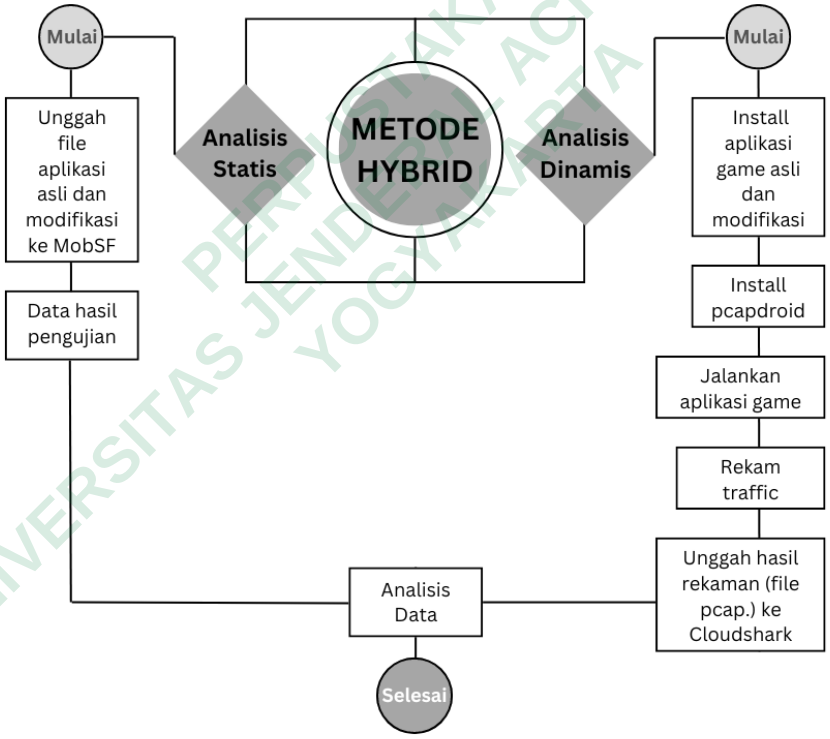
BAB 3
METODE PENELITIAN

Penelitian ini akan melakukan analisis terhadap 5 aplikasi *game* modifikasi Android menggunakan metode *Hybrid* dan pengenalan perubahan karakteristik aplikasi *game*. Metode *Hybrid* yang digunakan adalah analisis statis menggunakan MobSF, dan analisis dinamis menggunakan PCAPDroid. *File* pcap dari hasil analisis dinamis kemudian dibaca oleh *website* CloudShark untuk mendapatkan informasi lebih lanjut tentang komunikasi apa saja yang terjadi pada aplikasi *game*. Gambar 3.1 merupakan alur penelitian yang akan dilakukan:



Gambar 3.1 Alur Penelitian

3.1 BAHAN DAN ALAT PENELITIAN

Bahan yang diperlukan dalam melakukan analisis adalah aplikasi *game* asli diunduh dari *Play Store* dan *game* modifikasi bersumber dari situs pihak ketiga. *Game* yang akan dianalisis adalah 5 *game* populer, seperti Stickman Party,

Adorable Home, Subway Surfers, Brain Out, dan Zombie Tsunami. Aplikasi *game* versi modifikasi akan diunduh dari beberapa situs penyedia aplikasi mod, seperti GameModsAPK, An1, dan ModCombo.

Selain itu, diperlukan juga akses ke jaringan internet, baik jaringan Wi-Fi maupun jaringan seluler. Data lalu lintas jaringan ini akan menjadi dasar untuk analisis keamanan dan potensi ancaman pada *game* modifikasi Android.

Alat yang digunakan pada penelitian ini adalah 2 perangkat Android dan laptop yang memadai untuk menjalankan *software* dan aplikasi penunjang dalam analisis penelitian terhadap *game* modifikasi. Adapun spesifikasi *hardware* yang digunakan sebagai berikut :

1. Smartphone Android I
   a. Sistem Operasi : Android 14
   b. *Processor* : Snapdragon 695 5G
   c. RAM : 6GB
   d. Penyimpanan : 128GB
2. Smartphone Android II
   a. Sistem Operasi : Android 9
   b. *Processor* : Snapdragon 625
   c. RAM : 3GB
   d. Penyimpanan : 32GB
3. Laptop
   a. Sistem Operasi : Windows 10
   b. *Processor* : Intel Core i5 generasi 7200U
   c. RAM : 8GB
   d. Penyimpanan : 256GB (SSD)

Aplikasi atau *software* yang akan digunakan untuk melakukan analisis terhadap *game* modifikasi, ditunjukkan dalam Tabel 3.1 :

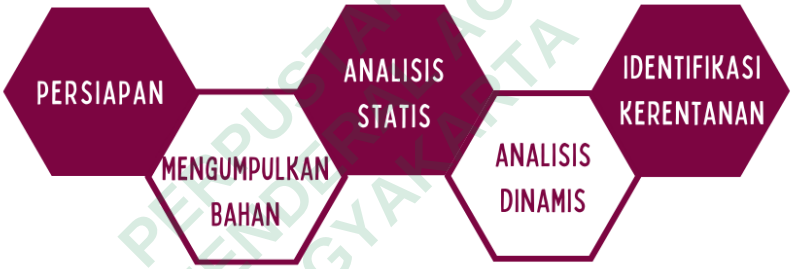
Tabel 3.1 Aplikasi yang Digunakan dan Fungsinya

No.	Aplikasi	Fungsi
1.	CloudShark	Website *Open Source* yang digunakan untuk membaca hasil tangkapan *file* pcap.

No.	Aplikasi	Fungsi
2.	MobSF	Digunakan untuk menganalisis aplikasi *game* asli dan modifikasi untuk mengidentifikasi potensi kerentanan keamanan dan ancaman lainnya.
3.	PCAPdroid	Digunakan untuk menangkap lalu lintas jaringan dari aplikasi *game* yang dijalankan pada perangkat Android.

3.2 JALAN PENELITIAN

Dalam penelitian ini akan dilakukan analisis menggunakan metode Packet Capture. Alur penelitian dibagi menjadi beberapa tahap seperti pada Gambar 3.2 :



Gambar 3.2 Jalan Penelitian

1. Persiapan

   Tahap awal penelitian ini dimulai dengan melakukan kajian pustaka untuk memahami penelitian terdahulu terkait metode, teori dan teknik yang relevan sebagai pendukung solusi yang diusulkan untuk penelitian ini. Kemudian, dilakukan persiapan pada perangkat Android untuk menginstal dan menjalankan *game* yang diunduh dari *Play Store*, dan perangkat Android lain untuk menjalankan *game* modifikasi. Selanjutnya, melakukan *set-up* sistem pada alat yang digunakan untuk analisis seperti MobSF.

2. Mengumpulkan Bahan Penelitian

   Pada tahap ini dilakukan pengambilan metadata yang mencakup informasi mengenai *game* yang akan diteliti, seperti pengembang, versi, tanggal rilis, ukuran *file*, dan sumber aplikasi. Selain itu, dilakukan

pengamatan terhadap perbedaan karakteristik kedua versi *game* seperti performa, *gameplay*, dan elemen lainnya.

3. Analisis Statis

   Tahap ini akan melakukan analisis statis berupa *scanning file* aplikasi *game*, dengan memanfaatkan *tools* MobSF pada *game* yang akan diteliti. Hasil *scanning* kemudian disimpan untuk diidentifikasi kerentannya setelah analisis dinamis selesai.

4. Analisis Dinamis

   Pada tahap ini, *game* yang akan dianalisis dijalankan bersamaan dengan aplikasi PCAPdroid untuk direkam komunikasinya selama 5 menit. Data yang di transmisikan pada saat *game* dijalankan, kemudian akan diunggah pada *website* CloudShark untuk diidentifikasi hasil IP apa saja yang muncul dan komunikasinya baik pada versi asli maupun versi modifikasi.

5. Identifikasi Kerentanan

Tahap ini akan mengumpulkan hasil analisis menggunakan Statis dan Dinamis untuk diidentifikasi kerentanan dan potensi ancaman keamanan lainnya. Adapun data yang diambil merupakan hasil kesimpulan dari temuan adanya kerentanan pada versi modifikasi seperti pada perbedaan dari segi metadata, karakteristik, analisis statis, dan analisis dinamis. Data-data tersebut kemudian dikumpulkan dan diperkecil lingkupnya untuk kemudian diidentifikasi celah kerentannya.