Nigrani

IPDR FORENSIC ANALYZER

A forensic-grade digital communication analysis system
built for Indian law enforcement agencies.

Analyze IP Detail Records (IPDR) with precision to detect applications,
VoIP calls, VPN usage, and generate court-ready forensic evidence packages.

v1.0.0 | Production Ready

Developed by HC S. Umesh | dev_soft.in

Digital Forensics & Telecom Analysis Solutions

Generated: 18 February 2026

Key Statistics

Nigrani at a glance

Metric	Value
Total Applications Detected	97+
VoIP Apps with Confidence Scoring	31
Detection Categories	10
Named VPN Services	9
Forensic Export Files	8 (PDF, CSV, JSON, TXT)
Supported Encodings	4 (UTF-8, Latin-1, CP1252, ISO-8859-1)
Confidence Scoring Weights	5 factors (Domain, Infra, STUN, Port, Traffic)
Classification Levels	3 (Inconclusive, Probable, Confirmed)
Infrastructure Providers	Meta, Google, Cloudflare, AWS, Azure, Telegram, App-owned
Input File Types	CSV, XLSX, XLS

Key Capabilities

Purpose-built features for telecom forensic investigations

Application Detection

[Forensic Grade]

Identify 97+ applications across messaging, email, cloud storage, browsers, VPN, cryptocurrency, AI, streaming, betting, and business VoIP categories using domain signatures and infrastructure analysis.

VoIP Call Detection

[Court Ready]

Detect voice and video calls from 31 VoIP-capable applications with weighted confidence scoring. STUN/TURN port detection, ephemeral port analysis, and bidirectional traffic verification.

VPN Detection

[ASN Enhanced]

Score-based VPN detection (0-100) with protocol identification (OpenVPN, WireGuard, IPSec/IKE, L2TP). ASN-based VPN provider identification across 9 named services.

Forensic Evidence Export

[SHA-256 Verified]

Generate court-ready forensic packages with PDF report, activity logs, session analysis, VoIP detections, IP-ASN mapping, SHA-256 file hashes, and complete metadata.

Geo Intelligence

[GeoLite2]

Enrich IP addresses with geographic location, city, country, and ASN/organization data using MaxMind GeoLite2 databases. Map communication endpoints globally.

Session Reconstruction

[Auto Grouping]

Automatically group records by subscriber with 30-minute inactivity gaps. Generate session summaries with total bytes transferred, domains visited, and apps used per session.

DOT Format Support

[Multi-File]

Native support for Department of Telecommunications (DOT) IPDR file format. Automatically handles metadata rows, footer cleanup, multi-file combining, and encoding detection.

Forensic Narratives

[Legal Safe]

Generate legally-safe forensic descriptions suitable for court disclosure. Confidence levels classified as Inconclusive, Probable, or Confirmed with supporting evidence breakdown.

Application Detection Categories

Comprehensive coverage across 10 categories of digital applications

Messaging & VoIP (20 apps)

WhatsApp, Telegram, Signal, Facebook Messenger, Discord, Viber, Skype, Google Meet, Google Voice, Wire, Session, Threema, Element/Matrix, BiP, Zangi, BIGO, IMO, Mastodon, BOTIM, Beeper

Business VoIP (10 apps)

OpenPhone, Aircall, Dialpad, Grasshopper, GoTo Connect, Ooma, Vonage, RingCentral, Nextiva, 8x8

Email Services (4 apps)

Gmail, Yahoo Mail, Hotmail/Outlook, ProtonMail

Cloud Storage (14 apps)

OneDrive, ProtonDrive, Google Drive, TeraBox, iCloud, Dropbox, MEGA, AWS S3, Alibaba Cloud, Apple Cloud and more

VPN Services (9 apps)

NordVPN, ProtonVPN, ExpressVPN, TurboVPN, FreeVPN, SecureVPN, SuperVPN, VPN360, OperaVPN

Browsers (8 apps)

Chrome, Brave, DuckDuckGo, Tor, Opera, Bing, Safari, Firefox

Crypto & Trading (9 apps)

CoinDCX, CoinSwitch, Binance, WazirX, KuCoin, ZebPay, MetaMask, TrustWallet, MudRex

AI Assistants (8 apps)

ChatGPT, Gemini, Deepseek, MetaAI, PerplexityAI, AskAI, Microsoft Copilot, Grok

Streaming (7 apps)

Netflix, Amazon Prime, Zee5, Hotstar, SonyLiv, MXPlayer, Twitch

Betting & Exchange (7 apps)

Laser247, KalyanExch, SkyExchange, LotusBook247, Fairbet, 99Exchange, BetBhai

VoIP Call Detection Engine

Weighted confidence scoring for forensic-grade voice/video call detection

Confidence Scoring Weights

Factor	Weight
Domain Match	30%
Infrastructure Match	15-25%
STUN/TURN Detection	15-20%
Media Port Analysis	15-25%
Traffic Pattern	15%

Detection Criteria

Parameter	Value
STUN/TURN Ports	3478, 3479, 5349, 19302
Ephemeral Ports	≥49152 (high port analysis)
Min Data Volume	100KB bidirectional
Min Duration	15 seconds
Video Threshold	>50 KB/s = video call

Classification Levels

Level	Description
Inconclusive	Insufficient evidence for determination
Probable Messaging/Voice/Video	Moderate confidence based on pattern matching
Confirmed Voice/Video Call	High confidence with corroborating evidence from multiple signals

Law Enforcement Use Cases

How Nigrani supports criminal investigations and digital forensics

Cyber Crime Investigation

Analyze suspect communication patterns across messaging apps, identify encrypted VoIP calls on WhatsApp/Signal/Telegram, detect use of privacy tools like VPNs and Tor browser, and establish digital timelines for court proceedings.

Financial Fraud & Crypto Tracking

Detect usage of cryptocurrency exchanges (Binance, WazirX, CoinDCX), trading platforms, and digital wallets (MetaMask, TrustWallet). Identify suspicious financial activity patterns in IPDR data.

Online Betting Investigation

Identify access to illegal betting platforms (Laser247, KalyanExch, SkyExchange, LotusBook247) through domain and infrastructure detection. Establish frequency and duration of suspect access patterns.

CDR/IPDR Court Submissions

Generate forensic evidence packages with SHA-256 hash verification, chain-of-custody documentation, and legally-safe forensic narratives suitable for presenting in Indian courts under IT Act provisions.

Suspect Communication Profiling

Build comprehensive digital profiles of suspects by analyzing which apps they use, when they communicate, who they contact (via IP analysis), and whether they use privacy-enhancing tools. Session reconstruction reveals usage patterns.

Missing Persons & Kidnapping

Trace last known digital activity through IPDR analysis. Identify geo-location via IP addresses, determine active communication channels, and reconstruct timeline of events leading to disappearance.

Narcotics & Organized Crime

Detect use of encrypted messaging apps (Signal, Wickr, Session) commonly used in drug trafficking. Identify communication bursts, unusual timing patterns, and VPN usage that may indicate coordinated criminal activity.

Terrorism & National Security

Analyze communication patterns for indicators of radicalization and coordination. Detect use of privacy-focused apps (Signal, Tor, ProtonMail), AI assistants, and encrypted cloud storage services.

Forensic Evidence Package

Court-ready export with complete chain-of-custody documentation

File	Description
report.pdf	Comprehensive PDF report with forensic analysis, charts, application detections, VoIP calls, and session summaries
summary.json	Machine-readable analysis summary with all detection metrics, confidence scores, and statistical breakdowns
activity_log.csv	Complete enriched activity data with per-row application detection, VoIP flags, geo data, and ASN information
session_analysis.csv	Reconstructed subscriber sessions with total bytes, duration, domains visited, and applications used
voip_detections.csv	Detected VoIP calls with application name, confidence score, classification level, and other party details
ip_asn_mapping.csv	Complete IP-to-ASN/Organization mapping with VPN confidence flags and infrastructure classification
metadata.txt	Analysis metadata including tool version, processing date, file statistics, and configuration parameters
file_hashes.txt	SHA-256 cryptographic hashes for every file in the package, ensuring integrity and tamper detection

Technical Specifications

System requirements and input format specifications

Required IPDR Columns

Field	Expected Column Name
Subscriber ID	Landline / MSISDN / MDN
Source IP	Source IP Address
Source Port	Source Port Number
Public IP	Public IP Address
Public Port	Public IP Port
Destination IP	Destination IP (IPv4/IPv6)
Destination Port	Destination Port Number
Timestamp	TIME1 / Event_Start_Time
Network Info	APN, PGW, IMSI
Duration	Session Duration
Data Volume	Up Link / Down Link bytes

DOT IPDR File Format

Parameter	Details
Rows 1-11	Metadata (auto-skipped)
Row 12	Column headers (auto-detected)
Rows 13+	Data records
Footer Rows	Auto-detected metadata rows removed
Encoding	UTF-8 / Latin-1 / CP1252 / ISO-8859-1
File Types	CSV, XLSX, XLS
Multi-File	Combine multiple IPDR files into single analysis
Geo Enrichment	MaxMind GeoLite2 (CSV format)

Deployment Options

Flexible deployment for different operational environments

Web Application

Browser-based Streamlit interface accessible from any device. No installation required. Ideal for centralized forensic labs with multiple analysts.

Best for: Forensic labs, multi-user access, quick analysis

Desktop Application

Native Windows application (PySide6) with offline USB dongle licensing. Complete standalone operation without internet connectivity.

Best for: Field officers, air-gapped networks, portable use

USB Dongle Distribution

All-in-one USB deployment with serial-bound license, installer, and documentation. Prevents unauthorized copying. Hand the USB to the customer.

Best for: Secure distribution, license management

USB Dongle Licensing Security

Feature	Details
Encryption	Fernet (AES-based) encryption for license files
Expiry	Date-based license validity enforcement
Clock Tamper	Detection and prevention of system clock manipulation
USB Detection	Automatic detection on removable and fixed drives
Serial Binding	License bound to specific USB drive serial number
Copy Protection	Prevents license file copying to unauthorized drives

Developer Information

Developed for Law Enforcement by

HC S. Umesh
Digital Forensics & Telecom Analysis Solutions

https://dev_soft.in

Document generated on 18 February 2026 at 11:58