Scavenger

SCAVENGER Mobile DEVICE

Introducing "Scavenger Mobile," a cutting-edge mobile application engineered to detect unauthorized and potentially malicious Base Transceiver Station (BTS) signals. This indispensable tool ensures the security of your mobile network infrastructure by identifying and mitigating the risks posed by fake BTS signals, which can jeopardize network integrity. Equipped with advanced features, including a dBm signal analyzer and compass and gyroscope integration, Scavenger Mobile accurately locates threatening signals. This manual offers a thorough guide to the application's functionalities, an in-depth explanation of its user interface, and comprehensive instructions for effectively utilizing its features.

Scavenger

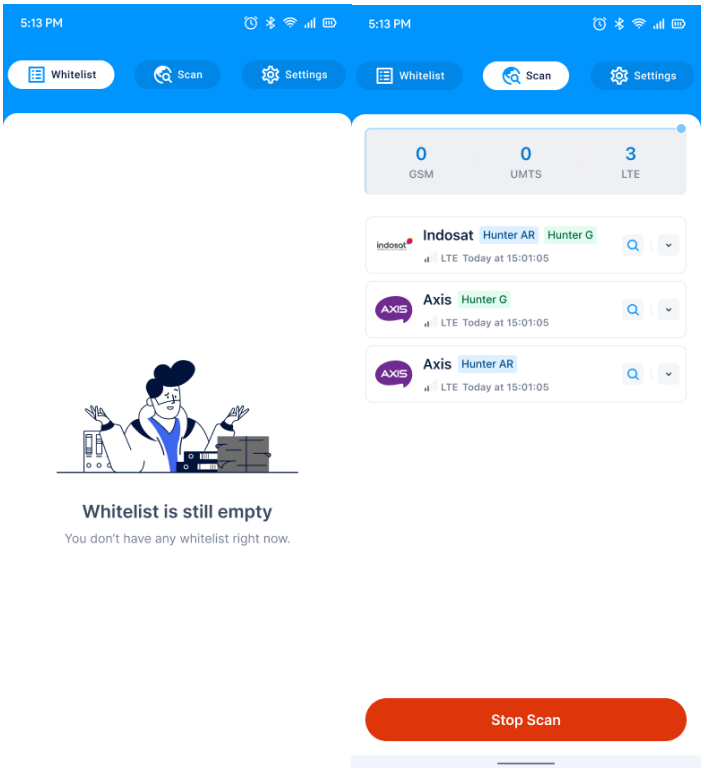
PRODUCT SPECIFICATION

BODY	Dimensions	173 x 77 x 10.3 mm (6.81 x 3.03 x 0.41 in)
	Weight	239 g (8.43 oz)
	Build	Glass front (Gorilla Glass Victus), glass back (Gorilla Glass 3), aluminum frame
	SIM	Dual SIM (Nano-SIM, dual stand-by)
		IPX4 water resistant Illuminated RGB logo (on the back) Pressure sensitive zones (Gaming triggers)
DISPLAY	Type	AMOLED, 1B colors, 165Hz, HDR10+, 800 nits (typ), 1200 nits (peak)
	Size	6.78 inches, 109.5 cm^2 (~82.2% screen-to-body ratio)
	Resolution	1080 x 2448 pixels (~395 ppi density)
	Protection	Corning Gorilla Glass Victus
PLATFORM	OS	Android 12, upgradable to Android 13
	Chipset	Qualcomm SM8475 Snapdragon 8+ Gen 1 (4 nm)
	CPU	Octa-core (1x3.19 GHz Cortex-X2 & 3x2.75 GHz Cortex-A710 & 4x1.80 GHz Cortex-A510)
	GPU	Adreno 730
MEMORY	Card slot	No
	Internal	128GB 8GB RAM, 128GB 12GB RAM, 256GB 12GB RAM, 512GB 16GB RAM
		UFS 3.1 NTFS support for external storage

Scavenger

MAIN FEATURES OVERVIEW

1. Home Screen

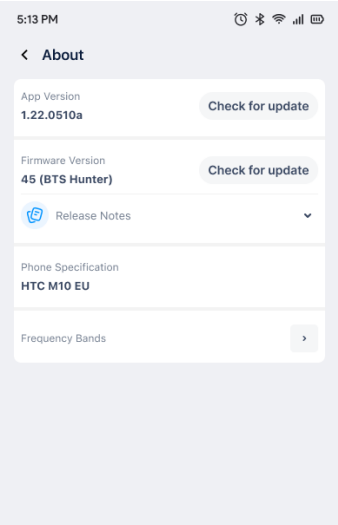


The Home Screen is the primary hub for accessing various functionalities of the Scavenger Mobile app.

- Whitelist: This section allows users to manage a list of known, trusted BTS signals. It prevents these signals from being flagged as threats, reducing false positives.
- Scan Button: Central to the application's operation, this button initiates the scanning process. Upon activation, the app searches for BTS signals within the vicinity, categorizing them based on their technology type.
- Settings: Provides access to a variety of configuration options, allowing users to tailor the app's operation to their specific needs.

- Signal Summary: A quick overview that displays the number of detected signals, segmented by technology type (GSM, UMTS, LTE). This provides an immediate snapshot of the network environment.
- Detected Signals List: Shows detailed information about each detected signal, including operator logos, technology details, and signal integrity indicators. Clicking on these entries reveals further technical specifications and potential threat assessments.

2. About Section

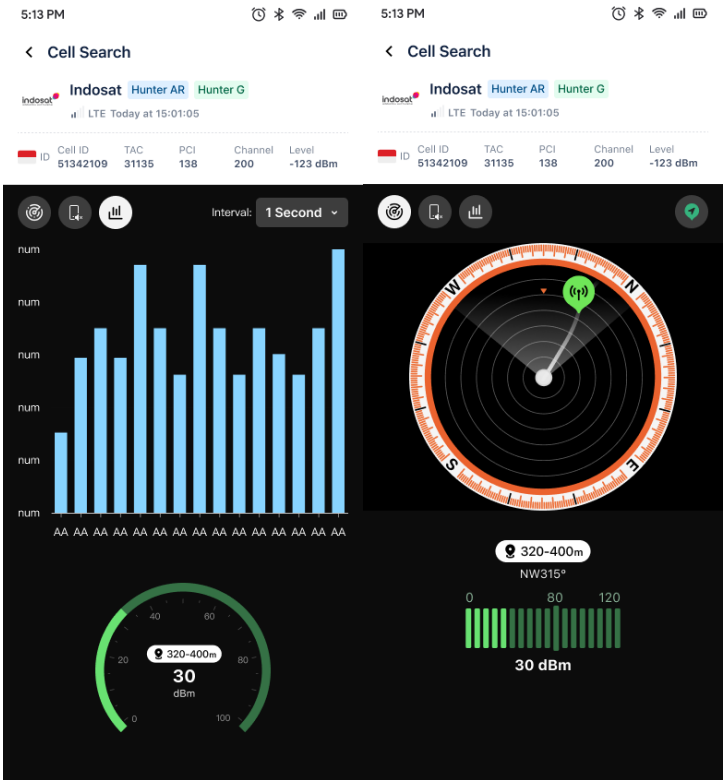


The "About" section provides crucial information regarding the application's version, firmware details, and device compatibility.

- App Version: This element displays the current version of the Scavenger Mobile application. It is vital for users to know this to ensure they are using the latest software with all available features and security updates.
- Firmware Version: Indicates the specific version of the firmware, which may include improvements and bug fixes for the BTS detection algorithms. The firmware version, labeled here as "45 (BTS Hunter)," is essential for the application's operational accuracy.
- Check for Update Buttons: Users can click these buttons to verify and download the latest updates for both the app and the firmware. Keeping the software updated is critical for maintaining system security and performance.

- Release Notes: A dropdown section providing a log of changes, including new features, enhancements, and bug fixes. This helps users stay informed about the improvements and modifications made in the latest versions.
- Phone Specification: This detail includes the model and specifications of the mobile device, such as "HTC M10 EU," ensuring compatibility and optimal operation.
- Frequency Bands: Outlines the supported frequency bands, crucial for identifying the range of signals that the device can detect.

3. Cell Search

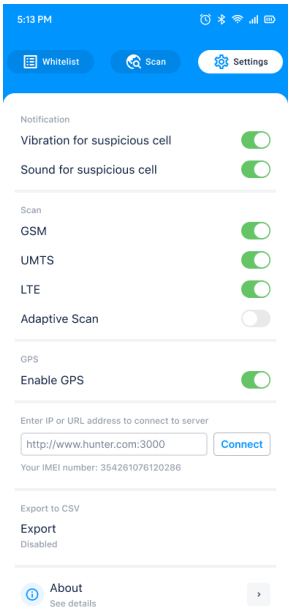


The "Cell Search" feature is a core component of the app, allowing users to identify and analyze nearby BTS signals.

- Network Information: Displays details such as the mobile operator (e.g., Indosat), technology type (LTE, UMTS, GSM), and the status of the signal (e.g., Hunter AR, Hunter G).

- ID and Technical Details: Includes specific technical identifiers like Cell ID, Tracking Area Code (TAC), Physical Cell ID (PCI), and the frequency channel. These identifiers are critical for pinpointing the exact source of the signal.
- Signal Level: Measured in dBm, this indicates the strength of the detected signal. A lower dBm value (e.g., -123 dBm) typically suggests a weaker signal.
- Signal Graphs: Provide a visual representation of signal strength over time or across different channels. This graphical data helps in understanding the stability and strength variations of the detected signal.
- Compass Interface: A visual compass indicating the direction of the detected BTS signal relative to the user's location. This feature, showing distances like "320-400m," assists in locating the physical source of the signal.

4. Settings

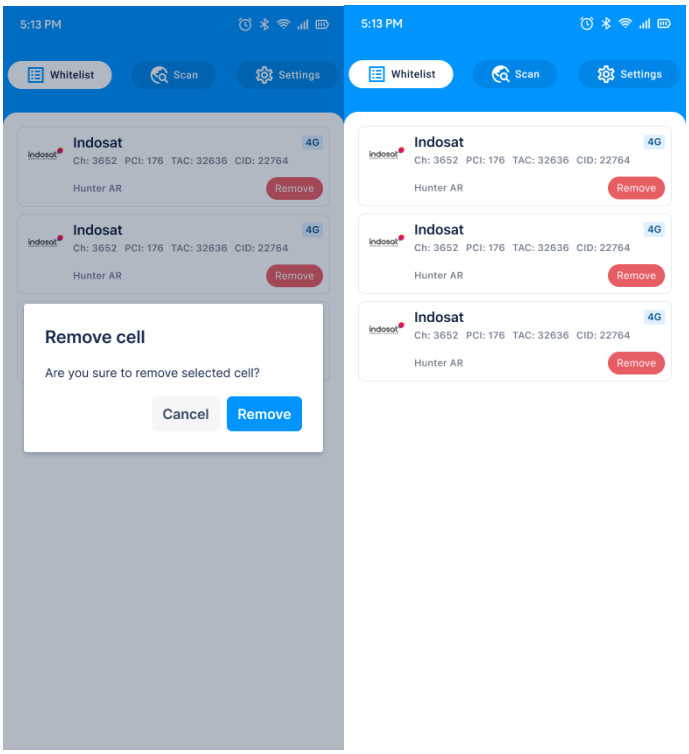


The "Settings" menu is where users can customize the behavior and notifications of the Scavenger Mobile app.

- Notification Preferences: Users can toggle settings for alerts, including vibration and sound notifications, when a suspicious cell is detected. These alerts are crucial for real-time threat detection.

- Scan Options: Allows users to select which types of network technologies to include in the scan (GSM, UMTS, LTE). This customization is important for focusing on specific types of networks or threats.
- Adaptive Scan: An advanced feature that adjusts the scanning frequency and methodology based on the detected signal environment, optimizing both performance and battery usage.
- GPS Settings: Enables or disables the use of GPS data to enhance the accuracy of location-based services within the app. Enabling GPS provides precise geolocation for detected signals, which is critical for identifying the physical location of suspicious BTS.
- Server Connection: This setting allows users to enter a URL or IP address to connect to a server, facilitating remote monitoring or data transfer. This is particularly useful for integrating Scavenger Mobile with larger network security systems.
- Export to CSV: Options for exporting data collected during scans. Users can choose to export data at the end of every scan, after each detection round, or disable export entirely. This functionality is essential for creating records for analysis or reporting.

5. Whitelist Management



Scavenger

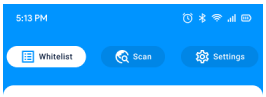
The Whitelist Management feature is designed to allow users to curate a list of trusted BTS signals that should not be flagged as threats.

- Cell List: Displays all cells that have been added to the whitelist, including technical details such as Channel, PCI, TAC, and CID. This helps users quickly identify and manage known safe signals.
- Remove Button: Provides the functionality to remove a BTS from the whitelist. This action is secured by a confirmation dialog to prevent accidental removal.
- Confirmation Dialog: A security feature that asks users to confirm the removal of a cell from the whitelist, ensuring deliberate and considered changes to the list.

MANUAL GUIDE
STEP BY STEP HOW TO USE DEVICE

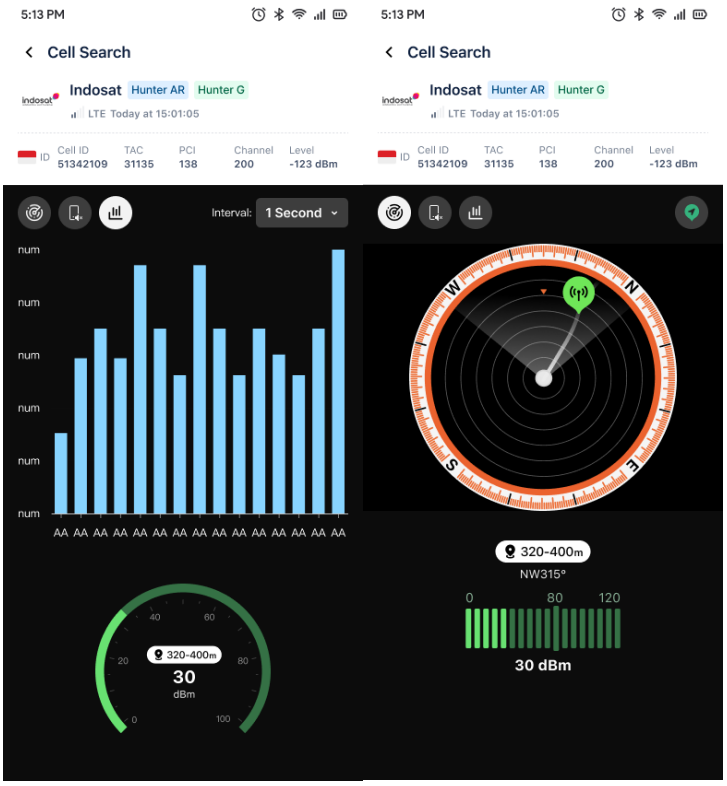
1. Checking for Updates

Regular updates are crucial for maintaining the effectiveness and security of Scavenger Mobile.



- **Step 1:** Open the app and navigate to the "About" section through the settings menu.
- **Step 2:** Tap on "Check for update" under both App Version and Firmware Version. This will check for and download the latest versions, ensuring you have the most up-to-date features and security patches.

2. Initiating a Cell Search

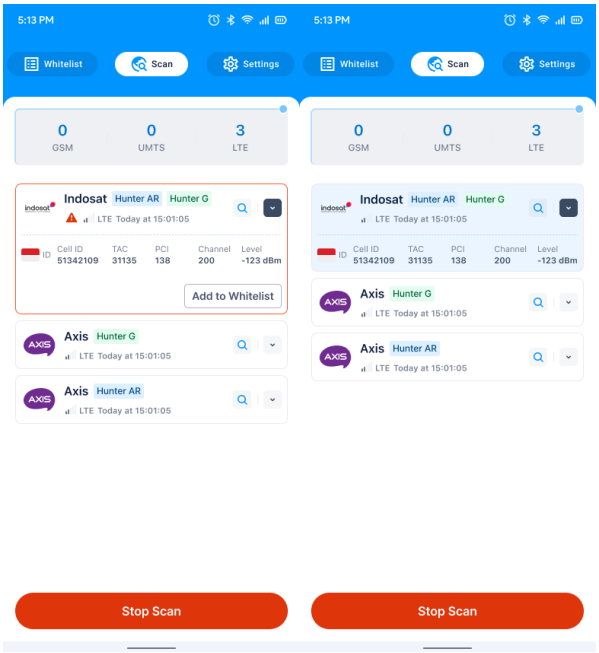


Scanning for BTS signals is the primary function of Scavenger Mobile.

- **Step 1:** From the Home screen, tap the "Scan" button to initiate a search for BTS signals in the vicinity.
- **Step 2:** The application will begin detecting and listing signals. The process involves a comprehensive scan across multiple frequency bands and network technologies.
- **Step 3:** As signals are detected, they will populate the detected signals list with real-time updates on their status and attributes. Use the compass and signal graphs for further analysis.

Scavenger

3. Viewing and Managing Detected Signals

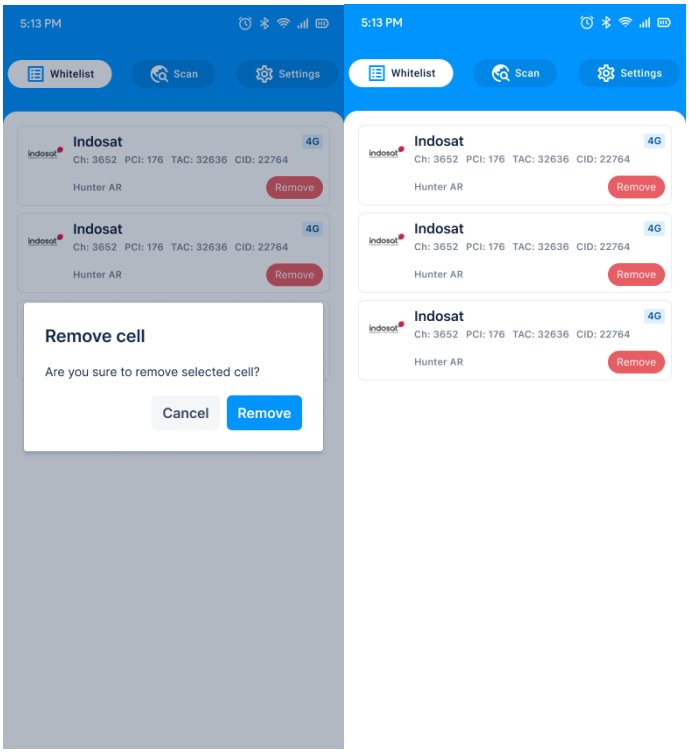


After initiating a scan, users can review and manage the detected signals.

- **Step 1:** Detected signals appear under the "Scan" tab, complete with detailed technical information.
- **Step 2:** Tap on any signal entry to access an expanded view with more detailed metrics, such as Cell ID, TAC, and PCI.
- **Step 3:** If a signal is recognized as benign, it can be added to the whitelist, preventing future alerts.

Scavenger

4. Managing the Whitelist

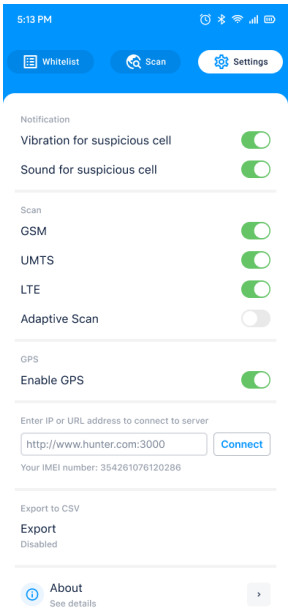


Proper management of the whitelist ensures that known safe signals are not repeatedly flagged.

- **Step 1:** Navigate to the "Whitelist" tab from the Home screen.
- **Step 2:** Review the list of currently whitelisted cells. Each entry provides comprehensive technical details to aid in verification.
- **Step 3:** To remove a cell from the whitelist, tap "Remove" next to the cell. A confirmation dialog will appear to ensure this action is intentional.

Scavenger

5. Configuring App Settings



Customizing app settings tailors Scavenger Mobile's functionality to user preferences.

- **Step 1:** Access the "Settings" tab from the Home screen.
- **Step 2:** Adjust notification settings to specify how alerts should be delivered. Enable options like vibration and sound for immediate notifications.
- **Step 3:** Select which network technologies to include in scans under the "Scan Options" section.
- **Step 4:** Enable GPS to use precise location data for signal detection and mapping.
- **Step 5:** If necessary, configure server settings by entering the appropriate URL or IP address for remote monitoring or data synchronization.

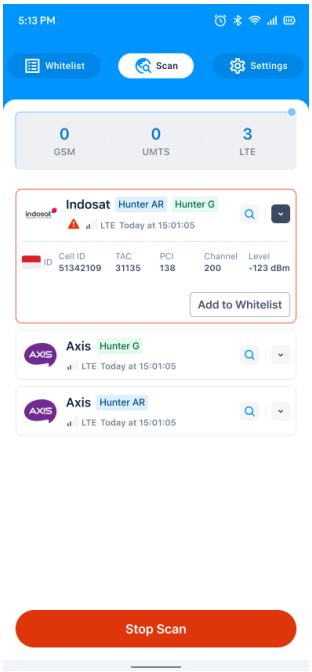
6. Exporting Data

Exporting data is essential for documentation, analysis, and reporting.

- **Step 1:** In the "Settings" menu, find the "Export to CSV" option.

- **Step 2:** Choose the desired export configuration: Disabled, Every round, or On stop scan. This flexibility allows users to manage data outputs according to their operational needs.

7. Handling Detected Threats



Scavenger Mobile is designed to alert users to potential threats in real-time.

- **Step 1:** When a suspicious cell is detected, users will receive an alert based on their notification settings.
- **Step 2:** Review the cell details to assess the threat. Important factors include signal strength, operator information, and signal anomalies.
- **Step 3:** For confirmed threats, ensure they are documented and reported appropriately. Additionally, update the whitelist to avoid future false positives.

Scavenger

Additional Tips and Best Practices

1. **Frequent Updates:** Regularly check for updates to the app and firmware to benefit from the latest security features and performance improvements.
2. **Data Security:** Always secure exported data and sensitive information, especially if it contains details about detected signals and potential threats.
3. **Training and Awareness:** Conduct training sessions for all users to familiarize them with the app's functionalities and best practices in identifying and handling BTS threats.
4. **Device Optimization:** Ensure that the mobile device used is fully compatible with the latest app version to avoid any functionality issues and maintain optimal performance.

Conclusion

This manual serves as a comprehensive resource for effectively utilizing the Scavenger Mobile application. By following the detailed instructions and understanding the technical aspects of each feature, users can significantly enhance their ability to detect and respond to unauthorized BTS signals. For further assistance or technical support, users are encouraged to contact the support team. Your feedback is essential for the ongoing enhancement of our products and services.