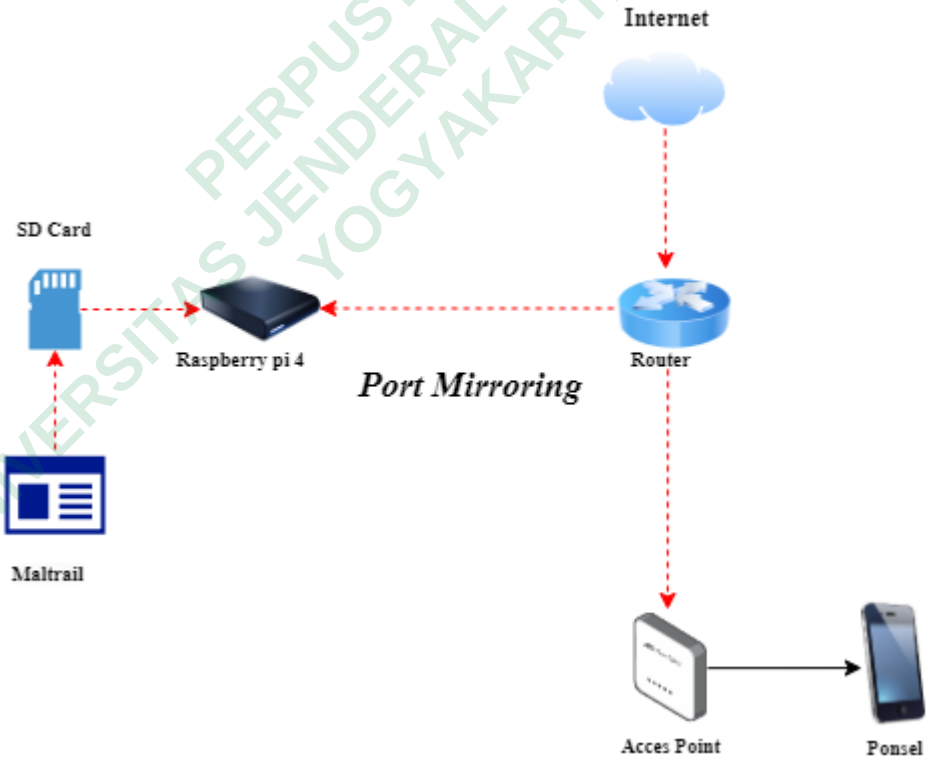
BAB 3
METODE PENELITIAN

Pada penelitian ini, metode yang digunakan adalah *port mirroring.* Ini adalah teknik penyalinan jaringan *traffic* dari port yang dilalui lalu lintas utama ke media lain. Penyalinan *traffic* menggunakan teknik *port mirroring* dilakukan dengan penyalinan *traffic* dari *acess point* yang sebelumnya sudah saling terkoneksi dengan ponsel Android *"China Brand"*, yang kemudian ditransfer dalam Raspberry Pi 4 yang terinstal aplikasi Maltrail., kemudian di lakukan dengan proses *live capture* pada Raspberry Pi. Metode *port mirroring* digunakan untuk membaca *Malicious traffic* pada ponsel Android *"China Brand"*. Berikut *Port Mirroring* pada topologi jaringan. Dapat dilihat pada gambar 3.1. dibawah ini



Gambar 3.1 *Port Mirroring*

3.1 BAHAN DAN ALAT PENELITIAN

Alat dan bahan yang digunakan dalam penelitian ini terdiri dari :

3.1.1 Ponsel Android

Ponsel Android adalah perangkat mobile yang menggunakan sistem operasi (OS) berbasis Android, yang dikembangkan oleh Google. Android di rancang khusus untuk perangkat seperti ponsel dan tablet, serta memberikan sumber perintah yang memungkinkan perangkat tersebut menjalankan berbagai jenis aplikasi. Ponsel Android ini menjadi objek utama dalam penelitian, dan akan menggunakan 5 ponsel yang berbeda yang di pastikan dapat terkoneksi wifi dan dapat di pantau menggunakan laptop. Ponsel Android tersebut akan di setting dan dikoneksikan ke jaringan internet dengan tujuan untuk mengambil IP address yang akan dijadikan bahan pengambilan *malware* dengan cara dikoneksikan pada aplikasi Maltrail.

3.1.2 Raspberry Pi 4

Raspberry Pi 4 adalah komputer papan tunggal yang digunakan untuk menjalankan program aplikasi Maltrail. Operating System (OS) yang digunakan adalah ubuntu 22.04.3 LTS. Raspberry Pi adalah komputer kecil yang menjalankan linux pada prosesor ARM. Raspberry Pi 4 terdiri dari Broadcom BCM2711, Quad-core Cortex-A72 (ARM v8) SoC 64-bit @ 1,8GHz, RAM LPDDR4 4GB Nirkabel 2,4 GHz dan 5,0 GHz IEEE 802.11ac, Bluetooth 5.0, Bluetooth Low Energy (BLE), Gigabit Ethernet, 2 port USB 3.0; 2 port USB 2.0, Header GPIO 40 pin standar Raspberry Pi, 2 × port mikro-HDMI® (mendukung hingga 4kp60), Port tampilan MIPI DSI 2 jalur, Port kamera MIPI CSI 2 jalur, Audio stereo 4 kutub dan port video komposit, H.265 (dekode 4kp60), H264 (dekode 1080p60, enkode 1080p30), OpenGL ES 3.1, Vulkan 1.0, Slot kartu Micro-SD untuk memuat sistem operasi dan penyimpanan data, 5V DC melalui konektor USB-C, 5V DC melalui header GPIO(Raspberry Pi, n.d.). Raspberry Pi sangat diminati, dan banyak proyek proyek digital menggunakan alat tersebut.

3.1.3 MikroTik

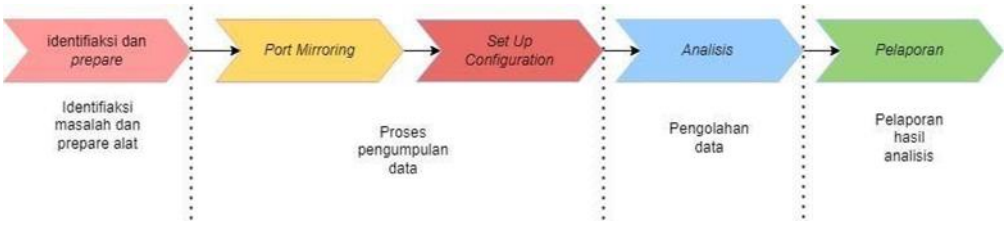
Mikrotik adalah Perusahaan yang mengembangkan sistem operasi (OS) dan perangkat lunak untuk jaringan komputer. Mikrotik RouterOS adalah sistem operasi yang dikembangkan oleh Mikrotik yang di rancang khusus untuk digunakan pada perangkat jaringan seperti router dan switch. Mikrotik RouterOS memiliki fitur yang sangat banyak dan mendukung berbagai protocol jaringan seperti IP, TCP/IP, OSPF, BGP, MPLS,VPN, Firewall dan masih banyak lagi. Hardware yang dikembangkan oleh Mikrotik biasanya disebut "Mikrotik Routerboard" atau "Mikrotik Device". Beberapa contoh perangkat Mikrotik yang populer adalah Routerboard RB750, RB951, RB2011, dan CCR (Cloud Core Router). Mikrotik yang digunakan dalam penelitian ini yaitu Mikrotik tipe TC RB941-2nD-TC yang merupakan varian dari seri hAP. Memiliki 4 buah port ethernet, 1 buah acces point embedded 2,4 GHz, antenna embedded 2x1,5 dbi.

3.1.4 Access Point

Access point merupakan perangkat jaringan yang digunakan untuk menghubungkan jaringan internet pada ponsel,laptop, dan perangkat lain yang membutuhkan jaringan internet. Access Point ini juga digunakan untuk membaca alamat IP. Tipe router yang digunakan adalah pada penelitian ini adalah Mi Router 4C yang memiliki kecepatan wifi 300Mbps yang memiliki 3 port Ethernet dan memiliki 4 antena eksternal ,serta memiliki penyimpanan memori 64MB.

3.2 JALAN PENELITIAN

Dalam penelitian ini akan menganalisis *Malicious traffic* pada sistem ponsel Android menggunakan Maltrail. Objek utama yang digunakan dalam penelitian ini adalah lima ponsel Android dengan merek yang berbeda. Metode yang digunakan adalah port mirroring. Pada penelitian ini terdiri dari 4 tahap utama, yaitu identifikasi dan prepare, proses pengumpulan data, analisis, dan pelaporan.



Gambar 3.2 Alur Penelitian

Tahap identifikasi dan persiapan dimulai dengan mendownload PI OS dari situs resminya dan menginstalnya pada perangkat Raspberry. PI OS yang digunakan pada penelitian ini adalah PI OS Lite. SD Card diperlukan untuk instalasi. Card rider mem-burn sistem operasi ke kartu SD berkapasitas 32 GB. Setelah sistem operasi terinstal, langkah selanjutnya adalah SSH dan konfigurasi Raspberry. Setelah dikonfigurasi, langkah selanjutnya adalah menginstal Maltrail di Raspberry dengan menggunakan command line. Langkah selanjutnya adalah mengkonfigurasi Maltrail.

Tahapan yang kedua yaitu tahap pengumpulan data. Selama tahapan ini peneliti akan melakukan konfigurasi pengujian yang terdapat didalmnya *set up port mirroring* dan *set up configuration* alat. Setelah melakukan *set up port mirroring* dan *set up configuration*, selanjutntya melakukan percobaan pada salah satu ponsel Android yang terhubung pada satu jaringan yang sama dengan Raspberry Pi, sehingga nanti akan muncul sebuah data. Dari data tersebut akan tercatat aktivitas pada ponsel Android yang sedang di uji coba.

Pada tahapan ketiga, yaitu tahapan analisis. Pada tahapan ini dilakukan pengelolaan data yaitu dengan melakukan pengumpulan data dari lima ponsel Android *"China Brand"* yang sudah tercatat dalam Maltrail. Pengambilan data ini akan dilakukan dalam kurung waktu selama 2 minggu.

Tahapan terakhir dari penelitian ini yaitu tahapan pelaporan. Setelah melakukan pengujian dan mendapatkan data yang diinginkan, maka akan di sajikan dalam sebuah laporan tugas akhir. Pelaporan ini mencakup perbandingan dari hasil pengujian lima ponsel Android *"China Brand"*.