Secfore

CUTTING-EDGE
MOBILE INTELLIGENCE

ABOUT
SECFORE

Secfore, a brand under Aspirify Enterprise Pvt. Ltd., has led India's Information Security landscape for nearly 20 years, driven by a passion for research and innovation.

MAKE IN INDIA

At **Secfore,** we pride ourselves on being a leading industry player, with a strong commitment to quality, innovation, and customer satisfaction.

Our Benefits

17+
Years of Vast
Industry Experience

100+
Information Security &
Forensics Experts

20+
Manufacturer
Supported

About Us

At **Secfore**, we are committed forensic professionals dedicated to delivering innovative solutions and groundbreaking research. Through collaboration and cutting-edge technology, we empower our clients and cultivate strong partnerships to meet their unique needs.

Our Core Principles

At **Secfore**, our commitment, accountability, sense of belonging, and strong ethics ensure that we deliver reliable and trustworthy solutions for our clients.

Our Team

We actively recruit top global talent to join our growing team, valuing dedication, integrity, hard work, collaboration, and exceptional technical expertise to provide our clients with innovative and effective solutions.

PRODUCT OVERVIEW
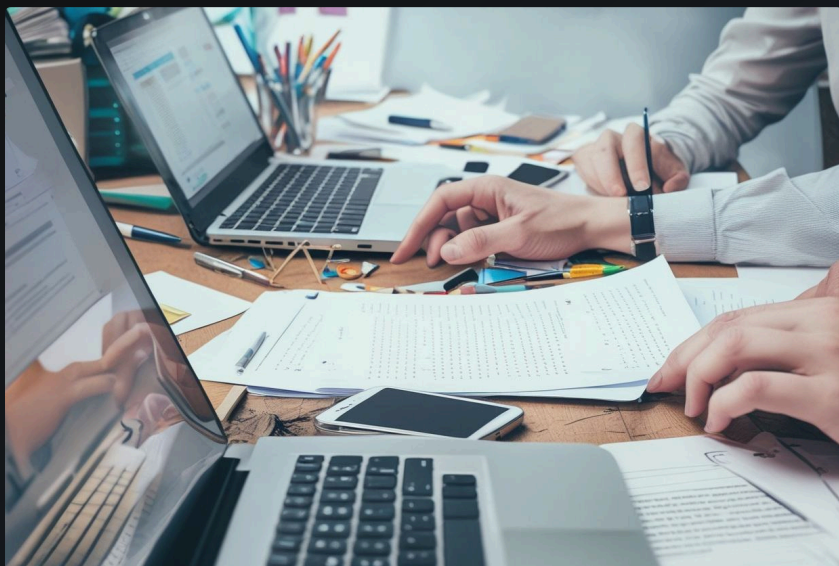
Supports the latest Android versions, including Logical and Full File System Extraction

Provides support for the latest iPhones, including Logical and Full File System Extraction **Beta**

AI-Embedded Solutions, Visualization, Analytics, and Cloud Extraction (Beta)

Extractor

A comprehensive platform for forensically sound extractions of Android and iOS devices. Smart Extract significantly reduces extraction time while offering versatility for diverse forensic needs.

Visualizer

Visualizer empowers investigators to parse, decode, decrypt, analyze, and explore evidence. Driven by AI, it provides unique insights, uncovers critical clues, and accelerates case resolution.

Minimum Requirement

- Processor: Intel Core i5, 11th Generation
- RAM: 8GB
- Operating System: Windows 10
- Storage: 500GB
- GPU: 6GB (*Exclusively for Image Classification)

Recommended Requirement

- Processor: Intel Core i7/i9, 12th Gen or above
- RAM: 32GB or higher
- Operating System: Windows 10 or higher
- Storage: 1TB SSD
- GPU: 8GB NVIDIA

SUPPORTED DEVICES

We support the latest Android devices and iOS (Beta), offering Logical Extraction, Full File System Extraction, App Data Extraction, and more.

|	
SAMSUNG	Samsung Galaxy S, Note, A, M, J series, On7 Pro, and more
G	Pixel 3a, 4 XL, 5, 5a, 6a, 7, 7 Pro, 8, 8 Pro
1+	OnePlus 6T, 7, 7T, 8T, 9, 9R, 10R, Nord CE2, Nord CE3, Nord 3
mi	Redmi Note 5–13, 8A–13C, A1+, 10, 9 Pro, 11, 12 Pro and more
iQOO	iQOO 7–12, 7–Neo 9, Z3–Z8, U1–U5, SE
vivo	Vivo S, Y Series (S1–S19, Y01–Y100)
OPPO	OPPO A52–A78, F9–F15, Reno Series
realme	Realme 1–12, 10 Pro, Narzo Series, GT Series
HUAWEI	Huawei P30 Lite, P50/Pro, Y9s/Prime, Nova 9SE; Honor 7X, 9A, 9N
motorola	Moto G Series (G1–G100, G42, G82 5G)
Infinix	Infinix Smart Series (Smart 1–Smart 8)
NOKIA	Nokia A Series, C Series, G Series, X Series
ZTE	ZTE V Series, A Series, Blade Series, Axon Series
nubia	Nubia V Series, Z Series, RedMagic Series
NOTHING	Nothing Phone (1), (2), (2a), and CMF Phone 1A/2A
LG	LG Nexus Series, G Series, V Series, Velvet, Wing
TECNO	Spark Go 2020/2021, Spark 7/7T, Spark 8/8C, Pop 5/6/9, Camon 30
Beta	iPhone X, Series 11 to 16, and iPads

SF EXTRACTOR
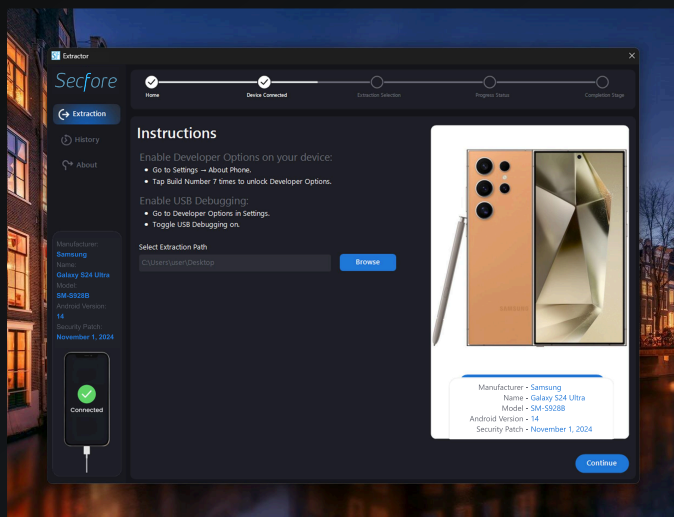
📱 Wide Support

Supports a wide range of devices.

✓ Supports various manufacturers and devices

✓ Broad compatibility with Android and iOS **(Beta)**

✓ Supports Custom App Data Extraction

⤴ Extraction Selection

Fast and Thorough Extraction.

✓ Extraction of App-Specific Data

✓ App Data Extraction, including Encrypted Apps
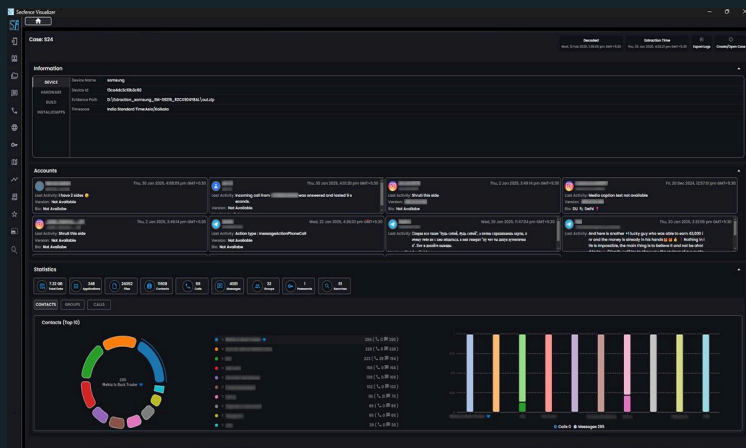
✓ Logical and File System Data Extraction
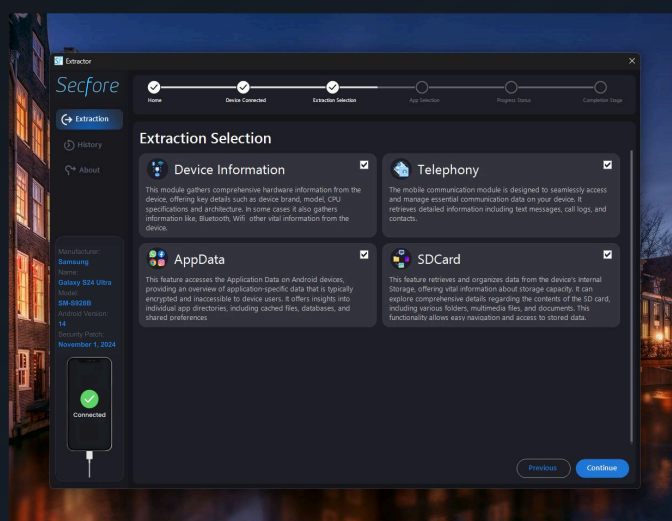
📄 Log Monitoring

A comprehensive log view that aggregates and displays all extracted data in one place.

✓ Real-time monitoring with enhanced visibility

✓ We provide dual functionality for App View and Log View with a simple click on the toggle

✓ Retrieve the extraction time for each app's data
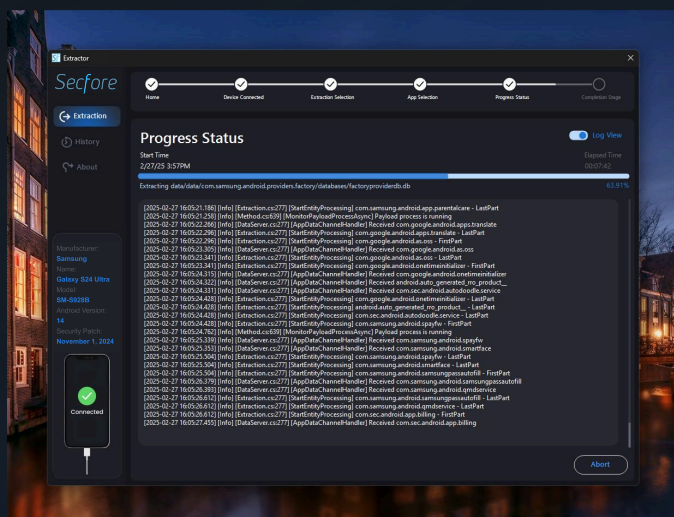
▣ VISUALIZER

🏠 Dashboard

Offers a comprehensive overview of all data at a glance.

- ✓ Detailed Device Information
- ✓ Owner's Information, including the top 10 contacts, social media profiles, and statistics
- ✓ Visual Analytics for Applications, Calls, and Messages Usage

⁺👥 Accounts

Shows device details, accounts, and social activity.

- ✓ Displays model, security patch, resolution, chipset, and RAM
- ✓ Lists linked accounts including WhatsApp, Instagram, Facebook, Gmail, and Zangi
- ✓ Tracks calls, call logs, and messages with interaction details
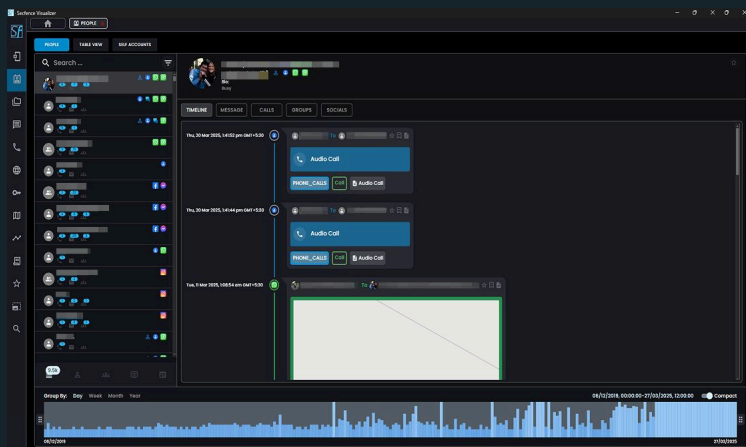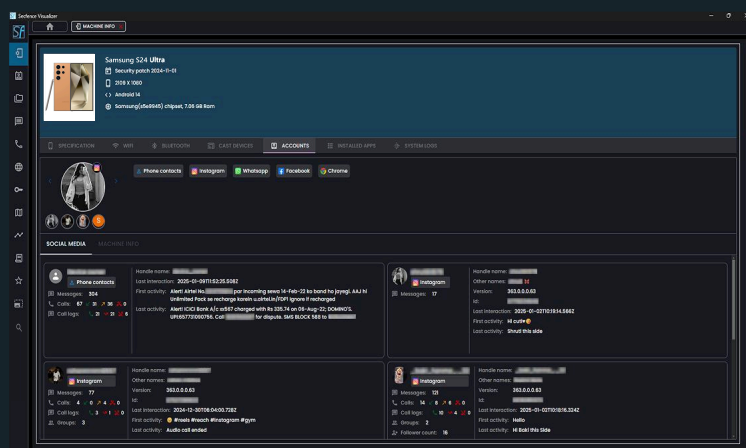
👥 People View

People View consolidates all entities into a single dashboard.

- ✓ View Calls, Messages, Transactions, and social media from a Person of Interest
- ✓ Cross-Messenger View
- ✓ Enhanced Filtering Options

◲ Gallery View

A consolidated view of all media data for effortless access and analysis.

✓ AI-Driven Image Classification

✓ Face and Person Detection

✓ Payment Data, QR Code Recognition, and OCR

✓ Detection of Nudity, Weapons, Vehicles, License Plates, Text, and Contextual Search
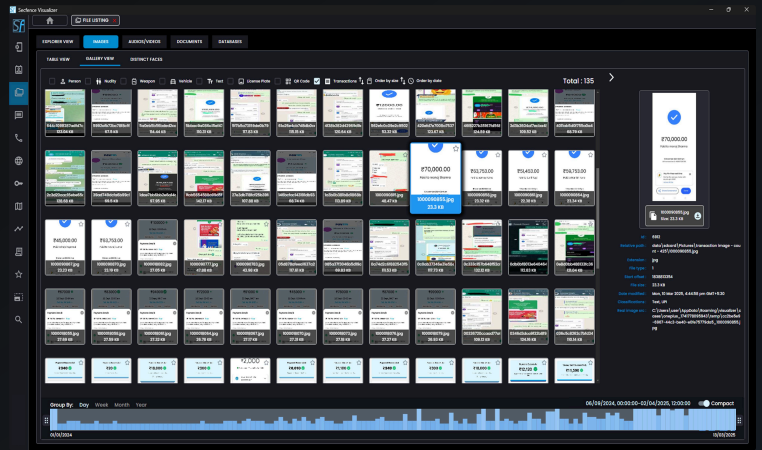

⬡ Hex Editor

Comprehensive analysis of known and unknown file formats.

✓ Integrated Hex Editor

✓ Byte Inspection Tool

✓ File Information

SQL SQLite Explorer

Analyzes SQLite databases to recover user and app data.

✓ Tree-view interface with powerful search for quick access to complex database structures

✓ View structured data with smart columns and specialized BLOB/binary viewers

✓ Powerful search, sorting, and customizable filters enable efficient analysis of database contents.
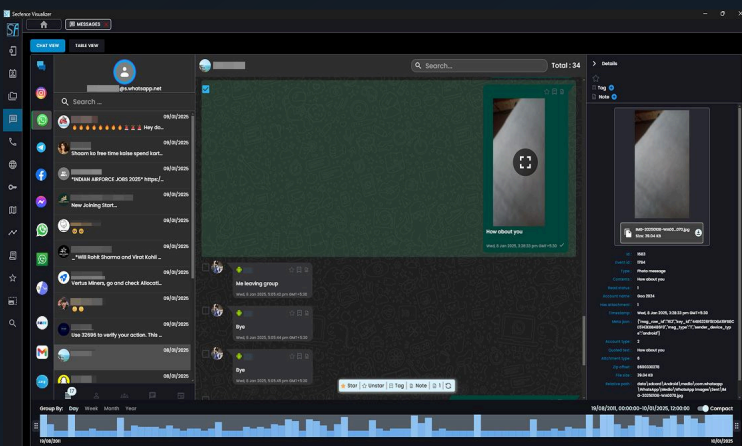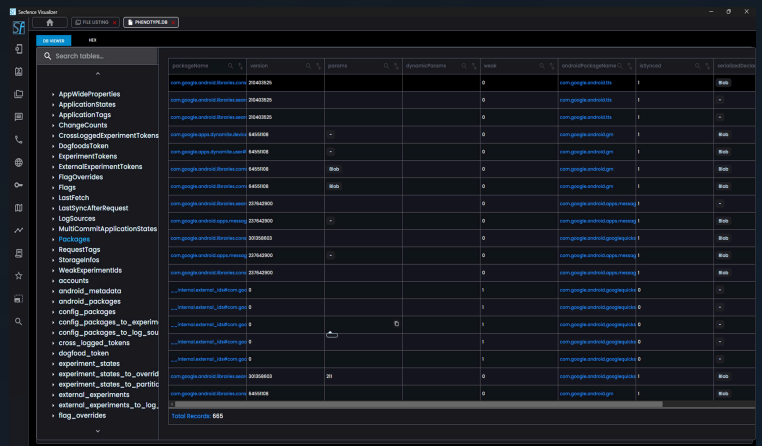
🗎 Smart View

Realistic representation to gain unparalleled insights.

✓ Combines communication and media data for complete context

✓ Media with previews from Telegram, WhatsApp (FM & GB), Facebook, Messenger, GPay, Paytm Chat, and Zangi

✓ SmartChrono – Simplifies timeline analysis with intuitive controls.

📞 Call Log

Shows contacts, call details, and graphical call insights.

✓ Displays VoIP, audio, and video calls with timestamps, status, and duration

✓ Call status, directions, and audio/video distribution visualized for quick analysis

✓ Calls can be grouped by day, week, month, or year for timeline-based investigation
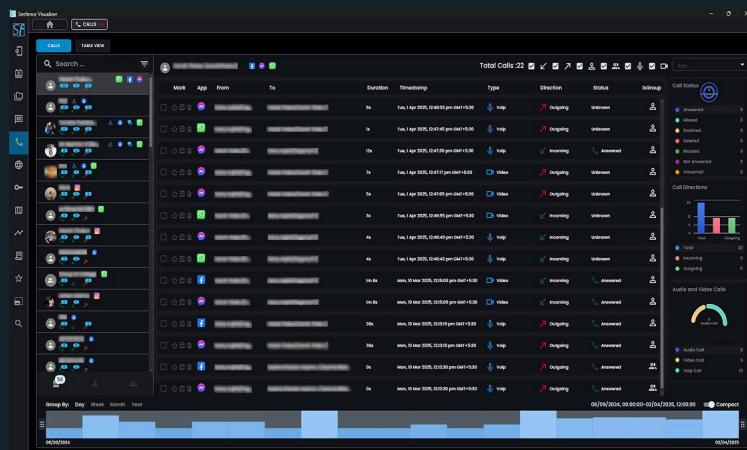
🌀 Browser

Displays browser activity with visited sites, timestamps, accounts, and URL paths.

✓ Displays browsing history with timestamps and account details

✓ Shows website titles, favicons, open tabs and URLs for quick identification

✓ Includes data paths for forensic analysis

🔒 Password

The interface provides a structured view of saved passwords.

✓ Displays the app where the credentials are used

✓ Records creation, last update, and last usage details

✓ Shows the username, password, and associated URL

📍 Geolocation

Location Intelligence: Integrating Data from Multiple Sources and Offline Maps.

✓ EXIF Data from Images

✓ Google Timeline Location

✓ Instant Messaging Data, including WhatsApp Live and Shared Location

✓ Additional Location-Based Data Artifacts
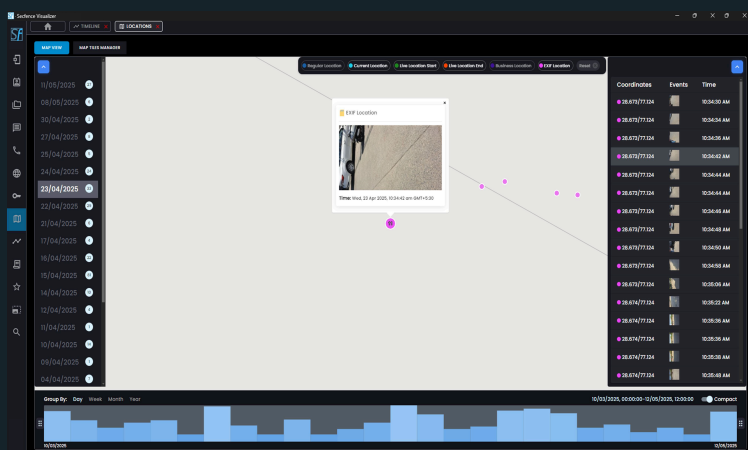
📈 Timeline

Examine events across evidence in a clear chronological sequence.

✓ Events from Instant Messaging, Browsers, Telephony, System Logs (Reboot, Install, etc.) and more

✓ Advanced Filtering Options

✓ Unique time-linked perspective

🖼️ Transaction

Shows structured transaction reports with timestamps, parties, types, banks, and reference IDs.

✓ Tracks debits and credits with timestamps

✓ Shows linked bank and account numbers

✓ Unique transaction identifiers for verification

✓ Google, Paytm, and UPI transaction history

🔍 Search

OCR and image-based advanced context search across data sources.

✓ Full-text and semantic search across logs, messages, transactions, and browser data

✓ Extracts and indexes text from scanned documents, images, and screenshots

✓ Context-aware indexing and retrieval of visual content based on metadata
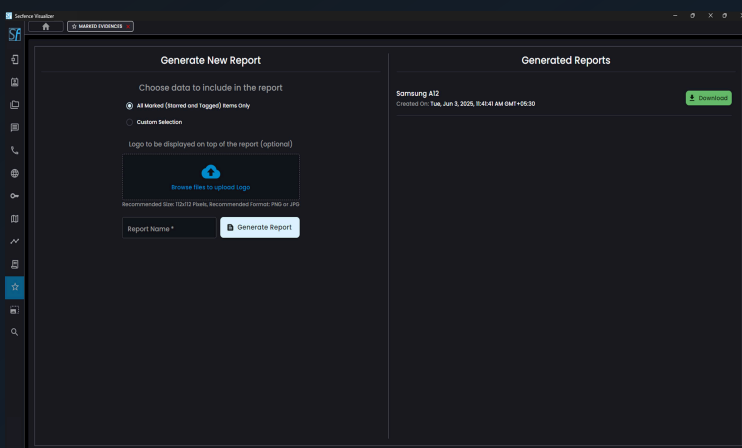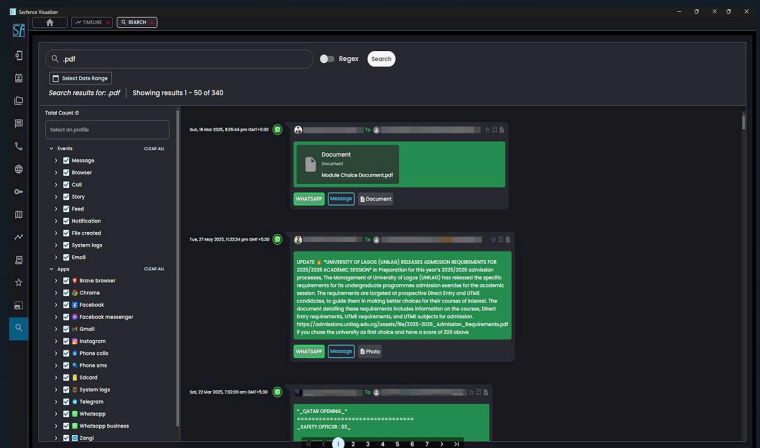
🏷️ Reporting

Includes case, examiner, agency, and hashes.

✓ Shows case, examiner, and timestamps

✓ Includes MD5, SHA-1, SHA-256, and SHA-512 hashes for validation

✓ Generates and views reports for legal and forensic use

✓ Customizable reports with agency logo support

REVEAL HIDDEN CLUES.
DISCOVER THE EVIDENCE.
CLOSE THE CASE.

SCAN TO CONNECT

SCAN TO CONNECT