BAB 4
HASIL PENELITIAN

4.1 Ringkasan Hasil Penelitian

Ringkasan hasil penelitian berisi uraian rinci tentang hasil yang didapatkan dari penelitian. Penelitian ini berhasil mengembangkan alat uji jaringan Wi-Fi dengan menggunakan sumber daya berbasis Baterai untuk mensimulasikan *Evil Twin Attack*. Simulasi *Evil Twin Attack* dilakukan dengan mengkonfigurasi OpenWRT dan Tailscale untuk membuat jaringan Wi-Fi palsu dan dirancang secara *remote* yang dilakukan di Lantai 1, Lantai 2, Lantai 3, Lantai 4, dan Gazebo di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta. Lokasi pengujian dipilih berdasarkan identifikasi dan penentuan jaringan Wi-Fi yang terdapat adanya akses internet jaringan Wi-Fi terbuka dengan SSID "UNJAYA". Hasil pengembangan alat uji dapat dilakukan untuk menangkap paket data jaringan Wi-Fi menggunakan *tools tcpdump* dan menghasilkan file tangkapan paket data dalam format .pcap yang disimpan pada subdirektori "pcap" di dalam direktori "remote_arkime" melalui *mounting* SSHFS pada Server Arkime. Kemudian, hasil file tangkapan paket data dalam format .pcap yang ditangkap akan dianalisis menggunakan Arkime melalui Arkime *Viewer*. Proses analisis paket data dilakukan untuk mengidentifikasi jumlah korban yang masuk ke dalam jaringan Wi-Fi palsu dan mengidentifikasi protokol yang diakses oleh korban. Proses identifikasi protokol dilakukan bertujuan untuk mencari protokol yang rentan yaitu HTTP dengan mencari data sensitif korban meliputi *username* dan *password* yang mungkin dikirim melalui protokol tersebut.

Selama proses pengujian dan hasil file tangkapan paket data di *import* ke Arkime untuk dapat ditampilkan pada Arkime *Viewer* terdapat jumlah korban yang terjebak ke dalam jaringan Wi-Fi palsu dengan mensimulasikan *Evil Twin Attack*. Hasil jumlah korban yang terjebak di Lantai 1 berjumlah 14 korban dengan proses pengujian yang berlangsung pada tanggal 23 Mei 2025 pukul 10.37 – 12.29. Hasil dari jumlah korban yang terjebak pada Lantai 1 dilakukan identifikasi untuk mengetahui *port* yang diakses oleh korban yang dimana hal ini bertujuan untuk mengetahui apakah korban mengakses *port* 80 atau protokol HTTP. Hasil identifikasi *port* yang diakses oleh korban pada Lantai 1 menunjukkan bahwa ada beberapa alamat IP korban yang mengakses *port* 80. Akses korban ditunjukkan dengan sesi komunikasi korban yang terlihat pada Arkime *Viewer* dengan memfilter alamat IP korban dan *port* 80. Kemudian, dilakukan identifikasi data sensitif korban pada fitur *Hunt* di Arkime *Viewer*. Namun, korban yang terjebak pada jaringan Wi-Fi palsu yang dilakukan di Lantai 1 belum menunjukkan bahwa adanya data sensitif dari korban.

Selanjutnya, hasil identifikasi jumlah korban yang terjabak di Lantai 2 berjumlah 10 korban dengan proses pengujian yang berlangsung pada tanggal 23 Mei 2025 pukul 14.15 – 16.01. Pada hasil identifikasi *port* yang diakses oleh korban pada Lantai 2 menunjukkan bahwa ada beberapa alamat IP korban yang mengakses *port* 80. Namun, ketika dilakukan identifikasi data sensitif korban pada fitur *Hunt* di Arkime *Viewer* belum terdapat adanya data sensitif dari korban.

Kemudian, hasil identifikasi jumlah korban yang terjabak di Lantai 3 berjumlah 22 korban dengan proses pengujian yang berlangsung pada tanggal 26 Mei 2025 pukul 11.25 – 13.03. Pada hasil identifikasi *port* yang diakses oleh korban pada Lantai 3 menunjukkan bahwa ada beberapa alamat IP korban yang mengakses *port* 80. Namun, ketika dilakukan identifikasi data sensitif korban pada fitur *Hunt* di Arkime *Viewer* belum terdapat adanya data sensitif dari korban.

Berikutnya, hasil identifikasi jumlah korban yang terjabak di Lantai 4 berjumlah 4 korban dengan proses pengujian yang berlangsung pada tanggal 27 Mei 2025 pukul 09.30 – 11.19. Pada hasil identifikasi *port* yang diakses oleh korban pada Lantai 4 menunjukkan bahwa ada beberapa alamat IP korban yang mengakses *port* 80. Namun, ketika dilakukan identifikasi data sensitif korban melalui fitur *Hunt* di Arkime *Viewer* belum terdapat adanya data sensitif dari korban.

Hasil identifikasi jumlah korban yang terakhir, dilakukan di Gazebo dengan berjumlah 52 korban dengan proses pengujian yang berlangsung pada tanggal 27 Mei 2025 pukul 14.25 – 15.58. Pada hasil identifikasi *port* yang diakses oleh korban di Gazebo menunjukkan bahwa ada beberapa alamat IP korban yang mengakses *port* 80. Namun, ketika dilakukan identifikasi data sensitif korban melalui fitur *Hunt* di Arkime *Viewer* belum terdapat adanya data sensitif dari korban.

4.2 Identifikasi dan Penentuan Jaringan Wi-Fi

Pada tahap yang pertama dalam penelitian ini yaitu mengidentifikasi dan menentukan jaringan Wi-Fi yang dijadikan objek penelitian. Objek penelitian dalam penelitian ini bertujuan untuk membuat jaringan Wi-Fi palsu dengan mensimulasikan *Evil Twin Attack*. Identifikasi dan penentuan jaringan Wi-Fi dilakukan di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dengan tujuan untuk memperoleh informasi dari jaringan Wi-Fi yang tersedia, meliputi *Service Set Identifier* (SSID), alamat *Media Access Control* (MAC) *Address*, frekuensi, *channel*, jenis enkripsi, dan *password* atau kata sandi. Demi menjaga kerahasiaan dan keamanan informasi data sensitif seperti akses *barcode* dan *password* jaringan Wi-Fi tidak ditampilkan secara eksplisit dalam laporan ini. Informasi data sensitif akan dilindungi atau disensor agar mencegah penyalahgunaan dan menjaga integritas data.

Dalam mengidentifikasi jaringan Wi-Fi yang tersedia di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dilakukan menggunakan teknik *Wardriving*. Teknik *Wardriving* adalah sebuah teknik dalam keamanan siber untuk mencari, mengumpulkan, dan merekam jaringan Wi-Fi dengan mengemudi atau jalan – jalan disekitar area tertentu. Salah satu alat atau *tools* yang digunakan untuk melakukan teknik *Wardriving* adalah WiGLE Wi-Fi. WiGLE Wi-Fi adalah alat atau *tools* berbentuk aplikasi *mobile* dan *website* untuk mengumpulkan data jaringan Wi-Fi seperti SSID, alamat MAC *Address*, frekuensi, *channel*, dan jenis enkripsi diberbagai tempat yang terdapat jaringan Wi-Fi (Buntoro & Adiguna, 2024).

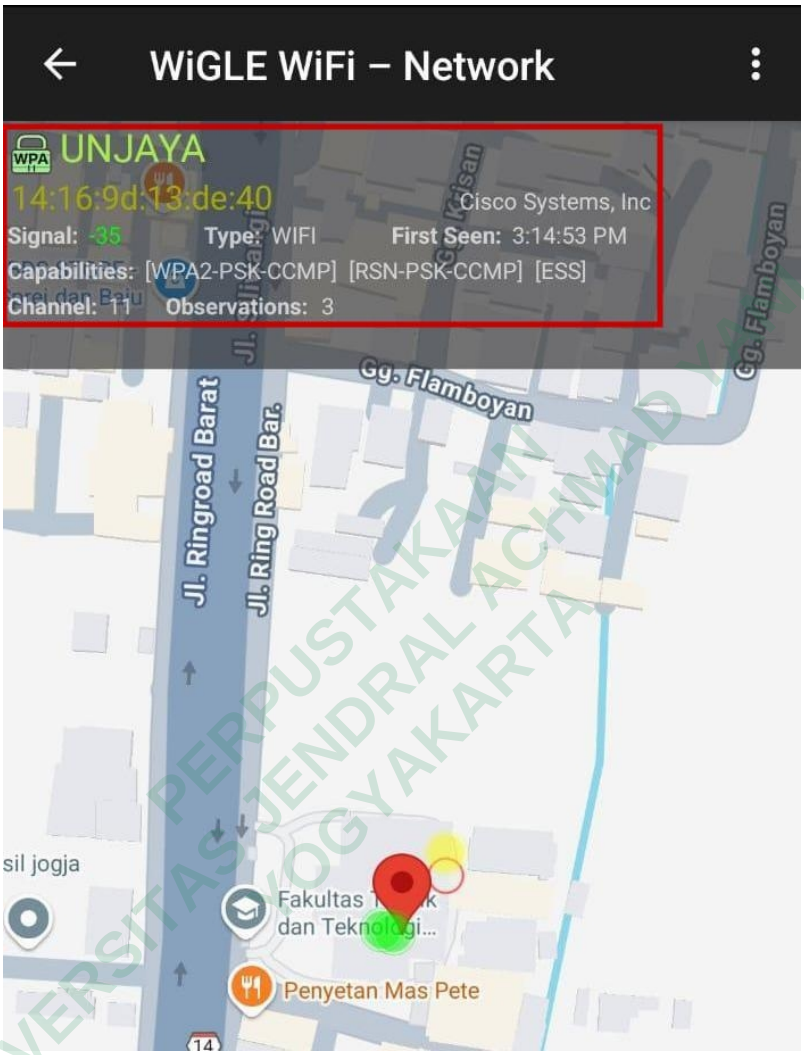
Dalam melakukan teknik *Wardriving* di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dilakukan dengan menjalankan aplikasi *mobile* WiGLE Wi-Fi dan mengaktifkan mode Wi-Fi pada *smartphone*. Ketika aplikasi WiGLE Wi-Fi dijalankan, terdapat informasi jaringan Wi-Fi yang tertangkap di area Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta sebagaimana yang ditampilkan pada Gambar 4.1.

Gambar 4.1 Hasil Tangkapan Jaringan Wi-Fi Menggunakan WiGLE Wi-Fi

Kemudian, di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta terdapat akses internet jaringan Wi-Fi terbuka dalam bentuk *scan barcode* yaitu dengan SSID "UNJAYA" sebagaimana yang ditampilkan pada Gambar 4.2.

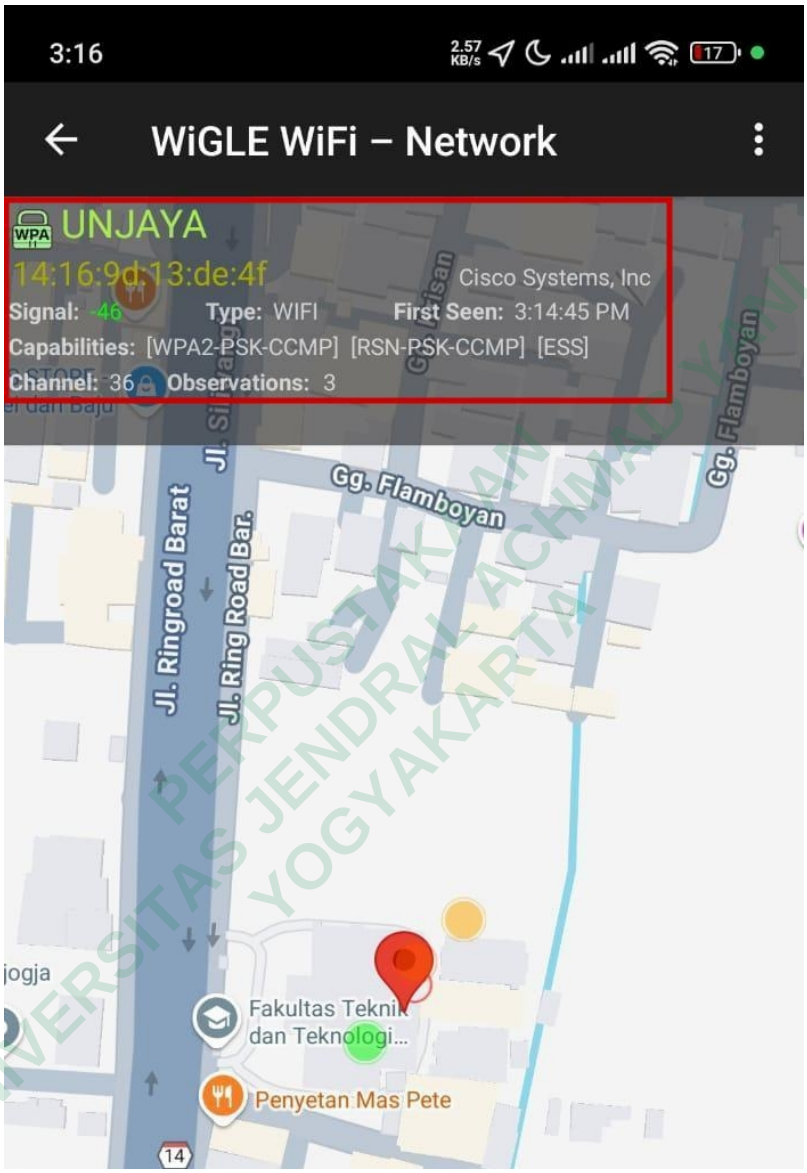
Gambar 4.2 Akses Internet Jaringan Wi-Fi Terbuka

Dengan adanya akses internet jaringan Wi-Fi terbuka dengan SSID "UNJAYA" di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dapat diperoleh bahwa jaringan Wi-Fi dengan SSID "UNJAYA" dapat diakses oleh siapa saja dengan melakukan *scan barcode* yang tersedia. Ketika akses internet terbuka dilakukan *scan barcode* melalui *smartphone* diperoleh *password* dari SSID "UNJAYA". Dari hasil *scan barcode* dan hasil tangkapan data jaringan Wi-Fi menggunakan WiGLE Wi-Fi dapat ditentukan objek penelitian yang digunakan untuk proses pengujian adalah jaringan Wi-Fi dengan SSID "UNJAYA". Identifikasi jaringan Wi-Fi dengan SSID "UNJAYA" menggunakan WiGLE Wi-FI diperoleh 2 data yang dimana dibedakan dengan frekuensi 2,4GHz dan 5GHz sebagaimana yang ditampilkan pada Gambar 4.3 dan Gambar 4.4.



Gambar 4.3 Data Frekuensi 2,4 GHz

Gambar 4.3 menunjukkan data SSID "UNJAYA dari frekuensi 2,4GHz dengan alamat MAC *Address* "14:16:9d:13:de:40", *channel* "11", dan jenis enkripsi "WPA2-PSK-CCMP".



Gambar 4.4 Data Frekuensi 5 GHz

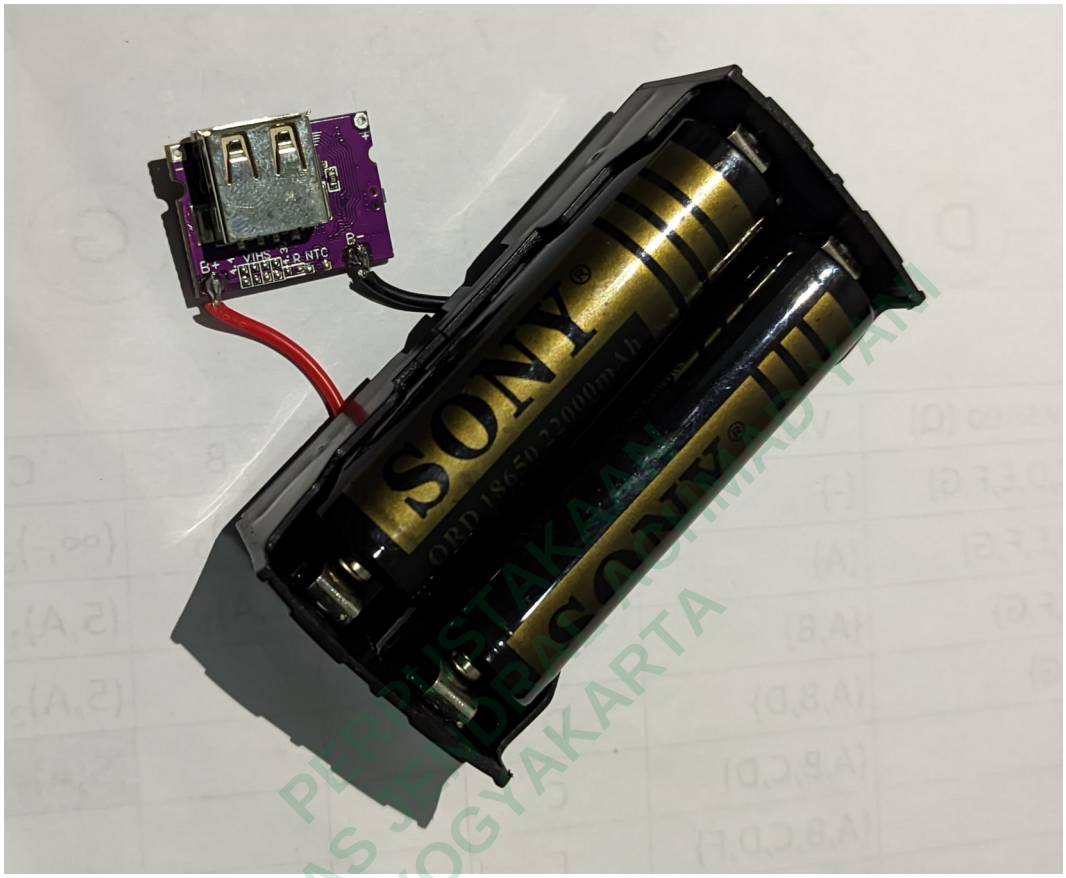
Gambar 4.4 menunjukkan data SSID "UNJAYA" dari frekuensi 5GHz dengan alamat MAC *Address* "14:16:9d:13:de:4f", *channel* "36", dan jenis enkripsi "WPA2-PSK-CCMP".

4.3 Perancangan dan Integrasi Sistem Pengujian

Sistem pengujian dirancang dengan tujuan untuk mensimulasikan *Evil Twin Attack* melalui pembuatan jaringan Wi-Fi palsu yang menyerupai jaringan Wi-Fi asli dengan SSID "UNJAYA" di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta dan menangkap paket data jaringan untuk dianalisis menggunakan Arkime. Sistem pengujian ini terdiri dari beberapa komponen yang saling terintegrasi untuk mendukung proses pengujian dan analisis paket data jaringan Wi-Fi.

4.3.1 Perancangan Sumber Daya

Perancangan sumber daya dilakukan untuk mendukung kelancaran proses selama pengujian berlangsung. Sumber daya yang dirancang berbasis portabel dengan menggunakan Baterai dan Modul *Power Bank* sebagai penyedia sumber daya atau sumber tegangan pada Raspberry Pi 4 Model B yang digunakan pada saat proses pengujian. Modul *Power Bank* digunakan juga sebagai perantara pengisian daya pada Baterai. Pada penelitian ini Modul *Power Bank* dan Baterai yang digunakan adalah IP5310 Modul *Power Bank* dan Baterai Sony ORD 18650 berkapasitas 22000mAh dengan tegangan 4.2V Li-ion yang saling terhubung melalui kabel. Perancangan dilakukan dengan menghubungkan IP 5310 Modul *Power Bank* dengan kabel ke *socket* Baterai yang didalamnya terdapat 2 Baterai Sony ORD 18650. Hasil perancangan sumber daya dapat dilihat pada Gambar 4.5. *Socket* Baterai yang digunakan dirangkai secara pararel menggunakan kabel agar tegangan Baterai yang dihasilkan bernilai tetap dan kapasitas baterai (mAh) Baterai akan bertambah dimana hal ini akan menentukan lamanya proses pengujian.



Gambar 4.5 Hasil Perancangan Sumber Daya

4.3.2 Konfigurasi OpenWRT

Dalam proses pembuatan jaringan Wi-Fi palsu untuk mensimulasikan *Evil Twin Attack*, OpenWRT dipilih karena bersifat *open source*, fleksibel, dan mendukung konfigurasi perangkat keras jaringan Wi-Fi. OpenWRT diimplementasikan sebagai Router pada perangkat keras Raspberry Pi 4 Model B. Raspberry Pi 4 Model B yang dikonfigurasi dengan OpenWRT digunakan sebagai alat uji keamanan jaringan Wi-Fi dalam penelitian ini dengan membuat jaringan Wi-Fi palsu. Pembuatan jaringan Wi-Fi palsu pada OpenWRT dilakukan dengan

beberapa tahap, diawali dengan instalasi OpenWRT pada SD *Card* berkapasitas 128GB yang berfungsi sebagai media penyimpanan file *image* dari sistem pengoperasian OpenWRT. Sistem pengoperasian OpenWRT diimplementasikan menggunakan versi 24.10.1 yang dapat diunduh melalui *link* https://firmware-selector.openwrt.org/?version=24.10. File *image* sistem pengoperasian OpenWRT yang diunduh, kemudian dilakukan *burning* ke dalam SD *Card* berkapasitas 128GB menggunakan aplikasi USB *Image Writer*. Ketika proses *burning* telah selesai, SD *Card* berkapasitas 128GB dipasang pada Raspberry Pi 4 Model B.

Selanjutnya, konfigurasi OpenWRT dilakukan ketika SD *Card* berkapasitas 128GB terpasang ke dalam Raspberry Pi 4 Model B dengan mengubah file *Dynamic Host Configuration Protocol* (DHCP) dan file *Network* pada OpenWRT. Perubahan pada file DHCP dan file *Network* bertujuan untuk menonaktifkan layanan DHCP dan mengubah alamat *Internet Protocol* (IP) pada OpenWRT sehingga OpenWRT dapat berfungsi sebagai *client* dalam jaringan Router. Konfigurasi DHCP dan *Network* ini bertujuan agar OpenWRT mendapatkan koneksi internet dari Router untuk proses instalasi *package* yang mendukung penggunaan Modem GSM. Modem GSM digunakan untuk menyediakan koneksi internet melalui jaringan seluler pada jaringan Wi-Fi palsu yang dibuat sehingga dapat memberikan fleksibilitas dalam proses pengujian dan pengembangan alat uji yang dapat digunakan di berbagai lokasi.

Dalam konfigurasi DHCP dan *Network* dilakukan pada saat Raspberry Pi 4 Model B yang dihubungkan ke Laptop melalui Kabel LAN dan mengubah pengaturan jaringan pada Laptop ke *mode* DHCP. Pengaturan jaringan pada Laptop bertujuan agar Laptop dapat menerima IP dari OpenWRT secara otomatis dan dinamis. Selain itu, pengaturan ini juga memungkinkan akses *Command Line Interface* (CLI) OpenWRT menggunakan protokol *Secure Shell* (SSH) melalui Terminal Laptop.

Setelah perubahan pengaturan pada jaringan Laptop, konfigurasi DHCP dan *Network* pada OpenWRT dilakukan melalui CLI OpenWRT. Konfigurasi DHCP dijalankan menggunakan perintah `vim /etc/config/dhcp`. Kemudian, konfigurasi DHCP dilakukan pada baris "config dhcp". Perubahan pada konfigurasi DHCP yang dilakukan adalah sebagai berikut:

```
config dhcp 'lan'
    option interface 'lan'
    option leasetime '12h'
    option dhcpv4 'server'
    option dhcpv6 'server'
    option ra 'server'
    option ra_slaac '1'
    list ra_flags 'managed-config
    list ra_flags 'other-config'
    option ignore '1'
```

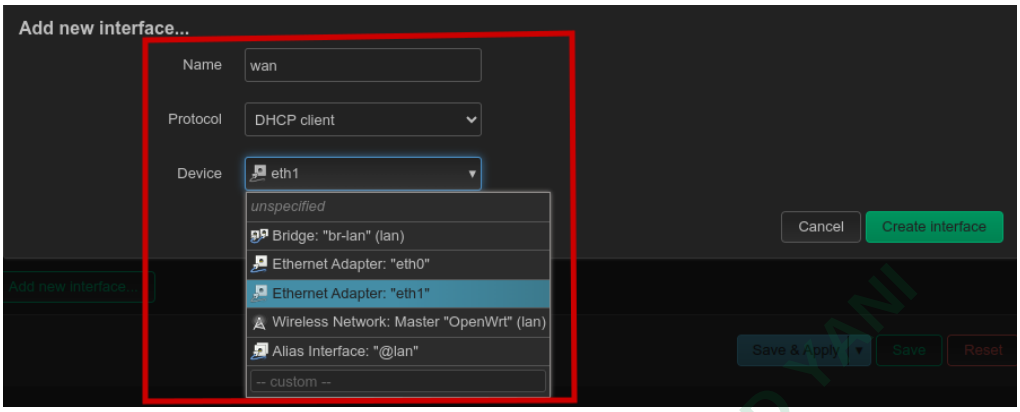
Selanjutnya, konfigurasi *Network* dilakukan dengan menjalankan perintah `vim /etc/config/network`. Kemudian, perubahan pengaturan dilakukan pada baris "config interface". Perubahan pada konfigurasi *Network* yang dilakukan adalah sebagai berikut:

```
config interface 'lan'
    option device 'br-lan'
    option proto 'static'
    option ipaddr '192.168.1.2'
    option netmask '255.255.255.0'
    option ip6assign '60'
    option dns '8.8.8.8'
    option gateway '192.168.1.1'
```

Setelah konfigurasi DHCP dan *Network* berhasil dilakukan, Raspberry Pi 4 Model B dan Laptop dihubungkan ke Router menggunakan Kabel LAN. Langkah ini bertujuan agar OpenWRT mendapatkan akses internet dari Router

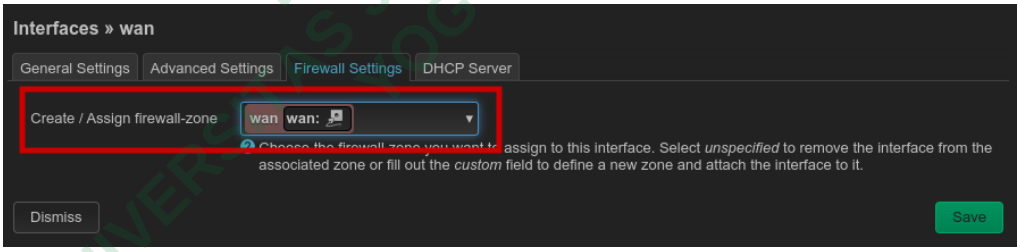
dan memungkinkan akses ke antarmuka *Lua Configuration Interface* (LuCI) OpenWRT. LuCI OpenWRT digunakan untuk mempermudah konfigurasi pada OpenWRT dalam pembuatan jaringan Wi-Fi palsu melalui antarmuka *website*. Akses LuCI OpenWRT dapat dilakukan melalui Google Chrome atau sejenisnya dengan menuliskan alamat IP dari OpenWRT yang telah diubah pada konfigurasi *Network* yaitu dengan alamat IP 192.168.1.2. Selanjutnya, proses instalasi *package* untuk mendukung koneksi internet melalui Modem GSM yang dilakukan pada menu *Software* di LuCI OpenWRT. Proses ini diawali dengan melakukan "*update list*" untuk memperbarui daftar *package* yang tersedia di OpenWRT. Ketika proses "*update list*" selesai, untuk instalasi *package* yang mendukung penggunaan Modem GSM dapat dilakukan dengan menginstal *package* "kmod-usb-net-rtl8152".

Package "kmod-usb-net-rtl8152" dipilih karena menyediakan dukungan untuk konverter *Universal Serial Bus* (USB) ke Ethernet. Dalam hal ini, *package* "kmod-usb-net-rtl8152" memungkinkan Modem GSM yang terhubung melalui USB Raspberry Pi 4 Model B dapat dikenali sebagai perangkat jaringan oleh OpenWRT. Kemudian, agar OpenWRT dapat mengenali Modem GSM diperlukan konfigurasi dengan membuat antarmuka baru untuk Modem GSM melalui menu *Interface* pada LuCI OpenWRT. Pembuatan antarmuka baru untuk Modem GSM dilakukan dengan mengisi konfigurasi sebagai berikut: "Name: wan, Protocol: DHCP Client, dan Device: eth1", sebagaimana yang ditampilkan pada Gambar 4.6.



Gambar 4.6 Pembuatan Antarmuka Baru Untuk Modem GSM

Selanjutnya, dilakukan pengaturan pada bagian *Firewall Settings* dengan tujuan untuk mengizinkan lalu lintas koneksi internet Modem GSM pada OpenWRT. Pengaturan *Firewall Settings* dilakukan dengan memilih opsi "Create/Assign firewall-zone" ke zona "wan", sebagaimana yang ditampilkan pada Gambar 4.7.



Gambar 4.7 Pengaturan *Firewall Settings*

Setelah OpenWRT berhasil mendapatkan koneksi internet dari Modem GSM, langkah berikutnya adalah mengembalikan konfigurasi DHCP dan *Network* ke pengaturan awal atau *default*. Hal ini dilakukan agar OpenWRT tidak lagi berfungsi sebagai *Client* dari Router dan alamat IP OpenWRT diubah menjadi 192.168.1.1. Selanjutnya, proses pembuatan jaringan Wi-Fi palsu pada OpenWRT untuk mensimulasikan *Evil Twin Attack* yang menyerupai jaringan Wi-Fi dengan

SSID “UNJAYA”. Pembuatan jaringan Wi-Fi palsu dilakukan dengan mengubah konfigurasi *Wireless* melalui CLI OpenWRT. Konfigurasi *Wireless* dilakukan dengan menjalankan perintah `vim /etc/config/wireless`. Perubahan konfigurasi *Wireless* pada OpenWRT yang dilakukan adalah sebagai berikut:

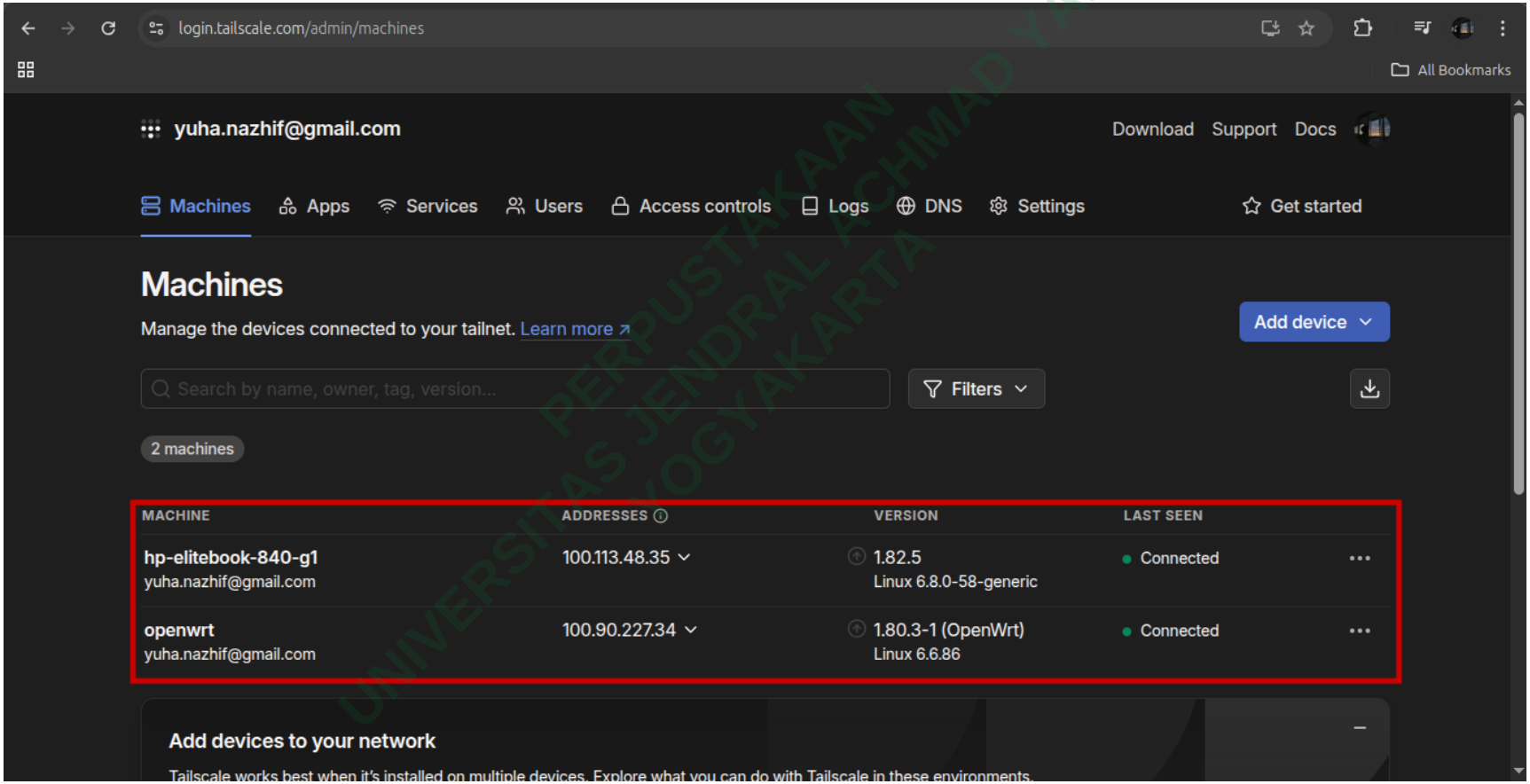
```
Config wifi-device ‘radio0’
    option type ‘mac80211’
    option path
‘platform/soc/fe300000.mmcnr/mmc_host/mmc1mmc1:001/mmc1:00
    option country ‘ID’
    option channel ‘11’
    option htmode ‘HT20’
    option hwmode ‘11g’
    option disabled ‘0’
config wifi-iface’default_radio0’
    option device ‘radio0’
    option network ‘lan’
    option mode ‘ap’
    option ssid ‘UNJAYA”
    option encryption ‘psk2’
    option key ‘*****’
```

4.3.3 Integrasi Tailscale

Dalam proses pemantauan, keamanan, dan akses terhadap OpenWRT secara jarak jauh atau *remote*, Tailscale digunakan sebagai penghubung antar perangkat jaringan dengan memanfaatkan teknologi Mesh VPN. Tailscale memungkinkan komunikasi aman antar perangkat dengan menghubungkan dua atau lebih perangkat ke dalam jaringan Tailscale yang dimana proses tersebut disebut dengan proses integrasi Tailscale.

Proses integrasi Tailscale dalam penelitian ini, diawali dengan melakukan instalasi Tailscale pada sistem pengoperasian Linux Mint yang

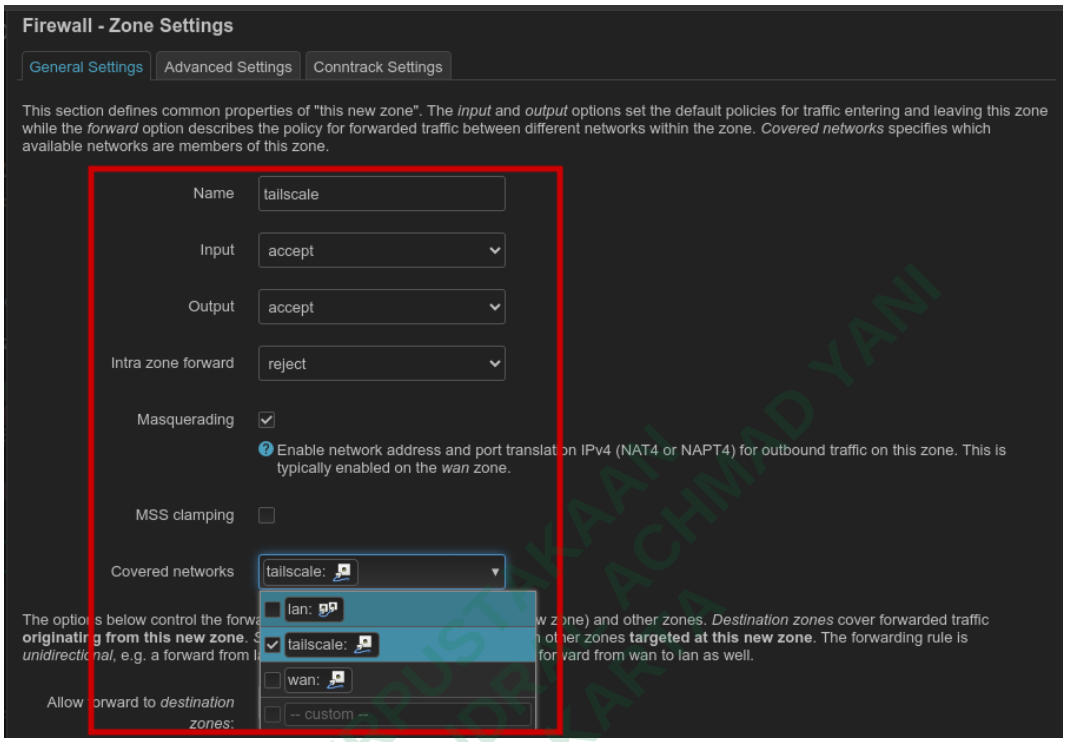
terpasang di Laptop dan OpenWRT yang terpasang di Raspberry Pi 4 Model B. Instalasi Tailscale pada sistem pengoperasian Linux Mint yang terpasang di Laptop dilakukan melalui Terminal Laptop. Sedangkan, instalasi Tailscale pada OpenWRT dilakukan melalui *Command Line Interface* (CLI) OpenWRT. Setelah instalasi Tailscale pada kedua perangkat berhasil, langkah selanjutnya adalah melakukan proses autentikasi dengan tujuan untuk menghubungkan kedua perangkat tersebut ke dalam jaringan Tailscale dimana hal ini memungkinkan perangkat saling berkomunikasi dengan menggunakan alamat *Internet Protocol* (IP) dan nama *Host* yang diberikan oleh Tailscale. Proses autentikasi dilakukan melalui Google Chrome atau sejenisnya dengan melakukan login ke akun Tailscale menggunakan akun Google atau akun lainnya yang didukung oleh Tailscale. Akun Tailscale digunakan untuk melihat daftar perangkat yang terhubung ke dalam jaringan Tailscale, sebagaimana yang ditampilkan pada Gambar 4.8.



Gambar 4.8 Daftar Perangkat Pada Akun Tailscale

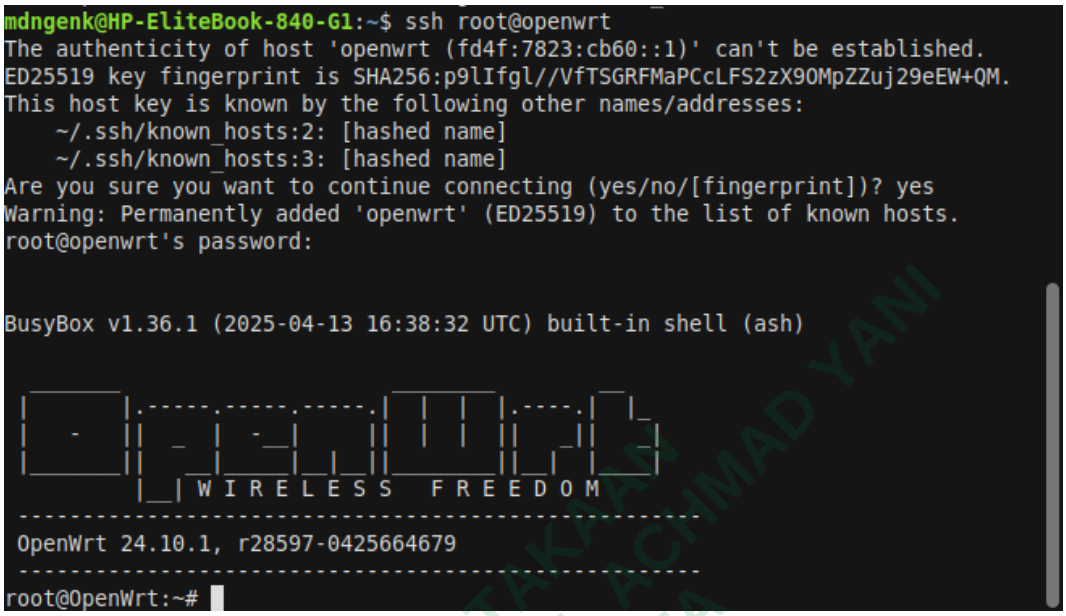
Selanjutnya, agar akses secara *remote* pada OpenWRT melalui jaringan Tailscale dapat berjalan dengan optimal, diperlukan konfigurasi pada OpenWRT yang dilakukan melalui *Lua Configuration Interface* LuCI OpenWRT dan akun Tailscale. Konfigurasi ini mencakup penambahan antarmuka baru, penambahan pengaturan *Firewall*, dan penambahan *port* 443 atau protokol *Hypertext Transfer Protocol Secure* (HTTPS). Penambahan antarmuka baru berfungsi sebagai jalur komunikasi antara OpenWRT dan jaringan Tailscale. Setelah itu, konfigurasi pengaturan *Firewall* dilakukan melalui menu *Firewall* di LuCI OpenWRT untuk mengizinkan lalu lintas dari perangkat lain di dalam jaringan Tailscale seperti akses protokol SSH dan HTTPS menggunakan alamat IP atau nama *Host* yang diberikan oleh Tailscale. Tampilan konfigurasi *Firewall* dapat dilihat pada Gambar 4.9. Langkah terakhir adalah menambahkan port 443 melalui menu *Access Controls* pada akun Tailscale dengan tujuan untuk membuka akses *remote* ke LuCI OpenWRT melalui protokol HTTPS dalam jaringan Tailscale. Konfigurasi penambahan port 433 pada menu *Access Controls* di akun Tailscale, ditunjukkan sebagai berikut:

```
{"action": "accept", "src": ["*"], "dst": ["*:22,443"]},
```



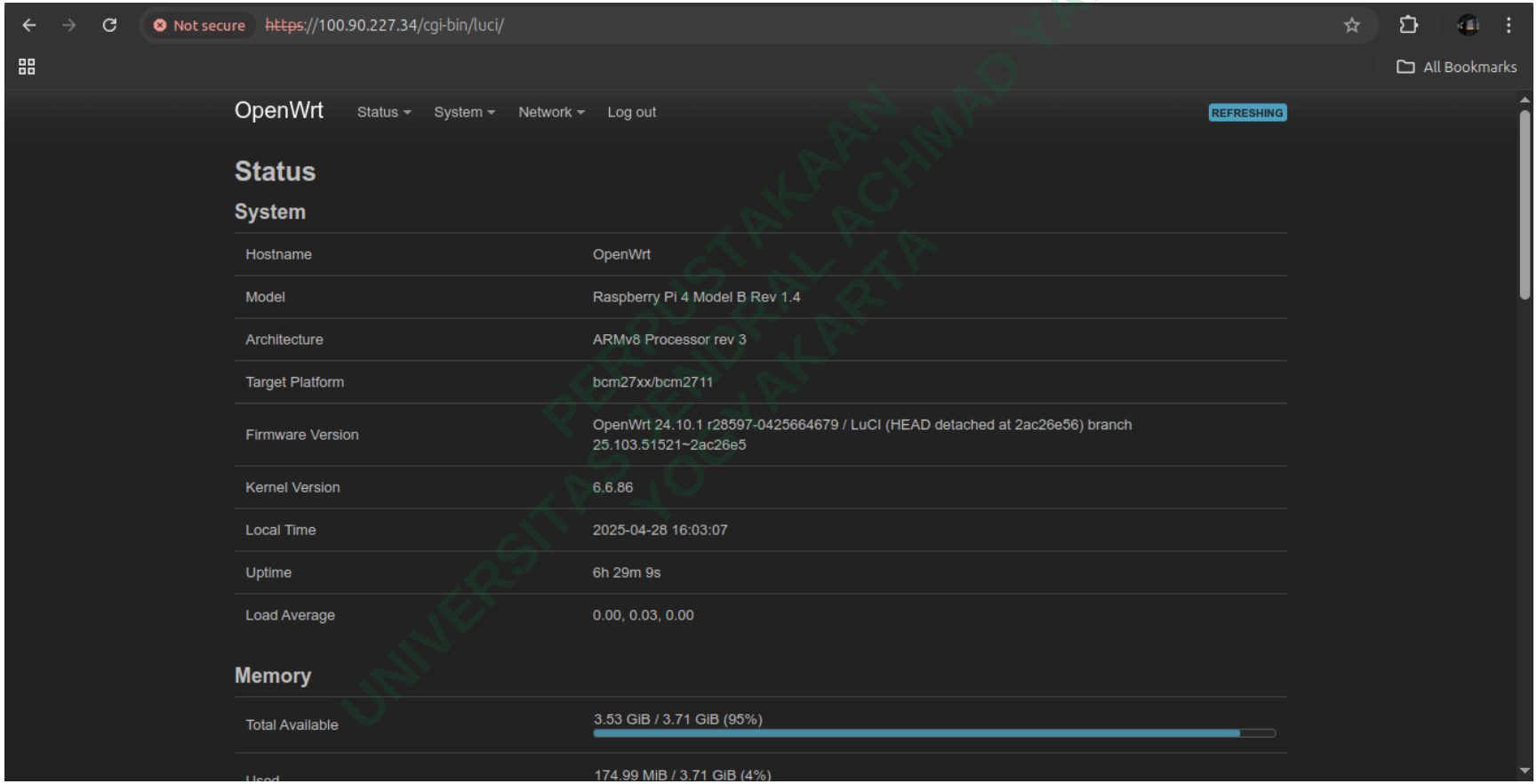
Gambar 4.9 Konfigurasi *Firewall* Untuk Tailscale

Pada saat konfigurasi telah selesai, OpenWRT dapat diakses secara *remote* dari jarak jauh menggunakan alamat IP atau nama *Host* yang diberikan oleh Tailscale melalui protokol SSH maupun HTTPS. Akses *remote* OpenWRT melalui protokol SSH dapat dilakukan dengan menuliskan nama *Host* yang diberikan oleh Tailscale pada terminal Laptop. Hasil *remote* OpenWRT melalui protokol SSH dengan menggunakan nama *Host* yang diberikan oleh Tailscale dapat dilihat pada Gambar 4.10.



Gambar 4.10 Hasil *Remote* OpenWRT Menggunakan Nama *Host* Tailscale

Kemudian, akses *remote* OpenWRT melalui protokol HTTPS dapat dilakukan dengan menggunakan alamat IP yang diberikan oleh Tailscale melalui Google Chrome atau sejenisnya, sebagaimana yang ditampilkan pada Gambar 4.11. Alamat IP atau nama *Host* yang diberikan Tailscale bersifat rahasia dan hanya dapat diakses oleh perangkat yang terhubung ke dalam jaringan Tailscale. Hal ini memungkinkan akses jaringan yang aman antar perangkat dimana hanya perangkat yang telah terautentikasi dan terdaftar ke dalam akun Tailscale yang memiliki izin untuk berkomunikasi dengan perangkat lainnya.



Gambar 4.11 Hasil *Remote* LuCI OpenWRT Menggunakan IP Tailscale

4.3.4 Konfigurasi Arkime

Pada proses analisis paket data jaringan Wi-Fi dalam penelitian ini dilakukan menggunakan Arkime. Arkime adalah sebuah *Network Traffic Analysis* (NTA) yang digunakan untuk menganalisis, menyimpan, mendeteksi aktivitas mencurigakan dan menangkap paket data (.pcap) dalam jaringan Wi-Fi. Oleh karena itu, Arkime dipilih dalam penelitian ini karena kemampuannya dalam melakukan *full packet capture* yang memungkinkan paket data yang dianalisis oleh Arkime dapat dilakukan secara *detail*.

Konfigurasi Arkime pada penelitian ini dilakukan pada sebuah Server yang menggunakan sistem pengoperasian Ubuntu Server 22.04.5 LTS. Dalam konfigurasi Arkime pada Server diawali dengan instalasi paket yang diperlukan untuk mendukung proses instalasi Arkime. Pada saat instalasi paket selesai, kemudian dilakukan penambahan kunci *GNU Privacy Guard* (GPG) untuk paket *Elasticsearch* guna memastikan paket yang diunduh asli dan tidak rusak serta dilakukan penambahan repositori *Elasticsearch*. *Elasticsearch* pada Arkime digunakan untuk menyimpan paket data jaringan Wi-Fi dalam format .pcap selama proses pengujian. Proses instalasi *Elasticsearch* dilakukan dengan menjalankan perintah `sudo apt install elasticsearch`. Setelah proses instalasi *Elasticsearch* selesai, langkah selanjutnya adalah membuat kata sandi pengguna *Elasticsearch*. Kata sandi pengguna dibuat otomatis oleh sistem yang digunakan sebagai syarat integrasi pada konfigurasi Arkime. Kemudian dilakukan proses inisialisasi dan verifikasi terhadap layanan *Elasticsearch* untuk memastikan bahwa *Elasticsearch* telah berjalan dan berfungsi dengan baik.

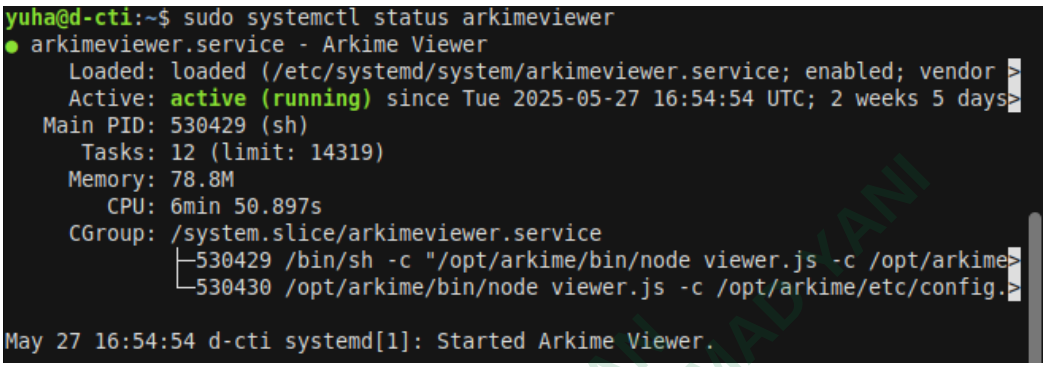
Ketika *Elasticsearch* sudah berjalan, unduh paket dan instal Arkime untuk mengintegrasikan dengan *Elasticsearch* dan melakukan konfigurasi Arkime sehingga paket data jaringan Wi-Fi dapat disimpan, dianalisis, dan ditampilkan melalui Arkime *Viewer*. Konfigurasi pada Arkime dilakukan untuk mengatur

antarmuka jaringan dan menghubungkan Arkime ke *Elasticsearch*. Konfigurasi Arkime dilakukan pada file *Configure* dengan menjalankan perintah `sudo /opt/arkime/bin/Configure`. Adapun konfigurasi Arkime yang dilakukan sebagai berikut.

```
    Found interfaces: lo;
    Semicolon ';' seperated list of interfaces to monitor
[eth1] eth0
    Install Elasticsearch server locally for demo, must have at
least 3G of memory, NOT recommended for production use (yes or
no) [no]
    OpenSearch/Elasticsearch server URL
[https://localhost:9200]
    OpenSearch/Elasticsearch user [empty is no user] elastic
    OpenSearch/Elasticsearch password [empty is no password]
password elastic
    Password to encrypt S2S and other things, don't use spaces
[must create one] password
    Arkime - Creating configuration files
    Installing sample /opt/arkime/etc/config.ini
    sed: can't read : No such file or directory
    Arkime - Installing /etc/security/limits.d/99-arkime.conf
to make core and memlock unlimited
    Download GEO files? You'll need a MaxMind account
https://arkime.com/faq#maxmind (yes or no) [yes] yes
```

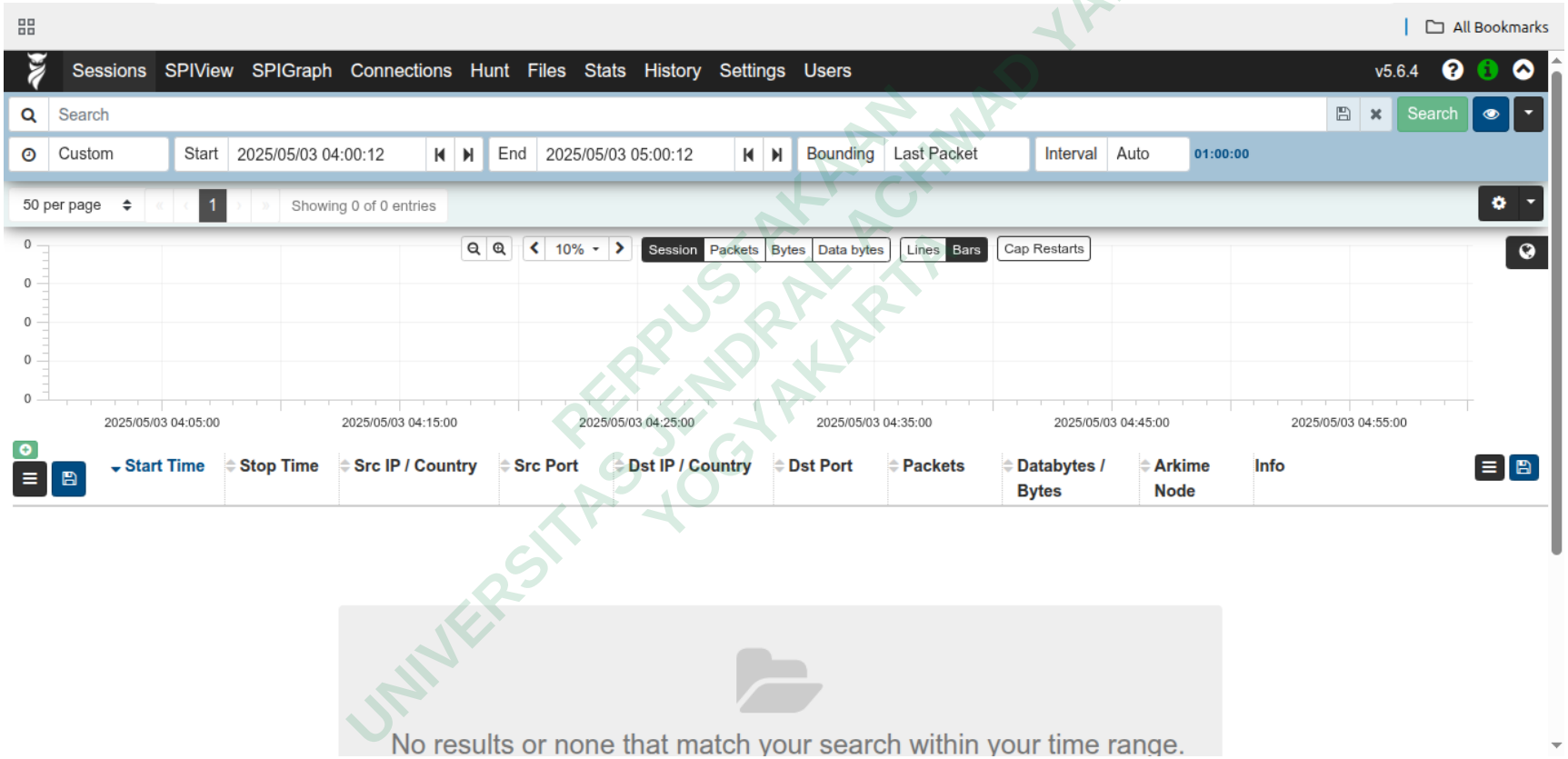
Selanjutnya, konfigurasi Arkime perlu diproses oleh *Elasticsearch* dengan memasukkan kata sandi *Elasticsearch* yang telah dibuat sebelumnya agar *database* Arkime dapat berfungsi dengan baik. Kemudian, Arkime perlu membuat akun pengguna untuk melakukan login ke antarmuka *website* Arkime atau Arkime *Viewer*. Setelah itu, aktifkan Arkime dan verifikasi layanan Arkime *Viewer* yang digunakan untuk melihat, mengidentifikasi, dan mengelola paket data jaringan berbasis antarmuka *website*. Ketika layanan Arkime *Viewer* diverifikasi dan

berhasil dijalankan maka akan muncul *active* seperti yang ditampilkan pada Gambar 4.12.



Gambar 4.12 Verifikasi Arkime *Viewer*

Akses Arkime *Viewer* dapat diakses melalui Google Chrome atau sejenisnya dengan menuliskan alamat IP Server yang diikuti oleh *port* Arkime *Viewer* melalui protokol HTTP. Port Arkime *Viewer* yang digunakan adalah *port* 8005. Tampilan antarmuka *website* Arkime *Viewer* dapat dilihat pada Gambar 4.13.



Gambar 4.13 Tampilan Antarmuka *Website* Arkime *Viewer*

4.3.5 *Mounting Secure Shell File System* (SSHFS)

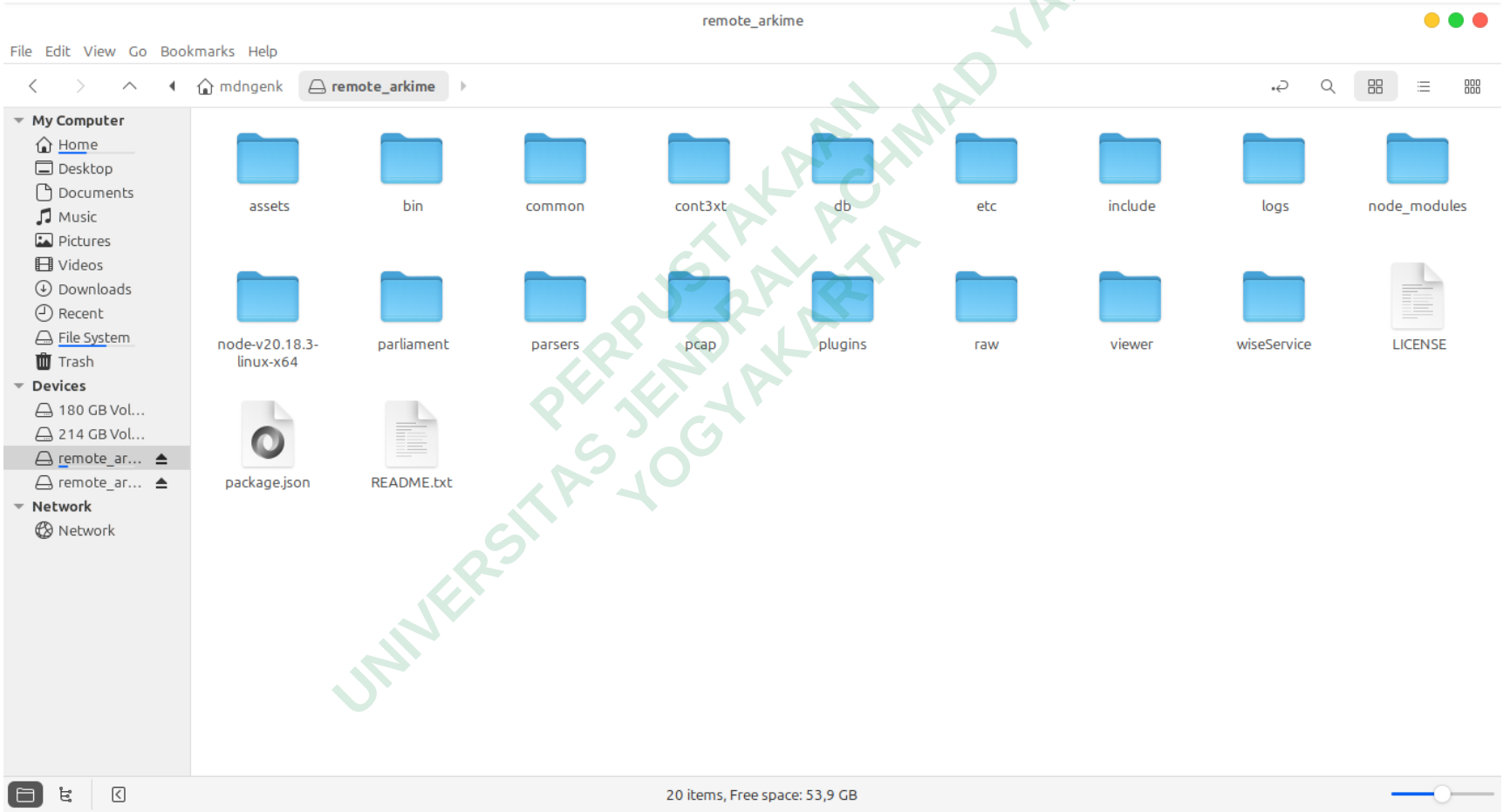
Tahap terakhir dalam perancangan dan integrasi sistem pengujian adalah proses *mounting Secure Shell File System* (SSHFS). Proses *Mounting* SSHFS dilakukan pada Laptop untuk dapat menerima dan mengirimkan file dari Arkime Server tanpa perlu memindahkan file secara manual. Proses *mounting* adalah proses untuk mengaitkan file atau direktori dari satu perangkat ke perangkat lain sehingga isi dari file atau direktori tersebut seperti bagian dari sistem lokal. Dengan SSHFS memungkinkan file dari Arkime yang terdapat di Arkime Server dipasang secara *remote* ke Laptop dengan proses *mounting* melalui protokol *Secure Shell* (SSH). Dalam hal ini, komunikasi antar perangkat dapat dilakukan secara aman dan efisien dikarenakan data yang dikirimkan akan dienkripsi selama proses pengiriman berlangsung.

Proses *mounting* SSHFS diawali dengan instalasi SSHFS yang dilakukan pada terminal Laptop. Selanjutnya, diperlukan pembuatan direktori baru pada Laptop untuk menerima isi dari direktori Arkime yang terdapat di Arkime Server. Kemudian, dibuat subdirektori di dalam direktori tersebut yang berfungsi untuk menyimpan file .pcap dari hasil proses pengujian yang dapat tersimpan juga pada direktori Arkime pada Arkime Server. Setelah itu, proses *mounting* SSHFS diperlukan dengan menambah konfigurasi ke dalam file sistem *fstab* agar proses *mounting* berjalan secara otomatis saat sistem dinyalakan ulang atau Laptop melakukan *reboot*. Konfigurasi file sistem *fstab* dilakukan dengan menjalankan perintah `sudo nano /etc/fstab` pada terminal Laptop. Adapun konfigurasi pada file sistem *fstab* sebagai berikut:

```
yuha@103.89.1.69:/opt/arkime /home/mdngenk/remote_arkime
fuse.sshfs noauto, x-
systemd.automount,_netdev,reconnect,IdentityFile=/home/mdngenk/.s
```

```
sh/id_ed25519,uid=1000,gid=1000,allow_other,default_permissions 0
0
```

Kemudian dari konfigurasi tersebut, hasil *mounting* SSHFS dapat dilihat pada direktori dan subdirektori yang sudah dibuat yang terdapat isi dari direktori Arkime yang terdapat di Arkime Server. Hasil *mounting* SSHFS dapat dilihat pada Gambar 4.14.

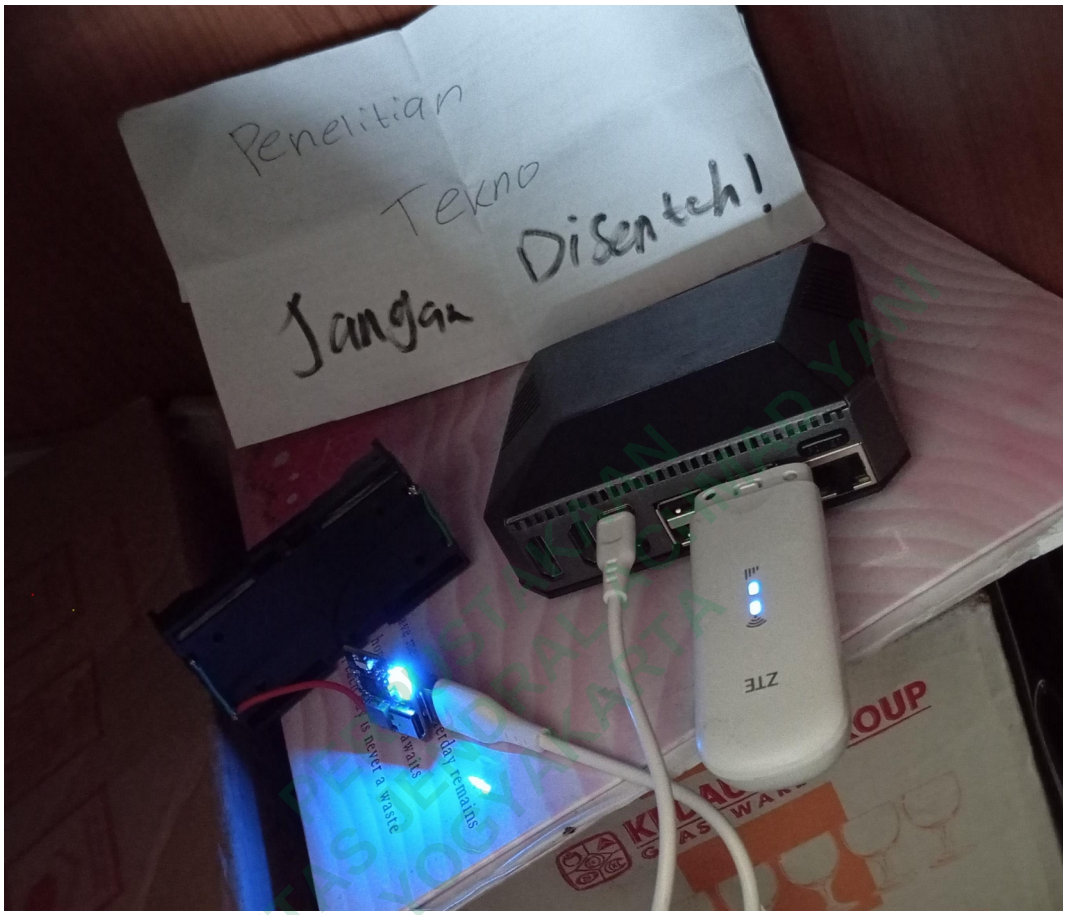


Gambar 4.14 Hasil *Mounting* SSHFS

4.4 Pengujian *Evil Twin Attack*

Pengujian *Evil Twin Attack* bertujuan untuk menguji keamanan jaringan Wi-Fi dengan mensimulasikan serangan *Evil Twin Attack* menggunakan jaringan Wi-Fi palsu berbasis OpenWRT yang terpasang pada Raspberry Pi 4 Model B dengan menyerupai jaringan Wi-Fi asli. Simulasi *Evil Twin Attack* dilakukan pada jaringan Wi-Fi dengan SSID "UNJAYA" yang terdapat di Lantai 1, Lantai 2, Lantai 3, Lantai 4, dan Gazebo Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta.

Dalam proses pengujian, diawali di Lantai 1 yang dilakukan dengan meletakkan alat uji berupa Raspberry Pi 4 Model B yang telah dikonfigurasi dengan OpenWRT dan dihubungkan dengan sumber daya berbasis Baterai. Proses pengujian di Lantai 1 dilakukan pada tanggal 23 Mei 2025 dan berlangsung pada pukul 10.37 – 12.29 atau selama 1 jam 52 menit hingga sumber daya berbasis Baterai habis. Proses pengujian di Lantai 1 dapat dilihat pada Gambar 4.15.



Gambar 4.15 Proses Pengujian Lantai 1

Kemudian, dilakukan penangkapan paket data korban di Lantai 1 dilakukan dengan menjalankan *tools tcpdump*. *Tools tcpdump* dipilih karena kemampuannya dalam menangkap paket data dalam lalu lintas jaringan Wi-Fi secara *real time* dan menyimpan hasil tangkapan paket data dalam format .pcap. Proses penangkapan paket data di Lantai 1 dilakukan pada terminal Laptop dengan menjalankan perintah `ssh root@100.90.227.34 tcpdump -i br-lan -w - 'not port 22 and not port 37823' | tee`

`/home/mdngenk/remote_arkime/pcap/lantai1.pcap`. Adapun penjelasan dari perintah tersebut, sebagai berikut:

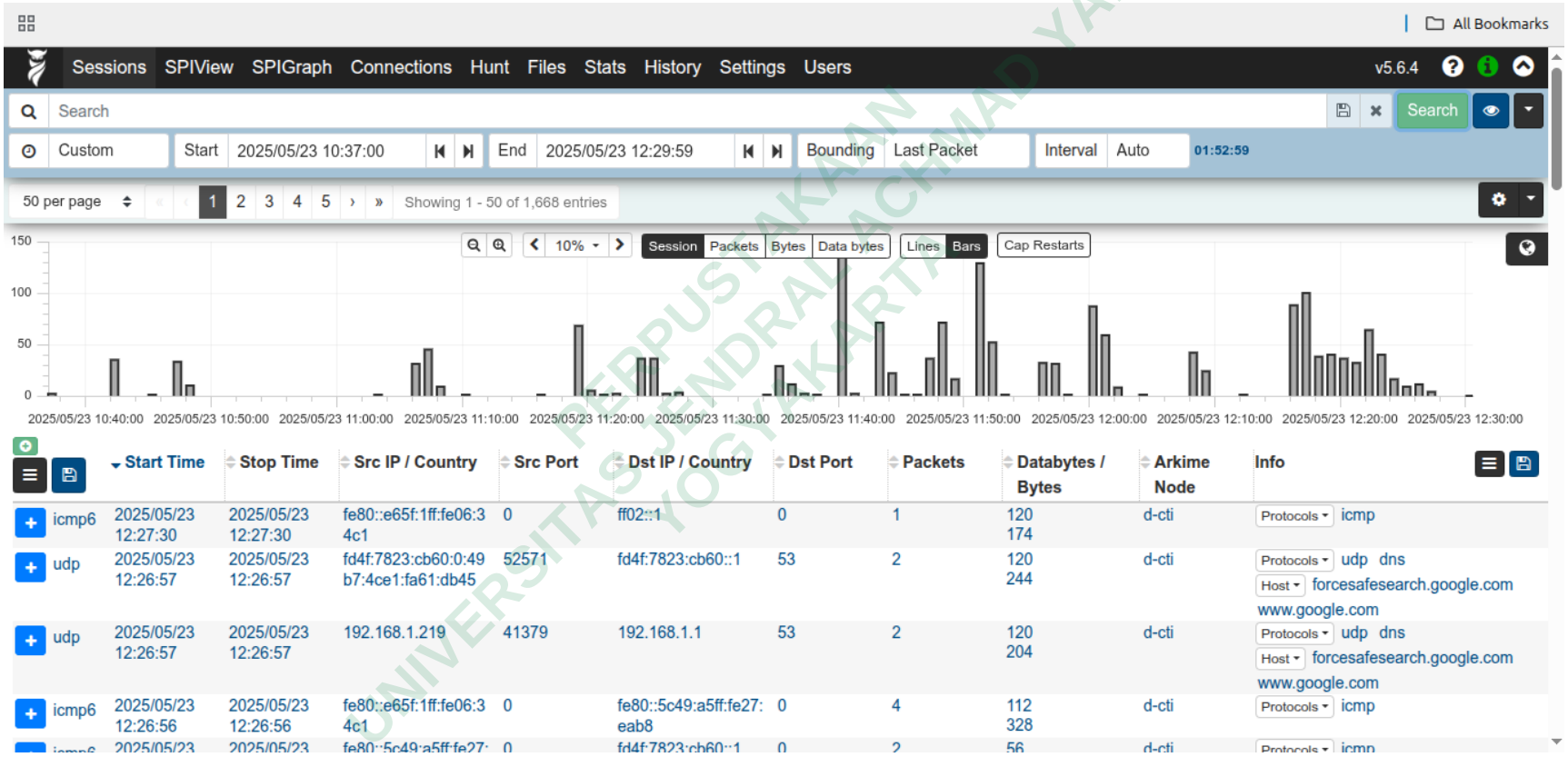
1. `ssh root@100.90.227.34` digunakan untuk mengakses OpenWRT secara *remote* menggunakan alamat IP yang diberikan oleh Tailscale.
2. `tcpdump -i br-lan` digunakan untuk menjalankan *tools tcpdump* dan menangkap lalu lintas jaringan pada interface br-lan. Interface br-lan merupakan interface jaringan pada OpenWRT yang berfungsi sebagai penghubung perangkat – perangkat ke jaringan OpenWRT atau dalam hal ini adalah jaringan Wi-Fi palsu yang disimulasikan dalam pengujian ini.
3. `-w -` digunakan untuk proses menulis hasil tangkapan paket data dalam format .pcap dan dikirim langsung ke Laptop melalui protokol SSH.
4. `'not port 22 and not port '37283'` digunakan agar proses penangkapan paket data tidak menangkap *port* 22 dan *port* 37283. *Port* 22 merupakan *port* dari SSH dan *port* 37283 adalah *port* dari Tailscale yang digunakan oleh OpenWRT.
5. `| tee /home/mdngenk/remote_arkime/pcap/lantai1.pcap` digunakan untuk mengalirkan dan menyimpan hasil tangkapan paket data ke dalam file .pcap yang disimpan pada subdirektori "pcap" di dalam direktori "remote_arkime".

Setelah itu, ketika proses pengujian di Lantai 1 telah menghasilkan file tangkapan paket data dalam format .pcap yang tersimpan pada subdirektori "pcap" di dalam direktori "remote_arkime", langkah selanjutnya adalah melakukan proses *import* hasil file tangkapan paket data Lantai 1 dalam format .pcap melalui Arkime Server. Dengan melalui *mounting* SSHFS pada tahap sebelumnya, hasil file tangkapan paket data juga tersimpan dalam Arkime Server. Proses *import* hasil tangkapan paket data Lantai 1 yang dilakukan melalui Arkime Server bertujuan untuk memproses, menyimpan, dan menampilkan hasil file tangkapan

paket data pada Arkime *Viewer*. Proses *import* file hasil paket data Lantai 1 dilakukan dengan menjalankan perintah `/opt/arkime/bin/capture -r /opt/arkime/pcap/lantai1.pcap`. Adapun penjelasan dari perintah tersebut, sebagai berikut:

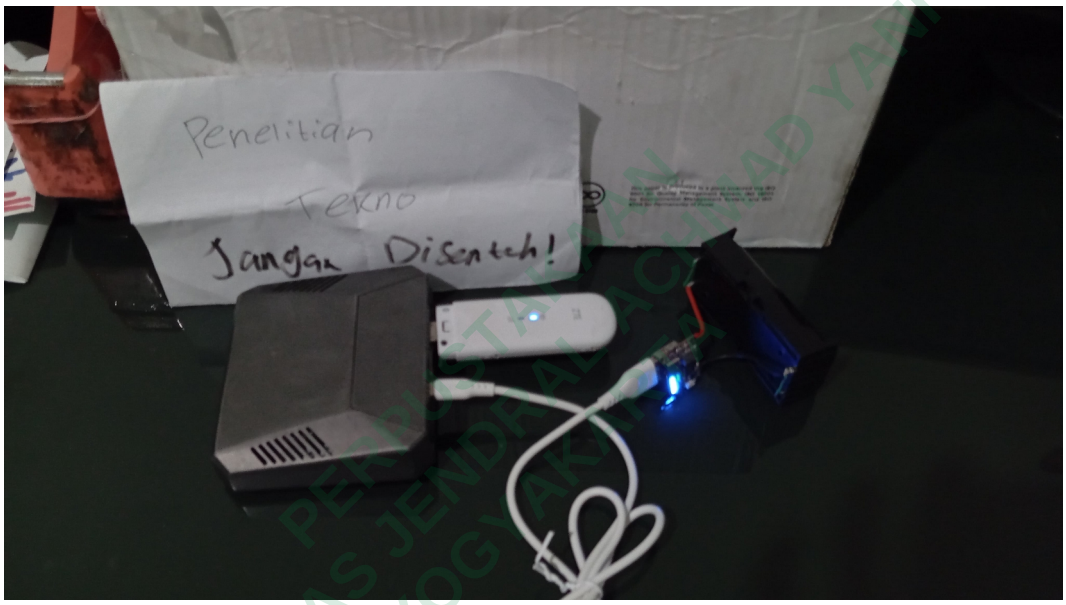
1. `/opt/arkime/bin/capture` adalah program capture yang dimiliki oleh Arkime untuk memproses paket data jaringan.
2. `-r` adalah kode yang digunakan untuk membaca data dari file .pcap yang akan diproses.
3. `/opt/arkime/pcap/lantai1.pcap` adalah alamat dari file .pcap yang berisi hasil tangkapan paket data yang akan dianalisis.

Hasil *import* tangkapan paket data di Lantai 1 dapat dilihat melalui Arkime *Viewer* menggunakan Google Chrome atau sejenisnya dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian yang dilakukan di Lantai 1. Hasil Arkime *Viewer* di Lantai 1 dapat dilihat pada Gambar 4.16.



Gambar 4.16 Hasil Arkime *Viewer* Lantai 1

Selanjutnya, proses pengujian dilakukan di Lantai 2 yang dilakukan dengan meletakkan alat uji dan sumber daya di area sekitar Lantai 2. Proses pengujian di Lantai 2 dilakukan pada tanggal 23 Mei 2025 dan berlangsung pada pukul 14.15 – 16.01 atau selama 1 jam 46 menit selama sumber daya berbasis Baterai habis. Proses Pengujian di Lantai 2 dapat dilihat pada Gambar 4.17.



Gambar 4.17 Proses Pengujian di Lantai 2

Dalam proses pengujian di Lantai 2 berlangsung, dilakukan penangkapan paket data korban menggunakan *tools tcpdump* dengan menjalankan perintah `ssh root@100.90.227.34 tcpdump -i br-lan -w - 'not port 22 and not port 37823' | tee /home/mdngenk/remote_arkime/pcap/lantai2.pcap` yang dilakukan pada terminal Laptop. Kemudian, hasil tangkapan paket data dalam format .pcap di Lantai 2 akan tersimpan pada subdirektori "pcap" di dalam direktori "remote_arkime" dan pada Arkime Server melalui *mounting* SSHFS. Selanjutnya, dilakukan proses *import* hasil tangkapan paket data di Lantai 2 melalui Arkime Server dengan menjalankan perintah `/opt/arkime/bin/capture`

`-r /opt/arkime/pcap/lantai2.pcap`. Setelah itu, hasil tangkapan paket data di Lantai 2 dapat dilihat melalui Arkime *Viewer* menggunakan Google Chrome atau sejenisnya dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian yang dilakukan di Lantai 2.

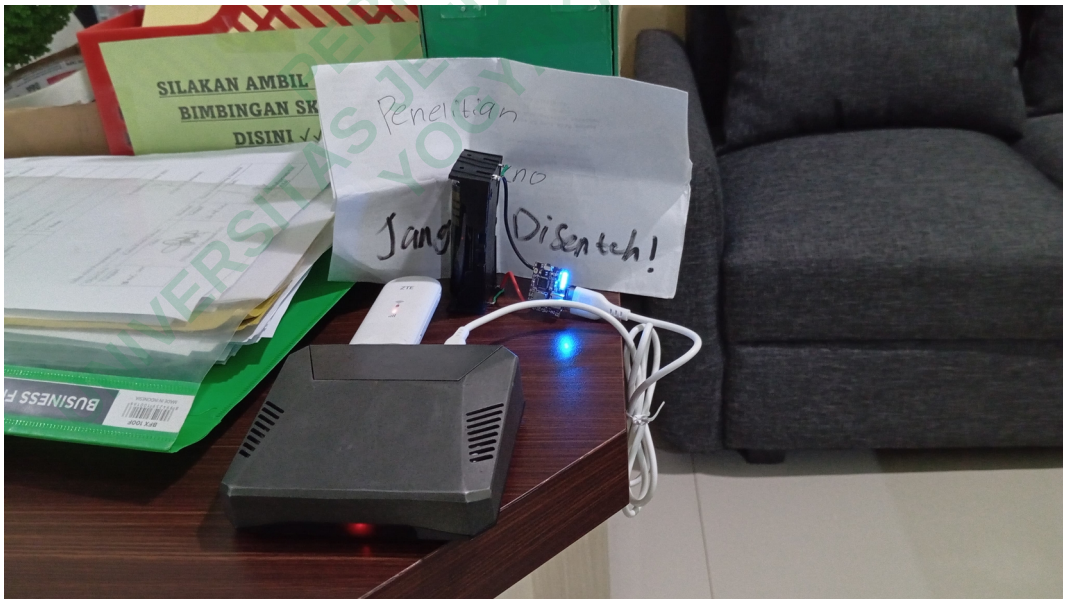
Proses pengujian berikutnya dilakukan di Lantai 3 dengan meletakkan alat uji dan sumber daya di area sekitar Lantai 3. Proses pengujian di Lantai 3 dilakukan pada tanggal 26 Mei 2025 dan berlangsung pada pukul 11.25 – 13.03 atau selama 1 jam 38 menit selama sumber daya berbasis Baterai habis. Proses Pengujian di Lantai 3 dapat dilihat pada Gambar 4.18.

Gambar 4.18 Proses Pengujian di Lantai 3

Dalam proses pengujian di Lantai 3 untuk menangkap paket data korban dilakukan menggunakan *tools tcpdump* dengan menjalankan perintah `root@100.90.227.34 tcpdump -i br-lan -w - 'not port 22 and not port 37823' | tee /home/mdngenk/remote_arkime/pcap/lantai3.pcap` yang dilakukan pada terminal Laptop. Kemudian, hasil tangkapan paket data di

Lantai 3 akan tersimpan pada subdirektori “pcap” di dalam direktori “remote_arkime” dan pada Arkime Server melalui *mounting* SSHFS. Selanjutnya, dilakukan proses *import* hasil tangkapan paket data di Lantai 3 melalui Arkime Server dengan menjalankan perintah `/opt/arkime/bin/capture -r /opt/arkime/pcap/lantai3.pcap`. Setelah itu, hasil tangkapan paket data dalam format .pcap di Lantai 3 dapat dilihat melalui Arkime *Viewer* menggunakan Google Chrome atau sejenisnya dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian yang dilakukan di Lantai 3.

Selanjutnya, proses pengujian dilakukan di Lantai 4 dengan meletakkan alat uji dan sumber daya di area sekitar Lantai 4. Proses pengujian di Lantai 4 dilakukan pada tanggal 27 Mei 2025 dan berlangsung pada pukul 09.30 – 11.19 atau selama 1 jam 49 menit selama sumber daya berbasis Baterai habis. Proses Pengujian di Lantai 4 dapat dilihat pada Gambar 4.19.



Gambar 4.19 Proses Pengujian di Lantai 4

Dalam proses pengujian di Lantai 4 untuk menangkap paket data korban dilakukan menggunakan *tools tcpdump* dengan menjalankan perintah `root@100.90.227.34 tcpdump -i br-lan -w - 'not port 22 and not port 37823' | tee /home/mdngenk/remote_arkime/pcap/lantai4.pcap` yang dilakukan pada terminal Laptop. Kemudian, hasil tangkapan paket data dalam format .pcap di Lantai 4 akan tersimpan pada subdirektori "pcap" di dalam direktori "remote_arkime" dan pada Arkime Server melalui *mounting* SSHFS. Selanjutnya, dilakukan proses *import* hasil tangkapan paket data di Lantai 4 melalui Arkime Server dengan menjalankan perintah `/opt/arkime/bin/capture -r /opt/arkime/pcap/lantai4.pcap`. Setelah itu, hasil tangkapan paket data di Lantai 4 dapat dilihat melalui Arkime *Viewer* menggunakan Google Chrome atau sejenisnya dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian yang dilakukan di Lantai 4.

Proses pengujian terakhir dilakukan di Gazebo dengan meletakkan alat uji dan sumber daya di area sekitar Gazebo. Proses pengujian di Gazebo dilakukan pada tanggal 27 Mei 2025 dan berlangsung pada pukul 14.25 – 15.58 atau selama 1 jam 33 menit selama sumber daya berbasis Baterai habis. Proses Pengujian di Gazebo dapat dilihat pada Gambar 4.20.

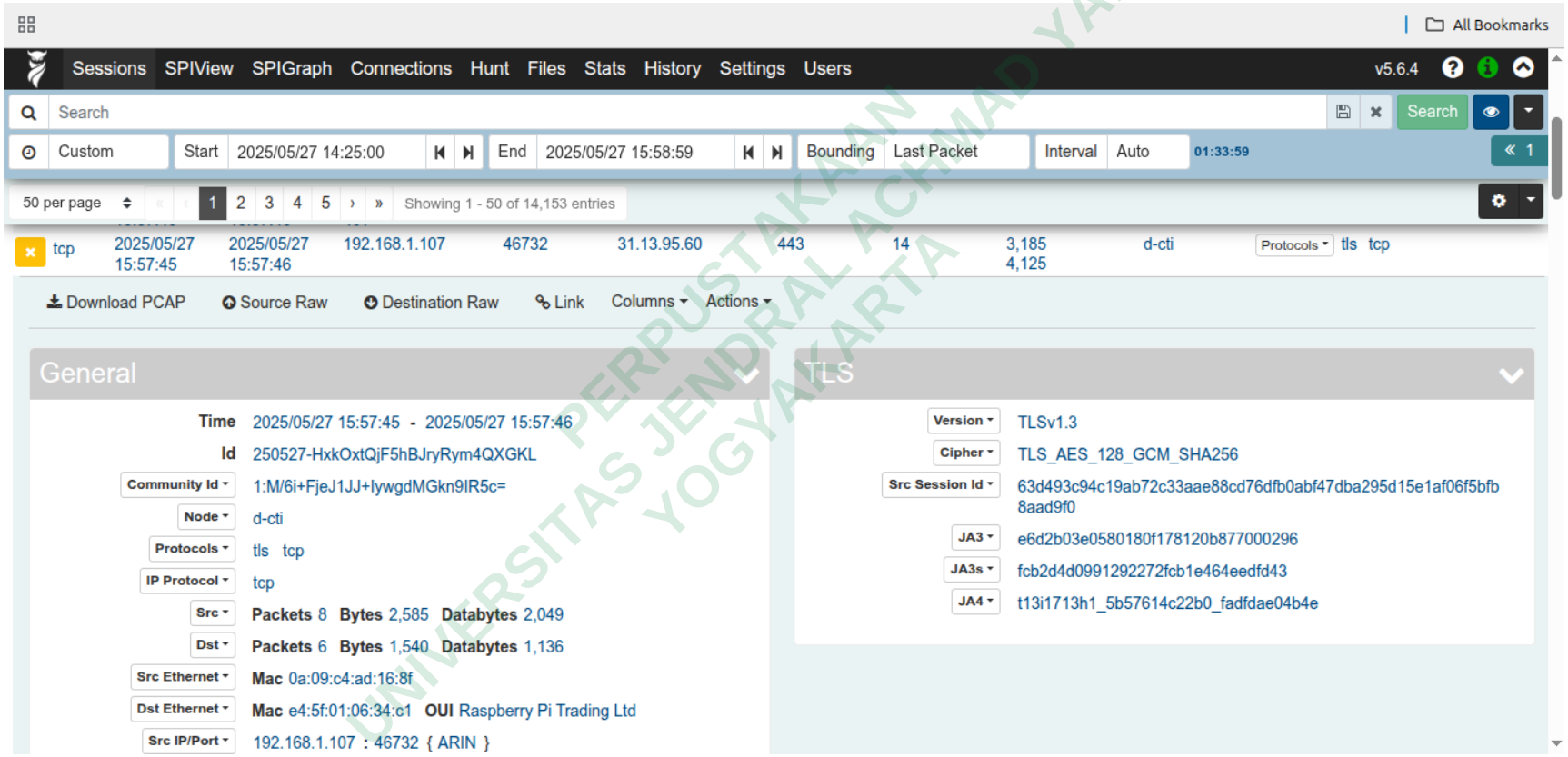
Gambar 4.20 Proses Pengujian di Gazebo

Dalam proses pengujian di Gazebo proses penangkapan paket data korban dilakukan menggunakan *tools tcpdump* dengan menjalankan perintah `root@100.90.227.34 tcpdump -i br-lan -w - 'not port 22 and not port 37823' | tee /home/mdngenk/remote_arkime/pcap/gazebo.pcap` yang dilakukan pada terminal Laptop. Kemudian, hasil tangkapan paket data dalam format .pcap di Gazebo akan tersimpan pada subdirektori "pcap" di dalam direktori "remote_arkime" dan pada Arkime Server melalui *mounting* SSHFS. Selanjutnya, dilakukan proses *import* hasil tangkapan paket data di Gazebo melalui Arkime Server dengan menjalankan perintah `/opt/arkime/bin/capture -r /opt/arkime/pcap/gazebo.pcap`. Setelah itu, hasil tangkapan paket data di Gazebo dapat dilihat melalui Arkime *Viewer* menggunakan Google Chrome atau sejenisnya dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian yang dilakukan di Gazebo.

4.5 Analisis Paket Data Hasil Pengujian

Analisis dilakukan terhadap hasil file tangkapan paket data yang diperoleh selama proses pengujian *Evil Twin Attack* dengan membuat jaringan Wi-Fi palsu SSID "UNJAYA" yang diimplementasikan pada Lantai 1, Lantai 2, Lantai 3, Lantai 4, dan Gazebo di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta. File tangkapan dalam format .pcap yang di *import* ke Arkime pada tahapan sebelumnya akan dianalisis melalui Arkime *Viewer*. Proses analisis bertujuan untuk mengidentifikasi aktivitas korban yang secara tidak sadar telah terhubung ke jaringan Wi-Fi palsu yang telah dibuat dalam tahap sebelumnya. Dalam proses analisis, dilakukan juga identifikasi protokol yang rentan atau berbahaya yang diakses oleh korban. Jenis protokol yang memiliki kerentanan dalam penelitian ini berfokus pada protokol *Hypertext Transfer Protocol* (HTTP). Kemudian, pada protokol HTTP dilakukan pencarian informasi data sensitif dari korban seperti *username* dan *password* yang mungkin terkirim melalui protokol tersebut.

Proses analisis menggunakan Arkime diawali dengan mengidentifikasi berapa jumlah korban yang terjebak dalam simulasi *Evil Twin Attack*. Identifikasi jumlah korban ini bertujuan untuk mengetahui seberapa jauh serangan *Evil Twin Attack* berhasil dilakukan. Dalam identifikasi jumlah korban dilakukan dalam Arkime *Viewer* pada fitur *Sessions* dengan menyesuaikan *Beginning Time* dan *Stop Time* sesuai dengan periode pengujian di setiap lokasi pengujian serta menekan tombol + yang tersedia untuk menampilkan detail informasi dari korban seperti alamat *Internet Protocol* (IP) dan *Media Access Control* (MAC) *Address*, sebagaimana yang ditampilkan pada salah satu lokasi pengujian dalam Gambar 4.21.



Gambar 4.21 Identifikasi Jumlah Korban Pada Fitur *Sessions*

Identifikasi jumlah korban yang terjebak ke dalam jaringan Wi-Fi palsu di setiap lokasi pengujian pada fitur *Sessions* di Arkime *Viewer* menunjukkan bahwa terdapat jumlah korban beserta alamat IP korban dan MAC *Address*. Hasil identifikasi jumlah korban menunjukkan di Lantai 1 terdapat 14 korban, Lantai 2 10 korban, Lantai 3 22 korban, Lantai 4 4 korban, dan Gazebo 52 korban, sebagaimana yang ditampilkan pada pada Tabel 4.1.

Tabel 4.1 Hasil Identifikasi Jumlah Korban

Lokasi	Tanggal Pengujian	Waktu Pengujian	Jumlah Korban	IP Korban	MAC *Address*
Lantai 1	23 Mei 2025	10.37 – 12.29	14	192.168.1.105	5c:d0:6e:3c:a0:e5
				192.168.1.112	a0:29:42:ed:ec:16
				192.168.1.114	da:95:f7:e4:dc:d2
				192.168.1.131	a6:bb:06:f9:6e:03
				192.168.1.135	5a:94:d8:04:63:7c
				192.168.1.136	0e:93:1e:73:07:32
				192.168.1.186	d2:d7:da:4f:c7:35
				192.168.1.187	14:ac:60:77:05:37
				192.168.1.198	fa:d0:13:2c:b5:92
				192.168.1.210	26:33:16:53:91:73
				192.168.1.219	5e:49:a5:27:ea:b8
				192.168.1.221	aa:fc:eb:a5:65:ee
				192.168.1.228	f6:03:19:ed:45:ec
				192.168.1.248	4a:1e:7c:3d:22:ef
Lantai 2	23 Mei 2025	14.15 – 16.01	10	192.168.1.149	12:96:9e:48:25:c4
				192.168.1.160	da:5b:01:fb:46:f7
				192.168.1.180	de:33:da:c3:7f:5b
				192.168.1.204	fe:8c:59:57:4d:01
				192.168.1.214	06:89:8d:6a:2b:5b

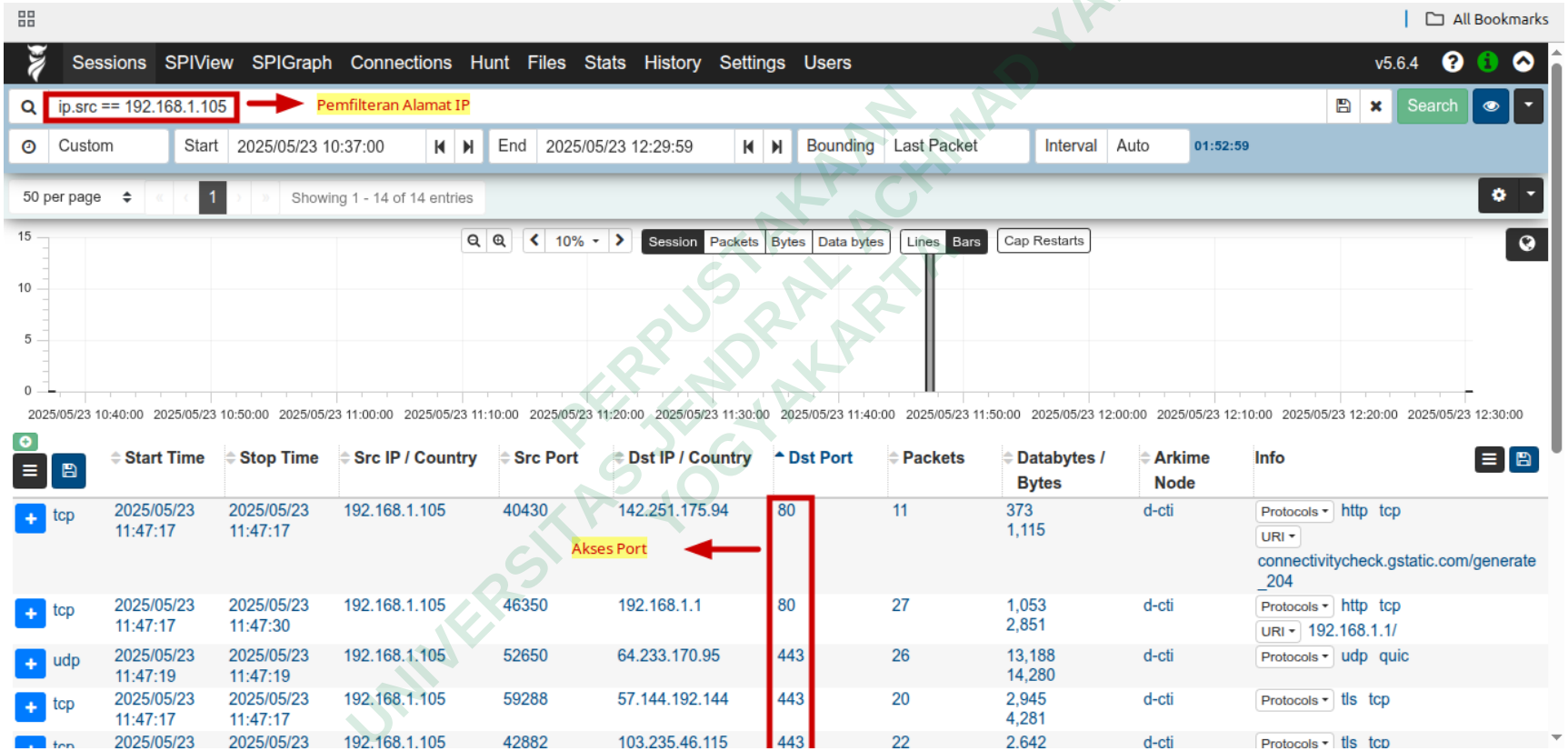
Lokasi	Tanggal Pengujian	Waktu Pengujian	Jumlah Korban	IP Korban	MAC *Address*
				192.168.1.226	b2:a6:b0:f9:3d:3e
				192.168.1.231	2a:1b:c5:a7:31:35
				192.168.1.234	fa:cf:1e:21:32:c6
				192.168.1.241	3e:71:db:55:92:98
				192.168.1.247	ca:55:84:4e:78:7e
Lantai 3	26 Mei 2025	11.25 – 13.03	22	192.168.1.102	a6:c3:73:9f:6f:22
				192.168.1.105	ca:0f:23:d8:e3:4e
				192.168.1.110	86:71:38:cb:83:a3
				192.168.1.123	06:ae:cd:52:d2:aa
				192.168.1.128	12:b1:ed:fb:1c:3b
				192.168.1.152	98:c8:b8:8d:fe:1b
				192.168.1.155	b2:80:41:83:31:d2
				192.168.1.164	3c:e9:f7:db:ff:b0
				192.168.1.167	8e:47:15:6a:03:c8
				192.168.1.168	16:88:9b:93:dc:6c
				192.168.1.170	e0:1f:88:43:7e:ba
				192.168.1.171	6a:2a:64:41:3f:21
				192.168.1.188	16:c2:4f:a0:ca:31
				192.168.1.192	f2:08:a0:a0:20:3e
				192.168.1.196	52:ca:3c:f0:c5:c3
				192.168.1.216	1e:13:c5:4b:8f:ee
				192.168.1.219	ee:ee:2e:4c:f8:cd
				192.168.1.221	8e:d9:d0:6a:58:5e
				192.168.1.229	5e:ef:ab:70:86:e7
				192.168.1.233	b6:68:09:ae:3c:fe
				192.168.1.234	4a:ad:db:e4:aa:18

Lokasi	Tanggal Pengujian	Waktu Pengujian	Jumlah Korban	IP Korban	MAC *Address*
				192.168.1.242	2e:84:8c:2b:46:cf
Lantai 4	27 Mei 2025	09.30 – 11.19	4	192.168.1.122	9a:4f:da:bf:05:27
				192.168.1.140	7a:e5:27:4a:2f:51
				192.168.1.160	8c:aa:ce:2c:40:d6
				192.168.1.216	10:08:b1:ae:18:91
Gazebo	27 Mei 2025	14.25 – 15.58	52	192.168.1.100	e8:bf:b8:01:79:5d
				192.168.1.101	e0:1f:88:4d:70:34
				192.168.1.105	ea:66:99:b8:01:9d
				192.168.1.106	96:46:f3:58:00:81
				192.168.1.107	0a:09:c4:ad:16:8f
				192.168.1.114	74:f2:fa:da:2f:07
				192.168.1.116	3e:aa:c6:a1:1d:f2
				192.168.1.117	f8:9e:94:d8:28:d6
				192.168.1.121	7e:7a:c9:89:fb:cc
				192.168.1.122	5e:81:81:1c:bf:93
				192.168.1.124	1e:36:41:2b:65:4d
				192.168.1.125	7e:f6:a6:02:83:8a
				192.168.1.126	48:fd:a3:07:47:40
				192.168.1.131	00:45:e2:e9:e2:29
				192.168.1.132	1e:ae:a1:55:85:df
				192.168.1.134	3e:83:33:25:7b:60
				192.168.1.135	5a:94:d8:04:63:7c
				192.168.1.136	12:d6:f4:d4:ef:8f
				192.168.1.142	62:11:ef:c3:de:99
				192.168.1.143	9a:33:ec:ae:74:b6
				192.168.1.144	ce:41:8e:00:a0:23

Lokasi	Tanggal Pengujian	Waktu Pengujian	Jumlah Korban	IP Korban	MAC *Address*
				192.168.1.146	1a:12:ad:c0:5e:5d
				192.168.1.154	74:f2:fa:da:bb:ed
				192.168.1.156	06:04:b4:c0:e6:1c
				192.168.1.157	82:37:38:10:31:a2
				192.168.1.158	5a:66:8a:26:fb:95
				192.168.1.160	90:e8:68:c7:86:a9
				192.168.1.161	06:e6:b4:c6:9b:ae
				192.168.1.162	6e:93:4f:29:90:ee
				192.168.1.163	58:fb:84:76:6c:9a
				192.168.1.164	fa:80:dc:24:2d:e2
				192.168.1.171	be:77:5b:3e:71:4e
				192.168.1.178	d2:ff:a3:9a:93:67
				192.168.1.185	0e:5b:52:7a:d1:df
				192.168.1.186	32:ec:b9:87:20:49
				192.168.1.189	be:2c:4f:02:f9:85
				192.168.1.193	5a:d3:1c:5a:44:5e
				192.168.1.194	ea:79:3b:80:fc:28
				192.168.1.197	0a:f7:f2:29:57:bc
				192.168.1.201	10:68:38:4e:63:3a
				192.168.1.202	c6:ab:35:81:77:b8
				192.168.1.211	b2:29:33:59:e7:5b
				192.168.1.215	ae:f9:0c:dc:18:72
				192.168.1.223	6e:95:fc:af:a5:72
				192.168.1.226	b2:a6:b0:f9:3d:3e
				192.168.1.227	06:de:ae:0e:c4:13
				192.168.1.228	f6:03:19:ed:45:ec

Lokasi	Tanggal Pengujian	Waktu Pengujian	Jumlah Korban	IP Korban	MAC *Address*
				192.168.1.229	aa:b7:de:22:a2:47
				192.168.1.231	ea:e3:36:1e:77:57
				192.168.1.232	9c:5f:5a:94:de:c1
				192.168.1.245	9c:f5:31:89:47:bf
				192.168.1.246	66:16:41:29:48:9a

Selanjutnya, dari hasil identifikasi jumlah korban yang ditampilkan pada Tabel 4.1 menunjukkan bahwa simulasi *Evil Twin Attack* yang dilakukan pada setiap lokasi pengujian berhasil dijalankan. Berdasarkan hasil tersebut, alamat IP yang teridentifikasi akan dianalisis lebih lanjut untuk mengetahui *port* yang diakses oleh masing – masing alamat IP yang ditampilkan pada Tabel 4.1. Dalam analasis untuk mengetahui *port* yang diakses oleh masing – masing alamat IP dilakukan pada fitur *Sessions* dengan melakukan pemfilteran alamat IP yang akan dianalisis, sebagaimana yang ditampilkan dengan salah satu alamat IP pada salah satu lokasi pengujian dalam Gambar 4.22.



Gambar 4.22 Identifikasi Akses *Port* Pada Alamat IP Korban

Identifikasi akses port pada alamat IP korban yang dilakukan dengan memfilter alamat IP korban pada fitur *Sessions* di Arkime *Viewer* menunjukkan terdapat hasil akses *port* yang dilakukan oleh alamat IP korban. Hasil identifikasi akses *port* pada alamat IP korban di setiap lokasi pengujian dapat dilihat pada Tabel 4.2.

Tabel 4.2 Hasil Identifikasi Akses *Port* Pada Alamat IP Korban

Lokasi	IP Korban	MAC *Address*	Akses *Port*
Lantai 1	192.168.1.105	5c:d0:6e:3c:a0:e5	80, 443, 5222, 5228, 5353
	192.168.1.112	a0:29:42:ed:ec:16	53, 80, 137, 443, 5222, 5353
	192.168.1.114	da:95:f7:e4:dc:d2	53, 80, 443, 3480, 3481, 3482, 5222, 5222, 5353, 36773, 60553
	192.168.1.131	a6:bb:06:f9:6e:03	53, 80, 123, 443, 853, 2002, 5228, 5353
	192.168.1.135	5a:94:d8:04:63:7c	53, 80, 443, 5222, 5223, 5353
	192.168.1.136	0e:93:1e:73:07:32	53, 80, 443, 5353
	192.168.1.186	d2:d7:da:4f:c7:35	7, 53, 80, 123, 443, 853, 1900, 5222, 5228, 65000
	192.168.1.187	14:ac:60:77:05:37	53, 80, 137, 443, 5353, 5355
	192.168.1.198	fa:d0:13:2c:b5:92	53, 80, 443, 5223, 5353
	192.168.1.210	26:33:16:53:91:73	53, 123, 443, 3480, 3481, 3482, 5223, 5353
	192.168.1.219	5e:49:a5:27:ea:b8	53, 80, 443, 853,

Lokasi	IP Korban	MAC *Address*	Akses *Port*
			5228
	192.168.1.221	aa:fc:eb:a5:65:ee	53, 80, 443, 5222, 5223, 5353
	192.168.1.228	f6:03:19:ed:45:ec	53, 80, 443, 993, 5223, 5353
	192.168.1.248	4a:1e:7c:3d:22:ef	80, 443, 5222, 5228, 5353, 8569, 8571, 8572, 8747, 8760, 8772, 8790, 9078, 9094, 9681, 12509, 12512, 12518
Lantai 2	192.168.1.149	12:96:9e:48:25:c4	53, 80, 443, 853, 5353
	192.168.1.160	da:5b:01:fb:46:f7	53, 80, 123, 443, 5222, 5223, 5353
	192.168.1.180	de:33:da:c3:7f:5b	53, 80, 123, 443, 5222, 5223, 5353
	192.168.1.204	fe:8c:59:57:4d:01	53, 80, 443, 5223, 5353
	192.168.1.214	06:89:8d:6a:2b:5b	53, 80, 443, 5223, 5353
	192.168.1.226	b2:a6:b0:f9:3d:3e	53, 80, 443, 3480, 3481, 3482, 5222, 5353, 7215, 8654, 8655, 8658, 8659, 8660, 8662, 8664, 8665, 8669, 8671, 8672, 8674, 8675, 8677, 8678, 8716, 8718, 8723, 8726, 9681, 27859
	192.168.1.231	2a:1b:c5:a7:31:35	80, 443, 853, 5222, 5228

Lokasi	IP Korban	MAC *Address*	Akses *Port*
	192.168.1.234	fa:cf:1e:21:32:c6	53, 80, 123, 443, 1392, 3480, 3481, 3482, 5222, 5223, 5353, 19015, 31124, 38282
	192.168.1.241	3e:71:db:55:92:98	53, 80, 443, 853, 1900, 5228
	192.168.1.247	ca:55:84:4e:78:7e	53, 80, 123, 443, 5222, 5223, 5353
Lantai 3	192.168.1.102	a6:c3:73:9f:6f:22	53, 137, 443, 5222, 5353, 5355
	192.168.1.105	ca:0f:23:d8:e3:4e	53, 80, 123, 443, 853, 1900, 3478, 5222, 5228, 8888, 9681
	192.168.1.110	86:71:38:cb:83:a3	53, 80, 443, 5223, 5353
	192.168.1.123	06:ae:cd:52:d2:aa	53, 80, 443, 3478, 5222, 5223, 5353, 7000
	192.168.1.128	12:b1:ed:fb:1c:3b	53, 80, 123, 443, 3480, 3481, 3482, 5222, 5223, 5353, 11640, 42439, 49816, 53499
	192.168.1.152	98:c8:b8:8d:fe:1b	80, 443, 5353
	192.168.1.155	b2:80:41:83:31:d2	53, 80, 443, 3478, 3480, 3481, 3482, 5223, 5353
	192.168.1.164	3c:e9:f7:db:ff:b0	80, 137, 138, 443, 1900, 5228
	192.168.1.167	8e:47:15:6a:03:c8	53, 80, 443, 853, 5222, 5228

Lokasi	IP Korban	MAC *Address*	Akses *Port*
	192.168.1.168	16:88:9b:93:dc:6c	53, 80, 123, 443, 5222, 5228, 5353
	192.168.1.170	e0:1f:88:43:7e:ba	80, 123, 443, 853, 5228, 5353
	192.168.1.171	6a:2a:64:41:3f:21	53, 80, 123, 443, 5222, 5223, 5353
	192.168.1.188	16:c2:4f:a0:ca:31	80, 443, 1900, 5222, 5228
	192.168.1.192	f2:08:a0:a0:20:3e	53, 5353
	192.168.1.196	52:ca:3c:f0:c5:c3	80, 443, 3478, 5222, 5228
	192.168.1.21	1e:13:c5:4b:8f:ee	53, 80, 443, 5
	192.168.1.219	ee:ee:2e:4c:f8:cd	53, 80, 123, 443, 3478, 5222, 5223, 5353, 8501, 8503, 8504, 8514, 8533, 8534, 8535, 8538, 8541, 8542, 8543, 8544, 8556, 8560, 8561, 8563, 8564, 8565, 8566, 8567, 8568, 8569, 8571, 8573, 8574, 8575, 8576, 8577, 8578, 8579, 8580, 8582, 8583, 8584
	192.168.1.221	8e:d9:d0:6a:58:5e	53, 443, 4500, 5222
	192.168.1.229	5e:ef:ab:70:86:e7	53, 80, 123, 443, 5223, 5353, 8535, 8536, 8539, 8540, 8541, 8542,8543, 8546, 8560, 8596, 8601, 8602, 8620, 8621, 8622, 8624,

Lokasi	IP Korban	MAC *Address*	Akses *Port*
			8625, 8626, 8627, 8628, 8629, 8630, 8631, 8632, 8633, 8634, 8639, 8640, 8641, 8645, 8646, 8647, 8648, 8650, 8656, 8657, 8658, 8662, 8663, 8668, 8679, 8686, 8688, 8693, 8710, 8713, 8714, 8715, 8716, 8718, 8719, 8720, 8721, 8722, 8723, 8725, 8729, 8732, 8735, 8737, 8739, 8740, 8741, 8742, 8743, 8745, 8747, 8748, 8749, 8750, 8751, 8753, 8771, 8776, 8781, 8782, 8783, 8792, 8797, 8800, 8815, 8897, 8902, 8905, 8906, 8986, 8987, 8989, 8995, 9007, 9025, 9028, 9031, 9045, 9054, 9055, 9063, 9072, 9115, 9122, 9143, 9160, 9681, 12010, 12019, 12022, 12023, 12025, 12028, 12029, 12031, 12033, 12042, 12044, 12047, 12049, 12050, 12058, 12062, 12065, 12066, 12068, 12069,

Lokasi	IP Korban	MAC *Address*	Akses *Port*
			12070, 12283, 12284, 12285, 12290, 12295, 12303, 12305, 12307, 12308, 12316, 12317, 12331, 12332, 12335, 12337, 12339, 12340, 12341, 12342, 12343, 12344, 12345, 12346, 12347, 12348, 12349, 12350
	192.168.1.233	b6:68:09:ae:3c:fe	80, 443, 853
	192.168.1.234	4a:ad:db:e4:aa:18	53, 80, 443, 5222, 5228
	192.168.1.242	2e:84:8c:2b:46:cf	53, 80, 443, 5223, 5228, 5353
Lantai 4	192.168.1.122	9a:4f:da:bf:05:27	53, 80, 443, 5223, 5353
	192.168.1.140	7a:e5:27:4a:2f:51	53, 80, 443, 5223, 5353
	192.168.1.160	8c:aa:ce:2c:40:d6	53, 80, 443, 853, 5222, 5228, 5353
	192.168.1.216	10:08:b1:ae:18:91	53, 80, 137, 443, 465, 993, 5222, 5228, 5353
Gazebo	192.168.1.100	e8:bf:b8:01:79:5d	53, 80, 137, 443, 1900, 5222, 5353, 5355
	192.168.1.101	e0:1f:88:4d:70:34	53, 80, 443, 853, 5222, 5228, 5353, 5001, 5002, 5003, 5004

Lokasi	IP Korban	MAC *Address*	Akses *Port*
	192.168.1.105	ea:66:99:b8:01:9d	53, 80, 123, 443, 5222, 5228, 5353, 7275
	192.168.1.106	96:46:f3:58:00:81	53, 80, 443, 853, 1900, 5222, 5228
	192.168.1.107	0a:09:c4:ad:16:8f	80, 123, 443, 853, 1900, 5222, 5228, 8888
	192.168.1.114	74:f2:fa:da:2f:07	53, 80, 123, 443, 853, 3478, 5222, 5228, 5353, 51715, 64365
	192.168.1.116	3e:aa:c6:a1:1d:f2	53, 80, 443, 5223, 5353
	192.168.1.117	f8:9e:94:d8:28:d6	53, 80, 137, 443, 1900, 5222, 5228, 5353, 5355
	192.168.1.121	7e:7a:c9:89:fb:cc	53, 80, 443, 853, 1900, 5222, 5228
	192.168.1.122	5e:81:81:1c:bf:93	53, 80, 443, 853, 5222, 5228
	192.168.1.124	1e:36:41:2b:65:4d	53, 80, 443, 853, 5222, 5228, 5353
	192.168.1.125	7e:f6:a6:02:83:8a	53, 80, 443, 853, 1900, 5228, 5353
	192.168.1.126	48:fd:a3:07:47:40	53, 80, 123, 443, 5222, 5228, 5353
	192.168.1.131	00:45:e2:e9:e2:29	53, 80, 123, 5353
	192.168.1.132	1e:ae:a1:55:85:df	853, 5353
	192.168.1.134	3e:83:33:25:7b:60	53, 80, 443, 5228
	192.168.1.135	5a:94:d8:04:63:7c	53, 80, 443, 5222, 5223, 5353

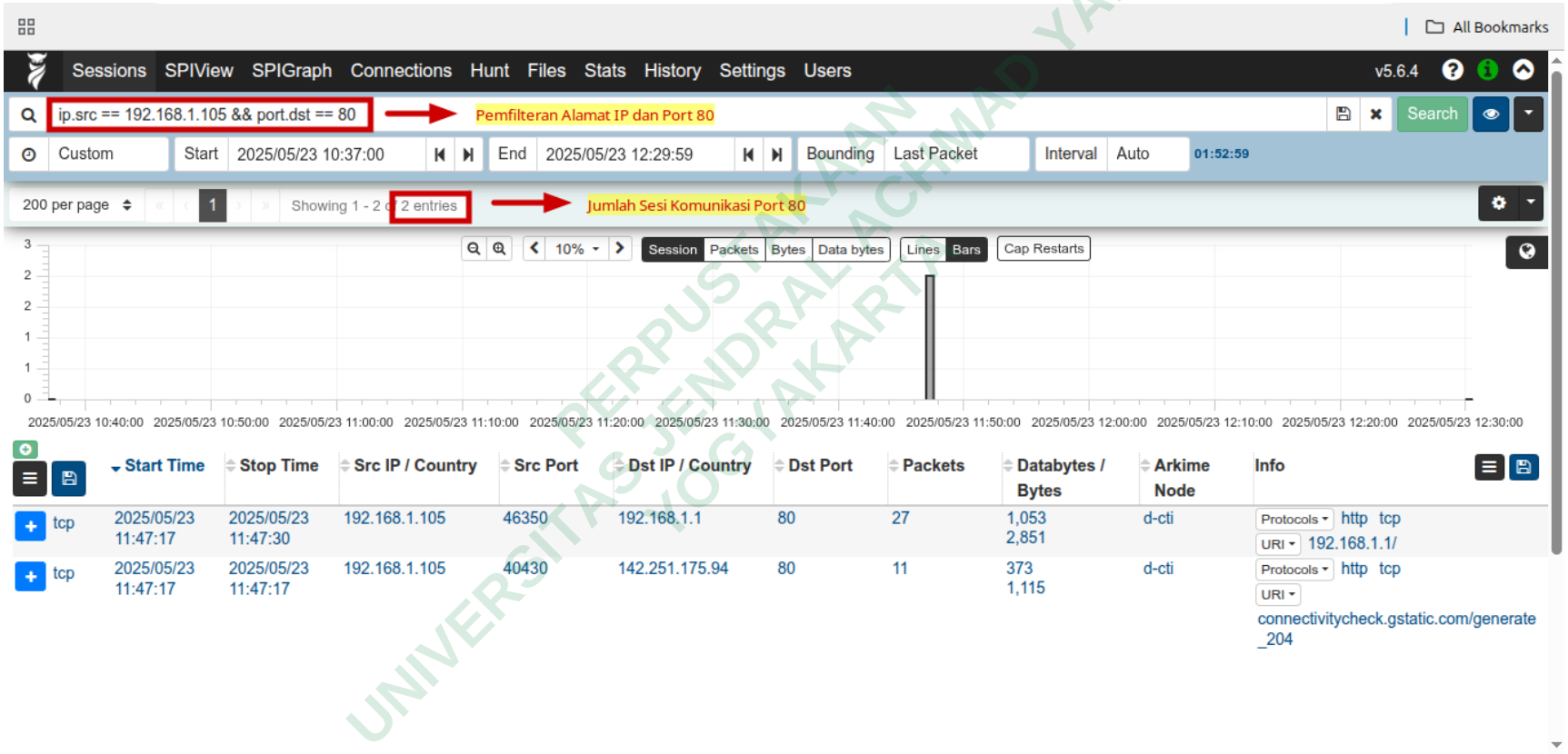
Lokasi	IP Korban	MAC *Address*	Akses *Port*
	192.168.1.136	12:d6:f4:d4:ef:8f	80, 443, 853, 5228
	192.168.1.142	62:11:ef:c3:de:99	53, 80, 123, 443, 853, 1900, 2002, 5222, 5228, 5353
	192.168.1.143	9a:33:ec:ae:74:b6	53, 80, 123, 443, 853, 1900, 2002, 5228, 5353
	192.168.1.144	ce:41:8e:00:a0:23	53, 80, 123, 443, 3478, 5222, 5223, 5353, 8516, 8518, 8522, 8529, 8624, 8632, 8639, 8643, 8648, 8684, 8687, 8689, 8691, 8693, 8696, 8698, 8701, 8702, 8708, 8709, 9502, 9681, 12143. 12173, 12181, 12182, 12242, 12277, 12280, 12293, 12336, 12345, 12349
	192.168.1.146	1a:12:ad:c0:5e:5d	53, 80, 123, 137, 443, 853, 1900, 5222, 5228, 5353, 13054, 65000
	192.168.1.154	74:f2:fa:da:bb:ed	80, 443, 5228, 5353
	192.168.1.156	06:04:b4:c0:e6:1c	53, 80, 443, 1900, 5222, 5228, 65000
	192.168.1.157	82:37:38:10:31:a2	7, 53, 80, 123, 443, 853, 1900, 3478, 5222, 5228, 9681, 16757
	192.168.1.158	5a:66:8a:26:fb:95	80, 443, 853, 1900,

Lokasi	IP Korban	MAC *Address*	Akses *Port*
			3478, 5222, 5228, 8888, 46726
	192.168.1.160	90:e8:68:c7:86:a9	137, 443, 5353, 5355
	192.168.1.161	06:e6:b4:c6:9b:ae	7, 53, 80, 123, 443, 853, 1900, 5228, 65000
	192.168.1.162	6e:93:4f:29:90:ee	53, 80, 443, 3478, 5228, 5353, 7824, 8888, 9681
	192.168.1.163	58:fb:84:76:6c:9a	80, 137, 443, 443, 1688
	192.168.1.164	fa:80:dc:24:2d:e2	53, 443, 853, 3478, 5353
	192.168.1.171	be:77:5b:3e:71:4e	7, 53, 80, 443, 853, 5228
	192.168.1.178	d2:ff:a3:9a:93:67	7, 53, 80, 443, 5228, 5353
	192.168.1.185	0e:5b:52:7a:d1:df	80, 443, 5222, 8888
	192.168.1.186	32:ec:b9:87:20:49	7, 53, 80, 123, 443, 5222, 5228, 5353
	192.168.1.189	be:2c:4f:02:f9:85	53, 80, 123, 443, 853, 1900, 2002, 5222, 5228, 5353
	192.168.1.193	5a:d3:1c:5a:44:5e	53, 80, 443, 853, 3478, 5222, 5228, 8888, 9681, 19302, 19305,
	192.168.1.194	ea:79:3b:80:fc:28	53, 80, 443, 853, 5222, 5228
	192.168.1.197	0a:f7:f2:29:57:bc	80, 443, 853, 5222, 5228

Lokasi	IP Korban	MAC *Address*	Akses *Port*
	192.168.1.201	10:68:38:4e:63:3a	53, 80, 137, 443, 1900, 5228, 5353, 5355
	192.168.1.202	c6:ab:35:81:77:b8	53, 80, 123, 443, 853, 1900, 2002, 5353
	192.168.1.211	b2:29:33:59:e7:5b	53, 80, 443, 5222, 5223, 5353
	192.168.1.215	ae:f9:0c:dc:18:72	53, 80, 443, 3478, 5222, 5223, 5353, 41558
	192.168.1.223	6e:95:fc:af:a5:72	53, 80, 123, 443, 5223, 5353
	192.168.1.226	b2:a6:b0:f9:3d:3e	53, 80, 443, 5222, 5223, 5353,
	192.168.1.227	06:de:ae:0e:c4:13	80, 443, 853, 5228, 8888
	192.168.1.228	f6:03:19:ed:45:ec	53, 80, 443, 5223, 5353
	192.168.1.229	aa:b7:de:22:a2:47	80, 443, 853, 5228, 5353
	192.168.1.231	ea:e3:36:1e:77:57	80, 443, 853, 5228, 5353
	192.168.1.232	9c:5f:5a:94:de:c1	53, 80, 443, 5228
	192.168.1.245	9c:f5:31:89:47:bf	53, 80, 443, 5228
	192.168.1.246	66:16:41:29:48:9a	53, 80, 443, 2623, 3480, 3481, 3482, 5222, 5223, 5353

Tabel 4.2 menunjukkan hasil identifikasi *port* yang diakses oleh korban yang dilakukan dengan pemfilteran alamat IP korban. Berdasarkan hasil yang ditunjukkan dari Tabel 4.2, terlihat alamat IP korban yang mengakses *port* 80.

Oleh karena itu, langkah selanjutnya adalah melakukan identifikasi *port* 80 atau protokol HTTP yang diakses oleh korban. Identifikasi *port* 80 bertujuan untuk mengetahui berapa jumlah *entries* atau berapa sesi komunikasi pada *port* 80 yang diakses oleh korban. Dalam analisis identifikasi *port* 80 dilakukan menggunakan fitur *Sessions* pada Arkime *Viewer* dengan melakukan pemfilteran berdasarkan alamat IP dan *port* 80, sebagaimana yang ditampilkan dengan salah satu alamat IP dan *port* 80 pada salah satu lokasi pengujian dalam Gambar 4.23.



Gambar 4.23 Identifikasi Sesi Komunikasi *Port* 80 Pada Alamat IP Korban

Identifikasi *port* 80 pada alamat IP korban di setiap lokasi pengujian yang dilakukan dengan pemfilteran alamat IP dan *port* 80 pada fitur Sessions menunjukkan adanya alamat IP yang mengakses *port* 80 dengan terdapat jumlah sesi komunikasi yang diakses alamat IP korban pada *port* 80. Hasil identifikasi *port* 80 pada alamat IP korban di setiap lokasi pengujian dapat dilihat pada Tabel 4.3.

Tabel 4.3 Hasil Identifikasi Sesi *Port* 80 Pada Alamat IP Korban

Lokasi	IP Korban	MAC *Address*	*Entries* atau Sesi
Lantai 1	192.168.1.105	5c:d0:6e:3c:a0:e5	2
	192.168.1.112	a0:29:42:ed:ec:16	1
	192.168.1.114	da:95:f7:e4:dc:d2	1
	192.168.1.131	a6:bb:06:f9:6e:03	19
	192.168.1.135	5a:94:d8:04:63:7c	1
	192.168.1.136	0e:93:1e:73:07:32	2
	192.168.1.186	d2:d7:da:4f:c7:35	27
	192.168.1.187	14:ac:60:77:05:37	4
	192.168.1.198	fa:d0:13:2c:b5:92	1
	192.168.1.219	5e:49:a5:27:ea:b8	1
	192.168.1.221	aa:fc:eb:a5:65:ee	1
	192.168.1.228	f6:03:19:ed:45:ec	1
	192.168.1.248	4a:1e:7c:3d:22:ef	4
Lantai 2	192.168.1.149	12:96:9e:48:25:c4	1
	192.168.1.160	da:5b:01:fb:46:f7	1
	192.168.1.180	de:33:da:c3:7f:5b	3
	192.168.1.204	fe:8c:59:57:4d:01	1
	192.168.1.214	06:89:8d:6a:2b:5b	2
	192.168.1.226	b2:a6:b0:f9:3d:3e	1

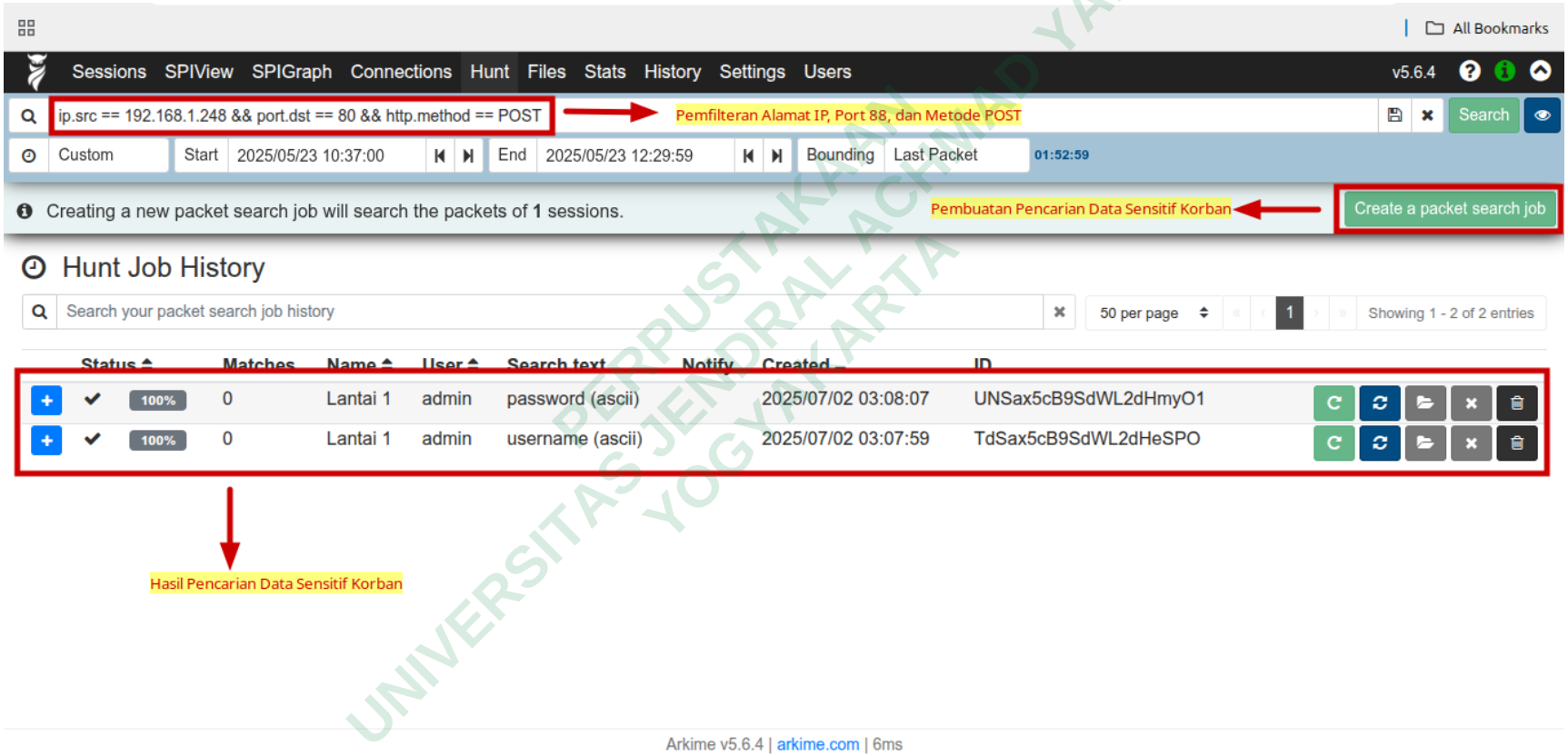
Lokasi	IP Korban	MAC *Address*	*Entries* atau Sesi
	192.168.1.231	2a:1b:c5:a7:31:35	1
	192.168.1.234	fa:cf:1e:21:32:c6	5
	192.168.1.241	3e:71:db:55:92:98	3
	192.168.1.247	ca:55:84:4e:78:7e	1
Lantai 3	192.168.1.105	ca:0f:23:d8:e3:4e	27
	192.168.1.110	86:71:38:cb:83:a3	1
	192.168.1.123	06:ae:cd:52:d2:aa	1
	192.168.1.128	12:b1:ed:fb:1c:3b	3
	192.168.1.152	98:c8:b8:8d:fe:1b	4
	192.168.1.155	b2:80:41:83:31:d2	1
	192.168.1.164	3c:e9:f7:db:ff:b0	1
	192.168.1.167	8e:47:15:6a:03:c8	2
	192.168.1.168	16:88:9b:93:dc:6c	11
	192.168.1.170	e0:1f:88:43:7e:ba	2
	192.168.1.171	6a:2a:64:41:3f:21	14
	192.168.1.188	16:c2:4f:a0:ca:31	6
	192.168.1.196	52:ca:3c:f0:c5:c3	1
	192.168.1.216	1e:13:c5:4b:8f:ee	3
	192.168.1.219	ee:ee:2e:4c:f8:cd	1
	192.168.1.229	5e:ef:ab:70:86:e7	1
	192.168.1.233	b6:68:09:ae:3c:fe	1
	192.168.1.234	4a:ad:db:e4:aa:18	2
	192.168.1.242	2e:84:8c:2b:46:cf	2
Lantai 4	192.168.1.122	9a:4f:da:bf:05:27	1
	192.168.1.140	7a:e5:27:4a:2f:51	1
	192.168.1.160	8c:aa:ce:2c:40:d6	2
	192.168.1.216	10:08:b1:ae:18:91	102

Lokasi	IP Korban	MAC *Address*	*Entries* atau Sesi
Gazebo	192.168.1.100	e8:bf:b8:01:79:5d	12
	192.168.1.101	e0:1f:88:4d:70:34	27
	192.168.1.105	ea:66:99:b8:01:9d	50
	192.168.1.106	96:46:f3:58:00:81	5
	192.168.1.107	0a:09:c4:ad:16:8f	1
	192.168.1.114	74:f2:fa:da:2f:07	23
	192.168.1.116	3e:aa:c6:a1:1d:f2	1
	192.168.1.117	f8:9e:94:d8:28:d6	1
	192.168.1.121	7e:7a:c9:89:fb:cc	5
	192.168.1.122	5e:81:81:1c:bf:93	7
	192.168.1.124	1e:36:41:2b:65:4d	4
	192.168.1.125	7e:f6:a6:02:83:8a	2
	192.168.1.126	48:fd:a3:07:47:40	5
	192.168.1.131	00:45:e2:e9:e2:29	1
	192.168.1.134	3e:83:33:25:7b:60	2
	192.168.1.135	5a:94:d8:04:63:7c	2
	192.168.1.136	12:d6:f4:d4:ef:8f	3
	192.168.1.142	62:11:ef:c3:de:99	10
	192.168.1.143	9a:33:ec:ae:74:b6	22
	192.168.1.144	ce:41:8e:00:a0:23	13
	192.168.1.146	1a:12:ad:c0:5e:5d	38
	192.168.1.154	74:f2:fa:da:bb:ed	2
	192.168.1.156	06:04:b4:c0:e6:1c	13
	192.168.1.157	82:37:38:10:31:a2	35
	192.168.1.158	5a:66:8a:26:fb:95	2
	192.168.1.161	06:e6:b4:c6:9b:ae	6
	192.168.1.162	6e:93:4f:29:90:ee	2

Lokasi	IP Korban	MAC *Address*	*Entries* atau Sesi
	192.168.1.163	58:fb:84:76:6c:9a	1
	192.168.1.171	be:77:5b:3e:71:4e	3
	192.168.1.178	d2:ff:a3:9a:93:67	4
	192.168.1.185	0e:5b:52:7a:d1:df	3
	192.168.1.186	32:ec:b9:87:20:49	8
	192.168.1.189	be:2c:4f:02:f9:85	22
	192.168.1.193	5a:d3:1c:5a:44:5e	9
	192.168.1.194	ea:79:3b:80:fc:28	5
	192.168.1.197	0a:f7:f2:29:57:bc	3
	192.168.1.201	10:68:38:4e:63:3a	2
	192.168.1.202	c6:ab:35:81:77:b8	19
	192.168.1.211	b2:29:33:59:e7:5b	1
	192.168.1.215	ae:f9:0c:dc:18:72	2
	192.168.1.223	6e:95:fc:af:a5:72	3
	192.168.1.226	b2:a6:b0:f9:3d:3e	1
	192.168.1.227	06:de:ae:0e:c4:13	1
	192.168.1.228	f6:03:19:ed:45:ec	1
	192.168.1.229	aa:b7:de:22:a2:47	2
	192.168.1.231	ea:e3:36:1e:77:57	2
	192.168.1.232	9c:5f:5a:94:de:c1	7
	192.168.1.245	9c:f5:31:89:47:bf	5
	192.168.1.246	66:16:41:29:48:9a	1

Tabel 4.3 menunjukkan hasil identifikasi sesi komunikasi pada *port* 88 yang diakses oleh korban yang diperoleh melalui pemfilteran alamat IP korban dan *port* 88. Berdasarkan hasil yang ditunjukkan dari Tabel 4.3, terlihat jumlah sesi komunikasi *port* 88 yang diakses oleh korban. Dengan demikian, langkah

terakhir dalam analisis paket data menggunakan Arkime pada penelitian ini adalah mengidentifikasi adanya data sensitif yang dikirimkan oleh korban melalui *port* 80 atau protokol HTTP. Identifikasi data sensitif korban melalui *port* 80 bertujuan untuk mengetahui apakah terdapat data sensitif dari korban seperti *username* dan *password* yang dikirim melalui *port* 80 dan metode POST. Metode POST dilakukan untuk memperkecil pencarian data sensitif korban dikarenakan data sensitif korban seperti *username* dan *password* dikirim ke server melalui *port* 80 atau protokol HTTP. Dalam proses identifikasi adanya data sensitif korban pada *port* 80 dilakukan menggunakan fitur *Hunt* pada Arkime *Viewer* dengan melakukan pemfilteran berdasarkan alamat IP korban, *port* 80, dan metode POST yang selanjutnya dilakukan pembuatan pencarian isi paket data sensitif dengan kata kunci *username* dan *password* pada fitur *Hunt* dengan menyesuaikan periode pengujian di setiap lokasi pengujian. Proses identifikasi pencarian data sensitif korban pada fitur *Hunt* dapat dilihat pada Gambar 4.24.



Gambar 4.24 Identifikasi Data Sensitif Korban Pada Fitur *Hunt*

Analisis pencarian data sensitif korban dengan kata kunci *username* dan *password* di setiap lokasi pengujian pada fitur *Hunt* dengan melakukan pemfilteran alamat IP korban, *port* 80, dan Metode POST menunjukkan bahwa hasil identifikasi pencarian data sensitif korban tidak ditemukan adanya data sensitif yang dikirim oleh korban melalui *port* 80 dalam Arkime *Viewer* yang ditunjukkan pada kolom *Matches* bernilai 0. Hasil analisis pencarian data sensitif korban dengan kata kunci *username* dan *password* di setiap lokasi pengujian dapat dilihat pada Tabel 4.4.

Tabel 4.4 Hasil Identifikasi Pencarian Data Sensitif Korban

Lokasi	IP Korban	MAC *Address*	Kredensial	
			Username	***Password***
Lantai 1	192.168.1.105	5c:d0:6e:3c:a0:e5	Tidak	Tidak
	192.168.1.112	a0:29:42:ed:ec:16	Tidak	Tidak
	192.168.1.114	da:95:f7:e4:dc:d2	Tidak	Tidak
	192.168.1.131	a6:bb:06:f9:6e:03	Tidak	Tidak
	192.168.1.135	5a:94:d8:04:63:7c	Tidak	Tidak
	192.168.1.136	0e:93:1e:73:07:32	Tidak	Tidak
	192.168.1.186	d2:d7:da:4f:c7:35	Tidak	Tidak
	192.168.1.187	14:ac:60:77:05:37	Tidak	Tidak
	192.168.1.198	fa:d0:13:2c:b5:92	Tidak	Tidak
	192.168.1.219	5e:49:a5:27:ea:b8	Tidak	Tidak
	192.168.1.221	aa:fc:eb:a5:65:ee	Tidak	Tidak
	192.168.1.228	f6:03:19:ed:45:ec	Tidak	Tidak
	192.168.1.248	4a:1e:7c:3d:22:ef	Tidak	Tidak
Lantai 2	192.168.1.149	12:96:9e:48:25:c4	Tidak	Tidak
	192.168.1.160	da:5b:01:fb:46:f7	Tidak	Tidak
	192.168.1.180	de:33:da:c3:7f:5b	Tidak	Tidak

Lokasi	IP Korban	MAC *Address*	Kredensial	
			Username	***Password***
	192.168.1.204	fe:8c:59:57:4d:01	Tidak	Tidak
	192.168.1.214	06:89:8d:6a:2b:5b	Tidak	Tidak
	192.168.1.226	b2:a6:b0:f9:3d:3e	Tidak	Tidak
	192.168.1.231	2a:1b:c5:a7:31:35	Tidak	Tidak
	192.168.1.234	fa:cf:1e:21:32:c6	Tidak	Tidak
	192.168.1.241	3e:71:db:55:92:98	Tidak	Tidak
	192.168.1.247	ca:55:84:4e:78:7e	Tidak	Tidak
Lantai 3	192.168.1.105	ca:0f:23:d8:e3:4e	Tidak	Tidak
	192.168.1.110	86:71:38:cb:83:a3	Tidak	Tidak
	192.168.1.123	06:ae:cd:52:d2:aa	Tidak	Tidak
	192.168.1.128	12:b1:ed:fb:1c:3b	Tidak	Tidak
	192.168.1.152	98:c8:b8:8d:fe:1b	Tidak	Tidak
	192.168.1.155	b2:80:41:83:31:d2	Tidak	Tidak
	192.168.1.164	3c:e9:f7:db:ff:b0	Tidak	Tidak
	192.168.1.167	8e:47:15:6a:03:c8	Tidak	Tidak
	192.168.1.168	16:88:9b:93:dc:6c	Tidak	Tidak
	192.168.1.170	e0:1f:88:43:7e:ba	Tidak	Tidak
	192.168.1.171	6a:2a:64:41:3f:21	Tidak	Tidak
	192.168.1.188	16:c2:4f:a0:ca:31	Tidak	Tidak
	192.168.1.196	52:ca:3c:f0:c5:c3	Tidak	Tidak
	192.168.1.216	1e:13:c5:4b:8f:ee	Tidak	Tidak
	192.168.1.219	ee:ee:2e:4c:f8:cd	Tidak	Tidak
	192.168.1.229	5e:ef:ab:70:86:e7	Tidak	Tidak
	192.168.1.233	b6:68:09:ae:3c:fe	Tidak	Tidak
	192.168.1.234	4a:ad:db:e4:aa:18	Tidak	Tidak
	192.168.1.242	2e:84:8c:2b:46:cf	Tidak	Tidak

Lokasi	IP Korban	MAC *Address*	Kredensial	
			Username	*Password*
Lantai 4	192.168.1.122	9a:4f:da:bf:05:27	Tidak	Tidak
	192.168.1.140	7a:e5:27:4a:2f:51	Tidak	Tidak
	192.168.1.160	8c:aa:ce:2c:40:d6	Tidak	Tidak
	192.168.1.216	10:08:b1:ae:18:91	Tidak	Tidak
Gazebo	192.168.1.100	e8:bf:b8:01:79:5d	Tidak	Tidak
	192.168.1.101	e0:1f:88:4d:70:34	Tidak	Tidak
	192.168.1.105	ea:66:99:b8:01:9d	Tidak	Tidak
	192.168.1.106	96:46:f3:58:00:81	Tidak	Tidak
	192.168.1.107	0a:09:c4:ad:16:8f	Tidak	Tidak
	192.168.1.114	74:f2:fa:da:2f:07	Tidak	Tidak
	192.168.1.116	3e:aa:c6:a1:1d:f2	Tidak	Tidak
	192.168.1.117	f8:9e:94:d8:28:d6	Tidak	Tidak
	192.168.1.121	7e:7a:c9:89:fb:cc	Tidak	Tidak
	192.168.1.122	5e:81:81:1c:bf:93	Tidak	Tidak
	192.168.1.124	1e:36:41:2b:65:4d	Tidak	Tidak
	192.168.1.125	7e:f6:a6:02:83:8a	Tidak	Tidak
	192.168.1.126	48:fd:a3:07:47:40	Tidak	Tidak
	192.168.1.131	00:45:e2:e9:e2:29	Tidak	Tidak
	192.168.1.134	3e:83:33:25:7b:60	Tidak	Tidak
	192.168.1.135	5a:94:d8:04:63:7c	Tidak	Tidak
	192.168.1.136	12:d6:f4:d4:ef:8f	Tidak	Tidak
	192.168.1.142	62:11:ef:c3:de:99	Tidak	Tidak
	192.168.1.143	9a:33:ec:ae:74:b6	Tidak	Tidak
	192.168.1.144	ce:41:8e:00:a0:23	Tidak	Tidak
	192.168.1.146	1a:12:ad:c0:5e:5d	Tidak	Tidak
	192.168.1.154	74:f2:fa:da:bb:ed	Tidak	Tidak

Lokasi	IP Korban	MAC *Address*	Kredensial	
			Username	*Password*
	192.168.1.156	06:04:b4:c0:e6:1c	Tidak	Tidak
	192.168.1.157	82:37:38:10:31:a2	Tidak	Tidak
	192.168.1.158	5a:66:8a:26:fb:95	Tidak	Tidak
	192.168.1.161	06:e6:b4:c6:9b:ae	Tidak	Tidak
	192.168.1.162	6e:93:4f:29:90:ee	Tidak	Tidak
	192.168.1.163	58:fb:84:76:6c:9a	Tidak	Tidak
	192.168.1.171	be:77:5b:3e:71:4e	Tidak	Tidak
	192.168.1.178	d2:ff:a3:9a:93:67	Tidak	Tidak
	192.168.1.185	0e:5b:52:7a:d1:df	Tidak	Tidak
	192.168.1.186	32:ec:b9:87:20:49	Tidak	Tidak
	192.168.1.189	be:2c:4f:02:f9:85	Tidak	Tidak
	192.168.1.193	5a:d3:1c:5a:44:5e	Tidak	Tidak
	192.168.1.194	ea:79:3b:80:fc:28	Tidak	Tidak
	192.168.1.197	0a:f7:f2:29:57:bc	Tidak	Tidak
	192.168.1.201	10:68:38:4e:63:3a	Tidak	Tidak
	192.168.1.202	c6:ab:35:81:77:b8	Tidak	Tidak
	192.168.1.211	b2:29:33:59:e7:5b	Tidak	Tidak
	192.168.1.215	ae:f9:0c:dc:18:72	Tidak	Tidak
	192.168.1.223	6e:95:fc:af:a5:72	Tidak	Tidak
	192.168.1.226	b2:a6:b0:f9:3d:3e	Tidak	Tidak
	192.168.1.227	06:de:ae:0e:c4:13	Tidak	Tidak
	192.168.1.228	f6:03:19:ed:45:ec	Tidak	Tidak
	192.168.1.229	aa:b7:de:22:a2:47	Tidak	Tidak
	192.168.1.231	ea:e3:36:1e:77:57	Tidak	Tidak
	192.168.1.232	9c:5f:5a:94:de:c1	Tidak	Tidak
	192.168.1.245	9c:f5:31:89:47:bf	Tidak	Tidak

Lokasi	IP Korban	MAC *Address*	Kredensial	
			Username	***Password***
	192.168.1.246	66:16:41:29:48:9a	Tidak	Tidak