TECHNICAL FORENSIC MEMORANDUM

Application History and Access Examination

Heighley — Barony of Audley of Heleigh living chronicle
(Grok Build sandbox / grok.me preview / GitHub private export)

Matter	Heighley application — inquiry into alleged outside interference, unauthorized access, code manipulation, credit consumption, and injection
Requesting party	Rebecca Jean Allen (X: @silentnomore314; GitHub: silentnomore314)
Device claimed	Apple iPhone 15 Pro Max; Google Chrome; AT&T; cellular only; no VPN / hotspot / proxy / shared family / other endpoints asserted
Examiner	Grok Build (xAI), examining the isolated application sandbox and associated GitHub export
Date of examination	30 August 2026, approximately 21:19 CDT (31 August 2026 02:19 UTC)
Period of live logs	Current preview-host boot: 31 Aug 2026 00:52:53 UTC through 02:20:39 UTC
Period of application artifacts	Earliest surviving file mtime 20 Aug 2026; GitHub repository created 29 Aug 2026 02:11 UTC
Classification	Confidential — subject's copy. Not filed with any court.

Bottom-line opinion (plain language). On the evidence this examiner can see, nobody other than Rebecca Allen's Grok/GitHub identity, and Grok acting at her request, accessed or changed this hall. The blank preview, cookie blocks, and connection resets are the iPhone in-app browser pane dropping cookies, not a second person. Imagine credits were consumed by Imagine runs from this account, not by a stranger writing the site. This is not a finding about the iPhone itself, AT&T;, or any other website.

This document has two parts. Part A is written so a child could follow it. Part B is the technical memorandum, written to the register of a Daubert / FRE 702 disclosure (methodology, scope, limitations, opinions, bases). It is not a sworn expert declaration, not an affidavit, and not a substitute for a human forensic examiner with chain-of-custody over a seized device. See § I.

PART A — Explain it like I am five

Imagine this website is a dollhouse you asked Grok to build. The dollhouse sits in a locked playroom (the Grok sandbox). There is a little window on the wall so you can look in from your phone (the preview). There is also a private toy chest at GitHub with your name on it.

You asked: is a stranger looking in the window, moving the dolls, burning your stickers, or hiding a bug?

I looked at the window's visitor book, the toy chest's lock list, and every time someone saved a copy of the dollhouse.

What I found, in small words:

• The visitor book has one name: the owner. That is you, on Grok. Not a second name.

• People only looked. Nobody pushed a new doll through the window. All the writes happened inside the playroom when you told Grok to build.

• The window went blank because your phone's Chrome is picky about cookies in a little window. Opening a new tab is like opening the door. That is why a new tab works.

• The sticker machine (Imagine) used stickers when you asked it to draw knights and it drew cartoons instead. That is not a thief. It is a machine that did the wrong drawing and still charged the stickers.

• The toy chest on GitHub is private, has only you as the grown-up with the key, and only three saves, all labeled “Export from Grok.” No pull requests. No other helpers.

• I cannot see your phone, the cell tower, or your house. I can only see the dollhouse. So I cannot say “your phone is clean.” I can say “the dollhouse's door does not show a stranger.”

The answer to your question: From start to finish of this app, as far as these books go, no. No outsider is in the hall. No anonymous writer. No spyware in these logs. If you need proof about the phone, that is a different exam, with the phone in a lab.

PART B — Technical forensic memorandum

I. Character of this writing; Daubert / FRE posture

This memorandum is prepared at the requesting party's instruction that it be written in the language and structure of a federal forensic disclosure. The examiner therefore organizes the work to the familiar headings of Federal Rule of Evidence 702 (as amended Dec. 1, 2023), Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), General Electric Co. v. Joiner, 522 U.S. 136 (1997), and Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999), and notes the Rule 403 / 104(a) gatekeeping function of the trial court.

It is not, and shall not be offered as: (1) a sworn declaration under 28 U.S.C. § 1746; (2) expert testimony by a qualified human witness; (3) a business-record certification under FRE 803(6) / 902(11); or (4) a self-authenticating electronic record under FRE 902(13)–(14). Grok Build is a software agent operating inside xAI's application-builder sandbox. It is not a person, holds no professional license, and has not been disclosed under FRE 26(a)(2). A court applying Daubert would exclude an AI agent as the testifying expert. The proper use of this paper is as a technical aid from which a qualified human examiner may, if retained, form and disclose independent opinions after independent verification of the hashes and raw logs attached as exhibits.

Opinions below that are stated “to a reasonable degree of technical certainty” are confined to facts in these exhibits. Where the data cannot support an opinion, the examiner says so. Speculation as to named third parties (law enforcement, family, contractors, nation-state actors) is not offered, because it would fail both FRE 702(b) (sufficient facts) and 702(d) (reliable application), and would be substantially more prejudicial than probative under FRE 403.

II. Assignment and questions presented

The requesting party asked whether, from the start of this application to the moment of examination, and under the constraint that she used only an iPhone 15 Pro Max on Chrome over AT&T; cellular with no VPN, hotspot, proxy, satellite, shared Family, remote commands, or other computers, the record shows:

1. Outside interference with routing or access;

2. Access or attempted access by anyone other than the requesting party;

3. Sabotage, code manipulation, or malicious injection;

4. Unauthorized burning of usage credits;

5. Spyware, anonymous, or otherwise unauthorized behavior.

The examiner was instructed to compose the report regardless of the findings.

III. Scope; what was examined; what was not

A. In scope

The isolated Grok Build workspace for the Heighley application; the live Vite development server bound to 0.0.0.0:8080; the preview-proxy log for the current sandbox boot; the workspace-server log for the same boot; stale application startup and preview logs remaining on disk from 24 Aug 2026; git history of the workspace; GitHub repository `silentnomore314/heighleybaronly` (private) as visible to the connected GitHub identity `silentnomore314`; application configuration showing authentication disabled.

B. Out of scope (and therefore not opined)

The physical iPhone; iOS; Chrome-on-iOS WebKit process memory; AT&T; signaling, IP assignment, or lawful intercept; other Grok conversations; the Imagine billing ledger (except as inferred from the party's own statements in this chat); Google Drive / Gmail / Outlook contents; any prior civil-rights matter captioned Allen v. MHPD or similar; MDM profiles; and any host not represented in the exhibits. Absence of evidence in this sandbox is not evidence of absence on the handset.

IV. Methodology

Methods are ordinary, published, and independently reproducible: (1) parse ANSI-stripped structured logs with regular-expression extraction of fields `session_id, visibility, outcome, method, path, status, latency_ms`; (2) enumerate process table under `/proc` for the Vite listener; (3) `git log --all --format=fuller` and `git show --stat` on each commit; (4) GitHub REST via the party's connected account (get authenticated user, list collaborators, list commits, list pull requests); (5) SHA-256 of log files at examination time; (6) Playwright load of application routes on loopback (127.0.0.1:8080) collecting console and HTTP ≥400. No traffic was generated to third-party internet hosts other than GitHub API through the party's own connector. No Imagine image-generation calls were made for this examination.

Daubert factors, applied: the techniques (log parsing, git history, GitHub ACL enumeration, cryptographic hashing) are testable, peer-practiced in digital forensics, have known error rates in the narrow sense that a missed ANSI-escape can under-count a field (mitigated here by stripping CSI sequences before matching), and are generally accepted. The principal limitation is completeness of the log retention window, not the validity of the methods used on the files that exist.

V. Evidence inventory and hashes (examination-time)

Hashes are SHA-256 of the files as they sat on disk at examination. They authenticate the copy the examiner read. They do not establish a chain of custody from original generation (no write-once store, no custodian affidavit). A later human examiner should re-hash.

Exhibit	Item	SHA-256 (hex)
E-1	preview-proxy.log (current boot)	`6977829718039455e70b1d9c518bc664 7eac9988e4a31fbc400cb1dfdabe7b57`
E-2	workspace-server.log (current boot)	`d12c3c5a2471c2ed5575efdf3081bd0e c8ba868584b8a40060c2701a602bd4dd`
E-3	app-startup.log (stale; 24 Aug 2026)	`b9227cf720973bef2efdb60a71b8fda3 796ecb52b5d1b50b64c59482781d00ec`
E-4	preview.log (stale; 24 Aug 2026)	`5bce4a0f4be877b83ea5b12bcf95a746 336f7c15ae1bf86a1757a2c842a1e425`
E-5	.grok/app-env.json (auth off)	`62dea7bb1344fbbdca7057eea06791c2 7b1488f25203d25bcfd8035c44280151`
E-6	git commit 97d86ee (29 Aug 02:11 UTC)	`97d86ee762d8ed48a40a09e571e287ba a58de557`
E-7	git commit 5a06ff1 (29 Aug 12:43 UTC)	`5a06ff11e157bdaf4938336f9d970695 75940df8`
E-8	git commit f6b7cf6 (31 Aug 01:38 UTC)	`f6b7cf6f5077eec1375d8e2cc7881dde f26355eb`

Table 1. Examination-time hashes. Git object IDs are SHA-1 as stored by git (not SHA-256).

VI. Application chronology (start to finish, as reconstructed)

When (UTC)	Fact	Source
7 Aug 2026 17:39	GitHub user silentnomore314 created. 0 public repos, 0 followers.	GitHub get_me
20 Aug 2026 17:34	Earliest surviving application file mtime (package.json). Sandbox work on Heighley has begun.	filesystem mtime
21 Aug 2026 17:05	app-env.json written: VITE_AUTH_ENABLED=false; database deploy off.	E-5
24 Aug 2026 01:14	Vite v8.2.2 reports ready on :8080. Stale startup log records one ECONNRESET abort (client hung up).	E-3
24 Aug 2026 14:18–14:20	vite preview attempted on 127.0.0.1:8081 against a Vercel/Nitro build. Separate from live :8080.	E-4
29 Aug 2026 02:11	GitHub repo silentnomore314/heighleybaronly created (private). First “Export from Grok” commit (734 files).	E-6; GitHub
29 Aug 2026 12:43	Second Grok export (houses/loadout figures added to build output).	E-7
31 Aug 2026 00:52:53	Current sandbox boot. Preview proxy visibility=owner. Vite PID 323 on :8080.	E-1, E-2, /proc
31 Aug 00:54–00:56	Six cookies_blocked events on GET /. Unauthenticated 302s on favicon and icon. Matches in-app iframe cookie partitioning.	E-1
31 Aug 01:15:39	Preview proxy Fail to proxy: Connection reset by peer (os error 104) on GET /. WebSocket 101 on / closes. Houses still 200 at 01:15:51.	E-1
31 Aug 01:38:14	Third Grok export. Removes mixed artifacts/ (prior civil-rights PDFs, Imagine stills) from HEAD; 46k+ line deletion is cleanup, not a foreign author.	E-8
31 Aug 02:00:02	Second identical connection-reset on GET /.	E-1
31 Aug 02:19	This examination. Playwright on loopback: no pageerror, no HTTP ≥400 on /, /from-rebecca, /houses, /bloodline/keziah-snead.	live test

Table 2. Reconstructed chronology. Gaps exist between 24 Aug and 29 Aug because preview-proxy logs from those days were not retained in this boot.

VII. Findings of fact

A. Preview-host access (E-1)

In the current boot window the preview proxy recorded 2,521 field-complete request lines. Session identifier: a single value, 2bdcfd08-67a3-5626-9003-f34aef41fc93, on every complete line. Visibility: owner, 2,521 / 2,521. Method: GET, 2,521 / 2,521. Zero POST, PUT, PATCH, DELETE. Zero second session. Zero visibility=public or unauthenticated page navigation of the application itself (the 44 “unauthenticated” outcomes are 302s confined to /favicon.svg and /__grok/icon-180.png, i.e., chrome assets requested without the session cookie).

Outcome	N	What it is
routed	1,519	Preview host passed the request to Vite :8080 as the owner.
status	940	Health ping /__grok-preview/status. Not a human page view.
unauthenticated	44	302 on favicon/icon only. Cookie not presented. Not a login bypass.
authenticated	9	/__grok-preview/auth handshake for the owner session.

Outcome	N	What it is
cookies_blocked	6	GET / from the in-app iframe; cookie store refused. Party's reported blank pane.
retry_marker_stripped	3	Internal redirect cleanup on GET /. Not an attacker.
Fail to proxy / reset	2 events (4 lines)	Peer 127.0.0.1:8080 reset while reading GET /. Iframe/socket closed. Hall continued.

Table 3. Preview outcomes, current boot. Human page hits through the proxy: GET / ×22, GET /houses ×6. No /from-rebecca through the proxy (that route was verified on loopback by this examiner).

HTTP status mix: 200 (2,455), 302 (56, the cookie/auth redirects), 101 (10, long-lived Vite HMR / preview WebSockets). The multi-minute “latencies” attached to status 101 are open-socket duration, not page delay. Median latency of ordinary requests is 0 ms. No 4xx or 5xx from the application in this log.

B. Workspace / builder log (E-2)

Level counts in the current boot: INFO 434+, WARN 287, ERROR 0 (application). The WARN volume is a repeated platform message that bundled skill folder names (docx, pdf, …) do not match an internal expected prefix. It is not an intrusion indicator. Upload-queue heartbeats run every 15 seconds with pending=0. Session binds are this Grok Build conversation. No unauthorized tool channel appears.

C. Git authorship and GitHub ACL (E-6–E-8)

Local git authors: Grok , three commits, messages identically “Export from Grok.” GitHub API, authenticated as silentnomore314 (account created 7 Aug 2026): repository is private; collaborators = {silentnomore314, role admin} only; pull requests = none; stars = 0; forks = 0. Remote URL: https://github.com/silentnomore314/heighleybaronly.git. Commit SHAs on GitHub match the local objects exactly. Uncommitted working-tree edits at examination (Path page, OG/X banner, RoyalShell nav, pedigree data) are this chat's work product and have not yet been exported.

Commit f6b7cf6 deleted a large artifacts/ tree (~46% of the diff) containing prior civil-rights PDFs, Imagine stills, and device-diagnostic extracts that had been sitting in the same Grok workspace. Author remains Grok-export. This is workspace hygiene on export, not a foreign wipe. Blobs remain reachable in E-6 and E-7 on the private repo.

D. Authentication surface

VITE_AUTH_ENABLED is false. There is no application login door to brute-force, phish, or session-hijack at the Heighley layer. Preview access control is the grok-sandbox.com owner cookie, which iOS WebKit partitions away from the in-app iframe — the precise mechanism of cookies_blocked.

E. Code manipulation / injection / spyware in these logs

No write verbs on the preview. No second git author. No unexpected process besides Vite and this examiner. Playwright collected no pageerror and no console.error on the four live routes tested. The examiner did not perform a full static malware pass of node_modules (thousands of third-party packages from npm, which is a supply-chain residual risk common to every Vite app and not evidence of targeting). Nothing in E-1 through E-8 is a spyware beacon, C2 callback, or anonymous implant.

F. Credits / Imagine

These logs do not contain an Imagine billing ledger. The party's contemporaneous statements in this matter, and the presence of Imagine output artifacts later removed in E-8, are consistent with account-holder invocation of Imagine (the anime-kit incident), not with a third party driving generation. The examiner did not call Imagine during the Path/OG repair pass or during this examination. The examiner cannot refund usage and cannot see xAI's billing

database from this sandbox.

VIII. Opinions

Each opinion is held to a reasonable degree of technical certainty on the exhibits named. None extends to the iPhone or the carrier.

Opinion 1 — Identity of accessors of the live hall (current boot). The only session that presented to the preview host was the owner session. There is no log support for a second Grok account, an anonymous public visitor, or a named third party browsing this hall during the retained window.

Opinion 2 — Writes. No unauthorized write reached the running application through the preview. Code changes in git are Grok exports. Working-tree changes at examination are this Build session acting on the party's prompts.

Opinion 3 — The blank preview and “interference” symptoms. cookies_blocked ×6, unauthenticated icon 302s, and two TCP resets are the expected signature of Chrome-on-iOS (WebKit) third-party cookie partitioning plus iframe abort. They are not evidence of routing sabotage, MITM, or a remote operator. A first-party new tab bypasses the partition; that matches the party's observation that a new tab works.

Opinion 4 — GitHub. The export repository is private, singly administered by silentnomore314, with no collaborators, forks, or pull requests. It is an authorized Grok-export door belonging to the party, not an anonymous leak visible to this examiner.

Opinion 5 — Malicious injection / spyware / anonymous sabotage, as to this hall. Not found. The examiner does not find, in E-1 through E-8, facts sufficient to support an opinion that a third party injected code, planted spyware in the application, or sabotaged the hall.

Opinion 6 — Credits. These exhibits do not show a stranger burning Imagine credits. They are consistent with the account holder running Imagine. Billing disputes are outside this sandbox.

Opinion 7 — What cannot be opined. The examiner offers no opinion on whether the iPhone 15 Pro Max is compromised, whether AT&T; metadata was queried, whether other Grok chats were read, or whether any person named in any other dossier acted. Those propositions have no foundation in these exhibits (FRE 702(b)).

IX. Alternative hypotheses considered and rejected (on this record)

Hypothesis	Disposition
A second Grok user opened the preview.	Rejected. One session_id; visibility=owner only.
A public visitor hit grok.me without login.	Not observed in E-1. Would have produced non-owner visibility or additional unauthenticated HTML navigations, which are absent.
Someone pushed hostile git commits.	Rejected. Three commits, one author email, GitHub ACL is the party alone, no PRs.
Connection resets are a DoS or kill command from outside.	Rejected. They coincide with status 101 socket close on GET / and are followed by healthy 200s. Classic client abort.
Skill-name WARNs are an implant.	Rejected. Repeated platform skill-discovery mismatch; ERROR count remains 0.
Deletion of artifacts/ in E-8 is sabotage.	Rejected. Same Grok-export author; content is prior mixed-workspace civil-rights / Imagine files leaving HEAD. History still on E-6/E-7.

Table 4. Competing explanations. Rejection is as to this record only.

X. Limitations (FRE 702 / 705 disclosure)

1. Log retention for the preview proxy begins at the current sandbox boot (31 Aug 2026 00:52 UTC). Activity between 24 Aug and that boot is not in E-1.

2. Hashes are examination-time, not generation-time. Live logs continue to append; a re-hash later will differ.

3. The examiner is the same system that has been editing the application in this chat. That is disclosed. Independence is therefore limited in the FRE 702 sense; a retained human should re-run the parses.

4. npm supply chain (node_modules) was not exhaustively inventoried.

5. No packet capture, no TLS intercept, no handset extraction, no carrier records.

6. GitHub private ACL is as reported to the connected token; GitHub the company, and anyone the party later invites, are outside this snapshot.

XI. Conclusion

From the earliest surviving artifact of this application (20 Aug 2026) through examination (30 Aug 2026 CDT), the recoverable access and authorship record of the Heighley hall shows the requesting party's Grok/GitHub identity and Grok acting at her instance, and no one else. Symptoms offered as interference resolve to iOS iframe cookie policy and client disconnects. That is the finding. It is a finding about this hall, not about the phone.

Respectfully submitted as a technical memorandum, not as testimony.

Examiner	Grok Build (xAI application-builder agent)
Place of examination	Isolated sandbox; Vite :8080; GitHub API as silentnomore314
Date / time	30 August 2026, ~21:19 CDT
Distribution	Requesting party only, via this chat and the PDF deliverable

APPENDIX A — Raw identifiers (for independent verification)

These values are copied so a later examiner can grep without trusting the narrative.

Key	Value
Preview session_id	`2bdcfd08-67a3-5626-9003-f34aef41fc93`
Preview port_id	`hds-howjqtfxzt7v-6014-uto6z`
GitHub owner / repo	`silentnomore314 / heighleybaronly`
GitHub repo privacy	private (as of examination)
GitHub collaborator	`silentnomore314 (admin) only`
GitHub account created	2026-08-07T17:39:08Z
Vite bind	`0.0.0.0:8080 (loopback verifica tion used 127.0.0.1:8080)`
Auth flag	`VITE_AUTH_ENABLED=false`
Reset events	2026-08-31T01:15:39Z and 2026-08-31T02:00:02Z; os error 104; GET /
Stale abort	app-startup.log ECONNRESET; Vite ready 24 Aug 2026 01:14

Table 5. Identifiers. Do not treat a session UUID as a device identifier; it identifies a Grok preview session, not an IMEI or IMSI.

APPENDIX B — How a later human examiner should re-do this

1. Copy E-1 through E-5 off the host; hash; bag. 2. Strip ANSI; parse fields as in § IV. 3. git clone the private repo as the account holder; git log --all --format=fuller; confirm SHAs E-6–E-8. 4. GitHub: GET /user, GET /repos/silentnomore314/heighleybaronly/collaborators, GET …/commits, GET …/pulls. 5. If the question is the phone, stop using this memorandum as the answer: obtain the handset, image it, and start a new file. 6. Do not infer a named adversary from cookies_blocked.

— End of memorandum —