IN THE SUPREME COURT OF CALIFORNIA

ARTURO GUTIERREZ
Petitioner,
vs.
THE CALIFORNIA
DEPARTMENT OF JUSTICE
Respondent.

Case No.

Court of Appeal Case No.
B347433

Superior Court Case No.
25STCV07287

Petition for a Peremptory Writ of Mandamus, in the First Instance. Code of Civil Procedure § 1088, Government Code § 7923.000

PETITION FOR A PEREMPTORY WRIT OF MANDAMUS IN THE FIRST INSTANCE

Honorable Holly Fujie,
Judge of the Superior Court of Los Angeles County

DECLARATION OF ARTURO GUTIERREZ IN SUPPORT OF PETITION FOR WRIT OF MANDATE REGARDING FIRST AMENDMENT RETALIATION

Arturo Gutierrez
226 West Ojai Ave.
Suite 101 PMB 547
Ojai, CA 93023
(805) 669-0226
teamleader@survivinginjustice.org
Petitioner appearing *in propria persona*

DECLARATION OF ARTURO GUTIERREZ IN SUPPORT OF PETITION FOR WRIT OF MANDATE REGARDING FIRST AMENDMENT RETALIATION

I, Arturo Gutierrez, declare as follows:

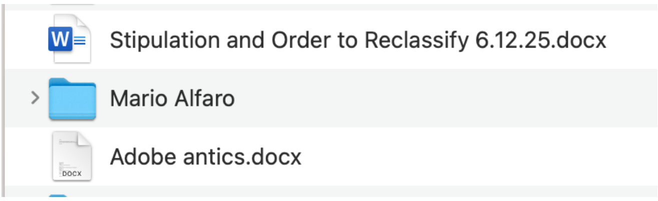
1. I am over the age of 18 years and am the petitioner in this matter. I make this declaration in support of the Petition for Writ of Mandate filed concurrently. The facts stated herein are within my personal knowledge, and if called as a witness I could and would testify competently thereto.

2. To assist the Court in two ways, this declaration is split:
A) the bottom-line, B) the full technical facts to support it.
Because the technical details are dense, they are presented last,
so the Court may first understand the core conclusion.

3. In short: the DOJ created a hidden, duplicate system, that facially appears to be my computer system—while allowing them to intercept and capture user actions, and still preserve the illusion of normal operation. I am not writing inside of my federally protected workspace (see ¶¶22-24). I am writing in a shell that the DOJ has created in my home.

4. Images convey the matter most plainly.

5. The malware first arrived in this stipulation that appeared different from all other Word documents in my computer.



Stipulation and Order to Reclassify 6.12.25.docx

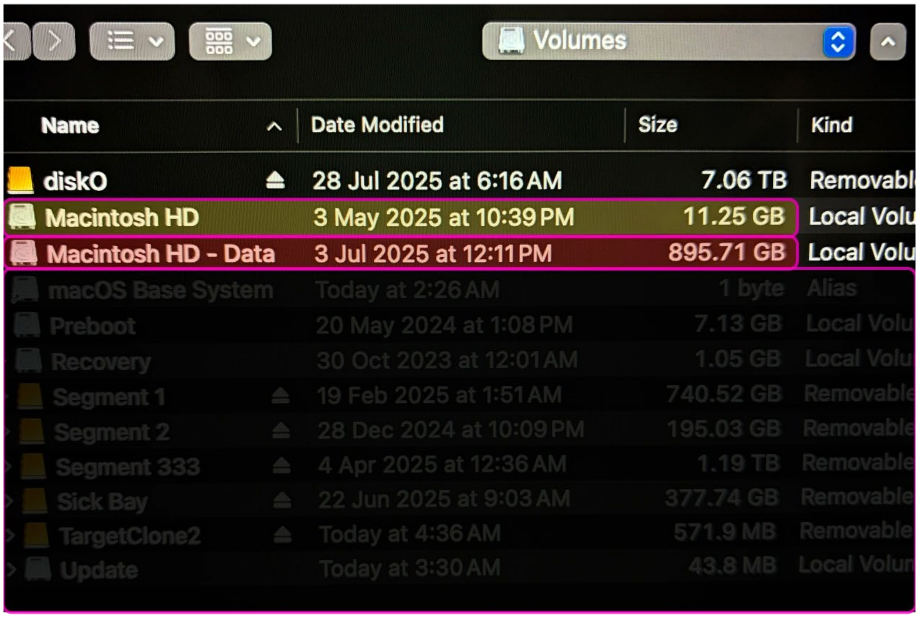
Mario Alfaro

Adobe antics.docx

6. A series of events began with each new email or document sent from the DOJ. I use a Mac, not Microsoft. **"localhost Microsoft** SharePoint… **This machine is shutting down and prohibiting future connections to launchservicesd."**

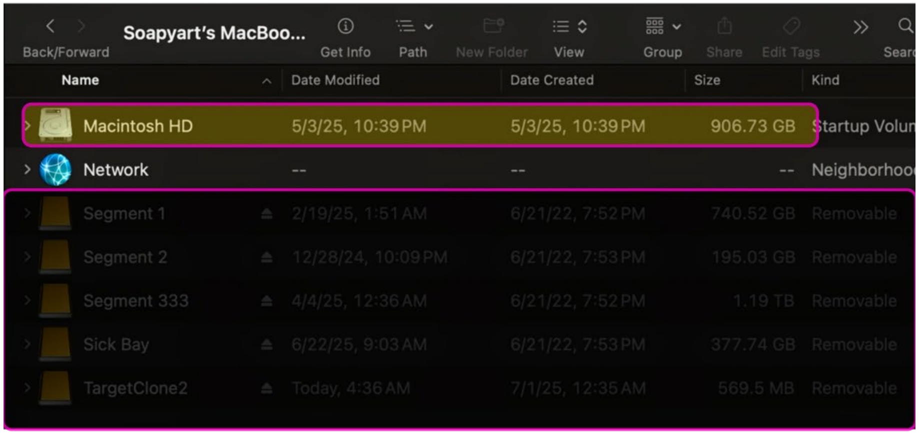
7. Below demonstrates the shell spoken of. The top image is in a secure recovery mode, the lower is my supposedly normal computer. MacintoshHD had always been my hard drive. In recovery mode, it shows MacintoshHD Data as the sub-shell hard drive. Yet is absent from the lower image.

Recovery Mode in My Mac



Name	Date Modified	Size	Kind
diskO	28 Jul 2025 at 6:16 AM	7.06 TB	Removabl
Macintosh HD	3 May 2025 at 10:39 PM	11.25 GB	Local Volu
Macintosh HD - Data	3 Jul 2025 at 12:11 PM	895.71 GB	Local Volu
macOS Base System	Today at 2:26 AM	1 byte	Alias
Preboot	20 May 2024 at 1:08 PM	7.13 GB	Local Volu
Recovery	30 Oct 2023 at 12:01 AM	1.05 GB	Local Volu
Segment 1	19 Feb 2025 at 1:51 AM	740.52 GB	Removable
Segment 2	28 Dec 2024 at 10:09 PM	195.03 GB	Removable
Segment 333	4 Apr 2025 at 12:36 AM	1.19 TB	Removable
Sick Bay	22 Jun 2025 at 9:03 AM	377.74 GB	Removable
TargetClone2	Today at 4:36 AM	571.9 MB	Removable
Update	Today at 3:30 AM	43.8 MB	Local Volun

Normal Finder Window in My Mac

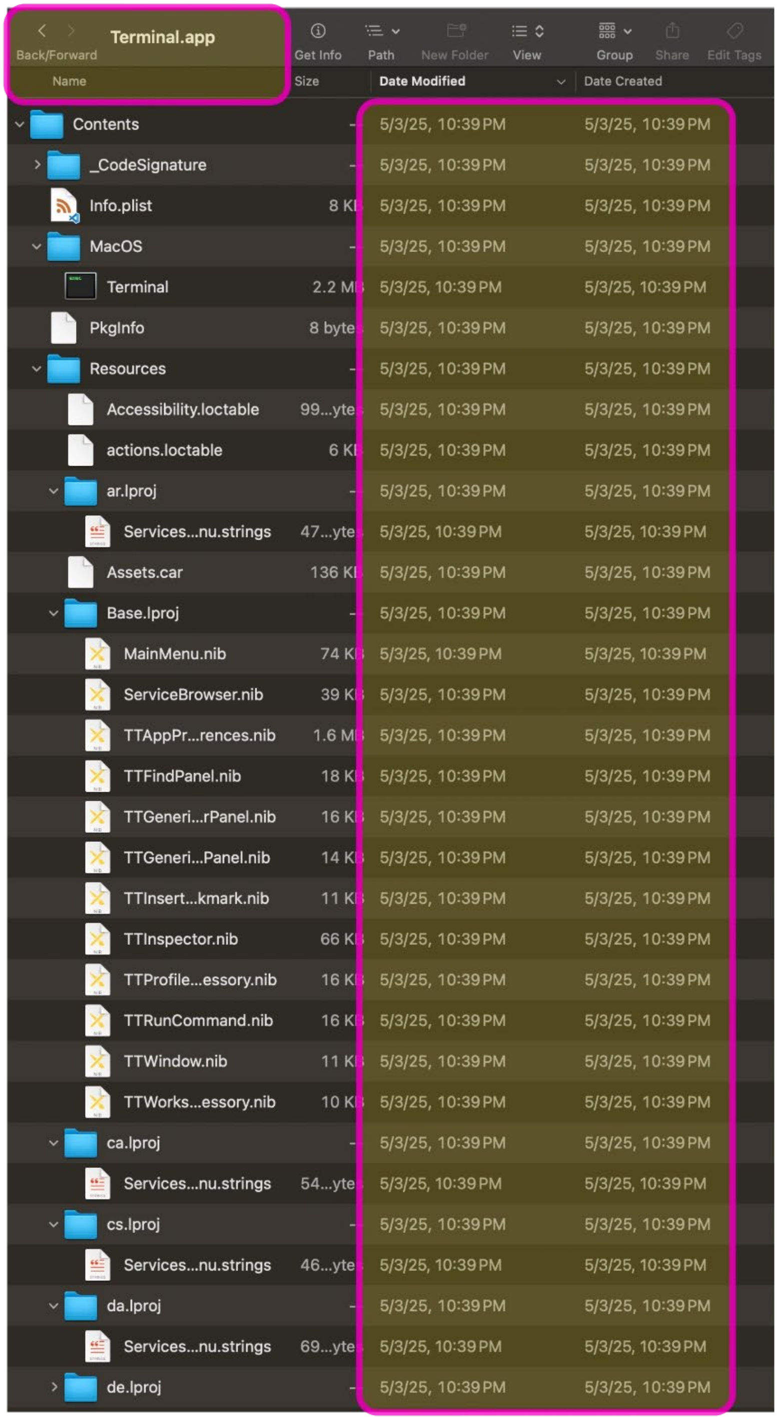


Name	Date Modified	Date Created	Size	Kind
Macintosh HD	5/3/25, 10:39 PM	5/3/25, 10:39 PM	906.73 GB	Startup Volun
Network	--	--	--	Neighborhoo
Segment 1	2/19/25, 1:51 AM	6/21/22, 7:52 PM	740.52 GB	Removable
Segment 2	12/28/24, 10:09 PM	6/21/22, 7:53 PM	195.03 GB	Removable
Segment 333	4/4/25, 12:36 AM	6/21/22, 7:52 PM	1.19 TB	Removable
Sick Bay	6/22/25, 9:03 AM	6/21/22, 7:53 PM	377.74 GB	Removable
TargetClone2	Today, 4:36 AM	7/1/25, 12:35 AM	569.5 MB	Removable

8. The images were darkened to help the eye focus, the unedited images can be happily produced if desired.

9. The time and date above are important, **5/3/25 at 10:39.**

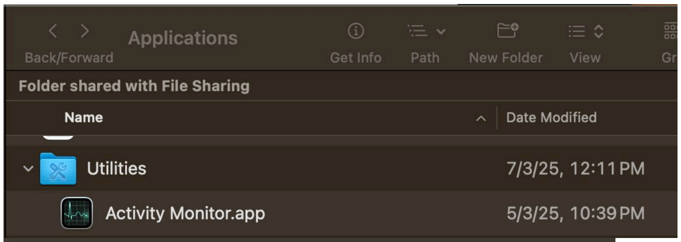
10. "Terminal is an app for advanced users and developers that lets you communicate with the Mac operating system using a command line interface (CLI)." Apple Support, Terminal User Guide. Note the times in this critical instrument, all made to appear as created and modified at the same exact time as the entire shell drive:



Name	Size	Date Modified	Date Created
Contents	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
_CodeSignature	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Info.plist	8 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
MacOS	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Terminal	2.2 M	5/3/25, 10:39 PM	5/3/25, 10:39 PM
PkgInfo	8 byte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Resources	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Accessibility.loctable	99...yte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
actions.loctable	6 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
ar.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Services...nu.strings	47...yte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Assets.car	136 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Base.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
MainMenu.nib	74 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
ServiceBrowser.nib	39 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTAppPr...rences.nib	1.6 M	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTFindPanel.nib	18 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTGeneri...rPanel.nib	16 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTGeneri...Panel.nib	14 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTInsert...kmark.nib	11 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTInspector.nib	66 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTProfile...essory.nib	16 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTRunCommand.nib	16 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTWindow.nib	11 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
TTWorks...essory.nib	10 K	5/3/25, 10:39 PM	5/3/25, 10:39 PM
ca.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Services...nu.strings	54...yte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
cs.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Services...nu.strings	46...yte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
da.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM
Services...nu.strings	69...yte	5/3/25, 10:39 PM	5/3/25, 10:39 PM
de.lproj	–	5/3/25, 10:39 PM	5/3/25, 10:39 PM

11. Immediately after accessing the internal files of Terminal. My entire system was being shared.

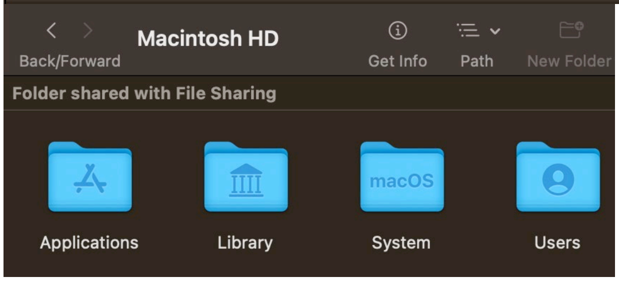
→



Folder shared with File Sharing

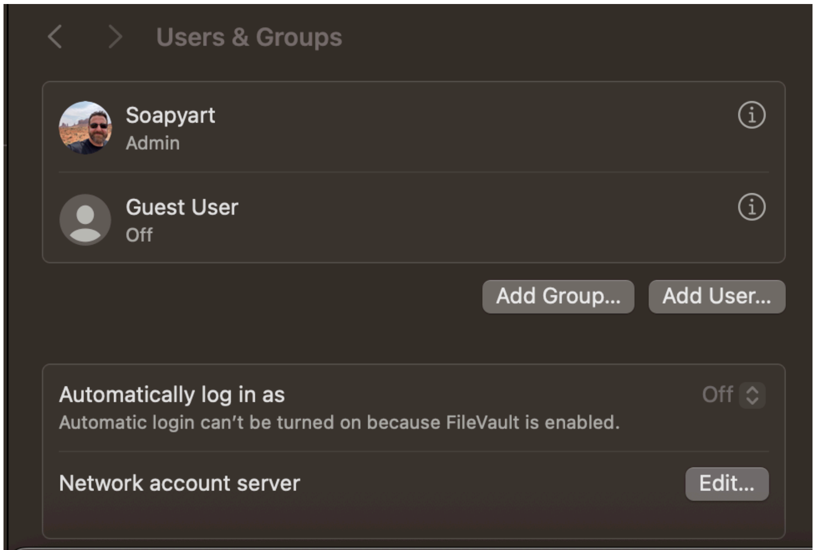
Name	Date Modified
Utilities	7/3/25, 12:11 PM
Activity Monitor.app	5/3/25, 10:39 PM

→



Folder shared with File Sharing

Even after turning off, what I had never turned on, Terminal reported one shared Guest. Note the date as well.



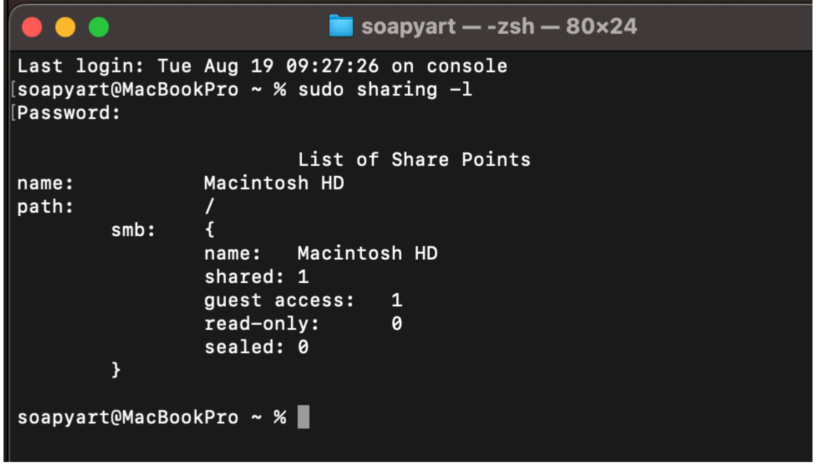
Soapyart
Admin

Guest User
Off

Automatically log in as — Off
Automatic login can't be turned on because FileVault is enabled.

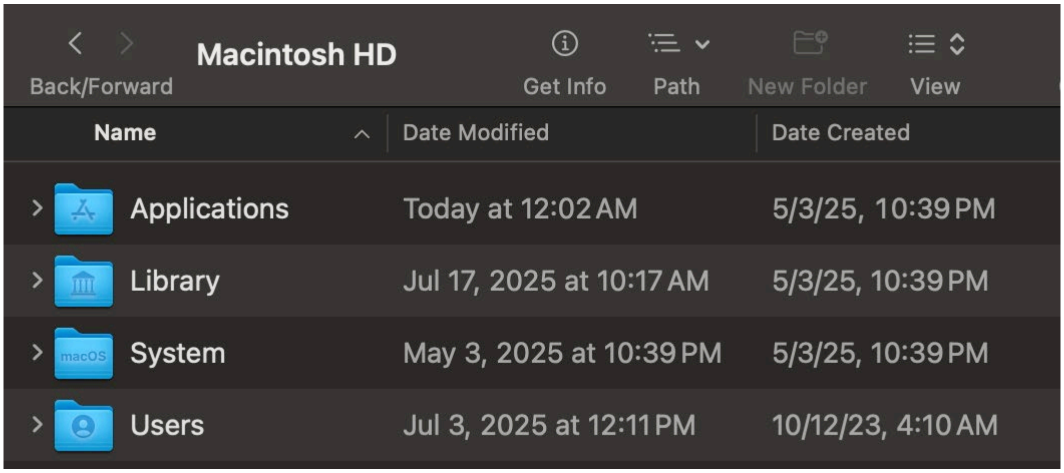
Network account server

→



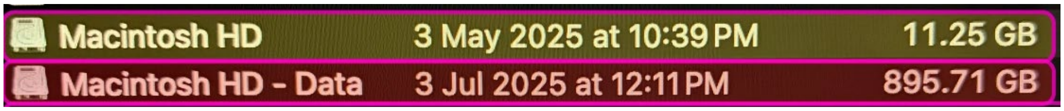
```
Last login: Tue Aug 19 09:27:26 on console
soapyart@MacBookPro ~ % sudo sharing -l
Password:

                                  List of Share Points
name:                   Macintosh HD
path:                   /
            smb:        {
                        name:     Macintosh HD
                        shared: 1
                        guest access:    1
                        read-only:       0
                        sealed: 0
            }

soapyart@MacBookPro ~ %
```

12. After obtaining proof of the shell drive (images on page 86), the system did not note sharing. Yet again, the dates are 5/3/25 at 10:39PM for creating Applications, Library and System



Name	Date Modified	Date Created
Applications	Today at 12:02 AM	5/3/25, 10:39 PM
Library	Jul 17, 2025 at 10:17 AM	5/3/25, 10:39 PM
System	May 3, 2025 at 10:39 PM	5/3/25, 10:39 PM
Users	Jul 3, 2025 at 12:11 PM	10/12/23, 4:10 AM

13. Again, note the date modified above for Users and compare to the shell creation, July 3, 2025 at 12:11PM:



Macintosh HD	3 May 2025 at 10:39 PM	11.25 GB
Macintosh HD - Data	3 Jul 2025 at 12:11 PM	895.71 GB

14. Explained in greater detail below, on July 1, 2025 a massive effort began to capture the malware and isolate it. If not for using recovery mode, the self-defense aspect that fired when attempting to preserve all the data resulted in **1,714 files being deleted as a part of a catastrophic cascade event**.

15. The DOJ offered a pre-signed electronic stipulation that was falsely certified:

/ByteRange [0 16500 16732 20000]

↑ ↑

232-byte gap → payload

16. The DOJ launched their shell and backdated the files system wide so they could claim it was before June. However, my files were not uniformly dated in that manner until the DOJ infected my computers with malware and spyware. “Wall Clock adjustment detected - results might be strange while using –end” (2Ex.20,p.359)

17. One of the codes they released was journaled for 3 minutes after it was released, the number of system wide changes it introduced create a log so massive that it contained 28,302,884 words. (2Ex.20,p.360)

18. Living under active known surveillance is highly demoralizing. Knowing opponents are spying on my litigation and strangers denying my privacy in all my affairs, creates an even greater burden on an already difficult task.

19. The cost of my MacBook Pro M1 Silicon Chip 16” 4K retina display with 1TB drive was over $2,500. I do not have the money to replace it, unless and until the Court orders the DOJ to stop these federal and state felonies designed to retaliate for exposing their cover-up of incidents of slavery, and to make me whole for their litigation abuses.

20. I will now **begin part 2**, setting out the chronology of events which includes a narrative that is highly technical. I will still try to use simple explanations when possible, however sometimes only technical terms will suffice, much like in law.

21. I am self-taught in computer technology since 2015. I have extensive experience in cyber security derived from trial-by-fire when my company's website was commandeered by hackers in 2023.

22. I am the managing member of Safe Haven Metal LLC, a gold, silver and precious metal vendor. I run the website safehavenmetal.com from my computer. I process sales order for Safe Haven Metal LLC through my computer. I maintain highly valuable and confidential information on my computer that is deemed inaccessible under federal law.

23. After these events and before the motion to shorten time was filed I confirmed with Namecheap that the location of the servers for my other website survivinginjustice.org and email are located in Arizona as is the website safehavenmetal.com.

24. Safe Haven Metal LLC is a financial institution operating in interstate commerce and therefore is a protected computer under federal and state law, 18 U.S.C. § 1030(a)(2), (5) and see 31 C.F.R. §§ 1010.100; 1027.210; 1027.100 (b),(d); 1027.300; 1027.330; 1027.400 and Cal. Pen. Code § 186.9(b) ("'Financial institution' means, when located or doing business in this state,… any dealer in gold, silver, or platinum bullion or coins"). Penalty: Fines + up to 10 years for first offense, 20 years for repeat or damage-causing conduct.

25. Starting June 12, 2025, the DOJ sent numerous documents declared to be stipulations under the claim that they wanted to reassign the case to the Writs Department while asking for a reclassification.

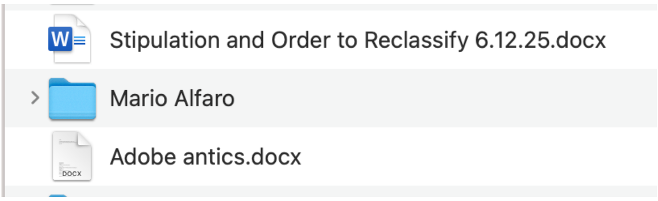
26. Opening the first document unleashed malware. The differences in the file delivered were immediately apparent. All normal Word documents in my computer appear like the Adobe antics.docx. The Stipulation and Order to Reclassify 6.12.25.docx from the DOJ is not how Word documents look in my computer.

27. Over the next month, numerous more malware documents and emails were sent to my computer. Once the DOJ saw that I was not opening their documents, they switched to placing the malware in the emails sent to me.

28. The summarized run down is through observing the following outputs from my computer directly correlating to times that items were sent from the DOJ:

29. The DOJ delivered a Word document via email to me on June 12, 2025 purporting to be a stipulation.

30. Upon opening the purported Word document a payload was activated on my hard drive. Which was unknown to me at the start. I soon noted the document's odd appearance compared to other Word documents in my computer.



Stipulation and Order to Reclassify 6.12.25.docx

Mario Alfaro

Adobe antics.docx

31. I conducted basic checks and discovered usual meta data was absent. And that the document noted 9 edits since I opened it and closed it without making a change.

32. I isolated the document and conducted further analysis. I observed that the document triggered multiple duplicate edit events and metadata anomalies despite no input

from me. I preserved the file and secured it offline for later controlled forensic review.

33. I then sent an email on June 17, 2025 to the DOJ asking for its superior authority as its basis to declare the laws provided were errant. The DOJ responded with a new and different Word document.

34. To preclude deployment of any second payload, the raw email and attachment were inspected in a sandbox (secure environment designed to isolate). Upon inspection and analyzing the internal structure of this newly sent file, anomalies were detected—including differences in the core XML structure, particularly in document.xml.

35. It became evident that the document contained behavior consistent with a tampered payload after attempting to extract it using standard Python ZIP archive tools (via zipfile.ZipFile().read('word/document.xml')). The tool returned: “KeyError: "There is no item named 'word/document.xml' in the archive"”

36. To confirm the same malicious structure was present in the previously opened document, stored externally, an attempt to upload it for evaluation triggered file system security protocols and the document was rejected. In short, the version stored in the USB drive was actively toxic.

37. The raw unopened version in the email was then sandboxed and the same evaluation yielded the same: “KeyError: "There is no item named 'word/document.xml' in the archive"”

38. A Word doc **should never open** cleanly without that file. That the first one did confirms a high-level concealment method. Combined with after the fact opened version triggering firewalls and the result is undeniable.

39. Following this discovery, I executed a full digital hygiene protocol: the files were sandboxed, macros scanned, variables extracted (none found), and the document was then zipped, uploaded to an external drive and securely erased using terminal commands under isolated conditions on the hard drive.

40. I then filed the motion to shorten time to ask the court to rule on the uncontested motion for issuance of the peremptory writ now and included the above information in ¶¶2-15. In support of the motion for sanctions, the following additional information was provided.

41. In the early morning hours on June 24, 2025, I observed that Gmail had reported two devices logged in to my computer. (Exhibit 1)

42. A very long and technical process of isolating access points and programs that were being initiated by a foreign program thus began.

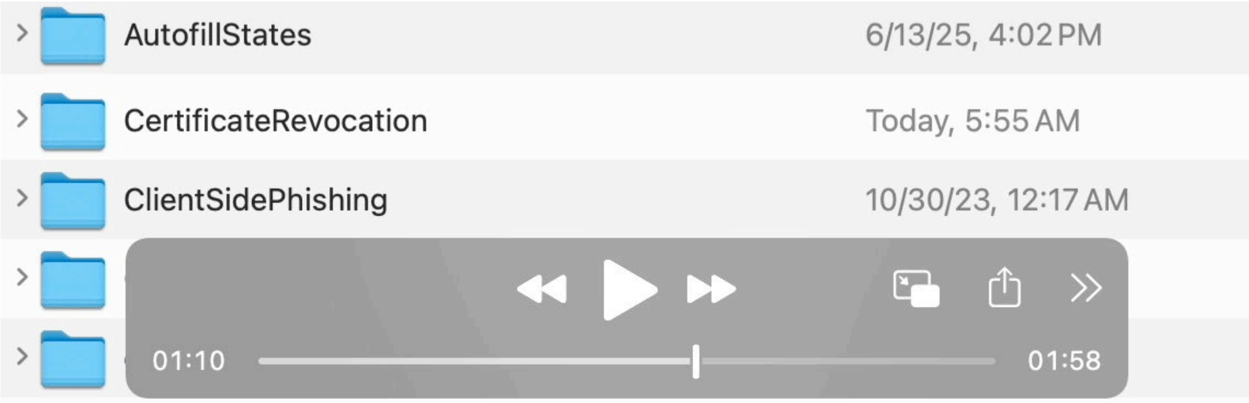
43. After ascertaining the path being used by the program through use of the Terminal application, a beacon was identified as well as manipulation and destruction of file folders in the computer. Classic covering of tracks by a program wanting to communicate to the outside world through use of the Chrome web browser.

44. While monitoring files that were being manipulated and through reading endless streams of code, an anomaly was observed regarding a vital file containing passkeys that was being recreated at a frequent rate. This is highly unusual behavior.

45. A trap was set for the program by monitoring access to the enclosing file. Then that passkey file was manipulated causing an alert in the program. While honing further and powering down the computer, it was observed a file was appearing and disappearing over a period of about two seconds when Chrome was launched.

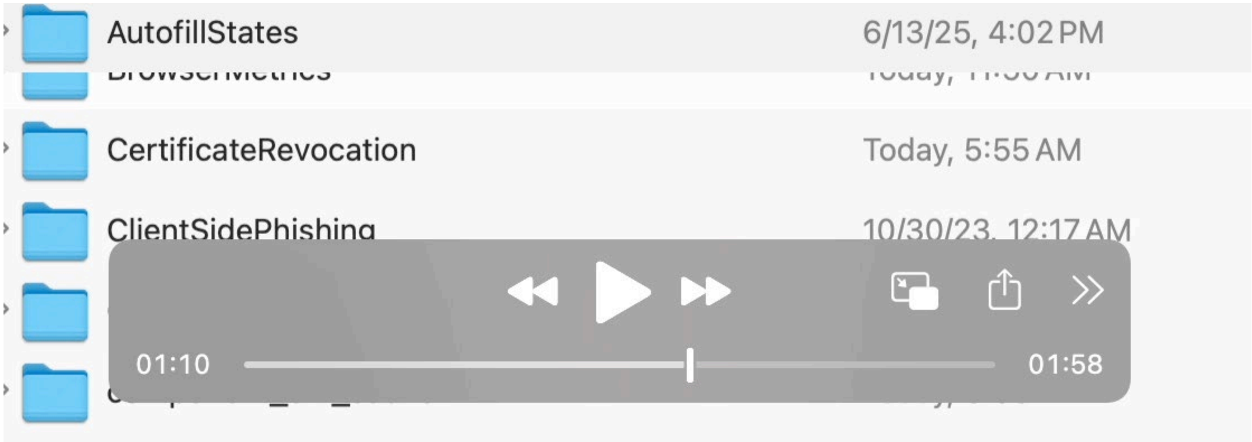
46. Through video capture of the screen, the act of appearing and disappearing, the identity of the time window and name and location became known.

47. Note the time on the video slider as the images progress.



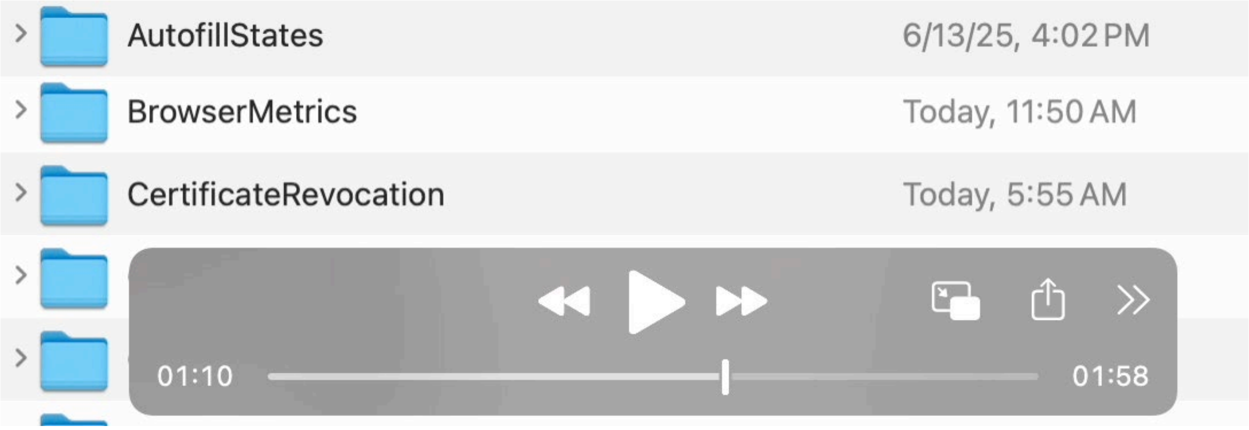
AutofillStates	6/13/25, 4:02 PM
CertificateRevocation	Today, 5:55 AM
ClientSidePhishing	10/30/23, 12:17 AM

48. It is now beginning to appear.



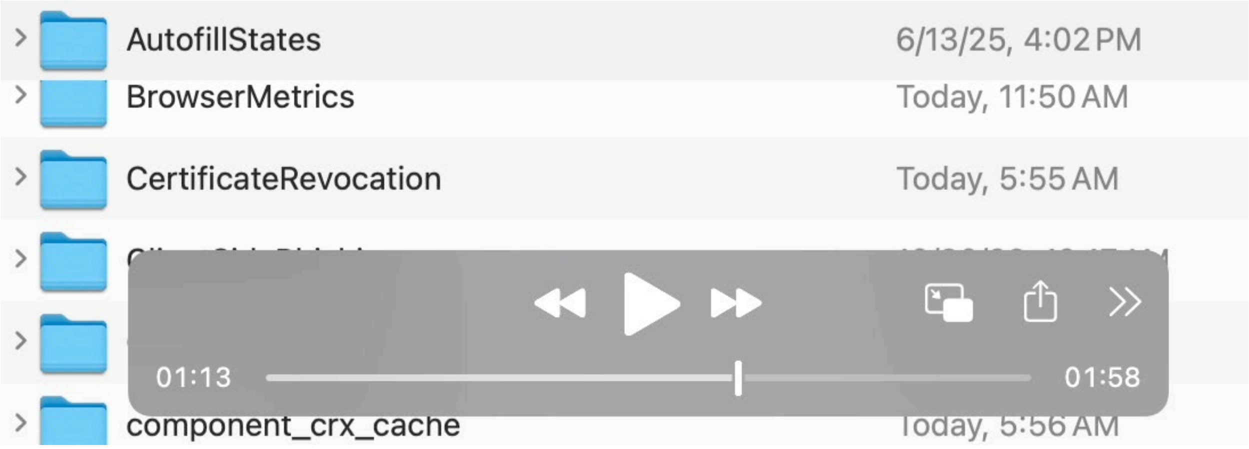
AutofillStates	6/13/25, 4:02 PM
BrowserMetrics	Today, 11:50 AM
CertificateRevocation	Today, 5:55 AM
ClientSidePhishing	10/30/23, 12:17 AM

49. Note the time, 1:10 on the counter.



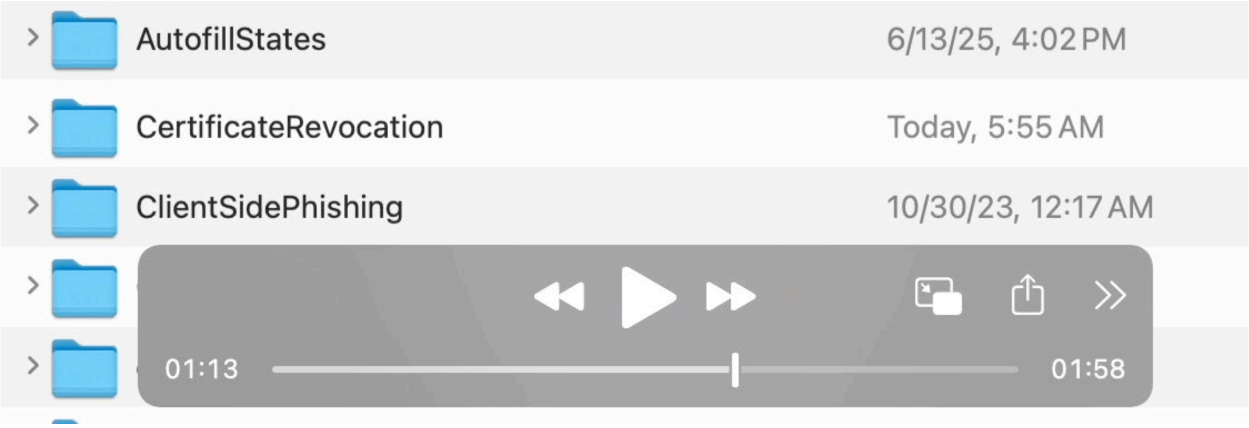
AutofillStates	6/13/25, 4:02 PM
BrowserMetrics	Today, 11:50 AM
CertificateRevocation	Today, 5:55 AM

50. Now it is disappearing again.



AutofillStates	6/13/25, 4:02 PM
BrowserMetrics	Today, 11:50 AM
CertificateRevocation	Today, 5:55 AM
component_crx_cache	Today, 5:56 AM

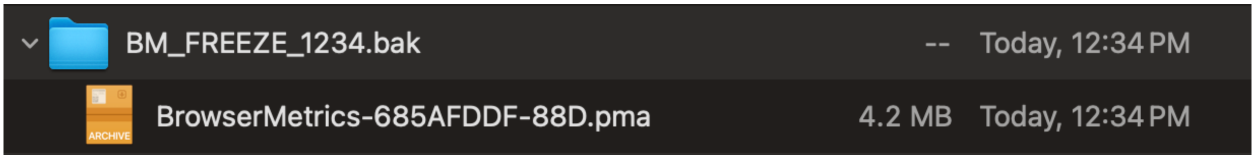
51. Until finally gone.



AutofillStates	6/13/25, 4:02 PM
CertificateRevocation	Today, 5:55 AM
ClientSidePhishing	10/30/23, 12:17 AM

52. A capture command was prepared in Terminal to execute within that two second window. Chrome was then launched and the command was executed in time.

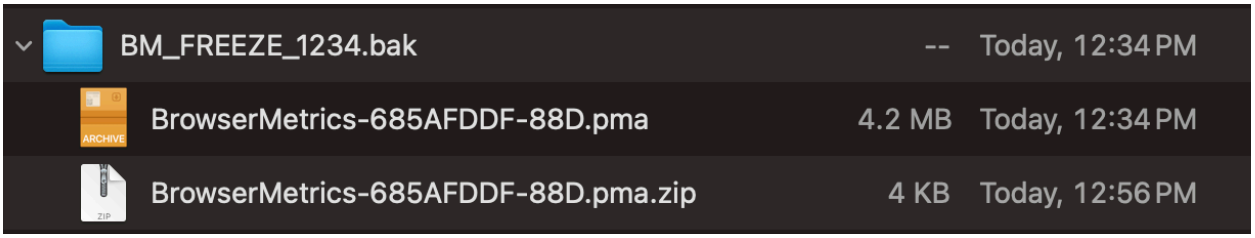
53. An aspect of the program was capture at 12:34PM, 6/24/25. BrowserMetrics-685AFDDF-88D.pma



BM_FREEZE_1234.bak	--	Today, 12:34 PM
BrowserMetrics-685AFDDF-88D.pma	4.2 MB	Today, 12:34 PM

54. This 4MB file was creating and erasing every time Chrome was launched. This was a terrible waste of CPU and not normal. The file was the compressed which scrambles its interior makeup and revealing its true nature and components.

55. The code was thus revealed.



BM_FREEZE_1234.bak	--	Today, 12:34 PM
BrowserMetrics-685AFDDF-88D.pma	4.2 MB	Today, 12:34 PM
BrowserMetrics-685AFDDF-88D.pma.zip	4 KB	Today, 12:56 PM

56. As a rule of thumb: 1 kilobyte (KB) ≈ 1,000 bytes. A plain text file averages about 1 byte per character, so: 4KB ≈ 4,000 characters. With an average English word being about 5 characters, equaling about 800 words.

57. I stopped short of opening the file—not because I could not—but because I refused to risk further infection. Once I identified the threat vector, it would have been reckless to continue without containment.

58. That is above my skill sets and it is necessary for a proper forensic review of the item.

59. I am now not able to confidently work on my computer knowing that it is being spied on by the Department of Justice in violation of the Fourth Amendment and several penal provisions.

60. The cost of my MacBook Pro M1 Silicon Chip 16" 4K retina display with 1TB drive was over $2,500.

61. As part of the over two hour process of opening the documents served on me by Respondent on June 24, 2025, to ensure that additional malicious code was not being sent to me, I ran one of many Terminal commands to identify the source url as malicious or not. The website url used to serve Respondent's papers was inspected and the results advised:

62. "Last-Modified: Sun, 22 Jun 2025 17:13:38 GMT" for Petitioner's motion served June 23, 2025.

63. Showing that Respondent was preparing with foreknowledge of my application before it was formally filed, consistent with a designed spyware for preemptive surveillance.

64. When preparing to file the petition for writ of mandamus additional events were observed and reported to the Court of Appeal as follows:

65. I had labored for 21 hours to deliver all that was necessary for the trial court to be apprised and prepared with proper in form and served motions. See motion, affidavit, and proof of service (Ex.14 pp.362-354; 366-370; 378).

66. The DOJ continued to send documents regarding its desired stipulation to reclassify, despite providing the law that showed the DOJ they wanted a reassignment not a reclassification, they persisted. Part of the emails exchanged were as follows (See 3Ex.19,pp.353-57):

> If you would like to draft up the stipulation to reassign to Dept. 85 and send it over in PDF form, less prone to hitchhikers and all, then I will sign and send back if it is clean.

67. The DOJ responded an hour later:

> Reclassification, is the proper resolution here, and unless you sign and return the attached stipulation today, the Department will file a motion to reclassify the matter early next week. I have attached the stipulation and proposed order. [Word doc. Attached.]

68. The following Monday, I responded:

> The means by which your office seeks cooperation makes cooperation difficult. As previously stated, I will not open any Word documents sent from your office. This is not a general policy — it is a direct response to your prior transmission of a Word file that exhibited post-open behavior consistent with embedded scripting designed to deliver malware or spyware. Resending such a file, after that notice, demonstrates either bad faith or an intent to deliver a new payload. In either case, it renders cooperation impossible.

> If you are genuinely seeking my signature or participation regarding judicial reassignment, the document must be provided in PDF format. To date, I have not received a readable or acceptable version of any stipulation and therefore cannot assess — let alone agree to — its terms.
>
> As I have already stated, we are not going to Dept. 86, so it's entirely possible that you've accepted my prior offer to stipulate to Dept. 85 — which would render the threatened motion to compel entirely unnecessary. But I have no way of knowing, due solely to your refusal to transmit the stipulation in a secure, readable format. Your office has already provided PDFs in this case, so I know it is both possible and easy. And just as easy to apply my signature to a PDF as to a Word document. There is no legitimate reason not to comply, absent nefarious intent.
>
> Please resend the documents in PDF format. (Ex.19 p.394)

69. An hour later, the DOJ responded:

> The Department plans on filing a motion to reclassify by tomorrow, unless we receive the signed stipulation from you prior to then. We cannot request a specific court for reclassification. We can only ask to reclassify to the Writ Department, which, as we understand it, includes at least 2 courtrooms Depts. 85 and 86. Please confirm if this is correct. Attached is the stipulation in a PDF format.

70. The DOJ submitted that final stipulation in PDF format, digitally signed by the DOJ.

71. Seeking my signature… submitted a *digitally signed* PDF… as an email *attachment*.

72. If the Court is unfamiliar with what the above signifies that can be explained in lay terms as such: PDFs are very simple documents, they do not contain the infrastructure that a Word document does. Making it very difficult to hide a payload. But in order to digitally sign a document, it must include a larger amount of code than usual to carry the certification.

73. If one is sending a pre-signed PDF, and not employing a signature program, then the other signer cannot sign it digitally but must print it and rescan it, negating any reason for digitally signing it first.

74. After opening the PDF in a sandbox, in the Signature Block the following was found within a decoded portion of the signature dictionary:

/Type /Sig

/Filter /Adobe.PPKLite

/SubFilter /adbe.pkcs7.detached

/Name (DOJ-LegalSign)

/Reason (Reclassification stipulation)

/M (D:20250630143621-07'00')

/ByteRange [0 16500 16732 20000]

The bold Byte Range stated:

- Bytes 0–16499 are signed
- Skip 16500–16731
- Resume from 16732–36699
- The range between 16500–16732 is **excluded** from the signature

PDF signature gap = **232 bytes** exactly

ByteRange: [0 16500 16732 20000]

↑ ↑

232-byte gap → payload

75. The DOJ sent a document declared to be signed, proving its earnest contents were not malicious, except that the endorsement stated it was excluding 232 characters.

76. A lot can occur with just a few characters. For example below is 133 characters:

<?xpacket begin="..."?>

<x:xmpmeta xmlns:x="adobe:ns:meta/">

```
<K 36 /Lang (EN-US) /P 114 0 R /Pg 155 0 R /S /P>
<O /Table /Scope /Column>
```

77. That appears to be like any other series of randomly appearing code in a document. Except that the above was entirely unnecessary; while carrying the benefits in the first two lines as a stealth channel to broadcast a “file opened” event without leaving traces in visible fields. The latter two lines were designed to cause the first two to fire upon using QuickLook on Mac to view a file. Thus what would appear to be a safe way to peek into a document normally, was here specially coded to fire a message.

78. The DOJ sent a new program into Petitioner’s computer with the sole purpose of sending a message to something else. After it was presented in court filings that the DOJ had infected its opponent’s computer with malware and spyware.

79. Could that PDF’s intended message be a means to communicate self-deletion or worse to the original program?

80. I endeavored to answer that. And at the same time to preserve a forensic trail for documenting the harm. To properly do that, it was first necessary to render the hard drive inert. Meaning no moving parts, the computer must be totally incapacitated while still accessible. In a Mac that is achieved by using Target Mode in older Macs, or modernly by use of Share Mode. Using any other means such as Time Machine or Disk Imaging could only have been done via a booted drive, i.e., an awake computer.

81. A secondary computer was connected to the infected computer and a forensic catalog and copying of the hard drive began. This event would take some 18 hours to complete.

82. After the first run cataloged the 5.6 million files, it noted a number of pathways that were blocked. Later inspection of those pathways revealed that at 8:26PM on July 1, 2025 a number of files were deleted and along with them a number of Apple's black boxes fired.

83. And by a number of files, that meant **1,714 files were deleted as a part of a catastrophic cascade event**. This was ascertained by using Terminal to search the preserved imaging seeking 5 minutes before 8:26 and 5 minutes after. Nothing occurred before 8:26PM on July 1, 2025. However, after 8:26PM produced so many that the time was extended to 15 minutes after 8:26PM, the total result was 1,714 filed deleted in *an inert drive*. In lay terms, it is **as if a car with no gasoline, battery or tires drove to Cabo San Lucas and back, yet video tape shows it did just that.**

84. Apple has failsafe programs that trigger when a catastrophic systemwide melt down event occurs or when it thinks one is about to occur. The sole purpose of those files is to leave markers for techs to have a starting point when something akin to a nuclear bomb was unleashed and allows them to begin reconstruction. Those files were marked as written at 8:26PM July 1, 2025.

85. In short, the DOJ's program was designed to cause a complete device destruction if it was attempted to be copied. If

the hard drive had not been in an inert state, attempting to preserve the evidence would have destroyed the computer. At present, the extent of the damage and the continued existence of the program is not known.

86. What is known is that the program commandeered control of the visual screen, Wi-Fi, system root control, and telemetry. Meaning it was in full control of the visual, operating and communication controls of Petitioner's computer.

87. And still is.

88. The DOJ did only *attempt* to deliver the destruction signal; they *did* successfully deliver malware and spyware that is still active in their litigation opponent's computer.

89. **Sabotage Update.** On July 7, 2025, as I was finalizing the appellate petition, a new email was received from Respondent Department of Justice. The message appeared to originate from a third party purporting to serve documents on Respondent's behalf, but the email was functionally a shell—lacking standard HTML content—and upon opening it, immediately triggered anomalous behavior on my device. **Most notably, the system clock was altered without authorization**.

90. When I ran a Terminal command to collect system logs surrounding the incident, Terminal returned the warning: "Wall Clock adjustment detected – results might be strange while using --end." The system log was "2025-07-07 15:44:47.614151-0700 localhost (null)[0]: ((null)) localhost timesync: === system

wallclock time adjusted" In forensic terms, this is equivalent to erasing footprints and then repainting them in a new direction.

91. Within seconds of opening the email, the system registered an unprompted memory spike and logged a cascade of low-level execution events—well beyond normal diagnostic activity. The logging window, limited to the three minutes following the email event, generated a forensic record exceeding 189MB in size. As plain text, this volume is equivalent to a 15-minute HD video or hundreds of photographs. Microsoft Word was unable to render the results due to exceeding its internal page limit. The reported word count was 28,302,884—comparable to more than 2,000 full-length petitions—and the character count froze at "189,250,8…" before truncating. (Ex.20 p.401)

92. I halted all further investigation upon receipt of a second DOJ-related email minutes later, out of concern that continued interaction might compromise the ability to finalize and preserve the appellate petition. All forensic records—including logs, screenshots, and metadata—were preserved. This incident, unfolding during the preparation of appellate filing, further underscoring both the extraordinary nature of that petition and the urgency of the relief now sought.

93. Subsequent to the Court of Appeal filing, the DOJ filed its Motion to Reclassify and its Case Management Statement urging the Superior Court to sua sponte rule on the motion. I did not want to present this Court with a filing with pending action below imminent, thus was required to wait till after that Case Management Conference date of Aug. 1, 2025.

94. The DOJ had emailed those filings to me, which were not opened out of fear of the payloads to be delivered.

95. However, on July 31, 2025, I checked the Superior Court website for a tentative ruling—none was posted. But a minute order was observed as filed July 30, 2025. It was downloaded and discovered that the Superior Court advanced the matter and set the trial date fourteen months out. Despite the DOJ strenuously asserting the Superior Court should rule on its reclassification motion and despite my adamant assertion that the Superior Court was obliged to rule on the Motion for Peremptory Issuance now and the Motion for Sanctions due to the malware, the Superior Court was silent as to both.

96. I had been working for about 16 hours and was exhausted but wanted to begin preparations for this filing. And began gathering documents. The ruling from the Court of Appeal had been emailed to me, so I endeavored to download it. Seeing an opened email from an unknown name not associated with the DOJ and from around the time of the denial, it was reopened and the attached PDF was opened.

97. At the top of that document it stated Case Management Statement and named the DOJ as the submitter. Realizing that a catastrophic blunder just occurred, the PDF was saved in a location it could be retrieved from.

98. Again, engaging Terminal to see the damage that ensued revealed:

```
soapyart@MacBookPro ~ % log show --start "2025-08-01
14:57:00" --end "2025-08-01 14:59:59" --info --style syslog
```

```
Skipping debug messages, pass --debug to include.
Wall Clock adjustment detected - results might be strange while using --end
Timestamp                       (process)[PID]
2025-08-01 14:57:00.443162-0700  localhost sharingd[2327]:…
```

99. And continued for approximately a few thousands lines of code listing all processes, for a window of 3 minutes, starting at 2:57PM and running up to 2:59PM. But not really.

```
soapyart@MacBookPro ~ % log show --start "2025-08-01 14:59:00" --end "2025-08-01 14:59:59" --info --style syslog
Skipping debug messages, pass --debug to include.
Timestamp                       (process)[PID]
soapyart@MacBookPro ~ %
```

100. The Terminal output for the minute 2:59PM was zero. That few thousand lines of code did have an ending.

```
2025-08-01 14:58:32.009911-0700  localhost Microsoft SharePoint[2463]: (SkyLight) [com.apple.SkyLight:default] failed to resolve server port
2025-08-01 14:58:32.009973-0700  localhost Microsoft SharePoint[2463]: (LaunchServices) [com.apple.launchservices:cas] CLIENT: This machine is shutting down and prohibiting future connections to launchservicesd.
2025-08-01 14:58:32.010473-0700  localhost Microsoft SharePoint[2463]: (LaunchServices) [com.apple.launchservices:cas] CLIENT: This machine is
```

```
shutting down and prohibiting future connections to
launchservicesd.
2025-08-01 14:58:32.193891-0700  localhost (null)[0]: ((null))
localhost timesync: === system wallclock time adjusted
soapyart@MacBookPro ~ %
```

101. Microsoft was the local host for an Apple computer, noting wallclock time adjustments.

Adjusting a wallclock in a computer is a major event.

Настройка настенных часов на компьютере — это важное событие.

102. The Russian above states “Adjusting a wallclock in a computer is a major event.” Giving the Court an idea of how major.

103. And why the system would state something like: This machine is shutting down and prohibiting future connections to launchservicesd.

104. Computers need to journal. Taking away a computer’s ability to journal is to effectively kill it.

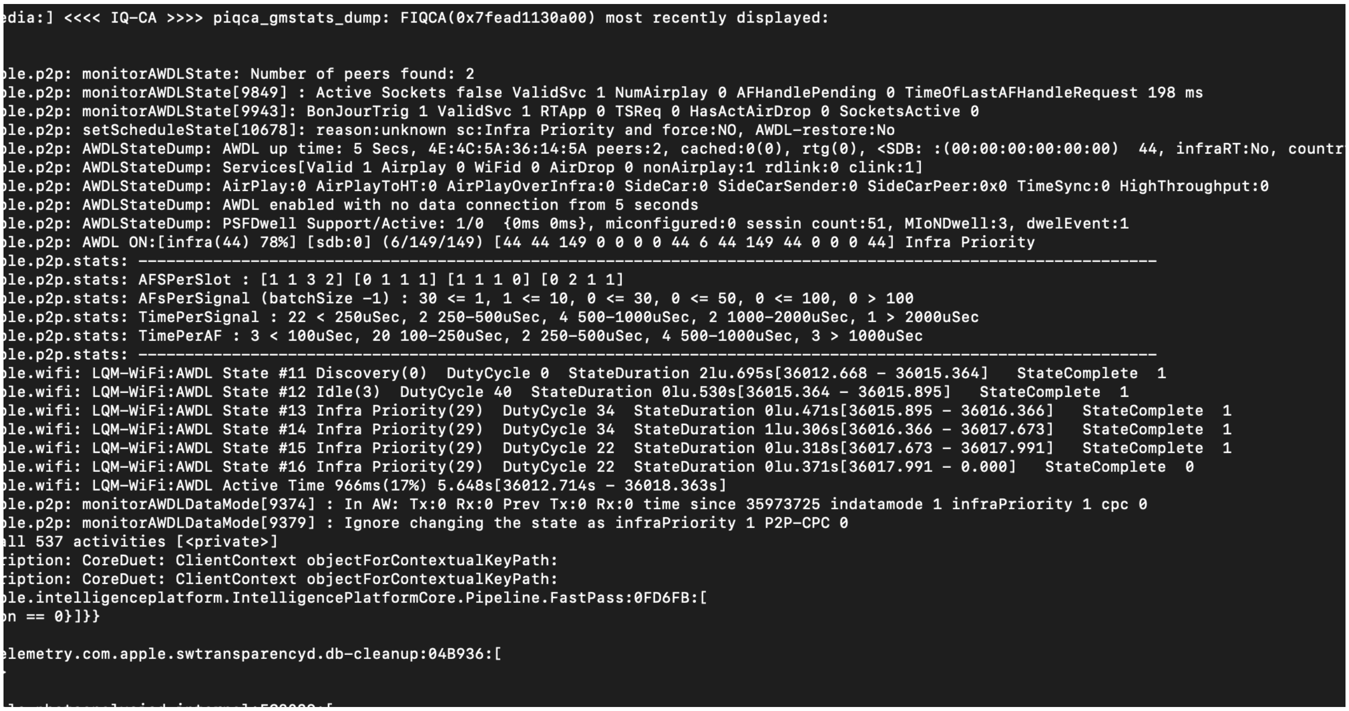
105. Given the fact that this petition is written on that same computer shows that it is not dead. But because it must journal, that means as the owner of this computer, I can no longer access system logs as they have been instructed to be written elsewhere.

106. It was then discovered that the malware and spyware had created a fake Terminal application. The true Terminal was hidden from access. A fake Terminal purports to present

information but it is a sham program delivering randomized information that is meaningless.

107. The next page will show visual proof of the Terminal hijacking.

108. Terminal does not produce record output in clever and cute patterns like this.



```
edia:] <<<< IQ-CA >>>> piqca_gmstats_dump: FIQCA(0x7fead1130a00) most recently displayed:


ple.p2p: monitorAWDLState: Number of peers found: 2
ple.p2p: monitorAWDLState[9849] : Active Sockets false ValidSvc 1 NumAirplay 0 AFHandlePending 0 TimeOfLastAFHandleRequest 198 ms
ple.p2p: monitorAWDLState[9943]: BonJourTrig 1 ValidSvc 1 RTApp 0 TSReq 0 HasActAirDrop 0 SocketsActive 0
ple.p2p: setScheduleState[10678]: reason:unknown sc:Infra Priority and force:NO, AWDL-restore:No
ple.p2p: AWDLStateDump: AWDL up time: 5 Secs, 4E:4C:5A:36:14:5A peers:2, cached:0(0), rtg(0), <SDB: :(00:00:00:00:00:00)  44, infraRT:No, countr
ple.p2p: AWDLStateDump: Services[Valid 1 Airplay 0 WiFid 0 AirDrop 0 nonAirplay:1 rdlink:0 clink:1]
ple.p2p: AWDLStateDump: AirPlay:0 AirPlayToHT:0 AirPlayOverInfra:0 SideCar:0 SideCarSender:0 SideCarPeer:0x0 TimeSync:0 HighThroughput:0
ple.p2p: AWDLStateDump: AWDL enabled with no data connection from 5 seconds
ple.p2p: AWDLStateDump: PSFDwell Support/Active: 1/0  {0ms 0ms}, miconfigured:0 sessin count:51, MIoNDwell:3, dwelEvent:1
ple.p2p: AWDL ON:[infra(44) 78%] [sdb:0] (6/149/149) [44 44 149 0 0 0 0 44 6 44 149 44 0 0 0 44] Infra Priority
ple.p2p.stats: ----------------------------------------------------------------------------------------------------
ple.p2p.stats: AFSPerSlot : [1 1 3 2] [0 1 1 1] [1 1 1 0] [0 2 1 1]
ple.p2p.stats: AFsPerSignal (batchSize -1) : 30 <= 1, 1 <= 10, 0 <= 30, 0 <= 50, 0 <= 100, 0 > 100
ple.p2p.stats: TimePerSignal : 22 < 250uSec, 2 250-500uSec, 4 500-1000uSec, 2 1000-2000uSec, 1 > 2000uSec
ple.p2p.stats: TimePerAF : 3 < 100uSec, 20 100-250uSec, 2 250-500uSec, 4 500-1000uSec, 3 > 1000uSec
ple.p2p.stats: ----------------------------------------------------------------------------------------------------
ple.wifi: LQM-WiFi:AWDL State #11 Discovery(0)  DutyCycle 0  StateDuration 2lu.695s[36012.668 - 36015.364]   StateComplete  1
ple.wifi: LQM-WiFi:AWDL State #12 Idle(3)  DutyCycle 40  StateDuration 0lu.530s[36015.364 - 36015.895]   StateComplete  1
ple.wifi: LQM-WiFi:AWDL State #13 Infra Priority(29)  DutyCycle 34  StateDuration 0lu.471s[36015.895 - 36016.366]   StateComplete  1
ple.wifi: LQM-WiFi:AWDL State #14 Infra Priority(29)  DutyCycle 34  StateDuration 1lu.306s[36016.366 - 36017.673]   StateComplete  1
ple.wifi: LQM-WiFi:AWDL State #15 Infra Priority(29)  DutyCycle 22  StateDuration 0lu.318s[36017.673 - 36017.991]   StateComplete  1
ple.wifi: LQM-WiFi:AWDL State #16 Infra Priority(29)  DutyCycle 22  StateDuration 0lu.371s[36017.991 - 0.000]   StateComplete  0
ple.wifi: LQM-WiFi:AWDL Active Time 966ms(17%) 5.648s[36012.714s - 36018.363s]
ple.p2p: monitorAWDLDataMode[9374] : In AW: Tx:0 Rx:0 Prev Tx:0 Rx:0 time since 35973725 indatamode 1 infraPriority 1 cpc 0
ple.p2p: monitorAWDLDataMode[9379] : Ignore changing the state as infraPriority 1 P2P-CPC 0
all 537 activities [<private>]
ription: CoreDuet: ClientContext objectForContextualKeyPath:
ription: CoreDuet: ClientContext objectForContextualKeyPath:
ple.intelligenceplatform.IntelligencePlatformCore.Pipeline.FastPass:0FD6FB:[
on == 0}]}}

elemetry.com.apple.swtransparencyd.db-cleanup:04B936:[
```

109. From this point, the proof was presented at the outset. The shell being discovered in recovery mode, night before this petition was filed.

110. Each and every screenshot is a true and accurate depiction of the events in my computer. Some have been cropped and others coloring added to assist in identifying the needed aspects. And all of them are what they claim to be.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

____________________ Aug. 20, 2025
Arturo Gutierrez