AI-Powered Network Packet Analysis for Enhanced Insights

Posted on September 7, 2025 by Admin

Case Study

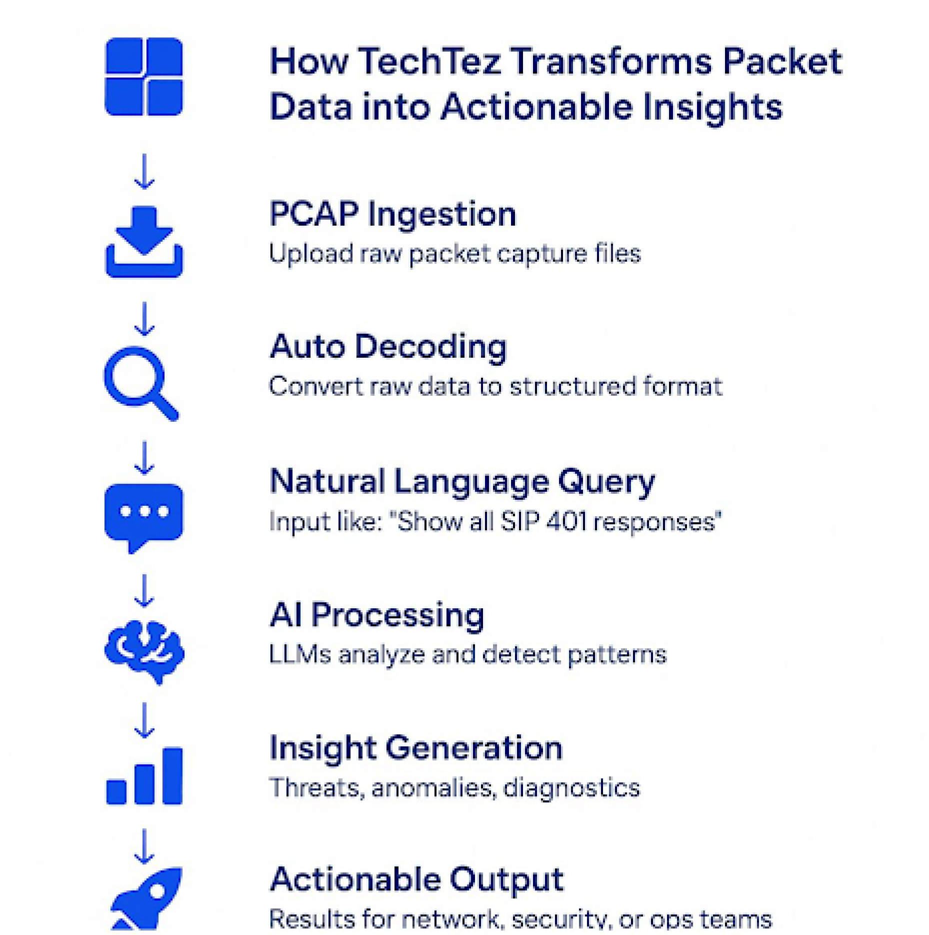
Linkedin X-twitter

Facebook

AI-Powered Network Packet Analysis for Enhanced Insights

Client

A telecom provider managing VoIP and 5G core traffic sought to modernize packet analysis across their operations and engineering teams.



How TechTez Transforms Packet Data into Actionable Insights

↓

PCAP Ingestion
Upload raw packet capture files

↓

Auto Decoding
Convert raw data to structured format

↓

Natural Language Query
Input like: "Show all SIP 401 responses"

↓

AI Processing
LLMs analyze and detect patterns

↓

Insight Generation
Threats, anomalies, diagnostics

↓

Actionable Output
Results for network, security, or ops teams

Challenges

Conventional network analysis tools face significant limitations in handling the volume and complexity of modern network packet capture (PCAP) files.

- ✓ **Lack of Native AI Capabilities:** Traditional tools lack built-in AI for direct analysis of PCAP files, relying on manual inspection or rule-based systems. This makes identifying subtle patterns or anomalies time-consuming and prone to error.

- ✓ **Data Complexity and Decoding:** Raw packet data is complex and requires extensive decoding prior to analysis. This adds time and complexity, hindering real-time insights or rapid incident response.

- ✓ **Difficulty in Deriving Actionable Insights:** Merely viewing packet data is insufficient; the real value lies in actionable insights like identifying threats or diagnosing performance issues. Traditional methods struggle to automatically glean these insights, demanding significant manual effort and domain expertise, leading to delayed responses.

- **Scalability and Time Consumption:** With increasing network traffic, PCAP files become enormous, and conventional methods often struggle to scale efficiently. Manually sifting through vast amounts of data is inefficient, increasing Mean Time To Respond (MTTR).

- **Limited Querying Capabilities:** Existing tools offer rigid filtering, restricting nuanced, context-aware investigations. Complex queries like "Show all SIP 401 Unauthorized responses with nonce values" are difficult to perform.

Our Solution:

TechTez addressed these pain points by developing an advanced, AI-powered packet analysis platform, placing automated intelligence and flexible query power directly into usKey Features:

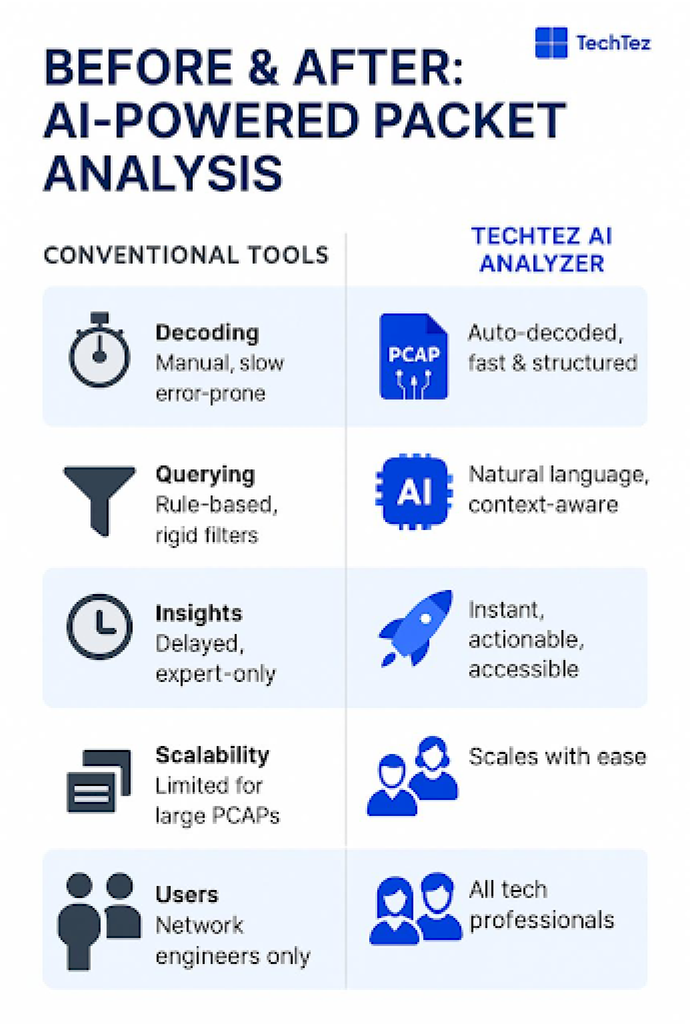
- ✓ **Intelligent Packet Decoding:** Fully automated decoding transforms raw packet data into clean, structured records—removing manual complexity and speeding up analysis.

- ✓ **Natural Language AI Query Engine:** Users simply ask questions in plain English (“Which packets contain Call-ID 12345?” “Show me all RTP streams with payload type 96”), and the platform delivers actionable results instantly.

- **Actionable Insights via LLMs:** Leveraging leading Large Language Models (ChatGPT, Ollama, Mistral, Gemini), the system identifies patterns, detects anomalies, and generates insights beyond traditional tool capabilities.

- **Comprehensive Protocol Support:** Deep analysis across all major protocols (SIP, RTP, DIAMETER, HTTP, GTP, TCP, UDP, IPv4/6, TLS/SSL, SCTP, NGAP, PFCP, and more).

- **Scalable & User-Friendly:** Optimized for performance with large datasets, the interface empowers both experts and non-specialists—democratizing access to critical network intelligence.



TechTez

BEFORE & AFTER: AI-POWERED PACKET ANALYSIS

CONVENTIONAL TOOLS	TECHTEZ AI ANALYZER
Decoding Manual, slow error-prone	Auto-decoded, fast & structured
Querying Rule-based, rigid filters	Natural language, context-aware
Insights Delayed, expert-only	Instant, actionable, accessible
Scalability Limited for large PCAPs	Scales with ease
Users Network engineers only	All tech professionals

Results & Impact

- Faster, More Accurate Diagnostics: Automated decoding and AI insights cut incident response time and reduced manual effort, freeing teams to focus on high-value tasks.

- Actionable Intelligence: Proactive threat detection, performance monitoring, and troubleshooting—made possible in seconds, not hours.

- Empowered Teams: Anyone can perform complex packet analysis via natural language, eliminating the steep learning curve for new users.

- ✓ Scale Without Limits: The platform processes the largest PCAPs effortlessly, ensuring continuous effectiveness as network traffic grows.

- ✓ Deeper, Granular Insights: Rich protocol and field support enable precise, context-aware investigations, unlocking a complete view of network events.

Outcomes

Reduction in incident response time
70%
Lower operational costs
30%
Less unplanned downtime
45%
jump in customer satisfaction

25%
improvement in bandwidth utilization
Up to 15%

Our Thought Leadership Guides

- Case Study

Simplifying Complex Telecom Integrations Using a Scalable Numbering Platform

A mid-sized SaaS company specializing in HR and payroll management faced a growing barrier:

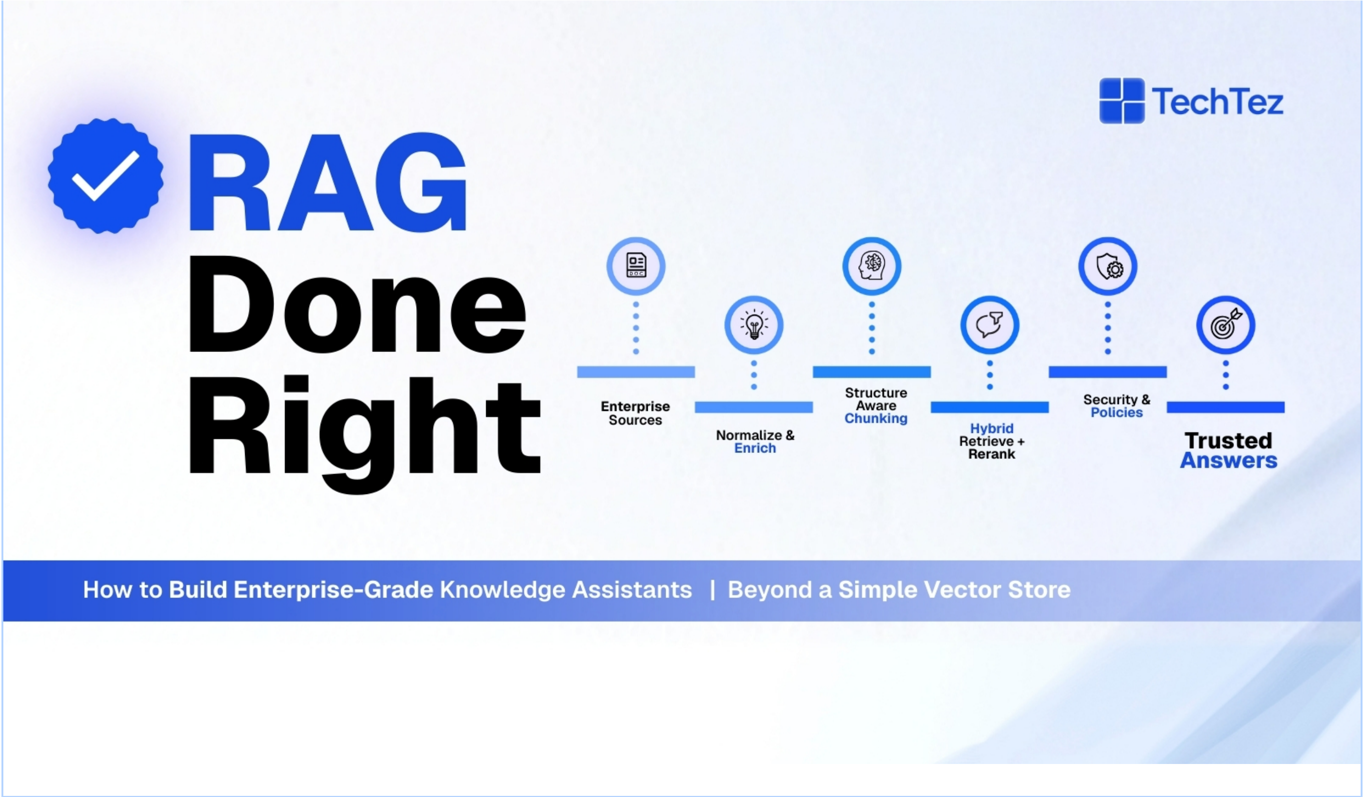
TechTez
Telecom Numbering Platform
Modernizing a Mission-Critical Telecom System with High Availability & Scalable Architecture

- Case Study

Agentic AI in Telecom & Healthcare: The Platform Engineering Playbook

- Case Study

RAG Done Right: How to Build Enterprise-Grade Knowledge Assistants



TechTez
RAG
Done
Right
Enterprise Sources
Normalize & Enrich
Structure Aware Chunking
Hybrid Retrieve + Rerank
Security & Policies
Trusted Answers
How to Build Enterprise-Grade Knowledge Assistants | Beyond a Simple Vector Store