BAB 3
METODE PENELITIAN

3.1 ALAT YANG DIGUNAKAN

3.1.1 PERANGKAT KERAS

Perangkat keras yang akan digunakan pada penelitian ini menggunakan 1 laptop, 1 *smartphone*, dan 1 *router* dengan spesifikasi sebagaimana terdapat pada Tabel 3.1.

Tabel 3. 1 Spesifikasi Perangkat Keras

Kategori	**Spesifikasi**	
Laptop	OS	Windows 11
	Processor	AMD Ryzen 3 5300U 2.6 GHz
	System Memori (RAM)	8 GB
	Storage (SSD)	512 GB
Smartphone	OS	Android
	Processor	Snapdragon 750
	System Memori (RAM)	6 GB
	Storage	128 GB
Router	OS	Mikrotik
	System Memori (RAM)	128 MB
	NAND *Storage*	128 MB

3.1.2 PERANGKAT LUNAK

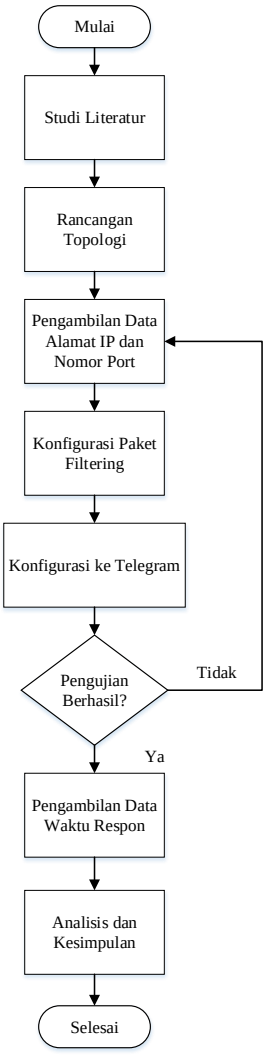
Perangkat lunak sebagai *tool* dan aplikasi yang akan digunakan pada penelitian ini yaitu sebuah *software* winbox dan aplikasi pesan instan Telegram seperti yang terlihat pada Tabel 3.2.

Tabel 3. 2 *Tools* dan Aplikasi

No	*Software*	Versi	Fungsi
1	*Winbox*	3.37 (64 Bit)	Konfigurasi *Packet Filtering* pada Mikrotik
2	Telegram	9.3.3	Sebagai penerima notifikasi

3.2 ALUR PENELITIAN

Penelitian ini dilakukan dengan melalui beberapa tahapan seperti pada diagram alur yang ditunjukkan pada Gambar 3.1.



Gambar 3. 1 Alur Penelitian

Gambar 3.1 menunjukan diagram alur perancangan sistem dalam penelitian ini. Langkah pertama dalam penelitian yaitu melakukan studi literatur beberapa penelitian terkait dengan pemblokiran akses internet dengan melakukan konfigurasi *packet filtering* pada *router* serta materi lain yang berhubungan dengan penelitian ini. Dengan membandingkan beberapa jurnal terkait dan melakukan perbandingan untuk menentukan judul dan juga fokus dari penelitian ini. Selain membandingkan dan menentukan fokus atau judul penelitian, tahap ini juga berfungsi untuk memahami konsep dasar dari topik tersebut.

Selanjutnya adalah menentukan rancangan topologi yang digunakan sebagai dasar dari arsitektur jaringan untuk membuat sistem yang mampu memblokir beberapa situs judi *online*, media sosial, dan *game online*. Topologi tersusun atas 1 buah *router mikrotik* yang digunakan untuk melakukan konfigurasi *packet filtering*, 3 buah laptop, dua di antaranya berperan sebagai *client* dan salah satunya menjadi *administrator system*, serta 3 buah *smartphone* sebagai *client*. Langkah selanjutnya adalah melakukan pengambilan data pertama dengan fitur *torch* yang merupakan salah satu *tools* pada *mikrotik* yang digunakan untuk melihat trafik jaringan secara *realtime* atau dapat dilakukan dengan menggunakan *tools nslookup* pada *command prompt* (cmd) dan akan memperoleh data yang berupa alamat IP dari situs judi *online*, media sosial, dan *game online* yang nantinya akan dikonfigurasi pada *mikrotik* di menu *filter rules* dengan cara memasukkan *chain* yang dipilih yaitu *chain forward* dengan protokol TCP/UDP, kemudian masukkan alamat IP dari situs judi *online*, media sosial, dan *game online* yang akan diblokir pada kolom *destination address*. Pilih *action drop* agar paket tersebut ditolak atau tidak diijinkan masuk. Selanjutnya melakukan konfigurasi pada *mikrotik* (*winbox*) agar ketika terjadi pelanggaran dalam pengaksesan internet *administrator system* akan menerima notifikasi melalui Telegram.

Setelah melakukan konfigurasi pada *mikrotik*, selanjutnya adalah melakukan pengujian dengan melakukan akses terhadap situs judi *online*/media sosial/*game online* apakah alamat IP yang didapatkan pada pengambilan data pertama berhasil diblokir atau tidak, jika berhasil maka langkah selanjutnya adalah melakukan pengambilan data kedua yang berupa waktu respon dari sistem notifikasi yang dilakukan sebanyak 20 kali kemudian diambil nilai rata-ratanya.

Selanjutnya data-data yang sudah diperoleh dikumpulkan dalam bentuk Tabel yang nantinya akan dianalisis dengan cara melihat *filter rules* apakah berhasil melakukan pemblokiran atau tidak dengan menggunakan alamat IP yang telah diperoleh serta menganalisis mengenai respon dari sistem notifikasi, setelah itu diambil kesimpulan ketika sudah selesai melakukan analisis.

3.3 RANCANGAN TOPOLOGI

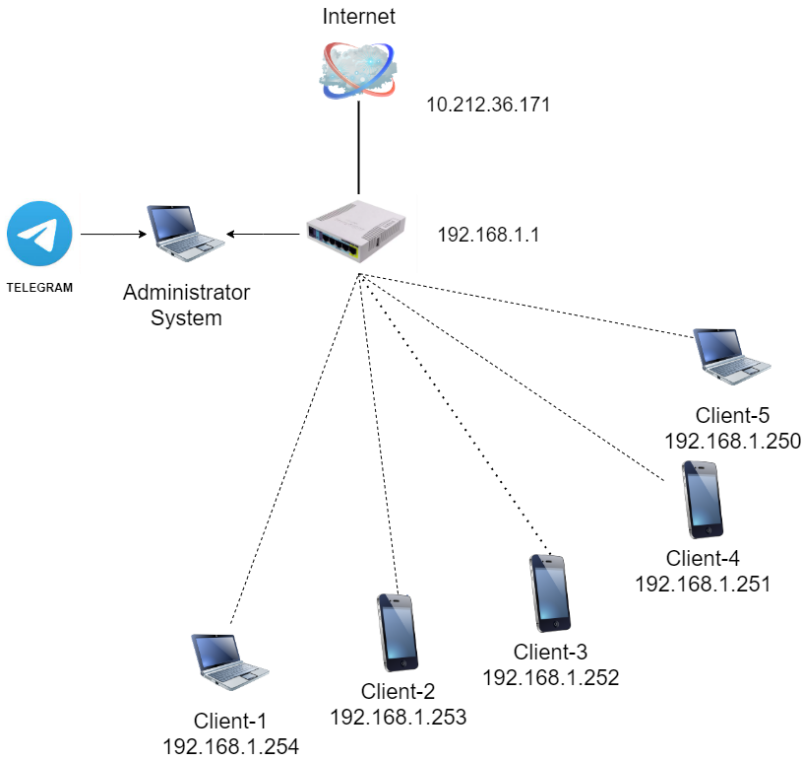
Rancangan topologi yang digunakan sebagai dasar dari arsitektur jaringan untuk membuat sistem yang mampu memblokir beberapa situs judi *online*, media sosial, dan *game online* terlihat seperti pada Gambar 3.2 yang tersusun atas sebuah koneksi internet yang disediakan oleh internet *service provider* dengan spesifikasi seperti yang terlihat pada Tabel 3.3, 1 buah *router* mikrotik yang digunakan untuk melakukan konfigurasi *packet filtering*, 3 buah laptop, dua di antaranya berperan sebagai *client* dan salah satunya menjadi *administrator system*, serta 3 buah *smartphone* sebagai *client*. Pada topologi ini, mikrotik berperan sebagai DHCP *server* yang mengatur dan memberikan alamat IP secara otomatis kepada *client*, contohnya perangkat laptop dan *smartphone* yang disebut sebagai DHCP *client* karena perangkat-perangkat tersebut menerima alamat IP dari DHCP *server*. Alamat IP yang diberikan oleh DHCP *Server* yaitu alamat IP dengan *subnet mask* /24 yang mana memiliki *range* dari 192.168.1.1 sampai 192.168.1.254. Untuk Mikrotik sendiri mendapatkan alamat IP 192.168.1.1 dengan *subnet mask* 255.255.255.0, sedangkan untuk perangkat *client* mendapatkan alamat IP dengan *range* 192.168.1.2 sampai 192.168.1.254 dengan *subnet mask* 255.255.255.0. *Client* dapat melakukan *browsing* dikarenakan terdapat suatu proses yang disebut NAT. Dimana proses tersebut berfungsi untuk mentranslasikan dari alamat IP *Private* yaitu 192.168.1.x ke alamat IP Publik dengan alamat IP 10.212.36.17. Proses tersebut terjadi di *Mikrotik.*

Perangkat-perangkat *client* tersebut, terhubung secara *wireless* dengan Mikrotik. *Administrator system* disini bertugas melakukan konfigurasi *packet filtering* yaitu dengan membuat beberapa *rules*, serta melakukan konfigurasi ke Telegram yang berfungsi untuk memberikan notifikasi, baik konfigurasi Telegram pada Mikrotik maupun pada laptop. Sehingga, ketika terjadi pengaksesan yang

tidak sesuai dengan *rules*, maka Mikrotik akan memberikan notifikasi kepada *Administrator System* melalui Telegram, yang mana notifikasi tersebut dapat diakses oleh *Administrator System* melalui laptop atau *smartphone*.

Tabel 3. 3 Spesifikasi Koneksi Internet

Kecepatan Internet	10 Mbps
Frekuensi *WiFi*	2,4 GHz
Lebar *Bandwidth*	20 MHz

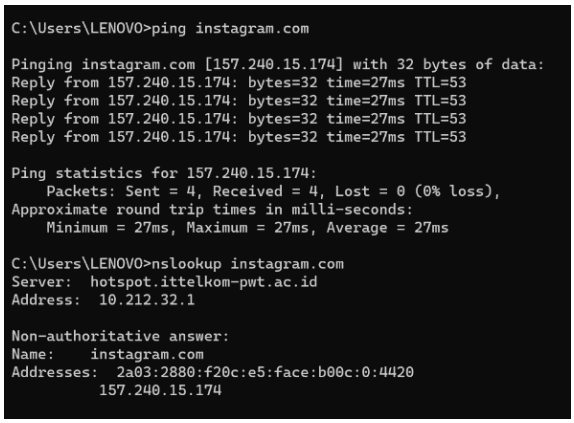


Gambar 3. 2 Topologi Jaringan

3.4 KONFIGURASI *PACKET FILTERING* PADA MIKROTIK

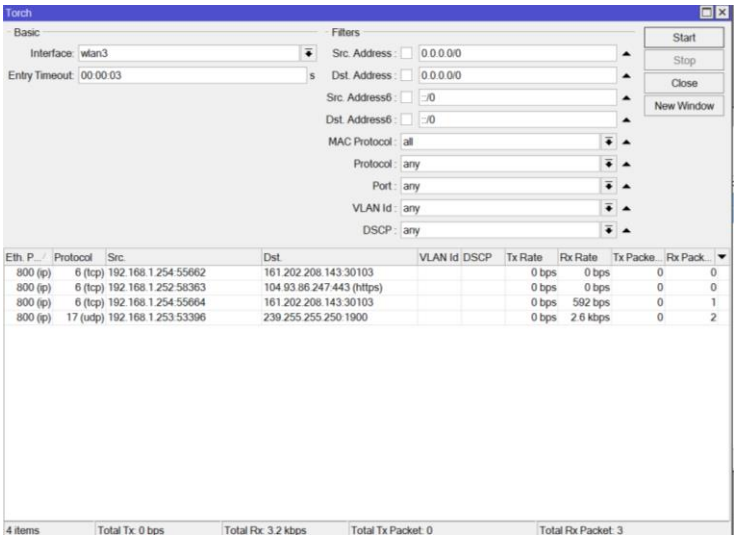
Pada penelitian ini, pemblokiran akan dilakukan dengan menggunakan *packet filtering* dengan berdasarkan alamat IP, nomor *port*, serta protokol yang digunakan, baik yang digunakan oleh situs, media sosial maupun *game online*. Namun sebelum melakukan konfigurasi *packet filtering*, pastikan sudah melakukan pengumpulan alamat IP mana saja yang akan diblokir dengan menggunakan fitur *torch*. Fitur *torch* merupakan salah satu *tools* pada mikrotik yang digunakan untuk

melihat trafik jaringan secara *realtime* atau dapat dilakukan dengan menggunakan *tools nslookup* pada *command prompt* (cmd).



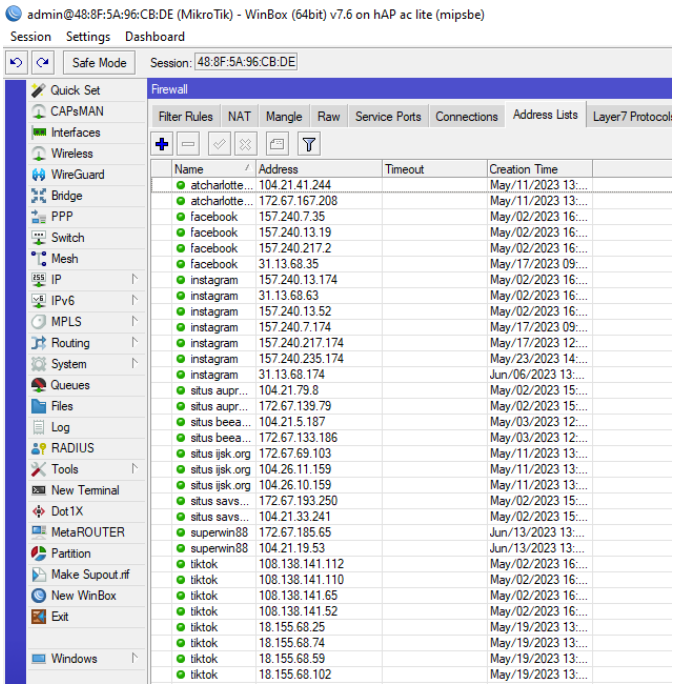
Gambar 3. 3 *Tools nslookup* pada *command prompt* (cmd)

Pada Gambar 3.3 peneliti menggunakan *tools nslookup* pada *command prompt* (cmd) untuk memperoleh alamat IP yang digunakan oleh Instagram yang akan diblokir. Pada Gambar 3.4 berikut merupakan tampilan dari fitur *torch* pada mikrotik yang berguna untuk memperoleh alamat IP (sekaligus nomor port yang membawanya).



Gambar 3. 4 Fitur *torch* pada mikrotik

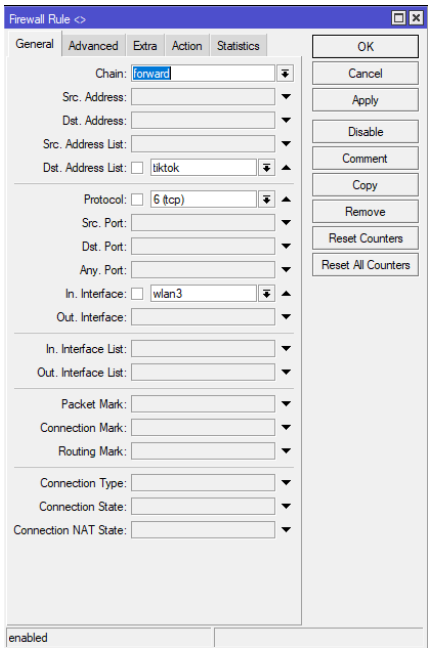
Setelah memperoleh beberapa alamat IP, selanjutnya alamat IP tersebut kemudian akan dikumpulkan pada menu *address lists* di *software winbox* seperti yang terlihat pada Gambar 3.5.



Gambar 3. 5 *Address Lists*

Konfigurasi *packet filtering* dilakukan dengan menggunakan alamat IP yang berhasil dikumpulkan pada menu *address lists* dan nomor *port* yang berhasil di-*capture* pada fitur *torch*, konfigurasi dilakukan pada *software winbox*, berikut proses konfigurasi *packet filtering*:

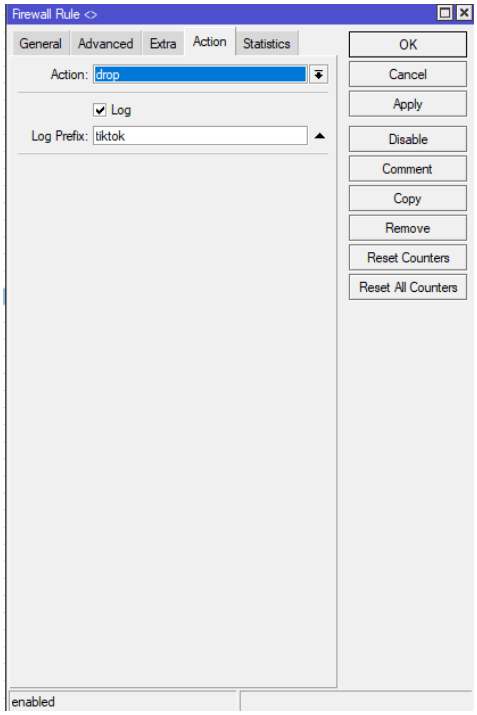
1. Membuat *New Filter Rules*



Gambar 3. 6 *Filter Rules*

Pada menu *new filter rules* seperti Gambar 3.6, dilakukan konfigurasi dengan memasukkan *chain forward*, protokol TCP/UDP, *In Interface* mana yang akan diberi kebijakan atau aturan. Untuk situs judi dan media sosial, *rules* atau aturan yang dibuat itu berdasarkan alamat IP yang digunakan, sehingga peneliti memasukkan alamat IP dari situs judi *online* dan media sosial seperti yang terlihat pada Gambar 3.6 pada kolom *dst. Address*. Sedangkan untuk *game online*, *rules* atau aturan yang dibuat itu berdasarkan nomor *port* yang digunakan, sehingga peneliti memasukkan nomor *port* berapa saja yang digunakan oleh *game online* pada kolom *dst. Port.*

2. Membuat *Action*



Gambar 3. 7 *Action* pada *Firewall Rules*

Pada Gambar 3.7, konfigurasi kolom *action* dengan *action drop* agar paket tersebut ditolak atau tidak diijinkan masuk. Selanjutnya melakukan pengelompokkan alamat IP yang didapatkan sesuai dengan kategorinya yang disebut log prefix. Misal tiktok, nantinya pada log mikrotik dan notifikasi Telegram akan muncul informasi sedang mengakses tiktok.

Packet Filtering akan bekerja ketika user mengakses *rules* yang telah dibuat. Sederhananya yaitu jika *administrator* sudah mengkonfigurasi *packet*

filtering terhadap alamat IP yang digunakan oleh tiktok (memblokir tiktok) maka ketika *client* melakukan akses ke tiktok akan ditolak. Dalam konfigurasi *packet filtering* ini diperlukan beberapa *sample* alamat IP dari situs dan media sosial yang akan diblokir seperti yang dapat dilihat pada Tabel 3.4. alamat IP tersebut diperoleh dengan menggunakan *tools nslookup* di *command prompt* (cmd).

Tabel 3. 4 Daftar alamat situs dan media sosial yang akan diblokir beserta IP-nya

Kategori	**Alamat**	***IP***
Situs (*Website*)	www.atcharlotte.org	104.21.41.244 172.67.167.208
	www.lk21.com	172.67.163.225 202.169.44.80
	www.ijsk.org	172.67.69.103 104.26.11.159 104.26.10.159
	www.superwin303.com	172.67.185.65 104.21.19.53
	www.savshow.com	104.21.33.241 172.67.193.250
Media Sosial	www.facebook.com	31.13.68.35 157.240.208.35
	www.youtube.com	172.217.194.136 172.217.194.91 172.217.194.93 172.217.194.190
	www.instagram.com	31.13.68.174 31.13.95.174
	www.tiktok.com	23.38.195.90 108.138.141.65 108.138.141.52 108.138.141.112 108.138.141.110
	www.twitter.com	104.244.42.193 104.244.42.129 104.244.42.1

Pada Tabel 3.5 berikut merupakan daftar aplikasi game online yang diblokir dengan menggunakan nomor *port*. Nomor *port* diperoleh dengan menggunakan fitur *torch* pada mikrotik.

Tabel 3. 5 Daftar Aplikasi *Game Online*

Kategori	**Game Online**				
Alamat/Aplikasi	**Mobile Legend**	**PUBG Mobile**	**Free Fire**	**Clash Royale**	**Stumble Guys**
Port					

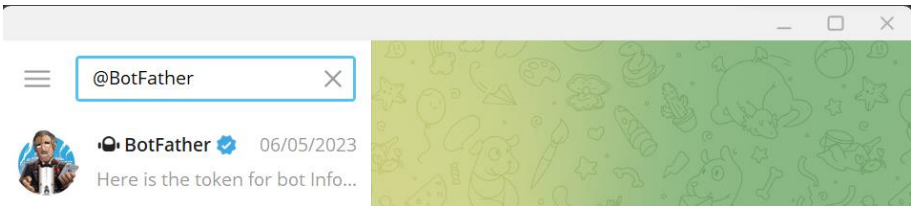
3.5 KONFIGURASI KE TELEGRAM

Setelah melakukan konfigurasi *packet filtering*, selanjutnya adalah melakukan konfigurasi ke Telegram yang dilakukan oleh *administrator system* pada laptop/PC dan Mikrotik. Konfigurasi ini digunakan untuk membuat pesan notifikasi Telegram yang kemudian akan diterima oleh *administrator system*. Untuk konfigurasi ke Telegram terdapat dua opsi, yaitu dapat menggunakan laptop/PC jika masih ada kaitannya dengan konfigurasi *packet filtering*, namun jika semua

konfigurasi *packet filtering* sudah stabil, konfigurasi ke Telegram dapat dilakukan dengan menggunakan *smartphone*.

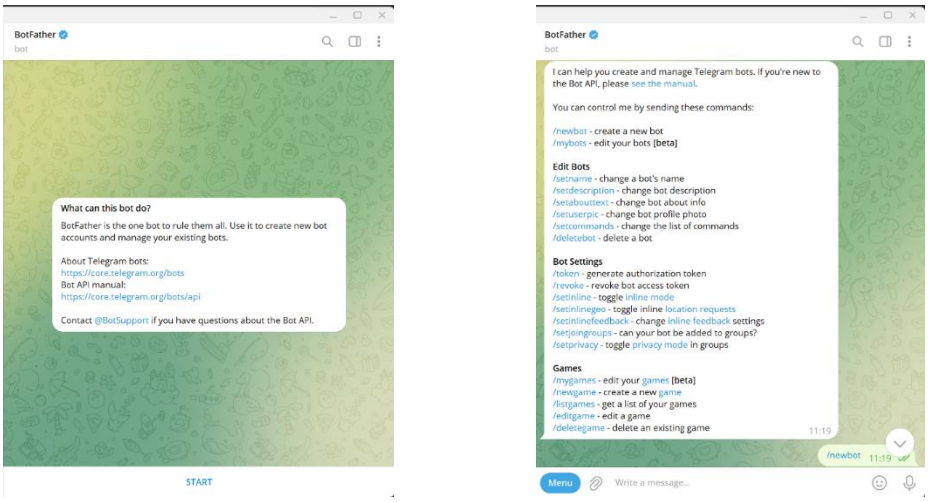
3.5.1 Konfigurasi Telegram di Laptop/PC (*Administrator System*)

Langkah awal konfigurasi Telegram di laptop/PC yaitu dengan melakukan pembuatan bot pada aplikasi Telegram desktop. Pembuatan bot dilakukan dengan menggunakan sebuah bot yang bernama @BotFather. @BotFather merupakan akun bot O*fficial* Telegram yang berfungsi untuk membuat bot Telegram. Pertama, pada *search* Telegram ketik @BotFather seperti pada Gambar 3.8 kemudian buka botnya dengan cara klik bot yang bercentang biru.



Gambar 3. 8 Bot Father

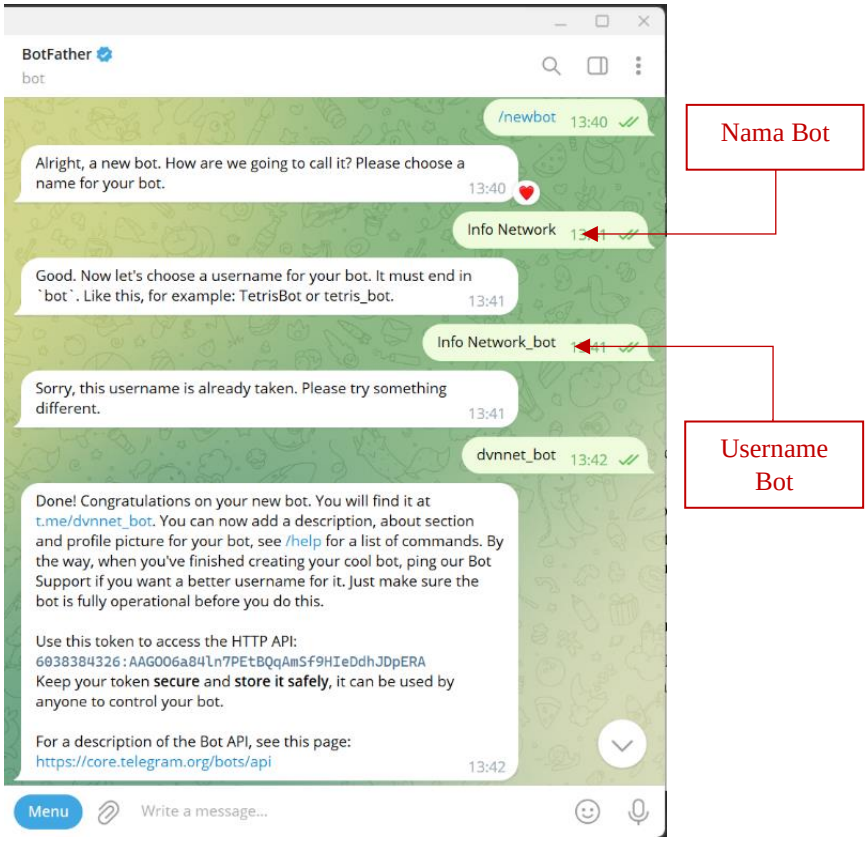
Setelah membuka botnya maka muncul tampilan seperti pada Gambar 3.9 (a) kemudian klik “start“ lalu pilih “newbot” pada tampilan seperti Gambar 3.9 (b) untuk melakukan proses pembuatan bot baru Telegram.



(a) **(b)**

Gambar 3. 9 (a) Tampilan Awal Bot Father (b) Menu Bot Father

Kemudian masukkan nama bot dan *username* untuk bot baru tersebut seperti pada Gambar 3.10. Disini peneliti menamai botnya dengan sebutan Info Network dengan *username* @dvnnet_bot lalu @BotFather akan mengirimkan sebuah token bot API Telegram yang digunakan untuk mendukung komunikasi dengan API Telegram.

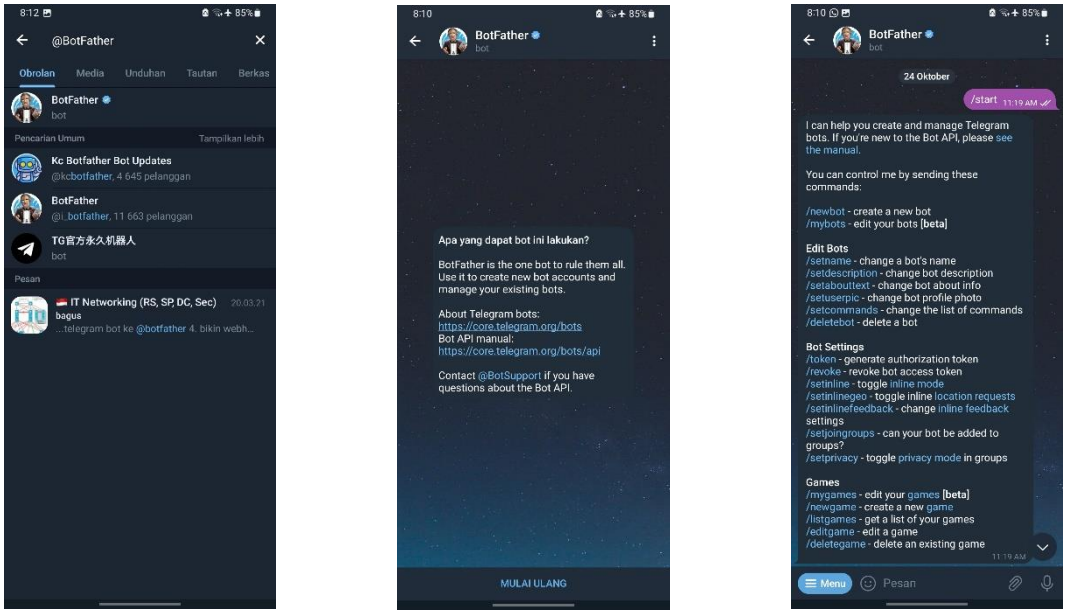


Gambar 3. 10 Proses Pembuatan Bot Telegram pada Laptop/PC

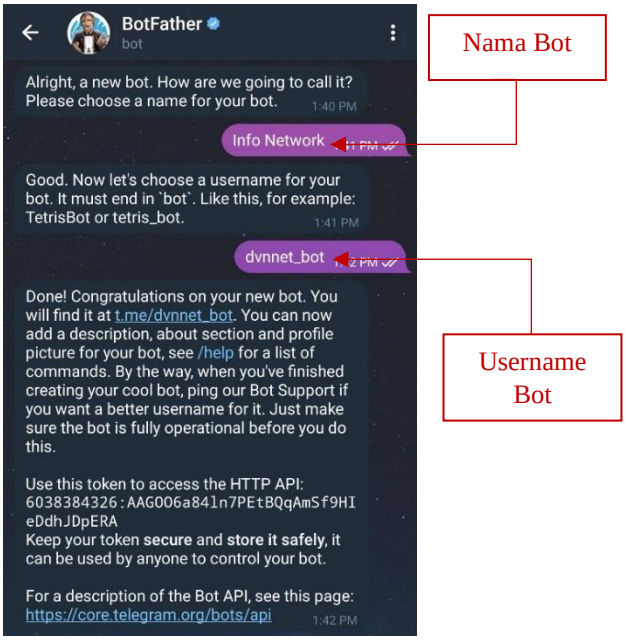
3.5.2 Konfigurasi Telegram di Smartphone (*Administrator System*)

Langkah awal konfigurasi Telegram di *smartphone* sama dengan konfigurasi di laptop yaitu dengan melakukan pembuatan bot pada aplikasi Telegram. Pembuatan bot dilakukan dengan menggunakan sebuah bot yang bernama @BotFather. @BotFather merupakan akun bot O*fficial* Telegram yang berfungsi untuk membuat bot Telegram. Pertama, pada *search* Telegram ketik @BotFather seperti pada Gambar 3.11 (a) kemudian buka botnya dengan cara klik bot yang bercentang biru.

Setelah membuka botnya maka muncul tampilan seperti pada Gambar 3.11 (b) kemudian klik “start” lalu pilih “newbot” pada tampilan seperti Gambar 3.11 (c) untuk melakukan proses pembuatan bot baru Telegram.



(a) **(b)** **(c)**



(d)

Gambar 3. 11 (a) *Search* Bot Father (b) Tampilan Awal Bot Father (c) Menu Bot Father (d) Proses Pembuatan Bot pada *Smartphone*

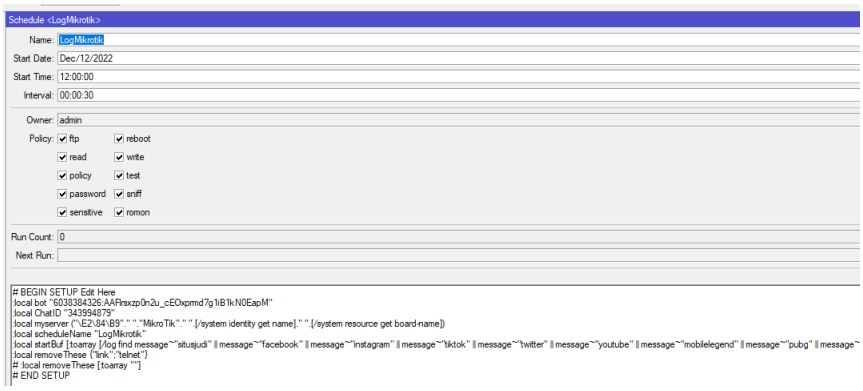
Kemudian masukkan nama bot dan username untuk bot baru tersebut seperti pada Gambar 3.11 (d). Disini peneliti menamai botnya dengan sebutan Info Network dengan username @dvnnet_bot lalu @BotFather akan mengirimkan sebuah token bot API Telegram yang digunakan untuk mendukung komunikasi dengan API Telegram.

3.5.3 Konfigurasi Telegram di Mikrotik

Setelah melakukan konfigurasi Telegram baik pada laptop maupun *smartphone*, selanjutnya adalah melakukan konfigurasi ke Telegram di Mikrotik yang dilakukan pada *software winbox*. Pada tahap ini, peneliti memasukkan sebuah *script* [33] dan *log prefix* ke *system scheduler* pada Mikrotik. *Script* dan *Log prefix* tersebut digunakan untuk membuat notifikasi yang kemudian akan diterima oleh *administrator system* melalui Telegram. Berikut proses konfigurasi ke Telegram:

1. Membuat *System Scheduler*

   System scheduler merupakan menu pada *software winbox* yang digunakan untuk memasukkan *script*. *Script* tersebut terdapat token bot API Telegram agar dapat membaca serta mengirim *log prefix* ke Telegram. *Script* akan dimasukkan pada *on event* yang terlihat seperti pada Gambar 3.12.



Gambar 3. 12 *Scheduler*

3.6 PENGUJIAN SISTEM

Pengujian konfigurasi *rules packet filtering* merupakan langkah selanjutnya yang dilakukan pada perangkat *client* dengan cara mengakses situs judi *online*, media sosial, dan *game online* yang sudah dikonfigurasi sebelumnya. Skenario

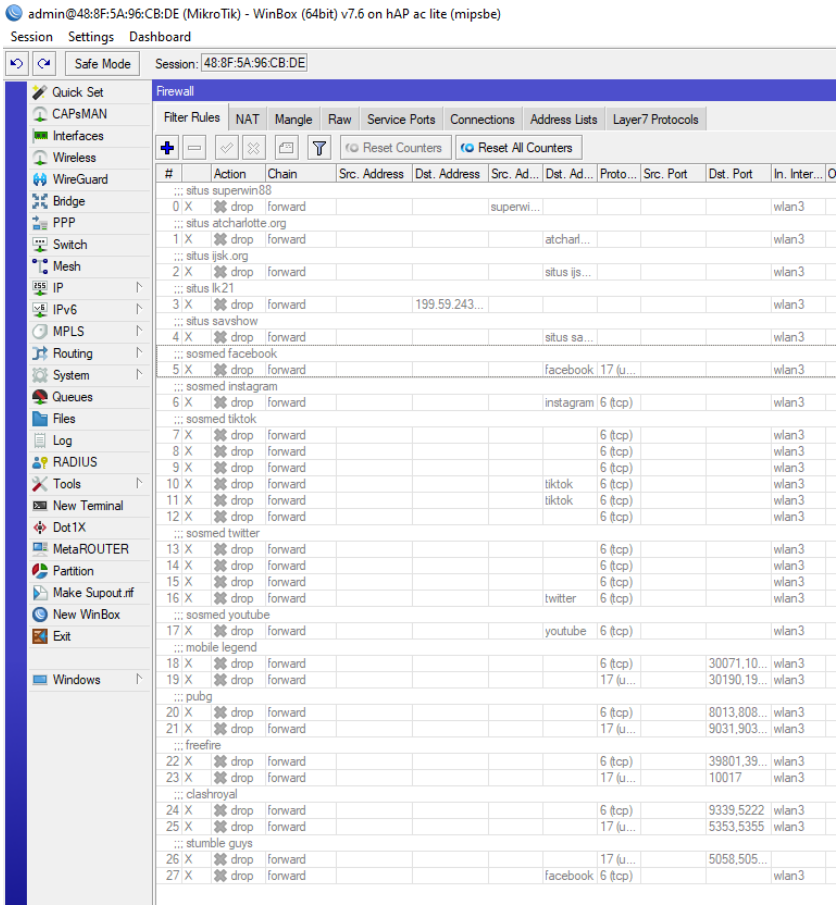
pengujian sistem yang dilakukan yaitu pada saat sebelum *rules* aktif dan sesudah *rules* aktif. Hasil dari pengujian akan dimasukkan ke dalam Tabel 3.6.

Tabel 3. 6 Pengujian pemblokiran

Kategori	Alamat/Aplikasi	Hasil Pengujian
Situs (*Website*)	www.atcharlotte.org	
	www.lk21.com	
	www.ijsk.org	
	www.superwin303.com	
	www.savshow.com	
Media Sosial	www.facebook.com	
	www.instagram.com	
	www.tiktok.com	
	www.twitter.com	
	www.youtube.com	
Game Online	Mobile Legend	
	Pubg Mobile	
	FreeFire	
	Clash Royale	
	Stumble Guys	

3.6.1 Pengujian Sebelum *Rules* Aktif

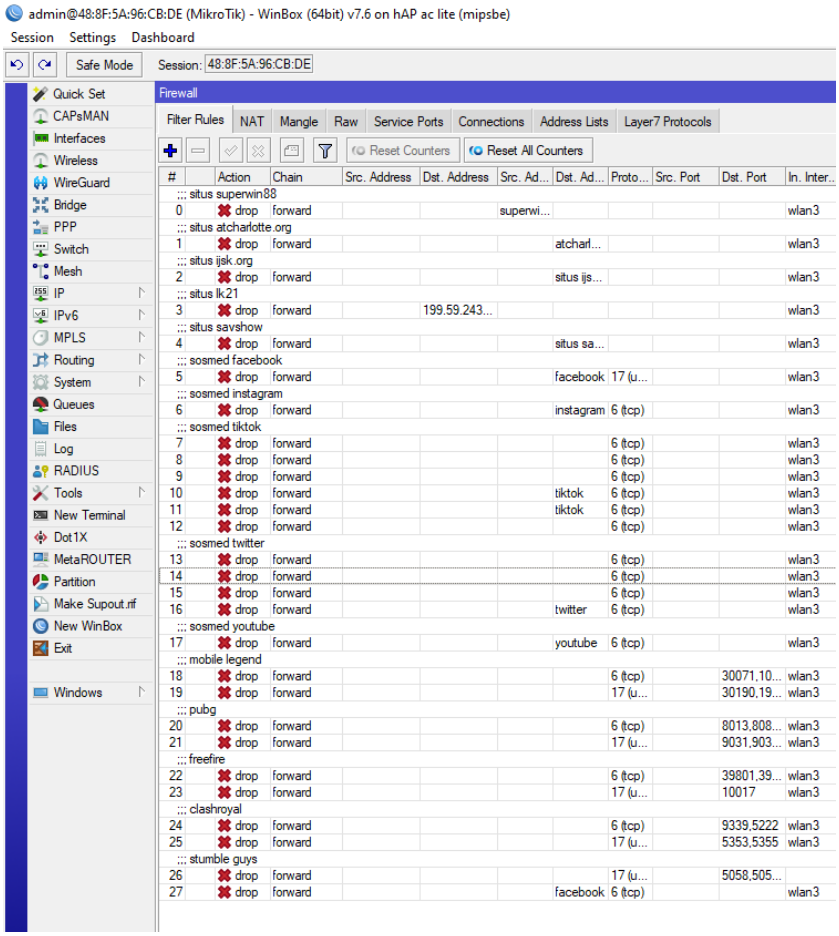
Pada pengujian kali ini yang dilakukan adalah ketika tidak ada *rules* atau aturan sama sekali, maka paket data yang masuk dengan alamat IP dan nomor *port* berapapun serta protokol apapun yang digunakan akan dapat melewati *router* tanpa ada pencocokan aturan terlebih dahulu oleh *firewall* (paket data diteruskan). Pada saat *rules* tidak aktif maka menu rules akan terlihat "*freeze*" seperti pada Gambar 3.13.



Gambar 3. 13 *Rules Packet Filtering* Tidak Aktif

3.6.2 Pengujian Sesudah *Rules* Aktif

Pada pengujian kali ini yang dilakukan adalah ketika terdapat *rules* atau aturan, maka paket data yang masuk akan dicocokkan terlebih dahulu oleh *firewall* dengan *rules* atau aturan yang dibuat. *Rules* atau aturan tersebut yaitu meliputi alamat IP, nomor *port* serta protokol yang digunakan. Jika paket data yang tiba tidak sesuai dengan aturan-aturan yang telah didefinisikan sebelumnya, *firewall* akan mengambil tindakan tegas dengan menolak paket data tersebut. Dengan kata lain, paket data tersebut akan dihentikan sebelum mencapai tujuannya. Tindakan ini sering disebut sebagai *"drop"* atau penolakan paket data. Sebaliknya, jika paket data cocok dengan aturan-aturan yang ada, *firewall* akan membiarkannya melintasi jaringan. Saat aturan aktif, antarmuka akan menampilkan indikator yang dapat dilihat seperti “menyala” pada Gambar 3.14, memberi tahu bahwa sistem perlindungan sedang berjalan dengan baik dan mengamankan jaringan dari ancaman potensial.



Gambar 3. 14 *Rules Packet Filtering* Aktif

3.7 SKENARIO PENGAMBILAN DATA

3.7.1 Pengambilan Data Alamat IP

Pada pengambilan data kali ini akan diperoleh data berupa alamat IP yang digunakan oleh situs judi dan media sosial. Alamat IP tersebut didapatkan dari *tools nslookup* pada *command prompt* (cmd). Pengambilan data ini dilakukan sebanyak 20 kali yang kemudian akan dimasukkan ke dalam Tabel 3.7.

Tabel 3. 7 Data Alamat IP yang diperoleh

Kategori	Alamat/Aplikasi	Alamat IP	Banyak Pengambilan
Situs (*Website*)	www.atcharlotte.org		20
	www.lk21.com		20
	www.ijsk.org		20

Kategori	Alamat/Aplikasi	Alamat IP	Banyak Pengambilan
	www.superwin303.com		20
	www.savshow.com		20
Media Sosial	www.facebook.com		20
	www.instagram.com		20
	www.tiktok.com		20
	www.twitter.com		20
	www.youtube.com		20

3.7.2 Pengambilan Data Nomor *Port*

Pada pengambilan data kali ini akan diperoleh data berupa nomor yang digunakan oleh *game online*. Nomor *port* tersebut didapatkan dari fitur *torch* pada Mikrotik. Pengambilan data ini dilakukan sebanyak 20 kali yang kemudian akan dimasukkan ke dalam Tabel 3.8.

Tabel 3. 8 Data Nomor *Port* yang diperoleh

Game Online	Nomor Port	Fungsi
Mobile Legend		
PUBG Mobile		
FreeFire		
ClashRoyale		
Stumble Guys		

3.7.3 Pengambilan Data Waktu Respon

Pada pengambilan data kali ini akan diperoleh data berupa nilai waktu respon sistem notifikasi. Pengambilan data tersebut bertujuan untuk mengetahui seberapa responsif sistem notifikasi bekerja ketika terjadi pelanggaran pengaksesan. Pengambilan data ini dilakukan sebanyak 20 kali dengan 2 *sample* aplikasi yaitu media sosial Instagram dan *game online* Mobile Legend. Kemudian data tersebut akan dikumpulkan pada Tabel 3.9 lalu diambil nilai rata-ratanya.

Tabel 3. 9 Data Waktu Respon Sistem Notifikasi

Waktu Respon (Detik)		
Pengambilan Ke-	**Instagram**	**Mobile Legend**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
Rata-Rata		