AI Agent Activity Forensic Report

Case ID	GL-20260812-001
Endpoint	LAPTOP-G7PVTSS3
Subject	Codex CLI session
Activity window	2026-08-12 00:19:54–00:22:15 EDT
Acquisition window	2026-08-12 00:22–00:31 EDT
Report generated	2026-08-12 02:15 EDT
Report version	1.2
Evidence acquired	~1.06 GB · 5 source groups

> **PRINCIPAL ARTIFACT**
>
> A directory containing 449 numbered, one-word text files that reconstruct a poem titled *Instructions for Surviving the Ordinary*.

Observed – the collector directly observed it during acquisition	**Agent-recorded** – the fact appears only in the agent's own transcript or output
Corroborated – two or more independent acquired sources support the same finding	**Verified** – directly validated against acquired evidence
Verified in scope – validated only within the stated tool, audit or collection boundary	**Not established** – the available evidence is insufficient to determine the fact either way

EXECUTIVE SUMMARY

Shortly after midnight on August 12, 2026, a **Codex CLI session** (GPT-5, codex-tui v0.147.0) operating from `C:\Users\[REDACTED]` performed a short sequence of file and inspection activity lasting approximately **2 minutes 21 seconds**. GhostLogic reconstructed the **available session timeline** from the acquired Codex transcript, sandbox audit logs, and filesystem observations.

Per the transcript, the session attempted a batch of read-only inspection calls that failed when the sandbox could not unlock required credentials. The transcript subsequently records an attempted write of `tool-call-demo.txt`; that file was **not**

found within the documented acquisition search scope (E7), and the available evidence does not establish whether the write failed, the file was later removed, or it was written to an unsearched location.

The transcript then records generation of a poem titled *"Instructions for Surviving the Ordinary"* and creation of **449 numbered text files** under `C:\Users\[REDACTED]\poem-one-word-each`, one word per file. The collector found the directory on disk, preserved its contents and manifest, and successfully reconstructed the poem from the numbered sequence.

Two sandbox self-audits recorded 272 scanned items and no findings **within the scope of those checks**; this does not independently establish that the session or workstation was free from compromise. The sequence described above is supported by the acquired evidence, subject to documented collection limitations: the Windows Security event log was not acquired (administrative elevation unavailable), and a separate 4.0 GB transcript archive was inventoried but not duplicated.

> **The agent said it created something.**
> **GhostLogic checked whether reality agreed.**

SESSION TIMELINE · AUGUST 12, 2026 (EDT)

00:19:54 — **Agent session starts** in the workstation home directory. First sandbox self-audit: 272 items scanned, no findings within scope.
E1 · E2 — Corroborated

00:20:07 — Batch of parallel read-only inspection calls issued; transcript records failure — the sandbox could not unlock its credentials.
E1 — Agent-recorded

00:20:22 — Transcript records an attempted write of `tool-call-demo.txt`. The file was not found within the documented acquisition search scope; cause not established.
E1 — Agent-recorded · E7

00:20:40 Agent is tasked with composing a poem, then splitting it one word per file.

E1 — Agent-recorded

00:20:54 Second sandbox self-audit — no findings within scope.

E2 — Verified in scope

00:21:07 **Poem artifact activity.** The transcript records generation of the poem and creation of 449 numbered, one-word files in `poem-one-word-each\`. The resulting directory and numbered sequence were found on disk and preserved during acquisition. The transcript also records verification of the first and last files.

E1 · E3 · E7 — Corroborated

00:22:15 Agent confirms completion; session ends — 2 min 21 s total.

E1 — Agent-recorded

00:22–31 **Evidence acquisition.** Event logs exported, servicing and agent log sets copied, artifact directory preserved with manifest and reassembled text; SHA-256 hashes computed for keyed exhibits.

E6 · E5 — Observed

> *When morning barges through the blinds*
> *wearing yesterday's wrinkled shirt,*
> *do not accuse it of repetition.*
> *The sun has only one good trick,*
> *and still, look how the dust applauds.*
>
> EXHIBIT E4 — OPENING STANZA, REASSEMBLED FROM FILES 006–035 OF 449

FINDINGS

FINDING	STATUS	SUPPORT
Codex session occurred	CORROBORATED	Transcript and sandbox audit logs (E1, E2)
Inspection calls failed	AGENT-RECORDED	Session transcript (E1)
`tool-call-demo.txt` write attempted	AGENT-RECORDED	Session transcript (E1)

FINDING	STATUS	SUPPORT
Demo file persisted successfully	NOT ESTABLISHED	Not found within the documented acquisition search scope (E7)
449-file poem directory created	CORROBORATED	Transcript, filesystem observation, manifest (E1, E3, E7)
Poem sequence reconstructed	VERIFIED	Preserved files (E3, E4)
No sandbox findings	VERIFIED IN SCOPE	Two audit records (E2)
Complete workstation visibility	NOT ESTABLISHED	Security log and archive limitations (E6)

EXHIBIT INDEX

ID	ITEM	SHA-256 (FIRST 16)
E1	Codex session transcript `rollout-2026-08-12T00-19-54-…0e1294.jsonl`	`46fc417d6adb9e12`
E2	Sandbox audit log `sandbox.2026-08-12.log`	`a444d43f984b87a9`
E3	Poem directory manifest (timestamped, 449 entries)	`07189b508c0e6178`
E4	Reassembled poem text	`2765b88d4cb5f3f0`
E5	Application event log export `Application.evtx`	`3e36cd48ad434097`
E6	Evidence acquisition and collection log `GL-20260812-001_EVIDENCE_ACQUISITION_LOG.md`	`c98fa76ff7356e2a`
E7	Filesystem acquisition observation `E7_FILESYSTEM_ACQUISITION_OBSERVATION.md`	`98c23ffdd8c8e484`

Full digests for all keyed exhibits are preserved in `GL-20260812-001_EVIDENCE_MANIFEST.sha256` inside the evidence set and verify with `sha256sum -c` (renamed on 2026-08-12 from `EVIDENCE_HASHES.sha256`, the name recorded in E6 at acquisition; exhibit digests unchanged).

- **E6 — collection log** (`GL-20260812-001_EVIDENCE_ACQUISITION_LOG.md`; written at acquisition as `README.md` and renamed to a case-specific filename and marked read-only on 2026-08-12, content and digest unchanged). Records the collection window (2026-08-12 00:22–00:31 EDT), the five source groups acquired, the deliberate exclusions (agent credential stores; the 4.0 GB conversation-transcript archive, inventoried by manifest instead of copied), the

collection failure (Security event log — export denied without Administrator elevation), and the collecting tool (a Claude Code session; tool version not recorded).

- **Manifest protection.** The manifest carries its own custody header (Case ID, creation timestamp 2026-08-12 01:22 EDT, collector identity) and is set read-only on the endpoint. Its own digest is `SHA-256 82eb9ba0a30853dee5560c3ca9e7aeaf138f1db27be70b62fbd34c0dc87c478d`, preserved separately from the evidence directory: in the user Documents folder on the endpoint (`GL-20260812-001_MANIFEST_DIGEST.txt`) and in this independently hosted report. No signing key was available to this collector, so the manifest is not digitally signed; the independently stored digest serves as the tamper reference, and the read-only attribute deters only casual modification.
- **E7 — filesystem observation.** Records the inspected scope (`C:\Users\[REDACTED]`, recursive, hidden and system files included), method (PowerShell `Get-ChildItem -Recurse -Force -Filter`), collector and timestamps, the null result for `tool-call-demo.txt` (0 matches; 1 access-denied path skipped), and the observed state of `poem-one-word-each\`: 449 files, directory created 2026-08-12 00:21:41.698 EDT, file write times 00:21:41.701–00:21:43.045 EDT.

EVIDENCE SET

FOLDER	SIZE	CONTENTS
`WindowsEventLogs\`	33 MB	Application, System, Setup, PowerShell, WindowsUpdateClient, Windows Defender (.evtx exports)
`WindowsLogs\`	363 MB	CBS, DISM, WindowsUpdate servicing logs
`Claude\`	239 MB	Agent debug, daemon, telemetry, task and session logs, plus a 5,275-file manifest of the uncopied transcript archive
`Codex\`	429 MB	Agent log directory, full session transcripts, 20 sandbox audit logs, structured log database
`CodexCreated\`	621 KB	The 449-file poem directory, its timestamped manifest, and the reassembled poem

CHAIN OF CUSTODY · SCOPE NOTES

- **Credentials excluded by policy.** Known agent credential stores (`auth.json`, `secrets\`) were excluded: the destination folder syncs to cloud storage, and live tokens must never leave the workstation. This exclusion does not establish that no sensitive values appear elsewhere in the acquired logs or transcripts; the acquired exhibits have not been scanned for credentials.
- **Transcript archive listed, not duplicated.** A 4.0 GB conversation-transcript archive was inventoried in full (5,275 files, timestamped) rather than copied. Claims resting on that archive would be unsupported by this evidence set.
- **Security event log not acquired** — export requires Administrator elevation; recorded in E6 as a collection failure affecting workstation-level visibility.
- Statements sourced only to the agent's transcript are labeled *Agent-recorded* and are treated as the agent's claims, not as established facts, unless corroborated by an independent acquired source.
- Event log exports contain all history retained by Windows, not only the incident window.
- **User-profile redaction.** The user-profile identifier in filesystem paths is displayed as `[REDACTED]` for publication. The acquired exhibits retain the original paths unaltered, and all digests were computed over the unaltered evidence.
- Agent transcripts record timestamps in UTC; all times in this report are converted to local EDT (UTC−04:00).
- Poem authorship is attributed to the session in the sense that the transcript records its generation; global originality of the text is outside the scope of this evidence.
