BAB 4
HASIL PENELITIAN

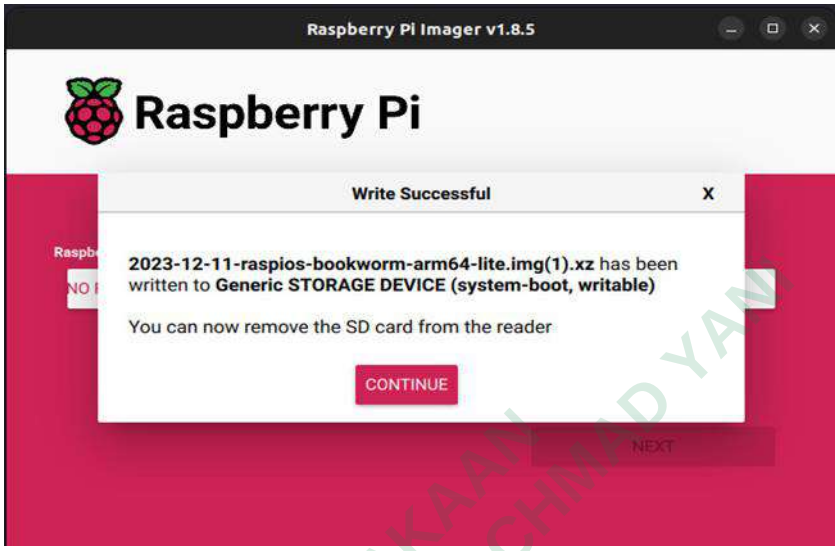
4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini memiliki sebuah tujuan untuk menggunakan AdGuardHome sebagai alternatif dalam mengurangi penyebaran malware yang berasal dari suatu hal yang diakses oleh lima ponsel Android "*China Brand*" tanpa intervensi pengguna. Sistem ini diimplementasikan pada perangkat Raspberry Pi 3 B. Penelitian akan berlangsung selama 24 jam untuk setiap 5 ponsel Android berbeda yang akan diujikan, dengan pengambilan data dari *query log* AdGuardHome dengan menggunakan CLI dan ekstrak dari file *query log* ke CSV selama lebih kurang 2 pekan, dimulai dari 6 Juni hingga 20 Juni 2024. Implementasi sistem dilakukan melalui serangkaian tahapan berikut.

4.2 INSTALASI SISTEM OPERASI RASPBERRY PI OS

Langkah awal dalam penelitian ini adalah menginstal sebuah *Operating System* (OS) pada Raspberry Pi 3 B. Untuk melakukan ini, penulis memerlukan Raspberry Pi Imager, sebuah perangkat lunak yang memfasilitasi unduhan dan instalasi OS, seperti yang ditampilkan dalam Gambar 4.1. Sistem operasi yang dipilih adalah versi lite (64-*bit*) karena fokus penelitian adalah pada penggunaan antarmuka atau *Command-Line Interface* (CLI). Sistem operasi dapat diunduh dari situs web resmi Raspberry Pi di https://www.raspberrypi.com/software/operating-systems/ . Proses instalasi OS melibatkan penggunaan SD Card yang disisipkan ke dalam pembaca kartu (*card reader*) untuk membantu proses *burning*. Proses ini biasanya memakan waktu lebih kurang 10 menit. Setelah proses *burning* selesai, SD Card dapat dilepaskan dari *card reader* dan dimasukkan ke dalam slot SD Card yang tersedia pada Raspberry Pi 3 B. Untuk melakukan konfigurasi awal dibutuhkan *hardware* tambahan, berupa kabel HDMI untuk menyambungkan Raspberry Pi dengan monitor, serta bantuan keyboard untuk mengoperasikan perangkat. Setelah Raspberry Pi 3 B dihidupkan, instruksi untuk melakukan

pengaturan awal akan muncul, termasuk pembuatan password, username, dan penyesuaian tata letak keyboard.

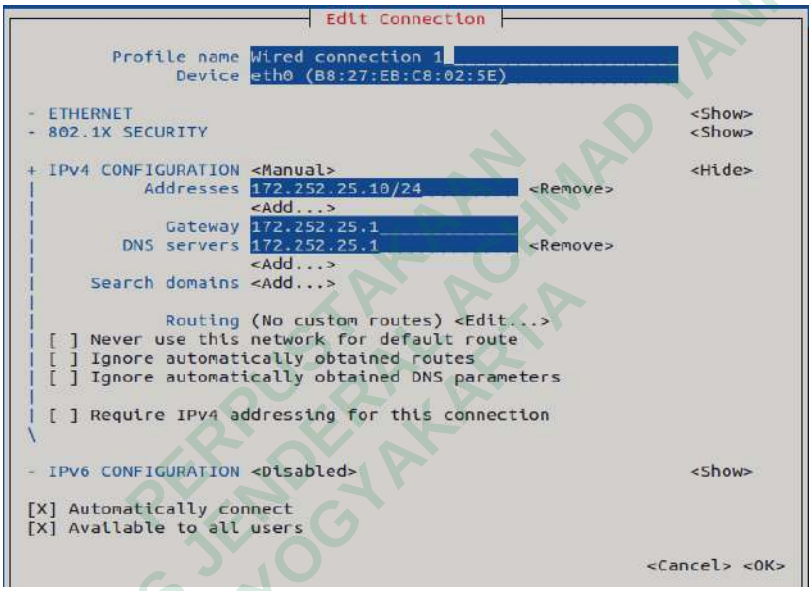


Gambar 4.1 Raspberry Pi Imager

Kemudian supaya perangkat dapat di *remote* yaitu dengan mengaktifkan protokol SSH pada Raspberry Pi 3 B. Langkah ini penting agar penulis dapat mengakses perangkat dari jarak jauh atau me-*remote* menggunakan pemanfaatan CLI tanpa harus berada di dekat Raspberry Pi 3 B secara fisik. Untuk mengaktifkan SSH, pengguna dapat menjalankan perintah "`raspi-config`" melalui terminal Raspberry Pi. Setelah perintah dimasukkan, akan muncul sebuah GUI (*Graphical User Interface*) yang menampilkan beberapa opsi. Di antara opsi-opsi tersebut, pilih "`Interfacing Options`". Selanjutnya, akan terdapat pilihan untuk SSH, yang kemudian dapat memilih untuk mengaktifkan SSH dengan memilih opsi "`enable SSH`". Langkah ini penting untuk memungkinkan akses ke terminal Raspberry Pi melalui SSH.

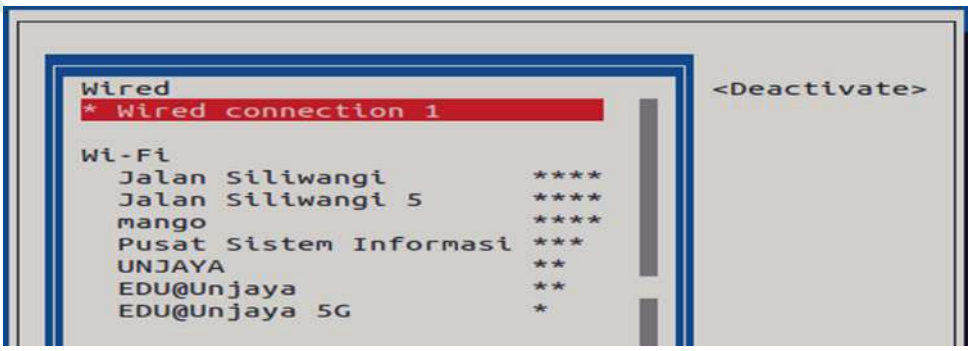
Secara umum, IP dari perangkat Raspberry Pi 3 B dapat berubah secara dinamis jika tidak diatur dalam mode statis. Hal ini terjadi karena perangkat menggunakan DHCP (*Dynamic Host Configuration Protokol*) secara bawaan dengan dampak dapat menyulitkan akses secara *remote* ke Raspberry Pi. Untuk mengatasi masalah ini dilakukan tindakan yaitu mengonfigurasi IP statis menggunakan bantuan nmtui (*Network Manager Text User Interface*) sebagai

pengelola koneksi jaringan. Untuk mengakses menggunakan perintah "`sudo nmtui`" maka akan muncul beberapa konfigurasi yang dapat dilakukan, diantara konfigurasi tersebut pilih *option* **"**`Edit a connection`**"** yang kemudian ubah dari hide ke show pada IPv4, lalu ubah *configuration* dari *Automatic* menjadi *Manual* supaya dapat dilakukannya pengaturan lanjutan, dengan membuat IP yaitu 172.252.25.10, dengan gateway 172.252.25.1 dan DNS Server 172.252.25.1 dengan men-*disable* IPv6 kemudian pilih OK**,** seperti pada Gambar 4.2.



Gambar 4.2 *Edit Connection nmtui*

Setelah selesai melakukan pengaturan pada *Edit Connection*, pilih "OK" dan lanjut melakukan konfigurasi pada *Activate a Connection* dengan kondisi *wired connection 1* dalam posisi <*Deactivate*> seperti pada Gambar 4.3.



Gambar 4.3 *Activate a Connection*

4.3 KONFIGURASI ADGUARDHOME PADA RASPBERRY PI 3 B

Setelah menyelesaikan pengaturan menggunakan *Graphical User Interface* (GUI) pada Raspberry Pi, perangkat Raspberry Pi 3 B dapat diakses dan menerima perintah melalui terminal dengan cara yang sama seperti menulis perintah langsung pada Raspberry Pi 3 B. Untuk memulai Raspberry Pi 3 B masukan perintah `` `ssh -l aldo 172.252.25.10` `` dengan memasukkan kata sandi dan ketika berhasil, tampilan terminal akan seperti dengan yang ditunjukkan di Gambar 4.4.

Gambar 4.4 Tampilan Awal Raspberry Pi 3 B

Dengan begitu perangkat telah terhubung, serta dapat melakukan pengkonfigurasian AdGuardHome di dalam Raspberry Pi 3 B dengan menggunakan beberapa perintah dari GitHub:

1. Melakukan unduhan AdGuardHome

```
Curl -s -S -L
https://raw.githubusercontent.com/AdguardTeam/AdGuardHome/master/scripts/install.sh | sh -s -- -v
```

Perintah bash tersebut digunkan untuk pengunduhan AdGuardHome ke dalam sistem perangkat melalui URL file *script* instalasi AdGuardHome

2. Ekstraksi file AdGuardHome

```
tar xvf AdGuardHome_linux_arm.tar.gz
```

Setelah `AdGuardHome_linux_arm.tar.gz` diekstrak akan terdapat file serta folder yang digunakan untuk menjalankan AdGuardHome pada direktori yang sedang digunakan.

3. Masuk kedalam direktori AdGuardHome

```
cd AdGuardHome
```

Setelah proses ekstraksi akan terdapat folder AdGuardHome. Dengan menjalankan perintah tersebut akan masuk kedalam sebuah direktori kerja baru yaitu AdGuardHome.

4. Menginstall AdGuardHome di sistem

```
Sudo./AdGuardHome -s install
```

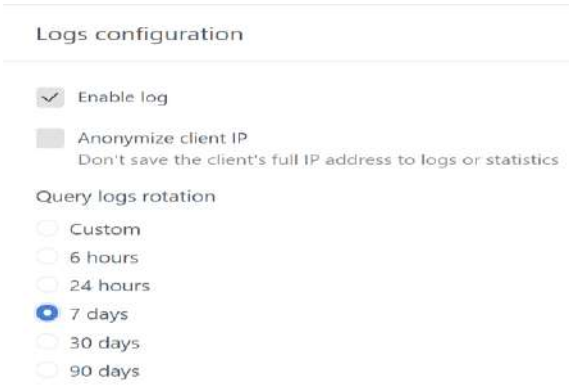
Perintah tersebut digunakan untuk melakukan instalasi AdGuardHome didalam sistem yang dijalankan dengan menggunakan perintah `Sudo` untuk mendapakan akses ke file dan direktori sistem yang dilindungi.

5. Menjalankan AdGuardHome

```
./AdGuardHome
```

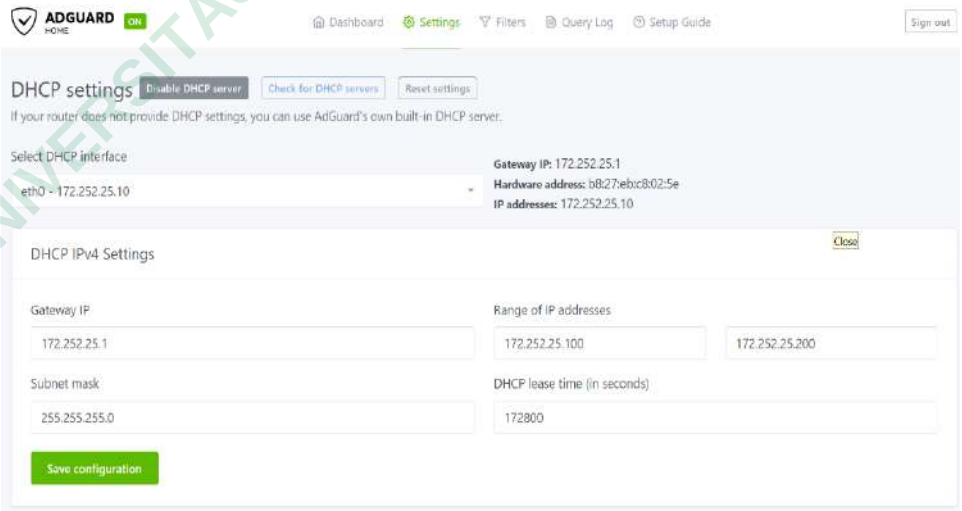
Setelah menjalankan perintah tersebut, akan mencari dan menjalankan sebuah file yang dapat dieksekusi AdGuardHome, dan memberikan alamat IP yang dapat digunakan untuk mengakses AdGuardHome melalui web browser. Dari sana, penulis dapat melakukan konfigurasi lebih lanjut untuk mencapai tujuan penelitian, yaitu pencegahan penyebaran malware dengan menggunakan AdGuardHome. Untuk konfigurasi yang dilakukan pada AdGuardHome adalah sebagai berikut:

1. Pengaturan pada bagian General settings terdapat beberapa check box yang harus dicentang seperti pada Gambar 4.5 dengan penjelasan singkat, yaitu:
   a. *Enable log* : Berfungsi untuk mengaktifkan pencatatan aktivitas kejadian di AdGuardHome dengan lebih mudah.
   b. *Query log rotation* : Hal ini bertujuan supaya *query log* akan secara otomatis dihapus dan diganti dengan yang baru untuk setiap 7 hari (sesuai custom).



Gambar 4.5 *General Setting* AdGuardHome

2. Masih terdapat beberapa pengaturan yang perlu dilakukan, termasuk pada pada bagian DNS setting terdapat beberapa yang perlu diinputkan, yaitu:
    a. *Upstream DNS servers* : Menambahkan beberapa DNS servers sebagai penyedia informasi lanjutan ketika AdGuardHome, tidak dapat menyelesaikan *query* DNS yaitu terdiri dari https:/dns.adguard-dns/com/dns-*query*, tls://dns.adguard-dns.com, quic://dns.adguard-dns.com, 8.8.8.8., 1.1.1.1, 94.140.14.14, https://dns10.quad9.net/dns-*query*.
    b. *Bootstrap DNS servers* : Melakukan penambahan DNS server supaya mengurangi latensi *query* DNS, sehingga menghasilkan browsing internet dengan performa yang lebih cepat serta melindungi jaringan dari pengalihan *query* DNS ke situs web palsu.
3. Demikian juga dengan pengaturan dilakukan pada DHCP IPv4 Setting di AdGuardHome yaitu, pada Select DHCP interface menginputkan eth0 - 172.252.25.10, yang kemudian pada Gateway IP dengan 172.252.25.1, Subnet mask 255.255.255.0, Range of IP addresses 172.252.25.100-172.252.25.120 dan yang terakhir DHCP lease time selama 172800 dengan *interface* seperti pada Gambar 4.6.



Gambar 4.6 DHCP Setting AdGuardHome

4. Untuk menyesuaikan pengaturan pemblokiran dan pemfilteran sesuai dengan tujuan penelitian, dilakukan konfigurasi dengan

mempertimbangkan fungsi-fungsi filter yang tersedia, termasuk mengaktifkan "AdGuard DNS filter". Ini mencakup "AdGuard *Base filter, Social Media filter, Tracking Protection filter, Mobile Ads filter*, serta *EasyList and EasyPrivacy*" yang berfungsi untuk mengoptimalkan penyaringan dan melindungi dari konten yang berbahaya.

Demikian tahapan persiapan selesai dengan terkonfigurasinya AdGuardHome pada perangkat Raspberry Pi 3 B

4.4 KONFIGURASI JARINGAN PADA RASPBERRY PI 3 B

Pada Raspberry Pi 3 B yang telah diinstal AdGuardHome dan ditempatkan dalam DMZ (*Demilitarized Zone*) ekosistem jaringan khusus, perlu dilakukan konfigurasi DNS *server* untuk mengarahkan ke IP AdGuardHome guna penyaringan *malware* dan pencegahan serangan. Untuk memastikan fungsi ini berjalan lancar, DHCP server pada router harus dinonaktifkan, sehingga Raspberry Pi 3 B dapat menangani pendistribusian IP ke perangkat *client* dalam satu jaringan yang sama.

4.5 PENGUJIAN SISTEM

Pengujian sistem dilakukan untuk memonitor hasil pengembangan sistem pertahanan yang menggunakan AdGuardHome pada Raspberry Pi 3 B. Tujuan pengujian ini adalah untuk melawan malvertising dan serangan internet lainnya. Selain itu, pengujian juga dilakukan untuk memverifikasi bahwa sistem beroperasi tanpa kesalahan yang signifikan dan dapat mengganggu penelitian yang dilakukan. Untuk melakukan pengujian ini yaitu dengan masuk kedalam Raspberry Pi 3 B menggunakan terminal terlebih dahulu, yang kemudian masuk kedalam *web admin* AdGuardHome pada browser dengan memasukan IP AdGuardHome yaitu 172.252.25.10 untuk melakukan pemantauan AdGuardHome.

Pada laptop ASUS VivoBook penulis, yang telah terhubung ke web admin AdGuardHome, pertama kali penulis harus melakukan login dengan memasukkan username dan password untuk mengaksesnya. Setelah proses login pertama kali selesai, penulis dapat terus mengakses dan memantau log*query* secara detail melalui dashboard web admin AdGuardHome tanpa perlu melakukan login ulang pada

perangkat yang sama. Pada tahap uji coba ini, penulis pertama-tama menggunakan ponsel Android untuk mengakses sebuah situs portal berita. Tujuan utamanya adalah untuk menguji seberapa efektif AdGuardHome dalam menghilangkan iklan *online* yang muncul selama browsing. Evaluasi dilakukan dengan membandingkan pengalaman menggunakan jaringan yang dilindungi oleh AdGuardHome dengan pengalaman tanpa perlindungan dari AdGuardHome, seperti yang terlihat pada Gambar 4.7 yang menampilkan situs yang diakses tanpa proteksi dari AdGuardHome dengan link website percobaan yang digunakan https://www.kompas.tv/olahraga/517817/link-live-streaming-belanda-vs-austria-di-euro-2024-malam-ini-kick-off-jam-23-00-wib?medium=headline&so=2

Gambar 4.7 Situs Kompas.tv yang mengandung iklan *online*

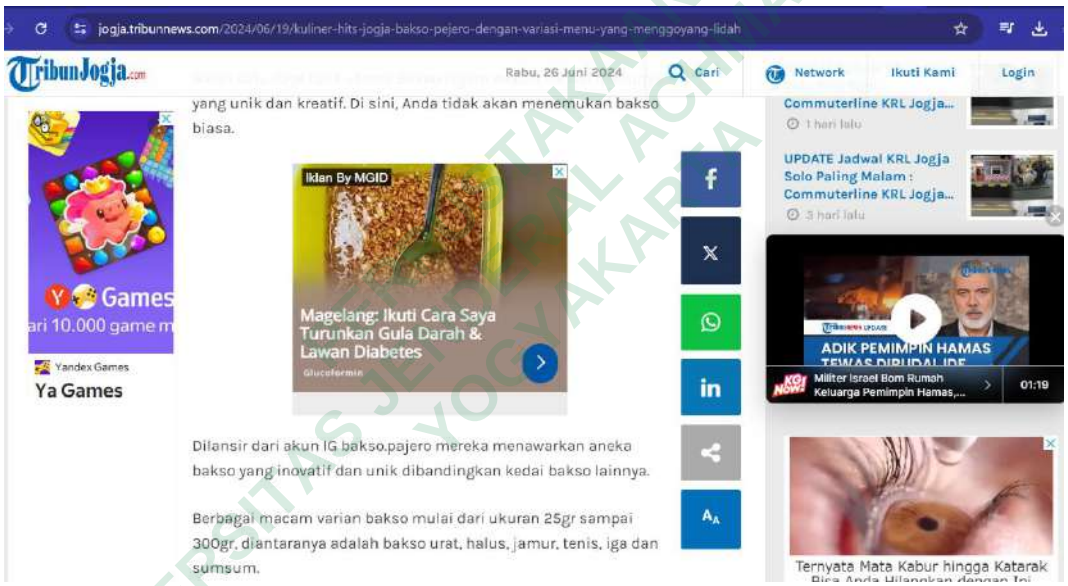
Setelah melakukan uji coba pada jaringan yang tidak terlindungi oleh AdGuardHome pada ponsel Android "*China Brand"* seperti pada Gambar 4.7,

adanya iklan *online* pada portal berita Kompas.tv yang tidak hanya mengganggu pengalaman pengguna dalam menjelajah internet tetapi juga dapat menimbulkan masalah seperti malvertising, di mana iklan yang tampil dapat menyembunyikan malware atau mengarahkan pengguna ke situs yang berbahaya. Kondisi ini tidak hanya mengganggu kenyamanan saat mengakses konten, tetapi juga memperlambat waktu muat halaman serta mengganggu fokus pada informasi yang ingin dilihat atau diakses.

Penulis melanjutkan dengan menguji jaringan yang dilindungi oleh AdGuardHome, seperti yang terlihat pada Gambar 4.8. Dengan tujuan untuk memeriksa sejauh mana efektivitas sistem dalam mengurangi atau menghilangkan iklan yang tidak diinginkan serta untuk memastikan perlindungan terhadap pengguna dari potensi serangan malware yang terkait dengan iklan *online*.

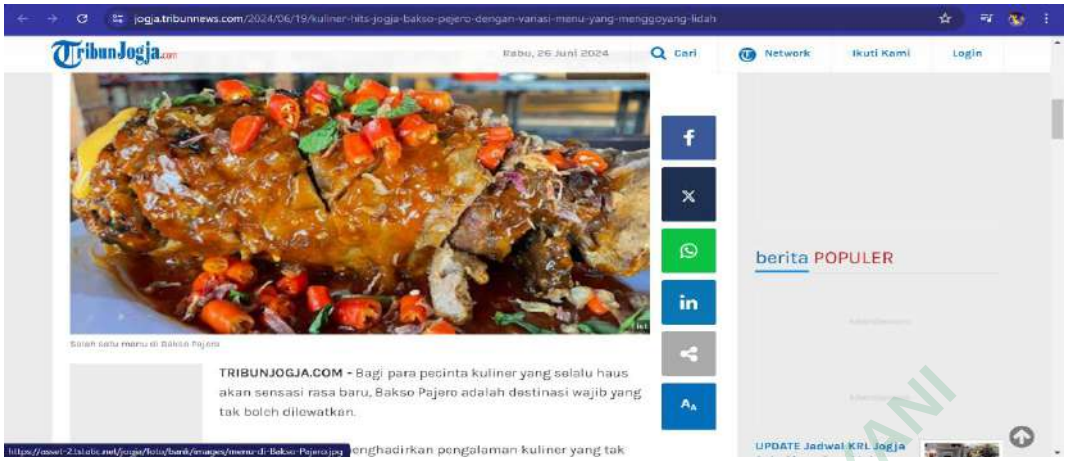
Gambar 4.8 Situs Kompas.tv tanpa mengandung iklan *online*

Pada Gambar 4.8 terlihat bahwa iklan *online* di situs Kompas.tv tidak muncul pada ponsel Android "*China Brand*". Meskipun fokus pengujian penelitian ini adalah pada ponsel Android merek "*China Brand*" dengan "*Fresh Install*" atau "*Modul Setelan Pabrik*". Untuk menguji keefektifan sistem AdGuardHome, pengujian juga akan dilakukan pada PC atau laptop. Hal ini dilakukan untuk memastikan bahwa AdGuardHome tidak hanya efektif bekerja pada perangkat ponsel Android, tetapi juga mampu memberikan perlindungan dan fungsi penyaringan yang optimal pada perangkat lain seperti PC atau laptop. Percobaan akan menggunakan web dari link https://jogja.tribunnews.com/2024/06/19/kuliner-hits-jogja-bakso-pejero-dengan-variasi-menu-yang-menggoyang-lidah



Gambar 4.9 Situs tribunnews.com yang mengandung iklan *online*

Pada Gambar 4.9 menunjukan bahwa iklan *online* muncul di portal berita tribunnews.com pada perangkat laptop penulis yang belum tersambung dengan jaringan yang terisolasi oleh AdGuardHome, sehingga iklan *online* terus bermunculan dan mengganggu kenyaman aktifitas berselancar di internet. Percobaan berikutnya juga akan dilakukan dengan menyambungkan pada jaringan yang terisolasi oleh AdGuardHome dan akan melakukan akses ulang pada situs yang sama seperti pada Gambar 4.10. Setelah menyambung pada jaringan yang terisolasi oleh AdGuardHome menunjukan portal berita tribunnews.com yang telah bersih dari iklan *online*.



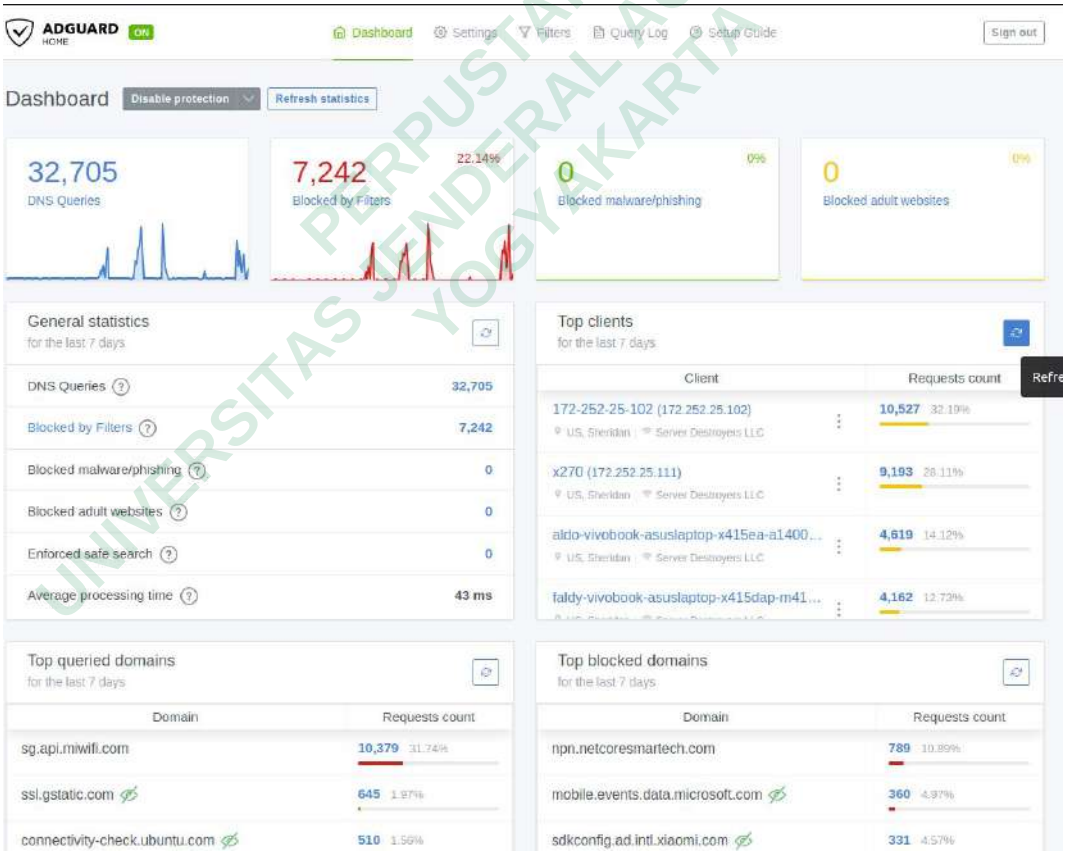
Gambar 4.10 Situs tribunnews.com tanpa mengandung iklan *online*

Setelah menyambung pada jaringan yang terisolasi oleh AdGuardHome menunjukan portal berita tribunnews.com yang telah bersih dari iklan *online*. Berdasarkan pengujian sistem yang telah dilakukan, membuktikan bahwa sistem AdGuardHome berfungsi dengan baik dan berhasil diterapkan untuk mengurangi resiko penyebaran melalui iklan *online* atau disebut dengan *malvertising.* Tidak hanya terbatas pada pemblokiran *online*, namun juga pada akses yang dilakukan berjalan lebih cepat dibanding dengan sebelumnya.

4.6 PEMBAHASAN

Penelitian mengenai implementasi AdGuardHome yang dikonfigurasikan pada perangkat Raspberry Pi 3B yang diintegrasikan dalam DMZ ekosistem jaringan khusus yang telah dirancang, akan digunakan sebagai persiapan untuk pengambilan data. Proses pengambilan data akan dilakukan dalam kurun waktu lebih kurang 2 pekan, yaitu dimulai dari tanggal 4 Juni sampai dengan 20 Juni 2024. Dalam penelitian yang dilakukan akan mengujikan 5 ponsel Android "*China Brand*" yang terhubungnya ke jaringan terisolasi oleh AdGuardHome dengan bantuan dari *Accsess point* sebagai pendistribusian jaringan secara *wireless*. Hal ini dilakukan secara bergantian sampai dengan yang terakhir sebagai syarat bahwa data sudah benar dan tidak ada kesalahan. Data yang akan dianalisis berasal dari *query log* yang dicatat oleh AdGuardHome setelah setiap ponsel Android terhubung ke jaringan khusus tersebut selama periode 1x24 jam.

Dalam penelitian yang dilakukan setiap dari 5 ponsel Android "*China Brand"* yang dijadikan objek penelitian, akan tersambung dengan jaringan khusus tanpa intervensi pengguna. Dalam pengerjaan akan dilakukan menggunakan bantuan CLI (*Command Line Interface*) pada terminal dengan OS (*Operating System*) berbasis Linux Ubuntu pada perangkat laptop penulis yaitu ASUS Vivobook. Sebelumnya penulis akan menampilkan *interface* dari *dashboard* AdGuardHome yang diakses melalui web browser seperti pada Gambar 4.11 dan tampilan dari *logquery* seperti pada Gambar 4.12. Terlebih dahulu masuk kedalam Raspberry Pi 3 B memasukkan perintah `ssh -l aldo 172.252.25.10` dan memasukkan password setelahnya. Setelah berhasil masuk ke dalam Raspberry Pi 3 B, maka dapat mengakses AdGuardHome melalui web browser dengan menuliskan IP-nya yaitu 172.252.25.10.

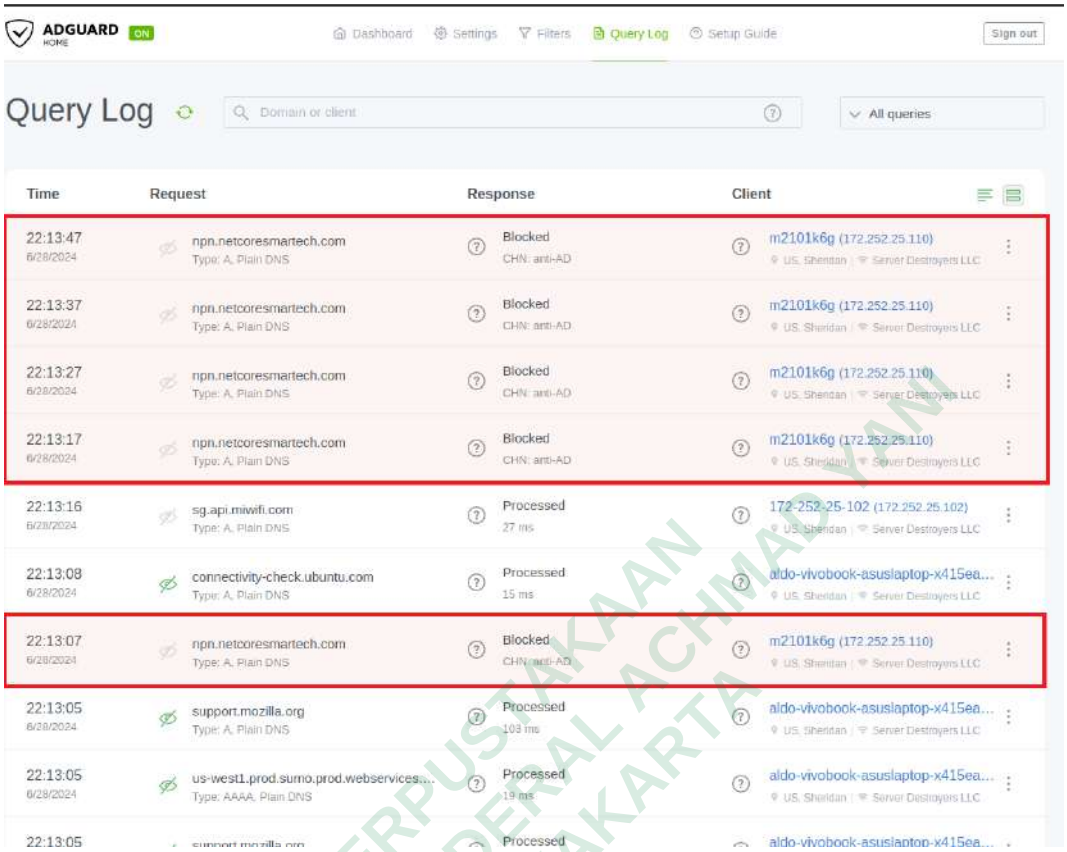


Gambar 4.11 Dashboard AdGuardHome

Seperti yang terlihat pada Gambar 4.11 bahwasanya tampilan pada dashboard AdGuardHome memiliki beberapa keterangan aktivitas yang dilakukan pada perangkat *client* yang terhubung menggunakan ekosistem jaringan khusus.

1. Bagian statistik umum memberikan gambaran menyeluruh tentang aktivitas jaringan, mencakup informasi seperti jumlah total *query* DNS yang diterima, jumlah *query* yang diblokir karena mengandung iklan, malware, atau situs dewasa, serta statistik lainnya. Selain itu, bagian ini juga mencatat rata-rata waktu yang diperlukan untuk memproses setiap *query* DNS dalam sistem.
2. Bagian daftar *client* ini menampilkan perangkat atau alamat IP yang terhubung ke AdGuardHome dan menggunakan layanan pemblokiran iklan dan pelacak. Selain itu, daftar ini juga mencatat jumlah *query* DNS yang dihasilkan oleh setiap *client*.
3. Bagian domain yang paling sering diakses dan diblokir memberikan informasi tentang domain yang paling sering diminta oleh perangkat dalam satu segmen jaringan dan domain yang paling sering diblokir oleh AdGuardHome. Data ini dapat memberikan informasi mengenai kebiasaan pengguna dalam menjelajahi internet melalui jaringan yang digunakan, serta menunjukkan seberapa efektif filter AdGuardHome dalam melindungi dari konten yang tidak diinginkan.

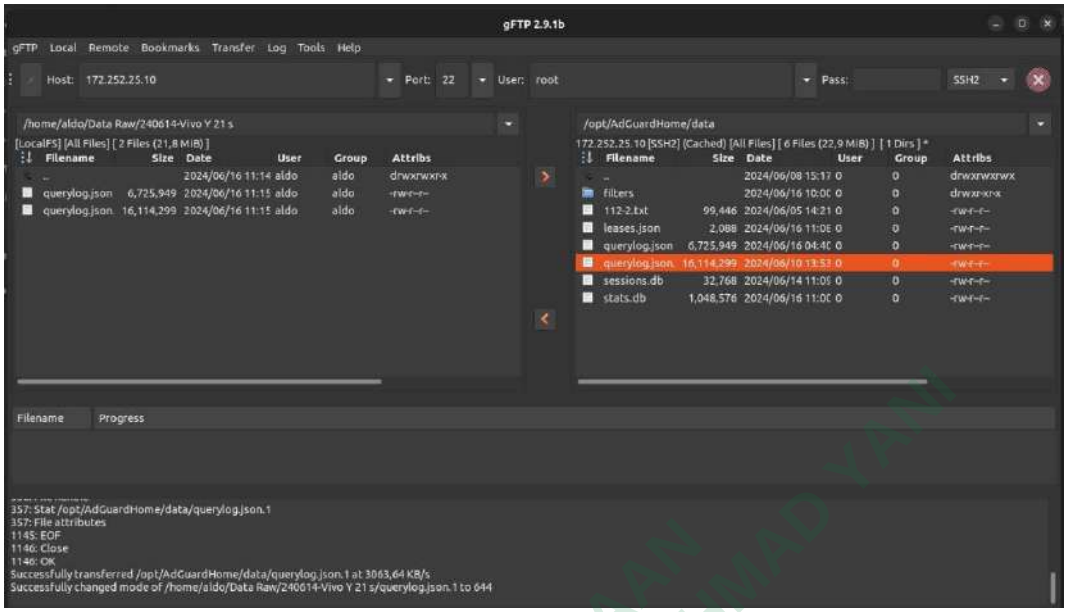
Penjelasan ini menggambarkan bahwa dashboard AdGuardHome merupakan sebuah *tools* yang berguna dalam memantau aktivitas dan statistik dari AdGuardHome. Melalui dashboard ini, dapat melihat jumlah *query* DNS yang diolah oleh AdGuardHome, jumlah *query* yang berhasil diblokir, serta informasi mengenai domain-domain yang paling sering diakses dan diblokir oleh sistem.



Gambar 4.12 *Query Log*

Gambar 4.12 menampilkan *query log* pada antarmuka web AdGuardHome, yang mencatat daftar permintaan DNS yang telah diolah oleh AdGuardHome. Setiap *entri* dalam log permintaan menunjukkan informasi tentang nama atau alamat IP *client* yang melakukan query, serta domain yang diminta. Selain itu, setiap query *client* juga menampilkan tindakan yang diambil oleh AdGuardHome terhadap permintaan tersebut, seperti izin, blokir, atau pengalihan.

Itulah sedikit tampilan antar muka AdGuardhome, namun dalam penelitian yang dilakukan akan menggunakan sebuah CLI guna dalam mempermudah penelitian yang dilakukan. Serta menggunakan sebuah software GFTP yang berfungsi untuk mentransfer file antar komputer atau server. Proses transfer file ini melibatkan memasukkan IP server, port, username, password, serta dengan protokol SSH2. Pengambilan data dilakukan dengan menarik file dari panel *remote* (server) ke panel lokal (komputer pengguna) seperti pada Gambar 4.13.

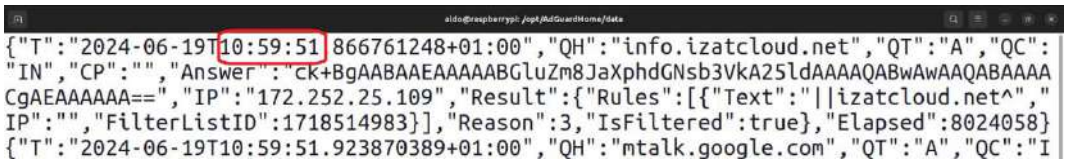


Gambar 4.13 GFTP

Setelah data yang dibutuhkan terkumpul, langkah berikutnya adalah mengkonversi data dari format JSON ke CSV menggunakan bantuan dari situ web https://www.convertCSV.com/json-to-CSV.htm#google_vignette. Tujuannya adalah untuk menyaring setiap data, yang diekstrak sebagai bukti dalam penelitian.

Kemudian penggunaan CLI dalam penelitian yang dilakukan akan mempermudah dalam mengidentifikasi, dikarenakan yang terhubung pada jaringan khusus tidak hanya terbatas pada 1 perangkat saja tetapi lebih dari satu. Sedangkan, penelitian akan berfokus pada IP dari perangkat yang akan dijadikan objek penelitian yaitu ponsel Android *"China Brand"* yang penulis sudah siapkan. Saat mengidentifikasi, terlebih dahulu memastikan IP dari perangkat untuk dapat mencari informasi dengan menggunakan perintah pada terminal. Selain itu untuk masuk mencari informasi, diharuskan masuk kedalam direktori data pada AdGuardHome untuk dapat mengakses file *query log* yang berisi data akses setiap *client*. Dengan menjalankan perintah "`cat querylog.json |grep 172.252.25.109 |less`". Perintah tersebut memiliki fungsi, `cat` digunakan untuk membaca dan menampilkan isi dari file (`querylog.json`), dengan `|` (*Pipe*) untuk memberikan input ke perintah selanjutnya, yaitu `grep` yang digunakan untuk mencari sebuah baris, dalam hal ini yang berisi data (`172.252.25.109`) dan

dilanjutkan dengan `less` untuk menampilkan hasil yang di *filter* dalam satu halaman seperti pada Gambar 4.14.



Gambar 4.14 Pemantauan Waktu Perangkat pada Terminal

Dengan adanya hal ini, akan membantu dan menyederhanakan proses penelitian, dengan mengetahui kapan perangkat *connect* ke jaringan khusus seperti pada Gambar 4.14 di tanda kotak merah. Hal ini penting, untuk menilai sesuai dengan pengambilan data yang direncanakan, yang berlangsung selama 1x24 jam untuk setiap perangkat yang dijadikan objek penelitian. Sebagai contoh jika perangkat tersambung pada jam 10:59 maka akan diambil data pada keesokan hari di jam yang sama.

Kemudian setelah dilakukan pengecekan, dapat melakukan pengambilan data berupa berapa banyak *query* serta berapa banyak blokir yang dilakukan oleh AdGuardHome pada IP 172.252.25.109, dengan menggunakan 2 perintah yaitu sebagai berikut.

1. `Cat querylog.json |grep 172.252.25.109 |wc -l`

   Perintah tersebut akan menjalankan fungsi untuk mencari baris yang terdapat string 172.252.25.109, dengan wc -l bertugas untuk menghitung jumlah baris yang terdapat 172.252.25.109 pada file querylog.
2. `Cat querylog.json |grep 172.252.25.109 |grep ":3," |wc -l`

   Perintah tersebut akan menjalankan fungsi untuk mencari baris yang terdapat 2 teks dalam 1 baris 172.252.25.109 dan ":3,". serta wc -l yang bertugas untuk menghitung jumlah baris yang terdapat 172.252.25.109 dan ":3," dalam 1 baris pada file querylog.json. Sebagai catatan bahwa ":3," merupakan angka dari fungsi blokir pada AdGuardHome.

dengan contoh hasil seperti pada Gambar 4.15.

Gambar 4.15 Data Total Query dan Blokir

Untuk pengambilan data pada 5 ponsel Android akan menggunakan metode tersebut dengan mencatat total dari query dan total blok yang kemudian nantinya akan dihitung dengan output persentase. Dalam penyebutan merk akan menggunakan inisial untuk setiap ponsel Androidnya dengan ketentuan seperti berikut.

Tabel 4.1 IP Perangkat dan Tanggal Penelitian

NO	Merk	IP	Tanggal	Waktu
1	Y1	172.252.25.113	4-5 juni 2024	15:26
2	Y2	172.252.25.114	13-14 Juni 2024	08:28
3	Y3	172.252.25.115	14-15 Juni 2024	16:44
4	Y4	172.252.25.109	19-20 Juni 2024	10:59
5	Y5	172.252.25.108	19-20 Juni 2024	10:56

Tabel 4.1 merupakan identitas dari setiap perangkat dengan IP sebagai tanda pengenal sekaligus dengan tanggal dan waktu saat perangkat tersambung dengan jaringan khusus, yang kemudian akan diambil data setelah 1x24 jam di waktu perangkat tersambung pada jaringan khusus. Setelah dilakukan pengambilan data pada ke 5 ponsel Android "*China Brand"* dalam kurun waktu 1x24 jam, didapatlah sebuah hasil penelitian seperti pada Tabel 4.2 dengan hasil perhitungan menggunakan rumus yang telah ditetapkan seperti sebagai berikut.

$$P = B/Q.\ 100\%$$

Keterangan: P = Persentase

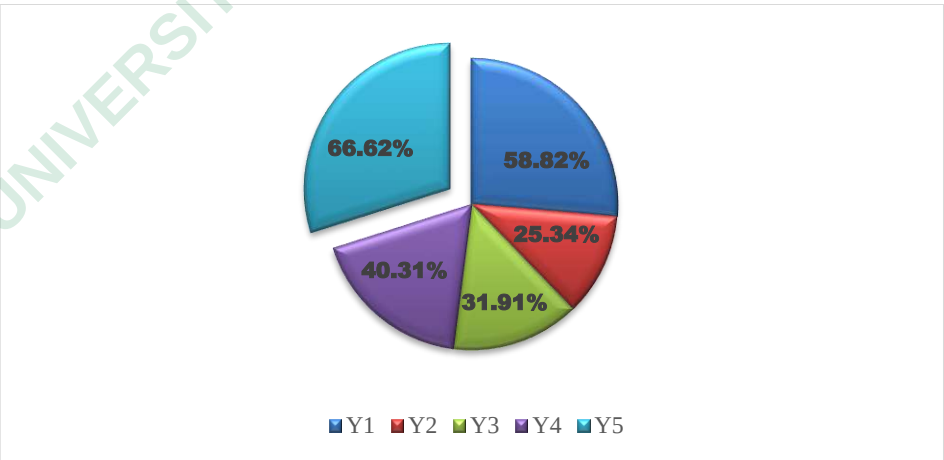
B= Blok

Q= Query

Tabel 4.2 Persentase Hasil Penelitian

No	Merk	Q	B	P
1	Y1	969	570	58.82%
2	Y2	817	207	25.34%
3	Y3	564	180	31.91%
4	Y4	712	287	40.31%
5	Y5	2316	1543	66.62%

Berdasarkan pengambilan data dari lima ponsel Android *merk* "*China Brand*" selama 24 jam, dari Tabel 4.2 menunjukkan bahwa persentase pemblokiran tertinggi terjadi pada ponsel Android Y5, mencapai 66.62% dari total *query* yang diblokir, sedangkan persentase pemblokiran terendah adalah pada ponsel Y2, yaitu sebesar 25.34%. Selain daripada itu, Y5 memiliki query terbanyak dengan total 2316 dan total blokir sebanyak 1543 dalam periode 1x24 jam.



Gambar 4.16 Persentase Chart

Dari Gambar 4.16 secara keseluruhan urutan persentase pemblokiran dari yang terendah hingga tertinggi adalah Y2 (25.34%), Y3 (31.91%), Y4 (40.31%), Y1 (58.82%), dan yang tertinggi adalah Y5 (66.62%).