BAB 3
METODE PENELITIAN

3.1 BAHAN PENELITIAN

Bahan inti yang akan digunakan pada penelitian ini merupakan *domain*. Daftar *domain* yang berpotensi terdapat iklan, *malware* ataupun pelacakan, terlebih dahulu perangkat akan mengirimkan sebuah DNS kepada AdGuardHome untuk dilakukan filtrasi terhadap keamanan domain tersebut. Penelitian ini akan dilakukan terhadap 5 ponsel Android "*China Brand"* kondisi "*fresh install"* atau "modul setelan pabrik" yang kemudian akan dilakukan analisis perbandingan dari setiap aktivitas ponsel Android selama 1x24 jam. Dalam pengambilan data menggunakan bantuan sebuah software GFTP (GNU File Transfer Protocol) yang digunakan untuk mentransfer file antar komputer dan menggunakan CLI (*Command Line Interface*)

Dalam penerapan penelitian yang akan dilakukan, AdGuardHome akan diintegrasikan pada perangkat Raspberry Pi 3 B. Sistem tersebut akan menjadi sebuah ekosistem jaringan khusus dan terbatas di Universitas Jenderal Achmad Yani Yogyakarta dengan ponsel Android yang terhubung pada satu segmen jaringan dengan Raspberry Pi. Proses penelitian ini akan dilakukan pada bulan juni 2024. Proses yang dimaksud adalah pengambilan data yaitu data *query log*.

3.2 ALAT PENELITIAN

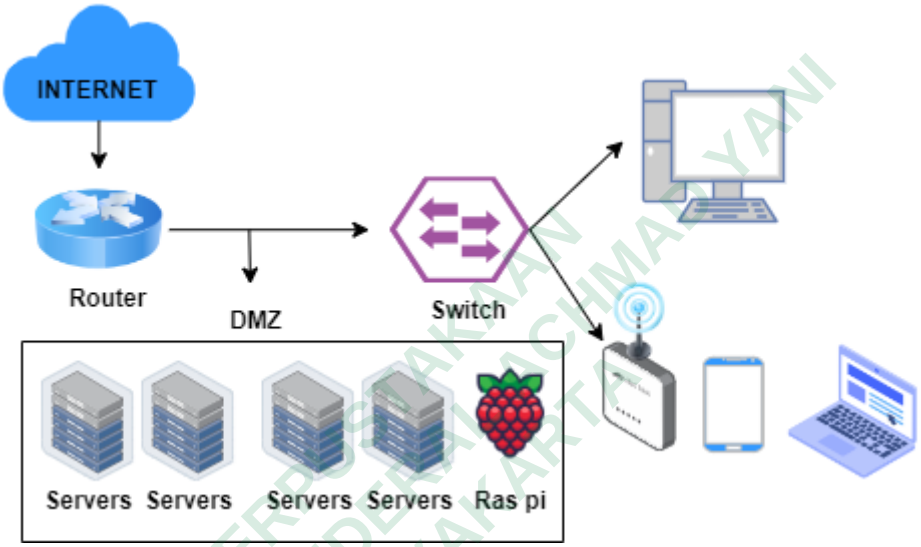
Pada penelitian yang akan dilakukan, memerlukan beberapa alat yang akan digunakan dalam mencapai dari tujuan penelitian ini, dengan keterangan singkat sebagai berikut:

1. RaspberryPi : Perangkat yang akan digunakan pada penelitian ini yaitu berupa single board compter, RaspberryPi 3 B.
2. RaspberryPI Imager : RaspberryPi Imager pada penelitian ini digunakan untuk proses *burning* pada sistem operasi Pi OS pada SD card.

3. Pi OS : Sistem operasi yang akan digunakan pada penelitian ini yaitu akan menggunakan versi lite (64-bit). Hal ini dikarenakan, sistem akan dijalankan hanya menggunakan *command line interface* (CLI).
4. SD Card : SD card akan digunakan untuk menyimpan sistem operasi yang akan digunakan pada pera ngkat Raspberry Pi. SD card yang akan digunakan oleh penulis berkapasitas 16 GB Merek robot.
5. Kabel HDMI : Kabel HDMI dalam penelitian ini akan digunakan sebagai alat bantu dalam menghubungkan perangkat raspberry ke layar monitor untuk melakukan instalasi linux pada raspi serta konfirgurasi pada ssh dengan service yang berjalan.
6. *Card Reader* : *Card reader* digunakan agar komputer dapat membaca dan dapat digunakan untuk mentransfer data yaitu berupa sistem operasi yang di-*download* melalui perangkat laptop yang kemudian akan disimpan pada SD Card.
7. AdGuardHome : AdGuardHome yaitu software ini dijadikan sebagai server DNS untuk menyaring permintaan DNS dari perangkat *client*. Ketika perangkat *client* mengirimkan permintaan DNS, AdGuardHome memeriksa domain yang diminta termasuk dalam daftar blokir internal atau sesuai dengan pola yang telah ditentukan. Jika domain tersebut terdaftar dalam daftar blokir, AdGuardHome akan mengirimkan jawaban palsu kepada *client*, misalnya dengan mengembalikan respons NXDOMAIN (domain tidak ada) atau alamat IP wildcard seperti 0.0.0.0. Hal ini membuat permintaan tersebut seolah-olah ditolak atau diblokir, sehingga pengguna tidak dapat mengakses situs atau layanan yang telah diblokir secara efektif. Dengan cara ini, AdGuardHome membantu memfilter dan melindungi perangkat dari mengakses situs web yang berpotensi berbahaya atau tidak diinginkan (Kalytta, n.d.).
8. *Router* : *Router* akan digunakan untuk mengatur jaringan yang akan dibangun sesuai dengan kebutuhan penelitian yang direncanakan.

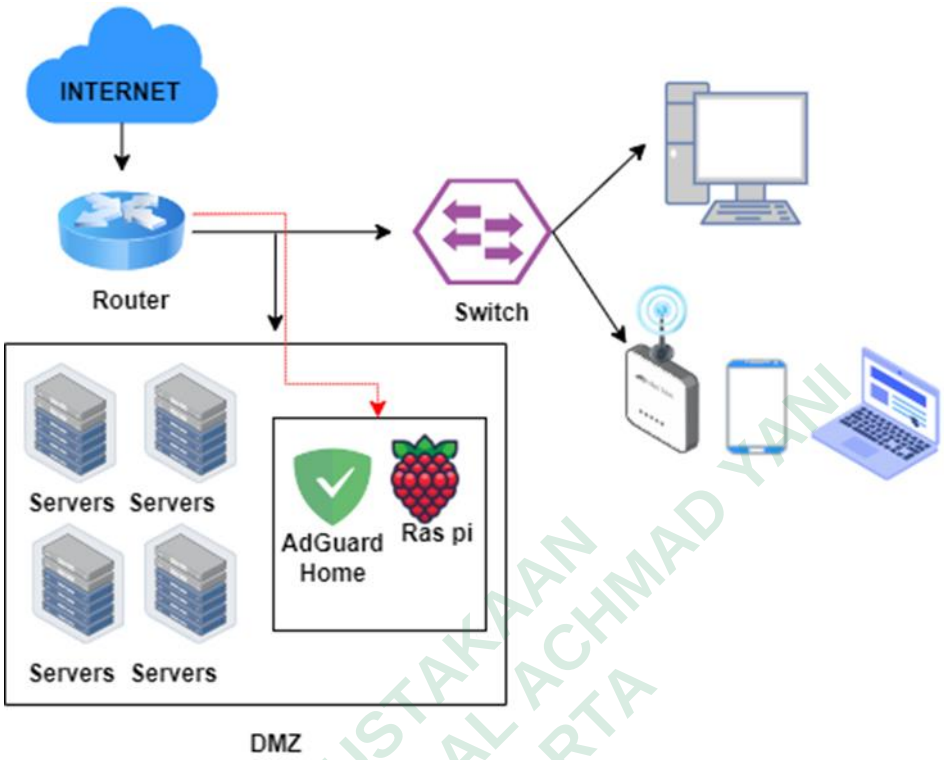
Access point : Accses point digunakan untuk menyebarkan jaringan ke perangkat *client*, dalam hal ini pada ponsel Android "*China Brand*". *Access point* yang digunakan yaitu MiRouter 4C

3.3 JALAN PENELITIAN



Gambar 3.1 Topologi Jaringan Tanpa Implementasi AdGuardHome

Berdasarkan dari Gambar 3.1. Pada saat terhubung ke internet, router akan mengumpulkan data dan informasi, yang kemudian dikirim melalui switch dan didistribusikan ke berbagai perangkat. Salah satunya adalah komputer yang terhubung melalui kabel LAN. Dilain sisi, kabel LAN juga disambungkan ke access point, yang memiliki tanggung jawab untuk menyebarkan jaringan secara nirkabel ke perangkat ponsel Android dan laptop. Namun, seperti yang ditunjukan pada gambar diatas, tidak adanya tools tambahan yang diberikan, yaitu AdGuardHome yang berfungsi sebagai pelindung jaringan dari iklan *online* yang berbahaya *(malvertising).* Akibatnya, iklan terus saja muncul saat pengguna mengakses internet karena router tidak melakukan penyaringan pada konten iklan yang mengganggu atau berbahaya *(malvertising).*

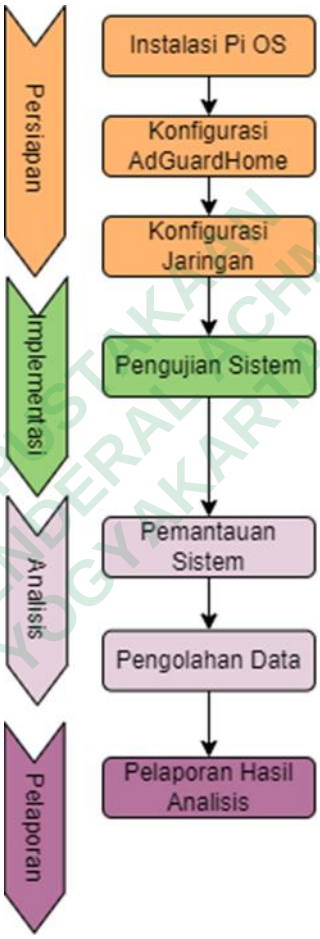


Gambar 3.2 Topologi Jaringan Dengan Implementasi AdGuardHome

Berdasarkan Gambar 3.2. Sudah adanya sebuah tools yang telah di konfigurasi pada sebuah topologi jaringan yaitu berupa AdGuardHome yang dijadikan sebuah server DNS untuk menjalankan mekanisme DNS *sinkhole* yang terintegrasi di dalam DMZ *(Demilitarized zone)* yang merupakan sebuah metode untuk mengamankan jaringan internal dari akses yang tidak sah oleh pihak eksternal, seperti hacker atau entitas lain yang berusaha masuk ke dalam sistem tanpa izin (Satriawan & Hari Trisnawan, 2021). DNS *Sinkhole* yaitu DNS *server* yang sengaja dikonfigurasi untuk memberikan hasil palsu (*false result*) untuk sebuah permintaan ke domain tertentu (Satriawan & Hari Trisnawan, 2021). Namun dalam mengatasi permasalahan *malvertising* ini, supaya berjalan sesuai dengan tujuan yang ingin dicapai, AdGuardHome dikonfigurasikan dengan IP router, sebab *router*lah yang menjembatani internet ke sebuah perangkat yang disalurkan melalui bantuan *switch*. Sistem ini bekerja dengan cara melakukan sebuah penyaringan terhadap akses internet yang dilakukan oleh *client*, dengan router mengirimkan

sebuah DNS ke AdGuardHome. Dengan demikian, AdGuardHome melakukan sebuah upaya penyaringan terhadap data yang diterima oleh router.

Setelah melakukan pembahasan secara singkat mengenai topologi yang dibangun untuk mencapai tujuan daripada penelitian ini yaitu melakukan tindakan antisipasi terhadap serangan malvertising, adapun langkah alur penelitian seperti pada Gambar 3.3.



Gambar 3.3 Alur Penelitian

Penelitian akan melalui empat tahapan utama yaitu tahapan persiapan, tahapan implementasi, tahapan analisis, dan yang terakhir tahapan pelaporan. Tahap persiapan dimulai dengan mengunduh PI OS dari situs web resmi dan menginstalnya ke perangkat Raspberry Pi. PI OS Lite dipilih karena penelitian yang akan dilakukan hanya menggunakan *Command Line Interface* (CLI), tanpa menggunakan *Graphical User Interface* (GUI). Untuk instalasi, diperlukan sebuah

card reader untuk mem*burn* sistem operasi ke SD Card merek robot berkapasitas 16 GB yang akan penulis gunakan. Setelah selesainya instalasi OS, langkah berikutnya adalah menginstal AdGuardHome dengan menggunakan beberapa *command line.* Tahap terakhir dari tahapan utama ini yaitu mengkonfigurasi jaringan pada perangkat Raspberry Pi dengan mengatur ke DHCP *(Dynamic Host Configuration) server*, dengan maksud untuk mendistribusikan alamat IP *client* secara otomatis kepada perangkat yang berada pada satu jaringan yang sama.

Tahapan utama yang kedua yaitu tahapan implementasi. Tahapan ini yaitu akan melakukan sebuah pengujian terhadap sistem yang sudah dibangun untuk memastikan bahwa AdGuardHome yang terpasang pada Raspberry Pi berjalan dengan baik. Dengan melakukan simulasi percobaan pada sebuah ponsel Android yang terhubung pada satu jaringan yang sama dengan Raspberry Pi, sehingga nanti akan muncul sebuah data berupa *query log* pada dashboard AdGuardHome yang terintegrasi pada Raspberry Pi. Dari hal tersebut, nantinya akan tercatat berupa akses yang diblok dengan adanya alasan pemblokiran yang dilakukan.

Pada tahapan selanjutnya, yaitu tahapan analisis. Pada tahapan ini dilakukan ketika, hasil dari pengujian sistem berjalan dengan baik dan seharusnya. Hal yang dilakukan pada tahap ini adalah melakukan sebuah analisis daripada sebuah DNS *Query* dari data yang diujikan pada 5 ponsel Android *"China Brand"*. Pengambilan data ini akan dilakukan dalam kurun waktu lebih kurang selama 2 pekan pada bulan juli 2024. Setelah mendapatkan data dari masing-masing ponsel Android, dilakukanlah sebuah pengolahan data berupa penghitungan akses query dari *client* yang diantaranya, pemblokiran pada *malvertising*, pemblokiran konten illegal, dan konten yang diperbolehkan atau dinyatakan telah aman dari sebuah *malvertising* atau sebuah *malware*.

Tahapan terakhir dari penelitian yang dilakukan yaitu tahapan pelaporan. Setelah dilakukanya sebuah pengujian dan mendapatkan data yang diinginkan, dituangkanlah kedalam sebuah laporan tugas akhir ini. Pelaporan ini akan mencakup perbandingan analisis yang dilakukan pada 5 ponsel Android *"China Brand"* sebelum dan sesudah dari pemanfaatan sistem pertahanan AdGuardHome.