Homeland Security Investigations
Office of the Assistant Special Agent in Charge

3000 Sidney Street, Suite 300
Pittsburgh, PA 15203

[LAW ENFORCEMENT SENSISTIVE]

February 18, 2025

David Coleman
Homeland Security Investigations
3000 Sidney Street, Suite 300
Pittsburgh, PA 15203

Honorable W. Scott Hardy
Joseph F. Weis, Jr. U.S. Courthouse
700 Grant Street
Pittsburgh, PA 15219

Dear Judge Hardy,

I am writing to provide my professional perspective and address the allegations raised by the defense in the case involving Mr. Seth Aikens. Special Scott Fell specifically requested my forensic assistance in this case. As the lead digital forensics investigator and examiner at HSI-Pittsburgh, I have nearly ten years of experience. In my time as a forensic investigator, I have developed a deep expertise of computer forensics. I have imaged/previewed data from hundreds of computers, mobile devices, and loose computer media. Throughout my career, I have encountered numerous encrypted devices and have never "lost" or "spoiled" any encrypted data.

Regarding the specific allegations that the defense stated in paragraphs 5 through 8 of their spoliation motion:

> The allegation made in paragraph number 5 is incorrect because the encrypted computers and encrypted computer media in question were never powered on. Therefore, "kill-switches" could not have been activated. The storage media (hard drives or solid-state drives) were previewed and/or imaged in a write-protected state, which does not affect "kill-switch" style encryption. Also, most of the encountered encryption was Microsoft BitLocker, which does not support "kill-switch" style encryption.
>
> The allegation made in paragraph number 6 is incorrect because the encrypted data can be accessed with the proper decryption keys. These keys were created by the defendant, Mr. Aikens. There was also unencrypted computer media that was able to be accessed and imaged in a forensically sound manner. For specific reference, please review the government's spreadsheet which lists the devices and pieces of computer media that were able to be accessed/imaged and the ones that are still encrypted.

The allegation made in paragraph number 7 is incorrect because the inaccessibility of the data is specifically due to the defendant's inaction of providing the proper decryption keys to unlock the data stored on these encrypted devices.

The allegation made in number 8 is incorrect. The data is not lost; it still exists in its encrypted state, waiting for the proper decryption keys to unlock it. As a real-life example, if an individual is unable to open a lockbox, the contents of the lockbox will remain unchanged until such time that lockbox is opened.

Given my extensive experience in digital forensics and my direct involvement in the handling of these devices, I can confidently assert several points. Firstly, at the current time, HSI Pittsburgh does not possess the forensic tools to "break-in" to devices encrypted with Microsoft BitLocker, or any other style of encryption. I can also assert that the government's procedures did not render the encrypted drives permanently inaccessible. All data, whether encrypted or unencrypted still exists in the state in which it was found; the government did nothing to spoil the data. The data remains intact on these drives and accessible with the appropriate decryption keys, if and when they are provided.

Thank you for considering my perspective in this matter. I am available to provide further clarification or testimony, if necessary.

Sincerely,

David J. Coleman
Computer Forensics Special Agent
Homeland Security Investigations
Pittsburgh, PA