



## PERANGKAT SCAVENGER

Dalam era digital yang semakin berkembang, menjaga keamanan jaringan seluler menjadi sangat penting. "Scavenger" adalah perangkat pintar mutakhir yang dirancang khusus untuk mendeteksi dan mengidentifikasi sinyal BTS (Base Transceiver Station) palsu. Alat analisa jaringan yang canggih ini membantu operator dan penyedia layanan dalam memantau aktivitas jaringan secara langsung, sehingga memastikan keamanan dan efisiensi jaringan.

Sebagai alat yang sangat penting dalam melindungi infrastruktur jaringan, "Scavenger" berperan besar dalam mendeteksi sinyal tidak sah yang dapat membahayakan keamanan jaringan. Panduan lengkap ini menjelaskan fitur-fitur perangkat secara rinci, memberikan gambaran jelas tentang antarmuka pengguna (UI), serta langkah-langkah penggunaan yang mudah dipahami. Dengan "Scavenger", Anda dapat menjaga keamanan jaringan Anda dari ancaman yang mungkin muncul dengan lebih percaya diri.

## SPESIFIKASI PRODUK



Item	Specifications
Dimensi Host (mm)	360*280*100
Berat	-
Prosesor	Intel
Modem	Telite 2G/3G, Quactel 4G
Hub USB	7 Port
USB Eksternal	USB A Female Mounting
Antena Indoor	Antena 10dbi 600-6000MHz 3G 4G LTE
Antena Outdoor	PCTEL 3.7M Penerima Pemindaian IBFLEX 698 MHz - 3.8 GHz
Jarak Kerja	10m - 500m
Waktu Pemasangan	-
Perangkat Lunak	Perangkat lunak Web Server yang disesuaikan
Penyimpanan Data	-
Mode Transmisi	WiFi Nirkabel
Suhu Lingkungan	-10°C~+45°C
Daya	≤50w
Sumber Daya	12VDC, Baterai eksternal [Opsional]

## Fitur Utama

### Ikhtisar

#### 1. Dashboard Utama

Dashboard Utama adalah pusat utama untuk mengakses berbagai fitur dari Scavenger.

Dashboard ini memberikan gambaran umum tentang status jaringan saat ini dan akses ke fitur-fitur utama.

The screenshot shows the main dashboard of the Scavenger application. At the top, there are four summary cards: 'All Scan Result' (0), 'Threats' (0), 'Device' (0), and 'Total Scanning Duration' (00:00:00). Below these are several filter and search options, including 'Last Seen', 'Device', 'Operator', 'Technology', '(A/UA/EA) RFCN', 'PSC/PCI', 'LAC/TAC', 'Cell ID', 'Rx Lev', 'MCC', 'MNC', and 'Hits'. A prominent feature is a central illustration of a person sitting at a desk with a laptop, surrounded by documents and a smartphone, with the text 'No data to show' and 'Please start scanning to retrieve data from it.' A 'Start Scan' button is located below the illustration. At the bottom, a pagination bar shows 'Showing 1-15 of 20' with pages 1 through 10.

**Jumlah Perangkat:** Menampilkan jumlah perangkat yang terhubung ke jaringan dan sedang dipantau secara aktif. Jumlah ini penting bagi administrator jaringan untuk memahami cakupan perangkat yang sedang diawasi.

**Jumlah Ancaman:** Menunjukkan jumlah ancaman yang terdeteksi, seperti sinyal BTS tidak sah, yang penting untuk menilai status keamanan jaringan saat ini.

**Durasi Pemindaian:** Menampilkan waktu yang telah berlalu sejak sesi pemindaian terakhir dimulai, memberikan konteks waktu untuk aktivitas pemantauan yang sedang berlangsung.



**Tombol Mulai Pemindaian:** Kontrol utama untuk memulai pemindaian jaringan guna mendeteksi dan mengidentifikasi sinyal BTS. Keberadaan tombol yang menonjol di dashboard memudahkan akses cepat untuk tindakan segera.

## 2. Panel Hasil Pemindaian Semua

Panel ini memberikan daftar rinci semua sinyal BTS yang terdeteksi selama pemindaian, dengan informasi mendalam untuk analisis lebih lanjut.

The screenshot shows the 'All Scan Result' section of the Scavenger dashboard. At the top, there are four summary cards: 'All Scan Result' (4), 'Threats' (1), 'Device' (1), and 'Total Scanning Duration' (00:02:15). Below these are tabs for 'All Scan Results' and 'Threat'. A table lists detected signals with columns for Last Seen, Device, Operator, Technology, (A/UA/EA) RFCN, PSC/PCI, LAC/TAC, Cell ID, Rx Lev, MCC, MNC, and Hits. The table shows four entries, each with a checkbox and a 'Details' icon. At the bottom, a navigation bar shows page numbers 1 through 10.

Last Seen	Device	Operator	Technology	(A/UA/EA) RFCN	PSC/PCI	LAC/TAC	Cell ID	Rx Lev	MCC	MNC	Hits
14/05/2024 17:13	Hunter AR_95	Three	GSM (2G)	93	-	24442	11103	-93 dbm	510	11	1
14/05/2024 17:13	Hunter AR_95	Indosat	GSM (2G)	91	-	24442	11101	-96 dbm	510	11	1
14/05/2024 17:13	Hunter AR_95	Axiata	GSM (2G)	91	-	24442	11103	-93 dbm	510	11	1
14/05/2024 17:13	Hunter AR_95	XL Axiata	GSM (2G)	91	-	24442	11101	-96 dbm	510	11	1

**Navigasi Tab:** Memungkinkan pengguna untuk beralih antara berbagai tampilan data, seperti "Semua Hasil Pemindaian," "Ancaman," dan informasi lain yang dikategorikan. Struktur ini membantu pengguna untuk fokus pada tipe data tertentu atau kondisi peringatan.

Tabel Hasil Pemindaian:

- Terakhir Terlihat:** Menunjukkan waktu kapan sinyal terakhir terdeteksi. Ini penting untuk melacak aktivitas dan frekuensi sinyal.
- Perangkat:** Mengidentifikasi perangkat yang terdeteksi, baik berdasarkan nama atau pengenal unik. Ini membantu dalam membedakan antara berbagai sumber sinyal.

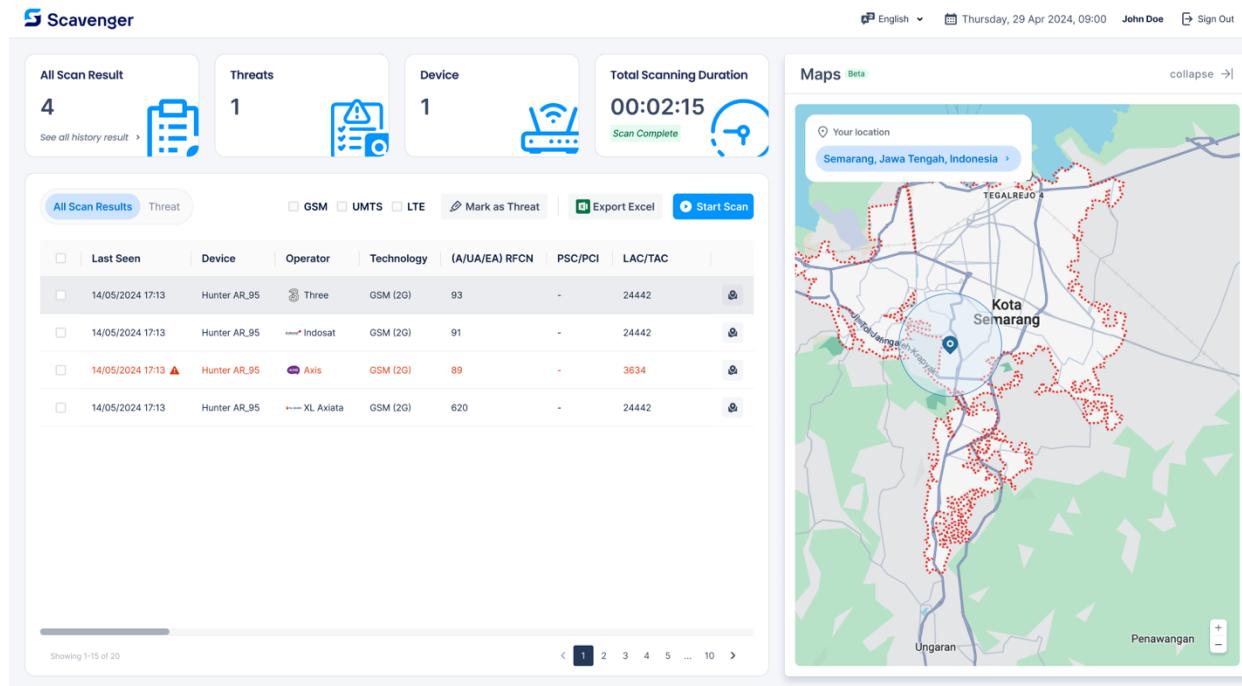
# Scavenger

- **Operator:** Menampilkan operator jaringan yang terkait dengan sinyal yang terdeteksi, membantu dalam verifikasi sinyal yang sah.
- **Teknologi:** Menunjukkan jenis teknologi jaringan (GSM, UMTS, LTE, dll.) yang digunakan, yang penting untuk memahami sifat sinyal yang terdeteksi.
- **(A)NATAI:** Merujuk pada nomor identifikasi sel atau pengenal unik serupa. Ini sangat penting untuk analisis teknis dan pelaporan.
- **PSC/PCI:** Physical Cell ID atau Primary Scrambling Code, memberikan detail untuk membedakan sinyal.
- **LAC/TAC:** Kode Area Lokasi atau Kode Area Pelacakan, yang merupakan pengenal geografis yang berguna untuk melacak sumber sinyal.
- **Bilah Filter:** Elemen antarmuka yang memungkinkan pengguna untuk memfilter hasil pemindaian berdasarkan parameter tertentu seperti waktu, operator, atau jenis teknologi. Fungsi ini sangat penting untuk fokus pada subset data yang relevan.

**Tombol Sortir:** Memungkinkan penyortiran data dalam tabel berdasarkan kolom yang dipilih, membantu dalam memprioritaskan dan mengatur informasi.

## 3. Bagian Peta

Bagian Peta memberikan representasi visual dari sinyal BTS yang terdeteksi, meningkatkan analisis spasial distribusi sinyal.



**Tampilan Peta:** Antarmuka geografis yang menunjukkan lokasi sinyal BTS yang terdeteksi. Alat visual ini sangat penting untuk memahami distribusi fisik dan potensi pengelompokan sinyal yang tidak sah.

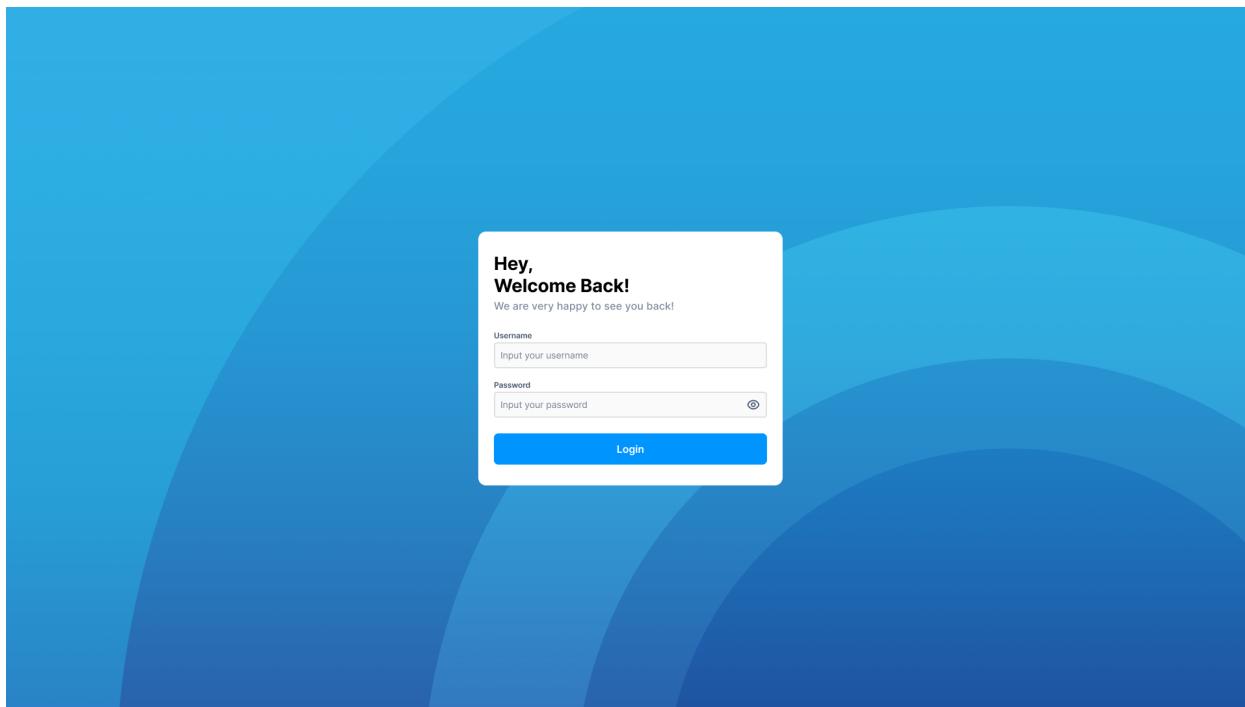
**Penanda Lokasi:** Menunjukkan lokasi spesifik dari sinyal yang terdeteksi di peta. Mengklik penanda akan menampilkan informasi rinci tentang sinyal tersebut, seperti frekuensi, operator, dan riwayat deteksi.

**Tombol Set Lokasi:** Memungkinkan pengguna untuk mendefinisikan area pemindaian dengan menetapkan lokasi menggunakan berbagai metode (lokasi GPS saat ini, pemilihan manual pada peta, atau dengan memasukkan koordinat). Fitur ini penting untuk pemindaian dan analisis yang ditargetkan.

## PANDUAN MANUAL

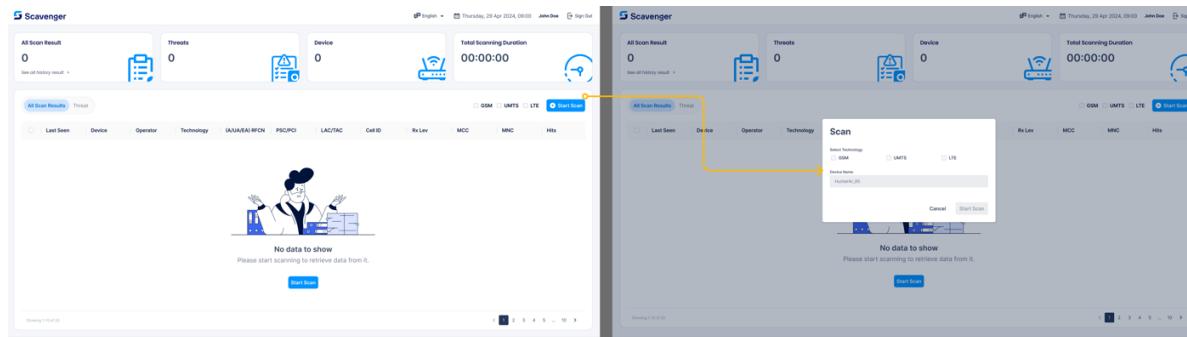
### LANGKAH-LANGKAH PENGGUNAAN PERANGKAT

#### 1. Masuk ke Sistem



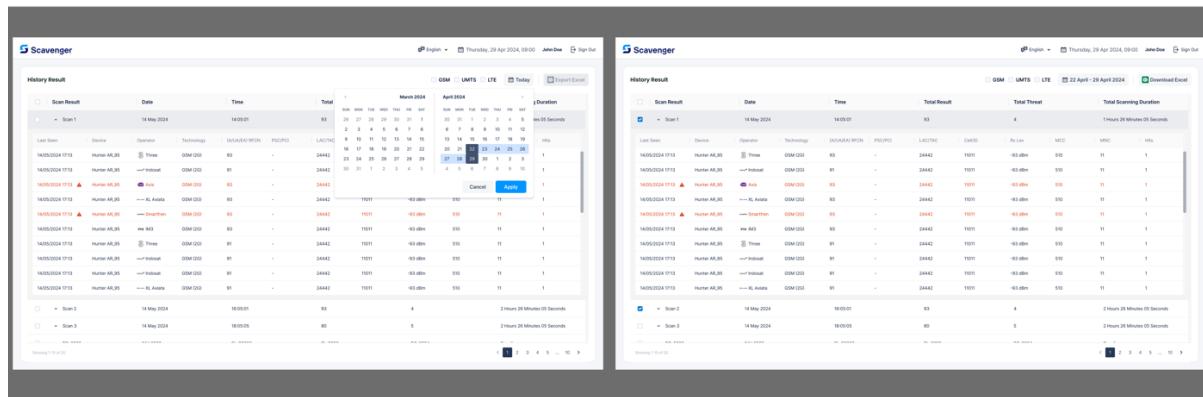
- **Langkah 1:** Buka aplikasi "Scavenger" di perangkat Anda.
- **Langkah 2:** Pada layar login, masukkan nama pengguna dan kata sandi Anda.
- **Langkah 3:** Klik "Login" untuk mengakses dashboard utama. Jika kredensial salah, akan muncul notifikasi untuk memasukkan ulang.

## 2. Memulai Pindai



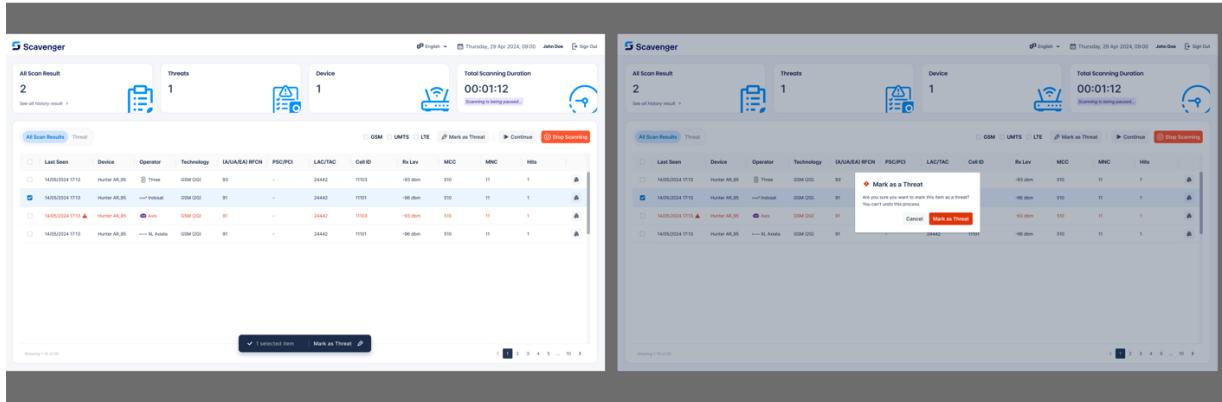
- Langkah 1:** Setelah masuk, navigasikan ke dashboard utama.
- Langkah 2:** Klik tombol "Mulai Pemindaian". Sistem akan memulai pemindaian, mengidentifikasi sinyal BTS dalam jangkauan yang ditentukan.
- Langkah 3:** Pantau "Durasi Pemindaian" untuk melacak kemajuan dan durasi pemindaian.

## 3. Melihat dan Memfilter Riwayat Hasil Pemindaian



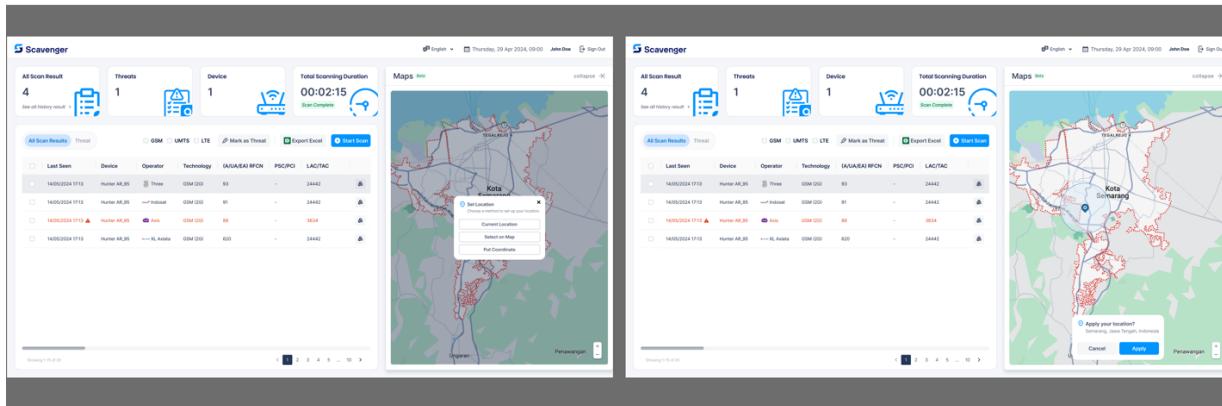
- Langkah 1:** Hasil dari pemindaian ditampilkan di panel "Semua Hasil Pemindaian".
- Langkah 2:** Gunakan bilah filter untuk menyaring hasil yang ditampilkan berdasarkan kriteria tertentu, seperti operator atau jenis teknologi.
- Langkah 3:** Klik pada entri mana pun di tabel untuk melihat informasi lebih rinci tentang sinyal, termasuk spesifikasi teknis dan pengenal.

## 4. Marking Suspicious Signals as Threats



- Step 1: Identify any suspicious signals from the scan results list.
- Step 2: Select the signal entry and click on the "Mark as Threat" option to classify the signal as a potential threat.
- Step 3: The marked signals can then be reviewed and investigated further for security implications.

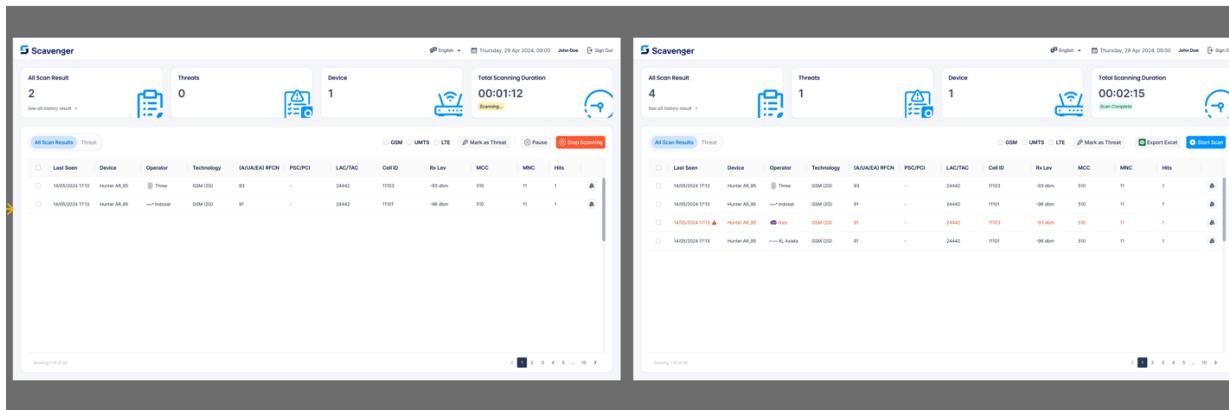
## 5. Menandai Sinyal Mencurigakan sebagai Ancaman



- Langkah 1:** Klik tombol "Set Lokasi" di dekat bagian peta.
- Langkah 2:** Pilih dari metode yang tersedia untuk menetapkan lokasi:
  - Lokasi Saat Ini:** Menggunakan GPS perangkat untuk menetapkan lokasi fisik saat ini.
  - Pilih di Peta:** Memilih lokasi secara manual dengan menavigasi antarmuka peta.
  - Set Koordinat:** Masukkan koordinat lintang dan bujur spesifik untuk penargetan yang tepat.

- **Langkah 3:** Konfirmasi pengaturan lokasi dengan mengklik "Terapkan." Peta dan pemindaian berikutnya akan diperbarui sesuai dengan pengaturan ini.

## 6. Menyimpan dan Mengekspor Hasil Pemindaian



Last Seen	Device	Operator	Technology	(A)IAU/EAI RFQN	PSC/PCI	LAC/TAC	Cell ID	Rx Lev	MCC	MNC	Hits
14/05/2024 07:13	Huawei AR-25	GSM (2G)	93	-	24442	1103	-93 dBm	010	11	1	1
14/05/2024 07:13	Huawei AR-25	GSM (2G)	91	-	24442	1101	-96 dBm	010	11	1	1

Last Seen	Device	Operator	Technology	(A)IAU/EAI RFQN	PSC/PCI	LAC/TAC	Cell ID	Rx Lev	MCC	MNC	Hits
14/05/2024 07:13	Huawei AR-25	GSM (2G)	93	-	24442	1103	-93 dBm	010	11	1	1
14/05/2024 07:13	Huawei AR-25	GSM (2G)	91	-	24442	1101	-96 dBm	010	11	1	1
14/05/2024 07:13	Huawei AR-25	GSM (2G)	91	-	24442	1103	-91 dBm	010	11	1	1
14/05/2024 07:13	Huawei AR-25	GSM (2G)	91	-	24442	1101	-96 dBm	010	11	1	1

- **Langkah 1:** Setelah menyelesaikan pemindaian dan menganalisis hasilnya, klik tombol "Ekspor Excel".
- **Langkah 2:** Pilih format file yang diinginkan dan tentukan lokasi untuk menyimpan data. Fitur ini memungkinkan pencatatan secara rinci dan analisis lebih lanjut.

## 7. Mengubah Bahasa

- **Langkah 1:** Klik pada menu Bahasa di bilah atas layar.
- **Langkah 2:** Pilih bahasa yang diinginkan untuk menerapkan perubahan, pilihan yang tersedia hanya Bahasa Inggris dan Bahasa Indonesia.

## 8. Keluar dari Sistem

- **Langkah 1:** Untuk keluar dari aplikasi dengan aman, klik pada nama pengguna yang ditampilkan di pojok kanan atas.
- **Langkah 2:** Pilih "Keluar" dari menu dropdown untuk mengakhiri sesi Anda dengan aman.

### Tips Tambahan dan Praktik Terbaik

1. **Pembaruan Berkala:** Pastikan aplikasi dan firmware selalu diperbarui ke versi terbaru untuk mendapatkan fitur baru dan peringkatan keamanan.
2. **Keamanan Data:** Tangani file ekspor dan informasi sensitif dengan hati-hati, menjaga privasi dan integritas data.



3. **Pelatihan Pengguna:** Sesi pelatihan rutin harus dilakukan untuk membiasakan pengguna dengan fitur-fitur dan praktik terbaik dalam menggunakan Scavenger.
4. **Pemeliharaan Sistem:** Pemeriksaan dan pemeliharaan perangkat lunak dan perangkat keras secara berkala direkomendasikan untuk memastikan kinerja optimal perangkat.

### Kesimpulan

Manual komprehensif ini dirancang untuk memberikan semua informasi yang diperlukan kepada pengguna agar dapat menggunakan perangkat "Scavenger" secara efektif. Dengan memahami setiap fitur dan mengikuti langkah-langkah operasional secara rinci, pengguna dapat meningkatkan keamanan jaringan mereka dengan mengidentifikasi dan menangani sinyal BTS yang tidak sah. Untuk bantuan atau dukungan teknis lebih lanjut, pengguna disarankan untuk menghubungi tim dukungan. Umpan balik yang berkelanjutan sangat dihargai karena berkontribusi pada peningkatan produk dan fungsionalitasnya.