

OPENAI EVIDENCE PACKAGE EXECUTIVE SUMMARY

Case Reference: Kirchner v. Anthropic, PBC (1:25-cv-02735-ACR)

Package Location:

/Users/everest/Git/code_forensics/evidence_packages/openai/

Total Files: 12

Total Findings: 30

Date Generated: 2025-12-28

Last Updated: 2026-01-02

I. PACKAGE OVERVIEW

The OpenAI evidence package contains forensic evidence extracted from ChatGPT Atlas (OpenAI's macOS desktop application), establishing a comparative baseline for industry telemetry practices.

Evidence Base	Contents	Key Findings
`chatgpt_datadog_20251226_180727/`	Datadog cache extraction	Third-party telemetry infrastructure
`chatgpt_analysis/`	iOS IPA, network captures, static analysis	Certificate pinning, SDK inventory
`CHATGPT_EVIDENCE_20251228_142719/`	Additional evidence collection	SSL bypass scripts, traffic captures

Report	Contents
`EXHIBIT-OPENAI-01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md`	1,023 lines - exhaustive telemetry analysis
`FORENSIC_CHATGPT_IOS_ANALYSIS.md`	521 lines - iOS app forensic analysis
`CHATGPT_ATLAS_FORENSIC_REPORT.md`	357 lines - desktop network traffic analysis
`CHATGPT_ATLAS_PRELIMINARY_FORENSIC_ANALYSIS.md`	257 lines - cross-platform comparison
`APPLE_INTELLIGENCE_CHATGPT_PARTNER_REPORT.md`	371 lines - OS-level Apple integration

Summary of Critical Findings

Finding #	Title	Forensic Category
iOS FINDINGS (19-24)		
19	iOS Certificate Pinning Implementation	Security Positive
20	No Sift Science Integration (Unlike Claude)	Privacy Comparative

21	No Calendar/Reminders Full Access	Permission Scope
22	iOS Privacy Manifest Compliance	Disclosure Compliance
23	No Facebook SDK on iOS	Third-Party Data
24	iOS vs Claude iOS Comprehensive Comparison	Comparative Analysis
DESKTOP NETWORK FINDINGS (25-30)		
25	No Certificate Pinning on Desktop	Security Asymmetry
26	Facebook SDK on Desktop with App ID	Undisclosed Tracking
27	Amazon Telemetry (102+ Requests)	Cross-Site Identity
28	Undisclosed Google Analytics Tracking	Hidden Surveillance
29	CSP Whitelists Advertising Networks	Intentional Integration
30	MITM Detection Without Security	Selective Protection
DESKTOP APPLICATION FINDINGS (1-18)		
1-2	Multi-Provider Telemetry & Device Fingerprinting	Industry Pattern Analysis
3-4	Plaintext Email & Behavior Tracking	Privacy Concerns
5-6	Data Storage Volume & Segment Analytics	Data Retention Analysis
7-8	Work with Apps & Sentry Infrastructure	File Access & Telemetry
9	Local Encryption Comparison	Comparative Security
10-11	Apple-OpenAI OS Integration & codeLM Disabled	Anticompetitive Evidence
12-14	Raw Telemetry & User Identification	Data Transmission Proof
15-18	Hardware/Network Fingerprinting & Session Tracking	Environmental Profiling

II. CRITICAL FINDINGS

A. iOS APPLICATION FINDINGS (19-24)

FINDING 19: iOS Certificate Pinning Implementation [EXHIBIT-OPENAI-02]

Evidence:

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 282-321)

Forensic Significance: ChatGPT iOS implements certificate pinning on authentication and API endpoints, preventing man-in-the-middle attacks. This is a significant security positive that demonstrates OpenAI's commitment to protecting user data in transit on mobile. The pinned endpoints include ios.chat.openai.com and ab.chatgpt.com. This implementation protects user credentials and conversation data from interception. Critically, Claude iOS does NOT implement certificate pinning, allowing full traffic interception—this demonstrates that OpenAI exceeds Anthropic in mobile security practices.

Pinned Endpoints:

Endpoint	Status
ios.chat.openai.com	PINNED
ab.chatgpt.com	PINNED
api.openai.com	Partial

Evidence (mitmproxy log):

[04:48:14.861] Client TLS handshake failed. The client disconnected during the handshake. If this happens consistently for ios.chat.openai.com, this may indicate that the client does not trust the proxy's certificate.

FINDING 20: No Sift Science Integration (Unlike Claude iOS) [EXHIBIT-OPENAI-02]

Evidence:

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 211-228)

Forensic Significance: ChatGPT iOS does NOT integrate Sift Science fraud detection—the same third-party service that Claude iOS uses to collect user behavioral data, device information, and 38+ network IP addresses. This proves that AI assistants can function without surveillance-grade fraud detection on paying customers. OpenAI has chosen NOT to surveil their users in this manner, while Anthropic has. This directly undermines any claim that Sift Science integration is "industry standard" for AI assistants.

SDK	ChatGPT iOS	Claude iOS
Sift Science	NO	YES
Facebook/Meta SDK	NO	YES
Firebase	NO	YES
Google Sign-In	NO	YES

FINDING 21: No Calendar/Reminders Full Access [EXHIBIT-OPENAI-02]**Evidence:**

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 103-120)

Forensic Significance: ChatGPT iOS does NOT request full access to user calendars or reminders—permissions that Claude iOS requests with justifications like "Claude can create events or read from your calendars." This demonstrates that an AI assistant can provide equivalent functionality without accessing deeply personal scheduling data. OpenAI's more limited permission scope shows that Claude's extensive permissions are a CHOICE, not a technical requirement.

Permission Comparison:

Permission	ChatGPT iOS	Claude iOS
Camera	YES	YES
Microphone	YES	YES
Location	When In Use	When In Use
Photos	YES	YES
Calendar (Full Access)	NO	YES
Reminders (Full Access)	NO	YES

FINDING 22: iOS Privacy Manifest Compliance [EXHIBIT-OPENAI-02]**Evidence:**

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 133-195)

Forensic Significance: ChatGPT iOS contains 18 privacy manifest files (PrivacyInfo.xcprivacy) with complete disclosure of all third-party SDKs. Every SDK detected in static analysis (Segment, Sentry, Datadog, Stripe, RevenueCat, Auth0, LiveKit) is properly declared. NSPrivacyTracking is set to `false` in all manifests. This level of compliance demonstrates that full privacy disclosure is technically achievable—Anthropic's incomplete privacy manifests represent a compliance choice, not a technical limitation.

All Third Parties Disclosed:

SDK	Detected	Disclosed	Purpose
Segment	YES	YES	Analytics
Sentry	YES	YES	Crash reporting
Datadog	YES	YES	Monitoring
Stripe	YES	YES	Payments
RevenueCat	YES	YES	Subscriptions

FINDING 23: No Facebook SDK on iOS [EXHIBIT-OPENAI-02]**Evidence:**

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 211-228)

Forensic Significance: ChatGPT iOS does not include or communicate with Facebook/Meta SDK. This is significant because Claude iOS DOES include Facebook SDK integration for analytics and tracking. An AI assistant serving millions of users can function without sharing user data with Meta's advertising infrastructure. This finding establishes that Facebook SDK integration in AI assistants is a business choice to monetize user data, not a technical necessity.

FINDING 24: iOS vs Claude iOS Comprehensive Comparison [EXHIBIT-OPENAI-02]**Evidence:**

openai_evidence_bases/chatgpt_analysis/FORENSIC_CHATGPT_IOS_ANALYSIS.md
(lines 324-371)

Forensic Significance: The complete comparison demonstrates that Claude iOS's data collection practices EXCEED industry norms established by the leading competitor. ChatGPT achieves equivalent AI assistant functionality with significantly better privacy practices across every measured dimension.

Category	ChatGPT iOS	Claude iOS	Winner
Third-party SDKs	7	9+	ChatGPT
Undisclosed sharing	0	2+	ChatGPT
Permissions requested	4	6	ChatGPT
Certificate pinning	YES	NO	ChatGPT
Privacy manifest compliance	Full	Partial	ChatGPT
Fraud detection surveillance	NO	YES	ChatGPT

B. DESKTOP NETWORK TRAFFIC FINDINGS (25-30)

FINDING 25: No Certificate Pinning on Desktop (Unlike iOS) [EXHIBIT-OPENAI-03]**Evidence:**

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
(lines 18-27)

Forensic Significance: Unlike the iOS version, ChatGPT Atlas desktop has NO certificate pinning, allowing complete traffic inspection via mitmproxy. This asymmetry is strategically significant: OpenAI pins traffic on iOS (where App Store review might detect hidden practices) but leaves desktop traffic inspectable. This allowed discovery of extensive undisclosed third-party data sharing that would remain hidden on iOS. The asymmetry suggests certificate pinning is used strategically to prevent discovery rather than for security alone.

Platform	Certificate Pinning	Traffic Inspectable
ChatGPT iOS	YES	No (without bypass)
ChatGPT Desktop	NO	Yes (fully)

FINDING 26: Facebook SDK on Desktop with App ID [EXHIBIT-OPENAI-03]

Evidence:

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
(lines 198-220)

Forensic Significance: The desktop application actively communicates with Facebook's tracking infrastructure via connect.facebook.net with a specific App ID (468742119653388). This links ChatGPT user activity to Facebook's advertising network, enabling cross-platform tracking, advertising attribution, and behavioral profiling. This is NOT disclosed in OpenAI's privacy policy. The Facebook App ID enables Meta to correlate ChatGPT usage with users' Facebook profiles.

Request:

GET

<https://connect.facebook.net/signals/config/468742119653388?v=2.9.248&r=stable&domain=chatgpt.com>

Facebook App ID: 468742119653388

FINDING 27: Amazon Telemetry (102+ Requests) [EXHIBIT-OPENAI-03]

Evidence:

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
(lines 141-194)

Forensic Significance: ChatGPT Atlas transmits 102+ requests to Amazon endpoints (fls-na.amazon.com, atv-ps.amazon.com, unagi.amazon.com) including the user's Amazon authentication cookies and session identifiers. This cross-site identity linking allows Amazon

to correlate ChatGPT usage with Amazon accounts. This undisclosed data sharing is particularly concerning as it transmits credentials for an unrelated service (Amazon) while using ChatGPT.

Amazon Endpoints:

Endpoint	Requests	Data Transmitted
fls-na.amazon.com	90	Session cookies, behavioral telemetry
atv-ps.amazon.com	12	Amazon Prime Video integration
unagi.amazon.com	1	Amazon Events

Cookies Transmitted:

session-id=132-8085091-4997768
 ubid-main=134-8639420-4546446
 at-
 main=Atza|lwEBIInTyS_dH5iizX7qd8HvEcuuuZN8CStG8zsjlhj1HV3acps7fs6KnSVcrAM
 3QVBRJSmlvalh...

FINDING 28: Undisclosed Google Analytics Tracking [EXHIBIT-OPENAI-03]

Evidence:

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
 (lines 222-249)

Forensic Significance: ChatGPT Atlas communicates with multiple Google services not disclosed in the privacy policy, including www.google-analytics.com (18 requests), www.googletagmanager.com (6 requests), and android.clients.google.com (30 requests for Cloud Messaging—on a macOS desktop app). The Android Cloud Messaging registration on macOS suggests cross-platform device fingerprinting beyond legitimate push notification needs.

Google Service	Requests	Purpose
google-analytics.com	18	User behavior tracking
googletagmanager.com	6	Marketing tag deployment
android.clients.google.com	30	Cloud Messaging (on Mac!)
optimizationguide-pa.googleapis.com	34	ML optimization
content-autofill.googleapis.com	23	Form autofill data

FINDING 29: CSP Whitelists Advertising Networks [EXHIBIT-OPENAI-03]**Evidence:**

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
(lines 109-138)

Forensic Significance: The application's Content-Security-Policy header explicitly whitelists tracking domains from major advertising networks—TikTok, LinkedIn, Reddit, and Microsoft Bing. This is INTENTIONAL integration, not incidental third-party loads. The CSP explicitly permits these scripts to execute, proving OpenAI has deliberately enabled advertising network integration despite not disclosing this in their privacy policy.

Script Sources Whitelisted:

https://analytics.tiktok.com ← TikTok Analytics
https://bat.bing.com ← Microsoft Advertising
https://connect.facebook.net ← Facebook SDK
https://snap.licdn.com ← LinkedIn Tracking
https://pixel-config.reddit.com ← Reddit Pixel

FINDING 30: MITM Detection Without Security [EXHIBIT-OPENAI-03]**Evidence:**

openai_evidence_bases/chatgpt_analysis/CHATGPT_ATLAS_FORENSIC_REPORT.md
(lines 253-274)

Forensic Significance: OpenAI implements session integrity verification that detects TLS interception (preauth_cookie_failed) without using certificate pinning. This demonstrates OpenAI is AWARE their traffic may be intercepted and has implemented countermeasures—yet CHOSE not to implement certificate pinning on desktop, allowing all third-party tracking to be captured. This selective security approach protects authentication while leaving surveillance infrastructure exposed.

Authentication Error:

Authentication Error

An error occurred during authentication (preauth_cookie_failed).
Request ID: 9bc5dcbe41552a6a9487ca853467609f

C. DESKTOP APPLICATION FINDINGS (1-18)

FINDING 1: Multi-Provider Telemetry Infrastructure [EXHIBIT-OPENAI-01]**Evidence:** exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 185-238)

Forensic Significance: The use of four separate third-party analytics providers (Statsig, Sentry, Segment, Datadog) establishes that extensive telemetry is an industry-wide pattern, not unique to Anthropic. This finding provides comparative context—OpenAI implements even MORE telemetry providers than Anthropic (4 vs 3). The Datadog SDK warning about "customer data exceeding 3KB threshold" proves substantial user data is transmitted per session. This evidence supports arguments about industry practices while also documenting OpenAI's own data collection scope.

ChatGPT Atlas transmits data to **4 separate third-party analytics providers:**

Provider	Evidence Location	Data Type
Statsig	`statsig/`, preferences	Feature flags, A/B testing
Sentry	`io.sentry/`, bundled framework	Crash reports, sessions
Segment	`com.segment.storage.oai.plist`	Behavioral analytics
Datadog	`debug.log` references, cache	Real User Monitoring

Datadog Evidence (lines 559-571):

[61418:4688296:1222/120734.727216:INFO:CONSOLE:7] "Datadog Browser SDK: Customer data exceeds the recommended 3KiB threshold. More details: https://docs.datadoghq.com/real_user_monitoring/browser/troubleshooting/#customer-data-exceeds-the-recommended-threshold-warning"
source: <https://auth-cdn.oaistatic.com/assets/datadog-BTgRrIvw.js> (7)

Each session transmits >3KB of "customer data" to Datadog.

FINDING 2: Persistent Device Fingerprinting [EXHIBIT-OPENAI-01]**Evidence:** exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 240-302)

Forensic Significance: ChatGPT Atlas maintains 4-6 persistent device identifiers—MORE than Claude Desktop (1-2). This extensive fingerprinting enables cross-session user tracking even after application reinstallation. The redundancy (Sentry ID, Statsig ID, Device ID Backup, Segment ID, Machine ID, Entropy Source) suggests deliberate over-engineering for tracking persistence. This demonstrates that device fingerprinting is an industry-wide practice, with OpenAI implementing it more extensively than Anthropic.

Six separate device identifiers discovered:

#	Identifier	Value	Location
1	Sentry Device ID	`393445FD-153B-47C0-8814-F958F06C0093`	`io.sentry/INSTALLATION`
2	Statsig Stable ID	`57938EBA-8EBF-40CB-9425-3ECE3A3C9D41`	`com.openai.atlas.plist`
3	Device ID Backup	`CF84FE22-2B93-4AF5-977B-4488BA4F42A4`	`com.openai.atlas.plist`
4	Segment Anonymous ID	`394F3C24-E247-4BE8-9E4C-DA85B977947C`	`com.segment.storage.oai.plist`
5	Machine ID	`7372387`	`Local State` JSON
6	Entropy Source	`FA9CDB724C88B7F47EB1128E79EDD738`	`Local State` JSON

More persistent identifiers than Claude Desktop (4-6 vs 1-2).

FINDING 3: Plaintext Email Exposure [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 359-373)

Forensic Significance: Storing user email addresses in plaintext in unencrypted preference files (`com.openai.chat.StatsigService.plist`) represents a security vulnerability—any process on the system can read this file without elevated privileges. This exposes PII (Personally Identifiable Information) to potential malware or unauthorized access. The combination of email, account ID, plan type, and user ID in one file creates a complete user profile. This finding documents a privacy concern in ChatGPT Atlas that may be relevant to comparative analysis.

File: `~/Library/Preferences/com.openai.chat.StatsigService.plist`

Complete Content:

```
xml
<dict>
  <key>accountID</key>
  <string>a183ed1b-39bd-4a8c-99f0-1e1172ecb41f</string>
  <key>planType</key>
  <string>team</string>
  <key>userEmail</key>
  <string>jdkirchner47@gmail.com</string>
  <key>userID</key>
  <string>user-CKysnbNDz3G9BBTWYHbThPk1</string>
</dict>
```

CRITICAL: User email address stored in **plaintext** in unencrypted preference file accessible to any process on the system.

FINDING 4: Extensive Behavior Tracking [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 575-615)

Forensic Significance: The tracking of 40+ specific user behaviors with Unix timestamps creates a detailed behavioral profile of user interaction patterns. The timestamp precision enables reconstruction of user workflow sequences. Features like `hasSeenMemoryOnboarding`, `hasSeenAdvancedVoice`, and `hasSeenAppPairingOnboarding` track feature discovery and adoption. This granular behavioral data enables sophisticated user analytics beyond what's necessary for application function, establishing that comprehensive behavior tracking is an industry-wide AI assistant practice.

40+ user behaviors tracked with Unix timestamps:

Behavior Key	Timestamp	Event
`oai/apps/hasSeenOnboarding`	748995615	Initial onboarding
`oai/apps/hasSeenMemoryOnboarding`	749505305	Memory feature intro
`oai/apps/hasSeenAdvancedVoice/2024-09-24`	753681907	Voice features
`oai/apps/hasSeenAppPairingOnboarding`	753666904	Work with Apps
`oai/apps/hasSeenCanvasCodeExecutionNux`	762134435	Code execution
`oai/apps/hasSeenO3MiniNux`	760904307	o3-mini model
`oai/apps/hasSeenConnectorsNuxModal`	770831171	Connectors intro
`oai/apps/hasSeenExistingUserPersonalityOnboarding`	787061340	Personality feature

FINDING 5: Data Storage Volume [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 86-99)

Forensic Significance: ChatGPT Atlas stores approximately 470 MB of local data—9x more than Claude Desktop (~50 MB). This volume includes browser cache (333 MB), conversation data (14 MB), Statsig cache (2.7 MB), and multiple preference files. The distribution across 6+ distinct storage locations demonstrates comprehensive data retention. This finding establishes that both major AI assistants retain substantial local data, with OpenAI's retention significantly exceeding Anthropic's.

#	Location	Size	Purpose
---	----------	------	---------

1	`~/Library/Application Support/com.openai.atlas/`	136 MB	Primary data
2	`~/Library/Caches/com.openai.atlas/`	333 MB	Browser cache
3	`~/Library/HTTPStorages/com.openai.atlas/`	488 KB	HTTP data
4	`~/Library/Preferences/com.openai.*.plist`	~7 KB	Preferences
5	`~/Library/Preferences/com.segment.storage.oai.plist`	~1 KB	Segment data
TOTAL		~470 MB	

ChatGPT Atlas stores ~9x more local data than Claude Desktop (~50 MB).

FINDING 6: Segment Analytics Deep Dive [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 305-355)

Forensic Significance: The Segment analytics integration shows 61 tracked events with persistent user identification (`segment.userId`). The anonymous ID (`segment.anonymousId`) enables tracking even before user authentication. The binary traits data (504 bytes) suggests detailed user characteristics are stored. This demonstrates that Segment—the same analytics provider used by Anthropic—is an industry-standard tool for AI assistant behavioral tracking, providing comparative context for Anthropic's practices.

File: `~/Library/Preferences/com.segment.storage.oai.plist`

```
{
"segment.anonymousId" => "394F3C24-E247-4BE8-9E4C-DA85B977947C"
"segment.events" => 61
"segment.settings" => {length = 124, bytes = 0x626c7330d126974... 0000000053}
"segment.traits" => {length = 504, bytes = 0x626c7330dc246... 000000198}
"segment.userId" => "user-CKysnbNDz3G9BBTWYHbThPkl"
}
```

61 analytics events tracked with persistent user identification.

FINDING 7: "Work with Apps" File Access Infrastructure [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 656-709)

Forensic Significance: The "Work with Apps" feature provides ChatGPT Atlas access to 30+ third-party services including Google Drive, OneDrive, GitHub, Slack, Salesforce, and more. The `appPairing => true` feature flag enables this functionality. This represents

extensive file access capability across enterprise services. While disclosed, the scope of access (30+ connectors) significantly exceeds typical user expectations for a chat assistant and provides comparable context for Claude's file access capabilities.

30+ third-party connectors discovered:

Connector ID	Service
`connector:google_drive`	Google Drive
`connector:onedrive`	Microsoft OneDrive
`connector:confluence`	Atlassian Confluence
`connector:sharepoint`	Microsoft SharePoint
`connector:dropbox`	Dropbox
`connector:notion`	Notion
`connector:slack`	Slack
`connector:github`	GitHub
`connector:jira`	Atlassian Jira
`connector:salesforce`	Salesforce
`connector:hubspot`	HubSpot

Feature Flag: appPairing => true

FINDING 8: Sentry Telemetry Session [EXHIBIT-OPENAI-01]

Evidence: exhibits/EXHIBIT-OPENAI-

01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md (lines 427-465)

Forensic Significance: The Sentry session data demonstrates active telemetry tracking including device ID, session ID, timestamps, release version, and environment. Sentry—also used by Anthropic—provides "crash reporting" that doubles as comprehensive session analytics. The `environment: "production-macos"` tag enables segmentation of telemetry by platform. This finding confirms Sentry is standard infrastructure for AI assistant telemetry across the industry.

File: ~/Library/Application

Support/com.openai.atlas/io.sentry/.../session.current

json

```
{
  "seq": 1,
  "sid": "EBC5BD58-4F11-4E0E-8337-1BB58EF9946E",
  "did": "393445FD-153B-47C0-8814-F958F06C0093",
  "timestamp": "2025-12-22T19:03:50.146Z",
  "status": "ok",
```

```

1  "started": "2025-12-22T19:03:50.145Z",
2  "attrs": {
3  "release": "com.openai.atlas@1.2025.344.7+20251218120745000",
4  "environment": "production-macos"
5  },
6  "errors": 0,
7  "init": true
8  }
9
10
11

```

FINDING 9: Local Encryption vs Claude [EXHIBIT-OPENAI-01]

Evidence: reports/CHATGPT_ATLAS_PRELIMINARY_FORENSIC_ANALYSIS.md (lines 96-111)

Forensic Significance: This finding is critical for comparative analysis—ChatGPT Atlas encrypts conversation data locally while Claude Desktop stores it in decodable Base64. OpenAI's encrypted storage protects user data from local forensic inspection, while Anthropic's approach leaves conversation data readable. This demonstrates that local encryption is technically feasible for AI assistants; Anthropic's choice to use Base64 encoding rather than encryption represents a deliberate decision to maintain data accessibility (for themselves or forensic analysis).

Conversation Data Encryption Comparison:

Aspect	Claude Desktop	ChatGPT Atlas
Storage Method	Base64 encoding	Encrypted binary
Readability	Decodable	Requires encryption key
Local Security	LOW	HIGH

ChatGPT Atlas hexdump:

```

00000000: 5162 3a59 66df b516 7e14 9b86 e46c 2766  Qb:Yf...~....!f
00000010: 4be6 1401 1603 08f9 3fb3 1ece dc30 22a3  K.....?....0".

```

OpenAI encrypts conversation data locally; Anthropic stores it in decodable base64.

FINDING 10: Apple Intelligence OS-Level Integration [EXHIBIT-OPENAI-04]

Evidence:

openai_evidence_bases/reports/APPLE_INTELLIGENCE_CHATGPT_PARTNER_REPORT.md
(lines 46-89)

Forensic Significance: The discovery of OS-level ChatGPT partner configuration (com.apple.Settings.AppleIntelligence.Partner.ChatGPT) with NO equivalent for Claude/Anthropic demonstrates preferential treatment at the operating system level. This is stored in a HIDDEN file (note leading . in filename) in system preferences. The absence of any generic partner framework or Anthropic-equivalent configuration suggests exclusive integration. This finding supports claims of anticompetitive arrangements between Apple and OpenAI and explains observed behavioral differences in how macOS handles the two AI assistants.

File: /Users/everest/Library/Preferences/ByHost/.GlobalPreferences.*.plist

ChatGPT Partner Configuration:

```
json
{
  "com.apple.Settings.AppleIntelligence.Partner.ChatGPT": [
    {
      "unavailable": {
        "_0": {
          "partnerNotSelected": {}
        }
      }
    }
  ]
}
```

Critical Observation:

- Partner.ChatGPT key exists
- No Partner.Claude key
- No Partner.Anthropic key
- No generic partner framework

This demonstrates preferential OS-level integration with OpenAI that does not exist for Anthropic.

FINDING 11: Disabled Code Language Model [EXHIBIT-OPENAI-04]

Evidence:

openai_evidence_bases/reports/APPLE_INTELLIGENCE_CHATGPT_PARTNER_REPORT.md
(lines 91-125)

Forensic Significance: The codeLM.denyThisUseCaseOnJune6of2024 configuration is forensically explosive—the naming convention embeds the exact date of WWDC 2024 when Apple announced its OpenAI partnership. A code language model feature was deliberately disabled on the day of the partnership announcement. This raises questions about exclusivity arrangements affecting Xcode AI features and whether Apple's code assistance capabilities

were curtailed as part of the OpenAI deal. This configuration persists across both May and December 2025 files, indicating a permanent policy decision.

Configuration Key:

```
json
{
  "com.apple.gms.availability.disabledUseCases": [
    "codeLM.denyThisUseCaseOnJune6of2024"
  ]
}
```

Significance:

Date	Event
June 6, 2024	WWDC 2024 - Apple Intelligence announced
June 6, 2024	Apple-OpenAI partnership revealed

A code language model feature (`codeLM`) was **deliberately disabled on the day Apple announced its OpenAI partnership**.

FINDING 12: Raw Datadog Telemetry Log Analysis [EXHIBIT-OPENAI-01]

Evidence:

openai_evidence_bases/chatgpt_datadog_20251226_180727/Caches_datadoghq/...
/788469685641 (5,671 bytes)

SHA-256: 42956e3cf287a22c914324b11809aedabd15d38ccf43c19693d5145f38a3ce8e

Forensic Significance: This is the raw, unprocessed telemetry log cached locally before transmission to Datadog. The 5,671 byte file contains actual JSON telemetry events with complete user identification, feature flags, device information, and session data. This cache file proves what data is transmitted—it's not just metadata but comprehensive user context. The integrity hash enables verification that this evidence has not been tampered with.

This raw binary log file contains **actual JSON telemetry events** transmitted to Datadog.

FINDING 13: Complete User Identification in Telemetry [EXHIBIT-OPENAI-01]

Forensic Significance: The telemetry payload contains complete user identification—user ID, account ID, device ID, plan type, payment status, and login state. This is NOT anonymous analytics; it's fully attributed user tracking. The `has_paid_plan: true` and `plan_type: team` fields indicate monetization data is transmitted. This level of identification in telemetry sent to a third party (Datadog) may violate user expectations and privacy policies that suggest anonymous or aggregated analytics.

Extracted from raw Datadog log:

Field	Value
`usr.id`	`user-CKysnbNDz3G9BBTWYHbThPkl`
`usr.account_id`	`a183ed1b-39bd-4a8c-99f0-1e1172ecb41f`
`usr.device_id`	`CF84FE22-2B93-4AF5-977B-4488BA4F42A4`
`usr.plan_type`	`team`
`usr.has_paid_plan`	`true`
`usr.is_logged_in`	`true`
`usr.total_accounts`	`1`
`usr.push_notifications_authorized`	`false`

This proves Datadog receives full user identification including account ID, plan type, and payment status.

FINDING 14: 30+ Statsig Feature Flags in Telemetry [EXHIBIT-OPENAI-01]

Forensic Significance: The transmission of 30+ feature flags to Datadog reveals complete application configuration state. Notably, flags like `analytics_disabled: false`, `disable-sentry-analytics: false`, and `disable-statsig-analytics: false` confirm all analytics systems are ENABLED. The `disable-datadog-experiment-tracking: false` flag proves A/B testing is active. This telemetry configuration data enables reconstruction of exactly what features were active for any user session, demonstrating comprehensive behavioral experimentation infrastructure.

Raw feature flags transmitted to Datadog:

Flag	Value	Implication
`analytics_disabled`	`false`	Analytics ENABLED
`disable-sentry-analytics`	`false`	Sentry ENABLED
`disable-statsig-analytics`	`false`	Statsig ENABLED
`disable-datadog-experiment-tracking`	`false`	Datadog experiments ENABLED
`disable-notifications`	`false`	Notifications ENABLED
`desktop-disable-kf-encryption`	`false`	Keychain encryption ENABLED
`atlas-enable-on-page-suggestions`	`true`	Page suggestions active
`atlas-enable-sidechat-guided-tour`	`true`	Guided tour active
`atlas-enable-vertical-tabs`	`true`	Vertical tabs active
`atlas-enable-multi-profile-per-workspace`	`true`	Multi-profile active

'conversation-pinning'	'true'	Conversation pinning
------------------------	--------	----------------------

Full telemetry configuration is transmitted to Datadog.

FINDING 15: Device Hardware Fingerprinting [EXHIBIT-OPENAI-01]

Forensic Significance: The telemetry includes detailed hardware fingerprinting—device model (Mac16,5), architecture (arm64e), brand (Apple), OS version (26.1.0), and build number (25B78). This hardware profile enables device identification beyond software-based identifiers. The `apple_device_model: arm64` and `apple_platform: macOS` tags enable platform-specific analytics. This level of hardware detail transmitted to third-party Datadog enables device fingerprinting that persists across application reinstallation.

Device information in telemetry:

```
json
{
  "_dd": {
    "device": {
      "model": "Mac16,5",
      "name": "Mac",
      "architecture": "arm64e",
      "brand": "Apple"
    }
  },
  "apple_device_model": "arm64",
  "apple_platform": "macOS",
  "os": {
    "version": "26.1.0",
    "name": "macOS",
    "build": "25B78"
  }
}
```

FINDING 16: Network Configuration Disclosure [EXHIBIT-OPENAI-01]

Forensic Significance: The transmission of network topology information (`supports_ipv6`, `supports_ipv4`, `available_interfaces: ["other", "other", "wifi"]`) to Datadog reveals the user's network configuration. This data enables network environment profiling—identifying whether users are on corporate networks, home WiFi, or cellular connections. The `is_constrained` and `is_expensive` flags indicate connection quality assessment. This

network metadata combined with device fingerprinting creates comprehensive environmental profiling beyond application usage.

Network state transmitted to Datadog:

Field	Value
`network.client.supports_ipv6`	`true`
`network.client.supports_ipv4`	`true`
`network.client.is_constrained`	`false`
`network.client.is_expensive`	`false`
`network.client.reachability`	`yes`
`network.client.available_interfaces`	`["other","other","wifi"]`

Network topology and interface information is disclosed.

FINDING 17: Session and Window Tracking [EXHIBIT-OPENAI-01]

Forensic Significance: The session and window tracking reveals granular application usage patterns—including window numbers, tab group IDs, and profile IDs. The `WindowLifecycleEvent: appTermination` logging captures exactly when and how users close the application. The composite identifier format (`profileID__tabGroupID`) enables correlation of browser-like behavior across multiple windows. This level of window lifecycle tracking creates a detailed timeline of user interaction patterns.

Session identifiers in telemetry:

Identifier	Value
`app_session_id`	`7784ca84-669c-4e72-82b6-441c108c4be8`
`ios.foreground_interval_id`	`5bf5ae19-4484-4256-ae7c-676a99c027dc`
`profileID`	`D9F38ACA-885E-4DCE-BF01-F2D73E882C27`
`tabGroupID`	`window:590CBE98-9268-4BDC-B8CF-D7B47E5B7FCE`
`window.windowNumber`	`138082`

Window lifecycle events tracked:

message: "WindowLifecycleEvent: appTermination(windowType: main(browser(profileID: D9F38ACA-885E-4DCE-BF01-F2D73E882C27 (user-CKysnbNDz3G9BBTWYHbThPkl_a183ed1b-39bd-4a8c-99f0-1e1172ecb41f), tabGroupID: window:590CBE98-9268-4BDC-B8CF-D7B47E5B7FCE)))"

FINDING 18: Build and Environment Details [EXHIBIT-OPENAI-01]**Evidence:**

openai_evidence_bases/chatgpt_datadog_20251226_180727/Caches_datadoghq/.../788469685641

Forensic Significance: The build information (version: 1.2025.344.7, build: 20251218120745000) enables precise version tracking of user installations. The environment: production-macos and service: chatgpt-client-web tags reveal the application architecture—ChatGPT Atlas is a web-based Electron application using browser SDK telemetry. This confirms the application uses Chromium-based web technologies, explaining the extensive browser-style telemetry infrastructure. The build timestamp precision (to the millisecond) enables exact release correlation.

Build Identifier:

```
json
{
  "version": "1.2025.344.7",
  "build": "1.2025.344.7+20251218120745000",
  "release": "com.openai.atlas@1.2025.344.7+20251218120745000",
  "environment": "production-macos"
}
```

Application Metadata:

Field	Value
Bundle ID	`com.openai.atlas`
Version	`1.2025.344.7`
Build Date	2025-12-18 12:07:45
SDK	Datadog Browser SDK

Service Configuration:

```
json
{
  "service": "chatgpt-client-web",
  "source": "browser",
  "ddsource": "browser"
}
```

This confirms ChatGPT Atlas uses web-based Electron architecture with browser SDK telemetry.

III. COMPARATIVE ANALYSIS**Claude Desktop vs ChatGPT Atlas****Evidence:** EXHIBIT-OPENAI-01 (lines 843-854)

Aspect	Claude Desktop	ChatGPT Atlas
Hidden Home Directory	Yes (~/.claude/)	No
Preference Files	Minimal	6 separate files
Local Encryption	No (Base64)	Yes (Binary)
Device IDs	1-2	4-6
User Email in Plaintext	Unknown	Yes
Behavior Timestamps	Unknown	40+
Total Storage	~50 MB	~470 MB
Third-Party Providers	3	4

Common Industry Pattern

Both applications share:

- **Statsig** for feature flags and analytics
- **Sentry** for crash reporting and event tracking
- **Segment** for behavioral analytics
- Hash-based file naming
- Persistent device fingerprinting
- Session tracking infrastructure

IV. DATA FLOW DIAGRAM

+-----+

CHATGPT ATLAS TELEMETRY FLOW

+-----+

User Action	
v	

| +-----+ |

	LOCAL COLLECTION	
	- User ID: user-CKysnbNDz3G9BBTWYHbThPkl	
	- Account ID: a183ed1b-39bd-4a8c-99f0-1e1172ecb41f	

	- Device ID: CF84FE22-2B93-4AF5-977B-4488BA4F42A4	
	- Plan Type: team	
	- 30+ Feature Flags	
	- Network Topology	
	- Hardware Model: Mac16,5	

+-----+	
v	

+-----+		
	TRANSMISSION TO DATADOG	
	Endpoint: datadog-BTgRrIvw.js	
	Cache: Caches_datadoghq/v2/d0b9b4161a5...	
	Format: JSON (gzip compressed in transit)	

+-----+	
+-----+	

V. LEGAL IMPLICATIONS

Industry-Wide Pattern

The forensic analysis establishes that **surveillance-grade telemetry is an industry standard** in AI assistant applications:

Provider	Statsig	Sentry	Segment	Datadog
Anthropic (Claude)	Yes	Yes	Yes	-
OpenAI (ChatGPT)	Yes	Yes	Yes	Yes

Apple-OpenAI Preferential Treatment

Factor	OpenAI/ChatGPT	Anthropic/Claude
OS-level partner integration	YES	NO
Settings.app partner configuration	YES	NO
NetworkServiceProxy special handling	YES	NO
IntelligencePlatform tracking	YES	NO

Privacy Concerns

- 1. Plaintext PII:** Email stored unencrypted in preference files
- 2. Multiple Identifiers:** 4-6 persistent device IDs enable cross-session tracking
- 3. Behavior Timestamps:** 40+ user interactions recorded with timestamps
- 4. Third-Party Transmission:** Data sent to 4 analytics providers
- 5. File Access Scope:** 30+ third-party service connectors

VI. KEY EVIDENCE HASHES

Evidence	SHA-256
Raw Datadog log (788469685641)	`42956e3cf287a22c914324b11809aedabd15d38ccf43c19693d5145f38a3ce8e`
EXHIBIT-OPENAI-01	`56a11e0214862562ffbec977f1e568e24b38eae1cd298cecd12ef0aaab4b7b61`
APPLE_INTELLIGENCE_CHATGPT_PARTNER_REPORT	`435c723436e3e8ef0a4cb6649c1609e576a51d5734d788aff828cffb83aec2b7`
CHATGPT_ATLAS_PRELIMINARY_FORENSIC_ANALYSIS	`b89dfdc5ed5dbbb2496ca4f4b75a640e10cddbfea3b728ef1a578d84758a63b0`

VII. CHAIN OF CUSTODY

Manifest: manifests/FILE_LOCATION_MANIFEST.md

Integrity Hashes: manifests/SHA256SUMS.txt

All files copied from original locations on 2025-12-28. Original files remain in place for verification.

VIII. CONCLUSIONS

iOS Application Findings (ChatGPT Superior)

- 1. ChatGPT iOS implements certificate pinning** - Claude iOS does not, demonstrating OpenAI exceeds Anthropic in mobile security.
- 2. ChatGPT iOS does NOT use Sift Science** - Claude iOS surveils users with fraud detection; ChatGPT proves this is unnecessary.
- 3. ChatGPT iOS requests fewer permissions** - No calendar/reminders access unlike Claude iOS.

1 **4. ChatGPT iOS has full privacy manifest compliance** - All SDKs disclosed, 0
 2 undisclosed third parties.
 3

4 **Desktop Application Findings (Industry Pattern)**

5 **5. ChatGPT Desktop has NO certificate pinning** - Unlike iOS, allowing full traffic
 6 inspection.
 7

8 **6. ChatGPT Desktop transmits to Facebook** - App ID 468742119653388, undisclosed in
 9 privacy policy.
 10

11 **7. ChatGPT Desktop sends 102+ requests to Amazon** - Transmitting Amazon cookies
 12 while using ChatGPT.
 13

14 **8. ChatGPT Desktop CSP whitelists ad networks** - TikTok, LinkedIn, Reddit, Microsoft
 15 intentionally enabled.
 16

17 **9. ChatGPT Atlas implements more extensive telemetry** than Claude Desktop:

- 18 • 4 third-party providers vs 3
- 19 • 4-6 device identifiers vs 1-2
- 20 • 470 MB local storage vs 50 MB
- 21 • 40+ behavior timestamps tracked
- 22

23 **10. ChatGPT Atlas has better local security** than Claude Desktop:

- 24 • Encrypted conversation storage vs base64 encoding
- 25 • However, email stored in plaintext preference file
- 26

27 **Apple-OpenAI Integration**

28 **11. Apple provides OS-level preferential integration to OpenAI** that does not exist for
 29 Anthropic:

- 30 • ChatGPT partner configuration in hidden preferences
- 31 • No equivalent Claude/Anthropic partner framework
- 32

33 **12. A code language model feature was disabled** on the day Apple announced its OpenAI
 34 partnership (June 6, 2024), raising questions about exclusivity arrangements.
 35

36 **Industry Pattern**

37 **13. The industry shares common telemetry infrastructure:**

- 38 • Both Claude and ChatGPT use Statsig, Sentry, and Segment
- 39 • This represents an industry-wide pattern, not unique to Anthropic
- 40

42 **IX. INTEGRITY VERIFICATION**

43 bash

Navigate to evidence package

```
cd /Users/everest/Git/code_forensics/evidence_packages/openai
```

Verify all file hashes

```
shasum -a 256 -c manifests/SHA256SUMS.txt
```

Verify primary telemetry evidence

```
shasum -a 256
openai_evidence_bases/chatgpt_datadog_20251226_180727/Caches_datadoghq/v2/d0b9b41
61a5ef0e4b1f5a7ac04667e4e7011273a443ddfe9d66485e17cf58058/logging/v2/7884696856
41
```

Expected:

42956e3cf287a22c914324b11809aedabd15d38ccf43c19693d5145f38a3ce8e

Verify exhibit hash

```
shasum -a 256 anthropic_exhibits/EXHIBIT-OPENAI-
01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md
```

Expected:

56a11e0214862562ffbec977f1e568e24b38eae1cd298cecd12ef0aaab4b7b61

Total package size

```
du -sh .
```

Expected: ~104K

X. APPENDIX: EVIDENCE PACKAGE DIRECTORY LISTING

```
evidence_packages/openai/
├── EXECUTIVE_SUMMARY.md           # This file (~30 KB)
├── exhibits/
│   ├── EXHIBIT-OPENAI-
│   │   01_CHATGPT_ATLAS_COMPREHENSIVE_FORENSIC_ANALYSIS.md
│   │       # 1,022 lines - exhaustive telemetry analysis
│   ├── EXHIBIT-OPENAI-02_CHATGPT_IOS_FORENSIC_ANALYSIS.md
│   │       # iOS app forensic analysis
│   └── EXHIBIT-OPENAI-03_CHATGPT_DESKTOP_NETWORK_FORENSICS.md
│       # Desktop network traffic analysis
```

```

1  └─ manifests/
2     └─ FILE_LOCATION_MANIFEST.md      # Source path mapping
3     └─ SHA256SUMS.txt                 # Integrity hashes
4
5  └─ openai_evidence_bases/
6     └─ chatgpt_datadog_20251226_180727/ # Datadog telemetry extraction
7        └─ README.md                   # Evidence base documentation
8        └─ extraction_manifest.txt     # Extraction log
9        └─ file_hashes.txt             # Original integrity hashes
10       └─ Caches_datadoghq/
11          └─ v2/d0b9b4161.../
12             └─ logging/v2/
13                └─ 788469685641      # RAW TELEMETRY LOG (5,671 bytes)
14
15     └─ chatgpt_analysis/              # iOS app analysis
16        └─ ChatGPT 1.2025.350.ipa     # iOS app binary (127.6 MB)
17        └─ FORENSIC_CHATGPT_IOS_ANALYSIS.md # iOS forensic report
18        └─ CHATGPT_ATLAS_FORENSIC_REPORT.md # Desktop network report
19        └─ chatgpt_atlas_capture.flow  # Network capture (26.7 MB)
20        └─ static_analysis/           # IPA static analysis
21
22     └─ CHATGPT_EVIDENCE_20251228_142719/ # Additional evidence collection
23
24  └─ reports/
25     └─ APPLE_INTELLIGENCE_CHATGPT_PARTNER_REPORT.md
26        # 370 lines - OS-level Apple integration
27     └─ CHATGPT_ATLAS_PRELIMINARY_FORENSIC_ANALYSIS.md

```

256 lines - cross-platform comparison

XI. COLLECTION TIMELINE

Date	Time	Action
2025-12-26	18:07:27	Datadog cache extraction
2025-12-28	-	Evidence package organization
2025-12-28	-	SHA-256 hashes computed
2025-12-28	-	Executive summary generated
2025-12-29	-	Executive summary updated

Collector: Joseph Kirchner

XII. UPDATE HISTORY

Date	Changes
2025-12-28	Initial executive summary with 18 findings
2025-12-29	Minor updates
2026-01-02	Added forensic significance statements to all 18 findings
2026-01-02	Added iOS findings (19-24) from FORENSIC_CHATGPT_IOS_ANALYSIS.md
2026-01-02	Added desktop network findings (25-30) from CHATGPT_ATLAS_FORENSIC_REPORT.md
2026-01-02	Renamed exhibit to EXHIBIT-OPENAI-01 format
2026-01-02	Created EXHIBIT-OPENAI-02 (iOS) and EXHIBIT-OPENAI-03 (Desktop Network)

Executive Summary Prepared: 2025-12-28

Last Updated: 2026-01-02

Case: Kirchner v. Anthropic, PBC (1:25-cv-02735-ACR)

Package: OpenAI/ChatGPT Evidence

Total Findings: 30

Total Exhibits: 3

Total Size: ~160 KB