

ScamCheck v4.2 Platinum Forensic Suite

User's Guide

Version: 4.2

Release Date: March 1, 2026

Copyright: © 2026 Iacoletti Software

Getting Started: Installation and Setup

ScamCheck v4.2 is designed for ease of access and can be used directly from your web browser. To operate the suite at peak performance, the following are required:

 **Compatible Device:** A modern smartphone, tablet, or computer (Laptop/Desktop).

 **Integrated Camera:** Highly recommended for utilizing the SNAP and AUDIT forensic capture features.

 **Modern Web Browser:** Optimized for the latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge, or Apple Safari.

 **Internet Connection:** Required for real-time communication with the Gemini 3 Flash multimodal engine.

 **Google Gemini API Key:** A valid API key is required to power the AI reasoning.

Access the Application

Navigate to the ScamCheck v4.2 web application in your browser.

Live Site: <https://louis57xl-coder.github.io/ScamCheck-v4.2/>

After clicking on this link, you will be greeted by the Configure API Key Screen. Getting your own free API key from Google AI Studio is simple and easy.

Obtaining and Installing a Free Gemini API Key

1. Access Google AI Studio: Click on the “Configure API Key” link to Google AI Studio shown in Figure 1.

2. Initialize a Project: Follow Google’s instructions to create a free account. When prompted, select “Create API key in new project.” You may name this project anything you want (e.g., “ScamCheck-Key”).

3. Select the Free Tier: Ensure you select the Free of Charge option which provides 1,000,000 TPM (Tokens Per Minute) with a 250 Forensic Audit (API Calls per day) limit.

4. Copy Your API Key: Once generated, click the “copy” icon to copy your personal Gemini API key to your clipboard.

Enter and Activate Your Key

1. Return to the ScamCheck application in your browser.

2. Paste your free Gemini API key into the input field.

 **Key Masking:** For your security, the key will be automatically masked (••••••••) once entered.

 **Password Management:** Your browser may prompt you to save this key; we recommend doing so for easier access during future sessions.

3. Finalize Activation: Click “SAVE & ACTIVATE”.

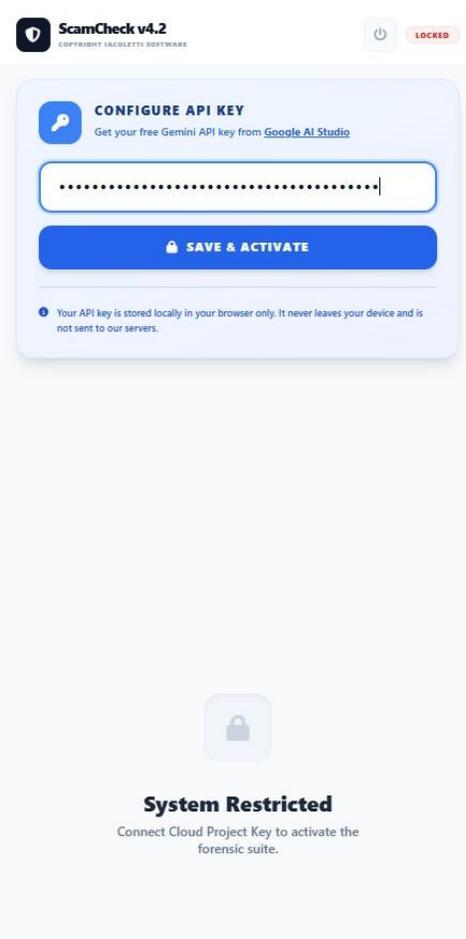


Figure 1: Obtain and enter your free Google API Key. Clicking "SAVE & ACTIVATE" takes you to the main Forensic Audit screen with your API key active.

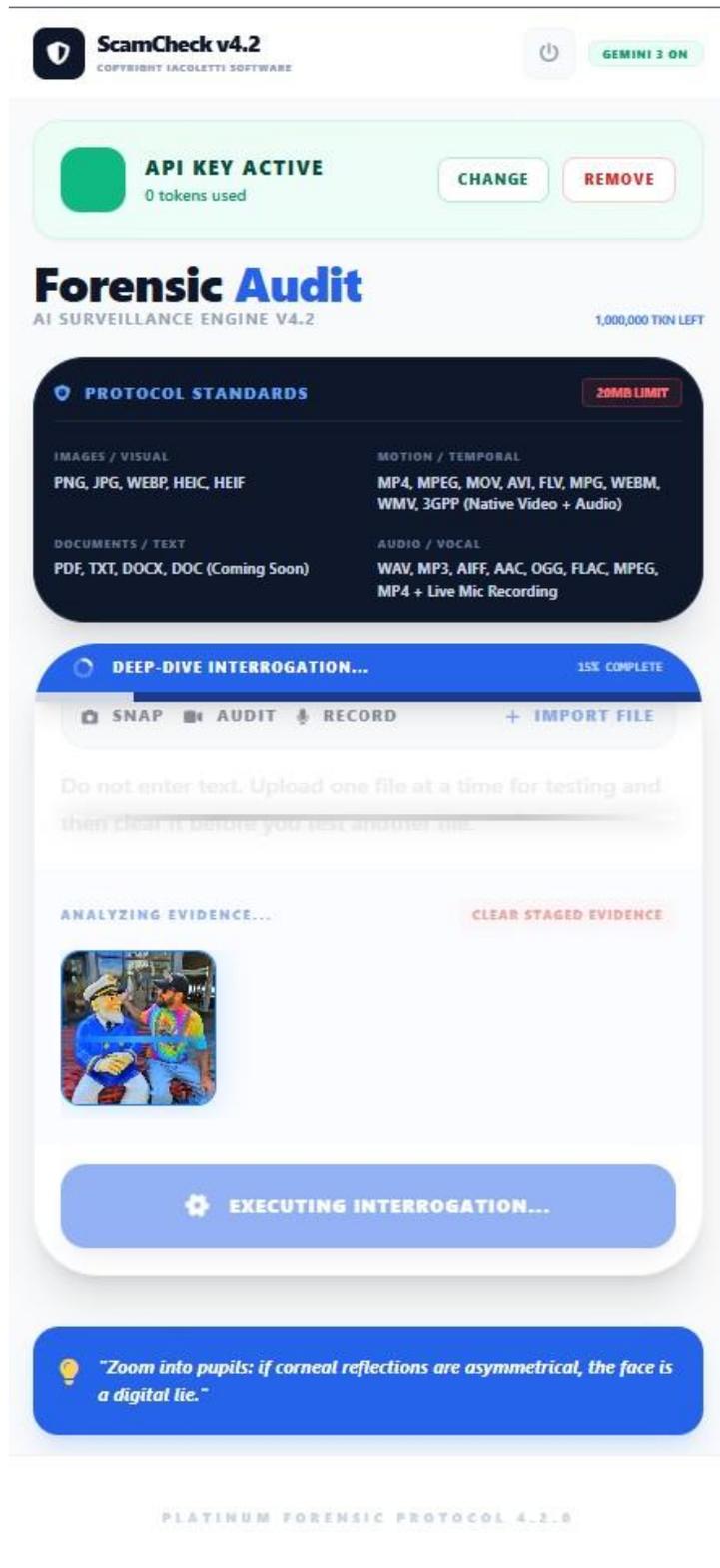


Figure 2: Forensic Audit Screen with file uploaded for forensic analysis

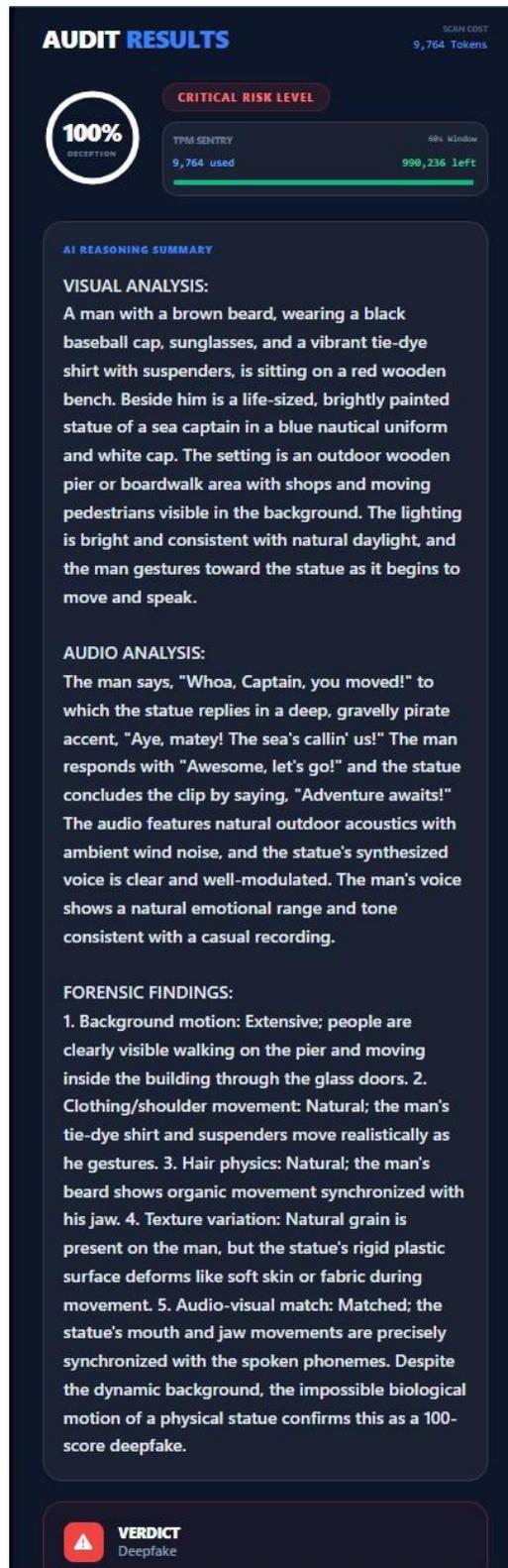


Figure 3: Forensic Audit Results Screen

Step-by-Step Forensic Audit Instructions

Step 1: Clear any previous results before staging a new file by pressing the **Clear Staged Evidence** button.

Step 2: Stage your evidence using one of the four input methods:

Input Methods

SNAP	Capture live photo or screenshot	Analyzing documents, chat logs, or generating image descriptions.
AUDIT	Record live video directly	Rapid, on-the-go forensic analysis and video scene descriptions.
RECORD	Capture live microphone audio	NEW in v4.2: Analyzing spoken content, voice authenticity, phone calls.
IMPORT FILE	Upload from your device	Handling all supported media types (Images, Video, Audio, Docs).

Note: Uploading multiple files and/or input of text directly is not supported. The evidence window also has No-Paste Security to prevent contamination.

Step 3: Initiate your forensic audit

Once your evidence is staged, click on the **"INITIATE FORENSIC AUDIT"** button. ScamCheck will pre-process your file, extract metadata, sample video frames, extract any audio track, and perform deep reasoning via Gemini Flash.

- A **Progress Meter** will display across the top, showing the percentage complete.
- Full analysis typically returns comprehensive results within **15-45 seconds**.

Note: Uploading multiple files and/or input of text directly is not supported. The evidence window also has No-Paste Security to prevent contamination.

Step 4. Performing a Forensic Audit

Summary of Supported File Formats

Images / Visual	JPG, PNG, WEBP, HEIC, HEIF + more	Full image spatial analysis
------------------------	-----------------------------------	-----------------------------

Motion / Temporal	MP4, MPEG, MOV, AVI, FLV, MPG, WEBM, WMV, 3GPP + more	14 random frames + extracted audio track
Documents / Text	PDF, TXT, DOCX*, DOC* + more	Metadata and content extraction
Audio / Vocal	MP3, WAV, AAC, AIFF, OGG, FLAC, MPEG, MP4 + more	Acoustic fingerprinting + transcription
Live Capture	SNAP (photo), AUDIT (video), RECORD (microphone)	Real-time forensic capture

** DOCX and DOC support is built in and ready. Full functionality will be enabled when Google graduates Gemini 3 Flash from "Preview" to "Stable" (expected September 2026).*

File Size & Optimization:

Please ensure your file is no larger than **20MB**. Trying to audit a file over 20MB (or more than one file at a time) will overload Gemini Flash and return an error message.

Step 5: Understanding Your Audit Results

The Results Panel Layout

After analysis completes, the Audit Results panel appears (Figure 3). The redesigned v4.2 panel is more compact and information-dense:

- **Top row:** AUDIT RESULTS title and Scan Cost token count.
- **Second row:** The deception probability dial, the Risk Level badge, and the compact **TPM Sentry** widget.
- **Main body:** The **AI Reasoning Summary** box (larger in v4.2 for the 3-part report).
- **Bottom:** The Verdict box and the **Discard Audit Data** button.

Cloud Rate Limit Monitor (TPM Sentry)

The TPM Sentry tracks your **Google Cloud Free Tier** usage in real-time. In v4.2, it is a compact inline widget displaying:

- Tokens used in the current 60-second window.
- Tokens remaining out of 1,000,000.
- A live progress bar showing consumption.

SCAN COST	The specific number of tokens required to analyze the current file.
CONSUMED	Total tokens used in your current 60-second window.
AVAILABLE NOW	Remaining tokens available for immediate audits (out of 1.0M).

- **No Charges:** You will never be billed while using a standard Free Google Cloud API key.
- **Daily Limit:** The TPM Sentry **DOES NOT** monitor the **250 API calls** allowed per day. If you exceed this, the system will return an error until Google's servers reset at 3am EDT/12AM PDT.
- **Reliability:** Your token balance automatically resets to exactly **1 million every 60 seconds**. It is highly unlikely that a typical user will exceed these limits.

The AI Reasoning Summary - The 3-Part Report

This is the most critical part of the report. In v4.2, it always follows a structured format:

- **Part 1 — What I See:** A detailed visual description of the media content (person, setting, actions).
- **Part 2 — What I Hear:** A transcription or paraphrase of spoken words, plus voice characteristics and acoustic environment. If no audio, it states "No audio present."
- **Part 3 — Forensic Red Flags:** An explicit checklist of every forensic indicator examined and whether any synthetic markers were found or ruled out.

FINAL VERDICT EXAMPLE FROM FIGURE 3

CRITICAL RISK LEVEL - 100%

The video displays a man with a brown beard, wearing a vibrant tie-dye shirt, sunglasses, and a baseball cap, sitting on a red wooden bench next to a fiberglass statue of a sea captain. The statue is depicted in a traditional blue sailor’s jacket with gold buttons and a white captain’s hat, set against an outdoor boardwalk environment with wooden decking and visible storefronts. I hear the man exclaim, “Whoa, Captain, you moved!” and “Awesome, let’s go!” while a deep, gravelly voice attributed to the statue responds with, “Aye, matey, the sea’s calling us” and “Adventure awaits!” Forensic interrogation reveals a 100% confirmed deepfake through impossible biological motion, as the static fiberglass statue’s mouth and arms animate fluidly in a way that defies physical reality. I checked for texture lock and found that the statue’s surface details remain unnaturally consistent while the geometry shifts, a clear indicator of image-to-video AI animation. Furthermore, the statue’s audio lacks the natural room tone and spatial echo present in the man’s speech, confirming it was layered in during post-production. My confidence level is absolute because a physical object is exhibiting complex CGI-driven movement.

VERDICT: DEEPPFAKE

Understanding Deception Scores

0–29%	Low	Evidence strongly consistent with authentic media.
30–49%	Medium	Some ambiguous indicators present; manual review recommended.
50–79%	High	Multiple corroborating synthetic artifacts found.
80–100%	Critical	Three or more unambiguous synthetic markers confirmed. High confidence this is a deepfake.

Epilogue and Methodologies Used

Welcome to the Future of Digital Self-Defense

In the year 2026, digital deception has evolved beyond simple phishing emails. We now face AI-assisted scams, hyper-realistic deepfakes, and synthetic personas designed to exploit human psychology on an industrial scale. Traditional security tools are no longer enough.

ScamCheck v4.2 is best in class within the AI fraud detection industry in its accuracy, representing a fundamental evolution into a complete **Universal Forensic Workstation**. By moving beyond simple text analysis into a comprehensive multimodal suite, it offers a level of forensic scrutiny that is currently unmatched by any other tool.

Imagine a world where AIs with super-human intelligence can quietly watch over your online activity and warn you of any attempted fraud, dishonesty, or insincerity before it happens. ScamCheck v4.2 achieves those capabilities by providing an easy-to-use multimodal forensic engine that serves as your guide for your digital and physical reality. It is fun to use, addictive, and fascinating. Once you start using it you will not be able to stop!

Beyond Security: The Power of Multimodal Intelligence

While ScamCheck v4.2 is an industry-leading standard for fraud detection, nothing compares to its versatility in general intelligence. Its **Multimodal Staging** allows for a breadth of utility that transcends basic security; for instance, capturing a video of a local landmark allows the AI to analyze the footage and provide detailed descriptive information about the landmark's history, appearance, and details.

Whether you are auditing a suspicious message or seeking high-fidelity, descriptive insights about your physical surroundings, ScamCheck v4.2 provides a unified forensic lens for any media input,

turning your computer or mobile device into a powerful window into reality for your situational awareness.

2. Key Features and Capabilities

Building on the near-perfect Romance Scam and "Pig Butchering" detection record of its predecessor ScamCheck v3.1, ScamCheck v4.2 evolves beyond the limited heuristics of prior versions. By integrating the state-of-the-art **Gemini 3 Flash engine**, v4.2 transitions from a text-based scanner into a Multimodal Forensic Workstation capable of analyzing deepfakes, synthetic media, and complex emotional manipulation in real-time.

Core Features Summary of ScamCheck v4.2

Universal Forensic Workstation	A high-fidelity staging area that analyzes more than just text. Drag and drop images, videos, audio files, and binary documents (up to 20MB) for instant multimodal processing.
Multimodal Analysis (Gemini 3 Flash)	Leverages the Gemini 3 Flash engine for principal-level reasoning. It performs frame-by-frame video analysis, identifies acoustic patterns, and extracts document metadata simultaneously.
"Principal-Level" Reasoning	Moves beyond keyword matching to identify the psychological structure of deception, such as the "Emotional Arc" manipulation found in sophisticated "Pig Butchering" schemes.
Acoustic Fingerprinting	Specifically engineered to detect "synthetic jitter" and "robotic prosody" in audio and video samples to identify AI-cloned voices and deepfakes. Now includes extracted audio track analysis from video files.
Privacy-First Architecture	Features a Local Vault where your API key and forensic results are stored exclusively in your browser's local memory; your data is never sent to external servers.
TPM Sentry	A real-time, sliding-window usage tracker that monitors your consumption to ensure you stay within the 1,000,000 tokens-per-minute limit of the Google Cloud Free Tier. Now displayed in a compact inline widget.

General Intelligence Utility	Enables the suite to be used for non-security tasks, such as Visual Identification of objects, Video Summarization, and Unstructured Data Extraction from screenshots.
Live Microphone Recording	New in v4.2: A dedicated RECORD button allows live microphone capture directly within the app. Recorded audio is staged as evidence for immediate forensic analysis.
Grok Imagine Detection	New in v4.2: Dedicated detection logic for image-to-video AI animations (Grok Imagine, Meta AI). Identifies 8 specific hallmarks.
AI Reasoning Summary	New in v4.2: Now provides a structured 3-part forensic report: (1) What I See, (2) What I Hear, (3) Forensic Red Flags.
Progress Meter	New in v4.2: An animated percent-complete progress bar displays while Gemini is processing your evidence, so you always know the audit is working.

What ScamCheck v4.2 Detects

This version of ScamCheck treats every input as a forensic case, scanning for the mechanical and linguistic markers of fraud:

- ✓ **Synthetic Deepfakes:** Identifies AI-cloned voices and face-swaps in audio/video via acoustic fingerprinting.
- ✓ **Algorithmic Affinity Manipulation:** Detects long-term "grooming" scripts where a scammer mirrors your behavior to build false trust.
- ✓ **Synthetic Personas:** Spots AI-generated profile pictures and fraudulent identities using visual artifact detection.
- ✓ **Phishing & Social Engineering:** Analyzes the underlying intent and urgency in text to identify sophisticated traps.
- ✓ **Document Forgery:** Audits images, videos, and documents for manipulated metadata and hidden fraudulent layers.
- ✓ **Grok Imagine / Image-to-Video Detection:** Specifically targets AI tools that animate still photographs, identifying them through 8 distinct forensic hallmarks.

Version 4.2 introduces refinements and optimizations building on the solid foundation of v4.1. Here is a complete summary of every change from v4.1 to v4.2:

Performance and Stability Improvements

1. Enhanced Detection Accuracy

ScamCheck v4.2 refines the existing multimodal detection algorithms introduced in v4.1, with improved accuracy for image-to-video AI tools such as Grok Imagine and Meta AI. The v4.2 update optimizes the detection of these 8 forensic hallmarks:

- **Motion Poverty:** Only the face/head moves while hair, clothing, shoulders, and background remain unnaturally frozen.
- **Texture Lock:** Skin, clothing, and background remain pixel-perfect across frames with zero natural grain variation.
- **Floating Face Syndrome:** The face appears composited onto a static body with no natural neck/torso synchronization.
- **Loop Artifacts:** Motion repeats in an identical cycle (blink, hair sway) that no real video ever replicates exactly.
- **Depth Inconsistency:** 3D parallax on the face but zero depth change in the background.
- **Grok Voice Signature:** Flat prosodic contour, missing breath sounds, unnatural word stress.
- **Phoneme-to-Lip Mismatch:** Lip movements are approximate but imprecise, especially on consonants B, P, M, F, V.
- **Edge Softening:** Blurred or feathered boundary between the animated face and the static background.

Scoring thresholds: 2 Grok markers = score 75+. Three or more markers = score 90+.

2. Optimized False Positive Prevention

V4.2 further refines the false positive prevention system introduced in v4.1, with enhanced recognition to prevent real videos from being incorrectly flagged as deepfakes. The system maintains the core principle: If the entire scene moves naturally together, the default is **AUTHENTIC** unless 3+ unambiguous synthetic markers are found.

3. JPEG Compression Artifact Awareness

V4.2 explicitly instructs the AI that beard texture warping, hair edge softening, and temporal inconsistency are normal JPEG compression artifacts. Bearded or long-haired subjects now require a 50% higher evidence threshold before any synthetic flag is raised.

3. Audio-Only Conservative Scoring

When analyzing audio with no video, the default score starts at 10 and requires overwhelming evidence to increase. The system will not score above 40 based solely on prosody, breath sounds, or frequency analysis, all of which can be affected by re-encoding.

3. Enhanced AI Reasoning Summary

The AI Reasoning Summary now follows a mandatory 3-part structure:

- **Part 1 — What I See:** Detailed visual description.
- **Part 2 — What I Hear:** Transcription and voice characteristics.
- **Part 3 — Forensic Red Flags:** An explicit checklist of every indicator checked and what was found or ruled out.

New Interface Features

3. Live Microphone Recording (RECORD Button)

A fourth button — **RECORD** — has been added. Pressing it launches a full-screen recording modal featuring an animated waveform, a live timer, and a Stop & Stage button. Recorded audio is staged for immediate analysis.

3. Progress Meter

While Gemini processes your evidence, an animated progress bar now displays across the top of the forensic input panel, showing "X% COMPLETE."

3. Redesigned Results Panel

The Audit Results panel has been redesigned for better readability. The risk dial is smaller and moved into a horizontal row with the compact TPM Sentry widget. The AI Reasoning Summary box is now approximately twice as large.

3. No-Paste Security in Evidence Window

The forensic evidence text input now blocks paste operations to maintain forensic integrity.

10. Video Audio Track Extraction

When a video file is uploaded, ScamCheck v4.2 automatically extracts the audio track, re-encodes it as a WAV file, and stages it as a separate **AUDIO TRK** evidence tile (shown with a purple badge) for combined visual and acoustic analysis.

11. DOCX/DOC File Picker Support

The file import picker now accepts .docx and .doc files. *Note: Google has temporarily disabled support for these MIME types in the Gemini Flash Preview API. Full functionality is expected to be restored by September 2026. ScamCheck v4.2 is ready for this update.*

IMPORTANT: Privacy-First Architecture

Your API key is stored locally in your browser's memory only. It **never leaves your device** and is never transmitted to our servers. This "Gold Standard" privacy-first architecture ensures that your forensic environment remains entirely isolated and secure.

How the AI "Thinks": Logic by File Type

The AI executes a **Multimodal Temporal Reasoning** protocol:

- **Video Analysis:** Looks for micro-stutters (jitter analysis), lip-sync mismatches (phoneme-to-viseme), and CGI aesthetic detection. Video analysis also includes audio analysis below.
- **Image Analysis:** Performs artifact extraction, metadata reconstruction, noise pattern inconsistency checks, and anatomical audits.
- **Audio Analysis:** Analyzes spectral centroid variance (frequency), acoustic environment matching, and searches for robotic clicks or frequency flattening.
- **Document Analysis:** Performs logical cross-examination for narrative pressure tactics (The Scam Trifecta: Urgency, Isolation, Pivot to Crypto), semantic consistency, and known script comparison.

How to Be Your Own "Forensic Lead"

If ScamCheck gives a "Low Risk" score but your gut tells you something is wrong, look for these manual cues:

- **The Profile Test:** Watch when the person turns their head. Look for ears or jawlines that "melt" or blur.
- **The Occlusion Check:** If someone passes their hand in front of their face, an AI mask often flickers.
- **Background Static:** Watch for objects in the background that warp or "breathe."
- **The Motion Test:** In a real video, the entire scene moves. If only the face moves, that is a major red flag.

3. Best Practices and Important Notes

Privacy & Operational Best Practices

Do's	Don't's
✓ Click " DISCARD AUDIT DATA " after each use.	✗ Share your API key with anyone.
✓ Store your API key securely in a password manager.	✗ Leave evidence in the staging area after a scan.
✓ Use on private, secure networks.	✗ Analyze sensitive content on public computers or unsecured Wi-Fi.
✓ Convert Word docs to PDF or TXT for now.	✗ Attempt to upload .docx or .doc files until Google's update.
✓ Clear the staging area before starting a NEW scan.	✗ Try to analyze multiple files at the same time.
✓ Verify AI results manually and use your professional judgment.	✗ Assume the AI is 100% infallible.

3. Conclusion

In an era of industrial-scale deception, ScamCheck v4.2 puts the power of state-of-the-art forensic AI back in your hands. You are no longer a passive target but an active, informed defender.

Key Takeaways

- ✓ **Configure your API key first** — It is stored locally for maximum privacy.
- ✓ **Stage evidence carefully** — Use **SNAP**, **AUDIT**, **RECORD**, or **IMPORT FILE**, one file at a time.
- ✓ **Read the full AI Reasoning Summary** — All three parts provide a complete forensic picture.
- ✓ **Watch the progress bar** — It confirms Gemini is actively analyzing your evidence.
- ✓ **Discard audit data after each use** — Maintain forensic hygiene.

-  **Verify results manually** — Always combine system verdicts with your own judgment.

 **DISCLAIMER:** This tool is for educational and protective purposes. AI analysis is probabilistic; always combine results with personal judgment and standard security protocols.

Security and Data Privacy Warning for Security and Forensics Specialists and Government Employees

While the free Google API key provides encryption in transit and at rest, it is not sufficient for handling Sensitive PII, Controlled Unclassified Information (CUI), or proprietary corporate data. Before using ScamCheck for these purposes, you are cautioned to ensure your environment is configured within an Assured Workloads folder or a dedicated enterprise-grade Google Cloud Project to meet FedRAMP Moderate, DoD IL4, or industry-specific compliance standards. Users must verify that no classified or highly restricted data is processed through this environment, as doing so may constitute a security spillage. Always consult with your Information Security Officer or Privacy Lead to confirm that your configuration aligns with organizational Acceptable Use Policies and zero-trust mandates.

Copyright © 2026 Iacoletti Software. All Rights Reserved.

Appendix: End User License Agreement (EULA)

Project: ScamCheck v4.2 (Safe-Horizon)

Version: 4.2

Licensor: Iacoletti Software

Date: March 1, 2026

IMPORTANT: PLEASE READ THIS AGREEMENT CAREFULLY.

This End User License Agreement ("Agreement") is a legal contract between you (the "Licensee") and **Iacoletti Software** (the "Licensor") for the use of the **ScamCheck v4.2** software, including all associated neural classifiers, AI models, source code, datasets, and documentation (collectively, the "Software"). By downloading, installing, or using the Software, you agree to be bound by the terms of this Agreement. If you do not agree, do not install or use the Software.

1. LICENSE GRANT

Subject to the terms of this Agreement, Iacoletti Software grants you a **personal, non-exclusive, non-transferable, revocable license** to use the Software solely for internal testing and evaluation, and non-commercial personal use.

2. INTELLECTUAL PROPERTY RIGHTS

The Software is the exclusive intellectual property of Iacoletti Software. All rights, title, and interest in and to the Software — including but not limited to the **unique 12-factor feature extraction logic**, trained neural network weights, model architecture, and underlying algorithms — remain the sole property of Iacoletti Software. This Agreement does not convey to you any interest in or to the Software, but only a limited right of use.

3. RESTRICTIONS

You shall not, directly or indirectly:

- **Reverse Engineer:** Decompile, disassemble, reverse engineer, or attempt to derive the source code, underlying ideas, algorithms, or model logic.
- **Redistribute:** Sell, rent, lease, sublicense, distribute, or otherwise transfer the Software or any rights thereto.
- **Modify:** Modify, translate, or create derivative works based on the Software.
- **Alter Markings:** Remove any proprietary notices, labels, or watermarks.

3. CONFIDENTIALITY

The Software contains valuable trade secrets and proprietary information. You agree to maintain confidentiality. You shall not disclose, publish, or share performance benchmarks, internal logic or code snippets, or screenshots of the backend or codebase to any third parties without prior written consent.

3. WARRANTY DISCLAIMER ("AS IS")

THE SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS," WITHOUT WARRANTY OF ANY KIND. IACOLETTI SOFTWARE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A

PARTICULAR PURPOSE, AND NON-INFRINGEMENT. YOU ACKNOWLEDGE THAT THE SOFTWARE MAY CONTAIN ERRORS OR OTHER PROBLEMS.

3. LIMITATION OF LIABILITY

IN NO EVENT SHALL IACOLETTI SOFTWARE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE.

3. TERMINATION

This license is effective until terminated. Iacoletti Software may terminate this Agreement at any time if you fail to comply with any term or condition. Upon termination, you must cease all use of the Software and immediately destroy all copies.

3. GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of the **Commonwealth of Virginia**, without regard to its conflict of laws principles.