CGEN · INTELLIGENCE REPORT

REA (Reverse Engineer Anything) rea.tools

Report ID: IR-DRAFT

Generated: October 30, 2026

BUSINESS

REA (Reverse Engineer Anything) rea.tools - the open-source AI revese-engineering tool.

REPORT

Identity & Overview

REA is an open-source toolkit that exposes reverse-engineering workflows through a command-line interface (CLI) and the Model Context Protocol (MCP). It gives AI coding assistants such as Codex and Claude Code a way to investigate existing software, including programs whose original source code you don't have - you point your agent at an application or browser session and ask how a particular feature works, and REA supplies tools to inspect the code and behavior. It hands AI agents the ability to inspect native binaries, Electron and JavaScript apps, .NET assemblies, Android APKs, firmware, SQLite databases, live websites and browser behavior, orchestrating tools reverse engineers already trust: Ghidra for headless disassembly, Hopper with automated setup, and IDA Pro through an MCP bridge.

The author uses the handle "morluto" and whose real name has not been publicly identified. The GitHub profile places morluto in "Sinsai," describes an interest in AI math, and notes solving the 33-year-old Erd■s problem #81 alongside a longtime collaborator N0zoM1z0, with personal research in agents, RL environments, and preference learning. The project's GitHub repository was created in April 2026 under the morluto account, built privately before public release; the first npm package appeared on July 12, 2026 at version 0.1.0, and a same-day update to 0.2.0 renamed the tool to REA and introduced the dynamic binary-session lifecycle that underpins later releases. There is no funding, no vendor, and no legal entity behind REA. The business model is purely open-source and MIT-licensed - morluto earns no revenue directly from REA itself.

MARKET POSITION

1. Ghidra

• What They Do: NSA-developed open-source binary reverse engineering framework

• Category: Open-source disassembler

• Pricing: Free

• Review Score: Not publicly available

2. IDA Pro (Hex-Rays)

• What They Do: Industry-standard commercial disassembler and decompiler for multi-architecture binaries

• Category: Commercial disassembler

• Pricing: Paid - from $1,099/yr

• Review Score: Not publicly available

3. Binary Ninja

• What They Do: Modern binary analysis platform with decompiler, debugger, and API

• Category: Commercial RE platform

• Pricing: Freemium - from $199 one-time

• Review Score: Not publicly available

4. Binary Ninja Sidekick

• What They Do: AI-assisted reverse engineering assistant embedded inside Binary Ninja

• Category: AI-native RE assistant

• Pricing: Freemium - from $30/mo

• Review Score: Not publicly available

5. RevEng.AI

• What They Do: Cloud-based AI-powered binary analysis and reverse engineering platform

• Category: Cloud RE / AI analysis

• Pricing: Not publicly listed

• Review Score: Not publicly available

6. GhidraMCP (LaurieWired)

• What They Do: Open-source MCP server connecting Ghidra to AI agents for native binary analysis

• Category: Open-source MCP bridge

• Pricing: Free

• Review Score: Not publicly available

7. ida-pro-mcp (GrecAndrei)

• What They Do: Local MCP server for IDA Pro with evidence-backed reverse engineering operations

• Category: IDA Pro MCP bridge

• Pricing: Free (requires IDA Pro license)

• Review Score: Not publicly available

REA occupies a newly carved niche: the AI-native reverse engineering orchestration layer. It is not a disassembler in the traditional sense - radare2, Binary Ninja, and IDA Pro all have their own MCP integrations already; REA is not the only MCP server for reverse engineering, it is the one that went viral. Its competitive differentiation is breadth: where most comparable tools target native binaries only, REA covers native, JavaScript/Electron, .NET, web, and Android, and can sit on top of Ghidra rather than replacing it. It sits above traditional disassemblers in the stack - as an orchestration and agent-integration layer - and its closest commercial analogues are Binary Ninja Sidekick and RevEng.AI.

Traction & Scale

REA's growth trajectory is one of the most extreme documented on GitHub in 2026. It had fewer than 10,000 GitHub stars on October 6 and surpassed 100,000 by October 12. By October 14 it had reached 234,477 stars with 58,512 forks, gaining roughly 90,000 stars in a single 36-hour stretch between October 12 and October 14. By late October,

the official repository showed roughly 374,000 stars and 93,000+ forks.

npm downloads for the rea-agents package were 798 per day on October 4, surging to 34,790 per day by October 10. The npm registry showed 33 published versions since the package first appeared on July 12, 2026, with three major versions between 4.0.1 on October 5 and 6.7.0 on October 18 - a thirteen-day span.

The security policy refers to "the maintainer" in the singular, while the repository had drawn contributions from 271 accounts as of October 21, 2026. Geographic reach is not formally documented, but contributors include accounts with French, Brazilian, and Dutch identifiers, and an unofficial French-language guide already exists. The project had more than 100 contributors and over 170 open issues and pull requests at the time of early reporting. Team size is effectively one named maintainer with a large open-source contributor base.

FINANCIAL PICTURE

REA has no funding, no vendor, and no legal entity behind it. The code is MIT licensed and the npm package is free. There is no disclosed revenue, no pricing tier on the REA tool itself, and no disclosed angel or VC investment. REA is free to use, though some tools it connects to (such as IDA Pro and Hopper) are not free, and users also pay for whichever AI model their coding agent uses.

The project's monetization path is currently undefined. morluto has not publicly announced any commercial plans, SaaS offering, or enterprise tier as of late October 2026. The REA README states clearly that it grants no tool licenses and that cracked copies or shared keys are not authorized, indicating morluto is careful about legal positioning but has not yet converted that awareness into a revenue model. Valuation is not applicable - this is an open-source individual project.

PUBLIC SENTIMENT

Community reception is broadly enthusiastic but analytically divided. The Hacker News thread that drove REA's viral moment drew 805 points and 337 comments, telling a more nuanced story than the headlines suggest. The most upvoted skeptical comment asked: "How exactly is this better than telling Claude to install Ghidra?" - with other commenters noting that radare2, Binary Ninja, and IDA Pro all have their own MCP integrations already.

The prevailing community use pattern appears to be software preservation and interoperability, not cloning competitors. Python bytecode analysis consistently produced useful logical-flow explanations for moderately sized, non-obfuscated Python files, with multiple researchers on Reddit and Hacker News calling results "genuinely helpful." In one structured test, 30 of 30 file-and-line locations were correct, and REA found an IPC channel a text search missed - but it completely missed all 8 reply-back locations.

On October 24, one social media post to more than 450,000 views reported that Claude now hits a safety check when asked to use REA for detailed reverse-engineering work, even after completing the research - a development generating its own wave of complaints. Scam tokens exploiting the REA name also surfaced, which commenters noted as a sign of the project's mainstream recognition.

Media & Press

REA raced up GitHub with hundreds of thousands of stars and tens of thousands of forks in a matter of days - one of the fastest climbs the platform has seen this year. Coverage spanned a wide range of outlets. InfoQ reported on the project once it crossed over 200,000 GitHub stars, noting it connects coding agents such as Claude Code and Codex to reverse-engineering tools like Ghidra, Hopper, and IDA.

Legal controversy quickly followed: on October 6, a website allowing players to run GTA 5 in their browser went live and was taken down hours later, and Rockstar, Activision, and Bethesda's legal teams swiftly acted to remove browser-based versions of their games. The potential for legal disputes increased, with concerns that implementing features through AI-assisted reverse engineering could lead to copyright infringement.

On October 13, 2026, a user reported in issue #2424 on the official repository that a lookalike repository, rea-tools/rea, had copied the README and added a "Windows Standalone .exe" section distributing malware. A Reddit thread titled "Anthropic secretly killed the REA train" appeared on r/Claude on October 21, 2026, and Kotaku covered it on October 24 in a piece titled "Claude's reverse-engineering capabilities may have been quietly nerfed."

CURRENT STATUS

REA is in an explosive growth phase but faces headwinds that could limit its practical utility without structural changes. REA itself is not broken or blocked - it is an MCP server that runs its analysis on the user's machine, and its repository was still shipping releases (rea-agents 6.7.0 as of October 25, 2026). REA's own README warns that "REA changes quickly, and new releases include frequent bug fixes," and the npm registry bore this out with 33 published versions in under four months.

The central constraint is AI model compliance: some users report that Claude stops REA sessions since October 24, 2026; Anthropic has not officially commented, but its published policy indicates generally available Claude models block most cyber work, with verified security teams able to apply for fewer blocks. Brazilian developer Fabio Akita also pushed back on industry doomsaying, arguing AI-built alternatives have many errors and missing features, and that it is difficult to analyze every function of a commercial product from the outside. The project is genuinely active, rapidly iterating, and attracting global attention - but it remains a solo-maintainer open-source project with no legal entity, no commercial backing, and tightening friction from AI safety classifiers.

SUMMARY VERDICT

REA (Reverse Engineer Anything) is the most virally successful developer tool of October 2026 - a single-maintainer, MIT-licensed MCP server and CLI that compressed an entire specialist discipline (binary reverse engineering) into a one-command install for any developer with an AI coding agent. It is real, functional, and genuinely useful within its documented limits; it is also overhyped, legally ambiguous, and operationally fragile at scale.

One-line assessment: REA is a breakthrough in accessibility for reverse engineering, not a breakthrough in reverse engineering itself - its value is orchestration and packaging, not novel analysis capability, and its durability depends on a single pseudonymous maintainer and the cooperation of AI labs whose safety classifiers are already pushing back.

For ordinary people and small businesses, REA is a practical tool for understanding how software you already own actually works under the hood - useful for recovering logic from lost codebases, auditing apps for privacy issues, or achieving compatibility with closed file formats. It is completely free to download and use (MIT license, zero cost), though you will need a free AI coding agent subscription and, for deep native analysis, potentially a licensed copy of a tool like IDA Pro or Hopper. For solo developers and small teams locked out of expensive specialist reverse engineering workflows, REA meaningfully lowers the barrier - but it requires technical comfort with the command line, and using it on software you don't own carries real legal risk depending on your jurisdiction and the terms of the software's license agreement.

FOLLOW-UP ANSWER

On the official statement question: there is none. That is the single most important fact here.

Anthropic has not published an official statement, and its October 8 Usage Policy update made no mention of reverse engineering. Users report Claude Opus 5.5 cutting off reverse-engineering and smart TV rooting requests - but Anthropic has not confirmed a block. Every outlet covering this story arrives at the same conclusion: reports regarding Claude are numerous and consistent, but Anthropic has not confirmed any change; for now it remains a user-reported situation, not an announced decision.

What the evidence actually shows - three confirmed facts and one key ambiguity:

1. **The blocking is real and consistent, but the mechanism is the existing classifier, not a targeted REA ban.** On October 6, 2026, Anthropic expanded its Cyber Verification Program and described the cyber safeguards on its generally available models as conservative, blocking most cyber work. Nothing in REA broke, and there is no confirmed Claude downgrade - what reverse engineers are hitting is Anthropic's cyber safety classifier.

2. **The trigger appears to be context, not the word "REA."** Anthropic's help pages say malware analysis and exploit validation may be interrupted, while secure code review, threat modeling, and finding vulnerabilities in your own source code are fine. Other users replied that REA still works for them and is refused only in cases like credential scraping.

3. **ChatGPT/Codex is also implicated, without confirmation.** Claude Opus 5.5 and ChatGPT now halt reverse-engineering requests in some configurations. Documented cases involving Codex include several GitHub reports of actions rejected with a generic "blocked by policy" that make no mention of reverse engineering. Again, no official OpenAI statement confirms a deliberate policy change targeting REA specifically.

The key ambiguity: it remains unclear whether recent disruptions represent a new crackdown or the existing classifier intercepting REA workflows more frequently - i.e., REA's viral surge may simply have sent more borderline prompts through classifiers that were always going to refuse them.

What users are switching to:

| Alternative | Type | Cost |

|---|---|---|

| Local open-weight models (Llama, Qwen, etc.) | Self-hosted, no provider filters | Free (hardware cost only) |

| Grok 4.3 / Gemini 3.1 Pro | Cloud, Western models | Paid subscription |

| Anthropic Cyber Verification Program | Unlock path for Claude | Free to apply, not guaranteed |

On r/LocalLLaMA, community reaction is moving toward local models, which can be paired with REA without provider filters. This is the dominant shift. Many users say this is why open-source and local models matter, and some say they now run REA only on local "abliterated" models to avoid account bans.

Among Western cloud models, Grok 4.3 and Gemini 3.1 Pro complete most RE tasks according to at least one routing guide, though Chinese open models can already do it, with one tester noting that Qwen 3.8-Flash-Next gets confused easily and burns tokens.

For users who want to stay on Claude, the Cyber Verification Program - through which security professionals can request fewer blocks - mentions classifiers that interrupt malware analysis and exploit validation, but reverse engineering, rooting, and televisions don't appear in its scope. One r/ClaudeAI user writes that approval didn't remove his blocks - a single case that can't be verified - so the CVP path is uncertain at best.

Bottom line: The blocking is real and user-documented across hundreds of reports, but it is Anthropic's pre-existing cybersecurity classifier doing its job at higher volume - not a targeted shutdown of REA. Anthropic has said nothing publicly about REA by name. The community has responded almost immediately with a structural workaround (local

models + REA's MCP server), which is exactly the outcome REA's open-source, runs-on-your-machine architecture was designed to enable.

Sources:

• AGTP on X: "Anthropic just appears to have quietly restricted Claude's reverse engineering abilities. Here's what you need to know. The claim comes from security account @0x0SojalSec, whose post hit 322.4K views on Oct 24, 2026. It says Claude can no longer "Reverse Engineer Anything," known as RE... / X - https://x.com/AGTPinsights/status/2113992592761524672

• Claude Opus 5.5 blocks smart TV reverse engineering, users report - https://pasqualepillitteri.it/en/news/27020/claude-opus-5-5-blocks-smart-tv-reverse-engineering-users-report

• Claude Blocks REA? Reverse Engineering Stops Mid-Task - https://iamag.it/en/news/claude-rea-reverse-engineering-guardrail-blocks

• Is Claude blocking reverse engineering? · Made with REA - https://madewithrea.com/guides/is-claude-blocking-reverse-engineering

• Why Is Claude Blocking Reverse Engineering? - https://capitalandcompute.net/blog/why-is-claude-blocking-reverse-engineering/

• X discussion: viral posts claim Anthropic "quietly killed" Claude's reverse engineering with the REA toolkit after a Samsung TV firmware teardown went viral; no official statement yet - AICoder - https://aicoder.com/news/news-20261025-x-discussion-claude-rea-reverse-engineering-blocked

• Reverse Engineering With AI: REA Setup When Claude Refuses - https://llmgateway.io/blog/reverse-engineering-with-ai-rea