Detailed Specification Sheet for Skynet Intel Drone Forensics Software

Skynet Intel Drone forensics suite powered by Rchobbytech Solutions Pvt. Ltd.

The Skynet Intel Forensics Software is a testament to India's technological prowess, proudly carrying the **"Made in India"** label. Designed and developed entirely within the country, this software is a flagship product under the "Make in India" initiative. Moreover, it leverages secure, third-party services for advanced decryption, plotting, and analytics, further reinforcing its foundation as a global product.

Table 1: General Specifications Overview:

Category	Details
About	Skynet Intel Forensics Software provides cutting-edge drone forensics solutions for law enforcement, intelligence agencies, and defence organizations.
Make	**Designed, Developed, and Tested in India** (Made in India Product)
Key Features	- Advanced payload analysis - Hover period detection - Anomalies Detection - Drone Activity Hotspot Analysis - Image metadata processing for forensic evidence - GPS and flight data analysis - Comprehensive outlier detection tools.
Package Contents	Includes high-performance workstations, forensic tools, external storage, manuals, and other accessories.
System Requirements	- OS: Linux (Ubuntu 18.04+), CAINE OS. - Processor: Intel i7/AMD Ryzen 5 or higher. - RAM: 64GB (32GB recommended). - Storage: 2TB SSD.
Functionalities	- Real-time replay of captured drone data - Comprehensive forensic analysis - Visualization tools (e.g., 3D flight paths) - Automated reporting templates.
Integration	- RESTful API for third-party system integration - Supports data formats (CSV, JSON, etc.) - Plugin extensibility for additional features.
Support & Training	- 24/7 support at skynetintel@dronestechlab.com - Training modules for users - Documentation and troubleshooting guides included.
Supported UAVs	Wide compatibility including DJI, Autel, Parrot, Skydio, Yuneec, and hobby drones. *[*Can incorporate Indian-made and foreign drones upon request with a three-month advance notice].*

Table 2: Deliverables Overview for Skynet Intel Forensics System:

Specification	Details
Minimum Requirements	- Laptop with pre-installed Skynet Intel Forensics software - Full forensic toolkit and external storage devices.
Delivery	All items are delivered within the timeline specified in the tender agreement.
Training	Mandatory training sessions for law enforcement and forensic teams to use the software effectively.
Updates & Support	- Regular software updates are provided *[*3 months minimum for new model decryption].* - Technical support is available for operational queries over an official query channel.
Warranty	- Hardware warranty: 1 year - Software: Updates are included for the duration of the license.
Licensing	Software is licensed with a limited, non-transferable duration based on the agreement.
Documentation	Includes user manuals, API documentation, and reporting templates.

Table 3: Workstation Technical Specifications:

Specification	Details
Operating System	- Linux (Ubuntu 18.04+ or derivatives) - CAINE OS (preferred forensic OS).
Processor	- Minimum: Intel i7 8th Gen or AMD Ryzen 5 equivalent. - Recommended: Intel i9 or AMD Ryzen 7 or higher for optimal performance.
RAM	- Minimum: 32GB DDR4. - Recommended: 64GB or higher for heavy forensic processing.
Storage	- SSD: Minimum 2 TB NVMe SSD for faster read/write speeds.
Graphics(Optional)	Optional Any compatible mode
Cache	- Minimum: 24MB L3 cache.

Table 4: Extraction and Decryption:

Extraction Method	Description
SD Card(not available for all drones)	Extracts data directly from a drone's onboard SD card. Compatible with FAT32, exFAT only.
Decryption Mode	Software should be capable of decrypting/parsing encrypted /unencrypted files/logs either through a dedicated server or a secured file transfer method.

Table 5: Supported Drones for Data Decryption and Analysis:

Manufacturer	Supported Models
DJI	Full Mavic Series (Mavic Mini to Mavic 3 Pro). Phantom Series (Phantom 3 to 4 Pro V2). Matrice Series (Matrice 200, 300 RTK, 600). Inspire 1 & 2, and DJI FPV.
Autel	EVO II Series, including RTK and Enterprise models. EVO Pro Series, Dual 640T, 320.
Parrot	Anafi Series, Bebop 2, and Bluegrass.
SwellPro (Splash)	SplashDrone 4, 3+, Fisherman Max FD2.
Skydio	Skydio 2+, Skydio X2D/X2E.
Yuneec	Typhoon H Series, H520E.
Hobby Drones	Pixhawk, Arducopter, PX4/Ardupilot-based drones.

Table 6: File Types for Decryption:

The Skynet Forensics Software supports the decryption and analysis of the following file types for drone forensic investigations. Other formats can also be supported based on specific requirements and requests.

File Type/Format	Description
DJI Log Files	Supported formats include .DAT, .TXT, and encrypted flight logs generated by DJI drones.
Pixhawk MAVLink	Includes .ULG and .BIN files are used by Pixhawk-based drones for flight telemetry and mission data.
Ardupilot Log Files	Covers .BIN and .LOG files generated by Ardupilot for flight telemetry.
Parrot Log Files	Parrot Anafi and other Parrot drones' flight log files (e.g., .TXT, .JSON).
Autel Log Files	Logs generated by Autel EVO drones, including encrypted telemetry files.
Yuneec Log Files	Covers telemetry and diagnostic logs from Yuneec drones (e.g., BIN. .CSV).
SwellPro Log Files	Logs for SplashDrone series, including diagnostic and operational data files.
Custom/Other Formats	Additional formats can be supported upon user request, including proprietary or encrypted file types.

Table 7: Key Features in Detail:

Feature	Description
Advanced Payload Analysis	Analyzes payload data for potential threats, including payload type and anomalies.
Hover Period Detection	Monitors the hover time of drones to identify unusual or suspicious patterns.
Anomalies Detection	Detects irregularities in flight behavior, such as erratic movements or deviations from planned routes.
Hotspot Analysis	Identifies areas with high drone activity to pinpoint potential security risks or surveillance zones.
Image Metadata Processing	Processes image metadata to extract forensic evidence, including timestamps and GPS coordinates.
GPS and Flight Data Analysis	Analyzes GPS logs and flight paths for detailed insights into drone operations and trajectories.
Comprehensive Outlier Detection Tools	Utilizes algorithms to identify outliers in flight patterns, aiding in forensic investigations.

Table 8: Features of Skynet Intel Digital Drone Forensics Software:

Feature	Description
Multi-Drone Data Correlation	Correlates data from multiple drones to analyze coordinated activities and patterns.
3D Flight Path Visualization	Visualizes drone flight paths in an interactive 3D environment for better analysis.
Multivariate Analysis	Analyzes multiple variables simultaneously to detect correlations and patterns across datasets.
Pattern Detection	Recognizes repeated flight behaviors or operational patterns indicative of specific drone activities.
Temporal Data Analysis	Examines data across time to identify trends or deviations in drone operations.
3D Environment Reconstruction	Reconstructs drone activity in a 3D environment for detailed spatial analysis.
Online and Offline Maps Integration	Supports integration with online mapping services (e.g., Google Maps) and offline map databases for seamless geospatial analysis.
Timestamps and Metadata Extraction	Extracts and processes timestamps geotags, and metadata for accurate event reconstruction.
Automated Report Creation	Generates comprehensive forensic reports, including key findings, visuals, and recommendations in PDF or CSV formats.