UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v-

JOSHUA ADAM SCHULTE,

Defendant.

S3 17 Cr. 548 (JMF)

MOTION OF DEFENDANT JOSHUA ADAM SCHULTE FOR A JUDGMENT OF ACQUITTAL OR NEW TRIAL

Joshua Adam Schulte
Metropolitan Detention Center (MDC)
P.O. Box 329002
Brooklyn, NY 11232

TABLE OF CONTENTS

I. TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

II. STATEMENT OF THE CASE

A. Overview

Joshua Adam Schulte respectfully renews his motion, under Fed. R. Crim. P. 29(a)-(c), for a judgment of acquittal on all counts. On July 13, 2022, the jury returned a guilty verdict as to all counts. However, the government failed to meet its burden and the Court should vacate the convictions. Alternatively, for those counts that the Court upholds as to sufficiency, it should still vacate and order a new trial in the interests of justice pursuant to Fed. R. Crim. P. 33.

B. Applicable Law

"Rule 29 permits a trial court to set aside a jury's guilty verdict and enter an acquittal if it determines the evidence was 'insufficient to sustain a conviction.'" *United States v. Blanco*, 811 Fed. Appx. 696, 701 (2d Cir. 2020) (referencing Fed. R. Crim. P. 29(a)). Acquittal is required if, viewing the evidence in the light most favorable to the government, no rational juror could properly find all the essential elements of the crime beyond reasonable doubt. E.g., *Jackson v. Virginia*, 443 U.S. 307, 319 (1979); *United States v. Torres*, 604 F.3d 58, 67 (2d Cir. 2010).

"Applying this standard does not mean that a reviewing court must affirm all jury verdicts. If 'we are to be faithful to the constitutional requirement that no person may be convicted unless the Government has proven guilt beyond a reasonable doubt, we must take seriously our obligation to assess the record to determine whether a jury could *reasonably* find guilt beyond a reasonable doubt.'" *United States v. Valle*, 807 F.3d 508, 515 (2d Cir. 2015) (quoting *United States v. Clark*, 740 F.3d 808, 811 (2d Cir. 2014)). "This standard does not mean that if there is any evidence that arguably could support a verdict, we must affirm. In any criminal trial there is always some evidence of guilt, otherwise there could not have been a prosecution." *Id.*

"While we defer to a jury's assessments with respect to credibility, conflicting testimony, and the jury's choice of the competing inferences that can be drawn from the evidence, specious inferences are not indulged, because it would not satisfy the Constitution to have a jury determine that the defendant is *probably* guilty. **If the evidence viewed in the light most favorable to the prosecution gives equal or nearly equal circumstantial support to a theory of guilt and a theory of innocence, then a reasonable jury must necessarily entertain a reasonable doubt."** (emphasis added) *Id.* See also *United States v. Lorenzo*, 534 F.3d 153, 159 (2d Cir. 2008).

Rule 33 permits a trial court to set aside a jury's guilty verdict and "grant a new trial if the interest of justice so requires." Fed. R. Crim. P. 33(a). The defendant can combine the motion for a new trial under Rule 33 with a motion for acquittal under Rule 29. *United States v. Rojas*, 574 F.2d 476 (9th Cir. 1978).

III. SUMMARY OF ARGUMENTS

Mr. Schulte should be acquitted of the MCC Espionage Counts Three and Four because the alleged content is not national defense information, it was not unlawfully possessed, it was not “documents” but “information”, and it was not willfully transmitted or attempted to be transmitted.

Mr. Schulte should be acquitted of CFAA Counts Seven and Eight because Mr. Schulte possessed an authorized key that granted him the authority to perform any and all administrative functions on the ESXi Server, and he did not intend to, nor cause damage or any harmful consequences.

Mr. Schulte should be acquitted of Count Nine, because the government did not establish there was any pending proceeding that Mr. Schulte knew about—nor that he obstructed.

Mr. Schulte should be acquitted of the WikiLeaks Espionage Counts One, Two, Five, and Six because the government’s case is literally *impossible*. The government does not propose any theory for how Mr. Schulte gathered national defense information or to where he gathered it—the evidence clearly shows that Mr. Schulte did not copy any information and that he had no removable drive to write it anyway. The government also failed to show that Mr. Schulte ever possessed the national defense information at his home or transmitted it to WikiLeaks. As for Counts Five and Six, the government failed to show what access controls existed for the altabackups directory.

Finally, the Court should grant Mr. Schulte a new trial due to the government’s failure to disclose and produce the relevant forensic images that it relied upon in its case-in-chief.

IV. MR. SCHULTE SHOULD BE ACQUITTED OF THE MCC COUNTS

A. Count Three: Illegal Transmission of Unlawfully Possessed National Defense Information

> *Count Three charges that, in or about September 2018, the defendant had unauthorized possession of documents, writings, or notes containing NDI related to the internal computer networks of the CIA, and willfully transmitted them to a third party not authorized to receive them.* (Charge at 21)
>
> *In order to find the defendant guilty of Count Two or Count Three, the Government must prove the following three elements beyond a reasonable doubt:*
>
> *First that, on or about the dates charged in the indictment, the defendant had unauthorized possession of, access to, or control over a document, writing, plan, instrument, or note;*
>
> *Second, that the information in that material was connected to the national defense; and,*
>
> *Third, that, on or about the dates in the Indictment, the defendant willfully communicated, delivered, or transmitted (or caused to be communicated, delivered, or transmitted) the document, writing, plan, instrument, or note to a person who was not entitled to receive it.* (Charge at 26)

The government alleged that Mr. Schulte emailed a reporter information about Hickock, which it claims is "National Defense Information." The email itself, GX 812, focuses on why the initial search warrants were unconstitutional. The point of the email is clearly to communicate the deficiency of the search warrants. The document discusses the search warrants for nine pages—and is largely vindicated by the government's Brady Letter that was released a few weeks after the email was drafted. The use of "Hickock" was clearly just to name the network connection—not to willfully expose national defense information.

1. Element 2: National Defense Information (Hickok)

> *The second element that the Government must prove beyond a reasonable doubt for purpose of Counts Two and Three is that the documents, writings, plans, instruments, or notes at issue are NDI.* (Charge at 28)

The government failed to prove that the statement "[t]hey don't include COG who was connected to our DEVLAN through HICOC, an intermediary network that connected both COG and EDG" is national defense information.

a) Hickok exposed by WikiLeaks in March 2017

Count Three charges Mr. Schulte with disclosing information that was already exposed by WikiLeaks and publicly accessible on the internet for over a year and a half. The government failed to show how 18-month-old publicly accessible information could possibly be national defense information; public information on WikiLeaks, the New York Times, the Washington Post, and other news outlets and throughout the internet is not "closely held", and therefore not "national defense information."

The government itself concedes in the stipulation marked as GX 3009, that at the time of the disclosure in September of 2018, the following appeared 18 months earlier in the WikiLeaks "Vault 7" release:

> HICKOK ... Used for transferring tools and their associated documentation between DEVLAN and [COG Network][;] Consists of two firewalls, a datastore that houses the files to be transferred, and the JIRA instance for discrepancy reporting.
>
> The operators also have an instance of Stash in the [COG Network], however synching between the two instances would not be possible without changing the location of the operator's version. It may be possible to relocate the operator's Stash instance to Hickok, which would allow synching with AED's version of Stash, similar to how the JIRA instance works today…
>
> In EDG we use JIRA to track issues on projects. JIRA sits on Hickock which is shared between us and COG.

It also included the following graphic:

The image part with relationship ID rId13 was not found in the file.

There was nothing disclosed by GX 812 that wasn’t already disclosed by WikiLeaks. Accordingly, this information was not “closely held” and therefore cannot possibly be NDI.

b) Hickok was shut down after WikiLeaks

Additionally, because of the WikiLeaks disclosure in 2017, “hickock” and every other exposed CIA network from 2017 was completely shut down. The CIA created new networks long before September of 2018. Hence, knowledge about “hickock” in 2018 was old news and could not possibly compromise any CIA network or national defense—DevLAN was already shattered and shuttered. See Tr. 1433 – Weber:

Q. *OK. Let's talk a little bit about WikiLeaks's publication. As you said, after the WikiLeaks disclosure on March 7, DevLAN was shut down, correct?*
A. *That's correct.*
Q. *It was no longer used, right?*
A. *To my knowledge, correct.*

See also Tr. 694 – Leonis:

Q. *OK. With respect to the WikiLeaks publication, I think you testified that after the WikiLeaks disclosure on March 7, 2017, the DevLAN network was shut down, correct?*
A. *Yes.*
Q. *It was no longer used, right?*
A. *No.*

c) Generic information about closed networks not NDI

Since DevLAN and hickock were closed networks that did not connect to the internet, it would be absurd to claim that knowledge of their names or how they were connected somehow constitutes a danger to the national security of the United States. Undoubtedly, the CIA, NSA, and other intelligence agencies across the world have closed networks that are not connected to the internet—so how could knowing the names of these networks harm the United States or benefit any foreign nation? Knowing that the CIA has a network called "DevLAN" does nothing for Russia because they cannot access the network anyway, and have no idea where it is even physically located. It's like telling the Russians the CIA have computers—such information is *so widely known that it cannot possibly be considered national defense information*. The CIA now uses a replacement DevLAN network. It almost certainly also contains a similar connection to COG's network—who are EDG's customers. So is this national defense information? Or simple logic derived from basic information so widely circulated—that EDG uses computer networks and develops software for COG—that it cannot possibly be considered national defense information. The mere fact that EDG and COG's closed networks connect in some way is simply far too generic to be classified, let alone national defense information.

Tellingly, the government did not put on a single classification expert at trial—not one. See Tr. 1461 – Weber:

Q. *And there is the developers are not those classification experts, correct?*
A. *To my knowledge that is correct.*
Q. *The CIA has classification experts, right?*
A. *That is correct.*

Q. *An entire group of classification experts, right?*
A. *I don't know the size or scope of the experts.*
Q. *But you never worked in that group, right?*
A. *That is correct.*

See also Tr. 1483 – Weber:

Q. *No. I was saying that you testified earlier that you are not a classification expert, correct?*
A. *No, I am not a classification expert.*

d) CIA provided Hickok User's Guide as unclassified

Finally, the government did not present a single shred of evidence that the CIA ever communicated any information to Mr. Schulte indicating that the connection between EDG and COG's networks was deemed classified. To the contrary, the Hickok User's Guide was labeled "unclassified" and distributed to Mr. Schulte during his employment there. See GX 616. Accordingly, Mr. Schulte had absolutely no reason to suspect that this information was classified or otherwise protected by the CIA.

2. Element 2: National Defense Information (COG employees)

The government also claimed that the number of COG employees was also national defense information. However, as an initial matter, this constitutes a constructive amendment of the indictment as the indictment specifically detailed documents "pertaining to internal computer networks of the CIA." Dkt. 405 at 3. The indictment does not charge the defendant with disseminating personnel information—which broadens the possible bases for conviction. An indictment is constructively amended if either the "proof at trial or the trial court's jury instructions so altered an essential element of the charge that, upon review, it is uncertain whether the defendant was convicted of conduct that was the subject of the grand jury's indictment." *United States v. Milstein*, 401 F.3d 53, 65 (2d Cir. 2005). This occurs "when the trial evidence or the jury charge operates to broaden the possible bases for conviction from that which appeared in the indictment." *United States v. Rigas*, 490 F.3d 208, 225 (2d Cir. 2007) (brackets and internal quotation marks omitted). Accordingly, the Court should not even consider this allegation.

However, in any case, the government failed to establish that Mr. Schulte was ever briefed on the number of personnel in COG, or otherwise knew this information. See Tr. 1611-12 – Weber:

Q. *As someone in EDG you are not briefed on how many people are in COG, right?*
A. *I believe that to be a correct statement.*
Q. *So any assessments that you would make on that would not be based on direct knowledge; right?*
A. *That's correct.*

Due to the principle of need-to-know, Mr. Schulte did not have a need-to-know the number of personnel in COG—he was never briefed or informed of this number. Since the government failed to prove that this information was ever communicated to Mr. Schulte, let alone that it was communicated to Mr. Schulte as classified information, the government failed to prove the COG-estimated-employees statement was NDI.

Furthermore, the government did not introduce a single document establishing the number of COG employees—they did not establish that 200 was, in fact, the number of COG employees. Information cannot be NDI if it is not true: If Mr. Schulte said the CIA kept aliens at Area 51, he could not be indicted, arrested, and punished since this information is false (at least, as far as he knows). Failing to establish that COG contained 200 employees, and that this information was classified, the government failed to prove that this information was national defense information.

3. Element 3: Willful Transmission

The third element that the Government must prove beyond a reasonable doubt for purpose of Count Two and Three is that, on or about the dates charged in the count at

> *issue, the defendant willfully communicated, delivered, or transmitted (or caused to be communicated, delivered, or transmitted) the document, writing, plan, instrument, or note to a person who was not entitled to receive it.* (Charge 28).
>
> *An act is done "willfully" if it is done voluntarily and intentionally and with the specific intent to do something the law forbids, that is to say, with a bad purpose either to disobey or disregard the law. In determining whether a defendant has acted willfully, however, it is not necessary for the Government to establish that the defendant was aware of the specific law or rule that his conduct may be violating.* (Charge 29).

The government did not establish that Mr. Schulte willfully transmitted the Hickok information. This "willfulness" requirement "eliminat[es] any genuine risk of holding a person 'criminally responsible for conduct he could not reasonably understand to be proscribed.'" *United States v. Hsu*, 364 F.3d 192, 197 (4th Cir. 2004) (quoting *United States v. Sun*, 278 F.3d 302, 309 (4th Cir. 2002)); see also *United States v. Truong Dinh Hung*, 629 F. 2d 908, 919 (4th Cir. 1980) (describing an act done "willfully" as an act committed with a "design to mislead or deceive another. That is, not prompted by an honest mistake as to one's duties, but prompted by some personal or underhanded motive."). In order to establish a willful transmission of National Defense Information, the defendant must know or have reason to believe that the information is, in fact, national defense information.

Considering all the information established in Element 2 (A.1.a-d), neither Mr. Schulte nor any reasonable person could possibly believe the Hickok statement to be classified let alone national defense information: (a) it was already disclosed publicly by WikiLeaks, (b) it was shut down after the leaks, (c) it was written too generically to be classified or sensitive in any way, (d) the CIA informed Mr. Schulte that Hickok was unclassified through its general user's guide (GX 616). Furthermore, the purpose of the email clearly is not to disseminate classified or sensitive information but to highlight the search warrants Mr. Schulte believed to be unclassified.

Accordingly, Mr. Schulte did not intentionally, willfully transmit the Hickok information for a bad purpose or to disobey or disregard the law.

4. Element 1: Possession

> *The first element that the Government must prove beyond a reasonable doubt for purpose of Counts Two and Three is that, on or about the dates charged in the count at issue, the defendant had unauthorized possession of, control over, or access to, the documents, writings, plans, instruments, or notes in question.*
>
> *In the case of Count Three, the Indictment charges that, in or about September 2018, the defendant, without authorization, possessed documents, writings, and notes pertaining to internal computer networks of the CIA, including DEVLAN.* (Charge 27)

The government failed to prove that Mr. Schulte unlawfully possessed tangible documents in September of 2018. In fact, the government presented a completely different case at trial—that Mr. Schulte lawfully possessed intangible information in September of 2018. Accordingly, even if the Court accepts the government's proof at trial, the result is a fatal variance. A variance occurs "when the charging terms of the indictment are left unaltered, but the evidence offered at trial proves facts materially different from those alleged in the indictment." *United States v. Thomas*, 274 F.3d 655, 670 (2d Cir. 2001) (internal quotation marks omitted). Unlike a constructive amendment claim, "a defendant must demonstrate prejudice to prevail on a variance claim." *Id.* The prejudice here is that the government failed to prove Element One of Count Three, requiring acquittal.

a) Mr. Schulte should have been charged under the "information" prong of the statute, requiring the additional reason-to-believe scienter

The items possessed were intangible information—not tangible documents—which required the government to prove the additional reason-to-believe scienter. This particular instance here is no different than *United States v. Rosen*, in which the defendant was accused of communicating intangible information orally. In fact, at the first trial in 2020 the government correctly charged Mr. Schulte under the “information” prong of the statute. And the reason why this distinction is so critical, is that intangible information cannot be easily assessed as classified—whereas tangible documents, clearly marked as classified, inform the possessor of its status. See, e.g. *United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006), aff'd, 557 F.3d at 192 (4th Cir. 2009) at 624 (emphasis added):

> Citing these parallels, defendants argue that the difficulty in determining whether orally transmitted information is classified is highly relevant to whether the statute provides constitutionally adequate notice. A comparison of the application of the statute as-applied here to intangible information and the application of the statute in the typical § 793 prosecution to the delivery of classified documents (or any other tangible item) illustrates this point. *All classified documents are clearly marked with a classification level and are often marked classified or unclassified at the paragraph level*. **For this reason, a person possessing such a document can easily determine: (i) whether the possession is authorized, (ii) which portions of the information the government is attempting to keep secret, and (iii) who else is entitled to receive the document.** *In contrast, a conversation about classified information, even one accompanied by a generic warning that “this information is classified,” is not likely to appraise the listener of precisely which portions of the information transmitted in the conversation are classified, or whether a more general description of the information retains its classification status such that it is sufficiently closely held and potentially damaging to the United States to violate the statute*. Defendants argue that the difficulty in determining the classification of intangible information renders the application of the statute to them unconstitutionally vague.

Thus, the reason-to-believe scienter is not necessary for documents clearly marked as relating to the national defense; however, this additional scienter is absolutely necessary for any other type of information, from which there are no similar markings designating the information as relating to the national defense. Judge Ellis goes on to explain how the statute accounts for these differences—the additional reason-to-believe scienter, which is required for any conviction of disseminating “information.”

> In addition to proving that the defendants committed the prohibited acts "willfully," the statute imposes an additional and significant scienter requirement when a person is accused of transmitting "information relating to the national defense." Thus, the statute, as-applied to these defendants also requires the government to prove that such information was communicated with "reason to believe it could be used to the injury of the United States or to the advantage of any foreign nation." 18 U.S.C. §§ 793(d), (e). This language accompanied Congress's amendment of the statute in 1950 adding the term "information" back into the provisions' list of enumerated items relating to the national defense, and it is clear from both the text and the legislative history that this additional scienter requirement applies only to the communication of intangible "information," and is intended to heighten the government's burden when defendants are accused of communicating intangible information.

Accordingly, the government altogether failed to prove that the items possessed were tangible "documents" with clear classification markings designating the documents relating to the national defense as opposed to intangible "information" with no such markings. Indeed, GX 812 contains no classification or NDI markings, and it is entirely unclear that this email and accompanying attachments relate to the national defense. Moreover, the government points to no originating source material that was provided to Mr. Schulte—was he ever informed of this information at all? Was he informed of this information orally? Since the intangible information required the additional reason-to-believe scienter that the government neither offered to the jury nor proved beyond a reasonable doubt, Mr. Schulte must be acquitted of Count Three due to this fatal variance.

b) Mr. Schulte should have been charged under § 793(d) instead of § 793(e)

The government charged Mr. Schulte with the unlawful possession of national defense information pursuant to 18 U.S.C. § 793(e). However, the intangible information he possessed was possessed lawfully—it was a product of his own memory, not tangible documents unlawfully stolen from the CIA. Mr. Schulte's retention of intangible information in his head cannot possibly be unlawful—there is no way for him to "return" intangible information he retains in his head. Furthermore, typing that information is simply a transportation from his head to a computer—it also cannot be unlawfully possessed. Anything Mr. Schulte writes is lawfully possessed by him—just as those who write books about their experience at the CIA and then submit those books for classification review—if classified information is discovered in those books, the individuals cannot be, and are not, prosecuted for the "unlawful possession of NDI." Accordingly, the government failed to prove that the Hickok information was unlawfully possessed. This is yet another fatal variance requiring the Court to acquit Mr. Schulte of Count Three.

***

The government came nowhere close to establishing sufficient evidence to convict Mr. Schulte of Count Three. In fact, Judge Crotty dismissed Count Three at the first trial in 2020—and the government failed to establish anything new at the second trial. "The Court, however, concludes that the evidence presented at trial was insufficient to establish beyond a reasonable doubt that the Hickok information (i.e., that Hickok connected DEVLAN to another group's network) was national defense information. The Government elicited no testimony establishing how this information related to national defense or explaining the utility of such information. See GX 616 (Hickok User Guide marked unclassified)." Dkt. 581 at 25. For the same reasons dictated by Judge Crotty, this Court should again dismiss Count Three.

B. Count Four: "Attempted" Illegal Transmission of Unlawfully Possessed National Defense Information

> *Count Four charges that, between July and September 2018, the defendant had unauthorized possession of documents, writings, and notes containing NDI related to tradecraft techniques, operations, and intelligence gathering tools used by the CIA, and attempted to transmit them to a third party or parties not authorized to receive them.* (Charge at 21)

Count Four is based on the following passages in Government Exhibits 801 and 809—and the following passages alone:

- Government Exhibit 801, page 3: "Which brings me to my next point—Do you know what my specialty was at the CIA? Do you know what I did for fun? Data hiding and crypto. I designed and wrote software to conceal data in a custom-designed file system contained with the drive slackspace of hidden partitions. I disguised data. I split data across files and file systems to conceal the crypto—analysis tools could NEVER detect random or pseudo-random data indicative of potential crypto. I designed and wrote my own crypto—how better to fool bafoons like forensic examiners and the FBI than to have custom software that doesn't fit into their 2-week class where they become forensic 'experts.'"
- Government Exhibit 809, page 8: "[tool from vendor report]—Bartender for [redacted] [vendor]."
- Government Exhibit 809, page 10: "Additionally, [Tool described in vendor report] is in fact Bartender. A CIA toolset for [operators] to configure for [redacted] deployment."
- Government Exhibit 809, page 11: "[@vendor] discovered [tool] in 2016, which is really the CIA's Bartender tool suite. Bartender was written to [redacted] deploy against various targets. The source code is available in the Vault 7 release." (Charge at 30)

With respect to Count Four, the government does not allege that Mr. Schulte transmitted anything—only that he "attempted" to transmit national defense information.

1. Element 1: Possession

For the same arguments detailed in Count Three (A.4), the government failed to prove beyond a reasonable doubt that Mr. Schulte unlawfully possessed tangible "documents"; Mr. Schulte should have been charged under the "information" prong of the statute, requiring the reason-to-believe scienter, and he should have been charged under section 793(d) for the *lawful* possession of information instead of section 793(e) for the *unlawful* possession of documents.

While here, the notebook entries for Malware of the Mind and the supposed planned "tweets" were tangible, the "information" prong still applies because the information derives from Mr. Schulte's head—not from any physical documents marked with classification designations. Indeed, "information" encompasses both tangible and intangible materials. "The phrase 'information relating to the national defense' is not defined by the statute, and therefore, as with any issue of statutory interpretation, the appropriate place to begin the analysis is with the plain meaning of the statute's words and the context in which they are used." *United States v. Rosen*, 445 F. Supp. 2d at 620; see also *United States v. Groce*, 398 F.3d 679, 681 (4th Cir. 2005). "The word 'information' is a general term, the plain meaning of which encompasses knowledge derived both from tangible and intangible sources." *Rosen* at 614. See, e.g., The American Heritage College Dictionary 698 (1993) (defining information as "knowledge derived from study, experience, or instruction" and "knowledge of a specific event or situation; intelligence.").

Moreover, the legislative history also confirms this definition of "information." The phrase "information relating to the national defense which the possessor has reason to believe could be used to the injury of the United States or to the advantage of a foreign nation" was added in 1950 to fix a potential loophole. See generally Edgar and Schmidt, Espionage Statutes, 73 Column. L. Rev. at 1021-31, 1050. "This formulation was not new, but was derived from similar language in section 2 of the Espionage Act, the predecessor to 18 U.S.C. § 794. As used in that provision, the term 'information related to the national defense' was understood to apply to information existing in both tangible and intangible form, and it is reasonable to conclude that the 1950 drafters intended to adopt the same meaning." *Rosen* at 616. Accordingly, "construing the term 'information' as including both tangible and intangible information is consistent with the plain meaning of the term and supported by the legislative history." *Id.*

Thus, here, even though the information was taken from Mr. Schulte's head and written in notebooks, since it is derived from an intangible source without any classification markings, it is still "information" requiring the reason-to-believe scienter. Accordingly, the Court must enter an order of acquittal on Count Four.

2. Malware of the Mind

The government alleged that Mr. Schulte "attempted" to transmit Malware of the Mind (GX 801) to unknown individuals at some unspecified time, and that this document he only ever shared with his attorneys, which discussed his case, somehow contained "national defense information."

Malware of the Mind is 145 pages long. It is a document that Mr. Schulte transmitted to his attorneys through paralegal Hannah Sotnick in March or April of 2018. See Tr. 1916. The government later seized Malware of the Mind from Mr. Schulte's legal work, searched every single page of the document, and claimed that page 84 of the 145-page document contained "national defense information" that Mr. Schulte "attempted" to transmit.

a) Element 2: National Defense Information

The government failed to prove that the Malware of the Mind document was national defense information. The government did not even ask a single CIA witness whether the information contained on page 84 was classified. Not a single CIA witness. Nor did a classification expert even testify at the trial. The information written on page 84 is far too generic to be classified—and without a testifying expert or even a single CIA witness to evaluate the paragraph, the government simply failed to prove that the Malware of the Mind information was even classified let alone national defense information.

b) Element 3: Attempted Transmission

To prove the charge of attempted illegal transmission of NDI, the Government must prove each of the following two elements beyond a reasonable doubt:

First, the defendant intended to commit the crime of illegally transmitting NDI; and

Second, the defendant did some act that was a substantial step in an effort to bring about or accomplish the crime. (Charge at 30)

(1) Intent to transmit

Mr. Schulte never intended to transmit Malware of the Mind to anyone. The government never presented any evidence indicating that Mr. Schulte intended to transmit Malware of the Mind in its entirety to any individual(s). In fact, the document's 145 pages strongly indicate that there was no possible way to transmit this document. How was Mr. Schulte going to transmit 145 pages? Type 145 pages into a cell phone?

The only part of Malware of the Mind that Mr. Schulte attempted to transmit was the first paragraph:

> *Today, we are facing a stealth constitutional crisis. A malware of the mind has entered and corrupted the justice system. Technology has advanced so rapidly that the law and law enforcement are decades behind and are unable to catch up. Into this chasm, defendant, defense attorneys, judges and juries are increasingly blindsided by the evolution of innovative prosecutorial techniques based on faux forensics, manipulation, and intentional misrepresentation, which are, in turn, nothing more than long-shot theories and in some cases blatant fabrications analogous to accusations of witchcraft and wizardry.*

This paragraph is unclassified, clearly related to the criminal justice system, and actually derived from Mr. Schulte's expert technical report for Mr. Amanat. See GX 1303-39 at 12 (Dated January 29, 2018 and predating Malware of the Mind). Moreover, it is clear from the notebooks that Mr. Schulte intended to rewrite "Malware of the Mind." See GX 809 at 8 ("Secondly, I want to rewrite article #10: Malware of the Mind!"). This entry was dated August 27. This task was never completed. Considering the significant time gap between when Malware of the Mind was completed and given to counsel in April of 2018 and October 1, 2018, when the government seized the document—7 full months—and not a single word of Malware of the Mind had ever been transmitted or scheduled for release, combined with the sole intention to rewrite

Malware of the Mind, the government completely failed to show that Mr. Schulte ever intended to transmit the document titled "Malware of the Mind" that was seized in October 2018.

(2) Substantial step to accomplish the crime

Not only was Malware of the Mind entirely unclassified and not intended for public dissemination, but there was also no substantial step taken to transmit it. Mr. Schulte first had to type 145 pages into a cell phone—which is practically impossible and never happened. Additionally, since Mr. Schulte intended to rewrite Malware of the Mind, it would first need to be rewritten before there could be any substantial step to transmit it—at which point the allegedly offensive page 84 would likely no longer exist. Accordingly, it was abundantly clear that no substantial step was ever taken to transmit Malware of the Mind.

3. Tweets

The government claimed that Mr. Schulte planned to release tweets containing national defense information to harm the United States. As with the first alleged "attempted transmission"—there was no actual transmission of anything These alleged tweets were never planned nor did they contain national defense information.

a) Element 2: National Defense Information

(1) Bartender exposed by WikiLeaks in March 2017

First, Bartender was released by WikiLeaks in Vault 7. It was public information for nearly two years before the alleged "draft tweet". (Tr. 1433 – Weber):

Q. *And the tools exposed by WikiLeaks were no longer used, correct?*
A. *At the time that is correct.*
Q. *The CIA tool Bartender was shut down, right?*
A. *The development for it was shut down, correct.*
Q. *I think as you testified earlier, it was previously – it was a tool that had been previously exposed, before WikiLeaks, right?*
A. *Correct.*

So it was not possible that anything about Bartender could possibly harm the national security of the United States—particularly considering Bartender had been shut down for nearly two years.

(2) Statement too generic to be classified

Next, the statement about Bartender is so generic that it cannot possibly be classified let alone national defense information. As an initial matter, CIA tool names are unclassified—so the name Bartender literally means nothing. If the CIA listed the names of its cyber tools, it would tell an adversary absolutely nothing about their functionality. See Tr. 1504-1505 – Weber:

Q. *All right. Let's move on to development. Project names by themselves are typically unclassified, correct?*
A. *The intention of the project name is for it to be unclassified.*
Q. *OK. Bartender, Margarita, Nader, you cannot tell what these tools do from the name, right?*
A. *That is the intention of the tool name, is to make it so that you can't -- you can't see what it does.*

So what was sensitive about the Bartender statement? See Tr. 1482-84 – Weber:

Q. *You testified on direct that disclosure on WikiLeaks gave you insight into the intentions of the tool, correct?*
A. *Potential insight, correct.*
Q. *And how witting the asset was to deploying it, correct?*
A. *If I recall correctly, the [Bartender Document] would have talked to that.*
Q. *And the [Bartender Document] was exposed by WikiLeaks, right?*
A. *I believe so, correct.*
Q. *The information specifically noted in the notebook, tool described in vendor report is in fact Bartender, CIA tool set for operators to configure for deployment; that statement is too generic to be classified, correct?*
A. *I have concerns about that statement. I would consider it to be classified because it points to an operator being witting to the usage of the tool.*
Q. *I think like you said earlier, you are not an expert in classification, correct?*
A. *I have been trained to make classification decisions on how it is outlined. I feel like the agency would that that is a classified statement.*
Q. *No. I was saying that you testified earlier that you are not a classification expert, correct?*
A. *No, I am not a classification expert.*
Q. *But, even so, the information here that you read, that information was all released by*

WikiLeaks, correct?
***A.** The information you just had me read was in your notebook.*
***Q.** Yes. That's correct. The question is that information was -- there is no new information in that statement from what WikiLeaks provided, correct?*
***A.** I would have to review what WikiLeaks put out but I believe -- I believe the [Bartender Document] would have made that statement.*

So, according to the CIA's own witness—who is not a classification expert—the Bartender statement in Mr. Schulte's notebooks were far too generic to be national defense information. And the only sensitive information disclosed in the notebooks was previously disclosed by WikiLeaks. Without testimony from a classification expert, the government simply failed to establish that the Bartender "tweets" were NDI.

b) Element 3: Attempted Transmission

The government alleged Mr. Schulte intended to transmit the tweet due to a page in his notebook that stated "19, 20, 21: schedule tweets 27th" (GX 809 at 15). But of course, it does not reference what tweets were to be scheduled. Additionally, the government testified that Mr. Schulte downloaded an application called "Buffer" for scheduling tweets. However, September 19, 20, and 21 came and went without any tweet scheduling. In fact, neither this Buffer account nor the twitter account were ever used. See Tr. 1864-65 – Schlessinger:

***Q.** You looked at the handle for Twitter, correct?*
***A.** Yes.*
***Q.** @freejasonbourne, correct?*
***A.** Yes.*
***Q.** And was there anything posted under that handle?*
***A.** Other than the picture, there was nothing.*
***Q.** You mean the photo of Matt Damon?*
***A.** Yes.*
***Q.** OK. But there were no tweets on there, right?*
***A.** No.*

See also Tr. 1932 – Schlessinger; see also DX 815:

***Q.** So this is a return from the Buffer account pursuant to your search warrant in October 2018, correct?*

A. *Yes. It appears to be a response from Buffer.*
Q. *Can you read this highlighted sentence?*
A. *Starting with: It appears?*
Q. *Yes.*
A. *It appears that this user signed up for our service on September 3rd, 2018, at which they linked a Twitter account but did not post any content through our service.*

So when was this attempt? When were these super damaging tweets to be posted? The government does not say. But, regardless, even if Mr. Schulte ever intended to post such tweets, he clearly changed his mind and did not do so. A conscious choice not to commit a crime, and the actions to support that choice prove that Mr. Schulte took no substantial step to "attempt" any such crime.

4. Information underlying Count Four cannot possibly constitute NDI since the government itself chose to disseminate it

Finally, the government went on and on about how the FBI showed up just in time to thwart Mr. Schulte and his attempts to wage a war against the United States and disseminate sensitive national defense information—and then the government itself publicly disclosed the very information it claimed was sensitive.

It is, in fact, the government who transmitted this alleged "national defense information" by presenting it in this criminal case. This fact strongly undermines the government's contention that this information was national defense information. If it were truly national defense information, the government would not have compromised it out of spite for a charge that already contains an actual transmission—let alone the additional WikiLeaks transmission charge itself. Would the CIA sacrifice information critical to the national defense of the United States for vengeance and spite? Of course not. See Tr. 1479 – Weber:

Q. *Through your experience at the CIA, the CIA has never deliberately exposed sensitive national defense information, correct?*

THE WITNESS: *I am not aware of a scenario where we have deliberately exposed sensitive -- I'm not aware of any scenario like that.*

Furthermore, it should be noted for the Court that the government abandoned introducing the Presnall Email that it litigated so ferociously to keep from being suppressed. The Presnall Email disclosed the location of Foreign Office West—a location publicly disclosed by WikiLeaks. And according to the government, the reason they abandoned this document was because "they could no longer protect the location" of Foreign Office West—which the government still considered classified. Accordingly, the only possible conclusion is that the information at the heart of Count Four is not classified—which is why the government does not mind "exposing" it to spitefully add an additional charge to the indictment against Mr. Schulte.

No, the information the government pretends is national defense information isn't even classified—it is generic, publicly available information that in no way endangers the United States. And without true classification experts to testify about the damage to national security of the information underlying Count Four—the government simply fails to show how this information is NDI.

C. Mr. Schulte knows real national defense information

As Mr. Schulte argued in summation, Counts Four and Five are sacrificial bunts—the government pretends unclassified, generic information is NDI just so it can introduce the prison notebooks and other prejudicial, inflammatory information solely to attack Mr. Schulte's character. It simply makes no sense at all that Mr. Schulte would choose such generic, obscure information to use in an "information war" to wage against the government—when in reality, he retains so much real national defense information that would be extremely damaging to the national security of the United States. Information that he could easily disclose despite his SAMs—including at the public trial itself in front of countless witnesses. If and when Mr.

Schulte ever decides to wage a war against the United States, he could easily cause true, catastrophic damage. See GX 3010:

> *As a result of the defendant's employment at the Central Intelligence Agency, he was privy to and remains aware of sensitive national defense information beyond what he is charged with disclosing or attempting to disclose in this case, the disclosure of which would be extremely damaging to national security.*

***

The MCC Counts are worse than a bad joke—they are both a selective and vindictive, malicious prosecution. There can be absolutely no question that Mr. Schulte did not believe his writings were sensitive, classified, or national defense information. Here, the government maliciously perverted the Espionage Act to use it as an offensive dagger to target Mr. Schulte rather than to protect the national security of the United States. Must Mr. Schulte live in absolute fear and terror that, for the rest of his life he better not write a single word, a single sentence—else the government may destroy his entire life?

If someone the CIA likes had written these statements, they would not have been prosecuted. Even if someone had accidentally disclosed classified information—the CIA still does not prosecute its own. But those the CIA dislikes—beware! The CIA and the government will pretend every sentence; every document you ever draft contains NDI.

This is not why Congress passed the Espionage Act. This is not why the Courts have upheld the Espionage Act. The government's MCC prosecution of Mr. Schulte is a despicable, reprehensible assault on the First Amendment, and an incorrigible perversion of the Espionage Act. Mr. Schulte should be acquitted of Counts Three and Four.

V. MR. SCHULTE SHOULD BE ACQUITTED OF THE CFAA COUNTS

> *The Computer Fraud and Abuse Act ("CFAA") imposes criminal and civil liability on one who, among other things, "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information... from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). "Without authorization" is not defined. However, "'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." Id. 1030(e)(6).*

United States v. Valle, 807 F.3d 508, 523 (2d Cir. 2015).

> *Let me turn, then to Counts Seven and Eight, each of which charges the defendant with causing the transmission of a harmful computer program, information, code or command.*
>
> *In order to find the defendant guilty of Count Seven or Count Eight, the Government must prove the following four elements beyond a reasonable doubt:*
>
> *First, that, on or about April 20, 2016, the defendant knowingly caused the unauthorized transmission of a program, information, code, or command to a protected computer;*
>
> *Second, that the defendant caused the transmission of the program, information, code, or command with the intent to damage or deny services to a computer or computer system;*
>
> *Third, that the defendant thereby caused damage; and*
>
> *Fourth, that the defendant's actions resulted in damage to a computer system used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.* (Charge at 37-38)

A. Mr. Schulte was the authorized owner of the ESXi server, possessing both the root primary key and the deed to the server

1. The email about verifying private key destruction related to the Atlassian servers

The government tried to pretend that an email Mr. Schulte sent about the Atlassian servers somehow implicated the ESXi Server. Specifically, in GX 1063, Mr. Schulte informs his division chief that he has "verified that all private keys with access have been destroyed/revoked." However, the subject of the email was "ISB infrastructure permissions transfer" and it was directly related to the transfer of the Atlassian products to ISB. See, e.g. GX

1064, a division-wide email sent 30 minutes later detailing the transfer of the Atlassian products to ISB. Indeed, Mr. Leonis testified that GX 1063 was directly related to the Atlassian products. See Tr. 620 – Leonis:

Q. *Just to clarify, the memorandum was specifically about the Atlassian products, correct?*
A. *It was about your admin privileges related to the Atlassian products, correct.*

Mr. Weber also confirmed that Mr. Leonis only specified the transfer of the Atlassian products. See Tr. 1578-79 – Weber:

Q. *Yes. You testified that you and ISB went out over the weekend, April 16, 2016, and removed all developer accesses to the Atlassian servers, correct?*
A. *We removed Atlassian administration access.*

[…]

Q. *OK. And this was specific to the Atlassian servers, right?*
A. *That is correct.*
Q. *You tested your keys to ensure they no longer worked, right?*
A. *That is correct.*
Q. *But you didn't remove your access to other, unrelated servers, right?*
A. *That is correct.*
Q. *You didn't remove your access to the Doxygen server, right?*
A. *Correct.*
Q. *Just the Atlassian products, right?*
A. *That is correct.*

And the Atlassian products were defined to be Stash, Confluence, Jira, Bamboo, and Crowd. See Tr. 1492 – Weber:

Q. *OK. But just to be clear, the Atlassian products we've heard about a lot -- Crowd, Stash, Confluence, Jira, Bamboo -- right?*
A. *Correct.*

Accordingly, the email from GX 1063 only related to the transfer of the Atlassian servers. It had absolutely nothing to do with the ESXi Server.

2. Mr. Schulte emailed Mr. Leonis about his continued access to the ESXi Server

Mr. Schulte directly emailed Mr. Leonis about his continued access to the ESXi Server. See GX 1071. See also Tr. 622 – Leonis:

Q. *OK. And this is also a notification to you, a request to transfer this to someone else; right?*
A. *Yes. Transfer the CMR to someone else.*
Q. *And my accesses too, right?*
A. *Yes. At the bottom it says "and my access."*

Mr. Leonis did not respond to the email and tell Mr. Schulte that he should not have access to the ESXi Server. In fact, the email demonstrates that Mr. Schulte maintained the ESXi Server in his CMR—that is to say, it was his accountable property. The CMR is essentially like the deed; Mr. Schulte was the owner and Point of Contact (POC) for the ESXi Server.

3. Nobody in OSB had the skillset to maintain the ESXi Server

Mr. Leonis does not respond to Mr. Schulte's email, nor does he remove Mr. Schulte's deed (CMR) or his accesses. And the primary reason was there were no others who had the skillset to maintain the ESXi Server. See Tr. 1578 – Weber:

Q. *OK. Right. You also testified on direct that ISB did not have any Linux administrators at that time, correct?*
A. *They -- they did not have anybody, to my knowledge, that was proficient in Linux.*
Q. *And you were not a Linux administrator either, correct?*
A. *That is correct.*

4. Mr. Schulte maintained his root key and the ESXi Server until he resigned

Mr. Schulte then continued to administer the ESXi Server up until his resignation. And in fact, according to the government's technical expert Mr. Leedom, Mr. Schulte's key remained on the Server—literally in the "Authorized Keys" file—until it was seized by the FBI following the WikiLeaks release. See Tr. 1052 – Leedom:

Q. *And it was on the ESXi server from the time I set it up in 2014 until the time I left the agency in November 2016, right?*
A. *I don't know the exact first date that it was -- it would have been on there but I know it was there when it was seized so it was still there.*
Q. *It was still there a year after I left?*
A. *I believe so.*
Q. *And this key is sitting on the ESXi server in plain sight, right?*
A. *The public key? Yes, it is an authorized keys file.*

5. The root ESXi key authorized any actions on the server

There was only one user account on the ESXi Server—the primary administrator or "root" account. See Tr. 1059 – Leedom:

Q. *So let's talk a little bit about the ESXi access in general. So you testified earlier I had my key on the ESXi server, correct?*
A. *Yes.*
Q. *And that's a root key, correct?*
A. *Yes. There is only, I think, one account on there.*
Q. *The primary administrator for the server, correct?*
A. *Yes.*

That primary administrator account authorized the user to perform any actions on the server. See Tr. 1059-60 – Leedom:

Q. *What types of commands are root users authorized to execute?*
A. *Pretty much everything.*
Q. *Anything, right?*
A. *Yes.*
Q. *By virtue root of server key the user is permitted to perform any command, correct?*
A. *Yes.*

***

As the owner and system administrator for the ESXi server—maintaining the primary key and the sole accountable property owner—Mr. Schulte had unlimited authorized access to the server. The government presented no evidence at trial that Mr. Schulte was ever informed not to exercise his administrative rights on the ESXi Server or that there were any policy or technical restrictions on system administrators.

B. Count Seven: Causing Transmission of Harmful Computer Program, Information, Code, or Command

> *In the case of Count Seven, the Indictment charges that the defendant transmitted commands on DEVLAN to manipulate the state of the Confluence virtual server on DEVLAN, including by (1) reverting the virtual server to a "snapshot," or past version of the system as it appeared on April 16, 2016; (2) restoring the system to a snapshot the defendant created on April 20, 2016; and (3) subsequently deleting the snapshot, thus erasing the records of his activities on the system.* (Charge at 38)

1. Element 1: Unauthorized Transmission of a Computer Program

> *The first element that the Government must prove beyond a reasonable doubt for purpose of Counts Seven and Eight is that the defendant knowingly caused the unauthorized transmission of a program, information, code, or command to a protected computer.* (Charge at 38)

The government failed to prove beyond a reasonable doubt that Mr. Schulte caused the unauthorized transmission of a program, information, code, or command to a protected computer. As has already been establishes in V.A., Mr. Schulte held both the CMR (i.e. title or deed) and the root key (authorized administrator access) to the ESXi Server. This root key authorized Mr. Schulte to perform any and all ESXi functions on the virtual machines. See Tr. 1493-94 – Weber:

Q. *OK. Well, you testified on direct that the ESXi server administrator doesn't have, necessarily have access to the VMs, right?*
A. *That would be my understanding. That's correct.*
Q. *OK. And that's set up because the ESXi administrator, his role, I think, that you testified he's only -- his role is a physical component, correct?*
A. *For how that translated into virtual environment, that's correct.*
Q. *OK. So you can't, with a root server key on an ESXi server, you can't access the virtual machines just with that, right?*
A. *Not within the virtual machines. That's my understanding.*
Q. *OK. But the role of that ESXi system administrator is, essentially encompasses power-offs, power-ons, snapshots, reversions, right?*
A. *That is my understanding. That is correct.*

It is the ESXi Server Administrator's job to perform snapshots and reversions. This job extends to all virtual machines under the ESXi Server—regardless of whether or not he has access to those virtual machines themselves. In fact, in the typical enterprise environment, the

ESXi Server Administrator does not have access to any of the virtual machines, but only manages the ESXi Server itself. See Tr. 1060-61 – Leedom:

Q. *So you can be a root user of the ESXi server and have no access to the VMs, correct?*
A. *Yes. That's correct.*
Q. *The virtual machines control their own access, correct?*
A. *They do.*

Accordingly, Mr. Schulte was authorized to perform snapshots and reversions on the Confluence Virtual Machine.

2. Element 2: Intent to Cause Damage or Deny Service

> *The second element that the Government must prove beyond a reasonable doubt for purpose of Counts Seven and Eight is that the defendant caused the transmission of the program, information, code, or command at issue with the intent to cause damage. (Charge at 39)*

Taking snapshots and reversions are typical administrative functions that are not inherently harmful like a computer virus or malicious action. See Tr. 1033 – Leedom:

Q. *So you know the process of taking a snapshot is a common system administration, correct?*
A. *Yes. I think I've said that too in previous testimony.*
Q. *OK. Taking a snapshot's not an inherently harmful computer command, correct?*
A. *No.*
Q. *The process of reverting a snapshot is also a common system administration, correct?*
A. *In some circumstances, yes.*

See also Tr. 1034 – Leedom:

Q. *But it's still, it's still common to run this in system administration practices, correct?*
A. *Like I said, for some instances, yes, you would revert a virtual machine.*
Q. *If you're going to, if you need to roll back a system, right?*
A. *Yes.*
Q. *And deleting a snapshot is not an inherently harmful computer command, correct?*
A. *No.*

Accordingly, since snapshots and reversions are typical procedures, there was absolutely no intent to cause damage to the Confluence Virtual Machine.

3. Element 3: Causing Damage

> *The third element that the Government must prove beyond a reasonable doubt for purpose of Counts Seven and Eight is that by transmitting the program, information, code, or command at issue, the defendant caused damage. 'Damage' means any impairment to the integrity or availability of data, a program, a system, or information.* (Charge at 40)

The snapshot, reversion, and snapshot deletion did not cause any damage to the Confluence Virtual Machine. The initial snapshot on April 20, 2016 saved the state of the Confluence VM. This allowed the machine to be safely reverted so it could return to the April 20, 2016 state later. The reversion to April 16, 2016 did not cause any damage to the system since the April 20, 2016 state was preserved. The final reversion back to the April 20, 2016 state not only did not cause any damage, but was in fact *necessary for the integrity of the Confluence VM*. If Mr. Schulte failed to execute the final reversion back to the April 20, 2016 snapshot, then all the data created or modified on the Confluence VM between April 16, 2016 and April 20, 2016 would have been lost. Damage could only be caused by *failing to execute that final reversion*. And finally, deleting the April 20, 2016 snapshot did not cause any damage to the system—it existed solely to save the state of the VM on April 20, 2016, so this state could be resumed. After this state was resumed, the snapshot was no longer necessary—no data was lost be deleting this snapshot since the system resumed from that very snapshot prior to its deletion. Accordingly, the snapshot/reversion/deletion caused no damage to the Confluence VM.

4. Element 4: Harmful Consequences

> *The fourth element that the Government must prove beyond a reasonable doubt for purpose of Counts Seven and Eight is that the defendant's actions disrupted a computer system used by or for any government agency in furtherance of the administration of justice, national defense or national security.* (Charge at 40)

The government failed to prove any harmful consequences from the snapshot or reversion itself. The Confluence VM resumed normally from the April 20, 2016 snapshot—no data was lost. There were no complaints from any users, and in fact, no one even noticed that the snapshot or reversion took place.

C. Count Eight: Causing Transmission of Harmful Computer Program, Information, Code, or Command

In the case of Count Eight, the Indictment charges that the defendant transmitted commands on DEVLAN to delete log files of activity on DEVLAN. (Charge at 38)

1. Element 1: Unauthorized Transmission of a Computer Program

The government failed to prove beyond a reasonable doubt that Mr. Schulte caused the unauthorized transmission of a program, information, code, or command to a protected computer. As has already been establishes in V.A., Mr. Schulte held both the CMR (i.e. title or deed) and the root key (authorized administrator access) to the ESXi Server. This root key authorized Mr. Schulte to perform any and all commands on the ESXi Server—including deleting files. See Tr. 1060 – Leedom:

Q. *By virtue root of server key the user is permitted to perform any command, correct?*
A. *Yes.*
Q. *The root key authorizes users to install programs, correct?*
A. *Yes.*
Q. *Root key authorizes the user to update the system, correct?*
A. *Yes.*
Q. *And root key authorizes the user to delete files, correct?*
A. *Yes. It will let you do pretty much any kind of administrative action.*
Q. *So the root user can technically reformat or completely wipe the system, right?*
A. *Yes, if they chose to do so.*

Mr. Schulte could have wiped the entire ESXi Server—and it would have been an authorized command. Deleting files is an authorized command for a server administrator.

2. Element 2: Intent to Cause Damage or Deny Service

The government failed to prove beyond a reasonable doubt that Mr. Schulte intended to cause damage or deny a service by deleting log files.

3. Element 3: Causing Damage

The government failed to prove beyond a reasonable doubt that Mr. Schulte caused any damage by deleting log files. The government experts could not say whether or not the log files were corrupted or contained any viable data. See Tr. 1073 – Leedom:

Q. *Were you able to review the contents of any of the log files?*
A. *Yes.*
Q. *The content -- I'm sorry -- of the unlinked log files?*
A. *I don't believe -- I think there was some file side from shell.log, but I don't believe there was any from the others.*

Furthermore, there was no activity that the logs would have captured that wasn't already recorded by the transcript files. See Tr. 974-75 – Leedom:

Q. *And you know all these very specific times on your timeline from the transcript files, right?*
A. *There are still estimates, I would call them very specific estimates, but yes.*
Q. *I mean, the point is there is no -- there is no files that were deleted or activity that was executed that is not – that you didn't find transcript files for, right?*
A. *Included in the timeline here as far as everything on the bottom? Everything on the bottom here comes from transcript files aside from the vault stuff.*

Accordingly, there was no damage to the ESXi Server.

4. Element 4: Harmful Consequences

Finally, the government did not prove beyond a reasonable doubt that there were any harmful consequences from the log file deletions. The government does not establish the system policy for log file deletions. See Tr. 1579-80 – Weber:

Q. *OK. Just briefly, you testified about deleting log files on direct, correct?*
A. *I testified if it made sense to delete log files.*
Q. *Specifically, you said that deleting old log files is something that happens, right?*
A. *I stated that standard practice often was setting upper limits on the age of the log files or the total size of the log files.*

But what was that policy? Would they have deleted those April 20, 2016 log files in December of 2016? Or January of 2017? At what point would those files have been discarded?

The government never defines the policy. But they certainly would have been deleted long before the WikiLeaks disclosure on March 7, 2017—so they would not have been available for the forensic experts in any case.

***

The CFAA was intended to target computer hacking, not second-guess authorized system administrators. See, e.g. *United States v. Valle*, *supra*; *Van Buren v. United States*, 141 S. Ct. 1648 (2021). If a system administrator damages a server due to incompetence, a mistake, or even deliberate malfeasance—this is an employer-employee problem, not computer hacking or a violation of federal law. Here, it is abundantly clear, even reviewing the evidence in the most favorable light to the government, that Mr. Schulte possessed the deed and administrator access key to the ESXi Server; he literally emailed his division chief and told him about these accesses. The CIA's failure to remove Mr. Schulte's accesses—even after Mr. Schulte directly informed them of his continued access—constitute permission and authorized access. Mr. Schulte should be acquitted of Counts Seven and Eight.

VI. MR. SCHULTE SHOULD BE ACQUITTED OF COUNT NINE

Count Nine charges the defendant with obstruction of justice.

In order to find the defendant guilty of Count Nine, the Government must prove the following three elements beyond a reasonable doubt:

First, that, between March and June of 2017, there was a proceeding pending before a federal court or grand jury;

Second, that the defendant knew of the proceeding; and

Third, that the defendant corruptly acted to obstruct or impede, or endeavored to obstruct or impede the proceeding. (Charge 40)

Specifically, Count Nine charges that between March and June 2017, the defendant made certain false statement to agents of the FBI during their investigation of the WikiLeaks leak.

A. Element 1: Pending Proceeding

The first element that the government must prove beyond a reasonable doubt for purpose of Count Nine is that, between March and June of 2017, there was a proceeding pending before a federal grand jury or a federal court. (Charge at 41)

The government established that there was a subpoena issued to Mr. Schulte at the conclusion of the FBI interrogation on March 15, 2017 to appear before a grand jury on March 17, 2017. However, the government failed to establish what happened with that subpoena or whether the grand jury continued to operate into June of 2017.

B. Element 2: Knowledge of Pending Proceeding

The second element that the Government must prove beyond a reasonable doubt for purpose of Count Nine is that the defendant knew that such a proceeding was in progress when he corruptly acted to obstruct or impede the proceeding. (Charge at 41)

The government only established that Mr. Schulte knew a grand jury would convene on March 17, 2017. The government never established that Mr. Schulte knew what a grand jury was, much less that it would convene through March, April, May, and June of 2017. The government wholly failed to prove Mr. Schulte had any knowledge of any pending proceeding.

C. Element 3: Obstruction of the Proceeding

> *The third element that the Government must prove beyond a reasonable doubt for purpose of Count Nine is that the defendant did corruptly obstruct or impede, or corruptly endeavored to obstruct or impede the proceeding at issue. (Charge at 42)*

Mr. Schulte did not obstruct the grand jury—he had no knowledge there was a grand jury, he never attended the grand jury, and he was never told that his statements to the FBI would be brought before the grand jury; regardless, his statements to the FBI were true. The government wholly failed to show how Mr. Schulte corruptly obstructed, impeded, or endeavored to obstruct or impede any proceeding.

Specifically, with respect to the alleged lies surround the OIG Email, they could not have possibly obstructed the grand jury since the FBI determined that Mr. Schulte was mistaken shortly after Mr. Schulte made those statements—and before the FBI could even report to a grand jury.

Finally, Mr. Schulte could not have known about the pending grand jury or endeavored to obstruct it before the FBI served him the grand jury subpoena. Accordingly, any and all alleged false statements before this period cannot be considered.

None of the seven alleged statements obstructed any judicial proceeding:

1. He denied having any involvement in unlawfully disclosing the Backup Files

This is a true statement. See VII.

2. He stated that he had not kept a copy of an email he sent to the Office of Inspector General containing false allegations of security issues at the CIA

Mr. Schulte told the FBI that he did not keep any classified information at his home—and at the time the FBI did not tell Mr. Schulte the classified email they were referencing was an email that Mr. Schulte had labeled “unclassified” but the CIA had later determined was “confidential.” Regardless, this statement was made before Mr. Schulte was informed of the grand jury, and could not have possibly obstructed the grand jury since the FBI shortly thereafter recovered the “classified” OIG email.

3. He denied having any classified materials in his apartment

See, *supra*. Mr. Schulte could not have possibly known the OIG email was classified—especially since he labeled it unclassified.

4. He denied ever taking information from the CIA and transferring it to an unclassified network

The government did not present any evidence that such a question or answer was ever given.

5. He denied ever making DEVLAN vulnerable to the theft of data

The government did not present any evidence that such a question or answer was ever given. FBI Agent Evanchec stated that he asked Mr. Schulte, “Did you make the system vulnerable to compromise?”, which is a different question and is also ambiguous—which system? The ESXi Server? A virtual machine? The entire DevLAN network? In any case, Mr. Schulte did not make the DevLAN network vulnerable to theft.

6. He denied housing information from the CIA on his home computer

The government did not present any evidence that such a question or answer was ever given. In any case, it is a true statement—the government provided absolutely no evidence that Mr. Schulte ever housed information from the CIA on his home computer.

7. He denied ever removing any classified information from the CIA and taking it home.

The government did not present any evidence that such a question or answer was ever given. In any case, it is a true statement—the government provided absolutely no evidence that Mr. Schulte ever removed any classified information from the CIA and took it home.

***

Accordingly, the Court should acquit Mr. Schulte of Count Nine.

VII. MR. SCHULTE SHOULD BE ACQUITTED OF THE WIKILEAKS ESPIONAGE COUNTS

The government alleged in its case-in-chief that Mr. Schulte used his root administrator key to access the ESXi server on April 20, 2016. At 5:35 p.m. Mr. Schulte reverted the Confluence Virtual Machine to an April 16th snapshot; the reason for this reversion is that the April 16th snapshot of the Confluence VM still contained Mr. Schulte's administrator root key that was later deleted; by reverting to the snapshot Mr. Schulte would have administrator access to the Confluence VM that he otherwise would not possess. The Confluence VM remained in this reverted state until 6:51 PM. During this 1 hour and 15-minute timeframe, Mr. Schulte copied the Stash and Confluence backup files containing approximately 200 GiB and 3 GiB respectively. From 5:55 to 6:58 PM, Mr. Schulte deleted log files of these activities.

A. The altabackups directory containing the backups had no access controls

The government's theory of theft relies entirely upon the predicate that the altabackups directory was locked down. If the altabackups were not locked down, then the snapshot-reversion theory is entirely irrelevant. If anyone can just open up the altabackups directory and copy the files, then there is no need to execute the snapshot-reversion to copy the files. See Tr. 949 – Leedom:

Q. *And it's fair to say that if one could access the directory shown in 1207-36, then a snapshot reversion is irrelevant, correct?*
A. *Yes.*

The access controls of the altabackups directory are critical to the government's case. Tr. 959 – Leedom:

Q. *You would agree that the access controls to Altabackup are critical, right?*
A. *Yes.*

The altabackup directory was setup with wide-open permissions such that anyone could access, copy, and steal the backups. All of the CIA employees who managed that altabackup directory told the FBI that this directory had no access controls. See, e.g. 3515-506 at 3 (Question 6: What permissions were set on Altabackup? A: There were none.). Furthermore, they indicated that AFD determined there were no access controls on the altabackup directory. It was only after the government decided upon a theory of prosecution that all the CIA witnesses changed their stories—each and every one of them changed their story from "there were no access controls on altabackup" to "there were some access controls on Altabackup, but I do not remember them."

The altabackup access controls are maintained within its own directory structure. Mr. Leedom testified about the access controls for some of these directories—See GX 1207-49-1207-52—but claimed none existed for the altabackup directory. The Court denied all discovery requests for the Altabackup server to independently conduct analyses on the access controls; accordingly, the defense could not cross-examine Mr. Leedom about these access controls, and were compelled to take his tests and analyses—whatever they were—as the gospel truth. See Tr. 952-53 – Leedom:

Q. *I'm just asking specifically during this type, April 2016, what were the access controls? Do you have a document that shows what the access controls were for that directory?*
A. *Altabackup in 2016?*
Q. *Yes.*
A. *No, no. You have to talk to, I guess, ISB. They were managing it at the time. But there's no, like, historical audit for the NetApp for -- for that.*
Q. *So you have no -- you have no ability to testify about what access controls existed on this directory in 2016, is that correct?*
A. *No, because we can use things -- like, when you attempted to mount it on the ESXi server and we saw that that failed, that shows that there was access control enabled on that share.*
Q. *We'll go into the data store in a little bit, but essentially, you're not relying on any document or any technical access control list; you're just inferring from what you've reviewed, is that*

correct?
A. *Right. You got to look at everything as a whole.*

Mr. Leedom could basically say anything he wanted without fear of cross examination, because he knew the defense never had access to the servers—and could not possibly know the answers to any of the questions.

1. Regular user could not execute a mount or datastore command

And how did Mr. Leedom establish access controls for the altabackup directory? He concluded there were access controls because a non-privileged user failed to mount the altabackup directory on the ESXi Server—a failure that had nothing to do with access controls on altabackup. See, GX 1703 at 57 ("SCHULTE LOGGED IN TO VMWARE-CLIENT AS REGULAR USER"), 58 ("SCHULTE ATTEMPTS TO CREATE A DATASTORE TO THE ALTABACKUPS"), 59 ("SCHULTE'S ATTEMPT FAILS").

Mr. Leedom himself acknowledged that creating a datastore, which is the same thing as mounting a remote directory, required administrator access:

Q. *OK. Creating a data store is a typical administrative function, right?*
A. *Yeah, it's something you would do to manage the – manage the server.*

So what does Mr. Leedom say to the fact that the error occurred because a regular user does not have the authority to mount or create datastores? He punts, knowing that, once again, the defense cannot cross examine him because we never had access to any of the servers at issue here. See Tr. 955-56 – Leedom:

Q. *So the failure to create the data store could and most likely occurred because a regular user simply does not have access to perform the mount, correct?*
A. *Well, the type of error that we received -- if you go back to the other --*
Q. *Well, no. I'm just asking based on this. If you're a regular user, you're not going to have the ability to be creating and mounting directories, right?*
A. *I'm not sure exactly, because there -- I don't think I had, like, audit for the user individually, like, at that level on that server. So I don't know if there's, like, a, you know, an explicit*

permission for data store management or not. But from the type of error that is shown, it leads me to believe that's more of a -- the NFS server actually denied the request and not the ESXi server saying you don't have the correct permission to, you know, create a data store. It was a -- the NFS server itself said I'm not going to let you do this, if that makes sense.

Mr. Leedom claims that he didn't "have audit for the user individually" and doesn't know if there is "an explicit permission for data store management or not." But of course, he had access to that information. The defense did not. So, that's it—by asserting he doesn't remember or doesn't know, Mr. Leedom earns a free pass on cross-examination. See VIII.A.5.

2. Even if datastore failed due to access controls on altabackup, error message does not indicate what those access controls are

Mr. Leedom agreed that, even if the datastore failed due to access controls, the error message does not indicate what those access controls were. See Tr. 956 – Leedom:

Q. *But it also doesn't say that -- it doesn't say anything about what or how much access controls the NFS server even has, right?*
A. *No. That wouldn't be in an error message.*

The access controls could be extremely light. They could simply deny anyone access to the altabackup directory who is not on that server's subnet. Most DevLAN users were on the altabackup's subnet, and therefore would be able to access the altabackups. OSB, however, had its own subnet—which is where the ESXi Server was located. See Tr. 957 – Leedom:

Q. *OK. But the configuration for the NFS could simply be not to share with this subnet or to only share within its own subnet, right?*
A. *Could be. That's kind of how, one way you could set up the allow list. You can say block a whole subnet. You can say only allow certain IPs.*

Basically, Mr. Leedom is just guessing what the altabackups permissions are based upon what is most beneficial for the government's case. But his guess as to the altabackups access controls is not based on a single piece of evidence—it is literally just that—a baseless guess.

3. Trial testimony suggests there were no access controls

Testimony from Mr. Weber suggests the opposite—that there were no access controls on altabackup. See Tr. 1524 – Weber:

Q. *All right. I want to talk a little bit about your testimony on direct about the mount command. Do you remember that?*
A. *Yes, I do.*
Q. *OK. So you testified on direct about using this mount command in your VM, correct?*
A. *That's correct.*
Q. *And this mount command is necessary in order to access the Altabackups, correct?*
A. *I believe that to be accurate.*
Q. *OK. And can you -- well, your VM is located on your computer, right?*
A. *That's correct.*

If Mr. Weber were using the mount command in his VM, then there cannot be any access controls on the altabackup directory.

Without access to the forensic crime scene, the entire DevLAN network, the defense could not conduct a similar analysis as Mr. Leedom, and search for regular DevLAN users mounting the altabackup directory—such as activity from Mr. Weber's VM. Because, if what Mr. Leedom claims were true, if the access controls no longer existed, then the forensic examiner must conduct a forensic examination of every single computer connected to DevLAN to hunt for clues as to what those permissions were—if any existed. Mr. Leedom performed this analysis. But the defense could neither cross-examine Mr. Leedom's results or conduct its own forensic examination—such as search for user activity, error logs, audits, or anything else that may give clues as to the access controls on the altabackup directory. See VIII.A.6.

***

Mr. Leedom testified that the access control list from April 2016 was not preserved. Mr. Leedom presented no forensic evidence that the altabackup directory was restricted in any way.

Mr. Leedom presented no forensic evidence for what the permissions and access controls were in April 2016. See Tr. 961 – Leedom:

Q. *OK. Just to be clear, for the access controls here, you have no documentation or no configuration files showing the exact access controls, right?*
A. *We do not have a configuration file for Altabackup from the NetApp that, like, shows the -- the allow or block list. It just wasn't available at the time.*

See also Tr. 1091 – Leedom:

Q. *But the access controls were lost before you were able to recover them, correct?*
A. *To some extent they were, yes.*
Q. *I mean you never recovered any access controls for the Altabackup, correct?*
A. *I think we had to, like, for the folder, like, you had to be root to access the folder. But all of the allow listing, IP address information for the config, we didn't have that.*
Q. *OK. So sitting here today, you don't know what the permissions on those allow and deny lists were, correct?*
A. *Correct.*

Without access controls, every DevLAN user could access and copy the altabackup directory. There would be absolutely no reason to perform a snapshot-reversion. Even considering this evidence in the most favorable light for the government, the government simply failed to present sufficient evidence that there were strict access controls preventing DevLAN users from directly accessing the altabackup directory; no rational, reasonable juror could possibly infer that the altabackup directory was restricted.

B. Timing Analysis can only establish a lower-bound

Both Stash and Confluence employ version control to keep track of all iterations for each file. See Tr. 985-86 – Leedom:

Q. *When the underlying Atlassian data from the servers is modified or deleted, a record of those changes is created, correct?*
A. *Yes; in the database.*
Q. *This allows a user to review all the changes over time, right?*
A. *For the most part, yes.*
Q. *This is sort of like tracked changes in Microsoft Word or in Google Docs, correct?*
A. *Yes.*

Q. *The user essentially has access to all prior versions of the data, right?*
A. *I believe so.*

Every time you modify a file, that change to the file is saved. And what this means is every successive backup contains all the data from all preceding backups. March 4th contains the data from March 3rd plus the new changes. So, it's really trivial to go through the data and select files from a particular date. See Tr. 986-87 – Leedom:

Q. *And each successive backup contains the data of all the prior backups, right?*
A. *To some extent.*
Q. *Due to the version control feature the backups are going to contain all the data preceding it?*
A. *In a general sense.*

The forensics can only establish one thing—what's called a lower-bound. This is the earliest backup that could have been taken. And the reason forensics can establish this, is because an old backup cannot possibly have new files. A backup taken on March 3, 2016, cannot contain files from March 4, 2016—those files haven't been created yet. So, if you have files from March 4th, then you can establish that March 4th is the lower-bound—it is the absolute earliest backup that could have been taken. See Tr. 988-89 – Leedom:

Q. *So if you have a commit log from Git all the way to March 7, 2017, right?*
A. *Assuming it is in tact and wasn't ever edited.*
Q. *OK, you could go back and select the commit from March 3rd?*
A. *You could. If it was there, yes, you could go back and --*
Q. *And Git makes this trivial to do, right?*
A. *It is easy to do.*
Q. *You testified that it may take some time to do this for Confluence, right?*
A. *Yes.*
Q. *And you also testified that sifting through the corrupt database would have also taken a lot of time, right?*
A. *Yeah. From my experience working with it, yes, it would have.*
Q. *And according to you, WikiLeaks spent the time to retrieve content from the corrupt database, correct?*
A. *Yes.*
Q. *They exerted that effort to do so, right?*
A. *It appears so. From what they posted and what is in the database, yes.*

See also Tr. 1185 – Berger:

Q. *So if you have this backup from March 7, 2016, at the end, right, you could go back to February 26, 2016? Correct?*
A. *Technically possible, yes.*
Q. *Well, it's very easy to do that in Git, correct?*
A. *Easier than Confluence, correct.*

But the reverse is not true—a new backup can, and does, contain old files. This is why no upper-bound can be established. If you have files from March 4th, they could come from any backup on or after March 4th. So a timing analysis for version-controlled backups is very limited. It can establish only a lower-bound. And in this case, the lower-bound is March 3, 2016. The data released by WikiLeaks could originate from each and every backup from March 3, 2016 to March 6, 2017.

Even considering this evidence in the most favorable light for the government, the government simply failed to present sufficient evidence that WikiLeaks possessed the March 3, 2016 backup file—instead of any file between March 3, 2016 and March 6, 2017; no rational, reasonable juror could possibly infer that this backup, and only this backup, was provided to WikiLeaks.

C. Count One: Illegal Gathering of National Defense Information in violation of 18 U.S.C. § 793(b)

> *Count One charges the defendant with illegal gathering of national defense information or "NDI." Specifically, it charges that, on or about April 20, 2016, the defendant, without authorization, copied backup files of certain electronic databases housed on a classified computer system maintained by the CIA.* (Charge at 20)
>
> *In order to find the defendant guilty of Count One, the Government must prove the following three elements beyond a reasonable doubt:*
>
> *First, that on or about April 20, 2016, the defendant copied, took, made, or obtained a sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note;*
>
> *Second, that the information in that material was connected to the national defense; and,*

> *Third, that the defendant acted with the purpose of obtaining information respecting the national defense and with the intent or with reason to believe that the information was to be used to the injury of the United States, or used to the advantage of a foreign country.* (Charge at 22)

The government proved Mr. Schulte's innocence of Count One in its case. The government claimed that Mr. Schulte copied the Stash and Confluence backup files utilizing the Confluence VM on April 20, 2016. The government presented evidence of all the commands that Mr. Schulte allegedly ran during that day including log deletions. However, nowhere within those commands was a remote login to the Confluence VM that was required to initiate the copy command nor was there a copy command. The government's case fails because it proves that it was impossible for Mr. Schulte to copy the information within the tiny window it manufactured—a fact it completely ignored throughout the trial.

The government's case is impossible for three primary reasons: (i) throughout the completely intact logs obtained from Mr. Schulte's CIA Workstation, there were no logins to the Confluence VM or copies from that VM; (ii) there were provably no drives connected to Mr. Schulte's CIA workstation during the copy period for Mr. Schulte to exfiltrate the data; and (iii) the government failed to show the bandwidth of the DevLAN network and whether it was even possible to exfiltrate 203 GiB in 75 minutes.

1. The completely intact logs from Mr. Schulte's CIA workstation prove there were no Confluence logins or copies

Mr. Leedom found transcript files from Mr. Schulte's CIA Workstation, and from these transcript files discovered the deletion of log files from the ESXi server and other activity that he attributed to Mr. Schulte. The government has a perfectly intact detailed picture of all the activity from Mr. Schulte's CIA Workstation during the 75-minute window of the alleged copy (including the before and after). The government details all of these commands through its exhibits GX 1203-XX and on Mr. Leedom's slideshow. There was no command to log into the Confluence VM nor any commands to copy any file from it. See Tr. 900-01 – Leedom:

Q. *And at no point in this exhibit or your forensic findings is any forensic artifact of a login to the Confluence virtual machine, correct?*
A. *I believe that's correct.*
Q. *At no point in Exhibit 1703 or your forensic findings is any forensic artifact that a copy command issued to copy the backups, correct?*
A. *That's correct.*
Q. *And, at no point in your Exhibit 1703 or your forensic findings is any forensic artifact of a CIA backup file copied to any of my devices from the CIA, correct?*
A. *I believe that's correct.*

See also Tr. 973 – Leedom:

Q. *You did a complete forensic analysis on the work station, right?*
A. *That's correct.*
Q. *You looked for a copy command during the reversion period, right?*
A. *Yes.*
Q. *Looked high and low, right?*
A. *That's correct.*
Q. *You did not find a copy command during the reversion, correct?*
A. *No.*
Q. *You did not find any logins to the Confluence virtual machine during the reversion, correct?*
A. *No, not that I believe.*

The reversion of the Confluence VM had absolutely no effect on the transcript logs from Mr. Schulte's CIA Workstation. See Tr. 969 – Leedom:

Q. *But of course, reverting or deleting the Confluence virtual machine has absolutely no effect on transcript files from my own CIA workstation, correct?*
A. *That's correct. If we're calling those -- the exhibits of all the commands, if that's what we're calling transcript files, we can call them that.*
Q. *OK.*

The transcript files logged every single command Mr. Schulte ran from his computer—including commands to log into remote computers and execute commands on those remote computers. This is clearly obvious from the transcript files showing log deletions and other commands executed on the ESXi Server—it is not the ESXi Server that logged these commands, but Mr. Schulte's CIA Workstation. So, if Mr. Schulte logged into the Confluence VM and executed commands, that activity would show up in two places—logged by the Confluence VM, which executed the commands, and from Mr. Schulte's computer, which issued the commands. Thus, even if the Confluence VM is reset by a reversion, and those logs were lost, that second log from the transcripts on Mr. Schulte's computer would remain. See Tr. 899 – Leedom:

Q. *That's not the question. The question is you recovered these log files from my virtual machine, correct?*
A. *That's correct.*
Q. *So if I -- if there was a command to log into the Confluence virtual machine from here and/or copy commands from the Confluence virtual machine that I would be running from my computer, right?*
A. *Yes.*
Q. *Those would not have been affected by the reversion, they would be found here, right?*
A. *Yeah. They could show up here. It is tough to say, like, exactly what would show up here because this is obviously, like, unallocated space and deleted data so it's not a hundred percent, but in this general type area are the logs from the VM, similar.*

Since the transcript files are logged from Mr. Schulte's own CIA Workstation—they are preserved no matter any snapshot or reversion. See Tr. 971 – Leedom:

Q. *I mean, if we look at this, you know, this was -- if this was a server, a virtual server and it was reverted, these files would remain on my work station, right?*
A. *Yes, because it came from your virtual machine.*
Q. *So the point is anything that you do to another server or another system is not going to affect logs or documents being produced on this work station, right?*
A. *That's correct.*
Q. *OK. Essentially since the source of these transcript files is my CIA work station, they are preserved no matter any snapshot or reversion, right?*
A. *Correct.*

Mr. Leedom's only counter is to say he would expect to see a command to log into the Confluence VM and then a copy command from within the Confluence VM itself—instead of a copy command from outside the VM. But regardless, if any such commands were executed, they would exist in the transcript files—the logs of activity from Mr. Schulte's CIA Workstation. See Tr. 899-900 – Leedom:

Q. *But you looked or you expected or you wanted to find a copy command from those logs, right?*
A. *I think if there was a copy command it would have been like in the virtual machine itself, not like outside of it.*
Q. *Then there would have been a login to the virtual machine, correct?*
A. *Yeah, at some point.*
Q. *Even the copy from the virtual machine itself, right, that would be taking place from my workstation computer, correct? Just like this. This is from the ESXi server, correct?*
A. *Correct.*
Q. *The ESXi server is not my virtual machine, correct?*
A. *That's correct.*
Q. *My login for my virtual machine to the ESXi server, correct?*
A. *Correct.*
Q. *OK. So on that same token, if I were to log into the Confluence virtual machine, you would see logs of Confluence on here as well, correct?*
A. *Yeah. If you did it from your -- like from your VM, yeah.*
Q. *Where else would I do it from?*
A. *I don't know.*
Q. *OK.*

DX 1209 proves Mr. Schulte's innocence beyond any and all reasonable doubt. If Mr. Schulte ran a copy command or a login command, it would be logged by his CIA Workstation. The only activity from Mr. Schulte's CIA Workstation shows Mr. Schulte log into the ESXi Server and execute commands from the ESXi Server. Specifically, Mr. Schulte executed an "ls" command at 5:29 PM. See GX 1203-1, GX 1703 at 92-93, DX 1209 at 1-4. **HE THEN ISSUES NO OTHER COMMANDS FROM HIS CIA WORKSTATION UNTIL 5:55 PM.** This is confirmed by DX 1209, which lists the very next command executed—another "ls" command—at 5:55 PM. See DX 1209 at 4-7, GX 1203-29, GX 1703 at 115-116. See Tr. 965-66 – Leedom:

MR. SCHULTE: *I move to introduce defense exhibit 1209 into evidence.*
MR. DENTON: *No objection.*
THE COURT: *Admitted.*
(Defendant's Exhibit 1209 received in evidence)
BY MR. SCHULTE:
Q. *And this is a transcript file showing remote access to the ESXi server, correct?*
A. *This is -- I believe this was recovered from unallocated space on your virt. machine.*
Q. *It's from the CIA workstation, but it's showing remote access on the ESXi server, right?*
A. *That's correct.*
Q. *And it's recording the commands as they're being typed from the workstation, correct?*
A. *Yes.*

Q. *OK. The first command executed here is LS-ALTR, correct; it lists the files?*
A. *That's correct.*
Q. *And this is the, you're basing it off the shell log, and it's showing it's 5:29, correct?*
A. *Yes. If this is the end of the, of the previous command, then yes, that's how I would have time stamped that.*
Q. *This is right at the beginning of your time line, right?*
A. *At 5:29? Yes.*
Q. *Yeah. All right. And the very next command is another LS-ALTR, right?*
A. *Yes, it is.*
Q. *And this command is 5:55 p.m., correct?*
A. *Yes, it appears to be.*
Q. *And this is after the backups are supposedly accessed, right?*
A. *I believe so.*

No command was executed when the backups were accessed at 5:42-5:43 PM. No copy command. No login command. Nothing.

Q. *So between this command at 5:29 and the very next command at 5:55, there are no commands here, right?*
A. *Not in this exhibit, no.*
Q. *I mean this is recovered directly from the workstation, right?*
A. *Yeah, from the unallocated space. Yes.*

You would expect to see a login or copy command precisely between the last line of the first "ls" command on page 4 of DX 1209 and the next "ls" command executed on the next line.

Q. *OK. And I mean you -- you show in your presentation, you know, all these events that are occurring during this time frame, right?*
A. *Yes.*

[…] Tr. 971-972 – Leedom:

Q. *And if I logged in here, or if I ran an SCP command here, you would see the transcript files on the CIA work station just like you do the ESXi server, right?*
A. *I mean, I can only speak to what we recovered so we didn't recover any commands like that.*

[…] Tr. 972-973 – Leedom:

Q. *But as for the transcript files, unallocated space, and my work station, you looked everywhere there for a copy command during the reversion; correct?*
A. *Yes. I searched through it for alt commands, not just copy, but.*
Q. *You were really looking for copy commands, right?*
A. *I mean, sure. Copy commands, like I said, any commands are really valuable so it is not like I searched only for copy commands.*

Q. *You really scrutinized the work station over the last five years, right?*
A. *Not like every day over the last five years but, yes, it was reviewed in some time in the last five years.*
Q. *You did a complete forensic analysis on the work station, right?*
A. *That's correct.*
Q. *You looked for a copy command during the reversion period, right?*
A. *Yes.*
Q. *Looked high and low, right?*
A. *That's correct.*
Q. *You did not find a copy command during the reversion, correct?*
A. *No.*
Q. *You did not find any logins to the Confluence virtual machine during the reversion, correct?*
A. *No, not that I believe.*
Q. *And you know all these very specific times on your timeline from the transcript files, right?*
A. *There are still estimates, I would call them very specific estimates, but yes.*
Q. *I mean, the point is there is no -- there is no files that were deleted or activity that was executed that is not – that you didn't find transcript files for, right?*
A. *Included in the timeline here as far as everything on the bottom? Everything on the bottom here comes from transcript files aside from the vault stuff.*

Mr. Leedom did not find any copy command, login command, or a single forensic artifact indicating that any such commands were ever executed on April 20, 2016. Tr. 974 – Leedom:

Q. *OK. Once and for all, forensically, based upon only your forensic findings, can you say that I copied the March 3rd, 2016 Confluence backup on April 20th, 2016?*
A. *There is no copy command, like, attributable to you for that.*

So it is not just the absence of the copy command or the login command, **but the fact that transcript files were generated during this time—and would have logged those commands if they had been executed.** Combined, the active transcript files logging all activity on April 20, 2016, and the absence of any copy or login command prove that Mr. Schulte did not login, access, or copy the backups on April 20, 2016.

2. There were no drives inserted into Mr. Schulte's computer during the timeframe

Mr. Leedom and the government recovered logs for every single device Mr. Schulte ever connected into his CIA Workstation. See Tr. 974-75 – Leedom:

Q. *Back to the logs. You have all -- again, you have all the logs from the CIA work station, right? From my CIA work station?*
A. *That we were able to recover, yes.*
Q. *You testified they're all in tact, right? There were no deletions of those files, right?*
A. *Yes. On the host I don't recall seeing like any evidence of deletion.*
Q. *And this includes logs of removable media, correct?*
A. *Yes.*
Q. *You have the logs for every device I ever connected into the CIA work station for how long, right?*
A. *Yes, in a general sense.*

And no removable drive, hard drive, or anything was ever connected into Mr. Schulte's CIA Workstation during the Confluence reversion. See Tr. 975 – Leedom:

Q. *During the reversion period there are no removable media connected to my CIA work station, correct?*
A. *I don't believe so. I don't think there was artifact of that. I know there was one that was connected, like, recently, the one that was connected to a write blocker, but I think that was -- that might have been on the 18th. Maybe. I don't quite remember the date for that but no to my knowledge I don't believe there was a USB artifact from during the reversion period from your work station.*
Q. *If there had been one you would have put it in your presentation, right?*
A. *Yes.*
Q. *It would have been important that removal media or large hard drive was being plugged in, right?*
A. *Yes. That would be important.*

And of course, there were no forensic artifacts of any backups copied to Mr. Schulte's CIA Workstation. See Tr. 975 – Leedom:

Q. *And there are no forensic artifacts showing any of the Atlassian backups copied to my CIA work station, right?*
A. *No.*

In fact, Mr. Leedom and the government found no forensic artifacts that indicated any backups were copied to any of Mr. Schulte's devices. See Tr. 976 – Leedom:

Q. *There are no forensic artifacts showing any of the Atlassian backups were ever copied to any devices I possessed or used at the CIA, correct?*
A. *Not to my knowledge.*

So with no removable media ever connected or any forensic artifacts of the backups, what is the government's theory? Tr. 978-79 – Leedom:

Q. *OK. So -- and again, with no removable devices connected, no logs that you have shown of network shares or copies to network shares -- I am struggling to see what would have the Confluence backups have been copied to?*
A. *So like I said, it could have been copied to a network location. I mean, it's tough in general because when we arrived on site it was a year afterwards and, like, we have spoken to the availability of network logs and some of those things are just not available. So, like, from all the evidence retrieved and everything that is there, this is how I put my theory together.*
Q. *But from my work station, again, the logs are all in tact there and there is nothing in those logs, right?*
A. *From the host? No.*
Q. *And you keep saying could have been copied. You see no forensic evidence of that, right?*
A. *Not from --*
THE COURT: *I think we have trod this ground plenty. Move on, please.*

The government simply has no idea. Even if the data was "staged" to some other server, it still would have had to be copied to a removable drive at some point to exfiltrate it from the CIA—but none of Mr. Schulte's devices contained any evidence of this. None were reformatted or wiped. Mr. Schulte did not even have any removable media large enough to hold the backups—at least, the government did not introduce any evidence at trial for this. Accordingly, with absolutely no theory and seemingly no possible way for Mr. Schulte to copy the data to a removable drive for exfiltration, it is incontrovertible that Mr. Schulte did not login, access, or copy the backups on April 20, 2016.

3. The government failed to show that the extremely large backup files could be copied within the extremely small timeframe

The backup files the government alleged Mr. Schulte illegally copied were over 200 GiB in size—massive. The government's window for copying these files was very narrow—only 75 minutes. The government did not present any evidence that Mr. Schulte copied any files let alone even accessed the Confluence VM. The best the government's witness could testify is that the files "could have been copied." See Tr. 979 – Leedom:

Q. *You testified it was possible to copy the backup files in an hour, right?*
A. *Yes.*

But what is Mr. Leedom's basis for this analysis? Tr. 979-80 – Leedom:

Q. *And your presentation slides do not show the forensic basis for your conclusion, right?*
A. *No, there is no --*
Q. *OK. You did not establish network speed, right?*
A. *I'm sorry?*
Q. *In your slides you don't establish network speed, right?*
A. *No.*
Q. *You don't address the variables that degrade the network speed, right?*
A. *No, not in my network slides.*
Q. *A forensic expert cannot validate your claims, right?*
A. *Can you explain?*
Q. *Yes. A forensic expert has no idea what test you performed, right?*
A. *I think those tests might have been in my notes.*
Q. *I'm talking about your presentation, sir.*
A. *Oh no.*
Q. *Your presentation -- in your presentation it does not reflect any tests you performed for network speed, right?*
A. *That's correct.*

In order for Mr. Leedom to give an estimate on the speed of a file transfer, he must first determine the network speed—including latencies, and then the drive write speed. Either of which could cause a bottleneck in the data transfer. A USB 1.0 device has significantly different speeds from a SATA device or a tape drive. Mr. Leedom establishes neither—he does not produce a computation or estimation of file transfer speeds on DevLAN, and since he has no theory as to what device the backups were copied to, he cannot even estimate the write speed of the unknown device. See Tr. 980-81 – Leedom:

Q. *The fact that you do not even have a theory as to what device the data was copied to, this also impacts your analysis, correct?*
A. *Can you define "impacts my analysis?" What do you mean by that?*
Q. *Yeah, sure. A theory of splitting the backup files across multiple drives or using slower drives obviously impacts the analysis, correct?*

A. *To some extent it impacts the conclusion just because I would say I don't have the, like, an exhibit for that. To the extent I don't have an exhibit that affects my analysis, yes.*
Q. *Without knowing precisely what device or where information was copied, you can't say how long it would have taken, right?*
A. *Oh, I don't know, I disagree.*
Q. *You disagree? You can theorize how long something takes to copy without specifying what it is being copied to?*
A. *I think if it was taken -- so like the tests that I ran were based on copying to, like, a network location or just the file transferring of the network in general, so whether it was, like, copied somewhere quickly and, like, staged and copied later or something like that, I can't say, obviously, like I don't have a log of a certain USB device or a certain firmware number that I could test. No, I don't have that.*
Q. *I mean, if it is being copied to a tape drive it is going to take a long time to copy, right?*
A. *If it was being copied to a tape drive it would take longer than being copied to, like, a solid state drive. On a matter of principle, yes.*

Essentially, Mr. Leedom took out the drive as part of the equation and just guessed that the backup was copied to a network share. Accordingly, he ignored the bottleneck caused by copying to a drive. But of course, there is absolutely no evidence that any CIA backups were copied to any file shares or Mr. Schulte's own workstation or devices. So, for this analysis that is critical for the feasibility of the government's theory, Mr. Leedom just guesses and completely ignores the bottleneck caused by the device—not to mention the fact that, even if it were copied to a network share, at the end of the day, it still requires *some device* that the backups must be copied to.

But even this analysis—in completely ignoring the device bottleneck—is suspect. Mr. Leedom simply fails to establish any network speed. See Tr. 982 – Leedom:

Q. *At 100 megabits per second it would take four hours to copy 200 gigabytes, correct?*
A. *It sounds close. I would want to run it through a calculator probably but that sounds somewhat close.*

At the standard 100 megabit Ethernet network speed, operating at the theoretical maximum (and practically impossible) 100mb/s, it would take over 4 hours to copy 200 gigabytes. This is easily confirmed by simple math. 100mb/s = 200 GB/X s. Converting 100 mb/s to GB/s, 100mb X 1 GB / (8 * 1024) mb = 100/8192 GB/s. So, 100/8192 GB/s = 200 GB/X s. X = 200 * 8192 / 100 = 16384 seconds. = 273 minutes. = 4.55 hours.

Even considering this evidence in the most favorable light for the government, the government simply failed to present sufficient evidence of DevLAN's bandwidth—and whether it was faster than the internet or standard 100-megabit network speed; there is simply no way a rational, reasonable juror could possibly determine the feasibility of copying 200 gigabytes of backups within the requisite 75-minute window. Accordingly, Mr. Schulte should be acquitted of Count One.

4. Mr. Schulte was in the bathroom when the backups were accessed

We know there is a break in action between the reversion at 5:35 PM and the next command executed on Mr. Schulte's Workstation at 5:55 PM. So what happened in this 20-minute window in which no commands were executed? Well, the badge records provide the answer: Mr. Schulte was in the bathroom. According to GX 111, the 8th floor bathroom is located in 8W81. 8W53A is the nearest entry to the vault from the bathroom. At 5:45 Mr. Schulte tries to badge in through this door. However, the doors can lock from the inside, and Mr. Schulte was forced to walk around to the front entrance—and badged in at 5:48 PM. Mr. Denton lied during his rebuttal and claimed that Mr. Schulte's workspace was right next to the bathroom—which was false. Mr. Schulte's workspace was in the middle of the vault, near the 8W53 entrance. Based on the badge records showing the time to walk from 8W53A to 8W53, it takes three minutes. So, even if Mr. Schulte walked from his desk to the bathroom and back, this would take at least three minutes—requiring him to leave the vault by 5:42, which is before the backup file is accessed (5:43 PM). But of course there would be no reason for Mr. Schulte simply to walk to the bathroom and back—so taking a conservative approach of 5 minutes in the bathroom, this requires Mr. Schulte to leave the vault by 5:40 PM—placing him outside the vault during the access of the backups.

Reviewing the badge records and workstation logs in tandem, the most likely scenario is Mr. Schulte executed the reversion at 5:35, then went to the bathroom, arriving around 5:40 PM, and exited at 5:45 PM. He then re-entered the vault at 5:48 PM, reached his desk about 5:50 PM, then executed the next command at 5:55 PM.

Confirmation of this would exist on Mr. Schulte's CIA Workstation—the logs of his screen lock and inactivity. But of course, the government refused to provide the defense with a forensic image of the CIA Workstation. The government also refused to provide security camera footage from April 20, 2016—both of which would confirm that Mr. Schulte was in the bathroom when the backups were accessed—and irrefutably prove Mr. Schulte's innocence.

5. Mr. Schulte could not have known he could access the Confluence VM by reverting it

The government's entire theory of prosecution—the snapshot-reversion of the Confluence VM depends upon Mr. Schulte's knowledge that, by reverting Confluence, he could then log in and access the VM. But Mr. Schulte did not take the April 16, 2016 snapshot and could not have possibly known his access keys existed in the snapshot. See Tr. 1031-33 – Leedom:

Q. *OK. Let's talk a little bit about the permission change in the April 16, 2016, snapshot. All right? On the next slide, 69, shows a list of authorized SSH keys before the snapshot, right?*
A. *That's correct.*
Q. *And 70 shows that all the SSH keys were removed, right?*
A. *Yes.*
Q. *And then a new one was added, right?*
A. *Yes.*
Q. *And the only way you concluded that the April 16, 2016, snapshot maintained my previous*

privileges is by actually reverting to the snapshot, right?
***A.** Yes. We have the snapshot.*

[…]

***Q.** Yeah. I'm sorry. So outside. Without looking, without running the reversion, you don't know any of this, right?*
***A.** The only thing you know about the snapshot without reverting the snapshot is what's in the, like, I don't know if it's the previous slide, where it shows the snapshot information, just, like, a time stamp and name, things like that. That's all you'd know about the time stamp -- or the snapshot.*
***Q.** OK. And then once you revert it, then that's when you could learn the privileges changes, right?*
***A.** Yes.*

6. Existence of transcript files proves Mr. Schulte's innocence

Mr. Leedom testified that the transcript files were not normal log files—normally, only the user's input of commands is recorded. See Tr. 1047 – Leedom:

***Q.** But the point is you are recording -- these files record user's input to the system, correct?*
***A.** Yes; commands that were executed.*
***Q.** ESXi, like you said, specifically writes the commands to a shell.log file, right?*
***A.** Yes.*
***Q.** But by default it does not record the output of the commands, correct?*
***A.** That's correct. I don't even think you can configure it to do that.*
***Q.** That's right.*

But Mr. Leedom did not find normal log files on Mr. Schulte's CIA Workstation—he found transcript files. See Tr. 1047 – Leedom:

***Q.** That's right. Let's turn to slide 116. So this is not normal system logging, correct?*
***A.** Correct.*
***Q.** This shows command input and output, correct?*
***A.** That's correct.*
***Q.** And these are known as transcript files, correct?*
***A.** That is one method that this data could be logged, yes.*

Transcript files are not normally generated, but can be manually created through user intervention. See Tr. 1051 – Leedom:

***Q.** But normally -- you agree, normally, you don't see output like this, correct?*
***A.** Correct.*

Q. *And the terminal itself does not log that, correct?*
A. *You can configure it, too.*
Q. *That would require user intervention, correct?*
A. *Yes, you can say that.*

And according to Mr. Leedom, it's good practice in system administration to record actions taken on the server—which can be done by generating transcript files through the script command. See Tr. 1049 – Leedom:

Q. *OK. But it's good practice to essentially record actions taken on enterprise systems, correct?*
A. *Yes.*
Q. *And system administrators do this through the script command, correct?*
A. *Like I said, I haven't used it but if a script command, you know, could create a log of that then, yes, I suppose you could use it for that but I haven't personally used it.*

Mr. Leedom offers absolutely no other explanation for the generation of transcript files. See Tr. 1051-52 – Leedom:

Q. *You testified on direct that when somebody does something nefarious or deletes documents that that's what you called a clue for your investigation; correct?*
A. *Yes.*
Q. *So wouldn't the fact that an individual purposefully recorded a session also be important to that analysis?*
A. *It would be but, like I said, I don't have any evidence of that.*
Q. *OK. So your testimony is that you simply don't have any idea about how or why these files were created?*
A. *No.*

Running the script command to enable verbose logging to record you committing a crime would be like installing a camera and setting it to record in a store before you rob it. It makes absolutely no sense that Mr. Schulte would configure the generation of transcript files while committing a crime. Since this is a contradiction, the only logical conclusion is Mr. Schulte was not committing any crime.

***

So how did Mr. Schulte gather the national defense information and to what device? The government simply ignored this critical question—they proposed no theory whatsoever of how Mr. Schulte could have copied the data within the small timeframe, especially without issuing a copy command or connecting a removable drive to copy the data. Without even a theory to these questions, the government wholly failed to prove element 1 (Charge at 21):

> *The first element that the Government must prove beyond a reasonable doubt for purpose of Count One is that the defendant copied, took, made, or obtained a sketch, photograph, photographic negative, blueprint, map, model, instrument, appliance, document, writing, or note. The Indictment specifically charges that, on or about April 20, 2016, the defendant copied without authorization the Backup Files housed on the classified DEVLAN computer system maintained by the CIA.*

7. Government's only evidence: March 3, 2016 backup access time

The government's only evidence that Mr. Schulte gathered NDI is that the access times for the March 3, 2016 Confluence backup file show an April 20, 2016 date. That's it. As an initial matter, "access" does not mean the file was copied—only that it was accessed. And there is no indication that Mr. Schulte ever accessed the file—and literally hundreds of other unexplored explanations.

The problem is WikiLeaks released data over a year after that file appears to be accessed. And we have no idea what happened in the year. Without proper logging on DevLAN, there is simply no way to know whether or not this file was even copied, let alone on April 20, 2016; there is nothing in the record that refutes other possibilities. The tech experts did not testify that they checked the most obvious possibilities: they did not present evidence that these other vulnerable sites were even investigated let alone cleared. It could simply be that someone in January of 2017 exploited DevLAN and stole the January 2017 backups. While stealing the backups, they noticed this April 20, 2016 access time on the March 3, 2016 backup. So they give WikiLeaks this backup file to throw off the investigation on the wrong path. It could be that the

March 3, 2016 backup file was never even accessed on April 20, 2016—but a touch command was used later, say in 2017, to change the access time to April 20, 2016 and throw off the investigation. In fact, the access time could be a direct byproduct of the Confluence snapshot itself—if Dave or Weber issued a command or set a process to execute while taking the snapshot, then those commands would also execute when Confluence was reverted to that snapshot. See Tr. 1028-29 – Leedom:

Q. *You were aware that Dave C. and Jeremy Weber took the April 16, 2016, snapshot, correct?*
A. *Yeah, that, that weekend. I think it was -- I don't know which one of them did it, but --*
Q. *If they initiated a process or cron job that ultimately touched the March 3, 2016, backup file, it would have been preserved in the snapshot, right?*
A. *Before or after they took the snapshot?*
Q. *Well, before, during.*
A. *If they ran a cron job to -- if they ran a cron job before taking the snapshot -- well, yeah, they didn't do any reversion, so, yes. I don't remember seeing anything like that from my review.*
Q. *The question was just would that be preserved in the snapshot?*
A. *If it happened before the snapshot was taken, yes.*

There are literally countless possibilities, each as equally likely as the next, and none of which involve Mr. Schulte or the copying of the March 3, 2016 backup on April 20, 2016. The government simply has no idea what files WikiLeaks received, or, perhaps even more critically—when they received those files. And what the government has tried to do is shift the burden of proof onto Mr. Schulte—**arguing that the lack of evidence against Mr. Schulte is evidence against Mr. Schulte.** Or that the lack of logging on DevLAN allowed Mr. Schulte to copy the CIA backups in some unknown, sophisticated manner; however, the lack of logging, and the government's lack of evidence should not be held against Mr. Schulte—but the government. It is the government's burden to show to the jury what happened—it is not enough to say, look, this file was accessed on April 20, 2016, and now we think WikiLeaks has it—so convict Mr. Schulte for stealing it.

There is simply insufficient evidence for any rational juror to conclude—beyond reasonable doubt—that Mr. Schulte copied and made off with the CIA backups on or about April 20, 2016.

8. The government failed to prove elements 2 and 3

Finally, the government failed to prove elements 2 and 3 beyond reasonable doubt.

D. Count Two: Illegal transmission of unlawfully possessed national defense information in violation of 18 U.S.C. § 793(e)

Count Two charges the defendant with illegal transmission of unlawfully possessed documents, writings, or notes containing NDI. Specifically, it charges that, between April and May 2016, the defendant, without authorization, retained copies of the Backup Files and communicated them to a third party not authorized to receive them, the organization WikiLeaks. (Charge at 20)

1. Element 1: Possession

In the case of Count Two, the Indictment charges that, between April and May 2016, the defendant, without authorization, retained documents, writings, plans, instruments, and notes in the form of copies of the Backup Files. (Charge at 25)

First of all, since the government failed to prove Count One, how could Mr. Schulte transmit information that he never possessed? How could Mr. Schulte ever transmit the national defense information when the only window in which he could have copied it—the 75-minute window on April 20, 2016—he never issued a copy command to copy it, never connected a removable drive to copy it to, and did not have the time or bandwidth to copy it?

Regardless of Count One, the government simply failed to prove that Mr. Schulte ever took any CIA backups to his home. See Tr. 1180-81 – Berger:

Q. *OK. So to your knowledge, you didn't find any CIA hard drives or thumb drives at my home, correct?*
A. *Again, I can't say one way or the other.*
Q. *I'm saying, to your knowledge, you didn't find them.*
A. *I'm not aware of any, no.*

Q. *Similarly, you found no evidence that any of my hard drives or moveable media what were ever connected to the CIA computers, correct?*
A. *I'm not aware of that, no.*
Q. *You found no model numbers or serial numbers on my CIA workstation that matched one of my personal drives, correct?*
A. *I'm not aware of any of that analysis, no.*
Q. *Specifically, you found no evidence that I copied the Vault 7 or Vault 8 data to my home computer, any of my devices, correct?*
A. *Specific evidence of those files?*
Q. *The question is you found no evidence that I copied the Vault 7 or Vault 8 data to my home computers, any of my devices, correct?*
A. *I did not find any specific forensic artifacts that indicate that, correct.*

[…] Tr. 1182 – Berger:

Q. *OK. But you don't have any evidence that there was any Confluence data on my home device from the forensics, right?*
A. *Other than that one folder named Brutal Kangaroo, correct.*
Q. *Same for Stash, right?*
A. *Correct.*
Q. *No evidence of any Atlassian products from the CIA, correct?*
A. *Correct.*
Q. *No evidence of any of the CIA backups on my home devices, correct?*
A. *Correct.*

FBI Special Agent Evanchec confirmed Mr. Berger's findings as well. See Tr. 360-61 – Evanchec:

Q. *OK. So with respect to the electronics in general, all in total, the FBI recovered some 20 terabytes or more, correct?*
A. *That's correct.*

[…]

Q. *OK. As we've already seen, after seizing and reviewing every single bit of data across all my electronic devices, you did not find any national defense information, correct?*
A. *That's my understanding and memory, yes, sir.*
Q. *No national defense information in those 20 terabytes of data, correct?*
A. *That's my understanding.*
Q. *You certainly didn't find any CIA backups of in my apartment, correct?*
A. *No, sir.*

2. Element 3: Willful Transmission

Similarly, for element three, the government did not find a single shred of evidence that Mr. Schulte ever transmitted any CIA backups or anything at all to WikiLeaks. See Tr. 1286 – Berger:

Q. *I'm asking about forensic evidence, specifically from my home.*
A. *Again, if we are talking about forensic artifacts within the virtual machine, no.*
Q. *No, not just the virtual machine, my entire home. All the electronic devices you analyzed from my home, is there any forensic evidence that suggests any data was transmitted to WikiLeaks from any of the frenzy[“forensic”] artifacts.*
A. *No.*

a) Mr. Schulte’s normal activity

So if there was not a single shred of evidence in Mr. Schulte’s apartment, what is the basis for the willful transmission? Mainly Google searches taken out-of-context.

Mr. Berger speculated that Mr. Schulte downloaded Tails and TOR because he visited the WikiLeaks website. But of course, FBI Agent Evanchec already testified that Mr. Schulte never visited the WikiLeaks website in April or May of 2016. See GX 1351. As for Tails, Mr. Schulte regularly downloaded Tails and other Linux distributions—including in August of 2016. As for TOR, Mr. Schulte never even used the Linux Mint VM, but, regardless, TOR was installed on that VM in October 2015. And what about that suspicious device that was purchased “same day delivery” from Amazon? It was a hard drive docking station used for an offline clone—to make forensic copies of drives—not to transmit data over the internet. It was also not necessary to function as a “USB adapter” to connect a hard drive to Mr. Schulte’s computer, because Mr. Schulte had eSATA ports and could connect a hard drive directly over a much faster connection than USB. See GX 1601-3. And most importantly, Mr. Schulte regularly bought computer equipment on Amazon, and through his Amazon Prime membership, received free shipping. See

DX 209-2. In fact, Mr. Schulte purchased the exact same hard drive docking station again in September 2016.

So what remains from Mr. Berger's "analysis"? The formatted drives and Google searches. On May 1, 2016, Mr. Schulte conducted Google searches for "best way to store user data" and "raid 5 or data backup." DX 302-1. At which point, Mr. Schulte decided to install a RAID 5 system. See Tr. 1263-64 – Berger:

Q. *If you're going to upgrade your RAID, you would copy your data to an external drive, right?*
A. *Generally, yes.*
Q. *Then you delete the old RAID, right?*
A. *Correct.*
Q. *And you remove the old drives, right?*
A. *Correct.*
Q. *Then you install the new drives, correct?*
A. *Correct.*
Q. *And then you create the new RAID, correct?*
A. *Correct.*
Q. *And finally, copy of your data -- and finally, you would copy your data onto the new RAID, right?*
A. *Yes, that's one way of doing it.*
Q. *After this was completed, you would have at least two copies of your data, correct?*
A. *Correct.*
Q. *And most security protocols would then recommend securely deleting the old drives, right?*
A. *If you weren't maintaining them as some kind of backup copy and you were getting rid of them, then yes, you should – you should be securely erasing it.*

This activity explains all the Google searches and why the home computer appeared to be "wiped" or "reformatted." Upgrading or installing a new RAID system would require these steps—and would ultimately format new drives. See Tr. 1217-18 – Berger:

Q. *And you are aware that you cannot increase the capacity of a RAID 5 system, right?*
A. *Under standard RAID 5, correct.*
Q. *And so Government Exhibit 1601-18, this shows the RAID controller configuration on the computer, correct?*

A. *Yes. It appears that way.*
Q. *You can only delete the RAID or create a new RAID, correct?*
A. *I believe so, yes.*
Q. *So if you wanted to add hard drives to a RAID 5 you have to create a new RAID 5 system, right?*
A. *Yes.*

b) Even if a jury found Mr. Schulte guilty on Count One, that alone cannot constitute a guilty verdict on Count Two

Mr. Berger believed Mr. Schulte transmitted information to WikiLeaks simply because he believed Mr. Schulte guilty on Count One. See Tr. 1285 – Berger:

Q. *So there is no evidence anything was ever transmitted to WikiLeaks, correct?*
A. *Incorrect.*
Q. *Incorrect. You found evidence that information was transmitted to WikiLeaks from the VM?*
A. *I believe your previous question didn't specify VM and only asked about evidence that data was transmitted to WikiLeaks. The evidence that data transmitted to WikiLeaks is that the data showed up on WikiLeaks.*
Q. *OK. So that's evidence that WikiLeaks received the data, correct?*
A. *Correct.*
Q. *That's not evidence that I transmitted anything to WikiLeaks, correct?*
A. *It is evidence the data was transmitted to WikiLeaks.*

However, even if the jury reached a conclusion that Mr. Schulte illegally gathered NDI—it cannot reach a verdict of guilty on Count Two based on this alone. How did Mr. Schulte transmit the data to WikiLeaks? He could have mailed them a drive. He could have met with them directly. He could have used a dead drop. He could have transmitted it from his New York City Apartment. But most importantly, when were the backups transmitted to WikiLeaks? February 2017? This would constitute a fatal variance in the indictment. Accordingly, the government had to present sufficient evidence to the jury that Mr. Schulte transmitted data to WikiLeaks from his home computer in Virginia on or about April-May 2016. And the government simply presented no such evidence.

c) Netflow Logs prove Mr. Schulte's innocence

Usually a defendant wrongfully convicted must go through rigorous process and procedures to uncover new evidence exonerating him—be it new advances in DNA evidence, technological advancements, etc. Ironically, in this case, the evidence exonerating Mr. Schulte can be found in DX 208 and DX 208-A.

Whenever you use your computer at home, your internet provider, be it Verizon, Comcast, or whoever, they record the amount of data you send and receive as well as the IP address of the recipient or sender. And they retain this data for the government should it come knocking. This data can irrefutably link you to every single data transfer you perform. Even if you use TOR or other proxies and anonymizers, your internet provider will still capture the fact that you transferred data across it. Mr. Leedom testified about the importance of netflow logs. See Tr. 919 – Leedom:

Q. *Can you explain for the jury what NetFlow logs are?*
A. *It is essentially, like, a summary of, like, bytes in and out of a network. So theoretically if you had NetFlow logs, network logs, you could determine, like, between like two points in time how much data transferred from one point to another point.*
Q. *So from that flow log you can determine basically the amount of data sent or received by each connection, correct?*
A. *Yes.*
Q. *Which would have been very huge in your incident response, correct?*
A. *Yes. So that was one of the first things I asked for when we showed up.*

Netflow logs were so critically important that they were the very first thing Mr. Leedom asked for. And what would the netflow logs show? If Mr. Schulte copied the backups, the netflow logs would show 200 gigabytes received by Mr. Schulte's workstation between the exact timeframe alleged by the government. And if he didn't—then the netflow logs would definitively prove that 200 gigabytes were NOT received by Mr. Schulte's workstation in the government's timeframe. In essence, we would not be here today litigating this issue because Mr. Schulte would be a free man. Unfortunately for Mr. Schulte, DevLAN did not keep those records.

However, fortunately for Mr. Schulte—Verizon did keep those logs. If netflow logs were the first thing Mr. Leedom asked for, then they were almost certainly the first thing Mr. Berger asked for—netflow logs are the single most important logs in tracking down data transfers. And indeed, subpoena records show that netflow logs were among the very first subpoenas issued—On March 9, 2017. But what did the government and Mr. Berger find in the Verizon netflow logs? That Mr. Schulte was not guilty of Count Two.

The mere fact that these records exist, but the government did not introduce them or testify about the conclusions from the netflow logs proves Mr. Schulte's innocence beyond any and all reasonable doubt. If Mr. Schulte had transmitted 200 gigabytes to WikiLeaks, the logs of that transfer would have been the first and last thing on display to the jury. The only possible conclusion is that the netflow logs prove Mr. Schulte's innocence, and so the government did not introduce them or talk about them at trial.

But of course, the netflow logs are admitted into evidence. And particularly, the netflow logs from April 20, 2016 to May 6, 2016: DX 208-A. It doesn't take a genius or even a technical expert to review these logs. The logs show a start time, end time, source IP, destination IP, and number of bytes transferred. All you need to do is sum up the bytes column in excel to determine the total number of bytes transferred—which is an order of magnitude below the size of the CIA backups.

But to be more accurate, only the data Mr. Schulte transmitted is relevant; the data Mr. Schulte received should be discarded since he cannot transmit information to WikiLeaks by receiving data. Since the netflow logs are specific to Mr. Schulte's Verizon account, there is one consistent IP address in each row—therefore this must be Mr. Schulte's IP address: 71.178.235.3. So, after discarding all rows in which 71.178.235.3 is listed as the destination—the recipient of data—we are left with only rows in which 71.178.235.3 is the source—the sender of data. This is easy to do in excel—sort by source IP, and discard all data with a source IP other than 71.178.235.3. Technically, you should then distinguish a single session or recipient who received the data; but, the conservative approach of assuming all the data Mr. Schulte sent was to WikiLeaks results in the same conclusion: he did not transmit the backups to anyone. In fact, **between April 20, 2016 and May 6, 2016, Mr. Schulte transmitted less than one gigabyte**. That's not even large enough for the small Confluence data let alone the giant Stash repositories. And even if you don't filter the data, but just sum up the bytes column of unadulterated DX 208-A, you reach the same conclusion—it was impossible for Mr. Schulte to transmit the CIA backups between April 20 and May 6, 2016.

According to the Verizon Netflow logs subpoenaed by the government, Mr. Schulte did not transmit the backups to anyone in April or May of 2016. He is not guilty of Count Two.

d) Netflow Logs prove Mr. Schulte's innocence in Count One

DX 208 shows all the data transferred by Mr. Schulte between March 2016 and March 2017. Since WikiLeaks received CIA backups, then whoever stole them must have transmitted them to WikiLeaks. But reviewing DX 208 in totality shows beyond any and all reasonable doubt that Mr. Schulte never transmitted any files as large as the CIA backups during this time. Since Mr. Schulte is not guilty of Count Two, and because he provably never transmitted the CIA backups to anyone, he must also be not guilty of Count One.

E. Count Five: Unauthorized Access to a Computer to Obtain Classified Information

Count Five charges the defendant with unauthorized access to a computer to obtain classified information.

In order to find the defendant guilty of Count Five, the Government must prove the following four elements beyond a reasonable doubt:

First, that, between April 18 and April 20, 2016, the defendant either accessed a computer without authorization or accessed a computer with authorization, but exceeded his authority in accessing the information in question;

Second, that the defendant knowingly accessed that computer;

Third, that the defendant obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations and that the defendant had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign nation; and

Fourth, that the defendant willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted or attempted to communicate, deliver or transmit or cause to be communicated, delivered or transmitted, the information to a person who was not entitled to receive it. (Charge at 31-32)

1. Element One/Two: Knowing Unauthorized Access

It is not entirely clear from the indictment whether the government charges Mr. Schulte with unauthorized access to the Confluence VM to obtain the backups or unauthorized access to the Altabackups server to obtain the backups—regardless, Element One is predicated on access controls for the altabackups. Since the government failed to show what access controls existed on the altabackup directory, it cannot possibly establish element one. See VII.A:

Q. *OK. Just to be clear, for the access controls here, you have no documentation or no configuration files showing the exact access controls, right?*
A. *We do not have a configuration file for Altabackup from the NetApp that, like, shows the -- the allow or block list. It just wasn't available at the time.*

What were the access controls for Altabackup? Who had the authority to access the backups stored in the altabackup directory on the Altabackup Server? Where were those access controls stored? Were they communicated to Mr. Schulte? The government answers none of these questions.

Moreover, the government failed to establish that Mr. Schulte ever logged in or otherwise accessed the Confluence VM or the Altabackup server. See Tr. 973 – Leedom (See also V.B):

Q. *You did not find any logins to the Confluence virtual machine during the reversion, correct?*
A. *No, not that I believe.*

2. Element Three: Obtained Protected Information

The government failed to prove that Mr. Schulte ever copied or otherwise obtained any CIA backups. See Tr. 973 – Leedom:

Q. *You did a complete forensic analysis on the work station, right?*
A. *That's correct.*
Q. *You looked for a copy command during the reversion period, right?*
A. *Yes.*
Q. *Looked high and low, right?*
A. *That's correct.*
Q. *You did not find a copy command during the reversion, correct?*
A. *No.*

See also VII.B.

3. Element Four: Willfully Communicated

The government failed to prove that Mr. Schulte ever transmitted the CIA backups to WikiLeaks or anyone. See Tr. 1286 – Berger:

Q. *No, not just the virtual machine, my entire home. All the electronic devices you analyzed from my home, is there any forensic evidence that suggests any data was transmitted to WikiLeaks from any of the frenzy artifacts.*
A. *No.*

See also VII.C.

F. Count Six: Unauthorized Access of a Computer to Obtain Information from a Department or Agency of the United States

Count Six charges the defendant with unauthorized access to a computer to obtain information from a department or agency of the United States.

In order to find the defendant guilty of Count Six, the Government must prove the following three elements beyond a reasonable doubt:

First, that, on or about April 20, 2016, the defendant either accessed a computer without authorization or accessed a computer with authorization, but exceeded his authority in accessing the information in question;

Second, that the defendant acted intentionally; and

Third, that the defendant obtained information from a department or agency of the United States. (Charge at 35)

Count Six is multiplicitous—it contains all the elements of Count Five. "An indictment is multiplicitous when it charges a single offense as an offense multiple times, in separate counts, when, in law and fact, only one crime has been committed." *United States v. Chacko*, 169 F.3d 140, 145 (2d Cir. 1999) (citing *United States v. Holmes*, 44 F.3d 1150, 1153-54 (2d Cir. 1995)). A multiplicitous charge violates the double jeopardy clause of the Fifth Amendment by punishing a person for the same crime more than once. See *United States v. Dixon*, 509 U.S. 688, 696 (1993). Where the conduct at issue implicates two different statutory offenses or different subsections of the same statute, "the test to be applied to determine whether there are two offenses or only one, is whether each provision requires proof of a fact which the other does not." *Blockburger v. United States*, 284 U.S. 299, 304 (1932). Count Five requires all three elements of Count Six:

Element One is the exact same between Counts Five and Six.

Element two of Count Five is "the defendant knowingly accessed that computer" and Element Two of Count Six is "the defendant acted intentionally"—which is the exact same thing:

> *"Knowingly" means to act voluntarily and deliberately, rather than mistakenly or inadvertently.* (Charge at 33)
>
> *"Intentionally" means to act deliberately or purposefully. That is, the defendant's acts must have been the product of the defendant's conscious objective rather than the product of a mistake or accident.* (Charge at 36)

Element Three of Count Five is "the defendant obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations and that the defendant had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign nation" and Element Three of Count Six is that "the defendant obtained information from a department or agency of the United States"—which, by definition, always encompasses "information protected against unauthorized disclosure for reasons of national defense." Information protected against unauthorized disclosure for reasons of national defense always resides within a department or agency of the United States, because only a department or agency of the United States can classify and designate information as national defense information.

	Accessed computer without authorization / exceeded authorization	Knowingly accessed computer / acted intentionally	Obtained information from a department or agency of the United States / Obtained protected information
Count Five	Element One	Element Two	Element Three
Count Six	Element One	Element Two	Element Three

Accordingly, convictions of both Count Five and Count Six violates the Double Jeopardy Clause of the Fifth Amendment; Count Six should be dismissed.

In the alternative, the Court should still conclude that there was insufficient evidence to convict Mr. Schulte of Count Six—for all the same reasons already discussed in VII.

VIII. RULE 33: NEW TRIAL

For any counts of conviction that the Court finds sufficient evidence for a rational juror to convict, the Court should vacate those convictions and order a new trial in the interests of justice pursuant to Fed. R. Crim. P. 33.

A. Inability to mount any defense due to lack of access to forensic crime scene

The government refused to turn over a single forensic image to the defense—not one. Not a forensic image of the FS01 Server that contained the altabackups directory and CIA backups. Not a forensic image of the ESXi Server that managed the virtual machines. Not the Confluence Virtual Machine that the government allege was hacked. Not even Mr. Schulte's own CIA Workstation that is the centerpiece to the government's case-in-chief. It was a one-sided trial in which the defense essentially did not even have the ability to call its own expert to testify—because, while the Court authorized payment for an expert, that expert was not permitted to conduct any forensic examinations. To call what happened in June and July of 2022 a fair trial is a mockery of justice.

The government's technical experts deliberately did not conduct certain critical analyses or simply "forgot" the results. The government's technical experts did not perform any test which could result in a favorable outcome for the defense—why conduct such a test when you know the defense cannot? Did the government's technical experts test if later backups contained all the information from the March 3, 2016 backup? Of course not—the results could be helpful to the defense. So they testified that they had no idea, but believed the later backups did not contain the information. Did the government's technical experts search for evidence that the altabackups directory had been directly mounted by Jeremy Weber or in Mr. Schulte's virtual machine? Of course not—the results could only be helpful to the defense. So they testified only about the single instance where a datastore failed and claimed that failure indicated restrictions on the altabackup directory. Did the government's technical experts test if Mr. Schulte locked his workstation and walked away at 5:35 PM until he returned from the bathroom at 5:50 PM? Of course not—the results could only be helpful to the defense. Why search for exonerating or exculpatory evidence? The defense has no ability to conduct its own forensic examination—so of course the government's technical experts did not search for anything that would be detrimental to the government's case.

Every step of the way the government's technical experts simply asked—would this test help us convict Mr. Schulte? If the answer was no—or the test could prove Mr. Schulte's innocence, then they did not conduct the test.

Did the government's technical experts conduct an examination of the offsite backup—or at the very least check the access times on the backups? Of course not—the results could only be helpful to the defense. Did the government's technical experts conduct an examination of Jira, Hickok, or COG's network? Of course not—the results could only be helpful to the defense. On cross examination, the government's technical expert could never recall conducting tests or simply did not conduct tests that could have uncovered helpful information for the defense.

Essentially, the government took fingerprints, hair samples, DNA, everything—they captured the entire crime scene. But instead of conducting forensic examinations of everything, they simply took one or two pieces of evidence helpful for their prosecution—and ignored the rest; no, not ignored—hid the rest. Because the government certainly did not allow defense experts to conduct their own tests.

1. DevLAN bandwidth analysis

The most critical issue is the DevLAN bandwidth analysis. In order for the government to prove that Mr. Schulte copied the CIA backups, it must establish that it was feasible to do so. The only time Mr. Schulte could have copied the backups was during the Confluence reversion—which only lasted 75 minutes. If the Stash and Confluence backups could not be copied within that time, then Mr. Schulte could not have possibly copied the backups and the jury would have to acquit. So what was the analysis? What is the speed of the DevLAN network? The government never says. The government's expert simply asserted that the copy was possible—without a single shred of evidence, test, or analysis. See Tr. 979-80 – Leedom:

Q. *You testified it was possible to copy the backup files in an hour, right?*
A. *Yes.*

[…]

Q. *In your slides you don't establish network speed, right?*
A. *No.*
Q. *You don't address the variables that degrade the network speed, right?*
A. *No, not in my network slides.*
Q. *A forensic expert cannot validate your claims, right?*
A. *Can you explain?*
Q. *Yes. A forensic expert has no idea what test you performed, right?*
A. *I think those tests might have been in my notes.*
Q. *I'm talking about your presentation, sir.*
A. *Oh no.*

[…]

Q. *Again, the forensic expert does not know what tests you performed, correct?*
A. *I disagree. I don't remember if they're in my notes or not.*

[…]

Q. *Your presentation -- in your presentation it does not reflect any tests you performed for network speed, right?*
A. *That's correct.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the

opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to the ESXi Server Altabackup/FS01 Server, all networking devices connecting them, and any and all other servers and networking devices that the data could have been copied to. The defense can then conduct a bandwidth test, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

2. Access to every DevLAN device

Because the government has absolutely no theory at all for how the CIA backups were copied, or to what device, the defense is entitled broad access to every single seized DevLAN device that could have conceivably been used. If the government had a very tight, specific theory—that server X was used or drive Y—then obviously Mr. Schulte would only need access to those specific servers or devices; Mr. Schulte need only challenge and disprove the government's theory as to those specific devices in order to reach a not guilty verdict. But in the alternative, where the government claims Mr. Schulte could have used every single device—Mr. Schulte then needs to disprove each and every device in order to reach a not guilty verdict. See Tr. 976-77 – Leedom:

Q. *I mean, without any removal media connected to my CIA work station during the reversion it is not possible to steal the backups, is it?*
A. *I mean, there is attached network shares, there is other ways than just removal media. You could stage the data or move it.*
Q. *I mean, you found no evidence of any of that though, right?*
A. *I don't have a whole lot of visibility for some of that.*
THE COURT: *Can you explain what you mean by attached network share?*
THE WITNESS: *Yes. So like we saw, as an example, like the home folders, that's all connected over the network to the various work stations so, like, that could be a potential location something could be copied to. It doesn't necessarily have to be copied straight to the machine.*

See also Tr. 978 – Leedom:

***Q.** OK. So -- and again, with no removable devices connected, no logs that you have shown of network shares or copies to network shares -- I am struggling to see what would have the Confluence backups have been copied to?*
***A.** So like I said, it could have been copied to a network location. I mean, it's tough in general because when we arrived on site it was a year afterwards and, like, we have spoken to the availability of network logs and some of those things are just not available. So, like, from all the evidence retrieved and everything that is there, this is how I put my theory together.*

The government cannot have its cake and eat it too—it cannot claim that any and all servers or devices could have been used in the theft while simultaneously refusing to provide those servers and devices to the defense for forensic examination. Because the government's theory is so general—that Mr. Schulte copied the backups to some unknown device for some unknown period of time and then exfiltrated some other unknown device—then all the DevLAN devices become relevant to the defense.

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. The defense must, and indeed has the right, to examine each of these devices and present an expert to testify that none of them could have been used; alternatively, the government could enter a stipulation for specific servers or devices—and acknowledge that they could not have been used in the theft. But without access to servers and devices that the government claims could have been used in the theft, whether to "stage" the data or actually exfiltrate it, the defense cannot answer the government's allegations and a grave injustice ensues.

3. Access to Schulte's CIA Workstation

Mr. Schulte's CIA Workstation is literally the central piece to the government's case—it contains the transcript files logging activity from April 20, 2016. But this relevant and critical piece of evidence for the government's case-in-chief was never provided to the defense. There are countless critical tests that the defense has been deprived of attempting. First and most critically, what actions were taken on April 20, 2016? What do the Windows Event Logs, VM logs, and other critical forensic artifacts that the defense cannot possibly know say about what happened on April 20, 2016? Mr. Leedom certainly had the opportunity to review the entire system and pick and choose the story he wanted to tell—but not the defense. There can be no question from the badge records that Mr. Schulte left at some point to use the bathroom—but what time? The screen-lock and unlock logs would tell us exactly what time. But did the government present those logs to the jury? No. Suspiciously, the government presented literally zero logs from Mr. Schulte's CIA Workstation to the jury—only the transcript files from his virtual machine. Why? What do the screen-lock and unlock logs show? What was Mr. Schulte working on during this time? Was his virtual machine even powered on? Were the transcript logs copied to his virtual machine? The defense was not permitted to conduct these tests.

Indeed, there were multiple lines of questioning that the defense could not continue because it did not have access to Mr. Schulte's CIA Workstation: Mr. Leedom could not be properly cross-examined, and Mr. Schulte did not have the ability to mount a proper defense.

Mr. Schulte's virtual machine was only 50 GB in size, and could not have possibly held the backups. But on cross-examination, Mr. Leedom "forgot" or could not "recall" the size of the VM—which killed the entire line of questioning because the defense did not even have any information indicating the size of the VM. See Tr. 976 – Leedom:

Q. *In fact, the virtual machine was only 50 gigabytes, right?*
A. *I don't remember the exact size.*
Q. *You don't remember the exact size?*
A. *No.*

Mr. Schulte's CIA Workstation, and particularly his VM, also contained numerous other transcript files—files that he purposefully recorded while performing system administration. When taken together in context with the April 20, 2016 transcripts, the evidence is overwhelming that (1) these files were deliberately generated and (2) they would record all activity during the timeframe including remote logins to the Confluence VM—which are actually recorded in some of the transcript files. But of course Mr. Leedom does not recall any of this. See Tr. 1050-51 – Leedom:

Q. *Yeah. The question was did you see any file or any data like this on the workstation from April 20th until I resigned in November?*
A. *I don't know the absolute last timestamp entry or anything from that machine. This activity was presented for being in the April 20 time frame. I don't know or remember what was there from after that.*

Mr. Schulte's CIA Workstation would also show the logs of all devices connected, and for how long. This and other related logs would be critical to show a jury that, during the April and May timeframe, Mr. Schulte only connected X drives into his computer—and none of which could hold the backups. Additionally, showing that these drives were never wiped and were never taken out of the CIA or connected to Mr. Schulte's home computers would go a long way to proving Mr. Schulte's innocence. See Tr. 975 – Leedom:

Q. *And you also recovered every single device I connected into the CIA work station, right?*
A. *I don't remember from, like, an inventory perspective. I don't remember.*
Q. *During the reversion period there are no removable media connected to my CIA work station, correct?*
A. *I don't believe so. I don't think there was artifact of that. I know there was one that was connected, like, recently, the one that was connected to a write blocker, but I think that was -- that might have been on the 18th. Maybe. I don't quite remember the date for that but no to my knowledge I don't believe there was a USB artifact from during the reversion period from your work station.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the

opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to Mr. Schulte's CIA Workstation—the heart of the government's case-in-chief. The defense can then conduct a forensic examination and independent analysis of the government's tests as well as perform tests that the government's own expert refused to perform, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

4. Access to Mr. Schulte's removable media and accountable property

Furthermore, access to all of Mr. Schulte's removable media and accountable property would be relevant and helpful to the defense in rebutting the government's allegations. Showing that all of Mr. Schulte's devices are accounted for, none were wiped, none were taken out of the CIA or connected to Mr. Schulte's home computers, and none were large enough to hold the backups would go a long way to proving Mr. Schulte's innocence. If none of these devices were used or could have been used in the theft, then the government is really left grasping for straws.

5. Access to ESXi Server

Access to the ESXi Server is also critical to the defense. The ESXi is the second of the three computers central to the government's case-in-chief and theory of theft. The government claims Mr. Schulte used his ESXi Server Administration privileges to revert the Confluence VM to access the altabackups on the Altabackup server. Forensic examination if this server is critical to the defense.

First of all, there was a history of corrupt log files and deleting them. Yet none of this could come out at trial. See Tr. 1074 – Leedom:

Q. *Can you say whether or not log files were corrupted on that day?*
A. *I don't -- I don't remember any -- I can't really speak to the actions they took other than changing the passwords.*

Mr. Schulte previously created a datastore on the ESXi Server and mounted the altabackups directory—definitively proving there were no access controls on the altabackup. But when questioning Mr. Leedom about this, once again Mr. Leedom "forgot" or could not "recall"—instantly killing this line of questioning because the defense did not have a forensic image of Mr. Schulte's workstation or the ESXi Server. See Tr. 954 – Leedom:

Q. *And in fact, the Altabackup data store previously existed on the ESXi server, correct?*
A. *I don't believe so.*
Q. *Did you review the forensic logs about the data stores on ESXi?*
A. *I did.*
Q. *And did you see that there was a data store for Altabackups previously mounted?*
A. *The only data store Altabackups that I remember seeing is this exhibit here, 1209-7.*

In fact, Mr. Schulte actually executed the mount command for the altabackups countless times in his virtual machine and on the other virtual servers from the ESXi Server—the IRC server, the Doxygen Server—many of these servers also mounted the altabackups. But, once again, Mr. Leedom did not "recall" ever seeing this activity—did he even look for it? And so, without access to a forensic image of the ESXi Server or Mr. Schulte's own Workstation, the defense could not cross-examine Mr. Leedom or present any defense.

The activity and history of the ESXi Server, particularly with respect to the Atlassian VMs was also critical to the case. Mr. Schulte's actions—his continued administration of the ESXi Server also indicated there was no malicious intent with his key; Mr. Schulte was literally continuing to do his job administering that server because there was no one else with the technical ability to do so. But of course, Mr. Leedom did not "recall" or "remember" any of this. See Tr. 1053-54 – Leedom:

Q. *And through your forensic examination I continued to update the ESXi server until I resigned in November, correct?*
A. *I don't understand. Update?*
Q. *I mean I continued to administer the server until I resigned, right?*

A. *You accessed the server until -- I think the server might have been turned off on -- a few days later.*
Q. *A few days later when?*
A. *I don't know if it was the 25th. I think the last entry for off.log was from the 18th, I don't think it was -- was used after. The session -- this April 20th session started on the 15th so that's why there is no entries for the 20th in there but I don't believe -- there is not, like, extra logins for the next six or eight months.*
Q. *No one logged into the ESXi server after April 20th?*
A. *I would have to review the off log. I don't remember.*
Q. *Well, you know the ESXi server was continually used after this point, right?*
A. *When you say "log in", I'm talking about the actual server itself, not logging in through vSphere to make a VM, I am talking about, like, using an SSHT or the root password for the server to log in to the server itself.*
Q. *Right.*
A. *Because you said server, administrate the server. For vSphere? I don't know. I don't remember.*

See also Tr. 1055-56 – Leedom:

Q. *And the ESXi server predated the Atlassian products, correct?*
A. *I don't remember.*
Q. *Through your forensic examination you learned that I retained access keys to multiple other servers, right?*
A. *At this point I only remember the key on the ESX server. I know there were failed logins to the Jira server, to the Stash server.*
Q. *The Doxygen server; through your examination of the Doxygen server you learned I still had my keys for that, right?*
A. *I don't remember.*
Q. *What about the IRC server? Do you remember doing that examination?*
A. *I do remember doing the IRC server. I don't remember when or what the status of your keys were for that.*
Q. *But you were aware up to this point of most of the virtual machines on the server I was administering, correct?*
A. *I don't know if I can speak to what you were administering or what.*
Q. *There were at least 20 or so different virtual machines on the ESXi server, right?*
A. *I believe so.*
Q. *And your testimony is that you don't recall if I continued to administer them or you don't recall -- is that your testimony?*
A. *Yeah. I don't recall, like, A, what administrative actions you were performing to, like, the development servers and -- yeah, that's the main -- that's the main part. Like, I was mostly focused on the Atlassian stuff.*

Mr. Schulte also regularly logged into the ESXi Server with his SSH key and kept his sessions open. Yet Mr. Leedom didn't remember any of this. See Tr. 1052-53 – Leedom:

Q. *And from your forensic examination you confirm that I always logged into the ESXi server using my key, right?*
A. *I don't remember if every single login was SSH only. I just don't remember but I know on the 20th you did -- well, I guess on the 15th you did.*

Access to the ESXi Server would also allow the defense to properly cross-examine Mr. Leedom with respect to Mr. Schulte's user-mode access to vSphere. Mr. Leedom claimed he didn't know what accesses were enabled for Mr. Schulte's user account. And without access to the ESXi Server, the defense could not respond. See, e.g. VII.A.1: Tr. 955-56 – Leedom:

Q. *Well, no. I'm just asking based on this. If you're a regular user, you're not going to have the ability to be creating and mounting directories, right?*
A. *I'm not sure exactly, because there -- I don't think I had, like, audit for the user individually, like, at that level on that server. So I don't know if there's, like, a, you know, an explicit permission for data store management or not. But from the type of error that is shown, it leads me to believe that's more of a -- the NFS server actually denied the request and not the ESXi server saying you don't have the correct permission to, you know, create a data store. It was a -- the NFS server itself said I'm not going to let you do this, if that makes sense.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to the ESXi Server. The defense can then conduct a forensic examination and independent analysis of the government's tests as well as perform tests that the government's own expert refused to perform, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

6. Access to the Altabackup Server

The third and final of the forensic crime scene at the heart of the government's case-in-chief that was never provided to the defense: The Altabackup/FS01 Server. And the most important reason that the defense should have been provided this server was establishing the access controls and content of the various shares—as well as disproving the government's theory that it was used as a “staging” ground for the CIA backups. There would have been decisive, definitive forensic proof if Mr. Schulte ever copied the CIA backups to the Altabackup server.

a) Content and access controls for Altabackup shares

Mr. Leedom could not “recall” any of the access controls or content of the various Altabackup shares. See Tr. 1002 – Leedom:

Q. *So the DevLAN home directories were set up publically, right?*
A. *Home folder, yes.*
Q. *Anyone could copy files to each other's home directories, right?*
A. *I don't remember, like, the exact details. I remember hearing about that but I don't know how regular an occurrence it was.*

See also Tr. 1006 – Leedom:

Q. *As part of your investigation did you review these shares?*
A. *Yes, for what was available.*
Q. *You reviewed the OSB test repo, correct?*
A. *I think for the exact folders, I don't know what all from this list of permissions there were actual folders for, but if there was a folder on the server I reviewed it. I don't remember at this point, it has been a long time. I can only speak to the five folders I think at Exhibit 4 in the presentation. Those, I remember. Outside of that, I don't really remember.*

See also Tr. 1007 – Leedom:

Q. *Each of these directories held copies of Confluence too, correct?*
A. *I don't know.*
Q. *You said you reviewed these directories, right?*
A. *I have never found copies of Confluence.*
Q. *And the OSB test repo or test 00 directory?*
A. *Like I said, I don't remember these other directories.*

See also Tr. 1092-93 – Leedom:

Q. *So your testimony is that you don't know what access his home directory was set to?*
A. *Sitting here today, I don't -- I don't recall the exact permissions. I just know -- I think hearing from Dave that they were -- they were changed. And I'm sure I reviewed them at some point in the past, but I don't remember exactly right now.*

b) The altabackups access controls

Mr. Leedom testified that he believed the altabackup directory contained very strict access controls. This testimony was not based upon a single shred of evidence—to the contrary, Mr. Leedom testified that the access controls were no longer "available." See Tr. 959 – Leedom:

Q. *You would agree that the access controls to Altabackup are critical, right?*
A. *Yes.*

See also Tr. 953:

Q. *So you have no -- you have no ability to testify about what access controls existed on this directory in 2016, is that correct?*
A. *No, because we can use things -- like, when you attempted to mount it on the ESXi server and we saw that that failed, that shows that there was access control enabled on that share.*

Indeed, the CIA's Advanced Forensic Division also determined there were no access controls on the altabackups directory. See DX 101-5 (never admitted at trial):

As such, there was a backup of the Atlassian products on the FIle Share that every DevLAN user had access to. Bottom line: subject pool is every DevLAN user now.

***

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. The defense must have the ability to examine the Altabackup server to conduct its own forensic examination and search for the proof that the altabackup directory was wide-open, that there were various copies of the backups littered throughout the Altabackup server and its various shares, and that there were no access controls for any of these shares. Once again, because the government claimed it did not find any access controls, the defense must be afforded wide latitude to search every single DevLAN device for forensic evidence that the altabackup directory contained no access controls in April and May of

2016. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

7. Timing Analysis

The government experts testified that they believed the information released by WikiLeaks came from one specific backup. While they agreed that, in theory, each and every backup contains all the data from the previous backups, they still held firmly onto their notion that one specific backup file was responsible. Did the government's experts test the subsequent backups to see whether they contained the same material? Of course not—doing so could only jeopardize their "theory." And of course—the defense was not provided any of the subsequent backups, and therefore could not perform these tests. See Tr. 1185 – Berger:

Q. *OK. Slide 44. So all the data from WikiLeaks can be found in every single backup from March 3 through -- from March 3, 2016, through March 6, 2017, correct?*
A. *I can't confirm that, no.*
Q. *You didn't do -- that wasn't part of your analysis?*
A. *I did not look at every single piece of data in every single Confluence backup, no.*

See also Tr. 1188 – Berger:

Q. *Yes, sir. But if a file is deleted, that file is still preserved in the version history, right?*
A. *In Confluence, yes, deleted files are still in the database. However, I don't know that there's not a mechanism to actually expunge a deleted file from the Confluence system.*
Q. *OK. So you've done no analysis to determine whether later backups actually expunge data from previous backups, correct?*
A. *I did not. I don't recall performing that analysis, no.*
Q. *OK. So, if that analysis turned out that no data was expunged, then any later backup would contain all the previous iterations, right?*
A. *If no data was expunged from the system, then yes, theoretically, a later backup would have all the previous backup to date or the previous data to date.*

And why didn't Mr. Berger perform that analysis? Apparently the government "didn't tell him to perform the analysis"—basic, standard analysis that any ***honest*** scientist would perform to test his hypothesis. See Tr. 1188-89 – Berger:

Q. *OK. So why was no analysis of that performed?*
A. *I can't answer that question.*
THE COURT: *Meaning you're not permitted to answer the question, or you just don't have an answer?*
THE WITNESS: *I don't have an answer. I just have the work that I was assigned to look at.*
THE COURT: *So you weren't asked to perform that analysis.*
THE WITNESS: *Correct.*

What kind of scientist doesn't complete his analysis or perform tests that could refute his hypothesis? Only the government—Mr. Berger and Mr. Leedom—had access to all the later backups. Yet, they did not perform the very simple test of taking a later backup and checking whether or not it contained all the data released by WikiLeaks. And worst of all, despite not performing this test—or any test at all that could disprove their hypothesis—they still proffered an "expert opinion" that only the March 3, 2016 backup could have been taken. See Tr. 1007-08 – Leedom:

A. *So I can definitively say that the content posted on March 7 for Confluence came from that March 3rd backup, that specific backup.*
Q. *You found it came from the specific March 3rd backup?*
A. *From my analysis of it; yes, that's my opinion.*
Q. *If WikiLeaks received a March 4th backup they would have the same data, right?*
A. *From what I described I think it is highly likely they have the March 3rd backup.*
Q. *That's not the question, though. The question is backups after March 3rd, March 4th, March 5th, all those backups, WikiLeaks could have those, right?*
A. *Like I said, I don't know exactly what they have.*

See also Tr. 1018 – Leedom:

Q. *You've testified that the backups after March 3 contained the same data, right?*
A. *It could.*
Q. *OK. So you can't say that it had to be -- the command had to be run on March 3, right?*
A. *I think I go a long way to showing that with this part of the presentation. I --*
Q. *If someone on, you know, in December accessed the server and ran this command, it would contain the same data WikiLeaks had, right?*
A. *It could potentially have the data from before.*
Q. *OK.*
A. *It's -- I don't think you'd be able to, you know, make an accurate one-to-one, like, March 3 copy without actually having the March 3 copy to, like, compare from. Just from what was missing in that database, I just don't think there's enough information there.*
Q. *I thought your testimony on direct was that it was possible; it would just take work.*

A. *Yeah, it would be a significant amount of work. I think --*
Q. *That's all I'm asking. It's possible, right?*
MR. DENTON: *Objection, your Honor. Can the witness finish the answer?*
THE COURT: *Sustained.*
Go ahead, Mr. Leedom.
A. *Yeah, and something that would be a big part of that would be, like, having to have that older backup. I think from, like, looking at what we reviewed and that it was clear they tried to get every morsel out of what was in there. So, in my opinion, if they had a later backup, we would see every morsel of what was in there from a later date, not from March 3.*
Q. *That's just your speculation, though, right?*
A. *My opinion.*
Q. *Because, like you said, you don't know actually what files WikiLeaks had, right?*
A. *I don't know exactly what files were on their server, no.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom and Mr. Berger's timing analysis. The defense should have access to every single backup from March 3, 2016 to March 6, 2017 so that it can actually perform the tests that the government refused to perform—and check if those backups contained the very information released by WikiLeaks. The defense could then finally call its own technical expert to rebut Mr. Leedom's and Mr. Berger's timing analysis. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

8. Direct access to Stash and Confluence servers

Due to the timing analysis, it is also critical that the defense have access to the Stash and Confluence servers, to, among other things, check the backup script. While the government claimed there was a character encoding error in the backups, the defense's expert found Unicode in several of the database entries—indicating that there is <u>*no character encoding error*</u>. This was also the finding of the CIA's Advanced Forensic Division. See DX 101-5 (never admitted at trial):

AFD previously assessed it was not possible that the info Wiki had to have come from a backup. As of Friday, that was walked back. The error they thought was in the backup script was not actually there.

So what caused the error in the script? Were all the databases really corrupted? The only way to test the government's theory is to perform a forensic examination of the Stash and Confluence servers.

But there are also numerous other reasons that the defense must have access to the Stash and Confluence servers. For one, the defense can test if the April 16, 2016 snapshot created by Dave and Jeremy Weber accesses the March 3, 2016 backup file—whether that access is a direct byproduct of the snapshot itself. See Tr. 1028-29 – Leedom:

Q. *If they initiated a process or cron job that ultimately touched the March 3, 2016, backup file, it would have been preserved in the snapshot, right?*
A. *Before or after they took the snapshot?*
Q. *Well, before, during.*
A. *If they ran a cron job to -- if they ran a cron job before taking the snapshot -- well, yeah, they didn't do any reversion, so, yes. I don't remember seeing anything like that from my review.*
Q. *The question was just would that be preserved in the snapshot?*
A. *If it happened before the snapshot was taken, yes.*

Confluence Chat was also the primary communication used when taking the server offline—the planned downtime on April 20, 2016 would have been recorded in Confluence Chat. Yet Mr. Leedom either "forgot" or did not even know that service existed. See Tr. 1043-44 – Leedom:

Q. *And in the course of your investigation you learned that there was a chat feature in Confluence, correct?*
A. *I think there was, like, a comment feature.*
Q. *No, I'm talking like instant messaging feature.*
A. *I don't remember an instant messaging feature in Confluence.*
Q. *You don't recall individual users sending messages on the system?*
A. *I know there was an IRC chat on the network.*
Q. *But you don't recall any chat feature that was actually in the web browser for Confluence?*
A. *Not that I remember at this time.*

[…]

Q. *No, I'm talking on DevLAN; through your investigation, did you not learn that there was a global message sent about the Confluence downtime on April 20th?*
A. *No, I don't -- I don't remember.*
THE COURT: *You don't remember at all or you don't remember there being such a message?*
THE WITNESS: *I don't remember there being such a message.*

The Confluence VM also permitted a regular user login—a user with a known, easy password that was never changed on April 16, 2016. Once again, the defense never had access to perform independent analyses or tests, and the government's experts either never performed the tests or "forgot" the results. See Tr. 1061-63 – Leedom:

Q. *And root password is the administrator password, right?*
A. *Yes, it is.*
Q. *But there was also a regular user account called Confluence, right?*
A. *Yes; a service account.*
Q. *And this regular user account also allowed you to log into the Confluence server, correct?*
A. *Yes. I don't remember the exact, like, permission string for it. It's an account that is automatically created when you install Confluence. The Confluence service uses it for things, I don't know what exactly.*
Q. *We can pull up the 1207-11, it is in evidence. So this is the file with both the users, right?*
A. *Yes.*
Q. *The Confluence user password was 123ABCDEF, right?*
A. *I don't remember.*
Q. *You don't remember the password to the Confluence system?*
A. *No.*
Q. *And this password was not changed though, correct?*
A. *I don't remember. I don't look at the before and after.*
Q. *We can look at the others. The other one is 1207-21, right?*
A. *Yes. They look to be the same.*
Q. *It is the same, right?*
A. *Yes.*
Q. *And this password, even though you don't recall it, it would still be reflected in the Confluence, right?*
A. *Are you talking about in the virtual machine?*
Q. *No. I mean, there was OSB's ESXi page on Confluence, correct?*
A. *There was a page, yes.*
Q. *And it contained the accounts for the -- to log in, correct?*
A. *I don't remember if it had the -- I don't remember if it had this password. It might have had a password for the, like -- I'm trying to say the password for the user account, for Confluence on disk. It doesn't necessarily have to be the same as the password for the web service, kind of store it in different places. I also don't ever recall seeing the Confluence account ever like logged into*

like that.
Q. *OK. So you don't recall if the user name and password was on the ESXi page? Is that right?*
A. *ESXi, I don't remember what that password hash resolves to so I don't remember which password that was. I know passwords were stored on that page. I don't know if it is that one specifically.*

And this Confluence regular user could access the altabackup mount. But Mr. Leedom claimed the Confluence user could not access the mount point. So, is the defense compelled to accept Mr. Leedom's incorrect findings or perform independent tests? See Tr. 1063-64 – Leedom:

Q. *OK. And the Alta backups were mounted on the public/mount directory, correct?*
A. *That directory does have permissions. It should be owned by root.*
Q. *The mount directly -- what permissions was it mounted as?*
A. *I believe it was owned by root. I mean, the share was mounted read/write but that folder on Confluence itself, I believe it to be owned by root.*
Q. *But it was mounted with read access, right?*
A. *Yeah, but that doesn't affect the owner. If you are not -- if you logged in as the Confluence user and not the root user, if you tried to access that folder I don't believe you would be able to.*
Q. *Why?*
A. *Because of the ownership permissions of that folder.*
Q. *Well, it doesn't matter who owns it, it matters what is the access controls on the folder, right?*
A. *The access controls on the folder would be the group that owns it, which I believe was the root group.*
Q. *I mean, you can set access controls to be -- to have anyone access that?*
A. *The root user could but not the --*
Q. *In Linux you can configure access controls through a different directory, right?*
A. *Yes, you can.*
Q. *So if you own a directory you can have somebody else access your directory, right?*
A. *If you change the permissions.*
Q. *OK. Do you know what the permissions were set to on that directory?*
A. *I believe it was root root. I believe it was owned by root.*
Q. *But you don't know for sure what it is sitting here, right?*
A. *I want to see the exhibit so I can confirm but that's what I remember.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to forensic images of the Stash and Confluence servers. The defense can then conduct a forensic examination and independent analysis of the government's tests as well as perform tests that the government's own expert refused to perform, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

9. Access to Brual Kangaroo, Nader, and Bartender Source Code

At trial, the government manipulated Mr. Schulte's research and google searches, which were based on his work at the CIA, into something suspicious or malicious. The government cannot classify the work Mr. Schulte was doing for them while simultaneously claiming the underlying research was suspicious or malicious. See Tr. 1193-95 – Berger:

Q. *So knowledge of specifically what type of software I'm writing would be relevant to what Google searches I would be running, correct?*
A. *It could be, yes.*
Q. *OK. And as a general rule, you knew through your investigation that most of the software written was focused on exfiltrating large quantities of data, correct?*
A. *I was not aware of that, no.*
Q. *OK. But these searches are conducted while I'm at work, correct?*
A. *I believe April 18, 2016, was a Monday and they were during what I would consider normal business hours, but I can't confirm whether you were actually at work at that time.*
Q. *OK. 53, these searches are programming-related searches, correct?*
A. *They're related to hashing algorithms, which could be used in programming, correct.*
Q. *I visit specifically multiple programming websites, correct?*
A. *It appears that way, yes.*
Q. *Programmers.stackexchange.com, correct?*
A. *Correct.*
Q. *And I think one of the searches that you didn't identify on direct here at 11:39 a.m. is specifically searches for FNV-1A Cplusplus, right?*
A. *Correct.*
Q. *What is C++?*
A. *It's a programming language.*
Q. *OK. And that's the programming language that I used to write malware at the CIA, correct?*
A. *I can't confirm that, but it wouldn't surprise me.*
Q. *And there's a visit to cplusplus.com, correct?*
A. *Yes.*
Q. *And again, writing hashing algorithms is obviously part of my job at the CIA, correct?*
A. *It could be.*
Q. *OK. I'm going to pull up what's already in evidence as Government Exhibit 407. So start and end dates there are from April 2016 to June 2016, correct?*

***A.** That's what it says, correct.*
***Q.** And this is -- this shows my name at the top, correct?*
***A.** It does.*
***Q.** OK. And the narrative here for the work that was being done during this period, it specifically mentioned thumb drive collection tools, correct?*
***A.** It would seem to indicate that, yes.*
***Q.** Tools to siphon data from various thumb drives and insert it into target computers, correct?*
***A.** Yes, that's what it says.*
***Q.** In which case fast hashing algorithms are critical to ensure the integrity of the collection, correct?*
***A.** Yes.*
***Q.** And it's also critical to ensure that you do not re-collect the same files and waste time, correct?*
***A.** That would be a wise decision, yes.*

Other lines of questioning were not even possible without source code—Eraser Portable could easily be explained with the source code from Brutal Kangaroo and Bartender. Indications that Mr. Schulte was both aware of, and actively used "time stomping" in malware would be obvious in the source code for all three.

The Bartender and Brutal Kangaroo source code would also help the defense counter the MCC charges—by contrasting Mr. Schulte's statements with the specifics in the tools and how it would not be possible to identify the tools based solely on Mr. Schulte's generic statements in his private notebooks.

The government cannot have its cake and eat it too—it cannot claim that Mr. Schulte's Google searches and research were suspicious and malicious while simultaneously refusing to provide the source code and underlying software requirements that necessitate that very research.

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to the Brutal Kangaroo, Nader, and Bartender source code. The defense can then conduct a forensic examination and independent analysis of the government’s tests as well as perform tests that the government’s own expert refused to perform, and present an expert to rebut both Mr. Leedom’s and Mr. Berger’s testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government’s case.

10. Access to Offsite backups

The offsite backup contained the exact same backups as those hosted on the Altabackup server. If WikiLeaks received a backup file as the government claims, it is equally likely it came from either DevLAN or the Offsite Backup. But the government never provided a single record in discovery from the Offsite Backup—no security mechanisms, access controls, the number of people who had access, literally nothing. And Mr. Leedom did not include anything about the Offsite Backup in his presentation. See Tr. 990-91 – Leedom:

Q. *I want to talk to you now about the CIA's offsite backup. Backups from the Altabackup server were regularly taken off DevLAN and moved to an offsite backup, correct?*
A. *From what I understand, yes.*
Q. *All the backups were stored at the offsite backup, right?*
A. *The offsite backups were stored there, yes.*
Q. *And it is possible that WikiLeaks received the backup file from the CIA's offsite backup, correct?*
A. *I disagree.*
Q. *All right. Well, let's pull up what is in evidence as Government Exhibit 602 and this is page 2 of the document. Do you see the offsite backup site?*
A. *Yes.*
Q. *WMA storage; right?*
A. *Yes.*
Q. *Backups from the Altabackup server were regularly taken off DevLAN and moved to the offsite backup, right?*
A. *Yes.*
Q. *Did you conduct a forensic examination of the offsite backup?*
A. *Yeah, we had a -- I think we had a copy of that as well.*
Q. *No. Did you conduct a forensic examination of the site?*
A. *I have never been to the site.*
Q. *So no.*
A. *I can't really speak to the collection at the site because I didn't, like there is a cart -- the FBI forensics thing. I know that, like, reviewing, like, I had access to review the data stored from*

there but as far as specific questions for seizures, things like that at the site, physical stuff, I can't really speak to.

See also Tr. 992 – Leedom:

***Q.** You don't present any of that in your presentation though, right?*
***A.** No. From what I understand it either, like, was an identical match to the data that we had or there wasn't any evidence of that type of thing over there.*
***Q.** Would your analysis be any different if the backups were taken from the offsite backup?*
***A.** If I was showing -- I would be showing something kind of similarly, like maybe an access time but I don't remember, honestly -- six years later now -- I don't remember the exact security requirements for accessing that site. I don't know if you could even, like, access the files that were there without physically being there. I don't remember.*

See also Tr. 1190 – Berger:

***Q.** OK. But forensically, you can't say whether or not WikiLeaks received a backup from the offsite backup, correct?*
***A.** I was not part of any analysis looking at offsite backups. I'm not aware of how they were stored or access control or anything like that.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to forensic images and discovery about the Offsite Backup. The defense can then conduct its own forensic examination, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

11. Access to Jira and Hickok

Similarly, COG also had direct access to the altabackups through Jira and Hickok. Anyone from COG simply needed to log into Jira to access the altabackups. But of course, Mr. Leedom could not confirm this because he did not "remember." See Tr. 994 – Leedom:

***Q.** I am just asking if Jira mounts the Altabackups.*
***A.** I know there are backups from Jira in Altabackup.*
***Q.** And it needs access to Altabackups so it can store the Jira backups, right?*
***A.** You can technically, like, SSH in and move them down. I don't know the frequency of the backups from Jira, I don't recall at this time so I don't know if it was something that were moved down over SSH or if it was set up in the same automated way that the other services were set up.*

I just don't recall at this point.
Q. *Would Jira connect directly to the Altabackup server, right?*
A. *I can't say. Other than the fact that there are backups from Jira there I can't say the exact connection.*

See also Tr. 996 – Leedom:

Q. *And in the history files there there were -- it showed that the Jira mounted Altabackups, right?*
A. *I don't remember.*

See also Tr. 998 – Leedom:

Q. *So I guess your testimony is essentially you don't remember or you don't know anything about the Jira setup?*
A. *Aside from what we just reviewed and the Jira backups that there are some Jira backups, I can't speak to the server configuration.*
Q. *That server configuration would have been very important in your forensic examination, right?*
A. *Yes.*
Q. *And you don't remember anything about it now?*
A. *No.*

See also Tr. 997 – Leedom:

Q. *Based on your forensic knowledge of the way the systems were set up, COG could have access to the Altabackup server, right?*
A. *I disagree from the -- it's hard for me to say without having reviewed Hickok and the logs. All I can really speak to is the configurations, like, since I can't confirm the mount for Altabackup on the time. I know that those backups were there. Whether they were there over NFS from the share or whether they were, like, moved down over SSH is kind of all I can really speak to. If it was mounted to Altabackup and you could SSH into it, then.*

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to forensic images and discovery about the Jira-Hickok connection. The defense can then conduct its own forensic examination, and present an expert to rebut Mr. Leedom’s testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government’s case.

12. Access to networking equipment and setup of international locations

Mr. Leedom recognized that DevLAN was a juicy target for hostile intelligence services. See Tr. 1000 – Leedom:

***Q.** I mean, do you know that adversaries to the United States try cyber operations against the United States?*
***A.** Yeah. In a general sense, yes.*
***Q.** And it is not unreasonable to think a foreign intelligence service might want access to DevLAN, correct?*
***A.** DevLAN or other classified networks I'm sure.*

Yet, Mr. Leedom did not even investigate this equally likely possibility—that DevLAN was exploited by a hostile foreign intelligence service that exfiltrated the data. I*d.*:

***Q.** So if they breached DevLAN through these connections they would have the ability to copy the backups, right?*
***A.** I can't really speak to that.*
***Q.** You can't speak to the fact if they are able to breach DevLAN whether they would have access to information on DevLAN?*
***A.** Well, I can't speak to the -- I don't know how anything about how that connection was set up, so.*

And this is not some crazy, obscure alternate theory—the CIA itself recognized the inadequacies and overall insecurity on the DevLAN Network. See GX 5001 at 3:

> *Day-to-day security practices had become woefully lax. The Development Network (DevLAN) on which CCI's work product resided had been certified and accredited, but CCI had not worked with CIMC to develop or deploy user activity monitoring or robust server audit capability. Most of our sensitive cyber weapons were not compartmented, users shared systems administrator-level passwords, there were no effective removable media controls, and historical data was available to users indefinitely. Furthermore, CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed. These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security.*
>
> *While CIA was an early leader in securing our enterprise information technology (IT) system, we failed to correct acute vulnerabilities to our mission IT systems. Because the stolen data resided on a mission system that lacked user activity monitoring and a robust server audit capability, we did not realize the loss had occurred until a year later, when WikiLeaks publicly announced it in March 2017. Had the data been stolen for the benefit*

> *of a state adversary and not published, we might still be unaware of the loss—as would be true for the vast majority of data on Agency mission systems.*

And yet, it was not part of Mr. Leedom's forensic examination? Mr. Leedom did not even consider this possibility? See Tr. 999 – Leedom:

Q. Each of the foreign offices has a system that's connected to DevLAN, right?
A. I can't speak to the configuration. I know we received evidence from the foreign offices. That's really the extent of the foreign offices that I can speak to.
Q. This connection is established over the Internet, right?
A. I don't know, I can't -- I can't speak to the actual, like, network connection.
Q. You did not conduct a forensic examination of the system in the foreign office?
A. The work station? It was connected to DevLAN.
Q. You are saying that you don't know how this -- how it was configured?
A. I don't know how the networking configuration from DevLAN to the foreign office is set up. I just know that -- and from what I have been told and what we received from evidence from the office that there were some workstations connected to DevLAN from the location.
Q. So you don't know if this -- these connections were misconfigured or otherwise insecure, right?
A. I can't speak to the actual connection.

And this is precisely why the judicial system in the United States requires an adversarial system—if the defense were required to depend upon the government's experts, then many people would be wrongly convicted simply because the government did not want their expert to examine other possibilities—just as occurred here. The government did not want Mr. Leedom to conduct a comprehensive forensic examination; instead, they directed him to what they wanted him to say, and then paid him substantially to do so. If indeed the Russians exploited DevLAN, and evidence of this exists on the seized networking devices, how could the defense ever discover this exculpatory evidence? Or the government for that matter? How can Mr. Schulte have a fair trial when the government actively avoided, ignored, and concealed any and all forensics that could have exonerated Mr. Schulte?

In accordance with the adversarial system of justice, the Due Process Clause of the Fifth Amendment, and the Confrontation Clause of the Sixth Amendment, the defense should have the

opportunity to challenge Mr. Leedom. In order to do so, the defense requires access to forensic images and discovery about the DevLAN-international connection. The defense can then conduct its own forensic examination, and present an expert to rebut Mr. Leedom's testimony. But without access to these critical and clearly material resources, the defense cannot challenge the government's case.

13. Defense gave the government its most important piece of evidence because it could not conduct its own tests

Finally, it should be noted that, due to the government's refusal to provide reciprocal access to the digital forensic crime scene, the defense's expert was compelled to turn over attorney-client privilege work product and strategy, including proposed tests. Through this absurd situation, the defense requested the government to perform certain tests that the government's experts did not think to run, ultimately resulting in the government's favorite exhibits—GX 1207-27 and 1207-30. If the defense were given appropriate access to the digital forensic crime scene, the defense's expert would not have revealed to the government these exhibits.

In essence, the government required any and all defense experts to work for them, and provide them their work product, strategy, and other privileged information. There is no other case in the history of the United States where such an arrangement was required.

14. Summary: A Manifest Injustice: Forcing the defense to depend entirely upon a government advocate in lieu of independent analysis [stymied]

In every other case involving digital forensics, the government provided the defense with the entire forensic crime scene—especially the computers and servers at the center of its prosecution. Computer fraud and abuse, computer hacking, exploitation—in every single case the government turned over the complete forensic images; never once did they claim that such images were "government files" that the defense was not permitted to review.

Yet, in the instant case, and for the first time in the history of the United States—the government asserts that computer forensics should not be treated like forensic science. The government asserts that computers and other electronics recovered at a crime scene are "government files" to which the defense is not permitted to conduct independent analysis and review. Instead, the defense must accept the government's expert's technical opinion as fact. The defense cannot use the technical experience and expertise of its own expert—but must rely entirely upon the government.

An analogy of these circumstances in the realm of forensic sciences would be the following: The government recovered forensics from a crime scene—hair, fingerprints, DNA. But, instead of testing the forensics—they pick and choose a few samples to test, and rely exclusively on circumstantial evidence. The defense demands access to the forensics to conduct their own tests on all the recovered evidence—but the government claims the defense cannot "search through the government's files." The defense never receives any of those forensics and proceeds to a "trial" where the defense loses. Throughout this time the forensics exonerates the defendant—it is someone else's hair, fingerprints, and DNA at the crime scene. But the defense never had the chance to discover and review it. The defendant goes to jail. Is this justice?

Every step of the way in this case the government either (i) did not even perform certain tests, (ii) forgot the results, or (iii) arrived at incorrect conclusions. The government's experts are not infallible. This Court cannot compel the defense to accept all the government expert's testimony and tests as truth. Why else did the Supreme Court find that the defense must have access to its own expert? Was it so that expert could sit on the sidelines and tell the defense he cannot testify about anything since he was never given access? Is it just a rubber stamp? Did the Supreme Court intend to require an expert for the defense but not actually require the government to provide him materials to actually review and apply his expertise? To actually conduct independent tests? Or was the intent to kill the adversarial system of justice?

Indeed, the government experts knew all they had to say was the three magic words: "I don't remember" and all cross-examination would immediately halt. In no other case in the history of the United States has a defendant been forced to accept the government's expert's analysis and forced to forego equal access and analysis by his own expert. Mr. Schulte's defense, his freedom, his very life depended upon the expert analysis and conclusions of a government expert—no, a government advocate. This is as far from justice as it can possibly get.

And the fact that the forensics were "classified" has absolutely no bearing on discovery under Rule 16. CIPA does not nullify Rule 16, the Fifth, or the Sixth Amendments. Indeed, the Supreme Court "make[s] clear that the privilege can be overcome when the evidence at issue is material to the defense." *United States v. Aref*, 533 F.3d at 79; See also *United States v. Fernandez*, 913 F.2d 148 (4th Cir. 1990) ("A finding that particular classified information is necessary to the defense is enough to defeat the contrary interest in protecting national security.").

"Were it otherwise, CIPA would be in tension with the defendant's fundamental constitutional right to present a complete defense." *United States v. Fernandez*, 913 F.2d at 154; "Few rights are more fundamental than that of an accused to present witnesses in his own defense." *Chambers v. Mississippi*, 410 US 284, 302 (1973). "Any rule that impedes the discovery of truth in a court of law impedes as well the doing of justice." *Hawkins v. United States*, 358 US 74, 81 (1958) (concurring opinion). The Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense, and "the right to present a defense... is a fundamental element of due process of law", *Washington v. Texas*, 388 US 14, 19 (1967).

Pursuant to Rovario, "[i]f the evidence is discoverable but the information is privileged, the court must next decide whether the information is helpful or material to the defense, i.e., useful 'to counter the government's case or to bolster a defense.'" *Id.* (quoting *United States v. Stevens*, 985 F.2d at 1180). "To be helpful or material to the defense, evidence need not rise to the level that would trigger the Government's obligation under *Brady v. Maryland*, 373 US 83 (1963), to disclose exculpatory information." *Id.* "[I]nformation can be helpful without being 'favorable' in the Brady sense." *United States v. Mejia*, 448 F.3d 436, 457 (D.C. Cir. 2006).

The necessity and relevance of the forensic images easily defeats the classified nature of the discovery. There can be no question that the forensic images of the three servers are fundamental to the government's case and critical to the defense. The defense must be permitted unfettered access to the forensic images of the alleged crime scene to properly prepare a defense—just as the government relied upon the forensic images to further its prosecution.

Mr. Schulte must have access to the forensics to testify as an expert

Mr. Schulte has a Fifth and Sixth Amendment right to review the very computers and servers that are the centerpiece to the government's case-in-chief. In no other case in the history of the United States has any defendant ever been denied access to review the evidence against him. But the very few items that the government "turned over" to the defense in "discovery," Mr. Schulte was not permitted to review because they were maintained at the CIA. Mr. Schulte has a right as the defendant, the lawyer, and a technical expert to review these materials directly. The government's chief technical expert, Mr. Leedom, had not even graduated college by the time Mr. Schulte was already working and gaining significant experience in the field. Mr. Schulte's expertise far eclipses both Mr. Leedom and Mr. Berger. Indeed, Mr. Schulte setup the majority of the computers and servers that constitute the government's case-in-chief; he possesses substantial significant technical knowledge that he alone possesses which could be profoundly beneficial to his own defense—and he is not permitted to contribute?

Mr. Schulte had a right to testify as an expert, but could not review the forensics and therefore could not do so.

In fact, as a defendant, he could not testify at all as a result of his inability to review the forensics. His testimony as to his actions in April of 2016 required technical proof—proof that could be provided to the jury. There was no reason it cannot be provided in SCIF to the defendant. And, the government did not provide a CIA witness to explain badge records.

15. The government must produce the discovery in the Southern District of New York

Makes it impossible to review for expert, lawyers, and Mr. Schulte. It was the government that moved to relocate the case from the E.D.VA. And it cannot punish Mr. Schulte for its own request by making it difficult for the defense to review discovery.

Q. And you testified they tried to get every morsel of data out of March 3, right?
A. My opinion.
Q. Right. So if they had a later backup and they restricted themselves to March 3, it would be the same, right?
A. Well, if you're restricting yourself, you're not getting every morsel out of it.
Q. Well, you'd get every morsel out of the March 3 data, right?

Q. The data released by WikiLeaks is contained in this file, correct?
A. I can't speak to that specific file. I don't know if I reviewed that specific file. Like I said, I did more Confluence review and less of a Stash review, but.

Expert could not testify, could only testify that he did not have access to any forensic images, and particularly any of the information given to government experts Leedom and Berger

Access controls (esp. altabackups); predicated access controls critical for count 1, 5, 6, 7

We cannot have access to all the backups to conduct our own timing analysis, but their own experts don't do the test and simply say they do not know whether or not later backups contain all the data from previous backups.

Specifically, when I crossed Mr. Leedom on the access controls of the Altabackup server, he continually claimed that none existed. But I could not cross him further because the Altabackup server was not provided to the defense.

When I crossed Mr. Leedom on the access controls to Dave's home directory, he claimed that Dave told him there were access controls. Despite requesting the access controls for the Altabackup server repeatedly, the government never produced them in discovery. Accordingly, I could not cross Mr. Leedom further.

When I crossed Mr. Leedom on whether the confluence user could access the Altabackups mount point, he claimed the user could not. Once again, the government never produced the Confluence VM to the defense, so I could not cross Mr. Leedom further.

Repeatedly, the government tech witness realized they can make any assertion or conclusion they want without reprecussions. Since the defense was not provided any of the forensics, they know any answer they give is not subject to cross-examination.

They can also claim that they do not remember. For example, Mr. Leedom said he did not remember anything about the offsite backup, the offsite locations, or the COG network, but was sure there was nothing important there. So, once again, there was no possible cross-examination. The defense was not provided access to any of these sites or networks, and therefore cannot properly cross-examine the witness.

It's not some remote possible, it's as equal an opportunity as any other possibility. What computer scientist or investigator does not conduct a necessary test or examination because he's afraid it may disprove his hypothesis? Mr. Berger and Mr. Leedom's testimony was not only irresponsible, but unethical and [against their profession]; should be fired.

B. Access to AFD reports and personnel

The CIA's Advanced Forensics Division (AFD) conducts forensic examinations and investigations into all CIA leaks. Mr. Schulte himself has been a part of multiple AFD consultations, and has read the reports that AFD releases based on its analyses and recommendations. Mr. Schulte specifically moved for these reports on September 14, 2021. See Dkt. 504. Specifically, lead FBI Agent Evanchec referenced at least two distinct AFD reports in a Lync message he sent to a colleague (See DX-101-5)

> Couple things: 1. AFD previously assessed it was not possible that the info Wiki had to have come from a backup. As of Friday, that was walked back. The error they thought was in the backup script was not actually there. As such, there was a backup of the Atlassian products on the File Share that every DevLAN user had access to. Bottom line: subject pool is every DevLAN user now. This may be significant in terms of PC for future warrants.

According to this Lync Message, there were at least two AFD assessments—one that indicated the information from WikiLeaks must have come from a backup, and a second that determined there was no error in the backup script, and the file share (presumably Altabackup) of the backups was accessible by every DevLAN user. Access to these AFD reports would have been critical to Mr. Schulte's defense. Yet, the government deliberately concealed them—and continues to do so. Mr. Schulte has seen the exact type of reports AFD generates based upon his own experience and consultation with AFD on previous leaks—he has direct knowledge that these reports exist, which is only conclusively corroborated by FBI Agent Evanchec's Lync Message

The government responded to the September 14, 2021 letter on November 15, 2021, Dkt. 591:

> With respect to materials from AFD, the Government has re-confirmed, as it previously informed defense counsel, that no such forensic report exists

So Mr. Evanchec just fabricated that entire Lync Message? The government doesn't want to produce the AFD reports to the defense because they are damning to the government's case—and there is no chance anyone will ever find out that they've concealed the reports since they're classified and safely at the CIA (or already destroyed).

Mr. Schulte sent multiple further letters requesting production of the concealed AFD Reports. See Dkt. 605, 644. 661, and even tried to involve the Second Circuit with an interlocutory appeal to compel a Brady hearing and testimony from CIA AFD personnel that was dismissed. See *United States v. Schulte*, 21-3125, Second Circuit.

The Court also quashed Mr. Schulte's subpoena of CIA AFD personnel with direct knowledge of their reports and forensic findings.

The government's concealment of the AFD reports and prevention of AFD personnel testifying about these reports constitutes malicious prosecution and an unconscionable abuse of power. There can be no question that these reports and testimony were both relevant and helpful to the defense—especially considering the reports revealed accurate information that directly refuted the government's technical experts; AFD would have testified that the Altabackups were not locked down, but were accessible by every DevLAN user, and that there was no character encoding error in the output from the backup script. Only the government knows what other exculpatory reports and evidence exist in those AFD reports.

C. Mr. Denton's false, prejudicial statements during rebuttal require a new trial

Yes / No / Maybe?

1. Falsely claimed Mr. Schulte "admitted" to committing the crime

Mr. DENTON: *…In some respects the evidence of transmission is the fact that someone outside of this secure building has this stuff. And so once you know that he stole it, and you know that because he has admitted what he did on April 20th and you know there is no other explanation for it --*
MR. SCHULTE: *Objection.*
THE COURT: *Overruled.*
MR. DENTON: *-- the fact that WikiLeaks has it proves that he transmitted it.*
(Tr. 2277 – Rebuttal)

The Court allowed Mr. Denton to tell the jury that Mr. Schulte admitted to committing the crime. Mr. Schulte did not testify. As the Court made clear throughout the trial, nothing Mr. Schulte said acting as an attorney could be considered evidence. If Mrs. Shroff or Mrs. Colson had made the same arguments, Mr. Denton could not have claimed that Mr. Schulte admitted anything. Yet, the Court's decision to permit Mr. Denton to tell the jury that Mr. Schulte admitted committing the crime—admitted *anything* constitutes clear abuse of discretion and requires a new trial. See Tr. 59:

THE COURT: Second, Mr. Schulte is representing himself which means that anything he says in that capacity is not evidence. Just as what the lawyers say, the questions they ask, the objections they make are not evidence, the same is true of Mr. Schulte. Any question that he asks, any objection that he makes, anything that he says in his opening statement or his closing, that is not evidence.

2. Falsely equated server administrator access with altabackups access controls to confuse the jury

And he also told you just a moment ago why being an administrator mattered. He spent a while talking about the Altabackups saying there were no user permissions, no user controls on the Altabackups, anybody could get there. But then he started talking about that time when he tried to get to the Altabackups and it didn't work. His answer was, well, of course it didn't work, I wasn't an administrator, I was using my regular user account.

Exactly. A regular user can't get to those Altabackups, you have got to be an administrator which, by the way, puts the lie to his whole claim that there were no access controls whatsoever on the Altabackups. He told you there were, only administrator could get there. That's access control. Not every regular person could get to it, not anyone could get into that folder and steal backup files. (Tr. 2270-71 – Rebuttal).

Mr. Denton tried to confuse the jury by conflating server permissions with directory access controls. In order to mount ***any*** directory, the user must be an administrator *on the server from which the command is executed*. This has nothing to do with the altabackups directory. If a regular user tried to mount the home directory that had zero access controls, then that command would also fail. If a regular user tried to mount any directory, then the command would fail; and the command fails because the regular user does not have the authority to execute the **mount command** on the server. The failure says nothing about access controls on the directory.

3. Falsely claimed character encoding error indicated March 3rd backup was taken

MR. DENTON: And when we focus on those backup files there is an important piece of forensic evidence that you didn't hear word one about from Mr. Schulte, which is the forensic analysis that Mr. Leedom did on that error in the backup script, the character and coding problem that meant that the database was broken, that those links between different parts of it didn't match up quite right. That's why the version of Confluence that's on WikiLeaks looks so strange in many respects, it is directly tied to that error in the script. And what does that error do? It means that you can't use a different version, you can't make March 4th look like March 3rd because those relationships are broken. You can't do it as a different version and so it is that backup file, that March 3rd backup file that you know was the one that was stolen and put on WikiLeaks. (Tr. 2272-73)

4. Falsely claimed Mr. Schulte worked next to the bathroom

I worked in the middle of the vault, not near the bathroom—there is no evidence on the record that I worked next to the bathroom.

D. Constant reminders to the jury that what Mr. Schulte says is not evidence

He did not tell the jury that both my statements and the governments were not evidence.

E. Requirement for CIPA 5 Notice of AFD while the government refused to provide the AFD reports in discovery

IX. CONCLUSION

For these reasons, this court should enter a judgment of acquittal on all counts. Alternatively, the Court should order a new trial.

Dated: New York, New York

January 12, 2023

Respectfully Submitted,
/s/ Joshua Adam Schulte
Joshua Adam Schulte
Metropolitan Detention Center
P.O. Box 329002
Brooklyn, NY 11232