**Laboratorium**
**Multimedia dan Internet of Things**
**Departemen Teknik Komputer**
***Institut Teknologi Sepuluh Nopember***

# Laporan Akhir
# Praktikum Jaringan Komputer

## Firewall  NAT

Muhammad Rifqi Abdillah - 5024231082

2025

# 1 Langkah-Langkah Percobaan

1. Langkah pertama dalam konfigurasi jaringan adalah melakukan reset pada router untuk memastikan bahwa seluruh pengaturan kembali ke kondisi default. Setelah proses reset selesai, pengguna dapat kembali masuk (login) ke antarmuka router untuk memulai konfigurasi dari awal. Selanjutnya, sambungkan kabel jaringan dari sumber internet ke port ether1 pada Router A.
2. etelah koneksi fisik tersambung, lakukan konfigurasi DHCP Client pada ether1 agar router dapat memperoleh alamat IP dari penyedia layanan internet secara otomatis.
3. Kemudian, tambahkan pengaturan alamat IP secara manual pada ether7 yang akan digunakan sebagai jalur koneksi antara Router A dan perangkat Switch, guna mendukung distribusi jaringan lokal.
4. Langkah berikutnya adalah mengatur DHCP Server pada Router MikroTik agar dapat mendistribusikan alamat IP secara otomatis kepada perangkat-perangkat klien di jaringan lokal.
5. Untuk memungkinkan akses internet, konfigurasi NAT (Network Address Translation) perlu diterapkan, sehingga alamat IP privat dari jaringan lokal dapat diterjemahkan ke alamat IP publik saat mengakses internet. Selain itu, konfigurasi keamanan jaringan juga dilakukan dengan menambahkan aturan pada firewall menggunakan fitur Filter Rules.
6. Dalam tahap selanjutnya, konfigurasi bridge diterapkan pada Router B untuk mengubah fungsinya menjadi seperti hub atau switch, sehingga hanya bertindak sebagai perangkat penghubung antarport tanpa melakukan routing. Port-port yang akan digunakan harus ditambahkan ke dalam bridge yang telah dikonfigurasi agar fungsi bridging berjalan dengan baik. Setelah semua pengaturan jaringan selesai, pastikan pengaturan alamat IP pada laptop atau perangkat klien telah disesuaikan, yakni diatur agar memperoleh alamat IP secara otomatis melalui DHCP.
7. Langkah terakhir adalah melakukan serangkaian pengujian terhadap seluruh konfigurasi yang telah diterapkan, guna memastikan bahwa semua fungsi jaringan seperti distribusi IP, koneksi internet, firewall, dan bridging berjalan dengan baik dan sesuai harapan.

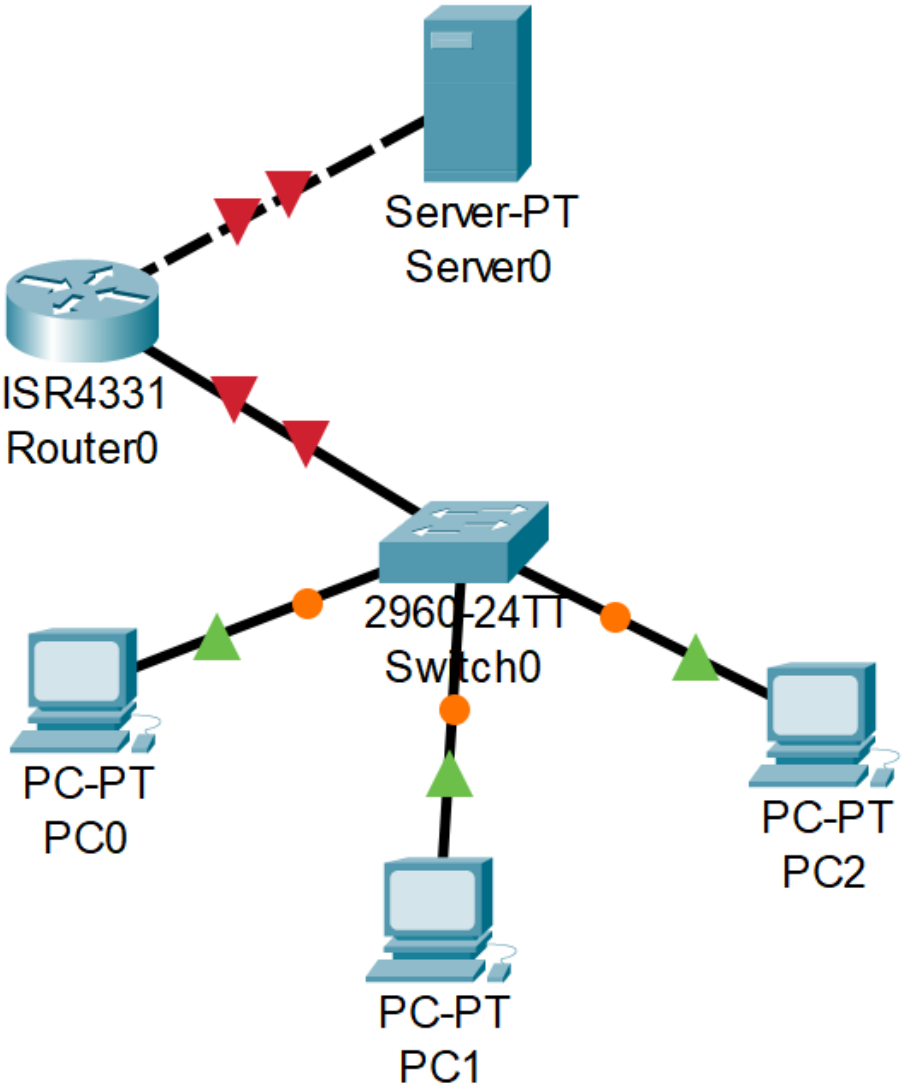
# 2 Analisis Hasil Percobaan

Praktikum berjalan dengan lancar dan didapatkan hasil seperti berikut. Penerapan NAT dengan metode masquerade memungkinkan klien mengakses internet, yang dibuktikan dengan keberhasilan ping ke 8.8.8.8. Pengujian firewall menunjukkan bahwa aturan pemblokiran ICMP dan konten seperti “speedtest” bekerja sesuai konfigurasi. Secara keseluruhan, praktikum ini membuktikan bahwa MikroTik mampu mengelola distribusi IP, koneksi internet, dan pembatasan akses secara efektif, serta memberikan pemahaman praktis mengenai manajemen jaringan.

# 3 Hasil Tugas Modul

## 1. Konfigurasi IP pada Router

```
Router> enable
```




**Gambar 1:** Hasil Tugas Modul

```
Router# configure terminal
Router(config)# interface g0/0
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface g0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

### 2. Konfigurasi IP PC dan Server

- PC1: 192.168.1.2 /24, Gateway: 192.168.1.1
- PC2: 192.168.1.3 /24, Gateway: 192.168.1.1
- PC3: 192.168.1.4 /24, Gateway: 192.168.1.1
- Server: 203.0.113.10 /24, Gateway: 203.0.113.1

### 3. Konfigurasi NAT di Router

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface g0/0 overload

Router(config)# interface g0/0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# interface g0/1
Router(config-if)# ip nat inside
Router(config-if)# exit
```

### 4. Konfigurasi Firewall (ACL)

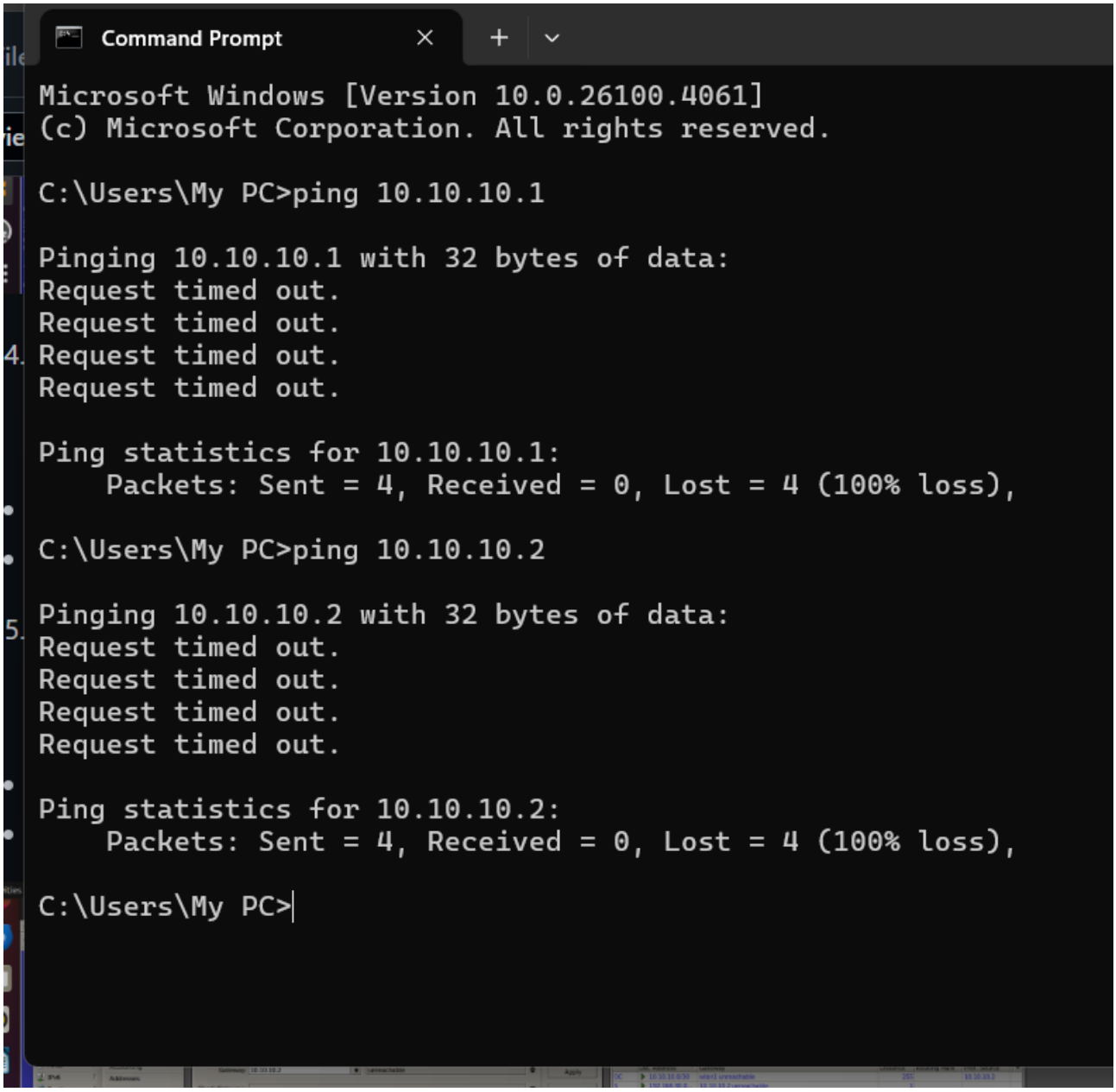
```
Router(config)# access-list 100 deny ip host 192.168.1.2 host 203.0.113.10
Router(config)# access-list 100 deny ip host 192.168.1.4 host 203.0.113.10
Router(config)# access-list 100 permit ip any any

Router(config)# interface g0/0
Router(config-if)# ip access-group 100 out
Router(config-if)# exit
```

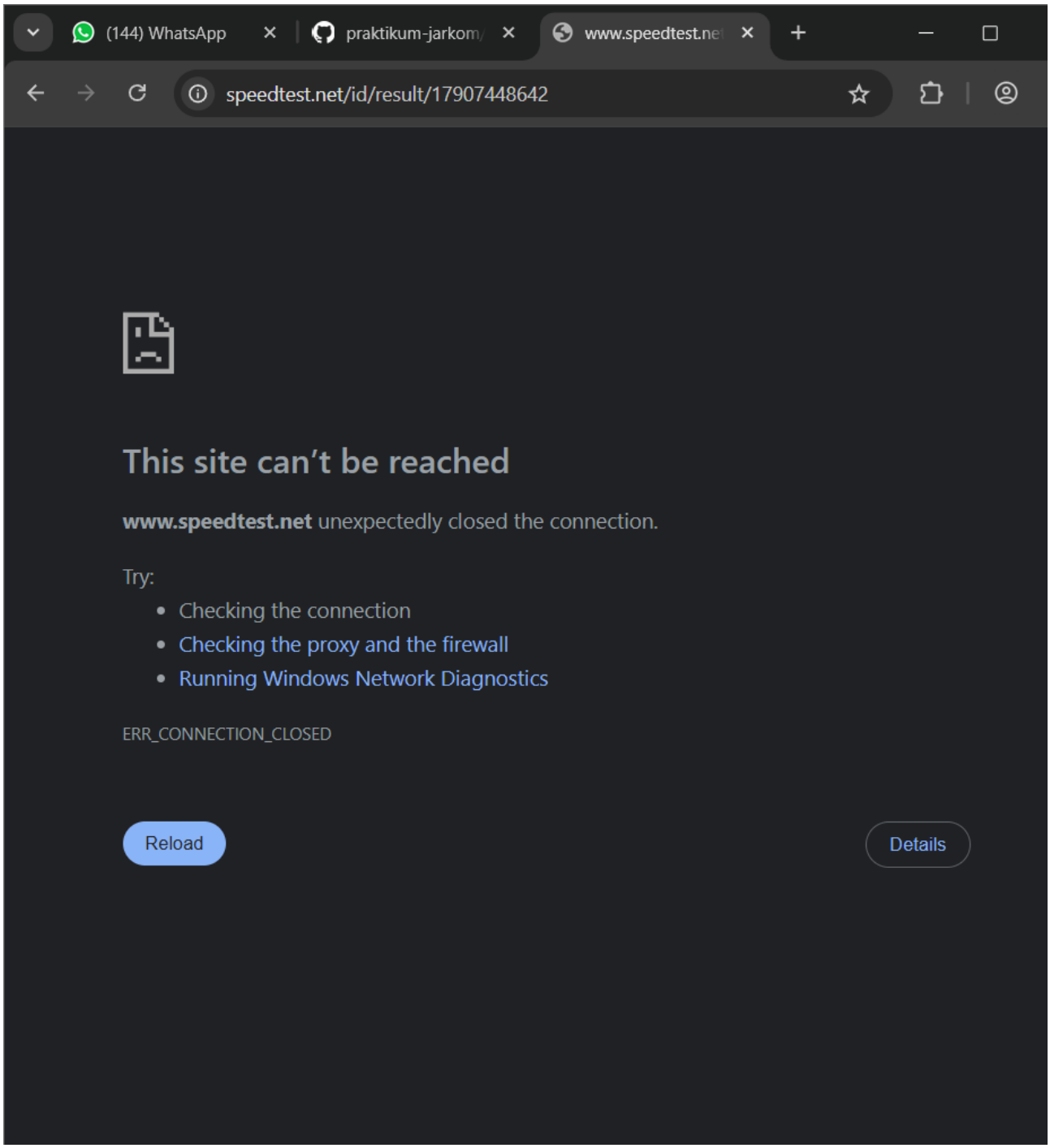
# 4 Kesimpulan

Penggunaan firewall berfungsi untuk mengamankan jaringan dengan cara menyaring lalu lintas data berdasarkan aturan tertentu. Melalui konfigurasi firewall, administrator jaringan dapat membatasi akses antarperangkat, memblokir protokol tertentu seperti ICMP, atau memfilter konten dan situs web yang tidak diinginkan. Fitur ini terbukti efektif dalam menjaga keamanan dan kontrol lalu lintas jaringan, seperti ditunjukkan saat pemblokiran ping dan akses ke situs tertentu berhasil dijalankan sesuai aturan yang ditetapkan. Network Address Translation (NAT) memungkinkan perangkat di jaringan lokal dengan IP privat untuk mengakses internet menggunakan satu alamat IP publik. Dengan menerapkan metode masquerade, router dapat menyamarkan alamat IP lokal dan meneruskannya ke jaringan luar, sekaligus menjaga struktur internal jaringan tetap tersembunyi. NAT juga berperan dalam efisiensi penggunaan IP publik dan memberikan perlindungan dasar terhadap akses langsung dari luar jaringan.

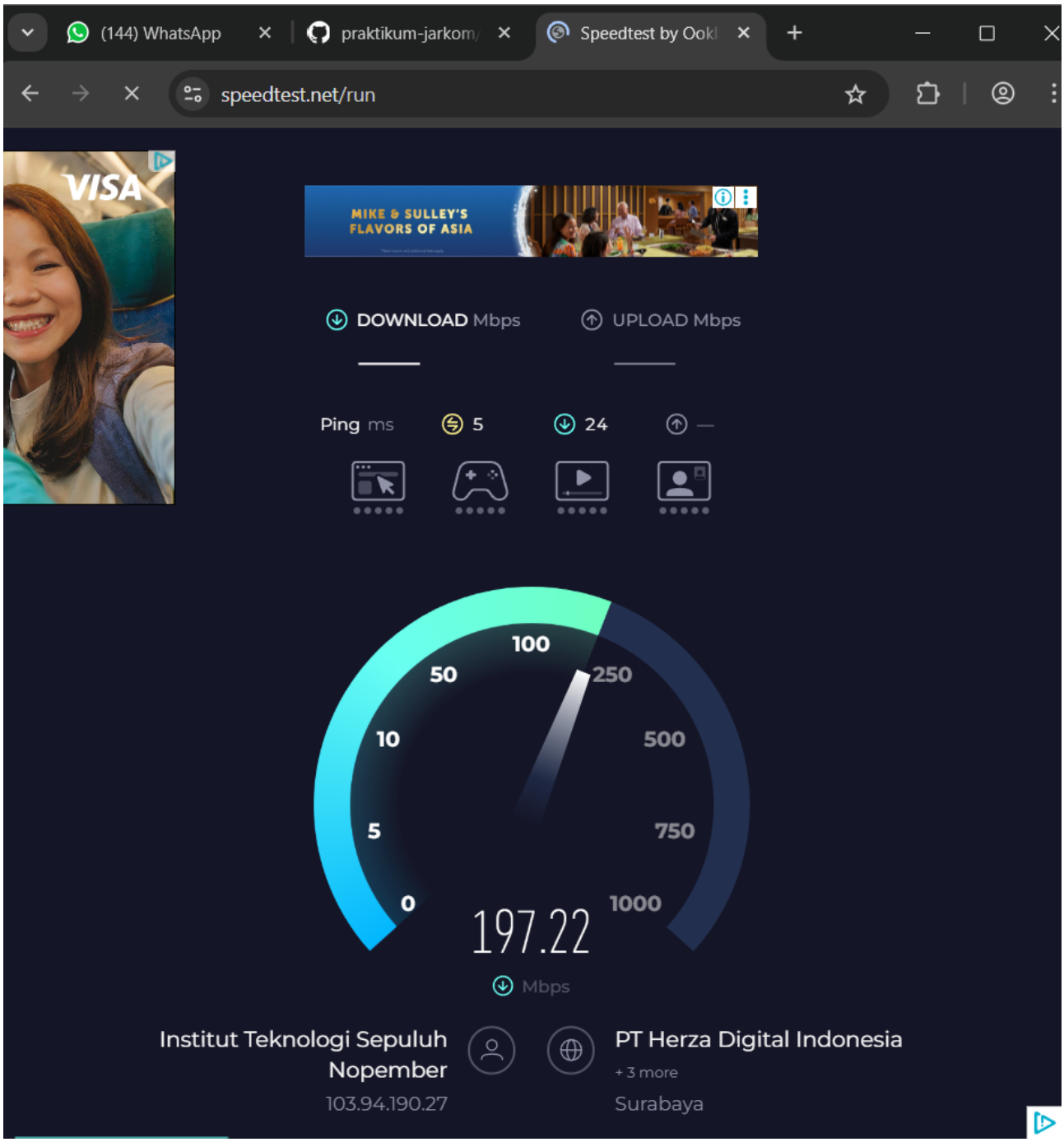
# 5 Lampiran




**Gambar 2:** Tes Ping




**Gambar 3:** Pencarian Terblokir




**Gambar 4:** Pencarian Speedtest Terblokir