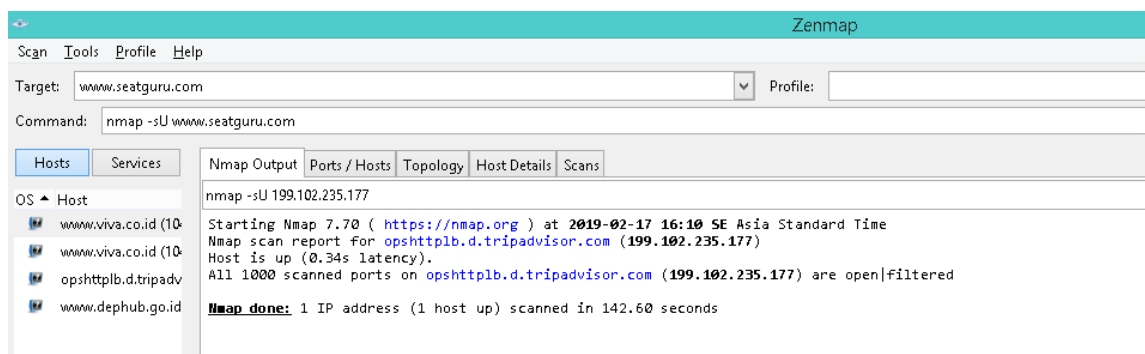
Menggunakan command *nmap -sS*



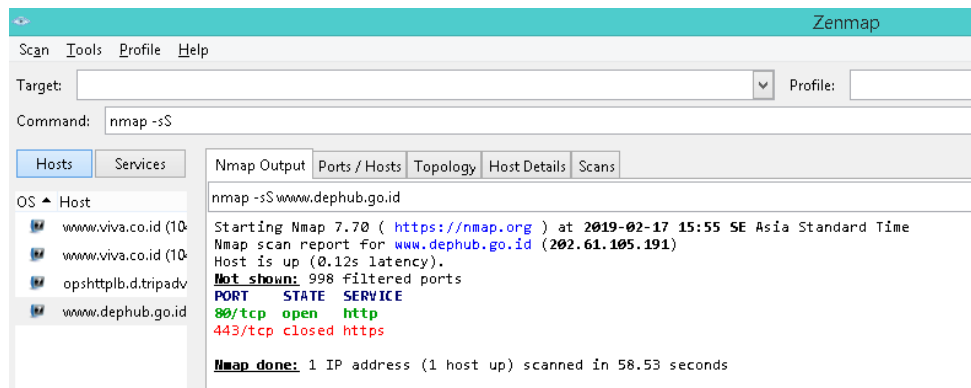
Menggunakan command *nmap -sV*



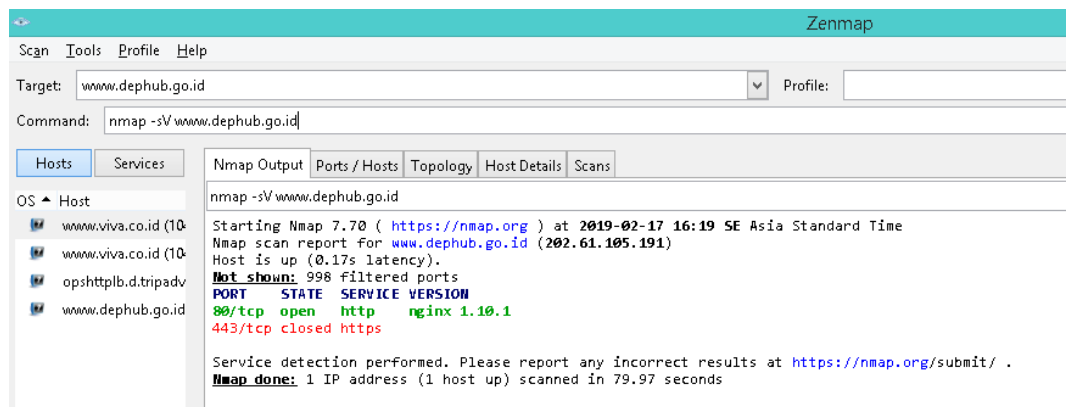
Menggunakan command *nmap -sU*



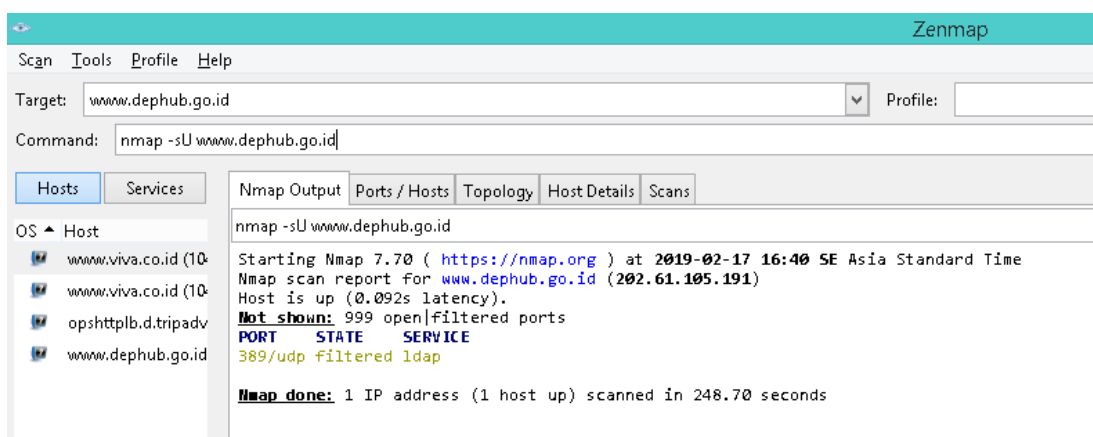
Menggunakan command *nmap -sS*



Menggunakan command *nmap -sV*



Menggunakan command *nmap -sU*



2.Scanning menggunakan Netspark

www.viva.co.id

The screenshot shows the Netsparker interface for scanning www.viva.co.id. The main window displays a vulnerability titled "Out-of-date Version (PHP)".

Vulnerability Details:

- CERTAINTY:** High (indicated by a red bar)
- URL:** <https://www.viva.co.id/sitemap.xml>
- IDENTIFIED VERSION:** 7.2.0
- LATEST VERSION:** 7.1.11
- VULNERABILITY DATABASE:** Result is based on 23/11/2017 vulnerability database content.

CLASSIFICATION:

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
OWASP PC	C1
CAPEC	310

Issues (23):

- Cookie Not Marked as Secure [3]
- Out-of-date Version (jQuery) [11]
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Insecure Frame (External) [11]
- Internal Server Error [2]
- Missing X-Frame-Options Header [11]
- Version Disclosure (PHP)
- [Possible] Phishing by Navigating Browser Tabs [11]
- [Possible] Cross-site Request Forgery in Login Form
- Referrer-Policy Not Implemented [11]
- Forbidden Resource [11]
- SameSite Cookie Not Implemented [3]
- Robots.txt Detected

Scan Information:

- Current Speed: 3.9 req/sec
- Average Speed: 4.1 req/sec
- Total Requests: 2634
- Failed Requests: 0
- HEAD Requests: 1025
- Elapsed Time: 00:10:37
- Start Time: 17/02/2019 14:57:38

www.seatgru.com

The screenshot shows the Netsparker interface for scanning www.seatgru.com. The main window displays a vulnerability titled "Out-of-date Version (Apache)".

Vulnerability Details:

- CERTAINTY:** High (indicated by a red bar)
- URL:** <https://www.seatgru.com/robots.txt>
- IDENTIFIED VERSION:** 2.4.25
- LATEST VERSION:** 2.4.29
- VULNERABILITY DATABASE:** Result is based on 23/11/2017 vulnerability database content.

CLASSIFICATION:

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
OWASP PC	C1
CAPEC	310

Issues (15):

- Version Disclosure (Apache)
- Referrer-Policy Not Implemented [6]
- Robots.txt Detected
- Missing X-XSS-Protection Header [6]
- Out-of-date Version (PHP)
- Subresource Integrity (SRI) Not Implemented [6]
- Content Security Policy (CSP) Not Implemented [6]
- HTTP Strict Transport Security (HSTS) Policy Not Enabled
- Crossdomain.xml Detected
- Apache Web Server Identified
- Out-of-date Version (Apache)
- Knowledge Base

Scan Information:

- Current Speed: 0.4 req/sec
- Average Speed: 0.9 req/sec
- Total Requests: 149
- Failed Requests: 0
- HEAD Requests: 17
- Elapsed Time: 00:02:37
- Start Time: 17/02/2019 15:09:40

www.dephub.go.id

The screenshot shows the Nessus interface for a scan of **www.dephub.go.id**. The main window displays a vulnerability titled **Out-of-date Version (PHP)** with a red severity bar. The URL is <http://www.dephub.go.id/>, the identified version is **7.0.26**, and the latest version is **7.1.11**. The vulnerability database result is based on 23/11/2017 content.

CLASSIFICATION

PCI 3.1	6.2
PCI 3.2	6.2
OWASP 2013	A9
OWASP PC	C1
CAPEC	310

VULNERABILITY DETAILS

The dashboard shows the scan progress for **Crawling & Attacking (2/3)...** at 25% completion. Scan information includes: Current Speed: 3,0 req/sec, Average Speed: 3,4 req/sec, Total Requests: 472, Failed Requests: 0, HEAD Requests: 136, Elapsed Time: 00:02:18, Start Time: 17/02/2019 15:14:21.

Issues (17)

- Password Transmitted over HTTP [3]
- Out-of-date Version (jQuery) [3]
- Insecure Frame (External) [2]
- Autocomplete Enabled [3]
- Version Disclosure (PHP)
- [Possible] Phishing by Navigating Browser Tabs [3]
- [Possible] Cross-site Request Forgery in Login Form [2]
- SameSite Cookie Not Implemented
- Referrer-Policy Not Implemented [3]
- Robots.txt Detected
- Nginx Web Server Identified
- Email Address Disclosure [11]
- Content Security Policy (CSP) Not Implemented [3]

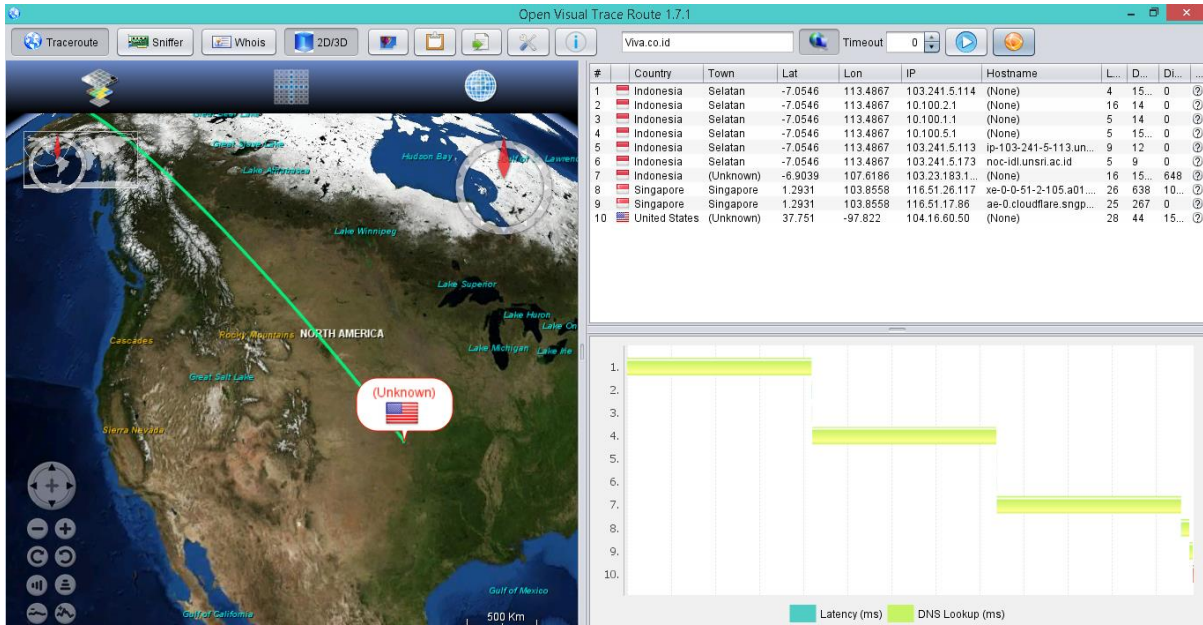
3.Scanning Menggunakan Traceroute

www.viva.co.id

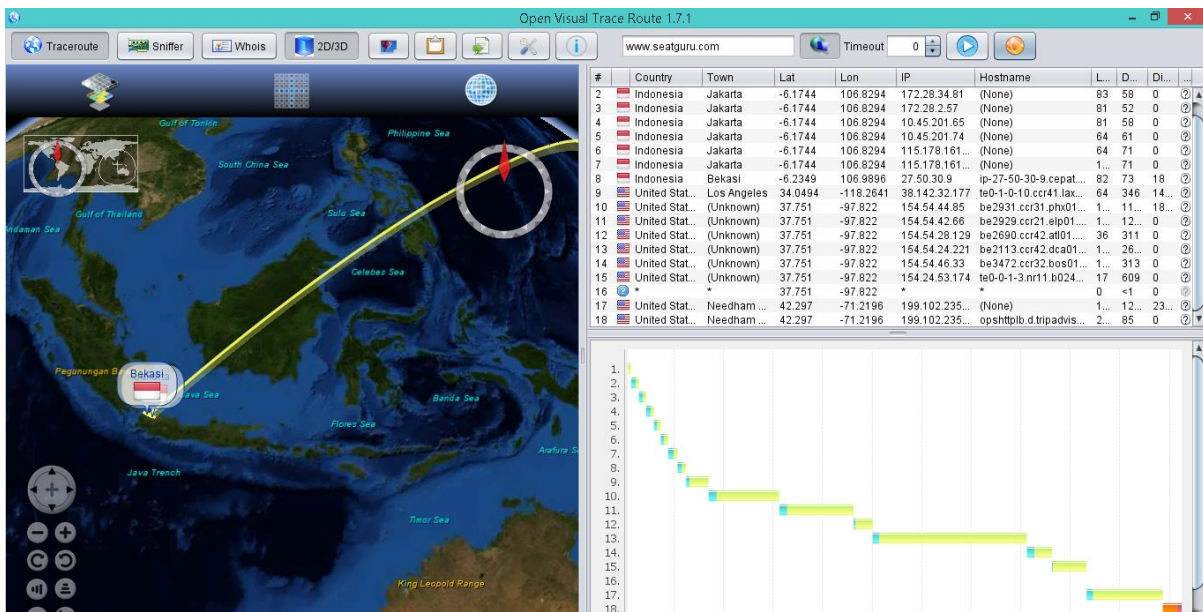
The screenshot shows the Open Visual Trace Route 1.7.1 interface for a traceroute to **Viva.co.id**. The map displays the path from Singapore through Indonesia to the destination. The table below provides the details for each hop.

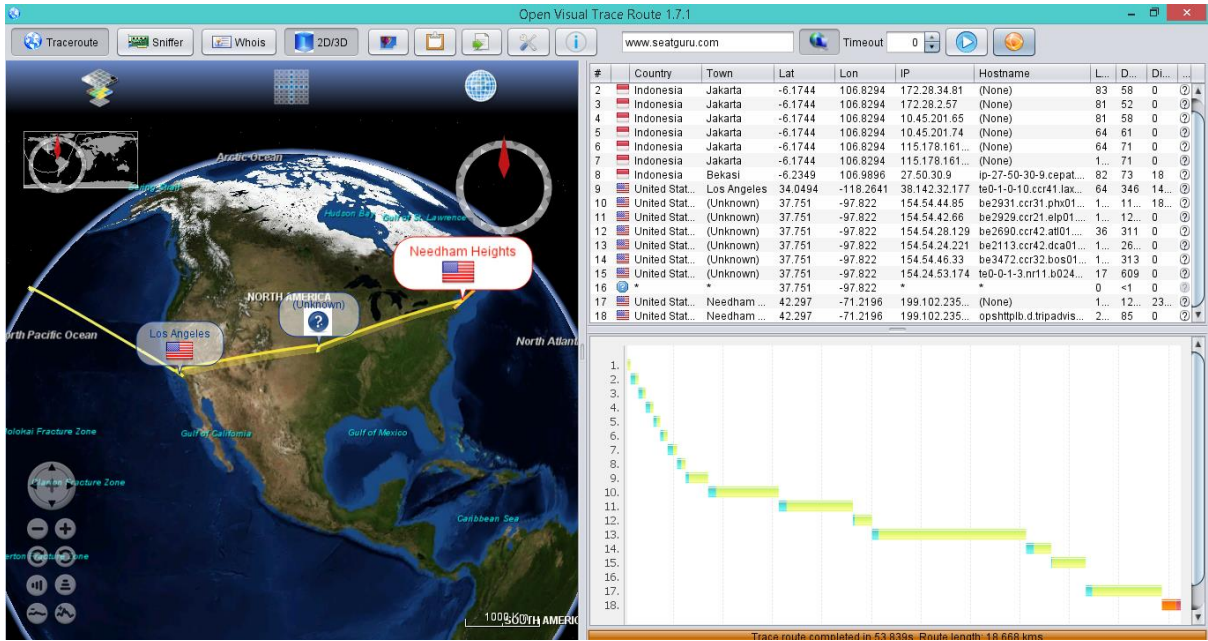
#	Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...
1	Indonesia	Selatan	-7.0546	113.4867	103.241.5.114	(None)	4	15...	0
2	Indonesia	Selatan	-7.0546	113.4867	10.100.2.1	(None)	16	14	0
3	Indonesia	Selatan	-7.0546	113.4867	10.100.1.1	(None)	5	14	0
4	Indonesia	Selatan	-7.0546	113.4867	10.100.5.1	(None)	5	15...	0
5	Indonesia	Selatan	-7.0546	113.4867	103.241.5.113	ip-103-241-5-113.un...	9	12	0
6	Indonesia	Selatan	-7.0546	113.4867	103.241.5.173	noc-id.unsri.ac.id	5	9	0
7	Indonesia	(Unknown)	-6.9039	107.6186	103.23.183.1...	(None)	16	15...	648
8	Singapore	Singapore	1.2931	103.8558	116.51.26.117	xe-0-0-51-2-105.a01...	26	638	10...
9	Singapore	Singapore	1.2931	103.8558	116.51.17.86	ae-0.cloudflare.sngp...	25	267	0
10	United States	(Unknown)	37.751	-97.822	104.16.60.50	(None)	28	44	15...

The chart below the table shows the performance metrics for each hop, with green bars representing Latency (ms) and yellow bars representing DNS Lookup (ms).



www.seatgru.com





www.dephub.go.id

