BAB 4
HASIL PENELITIAN

4.1 PERSIAPAN

Dilakukan persiapan pada perangkat Android dengan menginstal *game* baik yang melalui *Play Store* maupun situs penyedia mod, dan juga melakukan *set-up* sistem pada alat yang digunakan untuk analisis seperti MobSF dan PCAPDroid. Adapun langkah persiapan yang dilakukan sebagai berikut :

1. Menggunakan dua perangkat Android, Samsung dan Xiaomi

Gambar 4.1 Perangkat Android Samsung

Gambar 4.2 Perangkat Android Xiaomi

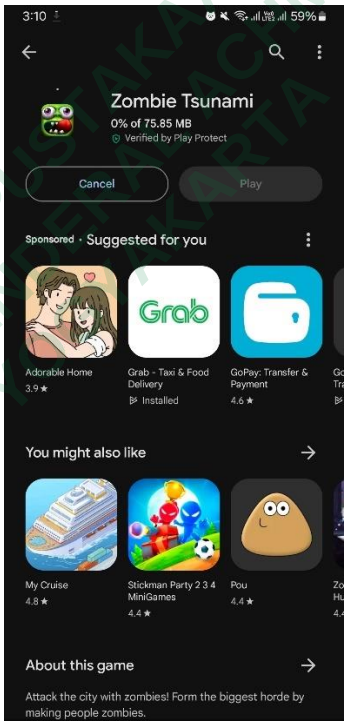
Adapun spesifikasi perangkat Android yang digunakan, dapat dilihat pada Tabel 4.1 :

Tabel 4.1 Spesifikasi Perangkat Android

DETAIL PERANGKAT	SPESIFIKASI	
	Samsung	**Xiaomi**
Nama Perangkat	Samsung A23 5G	Xiaomi Redmi S2
Nomor Model	SM-A236E	M1803E6G
Versi Android	14	9.0

DETAIL PERANGKAT	SPESIFIKASI	
	Samsung	**Xiaomi**
Processor	Qualcomm SM6375 Snapdragon 695 5G	Qualcomm MSM8953 Snapdragon 625
RAM	6GB	3GB
Memori Internal	128GB	32GB

2. Pengumpulan data aplikasi *game* asli didapatkan dengan mengunduh melalui *Play Store* dengan perangkat Android Samsung, seperti ditunjukkan pada Gambar 4.3 :



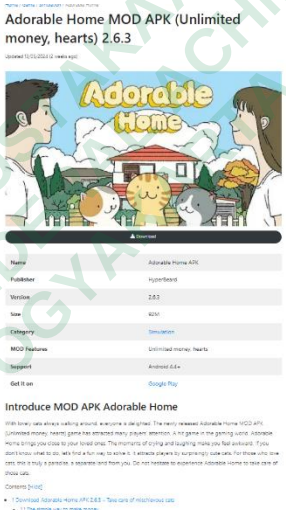
Gambar 4.3 Download Aplikasi *Game* di *Play Store*

Adapun *game* yang diambil sebagai objek merupakan *game* offline di *Play Store* yang telah diunduh lebih dari 10 juta kali, dari berbagai kategori *game*, seperti pada Tabel 4.2 :

Tabel 4.2 Kategori *Game*

Nama *Game*	Kategori	Jumlah Unduhan
Adorable Home	Simulasi	+10 Juta
Zombie Tsunami	Arcade	+500 Juta
Brain Out	Puzzle	+100 Juta
Subway Surfers	Arcade	+ 1 Miliyar
Stickman Party	Casual	+ 100 Juta

3. Pengumpulan data aplikasi *game* modifikasi didapatkan dengan mengunduh melalui berbagai situs penyedia *game* modifikasi dengan perangkat Xiaomi, ditunjukkan pada Gambar 4.4 :



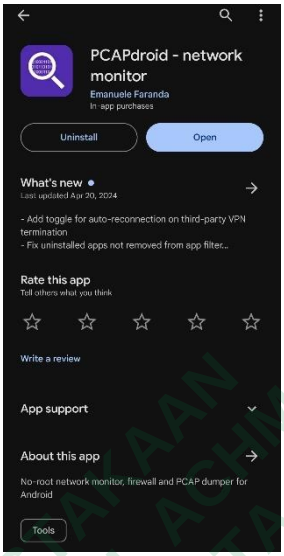
Gambar 4.4 Download Aplikasi *Game* Modifikasi

Adapun sumber situs penyedia *game* modifikasi yang diambil ditunjukkan pada Tabel 4.3 :

Tabel 4.3 Sumber *Game* Modifikasi

Nama *Game*	Sumber
Adorable Home	ModCombo
Zombie Tsunami	An1
Brain Out	GetModsAPK
Subway Surfers	ModCombo
Stickman Party	ModCombo

4. Pada masing-masing perangkat Android, diperlukan aplikasi PCAPDroid yang diunduh dari *Play Store* untuk melakukan perekaman paket pada *game* yang dijalankan, seperti pada Gambar 4.5 :

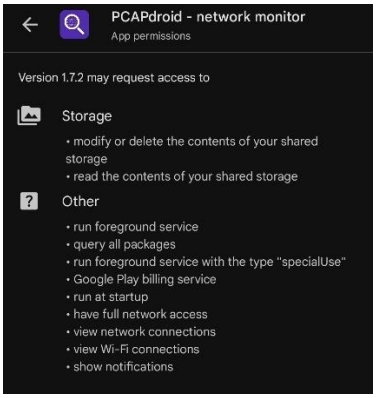


Gambar 4.5 Download Aplikasi PCAPDroid

Adapun spesifikasi aplikasi PCAPDroid yang telah diunduh dapat dilihat pada Tabel 4.4 :

Tabel 4.4 Spesifikasi Aplikasi PCAPDroid

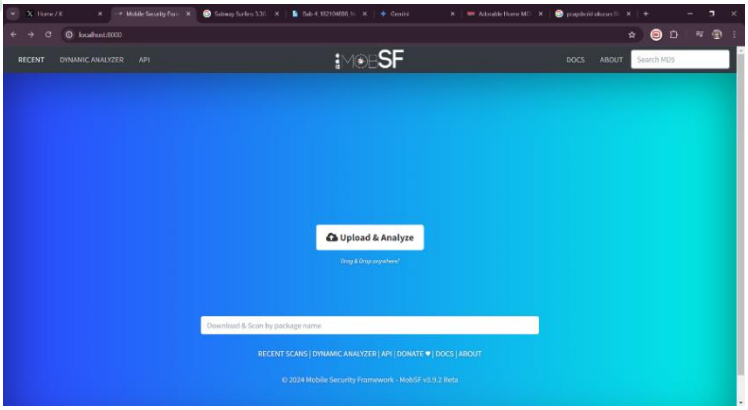
Komponen	Info Aplikasi
Penyedia aplikasi	Emanuele Faranda
Ukuran *file*	5.77MB
Versi aplikasi	1.7.2
Kompatibel dengan OS	Android 5.0 keatas
Tanggal rilis	26 Oktober 2019
Izin akses	Penyimpanan, dan izin lainnya.



Gambar 4.6 Data yang dibutuhkan pada aplikasi

Dari uraian pada Gambar dapat disimpulkan bahwa data yang dibutuhkan aplikasi PCAPDroid adalah penyimpanan (membaca, menulis, dan menghapus data) dan jaringan (menangkap paket data, melihat koneksi jaringan). Izin lain yang diperlukan untuk fitur opsional atau untuk menjalankan aplikasi dengan optimal.

5. Pengambilan data menggunakan MobSF perlu dilakukan beberapa persiapan instalasi perangkat lunak seperti Python versi 11, GIT, JDK, OpenSSL non-Light, dan wkhtmltopdf. Setelah selesai melakukan instalasi MobSF, nantinya akan dijalankan pada jaringan lokal atau localhost pada *browser*.



Gambar 4.7 Halaman Utama MobSF

Gambar 4.7 menampilkan halaman utama MobSF yang sudah berhasil dijalankan pada *browser*.

4.2 PENGUMPULAN BAHAN PENELITIAN

Dilakukan pengumpulan bahan penelitian berupa pengumpulan metadata aplikasi, analisis karakteristik aplikasi *game* mod dan teknik pengambilan data.

4.2.1 Metadata

Dalam pengumpulan metadata, data yang diambil mencakup informasi umum mengenai *game* yang akan diteliti dan melakukan pengamatan karakteristik pada kedua versi *game*. Perbandingan metadata versi asli dan versi modifikasi diuraikan sebagai berikut :

1. **Zombie Tsunami**

   Hasil perbandingan metadata pada aplikasi *game* Zombie Tsunami, menunjukkan bahwa versi asli dan versi mod memiliki beberapa perbedaan seperti nama paket yang berbeda, ukuran APK yang lebih besar, dan berasal dari sumber pihak ketiga. Selain itu, versi mod menawarkan fitur tambahan atau modifikasi yang tidak tersedia di versi asli, seperti uang tak terbatas. Perbandingan tersebut ditunjukkan pada Tabel 4.5 berikut :

Tabel 4.5 Perbandingan Metadata *Game* Zombie Tsunami

Aspek	*Game* Asli	*Game* Mod	Ket
Nama Aplikasi	Zombie Tsunami	Zombie Tsunami (MOD, Unlimited Money)	Penambahan Informasi
Nama Paket	net.mobi*game*.zombietsunami	zombie-tsunami-mod_4.5.133-an1.com	Perbedaan nama paket
Versi	4.5.133	4.5.133	
Pengembang	Mobi*game* SAS	Mobi*game* SAS	
Ukuran APK	68.42MB	77.85MB	Versi mod lebih besar
Tanggal Update	19 Januari 2024	19 Januari 2024	
Sumber	PlayStore	https://an1.com/1686-zombie-tsunami-mod.html	
Tanggal Unduh	16 Juni 2024	16 Juni 2024	

2. Adorable Home

Hasil perbandingan metadata pada aplikasi *game* Adorable Home menunjukkan bahwa, versi mod memiliki beberapa perbedaan dengan versi asli seperti, penambahan informasi modifikasi di judul, nama paket yang berbeda, ukuran APK yang lebih besar, serta tanggal update yang lebih baru. Selain itu versi modifikasi juga mengklaim fitur uang, hati tak terbatas, dan item terkunci yang telah terbuka. Perbandingan tersebut ditunjukkan pada Tabel 4.6 berikut:

Tabel 4.6 Perbandingan Metadata *Game* Adorable Home

Aspek	*Game* Asli	*Game* Mod	Ket
Nama Aplikasi	Adorable Home	Adorable Home Mod APK 2.7.1 (Unlimited money/Hearts/Unlocked)	Penambah informasi
Nama Paket	com.hyperbeard.adorablehome	Adorable-Home-2.7.0-MOD-ModCombo.io	Perbedaan nama paket
Versi	2.7.0	2.7.0	
Pengembang	HyperBeard	HyperBeard	
Ukuran APK	146.69MB	146.78MB	Versi mod sedikit lebih besar
Tanggal Update	9 Mei 2024	21 Juni 2024	
Sumber	PlayStore	https://modcombo.io/adorable-home.html	
Tanggal Unduh	16 Juni 2024	16 Juni 2024	

3. Brain Out

Hasil perbandingan metadata pada aplikasi *game* Brain Out menunjukkan bahwa, versi modifikasi memiliki penambahan informasi dan nama paket yang berbeda. Selain itu versi modifikasi juga memiliki ukuran yang lebih kecil daripada versi asli dan tanggal update yang lebih baru. Versi modifikasi juga menawarkan fitur berupa petunjuk tak terbatas. Perbandingan tersebut ditunjukkan dalam Tabel 4.7 berikut:

Tabel 4.7 Perbandingan Metadata *Game* Brain Out

Aspek	*Game* Asli	*Game* Mod	Ket
Nama Aplikasi	Brain Out	Brain Out MOD APK v2.8.5 [Unlimited Hints/No Ads] for Android	Penambahan informasi
Nama Paket	com.mind.quiz.brain.out	Brain-Out-v2.8.5-MOD-GMA-(Getmodsapk.com).apk	Perbedaan nama paket
Versi	2.8.5	2.8.5	
Pengembang	Focus apps	Focus apps	
Ukuran APK	123.3MB	98.1MB	Versi asli lebih besar
Tanggal Update	23 Januari 2024	15 April 2024	Versi mod lebih baru
Sumber	PlayStore	https://getmodsapk.com/brain-out-can-you-pass-mod-apk/	
Tanggal Unduh	16 Juni 2024	16 Juni 2024	

4. Subway Surfers

Hasil perbandingan metadata aplikasi *game* Subway Surfers menunjukkan bahwa, versi modifikasi memiliki penambahan informasi dan nama paket yang berbeda. Selain itu versi modifikasi juga memiliki ukuran yang lebih besar dan tanggal update terbaru. Versi modifikasi juga menawarkan fitur *unlock* semua karakter, koin dan kunci tak terbatas. Perbandingan tersebut ditunjukkan dalam Tabel 4.8 berikut:

Tabel 4.8 Perbandingan Metadata *Game* Subway Surfers

Aspek	*Game* Asli	*Game* Mod	Ket
Nama Aplikasi	Subway Surfers	Subway Surfers Mod APK 3.30.2 (Semua karakter, koin dan kunci tak terbatas)	Penambahan informasi
Nama Paket	com.kiloo.subwaysurf	Subway-Surfers-3.30.2-Mod-ModCombo.Com.apk	Perbedaan nama paket
Versi	3.30.2	3.30.2	

Aspek	*Game* Asli	*Game* Mod	Ket
Pengembang	SYBO *Games*	SYBO *Games*	
Ukuran APK	168.05MB	168.47MB	Versi mod lebih besar
Tanggal Update	10 Juni 2024	12 Juni 2014	Versi mod lebih baru
Sumber	PlayStore	https://modcombo.com/id/download/mod/subway-surfers-1058-1099	
Tanggal Unduh	16 Juni 2024	16 Juni 2024	

5. Stickman Party

Hasil perbandingan metadata aplikasi *game Stickman Party* menunjukkan bahwa, versi mod memiliki beberapa perbedaan seperti penambahan informasi nama, nama paket yang berbeda, ukuran yang lebih besar, dan pembaruan yang lebih baru. Selain itu versi modifikasi juga menawarkan fitur uang dan gems tak terbatas. Perbandingan tersebut ditunjukkan dalam Tabel 4.9 berikut:

Tabel 4.9 Perbandingan Metadata *Game* Stickman Party

Aspek	*Game* Asli	*Game* Mod	Ket
Nama Aplikasi	Stickman Party	Stickman Party Mod APK 2.3.8.3 (Menu/Unlimited money/Gems)	Penambahan informasi
Nama Paket	com.PlayMax.player*games*	Stickman-Party-2.3.8.3-Mod-ModCombo.io	Nama paket yang berbeda
Versi	2.3.8.3	2.3.8.3	
Pengembang	PlayMax *Game* Studio	PlayMax *Game* Studio	
Ukuran APK	61.39MB	101.68MB	Versi mod lebih besar
Tanggal Update	22 Agustus 2023	9 Oktober 2023	Versi mod

Aspek	*Game* Asli	*Game* Mod	Ket
			lebih baru
Sumber	PlayStore	https://modcombo.io/stickman-party.html	
Tanggal Unduh	16 Juni 2024	16 Juni 2024	

4.2.2 Perubahan Karakteristik Aplikasi *Game*

Perubahan dalam karakteristik aplikasi *game* didapatkan saat kedua versi *game* dijalankan pada masing-masing perangkat Android. Perubahan tersebut bisa mencakup *gameplay* dan konten dalam *game* termasuk bagaimana *game* tersebut mendapatkan gems atau uang dalam *game*. Perubahan karakteristik aplikasi *game* disajikan dalam uraian berikut :

1. Zombie Tsunami

Dalam permainan Zombie Tsunami, pemain akan memulai permainan dengan satu zombie dan bertugas untuk menyerang pejalan kaki untuk menambah jumlah zombie dalam gerombolan mereka. Untuk memperkuat karakter, terdapat fitur *power-up*, seperti raksasa zombie, ninja, atau bahkan UFO, yang memberikan kemampuan khusus sementara. Selain itu, ada berbagai rintangan dan jebakan yang harus dihindari, seperti bom, jurang, dan kendaraan.

Pada versi asli maupun modifikasi pada *game* Zombie Tsunami, tidak ada perubahan dari segi *gameplay*, maupun cara mendapatkan gems atau uang dalam *game*. Seperti ditunjukkan pada Gambar 4.8.

Gambar 4.8 *Gameplay Game* Zombie Tsunami

Perubahan yang terjadi terdapat pada jumlah koin dan gems saat memulai permainan. Pada versi asli yang ditunjukkan oleh Gambar 4.9, jumlah koin dan gems masih sangat sedikit dan tidak bisa digunakan untuk membeli item sama sekali.

Gambar 4.9 Tampilan Versi Asli *Game* Zombie Tsunami

Sementara pada versi modifikasi, ditunjukkan pada Gambar 4.10, sudah memiliki lebih dari 2 Milyar koin dan gems Koin yang sudah bisa digunakan begitu memulai permainan.

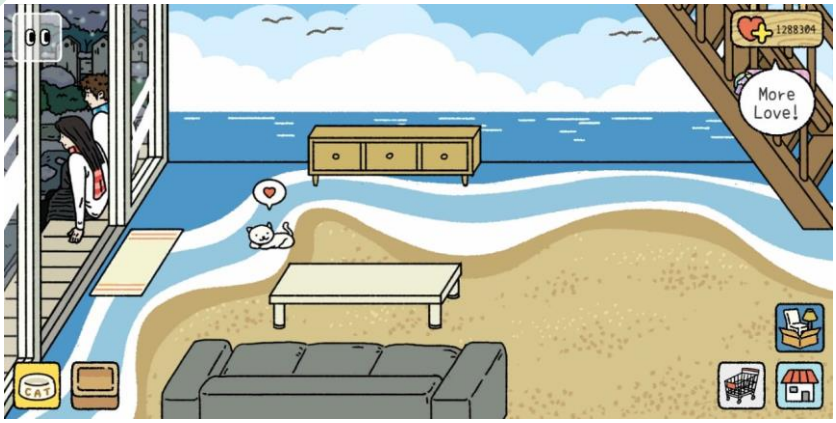
Gambar 4.10 Tampilan Versi Mod *Game* Zombie Tsunami

Sehingga dapat disimpulkan bahwa, versi mod *game* Zombie Tsunami memiliki perubahan signifikan pada jumlah koin dan gems yang tersedia di awal permainan. Perubahan tersebut mempengaruhi pengalaman permainan dengan memberikan akses lebih cepat dan lebih banyak ke dalam konten *game* tanpa harus menunggu lama.

2. Adorable Home

Game Adorable Home adalah permainan santai tentang mengelola kehidupan rumah tangga yang ideal. Permainan dimulai dengan memilih pasangan dan mengatur rumah mereka dengan dekorasi yang lucu dan furnitur yang nyaman. Fokus utama permainan adalah merawat hewan peliharaan, terutama kucing, yang membutuhkan perhatian melalui memberi makan, membersihkan, dan bermain. Pemain juga dapat mengumpulkan hati yang merupakan mata uang dalam *game* yang diperoleh dari interaksi dengan pasangan dan hewan peliharaan, dan dapat digunakan untuk membeli lebih banyak perabotan dan dekorasi.

Dalam versi modifikasi *game* Adorable Home, sudah terlihat perbedaan pada tampilan awal yaitu bagian jumlah hati yang banyak seperti pada Gambar 4.11. Hati tersebut sudah dapat digunakan untuk membeli item dan *unlock* item dalam *game*. Berbeda dengan versi asli seperti pada Gambar 4.12, yang hanya memiliki sedikit hati.



Gambar 4.11 Tampilan Versi Mod *Game* Adorable Home

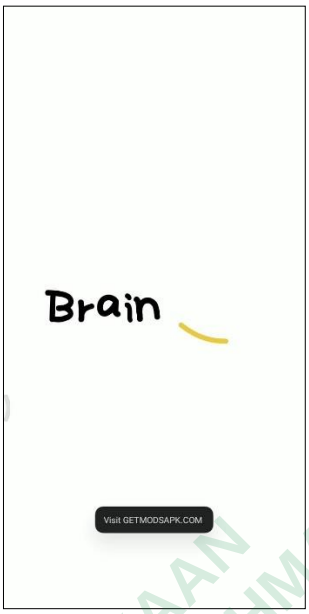
Gambar 4.12 Tampilan Versi Asli *Game* Adorable Home

Sehingga dapat disimpulkan bahwa, pada versi mod *game* Adorable Home, terdapat perubahan signifikan pada jumlah hati yang tersedia di awal permainan dan dapat digunakan untuk membeli item dan membuka konten dalam *game* secara cepat. Perubahan tersebut memungkinkan pemain untuk lebih leluasa dalam mengelola dan mendekorasi rumah serta merawat hewan peliharaan mereka tanpa harus menunggu terlalu lama untuk mengumpulkan hati.

3. Brain Out

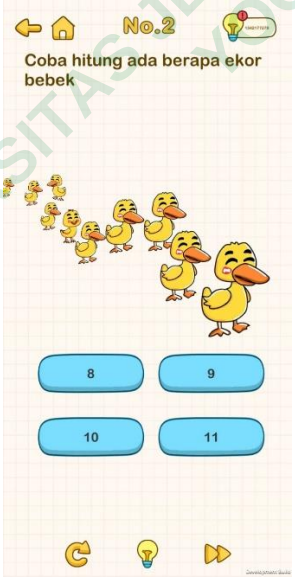
Brain Out adalah *game puzzle* interaktif yang menantang logika dan kreativitas pemain dengan serangkaian teka-teki unik. Setiap level menghadirkan pertanyaan atau tugas yang terlihat sederhana namun memerlukan pemikiran tak terduga untuk menyelesaikannya. Untuk membantu mempermudah permainan, terdapat fitur *hint* atau petunjuk yang dapat didapatkan dengan menggunakan koin yang diperoleh dari menyelesaikan level atau menonton iklan.

Pada versi modifikasi sudah terlihat jelas perbedaan terutama pada *loading screen* pada *game* seperti pada Gambar 4.13, yang mana muncul *popup* pembuat versi mod, yaitu “Visit GETMODSAPK.COM”.

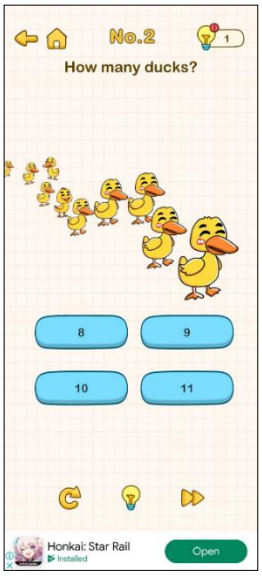


Gambar 4.13 *Loading Screen* Versi Mod *Game* Brain Out

Selain itu, pada versi mod juga sudah terdapat *unlimited hint* seperti pada Gambar 4.14, yang sudah dapat digunakan sejak mulai permainan. Berbeda dengan versi asli pada Gambar 4.15, yang masih hanya memiliki sedikit *hint*.



Gambar 4.14 Tampilan Versi Mod *Game* Brain Out



Gambar 4.15 Tampilan Versi Asli *Game* Brain Out

Versi asli juga memiliki banyak iklan yang tampil di sela permainan setiap menyelesaikan 4 level seperti pada Gambar 4.17, dan juga *banner*

iklan di layar bawah. Sementara pada versi mod tidak terdapat iklan sama sekali seperti ditunjukkan pada Gambar 4.16.

Gambar 4.16 Tampilan Versi Mod *Game* Brain Out

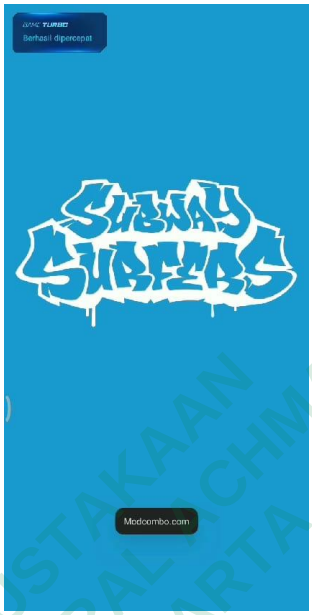
Gambar 4.17 Tampilan Versi Asli *Game* Brain Out

Sehingga dapat disimpulkan bahwa, versi mod *game* Brain Out terdapat dua perubahan utama yang signifikan. Pertama, *popup* pada *loading screen* yang mengarahkan pemain untuk mengunjungi situs "GETMODSAPK.COM", yang menunjukkan bahwa *game* tersebut adalah versi mod. Kedua, versi mod menawarkan *unlimited hint* yang tersedia sejak awal permainan dan tidak adanya iklan. Perubahan tersebut mempengaruhi permainan karena teka-teki dapat diselesaikan dengan cepat.

4. Subway Surfers

Dalam *game* Subway Surfers, pemain berperan sebagai seorang remaja yang melarikan diri dari penjaga keamanan di jalur kereta. Pemain harus menghindari rintangan dengan melompat, bergeser, dan berlari secepat mungkin sambil mengumpulkan koin dan kunci untuk meningkatkan skor dan membuka karakter dan papan luncur.

Pada versi modifikasi sudah terlihat jelas perbedaan terutama pada *loading screen* pada *game* seperti pada Gambar 4.18, yang mana muncul *popup* pembuat versi mod, yaitu “ModCombo.Com”.



Gambar 4.18 *Loading Screen* Versi Mod *Game* Subway Surfers

Dalam versi modifikasi juga sudah memiliki *unlimited* koin, kunci, dan papan luncur yang dapat digunakan langsung untuk *upgrade* papan luncur, sepatu, magnet koin, pengganda koin, dan *unlock* karakter seperti pada Gambar 4.19.

Gambar 4.19 Tampilan Awal Versi Mod *Game* Subway Surfers

Sehingga dapat disimpulkan bahwa, versi mod *game* Subway Surfers, memiliki dua perubahan utama yang signifikan. Pertama, pada *loading screen* terdapat *popup* yang mengindikasikan bahwa versi mod dibuat oleh "ModCombo.Com". Kedua saat memulai permainan, versi mod sudah memiliki unlimited koin, kunci, dan papan luncur yang dapat digunakan secara langsung untuk *upgrade* berbagai fitur dan membuka karakter. Perubahan tersebut mempengaruhi permainan karena dapat memberikan kemudahan bagi pemain untuk mengakses semua fitur dan konten yang tersedia dalam permainan.

5. Stickman Party

Stickman Party adalah sebuah *game* yang menawarkan banyak variasi *mini game* yang mencakup berbagai genre, seperti balapan, pertarungan, dan teka-teki, yang dapat dimainkan baik secara solo maupun *multiplayer*. Pemain mendapatkan koin dalam *game* dengan beberapa cara, seperti menyelesaikan *mini game*, mencapai prestasi tertentu, atau mengikuti tantangan yang disediakan setiap harinya. Koin yang dikumpulkan dapat digunakan untuk membuka konten tambahan atau membeli item dalam *game*.

Perubahan utama yang terjadi pada versi modifikasi adalah jumlah koin yang sudah tersedia yaitu *unlimited* dan dapat digunakan untuk membeli item mendandani karakter dalam *game* seperti pada Gambar 4.20.

Gambar 4.20 Tampilan Versi Mod *Game* Stickman Party

Sehingga dapat disimpulkan bahwa, versi mod Stickman Party memiliki perubahan signifikan terutama dalam jumlah koin yang digunakan untuk membeli item dalam *game*. Perubahan tersebut mempengaruhi permainan karena mempermudah pemain mendapatkan item yang diinginkan tanpa perlu menunggu lama.

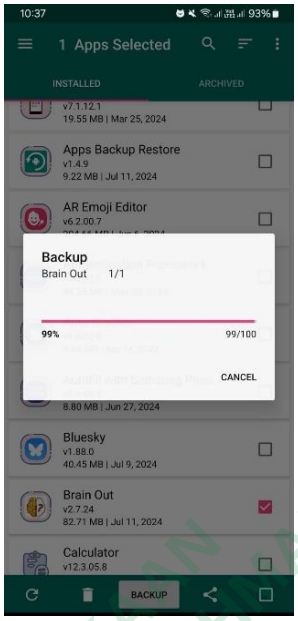
4.2.3 Teknik Pengumpulan Data

Untuk mendapatkan hasil analisis statis dan dinamis, dilakukan pengambilan data dengan *tools* yang digunakan yaitu MobSF untuk analisis statis dan PCAPDroid untuk analisis dinamis. Berikut merupakan uraian cara penggunaan masing-masing *tools* yang digunakan dalam pengambilan data :

1. MobSF

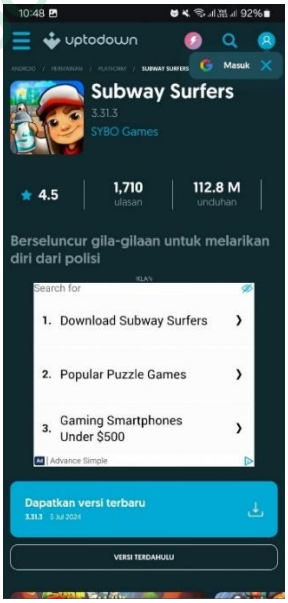
Sebelum melakukan analisis statis menggunakan MobSF, dibutuhkan *file* APK versi asli yang didapatkan dari aplikasi Apps Backup and Restore yang diunduh dari *Play Store* dan beberapa situs penyedia versi lama aplikasi Android. Berikut proses pengambilan data menggunakan analisis statis diuraikan sebagai berikut :

a. Untuk mendapatkan *file* APK pada aplikasi yang akan dianalisis, digunakan aplikasi Apps Backup and Restore pada aplikasi *game* yang telah diinstall sebelumnya. Gambar 4.21 merupakan proses pengambilan *file* APK.



Gambar 4.21 Proses Pengambilan *file* APK dengan Apps Backup and Restore

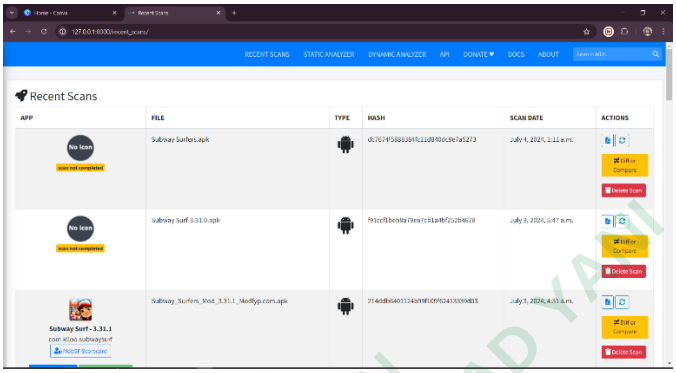
b. Selain menggunakan aplikasi Apps Backup and Restore, *file* APK juga didapatkan dari beberapa situs penyedia *archive* aplikasi seperti Uptodown dan APKcombo. Gambar 4.22 merupakan pengunduhan *file* aplikasi dari situs Uptodown.



Gambar 4.22 *Download file* Aplikasi Asli

c. *File* APK yang telah didapatkan, kemudian dilakukan analisis dengan *scanning file* menggunakan MobSF. Hasil *scan* itulah yang akan

diidentifikasi sebagai hasil analisis statis seperti pada Gambar 4.23 yang merupakan *history* hasil *scanning* pada Aplikasi yang dianalisis menggunakan MobSF.



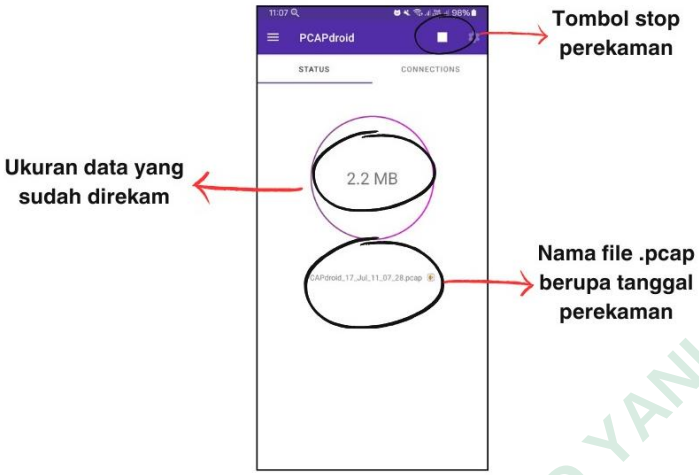
Gambar 4.23 *Recent Scan* pada MobSF

Setelah hasil *scan* didapatkan, maka dilakukan pelaporan hasil analisis statis dalam bentuk tabel perbandingan antara versi asli dan versi modifikasi.

2. PCAPDroid

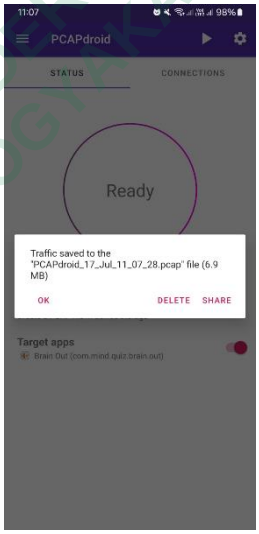
Pengambilan data menggunakan analisis dinamis menggunakan aplikasi PCAPDroid untuk menangkap paket pada saat aplikasi dijalankan di perangkat Android. Hasil perekaman akan menghasilkan file .pcap yang kemudian akan dianalisis menggunakan CloudShark. Berikut langkah untuk melakukan analisis dinamis menggunakan *packet analysis* :

a. Perangkat Android dalam keadaan kosong tanpa ada aplikasi lain yang dapat berjalan di latar belakang, dan aplikasi PCAPDroid sudah terpasang di perangkat. Mulai melakukan *scanning* pada aplikasi PCAPDroid selama kurang lebih 5 menit. Gambar 4.24 merupakan proses *scanning* perangkat Android menggunakan PCAPDroid.



Gambar 4.24 Proses *Scanning* Pada Aplikasi PCAPDroid

b. Setelah proses *scanning* selesai, *file* analisis yang memiliki format *file* .pcap dapat dibagikan dan otomatis tersimpan pada perangkat Android yang digunakan seperti pada Gambar 4.25.



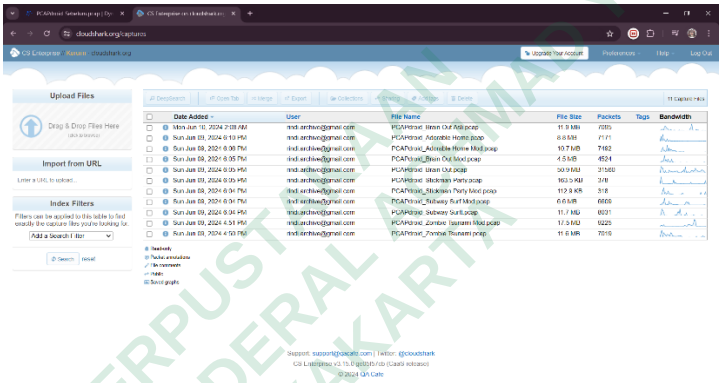
Gambar 4.25 *File* .pcap Hasil Analisis Dinamis

c. Hasil perekaman tersebut, diperoleh *file* .pcap yang kemudian akan dianalisis menggunakan *tools* Cloudshark. *File* tersebut disajikan dalam Tabel 4.10 berikut :

Tabel 4.10 Hasil *file* .pcap

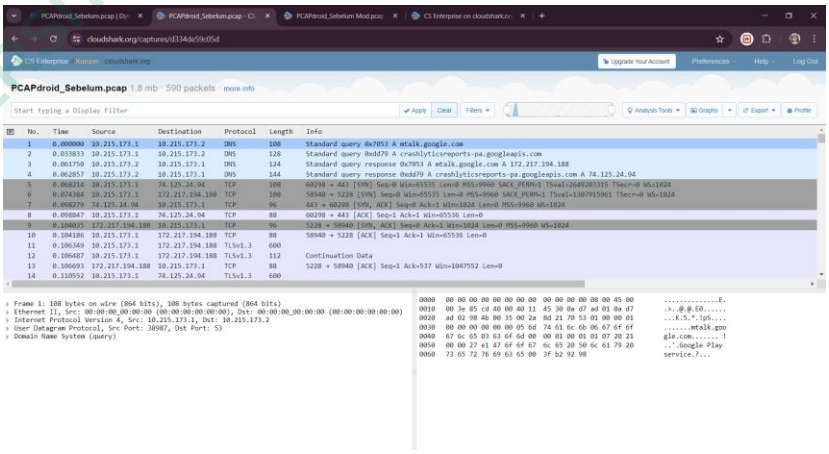
Perangkat Android	Ukuran File .pcap Aplikasi				
	Zombie Tsunami	**Brain Out**	**Adorable Home**	**Subway Surfers**	**Stickman Party**
Samsung	34 MB	11.9 MB	41.1 MB	10.1 MB	2.48 MB
Xiaomi	17.5 MB	18.2 MB	15.4 MB	4.16 MB	181 KB

d. *File* .pcap tersebut kemudian akan dibaca lebih lanjut menggunakan *tools* CloudShark. Gambar 4.26 merupakan halaman awal *website* CloudShark.



Gambar 4.26 Halaman Awal Website CloudShark

e. Berikutnya *file* .pcap di unggah dan menunggu hasil pembacaan *file* selesai. Hasil analisis *file* .pcap ditunjukkan pada Gambar 4.27.



Gambar 4.27 Contoh Hasil Analisis *File* .pcap

4.3 ANALISIS STATIS

Pengambilan data dengan metode analisis statis, membutuhkan *file* APK yang akan diunggah untuk dilakukan analisis menggunakan *tools* MobSF. Analisis ini akan menghasilkan informasi penting terkait aplikasi *game* seperti izin berbahaya, analisis sertifikat, dan analisis *manifest*. Adapun hasil analisis statis diperlukan untuk melihat sejauh mana aplikasi mengakses perangkat pengguna.

Perbandingan hasil analisis statis pada versi asli dan modifikasi diuraikan sebagai berikut :

1. Zombie Tsunami

Perbandingan analisis statis aplikasi *game* Zombie Tsunami versi asli dan versi modifikasi ditunjukkan pada Tabel 4.11 berikut:

Tabel 4.11 Analisis Statis Aplikasi *Game* Zombie Tsunami

Parameter	*Game* Asli	*Game* Mod
Nilai Checksum	SHA256 : 4f6e18e7139e990b50859db50c871c527188655a17b0126822426f605d9ea9b3	SHA256 : 0f890b33e2b7d4cc8bae3ad4b5c5f30b2ee863ff74c52f46370e30a3f2257c54
Informasi Sertifikat (X.509 Subject)	Country = France State = Unknown Locality = Paris Organization = Mobi*game* Organizational Unit = Unknown Common Name = Unknown	Country = Rusia State = Lazyland Locality = Lazyland Organization = A1 Organizational Unit = A1 Common Name = A1 *Email* = a1@tr4oo3r34r34sdfd.com
URL Aplikasi	https://play.google.com/store/apps/details?id=net.mobi*game*.zombietsunami&hl=en	https://an1.com/1686-zombie-tsunami-mod.html
Izin berbahaya	5 Dangerous	5 Dangerous
Analisis sertifikat	2 Warning	1 Warning
Analisis *manifest*	2 High	2 High
Email	Tidak ada	Terdapat 4 *email*

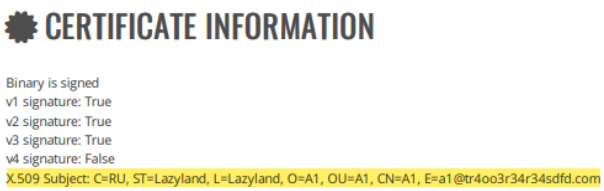
Berdasarkan Tabel 4.11 disimpulkan bahwa, terdapat perbedaan yang cukup signifikan pada nilai *checksum*, informasi sertifikat, analisis sertifikat, dan *email* yang terdapat pada aplikasi. Berikut uraian untuk memahami perbedaan tersebut :

Gambar 4.28 Nilai Checksum Versi Mod *Game* Zombie Tsunami

Gambar 4.29 Nilai Checksum Versi Asli *Game* Zombie Tsunami

Berdasarkan nilai checksum SHA256 versi mod seperti pada Gambar 4.28, berbeda dengan SHA256 versi asli seperti pada Gambar 4.29. Yang artinya, telah terjadi perubahan integritas data dan berpengaruh pada keamanan aplikasi.

Gambar 4.30 Informasi Sertifikat Versi Asli *Game* Zombie Tsunami



Gambar 4.31 Informasi Sertifikat Versi Mod *Game* Zombie Tsunami

Pada bagian informasi sertifikat khususnya X.509 Subject yang ditunjukkan pada Gambar 4.30, menunjukkan bahwa versi asli berasal dari negara Prancis dengan organisasi Mobigame yaitu pengembang game

Zombie Tsunami dengan informasi lain yang lebih terbatas. Sementara versi modifikasi seperti pada Gambar 4.31, memiliki informasi yang lengkap antara lain berasal dari negara Rusia namun negara bagian dan kota dummy juga organisasi A1 yang mengindikasikan situs penyedia game modifikasi An1 juga penambahan informasi email terkait organisasi penerbit game modifikasi.

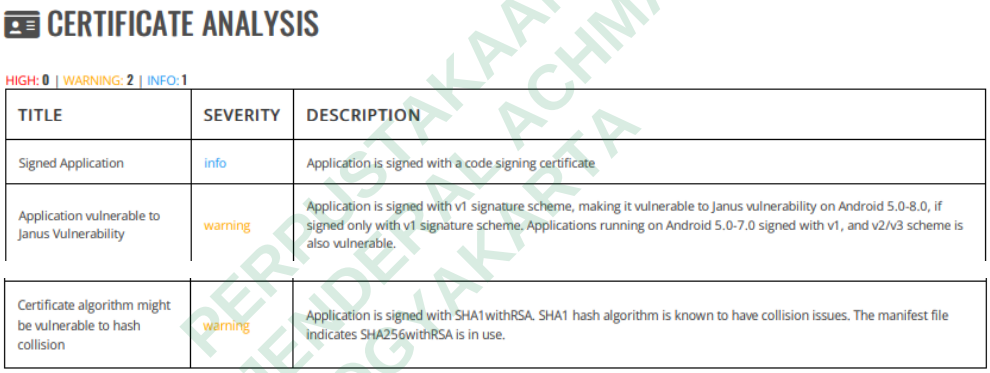
APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_INTERNAL_STORAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.

Gambar 4.32 Izin Berbahaya Versi Asli *Game* Zombie Tsunami

Pada izin berbahaya, kedua versi aplikasi game memiliki izin berbahaya yang sama, yaitu 5 izin berbahaya seperti ditunjukkan pada Gambar 4.32, ditampilkan bahwa pada READ_EXTERNAL_STORAGE yaitu mengizinkan aplikasi untuk membaca konten dari penyimpanan eksternal, dianggap berbahaya karena aplikasi dapat mengakses data sensitif pengguna yang tersimpan di penyimpanan eksternal. Pada bagian WRITE_EXTERNAL_STORAGE yaitu mengizinkan aplikasi untuk menulis ke penyimpanan eksternal, dianggap berbahaya karena memiliki potensi untuk mengakses dan memodifikasi data pengguna. Pada

READ_PHONE_STATE, yaitu mengizinkan aplikasi untuk mengambil informasi terkait status telepon, dianggap berbahaya karena aplikasi dapat mengumpulkan informasi pribadi tentang pengguna. Bagian POST_NOTIFICATIONS, yaitu mengizinkan aplikasi untuk menampilkan notifikasi, dianggap berbahaya karena berpotensi disalahgunakan untuk mengirim notifikasi spam. Bagian GET_TASK, yaitu mengizinkan aplikasi untuk mengambil informasi tentang aplikasi yang sedang berjalan dan baru saja berjalan, dianggap berbahaya karena berpotensi pada pencurian data atau penyalahgunaan privasi pada aplikasi lain yang sedang digunakan perangkat pengguna.

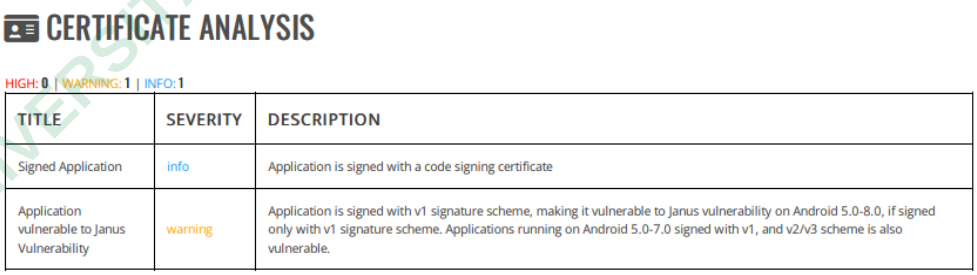


CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Gambar 4.33 Analisis Sertifikat Versi Asli *Game* Zombie Tsunami



CERTIFICATE ANALYSIS

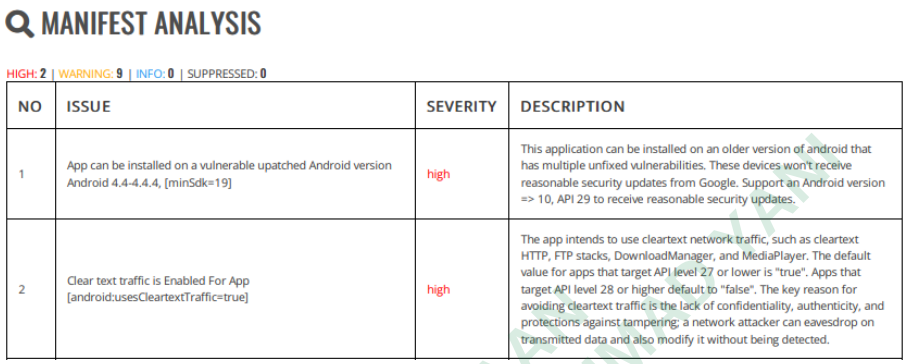
HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

Gambar 4.34 Analisis Sertifikat Versi Mod *Game* Zombie Tsunami

Sementara itu pada analisis sertifikat, versi asli memiliki 2 warning sementara versi mod hanya memiliki 1 warning. Seperti ditunjukkan pada Gambar 4.33 dan Gambar 4.34, perbedaan tersebut ditunjukkan pada versi asli yang memiliki peringatan "*Certificate algorithm might be vulnerable to hash collision*", yang artinya peringatan ini menunjukkan bahwa algoritma

sertifikat yang digunakan, yaitu SHA-1, rentan terhadap tabrakan *hash*. Tabrakan *hash* adalah situasi di mana dua input yang berbeda menghasilkan *hash* yang sama. Hal ini dapat memungkinkan penyerang untuk memalsukan identitas atau memanipulasi data.



MANIFEST ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

Gambar 4.35 Analisis *Manifest* Aplikasi *Game* Zombie Tsunami

Dari segi analisis *manifest*, kedua versi aplikasi memiliki tingkat bahaya yang sama, yaitu 2 tingkat tinggi seperti ditunjukkan pada Gambar 4.35. Pada masalah 1, aplikasi dapat diinstal pada versi Android lama (versi 4.4 - 4.4.4) yang memiliki banyak celah keamanan belum teratasi. Dikhawatirkan, perangkat yang menjalankan versi Android tersebut tidak lagi menerima pembaruan keamanan terbaru dari Google, sehingga lebih rentan terhadap serangan. Pada masalah 2, aplikasi dikonfigurasi untuk menggunakan komunikasi jaringan tanpa enkripsi (*cleartext traffic*), seperti HTTP tanpa enkripsi. Sehingga, jaringan rentan terhadap pencurian dan modifikasi oleh pihak ketiga yang tidak berwenang.

EMAILS

EMAIL	FILE
f0i@lpa.rp p6@h.b1a bpt@a.bk m@lakbj.i4hcg	apktool_out/lib/armeabi-v7a/libsigner.so
f0i@lpa.rp p6@h.b1a bpt@a.bk m@lakbj.i4hcg	lib/armeabi-v7a/libsigner.so

Gambar 4.36 Informasi *Email* pada Versi Mod *Game* Zombie Tsunami

Dari segi *email*, versi asli tidak terdapat *email* sementara versi mod terdeteksi memiliki 4 *email* seperti ditunjukkan pada Gambar 4.36. *Email* tersebut kemungkinan digunakan untuk mendistribusikan *file* "libsigner.so" ke beberapa alamat *email* melalui jalur *file* dan lokasi berbeda.

2. Adorable Home

Perbandingan analisis statis aplikasi *game* Adorable Home pada versi asli dan modifikasi ditunjukkan pada Tabel 4.11 berikut:

Tabel 4.11 Analisis Statis Aplikasi *Game* Adorable Home

Parameter	*Game* Asli	*Game* Mod
Nilai Checksum	SHA256 : c9235c205b7ceb80ee2d14e6087e9a914df2ac4ab51893291266390140 7df439	SHA256 : c8471fe5205cd43a24aa4acd664b9aec27fbe64d9cbd611a8051a43bb3eef1f7
Informasi Sertifikat (X.509 Subject)	Country = 57000 State = Mexico Locality = Nezahualcoyotl Organization = AppsOrama Organizational Unit = Developer Common Name = JoseTorres	Country = United State State = California Locality = Montaine View Organization = Android Organizational Unit = Android Common Name = Android *Email* = android@android.com
URL Aplikasi	https://adorable-home.en.uptodown.com/android/download/1016367343	https://modcombo.io/adorable-home.html
Izin berbahaya	2 Dangerous	2 Dangerous
Analisis sertifikat	1 Warning	2 Warning
Analisis *manifest*	1 High	1 High
Email	Terdapat 2 *Email*	Terdapat 2 *email*

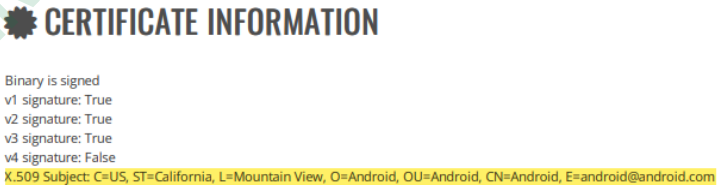
Berdasarkan Tabel 4.11 disimpulkan bahwa, terdapat perbedaan yang signifikan dari nilai *checksum*, informasi sertifikat, dan analisis sertifikat. Berikut uraian untuk memahami perbedaan tersebut :

Gambar 4.37 Nilai *Checksum* Versi Mod *Game* Adorable Home

Gambar 4.38 Nilai *Checksum* Versi Asli *Game* Adorable Home

Berdasarkan nilai *checksum* SHA256 versi mod seperti ditunjukkan pada Gambar 4.37, berbeda dengan SHA256 versi asli seperti pada Gambar 4.38. Yang artinya, telah terjadi perubahan integritas data dan berpengaruh pada keamanan aplikasi.

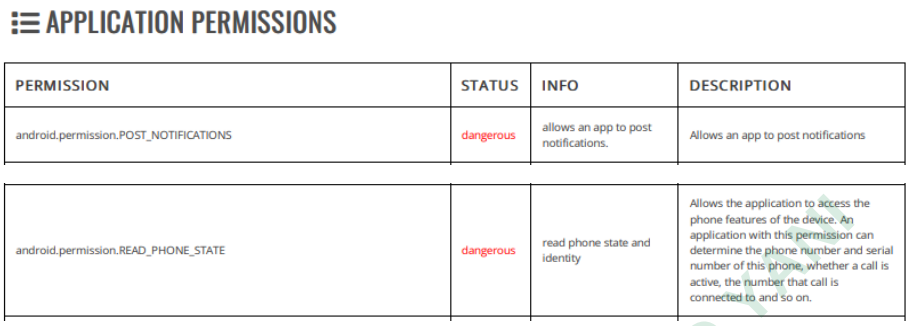
Gambar 4.39 Informasi Sertifikat Versi Asli *Game* Adorable Home



Gambar 4.40 Informasi Sertifikat Versi Mod *Game* Adorable Home

Pada bagian informasi sertifikat khususnya X.509 *Subject* seperti ditunjukkan pada Gambar 4.39, menunjukkan bahwa versi asli memiliki informasi pengembang yang sah seperti berasal dari Mexico, dengan organisasi unit Developer dalam organisasi AppsOrama dan Common Name Jose Torres. Sementara pada versi mod seperti ditunjukkan pada

Gambar 4.40, menunjukkan bahwa informasi yang diberikan mengacu pada Android. Perbedaan dalam informasi ini menunjukkan bahwa versi mod telah diubah asal-usulnya.

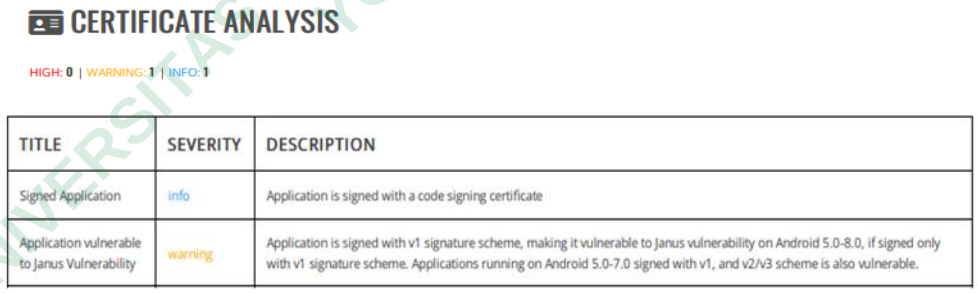


APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

Gambar 4.41 Izin Berbahaya Aplikasi *Game* Adorable Home

Kedua versi aplikasi *game* memiliki izin aplikasi yang terdeteksi berbahaya seperti ditunjukkan pada Gambar 4.41, menampilkan pada bagian POST_NOTIFICATIONS, yaitu izin aplikasi untuk menampilkan notifikasi, dianggap berbahaya karena berpotensi memberikan notifikasi spam. Dan pada bagian READ_PHONE_STATE, yaitu izin aplikasi untuk mengakses identitas telepon, dianggap berbahaya karena aplikasi dapat mengumpulkan informasi pengguna dan potensi penyalahgunaan data.

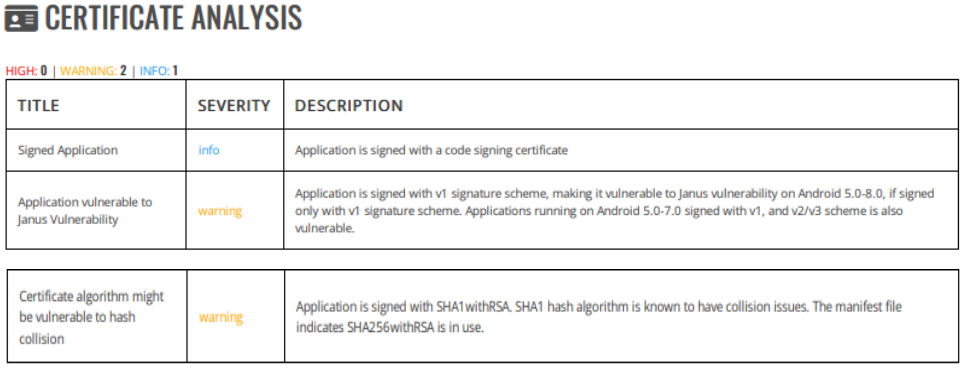


CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

Gambar 4.42 Analisis Sertifikat Versi Asli *Game* Adorable Home



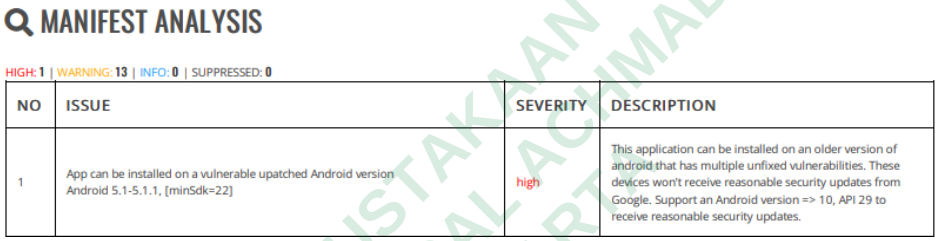
CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Gambar 4.43 Analisis Sertifikat Versi Mod *Game* Adorable Home

Pada analisis sertifikat, versi asli memiliki 1 *warning* dan versi mod 2 *warning* seperti ditunjukkan pada Gambar 4.42 dan Gambar 4.43. Perbedaan tersebut terletak pada versi modifikasi yang memiliki peringatan "*Certificate algorithm might be vulnerable to hash collision*", yang artinya peringatan ini menunjukkan bahwa algoritma sertifikat yang digunakan, yaitu SHA-1, mungkin rentan terhadap tabrakan hash. Hal ini dapat memungkinkan penyerang untuk memalsukan identitas atau memanipulasi data.



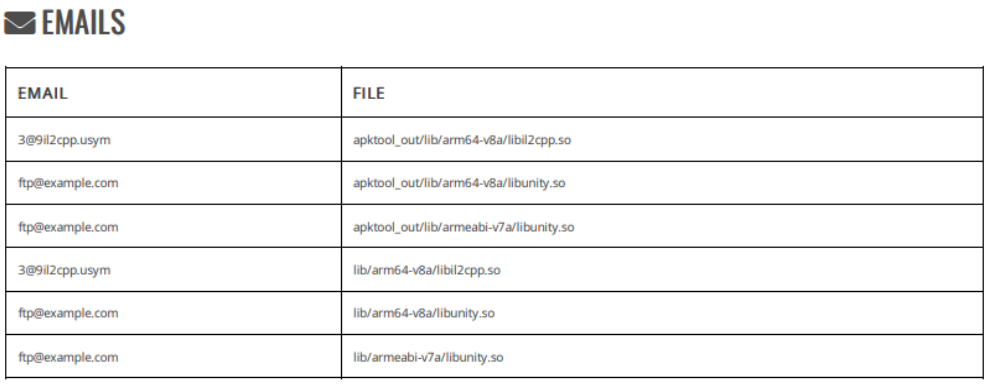
MANIFEST ANALYSIS

HIGH: 1 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

Gambar 4.44 Analisis *Manifest* Aplikasi *Game* Adorable Home

Dari segi analisis *manifest*, kedua versi aplikasi memiliki tingkat bahaya yang sama, yaitu 1 tingkat tinggi seperti ditunjukkan pada Gambar 4.44. Masalah tersebut karena, aplikasi dapat diinstal pada versi Android lama yaitu Android 5.1 hingga 5.1.1, yang memiliki banyak kerentanan yang belum diperbaiki. Dikhawatirkan, perangkat yang menjalankan aplikasi di versi Android tersebut tidak lagi menerima pembaruan keamanan terbaru dari Google, sehingga lebih rentan terhadap serangan.



EMAILS

EMAIL	FILE
3@9il2cpp.usym	apktool_out/lib/arm64-v8a/libil2cpp.so
ftp@example.com	apktool_out/lib/arm64-v8a/libunity.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libunity.so
3@9il2cpp.usym	lib/arm64-v8a/libil2cpp.so
ftp@example.com	lib/arm64-v8a/libunity.so
ftp@example.com	lib/armeabi-v7a/libunity.so

Gambar 4.45 Informasi *Email* Aplikasi *Game* Adorable Home

Berdasarkan *email*, kedua versi memiliki jumlah *email* yang sama yaitu 2 seperti ditunjukkan pada Gambar 4.45, kedua *email* tersebut terhubung ke beberapa *file* dalam folder “apktool_out” dan “lib”. Kemungkinan *email* tersebut digunakan untuk mengidentifikasi atau memantau penggunaan dan distribusi *file-file* tertentu dalam pengembangan aplikasi.

3. Brain Out

Perbandingan hasil analisis MobSF pada aplikasi *Game* Brain Out versi asli dan modifikasi ditunjukkan pada Tabel 4.13.

Tabel 4.12 Analisis Statis Aplikasi *Game* Brain Out

Parameter	*Game* Asli	*Game* Mod
Nilai Checksum	SHA256: : 338f3b065d2430fd41e3b8debd3b2180ecf2951bf7b6caa74890c1cb3cc4d384	SHA256 : 2abf83011ebfcf4ca82c6c7697a1e565bf5083dfffb61cedfb390aea61fc1ac3
Informasi Sertifikat (X.509 Subject)	Country = United State State = California Locality = Mountaine View Organization = Google Inc. Organizational Unit = Android Common Name = Android	Country = United State State = California Locality = Mountaine View Organization = Android Organizational Unit = Android Common Name = Android *Email* = android@android.com
URL Aplikasi	https://apkcombo.com/brain-out/com.mind.quiz.brain.out/	https://getmodsapk.com/brain-out-can-you-pass-mod-apk/
Izin berbahaya	3 Dangerous	3 Dangerous
Analisis sertifikat	1 Warning	2 Warning
Analisis *manifest*	1 High	1 High
Email	Terdapat 3 *Email*	Terdapat 2 *email*

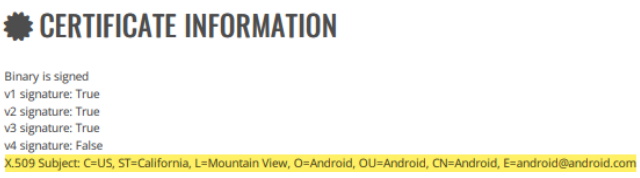
Berdasarkan Tabel 4.13 dapat disimpulkan bahwa, terdapat perbedaan signifikan pada nilai *checksum*, informasi sertifikat, dan *email*. Berikut uraian untuk memahami perbedaan tersebut :

Gambar 4.46 Nilai *Checksum* Versi Mod *Game* Brain Out

Gambar 4.47 Nilai *Checksum* Versi Asli *Game* Adorable Home

Pada nilai *checksum* SHA256 versi mod seperti ditunjukkan pada Gambar 4.46, berbeda dengan SHA256 versi asli seperti pada Gambar 4.47. Artinya, telah terjadi perubahan integritas data dan berpengaruh pada keamanan aplikasi.

Gambar 4.48 Informasi Sertifikat Versi Asli *Game* Brain Out



Gambar 4.49 Informasi Sertifikat Versi Mod *Game* Brain Out

Pada bagian informasi sertifikat X.509 *Subject* seperti pada Gambar 4.48 dan Gambar 4.49, pada versi asli dan versi mod memiliki informasi yang hampir sama namun hanya berbeda pada informasi organisasi dan penambahan *email* pada versi modifikasi.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

Gambar 4.50 Izin Berbahaya Aplikasi *Game* Brain Out

Kedua aplikasi *game* memiliki persamaan pada izin berbahaya yang terdeteksi yaitu 3 izin berbahaya seperti ditunjukkan pada Gambar 4.50, pada POST_NOTIFICATION, yaitu izin aplikasi untuk menampilkan notifikasi, dianggap berbahaya karena berpotensi memberikan notifikasi *spam*. Pada bagian READ_EXTERNAL_STORAGE, yaitu mengizinkan aplikasi untuk membaca konten dari penyimpanan eksternal, dianggap berbahaya karena aplikasi dapat mengakses data sensitif pengguna yang tersimpan di penyimpanan eksternal. Bagian READ_MEDIA_IMAGES, yaitu mengizinkan aplikasi membaca *file* gambar dari penyimpanan eksternal perangkat, dianggap berbahaya karena sifatnya yang sensitif dan dapat menimbulkan risiko privasi jika digunakan oleh aplikasi yang tidak tepercaya atau berbahaya.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

Gambar 4.51 Analisis Sertifikat Versi Asli *Game* Brain Out

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Gambar 4.52 Analisis Sertifikat Versi Mod *Game* Brain Out

Pada analisis sertifikat, versi asli memiliki 1 warning dan versi mod 2 warning seperti ditunjukkan pada Gambar 4.51 dan Gambar 4.52. Perbedaan terletak pada versi modifikasi yang memiliki peringatan "*Certificate algorithm might be vulnerable to hash collision*", yang artinya peringatan ini menunjukkan bahwa algoritma sertifikat yang digunakan, yaitu SHA-1, mungkin rentan terhadap tabrakan hash. Tabrakan hash adalah situasi di mana dua input yang berbeda menghasilkan hash yang sama. Hal ini dapat memungkinkan penyerang untuk memalsukan identitas atau memanipulasi data.

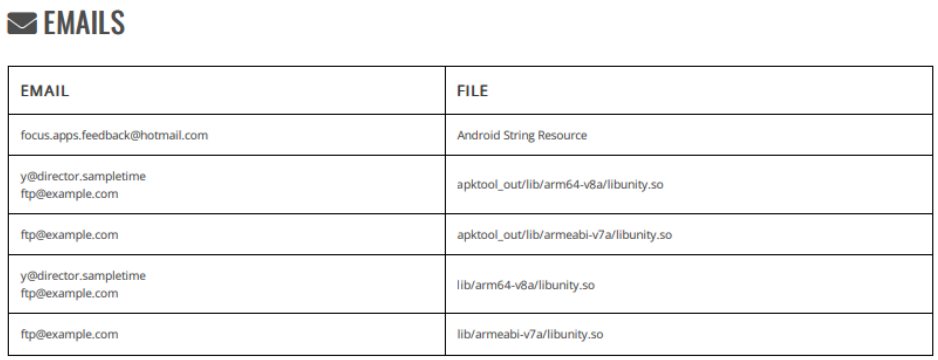
MANIFEST ANALYSIS

HIGH: 1 | WARNING: 15 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

Gambar 4.53 Analisis *Manifest* Aplikasi *Game* Brain Out

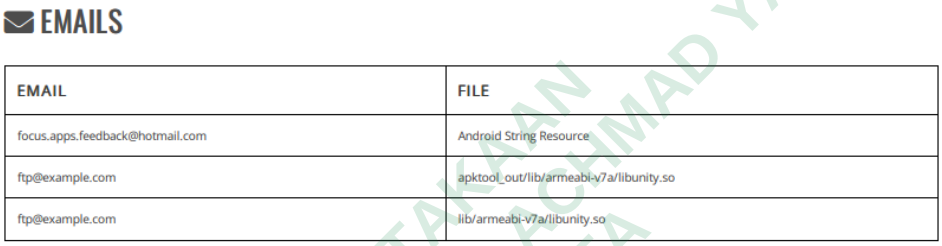
Pada analisis *manifest*, kedua versi aplikasi memiliki 1 masalah tingkat tinggi yang sama. Yaitu seperti ditunjukkan pada Gambar 4.53, karena aplikasi dapat diinstal pada versi Android lama yaitu Android 5.0 hingga 5.0.2, yang memiliki banyak kerentanan yang belum diperbaiki. Dikhawatirkan, perangkat yang menjalankan aplikasi di versi Android tersebut tidak lagi menerima pembaruan keamanan terbaru dari Google, sehingga lebih rentan terhadap serangan.



EMAILS

EMAIL	FILE
focus.apps.feedback@hotmail.com	Android String Resource
y@director.sampletime ftp@example.com	apktool_out/lib/arm64-v8a/libunity.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libunity.so
y@director.sampletime ftp@example.com	lib/arm64-v8a/libunity.so
ftp@example.com	lib/armeabi-v7a/libunity.so

Gambar 4.54 Informasi *Email* Versi Asli Aplkasi *Game* Brain Out



EMAILS

EMAIL	FILE
focus.apps.feedback@hotmail.com	Android String Resource
ftp@example.com	apktool_out/lib/armeabi-v7a/libunity.so
ftp@example.com	lib/armeabi-v7a/libunity.so

Gambar 4.55 Informasi *Email* Versi Mod Aplikasi *Game* Brain Out

Berdasarkan *email*, versi asli memiliki 3 *email* seperti ditunjukkan pada Gambar 4.54, alamat *email* "focus.apps.feedback@hotmail.com" dan "y@director.sampletime" dengan berbagai *file library* seperti "libunity.so" di direktori yang berbeda sesuai arsitektur. Sementara pada versi modifikasi seperti ditunjukkan pada Gambar 4.55, terjadi perubahan alamat *email* dari "focus.apps.feedback@hotmail.com" menjadi "3@9il2cpp.usym" dan adanya penambahan *file* "libil2cpp.so" bersama dengan "libunity.so" dalam direktori yang sama seperti versi asli. Perubahan tersebut kemungkinan adalah penggantian identitas dan perubahan penggunaan *library* dalam sistem aplikasi.

4. Subway Surfers

Perbandingan analisis statis aplikasi *game* Subway Surfers versi asli dan modifikasi ditunjukkan pada Tabel 4.14 berikut:

Tabel 4.13 Analisis Statis Aplikasi *Game* Subway Surfers

Parameter	*Game* Asli	*Game* Mod
Nilai Checksum	SHA256 : 6e6714cad043881748e2501c75fc24531fc8d32f797a1830c72761c4aae4cbcb	SHA256 : cc6e60f91d35b564c71af5be9705c1f72c5243663bf8b4fe940771b8a2623753
Informasi Sertifikat (X.509 Subject)	Country = 45 State = Jutland Locality = Aarhus Organization = Kiloo *Games* Organizational Unit = Kiloo Common Name = Jacob Møller	Country = United State State = California Locality = Mountaine View Organization = Android Organizational Unit = Android Common Name = Android *Email* = android@android.com
URL Aplikasi	https://subway-surfers.id.uptodown.com/android/download/1015669618	https://modcombo.com/id/download/mod/subway-surfers-1058-1099
Izin berbahaya	3 Dangerous	3 Dangerous
Analisis sertifikat	2 Warning	2 Warning
Analisis *manifest*	4 High	4 High
Email	Terdapat 1 *Email*	Terdapat 1 *email*

Berdasarkan Tabel 4.14 bahwa, terdapat perbedaan signifikan pada nilai *checksum* dan informasi sertifikat. Berikut uraian untuk memahami perbedaan tersebut :

Gambar 4.56 Nilai *Checksum* Versi Mod *Game* Subway Surfers

Gambar 4.57 Nilai *Checksum* Versi Asli *Game* Subway Surfers

Pada nilai checksum SHA256 versi mod seperti ditunjukkan pada Gambar 4.56, berbeda dengan SHA256 versi asli seperti pada Gambar 4.57. Yang artinya, telah terjadi perubahan integritas data dan berpengaruh pada keamanan aplikasi.

Gambar 4.58 Informasi Sertifikat Versi Asli *Game* Subway Surfers

Gambar 4.59 Informasi Sertifikat Versi Mod *Game* Subway Surfers

Pada bagian informasi sertifikat khususnya X.509 *Subject* seperti ditunjukkan pada Gambar 4.58, versi asli menunjukkan informasi spesifik terkait lokasi dan organisasi pengembang, yaitu Kiloo *Game*s, yang berlokasi di Aarhus, Jutland, Denmark dengan Common Name Jacob Møller. Sementara pada versi mod seperti pada Gambar 4.59, menunjukkan bahwa informasi yang diberikan mengacu pada Android. Perbedaan dalam informasi ini menunjukkan bahwa versi mod telah diubah asal-usulnya.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

Gambar 4.60 Izin Berbahaya Aplikasi *Game* Subway Surfers

Kedua aplikasi *game* memiliki persamaan pada izin berbahaya yang terdeteksi yaitu 3 izin berbahaya seperti ditunjukkan pada Gambar 4.60, pada bagian WRITE_EXTERNAL_STORAGE yaitu mengizinkan aplikasi untuk menulis ke penyimpanan eksternal, dianggap berbahaya karena memiliki potensi untuk mengakses dan memodifikasi data pengguna. Bagian READ_MEDIA_IMAGES, yaitu mengizinkan aplikasi membaca *file* gambar dari penyimpanan eksternal perangkat, dianggap berbahaya karena sifatnya yang sensitif dan dapat menimbulkan risiko privasi jika digunakan oleh aplikasi yang tidak tepercaya atau berbahaya. Pada POST_NOTIFICATION, yaitu izin aplikasi untuk menampilkan notifikasi, dianggap berbahaya karena berpotensi memberikan notifikasi spam.

CERTIFICATE ANALYSIS

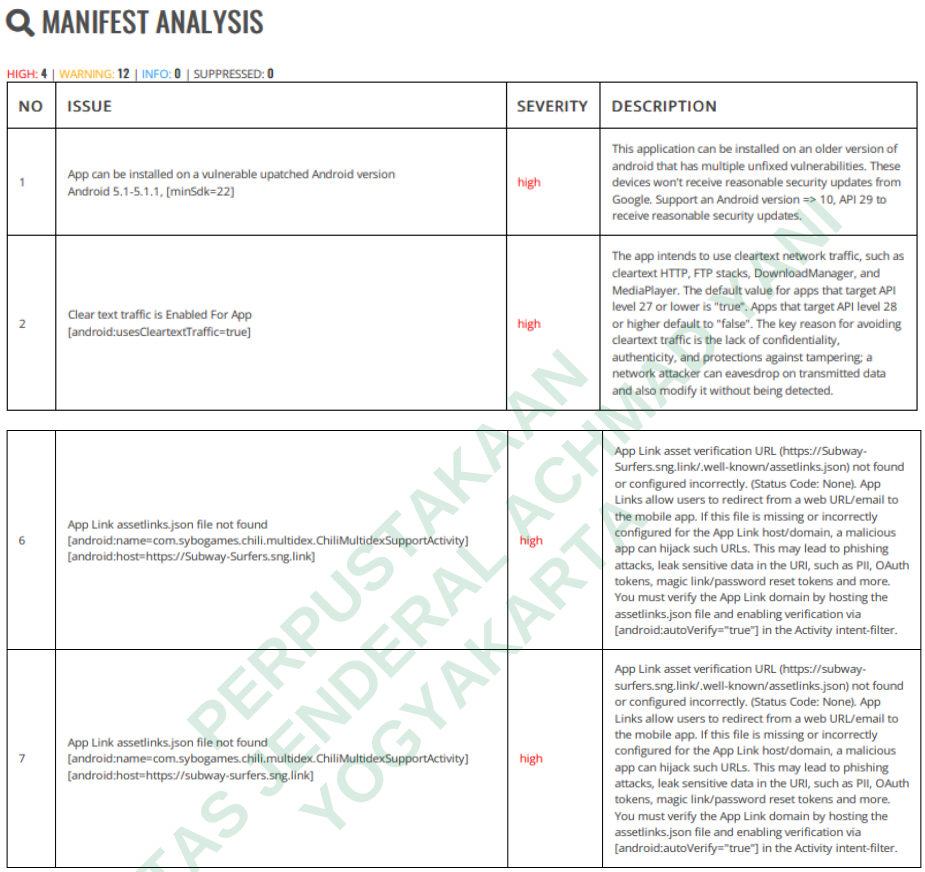
HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Gambar 4.61 Informasi Analisis Sertifikat Aplikasi *Game* Subway Surfers

Pada analisis sertifikat, kedua versi aplikasi memiliki peringatan yang sama seperti pada Gambar 4.61, yaitu aplikasi rentan terhadap *Janus Vulnerability* karena menggunakan skema tanda tangan v1, yang

membuatnya rentan pada Android 5.0-8.0 jika hanya menggunakan skema tanda tangan v1. Selain itu, algoritma sertifikat yang digunakan, SHA1 dengan RSA, diketahui memiliki masalah tabrakan hash.



MANIFEST ANALYSIS

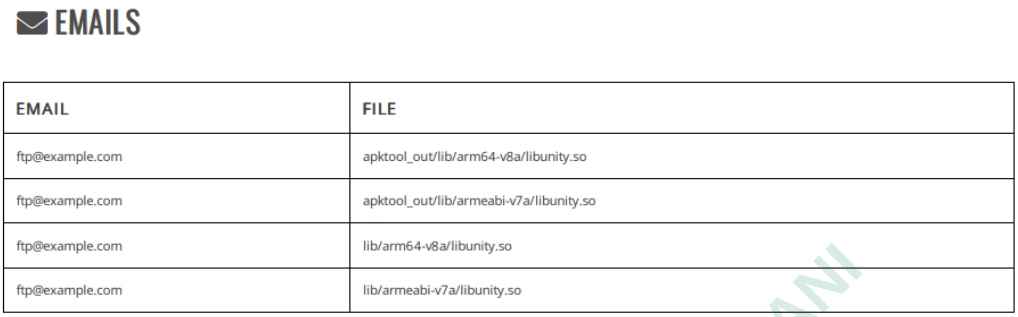
HIGH: 4 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
6	App Link assetlinks.json file not found [android:name=com.sybogames.chili.multidex.ChiliMultidexSupportActivity] [android:host=https://Subway-Surfers.sng.link]	high	App Link asset verification URL (https://Subway-Surfers.sng.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
7	App Link assetlinks.json file not found [android:name=com.sybogames.chili.multidex.ChiliMultidexSupportActivity] [android:host=https://subway-surfers.sng.link]	high	App Link asset verification URL (https://subway-surfers.sng.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

Gambar 4.62 Analisis *Manifest* Aplikasi *Game* Subway Surfers

Pada analisis *manifest*, kedua versi aplikasi *game* memiliki 4 masalah tingkat tinggi yang sama seperti ditunjukkan pada Gambar 4.62. Masalah pertama, aplikasi dapat diinstal pada versi Android lama (5.1-5.1.1) yang memiliki banyak kerentanan yang belum diperbaiki, sehingga tidak dapat menerima pembaruan keamanan yang memadai dari Google. Masalah kedua, aplikasi menggunakan lalu lintas jaringan teks biasa (cleartext), yang memungkinkan penyerang jaringan untuk menguping dan memodifikasi data yang dikirim tanpa terdeteksi. Ketiga dan keempat, *file* assetlinks.json untuk verifikasi App Link tidak ditemukan atau salah dikonfigurasi. Hal ini memungkinkan aplikasi berbahaya untuk membajak

URL yang seharusnya diarahkan ke aplikasi, yang dapat menyebabkan serangan phishing atau kebocoran data sensitif.



EMAILS

EMAIL	FILE
ftp@example.com	apktool_out/lib/arm64-v8a/libunity.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libunity.so
ftp@example.com	lib/arm64-v8a/libunity.so
ftp@example.com	lib/armeabi-v7a/libunity.so

Gambar 4.63 Informasi *Email* Aplikasi *Game* Subway Surfers

Berdasarkan *email*, kedua versi aplikasi memiliki 1 *email* yang sama seperti ditunjukkan pada Gambar 4.63. Versi mod dan versi asli memiliki kesamaan dalam alamat *email* yang sama "ftp@example.com" di setiap baris dan juga mencantumkan path *file* yang sama untuk *library* "libunity.so" di direktori yang sama.

5. Stickman Party

Perbandingan analisis statis pada aplikasi *game* Stickman Party versi asli dan versi modifikasi ditunjukkan pada Tabel 4.15 berikut:

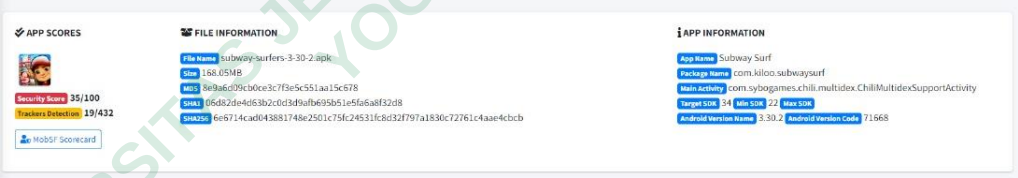
Tabel 4.14 Analisis Statis Aplikasi *Game* Stickman Party

Parameter	*Game* Asli	*Game* Mod
Nilai Checksum	SHA256 : 213d79f9cf2e9451a3aadb02108e443da72edcb010a645bc46220c31bd3c1738	SHA256 : : 24bc638f256e2ac8a5f782af3ebf443e7baa70ce59c95bd1bc07c5544986dc06
Informasi Sertifikat (X.509 Subject)	Country = United State State = California Locality = Mountain View Organization = Google Inc. Organizational Unit = Android Common Name = Android	Country = United State State = California Locality = Mountain View Organization = Android Organizational Unit = Android Common Name = Android *Email* = android@android.com

Parameter	*Game* Asli	*Game* Mod
URL Aplikasi	https://play.google.com/store/apps/details?id=com.PlayMax.player*games*&hl=en	https://modcombo.io/stickman-party.html
Izin berbahaya	1 Dangerous	1 Dangerous
Analisis sertifikat	1 Warning	2 Warning
Analisis *manifest*	1 High	1 High
Email	Tidak Terdapat	Terdapat 2 *email*

Berdasarkan Tabel 4.15 dapat disimpulkan bahwa, terdapat perbedaan signifikan pada nilai *checksum*, analisis sertifikat, dan *email*. Berikut uraian untuk memahami perbedaan tersebut :

Gambar 4.64 Nilai *Checksum* Versi Mod *Game* Stickman Party



Gambar 4.65 Nilai *Checksum* Versi Asli *Game* Stickman Party

Pada nilai checksum SHA256 versi mod seperti ditunjukkan pada Gambar 4.64, berbeda dengan SHA256 versi asli seperti pada Gambar 4.65. Yang artinya, telah terjadi perubahan integritas data dan berpengaruh pada keamanan aplikasi.

Gambar 4.66 Informasi Sertifikat Versi Asli *Game* Stickman Party

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

Gambar 4.67 Informasi Sertifikat Versi Mod *Game* Stickman Party

Pada bagian informasi sertifikat khususnya X.509 *Subject* seperti ditunjukkan pada Gambar 4.66 dan Gambar 4.67, menunjukkan bahwa versi asli dan versi mod memiliki informasi yang hampir sama namun hanya berbeda pada informasi organisasi dan penambahan *email* pada versi modifikasi.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

Gambar 4.68 Izin Berbahaya Aplikasi *Game* Stickman Party

Kedua aplikasi *game* memiliki 1 izin akses berbahaya seperti ditunjukkan pada Gambar 4.68, yaitu pada POST_NOTIFICATION, yaitu izin aplikasi untuk menampilkan notifikasi, dianggap berbahaya karena berpotensi memberikan notifikasi spam.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

Gambar 4.69 Analisis Sertifikat Versi Asli *Game* Stickman Party

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

Gambar 4.70 Analisis Sertifikat Versi Mod *Game* Stickman Party

Pada analisis sertifikat, versi asli memiliki 1 warning seperti ditunjukkan pada Gambar 4.69, dan versi modifikasi memiliki 2 warning seperti pada Gambar 4.70. Perbedaan tersebut terletak pada versi modifikasi yang memiliki peringatan "*Certificate algorithm might be vulnerable to hash collision*". Artinya, algoritma sertifikat yang digunakan, yaitu SHA-1, mungkin rentan terhadap tabrakan hash yang dapat memungkinkan penyerang untuk memalsukan identitas atau memanipulasi data.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

Gambar 4.71 Analisis *Manifest* Aplikasi *Game* Stickman Party

Pada analisis *manifest*, kedua versi aplikasi memiliki 1 masalah tingkat tinggi yang sama. Yaitu seperti ditunjukkan pada Gambar 4.71, karena aplikasi dapat diinstal pada versi Android lama yaitu Android 5.1 hingga 5.1.1, yang memiliki banyak kerentanan yang belum diperbaiki. Dikhawatirkan, perangkat yang menjalankan aplikasi di versi Android tersebut tidak lagi menerima pembaruan keamanan terbaru dari Google, sehingga lebih rentan terhadap serangan.

EMAILS

EMAIL	FILE
3@9il2cpp.usym	apktool_out/lib/arm64-v8a/libil2cpp.so
ftp@example.com	apktool_out/lib/arm64-v8a/libunity.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libunity.so
3@9il2cpp.usym	lib/arm64-v8a/libil2cpp.so
ftp@example.com	lib/arm64-v8a/libunity.so
ftp@example.com	lib/armeabi-v7a/libunity.so

Gambar 4.72 Informasi *Email* Versi Mod Aplikasi *Game* Stickman Party

Dari segi email, hanya versi modifikasi yang terdeteksi memiliki 2 *email* seperti pada Gambar 4.72. Alamat *email* tersebut adalah *email* "3@9il2cpp.usym" yang terhubung ke *file* "libil2cpp.so" di direktori "apktool_out/lib/arm64-v8a/". Juga alamat *email* "ftp@example.com" yang muncul dalam beberapa entri ke *file* "libunity.so", baik pada direktori "apktool_out/lib/arm64-v8a/" dan "apktool_out/lib/armeabi-v7a/". Alamat *email* tersebut digunakan dalam pengembangan atau manajemen proyek.

4.4 ANALISIS DINAMIS

Analisis dinamis dilakukan saat aplikasi *game* dijalankan dan mulai direkam *traffic*nya pada perangkat Android menggunakan aplikasi PCAPDroid. Hasil rekaman PCAPDroid merupakan *file* .pcap yang kemudian dibaca menggunakan *tools* Cloudshark. Adapun hasil analisis dinamis digunakan untuk mengetahui IP sumber melakukan pertukaran data pada IP apa saja saat aplikasi *game* dijalankan.

Sebelum melakukan analisis dinamis pada aplikasi, dilakukan perekaman pada perangkat yang akan digunakan sebelum aplikasi dipasang dan dijalankan. Berikut hasil analisis dinamis perangkat Android Samsung, ditunjukkan pada Tabel 4.16 :

Tabel 4.15 Analisis Dinamis Perangkat Android Samsung

Protokol	IP Sumber	IP Tujuan	Port Tujuan	Total Data
UDP		10.215.173.2	53	1.4 KB
		74.125.24.94		11.8 KB

Protokol	IP Sumber	IP Tujuan	Port Tujuan	Total Data
TCP	10.215.173.1	142.251.175.95	443	1.7 MB
		18.172.170.37		11.9 KB
		172.217.194.188		3.5 KB
		142.251.10.188	5228	6.3 KB

Berdasarkan hasil analisis dinamis pada perangkat Android Samsung ditunjukkan pada Tabel 4.16, ditemukan bahwa, IP sumber utama adalah 10.215.173.1 dengan port yang bervariasi. Seperti ditunjukkan pada Gambar 4.73, protokol UDP memiliki komunikasi menuju IP 10.215.173.2 dengan port 53 dan protokol TCP dengan sumber IP yang sama mengirimkan data ke berbagai IP tujuan pada port 443 dan 5228.

Viewing 6 ip Conversations for PCAPdroid_Sebelum.pcap

Clicking on a row will apply a *Display Filter* for that conversation.

Node A	Node B	Total Frames	Total Data	Frames A → B	Data A → B	Frames B → A	Data B → A
10.215.173.1	10.215.173.2	10	1.4 KB	5	568 B	5	872 B
10.215.173.1	74.125.24.94	19	11.8 KB	10	5.2 KB	9	6.7 KB
10.215.173.1	172.217.194.188	19	3.5 KB	10	1.9 KB	9	1.6 KB
10.215.173.1	142.251.175.95	494	1.7 MB	235	61.6 KB	259	1.7 MB
10.215.173.1	18.172.170.37	17	11.9 KB	9	5.8 KB	8	6.1 KB
10.215.173.1	142.251.10.188	31	6.3 KB	17	3.4 KB	14	2.9 KB

Gambar 4.73 Komunikasi Protokol Perangkat Android I

Hasil analisis dinamis perangkat Android I, ditunjukkan pada Tabel 4.17 :

Tabel 4.16 Analisis Dinamis Perangkat Android Xiaomi

Protokol	IP Sumber	IP Tujuan	Port Tujuan	Total Data
UDP	10.215.173.1	10.215.173.2	53	2 KB
		64.233.170.95	443	164.7 KB
	192.168.1.16	142.251.12.102		21.7 KB
		161.117.185.166		2.6 KB
		142.251.10.94		6.7 KB

Protokol	IP Sumber	IP Tujuan	Port Tujuan	Total Data
TCP	10.215.173.1	142.251.12.94		1.8 KB
		142.251.12.95		3.1 KB
		142.251.10.188	5228	13 KB
		142.251.10.139	80	660 B

Berdasarkan hasil analisis dinamis pada perangkat Android Xiaomi ditunjukkan pada Tabel 4.17, ditemukan bahwa, IP sumber utama adalah 10.215.173.1 dan 192.168.1.16 dengan port yang bervariasi. Seperti ditunjukkan pada Gambar 4.74, protokol UDP memiliki komunikasi menuju IP 10.215.173.2 dan 64.233.170.95 dengan port 53 dan 433. Sementara pada protokol TCP dengan sumber IP yang sama, mengirimkan data ke berbagai IP tujuan pada port 443, 5228 dan 80.

Viewing 9 ip Conversations for PCAPdroid_Sebelum Mod.pcap

Clicking on a row will apply a *Display Filter* for that conversation.

Node A	Node B	Total Frames	Total Data	Frames A → B	Data A → B	Frames B → A	Data B → A
10.215.173.1	10.215.173.2	18	2 KB	9	626 B	9	1.4 KB
192.168.1.16	142.251.12.102	127	21.7 KB	61	9.7 KB	66	12 KB
10.215.173.1	161.117.185.166	24	2.6 KB	12	1.8 KB	12	838 B
10.215.173.1	142.251.10.139	8	660 B	4	365 B	4	295 B
10.215.173.1	142.251.10.94	50	6.7 KB	26	3.9 KB	24	2.7 KB
10.215.173.1	142.251.10.188	86	13 KB	43	7 KB	43	6 KB
10.215.173.1	64.233.170.95	463	164.7 KB	232	128.9 KB	231	35.8 KB
10.215.173.1	142.251.12.95	15	3.1 KB	8	1.4 KB	7	1.6 KB
10.215.173.1	142.251.12.94	15	1.8 KB	8	1.1 KB	7	663 B

Gambar 4.74 Komunikasi Protokol Perangkat Android II

Setelah kedua perangkat di analisis, berikutnya dilakukan analisis dinamis pada aplikasi *game* versi asli dan mod di masing-masing perangkat. "Data Dikirim" adalah jumlah data yang dikirim dari IP sumber ke IP tujuan, dan "Data Diterima" adalah jumlah data yang diterima oleh IP sumber dari IP tujuan. Perbandingan hasil analisis dinamis pada versi asli dan modifikasi diuraikan sebagai berikut :

1. Zombie Tsunami

Berikut adalah tabel persamaan hasil analisis dinamis *packet analysis* pada aplikasi *game* Zombie Tsunami yang ditunjukkan pada Tabel 4.18:

Tabel 4.17 Analisis Dinamis Persamaan Aplikasi *Game* Zombie Tsunami

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
1.	10.215.173.2	5.9 KB	8 KB	1.7 KB	3 KB
2.	34.110.229.214	3.5 KB	20 KB	3.6 KB	20.7 KB
3.	34.117.147.68	13.1 KB	15.9 KB	12.8 KB	14.6 KB
4.	34.102.162.219	250.8 KB	1.5 MB	206.8 KB	1 MB
5.	35.244.205.3	3.4 KB	5 KB	2.6 KB	4.2 KB
6.	8.214.40.93	1.4 KB	544 B	1.2 KB	257 B
7.	142.251.175.95	2.3 KB	7 KB	3.8 KB	11.9 KB
8.	34.120.175.182	2.2 KB	19.3 KB	1.2 KB	18.5 KB
9.	34.36.171.56	2.9 KB	69.9 KB	3.8 KB	136.2 KB
10.	34.160.119.165	6.4 KB	207.9 KB	2.4 KB	144.3 KB
11.	34.149.87.163	149.5 KB	7.6 MB	63.3 KB	10.2 MB
	Total	**0.44 MB**	**9.45 MB**	**0.3 MB**	**11.87 MB**

Berdasarkan Tabel 4.18, terdapat 11 IP tujuan yang sama namun memiliki perbedaan pada data yang dikirim dan diterima. Terutama pada IP 34.149.87.163 yang mengalami peningkatan pengiriman data pada IP Sumber sebanyak 10.2 MB di versi mod. Selain itu meskipun

memiliki IP yang sama, namun total data yang diterima oleh IP sumber dari IP tujuan lebih banyak di versi mod.

Tabel 4.18 Analisis Dinamis Perbedaan Aplikasi *Game* Zombie Tsunami

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
1.	18.64.18.25	14.5 KB	508 KB	13.213.170.7	4.8 KB	12.1 KB
2.	142.251.175.94	16.7 KB	232.8 KB	185.151.204.7	2.6 KB	4.4 KB
3.	142.251.10.154	22.2 KB	169.2 KB	82.145.213.8	3.5 KB	8 KB
4.	192.229.145.170	11.8 KB	35.3 KB	142.251.223.52	1 KB	1.2 KB
5.	142.251.175.132	10.4 KB	69 KB	34.49.168.197	8.4 KB	4.2 KB
6.	142.250.189.163	14.6 KB	20.5 KB	18.161.49.122	1.3 KB	46.4 KB
7.	185.151.204.14	12.9 KB	16.8 KB	34.117.123.243	3 KB	5.2 KB
8.	157.240.208.16	7.8 KB	21.6 KB	18.67.175.111	33.2 KB	4.8 MB
9.	34.110.179.88	43.8 KB	24.2 KB	34.110.184.100	33.1 KB	9.4 KB
10.	142.251.10.157	5.6 KB	46.4 KB	18.64.18.115	3.8 KB	499.9 KB
11.	18.161.49.29	3.7 KB	48.1 KB	142.251.223.20	589 B	432 B
12.	47.241.91.242	6.9 KB	10.5 KB	18.154.7.55	1.3 KB	32.2 KB
13.	142.250.4.155	4.3 KB	46.1 KB	-	-	-

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
14.	74.125.130.94	4.3 KB	47.2 KB	-	-	-
15.	157.240.208.35	11.5 KB	18.4 KB	-	-	-
16.	74.125.24.94	4.4 KB	13.6 KB	-	-	-
17.	74.125.24.95	3.6 KB	15.6 KB	-	-	-
18.	64.233.170.156	3.7 KB	14.4 KB	-	-	-
19.	18.154.7.52	2.9 KB	10.4 KB	-	-	-
20.	18.64.37.45	2.3 KB	11.9 KB	-	-	-
21.	74.125.68.132	2.7 KB	21.1 KB	-	-	-
22.	106.10.248.147	5.6 KB	5.5 KB	-	-	-
23.	172.253.118.95	2.5 KB	6.8 KB	-	-	-
24.	210.210.145.10	2.7 KB	5.4 KB	-	-	-
25.	142.251.10.95	2.8 KB	6.6 KB	-	-	-
26.	142.251.221.116	848 B	924 B	-	-	-
27.	142.251.221.148	828 B	672 B	-	-	-
28.	34.101.5.52	760 B	836 B	-	-	-
	Total	**0.23 MB**	**1.43 MB**		**0.1 MB**	**5.02 MB**

Berdasarkan Tabel 4.19, versi *game* mod memiliki 12 IP yang tidak ada pada versi asli. Sementara versi asli terdapat 28 IP yang tidak ada di

versi mod. Hal tersebut menunjukkan, lebih banyak IP yang dihubungi oleh versi asli.

Selain itu, meskipun IP pada versi asli lebih banyak, namun total data yang diterima oleh IP sumber dari IP tujuan versi mod lebih besar yaitu sebanyak 5.02 MB. Sehingga dapat disimpulkan bahwa terjadi peningkatan penerimaan data pada versi mod dari IP sumber ke IP tujuan.

2. Adorable Home

Berikut adalah perbandingan hasil analisis dinamis *packet analysis* pada aplikasi *game* Adorable Home yang ditunjukkan pada Tabel 4.20:

Tabel 4.19 Analisis Dinamis Persamaan Aplikasi *Game* Adorable Home

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
1.	10.215.173.2	11.4 KB	19.4 KB	6.9 KB	14.6 KB
2.	34.111.113.40	4.6 KB	13 KB	1.7 KB	6 KB
3.	34.107.172.168	20 KB	21.6 KB	12.2 KB	17.6 KB
4.	18.64.18.46	5.5 KB	103.1 KB	3 KB	101.3 KB
5.	157.240.208.35	11.7 KB	18.6 KB	11.5 KB	17.2 KB
6.	18.64.37.125	22.7 KB	43.7 KB	13.5 KB	26.1 KB
7.	18.154.3.181	30.2 KB	666.2 KB	19 KB	667.2 KB
8.	34.110.229.214	3.8 KB	21.5 KB	2.7 KB	20.8 KB
9.	64.233.170.156	18.6 KB	162.4 KB	17.3 KB	323.4 KB
10.	192.229.145.170	19.2 KB	86.4 KB	6.2 KB	31.7 KB
11.	71.18.36.225	7.9 KB	19.2 KB	2.1 KB	10.9 KB

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
12.	35.244.205.3	3.5 KB	5 KB	2.6 KB	4.3 KB
13.	34.102.162.219	4.1 KB	8.7 KB	29.7 KB	37.2 KB
14.	34.110.179.88	4.9 KB	7.3 KB	10.8 KB	19.3 KB
15.	34.117.147.68	126 KB	93 KB	165.5 KB	162.6 KB
16.	34.120.175.182	3.6 KB	105.6 KB	1.3 KB	18.3 KB
17.	18.64.18.9	2.3 KB	7.2 KB	1.4 KB	6.7 KB
18.	18.64.18.114	2 KB	7.2 KB	1.1 KB	6.7 KB
19.	34.36.171.56	3.8 KB	70.9 KB	4 KB	149.5 KB
20.	47.90.201.72	2.3 KB	5.2 KB	1.5 KB	4.6 KB
21.	34.117.121.219	3.7 KB	11.6 KB	2 KB	10.1 KB
22.	35.186.249.41	4.2 KB	12.5 KB	4.3 KB	16.6 KB
23.	18.161.49.46	5.2 KB	7.3 KB	8.7 KB	7.4 KB
24.	108.138.141.74	28.5 KB	281.5 KB	27.5 KB	121.2 KB
25.	18.64.18.39	2.3 KB	7.2 KB	3.1 KB	7.6 KB
26.	18.64.18.107	2 KB	7.3 KB	1.1 KB	6.6 KB
27.	47.253.58.208	2.3 KB	5.3 KB	1.2 KB	4.6 KB
	Total	**0.35 MB**	**1.81 MB**	**0.36 MB**	**1.82 MB**

Berdasarkan Tabel 4.20, terdapat 27 IP tujuan yang sama namun memiliki perbedaan pada data yang dikirim dan diterima. Terutama pada IP 64.233.170.156 yang mengalami peningkatan pengiriman data pada IP Sumber sebanyak 323.4 KB di versi mod. Selain itu, meskipun

memiliki IP yang sama, namun total data yang diterima oleh IP sumber dari IP tujuan lebih banyak di versi mod.

Tabel 4.20 Analisis Dinamis Perbedaan Aplikasi *Game* Adorable Home

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
1.	216.239.35.4	248 B	248 B	52.27.146.183	1.5 KB	10.9 KB
2.	52.11.53.83	2.6 KB	11.9 KB	18.64.72.183	11.7 KB	465.9 KB
3.	18.67.171.42	77.7 KB	2.5 MB	44.198.68.153	15 KB	15.2 KB
4.	34.192.73.80	10.1 KB	20.5 KB	23.48.173.130	9 KB	19.4 KB
5.	210.210.145.11	13.7 KB	24.5 KB	74.125.130.102	1.5 KB	9.4 KB
6.	74.125.24.113	2.3 KB	10.4 KB	216.239.35.8	76 B	76 B
7.	103.17.182.30	124 B	124 B	74.125.130.95	1.5 KB	6 KB
8.	54.152.124.48	3.3 KB	7.4 KB	114.30.89.30	76 B	76 B
9.	74.125.68.95	2.3 KB	6.8 KB	52.23.29.76	2.4 KB	6.9 KB
10.	108.138.246.30	50.9 KB	46.4 KB	18.172.185.84	31.7 KB	26.8 KB
11.	18.154.7.64	2.9 KB	10.5 KB	8.214.25.108	2 KB	4.7 KB
12.	8.214.105.110	3.4 KB	5.5 KB	18.154.7.21	1.8 KB	9.7 KB
13.	18.173.121.107	9.5 KB	16.2 KB	54.157.113.44	5.1 KB	12.4 KB
14.	52.21.220.164	4.2 KB	7 KB	54.161.184.242	2.8 KB	5.9 KB
15.	18.64.37.125	22.7 KB	43.7 KB	18.154.7.22	1.5 KB	46.4 KB
16.	18.154.3.181	30.2 KB	666.2 KB	18.154.7.84	996 B	11 KB
17.	52.6.161.167	3.8 KB	6.4 KB	44.209.167.75	2 KB	7 KB
18.	44.214.202.168	4.9 KB	14.2 KB	210.210.145.179	3.9 KB	9.8 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	Data Dikirim	Data Diterima	IP Tujuan	Data Dikirim	Data Diterima
19.	18.161.49.121	3 KB	47.4 KB	23.48.173.66	8.6 KB	906 KB
20.	18.64.37.95	1.9 KB	11.4 KB	151.101.2.137	3.1 KB	78.8 KB
21.	23.214.169.139	8.7 KB	424.7 KB	18.64.18.89	4 KB	501.4 KB
22.	23.214.169.217	2.6 KB	5.6 KB	210.210.145.178	1.1 KB	6.5 KB
23.	151.101.66.137	4.9 KB	80 KB	35.174.217.241	2.6 KB	11.2 KB
24.	210.210.145.154	1.8 KB	28.3 KB	210.210.145.144	938 B	27.4 KB
25.	107.22.67.141	2.5 KB	6.4 KB	18.67.175.104	15.7 KB	816 KB
26.	18.64.18.25	12.9 KB	507.1 KB	71.18.36.248	4 KB	6.6 KB
27.	18.67.175.36	28.7 KB	825.4 KB	3.163.165.49	4.3 KB	13.3 KB
28.	210.210.145.147	2 KB	7.3 KB	34.117.123.243	3 KB	5.1 KB
29.	108.138.141.13	25.8 KB	344.2 KB	18.67.175.66	34.7 KB	8.7 MB
30.	210.210.145.177	3.2 KB	6 KB	18.154.7.47	1.6 KB	62.1 KB
31.	142.251.175.156	4 KB	41.8 KB	104.17.1.3	3.9 KB	7 KB
32.	74.125.68.132	8.6 KB	50.2 KB	142.250.75.227	30 KB	31.2 KB
33.	142.251.12.157	2.9 KB	39.9 KB	34.107.157.36	19.4 KB	35.2 KB
34.	74.125.130.94	15.3 KB	116 KB	210.210.145.139	8.7 KB	780.5 KB
35.	142.251.171.94	5.3 KB	14.9 KB	47.252.36.89	1.2 KB	4.6 KB
36.	23.48.173.9	6.9 KB	12 KB	44.208.111.72	1.4 KB	5.6 KB
37.	34.49.190.208	3.5 KB	78.5 KB	108.138.94.10	11.7 KB	9 KB
38.	142.251.175.119	1.9 KB	10.6 KB	18.64.18.74	1.5 KB	863 B

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
39.	23.48.173.139	3.6 KB	88.7 KB	34.228.138.100	1.4 KB	5.6 KB
40.	23.48.173.155	15.6 KB	709 KB	18.64.18.119	1.3 KB	768 B
41.	35.244.136.26	2.5 KB	8.2 KB	23.48.173.65	3.1 KB	6 KB
42.	34.160.136.185	6.7 KB	7.6 KB	82.145.213.8	25.7 KB	22 KB
43.	18.161.49.91	4.9 KB	7 KB	108.138.94.120	31.9 KB	14.9 KB
44.	108.138.246.11	3.1 KB	7.2 KB	52.220.206.13	33.9 KB	8.7 KB
45.	18.64.37.47	3.4 KB	7.8 KB	108.138.141.26	22.9 KB	40.2 KB
46.	35.190.78.8	9.6 KB	10 KB	52.77.92.190	18.8 KB	8.1 KB
47.	54.147.64.227	5.6 KB	7.3 KB	18.161.49.39	4.5 KB	6.7 KB
48.	23,214,169,163	2.7 KB	2.5 KB	18.64.37.37	7.4 KB	9.7 KB
49.	34.232.74.211	2.8 KB	1.7 KB	18.64.37.32	6.8 KB	3.5 KB
	Total	**0.4 MB**	**6.21 MB**		**0.41 MB**	**12.95 MB**

Berdasarkan Tabel 4.21, versi *game* mod dan *game* asli sama-sama memiliki 49 IP namun IP yang berbeda-beda. Selain itu meskipun memiliki jumlah yang sama, total data yang diterima oleh IP sumber dari IP tujuan pada versi mod lebih besar yaitu sebanyak 14.77 MB. Sehingga dapat disimpulkan bahwa terjadi peningkatan penerimaan data pada versi mod dari IP sumber ke IP tujuan.

3. Brain Out

Berikut adalah perbandingan hasil analisis dinamis *packet analysis* pada aplikasi *game* Brain Out yang ditunjukkan pada Tabel 4.22:

Tabel 4.21 Analisis Dinamis Persamaan Aplikasi *Game* Brain Out

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
1.	10.215.173.2	14.5 KB	21.1 KB	6.8 KB	13.1 KB
2.	157.240.208.16	8.6 KB	20.5 KB	12.2 KB	37.3 KB
3.	101.33.5.83	18.1 KB	565 KB	1 KB	7.3 KB
4.	34.102.162.219	1.1 MB	4.9 MB	266.3 KB	1.8 MB
5.	34.110.179.88	5.5 KB	7.2 KB	69.7 KB	27.7 KB
6.	34.117.147.68	21.2 KB	22.1 KB	14.2 KB	11 KB
7.	192.229.145.170	11.7 KB	29.3 KB	9.1 KB	72.2 KB
8.	34.110.229.214	4.2 KB	19.4 KB	2.8 KB	19.1 KB
9.	71.18.36.248	6.7 KB	19.8 KB	2.1 KB	17.1 KB
10.	17.253.60.253	124 B	124 B	76 B	76 B
11.	203.107.6.88	124 B	124 B	76 B	76 B
12.	8.222.217.87	1.9 KB	5.9 KB	2 KB	9.7 KB
13.	8.222.205.177	31.1 KB	37.7 KB	21.4 KB	29.8 KB
14.	172.217.194.132	4.8 KB	22.6 KB	7.3 KB	60.9 KB
15.	34.160.119.165	26.6 KB	770.1 KB	3.5 KB	243.6 KB
16.	34.149.87.163	88.5 KB	11 MB	36.6 KB	5 MB
17.	8.219.120.154	18.8 KB	22.5 KB	51.9 KB	72.2 KB

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
18.	74.125.130.94	3.5 KB	3.8 KB	3.1 KB	7.3 KB
19.	34.120.33.51	3.3 KB	6.3 KB	23.7 KB	11.3 KB
20.	74.125.200.154	25.7 KB	26.1 KB	51.9 KB	72.2 KB
	TOTAL	**1.39 MB**	**17.49 MB**	**0.54 MB**	**7.46 MB**

Berdasarkan Tabel 4.22, terdapat 20 IP tujuan yang sama namun memiliki perbedaan pada data yang dikirim dan diterima. Terutama pada IP 34.149.87.16 yang mengalami peningkatan pengiriman data pada IP Sumber sebanyak 11 MB di versi asli. Selain itu, data pada versi asli lebih banyak daripada versi mod.

Tabel 4.22 Analisis Dinamis Perbedaan Aplikasi *Game* Brain Out

No.	Versi Asli			Versi Mod		
	IP Tujuan	Data Dikirim	Data Diterima	IP Tujuan	Data Dikirim	Data Diterima
1.	172.217.194.95	6.1 KB	13.3 KB	74.125.200.94	1.6 KB	5.9 KB
2.	47.241.234.26	4.8 KB	1.7 KB	64.233.170.95	1.5 KB	6 KB
3.	13.227.254.57	3.5 KB	39.1 KB	43.152.160.176	3 KB	38.8 KB
4.	139.193.253.154	44.1 KB	3.4 MB	225.0.0.222	69.3 KB	0 B
5.	44.209.119.141	3.9 KB	8.1 KB	74.125.200.95	4.2 KB	24.5 KB
6.	142.251.175.155	21.9 KB	36.3 KB	47.246.109.108	4 KB	9.8 KB
7.	18.64.27.189	4.6 KB	25.9 KB	47.74.186.101	898 B	4.7 KB
8.	54.230.112.66	3.5 KB	7.3 KB	157.240.208.35	9.6 KB	17.3 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
9.	139.193.253.18	2.1 KB	7.5 KB	74.125.200.156	49 KB	174.8 KB
10.	23.23.224.14	7.2 KB	8 KB	18.67.175.56	2 KB	37.6 KB
11.	18.161.97.99	3.2 KB	7.4 KB	8.214.25.108	6.3 KB	13.9 KB
12.	34.128.182.103	71.8 KB	30.2 KB	18.154.7.29	8.8 KB	37.7 KB
13.	104.18.33.123	191.3 KB	24.2 MB	23.48.173.129	4.3 KB	425 KB
14.	139.193.253.147	4.6 KB	45.6 KB	18.209.125.252	1.9 KB	7.2 KB
15.	139.193.253.19	8.1 KB	58.8 KB	18.154.7.11	1.2 KB	11.2 KB
16.	139.193.253.10	1.6 KB	4.3 KB	18.154.7.82	1.4 KB	46.4 KB
17.	64.233.170.119	4.5 KB	20.3 KB	210.210.145.147	1.1 KB	6.7 KB
18.	139.193.253.145	2.5 KB	59.9 KB	18.172.185.59	2.1 KB	6.7 KB
19.	44.214.34.138	17.2 KB	15.2 KB	18.154.3.181	19.9 KB	625.1 KB
20.	23.215.35.16	4.9 KB	5.2 KB	18.64.18.89	4.3 KB	504.6 KB
21.	142.251.12.154	68.4 KB	69.7 KB	210.210.145.144	1.1 KB	27.5 KB
22.	172.253.118.154	2.6 KB	6.8 KB	44.208.111.72	1.4 KB	5.8 KB
23.	74.125.24.94	4.9 KB	9.6 KB	151.101.194.137	2.8 KB	78.8 KB
24.	142.251.12.95	2.6 KB	9.5 KB	18.172.185.103	4.4 KB	13.3 KB
25.	172,253,118,156	25.8 KB	26.1 KB	210.210.145.171	3.1 KB	6.1 KB
26.	185.151.204.7	110.5 KB	108.6 KB	35.244.205.3	2.6 KB	4.3 KB
27.	8.214.40.93	7.2 KB	2.7 KB	18.64.18.79	7.1 KB	18 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	Data Dikirim	Data Diterima	IP Tujuan	Data Dikirim	Data Diterima
28.	107.178.244.18	9.7 KB	26.6 KB	35.244.136.26	12.1 KB	13.9 KB
29.	142.251.175.154	54 KB	47 KB	34.120.175.182	1.2 KB	18.3 KB
30.	23.215.35.12	15.5 KB	14 KB	74.125.130.154	12.9 KB	59 KB
31.	18.154.7.14	5.1 KB	8.3 KB	172.253.118.94	22.3 KB	360.7 KB
32.	3.219.165.53	11.7 KB	25.4 KB	74.125.68.95	5.8 KB	19.6 KB
33.	34.102.164.161	7 KB	7.8 KB	172.217.194.94	6.3 KB	33.9 KB
34.	23.215.35.13	4 KB	2.8 KB	172.253.118.132	13.7 KB	93 KB
35.	54.230.112.118	2.8 KB	7.2 KB	142.250.217.195	63.2 KB	37.9 KB
36.	34.200.158.177	4.2 KB	6.4 KB	74.125.68.157	9.3 KB	49.9 KB
37.	8.214.59.91	4.4 KB	1.6 KB	202.158.60.144	6 KB	455.1 KB
38.	43.159.65.66	8.3 KB	153.9 KB	3.1.216.96	2.2 KB	1.5 KB
39.	172.253.118.157	6.9 KB	78.8 KB	34.144.225.12	2.4 KB	16.1 KB
40.	185.151.204.51	5.1 KB	11.2 KB	108.138.141.69	2.9 KB	291.5 KB
41.	34.111.241.145	9.6 KB	14.8 KB	18.244.51.63	974 B	8.2 KB
42.	103.132.192.30	7.2 KB	48.9 KB	18.154.7.22	6.9 KB	687.3 KB
43.	79.127.235.3	16.1 KB	228.3 KB	18.161.49.120	14 KB	1.6 MB
44.	47.246.158.105	2.8 KB	8 KB	185.151.204.9	16.1 KB	23.3 KB
45.	139.193.253.8	2.4 KB	57.5 KB	74.125.130.157	7.2 KB	10.4 KB
46.	74.125.200.157	5.4 KB	5.2 KB	202.158.59.205	16.6 KB	2.3 MB
47.	54.209.139.254	4.1 KB	12.4 KB	3.163.165.49	3.5 KB	13.1 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
48.	3.160.188.122	2.5 KB	7 KB	172.217.194.157	8.5 KB	15 KB
49.	-	-	-	216.58.201.99	25 KB	30.6 KB
50.	-	-	-	202.158.59.18	55.5 KB	1.3 MB
51.	-	-	-	74.125.130.132	3.5 KB	5.9 KB
52.	-	-	-	108.138.94.24	1.7 KB	6.6 KB
53.	-	-	-	74.125.200.94	1.6 KB	5.9 KB
	Total	**0.82 MB**	**27.01 MB**		**0.54 MB**	**9.61 MB**

Berdasarkan Tabel 4.23, perbedaan terletak pada jumlah IP tujuan pada versi asli yang tidak terdapat pada versi mod. Selain itu pada versi asli, total data yang diterima oleh IP sumber dari IP tujuan juga lebih besar yaitu sebanyak 27.01 MB. Sehingga dapat disimpulkan bahwa pada versi asli IP sumber lebih banyak menerima data dari IP tujuan.

4. Subway Surfers

Berikut adalah perbandingan hasil analisis dinamis *packet analysis* pada aplikasi *game* Subway Surfers yang ditunjukkan pada Tabel 4.24:

Tabel 4.23 Analisis Dinamis Persamaan *Game* Subway Surfers

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	**Data Diterima**	**Data Dikirim**	**Data Diterima**
1.	10.215.173.2	12.4 KB	19.5 KB	5.8 KB	12.7 KB

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	Data Diterima	Data Dikirim	Data Diterima
2.	104.18.42.2	47.7 KB	697.5 KB	3.8 KB	47.7 KB
3.	172.64.145.254	160.9 KB	1.7 MB	178.6 KB	53.3 KB
4.	18.67.175.53	5 KB	14.8 KB	1.5 KB	7.1 KB
5.	108.138.141.74	22.5 KB	328.2 KB	8.6 KB	44.8 KB
6.	34.102.162.219	4.1 KB	9.2 KB	3.1 KB	8.4 KB
7.	34.110.179.88	4.8 KB	7.3 KB	4.3 KB	6.4 KB
8.	34.117.147.68	82.1 KB	60 KB	79.2 KB	51.2 KB
9.	34.110.229.214	4.4 KB	21.1 KB	3.7 KB	19.6 KB
10.	34.117.123.243	13.8 KB	17.5 KB	17.9 KB	16.5 KB
11.	34.49.168.197	11.1 KB	5.2 KB	66.3 KB	15.4 KB
12.	18.64.18.119	3.9 KB	14.4 KB	4.9 KB	15.2 KB
13.	18.161.49.39	5.5 KB	7.2 KB	12.2 KB	8.1 KB
14.	18.67.175.78	2.7 KB	7.5 KB	5.5 KB	6.6 KB
15.	18.64.18.47	9.4 KB	29 KB	9.5 KB	11.1 KB
16.	18.161.49.46	10.7 KB	14.4 KB	4.3 KB	6.7 KB
17.	18.64.18.91	2 KB	7.2 KB	3.4 KB	2.4 KB
18.	18.67.175.74	6.2 KB	14.4 KB	1.8 KB	6.7 KB
19.	152.199.39.108	17.3 KB	218.5 KB	8.4 KB	21.4 KB
	TOTAL	**0.42 MB**	**3.19 MB**	**0.42 MB**	**0.36 MB**

Berdasarkan Tabel 4.24, terdapat 19 IP tujuan yang sama namun memiliki perbedaan pada data yang dikirim dan diterima. Terutama pada IP 172.64.145.254 yang mengalami peningkatan pengiriman data pada IP Sumber sebanyak 1.7 MB di versi asli. Selain itu, persamaan terletak pada jumlah data yang dikirim oleh IP sumber ke IP tujuan, namun total data yang diterima oleh IP sumber dari IP tujuan lebih banyak di versi asli.

Tabel 4.24 Analisis Dinamis Perbedaan Aplikasi *Game* Subway Surfers

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
1.	142.251.12.94	4.5 KB	13.6 KB	57.144.100.141	5.4 KB	18.6 KB
2.	74.125.24.95	2.2 KB	6.9 KB	139.193.253.32	6.3 KB	7.3 KB
3.	157.240.208.16	8 KB	20.7 KB	18.154.7.66	2.9 KB	62 KB
4.	54.147.66.51	2.5 KB	6 KB	54.230.112.66	25 KB	24.4 KB
5.	104.21.57.97	1.4 KB	6.2 KB	142.251.175.95	2.1 KB	5.8 KB
6.	210.210.145.16	14.2 KB	21.1 KB	18.64.27.189	6.8 KB	76.1 KB
7.	18.64.18.117	4.5 KB	68.1 KB	116.202.170.95	2.1 KB	6 KB
8.	18.244.214.84	21.2 KB	31 KB	142.251.12.156	15.3 KB	64 KB
9.	157.240.208.35	11.3 KB	18.2 KB	107.22.67.141	2.4 KB	7.3 KB
10.	142.251.10.156	37.4 KB	186.6 KB	3.160.196.49	3.4 KB	13.1 KB
11.	3.229.141.229	3.1 KB	8.1 KB	172.212.5.164	1.8 KB	4.6 KB
12.	18.154.3.181	28.4 KB	653.8 KB	34.232.246.224	2.6 KB	6 KB
13.	116.202.170.42	2.8 KB	6.6 KB	34.128.18.103	9.5 KB	4.3 KB
14.	151.101.194.137	5.1 KB	80.4 KB	192.229.145.170	7.6 KB	30 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	Data Dikirim	Data Diterima	IP Tujuan	Data Dikirim	Data Diterima
15.	108.138.141.69	22.1 KB	644.5 KB	35.244.136.26	25.4 KB	45.7 KB
16.	18.155.192.41	2.9 KB	7.2 KB	108.138.141.26	61.4 KB	363.3 KB
17.	20.39.59.188	7.6 KB	23.1 KB	57.152.71.188	18.5 KB	18.8 KB
18.	210.210.145.11	12.9 KB	20.6 KB	172.212.5.212	7.3 KB	62.7 KB
19.	210.210.145.154	2.1 KB	28.6 KB	34.197.152.180	7.2 KB	22.4 KB
20.	34.230.201.123	2.4 KB	6.3 KB	18.64.18.9	3.8 KB	8 KB
21.	44.209.170.100	4.5 KB	12.2 KB	57.152.69.114	45.4 KB	43.2 KB
22.	18.64.18.115	11.9 KB	506.4 KB	74.125.68.157	17.5 KB	25 KB
23.	35.244.205.3	3.4 KB	5 KB	172.253.118.156	1.8 KB	6.3 KB
24.	74.125.24.94	9.9 KB	82.1 KB	54.230.112.88	2.5 KB	6.7 KB
25.	142.251.10.154	4.7 KB	43.4 KB	142.251.175.149	9.9 KB	14 KB
26.	74.125.130.132	5.1 KB	44.7 KB	139.193.253.146	6.5 KB	10.4 KB
27.	74.125.130.154	3 KB	39.6 KB	64.185.181.238	13.3 KB	1 MB
28.	34.36.171.56	4.9 KB	133.7 KB	184.51.117.145	26.8 KB	128.8 KB
29.	18.64.18.74	2.4 KB	7.4 KB	142.251.12.155	10.7 KB	28.1 KB
30.	172.217.167.99	6.2 KB	13.6 KB	34.149.85.72	5.1 KB	10.2 KB
31.	20.33.12.99	13.2 KB	15.2 KB	54.230.112.46	12.2 KB	3.1 KB
32.	20.39.59.149	14.4 KB	18.3 KB	152.69.173.77	1.7 KB	5.5 KB
33.	142.251.12.95	2.7 KB	6.5 KB	57.152.64.16	4.5 KB	9.1 KB
34.	142.251.175.154	4.3 KB	6.3 KB	108.138.141.127	46.6 KB	444.7 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	Data Dikirim	Data Diterima	IP Tujuan	Data Dikirim	Data Diterima
35.	13.228.193.104	17.3 KB	19.8 KB	52.202.58.174	2 KB	5.6 KB
36.	18.238.192.39	27.2 KB	13.6 KB	52.84.45.27	50.6 KB	11.2 KB
37.	108.138.141.13	46.2 KB	654 KB	18.64.37.65	55.4 KB	18.1 KB
38.	34,110,184,100	31.4 KB	10.8 KB	18.244.51.44	2.1 KB	40.9 KB
39.	52.74.244.47	3.1 KB	6.9 KB	172.64.154.133	2.1 KB	25 KB
40.	210.210.145.144	2.7 KB	115.5 KB	3.208.175.71	3.2 KB	12 KB
41.	23.48.173.130	7.7 KB	606.4 KB	139.193.253.138	2.3 KB	905 B
42.	82.145.213.8	10.6 KB	9.3 KB	139.193.253.27	12.9 KB	11.9 KB
43.	23.48.173.136	2.3 KB	93.1 KB	139.193.253.35	1.8 KB	13.1 KB
44.	18.64.37.116	18.9 KB	48.3 KB	54.221.252.175	3.9 KB	12.3 KB
45.	44.214.202.168	37.3 KB	54.2 KB	139.193.253.139	1.9 KB	31.9 KB
46.	23.48.173.11	14.4 KB	14.4 KB	18.64.18.114	1.2 KB	728 B
47.	18.64.37.113	7.1 KB	15.2 KB	52.222.144.104	2.1 KB	6.7 KB
48.	52.206.95.67	3.3 KB	6.1 KB	57.144.100.141	5.4 KB	18.6 KB
49.	3.226.220.231	3.2 KB	4.9 KB	139.193.253.32	6.3 KB	7.3 KB
50.	20.33.14.1	4.1 KB	20.1 KB	18.154.7.66	2.9 KB	62 KB
51.	20.33.12.30	14.6 KB	19.2 KB	54.230.112.66	25 KB	24.4 KB
52.	104.18.36.54	1.4 KB	6.1 KB	142.251.175.95	2.1 KB	5.8 KB
53.	18.238.192.93	10.4 KB	15.5 KB	18.64.27.189	6.8 KB	76.1 KB
54.	-	-	-	116.202.170.95	2.1 KB	6 KB

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
55.	-	-	-	142.251.12.156	15.3 KB	64 KB
	Total	**0.58 MB**	**7.53 MB**		**0.56 MB**	**2.78 MB**

Berdasarkan Tabel 4.25, perbedaan terletak pada jumlah IP tujuan pada versi asli yang tidak terdapat pada versi mod. Selain itu pada versi asli, total data yang diterima oleh IP sumber dari IP tujuan juga lebih besar yaitu sebanyak 7.53 MB. Sehingga dapat disimpulkan bahwa pada versi asli IP sumber lebih banyak menerima data dari IP tujuan.

5. Stickman Party

Berikut adalah perbandingan hasil analisis dinamis *packet analysis* pada aplikasi *game* Stickman Party yang ditunjukkan pada Tabel 4.26:

Tabel 4.25 Analisis Dinamis Persamaan Versi Asli *Game* Stickman Party

No.	IP Tujuan	Versi Asli		Versi Mod	
		Data Dikirim	**Data Diterima**	**Data Dikirim**	**Data Diterima**
1.	10.215.173.2	2.7 KB	4.6 KB	1.3 KB	3 KB
2.	34.111.113.40	2.5 KB	6.6 KB	1.6 KB	5.9 KB
3.	34.149.127.98	1.7 KB	5.9 KB	1.1 KB	5.4 KB
4.	34.107.172.168	16.9 KB	12.9 KB	14.8 KB	11.5 KB
5.	34.96.113.148	12.4 KB	23 KB	9.9 KB	21.1 KB
	TOTAL	**0.03 MB**	**0.05 MB**	**0.02 MB**	**0.04 MB**

Berdasarkan Tabel 4.26, terdapat 5 IP tujuan yang sama namun memiliki perbedaan pada data yang dikirim dan diterima. Terutama pada IP 34.96.113.148 yang mengalami peningkatan pengiriman data pada IP Sumber sebanyak 23 KB di versi asli. Namun, total data yang diterima lebih besar pada versi asli.

Tabel 4.26 Analisis Dinamis Perbedaan Aplikasi *Game* Stickman Party

No.	Versi Asli			Versi Mod		
	IP Tujuan	**Data Dikirim**	**Data Diterima**	**IP Tujuan**	**Data Dikirim**	**Data Diterima**
1.	216.239.35.8	124 B	124 B	216.239.35.4	76 B	76 B
2.	74.125.68.147	3.4 KB	20.8 KB	142.251.12.105	10.9 KB	59.7 KB
3.	172.253.118.154	780 B	928 B	142.251.12.103	400 B	352 B
4.	157.240.208.16	7.2 KB	19.9 KB	142.251.12.147	400 B	352 B
5.	104.18.42.2	10.8 KB	4.3 KB	142.251.12.99	825 B	3.2 KB
6.	-	-	-	142.251.12.104	300 B	264 B
7.	-	-	-	142.251.12.106	300 B	264 B
8.	-	-	-	74.125.24.103	1.6 KB	16.2 KB
9.	-	-	-	142.251.12.156	589 B	736 B
	TOTAL	**0.02 MB**	**0.05 MB**		**0.02 MB**	**0.16 MB**

Berdasarkan Tabel 4.27, perbedaan terletak pada jumlah IP tujuan pada versi asli yang tidak terdapat pada versi mod. Selain itu pada versi mod, total data yang diterima oleh IP sumber dari IP tujuan juga lebih besar yaitu sebanyak 0.16 MB. Sehingga dapat disimpulkan bahwa pada versi asli IP sumber lebih banyak menerima data dari IP tujuan.

4.5 IDENTIFIKASI KERENTANAN

Tahap ini merupakan proses pengumpulan hasil analisis data pada aplikasi *game* versi modifikasi yang telah didapatkan untuk diidentifikasi kerentanannya. Adapun kerentanan tersebut merupakan hasil perbedaan antara *game* modifikasi dan *game* asli. Kumpulan data tersebut diuraikan dalam Tabel 4.28 berikut :

Tabel 4.27 Identifikasi Kerentanan Aplikasi *Game* Modifikasi

	Zombie Tsunami	**Adorable Home**	**Brain Out**	**Subway Surfers**	**Stickman Party**
Metadata	Terjadi perubahan yang signifikan pada ukuran dan nama paket.	Terjadi sedikit perubahan pada ukuran dan nama paket.	Ukuran APK lebih kecil dan perubahan nama paket.	Terjadi sedikit perubahan pada ukuran dan nama paket.	Terjadi perubahan yang signifikan pada ukuran dan nama paket.
Karakteristik	Terjadi perubahan signifikan pada jumlah uang dalam *game*.	Terjadi perubahan signifikan pada jumlah uang dalam *game*.	Muncul *popup watermark* pengembang sumber aplikasi mod pada *loading screen,* tidak ada iklan, dan perubahan pada uang dalam *game*.	Muncul *popup watermark* pengembang sumber aplikasi mod pada *loading screen*. Dan perubahan pada uang dalam *game*.	Terjadi perubahan signifikan pada jumlah uang dalam *game*.
Analisis Statis	Adanya perubahan integritas data dan *email* mencurigakan yang tidak ada pada versi asli.	Adanya perubahan integritas data.	Adanya perubahan integritas data, perubahan *email* untuk distribusi *file*, dan penambahan *file* pada direktori.	Adanya perubahan integritas data.	Adanya perubahan integritas data dan *email* mencurigakan yang tidak ada pada versi asli.

	Zombie Tsunami	Adorable Home	Brain Out	Subway Surfers	Stickman Party
Analisis Dinamis	Data yang diterima IP sumber mengalami peningkatan meski data IP pada versi mod lebih sedikit daripada IP di versi asli.	Data yang diterima IP sumber versi mod mengalami peningkatan.	IP tujuan versi mod lebih banyak.	Data yang diterima IP sumber versi mod mengalami penurunan yang drastis.	Data yang diterima IP sumber versi mod mengalami peningkatan.

Berdasarkan Tabel 4.28, disimpulkan bahwa *game* modifikasi menunjukkan berbagai celah kerentanan dari segi perubahan dan perbedaan yang cukup signifikan pada ukuran *file*, nama paket, karakteristik dalam *game*, perubahan integritas data, serta perilaku jaringan. Perbedaan tersebut mengindikasikan bahwa aplikasi *game* modifikasi tidak memenuhi standar keamanan atau persyaratan platform seperti Google *Play Store*. Sehingga, berpotensi pada celah keamanan dan kerentanan pada eksploitasi oleh pihak ketiga.